Introduction to Differential Galois Theory

Richard C. Churchill
Jerald J. Kovacic

October 27, 2006

Contents

Chapter 1

An application of differential Galois theory

Jerry:

One of the (many) places where our styles differ is in presenting examples. I prefer:

Examples 1.2.3:

(a) ...

(b) ...

whereas you prefer

Example 1.2.3. ...

Example 1.2.4. ...

For me the second method results in too many reference numbers, but I'm sure you can make analogous objections to my preference. In the end (assuming we are still speaking to each other) we may have to flip a coin.

Some of the footnotes appearing in what follows will eventually have to be replaced by references to later chapters. At some places I have included such indications, but I have not been consistent in doing so.

1.1 The Differential Galois Group of a Linear Differential Equation

Differential Galois theory is concerned with the nature of solutions of linear differential equations, both ordinary and partial. This chapter is an attempt to convey the flavor and utility of the subject without overwhelming the reader with technical details. This is achieved (if at all) by concentrating on the ordinary case and delaying all but the most elementary proofs to later chapters of the text.

Consider an n^{th}-order linear homogeneous ordinary differential equation

$$y^{(n)} + a_1(z)y^{(n-1)} + \cdots + a_{n-1}(z)y' + a_n(z)y = 0 \tag{1.1.1}$$

with coefficients (for simplicity) in the field $\mathbb{C}(z)$ of rational functions on the Riemann sphere $\mathbb{P}^1 \simeq \mathbb{C} \cup \{\infty\}$. Fix a point $z_0 \in \mathbb{C}$ which is a regular point for all coefficients and henceforth identify $\mathbb{C}(z)$ with the field K of associated germs at z_0: this enables us to work with function fields while avoiding the ambiguities of "multi-valued" functions. The usual differentiation operator $\frac{d}{dz}$ induces a "derivation" on K, i.e., an additive group homomorphism from K into K, denoted $k \mapsto k'$, satisfying the *Leibniz* or *product rule*

$$(fg)' = f \cdot g' + f' \cdot g, \qquad f, g \in K. \tag{1.1.2}$$

Do we or do we not spell Leibniz with a t? I don't care, but we need to make a choice and stick with it. To indicate this derivation is assumed we refer to K as a *differential field*.

Pick a basis $\{y_j\}_{j=1}^n$ of solution germs of (1.1.1) at z_0 and within the field of germs of meromorphic functions at z_0 consider the field extension $L \supset K$ generated by these elements. This is again a differential field, with derivation again induced by d/dz, and the derivation obviously extends that defined on K. $L \supset K$ is the *Picard-Vessiot extension* of K corresponding to (1.1.1); it is the analogue of the splitting field of a polynomial in ordinary Galois theory.

The *differential Galois group* of (1.1.1) is the group $G_{\mathrm{dg}}(L/K)$ of field automorphisms of L which commute with the derivation and fix K pointwise. We will be interested in what information this group provides about the solutions of (1.1.1), and how it can be computed. Our first result addresses the information question.

Theorem 1.1.1 : *For the differential Galois group $G := G_{\mathrm{dg}}(L/K)$ defined above the following statements are equivalent:*

(a) *G is finite;*

(b) *the field extension $L \supset K$ is finite, Galois in the usual sense, and G is the usual Galois group; and*

(c) *all solutions of (1.1.1) are algebraic over $K \simeq \mathbb{C}(z)$.*

In (b) "usual sense" means: in the sense of the classical Galois theory of polynomials. A more precise statement of (c) is: all germs of solutions of (1.1.1) at z_0 are germs of algebraic functions over $\mathbb{C}(z)$.

A proof is given in ... **(refer to a later section).**

The search for algebraic solutions of linear differential equations (as in (1.1.1)) was a major mathematical activity in the late nineteenth century. Consider, for example, the *hypergeometric equation*[1]

$$y'' + \frac{\gamma - (\alpha + \beta + 1)z}{z(1-z)}\, y' - \frac{\alpha\beta}{z(1-z)}\, y = 0, \tag{1.1.3}$$

wherein α, β, γ are complex parameters. In 1873 H.A. Schwarz[2] used a beautiful geometric argument involving spherical triangles to enumerate those parameter values for which all solutions were algebraic over $\mathbb{C}(z)$. This example will recur later in the chapter.

The historical precursor of the differential Galois group G was *monodromy group* of (1.1.1), i.e. the subgroup $M \subset G$ consisting of automorphisms of L induced by analytically continuing function germs of solutions at z_0 along inverses of loops of $\mathbb{P}^1 \smallsetminus S$ based at z_0, where $S \subset \mathbb{P}^1$ is the collection of singular points of the given equation.

1.2 Closed-Form Solutions

Let z_0 and $K \simeq \mathbb{C}(z)$ be as in the previous section and let $L \supset K$ be a field extension generated by germs of meromorphic functions at z_0 such that the operator d/dz defines a derivation $\ell \mapsto \ell'$ on L. The extension is *Liouvillian* if there is a finite sequence of intermediate fields

$$\mathbb{C}(z) = K = K_0 \subset K_1 \subset \cdots \subset K_n = L$$

such that the extended derivation on L restricts to a derivation on each K_j, and for $j = 1, \ldots, n$ the field K_j has the form $K_{j-1}(\ell)$ where either:

(a) $\ell'/\ell \in K_{j-1}$;

(b) $\ell' \in K_{j-1}$;, or

(c) ℓ is algebraic over K_{j-1}.

[1] Which is more commonly written

$$z(1-z)y'' + [\gamma - (\alpha + \beta + 1)z]y' - \alpha\beta y = 0.$$

[2] See, e.g., [25, Chapter VII, particularly the table on p. 128].

Or see Jeremy Gray, *Linear Differential Equations and Group Theory from Riemann to Poincaré*, **Birkhäuser, Boston, 1986, pages 98-108. This needs to be added to the references.**

Of course Kolchin would cite the original paper. That is

H.A. Schwarz, Ueber diejenigen Fälle, in welchen die Gaussische hypergeometrische Reihe eine algebraische Function ihres vierten Elementes darstellt, J.f.M. 75, 292-335 = Abh. II, 211-259.

An element $\ell \in K_j$ as in (a) is an *exponential of an integral over* K_{j-1}. Indeed, for obvious reasons one would generally write such an ℓ as $e^{\int k}$, where $k := \ell'/\ell \in K_{j-1}$. An element $\ell \in K_j$ as in (b) is an *integral over* K_{j-1}, and is often expressed as $\int k$ when $k := \ell' \in K_{j-1}$.

A function (germ) is *Liouvillian* if it is contained in some Liouvillian extension of K. Such functions are regarded as "elementary", or as being of "closed-form": they are obtained from rational functions by a finite sequence of adjunctions of exponentials, indefinite integrals, and algebraic functions. Logarithms, being indefinite integrals, are included, as are the elementary trigonometric functions (since they can be expressed in terms of exponentials). The differential Galois group of (1.1.1) gives information about the existence of closed form solutions.

1.3 The Connection with Algebraic Groups

The differential Galois group $G := G_{\mathrm{dg}}(L/K)$ of (1.1.1) is generally regarded as a matrix group. Specifically, any $g \in G$ defines a matrix $M_g = (m_{ij}(g)) \in \mathrm{Gl}(n, \mathbb{C})$ by

$$g \cdot y_j := \sum_{i=1}^{n} m_{ij}(g) y_i, \qquad j = 1, \ldots, n, \tag{1.3.1}$$

and the mapping $\rho : g \in G \mapsto M_g \in \mathrm{GL}(n, \mathbb{C})$ is a faithful matrix representation; one therefore identifies G with $\rho(G) \subset \mathrm{GL}(n, \mathbb{C})$. **We will prove in §...** that latter is actually an *algebraic group*, i.e., that there is a finite collection $\{p_k(x_{ij})\}$ of complex polynomials in n^2 variables such that $g \in G \simeq \rho(G)$ if and only if $p_k(m_{ij}(g)) = 0$ for all k.

Since the monodromy group of (1.1.1) is a subgroup of G it can also be regarded as a matrix group. However, it is generally not algebraic. The associated matrices are known classically as the *monodromy* or *circuit matrices* of the equation. The generators for the monodromy group of the hypergeometric equation were computed explicitly by Riemann, based on earlier work of E.E. Kummer, for all choices of the parameter values. **(See Gray, pages 23-28 and 39-44)** Since knowing the generators amounts to knowing the group, it seems fair to say that Riemann actually computed the monodromy group of the hypergeometric equation (at a time when group theory was in it's infancy). Unfortunately, progress in computing this group for other equations has been remarkably slow. The differential Galois group G has proven far more amenable to calculation.

To make the algebraic group concept a bit more transparent we offer two simple examples. (i) The subgroup $G \subset \mathrm{GL}(2, \mathbb{C})$ consisting of 2×2 complex matrices of the form

$$\begin{pmatrix} \lambda & 0 \\ \delta & \lambda^{-1} \end{pmatrix}, \qquad \lambda, \delta \in \mathbb{C}, \qquad \lambda \neq 0\,, \tag{1.3.2}$$

is algebraic: a matrix $m = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} \in \mathrm{GL}(2,\mathbb{C})$ is in G if and only if for $p_1(x_{11}, x_{12}, x_{21},, x_{22}) = x_{11}x_{22} - x_{21}x_{12} - 1 = \det((x_{ij})) - 1$ and $p_2(x_{11}, x_{12}, x_{21}, x_{22}) = x_{12}$ we have $p_1(m_{11}, m_{12}, m_{21}, m_{22}) = 0$ and $p_2(m_{11}, m_{12}, m_{21}, m_{22}) = 0$.
(ii) The subgroup $\mathrm{SL}(n,\mathbb{C})$ of unimodular (i.e., determinant 1) matrices of $\mathrm{GL}(n,\mathbb{C})$ is algebraic. Here we need only one polynomial, i.e., $p(x_{ij}) = \det((x_{ij})) - 1$.

It is the rich structure of algebraic groups which make differential Galois groups relatively easy to compute in comparison with monodromy groups. What turns out to be important is the fact that any algebraic subgroup $H \subset \mathrm{GL}(n,\mathbb{C})$ can be viewed as a topological space which is a finite union of disjoint closed connected components, and the *component of the identity*, i.e., that component H^0 containing the identity matrix, is always a normal subgroup of finite index[3]. Example: The group $\mathrm{SL}(n,\mathbb{C})$ is connected[4], hence $\mathrm{SL}(n,\mathbb{C})^0 = \mathrm{SL}(n,\mathbb{C})$.

One of the fundamental results of ordinary Galois theory is that a given polynomial equation is solvable by radicals if and only if the corresponding Galois group is solvable. We are now in a position to give the differential algebraic analogue.

Theorem 1.3.1 : *The Picard-Vessiot extension $L \supset K \simeq \mathbb{C}(z)$ of (1.1.1) is a Liouvillian extension if and only if the component of the identity of the differential Galois group is solvable.*

The proof is given in §...

When the component of the identity is solvable it is conjugate to a subgroup of the group of lower triangular matrices; this is the *Lie-Kolchin Theorem* **(which we will prove in §...)**. Consequence: $\mathrm{SL}(2,\mathbb{C})$ is not solvable.

For the remainder of this chapter our concern will be with algebraic subgroups of $\mathrm{SL}(2,\mathbb{C})$.

Theorem 1.3.2 : *For any algebraic subgroup $G \subset \mathrm{SL}(2,\mathbb{C})$ one of the following possibilities holds:*

(a) *G is "reducible", i.e., conjugate to a subgroup of the group*

$$\{\, m \in \mathrm{SL}(2,\mathbb{C}) \,:\, m = \begin{pmatrix} \lambda & 0 \\ \delta & \lambda^{-1} \end{pmatrix}, \quad \lambda, \delta \in \mathbb{C}, \quad \lambda \neq 0 \,\}.$$

(b) *G is "imprimitive", i.e., conjugate to a subgroup of $D \cup \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} D$, where D is the group of diagonal matrices in $\mathrm{SL}(2,\mathbb{C})$, i.e.,*

$$D := \{\, m \in \mathrm{SL}(2,\mathbb{C}) \,:\, m = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}, \quad \lambda \in \mathbb{C}\backslash\{0\} \,\}.$$

[3]See, e.g., [**?**, Chapter IV, Lemma 4.5, p. 28].
[4]See, e.g., [32, Exercise 2.2.2, p. 37].

(c) *G is finite, contains the negative $-I$ of the identity matrix I, and the factor group $G/\{I,-I\}$ is isomorphic to either*

(i) *the alternating group A_4* (the "projectively tetrahedral case"),

(ii) *the symmetric group S_4* (the "projectively octahedral case"), *or*

(iii) *the alternating group A_5* (the "projectively icosahedral case").

(d) $G = \mathrm{SL}(2,\mathbb{C})$.

The possibilities are not mutually exclusive, e.g., any algebraic subgroup of D is both reducible and imprimitive. Moreover, (a) and (b) include finite groups, i.e., cyclic, dihedral and octahedral, although not those given in (c).

Proof : See [**?**, pp. 7 and 27]. **Jerry: In this case [and some which follow] we may want to leave the reference and NOT give a proof. However, much depends on how things get written up later. Frankly, I like your proofs of the various parts of this theorem, but working out (c) would add many pages. (I'll have more to say on those particular groups later.)** **q.e.d**.

1.4 Equations of Second-Order

In this section we specialize (1.1.1) to the case $n = 2$, i.e., to

$$y'' + a_1(z)y' + a_2(z)y = 0\,. \tag{1.4.1}$$

The associated equation

$$y'' + (a_2(z) - \tfrac{1}{4}\,a_1^2(z) - \tfrac{1}{2}\,a_1'(z))y = 0 \tag{1.4.2}$$

is called the *normal form* of (1.4.1) and (1.4.1) is the *standard form*[5] of (1.4.2). One checks easily that $y = y(z)$ is a solution of (1.4.1) if and only if $w = w(z) := e^{\frac{1}{2}\int^x a_1(t)dt}y(z)$ is a solution of (1.4.2), and since our concern is with the nature of solutions there is no loss of generality in replacing (1.4.1) with (1.4.2).

Examples 1.4.1 :

(a) The normal form of the hypergeometric equation

$$y'' + \frac{\gamma - (\alpha+\beta+1)z}{z(1-z)}\,y' - \frac{\alpha\beta}{z(1-z)}\,y = 0$$

is

$$y'' + \frac{1}{4}\left\{\frac{1-\lambda^2}{z^2} + \frac{1-\nu^2}{(z-1)^2} - \frac{\lambda^2-\nu^2+\mu^2-1}{z} + \frac{\lambda^2-\nu^2+\mu^2-1}{z-1}\right\} y = 0\,,$$

[5] I have introduced the "standard form" terminology for convenience.

where

$$\begin{aligned} \lambda &:= 1-\gamma \\ \nu &:= \gamma-(\alpha+\beta) \\ \mu &:= \pm(\alpha-\beta)\,. \end{aligned}$$

(b) Equation (1.4.1) is known as *Riemann's equation* when

$$\begin{aligned} a_1(z) &= \frac{1-\eta_1-\mu_1}{z}+\frac{1-\eta_2-\mu_2}{z-1} \quad \text{and} \\ a_2(z) &= \frac{\eta_1-\mu_1}{z^2}+\frac{\eta_2-\mu_2}{(z-1)^2}+\frac{\eta_3\mu_3-\eta_1\mu_1-\eta_2\mu_2}{z(z-1)}\,, \end{aligned}$$

where the complex parameters η_j, μ_j are subject to the single constraint $\sum_j(\eta_j-\mu_j)=1$. The normal form is

$$y''+\frac{1}{4}\left\{\frac{1-(\eta_1-\mu_1)^2}{z^2}+\frac{1-(\eta_2-\mu_2)^2}{(z-1)^2}+\frac{\nu}{z}-\frac{\nu}{z-1}\right\}y=0\,,$$

where

$$\nu := 1-(\eta_1-\mu_1)^2-(\eta_2-\mu_2)^2+(\eta_3-\mu_3)^2\,.$$

(c) Examples (a) and (b) are special cases of second-order "Fuchsian equations," which for our immediate purposes can be defined as second-order equations of the form

$$y''+\left(\sum_{j=1}^{m}\frac{A_j}{z-a_j}\right)y'+\left(\sum_{j=1}^{m}\frac{B_j}{(z-a_j)^2}+\sum_{j=1}^{m}\frac{C_j}{z-a_j}\right)y=0\,.$$

Here the "singularities" $a_1,\ldots,a_m\in\mathbf{C}$ are assumed distinct, and the sole restriction on the the complex constants A_j, B_j and C_j is $\sum_j C_j=0$. The normal form is

$$y''+\frac{1}{4}\left(\sum_{j=1}^{m}\frac{\hat{B}_j}{(z-a_j)^2}+\sum_{j=1}^{m}\frac{\hat{C}_j}{z-a_j}\right)y=0\,,$$

where

$$\begin{aligned} \hat{B}_j &:= \tfrac{1}{4}(1+4B_j-(1-A_j)^2)\,, \\ \hat{C}_j &:= C_j-\tfrac{1}{2}A_j\left(\textstyle\sum_{i\neq j}\frac{A_i}{a_j-a_i}\right)\,, \end{aligned}$$

and is again Fuchsian.

(d) The normal form of Bessel's equation

$$y''+\frac{1}{z}y'+\left(1-\frac{\nu^2}{z^2}\right)y=0$$

("of order ν")[6] is

$$y'' + \frac{1}{4}\left(\frac{1-4(\nu^2-z^2)}{z^2}\right) y = 0\,.$$

Neither equation is Fuchsian.

(e) Airy's equation

$$y'' - zy = 0$$

is already in normal form. (The standard form is exactly the same equation.) This is again a non-Fuchsian example.

To ease notation we rewrite (1.4.2) as

$$y'' = r(z)y, \qquad r(z) \in \mathbb{C}(z)\,. \tag{1.4.3}$$

The benefit of the normal form is given by the following result.

Proposition 1.4.2 : *The differential Galois group of* (2.2.13) *is an algebraic subgroup of* $\mathrm{SL}(2,\mathbb{C})$.

A proof will be given in §... .

Recall that when $y = y(z)$ is a non-zero solution a solution of (2.2.13) a linearly independent over $\mathbb{C}$ is provided by

$$w = w(z) = y(z)\int^z \frac{1}{(y(t))^2}dt \tag{1.4.4}$$

("reduction of order"), and so to understand the nature of the solutions of (2.2.13) we really need only understand the nature of any particular non-zero solution. This is where the differential Galois group can be quite helpful.

In the following result we place the emphasis on the reducible case for illustrative purposes.

[6] Bessel's equation is commonly written as

$$z^2y'' + zy' + (z^2-\nu^2)y = 0\,;$$

we are simply adopting the format (1.4.1).

Theorem 1.4.3 : *Let* $G \subset \mathrm{SL}(2,\mathbb{C})$ *denote the differential Galois group of* (2.2.13).

(a) (The Reducible Case) *The following statements are equivalent:*

(i) G *is reducible;*

(ii) *equation* (2.2.13) *has a solution of the form* $y = e^{\int^z \theta(t)dt}$ *with* $\theta(z) \in K \simeq \mathbb{C}(z)$ *;*

(iii) *the Riccati equation* $w' + w^2 = r$ *has a solution* $\theta \in K$ *; and*

(iv) *the linear operator* $\mathcal{L} = \frac{d^2}{dz^2} - r$ *factors in the non-commutative polynomial ring* $K[\frac{d}{dz}]$*, and when expressed as a product of monic polynomials that factorization must be*

$$\frac{d^2}{dz^2} - r = (\frac{d}{dz} + \theta)(\frac{d}{dz} - \theta),$$

where θ *is as in* (iii).

(b) (The Imprimitive Case) *When* G *is not reducible the following statements are equivalent:*

(i) G *is imprimitive; and*

(ii) *equation* (2.2.13) *has a solution of the form* $y = e^{\int^z \theta(t)dt}$ *with* θ *algebraic of degree* 2 *over* K.

(c) (The Remaining Finite Cases) *When* G *is not reducible and not imprimitive the following statements are equivalent:*

(i) G *is finite; and*

(ii) *all solutions of* (2.2.13) *are algebraic over* K.

(d) *When none of* (a)-(c) *hold* $G = \mathrm{SL}(2,\mathbb{C})$.

Proof :

(a)

(i) $\Rightarrow$ (ii) : By assumption there is a solution $y = y(z)$ of (2.2.13) such that for each $g \in G$ there is a $\lambda_g \in \mathbb{C}$ such that $g \cdot y = \lambda_g y$. (This can be seen by writing λ^{-1} in (1.3.2) as λ_g and using $y = y(z)$ as the second basis element.) Since g commutes with d/dz it follows that $g \cdot y' = (\lambda_g y)' = \lambda_g y'$. For $\theta := y'/y$, which we note implies $y = e^{\int \theta}$, we then have

$$g \cdot \theta = g \cdot (y'/y) = (g \cdot y')/(g \cdot y) = \lambda_g y'/\lambda_g y = y'/y = \theta,$$

and since K is the fixed field of G we conclude that $\theta \in K$.

(ii) $\Rightarrow$ (i) : We have

$$\begin{aligned}(\frac{g\cdot y}{y})' &= \frac{y\,g\cdot y' - y'\,g\cdot y}{y^2}\\ &= \frac{y\,g\cdot \theta y - \theta y\,g\cdot y}{y^2}\\ &= \frac{\theta(y\,g\cdot y - y\,g\cdot y)}{y^2}\\ &= 0,\end{aligned}$$

hence $\lambda_g := g\cdot y/y \in \mathbb{C}$. (In other words: when y is used as the second element of a basis the matrix of g is lower triangular.) Since $g \in G$ is arbitrary this gives reducibility.

(ii) $\Leftrightarrow$ (iii) : For $y = e^{\int\theta}$ we have $y' = \theta y$ and $y'' = (\theta' + \theta^2)y$, hence $y'' = ry \;\Leftrightarrow\; \theta' + \theta^2 = r$.

(iii) $\Leftrightarrow$ (iv) : From the chain-rule we have[7] $\frac{d}{dz}t = t\frac{d}{dz} + t'$ for any $y \in K$, and when $s \in K$ also holds it follows that

$$\begin{aligned}(\frac{d}{dz} - s)(\frac{d}{dz} - t) &= \frac{d^2}{dz^2} - \frac{d}{dz}t - s\frac{d}{dz} + st\\ &= \frac{d^2}{dz^2} - (t\frac{d}{dz} + t') - s\frac{d}{dz} + st\\ &= \frac{d^2}{dz^2} - (s+t)\frac{d}{dz} - t' + st,\end{aligned}$$

whereupon picking $t = -s := \theta$ we obtain

$$(\frac{d}{dz} + \theta)(\frac{d}{dz} - \theta) = \frac{d^2}{dz^2} - (\theta' + \theta^2).$$

The equivalence follows easily.

(b) **This will be established in §... .**

(c) By Theorems 1.3.2 and 1.1.1.

(d) By Theorem 1.3.2.

q.e.d.

Write $r \in \mathbb{C}(z)$ as s/t, where $s, t \in \mathbb{C}[z]$ are relatively prime. The poles of r in the complex plane then coincide with the zeros of t, and the order of such a pole is the multiplicity of the corresponding zero. In the sequel "pole" will always mean "pole in the complex plane". The *order of* r *at* ∞ is defined to be $\deg(t) - \deg(s)$.

[7]The definition of $\frac{d}{dz}t : K \to K$ as an operator is $\frac{d}{dz}t : k \mapsto \frac{d}{dz}(tk)$. Since the chain-rule gives

$$\frac{d}{dz}(tk) = t\,\frac{d}{dz}k + (\frac{d}{dz}t)\cdot k = t\,\frac{d}{dz}k + t'\cdot k$$

we see that

$$\frac{d}{dz}t = t\,\frac{d}{dz} + t'.$$

Theorem 1.4.4 : *Necessary conditions in the first three respectively cases of* Theorem 1.4.3 *are as follows.*

> Case I : *Any pole of* r *has order* 1 *or even order, and the order of* r *at* ∞ *must be even or else be greater than* 2.
>
> Case II : *The rational function* r *must have at least one pole which is of order* 2 *or of odd order greater than* 2.
>
> Case III : *The order of each pole of* r *cannot exceed* 2 *and the order of* r *at* ∞ *must be at least* 2. *Moreover, if the partial fraction expansion of* r *is*
>
> $$r = \sum_i \frac{\alpha_i}{(z-c_i)^2} + \frac{\beta_j}{z-d_j}\,,$$
>
> *and if* $\gamma := \sum_i \alpha_i + \sum_j \beta_j d_j$, *then each* $\sqrt{1+4\alpha_i}$ *must be a rational number,* $\sum_j \beta_j = 0$ *must hold, and* $\sqrt{1+4\gamma}$ *must also be a rational number.*

A sketch of the argument for Case I should convey the spirit of the proof. First recall from Theorem 1.4.3(a) that $e^{\int \theta}$ is a solution of (2.2.13) if and only if $\theta' + \theta^2 = r$. One obtains the necessary conditions of Case I by substituting pole (i.e., Laurent) expansions of r and θ (in the second case with undetermined coefficients) into this equation and comparing exponents.

A complete proof will be given in §... .

Examples 1.4.5 :

(a) *Airy's equation has no Liouvillian solutions. More generally, equation* (2.2.13) *has no elementary solutions when* r *is a polynomial of odd degree.* (Airy's equation is introduced in Example 1.4.1(e).) The function r has no poles (in the complex plane), and the order at ∞ is an odd negative number. The necessary conditions of Cases I-III are therefore violated.

(b) *Bessel's equation has Liouvillian solutions if and only if* ν *is one-half of an odd integer.* Here the necessary conditions for Case III fail, but not those for Cases I and II. However, with a bit more work **(which will be carried out in §...)** one can eliminate Case II and prove that Case I holds if and only if n has the stated form.

1.5 Examples of Differential Galois Group Calculations

In this section we specialize Example 1.4.1(c) to the case $m = 2$ (i.e., two finite singularities). Specifically, we consider the normal form

$$y'' + \frac{1}{4}\left(\sum_{j=1}^{2}\frac{\hat{B}_j}{(z-a_j)^2} + \sum_{j=1}^{2}\frac{\hat{C}_j}{z-a_j}\right) y = 0 \tag{1.5.1}$$

of

$$w'' + \left(\sum_{j=1}^{2}\frac{A_j}{z-a_j}\right) w' + \left(\sum_{j=1}^{2}\frac{B_j}{(z-a_j)^2} + \sum_{j=1}^{2}\frac{C_j}{z-a_j}\right) w = 0\,.$$

The hypergeometric and Riemann equations are particular cases.

