

GEOMETRIC CHARACTERIZATION OF STRONGLY NORMAL EXTENSIONS

JERALD J. KOVACIC

ABSTRACT. This paper continues previous work in which we developed the Galois theory of strongly normal extensions using differential schemes. In the present paper we derive two main results. First, we show that an extension is strongly normal if and only if a certain differential scheme splits, i.e. is obtained by base extension of a scheme over constants. This gives a geometric characterization to the notion of strongly normal. Second, we show that Picard-Vessiot extensions are characterized by their Galois group being affine. Our proofs are elementary and do not use “group chunks” or cohomology. We end by recalling some important results about strongly normal extensions with the hope of spurring future research.

INTRODUCTION

In [17] we developed the theory of strongly normal extensions using tensor products and differential schemes. The present paper continues that work.

Let \mathcal{F} be a differential field of characteristic 0 with algebraically closed field of constants \mathcal{C} . Let \mathcal{G} be a finitely differentially generated extension of \mathcal{F} . The central idea of [17] is to study $\mathcal{P} = \mathcal{G} \otimes_{\mathcal{F}} \mathcal{G}$ and $P = \text{diffspec } \mathcal{P}$. One of the more important results is that if \mathcal{G} is strongly normal over \mathcal{F} , then P splits. This means that P , as a differential scheme over $G = \text{diffspec } \mathcal{G}$, is obtained by base extension from a scheme over $C = \text{spec } \mathcal{C}$.

The first few sections briefly summarize some needed results from [17] and then we prove our first main result. We show the converse of the above, i.e. if \mathcal{G} has field of constants \mathcal{C} and P splits, then \mathcal{G} is strongly normal over \mathcal{F} . This gives a geometric interpretation to the notion of strongly normal extension.

Kolchin and Lang [13] give a different characterization, namely that there exists a model for the field extension \mathcal{G} over \mathcal{F} which is a torsor (principal homogeneous space) for the Galois group. The proof requires use of Weil’s “group chunks” (as extended by Rosenlicht [24]). In [17] we were able to avoid use of this device. Here too we do not use it.

Next we describe the Picard-Vessiot theory for partial differential fields. We need to do this since most treatments in the literature restrict themselves to ordinary differential fields. This is unfortunate. There is little added difficulty in treating the partial case. Also, one can find in the literature at least six different definitions of Picard-Vessiot extensions, thus one is almost forced to restate the definitions in every paper. We choose the one from Kolchin’s book [11].

Received by the editors December 12, 2003 and, in revised form, September 19, 2004.

2000 *Mathematics Subject Classification.* Primary 12H05, 12F10; Secondary 14A15, 14L15.

©2006 American Mathematical Society
 Reverts to public domain 28 years from publication

Our goal is not to give yet another presentation of Picard-Vessiot theory, so our treatment is brief. Instead we concentrate on proving our second main theorem. It states that a strongly normal extension is Picard-Vessiot if and only if its Galois group is affine. This was first shown by Kolchin ([9, Theorem 2, p. 891]). However, his proof requires knowing that Galois cohomology of the general linear group is trivial and that this implies that the rational cohomology is also trivial. Our proof is more elementary; it relies on a few simple theorems about almost constant differential rings from [17, Section 5, p. 4482].

Examples of strongly normal extensions are not easy to find. Picard-Vessiot extensions are certainly strongly normal. There is only one other *explicit* example in the literature, namely Example 2.7. The reason for this may be because the theory has not yet been extensively studied. We hope that this paper, and its predecessor, will encourage further research.

To that end, we summarize some important results in the last few sections. The Chevalley-Barsotti theorem (Proposition 12.2) leads to a tower of Δ -fields consisting of a finite (Galois) extension, a Picard-Vessiot extension, and one generated by abelian functions. Thus a strongly normal extension decomposes into three parts, two of which have been extensively studied.

There is a “factory” for creating strongly normal extensions: the logarithmic derivative. In Section 13 we give the definition and state results. Unfortunately the references for these results use Weil style algebraic geometry; they await modernization. The next section applies this to the case of hyperelliptic Jacobians.

In Section 15 we state Kolchin’s theorem which asserts that every connected algebraic group is the Galois group of some strongly normal extension. Thus strongly normal extensions are abundant. Unlike Picard-Vessiot extensions, however, one cannot simply start with a (non-linear) differential equation and produce a strongly normal extension. The first Painlevé transcendent gives a counterexample. There has been some work to determine what property of a differential equation ensures that a solution is contained in a strongly normal extension. We give some references in Section 15.

1. NOTATION

We assume familiarity with [17]. For the basic notions of differential algebra, see Kolchin [11], Kaplansky [5], Magid [18] or van der Put-Singer [29]. Except for [11] and an appendix of [29], these books restrict themselves to ordinary differential fields. We do not. The bibliography in [29] is especially recommended; it has almost 300 entries. For the Galois theory of strongly normal extensions we use the methods and notation of [17]. For more information about `diffspec` see [16].

The set of (commuting) derivation operators is denoted by $\Delta = \{\delta_1, \dots, \delta_m\}$. The free commutative monoid on Δ is denoted by Θ , thus an element $\theta \in \Theta$ has the form $\theta = \delta_1^{e_1} \cdots \delta_m^{e_m}$ for some (unique) $e_i \in \mathbb{N}$. The “identity derivation operator” ($e_i = 0$ for all i) is denoted by 1.

We use the prefix Δ in lieu of the word “differential”, e.g. Δ -ring, Δ -ideal, Δ -field. The ring of constants of a Δ -ring \mathcal{R} is denoted by \mathcal{R}^Δ . Throughout this paper, \mathcal{F} is a fixed Δ -field of characteristic 0 with algebraically closed field of constants $\mathbb{C} = \mathcal{F}^\Delta$, and \mathcal{G} is a finitely Δ -generated extension of \mathcal{F} .

All Δ -rings are assumed to be algebras over \mathcal{F} , or over \mathbb{C} if they are rings of constants. In particular all Δ -rings are Keigher rings ([16, Definition 2.3, p. 73]),

in fact even Ritt algebras. The following symbols will be used frequently in what follows:

$$\mathcal{P} = \mathcal{G} \otimes_{\mathcal{F}} \mathcal{G}, \quad P = \text{diffspec } \mathcal{P},$$

and

$$G = \text{diffspec } \mathcal{G}, \quad F = \text{diffspec } \mathcal{F}, \quad C = \text{diffspec } \mathcal{C} = \text{spec } \mathcal{C}.$$

2. STRONGLY NORMAL EXTENSIONS

Definition 2.1. By a Δ -isomorphism σ of \mathcal{G} over \mathcal{F} we mean a Δ -homomorphism (necessarily injective) of \mathcal{G} into some Δ -extension of \mathcal{G} with $\sigma|_{\mathcal{F}} = \text{id}$.

Definition 2.2. Let σ be a Δ -isomorphism of \mathcal{G} over \mathcal{F} . Define

$$\begin{aligned} \bar{\sigma}: \mathcal{P} &\rightarrow \mathcal{G}[\sigma\mathcal{G}] \quad \text{by} \quad \bar{\sigma}(a \otimes b) = a\sigma b, \quad \text{and} \\ \mathfrak{p}_{\sigma} &= \ker \bar{\sigma}. \end{aligned}$$

Evidently \mathfrak{p}_{σ} is a prime Δ -ideal of \mathcal{P} . By [17, Proposition 6.4, p. 4485], every prime Δ -ideal of \mathcal{P} is of this form.

Definition 2.3. Let \mathcal{G} be a finitely Δ -generated extension of \mathcal{F} . Then \mathcal{G} is *strongly normal over \mathcal{F}* if every Δ -isomorphism σ of \mathcal{G} over \mathcal{F} satisfies

- (1) $\sigma|_{\mathcal{G}^{\Delta}} = \text{id}$ and
- (2) $\mathcal{G}\sigma\mathcal{G} = \mathcal{G}\mathcal{C}(\sigma) = \sigma\mathcal{G}\mathcal{C}(\sigma)$, where $\mathcal{C}(\sigma) = (\mathcal{G}\sigma\mathcal{G})^{\Delta}$.

It follows by [17, Proposition 12.2, p. 4489] that $\mathcal{G}^{\Delta} = \mathcal{C}$.

Proposition 2.4. Suppose that $\mathcal{G}^{\Delta} = \mathcal{C}$ and that every Δ -isomorphism σ of \mathcal{G} over \mathcal{F} satisfies

$$\sigma\mathcal{G} \subset \mathcal{G}\mathcal{D}_{\sigma},$$

where \mathcal{D}_{σ} is some field of constants. Then \mathcal{G} is strongly normal over \mathcal{F} .

Proof. [17, Proposition 12.15, p. 4490]. □

Definition 2.5. If \mathcal{G} is strongly normal over \mathcal{F} , the group of all Δ -automorphisms of \mathcal{G} over \mathcal{F} is called the *Galois group of \mathcal{G} over \mathcal{F}* and is denoted by $\text{Gal}(\mathcal{G}/\mathcal{F})$.

By [17, Corollary 14.4, p. 4494], $\sigma \in \text{Gal}(\mathcal{G}/\mathcal{F})$ if and only if \mathfrak{p}_{σ} is a maximal Δ -ideal. Thus $\text{Gal}(\mathcal{G}/\mathcal{F})$ is canonically identified with the set of closed points of P .

In the following simple examples we restrict our attention to ordinary Δ -fields ($m = 1$) and denote the derivation by $'$.

Example 2.6. Picard-Vessiot extensions are strongly normal. For the case of partial Δ -fields see Proposition 6.2. Here we define \mathcal{G} to be a Picard-Vessiot extension of \mathcal{F} if

- (1) $\mathcal{G}^{\Delta} = \mathcal{C}$,
- (2) $\mathcal{G} = \mathcal{F}\langle\omega\rangle$, where $\omega = (\omega_1, \dots, \omega_n)$ is a fundamental system of solutions of a linear homogeneous differential equation

$$L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \dots + a_0y = 0.$$

Let σ be a Δ -isomorphism of \mathcal{G} over \mathcal{F} into some Δ -extension field \mathcal{E} of \mathcal{G} . ω is a fundamental system of solutions of $L(y) = 0$ in \mathcal{E} , and each $\sigma\omega_i$ is also a solution of $L(y) = 0$. Therefore $\sigma\omega_i$ is a linear combination $\omega_1, \dots, \omega_n$ over $\mathcal{D}_{\sigma} = \mathcal{E}^{\Delta}$. By Proposition 2.4, \mathcal{G} is strongly normal over \mathcal{F} .

The Galois group of \mathcal{G} over \mathcal{F} is affine, and therefore isomorphic to a subgroup of $\text{GL}_{\mathcal{C}}(n)$. See also Proposition 6.7.

Example 2.7. Elliptic extensions are strongly normal. Let $E \subset \mathbb{P}^2$ be the non-singular elliptic curve with Weierstraß equation

$$Y^2Z = X^3 + a_4XZ^2 + a_6Z^3, \quad a_4, a_6 \in \mathbb{C}.$$

Here we are using the notation of Silverman [25, Section 1, p. 46].

