Picard-Vessiot theory, algebraic groups and group schemes

Jerald J. Kovacic
Department of Mathematics
The City College of The City University of New York
New York, NY 10031
email: jkovacic@verizon.net
URL: mysite.verizon.net/jkovacic

September 30, 2005

Abstract

We start with the classical definition of Picard-Vessiot extension. We show that the Galois group is an algebraic subgroup of $\mathrm{GL}(n)$. Next we introduce the notion of Picard-Vessiot ring and describe the Galois group as spec of a certain subring of a tensor product. We shall also show existence and uniqueness of Picard-Vessiot extensions, using properties of the tensor product. Finally we hint at an extension of the Picard-Vessiot theory by looking at the example of the Weierstraß $\wp$-function.

We use only the most elementary properties of tensor products, spec, etc. We will define these notions and develop what we need. No prior knowledge is assumed.

1 Introduction

Throughout this talk we fix an ordinary ∂-field $\mathcal{F}$ of characteristic 0 and with algebraically closed field of constants

$$\mathcal{C} = \mathcal{F}^{\partial}$$

If you want, you may assume that $\mathcal{F} = \mathbb{C}(x)$ is the field of rational functions of a single complex variable.

I usually use the prefix ∂- instead of the word "differential". Thus I speak of ∂-rings and ∂-fields, ∂-ideals, etc.

2 Classical Picard-Vessiot theory

We consider a linear homogeneous ∂-equation

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

Definition 2.1. By a *fundamental system of solutions* of $L(y) = 0$, we mean a set $\eta_1, \dots, \eta_n$ of elements of some ∂-extension field $\mathcal{G}$ of $\mathcal{F}$ such that

1. $L(\eta_i) = 0$,
2. $\eta_1, \dots, \eta_n$ are linearly independent over $\mathcal{C}$.

We usually write $\eta = (\eta_1, \dots \eta_n)$ for the row vector.

Definition 2.2. By a *Picard-Vessiot extension for L* we mean a ∂-field $\mathcal{G}$ containing $\mathcal{F}$ such that

1. $\mathcal{G}^{\partial} = \mathcal{F}^{\partial} = \mathcal{C}$,
2. $\mathcal{G} = \mathcal{F}\langle \eta_1, \dots, \eta_n \rangle$ where $\eta_1, \dots, \eta_n$ is a fundamental system of solutions of $L(y) = 0$.

Definition 2.3. Suppose that $\mathcal{G}$ is a Picard-Vessiot extension. Then the group of ∂-automorphisms of $\mathcal{G}$ over $\mathcal{F}$,

$$G(\mathcal{G}/\mathcal{F}) = \partial\text{- Aut}(\mathcal{G}/\mathcal{F})$$

is called the *Galois group* of $\mathcal{G}$ over $\mathcal{F}$.

Proposition 2.4. *Suppose that $\mathcal{G}$ is a Picard-Vessiot extension. If $\sigma \in G(\mathcal{G}/\mathcal{F})$ then there is an invertible matrix $c(\sigma)$ with constant coefficients such that*

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

The mapping

$$c\colon G(\mathcal{G}/\mathcal{F}) \to \mathrm{GL}(n)$$

is an injective homomorphism.

Proof. The easiest way to see this is to look at the Wronskian matrix.

$$W = \begin{pmatrix} \eta_1 & \cdots & \eta_n \\ \eta_1' & \cdots & \eta_n' \\ \vdots & & \vdots \\ \eta_1^{(n-1)} & \cdots & \eta_n^{(n-1)} \end{pmatrix}$$

Because $\eta_1, \ldots, \eta_n$ are linearly independent over $\mathcal{C}$ the Wronskian is invertible.

A simple computation shows that

$$W' = \begin{pmatrix} \eta_1' & \cdots & \eta_n' \\ \eta_1'' & \cdots & \eta_n'' \\ \vdots & & \vdots \\ \eta_1^{(n)} & \cdots & \eta_n^{(n)} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & \cdots\cdots & & 0 \\ \vdots & 0 & 1 & & & \vdots \\ \vdots & & 0 & \ddots & & \vdots \\ \vdots & & & \ddots & 1 & 0 \\ 0 & \cdots\cdots & & & 0 & 1 \\ -a_0 & -a_1 & \cdots\cdots & & -a_{n-2} & -a_{n-1} \end{pmatrix} \begin{pmatrix} \eta_1 & \cdots & \eta_n \\ \eta_1' & \cdots & \eta_n' \\ \vdots & & \vdots \\ \eta_1^{(n-1)} & \cdots & \eta_n^{(n-1)} \end{pmatrix}$$

i.e.

$$W'W^{-1} = A = \begin{pmatrix} 0 & 1 & 0 & \cdots\cdots & & 0 \\ \vdots & 0 & 1 & & & \vdots \\ \vdots & & 0 & \ddots & & \vdots \\ \vdots & & & \ddots & 1 & 0 \\ 0 & \cdots\cdots & & & 0 & 1 \\ -a_0 & -a_1 & \cdots\cdots & & -a_{n-2} & -a_{n-1} \end{pmatrix}$$

The matrix A is called the *companion matrix* for L.

Differentiate

$$c(\sigma) = W^{-1}\sigma W$$

and you get 0, so $c(\sigma) \in \mathrm{GL}_{\mathcal{C}}(n) = \mathrm{GL}(\mathcal{C})$. The first row of W is η so

$$\sigma W = W c(\sigma) \qquad \text{implies that} \qquad \eta = \eta c(\sigma)\,.$$

Suppose that $\sigma, \tau \in G(\mathcal{G}/\mathcal{F})$. Then

$$c(\sigma\tau) = W^{-1}\sigma(Wc(\tau)) = W^{-1}\sigma(W)c(\tau) = c(\sigma)c(\tau)\,,$$

because $c(\tau)$ has constant coordinates and therefore is left fixed by σ. Therefore c is a homomorphism of groups. c is injective since $\mathcal{G} = \mathcal{F}\langle\eta\rangle = \mathcal{F}(W)$.

□

3 Algebraic subgroups of $\mathrm{GL}(n)$

Here we take a "classical" point of view, later on we shall be more "modern" and use group schemes.

We start by putting a topology on "affine m-space"

$$\mathbb{A}^m = \mathcal{C}^m$$

Definition 3.1. A subset X of $\mathbb{A}^m$ is *Zariski closed* if there exists a finite set of polynomials in m variables

$$f_1, \ldots, f_r \in \mathcal{C}[X_1, \ldots, X_m]$$

such that X is the "zero set" of $f_1 = \cdots = f_r = 0$, i.e.

$$X = \{(a_1, \ldots, a_m) \in \mathcal{C}^m \mid f_1(a_1, \ldots, a_m) = \cdots = f_r(a_1, \ldots, a_m) = 0\}\,.$$

We can drop the adjective "finite" in the definition. Indeed X being the zero set of a collection f_i $(i \in I)$ of polynomials is equivalent to saying that X is the zero set of the entire ideal

$$\mathfrak{a} = ((f_i)_{i \in I})$$

and even the radical ideal

$$\sqrt{\mathfrak{a}} = \{f \mid f^e \in \mathfrak{a} \quad \text{for some } e \in \mathbb{N}\}$$

By the Hilbert Basis Theorem this ideal is generated by a finite number of polynomials.

Theorem 3.2. *(Hilbert Nullstellensatz) There is a bijection between closed subsets of* $\mathbb{A}^m$ *and radical ideals of* $\mathcal{C}[X_1, \ldots, X_m]$.

Now let's put a topology on $\mathrm{GL}(n)$, the set of invertible $n \times n$ matrices with coefficients in $\mathcal{C}$. We do this by embedding $\mathrm{GL}(n)$ into $\mathbb{A}^{n^2+1}$:

$$\begin{pmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & & \vdots \\ c_{n1} & \cdots & c_{nn} \end{pmatrix} \longmapsto (c_{11}, \ldots, c_{1n}, \ldots, c_{n1}, \ldots, c_{nn}, 1/\det c_{ij}) \in \mathbb{A}^{n^2+1}.$$

The image is closed, it is the zero set of

$$\det(X_{ij})Y = 1$$

where Y is the $(n^2+1)^{\mathrm{st}}$ coordinate.