The nature of the associated differential Galois group in this context is easily determined. To indicate how this is done define

$$A_3 := 2 - (A_1 + A_2)\,, \quad B_3 := \sum_{j=1}^{2}(B_j + C_j a_j)\,,$$

and

$$t_j := -2\cos\pi\sqrt{(A_j-1)^2 - 4B_j}, \quad j = 1,2,3\,.$$

Examples 1.5.1 :

(a) For the hypergeometric equation one has

$$\begin{aligned} t_1 &= -2\cos\pi(\gamma-1) \\ t_2 &= -2\cos\pi(\gamma-(\alpha+\beta)) \\ t_3 &= -2\cos\pi(\alpha-\beta)\,. \end{aligned}$$

(b) For Riemann's equation one has

$$t_j = -2\cos\pi(\eta_j - \mu_j) \quad j = 1,2,3\,.$$

Now let

$$\sigma := t_1^2 + t_2^2 + t_3^2 - t_1 t_2 t_3\,.$$

Theorem 1.5.2 : *The differential Galois group of* (1.5.1) *is:*

(a) *reducible if and only if* $\sigma = 4$ *;*

(b) *imprimitive but not reducible if and only if* $\sigma \neq 4$ *and at least two of* t_1, t_2 *and* t_3 *are zero ;*

(c_i) *projectively tetrahedral if and only if* $\sigma = 2$ *and* $t_1, t_2, t_3 \in \{0, \pm 1\}$;

(c_{ii}) *projectively octahedral if and only if* $\sigma = 3$ *and* $t_1, t_2, t_3 \in \{0, \pm 1, \pm\sqrt{2}\}$;

(c_{iii}) *projectively icosahedral if and only if* $\sigma \in \{2-\mu_2, 3, 2+\mu_1\}$ *and* $t_1, t_2, t_3 \in \{0, \pm\mu_2, \pm 1, \pm\mu_1\}$, *where* $\mu_1 := \frac{1}{2}(1+\sqrt{5})$ *and* $\mu_2 = -\frac{1}{2}(1-\sqrt{5}) = \mu_1^{-1}$; *and*

(d) *otherwise is* $\mathrm{SL}(2, \mathbf{C})$.

Jerry - We may simply have to reference this proof - it is quite long and not relevant to the rest of what we are writing. On the other hand, there may be a way to dig it out of your proof of Theorem 1.3.2(c). Indeed, the proofs of (a) and (b) are short and easy - as usual, (c) is the bad case.

For a proof[8] see [5], and for a generalization of assertions (c_i)-(c_{iii}) see [20].

Examples 1.5.3 :

(a) For the hypergeometric equation one can use Theorem 1.5.2(a) to conclude that the reducible case holds for the normal form if and only if at least one of α, β, $\gamma - \alpha$ and $\gamma - \beta$ is an integer[9]. If this is not the case one can deduce from (b) that the group is imprimitive if and only if at least two of γ, $\gamma - (\alpha + \beta)$ and $\alpha - \beta$ are halves of odd integers. Finally, from (c) one can reproduce the result of Schwarz on algebraic solutions discussed in §1. (When the differential Galois group is finite it coincides with the monodromy group.)

(b) For Riemann's equation the reducible case holds for the normal form if and only if at least one of the four quantities $\eta_1+\eta_2+\eta_3$, $\eta_1+\eta_2+\mu_3$, $\eta_1+\mu_2+\eta_3$ and $\mu_1+\eta_2+\eta_3$ is an integer[10].

(c) Lagrange's equation is

$$w'' - \frac{2z}{1-z^2}w' + \frac{\lambda}{1-z^2}w = 0\,,$$

where $\lambda \in \mathbb{R}$. The normal form is

$$y'' + \frac{1}{4}\left(\frac{1}{(z-1)^2} + \frac{1}{(z+1)^2} - \frac{2\lambda+1}{z-1} + \frac{2\lambda+1}{z+1}\right)y = 0\,.$$

Here one computes that

$$t_1 = t_2 = -2, \quad t_3 = -2\cos\pi\sqrt{1+4\lambda}$$

[8] A proof of (a) can also be found in [2, Proposition 2.22, pgs 1647-8].

[9] See, e.g., [2, Theorem 2.24 and Corollary 2.27, p. 1648]. For a classical perspective on this condition see [25, Chapter VI, §23, p. 90]. **The proof is not long and can easily be included.**

[10] See, e.g., [2, Corollary 2.27, p. 1648].

and

$$\sigma = 4\left(\cos(\pi\sqrt{1+4\lambda}) + 1\right)^2 + 4\,.$$

Using Theorem 1.5.2 one sees that the differential Galois group of the normal form is reducible if and only if $\lambda = k(k+1)$, where k is an integer, and otherwise is $\mathrm{SL}(2,\mathbb{C})$.

Chapter 2

Differential structures

One can regard elementary linear algebra as the study of linear transformations between finite-dimensional vector spaces, with matrices entering primarily as basis descriptions of these entities, or as the study of matrices with applications to linear transformations between vector spaces. The first view is geometric; the second computational. On can approach linear differential equations similarly: as the study of entities herein called "differential structures," with linear differential equations appearing merely as basis descriptions, or as the study of linear differential equations with applications to differential structures. We prefer the geometric approach in both cases.

2.1 Generalities on Derivations

Our first task is to generalize the discussion surrounding (1.1.2).

Let R be a (not necessarily commutative) ring with identity. An additive group endomorphism $\delta : r \in R \mapsto r' \in R$ is a *derivation* if the *Leibniz* or *product rule*

$$(rs)' = rs' + r's \tag{2.1.1}$$

holds for all $r, s \in R$. One also writes r' as $r^{(1)}$ and defines $r^{(n)} := (r^{(n-1)})'$ for $n \geq 2$. The notation $r^{(0)} := r$ proves convenient.

The usual derivative operator $\frac{d}{dz}$ on the polynomial ring $\mathbb{C}[z]$ is the basic example of a derivation. For a second example consider $\frac{d}{dz}$ extended to the quotient field $\mathbb{C}(z)$. Since $\mathbb{C}(z)$ is isomorphic to the field $\mathcal{M}(\mathbb{P}^1)$ of meromorphic functions on the Riemann sphere $\mathbb{P}^1$ the operator $\frac{d}{dz}$ can be viewed as a "local" (i.e., "around 0") description of a derivation on $\mathcal{M}(\mathbb{P}^1)$. The same derivation is described in terms of the usual coordinate $t = 1/z$ around ∞ by $-t^2 \frac{d}{dt}$. This local coordinate viewpoint of a globally defined object is implict in classical treatments of linear differential equations on $\mathbb{P}^1$. By passing to the germ level at a point $z_0 \in \mathbb{P}^1$ we obtain the derivation considered in the previous chapter.

For an additional example of a derivation note that the zero mapping $r \in R \mapsto 0 \in R$ on any ring R satisfies the required properties; this is the *trivial*

derivation.

For a non-commutative example choose an integer $n > 1$, let R be the collection of $n \times n$ matrices with entries in a commutative ring A with a derivation $a \mapsto a'$, and for $r = (a_{ij}) \in R$ define $r' := (a'_{ij})$.

When $r \mapsto r'$ is a derivation on R one sees from additivity that $0' = (0+0)' = 0' + 0'$, hence

$$0' = 0, \tag{2.1.2}$$

and from the Leibniz rule (2.1.1) that $1' = (1 \cdot 1)' = 1 \cdot 1' + 1' \cdot 1 = 1' + 1'$, hence

$$1' = 0\,. \tag{2.1.3}$$

When $r \in R$ is a unit it then follows from $1 = rr^{-1}$ and (2.1.1) that

$$0 = (rr^{-1})' = r \cdot (r^{-1})' + r' \cdot r^{-1},$$

whence

$$(r^{-1})' = -r^{-1} \cdot r' \cdot r^{-1}\,. \tag{2.1.4}$$

This formula will prove particularly useful in connection with the matrix example introduced above. When R is commutative it assumes the more familiar form

$$(r^{-1})' = -r' r^{-2}\,. \tag{2.1.5}$$

A ring, integral domain or field equipped with a (single) derivation is called a(n *ordinary*) *differential ring, differential domain* or *differential field* respectively. Derivations will be denoted $r \mapsto r'$ unless confusion might otherwise result.

An element r of a differential ring R satisfying $r' = 0$ is said to be (a) *constant*. From additivity, (2.1.2), (2.1.3) and the Leibniz rule we verify easily that the collection $R_C \subset R$ of constants is a subring of R which contains the image of $\mathbb{Z}$ under the usual mapping $n \mapsto n \cdot 1_R$. If R is a domain the same obviously holds for R_C, and from (2.1.5) we see that R_C is a field if R is a field. When any of the three respective cases requires clarification we speak of the *ring, domain* or *field of constants*. Example: For the differential ring $(\mathbb{C}(z), d/dz)$ one has $(\mathbb{C}(z))_C = \mathbb{C}$.

When K is a differential field the determinant

$$W := W(k_1, \ldots, k_n) := \det \begin{pmatrix} k_1 & k_2 & \cdots & & k_n \\ k_1' & k_2' & & \vdots & k_n' \\ k_1^{(2)} & k_2^{(2)} & & & \vdots \\ \vdots & & & & \\ k_1^{(n-1)} & k_2^{(n-1)} & \cdots & \cdots & k_n^{(n-1)} \end{pmatrix} \tag{2.1.6}$$

is called the *Wronskian* of the elements $k_1, \ldots, k_n \in K$. This entity is useful for determining linear (in)dependence over the subfield $K_C \subset K$.

Proposition 2.1.1 : *Elements $k_1, \ldots, k_n$ of a differential field K are linearly dependent over the field of constants K_C if and only if their Wronskian is* 0.

Proof :

$\Rightarrow$ For any $c_1, \ldots, c_n \in K_C$ and any $0 \leq m \leq n$ we have $(\sum_j c_j k_j)^{(m)} = \sum_j c_j k_j^{(m)}$. In particular, when $\sum_j c_j k_j = 0$ the same equality holds when k_j is replaced by the j^{th} column of the Wronskian and 0 is replaced by a column of zeros. The forward assertion follows.

$\Leftarrow$ The vanishing of the Wronskian implies a dependence relation (over K) among columns, and as a result there must be elements $c_1, \ldots, c_n \in K$, not all 0, such that

$$\sum_{j=1}^{n} c_j k_j^{(m)} = 0 \qquad \text{for} \qquad m = 0, \ldots, n-1. \tag{i}$$

What requires proof is that the c_j may be chosen in K_C, and this we establish by induction on n. As the case $n = 1$ is trivial we assume $n > 1$ and that the result holds for any subset of K with at most $n-1$ elements.

If there is also a dependence relation (over K) among the columns of the Wronskian of $y_2, \ldots, y_n$, e.g., if $c_1 = 0$, then by the induction hypothesis the elements $y_2, \ldots, y_n \in K$ must be linearly dependent over K_C. But the same then holds for $y_1, \ldots, y_n$, which is precisely what we want to prove. We therefore assume (w.l.o.g.) that $c_1 = 1$ and that the columns of the Wronskian of $y_2, \ldots, y_k$ are linearly independent over K. From (i) we then have

$$0 = (\sum_{j=1}^{n} c_j k_j^{(m)})' = \sum_{j=1}^{n} c_j k_j^{(m+1)} + \sum_{j=2}^{n} c_j' k_j^{(m)} = 0 + \sum_{j=2}^{n} c_j' k_j^{(m)} = \sum_{j=2}^{n} c_j' k_j^{(m)}$$

for $m = 0, \ldots, n-2$, thereby forcing $c_2' = \cdots = c_n' = 0$. But this means $c_j \in K_C$ for $j = 1, \ldots, n$, and the proof is complete. **q.e.d.**

Jerry: Your C^∞-Wronskian example should go here. Moreover, I have no objection if you want to replace the proof above with your proof.

2.2 Differential Structures

In this section K denotes a differential field with derivation $k \mapsto k'$ and V is a K-space (i.e., a vector space over K). *The collection of $n \times n$ matrices with entries in K is denoted $\mathfrak{gl}(n, K)$.*

A *differential structure* on V is an additive group homomorphism $D : V \to V$ satisfying

$$D(kv) = k'v + kDv, \qquad k \in K, \qquad v \in V, \tag{2.2.1}$$

where Dv abbreviates $D(v)$. The *Leibniz rule* terminology is also used with (2.2.1). Vectors $v \in V$ satisfying $Dv = 0$ are said to be *horizontal* (w.r.t. D).

The zero vector $0 \in V$ always has this property; other such vectors need not exist.

When $D : V \to V$ is a differential structure the pair (V, D) is called a *differential module*.

As an example of a differential structure take $V := K^n$ and define $D : V \to V$ by

$$D(k_1, k_2, \ldots, k_n) := (k_1', k_2', \ldots, k_n'). \tag{2.2.2}$$

Further examples will be evident from Proposition 2.2.2.

Since K_C is a subfield of K we can regard V as a vector space over K_C by restricting scalar multiplication to $K_C \times V$.

Proposition 2.2.1 :

(a) *Any differential structure $D : V \to V$ is K_C-linear.*

(b) *The collection of horizontal vectors of a differential structure $D : V \to V$ coincides with the kernel* $\ker D$ *of D when D is considered as a K_C-linear mapping*[1].

(c) *The horizontal vectors of a differential structure $D : V \to V$ constitute a K_C-subspace of* (the K_C-space) V.

Proof :

(a) Immediate from (2.2.1).

(b) Obvious from the definition of horizontal.

(c) Immediate from (b).

q.e.d.

A differential structure can be viewed as a coordinate-free formulation of a first-order system of linear ordinary differential equations. Specifically, suppose V is finite-dimensional, $\mathbf{e} = (e_j)_{j=1}^n \subset V^n$ is a(n ordered) basis, and $B = (b_{ij}) \in \mathfrak{gl}(n, K)$ is defined by

$$De_j := \sum_{j=1}^{n} b_{ij} e_i, \qquad j = 1, \ldots, n. \tag{2.2.3}$$

(Example: For D as in (2.2.2) and[2] $e_j = (0, \ldots, 0, 1, 0, \ldots, 1)$ [1 in slot j] for $j = 1, \ldots, n$ we have $B = (0)$ [the zero matrix].) We refer to B as the *defining* $(\mathbf{e})$*-matrix* of D, or as the *defining matrix of D relative to the basis* $\mathbf{e}$. Note that for any $v = \sum_{j=1}^n v_j e_j \in V$ the Leibniz rule (2.2.1) gives

$$Dv = \sum_{i=1}^{n} (v_i' + \sum_{j=1}^{n} b_{ij} v_j) e_i. \tag{2.2.4}$$

[1] When D is not linear the "kernel" terminology is generally replaced by "zero set" or "vanishing set", or is indicated by means of the notation $D^{-1}(\{0\})$.

[2] The superscript τ ("tau") denotes transposition.

If for any $w = \sum_{j=1}^{n} w_j e_j \in V$ we write $w_{\mathbf{e}}$ (resp. $w'_{\mathbf{e}}$) for the column vector with j^{th}-entry w_j (resp. w'_j) this last equality can be expressed in the matrix form

$$(Dv)_{\mathbf{e}} = v'_{\mathbf{e}} + Bv_{\mathbf{e}}, \tag{2.2.5}$$

and we conclude that $v \in V$ is horizontal if and only if $v_{\mathbf{e}}$ is a solution of the first-order linear system

$$x' + Bx = 0, \tag{2.2.6}$$

wherein $x = (x_1, \ldots, x_n)^\tau$. This is the *defining* $(\mathbf{e})$*-equation* of D.

Linear systems of ordinary differential equations of the form (2.2.6) are called *homogeneous*. One can also ask for solutions of *inhomogeneous* systems, i.e., systems of the form

$$x' + Bx = b, \tag{2.2.7}$$

wherein $0 \neq b \in K^n$ is given. For $b = w_{\mathbf{e}}$ this is equivalent to the search for a vector $v \in V$ satisfying

$$Dv = w\,. \tag{2.2.8}$$

Equation (2.2.6) is the *homogeneous equation corresponding to* (2.2.7).

Proposition 2.2.2 : *When* $\dim_K V < \infty$ *and* $\mathbf{e}$ *is a basis the correspondence between differential structures* $D : V \to V$ *and* $n \times n$ *matrices* B *defined by* (2.2.3) *is bijective; the inverse assigns to a matrix* $B \in \mathfrak{gl}(n, K)$ *the differential structure* $D : V \to V$ *defined by* (2.2.5).

Proof : The proof is by routine verification. **q.e.d.**

Since the correspondence between matrices $B \in \mathfrak{gl}(n, K)$ and linear systems $x' + Bx$ is also bijective, the statement opening the paragraph surrounding (2.2.3) should now be clear.

Proposition 2.2.3 :

(a) *The solutions of* (2.2.6) *within* K^n *form a vector space over* K_C.

(b) *When* $\dim_K V = n < \infty$ *and* $\mathbf{e}$ *is a basis of* v *the* K*-linear isomorphism* $v \in V \mapsto v_{\mathbf{e}} \in K^n$ *restricts to a* K_C*-linear isomorphism between the* K_C*-subspace of* V *consisting of horizontal vectors and the* K_C*-subspace of* K^n *consisting of solutions of* (2.2.6).

Proof :

(a) When $y_1, y_2 \in K^n$ are solutions and $c_1, c_2 \in K_C$ we have

$$\begin{aligned}(c_1y_1 + c_2y_2)' &= (c_1y_1)' + (c_2y_2)' \\ &= c'_1y_1 + c_1y'_1 + c'_2y_2 + c_2y'_2 \\ &= 0 \cdot y_1 + c_1(-By_1) + 0 \cdot y_2 + c_2(-By_2) \\ &= -Bc_1y_1 - Bc_2y_2 \\ &= -B(c_1y_1 + c_2y_2)\,.\end{aligned}$$

(b) That the mapping restricts to a bijection between horizontal vectors and solutions was already noted immediately before (2.2.6), and since the correspondence $v \mapsto v_{\mathbf{e}}$ is K-linear and K_C is a subfield of K any restriction to a K_C-subspace must be K_C-linear.

q.e.d.

Suppose $\hat{\mathbf{e}} = (\hat{e}_j)_{j=1}^n \subset V^n$ is a second basis and $P = (p_{ij})$ is the transition matrix, i.e., $e_j = \sum_{i=1}^n p_{ij}\hat{e}_i$. Then the defining $\mathbf{e}$ and $\hat{\mathbf{e}}$-matrices B and A of D are easily seen to be related by

$$A := P^{-1}BP + P^{-1}P', \tag{2.2.9}$$

where $P' := (p'_{ij})$. The transition from B to A is viewed classically as a change of variables: substitute $x = Pw$ in (2.2.6); then note from

$$0 = (Pw)' + BPw = Pw' + P'w + BPw$$

that

$$w' + (P^{-1}BP + P^{-1}P')w = 0\,.$$

The modern viewpoint is to regard $(B, P) \mapsto P^{-1}BP + P^{-1}P'$ as defining a right action of $GL(n, K)$ on $\mathfrak{gl}(n, K)$; this is the action by *gauge transformations*.

The concept of an n^{th}-order linear homogeneous equation in the context of a differential field K is formulated in the obvious way: an element $k \in K$ is a solution of

$$y^{(n)} + \ell_1 y^{(n-1)} + \cdots + \ell_{n-1}y' + \ell_n y = 0\,, \tag{2.2.10}$$

where $\ell_1, \ldots, \ell_n \in K$, if and only if

$$k^{(n)} + \ell_1 k^{(n-1)} + \cdots + \ell_{n-1}k' + \ell_n k = 0\,, \tag{2.2.11}$$

where $k^{(2)} := k'' := (k')'$ and $k^{(j)} := (k^{(j-1)})'$ for $j > 2$. Using a Wronskian argument one can easily prove that (2.2.10) has at most n solutions (in K) linearly independent over K_C.

As in the classical case $k \in K$ is a solution of (2.2.10) if and only if the column vector $(k, k', \ldots, k^{(n-1)})^\tau$ is a solution of

$$x' + Bx = 0, \qquad B = \begin{pmatrix} 0 & -1 & 0 & \cdots & & 0 \\ \vdots & 0 & -1 & & & \vdots \\ & & 0 & \ddots & & \\ & & & \ddots & -1 & 0 \\ & & & & 0 & -1 \\ \ell_n & \ell_{n-1} & \cdots & \cdots & \ell_2 & \ell_1 \end{pmatrix}. \tag{2.2.12}$$

Indeed, one has the following analogue of Proposition 2.2.3.

Proposition 2.2.4 :

(a) *The solutions of* (2.2.10) *within* K *form a vector space over* K_C.

(b) *The* K_C*-linear mapping* $(y, y', \ldots, y^{(n-1)})^\tau \in K^n \mapsto y \in K$ *restricts to a* K_C*-linear isomorphism between the* K_C*-subspace of* V *consisting of horizontal vectors and the* K_C*-subspace of* K *described in* (a).

Proof : The proof is a routine verification. **q.e.d.**

Example 2.2.5 : Assume $K = \mathbb{C}(z)$ with derivation $\frac{d}{dz}$ and consider the first-order system

$$x' + \begin{pmatrix} \left(\frac{6z^4+(1-2\nu^2)z^2-1}{z(2z^4-1)}\right) & \frac{4z^6-4\nu^2z^4-8z^2+1}{z^4(2z^4-1)} \\ -\left(\frac{z^2(z^4+z^2-\nu^2)}{2z^4-1}\right. & \frac{(2\nu^2-1)z^2+3}{z(2z^4-1)} \end{pmatrix} x = 0\,, \qquad \text{(i)}$$

i.e.,

$$\begin{array}{ccccccccc} x_1' & + & \left(\frac{6z^4+(1-2\nu^2)z^2-1}{z(2z^4-1)}\right)x_1 & + & \left(\frac{4z^6-4\nu^2z^4-8z^2+1}{z^4(2z^4-1)}\right)x_2 & = & 0 \\ x_2' & - & \left(\frac{z^2(z^4+z^2-\nu^2)}{2z^4-1}\right)x_1 & + & \left(\frac{(2\nu^2-1)z^2+3}{z(2z^4-1)}\right)x_2 & = & 0 \end{array}\,,$$

wherein ν is a complex parameter. This has the form (2.2.6) with

$$B := \begin{pmatrix} \left(\frac{6z^4+(1-2\nu^2)z^2-1}{z(2z^4-1)}\right) & \frac{4z^6-4\nu^2z^4-8z^2+1}{z^4(2z^4-1)} \\ -\left(\frac{z^2(z^4+z^2-\nu^2)}{2z^4-1}\right. & \frac{(2\nu^2-1)z^2+3}{z(2z^4-1)} \end{pmatrix},$$

and with the choice

$$P := \begin{pmatrix} \frac{-1}{z^2(2z^4-1)} & \frac{2z}{2z^4-1} \\ \frac{z^3}{2z^4-1} & \frac{-z^2}{2z^4-1} \end{pmatrix}$$

one sees that the transformed system

$$x' + Ax = 0, \qquad \text{where} \qquad A := P^{-1}BP + P^{-1}P' = \begin{pmatrix} 0 & -1 \\ 1-\frac{\nu^2}{z^2} & -\frac{1}{z} \end{pmatrix}, \quad \text{(ii)}$$

assumes the form seen in (2.2.12). The system (i) is thereby reduced to

$$y'' + \frac{1}{z}\,y' + \left(1 - \frac{\nu^2}{z^2}\right) y = 0\,, \qquad \text{(iii)}$$

i.e., to Bessel's equation (recall Example 1.4.1(d)).

We regard (i)-(ii) as distinct basis descriptions of the same differential structure, and (iii) and (iv) as additional ways of describing that structure.

Converting the n^{th}-order equation (2.2.10) to the first-order system (2.2.12) is standard practice. Less well-known is the fact that any first-order system of n equations can be converted to the form (2.2.12), and as a consequence can be expressed n^{th}-order form[3].

Jerry: Should we include the Cyclic Vector Theorem? This might be the place for it, or perhaps we need another section.

For many purposes n^{th}-order form has distinct advantages, e.g., explicit solutions are often easily constructed with series expansions.

[3]See, e.g., [**?**].

Proposition 2.2.6 : *When V is a K-space with differential structure $D : V \to V$ the following assertions hold.*

(a) *A collection of horizontal vectors within V is linearly independent over K if and only if it is linearly independent over K_C.*

(b) *The collection of horizontal vectors of V is a vector space over K_C of dimension at most* $\dim_K(V)$.

Proof :

(a) $\Rightarrow$ Immediate from the inclusion $K_C \subset K$. (In this direction the horizontal assumption is unnecessary.)

$\Leftarrow$ If the implication is false there is a collection of horizontal vectors in V which is K_C-(linearly) independent but K-dependent, and from this collection we can choose vectors $v_1, \ldots, v_m$ which are K-dependent with $m > 1$ minimal w.r.t. this property. We can then write $v_m = \sum_{j=1}^{m-1} k_j v_j$, with $k_j \in K$, whereupon applying D and the hypotheses $Dv_j = 0$ results in the identity $0 = \sum^{m-1} k_j' v_j$. By the minimality of m this forces $k_j' = 0,\ j = 1, \ldots, m-1$, i.e., $k_j \in K_C$, and this contradicts linear independence over K_C.

(b) This is immediate from (a) and the fact that any K-linearly independent subset of V can be extended to a basis.

q.e.d.

Suppose $\dim_K V = n < \infty$, $\mathbf{e}$ is a basis of V, and $x' + Ax = 0$ is the defining $\mathbf{e}$-equation of D. Then assertion (c) of the preceding result has the following standard formulation.

Corollary 2.2.7 : *For any matrix $B \in \mathfrak{gl}(n, K)$ a collection of solutions of*

$$x' + Bx = 0 \tag{i}$$

within K^n is linearly independent over K if and only if the collection is linearly independent over K_C. In particular, the K_C-subspace of K^n consisting of solutions of (i) *has dimension at most* $\dim_K V$.

Proof : By Proposition 2.2.3. **q.e.d.**

Equation (i) of Corollary 2.2.7 is always satisfied by the column vector $x = (0, 0, \ldots, 0)^\tau$; this is the *trivial solution*, and any other is *non-trivial*. Unfortunately, non-trivial solutions (with entries in K) need not exist. For example, the linear differential equation $y' - y = 0$ admits only the trivial solution in the field $\mathbb{C}(z)$: for non-trivial solutions one must recast the problem so as to include the extension field $(\mathbb{C}(z))(\exp(z))$.

Corollary 2.2.8 : *For any elements $\ell_1, \ldots, \ell_{n-1} \in K$ a collection of solutions $\{y_j\}_{j=1}^m \subset K$ of*

$$y^{(n)} + \ell_1 y^{(n-1)} + \cdots + \ell_{n-1} y' + \ell_n y = 0 \tag{i}$$

is linearly independent over K_C if and only if the collection $\{(y_j, y_j', \ldots, y_j^{(n-1)}\}_{j=1}^m$ is linearly independent over K. In particular, the K_C-subspace of K consisting of solutions of (i) *has dimension at most n.*

Proof : Use Proposition 2.2.4(b) and Corollary 2.2.7. **q.e.d.**

A non-singular matrix $M \in \mathfrak{gl}(n, K)$ is a *fundamental matrix solution* of

$$x' + Ax = 0, \qquad A \in \mathfrak{gl}(n, K), \tag{2.2.13}$$

if M satisfies this equation, i.e., if

$$M' + AM = 0, \tag{2.2.14}$$

wherein $0 \in \mathfrak{gl}(n, K)$ represents the zero matrix.