Definition 2.8. A Δ -extension field \mathcal{G} of \mathcal{F} is *elliptic* if

- (1) $\mathcal{G}^\Delta = \mathbb{C}$,
- (2) $\mathcal{G} = \mathcal{F}\langle\eta\rangle$, where $\eta'^2 = \alpha^2(\eta^3 + a_4\eta + a_6)$ for some $\alpha \in \mathcal{F}$.

If $\mathcal{F} = \mathbb{C}(z)$, with $z' = 1$, then $\mathcal{F}\langle\wp(\frac{1}{2}z)\rangle$ is an example (with $\alpha = 1$). Kolchin [8, section 6, p. 227] generalizes our definition to partial Δ -fields, however for him the coefficient of X^3 is 4 and he calls the element η *Weierstrassian*.

Let σ be a Δ -isomorphism of \mathcal{G} over \mathcal{F} , $\sigma \neq \text{id}$. Then $[\sigma\eta, \sigma\eta'/\alpha, 1]$ and $[\eta, \eta'/\alpha, 1]$ are two elements of E , and we may form their difference $[c, d, 1]$. Using the formulas of Silverman [25, Group Law Algorithm 2.3, p. 58] we have

$$c = \frac{1}{\alpha^2} \left(\frac{\eta' + \sigma\eta'}{\eta - \sigma\eta} \right)^2 - \eta - \sigma\eta,$$

$$d = -\frac{1}{\alpha} \left(\frac{\eta' + \sigma\eta'}{\eta - \sigma\eta} \right) \gamma + \frac{1}{\alpha} \frac{\eta\sigma\eta' + \eta'\sigma\eta}{\eta - \sigma\eta}.$$

We claim that c and d are constants (of $\mathcal{G}\sigma\mathcal{G}$). Using the differential equation $\eta'^2 = \alpha(\eta^3 + a_4\eta + a_6)$, we compute

$$\eta'' = \frac{\alpha'}{\alpha} \eta' + \alpha^2 \left(\frac{3}{2} \eta^2 + \frac{1}{2} a_4 \right).$$

Next we compute

$$\left(\frac{\eta' + \sigma\eta'}{\eta - \sigma\eta} \right)' = \frac{\alpha'}{\alpha} \frac{\eta' + \sigma\eta'}{\eta - \sigma\eta} + \frac{1}{2} \alpha^2 (\eta + \sigma\eta).$$

From these formulas, we get that $c' = 0$. d is also a constant since $d^2 = c^3 + a_4c + a_6$. The formula

$$[\sigma\eta, \sigma\eta'/\alpha, 1] = [\eta, \eta'/\alpha, 1] + [c, d, 1]$$

gives

$$\sigma\eta = \left(\frac{d - \eta'/\alpha}{c - d} \right)^2 - c - \eta,$$

which, using Proposition 2.4, shows that \mathcal{G} is strongly normal over \mathcal{F} .

The Galois group is a subgroup of the \mathbb{C} -rational points of E . In fact it is easy to see that the mapping

$$\sigma \mapsto [c, d, 1], \quad \text{id} \mapsto [1, 0, 0]$$

gives an injective homomorphism of $\text{Gal}(\mathcal{G}/\mathcal{F})$ into the subgroup of \mathbb{C} -rational points of E . The details are worked out in [17, Example 29.2, p. 4511] in the special case where $\alpha = 1$. The general case is similar.

3. DIFFERENTIAL SCHEMES

Definition 3.1. Let \mathcal{R} be a reduced Δ -ring and let $X = \text{diffspec } \mathcal{R}$. The *local ringed space of constants*, denoted by X^Δ , is defined as follows:

- (1) The topological space X^Δ is the same as that of X .
- (2) If $U \subset X^\Delta$ is open, then

$$\mathcal{O}_{X^\Delta}(U) = \mathcal{O}_X(U)^\Delta.$$

In general X^Δ is only a local ringed space, not a scheme. The stalk $\mathcal{O}_{X^\Delta, \mathfrak{p}}$ is isomorphic to $(\mathcal{R}_{\mathfrak{p}})^\Delta$, but not necessarily to $(\mathcal{R}^\Delta)_{\mathfrak{p}^\Delta}$. For details see [17, Section 26, p. 4508].

Definition 3.2. Let \mathcal{R} be a reduced Δ -ring and let $X = \text{diffspec } \mathcal{R}$. We say that X *splits* if there is a scheme Y over C such that

$$X \approx G \times_C Y,$$

as Δ -schemes over G .

If X splits, then, by [17, Proposition 28.2, p. 4510], X^Δ is a scheme and $X^\Delta \approx Y$. Note that X^Δ need not be affine; for an example see [17, Section 29, p. 4511]. Indeed X^Δ is an affine scheme if and only if \mathcal{R} is almost constant, i.e. the inclusion

$$\mathcal{R}^\Delta \subset \mathcal{R}$$

induces a bijection between the set of radical Δ -ideals of \mathcal{R} and radical ideals of \mathcal{R}^Δ ([17, Proposition 27.1, p. 4509]).

4. CHARACTERIZATION OF STRONGLY NORMAL EXTENSIONS

In this section we show that \mathcal{G} is strongly normal over \mathcal{F} if and only if P splits, thus giving a geometric characterization to the notion of strongly normal extension. The “heavy lifting” was done in [17]; the proof here simply makes use of results from that paper.

Theorem 4.1. *Let \mathcal{G} be a finitely Δ -generated extension of \mathcal{F} with $\mathcal{G}^\Delta = \mathcal{C}$. Then \mathcal{G} is a strongly normal extension of \mathcal{F} if and only if P splits.*

Proof. If \mathcal{G} is strongly normal over \mathcal{F} , then P splits by [17, Theorem 33.2, p. 4516]. Conversely, suppose that P splits. Let σ be any Δ -isomorphism of \mathcal{G} over \mathcal{F} and set $\mathfrak{p} = \mathfrak{p}_\sigma$. By hypothesis, there exists an isomorphism

$$f: P \rightarrow G \times_C P^\Delta$$

over G . Let $\mathfrak{q} = f(\mathfrak{p})$. Choose an affine open subset $U \subset P^\Delta$ such that $\mathfrak{q} \in G \times_C U$, say $U = \text{spec } \mathcal{D}$, where we think of \mathcal{D} as a Δ -ring of constants. Then

$$G \times_C U = \text{diffspec}(\mathcal{G} \otimes_{\mathcal{C}} \mathcal{D}).$$

The isomorphism f induces an isomorphism of stalks

$$f_{\mathfrak{p}}^\# : (\mathcal{G} \otimes_{\mathcal{C}} \mathcal{D})_{\mathfrak{q}} \rightarrow \mathcal{P}_{\mathfrak{p}}.$$

We also have a surjective homomorphism

$$\bar{\sigma}_{\mathfrak{p}} : \mathcal{P}_{\mathfrak{p}} \rightarrow \mathcal{G}\sigma\mathcal{G}$$

induced by $\bar{\sigma} : \mathcal{P} \rightarrow \mathcal{G}[\sigma\mathcal{G}]$, and the composition

$$g : (\mathcal{G} \otimes_{\mathcal{C}} \mathcal{D})_{\mathfrak{q}} \xrightarrow{f_{\mathfrak{p}}^\#} \mathcal{P}_{\mathfrak{p}} \xrightarrow{\bar{\sigma}_{\mathfrak{p}}} \mathcal{G}\sigma\mathcal{G}$$

is a surjective Δ -homomorphism. Let $\mathcal{D}_\sigma = g(1 \otimes_{\mathbb{C}} \mathcal{D})$, so that \mathcal{D}_σ is a field of constants. Since every element of $\mathcal{G}\mathcal{G}$ is the quotient of elements of

$$g(\mathcal{G} \otimes_{\mathbb{C}} \mathcal{D}) = \mathcal{G}[\mathcal{D}_\sigma],$$

we can apply Proposition 2.4 to conclude that \mathcal{G} is strongly normal over \mathcal{F} . \square

5. LOGARITHMIC DERIVATIVE OF MATRICES

In this section we summarize facts about the logarithmic derivative of matrices for partial Δ -fields. This will be the basis of our definition of Picard-Vessiot extension. For the generalization to non-matric groups see Section 13. Most of the results cited are easy computations, so we merely hint at the proofs.

Definition 5.1. If $\eta \in \text{Mat}_{\mathcal{G}}(n)$, then $\delta_i \eta \in \text{Mat}_{\mathcal{G}}(n)$ ($i = 1, \dots, m$) is the matrix formed by applying δ_i to each coordinate of η , i.e. $(\delta_i \eta)_{jk} = \delta_i(\eta_{jk})$. If $\eta \in \text{GL}_{\mathcal{G}}(n)$, then

$$\ell \delta_i \eta = \delta_i \eta \eta^{-1} \in \text{Mat}_{\mathcal{G}}(n)$$

is called the *logarithmic derivative* of η with respect to δ_i .

Using the product rule on $\delta_i(\eta \eta^{-1}) = \delta_i(\text{id}) = 0$, we get

$$\delta_i(\eta^{-1}) = -\eta^{-1} \delta_i \eta \eta^{-1}.$$

From this and the fact that the derivations commute, we get

$$\delta_i(\ell \delta_j \eta) - \delta_j(\ell \delta_i \eta) = [\ell \delta_i \eta, \ell \delta_j \eta] = \ell \delta_i \eta \ell \delta_j \eta - \ell \delta_j \eta \ell \delta_i \eta \quad (1 \leq i, j \leq m).$$

Definition 5.2. The \mathbb{C} -vector space of all $\mathbf{A} = (A_1, \dots, A_m) \in \text{Mat}_{\mathcal{G}}(n)^m$ that satisfy the *integrability conditions*

$$\delta_i A_j - \delta_j A_i = [A_i, A_j] \quad (1 \leq i, j \leq m)$$

is denoted by $\mathbf{I}_{\mathcal{G}}(n)$.

Definition 5.3. If $\eta \in \text{GL}_{\mathcal{G}}(n)$, then

$$\ell \Delta \eta = (\ell \delta_1 \eta, \dots, \ell \delta_m \eta) \in \mathbf{I}_{\mathcal{G}}(n)$$

is called the *logarithmic derivative* of η .

Observe that the group $\text{GL}_{\mathcal{G}}(n)$ acts on $\mathbf{I}_{\mathcal{G}}(n)$ by conjugation

$$\eta \mathbf{A} \eta^{-1} = (\eta A_1 \eta^{-1}, \dots, \eta A_m \eta^{-1})$$

and that $\ell \Delta: \text{GL}_{\mathcal{G}}(n) \rightarrow \mathbf{I}_{\mathcal{G}}(n)$ is a crossed homomorphism, i.e.

$$\ell \Delta(\eta \xi) = \ell \Delta \eta + \eta \ell \Delta \xi \eta^{-1}.$$

This formula is sometimes called the *gauge transformation*.

Proposition 5.4. $\ell \Delta \eta = \ell \Delta \xi$ if and only if $\xi = \eta c$ for some $c \in \text{GL}_{\mathcal{G}\Delta}(n)$.

Proof. Compute $\ell \Delta(\eta^{-1} \xi)$. \square

The next proposition asserts a kind of surjectivity.