Definition 3.3. A subset $X \subset \mathrm{GL}(n)$ is *Zariski closed* is if it closed in the subset topology as a subset of $\mathbb{A}^{n^2+1}$.

Definition 3.4. A *linear algebraic group* is a closed subgroup of $\mathrm{GL}(n)$ for some n.

4 The Galois group of a Picard-Vessiot extension

In this section $\mathcal{G}$ is a Picard-Vessiot extension of $\mathcal{F}$.

Proposition 4.1. *The image of*

$$c\colon G(\mathcal{G}/\mathcal{F}) \to \mathrm{GL}(n)$$

is an algebraic subgroup of $\mathrm{GL}(n)$*.*

Proof. Let $y_1, \dots, y_n$ be ∂-indeterminates over $\mathcal{F}$. This means that

$$y_1, \dots, y_n, y_1', \dots, y_n', y_1'', \dots y_n'', \dots$$

is an infinite family of indeterminates over $\mathcal{F}$. We use vector notation and write $y = (y_1, \dots, y_n)$. Then

$$\mathcal{F}\{y\} = \mathcal{F}[y, y', \dots]$$

is a polynomial ring in an infinite number of variables. There is a homomorphism ϕ over $\mathcal{F}$, called the *substitution homomorphism*, defined by

$$\begin{aligned} \phi\colon \mathcal{F}\{y\} &\longrightarrow \mathcal{F}\{\eta\} \\ y_i &\longmapsto \eta_i \\ y_i' &\longmapsto \eta_i' \\ &\vdots \end{aligned}$$

Evidently, it is a ∂-homomorphism. Let $\mathfrak{p}$ be its kernel

$$0 \longrightarrow \mathfrak{p} \longrightarrow \mathcal{F}\{y\} \xrightarrow{\phi} \mathcal{F}\{\eta\} \longrightarrow 0$$

For $C \in \mathrm{GL}(n)$ we let ρ_C be the substitution homomorphism

$$\begin{aligned} \rho_C\colon \mathcal{F}\{y\} &\longrightarrow \mathcal{F}\{y\} \\ y &\longmapsto yC \end{aligned}$$

This means

$$y_i \longmapsto \sum_j y_j C_{ji}\,.$$

Lemma 4.2. *C is in the image of $c\colon G(\mathcal{G}/\mathcal{F}) \to \mathrm{GL}(n)$ if and only if*

$$\rho_C \mathfrak{p} \subset \mathfrak{p} \qquad \textit{and} \qquad \rho_{C^{-1}} \mathfrak{p} \subset \mathfrak{p}$$

(This is equivalent to $\rho_C \mathfrak{p} = \mathfrak{p}$.)

Proof. Suppose that $C = c(\sigma)$ for some $\sigma \in G(\mathcal{G}/\mathcal{F})$. We have both

$$\sigma\eta = \eta C \qquad \text{and} \qquad \rho_C y = yC$$

We have the commutative diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathfrak{p} & \longrightarrow & \mathcal{F}\{y\} & \xrightarrow{\phi} & \mathcal{F}\{\eta\} & \longrightarrow & 0 \\
 & & & & \downarrow{\scriptstyle \rho_C} & & \downarrow{\scriptstyle \sigma} & & \\
0 & \longrightarrow & \mathfrak{p} & \longrightarrow & \mathcal{F}\{y\} & \xrightarrow{\phi} & \mathcal{F}\{\eta\} & \longrightarrow & 0
\end{array}$$

To show that $\rho_C \mathfrak{p} \subset \mathfrak{p}$, we "chase" the diagram. If $a \in \mathfrak{p}$ then $\phi a = 0$ so

$$0 = \sigma(\phi a) = \phi(\rho_C a)$$

which implies that

$$\rho_C a \in \ker \phi = \mathfrak{p}\,.$$

We have shown that

$$\rho_C \mathfrak{p} \subset \mathfrak{p}\,.$$

For the other inclusion, use σ^{-1}.

Now suppose that $\rho_C \mathfrak{p} = \mathfrak{p}$. Then there is a ∂-homomorphism ψ

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathfrak{p} & \longrightarrow & \mathcal{F}\{y\} & \xrightarrow{\phi} & \mathcal{F}\{\eta\} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \rho_C} & & \downarrow{\scriptstyle \rho_C} & & \vdots{\scriptstyle \psi} & & \\
0 & \longrightarrow & \mathfrak{p} & \longrightarrow & \mathcal{F}\{y\} & \xrightarrow{\phi} & \mathcal{F}\{\eta\} & \longrightarrow & 0
\end{array}$$

In fact ψ is defined by

$$\psi a = \phi(\rho_C A), \qquad \text{where} \qquad \phi A = a \qquad (a \in \mathcal{F}\{\eta\}, A \in \mathcal{F}\{y\})\,.$$

Since $\phi y = \eta$, we have the matrix equation

$$\psi\eta = \phi(\rho_C(y)) = \phi(yC) = \eta C$$

We can see that ψ is bijective by diagram chasing. Tberefore ψ extends to a ∂-automorphism of the field of quotients

$$\sigma \colon \mathcal{F}\langle\eta\rangle = \mathcal{G} \to \mathcal{G}$$

So $\sigma \in G(\mathcal{G}/\mathcal{F})$ and since $\sigma\eta = \eta C$,

$$c(\sigma) = C\,.$$

□

We think of $\mathfrak{p}$ as a vector space over $\mathcal{F}$ and choose a basis $\mathcal{A}$ for it. We also extend $\mathcal{A}$ to a basis $\mathcal{B}$ of $\mathcal{F}\{y\}$ over $\mathcal{F}$, so that $\mathcal{A} \subset \mathcal{B}$.

Lemma 4.3. *There exist polynomials*

$$Q_{bc} \in \mathcal{F}[X_{11}, \ldots, X_{nn}] \qquad b, c \in \mathcal{B}$$

with the property that for every $C \in \mathrm{GL}(n)$ and $b \in \mathcal{B}$,

$$\rho_C(b) = \sum_{d \in \mathcal{B}} Q_{bc}(C)\, d\,.$$

Proof. We first examine how ρ_C acts on $\mathcal{F}\{y\}$. Let $\mathcal{M}$ be the set of monomials, thus an element M of $\mathcal{M}$ is a power product

$$M = \prod_{k=1}^{r} \big(y_{i_k}^{(e_k)}\big)^{f_k}$$

of the y_i and their derivatives. Since the coordinates of C are constants,

$$\rho_C(y_i^{(e)}) = \sum_k y_k^{(e)} C_{ki}\,.$$

The right hand side is linear combination of the $y_i^{(e)}$ with coefficients that are coordinates of C. If we apply ρ_C to a monomial we will get product of these right hand sides which is a linear combination of monomials with coefficients that are polynomials over $\mathbb{Z}$ in the coordinates of C. I.e. there exist polynomials

$$P_{MN} \in \mathbb{Z}[X_{11}, \ldots, X_{nn}] \qquad M, N \in \mathcal{M}$$

such that

$$\rho_C M = \sum_{N \in \mathcal{M}} P_{MN}(C) N\,.$$

Because $\mathcal{B}$ and $\mathcal{M}$ are both bases of $\mathcal{F}\{y\}$ over $\mathcal{F}$, we can express each element of $\mathcal{B}$ as a linear combination over $\mathcal{F}$ of monomials, and, conversely, every monomial as a linear combination over $\mathcal{F}$ of elements of $\mathcal{B}$. It follows that there exist polynomials

$$Q_{bc} \in \mathcal{F}[X_{11}, \ldots, X_{nn}] \qquad b, c \in \mathcal{B}$$

with the property that for every $C \in \mathrm{GL}(n)$ and $b \in \mathcal{B}$,

$$\rho_C(b) = \sum_{d \in \mathcal{B}} Q_{bc}(C)\, d\,.$$

□

Lemma 4.4. *There is a (possibly infinite) family of polynomials*

$$R_i \in \mathcal{F}[X_{11}, \ldots, X_{nn}, Y] \qquad i \in I$$

such that $C \in \mathrm{GL}(n)$ *is in the image of* c *if and only if*

$$R_i(C, \tfrac{1}{\det C}) = 0, \qquad i \in I$$

Proof. We know, by Lemma 4.2, that $C \in \mathrm{GL}(n)$ is in the image of c if and only if

$$\rho_C \mathfrak{p} \subset \mathfrak{p} \qquad \text{and} \qquad \rho_{C^{-1}} \mathfrak{p} \subset \mathfrak{p}\,.$$

