

Strongly normal extensions

Jerald J. Kovacic

The City College of CUNY, New York, NY

This file is available at:

<http://www.sci.ccny.cuny.edu/~ksda/gradcenter.html>

January 25, 2008

The differential Galois theory of strongly normal extensions is ripe for study. It has been neglected, possibly because Kolchin used his own axiomatic definition of algebraic group. Instead, we use differential schemes, another area ripe for study.

We start with a sketch of Picard-Vessiot theory emphasizing its connection with tensor products.

After defining strongly normal extensions, we show that an approach similar to that used for Picard-Vessiot theory also works for strongly normal extensions. However we must replace differential rings with differential schemes. This is not surprising as the Galois group is a group scheme that is not necessarily affine. Strongly normal extensions are abundant; every connected group scheme is the Galois group of some strongly normal extension. And there is a “factory” to produce them - the logarithmic derivative. Yet explicit examples are difficult to find. There has been some work on characterizing the type of equation needed, but much more is needed.

For ease of exposition we restrict our attention to ordinary Δ -rings.

We fix a base field K , which is a Δ -field of characteristic 0. All Δ -rings are assumed to contain K .

This implies that they are \mathbb{Q} algebras, i.e. Ritt algebras. In characteristic p is it better to use Hasse-Schmidt or iterated derivations.

We also assume that $C = K^\Delta$, the field of constants of K , is algebraically closed. This permits us to use group schemes as topological spaces rather than as representable functors.

In Galois theory, one starts with a polynomial equation

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0 = 0,$$

and considers the set of all of its roots $\{\eta_1, \dots, \eta_n\}$. Then the group of permutations of these roots is the Galois group of the equation.

There is an exact analog for differential algebra: the Picard-Vessiot theory.

Linear homogeneous differential equations

Start with a linear homogeneous differential equation

$$L(y) = a_n y^{(n)} + a_{n-1} y^{(n-1)} + \dots + a_0 y = 0.$$

There is a “fundamental system of solutions”, η_1, \dots, η_n , with the property that any solution can be expressed as a linear combination of these and constants.

This means that there is a “formula”

$$F = \sum_{i=1}^n y_i C_i \in K[y_1, \dots, y_n][C_1, \dots, C_n]$$

such that

$$\eta = F(\eta_1, \dots, \eta_n, c_1, \dots, c_n)$$

is a solution for every choice of constants c_1, \dots, c_n and every solution is of this form.

This is called a “superposition formula” (particularly by physicists).

Let $L = K\langle\eta_1, \dots, \eta_n\rangle$. If σ is a Δ -automorphism of L over K then

$$\sigma\eta_j = F(\eta_1, \dots, \eta_n, c_{1j}(\sigma), \dots, c_{nj}(\sigma)).$$

for some constants $c_{ij}(\sigma)$.

The set of Δ -automorphisms forms a group under composition, and that induces a group structure on the set of $c_{ij}(\sigma)$.

In fact, the mapping

$$\sigma \mapsto (c_{ij}(\sigma)) \in \text{GL}(n, C)$$

gives an injective homomorphism from the group of all Δ -automorphisms of L over K onto an algebraic subgroup of $\text{GL}(n, C)$.

The Weierstraß \wp -function satisfies the differential equation

$$y'^2 = 4y^3 - g_2y - g_3$$

where $g_2, g_3 \in \mathbb{C}$ and $g_2^3 \neq 27g_3^2$. There is a superposition formula:

$$F = -(y + C) + \frac{1}{4} \left(\frac{y' - D}{y - C} \right)^3 \in K\langle y \rangle(C, D).$$

If c, d are constants with $d^2 = 4c^3 - g_2c - g_3$ then

$$\eta = F(\wp, c, d)$$

is a solution of the differential equation and every solution has this form.

Here \wp is called a “fundamental solution” since every other solution can be expressed in terms of it and constants.