Proposition 2.2.9 : *A matrix $M \in \mathfrak{gl}(n, K)$ is a fundamental matrix solution of* (2.2.13) *if and only if the columns of M constitute n solutions of that equation linearly independent over K_C.*

Of course linear independence over K is equivalent to the non-vanishing of the Wronskian $W(y_1, \ldots, y_n)$.

Proof : First note that (2.2.14) holds if and only if the columns of M are solutions of (2.2.13). Next observe that M is non-singular if and only if these columns are linearly independent over K. Finally, note from Propositions 2.2.3(b) and 2.2.6(a) that this will be the case if and only if these columns are linearly independent over K_C. **q.e.d.**

Proposition 2.2.10 : *Suppose $M, N \in \mathfrak{gl}(n, K)$ and M is a fundamental matrix solution of* (2.2.13)*. Then N is a fundamental matrix solution if and only if $N = MC$ for some matrix $C \in \mathfrak{gl}(n, K_C)$.*

Proof :

$\Rightarrow$: By (2.1.4) we have

$$\begin{aligned}(M^{-1}N)' &= M^{-1} \cdot N' + (M^{-1})' \cdot N \\ &= M^{-1} \cdot (-AN) + (-M^{-1}M'M^{-1}) \cdot N \\ &= -M^{-1}AN + (-M^{-1})(-AM)(-M^{-1})N \\ &= -M^{-1}AN + M^{-1}AN \\ &= 0\,.\end{aligned}$$

$\Leftarrow$: We have $N' = (MC)' = M'C = -AM \cdot C = -A \cdot MC = -AN$.

q.e.d.

2.3 Dual Structures and Adjoint Equations

Jerry: This entire section could easily be jettisoned; nothing it contains is essential to what we have discussed. I included it because the adjoint equation would be second nature to the audience I am aiming at, whereas this would not be the case with differential structures, and some justfication of the geometric approach therefore seems warrented. For me the adjoint equation suits this task perfectly, since the differential structure approach seems completely natural. Moreover, the proposition formulations and proofs, although not deep, are original (which is not to be confused with "correct!"), thereby allowing for a fresh ("stale?") treatment of a classical topic. Finally, if we later include other "constructions" of linear differential equations, as in the Tannakian approach, we would certainly need to include this topic.

Differential strutures allow for a simple conceptual formulation of the "adjoint equation" of a linear ordinary differential equation.

In this section V is a vector space of dimension $0 \leq n < \infty$ over a differential field K and $D : V \to V$ is a differential structure. Recall that the dual space V^* of V is defined as the K-space of linear functionals $v^* : V \to K$, and the dual basis $\mathbf{e}^*$ of a basis $\mathbf{e} = \{e_\alpha\}$ of V is the basis $\{e^*_\alpha\}$ of V^* satisfying $e^*_\beta e_\alpha = \delta_{\alpha\beta}$ (where $\delta_{\alpha\beta}$ is the usual Kronecker delta, i.e., $\delta_{\alpha\beta} := 1$ if and only if $\alpha = \beta$; otherwise $\delta_{\alpha\beta} := 0$.).

There is a dual differential structure $D^* : V^* \to V^*$ on the dual space V^* naturally associated with D: the definition is

$$(D^*u^*)v = \delta(u^*v) - u^*(Dv), \qquad u^* \in V^*,\ v \in V. \tag{2.3.1}$$

One often sees u^*v written as $\langle v, u^* \rangle$, and when this notation is used (2.3.1) becomes

$$\delta\langle v, u^* \rangle = \langle Dv, u^* \rangle + \langle v, D^*u^* \rangle. \tag{2.3.2}$$

This is known classically as the *Lagrange identity*; it implies that $u^*v \in K_C$ whenever v and u^* are horizontal.

When $\mathbf{e} \subset V^n$ is a basis and $B \in \mathfrak{gl}(n, K)$ is the defining $\mathbf{e}$-matrix of D one verifies by elementary calculation that the defining $\mathbf{e}^*$-matrix of D^* is $-B^\tau$,

Jerry: we might want to include the calculation.

where $\mathbf{e}^* \subset (V^*)^n$ is the basis dual to $\mathbf{e}$; the defining $\mathbf{e}^*$-equation of D^* is therefore

$$y' - B^\tau y = 0. \tag{2.3.3}$$

This is the *adjoint equation* of (2.2.6). Note from the usual identification $V^{**} \simeq V$ and $-(-B^\tau)^\tau = B$ that (2.2.6) can be viewed as the adjoint equation of

(2.3.3). Intrinsically: the identification $V \simeq V^{**}$ has the consequence $D^{**} := (D^*)^* \simeq D$.

Equations (2.2.6) and (2.3.3) are interchangeable in the sense that information about either one can always be obtained from information about the other.

Proposition 2.3.1 : *Suppose $M \in \mathfrak{gl}(n, K)$. Then M is a fundamental matrix solution of (2.2.6) if and only if $(M^\tau)^{-1}$ is a fundamental matrix solution of (2.3.3).*

Proof : Using (2.1.4), $(M^\tau)^{-1} = (M^{-1})^\tau$ and $(M^\tau)' = (M')^\tau$ we have

$$\begin{array}{rcl} M' + BM = 0 & \Leftrightarrow & (M')^\tau + M^\tau B^\tau = 0 \\ & \Leftrightarrow & -(M^\tau)^{-1}(M')^\tau(M^\tau)^{-1} + (M^\tau)^{-1}M^\tau B^\tau (M^\tau)^{-1} = 0 \\ & \Leftrightarrow & -(M^{-1})^\tau(M')^\tau(M^{-1})^\tau + B^\tau(M^{-1})^\tau = 0 \\ & \Leftrightarrow & -(M^{-1}M'M^{-1})^\tau + B^\tau(M^{-1})^\tau = 0 \\ & \Leftrightarrow & ((M^{-1})')^\tau - B^\tau(M^\tau)^{-1} = 0 \\ & \Leftrightarrow & ((M^\tau)^{-1})' - B^\tau(M^\tau)^{-1} = 0\,. \end{array}$$

q.e.d.

Dual differential structures are extremely useful for solving equations of the form $Du = w$, wherein $w \in V$ is given. The main result in this direction is the following.

Proposition 2.3.2 : *Suppose $(v_m^*)_{j=1}^n$ is a basis of V^* consisting of horizontal vectors and $(v_j)_{j=1}^n$ is the dual basis of $V \simeq V^{**}$. Then the following statements hold.*

(a) *All v_j are horizontal.*

(b) *Suppose $w \in V$ and there are elements $k_j \in K$ such that $k_j' = \langle w, v_j^* \rangle$ for $j = 1, \ldots, n$. Then the vector*

$$u := \sum_j k_j v_j \in V$$

satisfies

$$Du = w\,.$$

Proof :

(a) From $\langle v_i, v_j^* \rangle \in \{0, 1\} \subset K_C$, Lagrange's identity (2.3.2) and the $D^* v_j^* = 0$ hypotheses we have

$$\begin{array}{rcl} 0 & = & \langle v_i, v_j^* \rangle' \\ & = & \langle Dv_i, v_j^* \rangle + \langle v_i, D^* v_j^* \rangle \\ & = & \langle Dv_i, v_j^* \rangle\,, \end{array}$$

and since (v_j^*) is a basis this forces $Dv_i = 0$ for $i = 1, \ldots, n$.

(b) First note that for any $v \in V$ we have

$$v = \sum_j \langle v, v_j^* \rangle v_j \,. \tag{i}$$

Indeed, we can always write v in the form $v = \sum_i c_i v_i$, where $c_i \in K$, and applying v_j^* to this identity then gives $\langle v, v_j^* \rangle = \sum_i c_i \langle v_i, v_j^* \rangle = c_j$.

From (a) and (i) we then have

$$\begin{array}{rcl} Du & = & \sum_j D(k_j v_j) \\ & = & \sum_j (k_j' v_j + k_j D v_j) \\ & = & \sum_j (\langle w, v_j^* \rangle v_j + k_j \cdot 0) \\ & = & \sum_j \langle w, v_j^* \rangle v_j \\ & = & w \,. \end{array}$$

q.e.d.

The following corollary explains the relevance of the adjoint equation for solving inhomogeneous systems. In the statement we adopt more classical notation: when $k, \ell \in K$ satisfy $\ell' = k$ we write ℓ as $\int k$, omit specific reference to ℓ, and simply assert that $\int k \in K$. Moreover, we use the usual inner product $\langle y, z \rangle := \sum_j y_j z_j$ to identify K^n with $(K^n)^*$, i.e., we identify the two spaces by means of the K-isomorphism $v \in K^n \mapsto (w \in K^n \mapsto \langle w, v \rangle \in K) \in (K^n)^*$.

Corollary 2.3.3[4]**:** *Suppose:*

(a) $B \in \mathfrak{gl}(n, K)$*;*

(b) $b \in K^n$*;*

(c) $(z_j)_{j=1}^n$ *is a basis of* K^n *consisting of solutions of the adjoint equation*

$$x' - B^\tau x = 0 \tag{i}$$

of

$$x' + Bx = 0\,; \tag{ii}$$

(d) $\int \langle b, z_j \rangle \in K$ *for* $j = 1, \ldots, n$*; and*

(e) $(y_i)_{i=1}^n$ *is a basis of* K^n *satisfying*

$$\langle y_i, z_j \rangle = \begin{cases} 1 & \text{if } \ i = j \\ 0 & \text{otherwise.} \end{cases} \tag{iii}$$

Then $(y_j)_{j=1}^n$ *is a basis of solutions of the homogeneous equation* (ii) *and the vector*

$$y := \sum_j (\int \langle b, z_j \rangle) \cdot y_j \tag{iv}$$

is a solution of the inhomogeneous system

$$x' + Bx = b\,. \tag{v}$$

The appearance of the integrals in (iv) explains why solutions of (i) are called *integrating factors* of (ii) (and vice-versa, since, as already noted, (i) may be regarded as the adjoint equation of (ii)).

The result is immediate from Proposition 2.3.2. However, it is a simple enough matter to give a direct proof, and we therefore do so.

Proof : Hypothesis (d) identifies $(z_j)_{j=1}^n$ with the dual basis of $(y_i)_{i=1}^n$. In particular, it allows us to view $(z_j)_{j=1}^n$ as a basis of $(K^n)^*$.

To prove that the x_j satisfy (ii) simply note from (iii) and (i) that

$$\begin{aligned} 0 &= \langle y_i, z_j \rangle' \\ &= \langle y_i', z_j \rangle + \langle y_i, z_j' \rangle \\ &= \langle y_i', z_j \rangle + \langle y_i, B^\tau z_j \rangle \\ &= \langle y_i', z_j \rangle + \langle B y_i, z_j \rangle \\ &= \langle y_i' + B y_i, z_j \rangle. \end{aligned}$$

Since $(z_j)_{j=1}^n$ is a basis (of $(K^n)^*$) it follows that

$$y_j' + B y_j = 0\,, \qquad j = 1, \ldots, n. \tag{vi}$$

[4]For a classical account of this result see, e.g., [25, Chapter III, §10, pp. 36-39]. In fact the treatment in this reference was the inspiration for our formulation of this corollary.

Next observe, as in (i) of the proof of Proposition 2.3.2, that for any $b \in K^n$ condition (iii) implies

$$b = \sum_j \langle b, z_j \rangle y_j \,.$$

It then follows from (vi) that

$$\begin{array}{rcl} y' & = & \sum_j \left((\int \langle b, z_j \rangle) \cdot y_j' + \langle b, z_j \rangle y_j \right) \\ & = & \sum_j \left(-(\int \langle b, z_j \rangle) \cdot B y_j + \langle b, z_j \rangle y_j \right) \\ & = & -B \sum_j (\int \langle b, z_j \rangle) \cdot y_j + \sum_j \langle b, z_j \rangle y_j \\ & = & -By + b \,. \end{array}$$

q.e.d.

Corollary 2.3.3 was formulated so as to make the role of the adjoint equation evident. The following alternate formulation is easier to apply in practice.

Corollary 2.3.4 : *Suppose $B \in \mathfrak{gl}(n, K)$ and $M \in \mathrm{Gl}(n, K)$ is a fundamental matrix solution of*

$$x' + Bx = 0. \tag{i}$$

Denote the j^{th}-columns of M and $(M^\tau)^{-1}$ by y_j and z_j respectively, and suppose $b \in K^n$ and $\int \langle b, z_j \rangle \in K$ for $j = 1, \ldots, n$. Then

$$y := \sum_j (\int \langle b, z_j \rangle) \cdot y_j \tag{ii}$$

is a solution of the inhomogeneous system

$$x' + Bx = b \,. \tag{iii}$$

Proof : By Proposition 2.2.9 the z_j form a basis of K^n, and from $(M^\tau)^{-1} = (M^{-1})^\tau$ and $M^{-1}M = I$ we see that

$$\langle y_i, z_j \rangle = \begin{cases} 1 & \text{if } \ i = j \\ 0 & \text{otherwise.} \end{cases}$$

The result is now evident from Corollary 2.3.3. **q.e.d.**

Finally, consider the case of an n^{th}-order linear equation

$$u^{(n)} + \ell_1 u^{(n-1)} + \cdots + \ell_{n-1} u' + \ell_n u = 0 \,. \tag{2.3.4}$$

In this instance the *adjoint equation* generally refers to the n^{th}-order linear equation

$$(-1)^n v^{(n)} + (-1)^{n-1} (\ell_1 v)^{(n-1)} + \cdots + (-1)(\ell_{n-1} v)' + \ell_n v = 0 \,, \tag{2.3.5}$$

e.g., the adjoint equation of

$$u'' + \ell_1 u' + \ell_2 u = 0 \tag{2.3.6}$$

is

$$v'' - \ell_1 v' + (\ell_2 - \ell_1') v = 0 \,. \tag{2.3.7}$$

Examples 2.3.5 :

(a) The adjoint equation of Bessel's equation

$$y'' + \frac{1}{x}\,y' + (1 - \frac{\nu^2}{x^2})\,y = 0$$

is

$$z'' - \frac{1}{x}\,z' + (1 - \frac{\nu^2 - 1}{x^2})\,z = 0\,.$$

(b) The adjoint equation of any second-order equation of the form

$$y'' + \ell_2 y = 0$$

is the identical equation (despite the fact that they describe differential structures on spaces dual to one another).

To understand why the "adjoint" terminology is used with (2.3.5) first convert (2.3.4) to the first order form (2.2.12) and write the corresponding adjoint equation accordingly, i.e., as

$$x' - B^\tau x = 0, \qquad -B^\tau = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -\ell_n \\ 1 & 0 & 0 & & 0 & -\ell_{n-1} \\ 0 & 1 & 0 & & \vdots & \vdots \\ & & \ddots & \ddots & & \\ \vdots & & & 1 & 0 & -\ell_2 \\ 0 & & & 0 & 1 & -\ell_1 \end{pmatrix}. \qquad (2.3.8)$$

The use of the terminology is then explained by the following result.

Proposition 2.3.6 : *A column vector $x = (x_1, \ldots, x_n)^\tau \in K^n$ is a solution of* (2.3.8) *if any only if x_n is a solution of* (2.3.5) *and*

$$x_{n-j} = (-1)^j x_n^{(j)} + \sum_{i=0}^{j-1} (-1)^i (\ell_{j-i} x_n)^{(i)} \qquad \textit{for} \qquad j = 1, \ldots, n-1\,. \quad \text{(i)}$$

Proof :

$\Rightarrow$ If $x = (x_1, \ldots, x_n)^\tau$ satisfies (2.3.8) then

$$x_j' = -x_{j-1} + \ell_{n+1-j} x_n \qquad \text{for} \qquad j = 1, \ldots, n\,, \qquad \text{(ii)}$$

where $x_0 := 0$. It follows that

$$\begin{aligned} x_n' &= -x_{n-1} + \ell_1 x_n, \\ x_n'' &= -x_{n-1}' + (\ell_1 x_n)' \\ &= -(-x_{n-2} + \ell_2 x_n) + (\ell_1 x_n)' \\ &= (-1)^2 x_{n-2} + (-1)\ell_2 x_n + (\ell_1 x_n)', \\ x_n^{(3)} &= (-1)^2 x_{n-2}' + (-1)(\ell_2 x_n)' + (\ell_1 x_n)'' \\ &= (-1)^2(-x_{n-3} + \ell_3 x_n) + (-1)(\ell_2 x_n)' + (\ell_1 x_n)'' \\ &= (-1)^3 x_{n-3} + (-1)^2 \ell_3 x_n + (-1)(\ell_2 x_n)' + (\ell_1 x_n)'', \end{aligned}$$

and by induction (on j) that

$$x_n^{(j)} = (-1)^j x_{n-j} + \sum_{i=0}^{j-1} (-1)^{j-1-i} (\ell_{j-i} x_n)^{(i)}\,, \qquad j = 1, \ldots, n\,.$$

This is equivalent to (i), and equation (2.3.5) amounts to the case $j = n$.

$\Leftarrow$ Conversely, suppose x_n is a solution of (2.3.5) and that (i) holds. We must show that (iii) holds or, equivalently, that

$$x_{n-j}' = -x_{n-(j+1)} + \ell_{j+1} x_n \qquad \text{for} \qquad j = 1, \ldots, n.$$

This, however, is immediate from (i). Indeed, we have

$$\begin{aligned} x_{n-j}' &= (-1)^j x_n^{(j+1)} + \textstyle\sum_{i=0}^{j-1} (-1)^i (\ell_{j-i} x_n)^{i+1} \\ &= (-1)^j x_n^{(j+1)} + \textstyle\sum_{i=1}^{j} (-1)^{i+1} (\ell_{j+1-i} x_n)^{(i)} \\ &= (-1)^j x_n^{(j+1)} + \textstyle\sum_{i=0}^{j} (-1)^{i+1} (\ell_{j+1-i} x_n)^{(i)} + \ell_{j+1} x_n \\ &= -\left((-1)^{j+1} x_n^{(j+1)} + \textstyle\sum_{i=0}^{j} (\ell_{j+1-i} x_n)^{(i)} \right) + \ell_{j+1} x_n \\ &= -x_{n-(j+1)} + \ell_{j+1} x_n\,. \end{aligned}$$

q.e.d.

For completeness we record the n^{th}-order formulation of Corollary 2.3.4.

Proposition 2.3.7 ("Variation of Constants") : *Suppose $\ell_1, \ldots, \ell_n \in K$ and $\{y_1, \ldots, y_n\} \subset K^n$ is a collection of solutions of the n^{th}-order equation*

$$u^{(n)} + \ell_1 u^{(n-1)} + \cdots + \ell_{n-1} u' + \ell_n u = 0 \tag{i}$$

linearly independent over K_C. Let

$$M := \begin{pmatrix} y_1 & y_2 & \cdots & & y_n \\ y_1' & y_2' & & \vdots & y_n' \\ y_1^{(2)} & y_2^{(2)} & & & \vdots \\ \vdots & & & & \\ y_1^{(n-1)} & y_2^{(n-1)} & \cdots & \cdots & y_n^{(n-1)} \end{pmatrix}$$

and let $(z_1, \ldots, z_n)$ *denote the* n^{th}*-row of the matrix* $(M^\tau)^{-1}$*. Suppose* $k \in K$ *is such that* $\int kz_j \in K$ *for* $j = 1, \ldots, n$*. Then*

$$y := \sum_j (\int kz_j) \cdot y_j \tag{ii}$$

is a solution of the inhomogeneous equation

$$u^{(n)} + \ell_1 u^{(n-1)} + \cdots + \ell_{n-1} u' + \ell_n u = k\,. \tag{iii}$$

Proof : Convert (i) to a first-order system as in (2.2.12) and note from Propositions 2.1.1 and 2.2.4 that M is a fundamental matrix solution. Denote the j^{th}-column of M by $\hat{y}_j$ and apply Corollary 2.3.4 with $b = (0, \ldots, 0, k)^\tau$ and y_j (in that statement) replaced by $\hat{y}_j$ so as to achieve

$$\hat{y}' + B\hat{y} = b.$$

Now write $\hat{y} = (y, \hat{y}_2, \ldots, \hat{y}_n)^\tau$ and eliminate $\hat{y}_2, \ldots, \hat{y}_n$ in the final row of (iii) by expressing these entities in terms of y and derivatives thereof: the result is (iii).

q.e.d.

Since our formulation of Proposition 2.3.7 is not quite standard[5], a simple example seems warranted.

Example 2.3.8 : For $K = \mathbb{C}(x)$ with derivation $\frac{d}{dx}$ we consider the inhomogeneous second-order equation

$$u'' + \frac{2}{x}\,u' - \frac{6}{x^2}\,u = x^3 + 4x\,, \tag{i}$$

and for the associated homogeneous equation

$$u'' + \frac{2}{x}\,u' - \frac{6}{x^2}\,u = 0$$

take $y_1 = x^2$ and $y_2 = 1/x^3$ so as to satisfy the hypothesis of Proposition 2.3.7. In the notation of that proposition we have

$$M = \begin{pmatrix} x^2 & \frac{1}{x^3} \\ 2x & -\frac{3}{x^4} \end{pmatrix}, \qquad (M^\tau)^{-1} = \begin{pmatrix} \frac{3}{5x^2} & \frac{2x^3}{5} \\ \frac{1}{5x} & -\frac{x^4}{5} \end{pmatrix},$$

and from the second matrix we see that $z_1 = 1/5x$, $z_2 = -x^4/5$. A solution to (i) is therefore given by

$$\begin{aligned} y &= \left(\int \tfrac{1}{5x} \cdot (x^3 + 4x)\right) \cdot x^2 + \left((-1) \int \tfrac{x^4}{5} \cdot (x^3 + 4x)\right) \cdot \frac{1}{x^3} \\ &= \frac{x^5}{24} + \frac{2x^3}{3}\,, \end{aligned}$$

as is easily checked directly.

[5] Cf. [7, Chapter 3, §6, Theorem 6.4, p. 87].

2.4 Extensions of Differential Structures

Consider the second-order linear differential equation

$$y'' + y = 0, \qquad ' := \tfrac{d}{dx}. \tag{2.4.1}$$

One can take the "general solution" to be either $y = c_1 \sin x + c_2 \cos x,\ c_1, c_2 \in \mathbb{R}$, or $y = c_1 e^{ix} + c_2 e^{-ix},\ c_1, c_2 \in \mathbb{C}$, i.e., one can use either $\{\sin x, \cos x\}$ or $\{e^{ix}, e^{-ix}\}$ as a basis of solutions. In terms of differential structures the latter viewpoint results from the former by "extending the base (field)." This is most easily explained in terms of tensor products. Since knowledge of these entities is not assumed on the part of readers, and since they play such a dominant role in the following chapters, we begin with the basic definitions.

For the remainder of the section R denotes a commutative ring, $p \geq 1$ is an integer, and $M_1, M_2, \ldots, M_p$ and N are (left) R-modules.

A mapping $\beta : \times_j M_j := M_1 \times \cdots \times M_p \to N$ is *p-linear* if for each $(m_1, \ldots, m_p) \in \times_j M_j$ and each $1 \leq j \leq p$ the mapping from M_j into N defined by $m \in M_j \mapsto \beta(m_1, \ldots, m_{j-1}, m, m_{j+1}, \ldots, m_p) \in N$ is R-linear. When $p = 2$ or 3 one speaks of a *bilinear* or *trilinear mapping*, and when reference to R is needed one speaks of a *p-linear mapping over R* or, in the cases $p = 2$ and $p = 3$, of an *R-bilinear* or *R-trilinear mapping*. Example: the usual inner product $(v, w) \in \mathbb{R}^n \times \mathbb{R}^n \mapsto \langle v, w \rangle \in \mathbb{R}$ and the usual cross (or "vector") product $(u, v) \in \mathbb{R}^3 \times \mathbb{R}^3 \mapsto u \times v \in \mathbb{R}^3$ are bilinear; the usual "triple (scalar) product" $(u, v, w) \in \mathbb{R}^3 \times \mathbb{R}^3 \times \mathbb{R}^3 \mapsto \langle u, v \times w \rangle \in \mathbb{R}$ is trilinear.

Of course the zero mapping $(m_1, m_2, \ldots, m_p) \in \times_j M_j \mapsto 0 \in N$ is p-linear. This is the *trivial p-linear mapping* (into N); any other is *non-trivial*. The following result gives a sufficient condition for the existence of non-trivial p-linear mappings.

Proposition 2.4.1 : *Suppose $M_1, M_2, \ldots, M_p$ are free with bases $B_j \subset M_j,\ j = 1, 2, \ldots, p$. Then for any element $b = (b_1, b_2, \ldots, b_p) \in B := \times_j B_j \subset \times_j M_j$ there is a p-linear mapping $\beta : \times_j M_j \to R$ such that $\beta(b) \neq 0$ and $\beta(\hat{b}) = 0$ for $\hat{b} \in B \setminus \{b\}$.*

The hypotheses hold, in particular, when R is a field. Of course in that context the M_j would more likely be described as vector spaces over R.

Proof : By freeness we can choose an R-linear mapping $g_j : M_j \to R$ such that $g_j(b_j) \neq 0$ and $g_j(\hat{b}) = 0$ for $\hat{b} \in B_j \setminus \{b_j\}$. The p-linear mapping $\beta : (m_1, m_2, \ldots, m_p) \mapsto \prod_j g_j(m)$ has the asserted properties. **q.e.d.**

A *tensor product* (*over R*) for the R-modules $M_1, \ldots, M_p$ consists of an R-module T together with a p-linear mapping $\alpha : \times_j M_j \to T$ having the following "universal" property: to any p-linear mapping $\beta : \times_j M_j \to N$ into any R-module N there corresponds a unique R-linear mapping $f_\beta : T \to N$ for which

the diagram

$$\begin{array}{ccc} \times_j M_j & \xrightarrow{\alpha} & T \\ & \overset{\beta}{\searrow} & \downarrow f_\beta \\ & & N \end{array} \tag{2.4.2}$$

is commutative. One sees easily from uniqueness that the correspondence $\beta \mapsto f_\beta$ between p-linear mappings from $\times_j M_j$ into N and R-linear mappings from T into N is bijective: a tensor product reduces the study of p-linear mappings to that of R-linear mappings.

Examples 2.4.2 :

(a) Let $n \geq 1$ be an integer and regard $\mathbb{R}^n$ as a subset of $\mathbb{C}^n$ by means of the mapping $(r_1, r_2, \ldots, r_n) \in \mathbb{R}^n \mapsto (r_1, r_2, \ldots, r_n) \in \mathbb{C}^n$. Moreover, regard $\mathbb{C}$ and $\mathbb{C}^n$ as real vector spaces by restricting scalar multiplication to real numbers. *We claim that the real bilinear mapping* $\alpha : (c, (r_1, r_2, \ldots, r_n)) \in \mathbb{C}\times\mathbb{R}^n \mapsto (cr_1, cr_2, \ldots, cr_n) \in \mathbb{C}^n$ *is a tensor product for the real vector spaces* $\mathbb{C}$ *and* $\mathbb{R}^n$.