Recall that $\mathcal{A}$ is a basis of $\mathfrak{p}$ over $\mathcal{F}$ and, by the previous lemma,

$$\rho_C(a) = \sum_b Q_{ab}(C)\, b$$

so $\rho_C \mathfrak{p} \subset \mathfrak{p}$ if and only if

$$Q_{ab}(C) = 0 \qquad \text{for every } a \in \mathcal{A}, b \in \mathcal{B}, b \notin \mathcal{A}\,.$$

Similarly $\rho_{C^{-1}} \mathfrak{p} \subset \mathfrak{p}$ if and only if

$$Q_{ab}(C^{-1}) = 0 \qquad \text{for every } a \in \mathcal{A}, b \in \mathcal{B}, b \notin \mathcal{A}\,.$$

Of course, the coordinates of C^{-1} are $\frac{1}{\det C}$ times polynomials in the coordinates of C. Thus there exist polynomials

$$R_{ab} \in \mathcal{F}[X_{11}, \ldots, X_{nn}, Y]$$

such that

$$R_{ab}(C, \tfrac{1}{\det C}) = Q_{ab}(C^{-1})$$

□

To conclude the proof of the theorem we need to find polynomials as above, except that the coefficients should be in $\mathcal{C}$ not $\mathcal{F}$.

Choose a basis Λ of $\mathcal{F}$ over $\mathcal{C}$. We then can write

$$R_i = \sum_{\lambda\in\Lambda} S_{i\lambda}\,\lambda$$

where

$$S_{i\lambda} \in \mathcal{C}[X_{11}, \ldots, X_{nn}, Y]\,.$$

If $R_i(C, \frac{1}{\det C}) = 0$ then

$$0 = \sum_{\lambda\in\Lambda} S_{i\lambda}(C, \tfrac{1}{\det C})\,\lambda$$

Because the elements of Λ are linearly independent over $\mathcal{C}$, we must have

$$S_{i\lambda}(C, \tfrac{1}{\det C}) = 0 \qquad \text{for all } \lambda \in \Lambda$$

It follows from the previous lemma that $C \in \mathrm{GL}(n)$ is in the image of c if and only if

$$S_{i\lambda}(C, \tfrac{1}{\det C}) = 0 \qquad \text{for all } i \in I \text{ and } \lambda \in \Lambda$$

This proves the theorem. □

5 Matrix equations

Starting with a linear homogeneous ∂-equation (a scalar ∂-equation) we chose a fundamental system of solutions $\eta_1, \ldots, \eta_n$ and formed the Wronskian

$$\begin{pmatrix} \eta_1 & \cdots & \eta_n \\ \vdots & & \vdots \\ \eta_1^{(n-1)} & \cdots & \eta_n^{(n-1)} \end{pmatrix}$$

We discovered that

$$W' = AW$$

where

$$A = \begin{pmatrix} 0 & 1 & 0 & \dots\dots & & 0 \\ \vdots & 0 & 1 & & & \vdots \\ \vdots & & 0 & \ddots & & \vdots \\ \vdots & & & \ddots & 1 & 0 \\ 0 & \dots\dots\dots & & & 0 & 1 \\ -a_0 & -a_1 & \dots\dots & & -a_{n-2} & -a_{n-1} \end{pmatrix}$$

was a matrix with coefficients in $\mathcal{F}$.

We can also start with a matrix equation

$$Y' = AY$$

where $A \in \mathrm{Mat}_{\mathcal{F}}(n)$ is *any* matrix with coordinates in $\mathcal{F}$, and look for a solution matrix Z that is invertible. The matrix Z is called a *fundamental solution matrix* for the matrix ∂-equation.

6 The Picard-Vessiot ring

Let $A \in \mathrm{Mat}_{\mathcal{F}}(n)$ be a given $n \times n$ matrix with coefficients in $\mathcal{F}$.

Definition 6.1. By a *Picard-Vessiot ring for A* we mean an integral domain $\mathcal{R}$ such that

1. $(\mathrm{qf}\,\mathcal{R})^\partial = \mathcal{F}^\partial = \mathcal{C}$,
2. $\mathcal{R} = \mathcal{F}[Z, Z^{-1}]$ where $Z'Z^{-1} = A \in \mathrm{Mat}_{\mathcal{F}}(n)$.

Item 2 could also be written $\mathcal{R} = \mathcal{F}[Z, \frac{1}{\det Z}]$. There is a popular "abuse of notation" that writes $\mathcal{R} = \mathcal{F}[Z, \frac{1}{\det}]$.

Proposition 6.2. *If* $\mathcal{G} = \mathcal{F}\langle\eta\rangle = \mathcal{F}(W)$ *is a Picard-Vessiot extension, as before, then* $\mathcal{R} = \mathcal{F}[W, W^{-1}]$ *is a Picard-Vessiot ring.*

Conversly, if $\mathcal{R}$ *is a Picard-Vessiot ring then* $\mathcal{G} = \mathrm{qf}\,\mathcal{R}$ *is a Picard-Vessiot extension.*

If $\mathcal{F}$ contains a non-constant this is a consequence of the "cyclic vector theorem". If $\mathcal{F} = \mathcal{C}$ it must (and can be) proven by a different method.

Definition 6.3. By the *Galois group* of $\mathcal{R}$ over $\mathcal{F}$, denoted $G(\mathcal{R}/\mathcal{F})$ we mean the group of a ∂-automorphisms of $\mathcal{R}$ over $\mathcal{F}$.

Proposition 6.4. *If* $\mathcal{G} = \operatorname{qf} \mathcal{R}$, *then* $G(\mathcal{R}/\mathcal{F}) = G(\mathcal{G}/\mathcal{F})$.

7 Differential simple rings

Definition 7.1. Let $\mathcal{R}$ be a ∂-ring. We say that $\mathcal{R}$ is ∂-*simple* if $\mathcal{R}$ has no proper non-trivial ∂-ideal.

In algebra (not ∂-algebra) a simple (commutative) ring R is uninteresting. Indeed (0) is a maximal ideal and the quotient

$$R/(0) = R$$

is a field, i.e. R is a field. But in ∂-algebra the concept is very important.

Example 7.2. Let $\mathcal{R} = \mathbb{C}[x]$ where $x' = 1$ is ∂-simple. If $\mathfrak{a} \subset \mathcal{R}$ is a non-zero ∂-ideal then it contains a non-zero polynomial. Choose a non-zero polynomial $P(x)$ in $\mathfrak{a}$ having smallest degree. But $P' \in \mathfrak{a}$ has smaller degree, so $P' = 0$. But that makes $P \in \mathbb{C}$ so $1 \in \mathfrak{a}$.

Note that (0) is a maximal ∂-ideal (there is no proper ∂-ideal containing it) but is not a maximal ideal.

More generally, if $\mathcal{R}$ is any ∂-ring and $\mathfrak{m}$ a maximal ∂-ideal of $\mathcal{R}$ then $\mathcal{R}/\mathfrak{m}$ is ∂-simple. It is a field if and only if $\mathfrak{m}$ is a maximal ideal.

Proposition 7.3. *Let $\mathcal{R}$ be a Picard-Vessiot ring. Then $\mathcal{R}$ is ∂-simple.*

Proposition 7.4. *Suppose that $\mathcal{R}$ is a ∂-simple ring containing $\mathcal{F}$. Then*

1. *$\mathcal{R}$ is an integral domain, and*

2. $(\operatorname{qf} \mathcal{R})^\partial = \mathcal{C}$.

This suggests a way of creating Picard-Vessiot rings.