Definition

We say that a system of differential equations has a “superposition formula” if there is a set of solutions η_1, \dots, η_n , called a “fundamental system of solutions” and a Δ -rational function

$$F \in K\langle y_1, \dots, y_n \rangle(C_1, \dots, C_r)$$

such that every solution is of the form

$$\eta = F(\eta_1, \dots, \eta_n, c_1, \dots, c_r)$$

for some constants c_1, \dots, c_r .

This should be taken with a grain of salt as we do not specify where the constants come from.

Definition

A strongly normal extension is a Δ -field extension field L of K such that

- 1 L is generated by a fundamental system of solutions of a system of Δ -equations with a superposition formula,
- 2 $L^\Delta = C$.

We will make this more precise.

But there is another approach to Galois theory.

A field extension L of K is normal every isomorphism (into some extension field of L) is an automorphism.

The equivalent condition for Δ -algebra is too strong; it implies that L is algebraic over K .

Ellis Kolchin tried some alternative definitions.

Definition

L is *weakly normal* if K is the fixed field of the set of all Δ -automorphisms of L over K .

He was unable to prove much with this definition.

Definition

L is *normal* over K if it is weakly normal over every intermediate Δ -field.

With this one he did a little better:

Theorem

Suppose that L is normal over K and let $\text{Gal}(L/K)$ be the group of Δ -automorphisms of L over K . Then the mapping

$$M \rightarrow \text{Gal}(L/M) \quad \text{where} \quad K \subset M \subset L$$

is bijective onto a certain subset of the set of all subgroups of $\text{Gal}(L/K)$.

Kolchin referred to the underlined phrase as a blemish (“a minor imperfection”). He was unable to characterize the sets.

Kolchin observed that if we have a superposition formula then the Galois group of all Δ -automorphisms of L over K can be described as an algebraic group of constants. This is the characterization he needed.

Definition

By a Δ -isomorphism of L over K we mean a Δ -isomorphism of L over K onto a Δ -subfield of a Δ -field E where $L \subset E$.

This is what Kaplansky calls an “admissible isomorphism”. It allows us to form the field compositum

$$L\sigma L \subset E.$$

If you have the notion of “universal Δ -field” you can require that all Δ -isomorphisms have target in this universal Δ -field. In this case you can speak about the *set of Δ -isomorphisms*.

If σ is a Δ -isomorphism of L over K then we define

$$C(\sigma) = (L\sigma L)^\Delta.$$

Definition

A Δ -isomorphism σ is *strong* if

- $\sigma(c) = c$ whenever $c \in L^\Delta$
- $L\sigma L = LC(\sigma) = \sigma LC(\sigma)$.

Definition

L is *strongly normal* over K if

- L is finitely Δ -generated over K ,
- every Δ -isomorphism of L over K is strong, and
- $L^\Delta = C$,

Thus L is strongly normal if every Δ -isomorphism satisfies

$$L\sigma L = LC(\sigma) = \sigma LC(\sigma).$$

If $L = K\langle\eta_1, \dots, \eta_n\rangle$ where the η_i are solutions of some Δ -equation, then $\sigma\eta_i$ is also a solution and the condition is that $\sigma\eta_i$ be a Δ -rational function of η_1, \dots, η_n and constants.

Suppose that L is strongly normal over K and let $\text{Gal}(L/K)$ denote the group of Δ -automorphisms of L over K .

Theorem

$\text{Gal}(L/K)$ may be identified with an algebraic group defined over C (not necessarily affine). There is a bijection between intermediate Δ -fields and closed subgroups of $\text{Gal}(L/K)$.

There are no blemishes here. Examples are Picard-Vessiot extensions, and Weierstraß extensions.

Theorem

Suppose that L is strongly normal over K .

- *L is a finite normal extension if and only if $\text{Gal}(L/K)$ is finite.*
- *L is a Picard-Vessiot extension if and only if $\text{Gal}(L/K)$ is linear (equivalently affine).*
- *L is a Weierstraß extension if and only if $\text{Gal}(L/K)$ is isomorphic to the elliptic curve.*

Given a linear homogeneous differential equation we can always produce a Picard-Vessiot extension. If

$$A \in \text{Mat}(n, K)$$

then there exists a Δ -extension field L and $\alpha \in \text{GL}(n, L)$ with

$$\ell\delta \alpha = \alpha' \alpha^{-1} = A$$

such that $L = K(\alpha)$ is a Picard-Vessiot extension of K , i.e. $L^\Delta = C$.