Proposition 5.5. *Let $\mathbf{A} \in \mathbf{I}_{\mathcal{F}}(n)$. Then there exists a Δ -extension field \mathcal{G} of \mathcal{F} and $\eta \in \mathrm{GL}_{\mathcal{G}}(n)$ such that $\ell\Delta\eta = \mathbf{A}$ and $\mathcal{G}^{\Delta} = \mathcal{C}$.*

Proof. Let $X = (X_{jk})_{1 \leq j, k \leq n}$ be a family of indeterminates over \mathcal{F} . Extend the derivations on \mathcal{F} to $\mathcal{F}[X]$ by defining

$$\delta_i X = A_i X,$$

where $\mathbf{A} = (A_1, \dots, A_m)$. Since \mathbf{A} satisfies the integrability conditions, these derivations commute. Next, extend the derivations to the ring $\mathcal{R} = \mathcal{F}[X, (\det X)^{-1}]$ using the quotient rule. Let \mathfrak{m} be a maximal Δ -ideal of \mathcal{R} , $\mathcal{G} = \mathrm{qf}(\mathcal{R}/\mathfrak{m})$ and let η be the image of X . Since \mathcal{R}/\mathfrak{m} is Δ -simple, $\mathcal{G}^{\Delta} = \mathcal{C}$, by [17, Proposition 13.7, p. 4491]. Evidently $\ell\Delta\eta = \mathbf{A}$. \square

The next two propositions will be used in subsequent sections.

Proposition 5.6. $\ell\Delta(\det \eta) = \mathrm{tr}(\ell\Delta\eta)$.

Proof. Here tr acts coordinate-wise on $\mathbf{I}_{\mathcal{G}}(n)$, producing an element of $\mathbf{I}_{\mathcal{G}}(1)$, and $\ell\Delta$ maps $\mathrm{GL}_{\mathcal{G}}(1)$ into $\mathbf{I}_{\mathcal{G}}(1)$. Let \mathcal{G}_a be an algebraic closure of \mathcal{G} and choose $T \in \mathrm{GL}_{\mathcal{G}_a}(n)$ such that $\xi = T\eta T^{-1}$ is upper triangular. We know that $\det \xi = \det \eta$, and it is easy to compute that $\mathrm{tr}(\ell\Delta\xi) = \mathrm{tr}(\ell\Delta\eta)$ using the gauge transformation formula. Thus we may assume that η is upper triangular. But in that case the formula of the proposition is immediate. \square

Suppose that $M, N \in \mathrm{Mat}_{\mathcal{G}}(n)$. Define $M \otimes N \in \mathrm{Mat}_{\mathcal{P}}(n)$ by the formula

$$(M \otimes N)_{jk} = \sum_{r=1}^n M_{jr} \otimes N_{rk} \in \mathcal{P}.$$

Another way of writing this is

$$M \otimes N = \begin{pmatrix} M_{11} \otimes 1 & \dots & M_{1n} \otimes 1 \\ \vdots & & \vdots \\ M_{n1} \otimes 1 & \dots & M_{nn} \otimes 1 \end{pmatrix} \begin{pmatrix} 1 \otimes N_{11} & \dots & 1 \otimes N_{1n} \\ \vdots & & \vdots \\ 1 \otimes N_{n1} & \dots & 1 \otimes N_{nn} \end{pmatrix}.$$

Proposition 5.7. *Suppose that $\eta \in \mathrm{GL}_{\mathcal{G}}(n)$ satisfies $\ell\Delta\eta \in \mathbf{I}_{\mathcal{F}}(n)$. Then*

$$z = \eta^{-1} \otimes \eta \in \mathrm{Mat}_{\mathcal{P}^{\Delta}}(n)$$

and

$$w = \det \eta \otimes (\det \eta)^{-1} \in \mathcal{P}^{\Delta}.$$

Proof. Suppose that $\ell\delta_i\eta = A_i \in \mathrm{Mat}_{\mathcal{F}}(n)$ for $i = 1, \dots, m$. Then

$$\delta_i z = -\eta^{-1} \delta_i \eta \eta^{-1} \otimes \eta + \eta^{-1} \otimes \delta_i \eta = -\eta^{-1} A_i \otimes \eta + \eta^{-1} \otimes A_i \eta = 0.$$

For the second formula, use Proposition 5.6, or compute $\det(z^{-1})$. \square

6. PICARD-VESSIOT EXTENSIONS

Most treatments of Picard-Vessiot theory restrict themselves to ordinary differential fields. However there are at least six different definitions of Picard-Vessiot extension for partial differential fields: Kolchin [7, p. 599], Singer [26, p. 758], Takeuchi [27, p. 492], Buium [3, Chapter I, Section 3, p. 17], van der Put-Singer [29, Definition D.14, Appendix D] and Kolchin [11, p. 410], which is the one we shall use.

Definition 6.1. \mathcal{G} is a *Picard-Vessiot extension* of \mathcal{F} if there exists $\eta \in \mathrm{GL}_{\mathcal{G}}(n)$, for some $n \in \mathbb{N}$, such that

- (1) $\ell\Delta\eta \in \mathbf{I}_{\mathcal{F}}(n)$,
- (2) $\mathcal{G} = \mathcal{F}\langle\eta\rangle = \mathcal{F}(\eta)$,
- (3) $\mathcal{G}^{\Delta} = \mathbb{C}$.

When we write a Picard-Vessiot extension in the form $\mathcal{G} = \mathcal{F}(\eta)$ we implicitly mean that $\eta \in \mathrm{GL}_{\mathcal{G}}(n)$ and $\ell\Delta\eta \in \mathbf{I}_{\mathcal{F}}(n)$.

Proposition 6.2. *A Picard-Vessiot extension of \mathcal{F} is strongly normal over \mathcal{F} .*

Proof. Write $\mathcal{G} = \mathcal{F}(\eta)$. Let σ be a Δ -isomorphism of \mathcal{G} over \mathcal{F} and let $\mathcal{D} = (\mathcal{G}\sigma\mathcal{G})^{\Delta}$. Because $\ell\Delta\sigma\eta = \sigma\ell\Delta\eta = \ell\Delta\eta$, Proposition 5.4 gives the existence of $c \in \mathrm{GL}_{\mathcal{D}}(n)$ with $\sigma\eta = c\eta$. \square

By [17, Proposition 13.8, p. 4492], there exists a Δ -simple subring $\mathcal{R} \subset \mathcal{G}$ with $\mathcal{G} = \mathrm{qf}\mathcal{R}$. In the case of a Picard-Vessiot extension we can explicitly find that ring.

Proposition 6.3. *If $\mathcal{G} = \mathcal{F}(\eta)$ is a Picard-Vessiot extension, then $\mathcal{F}[\eta, \eta^{-1}]$ is Δ -simple.*

Proof. Let $\mathcal{R} = \mathcal{F}[\eta, \eta^{-1}]$ and let $\mathfrak{p} \subset \mathcal{R}$ be a prime Δ -ideal. Choose a maximal Δ -ideal $\mathfrak{m} \subset \mathcal{G} \otimes \mathcal{R}$ that contains $\mathcal{G} \otimes \mathfrak{p}$ and let

$$\pi: \mathcal{G} \otimes \mathcal{R} \rightarrow (\mathcal{G} \otimes \mathcal{R})/\mathfrak{m}$$

be the quotient homomorphism. We identify \mathcal{G} with the image of $\mathcal{G} \otimes 1$, and let ξ be the image of $1 \otimes \eta$, so that

$$(\mathcal{G} \otimes \mathcal{R})/\mathfrak{m} = \mathcal{G}[\xi, \xi^{-1}].$$

Note that the restriction

$$\pi_1: 1 \otimes \mathcal{R} \rightarrow \mathcal{F}[\xi, \xi^{-1}]$$

is surjective and the kernel contains $1 \otimes \mathfrak{p}$. We claim that it is an isomorphism, and hence that $\mathfrak{p} = (0)$.

Because \mathfrak{m} is a maximal Δ -ideal, $\mathcal{G}[\xi, \xi^{-1}]$ is Δ -simple, and, by [17, Proposition 13.7, p. 4491],

$$\mathcal{G}(\xi)^{\Delta} = \mathcal{G}^{\Delta} = \mathbb{C}.$$

Since $\ell\Delta\eta \in \mathbf{I}_{\mathcal{F}}(n)$, $\ell\Delta\xi = \ell\Delta\eta$. Hence, by Proposition 5.4, there exists $c \in \mathrm{GL}_{\mathbb{C}}(n)$ with $\xi = \eta c$. Therefore $\mathcal{F}[\xi, \xi^{-1}] = \mathcal{F}[\eta, \eta^{-1}]$, which proves our claim. \square

Proposition 6.4. *Let $\mathbf{A} \in \mathbf{I}_{\mathcal{F}}(n)$. Then there exists a Picard-Vessiot extension $\mathcal{G} = \mathcal{F}(\eta)$ with $\ell\Delta\eta = \mathbf{A}$. Moreover, \mathcal{G} is unique up to Δ -isomorphism over \mathcal{F} .*

Proof. Existence is Proposition 5.5. Suppose that $\mathcal{F}(\xi)$ is another Picard-Vessiot extension with $\ell\Delta\xi = \mathbf{A}$. Let $\mathcal{S} = \mathcal{F}[\xi, \xi^{-1}]$ and let \mathfrak{m} be a maximal Δ -ideal of $\mathcal{G} \otimes \mathcal{S}$. Consider the quotient homomorphism

$$\pi: \mathcal{G} \otimes \mathcal{S} \rightarrow (\mathcal{G} \otimes \mathcal{S})/\mathfrak{m} = \mathcal{G}[\zeta, \zeta^{-1}].$$

Since $\mathcal{F}[\zeta, \zeta^{-1}]$ is Δ -simple, $\mathcal{F}(\zeta)^\Delta = \mathcal{C}$. By Proposition 5.4, there exists $c \in \mathrm{GL}_{\mathcal{C}}(n)$ such that $\zeta = \eta c$, which implies that $\mathcal{F}[\zeta, \zeta^{-1}] = \mathcal{F}[\eta, \eta^{-1}]$. However, by Proposition 6.3, $1 \otimes \mathcal{S} \rightarrow \mathcal{F}[\zeta, \zeta^{-1}]$ is an isomorphism, which makes $\mathcal{F}[\eta, \eta^{-1}]$ isomorphic to $\mathcal{S} = \mathcal{F}[\xi, \xi^{-1}]$. \square

In [17, Section 33, p. 4516], we showed that $P = \mathrm{diffspec} \mathcal{P}$ splits for any strongly normal extension. However, the proof for a Picard-Vessiot extension is much easier than the one given there.

Let $\mathcal{G} = \mathcal{F}(\eta)$ be a Picard-Vessiot extension and set $\mathcal{R} = \mathcal{F}[\eta, \eta^{-1}]$. Then \mathcal{G} is the ring of fractions of \mathcal{R} by the multiplicative set \mathcal{R}^* . By Proposition 6.3, \mathcal{R} is Δ -simple, which implies that \mathcal{R}^* consists of Δ -units ([17, Proposition 13.4, p. 4491]). We have

$$P = \mathcal{G} \otimes_{\mathcal{F}} \mathcal{G} = (\mathcal{G} \otimes_{\mathcal{F}} \mathcal{R})[(1 \otimes \mathcal{R}^*)^{-1}] = (\mathcal{R} \otimes_{\mathcal{F}} \mathcal{R})[(\mathcal{R}^* \otimes \mathcal{R}^*)^{-1}],$$

so, by [17, Proposition 22.2, p. 4502],

$$P = \mathrm{diffspec} \mathcal{P} \approx \mathrm{diffspec}(\mathcal{G} \otimes_{\mathcal{F}} \mathcal{R}) \approx \mathrm{diffspec}(\mathcal{R} \otimes_{\mathcal{F}} \mathcal{R}).$$

These isomorphisms illustrate an anomaly for Δ -schemes: $\mathrm{diffspec}(\mathcal{R} \otimes_{\mathcal{F}} \mathcal{R})$ is a Δ -scheme over \mathcal{G} even though $\mathcal{R} \otimes_{\mathcal{F}} \mathcal{R}$ is not a \mathcal{G} -algebra.