Theorem 7.5. *Let $A \in \operatorname{Mat}_{\mathcal{F}}(n)$. Then there exists a Picard-Vessiot ring $\mathcal{R}$ for A.*

Proof. Let $y = (y_{ij})$ be a family of n^2 ∂-indeterminates over $\mathcal{F}$ and let

$$\mathcal{S} = \mathcal{F}\{y\}[\tfrac{1}{\det y}]$$

(The derivation on $\mathcal{F}\{y\}$ extends to $\mathcal{S}$ by the quotient rule.) We want to find a maximal ∂-ideal of $\mathcal{S}$ that contains the ∂-ideal

$$\mathfrak{a} = [y' - Ay]$$

We can do this, using Zorn's Lemma, as long as $\mathfrak{a}$ is proper, i.e. no power of $\det y$ is in $\mathfrak{a}$. But this is certainly true since every element of $\mathfrak{a}$ has order at least 1 and $\det y$ has order 0.

Let $\mathfrak{m}$ be a maximal ∂-ideal of $\mathcal{S}$ that contains $\mathfrak{a}$ and set

$$\mathcal{R} = \mathcal{S}/\mathfrak{m}$$

$\mathcal{R}$ is ∂-simple so it is a domain and $(\operatorname{qf} \mathcal{R})^\partial = \mathcal{C}$. If Z is the image of the matrix y in $\mathcal{R}$ then

$$Z' = AZ$$

since $\mathfrak{a}$ is contained the kernel of $\mathcal{S} \to \mathcal{R}$. □

Corollary 7.6. *Given a linear homogeneous ∂-equation $L(y) = 0$ there exists a Picard-Vessiot extension for L.*

8 Example where $[y' - A]$ is not maximal

The example I gave at the seminar was wrong. I had forgotten that the containing ring is $\mathcal{F}\{\}[\frac{1}{\det y}]$.

Let $\mathcal{F} = \mathbb{C}(e^x)$ and $A = 1$ (a 1×1 matrix). The we must look at the ideal

$$[y' - y] \subset \mathcal{F}\{y\}[\tfrac{1}{y}] = \mathcal{F}\{y, \tfrac{1}{y}\}$$

I had asserted that $[y' - y] \subset [y]$, which is indeed true, but not relevant, since $1 \in [y]$. However

$$[y' - y] \subset [y - e^x]\,.$$

Indeed

$$y' - y = (y - e^x)' - (y - e^x)$$

Also $[y - e^x]$ is a maximal ∂-ideal (even a maximal ideal) since it is the kernel of the substitution homomorphism

$$\mathcal{F}\{y, \tfrac{1}{y}\} \to \mathcal{F}\{e^x, e^{-x}\} = \mathbb{C}(e^x) = \mathcal{F}$$

9 Tensor products

Let $\mathcal{R}$ and $\mathcal{S}$ be ∂-rings that both contain $\mathcal{F}$. We are interested in the tensor product

$$\mathcal{R} \otimes_{\mathcal{F}} \mathcal{S}$$

This is a ∂-ring. The easiest way to describe it uses vector space bases.

Let $\{x_i\}$, $(i \in I)$, be a vector space basis of $\mathcal{R}$ over $\mathcal{F}$ and $\{y_j\}$, $(j \in J)$, be a basis of $\mathcal{S}$ over $\mathcal{F}$. Consider the set of all pairs (x_i, y_j) and the set $\mathcal{R} \otimes_{\mathcal{F}} \mathcal{S}$ of all formal finite sums

$$\sum_{i.j} a_{ij}(x_i, y_j) \qquad \text{where } a_{ij} \in \mathcal{F}$$

$\mathcal{R} \otimes_{\mathcal{F}} \mathcal{S}$ is a vector space over $\mathcal{F}$ with basis (x_i, y_i).

If $x = \sum_i a_i x_i \in \mathcal{R}$ and $y = \sum_j b_j y_j \in \mathcal{S}$ we write

$$x \otimes y = \sum_i \sum_j a_i b_j (x_i, y_j) \in \mathcal{R} \otimes_{\mathcal{F}} \mathcal{S}$$

We have

1. $(x+\overline{x})\otimes y = x\otimes y + \overline{x}\otimes y$
2. $x\otimes(y+\overline{y}) = x\otimes y + x\otimes\overline{y}$
3. $a(x\otimes y) = ax\otimes y = x\otimes ay$

One defines multiplication so that

$$(x\otimes y)(\overline{x}\otimes\overline{y}) = x\overline{x}\otimes y\overline{y}$$

and shows that $\mathcal{R}\otimes_{\mathcal{F}}\mathcal{S}$ is a ring. Finally we define a derivation with the property

$$(x\otimes y)' = x'\otimes y + x\otimes y'$$

and we get a ∂-ring.

We have two "canonical" mappings

$$\begin{aligned}\alpha\colon \mathcal{R} &\longrightarrow \mathcal{R}\otimes_{\mathcal{F}}\mathcal{S}\\ a &\longmapsto a\otimes 1\end{aligned}$$

and

$$\begin{aligned}\beta\colon \mathcal{S} &\longrightarrow \mathcal{R}\otimes_{\mathcal{F}}\mathcal{S}\\ a &\longmapsto 1\otimes a\end{aligned}$$

10 $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}$

Be careful. Tensor products are usually much worse than the rings you started with. For example

$$\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}$$

is not a field, in fact it is not even an integral domain! Indeed

$$(i\otimes 1 + 1\otimes i)(i\otimes 1 - 1\otimes i) = -1\otimes 1 - i\otimes i + i\otimes i - 1\otimes -1 = 0$$

In fact $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}\approx\mathbb{C}\times\mathbb{C}$. Every element of $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}$ has the form

$$x = a(1\otimes 1) + b(i\otimes 1) + c(1\otimes i) + d(i\otimes i)$$

We define $\phi\colon \mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}\to\mathbb{C}^2$ by

$$\phi(x) = \big((a+d)+(b-c)i,\ (a-d)+(b+c)i\big)$$

It is straightforward to check that ϕ is an isomorphism or rings.

11 Uniqueness of a Picard-Vessiot ring

Suppose that $\mathcal{R}$ and $\mathcal{S}$ are both Picard-Vessiot rings for the matrix A. Say

$$\mathcal{R} = \mathcal{F}[Z, Z^{-1}] \qquad \mathcal{S} = \mathcal{F}[W, W^{-1}]$$

where

$$Z'Z^{-1} = A = W'W^{-1}$$

If Z and W were in some common ring extension $\mathcal{T}$ of both $\mathcal{R}$ and $\mathcal{S}$, then

$$W = ZC$$

for some matrix of constants, $C \in \mathcal{T}^\partial$. We can easily find a common ring extension of both $\mathcal{R}$ and $\mathcal{S}$, namely

$$\mathcal{R}\otimes_{\mathcal{F}}\mathcal{S}$$

And we can find one whose ring of constants is $\mathcal{C}$

$$\mathcal{T} = (\mathcal{R}\otimes_{\mathcal{F}}\mathcal{S})/\mathfrak{m}$$

where $\mathfrak{m}$ is a maximal ∂-ideal of $\mathcal{R}\otimes_{\mathcal{F}}\mathcal{S}$. (It is ∂-simple!)

Proposition 11.1. *Suppose that $\mathfrak{m}$ is a maximal ∂-ideal of $\mathcal{R}\otimes_{\mathcal{F}}\mathcal{S}$ and let*

$$\pi\colon \mathcal{R}\otimes_{\mathcal{F}}\mathcal{S} \to (\mathcal{R}\otimes_{\mathcal{F}}\mathcal{S})/\mathfrak{m} = \mathcal{T}$$

be the canonical homomorphism. Then

$$\phi\colon \mathcal{R} \xrightarrow{\ \alpha\ } \mathcal{R}\otimes_{\mathcal{F}}\mathcal{S} \xrightarrow{\ \pi\ } \mathcal{T}$$

and

$$\psi\colon \mathcal{S} \xrightarrow{\ \beta\ } \mathcal{R}\otimes_{\mathcal{F}}\mathcal{S} \xrightarrow{\ \pi\ } \mathcal{T}$$

are isomophisms.