The logarithmic derivative of matrices extends to arbitrary algebraic groups defined over \mathbb{C} .

Suppose that G is a connected algebraic group defined over C (or an integral group scheme of finite type over $\text{Spec } C$). Let E be some Δ -extension field of K .

Theorem

If α is an E -rational point of G then there is an element of the Lie algebra

$$\ell\delta\alpha \in \text{Lie}_E(G) = E \otimes_C \text{Lie}(G)$$

such that

$$(\ell\delta\alpha(f))(\alpha) = (f(\alpha))'$$

whenever $f \in \mathcal{O}_{G\alpha}$.

Definition

$\ell\delta\alpha$ is called the *logarithmic derivative of α* .

Theorem

If α and β are E -valued points of G then

$$l\delta(\alpha\beta) = l\delta\alpha + \text{Ad}(\alpha)(l\delta\beta)$$

where Ad is the adjoint action of G on its lie algebra.

Theorem

If $l\delta\alpha = l\delta\beta$ then there exists an E^Δ valued point c of G with $\beta = \alpha c$.

Theorem

If α is an E valued point of G and σ is a Δ -isomorphism of E (into some Δ -field containing E) then

$$l\delta\sigma\alpha = \sigma l\delta\alpha.$$

Theorem

Suppose that G is a connected algebraic group defined over C and $\alpha \in G$ has the properties:

- $\ell\delta\alpha \in \text{Lie}_K(G)$,
- $L = K(\alpha)$,
- $L^\Delta = C$.

Then L is a strongly normal extension of K .

In this case L is called a G -primitive extension of K .

Just as in the Picard-Vessiot theory we have existence and uniqueness.

Theorem

Let $A \in \text{Lie}_K(G)$. Then there exists a Δ -field extension L of K and an L rational point α satisfying the properties of the previous theorem. In addition L is unique up to Δ -isomorphism.

Thus the logarithmic derivative is a factory for producing strongly normal extensions.

However we cannot assert that every strongly normal extension is a G -primitive extension for some G . This is a cohomological question and reduces to the question of whether or not a given torsor for G has a K -rational point.

Theorem

Let G be a connected algebraic group defined over C . Then there exists a Δ -field K and a strongly normal extension L over K such that $\text{Gal}(L/K) = G(C)$.

Actually Kolchin proved this without using the logarithmic derivative. If G is not connected, the result is not known. The inverse problem for strongly normal extensions is completely solved over $C(x)$ and many other fields. Using a sequence of reductions one gets to the hard case: non-connected linear algebraic groups. Abelian varieties pose little problem.

On the other hand, differential equations giving rise to strongly normal extensions are very complicated.

For example, consider a hyperelliptic curve of genus 2

$$s^2 = f(t) = t(t-1)(t+1)(t-2)(t+2) = t^5 - 5t^3 + 4t$$

Suppose that

$$\xi_1^2 = f(\eta_1) \quad \text{and} \quad \xi_2^2 = f(\eta_2)$$

and that there exist $a, b \in K$ with

$$a = \frac{\eta_1'}{\xi_1} + \frac{\eta_2}{\xi_2}$$
$$b = \frac{\eta_1'}{\xi_1} \eta_1 + \frac{\eta_2'}{\xi_2} \eta_2$$

Let

$$E = K\langle \eta_1, \eta_2, \xi_1, \xi_2 \rangle.$$

If L is the subfield of E consisting of all expressions in η_1, ξ_i that are symmetric in $i = 1, 2$, then L is a strongly normal extension of K and $\text{Gal}(L/K)$ is identified with a subgroup of the Jacobian of the hyperelliptic curve of genus 2.