Proposition 6.5. *If $\mathcal{G} = \mathcal{F}(\eta)$ is a Picard-Vessiot extension and $\mathcal{R} = \mathcal{F}[\eta, \eta^{-1}]$, then*

$$(\mathcal{R} \otimes_{\mathcal{F}} \mathcal{R})^\Delta = \mathcal{P}^\Delta.$$

Proof. For $\gamma \in \mathcal{P}^\Delta$ we define

$$\mathfrak{a} = \{b \in \mathcal{R} \mid (1 \otimes b)\gamma \in \mathcal{G} \otimes \mathcal{R}\}.$$

Because γ is a constant, \mathfrak{a} is a Δ -ideal. But \mathcal{R} is Δ -simple, so $\mathfrak{a} = (1)$ and therefore $\gamma \in \mathcal{G} \otimes_{\mathcal{F}} \mathcal{R}$. Using a similar argument we conclude that $\gamma \in \mathcal{R} \otimes_{\mathcal{F}} \mathcal{R}$. \square

Proposition 6.6. $\mathcal{R} \otimes_{\mathcal{F}} \mathcal{R} = (\mathcal{R} \otimes_{\mathcal{F}} 1)[\mathcal{P}^\Delta]$.

Proof. We have $\mathcal{R} = \mathcal{F}[\eta, \eta^{-1}] = \mathcal{F}[\eta, (\det \eta)^{-1}]$. By Proposition 5.7

$$1 \otimes \eta = (\eta \otimes 1)z \quad \text{and} \quad 1 \otimes (\det \eta)^{-1} = ((\det \eta)^{-1} \otimes 1)w.$$

\square

Proposition 6.7. $\mathcal{G} \otimes_{\mathcal{F}} \mathcal{R}$ is almost constant, and hence P^Δ is an affine scheme. Moreover $P \approx \mathrm{spec} \mathcal{P}^\Delta = \mathrm{spec}(\mathcal{R} \otimes_{\mathcal{F}} \mathcal{R})^\Delta$.

Proof. The first statement is [17, Corollary 5.8, p. 4484], the remainder is [17, Proposition 27.1, p. 4509]. \square

In Theorem 10.5 we shall prove the converse of this proposition. The Δ -coring structure on \mathcal{P} that is described in [17, Section 16, p. 4494] restricts to $\mathcal{R} \otimes_{\mathcal{F}} \mathcal{R}$ and then further to $(\mathcal{R} \otimes_{\mathcal{F}} \mathcal{R})^\Delta = \mathcal{P}^\Delta$. This makes \mathcal{P}^Δ into a Hopf algebra. We leave the details to the reader.

7. LINEAR DIFFERENTIAL EQUATIONS

An alternative approach to the Picard-Vessiot theory is to use linear ideals of finite linear dimension, as in Kolchin [11, p. 150]. For the ordinary case this means considering a linear homogeneous differential equation. The cyclic vector theorem (see, for example, Churchill-Kovacic [4]) allows us to translate from one formulation to the other. A similar situation exists in the partial case. We assume that \mathcal{F} does not consist of constants alone, specifically that \mathcal{F} contains an element whose δ_1 derivative is not 0.

Given a fundamental system of zeros of a linear differential ideal of finite linear dimension, one can form a generalized Wronskian matrix as in Lemma 8.2 (below) or Kolchin [11, Corollary 3, p. 153]. This gives the matrix η with $\ell\Delta\eta \in \mathbf{I}_{\mathcal{F}}(n)$.

Conversely, suppose we are given $\eta \in \mathrm{GL}_{\mathcal{G}}(n)$ with $\ell\Delta\eta = \mathbf{A}$. By [4, Cyclic Vector Theorem, p. 200] there exists $T \in \mathrm{GL}_{\mathcal{F}}(n)$ such that

$$\ell\delta_1(T\eta) = \ell\delta_1 T + T A_1 T^{-1} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ a_0 & a_1 & a_2 & \cdots & a_{n-2} & a_{n-1} \end{pmatrix}.$$

This implies that $\xi = T\eta$ has the form

$$\xi = \begin{pmatrix} g_1 & \cdots & g_n \\ \delta_1 g_1 & \cdots & \delta_1 g_n \\ \vdots & & \vdots \\ \delta_1^{n-1} g_1 & \cdots & \delta_1^{n-1} g_n \end{pmatrix},$$

where $g_1, \dots, g_n \in \mathcal{G} = \mathcal{F}(\eta)$. Note that ξ is an “ordinary” Wronskian matrix in δ_1 alone. Hence g_1, \dots, g_n are solutions of the ordinary differential equation

$$\delta_1^n y = a_{n-1} \delta_1^{n-1} y + \cdots + a_1 \delta_1 y + a_0 y.$$

If the first row of $\ell\delta_j T + T A_j T^{-1}$ is $(b_{j,0} \ b_{j,1} \ \cdots \ b_{j,n-1})$, then g_1, \dots, g_n are solutions of

$$\begin{aligned} \delta_2 y &= b_{2,n-1} \delta_1^{n-1} y + \cdots + b_{2,1} \delta_1 y + b_{2,0} y, \\ &\vdots \\ \delta_m y &= b_{m,n-1} \delta_1^{n-1} y + \cdots + b_{m,1} \delta_1 y + b_{m,0} y. \end{aligned}$$

Thus we get one equation of n^{th} order in δ_1 alone, and $n-1$ equations of first order in the other derivatives.

8. PICARD-VESSIOT ELEMENTS

In this section \mathcal{G} is a strongly normal extension of \mathcal{F} (not Picard-Vessiot). If S is any subset of \mathcal{G} , then $\mathcal{F}[S]$ denotes the \mathcal{F} -vector subspace of \mathcal{G} spanned by S . If $g \in \mathcal{G}$, then $\mathcal{F}[\Theta g]$ denotes the \mathcal{F} -vector space spanned by $\Theta g = \{\theta g \mid \theta \in \Theta\}$. Similarly, $\mathcal{C}[S]$ denotes the \mathcal{C} -vector space spanned by S and $\mathcal{C}[\mathrm{Gal}(\mathcal{G}/\mathcal{F})g]$ the \mathcal{C} -vector space spanned by $\mathrm{Gal}(\mathcal{G}/\mathcal{F})g = \{\sigma g \mid \sigma \in \mathrm{Gal}(\mathcal{G}/\mathcal{F})\}$. In general these vector

spaces are infinite dimensional. We are interested in the conditions that they be finite dimensional. We start with a “well-known” lemma about Wronskians.

Lemma 8.1. *Suppose that $a_1, \dots, a_n \in \mathcal{G}$ are linearly independent over \mathcal{C} . Then there exist $\theta_1, \dots, \theta_n \in \Theta$, with $\theta_1 = 1$, such that*

$$\det(\theta_i a_j)_{1 \leq i, j \leq n} \neq 0.$$

Proof. This is a special case ($r = 1$) of Kolchin [11, Theorem 1, p. 86]. \square

One can restrict the θ_i to have order smaller than i . This gives the usual Wronskian in the ordinary ($m = 1$) case.

Lemma 8.2. *Let $g_1, \dots, g_r \in \mathcal{G}$ and suppose that $\mathcal{C}[\text{Gal}(\mathcal{G}/\mathcal{F})g_1, \dots, \text{Gal}(\mathcal{G}/\mathcal{F})g_r]$ has finite dimension over \mathcal{C} with basis a_1, \dots, a_n . Then there exist $\theta_1, \dots, \theta_n \in \Theta$, with $\theta_1 = 1$, such that*

$$\eta = (\theta_i a_j)_{1 \leq i, j \leq n} \in \text{GL}_{\mathcal{G}}(n) \quad \text{and} \quad \ell \Delta \eta \in \mathbf{I}_{\mathcal{F}}(n).$$

Proof. The existence of $\eta \in \text{GL}_{\mathcal{G}}(n)$ follows from the previous lemma. For any $\sigma \in \text{Gal}(\mathcal{G}/\mathcal{F})$ there exists $c(\sigma) \in \text{GL}_{\mathcal{C}}(n)$ such that

$$\sigma a_j = \sum_{i=1}^n a_i c_{ij}(\sigma) \quad (j = 1, \dots, n).$$

Therefore

$$\sigma \eta = \eta c(\sigma)$$

and hence $\sigma \ell \Delta \eta = \ell \Delta \sigma \eta = \ell \Delta \eta$. This being true for every $\sigma \in \text{Gal}(\mathcal{G}/\mathcal{F})$, we conclude that $\ell \Delta \eta \in \mathbf{I}_{\mathcal{F}}(n)$ ([17, Proposition 15.3, p. 4494]). \square

Lemma 8.3. *Suppose that $a_1, \dots, a_n \in \mathcal{G}$ are linearly independent over \mathcal{F} . Then there exist $\sigma_1, \dots, \sigma_n \in \text{Gal}(\mathcal{G}/\mathcal{F})$, with $\sigma_1 = \text{id}$, such that*

$$\det(\sigma_i a_j)_{1 \leq i, j \leq n} \neq 0.$$

Proof. The condition that $\sigma_1 = \text{id}$ is a “red herring”, if $\sigma_1 \neq \text{id}$ we could simply apply σ_1^{-1} to each coordinate of the matrix.

We use induction on n . The case $n = 1$ being trivial, we suppose that $n > 1$ and that the result is proven for $n - 1$. By the induction hypothesis there exist $\sigma_1, \dots, \sigma_{n-1} \in \text{Gal}(\mathcal{G}/\mathcal{F})$, with $\sigma_1 = \text{id}$, such that

$$\det(\sigma_i a_j)_{1 \leq i, j \leq n-1} \neq 0.$$

Suppose that

$$\det \begin{pmatrix} \sigma_1 a_1 & \dots & \sigma_1 a_n \\ \vdots & & \vdots \\ \sigma_{n-1} a_1 & \dots & \sigma_{n-1} a_n \\ \sigma a_1 & \dots & \sigma a_n \end{pmatrix} = 0$$

for every $\sigma \in \text{Gal}(\mathcal{G}/\mathcal{F})$. The columns of the matrix are linearly dependent, so there exist $b_1, \dots, b_n \in \mathcal{G}$, not all 0, with

$$(8.1) \quad \begin{aligned} b_n \sigma_i a_n &= \sum_{j=1}^{n-1} b_j \sigma_i a_j & \text{for } i = 1, \dots, n-1, \text{ and} \\ b_n \sigma a_n &= \sum_{j=1}^{n-1} b_j \sigma a_j. \end{aligned}$$

The first set of equations, in matrix form, is

$$\begin{pmatrix} \sigma_1 a_1 & \cdots & \sigma_1 a_{n-1} \\ \vdots & & \vdots \\ \sigma_{n-1} a_1 & \cdots & \sigma_{n-1} a_{n-1} \end{pmatrix} \begin{pmatrix} b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = b_n \begin{pmatrix} \sigma_1 a_n \\ \vdots \\ \sigma_{n-1} a_n \end{pmatrix}.$$

Since the matrix on the left is invertible, we cannot have $b_n = 0$, so we may assume that $b_n = 1$. Also b_1, \dots, b_{n-1} are determined by this equation and therefore are independent of σ .