To prove this let $\mathbf{e} := (e_j)_{j=1}^n$ denote the usual (or "standard") basis of $\mathbb{R}^n$, i.e., let $e_j := (0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbb{R}^n$ for $j = 1, 2, \ldots, n$ (the 1 being in slot j). As a basis for the real vector space $\mathbb{C}^n$ choose $(e_1, e_2, \ldots, e_n, ie_1, ie_2, \ldots, ie_n)$. Given a real bilinear mapping $\beta : \mathbb{C}\times\mathbb{R}^n \to N$ into a real vector space N we can (because vector spaces are free on their bases) specify a unique real linear mapping $f_\beta : \mathbb{C}^n \to N$ by means of the assignments

$$f_\beta e_j := \beta(1, e_j) \qquad \text{and} \qquad f_\beta(ie_j) := \beta(i, e_j), \qquad j = 1, \ldots, n. \tag{i}$$

We claim that $f_\beta \circ \alpha = \beta$, i.e., that the relevant diagram commutes. To verify this first note that for $a + ib \in \mathbb{C}$ and $(r_1, r_2, \ldots, r_n) \in \mathbb{R}^n$ we have

$$\begin{aligned} \alpha(a + ib, (r_1, r_2, \ldots, r_n)) &:= ((a + ib)r_1, (a + ib)r_2, \ldots, (a + ib)r_n) \\ &= (ar_1 + ibr_1, ar_2 + ibr_2, \ldots, ar_n + ibr_n) \\ &= \textstyle\sum_j (ar_j e_j + br_j ie_j), \end{aligned}$$

and as a result we see that

$$\begin{aligned} (f_\beta \circ \alpha)(a + ib, (r_1, r_2, \ldots, r_n)) &= f_\beta(\textstyle\sum_j (ar_j e_j + br_j ie_j)) \\ &= \textstyle\sum_j ar_j f_\beta e_j + \sum_j br_j f_\beta ie_j \\ &= \textstyle\sum_j ar_j \beta(1, e_j) + \sum_j br_j \beta(i, e_j) \\ &= \textstyle\sum_j \beta(ar_j + ibr_j, e_j) \\ &= \textstyle\sum_j \beta(a + ib, r_j e_j) \\ &= \beta(a + ib, \textstyle\sum_j r_j e_j) \\ &= \beta(a + ib, (r_1, r_2, \ldots, r_n)). \end{aligned}$$

Commutativity is thereby established.

As for uniqueness, suppose $g : \mathbb{C}^n \to N$ is a real linear mapping such that $g \circ \alpha = \beta$. Then for $j = 1, 2, \ldots, n$ we have

$$\beta(1, e_j) = g(\alpha(1, e_j)) = Te_j$$

as well as

$$\beta(i, e_j) = g(\alpha(i, e_j)) = Tie_j,$$

and $g = f_\beta$ is then evident from (i) (and the discussion leading to those formulas).

(b) *Whenever $S \supset R$ is an extension of rings the R-bilinear mapping $\alpha : (r, s) \in R \times S \mapsto rs \in S$ is a tensor product for the R-modules S and R.* Indeed, given an R-bilinear mapping $\beta : R \times S \to N$ into an R-module N define an R-linear mapping $f_\beta : S \to N$ by $f_\beta(s) := \beta(1, s)$. For $(r, s) \in R \times S$ one has $\alpha(r, s) = r\alpha(1, s) = \alpha(1, rs)$, and from

$$\begin{array}{rcl} (f_\beta \circ \alpha)(r, s) & = & f_\beta(\alpha(r, s)) \\ & = & f_\beta(\alpha(1, rs)) \\ & = & f_\beta(rs) \\ & = & \beta(1, rs) \\ & = & \beta(r, s) \end{array}$$

that the relevant diagram is commutative. If $g : S \to N$ is an R-linear mapping such that $g \circ \alpha = \beta$ then for $s \in S$ we have

$$g(s) = g(\alpha(1, s)) = (g \circ \alpha)(1, s) = \beta(1, s) = f_\beta(s),$$

and uniqueness follows.

(c) *Suppose $\alpha : \times_j M_j \to T$ is a tensor product for R-modules $M_1, M_2, \ldots, M_p$ and $g : T \to U$ is an R-module isomorphism. Then $g \circ \alpha : \times_j M_j \to U$ is also a tensor product for these modules.* When $\beta : \times_j M_j \to N$ is p-linear one checks easily that the composition $f_\beta \circ g^{-1} : U \to N$ is the unique R-linear mapping satisfying $\beta = (f_\beta \circ g^{-1}) \circ (g \circ \alpha)$.

The uniqueness argument of Example 2.4.2(a) generalizes as follows.

Proposition 2.4.3 : *Suppose R is a commutative ring, M and N are R-modules, X is a set, and $g : X \to M$ and $h : X \to N$ are set mappings such that $g(X)$ generates M. Then there is at most one R-linear mapping $f : M \to N$ which renders the diagram*

$$\begin{array}{ccc} X & \xrightarrow{g} & M \\ & \overset{h}{\searrow} & \downarrow f \\ & & N \end{array}$$

commutative.

An important special case occurs when $X \subset M$ and X generates M: take g to be inclusion.

Proof : By assumption any $m \in M$ may be written (not necessarily uniquely) as a finite sum $m = \sum r_j g(x_j)$ with $r_j \in R$ and $x_j \in X$. If $\hat{f} : M \to N$ is any R-linear mapping rendering the diagram commutative we have

$$\begin{aligned} \hat{f}(m) &= \hat{f}(\textstyle\sum_j r_j g(x_j)) \\ &= \textstyle\sum_j \hat{f}(g(x_j)) \\ &= \textstyle\sum_j (\hat{f} \circ g)(x_j) \\ &= \textstyle\sum_j h(x_j). \end{aligned}$$

Since the final expression is independent of $\hat{f}$, uniqueness follows. **q.e.d.**

Suppose $\alpha : \times M_j \to T$ and $\gamma : \times M_j \to U$ are tensor products for the R-modules $M_1, M_2, \ldots, M_p$. Then there must be unique R-linear mappings $f_\gamma : T \to U$ and $f_\alpha : U \to T$ which make the diagram

$$\begin{array}{ccccc} T & \xrightarrow{f_\gamma} & U & \xrightarrow{f_\alpha} & T \\ & {\scriptstyle\alpha}\nwarrow & \uparrow{\scriptstyle\gamma} & \nearrow{\scriptstyle\alpha} & \\ & & \times_j M_j & & \end{array} \tag{2.4.3}$$

commute, and since the triangle formed by the outer boundary also commutes when the top composition is replaced by id_T it follows from uniqueness that $f_\alpha \circ f_\gamma = \mathrm{id}_T$. A similar argument gives $f_\gamma \circ f_\alpha = \mathrm{id}_U$, and we conclude that f_α and f_γ are R-linear isomorphisms. This establishes the following result, which is often summarized by the (under)statement: *tensor products are unique up to isomorphism.*

Proposition 2.4.4 : *Suppose $\alpha : \times_j M_j \to T$ and $\gamma : \times_j M_j \to U$ are tensor products for $M_1, M_2, \ldots, M_p$. Then there is a unique R-module isomorphism $f_\gamma : T \to U$ making the diagram*

$$\begin{array}{ccc} T & \xrightarrow{f_\gamma} & U \\ & {\scriptstyle\alpha}\nwarrow \quad \nearrow{\scriptstyle\gamma} & \\ & \times_j M_j & \end{array}$$

commute.

One can always construct a tensor product for $M_1, M_2, \ldots, M_p$ as follows: form the free R-module M generated by the Cartesian product $\times_j M_j$; factor

out the R-submodule $\hat{M}$ generated by elements of the form

$$\begin{gathered}(m_1,\dots,m_{k-1},m_k+\hat{m}_k,m_{k+1},\dots,m_p)-(m_1,\dots,m_{k-1},m_k,m_{k+1},\dots,m_p)\\ -(m_1,\dots,m_{k-1},\hat{m}_k,m_{k+1},\dots,m_p)\ \text{ and}\\ (m_1,\dots,m_{k-1},rm_k,m_{k+1},\dots,m_p)-r(m_1,\dots,m_p),\end{gathered}\tag{2.4.4}$$

wherein r varies through R. This quotient is denoted $M_1\otimes_R M_2\otimes_R\cdots\otimes_R M_p$ or $\bigotimes_j M_j$, and the subscript R is dropped when the ring is clear from context. The coset in $\bigotimes_j M_j$ of an element $(m_1,m_2,\dots,m_p)\in M$ is denoted $m_1\otimes m_2\otimes\cdots\otimes m_p$ and is called the *tensor product* of $m_1,m_2,\dots,m_p$. In particular, a typical element of $\bigotimes_j M_j$ can be expressed (although not uniquely) as a finite sum $\sum_j r_j m_{1j}\otimes m_{2j}\otimes\cdots\otimes m_{pj}$ with $r_j\in R$. By composing the inclusion mapping $\times_j M_j\hookrightarrow M$ with the canonical homomorphism $M\to M/\hat{M}$ one defines a p-linear mapping $\alpha:\times_j M_j\to M/\hat{M}$ over R satisfying

$$\alpha:(m_1,m_2,\dots,m_p)\in\times_j M_j\mapsto m_1\otimes m_2\otimes\cdots\otimes m_p\in\bigotimes_j M_j.\tag{2.4.5}$$

Jerry: I cannot get the "times" in the above formula into boldmath. In fact I have huge problems with boldmath.

Proposition 2.4.5 : *The p-linear mapping* $\alpha : \times_j M_j \to \bigotimes_j M_j$ *defined in* (2.4.5) *is a tensor product for* $M_1, M_2, \ldots, M_p$.

It is customary to refer to $\alpha : \times_j M_j \to \bigotimes_j M_j$, and on occasion to the R-module $\times_j M_j$ alone, as "the" tensor product of $M_1, M_2, \ldots, M_p$. Indeed, any other tensor product must be isomorphic in the sense of Proposition 2.4.4.

Proof : Suppose $\beta : \times_j M_j \to N$ is a p-linear mapping into an R-module N and let M and $\hat{M}$ be as in the previous paragraph. Since M is free there is a unique R-linear mapping $\theta : M \to N$ which makes the diagram

$$\begin{array}{ccc} & & M \\ & \overset{\text{inc}}{\nearrow} & \\ \times_j M_j & & \downarrow \theta \\ & \underset{\beta}{\searrow} & \\ & & N \end{array}$$

commute. From the fact that β is p-linear we see from (2.4.4) that $\hat{M} \subset \ker \theta$, and as a result the mapping θ induces an R-linear mapping $f_\beta : \bigotimes M_j \to N$ which renders the next diagram commutative:

$$\begin{array}{ccc} & & \bigotimes_j M_j \\ & \overset{\alpha}{\nearrow} & \\ \times M_j & & \downarrow f_\beta \\ & \underset{\beta}{\searrow} & \\ & & N. \end{array}$$

For uniqueness recall Proposition 2.4.3. **q.e.d.**

Examples 2.4.6 :

(a) *For any* $n \geq 1$ *the real vector spaces* $\mathbb{C}^n$ *and* $\mathbb{C} \otimes_R \mathbb{R}^n$ *are isomorphic.* Indeed, both spaces arise as tensor products of the real vectors spaces $\mathbb{C}$ and $\mathbb{R}^n$ (recall Example 2.4.2(a)).

(b) *For any ring extension* $S \supset R$ *there is an isomorphism* $R \otimes_R S \simeq S$ *characterized by* $r \otimes s \mapsto rs$, $(r, s) \in R \times S$. Here recall Example 2.4.2(b).

(c) *For relatively prime positive integers* m *and* n *one has* $(\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z}) = 0$. (Tensoring over $\mathbb{Z}$ makes sense since any commutative ring may be considered a $\mathbb{Z}$-module.) Indeed, by assumption there are integers a, b such

that $am + bn = 1$, and for $[p] \in \mathbb{Z}/m\mathbb{Z}$ and $[q] \in \mathbb{Z}/n\mathbb{Z}$ the $\mathbb{Z}$-bilinearity gives

$$\begin{aligned} [p] \otimes [q] &= 1 \cdot ([p] \otimes [q]) \\ &= (am + bn) \cdot ([p] \otimes [q]) \\ &= a \cdot ([mp] \otimes [q]) + b \cdot ([p] \otimes [nq]) \\ &= a \cdot (0 \otimes [q]) + b \cdot ([p] \otimes 0) \\ &= 0. \end{aligned}$$

The example shows that tensoring can involve collapsing, i.e., that the tensor product of R-modules need not be "bigger" than any or all of the given modules.

Let $N_1, N_2, \ldots, N_p$ be R-modules, let $\alpha : \times_j M_j \to \bigotimes_j M_j$ denote the tensor product, and let $T_j : M_j \to N_j$ be R-linear mappings, $j = 1, 2, \ldots, p$. Then the mapping $\beta : \times_j M_j \to N$ defined by

$$\beta : (m_1, m_2, \ldots, m_p) \mapsto T_1 m_1 \otimes T_2 m_2 \otimes \cdots \otimes T_p m_p \in \bigotimes_j N_j \tag{2.4.6}$$

is p-linear, and as a result there must be a unique R-linear mapping from $\bigotimes_j M_j$ into $\bigotimes_j N_j$, denoted $T_1 \otimes T_2 \otimes \cdots \otimes T_p$, which renders the diagram

$$\begin{array}{ccc} \times_j M_j & \xrightarrow{\alpha} & \bigotimes_j M_j \\ & \overset{\beta}{\searrow} & \downarrow {\scriptstyle T_1 \otimes T_2 \otimes \cdots \otimes T_p} \\ & & \bigotimes_j N_j \end{array} \tag{2.4.7}$$

commutative. In particular, for all $m_1 \otimes m_2 \otimes \cdots \otimes m_p \in M_1 \otimes M_2 \otimes \cdots \otimes M_p$ one has

$$(T_1 \otimes T_2 \otimes \cdots \otimes T_p)(m_1 \otimes m_2 \otimes \cdots \otimes m_p) = T_1 m_1 \otimes T_2 m_2 \otimes \cdots \otimes T_p m_p. \tag{2.4.8}$$

The R-linear mapping $T_1 \otimes T_2 \otimes \cdots \otimes T_p$ is called the *tensor product* of the mappings $T_1, T_2, \ldots, T_p$. An important application of this construction occurs in the proof of the following result.

Proposition 2.4.7 : *Suppose $R \subset S$ is an extension of rings and M is an R-module. Then $S \otimes_R M$ can be given the structure of an S-module with scalar multiplication satisfying*

$$s \cdot (t \otimes m) = st \otimes m, \qquad s, t \in S, \qquad m \in M, \tag{i}$$

and this structure is uniquely determined by (i).

Unless specifically stated to the contrary, this S-module structure on $S \otimes_R M$ will always be assumed. In the special case $\mathbb{R} \subset \mathbb{C}$ of a ring extension one generally refers to $\mathbb{C} \otimes_R M$ as the *complexification* of M.

Proof : For each $s \in S$ define an R-linear mapping $\mu_s : S \to S$ by $t \mapsto st$. Then the tensor product $\mu_s \otimes \mathrm{id}_M : S \otimes_R M \to S \otimes_R M$ satisfies $t \otimes m \mapsto st \otimes m$, and is the unique such R-linear mapping. This defines "left multiplication by s," and the required properties of an S-module can now be verified by straightforward calculation, e.g., for $s_1, s_2, t \in S$ and $m \in M$ we see from

$$\begin{aligned}(s_1 + s_2) \cdot (t \otimes m) &= (s_1 + s_2)t \otimes m \\ &= (s_1 t + s_2 t) \otimes m \\ &= s_1 t \otimes m + s_2 t \otimes m \\ &= s_1 \cdot (t \otimes m) + s_2 \cdot (t \otimes m)\end{aligned}$$

that $(s_1 + s_2) \cdot m = s_1 \cdot m + s_2 \cdot m$ for any $m \in M$. **q.e.d.**

Of course the S-module $S \otimes_R M$ of Proposition 2.4.7 is also an R-module, with scalar multiplication as in (i), but with s now restricted to R. When the mapping $m \in M \mapsto 1 \otimes m \in S \otimes_R M$ is an embedding one views M as an R-submodule of $S \otimes_R M$, and speaks of the latter as being obtained from M by "extending the base (ring of scalars)." Indeed, this terminology is used even when $m \mapsto 1 \otimes m$ is not an embedding.

This raises the question: when is $m \mapsto 1 \otimes m$ an embedding? The following sufficient condition will serve our purposes.

Proposition 2.4.8 : *Suppose M is a free R-module with basis B and $S \supset R$ is a ring extension. Then:*

(a) *the mapping $m \in M \mapsto 1 \otimes m \in S \otimes_R M$ is an embedding;*

(b) *the collection $\{\, 1 \otimes b_\gamma \,:\, b_\gamma \in B \,\}$ is a basis for the S-module $S \otimes_R M$; and*

(c) *when B is finite one has*

$$\dim_R M = \dim_S (S \otimes_R M). \tag{i}$$

In particular, when M is free, e.g., when R is a field, we can view M as an R-submodule of $S \otimes_R M$ by identifying M with $\{1 \otimes m : m \in M\} \subset S \otimes_R M$. In practice this is done quite informally, e.g., when $m \in M$ one is apt to write $1 \otimes m \in S \otimes_R M$ as $m \in S \otimes_R M$, and we will follow such customs.

Proof :

(a) Pick $0 \neq m \in M$ and express m as a finite sum $m = \sum_j r_j b_j$ with $b_j \in B$, $j = 1, 2, \ldots, n$. Fix $1 \leq i \leq n$ and let $f_i : M \to R$ be the R-linear mapping characterized by $f_i(b_j) = 0$ if $i = j$; $f_i(b_j) = 0$ otherwise. Then $\mathrm{id}_S \otimes f_i : S \otimes_R M \to S \otimes_R R$ satisfies $(\mathrm{id}_S \otimes f_i)(1 \otimes m) = r_i$, and we conclude that $1 \otimes m = 0$ if and only if $r_j = 0$ for all j. Assertion (a) follows.

(b) Any vector $v \in S \otimes_R M$ can be written as a finite sum $v = \sum_j s_j \otimes m_j$, and there is a finite subset $\{b_1, b_2, \ldots, b_r\} \subset B$ such that each m_j has the form

$b_j = \sum_{i=1}^{r} r_{ij} b_i$ with each $r_{ij} \in R$. We can then write $m = \sum_j s_j \otimes (\sum_i r_{ij} b_i)$, and from $s_j \otimes r_{ij} b_i = r_{ij} s_j (1 \otimes b_i)$ we conclude that $\{1 \otimes b_\gamma\}$ spans $S \otimes_R M$.

To establish linear independence suppose in $S \otimes_R M$ we can express 0 as a finite sum $\sum_{j=1}^{n} s_j (1 \otimes b_j) = \sum_j s_j \otimes b_j$ with $s_j \in S$ and $b_j \in B$. Fix $1 \leq i \leq n$ and let $f_i : M \to R \subset S$ be the R-linear mapping characterized by $f(b_i) = 0$ and $f(b) = 0$ for all $b \in B \smallsetminus \{b_i\}$. Then the R-bilinear mapping $\beta : (s, m) \in S \times M \mapsto s f(m) \in S$ induces an R-linear mapping $f_\beta : S \otimes_R M \to S$ characterized by $s \otimes m \mapsto s f_i(m)$, hence $0 = f_i(0) = f_i(\sum_j s_j \otimes b_j) = \sum_j f_i(s_j \otimes b_j) = \sum_j s_j f_i(b_j) = s_i$, and linear independence follows.

(c) Immediate from (b).

q.e.d.

We are now in a position to apply the tensor product idea to differential structures.

Proposition 2.4.9 : *To any differential field extension $L \supset K$ there corresponds a unique differential structure $D_L : L \otimes_K V \to L \otimes_K V$ extending $D : V \to V$, and this structure is characterized by the property*

$$D_L(\ell \otimes_K V) = \ell' \otimes_K v + \ell \otimes_K Dv, \qquad \ell \otimes_K v \in L \otimes_K V. \tag{i}$$

In accordance with Proposition 2.4.8 we are here viewing V as a K-subspace of $L \otimes_K V$ by identifying V with its image under the embedding $v \mapsto 1 \otimes_K v$. Assuming (i) we have $D_L(1 \otimes_K v) = 1 \otimes_K Dv \simeq Dv$ for any $v \in V$, and this is the meaning of D_L "extending" D.

One is tempted to prove the proposition by constructing mappings $\delta \otimes_K \mathrm{id}_V : L \otimes_K V \to L \otimes_K V$ and $\mathrm{id}_L \otimes_K D : L \otimes_K V \to L \otimes_K V$ by appealing to the discussion surrounding (2.4.7), and to then define $D_L := \delta \otimes_K \mathrm{id}_V + \mathrm{id}_L \otimes_K D$. Unfortunately, that discussion does not apply: D is not K-linear when the subfield $K_C \subset K$ is proper. One way around the problem is to first work over K_C, and then pass to a quotient.

In the proof we denote the derivation $\ell \mapsto \ell'$ by $\delta : L \to L$, and we also write the restriction $\delta|_K$ as δ.

Proof : Begin by viewing L and V as K_C spaces and note from the Leibniz rule (2.2.1) that D is K_C-linear. A K_C-linear mapping $\hat{D} : L \otimes_{K_C} V \to L \otimes_{K_C} V$ is therefore defined by

$$\hat{D} := \delta \otimes_{K_C} \mathrm{id}_V + \mathrm{id}_{K_C} \otimes_{K_C} D\,. \tag{ii}$$

(Recall the discussion surrounding (2.4.7).) Now define $Y \subset L \otimes_{K_C} V$ to be the K_C-subspace generated by all vectors of the form $\ell k \otimes_{K_C} v - \ell \otimes_{K_C} kv$, where

$\ell \in L,\ k \in K$ and $v \in V$. Then from the calculation

$$\begin{aligned}\hat{D}(\ell k \otimes_{K_C} v - \ell \otimes_{K_C} kv) &= \delta(\ell k) \otimes_{K_C} v + \ell k \otimes_{K_C} Dv \\ &\quad - \delta(\ell) \otimes_{K_C} kv - \ell \otimes_{K_C} D(kv) \\ &= \ell k' \otimes_{K_C} v + k\ell' \otimes_{K_C} v + \ell k \otimes_{K_C} Dv \\ &\quad - \ell' \otimes_{K_C} kv - \ell \otimes_{K_C} (k'v + kDv) \\ &= \ell k' \otimes_{K_C} v - \ell \otimes_{K_C} k'v \\ &\quad + \ell' k \otimes_{K_C} v - \ell \otimes_{K_C} k'v \\ &\quad + \ell k \otimes_{K_C} Dv - \ell \otimes_{K_C} kDv\end{aligned}$$

we see that Y is $\hat{D}$-invariant, and $\hat{D}$ therefore induces a K_C-linear mapping $\tilde{D} : (L \otimes_{K_C} V)/Y \to (L \otimes_{K_C} V)/Y$ which by (ii) satisfies

$$\tilde{D}([\ell \otimes_{K_C} v]) = [\ell' \otimes_{K_C} v] + [\ell \otimes_{K_C} Dv], \tag{iii}$$

where the bracket [ ] denotes the equivalence class (i.e., coset) of the accompanying element.

Now observe that when $L \otimes_{K_C} V$ is viewed as an L-space (*resp.* K-space), Y becomes an L-subspace (*resp.* a K-subspace), and it follows from (iii) that $\tilde{D}$ is a differential structure when the L-space (*resp.* K-space) structure is assumed.

In view of the K-space structure on $(L \otimes_{K_C} V)/Y$ the K-bilinear mapping[6] $(\ell, v) \mapsto [\ell \otimes_{K_C} v]$ induces a K-linear mapping $T : L \otimes_K V \to (L \otimes_{K_C} V)/Y$ which one verifies to be K-isomorphism. It then follows from (iii) and (iv) that the mapping $D_L := T^{-1} \circ \tilde{D} \circ T : L \otimes_K V \to L \otimes_K V$ satisfies (i), allowing us to conclude that D_L is a differential structure on the L-space $L \otimes_K V$.

As for uniqueness, suppose $\check{D} : L \otimes_K V \to L \otimes_K V$ is any differential structure extending D, i.e., having the property

$$\check{D}(1 \otimes_K v) = 1 \otimes_K Dv, \qquad v \in V\,.$$

Then for any $\ell \otimes_K v \in L \otimes_K V$ one has

$$\begin{aligned}\check{D}(\ell \otimes_K v) &= \check{D}(\ell \cdot (1 \otimes_K v)) \\ &= \ell' \cdot (1 \otimes_K v) + \ell \cdot \check{D}(1 \otimes_K v) \\ &= \ell' \otimes_K v + \ell \cdot (1 \otimes_K Dv) \\ &= \ell' \otimes_K v + \ell \otimes_K Dv \\ &= D_L(\ell \otimes_K v),\end{aligned}$$

hence $\check{D} = D_L$. **q.e.d.**

Proposition 2.4.10 : *Suppose* **e** *is a basis of* V *and*

$$x' + Bx = 0 \tag{i}$$

is the defining **e***-equation for* D*. Let* $L \supset K$ *be a differential field extension and consider* **e** *as a basis for the* L*-space* $L \otimes_K V$*. Then the defining* **e***-equation for the extended differential structure* $D_L : L \otimes_K V \to L \otimes_K V$ *is also* (i)*.*

[6] Which we note is <u>not</u> L-bilinear, since for $v \in V$ the product ℓv is only defined when $\ell \in K$.

In particular, $y'' + y = 0$, when expressed in the first-order form

$$x' + \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} x, \qquad x := \begin{pmatrix} y \\ y' \end{pmatrix},$$

can be regarded as the defining equation for two different differential structures, the second being the complexification of the first. At the conceptual level this is what distinguishes the two choices for a "general solution" of the equation given at the beginning of the section.

Proof : Since D_L extends D the **e** matrices of these two differential structures are the same. **q.e.d**.

The final proposition of the section is a technical result needed needed later in the text. **(andd for that reason should probably be delayed.)**

Proposition 2.4.11 : *Suppose* **e** *and* **ê** *are two bases of* V *and*

$$x' + Bx = 0$$

and

$$x' + Ax = 0$$

are the defining **e** *and* **ê**-*equations of* D *respectively. Let* $L \supset K$ *be a differential field extension in which both equations have fundamental matrix solutions. Then the field extensions of* K *generated by the entries of these fundamental matrix solutions are the same.*

Proof : For the transition matrix $P \in \mathrm{GL}(n, K)$ between bases we have[7] $A = P^{-1}BP + P^{-1}P'$, and all the entries of P, P^{-1} and P' belong to K. **q.e.d**.

Jerry: One really wants that the RING extensions generated by the fm-solutions AND THEIR INVERSES are the same. Then one can talk about PV RINGS. This involves very little additional work.

2.5 An Intrinsic Definition of the Differential Galois Group

Here K *is a differential field and* (V, D) *is a differential module. We assume* $\dim_K V = n < \infty$.

When $L \supset K$ is a differential field extension one also has $L_C \supset K_C$ for the corresponding fields of constants. When $L_C = K_C$ one speaks of an extension with *no new constants*, or of a *no new constants* extension. This is automatically the case with the extensions of fields of germs of meromorphic functions considered in the early sections of the text. In a purely algebraic setting it is often a crucial hypothesis.