Set (following Mumford Theta II)

$$u_1 = -(\eta_1 + \eta_2)$$

$$u_2 = \eta_1 \eta_2$$

$$v_1 = \frac{\xi_1 - \xi_2}{\eta_1 - \eta_2}$$

$$v_2 = \frac{\xi_2 \eta_1 - \xi_1 \eta_2}{\eta_1 - \eta_2}$$

These are the coordinates of an affine patch of the Jacobian of the curve.

Theorem

$L = K(u_1, u_2, v_1, v_2)$ is a strongly normal extension of K whose Galois group is contained in the Jacobian of the hyperelliptic curve of genus 2.

One can write down the equations satisfied by the coordinates of the Jacobian. First the algebraic equations:

$$\begin{aligned}0 &= 4 - 2v_1v_2 + 5u_2 + u_2^2 - 3u_2u_1^2 + u_1v_1^2 - 5u_1^2 + u_1^4 \\0 &= u_2u_1^3 + u_2v_1^2 - v_2^2 - 5u_1u_2 - 2u_1u_2^2\end{aligned}$$

These can be combined to get a quartic equation for v_1 over $K(u_1, u_2)$ and then a quadratic equation for v_2 over $K(u_1, u_2, v_1)$. Then the differential equations

$$\begin{aligned}u_1' &= -av_2 \\u_2' &= -bv_2 - a(v_2u_1 - u_2v_1)\end{aligned}$$

where $a, b \in K$.

The derivatives of v_1 and v_2 are a mess and can be obtained by differentiating the quartic and quadratic equations for v_1 and v_2 .

One can argue that ordinary Galois theory is about ring extensions not field extensions. It is just “luck” that $K[\alpha_1, \dots, \alpha_n]$ turns out to be a field.

This observation is used in the current treatment of Picard-Vessiot theory.

Let $L = K(\alpha)$ be a Picard-Vessiot extension of K with $\alpha \in \text{GL}(n, L)$ and $\ell\delta\alpha = A \in \text{Mat}(n, K)$.

We define the Picard-Vessiot ring by:

$$P = K[\alpha, 1/\det \alpha] = K[\alpha, \alpha^{-1}].$$

Theorem

P is independent of the choice of α . I.e. if $L = K(\beta)$ where $\beta \in \text{GL}(r, L)$ and $\ell\delta\beta = B \in \text{Mat}(r, K)$ then

$$K[\alpha, \alpha^{-1}] = K[\beta, \beta^{-1}].$$

A field (not a Δ -field) may be characterized by the following equivalent conditions.

- 1 it has no proper non-zero ideal,
- 2 (0) is a maximal ideal
- 3 every non-zero element is a unit.

A unit is an element a with $1 \in (a)$.

Definition

In a Δ -ring an element a with $1 \in [a]$ is called a Δ -unit.

Definition

A Δ -ring is Δ -simple if it satisfies the following equivalent conditions.

- 1 it has no proper non-zero Δ -ideal,
- 2 (0) is a maximal Δ -ideal,
- 3 every non-zero element is a Δ -unit.

So a Δ -simple ring is a close analog to a field.

Theorem

If R is Δ -simple then R is a domain and, if R is finitely generated (even finitely Δ -generated) over K then

$$\text{qf}(R)^\Delta = C.$$

Theorem

The Picard-Vessiot ring P is Δ -simple.

There is a more precise statement.

Theorem

Suppose that P is a domain with $P = K[\alpha, \alpha^{-1}]$, where $\ell\delta\alpha \in \text{Mat}(n, K)$. Then P is Δ -simple if and only if $K(\alpha)^\Delta = C$.

Some authors use this fact to give a different definition of Picard-Vessiot extension.

Let P be a Picard-Vessiot ring.

Definition

Let

$$D = (P \otimes_K P)^\Delta$$

For many purposes $L \otimes_K L$ works the same, and sometimes is better since L is a field. For example

Theorem

There is a bijection between radical (prime, maximal) Δ -ideals of $P \otimes_K P$ and radical (prime, maximal) Δ -ideals of $L \otimes_K L$.