For any $\tau \in \text{Gal}(\mathcal{G}/\mathcal{F})$ we may successively set $\sigma = \tau^{-1}\sigma_i$, $i = 1, \dots, n-1$, to get

$$\sigma_i a_n = \tau(\sigma a_n) = \sum_{j=1}^{n-1} \tau b_j \sigma_i a_j.$$

Therefore

$$\sum_{j=1}^{n-1} (\tau b_j - b_j) \sigma_i a_j = 0 \quad \text{for } i = 1, \dots, n-1.$$

This implies that $\tau b_j = b_j$ for every $\tau \in \text{Gal}(\mathcal{G}/\mathcal{F})$. Therefore, by [17, Proposition 15.3, p. 4494], $b_j \in \mathcal{F}$. Because $\sigma_1 = \text{id}$, Equation (8.1) (with $i = 1$) shows that a_1, \dots, a_n are linearly dependent over \mathcal{F} , which is a contradiction. \square

Proposition 8.4. *For $g \in \mathcal{G}$ the following are equivalent:*

- (1) $\mathcal{F}|\Theta g|$ has finite dimension over \mathcal{F} .
- (2) $\mathcal{C}|\text{Gal}(\mathcal{G}/\mathcal{F})g|$ has finite dimension over \mathcal{C} .
- (3) $1 \otimes g \in (\mathcal{G} \otimes 1)[\mathcal{P}^\Delta]$.

Proof. (1) \Rightarrow (2). Suppose that $\mathcal{F}|\Theta g|$ has basis a_1, \dots, a_n . For any $\theta_1, \dots, \theta_{n+1} \in \Theta$ there exist $f_{ik} \in \mathcal{F}$ with

$$\theta_i g = \sum_{k=1}^n f_{ik} a_k \quad (i = 1, \dots, n+1).$$

Hence, for any $\sigma_1, \dots, \sigma_{n+1} \in \text{Gal}(\mathcal{G}/\mathcal{F})$,

$$\theta_i \sigma_j g = \sigma_j \theta_i g = \sum_{k=1}^n f_{ik} \sigma_j a_k \quad (1 \leq i, j \leq n+1).$$

In matrix form this is

$$\begin{pmatrix} \theta_1 \sigma_1 g & \cdots & \theta_1 \sigma_{n+1} g \\ \vdots & & \vdots \\ \theta_{n+1} \sigma_1 g & \cdots & \theta_{n+1} \sigma_{n+1} g \end{pmatrix} = \begin{pmatrix} f_{11} & \cdots & f_{1n} \\ \vdots & & \vdots \\ f_{n+1,1} & \cdots & f_{n+1,n} \end{pmatrix} \begin{pmatrix} \sigma_1 a_1 & \cdots & \sigma_{n+1} a_1 \\ \vdots & & \vdots \\ \sigma_1 a_n & \cdots & \sigma_{n+1} a_n \end{pmatrix}.$$

Since the ranks of the matrices on the right are no bigger than n ,

$$\det(\theta_i \sigma_j g)_{1 \leq i, j \leq n+1} = 0.$$

It follows from Lemma 8.1 that $\sigma_1 g, \dots, \sigma_{n+1} g$ are linearly dependent over \mathcal{C} .

(2) \Rightarrow (1). Let a_1, \dots, a_n be a basis of $\mathcal{C}|\text{Gal}(\mathcal{G}/\mathcal{F})g|$. For any $\sigma_1, \dots, \sigma_{n+1} \in \text{Gal}(\mathcal{G}/\mathcal{F})$ there exist $c_{ik} \in \mathcal{C}$ with

$$\sigma_i g = \sum_{k=1}^n c_{ik} a_k \quad (i = 1, \dots, n+1).$$

Hence, for any $\theta_1, \dots, \theta_{n+1} \in \Theta$,

$$\sigma_i \theta_j g = \theta_j \sigma_i g = \sum_{k=1}^n c_{ik} \theta_j a_k \quad (1 \leq i, j \leq n+1).$$

As above, this implies that

$$\det(\sigma_i \theta_j g)_{1 \leq i, j \leq n+1} = 0.$$

By Lemma 8.3, $\theta_1 g, \dots, \theta_{n+1} g$ are linearly dependent over \mathcal{F} .

(2) \Rightarrow (3). Let a_1, \dots, a_n be a basis of $\mathcal{C}[\text{Gal}(\mathcal{G}/\mathcal{F})g]$ with $a_1 = g$ and choose η satisfying the conditions of Lemma 8.2. Note that $\eta_{11} = g$.

By Proposition 5.7

$$z = \eta^{-1} \otimes \eta \in \text{Mat}_{\mathcal{P}^\Delta}(n),$$

hence

$$1 \otimes g = 1 \otimes \eta_{11} = ((\eta \otimes 1)z)_{11} \in (\mathcal{G} \otimes 1)[\mathcal{P}^\Delta].$$

(3) \Rightarrow (2). Suppose that

$$1 \otimes g = \sum_{i=1}^n (a_i \otimes 1) c_i \in (\mathcal{G} \otimes 1)[\mathcal{P}^\Delta].$$

For any $\sigma \in \text{Gal}(\mathcal{G}/\mathcal{F})$

$$\sigma g = \bar{\sigma}(1 \otimes g) = \sum_{i=1}^n a_i \bar{\sigma}(c_i).$$

Hence σg is in the \mathcal{C} -vector space spanned by a_1, \dots, a_n . \square

Definition 8.5. An element $g \in \mathcal{G}$ is *Picard-Vessiot over \mathcal{F}* if it satisfies the equivalent conditions of Proposition 8.4.

Another characterization is that g is a zero of a linear Δ -ideal of finite linear dimension; see Kolchin [11, Section 5, p. 150].

Proposition 8.6. Let $\eta \in \text{GL}_{\mathcal{G}}(n)$ be such that $\ell \Delta \eta \in \mathbf{I}_{\mathcal{F}}(n)$. Then each η_{ij} ($1 \leq i, j \leq n$) is Picard-Vessiot over \mathcal{F} and so is $(\det \eta)^{-1}$.

Proof. Proposition 5.7. \square

9. PICARD-VESSIOT RING

In this section \mathcal{G} is a strongly normal extension of \mathcal{F} . By Proposition 8.4 (3), the set of all Picard-Vessiot elements of \mathcal{G} over \mathcal{F} is a Δ -ring.

Definition 9.1. The Δ -ring of all elements of \mathcal{G} that are Picard-Vessiot over \mathcal{F} is denoted by $\mathcal{V} = \mathcal{V}(\mathcal{G}/\mathcal{F})$. The field of quotients of \mathcal{V} is denoted by $\mathcal{L} = \mathcal{L}(\mathcal{G}/\mathcal{F})$.

Proposition 9.2. $\mathcal{G} \otimes_{\mathcal{F}} \mathcal{V} = (\mathcal{G} \otimes_{\mathcal{F}} 1)[\mathcal{P}^\Delta] \approx \mathcal{G} \otimes_{\mathcal{C}} \mathcal{P}^\Delta$.

Proof. The equality comes from Proposition 8.4, the isomorphism from [17, Proposition 2.1, p. 4479]. \square

The following two propositions generalize Propositions 6.3 and 6.5.

Proposition 9.3. \mathcal{V} is Δ -simple.

Proof. Let $\mathfrak{a} \subset \mathcal{V}$ be a non-zero Δ -ideal and let $g \in \mathfrak{a}$ with $g \neq 0$. Choose a basis a_1, \dots, a_n of $\mathcal{C}[\text{Gal}(\mathcal{G}/\mathcal{F})g]$ with $a_1 = g$ and, by Lemma 8.2, $\theta_1, \dots, \theta_n \in \Theta$ with $\theta_1 = 1$, satisfying

$$\eta = (\theta_i a_j)_{1 \leq i, j \leq n} \in \text{GL}_{\mathcal{G}}(n) \quad \text{and} \quad \ell \Delta \eta \in \mathbf{I}_{\mathcal{F}}(n).$$

By Proposition 8.6, each $\theta_i a_j$ is in \mathcal{V} . Using Kramer's rule on the first column, we see that $\det \eta \in \mathfrak{a}$. But, by Proposition 8.6, $(\det \eta)^{-1} \in \mathcal{V}$, so $1 \in \mathfrak{a}$. \square

Proposition 9.4. $\mathcal{P}^{\Delta} = (\mathcal{V} \otimes \mathcal{V})^{\Delta}$.

Proof. Let $c \in \mathcal{P}^{\Delta}$. Among all possible expressions

$$c = \sum_{i=1}^n a_i \otimes b_i$$

we choose one with n minimal. It follows that a_1, \dots, a_n are linearly independent over \mathcal{F} and so are b_1, \dots, b_n . Using Lemma 8.3, choose $\sigma_1, \dots, \sigma_n \in \text{Gal}(\mathcal{G}/\mathcal{F})$ with

$$\det(\sigma_i a_j) \neq 0.$$

For each $i = 1, \dots, n$, define $\tau_i: \mathcal{P} \rightarrow \mathcal{P}$ by $\tau_i(a \otimes b) = \sigma_i a \otimes b$. Note that τ_i is a Δ -homomorphism, so $\tau_i c \in \mathcal{P}^{\Delta}$. We have

$$\begin{pmatrix} \sigma_1 a_1 \otimes 1 & \cdots & \sigma_1 a_n \otimes 1 \\ \vdots & & \vdots \\ \sigma_n a_1 \otimes 1 & \cdots & \sigma_n a_n \otimes 1 \end{pmatrix} \begin{pmatrix} 1 \otimes b_1 \\ \vdots \\ 1 \otimes b_n \end{pmatrix} = \begin{pmatrix} \tau_1 c \\ \vdots \\ \tau_n c \end{pmatrix}.$$

The matrix on the left is invertible, therefore

$$1 \otimes b_i \in (\mathcal{G} \otimes 1)[\mathcal{P}^{\Delta}],$$

which means that $b_i \in \mathcal{V}$. Similarly $a_i \in \mathcal{V}$. \square

10. CHARACTERIZATION OF PICARD-VESSIOT EXTENSIONS

As before, \mathcal{G} is a strongly normal extension of \mathcal{F} , $\mathcal{V} = \mathcal{V}(\mathcal{G}/\mathcal{F})$ and $\mathcal{L} = \mathcal{L}(\mathcal{G}/\mathcal{F}) = \text{qf}(\mathcal{V})$.

Proposition 10.1. \mathcal{L} is a Picard-Vessiot extension of \mathcal{F} .