Proof. The kernel of ϕ is a proper ∂-ideal of $\mathcal{R}$. Because $\mathcal{R}$ is ∂-simple, this ideal must be (0), so ϕ is injective.

Since $Z' = AZ$ and $W' = AW$ and A has coefficients in $\mathcal{F}$,

$$C = \pi(1 \otimes W)\pi(Z \otimes 1)^{-1}$$

is a matrix of constants and hence has coordinates in $\mathcal{C}$. Therefore

$$\pi(1 \otimes W) = C\pi(Z \otimes 1) = \pi(CZ \otimes 1)$$

and

$$\pi(1 \otimes \mathcal{S}) \subset \pi(\mathcal{R} \otimes 1)$$

or

$$\mathcal{T} = \pi(\mathcal{R} \otimes \mathcal{S}) \subset \pi(\mathcal{R} \otimes 1) = \pi(\alpha(\mathcal{R}))\,.$$

□

The following proposition says that a Picard-Vessiot ring for A is unique up to ∂-isomorphism. It follows that a Picard-Vessiot extension for a linear homogeneous ∂-equation is also unique up to a ∂-isomorphism.

Theorem 11.2. *$\mathcal{R}$ and $\mathcal{S}$ are ∂-isomorphic.*

Proof. Both $\mathcal{R}$ and $\mathcal{S}$ are ∂-isomorphic to $\mathcal{T}$. □

12 $\mathcal{R} \otimes_{\mathcal{F}} \mathcal{R}$

We continue to assume that $\mathcal{R}$ is a Picard-Vessiot ring. Here we are interested in the ∂-ring

$$\mathcal{R} \otimes_{\mathcal{F}} \mathcal{R}$$

and in particular relating it to the Galois group $G(\mathcal{R}/\mathcal{F})$.

Let $\sigma \in G(\mathcal{R}/\mathcal{F})$. Define a mapping

$$\bar{\sigma} \colon \mathcal{R} \otimes_{\mathcal{F}} \mathcal{R} \to \mathcal{R}$$

by

$$\bar{\sigma}(a \otimes b) = a\sigma b\,.$$

Proposition 12.1. *If $\sigma \in G(\mathcal{R}/\mathcal{F})$ then the kernel of $\bar{\sigma}$ is a maximal ∂-ideal $\mathfrak{m}_\sigma$.*

Proof.

$$(\mathcal{R} \otimes_{\mathcal{F}} \mathcal{R})/\mathfrak{m}_\sigma \approx \mathcal{R}$$

Because $\mathcal{R}$ is ∂-simple, $\mathfrak{m}_\sigma$ is a maximal ∂-ideal. □

Proposition 12.2. *Let $\sigma \in G(\mathcal{R}/\mathcal{F})$. Then $\mathfrak{m}_\sigma$ is generated as an ideal by*

$$\sigma a \otimes 1 - 1 \otimes a \qquad a \in \mathcal{R}\,.$$

Proof. If $a \in \mathcal{R}$ then

$$\bar{\sigma}(\sigma a \otimes 1 - 1 \otimes a) = \sigma a - \sigma a = 0$$

so $\sigma a \otimes 1 - 1 \otimes a \in \mathfrak{m}_\sigma$.

Now suppose that

$$x = \sum_i a_i \otimes b_i \in \mathfrak{m}_\sigma \qquad \text{so that} \qquad \sum_i a_i \sigma b_i = 0$$

Then

$$\begin{aligned} x &= \sum_i (a_i \otimes 1)(1 \otimes b_i - \sigma b_i \otimes 1) + \sum_i a_i \sigma b_i \otimes 1 \\ &= -\sum_i (a_i \otimes 1)(\sigma b_i \otimes 1 - 1 \otimes b_i) \end{aligned}$$

□

With this we can prove the converse of Proposition 12.1.

Theorem 12.3. *Let $\mathfrak{m}$ be a maximal ∂-ideal of $\mathcal{R} \otimes_{\mathcal{F}} \mathcal{R}$. Then there exists $\sigma \in G(\mathcal{G}/\mathcal{F})$ such that $\mathfrak{m} = \mathfrak{m}_\sigma$.*

Proof. Set

$$\mathcal{T} = (\mathcal{R} \otimes_{\mathcal{F}} \mathcal{R})/\mathfrak{m}, \qquad \pi\colon \mathcal{R} \otimes_{\mathcal{F}} \mathcal{R} \to \mathcal{T}$$

By Proposition 11.1 the mappings

$$\begin{aligned} &\pi \circ \alpha \colon \mathcal{R} \to \mathcal{T} \qquad \text{and} \\ &\pi \circ \beta \colon \mathcal{R} \to \mathcal{T} \end{aligned}$$

are isomorphisms.

Define

$$\sigma \colon \mathcal{R} \to \mathcal{R} \qquad \text{by} \qquad \sigma = (\pi \circ \alpha)^{-1} \circ (\pi \circ \beta)$$

i.e., so that

$$\begin{array}{ccccc} \mathcal{R} & & \xrightarrow{\quad\sigma\quad} & & \mathcal{R} \\ \big\downarrow{\scriptstyle\beta} & & & & \big\downarrow{\scriptstyle\alpha} \\ \mathcal{R} \otimes_{\mathcal{F}} \mathcal{R} & \xrightarrow{\pi} & \mathcal{T} & \xleftarrow{\pi} & \mathcal{R} \otimes_{\mathcal{F}} \mathcal{R} \end{array}$$

commutes.

Let $a \in \mathcal{R}$, then But

$$\pi(\sigma a \otimes 1 - 1 \otimes a) = \pi(\alpha(\sigma a)) - \pi(\beta a) = (\pi \circ \alpha \circ \sigma)(a) - (\pi \circ \beta)(a) = 0$$

Therefore

$$\sigma a \otimes 1 - 1 \otimes a \in \ker \pi = \mathfrak{m}$$

By Proposition 12.2

$$\mathfrak{m}_\sigma \subset \mathfrak{m}$$

But $\mathfrak{m}_\sigma$ is a maximal ∂-ideal, therefore

$$\mathfrak{m}_\sigma = \mathfrak{m}\,.$$

□

We have shown that $G(\mathcal{R}/\mathcal{F})$ is in bijective correspondence (i.e. can be identified with the set of maximal ∂-ideals of $\mathcal{R} \otimes_{\mathcal{F}} \mathcal{R}$, i.e.

$$G(\mathcal{R}/\mathcal{F}) \approx \max \operatorname{diffspec}(\mathcal{R} \otimes_{\mathcal{F}} \mathcal{R})\,.$$

We have diffspec but we want spec.

13 $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ bis

$\mathbb{C}$ is a Galois extension of $\mathbb{R}$ with Galois group $\{\mathrm{id}, \gamma\}$, γ being complex conjugation. It turns out that $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ has precisely two prime ideals and they are both maximal. The first is generated by

$$a \otimes 1 - 1 \otimes a \qquad a \in \mathbb{C}$$

which corresponds the the identity automorphism, and the other generated by

$$\gamma a \otimes 1 - 1 \otimes a \qquad a \in \mathbb{C}$$

which corresponds to the automorphism γ. Thus

$$\max \operatorname{spec}(\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}) = \operatorname{spec}(\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C})$$

is a finite scheme, which is in fact a group scheme and is isomorphic to the Galois group.

14 The constants of $\mathcal{R} \otimes_{\mathcal{F}} \mathcal{R}$

Definition 14.1. Let

$$\mathcal{K} = (\mathcal{R} \otimes_{\mathcal{F}} \mathcal{R})^{\partial}$$

Remember that $\mathcal{R}^{\partial} = \mathcal{C}$, so we might expect $\mathcal{K}$ to be rather small (maybe $\mathcal{K} = \mathcal{C}$). This is very far from the truth.