Theorem

$$D = (P \otimes_K P)^\Delta = (L \otimes_K L)^\Delta.$$

Theorem

The Δ -homomorphism

$$P \otimes_C D \longrightarrow P \otimes_K P$$

$$a \otimes d \longmapsto (a \otimes 1)d$$

is an isomorphism.

We even have a converse.

Theorem

Suppose that R is a Δ - K -algebra that is finitely generated (as an algebra) over K and is Δ -simple. Also suppose that E is a C -algebra (thought of as a Δ -ring with trivial derivation) and there is an R -isomorphism

$$R \otimes_K R \approx R \otimes_C E.$$

Then R is a Picard-Vessiot ring and $E \approx (R \otimes_K R)^\Delta$.

The theorem states that

$$L = K(\alpha), \quad \alpha \in \mathrm{GL}(n, L)$$

with $\ell\delta \alpha = A \in \mathrm{Mat}(n, K)$, and that

$$R = P = K[\alpha, \alpha^{-1}].$$

Suppose that L is a strongly normal extension of K . We can consider

$$L \otimes_K L.$$

This is reduced but need not be a domain.

Let

$$D = (Q(L \otimes_K L))^{\Delta}.$$

Here Q signifies the complete ring of fractions (denominators are not divisors of zero).

Theorem

The Δ -homomorphism

$$\begin{aligned} L \otimes_C D &\longrightarrow Q(L \otimes_K L) \\ a \otimes d &\longmapsto \frac{a \otimes 1}{1 \otimes 1} d \end{aligned}$$

is injective and extends to a Δ -isomorphism

$$Q(L \otimes_C D) \approx Q(L \otimes_K L).$$

We even have a converse.

Theorem

Suppose that L is a Δ -field extension of K that is finitely generated (as a field) over K and has the property that $L^\Delta = K$. Also suppose that E is a C -algebra (thought of as a Δ -ring with trivial derivation) and there is an L -isomorphism

$$Q(L \otimes_K L) \approx Q(L \otimes_C E).$$

Then L is a strongly normal extension of K and $E \approx Q(L \otimes_K L)^\Delta$.

Suppose that $\sigma \in \text{Gal}(L/K)$, i.e. σ is a Δ -automorphism of σ over K . We define

$$\bar{\sigma}: L \otimes_K L \rightarrow L, \quad \bar{\sigma}(a \otimes_K b) = a\sigma b$$

and

$$\mathfrak{p}_\sigma = \ker \bar{\sigma}.$$

Theorem

The mapping $\sigma \mapsto \mathfrak{p}_\sigma$ is a bijection from $\text{Gal}(L/K)$ onto the set of maximal Δ -ideals of $L \otimes_K L$.

Thus the set of closed points of $\text{Diffspec}(L \otimes_K L)$ is the Galois group.

If L is a Picard-Vessiot extension of K we can get a lot more.

Theorem

There is a bijection between (prime, radical, maximal) ideals of D and (prime, radical, maximal) Δ -ideals of $P \otimes_K P$.

Corollary

There is a bijection from $\text{Gal}(L/K)$ onto the set of maximal ideals of D . Thus $\text{Gal}(L/K)$ may be identified with the set of closed (equivalently C -rational) points of $\text{spec } D$.

I.e. $\text{Gal}(L/K)$ can be identified with $\text{MaxSpec } D$.

Now let L be a strongly normal extension of K .

Definition

Let

$$X = \text{Diffspec}(L \otimes_K L).$$

Here Diffspec is the set of prime Δ -ideals. There is a natural way to introduce a sheaf of Δ -rings - e.g. follow Hartshorne.

If L is a Picard-Vessiot extension then X is isomorphic to $\text{Diffspec}(P \otimes_K P)$.

Theorem

The mapping

$$\mathrm{Gal}(L/K) \rightarrow X \quad \sigma \mapsto \mathfrak{p}_\sigma$$

is a bijection between $\mathrm{Gal}(L/K)$ and the closed (equivalently C -rational) points of X .

Thus $\mathrm{Gal}(L/K)$ may be identified with $X(C)$, the set of C -rational points of the Δ -scheme X .