Proof. By [17, Proposition 12.4, p. 4490], \mathcal{G} is finitely generated over \mathcal{F} as a field, and therefore, by [22, Theorem 4.1.5, p. 99], so is \mathcal{L} , say $\mathcal{L} = \mathcal{F}(g_1, \dots, g_r)$. We may assume that g_1, \dots, g_r are in \mathcal{V} and are linearly independent over \mathcal{C} . Choose a basis a_1, \dots, a_n of

$$\mathcal{C}[\text{Gal}(\mathcal{G}/\mathcal{F})g_1, \dots, \text{Gal}(\mathcal{G}/\mathcal{F})g_r]$$

with $a_i = g_i$ for $i = 1, \dots, r$. Observe that $a_i \in \mathcal{L}$ for $i = 1, \dots, n$. By Lemma 8.2 there exist $\theta_1, \dots, \theta_n \in \Theta$, with $\theta_1 = 1$ such that

$$\eta = (\theta_i a_j)_{1 \leq i, j \leq n} \in \text{GL}_{\mathcal{L}}(n) \quad \text{and} \quad \ell \Delta \eta \in \mathbf{I}_{\mathcal{F}}(n).$$

Since $\eta_{1i} = a_i = g_i$ for $i = 1, \dots, r$, $\mathcal{L} = \mathcal{F}(\eta)$. We also have $\mathcal{L}^{\Delta} \subset \mathcal{G}^{\Delta} = \mathcal{C}$, hence \mathcal{L} is a Picard-Vessiot extension of \mathcal{F} . \square

Proposition 10.2. If $\mathcal{G} = \mathcal{F}(\eta)$ is a Picard-Vessiot extension of \mathcal{F} , then $\mathcal{V} = \mathcal{F}[\eta, \eta^{-1}]$.

Proof. By Proposition 5.7,

$$1 \otimes \eta = (\eta \otimes 1)z \in (\mathcal{G} \otimes 1)[\mathcal{P}^\Delta]$$

and

$$1 \otimes (\det \eta)^{-1} = ((\det \eta)^{-1} \otimes 1)w \in (\mathcal{G} \otimes 1)[\mathcal{P}^\Delta],$$

which shows that $\mathcal{F}[\eta, \eta^{-1}] \subset \mathcal{V}$. By definition of \mathcal{V} , and Proposition 8.4,

$$\mathcal{G} \otimes \mathcal{V} \subset (\mathcal{G} \otimes 1)[\mathcal{P}^\Delta] \subset \mathcal{G} \otimes \mathcal{F}[\eta, \eta^{-1}],$$

hence $\mathcal{F}[\eta, \eta^{-1}] = \mathcal{V}$. \square

Corollary 10.3. *If $\mathcal{G} = F(\eta)$ is a Picard-Vessiot extension of \mathcal{F} , then the Δ -ring $\mathcal{F}[\eta, \eta^{-1}]$ is independent of the choice of η .*

This means that if $\mathcal{G} = \mathcal{F}(\eta) = \mathcal{F}(\xi)$, then $\mathcal{F}[\eta, \eta^{-1}] = \mathcal{F}[\xi, \xi^{-1}]$. The matrices η and ξ do not even need to be the same size!

Proposition 10.4. *Let \mathcal{G} be a strongly normal extension of \mathcal{F} . Then \mathcal{L} is the largest Picard-Vessiot extension of \mathcal{F} contained in \mathcal{G} .*

Proof. Suppose that $\mathcal{H} = \mathcal{F}(\eta)$ is a Picard-Vessiot extension of \mathcal{F} that is contained in \mathcal{G} . By the previous proposition,

$$\mathcal{F}[\eta, \eta^{-1}] = \mathcal{V}(\mathcal{H}/\mathcal{F}) \subset \mathcal{V}(\mathcal{G}/\mathcal{F}) \subset \mathcal{L},$$

hence $\mathcal{H} \subset \mathcal{L}$. \square

Theorem 10.5. *Suppose that \mathcal{G} is strongly normal over \mathcal{F} . Then the following are equivalent:*

- (1) \mathcal{G} is a Picard-Vessiot extension of \mathcal{F} ,
- (2) \mathcal{P} is almost constant,
- (3) \mathcal{P}^Δ is affine.

Proof. (1) \Rightarrow (2). By Proposition 6.6, $\mathcal{G} \otimes_{\mathcal{F}} \mathcal{V}$ is almost constant. But \mathcal{P} is the ring of quotients of $\mathcal{G} \otimes_{\mathcal{F}} \mathcal{V}$ by the multiplicative set $1 \otimes \mathcal{V}^*$. By Proposition 9.3, \mathcal{V} is Δ -simple, and therefore, by [17, Proposition 13.4, p. 4491], consists of Δ -units. [17, Proposition 5.4, p. 4483] implies that \mathcal{P} is almost constant.

(2) \Rightarrow (1). Suppose that \mathcal{P} is almost constant. We claim that $\mathcal{G} = \mathcal{L}$, which, by Proposition 10.1, is a Picard-Vessiot extension of \mathcal{F} . For this it suffices to prove that $\text{Gal}(\mathcal{G}/\mathcal{L}) = \{\text{id}\}$. Let $\sigma \in \text{Gal}(\mathcal{G}/\mathcal{L})$ and let $\mathfrak{p} = \mathfrak{p}_\sigma$. Then

$$\mathfrak{p}_\sigma \cap (\mathcal{V} \otimes \mathcal{V}) = \mathfrak{p}_{\text{id}} \cap (\mathcal{V} \otimes \mathcal{V}).$$

By Proposition 9.4, $\mathcal{P}^\Delta \subset \mathcal{V} \otimes \mathcal{V}$, therefore

$$\mathfrak{p}_\sigma \cap \mathcal{P}^\Delta = \mathfrak{p}_{\text{id}} \cap \mathcal{P}^\Delta.$$

Because \mathcal{P} is almost constant, $\mathfrak{p}_\sigma = \mathfrak{p}_{\text{id}}$. By [17, Propositions 37.3 and 37.4, p. 4521], $\sigma = \text{id}$.

(2) \Leftrightarrow (3). [17, Proposition 27.1, p. 4509]. \square

11. RELATIVE PICARD-VESSIOT CLOSURE

As before, \mathcal{G} is a strongly normal extension of \mathcal{F} , $\mathcal{V} = \mathcal{V}(\mathcal{G}/\mathcal{F})$ and $\mathcal{L} = \mathcal{L}(\mathcal{G}/\mathcal{F}) = \text{qf}(\mathcal{V})$. Proposition 10.4 asserts that \mathcal{L} is the largest Picard-Vessiot extension of \mathcal{F} contained in \mathcal{G} . Here we show that \mathcal{L} has no proper Picard-Vessiot extensions in \mathcal{G} , thus \mathcal{L} is the “Picard-Vessiot closure” of \mathcal{F} in \mathcal{G} . We do not have an elementary proof of this, but rather rely on a structure theorem of Rosenlicht.

Proposition 11.1. *Let X be an algebraic group defined over \mathbb{C} . Then there exists a connected normal algebraic subgroup D of X , defined over \mathbb{C} , such that X/D is linear and such that the kernel of any rational homomorphism of X to a linear group contains D . Any rational homomorphism of D onto a linear group is trivial.*

Proof. (We have used X rather than the traditional G since we have previously defined G to be $\text{diffspec } \mathcal{G}$.) The existence of D is Rosenlicht [24, Corollary 3, p. 431], the last statement is [24, Corollary 5, p. 440]. \square

Proposition 11.2. *$D = \text{Gal}(\mathcal{G}/\mathcal{L})$ is the smallest normal algebraic subgroup of $\text{Gal}(\mathcal{G}/\mathcal{F})$ giving rise to a linear factor group.*

Proof. If $D' \subset D$ and \mathcal{L}' is the fixed field of D' , then, by [17, Theorem 20.5, p. 4500], \mathcal{L}' is strongly normal over \mathcal{F} and by Theorem 10.5, \mathcal{L}' is Picard-Vessiot over \mathcal{F} . Hence, by Proposition 10.4, $\mathcal{L}' \subset \mathcal{L}$. \square

Proposition 11.3. *\mathcal{L} has no proper Picard-Vessiot extension in \mathcal{G} .*

Proof. Suppose that

$$\mathcal{F} \subset \mathcal{L} \subset \mathcal{H} \subset \mathcal{G}$$

with \mathcal{H} Picard-Vessiot over \mathcal{L} . By [17, Theorem 20.5, p. 4500], we have a surjective homomorphism

$$D = \text{Gal}(\mathcal{G}/\mathcal{L}) \rightarrow \text{Gal}(\mathcal{G}/\mathcal{L}) / \text{Gal}(\mathcal{G}/\mathcal{H}) \approx \text{Gal}(\mathcal{H}/\mathcal{L}).$$

By Proposition 11.1, $\text{Gal}(\mathcal{H}/\mathcal{L}) = \{1\}$ so $\mathcal{H} = \mathcal{L}$. \square

By Rosenlicht [24, Corollary 1, p. 433], we know that $D = \text{Gal}(\mathcal{G}/\mathcal{L})$ is commutative, in fact central in $\text{Gal}(\mathcal{G}/\mathcal{F})$. Unfortunately we cannot conclude that D is an Abelian variety, Rosenlicht [24, middle of p. 441] gives a counterexample.

If \mathcal{E} is a Picard-Vessiot extension of \mathcal{F} and \mathcal{H} is a Picard-Vessiot extension of \mathcal{E} , it does not follow that \mathcal{H} is a Picard-Vessiot extension or even contained in a Picard-Vessiot extension of \mathcal{F} . Magid [19, bottom of p. 12] has an example with all the details worked out. However, one might hope that \mathcal{H} is contained in a *strongly normal extension* of \mathcal{F} . Even that is false.

Proposition 11.4. *Suppose that \mathcal{E} is a Picard-Vessiot extension of \mathcal{F} , and \mathcal{H} is a Picard-Vessiot of \mathcal{E} . If \mathcal{H} is contained in a strongly normal extension of \mathcal{F} , then it is contained in a Picard-Vessiot extension of \mathcal{F} .*

Proof. If \mathcal{G} is strongly normal over \mathcal{F} with $\mathcal{H} \subset \mathcal{G}$, then $\mathcal{E} \subset \mathcal{L} = \mathcal{L}(\mathcal{G}/\mathcal{F})$ by Proposition 10.4. By the previous proposition $\mathcal{H}\mathcal{L} = \mathcal{L}$, so $\mathcal{H} \subset \mathcal{L}$. \square

12. ABELIAN EXTENSIONS

Definition 12.1. A strongly normal extension \mathcal{G} over \mathcal{F} is said to be *abelian* if $\text{Gal}(\mathcal{G}/\mathcal{F})$ is an abelian variety.

The following is sometimes called the Chevalley-Barsotti structure theorem.

Proposition 12.2. *Let X be a connected algebraic group over \mathbb{C} . Then there exists a linear connected normal algebraic subgroup L of X such that X/L is an abelian variety.*

Proof. Rosenlicht [24, Theorem 16, p. 439]. □

Thus, for any algebraic group, there is a chain of subgroups

$$X \supset X^\circ \supset L \supset 1,$$

where X° is the connected component of the identity. If X is the Galois group of a strongly normal extension \mathcal{G} of \mathcal{F} , we have a tower of fields

$$\mathcal{F} \subset \mathcal{F}^\circ \subset \mathcal{E} \subset \mathcal{G}.$$

\mathcal{F}° is a finite normal extension of \mathcal{F} with Galois group X/X° , \mathcal{E} is an abelian extension of \mathcal{F} with Galois group X°/L , and \mathcal{G} is a Picard-Vessiot extension of \mathcal{E} with Galois group L . The first and third steps of this tower have been extensively studied. But the middle step, and how the three fit together, are less familiar.