Example 14.2. Let $\mathcal{F} = \mathbb{C}(x)$ and let

$$Z = (e^x) \in \mathrm{GL}(1)$$

Note that

$$Z' = Z, \qquad \text{so} \qquad A = 1\,.$$

The Picard-Vessiot ring is

$$\mathcal{R} = \mathcal{F}[e^x, e^{-x}]\,.$$

Then

$$(e^x \otimes e^{-x})' = e^x \otimes e^{-x} + e^x \otimes (-e^{-x}) = 0$$

so

$$c = e^x \otimes e^{-x} \in \mathcal{K}$$

Example 14.3. Now let

$$Z = \begin{pmatrix} 1 & \log x \\ 0 & 1 \end{pmatrix}$$

Here

$$\begin{aligned} Z' &= \begin{pmatrix} 0 & \frac{1}{x} \\ 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & \frac{1}{x} \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & \log x \\ 0 & 1 \end{pmatrix} \\ &= AZ \end{aligned}$$

and

$$\mathcal{R} = \mathcal{F}[\log x]$$

Let

$$c = \log x \otimes 1 - 1 \otimes \log x$$

then

$$c' = \frac{1}{x} \otimes 1 - 1 \otimes \frac{1}{x} = 0$$

so $\gamma \in \mathcal{K}$.

If $M, N \in \mathrm{Mat}_{\mathcal{R}}(n)$ we define

$$M \otimes N \in \mathrm{Mat}_{\mathcal{R} \otimes_{\mathcal{F}} \mathcal{R}}(n)$$

be the matrix whose ij^{th} coordinate is

$$(M \otimes N)_{ij} = \sum_k M_{ik} \otimes N_{kj}$$

Proposition 14.4. *Suppose that* $\mathcal{R} = \mathcal{F}[Z, Z^{-1}]$. *Then*

$$\gamma = Z \otimes Z^{-1}$$

is a matrix of constants.

Theorem 14.5.

$$\mathcal{K} = \mathcal{C}[\gamma, \gamma^{-1}]$$

15 Ideals in $\mathcal{R} \otimes_{\mathcal{C}} \mathcal{K}$

Definition 15.1. Let

$$I(\mathcal{K})$$

denote the set of ideals of $\mathcal{K}$ and

$$\mathcal{I}(\mathcal{R} \otimes_{\mathcal{C}} \mathcal{K})$$

the set of ∂-ideals of $\mathcal{R} \otimes_{\mathcal{C}} \mathcal{K}$.

Suppose that $\mathfrak{a}_o$ is an ideal of $\mathcal{K}$, then

$$\mathcal{R} \otimes_{\mathcal{C}} \mathfrak{a}_o$$

is a ∂-ideal of $\mathcal{R} \otimes_{\mathcal{C}} \mathcal{K}$. This gives a mapping

$$\Phi \colon I(\mathcal{K}) \longrightarrow \mathcal{I}(\mathcal{R} \otimes_{\mathcal{C}} \mathcal{K})$$

If $\mathfrak{a} \in \mathcal{R} \otimes_{\mathcal{C}} \mathcal{K}$ is a ∂-ideal then

$$\{c \in \mathcal{K} \mid 1 \otimes c \in \mathfrak{a}\}$$

is an ideal of $\mathcal{K}$ and we have a mapping

$$\Psi \colon \mathcal{I}(\mathcal{R} \otimes_{\mathcal{C}} \mathcal{K}) \longrightarrow I(\mathcal{K})$$

Theorem 15.2. *The mappings Φ and Ψ are bijective and inverse to each other.*

The mappings Φ and Ψ are order-preserving, so we get a bijection between maximal ideals of $\mathcal{K}$ and maximal ∂-ideals of $\mathcal{R} \otimes_{\mathcal{C}} \mathcal{K}$.

16 $\mathcal{R} \otimes_{\mathcal{F}} \mathcal{R} \approx \mathcal{R} \otimes_{\mathcal{C}} \mathcal{K}$

This is one of the most important theorems of Picard-Vessiot rings.

Recall that

$$\mathcal{K} = (\mathcal{R} \otimes_{\mathcal{F}} \mathcal{R})^{\partial}$$

so, in particular, $\mathcal{K} \subset \mathcal{R} \otimes_{\mathcal{F}} \mathcal{R}$. We have a homomorphism

$$\phi\colon \mathcal{R} \otimes_{\mathcal{C}} \mathcal{K} \longrightarrow \mathcal{R} \otimes_{\mathcal{F}} \mathcal{R}$$

given by

$$r \otimes k \longmapsto (r \otimes 1)\, k$$

Theorem 16.1. $\mathcal{R} \otimes_{\mathcal{F}} \mathcal{R} \approx \mathcal{R} \otimes_{\mathcal{C}} \mathcal{K}$

Proof. We consider

$$\phi\colon \mathcal{R} \otimes_{\mathcal{C}} \mathcal{K} \longrightarrow \mathcal{R} \otimes_{\mathcal{F}} \mathcal{R}$$

The kernel is a ∂-ideal of $\mathcal{R} \otimes_{\mathcal{C}} \mathcal{K}$. By Theorem 15.2, there is an ideal $\mathfrak{a}_o \subset \mathcal{K}$ with

$$\mathcal{R} \otimes \mathfrak{a}_o = \ker \phi$$

But ϕ restricted to $1 \otimes \mathcal{K}$ is injective, so $\mathfrak{a}_o = 0$. Therefore ϕ is injective.

For surjectivity we need to show that $1 \otimes \mathcal{R} \subset \mathcal{R} \otimes 1)[\mathcal{K}]$. But

$$1 \otimes Z = (Z \otimes 1)(Z^{-1} \otimes Z) = (Z \otimes 1)\gamma \in (\mathcal{R} \otimes 1)[\mathcal{K}]$$

□

17 spec $\mathcal{K}$

Theorem 17.1. *If $\mathcal{R}$ is a Picard-Vessiot ring and*

$$\mathcal{K} = (\mathcal{R} \otimes_{\mathcal{F}} \mathcal{R})^{\partial}$$

then

$$\begin{aligned} G(\mathcal{R}/\mathcal{F}) &\approx \max \operatorname{diffspec}(\mathcal{R} \otimes_{\mathcal{F}} \mathcal{R}) \\ &\approx \max \operatorname{diffspec}(\mathcal{R} \otimes_{\mathcal{C}} \mathcal{K}) \\ &\approx \max \operatorname{spec} \mathcal{K} \end{aligned}$$

Proof. The first line is Theorem 12.3, the second line is Theorem 16.1 and the last is Theorem 15.2. □

18 Zariski topology on $\operatorname{spec} \mathcal{K}$

$X = \operatorname{spec} \mathcal{K}$ is the set of prime ideals of $\mathcal{K}$. If $\mathfrak{a} \subset \mathcal{K}$ is a radical ideal, then we define

$$V(\mathfrak{a}) = \{\mathfrak{p} \in K \mid \mathfrak{a} \subset \mathfrak{p}\}$$

Note that V is order-reversing:

$$\mathfrak{a} \subset \mathfrak{b} \Longrightarrow V(\mathfrak{a}) \supset V(\mathfrak{b})$$

Also

$$\begin{aligned} V((1)) &= \emptyset \\ V((0)) &= X \\ V(\mathfrak{a} \cap \mathfrak{b}) &= V(\mathfrak{a}) \cup V(\mathfrak{b}) \\ V(\bigcup_i \mathfrak{a}_i) &= \bigcap_i V(\mathfrak{a}_i) \end{aligned}$$

We put a topology on X, called the *Zariski topology*, by defining the closed sets to be sets of the form $V(\mathfrak{a})$ for some radical ideal $\mathfrak{a}$ of $\mathcal{K}$.

By a *closed point* $\mathfrak{p}$ of X we mean a point (prime ideal) such that

$$V(\mathfrak{p}) = \{\mathfrak{p}\}.$$

Thus the closed points are precisely the maximal ideals, i.e. the set of closed points is what I previously called $\operatorname{max\,spec} \mathcal{K}$.

We can do the same thing for ∂-rings $\mathcal{R}$. Thus $\operatorname{diffspec} \mathcal{R}$ is the set of prime ∂-ideals, if $\mathfrak{a}$ is a radical ∂-ideal of $\mathcal{R}$ then $V(\mathfrak{a})$ is defined similarly. And we get a topology, called the *Kolchin topology.* The set of closed points is $\operatorname{max\,diffspec} \mathcal{R}$.

Beware Despite the similarity of definitions of $\operatorname{diffspec} \mathcal{R}$ and $\operatorname{spec} \mathcal{K}$, there are vast differences in the theory.