A *Picard-Vessiot extension* of (V, D) is a differential field extension $L \supset K$ satisfying the following conditions:

(a) the extension has no new constants;

(b) the L-space $L \otimes_K V$ admits a basis consisting of horizontal vectors of D_L;

(c) when $M \supset K$ is any other differential extension satisfying (a) and (b) there is an field embedding $\varphi : L \to M$ over K which commutes with the derivations δ_K and δ_M on L and M respectively, i.e., which satisfies

$$\varphi \circ \delta_L = \delta_M \circ \varphi\,; \tag{2.5.1}$$

and

[7] Recall the discussion surrounding (2.2.9).

(d) any field embedding $\eta : L \to L$ over K which commutes with δ_L is an automorphism.

The *differential Galois group* of (V, D) corresponding to an associated Picard-Vessiot extension is the group G_L of automorphisms of L over K which commute with the derivation δ_L on L, but only up to isomorphism. Indeed, when $M \supset K$ is any other Picard-Vessiot extension for (V, D) we have field embeddings $\varphi_{LM} : L \to M$ and $\varphi_{ML} : M \to L$ as in (c), and by (d) the composition $\eta := \varphi_{ML} \circ \varphi_{LM} : L \to L$ must be an automorphism. When $g \in G_M$ we see from (d) that the mapping $\ell \in L \mapsto \varphi_{ML}(g \cdot \varphi_{LM}(\ell))$ is in G_L, and one sees easily that this establishes an isomorphism between G_M and G_L. One therefore refers to G_L as "the" differential Galois group of (V, D).

Two questions immediately arise.

- In the case $K = \mathbb{C}(z)$ with derivation $\frac{d}{dz}$ is the differential Galois group as defined above the same (up to isomorphism) as that defined earlier for a defining basis equation? The answer is yes, and the result will be established later in the text.

- Does a Picard-Vessiot extension exist for any differential module (V, D)? Here the answer is no; the standard existence proof, which we will give, requires characteristic zero and algebraically closed assumptions on K_C.

The Coddington-Levinson reference in the bibiligraphy is new.

Chapter 3

Differential rings

In this chapter we record some basic facts from differential algebra. The most comprehensive reference for this material is Kolchin's book [12]. Other references are [9], [21] and [33]. Only Kolchin and an appendix of van der Put and Singer treat partial differential fields, as we do here.

We will, on occasion, need to consider a non-commutative ring, namely the ring of linear differential operators. However, except in that case, we assume our rings are commutative and have a unit 1; the zero ring 0 is the unique ring with $1 = 0$. Homomorphisms always take the unit to the unit; the unit of a subring is the same as that of the including ring. As usual $\mathbb{N}$ and $\mathbb{Z}$ denotes the ring of natural numbers (including 0) and the ring of integers, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ denote the fields of rational, real and complex numbers.

Throughout this book, all rings are assumed to be $\mathbb{Q}$-algebras.

In Sections 3.10 and 3.2 we discuss some consequences of this assumption. See also Proposition 3.10.2 and Example 3.10.3.

Throughout this book R denotes a Δ-ring (a $\mathbb{Q}$-algebra by our assumption) and k denotes a Δ-field (of characteristic 0 by our assumption). See the first section of this chapter for the definitions of Δ-ring and field.

3.1 Δ-rings

If R is any ring then a derivation δ on R is an additive mapping that satisfies the product (or Leibnitz) rule. Thus, for every $a, b \in R$,

1. $\delta(a + b) = \delta a + \delta b$, and
2. $\delta(ab) = \delta(a)b + a\delta(b)$.

An example is the trivial derivation with

$$\delta a = 0 \qquad \text{for all } a \in R.$$

Using the product rule, we have

$$\delta(1) = \delta(1 \cdot 1) = \delta 1 \cdot 1 + 1 \cdot \delta 1 = 2\delta(1).$$

Therefore $\delta(1) = 0$. The power rule

$$\delta(a^n) = na^{n-1}, \qquad n \in \mathbb{N},$$

follows from the product rule by induction. If b is invertible then

$$0 = \delta(1) = \delta\left(b \cdot \frac{1}{b}\right) = \delta b \cdot \frac{1}{b} + b \cdot \delta\left(\frac{1}{b}\right).$$

Thus

$$\delta\left(\frac{1}{b}\right) = -\frac{\delta b}{b^2}.$$

The quotient rule

$$\delta\left(a/b\right) = \frac{b\delta a - a\delta b}{b^2}$$

then comes immediately from the product rule.

We fix a set of symbols

$$\Delta = \{\delta_1, \ldots, \delta_m\}.$$

Definition 3.1.1 A ring on which Δ acts as a set of commuting derivations is called a *differential ring*. A differential ring is *ordinary* if $m = 1$ and is *partial* if $m > 1$.

Suppose that R is a differential ring. Then, for $\delta, \delta' \in \Delta$ and $a, b \in R$,

1. $\delta(a + b) = \delta a + \delta b$
2. $\delta(ab) = a\delta b + \delta ab$,
3. $\delta(\delta' a) = \delta'(\delta a)$.

We usually use the prefix Δ in place of the word "differential", e.g. Δ-ring, Δ-field. If R is an ordinary Δ-ring we usually denote the derivation by prime ($'$), i.e. $a' = \delta_1 a$ for $a \in R$. For iterated derivations we use the notation

$$a^{(n)} = \delta_1^n a.$$

However on some occasions it is useful to use the symbol δ (but we usually drop the subscript).

Example 3.1.2 If R is any ring, then we may think of R as a Δ-ring by making the derivations act trivially, i.e.

$$\delta a = 0, \qquad a \in R, \quad \delta \in \Delta.$$

Example 3.1.3 Consider the ring of polynomials in one variable x $R = \mathbb{C}[x]$. We can make R into an ordinary Δ-ring by defining

$$\delta = \frac{d}{dx}.$$

Similarly $k = \mathbb{C}(x)$, the field of rational functions of one variable, can be made into a Δ-field.

Example 3.1.4 The ring $R = \mathbb{C}(x)[e^x, \log x]$ is an ordinary Δ-ring with derivation $\delta = d/dx$. However $\mathbb{C}[x][e^x, \log x]$ is not. It does not contain the derivative of $\log x$. But other derivations do make it a differential ring, for example the "Euler derivation"

$$\delta = x\frac{d}{dx}.$$

Example 3.1.5 In the example above we put the derivation d/dx on $R = \mathbb{C}[x]$. But there are others choices. For example, if

$$p \in R = \mathbb{C}[x]$$

Then there is a unique way of making R into an ordinary Δ-ring such that

$$x' = \delta x = p.$$

We are forced to define

$$\delta = p\,\frac{d}{dx},$$

and it is easy to see that this is a derivation.

Example 3.1.6 More generally, if $R = \mathbb{C}[x_1, \ldots, x_m]$ is the ring of polynomial functions of m variables we may make R into a Δ-ring by defining

$$\delta_i = \frac{\partial}{\partial x_i}, \qquad i = 1, \ldots, m.$$

Example 3.1.7 If k is the field of functions of m complex variables $z_1, \ldots, z_m$ that are meromorphic in a given region we may make k into a Δ-field by defining

$$\delta_i = \frac{\partial}{\partial z_i}.$$

We may make $\mathbb{C}[x_1, \ldots, x_m]$ into a Δ-ring in other ways, but the situation is complicated by the requirement that our derivations commute.

Example 3.1.8 Let $R = \mathbb{C}[x_1, x_2]$. Choose

$$p_1, p_2, q_1, q_2 \in R.$$

Suppose we wanted to make R into a Δ-ring with two derivations that satisfy:

$$\begin{aligned} \delta_1 x_1 &= p_1, \qquad & \delta_1 x_2 &= p_2 \\ \delta_2 x_1 &= q_1, \qquad & \delta_2 x_2 &= q_2. \end{aligned}$$

Evidently we would have

$$\delta_1 = p_1 \frac{\partial}{\partial x_1} + p_2 \frac{\partial}{\partial x_2}, \qquad \text{and}$$
$$\delta_2 = q_1 \frac{\partial}{\partial x_1} + q_2 \frac{\partial}{\partial x_2}.$$

However we require that the derivations commute. Therefore

$$\delta_1\delta_2 x_1 = \delta_2\delta_1 x_1 \qquad \text{and} \qquad \delta_1\delta_2 x_2 = \delta_2\delta_1 x_2.$$

This restricts our choice. We need

$$q_1 \frac{\partial p_1}{\partial x_1} + q_2 \frac{\partial p_1}{\partial x_2} = p_1 \frac{\partial q_1}{\partial x_1} + p_2 \frac{\partial q_1}{\partial x_2},$$
$$q_1 \frac{\partial p_2}{\partial x_1} + q_2 \frac{\partial p_2}{\partial x_2} = p_1 \frac{\partial q_2}{\partial x_1} + p_2 \frac{\partial q_2}{\partial x_2}$$

Conditions such as these are often called *integrability conditions*.

3.2 Constants

In analysis, a "constant" is simply a complex or real number. In our setting we need an algebraic definition. We use the result from analysis that a function is constant if and only if all of its derivatives are identically zero.

Definition 3.2.1 If R is a Δ-ring we denote by R^Δ the *ring of constants of* R, defined by

$$R^\Delta = \{a \in R \mid \delta a = 0 \text{ for } \delta \in \Delta\}.$$

As we saw in the first section, $\delta 1 = 0$. By additivity, n (by which we mean the n-termed sum $1 + \cdots + 1$) is a constant for every $n \in \mathbb{Z}$. Since $\mathbb{Q} \subset R$ (which we assume) the quotient rule implies that $\mathbb{Q} \subset R^\Delta$. There exist non-trivial derivations of $\mathbb{R}$ and $\mathbb{C}$ (extend Proposition 3.6.1, below, to an infinite set of indeterminates), however whenever these appear (in examples only) we assume that they are given the trivial derivation.

Proposition 3.2.2 *If R is a Δ-ring, then R^Δ is a ring. If K is a Δ-field, then K^Δ is a field.*

Proof. The fact that R^Δ is a ring follows immediately from the facts that a derivation is additive and satisfies the product rule. Suppose that $a \in K^\Delta$, $a \neq 0$. Then a has an inverse b in K, and the quotient rule implies that b is also a constant. **q.e.d.**

In this book we restrict our attention to characteristic 0. One reason is that Δ-fields of characteristic p have "too many" constants.

Example 3.2.3 If k is a Δ-field of characteristic p then, for every $a \in k$,

$$\delta(a^p) = p\, a^{p-1}\delta a = 0.$$

So k^Δ is quite large; indeed, it contains all of k^p. The correct way to treat non-zero characteristic is to use "iterated" or Hasse-Schmidt derivations. This was done first by [24] and more recently by [23]. We will not pursue that theory here.

3.3 Linear Δ-operators

Just as in calculus, we have need to consider "higher" derivatives

Definition 3.3.1 Θ denotes the free commutative monoid generated by Δ. An element θ of Θ is called a *derivative operator*.

Thus an element θ of Θ has a unique representation of the form

$$\theta = \delta_1^{e_1} \cdots \delta_m^{e_m}$$

for some $e_1, \ldots, e_m \in \mathbb{N}$. The unit of Θ is

$$1 = \delta_1^0 \cdots \delta_m^0.$$

We think of θ as an operator. If a is an element of a Δ-ring and

$$\theta = \delta_1^{e_1} \cdots \delta_m^{e_m}$$

then

$$\theta(a) = \delta_1^{e_1} \cdots \delta_m^{e_m}(a).$$

In this sense 1 is the identity operator, $1(a) = 1$.

Definition 3.3.2 If

$$\theta = \delta_1^{e_1} \ldots \delta_m^{e_m} \in \Theta$$

then the *order of* θ is

$$\operatorname{ord}\theta = e_1 + \cdots + e_m.$$

For each $n \in \mathbb{N}$, we let

$$\Theta(n) = \{\theta \in \Theta \mid \operatorname{ord}\theta \leq n\}.$$

Definition 3.3.3 Let R be a Δ-ring. The free R-module with set of generators Θ is called the *ring of linear* Δ*-operators* and is denoted by $R[\Delta]$.

An element $a \in R \subset R[\Delta]$ denotes the scalar multiplication operator, i.e.

$$a(b) = ab.$$

An element of $R[\Delta]$ is a finite sum

$$L = \sum_{i=1}^{r} a_i \theta_i$$

where $a_i \in R$ and $\theta_i \in \Theta$. We call elements of $R[\Delta]$ linear differential operators. If a is an element of some Δ-R-algebra and

$$L = \sum_{i=1}^{r} a_i \theta_i \in R[\Delta]$$

then

$$L(a) = \sum_{i=1}^{r} a_i \theta_i(a).$$

Thus each $\delta \in \Delta$ acts as the (given) derivation on the R-algebra and elements of R act as scalar multiplication.

In the case of ordinary Δ-rings, an element of $R[\Delta]$ has the form

$$L = a_n \delta^n + \cdots + a_1 \delta + a_0$$

(here we have written δ instead of δ_1). This is a linear differential operator as studied in a course on ODE (ordinary differential equations).

Definition 3.3.4 Let R be a Δ-ring. Define a non-commutative ring structure on $R[\Delta]$ where multiplication is composition of operators.

We often use juxtaposition to indicate the ring multiplication, however we sometimes use the symbol $\circ$ to emphasize the definition.

If $\delta_i, \delta_j \in \Delta$ then

$$\delta_i \delta_j = \delta_j \delta_i$$

since the derivations commute. However if $a \in R$ then

$$\delta_i \circ a = \delta_i(a) + a\delta_i.$$

Indeed, for any $b \in R$

$$(\delta_i \circ a)(b) = \delta_i(ab) = \delta_i(a)b + a\delta_i(b).$$

We shall study this non-commutative ring much more in Chapter ???.

3.4 Δ-subrings and Δ-extensions

Definition 3.4.1 By a Δ-*subring* of R we mean a subring S that is a Δ-ring under the restriction of the derivations on R. Similarly, if K is a Δ-field then by a Δ-*subfield* of K we mean a Δ-subring that is a field. If E is a Δ-field that contains K as a Δ-subring then E is called a Δ-*extension field of* K.

Throughout this book, all Δ-rings are assumed to be $\mathbb{Q}$-algebras.

In the literature this is called a *Ritt algebra*. (A Ritt algebra is often incorrectly defined to be a Δ-ring that contains $\mathbb{Q}$. This excludes the 0 ring, which can appear, for example, as a ring of fractions, or a ring associated with the empty set of a Δ-scheme.) We will see in Example 3.10.3 why it is useful to restrict our rings to be Ritt algebras.

Definition 3.4.2 Let S be a Δ-ring and R a Δ-subring. Let $\eta_1, \ldots, \eta_n$ be a family of elements of S. Then

$$R\{\eta_1, \ldots, \eta_n\}$$

denotes the smallest Δ-subring of S that contains R and each η_i. If E is a Δ-extension field of a Δ-field K then

$$K\langle \eta_1, \ldots, \eta_n \rangle$$

denotes the smallest Δ-subfield of E that contains K and each η_i.

Thus

$$R\{\eta_1, \ldots, \eta_n\} = R[(\theta\eta_i)_{\theta\in\Theta, i=1,\ldots,n}].$$

and

$$K\langle \eta_1, \ldots, \eta_n \rangle = \mathrm{qf}(K\{\eta_1, \ldots, \eta_n\}).$$

Definition 3.4.3 Let S be a Δ-ring containing R (as a Δ-subring). Then S is *finitely Δ-generated over R* if there is a finite family $\eta_1, \ldots, \eta_n$ of elements of S such that

$$\S = R\{\eta_1, \ldots, \eta_n\}.$$

Similarly a Δ-extension field E of K is *finitely Δ-generated over K* if there is a finite family $\eta_1, \ldots, \eta_n$ of elements of E with

$$E = K\langle \eta_1, \ldots, \eta_n \rangle.$$

Our primary interest is in Δ-rings R that are finitely Δ-generated over k. In fact, except for rings of Δ-polynomials (Section 3.9), our rings will even be *finitely generated* over k, i.e. of the form $k[\eta_1, \ldots, \eta_n]$.

As we shall see, constants play an important role in the Galois theory. The following result is basic. Other results can be found in Section 3.12.

Proposition 3.4.4 *Suppose that R is an integral domain containing a Δ-field K. Then any constant of R that is algebraic over K is algebraic over K^Δ.*

Proof. Let $c \in R^\Delta$ be algebraic over K, with

$$P = X^d + P_{d-1}X^{d-1} + \cdots + P_0 \in K[X]$$

being the monic polynomial of least degree with coefficients in K satisfying $P(c) = 0$. Then, for each $\delta \in \Delta$,

$$0 = \delta(P(c)) = \delta P_{d-1} c^{d-1} + \cdots + \delta P_0,$$

because $\delta c = 0$. The minimality of P implies that

$$\delta P_{d-1} = \cdots = \delta P_0 = 0,$$

i.e. each $P_j \in K^\Delta$, so c is algebraic over K^Δ. **q.e.d.**

Corollary 3.4.5 *If K is a Δ-field then K^Δ is algebraically closed in K.*

Proof. This means that if $a \in K$ is algebraic over K^Δ, then a is in K^Δ. This is immediate from the proposition; take $R = K$. **q.e.d.**

3.5 Rings of fractions

Recall that a multiplicative set of R is a subset S of R satisfying

1. $1 \in S$, and
2. if $a \in S$ and $b \in S$ then $ab \in S$.

Some authors do not permit 0 to be an element of a multiplicative set. For algebraic geometry it is essential that 0 be allowed; for us it does not matter. Given a multiplicative set $S \subset R$ we can form the ring of fractions

$$RS^{-1}.$$

See, for example, [19, Section 4, p. 107] or ???. An element of RS^{-1} is a denoted by

$$\frac{a}{b},$$

where $a \in R$ and $b \in S$. This symbol denotes an equivalence class where

$$\frac{a}{b} = \frac{c}{d}$$

if there exists $s \in S$ with

$$s(ad - cb) = 0 \in R.$$

If $0 \in S$ then RS^{-1} is the 0 ring. We let

$$\phi_S \colon R \to RS^{-1}, \qquad \phi_S(a) = \frac{a}{1}.$$

be the canonical homomorphism. The kernel of ϕ_S is

$$\ker \phi_S = \{a \in R \mid sa = 0 \text{ for some } s \in S\}.$$

Proposition 3.5.1 *Let S be a multiplicative set of R. Then there is a unique way to make RS^{-1} into a Δ-ring so that ϕ_S is a Δ-homomorphism.*

Proof. If ϕ_S is a Δ-homomorphism we need

$$\delta\left(\frac{a}{1}\right) = \delta\phi_S(a) = \phi_S(\delta a) = \frac{\delta a}{1}$$

for every $a \in R$ and $\delta \in \Delta$. If $b \in S$ then

$$0 = \delta(1) = \delta\left(\frac{b}{1}\frac{1}{b}\right) = \frac{\delta b}{1}\frac{1}{b} + \frac{b}{1}\,\delta\left(\frac{1}{b}\right),$$

so

$$\delta\left(\frac{1}{b}\right) = \frac{\delta b}{b^2}.$$

The product rule then gives

$$\delta\left(\frac{a}{b}\right) = \frac{b\delta a - a\delta b}{b^2}.$$

Thus the extension of δ to RS^{-1} is unique, if it exists.

To show that it exists, we need to show that it is well-defined. If $a/b = c/d$ then there exists $s \in S$ with $s(ad - bc) = 0$. Therefore

$$0 = \delta s(ad - bc) + s(a\delta d + d\delta a - b\delta c - c\delta b).$$

Multiply by bds to get

$$\begin{aligned} 0 = {} & bds\delta s(ad - bc) + \\ & s^2\big((b\delta a - a\delta b)d^2 - (d\delta c - c\delta d)b^2 + (ad - bc)(d\delta b + b\delta d)\big) \\ = {} & s^2\big((b\delta a - a\delta b)d^2 - (d\delta c - c\delta d)b^2\big). \end{aligned}$$

It is equally easy to show that δ is a derivation, that the derivations commute and that h is a Δ-homomorphism. **q.e.d.**

If $c \in R$ then, as usual, $R[1/c]$ denotes the Δ-ring of fractions RS^{-1} where

$$S = \{c^d \mid d \in \mathbb{N}\}.$$

Here we define $c^0 = 1$, even if $c = 0$. $R[1/c]$ is the 0 ring if c is nilpotent. However, that case will not appear in this book (except perhaps by accident).

We also will consider the field of fractions $\mathrm{qf}(R)$ of a Δ-integral domain. This is the ring of fractions

$$RS^{-1}$$

where $S = R^{)}$ is the multiplicative set consisting of all non-zero elements of R. In this case the canonical homomorphism $R \to \mathrm{qf}(R)$ is injective and we identify R with its image.

3.6 Extensions of derivations

Suppose that R is a Δ-ring and S is a ring (not Δ-ring) containing R. In the previous section we saw that if S is a ring of fractions of R then there is a unique way to extend the derivations from R to S. In general there may be many ways to extend the derivations. (If we did not assume that R is a $\mathbb{Q}$ algebra there may be no ways of doing so. See Example 3.6.3 below.) In this section we record a few results but leave an exhaustive study to another venue. We start with an ordinary Δ-field. Compare with Example 3.1.5.

Proposition 3.6.1 *Suppose that k is an ordinary Δ-field. Let $(X_1, \dots, X_n)$ be be a family of indeterminates over k. For each $j = 1, \dots, n$ we suppose given*

$$a_j \in k[(X_1, \dots, X_n].$$

Then there is a unique structure of Δ-ring on $k[(X_1, \dots, X_n]$ extending the derivation on k and having the property

$$X_j' = a_j.$$

Proof. This is [3, V.16.2, Proposition 3, p. A.V.128], but we sketch a direct proof here.

For any $P \in R = k[(X_1, \dots, X_n]$, we let P^δ denote the polynomial obtained by differentiating the coefficients of P. Thus, if

$$P = \sum P_{e_1,\dots,e_n} X_1^{e_1} \cdots X_n^{e_n},$$

then

$$P^\delta = \sum P'_{e_1,\dots,e_n} X_1^{e_1} \cdots X_n^{e_n}.$$

This defines a derivation on R that extends that of k. We denote it by ∇ so that

$$\nabla P = P^\delta.$$

Now define

$$\delta = \nabla + \sum_{j=1}^{n} a_j \frac{\partial}{\partial X_j}.$$

This is a sum of derivations on R and therefore is a derivation on R. It clearly has the required properties. The additivity of derivations and the product rule imply that this derivation is the only one possible satisfying the properties of the proposition. **q.e.d**.

If $m = \operatorname{card} \Delta > 1$ (partial Δ-fields) the situation is made more complicated by the requirement that the derivations commute. See Example 3.1.8. Given

$$a_{ij} \in R \qquad i = 1, \dots, m \quad j = 1, \dots, n,$$

there are unique derivations of R extending those on k that satisfy

$$\delta_i X_j = a_{ij}.$$

However these derivations need not commute. In Section ??? we will see an example where they, in fact, do commute.

Proposition 3.6.2 *Let K be a Δ-field and E an algebraic extension of K. Then there is a unique way to make E a Δ-extension field of K.*

Proof. Let $\delta \in \Delta$. We first show that δ has a unique extension to a derivation of E. This follows from [3, V.16.2, Proposition 4(b), p. A.V.129] but we sketch the proof here.

By Zorn's Lemma we may find a maximal extension L of K in E to which δ extends uniquely. Suppose that $x \in E$, $x \notin L$. Let $P \in L[X]$ be the minimal monic polynomial that vanishes on x. Then

$$P'(x) = \frac{dP}{dX}(x) \neq 0$$

and therefore has an inverse in $L[x]$. Define

$$u = -P^{\delta}(x)P'(x)^{-1}.$$

If δ extends to $L[x]$ then, using the additivity of δ and the product rule, we must have

$$0 = \delta(P(x)) = P^{\delta}(x) + P'(x)\delta x$$

which forces

$$\delta x = u.$$

Any element $y \in L[x]$ can be written as a polynomial Q in x (uniquely if the degree of the degree of Q is smaller than the degree of L). Say

$$y = Q(x).$$

Then we must have

$$\delta y = Q^{\delta}(x) + Q'(x)u.$$

Thus, if there is an extension of δ, it is unique.

To show the existence of an extension we must first show that the formula

$$\delta y = Q^{\delta}(x) + Q'(x)u$$

is independent of the choice of Q. But, if

$$y = Q(x) = R(x)$$

then $R - Q = AP$ for some polynomial A so

$$R^{\delta}(x)+R'(x)u = P^{\delta}(x)+P'(x)u+(A^{\delta}(x)+A'(x)u)P(x)+A(x)(P^{\delta}(x)+P'(x)u).$$

But $P\delta(x) + P'(x)u = 0$ by definition of u and $P(x) = 0$ by definition of P. So δ is well-defined. The additivity of δ and the product rule are easy to check.

Finally we need to show that two elements δ and δ' in Δ commute on $L(x)$. Note that

$$\delta\delta' - \delta'\delta$$

is a derivation on $L(x)$ that restricts to the trivial derivation on L. By what we have shown, this trivial derivation on L extends uniquely to a derivation on $L(x)$. This extension must be trivial, so $\delta\delta' - \delta'\delta = 0$ on $L(x)$. **q.e.d.**

Note that we used our assumption that K is a field of characteristic 0 by asserting that $P'(x)$ is invertible. This is true as long as x is separable over L (or K). However for an inseparable extension there may be no way or many ways to extend the derivation.

Example 3.6.3 Let K be a Δ-field of characteristic p, $a \in K$ having no p-th root in K and x a p-th root of a in some extension field. Thus

$$P = X^p - a$$

is the minimal polynomial for x. If δ is a derivation on $K[x]$ then we must have

$$0 = \delta P(x) = -\delta a + px^{p-1}\delta x = -\delta a.$$

If $a \notin K^\Delta$ there can not be any extension of δ to $K[x]$. On the other hand, if $a \in K^\Delta$ then this equation tells us nothing about δx. In fact, it may be chosen arbitrarily in $K[x]$.

3.7 Δ-ideals and Δ-homomorphisms

Definition 3.7.1 Let R be a Δ-ring. By a Δ-*ideal* $\mathfrak{a}$ *of* R we mean an ideal that is closed under Δ, i.e.

$$\delta a \in \mathfrak{a} \qquad \text{for all } a \in \mathfrak{a} \text{ and } \delta \in \Delta.$$

Δ-ideals are far less plentiful than non-differential ideals.

Example 3.7.2 Let $R = \mathbb{C}[x]$ be the ordinary Δ-ring with $x' = 1$ (i.e. $\delta = d/dx$). We claim that R has no proper non-zero Δ-ideal. Suppose that $\mathfrak{a}$ is a non-zero ideal of R and let $P \in \mathfrak{a}$, $P \neq 0$. We suppose that P has degree n (as a polynomial in x) and is monic. Then

$$P^{(n)} = n! \in \mathfrak{a}$$

so $\mathfrak{a} = R$ (recall that R is assumed to contain a field of characteristic 0).