Kolchin [10] characterizes abelian extensions using invariant differentials. An updated version of that work would certainly use the logarithmic derivative, defined in the next section. The following example is presented in [10, Section 3, p. 788]. Kolchin also proves that every abelian extension of $\mathbb{C}(z)$ is of this form.

Let $X = \mathbb{C}^g/\Lambda$ be an abelian variety, where Λ is a non-degenerate lattice. Use $\mathbf{u} = (u_1, \dots, u_g)$ for the coordinate functions on \mathbb{C}^g and let $f_1(\mathbf{u}), \dots, f_n(\mathbf{u})$ be generators of the field of functions meromorphic on \mathbb{C}^g and periodic for Λ . Choose meromorphic functions of one variable, $\mathbf{a}(z) = (a_1(z), \dots, a_g(z))$, with the property that

$$a'_i(z) \in \mathbb{C}(z), \quad i = 1, \dots, g.$$

Then

$$\mathcal{G} = \mathbb{C}(z)(f_1(\mathbf{a}(z)), \dots, f_n(\mathbf{a}(z)))$$

is a strongly normal extension of $\mathbb{C}(z)$ whose Galois group is a subgroup of (the \mathbb{C} -rational points of) X .

13. LOGARITHMIC DERIVATIVE

The logarithmic derivative of matrices, described in Section 5, extends to arbitrary integral group schemes of finite type over $C = \text{spec } \mathbb{C}$. This was done using the Weil language of algebraic geometry in Kolchin [11, Section 7, p. 418] and Kovacic [15, Appendix, p. 532]. The logarithmic derivative in the setting of schemes is defined by Buim [3, Section 3.15, p. 24]. However he does not prove much about it, and to do so here would require more space than we are willing to use. Instead we simply state the definition, following Buim, and then some results, following Kolchin and Kovacic. Proofs (using Weil style algebraic geometry) are found in the references cited above. A complete treatment in modern language awaits development. The propositions here should be compared with those of Section 5.

Let \mathcal{G} be any Δ -field containing \mathcal{F} (and therefore \mathcal{C}) and let X be an irreducible group scheme of finite type over \mathcal{C} . Let a be a \mathcal{G} -valued point of X , which we can identify with a closed point of $X_{\mathcal{G}}$ that is rational over \mathcal{G} . We use the same symbol, a . We write the canonical mapping $\mathcal{O}_{X_{\mathcal{G}},a} \rightarrow \mathcal{G}$ as $f \mapsto f(a)$.

For each $i = 1, \dots, m$, we wish to define a tangent vector $\delta_{i,a}$ to X at a , i.e. a local derivation of $\mathcal{O}_{X_{\mathcal{G}},a}$ into \mathcal{G} over \mathcal{G} . Let $a_o \in X$ be the projection of a . Since $\mathcal{O}_{X_{\mathcal{G}},a}$ is a ring of quotients of $\mathcal{O}_{X,a_o} \otimes_{\mathcal{C}} \mathcal{G}$, it suffices to define the action of $\delta_{i,a}$ on \mathcal{O}_{X,a_o} .

Definition 13.1. For $i = 1, \dots, m$ we let $\delta_{i,a}$ be the local derivation of $\mathcal{O}_{X_{\mathcal{G}},a}$ over \mathcal{G} with the property that

$$\delta_{i,a}(f) = \delta_i(f(a)),$$

whenever $f \in \mathcal{O}_{X,a_o}$.

Let $\text{Lie}_{\mathcal{G}}(X) = \text{Lie}(X_{\mathcal{G}})$ denote the Lie algebra of *right* invariant derivations on $X_{\mathcal{G}}$. (Using right invariant derivations rather than left makes the formulas here similar to those of Section 5.)

Definition 13.2. For each $i = 1, \dots, m$, denote by $\ell\delta_i a$ the element of $\text{Lie}_{\mathcal{G}}(X)$ satisfying

$$(\ell\delta_i a(f))(a) = \delta_{i,a}(f).$$

Thus, $(\ell\delta_i a(f))(a) = \delta_i f(a)$ whenever $f \in \mathcal{O}_{X,a_o}$. We can give $\mathcal{O}_{X_{\mathcal{G}}}$ a natural structure of a sheaf of Δ -rings. Indeed, in the affine case $X = \text{spec } \mathcal{D}$,

$$\mathcal{O}_{X_{\mathcal{G}}}(X_{\mathcal{G}}) = \mathcal{D} \otimes_{\mathcal{C}} \mathcal{G},$$

which can be made into a Δ -ring by considering \mathcal{D} to be a ring of constants. This is what Buism [3, p. 4] calls the “trivial lifting” of Δ . It allows us to make $\text{Lie}_{\mathcal{G}}(X)$ into a Δ -vector space over \mathcal{C} by defining

$$\delta_i(A) = \delta_i \circ A - A \circ \delta_i, \quad A \in \text{Lie}_{\mathcal{G}}(X), \quad i = 1, \dots, m.$$

Definition 13.3. The \mathcal{C} -vector space of all $\mathbf{A} = (A_1, \dots, A_m) \in \text{Lie}_{\mathcal{G}}(X)^m$ that satisfy the *integrability conditions*

$$\delta_i A_j - \delta_j A_i = [A_i, A_j] \quad (1 \leq i, j \leq m)$$

is denoted by $\mathbf{I}_{\mathcal{G}}(X)$.

If a is a \mathcal{G} -valued point of X , then

$$\ell\Delta a = (\ell\delta_1 a, \dots, \ell\delta_m a) \in \mathbf{I}_{\mathcal{G}}(X).$$

Definition 13.4. If a is a \mathcal{G} -valued point of X , then $\ell\Delta a = (\ell\delta_1 a, \dots, \ell\delta_m a) \in \mathbf{I}_{\mathcal{G}}(X)$ is called the *logarithmic derivative* of a .

The group X acts on the Lie algebra by the adjoint operation and $\ell\Delta: X_{\mathcal{G}} \rightarrow \mathbf{I}_{\mathcal{G}}(X)$ is a crossed homomorphism, i.e.

$$\ell\Delta(ab) = \ell\Delta a + \text{Ad}(a)(\ell\Delta b).$$

Proposition 13.5. $\ell\Delta a = \ell\Delta b$ if and only if $b = ac$ for some $c \in X_{\mathcal{G}^{\Delta}}$.

Since the residue class field $\kappa(a_o) = \mathcal{O}_{X,a_o}/\mathfrak{m}_{X,a_o}$ is identified with a subfield of \mathcal{G} , we can define

$$\mathcal{F}\langle a \rangle = \mathcal{F}\langle \kappa(a_o) \rangle.$$

Proposition 13.6. *Suppose that a is a \mathcal{G} -valued point of X such that*

- (1) $\ell\Delta a \in \mathbf{I}_{\mathcal{F}}(X)$,
- (2) $\mathcal{G} = \mathcal{F}\langle a \rangle$,
- (3) $\mathcal{G}^{\Delta} = \mathcal{C}$.

Then \mathcal{G} is a strongly normal extension of \mathcal{F} , and there is an injective homomorphism of $\text{Gal}(\mathcal{G}/\mathcal{F})$ into the \mathcal{C} -rational points of X .

\mathcal{G} is called a X -primitive extension of \mathcal{F} and a is an X -primitive.

Proposition 13.7. *Let $\mathbf{A} \in \mathbf{I}_{\mathcal{F}}(X)$. Then there exists a Δ -extension field \mathcal{G} of \mathcal{F} and a \mathcal{G} -valued point a of X such that $\ell\Delta a = \mathbf{A}$ and $\mathcal{G}^{\Delta} = \mathcal{C}$.*

14. EXAMPLES OF STRONGLY NORMAL EXTENSIONS

Proposition 13.6 provides a factory for producing examples of strongly normal extensions. The trick, of course, is to compute $\ell\Delta$.

Example 14.1. Consider the elliptic curve of Example 2.7. As we had observed, $a = [\eta, \eta'/\alpha, 1]$ is a \mathcal{G} -valued point of E . We claim that it is an E -primitive over \mathcal{F} .

Let $x = X/Z, y = Y/Z$ be the non-homogeneous coordinate functions (Silverman [25, p. 46]). Then $\text{Lie}_{\mathcal{G}}(E)$ is generated, as a \mathcal{G} -vector space, by

$$y \frac{d}{dx}.$$

This is “well known” and is verified computationally in Kolchin [11, Example 3, p. 328]. Let us write

$$\ell\delta a = Ay \frac{d}{dx},$$

for some $A \in \mathcal{G}$. Then, using Definition 13.2, we have

$$A \frac{\eta'}{\alpha} = \left(Ay \frac{dx}{dx} \right)(a) = \ell\delta a(x)(a) = \delta(x(a)) = \eta',$$

so that $A = \alpha \in \mathcal{F}$.

Example 14.2. Consider a hyperelliptic curve C of genus g

$$y^2 = f(x) = 4 \prod_{k=1}^{2g+1} (x - e_k),$$

where $e_1, \dots, e_{2g+1} \in \mathcal{C}$ are distinct. Using Proposition 13.6 we can construct a strongly normal extension having the Galois group a subgroup of the abelian variety $\text{Jac}(C)$, the Jacobian of C . (For an algebraic treatment of the Jacobian, see Mumford [21]. The appendix of Koblitz [6] is a nice introduction, although the emphasis is on cryptography.) Mumford [21, Theorem 3.1, p. 42] computes the Lie algebra using analytic methods, and his answer is phrased in terms of certain symmetric functions of $\mathbf{x} = (x_1, \dots, x_g)$ and $\mathbf{y} = (y_1, \dots, y_g)$. We prefer expressing the derivatives as (necessarily symmetric) functions of \mathbf{x} and \mathbf{y} themselves.

We use the notation

$$\sigma_k(x_1, \dots, \hat{x}_i, \dots, x_g) = \sum_{\substack{1 \leq j_1 < \dots < j_k \leq g \\ j_1 \neq i, \dots, j_k \neq i}} x_{j_1} \cdots x_{j_k}$$

for the the k -th elementary symmetric functions of $g-1$ variables, x_i being omitted.

Definition 14.3. For $k = 0, \dots, g-1$, define derivations D_k of $\mathcal{C}(\mathbf{x}, \mathbf{y})$ over \mathcal{C} by

$$D_k = \sum_{i=1}^g \sigma \sigma_k(x_1, \dots, \hat{x}_i, \dots, x_g) \frac{y_i}{\prod_{j \neq i} (x_i - x_j)} \frac{\partial}{\partial x_i}.$$

It can be shown that D_k are right invariant and form a basis of $\text{Lie}(\text{Jac}(C))$. Let \mathcal{G} be an extension of \mathcal{F} and fix a point of $\text{Jac}(C)_{\mathcal{G}}$

$$a = (\eta_1, \xi_1) + \dots + (\eta_g, \xi_g) - g\infty.$$

We wish to compute

$$\ell \delta a \in \text{Lie}_{\mathcal{G}}(\text{Jac}(C)),$$

i.e. find $A_0, \dots, A_{g-1} \in \mathcal{G}$ with

$$\ell \delta a = \sum_{k=0}^{g-1} (-1)^k A_k D_{g-1-k}.$$

Using Definition 13.2 (with $f = x_1, \dots, x_g$) it is not difficult to see that

$$A_k = \sum_{i=1}^g \frac{\eta'_i}{\xi_i} \eta_i^k, \quad k = 0, \dots, g-1.$$

Proposition 14.4. Suppose that η_i, ξ_i satisfy

- (1) $\xi_i^2 = f(\eta_i)$ for $i = 1, \dots, g$, and
- (2) $A_k = \sum_{i=1}^g \frac{\eta'_i}{\xi_i} \eta_i^k \in \mathcal{F}$ for $k = 0, \dots, g-1$.