I want to describe $\operatorname{max\,spec} \mathcal{K}$ a little further. We know that

$$\mathcal{K} = \mathcal{C}[\gamma, \tfrac{1}{\det \gamma}]$$

where $\gamma = Z^{-1} \otimes Z \in \mathrm{Mat}_{\mathcal{K}}(n)$. Let $X = (X_{ij})$ be indeterminates over $\mathcal{C}$ and Y another indeterminate. Then

$$\begin{aligned} \pi\colon C[X,Y] &\longrightarrow \mathcal{K} \\ X &\longmapsto \gamma \\ Y &\longmapsto \frac{1}{\det \gamma} \end{aligned}$$

We have an exact sequence

$$0 \longrightarrow \mathfrak{a} \longrightarrow \mathcal{C}[X,Y] \xrightarrow{\pi} \mathcal{K} \longrightarrow 0$$

where $\mathfrak{a}$ is the kernel of π.

An element of $\max\operatorname{spec}\mathcal{K}$ comes from a maximal ideal of $\mathcal{C}[X,Y]$ that contains $\mathfrak{a}$ and conversely, i.e.

$$\max\operatorname{spec}\mathcal{K} \approx \{\mathfrak{m} \subset \mathcal{C}[X,Y] \mid \mathfrak{m} \text{ is a maximal ideal that contains } \mathfrak{a}\}$$

If $c \in \mathrm{GL}(n)$ is a zero of $\mathfrak{a}$ then

$$\mathfrak{m} = (X - c, (\det c)Y - 1)$$

is a maximal ideal containing $\mathfrak{a}$. The converse is also true - this is the weak Hilbert Nullstellensatz. Therefore the set of maximal ideals containing $\mathfrak{a}$, $\max\operatorname{spec}\mathcal{K}$, is the zero set of $\mathfrak{a}$.

19 Affine scheme and morphisms

Theorem 19.1. *Let R and S be $\mathcal{C}$-algebras. An algebra homomorphism*

$$\phi\colon R \to S$$

induces a scheme morphism

$$^{a}\phi\colon \operatorname{spec} S \to \operatorname{spec} R$$

Conversely, a scheme morphism

$$f\colon \operatorname{spec} S \to \operatorname{spec} R$$

induces an algebra homomorphism

$$f^{\#}\colon R \to S$$

There is a bijection

$$\operatorname{Mor}(\operatorname{spec} S, \operatorname{spec} R) \approx \operatorname{Hom}(R, S)$$

Note that the arrows get reversed.

Theorem 19.2. *Let R and S be $\mathcal{C}$-algebras. Then*

$$\operatorname{spec} R \times \operatorname{spec} S = \operatorname{spec}(R \otimes_{\mathcal{C}} S)$$

20 Group scheme

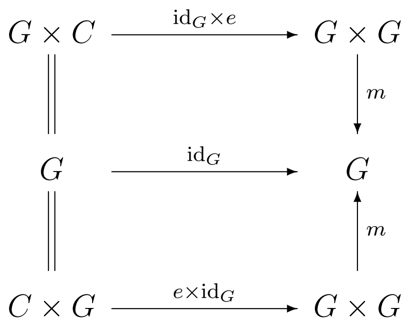
A group in the category of sets is well-known. But a group in the category of schemes is somewhat different. It is NOT a group in the category of sets. In category theory one deals with objects and arrows. Here too. We write $G = \operatorname{spec} \mathcal{K}$ and $C = \operatorname{spec} \mathcal{C}$. All products are over C, i.e. $\times = \times_C$.

Definition 20.1. $G = \operatorname{spec} \mathcal{K}$ is a *group scheme* if there are mappings

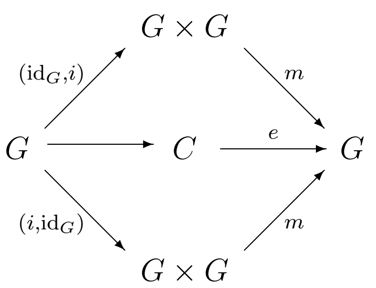
$$\begin{aligned} &m\colon G \times G \to G, && \text{(multiplication)} \\ &e\colon C \to G, && \text{(identity)} \\ &i\colon G \to G, && \text{(inverse)} \end{aligned}$$

such that the following diagrams commute.

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{m \times \mathrm{id}_G} & G \times G \\ \Big\downarrow{\scriptstyle \mathrm{id}_G \times m} & & \Big\downarrow{\scriptstyle m} \\ G \times G & \xrightarrow{m} & G \end{array} \qquad \text{(associativity)}$$



(identity)



(inverse)

21 Hopf algebra

We can translate the group scheme mappings into algebra homomorphisms.

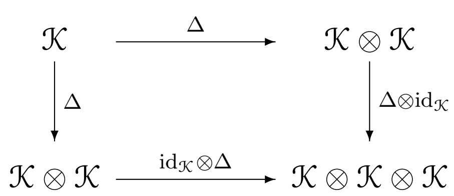
Definition 21.1. $\mathcal{K}$ is a *Hopf algebra* if there are mappings

$\Delta\colon \mathcal{K} \to \mathcal{K} \otimes \mathcal{K},$ (comultiplication)

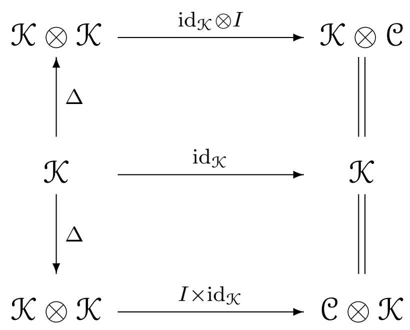
$I\colon \mathcal{K} \to \mathcal{C},$ (coidentity)

$S\colon \mathcal{K} \to \mathcal{K},$ (coinverse or antipode)

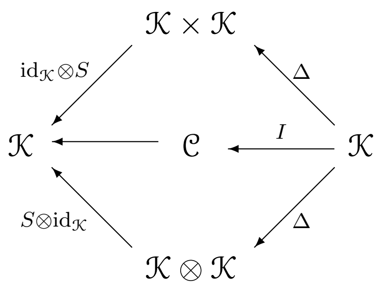
such that the following diagrams commute.



(coassociativity)



(coidentity)



(antipode)

Theorem 21.2. *$\mathcal{K}$ is a Hopf algebra if and only if* $\operatorname{spec} \mathcal{K}$ *is a group scheme.*

22 Sweedler coring

There is a natural structure of coring (which I will not define) on $\mathcal{R} \otimes_{\mathcal{F}} \mathcal{R}$ defined by

$$\begin{aligned} \Delta\colon \mathcal{R} \otimes_{\mathcal{F}} \mathcal{R} &\longrightarrow (\mathcal{R} \otimes_{\mathcal{F}} \mathcal{R}) \otimes_{\mathcal{R}} (\mathcal{R} \otimes_{\mathcal{F}} \mathcal{R}) \\ a \otimes b &\longmapsto a \otimes 1 \otimes 1 \otimes b \end{aligned}$$

$$\begin{aligned} I\colon \mathcal{R} \otimes_{\mathcal{F}} \mathcal{R} &\longrightarrow \mathcal{F} \\ a \otimes b &\longmapsto ab \end{aligned}$$

$$\begin{aligned} S\colon \mathcal{R} \otimes_{\mathcal{F}} \mathcal{R} &\longrightarrow \mathcal{R} \otimes_{\mathcal{F}} \mathcal{R} \\ a \otimes b &\longmapsto b \otimes a \end{aligned}$$

This looks like a Hopf algebra but, in fact, is not quite.