Definition 3.7.3 Let R and S be Δ-rings. By a Δ-*homomorphism* of R into S we mean a homomorphism ϕ that commutes with the derivations, i.e.

$$\delta\phi(a) = \phi(\delta a), \qquad \text{for } a \in R \text{ and } \delta \in \Delta.$$

Definition 3.7.4 Suppose that R and S are Δ-rings that contain a common Δ-subring T. Then a Δ-homomorphism $\phi\colon R \to \S$ is *over* T if the restriction of ϕ to T is the identity.

Proposition 3.7.5 *Suppose that K is an algebraic extension of k and $\phi\colon K \to L$ is a homomorphism over k. Then ϕ is a Δ-homomorphism.*

Proof. To simplify the notation we assume that $L = \mathrm{im}(\phi)$. If $\delta \in \Delta$, then

$$\phi \circ \delta \circ \phi^{-1}$$

is a derivation on L that restricts to δ on k. But, by Proposition 3.6.2 there is a *unique* derivation on L with a given restriction to k. Therefore

$$\phi \circ \delta \circ \phi^{-1} = \delta$$

which makes ϕ a Δ-homomorphism. **q.e.d.**

Proposition 3.7.6 *Suppose that R and S are Δ-rings and $\phi\colon R \to S$ is a Δ-homomorphism. Then* $\ker\phi$ *is a Δ-ideal.*

Proof. If $a \in \ker\phi$, then, for $\delta \in \Delta$,

$$0 = \delta(\phi a) = \phi(\delta a)$$

so $\delta a \in \ker\phi$. **q.e.d.**

Proposition 3.7.7 *Let $\mathfrak{a}$ be a Δ-ideal of R. Then $R/\mathfrak{a}$ has a unique structure of Δ-ring so that the canonical mapping $R \to R/\mathfrak{a}$ is a Δ-homomorphism.*

Proof. For $\delta \in \Delta$, and $a \in R$, we must define

$$\delta(a + \mathfrak{a}) = \delta a + \mathfrak{a},$$

however we must show that this is well-defined. Suppose that $a + \mathfrak{a} = b + \mathfrak{a}$. Let $c = b - a \in \mathfrak{a}$, then

$$\delta b = \delta a + \delta c.$$

The last term is in $\mathfrak{a}$ since $\mathfrak{a}$ is a Δ-ideal, therefore

$$\delta b + \mathfrak{a} = \delta a + \mathfrak{a}.$$

We must also show that this formula defines a derivation on $R/\mathfrak{a}$ and that the derivations commute. But this is easy. **q.e.d.**

Using this proposition we can give an alternate proof of Proposition 3.7.5. Indeed ϕ (of Proposition 3.7.5) has kernel (0), which is a Δ-ideal.

Proposition 3.7.8 *Suppose that $\phi\colon R \to S$ is a Δ-homomorphism of Δ-rings. If $\mathfrak{b}$ is a Δ-ideal of S then $\mathfrak{a} = \phi^{-1}\mathfrak{b}$ is a Δ-ideal of R.*

Proof. If $a \in \mathfrak{a}$ then $\phi(a) \in \mathfrak{b}$ so, for $\delta \in \Delta$,

$$\phi(\delta a) = \delta(\phi a) \in \mathfrak{b}$$

which says that $\delta a \in \mathfrak{a}$. **q.e.d.**

In fact, there is a bijection between Δ-ideals of S and Δ-ideals of R that contain $\ker \phi$.

Definition 3.7.9 Let S be a subset of R. Then $[S]$ denotes the smallest Δ-ideal of R that contains S.

Thus

$$[S] = (\Theta S) = \{\textstyle\sum_i r_i \theta_i s_i \mid r_i \in R, \theta_i \in \Theta, s_i \in S\}.$$

This is the ideal generated by all θs where $\theta \in \Theta$ and $s \in S$.

3.8 Tensor product

We will have occasion to use tensor products of rings (or modules), but only in the very simplest of cases; the base ring will always be a field. For a treatment of tensor products for that special case see [34, Ch. III, §14, p. 179]. However to show that the tensor product of two Δ-rings is itself a Δ-ring it is more convenient to use the treatment of [1, p. 24–31] or [19, Chapter XVI, p. 601]. We sketch the construction below. Recall that we assume that all Δ-rings are Δ-k-algebras. Since the base ring for the tensor product in this section will always be that field we write $\otimes$ instead of $\otimes_k$.

Let R and S be Δ-k-algebras. Following [1, proof of Proposition 2.12, p. 24] we let

$$C = k^{(R \times S)}.$$

This is the set of formal finite linear combinations of elements of $R \times S$ with coefficients in k, i.e. expressions of the form

$$\sum_{i=1}^{n} a_i(r_i, s_i) \qquad a_i \in k, r_i \in R, s_i \in S.$$

C is a k-vector space. Let D be the k-subspace generated by

$$\begin{gathered}(r_1 + r_2, s) - (r_1, s) - (r_2, s)\\ (r, s_1 + s_2) - (r, s_1) - (r, s_2)\\ (ar, s) - a(r, s)\\ (r, as) - a(r, s)\end{gathered}$$

where $r, r_1, r_2 \in R$, $s, s_1, s_2 \in S$, and $a \in k$.

We make C into a ring in the obvious way:

$$\Big(\sum_{i=1}^{n} a_i(r_i, s_i)\Big)\Big(\sum_{j=1}^{t} b_j(t_j, u_j)\Big) = \sum_{j=1}^{n}\sum_{j=1}^{t} a_i b_j (r_i t_j, s_i u_j).$$

The identity is $(1,1)$. It is easy to see that D is an ideal in C. Then

$$R \otimes S = C/D.$$

The image of (r,s) is denoted by $r \otimes s$. There are canonical ring homomorphisms

$$\begin{array}{rcl} R \to & C & \to R \otimes S \\ r \mapsto & (r,1) & \mapsto r \otimes 1 \end{array} \quad \text{and} \quad \begin{array}{rcl} S \to & C & \to R \otimes S \\ s \mapsto & (1,s) & \mapsto 1 \otimes s, \end{array}$$

and $R \otimes S$ is generated as a ring by the images of R and S.

Proposition 3.8.1 *$R \otimes S$ has the unique structure of Δ-ring so that the canonical mappings are Δ-homomorphisms.*

Proof. Let $\delta \in \Delta$. In order that the product rule hold, we must have

$$\delta(r \otimes s) = \delta\big((r \otimes 1)(1 \otimes s)\big) = \delta(r \otimes 1)(1 \otimes s) + (r \otimes 1)\delta(1 \otimes s).$$

In order that the canonical homomorphisms be differential we need

$$\begin{aligned} \delta(r \otimes s) &= (\delta r \otimes 1)(1 \otimes s) + (r \otimes 1)(1 \otimes \delta s) \\ &= \delta r \otimes s + s \otimes \delta r. \end{aligned}$$

Thus δ is uniquely determined, if it exists.

To show that $R \otimes S$ is a Δ-ring we use the construction above. First note that C is a Δ-ring by the formula

$$\delta\Big(\sum_i a_i(r_i, s_i)\Big) = \sum_i \big(\delta a_i(r_i, s_i) + a_i(\delta r_i, s_i) + a_i(r_i, \delta s_i)\big)$$

where $\delta \in \Delta$. Evidently δ is additive and the various $\delta \in \Delta$ commute. It is a bit tedious to check product rule. The homomorphisms

$$\begin{array}{rcl} R \longrightarrow & C \\ r \longmapsto & (r,1) \end{array} \quad \text{and} \quad \begin{array}{rcl} S \longrightarrow & C \\ s \longmapsto & (1,s) \end{array}$$

are Δ-homomorphisms. Next note that D is a Δ-ideal. Therefore

$$R \otimes S = C/D$$

has the structure of Δ-ring and the canonical homomorphisms

$$R \to C \to R \otimes S \qquad \text{and} \qquad S \to C \to R \otimes S$$

are Δ-homomorphisms. **q.e.d.**

So far there has been no need to assume that k is a field. We could as well have used $R \otimes_B S$ where B is any Δ-ring and R and S are Δ-B-algebras. However the following propositions do require that k be a Δ-field.

Proposition 3.8.2 *Suppose that* P *and* Σ *are bases of* R *and* S *over* k*. Then the set*

$$\rho \otimes \sigma \qquad \rho \in \mathrm{P}, \sigma \in \Sigma$$

is a basis for $R \otimes S$*. In particular the canonical homomorphisms*

$$R \to R \otimes S \qquad \textit{and} \qquad S \to R \otimes S$$

are injective.

Proof. The first statement is [19]*Corollary 2.4, p. 609. Assume that the basis Σ of S contains 1. Suppose that

$$\sum_{i=1}^{n} a_i \rho_i$$

is in the kernel of the canonical mapping, where $a_i \in k, \rho_i \in \mathrm{P}$. Then

$$\sum_i a_i(\rho_i \otimes 1) = 0.$$

By the first statement, $a_i = 0$ for $i = 1, \ldots, n$. **q.e.d.**

We sometimes identify R and S with their images in $R \otimes S$. Over a ring the tensor product can "collapse" to 0:

$$\mathbb{Z}/(2) \otimes_{\mathbb{Z}} \mathbb{Z}/(3) = 0.$$

But over a field this cannot occur: $R \otimes S = 0$ if and only if $R = 0$ or $S = 0$. The following result will be used in Proposition 5.7.9.

Proposition 3.8.3 *Let* R*,* S *and* T *be* k*-algebras with* $S \subset T$*. If* $R \otimes S = R \otimes T$ *then* $S = T$*.*

Proof. Let P be a basis of R, Σ a basis of S and T a basis of T with $\Sigma \subset \mathrm{T}$. We assume that $1 \in \mathrm{P}$. Then, for $\tau \in \mathrm{T}$,

$$1 \otimes \tau \in R \otimes S$$

so

$$1 \otimes \tau = \sum_{\rho \in \mathrm{P}, \sigma \in \Sigma} a_{\rho\sigma} \rho \otimes \sigma.$$

By the preceding proposition, $a_{\rho\sigma} = 0$ if $\rho \neq 1$ or $\sigma \neq \tau$ and $a_{1\tau} = 1$. In particular, $\tau \in \Sigma$. **q.e.d.**

The following proposition is [34, Theorem 35, p. 184].

Proposition 3.8.4 *Let $\mathfrak{a} \subset R$ and $\mathfrak{b} \subset S$ be Δ-ideals. Then*

$$\mathfrak{a} \otimes S + R \otimes \mathfrak{b}$$

is a Δ-ideal of $R \otimes S$ and

$$(R \otimes S)/(\mathfrak{a} \otimes S + R \otimes \mathfrak{b})$$

is isomorphic to

$$(R/\mathfrak{a}) \otimes (S/\mathfrak{b}).$$

$\mathfrak{a} \otimes S + R \otimes \mathfrak{b}$ may also be described as the ideal generated by $\mathfrak{a}$ and $\mathfrak{b}$ (thinking of R and S as subsets of $R \otimes S$). We also have

$$\mathfrak{a} \otimes S + R \otimes \mathfrak{b} = \Big\{ \sum_i a_i \otimes b_i \mid a_i \in \mathfrak{a} \text{ or } b_i \in \mathfrak{b} \Big\}.$$

If $\mathfrak{a}$ and $\mathfrak{b}$ are prime, it does *not* follow that $\mathfrak{a} \otimes S + R \otimes \mathfrak{b}$ is prime.

Example 3.8.5 Suppose that $k = \mathbb{C}(x)$ and $K = \mathbb{C}(\sqrt{x})$. We consider

$$K \otimes K.$$

K, being a field, has a unique prime Δ-ideal, namely (0). But

$$(0) \otimes K + K \otimes (0) = (0)$$

is not prime, i.e. $K \otimes K$ is not an integral domain. Indeed

$$(\sqrt{x} \otimes 1 + 1 \otimes \sqrt{x})(\sqrt{x} \otimes 1 - 1 \otimes \sqrt{x}) = x \otimes 1 - 1 \otimes x = 0.$$

3.9 Δ-polynomials

Definition 3.9.1 Suppose that η is an element of some Δ-extension field of k. We say that η is Δ-*algebraic over* k if the family

$$(\theta\eta)_{\theta \in \Theta}$$

is algebraically dependent over k. In the contrary case we say that η is Δ-*transcendental over* k.

Thus η is Δ-algebraic if it "satisfies a differential polynomial equation", i.e. there is a polynomial

$$P \in k[X_1, \ldots, X_n],$$

for some $n \in \mathbb{N}$, and $\theta_1, \ldots, \theta_n \in \Theta$ such that

$$P(\theta_1\eta, \ldots, \theta_n\eta) = 0.$$

If k is an ordinary Δ-field then η is Δ-algebraic over k if there is a polynomial in $P \in k[X_0, \ldots, X_d]$ with

$$P(\eta, \eta', \eta'', \ldots, \eta^{(d)}) = 0.$$

Example 3.9.2 e^x satisfies

$$(e^x)' - e^x = 0.$$

The Bessel function $J_n(x)$ satisfies

$$x^2 J_n(x)'' + x J_n(x)' + (x^2 - n^2) J_n(x) = 0.$$

The Weierstrass p-function $\wp(x)$ satisfies

$$\wp(x)'^2 = 4\wp(x)^3 - g_2\wp(x) - g_3.$$

Functions that are Δ-transcendental are sometimes called *transcendentally transcendental*.

Example 3.9.3 Euler's gamma function

$$\Gamma(x) = \int_0^\infty t^{x-1} e^{-t} dt$$

is Δ-transcendental [28].

Example 3.9.4 The (lower) incomplete gamma function is

$$\gamma(a, x) = \int_0^x t^{a-1} e^{-t} dt.$$

If we think of this as a function of x, with a as a parameter, it is Δ-algebraic over $\mathbb{C}(x)$. Indeed,

$$\frac{d\gamma(a,x)}{dx} = x^{a-1} e^{-x},$$

so

$$\frac{d^2\gamma(a,x)}{dx^2} = \frac{a-1-x}{x}\gamma(a,x).$$

On the other hand, if we think of $\gamma(a, x)$ as a function of a, with x as a parameter, then it is Δ-transcendental over $\mathbb{C}(x)$. [28] has more examples and references.

Thinking of $\gamma(a, x)$ as a function of two variables, i.e.

$$\Delta = \left\{ \frac{\partial}{\partial a}, \frac{\partial}{\partial x} \right\},$$

then $\gamma(a, x)$ is Δ-algebraic over $\mathbb{C}(a, x)$. As we saw above

$$\frac{\partial^2\gamma(a,x)}{\partial x^2} = \frac{a-1-x}{x}\gamma(a,x).$$

More generally we have the following definition.

Definition 3.9.5 A family $\eta_1, \ldots, \eta_n$ of elements of some Δ-extension field of k is said to be Δ-*algebraically dependent* if the family $(\theta\eta_i)_{\theta\in\Theta, i=1,\ldots,n}$ is algebraically dependent. In the contrary case $\eta_1, \ldots, \eta_n$ are said to be Δ-*algebraically independent* or to be a set of Δ-*indeterminates over* k.

Proposition 3.9.6 *For each $n \in \mathbb{N}$ there is a set $y_1, \ldots, y_n$ of Δ-indeterminates over k.*

Proof. Let $(X_{\theta,j})_{\theta\in\Theta, j=1,\ldots,n}$ be a family of indeterminates over k and set

$$R = k[(X_{\theta j})_{\theta\in\Theta, j=1,\ldots,n}].$$

By Proposition 3.6.1, there is a unique structure of Δ-ring on R such that for every $\delta \in \Delta$

$$\delta X_{\theta j} = X_{\delta\theta j}.$$

Set

$$y_j = X_{1j}.$$

We need to show that the derivations commute. If $\delta, \delta' \in \Delta$ then

$$\delta\delta' X_{\theta j} = \delta X_{\delta'\theta j} = X_{\delta\delta'\theta j} = X_{\delta'\delta\theta j} = \delta' X_{\delta\theta j} = \delta'\delta X_{\theta j}.$$

q.e.d.

Definition 3.9.7 If $y_1, \ldots, y_n$ are Δ-indeterminates, then $k\{y_1, \ldots, y_n\}$ is the *ring of Δ-polynomials over k*.

So a Δ-polynomial in $y_1, \ldots, y_n$ is simply a polynomial in $y_1, \ldots, y_n$ and all their derivatives.

Definition 3.9.8 Let $y_1, \ldots, y_n$ be Δ-indeterminates over k and let $\eta_1, \ldots, \eta_n$ be elements of some Δ-extension field of k. The Δ-homomorphism over k

$$\begin{aligned} k\{y_1, \ldots, y_n\} &\longrightarrow k\{\eta_1, \ldots, \eta_n\} \\ y_i &\longmapsto \eta_i, \end{aligned}$$

is called the *substitution homomorphism*. If $P \in k\{y_1, \ldots, y_n\}$ then we usually write

$$P(\eta_1, \ldots, \eta_n)$$

instead of $s(P)$.

3.10 Radical and prime Δ-ideals

Δ-rings are rarely Noetherian.

Example 3.10.1 [27, p. 12] Consider the ring $k\{y\}$ of ordinary Δ-polynomials in one indeterminate. Then

$$[y'y''] \subsetneq [y'y'', y''y'''] \subsetneq [y'y'', y''y''', y''y^{(3)}] \subsetneq \cdots$$

is an infinite proper ascending chain of Δ-ideals. Thus $k\{y\}$ fails to be a Noetherian Δ-ring. To prove this we need to show that

$$y^{(n)}y^{(n+1)} \notin [(y^{(i)}y^{(i+1)} \mid i = 1, \ldots, n-1].$$

Suppose the contrary,

$$y^{(n)}y^{(n+1)} = \sum_{i=1}^{n-1} \sum_{j=0}^{t} A_{ij} \left(y^{(i)}y^{(i+1)}\right)^{(j)} \tag{3.10.1}$$

for some $A_{ij} \in k\{y\}$. The left hand side has degree 2 (in the indeterminate $y, y', \ldots$), so all the terms on the right of higher degree must cancel. This allows us to assume that

$$A_{ij} \in k.$$

Define the *weight* of a Δ-monomial to be the sum of the orders of the derivatives, so the weight of

$$(y^{(e_1)})^{d_1} \cdots (y^{(e_r)})^{d_r}$$

is

$$d_1e_1 + \cdots + d_re_r.$$

Note that $y^{(i)}y^{(i+1)}$ has weight $2i+1$, and

$$\left(y^{(i)}y^{(i+1)}\right)' = (y^{(i+1)})^2 + y^{(i)}y^{(i+2)}$$

has weight $2i+2$. In general

$$\left(y^{(i)}y^{(i+1)}\right)^{(j)}$$

has weight $2i+1+j$.

Getting back to Equation 3.10.1, we see that the left hand side has weight $2n+1$. The terms on the right hand side that have weight $2n+1$ are

$$A_{ij} \left(y^{(i)}y^{(i+1)}\right)^{(j)}$$

where $2i+1+j = 2n+1$. Therefore

$$y^{(n)}y^{(n+1)} = \sum_{i=1}^{n-1} A_{i,2n-2i} \left(y^{(i)}y^{(i+1)}\right)^{(2n-2i)},$$

where $B_i = A_{i,2n-2i} \in k$. The monomial $y'y^{(2n)}$ appears in

$$(y'y'')^{(2n-2)}$$

and in no other term. Hence $A_{1,2n-2} = 0$. But then

$$y^{(n)}y^{(n+1)} = 0$$

which is absurd.

On the other hand radical ideals behave much better. In the literature, the smallest radical Δ-ideal containing S is denoted by $\{S\}$ and is called a *perfect* Δ-ideal. In general it must be defined recursively as in [12, p. 122]. However our assumption that R is a Ritt algebra (an algebra over $\mathbb{Q}$) permits us to make a simplification.

Proposition 3.10.2 *If $\mathfrak{a}$ is a Δ-ideal of R then*

$$\sqrt{\mathfrak{a}} = \{a \in R \mid a^n \in \mathfrak{a} \text{ for some } n \in \mathbb{N}\}$$

is a radical Δ-ideal.

Proof. Let $a \in \sqrt{\mathfrak{a}}$ so that, say, $a^n \in \mathfrak{a}$. We claim that for any $\delta \in \Delta$, and $k = 0, \ldots, n$,

$$a^{n-k}(\delta a)^{2k} \in \mathfrak{a}\ .$$

The case $k = 0$ is by assumption. Differentiating, we get

$$(n-k)a^{n-k-1}(\delta a)^{2k+1} + 2ka^{n-k}(\delta a)^{2k-1}(\delta^2 a) \in \mathfrak{a}\ .$$

Multiply by δa and note that the second term is then in $\mathfrak{a}$. Because we can divide by $n - k$ we have

$$a^{n-k-1}(\delta a)^{2k+2} \in \mathfrak{a}\ ,$$

which completes the induction. Putting $k = n$ we see that

$$(\delta a)^{2n+2} \in \mathfrak{a}$$

so that $\delta a \in \sqrt{\mathfrak{a}}$. **q.e.d.**

In particular $\{S\} = \sqrt{[S]}$. We use the later notation and simply call it the *radical Δ-ideal generated by S*. If $a \in \sqrt{[S]}$ then

$$a^d = \sum_i c_i \theta_i b_i$$

where $d \in \mathbb{N}$, $c_i \in R$, $\theta_i \in \Theta$ and $s_i \in S$ (not necessarily distinct). In the preceding proposition we made use of our assumption that all Δ-rings are $\mathbb{Q}$ algebras. If this assumption were not made then this proposition would be false.

Example 3.10.3 Consider the ordinary Δ-ring $\mathbb{Z}[x]$ where $x' = 1$. Then the ideal

$$(2, x^2) \subset \mathbb{Z}[x]$$

is a Δ-ideal (since $(x^2)' = 2x$) so

$$R = \mathbb{Z}[x]/(2, x^2)$$

is a Δ-ring. However it is not a $\mathbb{Q}$ algebra. Writing $\overline{x}$ for the image of x in R we have $\overline{x}^2 = 0$ so

$$\overline{x} \in \sqrt{[0]}$$

but $\overline{x}' = 1$ is not in $\sqrt{[0]}$.

In fact R has no prime Δ-ideal (Diffspec $R = \emptyset$). Indeed any prime Δ-ideal would have to contain $\sqrt{[0]}$ and therefore 1. This cannot happen in algebra: every non-zero ring contains a prime ideal (Spec $R = \emptyset$ if and only if $R = 0$.)

The next proposition will be used frequently in the sequel. We need a lemma first.

Lemma 3.10.4 *Let $a, b \in R$ and $\theta \in \Theta$. If d is the order of θ then*

$$a^{d+1}\theta b \in [ab].$$

Proof. The result is obvious if $d = 0$ (i.e. $\theta = 1$). Write

$$\theta = \delta\theta'$$

for some $\delta \in \Delta$ and $\theta' \in \Theta$ has order $d - 1$. By the induction hypothesis,

$$a^d\theta' b \in [ab]$$

so

$$a\delta(a^d\theta' b) = da^d\delta a\theta' b + a^{d+1}\delta\theta' b \in [ab].$$

By induction, the first term on the right is in $[ab]$. **q.e.d.**

Proposition 3.10.5 *Let S and T be subsets of R. Then*

$$\sqrt{[S]}\sqrt{[T]} \subset \sqrt{[S]} \cap \sqrt{[T]} = \sqrt{[ST]}\ .$$

Proof. The first inclusion is obvious. Let $a \in \sqrt{[S]} \cap \sqrt{[T]}$ so that $a^s \in [S]$ and $a^t \in [T]$ for some $s, t \in \mathbb{N}$. Then $a^{s+t} \in [S][T]$ Using the lemma we see easily that

$$[S][T] \subset \sqrt{[ST]}$$

so that $a \in \sqrt{[ST]}$. Now let $a \in \sqrt{[ST]}$. Therefore, for some $n \in \mathbb{N}$,

$$a^n \in [ST] \subset [S] \cap [T]$$

hence $a \in \sqrt{[S]}$ and $a \in \sqrt{[T]}$. **q.e.d.**

Proposition 3.10.6 *Suppose that $\mathfrak{a}$ is a Δ-ideal of R and that Σ is a multiplicative set with $\Sigma \cap \mathfrak{a} = \emptyset$. Let $\mathfrak{m}$ be a Δ-ideal containing $\mathfrak{a}$ that is maximal with respect to avoiding Σ. Then $\mathfrak{m}$ is prime.*

Proof. First observe that $\sqrt{\mathfrak{m}}$ is also disjoint from Σ and, by maximality, $\mathfrak{m} = \sqrt{\mathfrak{m}}$. Suppose that $ab \in \mathfrak{m}$ but $a \notin \mathfrak{m}$ and $b \notin \mathfrak{m}$, so that $s \in \sqrt{[\mathfrak{m}, a]}$ and $t \in \sqrt{[\mathfrak{m}, b]}$ for some $s, t \in \Sigma$. But then

$$st \in \sqrt{[\mathfrak{m}, a]}\sqrt{[\mathfrak{m}, b]} \subset \sqrt{[\mathfrak{m}, ab]} = \mathfrak{m}$$

which is a contradiction. **q.e.d.**

Corollary 3.10.7 *Let S be a subset of R and $b \in R$ Then there is a prime Δ-ideal of R containing S but not b if and only if no power of b is in $[S]$, i.e. $b \notin \sqrt{[S]}$.*

Proof. Take Σ to be the set consisting of 1 and all powers of b. **q.e.d.**

If $P \in k\{y_1, \ldots, \mathfrak{y}_n\}$ and $P(\eta_1, \ldots, \eta_n) = 0$ we call $(\eta_1, \ldots, \eta_n)$ a *zero of* P. The question arises: does every Δ-polynomial have a zero? The answer is "yes", but unfortunately it is the wrong question. Consider the ordinary Δ-polynomial

$$P = y' - y.$$

Evidently P has a zero, namely 0 itself. What we really want is a zero of P that is not a zero of the Δ-polynomial y. We start with a set S of Δ-polynomials and another Δ-polynomial C. We are interested in finding a zero of all the Δ-polynomials in S having the property that C does not vanish at it.

Proposition 3.10.8 *Let $S \subset k\{y_1, \ldots, y_n\}$ be a set of Δ-polynomials and $C \in k\{y_1, \ldots, y_n\}$. Then there exist $\eta_1, \ldots, \eta_n$ in some Δ-extension field of k with*

$$\begin{aligned} &P(\eta_1, \ldots, \eta_n) = 0 \qquad && \text{for all } P \in S, \\ &C(\eta_1, \ldots, \eta_n) \neq 0, \end{aligned}$$

if and only if no power of C is in $[S]$.

Proof. By the preceding corollary, there is a prime Δ-ideal $\mathfrak{p}$ containing $[S]$ that does not contain C. Then

$$\mathrm{qf}(k\{y_1, \ldots, y_n\}/\mathfrak{p})$$

is a Δ-extension field of k. If η_i is the image of y_i in this field, then $(\eta_1, \ldots, \eta_n)$ is a zero of S but not of C. **q.e.d.**

Of course, it may not be apparent whether some power of C is in $[S]$ or not, even if $C = 1$, particularly for partial Δ-polynomials. As a simple example, consider the Δ-field $k = \mathbb{C}(x, t)$ where

$$\delta_1 = \frac{\partial}{\partial x} \qquad \text{and} \qquad \delta_2 = \frac{\partial}{\partial t}.$$

If y is a Δ-indeterminate and

$$S = \{\delta_1 y + t, \delta_2 y - x\},$$

then

$$\delta_2(\delta_1 y + t) - \delta_1(\delta_2 y - x) = 2 \in [S].$$

So the system S has no solution: it is inconsistent. The technique of characteristic sets can be used to decide consistency, the membership problem for Δ-ideals and other problems. For a tutorial on this subject see [31].