Then $\mathcal{F}(\eta_1, \xi_1, \dots, \eta_g, \xi_g)_{\text{sym}}$ is a strongly normal extension of \mathcal{F} whose Galois group is a subgroup of $\text{Jac}(C)$.

For $g = 1$ we have $A_0 = \frac{\eta'_1}{\xi_1}$ which can be rewritten as

$$\eta'^2 = A_0^2 \xi^2 = A_0^2 f(\eta).$$

This is the result of Example 14.1. For $g = 2$ we get

$$\begin{aligned} A_0 &= \frac{\eta'_1}{\xi_1} + \frac{\eta'_2}{\xi_2}, \\ A_1 &= \frac{\eta'_1}{\xi_1} \eta_1 + \frac{\eta'_2}{\xi_2} \eta_2. \end{aligned}$$

Example 14.5. Suppose that $\mathcal{F} = \mathbb{C}(z)$, let $\mathbf{u} = (u_1, \dots, u_g)$ be g complex variables and define the hyperelliptic Kleinian \wp -functions

$$\wp_{ij}(\mathbf{u}), \quad 1 \leq i, j \leq g,$$

as in Baker [1, p. 36] or Buchstaber et al. [2, p. 9]. Let $x_1(\mathbf{u}), \dots, x_g(\mathbf{u})$ be solutions of the equation

$$P(X; \mathbf{u}) = X^g - \wp_{g,g}(\mathbf{u})X^{g-1} - \wp_{g,g-1}(\mathbf{u})X^{g-2} - \dots - \wp_{g,1}(\mathbf{u}) = 0,$$

and define

$$y_i(\mathbf{u}) = -\frac{\partial P(X; \mathbf{u})}{\partial u_g}(x_i).$$

Suppose that $\mathbf{a} = (a_1(z), \dots, a_g(z))$ are g functions of z , $\eta_i = x_i(\mathbf{a})$ and $\xi_i = y_i(\mathbf{a})$. Then, using Buchstaber et al. [2, p. 11],

$$\ell\delta((\eta_1, \xi_1) + \dots + (\eta_g, \xi_g) - g\infty) = a_1(z)'D_0 + \dots + a_g'(z)D_{g-1}.$$

If we suppose that $a_i(z)' \in \mathbb{C}(z)$, then

$$\mathcal{G} = \mathbb{C}(z)(\eta, \xi)_{\text{sym}} = \mathbb{C}(z)(\wp_{ij}(\mathbf{a}(z))_{1 \leq i, j \leq g})$$

is a strongly normal extension of $\mathbb{C}(z)$ whose Galois group is a subgroup of $\text{Jac}(C)$.

15. EXISTENCE OF STRONGLY NORMAL EXTENSIONS

Galois groups of strongly normal extensions are quite abundant as the following proposition shows.

Proposition 15.1. *Let X be a connected algebraic group over \mathbb{C} . There exist Δ -fields $\mathcal{F} \subset \mathcal{G}$ such that \mathcal{G} is a strongly normal extension of \mathcal{F} whose Galois group is isomorphic to the group of \mathbb{C} -rational points of X .*

Proof. Kolchin [9, Theorem 2, p. 880]. □

Kolchin's proof is quite intricate. It uses invariant derivations and surely can (and should) be recast using the logarithmic derivative. Note that we do not fix \mathcal{F} in advance. To do so would be to solve the “inverse problem”, which, for strongly normal extensions, is treated in Kovacic [14].

On the other hand, strongly normal extensions are not easily obtained from equations. A linear homogeneous differential equation gives rise to a Picard-Vessiot extension, but a non-linear differential equation need not give rise to a strongly normal extension.

Example 15.2. Let $\mathcal{F} = \mathbb{C}(z)$ and consider the first Painlevé equation

$$y'' = 6y^2 + z.$$

Proposition 15.3. *If \mathcal{G} is strongly normal over \mathcal{F} and $\eta \in \mathcal{G}$ satisfies the first Painlevé equation, then η is algebraic over \mathcal{F} .*

Proof. Nishioka [23, p. 63]. □

Corollary 15.4. *Painlevé's first transcendent is not contained in any strongly normal extension of \mathcal{F} .*

Nishioka [23] and Umemura [28] have studied the question of which non-linear equations have solutions in a strongly normal extension. They show that a non-linear differential equation has a solution in a strongly normal extension if and only if “the solution depends rationally on arbitrary constants”.

Matsuda [20] studies first order differential equations. He shows that a solution is contained in a strongly normal extension if and only if the equation has “no moveable singularities”. Buium [3] extended this work to arbitrary order. His definition of “no moveable singularities” is that there exists a projective model having certain properties, however Example 15.2 seems to indicate that his definition does not correspond to the classical one.

REFERENCES

1. Baker, H. F., *An introduction to the theory of multiply periodic functions*, Cambridge University Press, Cambridge, England, 1907.
2. Buchstaber, V. M., Enolskiĭ, V. Z., Leikin, D. V., *Hyperelliptic Kleinian functions and applications*, Solitons, geometry, and topology: on the crossroad, Amer. Math. Soc. Transl. Ser. 2, 179, 1–33, Amer. Math. Soc., Providence, RI, 1997. MR1437155 (98b:14029)
3. Buium, Alexandru, *Differential function fields and moduli of algebraic varieties*, Lecture Notes in Mathematics, 1226, Springer-Verlag, Berlin, 1986, x+146. MR0874111 (88e:14010)
4. Churchill, R. C., Kovacic, Jerald J., *Cyclic vectors*, Differential algebra and related topics (Newark, NJ, 2000), 191–218, World Sci. Publishing, River Edge, NJ, 2002. MR1921700 (2003h:12007)
5. Kaplansky, Irving, *An introduction to differential algebra*, Hermann, Paris, 1976, 64. MR0460303 (57:297)
6. Koblitz, Neal, *Algebraic aspects of cryptography, with an appendix by Alfred J. Menezes, Yi-Hong Wu and Robert J. Zuccherato*, Algorithms and Computation in Mathematics, 3, Springer-Verlag, Berlin, 1998, x+206. MR1610535 (2000a:94012)
7. Kolchin, E. R., *Picard-Vessiot theory of partial differential fields*, Proc. Amer. Math. Soc., 3, 1952, 596–603. (Reprinted in [12].) MR0049883 (14:241c)
8. Kolchin, E. R., *Galois theory of differential fields*, Amer. J. Math., 75, 1953, 753–824. (Reprinted in [12].) MR0058591 (15:394a)
9. Kolchin, E. R., *On the Galois theory of differential fields*, Amer. J. Math., 77, 1955, 868–894. (Reprinted in [12].) MR0073588 (17:455a)
10. Kolchin, E. R., *Abelian extensions of differential fields*, Amer. J. Math., 82, 1960, 779–790. (Reprinted in [12].) MR0132066 (24:A1913)
11. Kolchin, E. R., *Differential algebra and algebraic groups*, Academic Press, New York, 1973, xviii+446. MR0568864 (58:27929)
12. Kolchin, Ellis, *Selected works of Ellis Kolchin with commentary*, American Mathematical Society, Providence, RI, 1999, xiv+639. MR1677530 (2000g:01042)
13. Kolchin, Ellis, Lang, Serge, *Algebraic groups and the Galois theory of differential fields*, Amer. J. Math., 80, 1958, 103–110. MR0094596 (20:1109)
14. Kovacic, J., *On the inverse problem in the Galois theory of differential fields. II.*, Ann. of Math. (2), 93, 1971, 269–284. MR0285514 (44:2732)
15. Kovacic, J., *Pro-algebraic groups and the Galois theory of differential fields*, Amer. J. Math., 95, 1973, 507–536. MR0340228 (49:4983)
16. Kovacic, Jerald J., *Differential schemes*, Differential algebra and related topics (Newark, NJ, 2000), 71–94, World Sci. Publishing, River Edge, NJ, 2002. MR1921695 (2003i:12010)
17. Kovacic, Jerald J., *The differential Galois theory of strongly normal extensions*, Trans. Amer. Math. Soc., 355, 2003, 11, 4475–4522 (electronic). MR1990759 (2004i:12008)
18. Magid, Andy R., *Lectures on differential Galois theory*, University Lecture Series, 7, American Mathematical Society, Providence, RI, 1994, xiv+105. MR1301076 (95j:12008)
19. Magid, Andy R., *The Picard-Vessiot antiderivative closure*, J. Algebra, 244, 2001, 1, 1–18. MR1856528 (2003a:12005)
20. Matsuda, Michihiko, *First-order algebraic differential equations*, Lecture Notes in Mathematics, 804, Springer, Berlin, 1980, vi+111. MR0576060 (82d:12015)
21. Mumford, David, *Tata lectures on theta. II*, Progress in Mathematics, 43, Birkhäuser Boston, Inc. Boston, MA, 1984, xiv+272. MR0742776 (86b:14017)
22. Nagata, Masayoshi, *Field theory*, Marcel Dekker, Inc., New York, 1977, vii+268. MR0469887 (57:9667)
23. Nishioka, Keiji, *A note on the transcendency of Painlevé's first transcendent*, Nagoya Math. J., 109, 1988, 63–67. MR0931951 (89c:12003)
24. Rosenlicht, Maxwell, *Some basic theorems on algebraic groups*, Amer. J. Math., 78, 1956, 401–443. MR0082183 (18:514a)
25. Silverman, Joseph H., *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, 106, Springer-Verlag, New York, 1986, xii+400. MR0817210 (87g:11070)
26. Singer, Michael F., *Algebraic relations among solutions of linear differential equations*, Trans. Amer. Math. Soc., 295, 1986, 2, 753–763. MR0833707 (87f:12015)

- 27. Takeuchi, Mitsuhiro, *A Hopf algebraic approach to the Picard-Vessiot theory*, J. Algebra, 122, 1989, 2, 481–509. MR0999088 (90j:12016)
- 28. Umemura, Hiroshi, *Birational automorphism groups and differential equations*, Nagoya Math. J., 119, 1990, 1–80. MR1071899 (91j:12015)
- 29. van der Put, Marius, Singer, Michael F., *Galois theory of linear differential equations*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 328, Springer-Verlag, Berlin, 2003, xviii+438. MR1960772 (2004c:12010)

DEPARTMENT OF MATHEMATICS, THE CITY COLLEGE OF THE CITY UNIVERSITY OF NEW YORK,
NEW YORK, NEW YORK 10031

E-mail address: jkovacic@member.ams.org

URL: <http://mysite.verizon.net/jkovacic>