Proposition 22.1. *The mappings above restrict to*

$$\begin{aligned} \Delta^{\partial}\colon \mathcal{K} &\longrightarrow \mathcal{K} \otimes_{\mathcal{C}} \mathcal{K} \\ I^{\partial}\colon \mathcal{K} &\longrightarrow \mathcal{C} \\ S^{\partial}\colon \mathcal{K} &\longrightarrow \mathcal{K} \end{aligned}$$

Theorem 22.2. $\mathcal{K}$ *together with* Δ^{∂}, I^{∂} *and* S^{∂} *is a Hopf algebra.*

Theorem 22.3. $\operatorname{spec} \mathcal{K}$ *is a group scheme.*

23 Matrices return

We can compute the comultiplication Δ on $\mathcal{K}$. Recall that

$$\mathcal{K} = \mathcal{C}[\gamma, \frac{1}{\det \gamma}], \qquad \gamma = Z^{-1} \otimes Z\,.$$

so

$$\Delta(\gamma) = Z^{-1} \otimes_{\mathcal{F}} 1 \otimes_{\mathcal{R}} 1 \otimes_{\mathcal{F}} Z = Z^{-1} \otimes_{\mathcal{F}} Z \otimes_{\mathcal{R}} Z^{-1} \otimes_{\mathcal{F}} Z\gamma \otimes_{\mathcal{R}} \gamma$$

because Z has coordinates in $\mathcal{R}$. Thus

$$\Delta^\partial(\gamma) = \gamma \otimes_\mathcal{C} \gamma$$

i.e.

$$\Delta^\partial(\gamma_{ij}) = \sum_k \gamma_{ik} \otimes_\mathcal{C} \gamma_{kj}$$

which is matrix multiplication.

Also

$$I(\gamma) = I(Z^{-1} \otimes Z) = Z^{-1}Z = 1 \in \mathrm{GL}_\mathcal{R}(n)$$

so

$$I^\partial(\gamma) = 1 \in \mathrm{GL}_\mathcal{C}(n)$$

Finally

$$S(\gamma) = S(Z^{-1} \otimes_\mathcal{F} Z) = Z \otimes_\mathcal{F} Z^{-1} = (Z^{-1} \otimes Z)^{-1} = \gamma^{-1}$$

24 The Weierstraß $\wp$-function

Up to now we have dealt only with Picard-Vessiot extensions. The Galois group is a subgroup of $\mathrm{GL}(n)$, in particular, it is affine. There is a more general theory, the theory of strongly normal extensions. Here we examine one simple example. We use classical language of algebraic geometry.

Start with projective 2-space $\mathbb{P}^2 = \mathbb{P}^2(\mathbb{C})$. This is the set of equivalence class of triples

$$(a, b, c) \in \mathcal{C}^3 \qquad (a, b, c) \neq 0\,,$$

modulo the equivalence relation

$$(a, b, c) \sim (\lambda a, \lambda b, \lambda c) \qquad \lambda \in \mathcal{C}, \lambda \neq 0\,.$$

The equivalence class of (a, b, c) is denoted $[a, b, c]$.

Recall that a polynomial $P \in \mathcal{C}[X, Y, Z]$ is *homogeneous* if every term has the same degree. A subset $S \subset \mathbb{P}^2$ is *closed* (in the Zariski topology) if it is the set of all zeros of a finite set of homogeneous polynomials

$$f_1, \ldots, f_r \in \mathcal{C}[X, Y, Z]$$

We define $E \subset \mathbb{P}^2$ to be the *elliptic curve*, the zero set of the single homogeneous polynomial

$$Y^2Z - 4X^3 + g_2XZ^2 + g_3Z^3$$

where $g_2, g_3 \in \mathbb{C}$ and the discriminant $g_2^3 - 27g_3^2$ is not 0.

If $[a, b, c] \in E$ and $c \neq 0$ then

$$[a, b, c] = [\frac{a}{c}, \frac{b}{c}, 1] = [x, y, 1], \qquad y^2 = 4x^3 - g_2x - g_3 .$$

If $c = 0$ then it follows that $a = 0$. We get the single point $[0, 1, 0]$ which we denote by ∞.

We can interpret the equation $y^2 = 4x^3 - g_2x - g_3$ as defining a Riemann surface. It has genus 1. We can integrate on this surface and the integral is defined up to homotopy (which we call “periods”).

Theorem 24.1. *(Abel) Given $P_1, P_2 \in E$ there is a unique $P_3 \in E$ such that*

$$\int_{\infty}^{P_1} \frac{dt}{s} + \int_{\infty}^{P_2} \frac{dt}{s} = \int_{\infty}^{P_3} \frac{dt}{s} \qquad \textit{(mod periods)}$$

Here t is a dummy variable and $s^2 = 4t^3 - g_2t - g_3$.

This puts an addition on E and makes it an algebraic group.

It turns out that

$$-[x, y, 1] = [x, -y, 1]$$

Suppose that $[x_1, y_1, 1]$ and $[x_2, y_2, 1]$ are in E and $x_1 \neq x_2$. Then

$$[x_1, y_1, 1] + [x_2, y_2, 1] =$$
$$[-(x_1 + x_2) + \tfrac{1}{4}\Big(\frac{y_2 - y_1}{x_2 - x_1}\Big)^2,\ -\Big(\frac{y_2 - y_1}{x_2 - x_1}\Big)x_3 - \frac{y_1x_2 - y_2x_1}{x_2 - x_1},\ 1]$$

Weierstraß inverted the integral to define $\wp(x)$:

$$x = \int_{\infty}^{\wp(x)} \frac{dt}{s} .$$

so that

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3\,.$$

In general, we simply define $\wp$ to be a solution of this ∂-equation.

Definition 24.2. A ∂-field extension $\mathcal{G}$ of $\mathcal{F}$ is said to be *Weierstrassian* if

1. $\mathcal{G}^\partial = \mathcal{F}^\partial = \mathcal{C}$,
2. $\mathcal{G} = \mathcal{F}\langle\wp\rangle$ where $\wp'^2 = 4\wp^3 - g_2\wp - g_3$.

Compute

$$2\wp'\wp'' = 12\wp^2\wp' - g_2\wp' \qquad \text{to get} \qquad \wp'' = 6\wp^2 - \tfrac{1}{2}g_2\,,$$

therefore

$$\mathcal{G} = \mathcal{F}\langle\wp\rangle = \mathcal{F}(\wp, \wp')\,.$$

Let $G(\mathcal{G}/\mathcal{F})$ be the group of all ∂-automorphisms of $\mathcal{G}$ over $\mathcal{F}$. If $\sigma \in G(\mathcal{G}/\mathcal{F})$ then

$$\sigma\wp'^2 = 4\sigma\wp^3 - g_2\sigma\wp - g_3$$

We may think of $[\wp, \wp', 1]$ as an element of $E(\mathcal{G})$, the elliptic curve with coordinates in $\mathcal{G}$. (Recall E had coordinates in $\mathcal{C}$.) The above equation shows that $\sigma[\wp, \wp', 1]$ is also an element of $E(\mathcal{G})$. So we can subtract these points.

Assume that $\sigma\wp \neq \wp$ and let

$$[\gamma, \delta, 1] = \sigma[\wp, \wp', 1] - [\wp', \wp, 1] = [\sigma\wp, \sigma\wp', 1] + [\wp, -\wp', 1]\,.$$

From the formulas above we have:

$$\gamma = -(\sigma\wp + \wp) + \tfrac{1}{4}\left(\frac{-\wp' - \sigma\wp'}{\wp - \sigma\wp}\right)^2$$

We claim that γ is a constant. First compute

$$\left(\frac{\wp' + \sigma\wp'}{\wp - \sigma\wp}\right)' = 2(\wp - \sigma\wp)$$

and then

$$\gamma' = -\sigma\wp' - \wp' + \tfrac{1}{2}\Big(\frac{\wp' + \sigma\wp'}{\wp - \sigma\wp}\Big)2(\wp - \sigma\wp) = 0$$

Because

$$\delta^2 = 4\gamma_3 - g_2\gamma - g_3\,,$$

δ is also a constant.

By assumption, $\mathcal{G}^\partial = \mathcal{F}^\partial = \mathcal{C}$ so $[\gamma, \delta, 1] \in E$.

Theorem 24.3. *There is an mapping*

$$G(\mathcal{G}/\mathcal{F}) \longrightarrow E$$

given by

$$\sigma \longmapsto \sigma[\wp, \wp', 1] - [\wp, \wp', 1]$$

It is injective and the image is an algebraic subgroup of E.