3.11 Maximal Δ-ideals

Definition 3.11.1 By a *maximal Δ-ideal* of a Δ-ring R we mean a Δ-ideal of R that is maximal among the Δ-ideals of R.

Note that a maximal Δ-ideal need not be a maximal ideal. There may exist ideals strictly containing it (but not Δ-ideals).

Example 3.11.2 As in Example 3.7.2, we let $R = \mathbb{Q}[x]$ be the ordinary Δ-ring with $x' = 1$. In that example we saw that R has no proper non-zero Δ-ideal. Thus (0) is a maximal Δ-ideal but it is not a maximal ideal.

Proposition 3.11.3 *Let $\mathfrak{m}$ be a maximal Δ-ideal of R. Then $\mathfrak{m}$ is prime.*

Proof. Proposition 3.10.6 where $\Sigma = \{1\}$. **q.e.d.**

An ideal M of a ring R is maximal if and only if R/M is a field. This is equivalent to saying that R/M has no proper non-trivial ideal. We have a similar condition.

Definition 3.11.4 A Δ-ring R is said to be *Δ-simple* if it has no proper non-zero Δ-ideal.

Proposition 3.11.5 *A Δ-ideal $\mathfrak{m}$ of R is a maximal Δ-ideal if and only $R/\mathfrak{m}$ is Δ-simple.*

Proof. The set of Δ-ideals of $R/\mathfrak{m}$ is in bijective correspondence with the set of Δ-ideals of R that contain $\mathfrak{m}$. **q.e.d.**

In particular, a Δ-ring R is Δ-simple if and only if (0) is a maximal Δ-ideal. Because a maximal Δ-ideal is prime, it follows that a Δ-simple ring is an integral domain. The next result will be used frequently in what follows. It is another result concerning constants. The simple proof is based on an idea of Alberto Baider.

Proposition 3.11.6 *Suppose R is a Δ-simple ring containing a Δ-field k and that R is finitely generated (not finitely Δ-generated) over k. Then $\mathrm{qf}(R)^\Delta$ is algebraic over k^Δ.*

Proof. Let $c \in \mathrm{qf}(R)^\Delta$. Define the "set of denominators"

$$\mathfrak{a} = \{b \in R \mid bc \in R\}.$$

Evidently $\mathfrak{a}$ is a non-zero ideal and it is a Δ-ideal because c is a constant. But R is Δ-simple, so $1 \in \mathfrak{a}$ and $c \in R^\Delta$. Because $\mathrm{qf}(R)$ is a field, every non-zero element of R^Δ is invertible.

By Proposition 3.4.4, we need only show that c is algebraic over k. Suppose not, so c is transcendental over k. We know [1, Proposition 5.23, p. 66] that there exists a polynomial $P \in k[c]$ such that any homomorphism

$$\phi\colon k[c] \longrightarrow k,$$

with $\phi(P) \neq 0$, extends to a homomorphism (not Δ-homomorphism) of R into an algebraic closure of k. Choose $d \in C$ with $P(d) \neq 0$ and let

$$\phi\colon k[c] \longrightarrow k, \qquad c \longmapsto d,$$

be the substitution homomorphism. $c - d \in R^\Delta$ and therefore, by the above remarks, must either be 0 or be invertible in R^Δ. But it cannot be invertible since $\phi(c - d) = 0$, so $c = d \in C$ which contradicts the assumption that c is transcendental over k. **q.e.d.**

The result is also true if R is finitely Δ-generated. Instead of extending a homomorphism we need to extend a Δ-homomorphism. That can be done, by [12, Theorem 3, p. 140], but the proof is more difficult and we do not need the added generality.

The fact that there may be constants in $\mathrm{qf}(R)$ algebraic over C adds complications to the Picard-Vessiot theory. Rather than dealing with that here we make a simplifying assumption.

Corollary 3.11.7 *Assume that $C = k^\Delta$ is algebraically closed. If R is a Δ-simple ring finitely generated over k then*

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

3.12 The Wronskian

The Wronskian determinant gives a criterion for solutions of a linear homogeneous ordinary differential equation to be linearly independent over constants. We generalize that theorem here. We also introduce the Wronskian *matrix* which will play an important role in the Picard-Vessiot theory.

Definition 3.12.1 Suppose that K is an ordinary Δ-field and $\eta = (\eta_1, \ldots, \eta_n)$ is an n-tuple of elements of K. Then the *Wronskian matrix* of η is the matrix

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

The *Wronskian determinant* is the determinant of the Wronskian matrix.

Proposition 3.12.2 *Let K be an ordinary Δ-field with field of constants $C = K^\Delta$. $\eta_1, \ldots, \eta_n \in K$ are linearly dependent over C if and only if*

$$\det W(\eta) = 0.$$

Proof. Suppose first that

$$c_1\eta_1 + \cdots + c_n\eta_n = 0,$$

where $c_1, \ldots, c_n \in C$ are not all zero. Differentiate this equation successively to get the vector equation

$$c_1 \begin{pmatrix} \eta_1 \\ \vdots \\ \eta_1^{(n-1)} \end{pmatrix} + \quad \cdots \quad + c_n \begin{pmatrix} \eta_n \\ \vdots \\ \eta_n^{(n-1)} \end{pmatrix} = 0.$$

Thus the columns of the Wronskian matrix are linearly dependent so the Wronskian determinant is zero.

Conversely, suppose that $\det W(\eta) = 0$. We may suppose that no proper subset of $\eta_1, \ldots, \eta_n$ has the property that its Wronskian determinant vanishes. The case $n = 1$ is trivial, so we may assume that $n > 1$. Therefore

$$\det W(\eta_1, \ldots, \eta_{n-1}) \neq 0.$$

Since the columns of the Wronskian matrix $W(\eta_1, \ldots, \eta_n)$ are linearly dependent *over* K there exist $a_1, \ldots, \mathfrak{a}_n \in K$, not all zero, with

$$\sum_{j=1}^{n} a_j \eta_j^{(i-1)} = 0, \qquad i = 1, \ldots, n.$$

By what we have already proven, $\eta_1, \ldots, \eta_{n-1}$ are linearly independent over C, therefore, because K is a field, we may assume that $a_n = 1$. We claim that each a_i is in C. Differentiating the above equation we get

$$\sum_{j=1}^{n-1} a_j' \eta_j^{(i-1)} + \sum_{j=1}^{n} a_j \eta_j^{(i)} = 0.$$

The second term is zero for $i = 1, \ldots, n-1$, therefore

$$\sum_{j=1}^{n-1} a_j' \eta_j^{(i-1)} = 0, \qquad i = 1, \ldots, n-1,$$

i.e.

$$\begin{pmatrix} \eta_1 & \cdots & \eta_{n-1} \\ \vdots & & \vdots \\ \eta_1^{(n-2)} & \cdots & \eta_{n-1}^{(n-2)} \end{pmatrix} \begin{pmatrix} a_1' \\ \vdots \\ a_{n-1}' \end{pmatrix} = W(\eta_1, \ldots, \eta_{n-1}) \begin{pmatrix} a_1' \\ \vdots \\ a_{n-1}' \end{pmatrix} = 0.$$

It follows that

$$a_j' = 0, \qquad j = 1, \ldots, n-1.$$

q.e.d.

We actually use the contrapositive more than the proposition itself.

Corollary 3.12.3 *Let K be an ordinary Δ-field with field of constants $C = K^{\Delta}$. Let $\eta_1, \ldots, \eta_n \in K$. Then the $\eta_1, \ldots, \eta_n$ are linearly independent over C if and only if* $\det W(\eta) \neq 0$.

Note that K is any Δ-field that contains the family $\eta = (\eta_1, \ldots, \eta_n)$. In other words, if the Wronskian determinant vanished then η is linearly dependent over the constants of *any* Δ-field that contains η. We say simply that $\eta_1, \ldots, \eta_n$ are linearly dependent (or independent) *over constants*.

We can generalize the result slightly by replacing K by a Δ-integral domain domain R. Then the vanishing of the Wronskian determinant implies that $\eta_1, \ldots, \eta_n$ are linearly dependent over $\mathrm{qf}(R)^{\Delta}$, which unfortunately is *not* the same as $\mathrm{qf}(R^{\Delta})$. If R is not an integral domain, there is little that we can say.

Example 3.12.4 Consider the following real valued functions.

$$u = \begin{cases} e^{-\frac{1}{x^2}}, & \text{if } x \neq 0 \\ 1 & \text{if } x = 1 \end{cases}$$

$$v = \begin{cases} e^{-\frac{1}{x^2}}, & \text{if } x > 0 \\ 1 & \text{if } x \leq 1 \end{cases}$$

$$w = 1$$

These are C^{∞} functions which are not linearly dependent. However their Wronskian determinant is identically 0 on the entire real line. This does not contradict our result since the ring of C^{∞} functions is not an integral domain.

For partial Δ-fields we need to consider many "Wronskians". [12, Theorem 1, p. 86] is a further generalization of the material presented here.

The first row of a Wronskian matrix is, as expected,

$$\eta = (\eta_1, \ldots, \eta_n)$$

But for the second row we have m choices:

$$\delta_1\eta, \delta_2\eta \ldots \delta_m\eta.$$

We also allow η (redundantly) to get $m + 1 = \binom{m+1}{1}$ choices:

$$\eta,\ \delta_1\eta, \delta_2\eta \ldots, \delta_m\eta.$$

For the third row we have

$$\begin{aligned} &\eta, \quad \delta_1\eta, \delta_2\eta \ldots \delta_m\eta, \\ &\delta_1^2\eta, \delta_1\delta_2, \ldots, \delta_1\delta_m\eta, \\ &\delta_2^2\eta, \delta_2\delta_3, \ldots, \delta_2\delta_m\eta, \\ &\quad \vdots \\ &\delta_m^2\eta. \end{aligned}$$

There are $\binom{m+2}{2}$ choices. And so on.

Definition 3.12.5 By a *order-restricted n-tuple* (of derivative operators) we mean an n-tuple of derivative operators $\theta = (\theta_1, \ldots, \theta_n)$ where

$$\operatorname{ord} \theta_i < i, \qquad i = 1, \ldots, n.$$

Thus $\operatorname{ord} \theta_1 = 0$, so $\theta_1 = 1$, $\operatorname{ord} \theta_2 \leq 1$, so θ_2 is one of $1, \delta_1, \ldots, \delta_m$, etc. Another way of saying this is that

$$\theta_i \in \Theta(i-1).$$

We define the Wronskian matrix using an arbitrary n-tuple of derivations, however the important case is where it is order-restricted.

Definition 3.12.6 Let $\theta = (\theta_1, \ldots, \theta_n)$ be an n-tuple of derivative operators. By the *Wronskian matrix of η with respect to θ* is meant the matrix

$$W_\theta(\eta) = W_{\theta_1,\ldots,\theta_n}(\eta_1, \ldots, \eta_n) = \begin{pmatrix} \theta_1\eta_1 & \cdots & \theta_1\eta_n \\ \vdots & & \vdots \\ \theta_n\eta_1 & \cdots & \theta_n\eta_n \end{pmatrix}.$$

By the *Wronskian determinant* we mean the determinant of the Wronskian matrix.

Proposition 3.12.7 *Let K be a Δ-field and let $C = K^\Delta$. If $\eta_1, \ldots, \eta_n \in K$ are linearly dependent over C then*

$$\det W_\theta(\eta) = 0$$

for every n-tuple θ. Conversely, if

$$\det W_\theta(\eta) = 0$$

for every order-restricted *n-tuple, then $\eta_1, \ldots, \eta_n$ are linearly dependent over C.*

Proof. Suppose first that

$$c_1\eta_1 + \cdots + c_n\eta_n = 0,$$

where $c_1, \ldots, c_n \in C$ are not all zero. Differentiate this equation successively to get the vector equation

$$c_1 \begin{pmatrix} \theta_1\eta_1 \\ \vdots \\ \theta_n\eta_1 \end{pmatrix} + \quad \cdots \quad + c_n \begin{pmatrix} \theta_1\eta_n \\ \vdots \\ \theta_n\eta_n \end{pmatrix} = 0.$$

Thus the columns of the Wronskian matrix are linearly dependent so the Wronskian determinant is zero.

Conversely, suppose that

$$\det W_\theta(\eta) = 0$$

for every order-restricted n-tuple $\theta = (\theta_1, \ldots, \theta_n)$. If $n = 1$ this says that $\eta_1 = 0$ which means that the family (η_1) is linearly dependent over C (even over $\mathbb{Q}$). We assume that $n > 1$ and that the proposition is proved for lesser values of n. Therefore

$$\det W_{\theta_1,\ldots,\theta_{n-1}}(\eta_1, \ldots, \eta_{n-1}) \neq 0,$$

for some order-restricted $n-1$-tuple $(\theta_1, \ldots, \theta_{n-1})$.

Let θ be any element of $\Theta(n-1)$. Then $(\theta_1, \ldots, \theta_{n-1}, \theta)$ is an order-restricted n-tuple and, by hypothesis,

$$\det W_{\theta_1,\ldots,\theta_{n-1},\theta}(\eta) = 0.$$

In particular we may choose $\theta = \delta_k\theta_i$ for $k = 1, \ldots, m$, $i = 1, \ldots, n-1$. It follows that the matrix

$$\begin{pmatrix}
\theta_1\eta_1 & \ldots\ldots & \theta_1\eta_n \\
\vdots & & \vdots \\
\theta_{n-1}\eta_1 & \ldots\ldots & \theta_{n-1}\eta_n \\
\delta_1\theta_1\eta_1 & \ldots\ldots & \delta_1\theta_1\eta_n \\
\vdots & & \vdots \\
\delta_1\theta_{n-1}\eta_1 & \ldots\ldots & \delta_1\theta_{n-1}\eta_n \\
\vdots & & \vdots \\
\delta_m\theta_1\eta_1 & \ldots\ldots & \delta_m\theta_1\eta_n \\
\vdots & & \vdots \\
\delta_m\theta_{n-1}\eta_1 & \ldots\ldots & \delta_m\theta_{n-1}\eta_n
\end{pmatrix}$$

has rank no bigger than $n-1$. Therefore the columns are linearly dependent over K, i.e. there exist $a_1, \ldots, \mathfrak{a}_n \in K$, not all zero, with

$$\sum_{j=1}^{n} a_j\theta_i\eta_j = 0, \qquad i = 1, \ldots, n-1,$$

and

$$\sum_{j=1}^{n} a_j\delta_k\theta_i\eta_j = 0, \qquad i = 1, \ldots, n-1, \quad k = 1, \ldots, m.$$

However $\det W_{\theta_1,\ldots,\theta_{n-1}}(\eta_1, \ldots, \eta_{n-1}) \neq 0$, thus the column vectors

$$\begin{pmatrix} \theta_1\eta_1 \\ \vdots \\ \theta_{n-1}\eta_1 \end{pmatrix} \quad \cdots \quad \begin{pmatrix} \theta_1\eta_{n-1} \\ \vdots \\ \theta_{n-1}\eta_{n-1} \end{pmatrix}$$

are linearly independent over K. We must have $a_n \neq 0$. Because K is a field we may assume that $a_n = 1$. We claim that each a_j is in C.

For $i = 1, \ldots, n-1$ and $k = 1, \ldots, m$, we have

$$\begin{aligned} 0 = \delta_k\Big(\sum_{j=1}^{n} a_j\theta_i\eta_j\Big) &= \sum_{j=1}^{n-1} \delta_k a_j\theta_i\eta_j + \sum_{j=1}^{n} a_j\delta_k\theta_i\eta_j \\ &= \sum_{j=1}^{n-1} \delta_k a_j\theta_i\eta_j. \end{aligned}$$

It follows that $\delta_k a_j = 0$ for $j = 1, \ldots, n-1$ and $k = 1, \ldots, m$. **q.e.d.**

We use the contrapositive more than the above proposition.

Corollary 3.12.8 *Let K be a Δ-field. If $\eta_1, \ldots, \eta_n \in K$ are linearly independent over K^Δ, then there is an order-restricted n-tuple θ such that*

$$\det W_\theta(\eta) \neq 0.$$

3.13 Results from ring theory

We end this chapter with a section that collects some result from ring theory that we will be using, but that are not commonly studied today. In this section k is a field (not necessarily a Δ-field).

Let R be an integral domain that is finitely generated over k. Then

$$\operatorname{trdeg} R$$

denotes the transcendence degree of $\operatorname{qf}(R)$ over k. (See [34, p. 100, bottom].

Proposition 3.13.1 *Suppose that R and S are integral domains that are finitely generated over k. If $\phi\colon R \to S$ is a surjective homomorphism over k then*

$$\operatorname{trdeg} S \leq \operatorname{trdeg} R.$$

If $\operatorname{trdeg} S = \operatorname{trdeg} R$ *then ϕ is an isomorphism.*

Proof. [34, Theorems 28 and 29, p. 101]. **q.e.d.**

Corollary 3.13.2 *Let R be an integral domain finitely generated over k. Then every surjective endomorphism is an automorphism.*

Chapter 4

Linear homogeneous ODE

In the Galois theory of polynomial equations, one associates a finite group to a given equation. Properties of the group are reflected in the equation (or the solutions of it) and vice versa. Similarly, to any linear homogeneous ordinary differential equation, we may assign a group. In this case it is a linear algebraic group. As we saw in Chapter **??**, properties of the group are reflected in the solutions of the equation.

In this chapter we define Picard-Vessiot extension. This is the analogue of normal extension; it is a Δ-field extension that contains sufficiently many solutions of the differential equation. We give the definition and some examples. We also state some of the important theorems. However we defer the proofs, and a deeper discussion of them, to the following chapter.

In that chapter we will generalize what we have done here to systems of partial differential equations. The general theory is no easier in the special case treated in the present chapter, so it makes sense to prove the theorems in the more general setting.

Throughout this chapter we restrict our attention to *ordinary* Δ-rings and fields. Thus we have a single derivation operator, denoted by δ. If a is an element of a Δ-ring, we usually write a' instead of δa and $a^{(n)}$ instead of $\delta^n a$.

Throughout this chapter k is an *ordinary* Δ-field of characteristic zero. The field of constants of k is

$$C = k^{\Delta}.$$

We assume that C is algebraically closed. For an example of what goes wrong if we do not make that assumption, see Example 4.6.1.

4.1 Fundamental system of solutions

Consider a linear homogeneous ordinary differential equation (ODE)

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

where y is a Δ-indeterminate and $a_0, \ldots, a_{n-1} \in k$. We are interested in solutions that lie in some Δ-extension field of k. Alternatively we could have started with a linear homogeneous Δ-polynomial. Then we would talk about the zeroes of that polynomial. A third possibility is to start with a linear differential operator

$$L = \delta^n - a_{n-1}\delta^{n-1} - \cdots - a_0 \in k[\delta].$$

(See Definition 3.3.3.) Clearly, which of these three we use does not matter. Since the shortest term is "Δ-operator", that is what we choose. We still speak of solutions of L but really mean solutions of the equation $L(y) = 0$ (or zeros of the Δ-polynomial $L(y)$).

Definition 4.1.1 By a *solution* of L we mean an element η of some Δ-extension field K of k such that

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

A solution always exists, namely the trivial solution $\eta = 0$. Observe that the set of all solutions in a given Δ-field K forms a vector subspace of K over the field of constants K^Δ. We would like to find a basis of that vector space. First we show that its dimension is no bigger than n (so, in particular, it is finite dimensional).

Proposition 4.1.2 *Suppose that $\eta_1, \ldots, \eta_{n+1}$ are $n+1$ solutions of L in K. Then they are linearly dependent over K^Δ.*

Proof. Using Proposition 3.12.2, we need to show that the Wronskian determinant

$$\det W(\eta_1, \ldots, \eta_{n+1}) = \det \begin{pmatrix} \eta_1 & \cdots & \eta_{n+1} \\ \vdots & & \vdots \\ \eta_1^{(n)} & \cdots & \eta_{n+1}^{(n)} \end{pmatrix}$$

is 0. Because of the equation $L(\eta_i) = 0$,

$$\eta_i^{(n)} = a_{n-1}\eta_i^{(n-1)} + \cdots + a_0\eta_i$$

so the last row is a linear combination of the preceding ones, and the determinant is 0. **q.e.d**.

Definition 4.1.3 By a *fundamental system* (of solutions) for L we mean n solutions $\eta_1, \ldots, \eta_n \in K$ that are linearly independent over K^Δ.

By Corollary 3.12.3, $\eta_1, \ldots, \eta_n$ is a fundamental system of solutions if and only if $\det W(\eta) \neq 0$. We often use vector notation

$$\eta = (\eta_1, \ldots, \eta_n).$$

In this context we compute derivatives coordinate-wise

$$\eta' = (\eta_1', \ldots, \eta_n').$$

Proposition 4.1.4 *Let η be a fundamental system for L. Then*

$$k\{\eta\} = k[\eta, \eta', \ldots, \eta^{(n-1)}].$$

In particular, $k\{\eta\}$ is finitely generated over k.

Proof. In fact, η need not be a fundamental system, but merely be solutions of L. The result follows immediately from the fact that

$$\eta_i^{(n)} = a_{n-1}\eta_i^{(n-1)} + \cdots + a_0\eta_i.$$

q.e.d.

Recall that $\mathrm{GL}_{K^\Delta}(n)$ denotes the *general linear group*, the group of all n by n matrices with non-zero determinant and coefficients in K^Δ.

Proposition 4.1.5 *Suppose that η and ξ are two fundamental systems for L in K. Then there exists*

$$c \in GL_{K^\Delta}(n)$$

with

$$\xi = \eta\, c.$$

Proof. By Proposition 4.1.2,

$$\eta_1, \ldots, \eta_n, \xi_j$$

are linearly dependent over K^Δ. Since the family η is linearly independent, we have

$$\xi_j = \sum_{i=1}^{n} c_{ij}\eta_i$$

for some $c_{ij} \in K^\Delta$. Thus

$$(\xi_1, \cdots, \xi_n) = (\eta_1, \cdots, \eta_n) \begin{pmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & & \vdots \\ c_{n1} & \cdots & c_{nn} \end{pmatrix}.$$

Similarly

$$(\eta_1, \cdots, \eta_n) = (\xi_1, \cdots, \xi_n) \begin{pmatrix} d_{11} & \cdots & d_{1n} \\ \vdots & & \vdots \\ d_{n1} & \cdots & d_{nn} \end{pmatrix}.$$

Thus $\xi = \eta c = \xi dc$. Since the family ξ is linearly independent over K^Δ we must have $dc = 1$, hence c is invertible. **q.e.d.**

4.2 Existence

In this section we prove the existence of a fundamental system in some Δ-extension field K of k for the Δ-operator

$$L = \delta^n - a_{n-1}\delta^{n-1} - \cdots - a_0\delta.$$

We shall make use of the following lemma.

Lemma 4.2.1 *Let $y_1, \ldots, y_n$ be n Δ-indeterminates over k and let consider the radical Δ-ideal $\mathfrak{a}$ of $k\{y_1, \ldots, y_n\}$ generated by $L(y_1), \ldots, L(y_n)$:*

$$\mathfrak{a} = \sqrt{[L(y_1), \ldots, L(y_n)]}.$$

Then the Wronskian matrix $W(y_1, \ldots, y_n)$ is not in $\mathfrak{a}$.

Proof. Suppose, on the contrary, that $W(y_1, \ldots, y_n) \in \mathfrak{a}$. Then we may have

$$W(y_1, \ldots, y_n)^e = \sum_{j=1}^{n} \sum_{i=0}^{d} A_{ij}(L(y_j))^{(i)}, \tag{4.2.1}$$

where $A_{ij} \in k\{y_1, \ldots, y_n\}$. Choose d minimal, so that there is a d-th derivative $L(y_j)^{(d)}$ that appears on the right hand side with non-zero coefficient. Note that the order of every term in this equation is bounded by $n + d$.

Think of this equation as an equality of polynomials (not Δ-polynomials) in the indeterminates

$$y_1, \ldots, y_n,\ y_1', \ldots, y_n',\ \ldots,\ y_1^{(n+d)}, \ldots, y_n^{(n+d)}.$$

Observe that

$$L(y)^{(d)} = y^{(n+d)} - M(y)$$

where $M(y)$ has order less than $n + d$. In Equation 4.2.1 we can make the substitution

$$y_j^{(n+d)} \longmapsto M_d(y_j).$$

This does not affect the left hand side since the order of the Wronskian is smaller than n, and it modifies the right hand side by lowering the integer d. But this is a contradiction. **q.e.d**.

Proposition 4.2.2 *There is a Δ-extension field K of k that contains a fundamental system for L.*

Proof. Let

$$\mathfrak{a} = \sqrt{[L(y_1), \ldots, L(y_n)]}$$

be as in the lemma. Then, by Corollary 3.10.7, there is a prime Δ-ideal $\mathfrak{p}$ of $k\{y_1, \ldots, y_n\}$ such that

1. $\mathfrak{a} \subset \mathfrak{p}$, and
2. $\det W(y_1, \ldots, y_n) \notin \mathfrak{p}$.

Let

$$K = \mathrm{qf}(k\{y_1, \ldots, y_n\}/\mathfrak{p}),$$

and let η_j be the image of y_j in K (i.e. η_j is the coset $y_j + \mathfrak{p}$). Then

$$L(\eta_j) = 0$$

because $L(y_j) \in \mathfrak{a} \subset \mathfrak{p}$ and

$$w(\eta_1, \ldots, \eta_n) \neq 0$$

since $w(y_1, \ldots, y_r) \notin \mathfrak{p}$. **q.e.d.**

However we do not have uniqueness. In the proof of the proposition we made a choice of prime Δ-ideal $\mathfrak{p}$. We could have chosen $\mathfrak{p}$ as small as possible, but the following example shows that this is not a very good choice.

Example 4.2.3 Consider the ordinary Δ-field

$$k = \mathbb{C}(e^x),$$

where the derivation is $\delta = d/dx$, and the linear homogeneous Δ-equation

$$L(y) = y' - y = 0.$$

The Wronskian determinant $\det W(y)$ is y.

It is not difficult to see that the Δ-ideal $[L(y)]$ is prime so a minimal prime $\mathfrak{p}$ would be $\mathfrak{p} = [L(y)]$. Thus the solution η constructed in the proof of the previous proposition would be the image of y in

$$k\{y\}/[L(y)].$$

Observe that $y - e^x \neq [L(y)]$, since every element of $[L(y)]$ has order at least 1. Therefore $\eta \neq e^x$. But then

$$\eta = ke^x$$

for some constant k *not* in $\mathbb{C}$. This is algebraically fine but leads us far away from "real life" (analysis).