But we want a group scheme not a Δ -group scheme, so we apply our handy constant functor.

For a Picard-Vessiot extension we have

$$\begin{aligned} X = \text{Diffspec}(L \otimes_K L) &\approx \text{Diffspec}(P \otimes_K P) \approx \text{Diffspec}(P \otimes_C D) \\ &\approx \text{Diffspec } P \times_{\text{Spec } C} \text{Spec } D \end{aligned}$$

and X is homeomorphic to $\text{Spec } D$.

We do something similar for strongly normal extensions.

Definition

Let X^Δ be the local ringed space where

- the topological spaces X and X^Δ are the same,
- for the sheaf

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

For an arbitrary Δ -scheme, X^Δ is merely a ringed space; it is not necessarily a scheme.

Theorem

If L is strongly normal over K , then X^Δ is a group scheme of finite type over $\text{spec } C$. It is canonically isomorphic to $\text{Gal}(L/K)$.

Where does the group structure come from?

There is a “standard” Sweedler coring structure on $L \otimes_K L$.
comultiplication:

$$\begin{aligned} L \otimes_K L &\rightarrow (L \otimes_K L) \otimes_L (L \otimes_K L) \\ a \otimes_K b &\longmapsto (a \otimes_K 1) \otimes_L (1 \otimes_K b) \end{aligned}$$

coidentity:

$$L \otimes_K L \rightarrow L \quad a \otimes_K b \mapsto ab$$

coinverse:

$$L \otimes_K L \rightarrow L \otimes_K L \quad a \otimes_K b \mapsto b \otimes_K a.$$

For a Picard-Vessiot extension we have the following:

Theorem

The co-operations induce a Hopf algebra structure on D and makes P into a D -comodule algebra. The ring of coinvariants is K .

Thus $\text{Spec } D$ is a group scheme and $\text{Spec } P$ is a torsor. This makes the Picard-Vessiot ring P into an example of a Hopf-Galois extension of K .

In Picard-Vessiot theory we had the fundamental isomorphism

$$P \otimes_K P \approx P \otimes_C D.$$

Applying Diffspec we have

$$X = \text{Diffspec}(P \otimes_K P) \approx \text{Diffspec } P \times_{\text{Diffspec } C} \text{Diffspec } D.$$

For strongly normal extensions we have a similar formula.

Theorem

$$X = \text{Diffspec}(L \otimes_K L) \approx \text{Diffspec } L \times_{\text{Diffspec } C} X^\Delta$$

Just as in Picard-Vessiot theory, we have a converse.
Assume that L is a Δ -field extension of K with $L^\Delta = K$.

Definition

Let X be a Δ -scheme over $\text{diffspec } K$. We say that X *splits* over L if there is a scheme Y over $\text{Spec } C$ such that

$$X \approx \text{Diffspec } L \times_{\text{Diffspec } C} Y$$

Here we put the trivial structure of Δ -scheme on Y and consider the product in the category of Δ -schemes.
Another way to say this is to say that X “descends to constants”.

Let $X = \text{diffspec}(L \otimes_K L)$.

Theorem

Suppose that X splits over L . Then L is a strongly normal extension of K .

Moreover, if $X \approx \text{diffspec } L \times_{\text{diffspec } C} Y$ then $Y \approx X^\Delta$.

There is another approach to Galois theory that uses adjoint functors.

Let \mathcal{D} denote the category of Δ -rings and \mathcal{R} the category of rings. Then we have adjoint functors

$$F: \mathcal{D}^\circ \rightarrow \mathcal{R}^\circ, \quad F(R) = R^\Delta$$

and

$$U: \mathcal{R}^\circ \rightarrow \mathcal{D}^\circ, \quad U(A) = A$$

The following theorem is due to Janelidze.

Theorem

If P is a Picard-Vessiot ring then P is a normal extension with respect to the adjoint functors above.

I *feel* that there is a similar theorem for strongly normal extensions but have not been able to nail down the details.

These slides are available at

<http://www.sci.ccny.cuny.edu/~ksda/gradcenter.html>