Another possibility is to choose $\mathfrak{p}$ as large as possible, i.e. maximal with respect to the condition that it not contain any power of $\det W(y_1, \ldots, y_n)$. To simplify the discussion (but not the notation) we make use of the ring of fractions

$$S = k\{y_1, \ldots, y_n, 1/\det W(y)\}.$$

We then can use use the fact that a Δ-ideal $\mathfrak{p}$ of $k\{y_1, \ldots, y_n\}$ which maximal with respect to avoiding all powers of $\det W(y)$ corresponds to a maximal Δ-ideal $\mathfrak{m}$ of S. The later is not only easier to say, but also has nice properties.

Let $\eta_1, \ldots, \eta_n \in K$ be a fundamental system of solutions of $L(y) = 0$. To simplify notation we use vector notation

$$y = (y_1, \ldots, y_n) \qquad \text{and} \qquad \eta = (\eta_1, \ldots, \eta_n).$$

Let $\mathfrak{p}$ be the kernel of the substitution homomorphism

$$\begin{aligned}\mathfrak{p} = \ker : k\{y\} &\longrightarrow K,\\ y_i &\longmapsto \eta_i,\end{aligned}$$

and

$$\begin{aligned}\mathfrak{m} = \ker : k\{y, 1/\det W(y)\} &\longrightarrow K,\\ y_i &\longmapsto \eta_i.\end{aligned}$$

Proposition 4.2.4 *With the notation above, the following conditions are equivalent.*

1. $\mathfrak{p}$ *is a* Δ*-ideal that is maximal with respect to the condition that it not contain any power of* $\det W(y)$.
2. $\mathfrak{m}$ *is a maximal* Δ*-ideal.*
3. $k\{\eta, 1/\det W(\eta)\}$ *is* Δ*-simple.*
4. $k\langle\eta\rangle^{\Delta} = C$.

Proof. $1 \Leftrightarrow 2$ is Proposition **??**, $2 \Leftrightarrow 3$ is Proposition 3.11.5, and $3 \Rightarrow 4$ is Corollary 3.11.7. That leaves $4 \Rightarrow 3$.

Let

$$R = k\{\eta, 1/\det W(\eta)\} \qquad \text{and} \qquad K = \langle\eta\rangle.$$

We consider

$$K \otimes R.$$

This is a finitely generated ring over K (see Proposition 4.1.4). Suppose that $\mathfrak{a} \subset R$ is a proper Δ-ideal, we need to show that $\mathfrak{a} = (0)$. By Proposition 3.8.4

$$(K \otimes R)/(K \otimes \mathfrak{a}) \approx K \otimes (R/\mathfrak{a}) \neq 0.$$

Therefore $K \otimes \mathfrak{a}$ is a proper Δ-ideal of $K \otimes R$. Choose a maximal Δ-ideal $\mathfrak{m}$ with

$$K \otimes \mathfrak{a} \subset \mathfrak{m} \subset K \otimes R$$

and consider the canonical homomorphism

$$\pi \colon K \otimes R \to S = (K \otimes R)/\mathfrak{m}.$$

We denote the restrictions of π by

$$\pi_K \colon K \to S \qquad \text{and} \qquad \pi_R \colon R \to S.$$

Here we identify K and R with subrings of $K \otimes R$. Of course π_K is an isomorphism of K onto its image (K is a field after all). We could identify K with its image, however the argument might be clearer if we do not.

Let ξ be the image of $1 \otimes \eta$. Then

$$S = \pi_K(K)[\xi, 1/\det W(\xi)].$$

Note that S is finitely generated over $\pi_K(K)$ and Δ-simple (since $\mathfrak{m}$ is a maximal Δ-ideal), so, by Corollary 3.11.7,

$$\mathrm{qf}(S)^\Delta = \pi_K(K)^\Delta = C.$$

By Proposition 4.1.5 there is an invertible matrix

$$c \in GL_C(n)$$

with

$$\xi = \pi(\eta \otimes 1)\, c$$

Therefore

$$\pi_R(R) = k[\xi, 1/\det W(\xi)] = \pi_K(k[\eta, 1/\det \eta]).$$

This shows that

$$\pi_R \colon R \to \pi_K(k[\eta, 1/\det \eta]) \approx R.$$

is surjective. It also shows that the transcendence degree of R over k is the same as $\pi_R(R)$. By Proposition 3.13.1, π_R is an isomorphism and therefore $\mathfrak{a} = (0)$. **q.e.d**.

It is the last condition that is traditionally used in the definition of a Picard-Vessiot extension.

Definition 4.2.5 Let $\eta = (\eta_1, \ldots, \eta_n)$ be a fundamental system for L. We say that $k\langle\eta\rangle$ *has no new constants*, or η *introduces no new constants*, if

$$k\langle\eta\rangle^\Delta = C.$$

Proposition 4.2.6 *There is a fundamental system for L that introduces no new constants.*

Proof. In the proof of 4.2.2, choose $\mathfrak{p}$ maximal with respect to the condition that it not contain the Wronskian determinant $\det W(y)$. **q.e.d**.

We have used the assumption that C be algebraically closed in the last two propositions. If C were not algebraically closed we would have to replace Proposition 4.2.4(4) with

$4'$ K^Δ is algebraic over C.

The proof of that proposition still goes through. However Proposition 4.2.6 would be false. See Example 4.6.1 below. We could replace the condition "no new constants" with "no new transcendental constants". That would make Proposition 4.2.6 true. For simplicity, however, we continue to assume that C is algebraically closed.

4.3 Uniqueness

We continue to study the Δ-operator

$$L = \delta^n - a_{n-1}\delta^{n-1} - \cdots - a_0.$$

Proposition 4.3.1 *Suppose that η and ξ are two fundamental systems that introduce no new constants. Then*

$$k\{\eta, 1/\det W(\eta)\} \qquad \textit{and} \qquad k\{\xi, 1/\det W(\xi)\}$$

are isomorphic over k.

Proof. Let

$$R = k\{\eta, 1/\det W(\eta)\} \qquad \text{and} \qquad S = k\{\xi, 1/\det W(\xi)\},$$

and consider the tensor product

$$R \otimes S = R \otimes_k S.$$

Choose a maximal Δ-ideal $\mathfrak{m}$ of $R \otimes S$ and let

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

be the canonical Δ-homomorphism. Note that

$$\pi_R = \pi \,|\, R\colon R \to T \quad \text{and} \quad \pi_S = \pi \,|\, S\colon S \to T$$

are injective because R and S, by Proposition 4.2.4, are Δ-simple. But T is also Δ-simple and finitely generated over k, hence

$$\mathrm{qf}(T)^\Delta = k^\Delta = C.$$

By Proposition 4.1.5 there is an invertible matrix $c \in GL_C(n)$ with

$$\pi_S(\xi) = \pi_R(\eta)c.$$

Therefore

$$\operatorname{im} \pi_R = \operatorname{im} \pi_S.$$

Since π_R and π_S are both injective. R and S Δ–isomorphic. **q.e.d.**

4.4 Picard-Vessiot extensions

As before, we assume given a Δ-operator

$$L = \delta^n - a_{n-1}\delta^{n-1} - \cdots - a_0.$$

Definition 4.4.1 Let K be a Δ-extension field of k. We say that K is a *Picard-Vessiot extension (of k) for L* if

1. $K = k\langle\eta\rangle$ for some fundamental system,

2. $K^{\Delta} = C$.

We say that K is a *Picard-Vessiot extension* if there exists a linear homogeneous Δ-equation $L(y) = 0$ such that K is a Picard-Vessiot for L.

The second condition simply says that η introduces no new constants. We state the definition this way because this is the usual form found in the literature. Also this definition is valid even if C is not algebraically closed [12, Chapter VI]. Note that we define a *Picard-Vessiot extension for L*. This follows modern practice but was not present in the original definition. In [11] only the notion of Picard-Vessiot extension is defined.

Given L we can always find a Picard-Vessiot extension for L (Proposition 4.2.6) and it is unique up to Δ-isomorphism (Proposition 4.3.1).

Definition 4.4.2 Let K be a Picard-Vessiot extension. Then the group of all Δ-automorphisms of K over k is called the *Galois group* of K over k and is denoted by

$$\mathrm{Gal}(K/k).$$

The group operation is composition of automorphisms. In the next section we will give some examples. However first we want to show how the Galois group of Δ-automorphisms may be embedded into $\mathrm{GL}_C(n)$. This mapping is not canonical; we discuss this further in Section **??**.

Let K be a Picard-Vessiot extension for L and choose a fundamental system of solutions $\eta = (\eta_1, \ldots, \eta_n)$ with $K = k\langle\eta\rangle$. (It is this choice that makes our embedding non-canonical.) Let $\sigma \in \mathrm{Gal}(K/k)$, i.e. σ is a Δ-automorphism of K over k. Then

$$L(\sigma\eta_i) = \sigma(L(\eta_i)) = 0,$$

so $\sigma\eta_i$ is also a solution of $L(y) = 0$. Because σ is an automorphism,

$$W(\sigma\eta)) = \sigma(W(\eta)) \neq= 0.$$

Therefore $\sigma\eta$ is a also a fundamental system of solutions. By Proposition 4.1.5 there is a matrix

$$c(\sigma) \in \mathrm{GL}_C(n)$$

with

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

Proposition 4.4.3 *With the notation above,*

$$c\colon\ \mathrm{Gal}(K/k) \longrightarrow \mathrm{GL}_C(n)$$

is an injective homomorphism of groups.

Proof. We first show that c is a homomorphism. Let $\sigma, \tau \in \mathrm{Gal}(K/k)$. Recall that $c(\tau)$ is a matrix with coefficients in $C = k^{\Delta}$, so σ will leave that matrix fixed. Therefore

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

Now suppose that $c(\sigma) = 1$. Then

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

Thus σ leaves η fixed and therefore leaves all of K fixed, i.e. is the identity automorphism. **q.e.d**.

We can rewrite the formula

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

in a way that is sometimes more convenient. Notice that the coordinates of $c(\sigma)$ are constant so also we have

$$\sigma\eta^{(i)} = \eta^{(i)} c(\sigma).$$

for any $i \geq 0$. Therefore the equation can be written

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

4.5 Examples

In this section $k = \mathbb{C}(x)$ where $x' = 1$ unless otherwise specified.

Example 4.5.1 Consider the Δ-equation

$$y' - y = 0.$$

The order of this equation is $n = 1$ so a fundamental system consists of a single non-zero solution. We choose e^x. Then

$$K = k\langle e^x \rangle = k(e^x)$$

is a Picard-Vessiot extension for L. Any Δ-automorphism σ of K over k has the property

$$\sigma e^x = c(\sigma)e^x$$

for some $c(\sigma) \in \mathbb{C}$, $c(\sigma) \neq 0$. Because e^x is transcendental over k every complex number comes from a Δ-automorphism. Thus

$$\mathrm{Gal}(K/k) \approx \mathbb{C}^* = \mathrm{GL}_{\mathbb{C}}(1),$$

which is sometimes denoted by $\mathbf{G_m}$ and called the *multiplicative group of the line.*

Example 4.5.2 Consider the Δ-equation

$$y'' + \frac{1}{x}y' = 0.$$

This equation arose by differentiating the inhomogeneous equation

$$y' = \frac{1}{x}.$$

A fundamental system of solutions is

$$\eta = (1, \log x).$$

If $\sigma \in \mathrm{Gal}(K/k)$,

$$\sigma(1, \log x) = (1, \log x + k(\sigma) = (1, \log x) \begin{pmatrix} 1 & k(\sigma) \\ 0 & 1 \end{pmatrix},$$

for some $k(\sigma) \in \mathbb{C}$. Therefore

$$c(\sigma) = \begin{pmatrix} 1 & k(\sigma) \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_{\mathbb{C}}(2).$$

Again every element of $\mathbb{C}$ occurs as some $k(\sigma)$ so $\mathrm{Gal}(K/k)$ is isomorphic to the set of all matrices of the above form. Since

$$\begin{pmatrix} 1 & k_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & k_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & k_1 + k_2 \\ 0 & 1 \end{pmatrix}$$

this group is isomorphic to $\mathbb{C}$ with addition. It is sometimes denoted $\mathbf{G_a}$ and called the *additive group of the line*.

Example 4.5.3 Consider Airey's equation

$$y'' - xy = 0.$$

Let $\eta = (\eta_1, \eta_2)$ be a fundamental system for L. If $\sigma \in \mathrm{Gal}(K/k)$ then

$$\sigma(\eta_1, \eta_2) = (\eta_1, \eta_2) \begin{pmatrix} c_{11}(\sigma) & c_{12}(\sigma) \\ c_{21}(\sigma) & c_{22}(\sigma) \end{pmatrix}$$

so

$$c\colon \mathrm{Gal}(K/k) \longrightarrow \mathrm{GL}_{\mathbb{C}}(2).$$

We claim that the image is contained in $\mathrm{SL}_{\mathbb{C}}(2)$ (the special linear group consisting of matrices with determinant 1).

First observe that the Wronskian determinant $\det W(\eta)$ is a constant.

$$(\det W(\eta))' = (\eta_1\eta_2' - \eta_1'\eta_2)' = \eta_1'\eta_2' + \eta_1 x\eta_2 - x\eta_1\eta_2 - \eta_1'\eta_2' = 0.$$

Therefore $\det W(\eta) \in \mathbb{C}$ and is left fixed by every automorphism. As explained at the end of the previous section, we have

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

hence

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

It follows that $\det c(\sigma) = 1$.

It turns out that the image of c is $\mathrm{SL}_C(2)$ [16] but we will not prove that here.

Example 4.5.4 In this example we take $k = \mathbb{C}$ and consider a Δ-operator

$$L = \delta^n + a_{n-1}\delta^{n-1} + \cdots + a_0,$$

where $a_0, \ldots, a_{n-1} \in \mathbb{C}$. Thus the equation $L(y) = y$ has constant coefficients. If the auxiliary equation

$$X^n + a_{n-1}X^{n-1} + \cdots + a_0 = 0$$

has no repeated roots then a fundamental system of solutions is

$$e^{r_1 x}, \ldots, e^{r_n x},$$

where $r_1, \ldots, r_n$ are the roots. (See, for example, [26, Chapter 6].) Then $e^{r_i x}$ is a solution of

$$y' - r_i y = 0.$$

If $\sigma \in \mathrm{Gal}(K/k)$ then, as in Example 4.5.1,

$$\sigma e^{r_i x} = c_i(\sigma) e^{r_i x}.$$

Therefore

$$c\colon\ \mathrm{Gal}(K/k) \longrightarrow \begin{pmatrix} c_1(\sigma) & 0 & \cdots & 0 \\ 0 & c_2(\sigma) & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & c_n(\sigma) \end{pmatrix}.$$

Of course there may be relations between $c_1, \ldots, c_n$. In fact, if

$$\sum_{i=1}^{n} z_i r_i = 0,$$

where $z_1, \ldots, z_n \in Zset$, then

$$\prod_{i=1}^{n} c_i^{z_i} = 1.$$

Example 4.5.5 In the previous example, if the auxiliary equation has multiple roots then a fundamental system of solutions has the form

$$\begin{gathered} e^{r_1 x}, xe^{r_1 x}, \ldots, x^{m_1-1}e^{r_1 x}, \\ \vdots \\ e^{r_t x}, xe^{r_t x}, \ldots, x^{m_t-1}e^{r_t x}, \end{gathered}$$

where r_i has multiplicity m_i. Note that $\sigma \in \mathrm{Gal}(K/k)$ takes x to $x+k$ for some $k \in \mathbb{C}$. Then $c(\sigma)$ is the matrix with blocks

$$\begin{pmatrix} B_1 & & & \\ & B_2 & & 0 \\ & & \ddots & \\ & 0 & & B_t \end{pmatrix}$$

where each block is of the form (omitting σ)

$$B_i = \begin{pmatrix} c_i & k & k^2 & \ldots & k^{m_i-1} \\ & c_i & 2k & \ldots & (m_i-1)k^{m_i-2} \\ & & c_i & & \\ & 0 & & \ddots & \vdots \\ & & & & c_i \end{pmatrix}$$

However we can choose a different Δ-operator that gives the same Picard-Vessiot extension. For example

$$M = (\delta - r_1)^{m_1} \cdots (\delta - r_t)^{m_t}(\delta^2 - \delta).$$

In this case a fundamental system of solutions is

$$e^{r_1 x}, \ldots, e^{r_t x}, 1, x$$

and $c(\sigma)$ is

$$\left(\begin{array}{ccc:cc} c_1 & & & & \\ & \ddots & & & \\ & & c_t & & \\ \hdashline & & & 1 & k \\ & & & & 1 \end{array}\right)$$

4.6 If C is not algebraically closed

We have assumed that $C = k^\Delta$ is algebraically closed. We used that assumption in showing that, given a Δ-operator, there exists a unique Picard-Vessiot extension for that operator (Propositions 4.2.6 and 4.3.1). They would be false without that assumption. This is the main result of [30, Section 6, p. 816].

Example 4.6.1 Let

$$k = \mathbb{R}\langle i \sin 2x \rangle.$$

Using Seidenberg's notation, we set

$$a = \frac{i}{2} \sin 2x.$$

Then

1. $a' = i \cos 2x$,
2. $a'' = -4a$,
3. $a'^2 = -4a^2 - 1$.

Thus

$$k = \mathbb{R}(a)[a'],$$

where a is transcendental over $\mathbb{R}$ and a' is algebraic of degree 2 over $\mathbb{R}(a)$.

We first claim that $k^\Delta = \mathbb{R}$. Suppose that

$$c = A + Ba' \in k^\Delta,$$

where $A, B \in k(a)$. Then

$$\begin{aligned} 0 = c' &= \frac{dA}{da}\, a' + \frac{dB}{da}\, a'^2 + B\, a'' \\ &= \frac{dA}{da}\, a' - (4a^2 + 1)\frac{dB}{da} - 4aB. \end{aligned}$$

Therefore $dA/da = 0$ so $A \in \mathbb{R}$, and

$$(4a^2 + 1)\frac{dB}{da} + aB = 0.$$

Assume that $B \neq 0$ and write

$$B = (4a^2 + 1)^r \frac{C}{D}$$

where $r \in \mathbb{Z}$ and $C, D \in \mathbb{R}[a]$ are not divisible by (the irreducible polynomial) $4a^2 + 1$. From the equation above we have

$$\begin{gathered} (4a^2 + 1)\Big(r(4a^2 + 1)^{r-1} 8a \frac{C}{D} + (4a^2 + 1)^r \frac{D\frac{dC}{da} - C\frac{dD}{da}}{D^2}\Big) + \\ a(4a^2 + 1)^r \frac{C}{D} = 0, \end{gathered}$$

or

$$(4a^2 + 1)\Big(D\frac{dC}{da} - C\frac{dD}{da}\Big) + a(1 + 8r)CD = 0.$$

But this contradicts the condition that $a^2 + 1$ does not divide C or D. Therefore $B = 0$ and $c = A \in \mathbb{R}$.

We next claim that any solution η of the differential equation

$$y'' + y = 0$$

introduces new constants. In fact, we claim more. If

$$u = \frac{\eta'}{\eta},$$

then we claim that

$$k\langle u\rangle^{\Delta} \neq \mathbb{R}.$$

It is easy to see that

$$u' = -1 - u^2.$$

If $1 + u^2 = 0$ then $u = \pm i$ which is a new constant. So we may assume that $1 + u^2 \neq 0$. Let

$$c = \frac{a + a'u - au^2}{1 + u^2}.$$

Then

$$\begin{aligned} c' &= \frac{(1+u^2)\big(a' + a''u + a'u' - a'u^2 - 2auu'\big) - (a + a'u - au^2)2uu'}{(1+u^2)^2} \\ &= \frac{a' - 4au - a'(1+u^2) - a'^2u + 2au(1+u^2) + 2u(a + a'u - au^2)}{1+u^2} \\ &= 0. \end{aligned}$$

If $c \notin \mathbb{R}$ then c is a new constant, so we assume that $c \in \mathbb{R}$. The formula

$$c = \frac{a + a'u - au^2}{1 + u^2}$$

implies that

$$(c + a)u^2 - a'u + (c - a) = 0.$$

Using the quadratic formula we get

$$u = \frac{a' \pm \sqrt{a'^2 - 4(c+a)(c-a)}}{2(c+a)}.$$

This implies that

$$\sqrt{a'^2 - 4(c^2 - a^2)} = \sqrt{-1 - 4c^2} = i\sqrt{1 + 4c^2} \in k\langle u\rangle.$$

Since $\sqrt{1 + 4c^2} \in \mathbb{R}$, we have $i \in k\langle u\rangle$, which is a new constant.

However we may choose a Δ-extension field whose constants are algebraic over C, even a normal (Galois) extension. [8] developed a Picard-Vessiot theory for this case however was unable to get a bijection between all intermediate Δ-fields and (certain) subgroups of the Galois group. His approach appears to have been dropped.

[12, Chapter VII] also develops the theory without assuming that C is algebraically closed. He makes use of a universal Δ-field.

4.7 Summary of Picard-Vessiot theory

Rather than develop the Picard-Vessiot theory for ordinary Δ-operators, and then again for partial, we will simply state some of the main results of Picard-Vessiot theory here. All these results will be proved in a subsequent chapter in the more general case.

We let K be a Picard-Vessiot extension of k for the Δ-operator L and let $\eta = (\eta_1, \ldots, \eta_n)$ be a fundamental system. Then, as explained above,

$$c\colon \mathrm{Gal}(K/k) \longrightarrow \mathrm{GL}_C(n).$$

Theorem 4.7.1 *The image of c is an algebraic subgroup of* $\mathrm{GL}_C(n)$.

This means that the image is a subgroup (of course) and is closed in the Zariski topology. Thus the image is the set of invertible matrices that are solutions of a set of polynomial equations

$$\mathrm{im}\, c = \{g \in \mathrm{GL}_C(n) | P_i(g_1 1, \ldots, g_n n) = 0\}$$

for some set of polynomials

$$P_i \in k[X_{11}, \ldots, X_{nn}].$$

The Hilbert basis theorem asserts that a finite set of polynomials suffice, however that result is not needed here.

Theorem 4.7.2 *There is a bijective correspondence between intermediate Δ-fields*

$$k \subset E \subset K$$

and closed (in the Zariski topology) subgroups of $c(\mathrm{Gal}(K/k))$.

This is the first Fundamental Theorem of Galois Theory. It is trivial to check that K is a Picard-Vessiot extension of E so we may consider $\mathrm{Gal}(K/E)$, which is a subgroup of $\mathrm{Gal}(K/k)$.

Theorem 4.7.3 *Suppose that E is an intermediate Δ-field*

$$k \subset E \subset K$$

Then E is a Picard-Vessiot extension of k if and only if $\mathrm{Gal}(K/E)$ *is a normal subgroup of* $\mathrm{Gal}(K/k)$ *and if this is the case then*

$$\mathrm{Gal}(E/k) \approx \mathrm{Gal}(K/k)/\,\mathrm{Gal}(K/E).$$

This is the second Fundamental Theorem of Galois Theory. Similary to what happens in the Galois theory of algebraic equations, the solvability of the group is reflected in the type of solutions.

Theorem 4.7.4 *L has a fundamental system of Liouvillian solutions if and only if there is* $\mathrm{Gal}(K/k)$ *is solvable.*

If n is small, then we can list all possible closed subgroups of $\mathrm{GL}_C(n)$. We can then infer information about the solutions for each of the possible cases. This is the basis of the algorithm that was described in Chapter **??**.

4.8 Vector differential equations

Suppose that K is a Picard-Vessiot extension for the Δ-operator L and $\eta = (\eta_1, \ldots, \eta_n)$ is a fundamental system. It is sometimes more convenient to deal with the Wronskian matrix

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

The fundamental system is the first row of this matrix. Now consider a column. (We write η instead of η_i to simplify the notation.)

$$\begin{pmatrix} \eta \\ \eta' \\ \vdots \\ \eta^{(n-1)} \end{pmatrix}$$

The derivative of each coordinate is the next one lower except for the last which is

$$\eta^{(n-1)\prime} = a_0\eta + \ldots + a_{n-1}\eta^{(n-1)}.$$

In matrix form this is

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

The matrix on the right is called the *companion matrix* for the Δ-operator L. Denote it by A. Then we have the matrix equation

$$W(\eta)' = AW(\eta).$$

Often one introduces Δ-indeterminates $y_1, \ldots, y_n$ and considers the *column* vector

$$Y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

Then the equation (or system of equations)

$$Y' = AY$$

is called a *vector* Δ*-equation*. In this context, $L(y) = 0$ is called a *scalar* Δ*-equation*.

Of course, we can start with an arbitrary matrix A, not necessarily in the "companion" form given above, and try to solve the vector Δ-equation. If $k \neq C$ then we do not get anything new. The cyclic vector theorem says that we may make a change of (dependent) variables to change A to companion form, and from that we can recover a Δ-operator. For details, see [6].

It is the matrix equation

$$W(\eta)' = AW(\eta)$$

that we generalize in the next chapter. We will then continue studying Picard-Vessiot extensions for matrix Δ-equations.

Chapter 5

Matrix differential equations

In the previous chapter we investigated a linear homogeneous ODE (ordinary differential equation). For partial Δ-fields an analogue is a system of linear homogeneous PDE of finite linear dimension. This is point of view of [12, Chapter IV, Section 5, p. 150]. An alternative treatment is to use matrix equations as discussed in Section 4.8. It is that approach that we shall generalize in this chapter.

Throughout this chapter k is a Δ-field (either partial or ordinary) of characteristic 0 with algebraically closed field of constants $C = k^{\Delta}$. If K is any Δ-extension field of k, we denote by

$$\mathrm{GL}_K(n)$$

the *general linear group* consisting of invertible n by n matrices with entries in k, and by

$$\mathrm{Mat}_K(n)$$

the non-commutative ring of all n by n matrices with entries in K.

5.1 Logarithmic derivative

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. In this section K is a Δ-extension field K of k.

Definition 5.1.1 Let $A \in \mathrm{Mat}_K(n)$. For $\delta \in \Delta$, we let $\delta A \in \mathrm{Mat}_K(n)$ be the matrix formed by applying δ to each entry of A, i.e.

$$\delta \begin{pmatrix} A_{11} & \cdots & A_{1n} \\ \vdots & & \vdots \\ A_{n1} & \cdots & A_{nn} \end{pmatrix} = \begin{pmatrix} \delta A_{11} & \cdots & \delta A_{1n} \\ \vdots & & \vdots \\ \delta A_{n1} & \cdots & \delta A_{nn} \end{pmatrix}.$$

Since $\mathrm{Mat}_K(n)$ is not commutative, it is not a Δ-ring as we have defined it. And one must be careful about order when applying the product rule, quotient rule, etc. It is easy to check that

$$\delta(AB) = \delta AB + A\delta B,$$

not $\delta AB + \delta BA$, and

$$\delta(A^{-1}) = -A^{-1}\delta A A^{-1} \qquad \text{(if } A \text{ is invertible)}$$

Definition 5.1.2 If $\alpha \in \mathrm{GL}_K(n)$, then, for $\delta \in \Delta$,

$$\ell\delta\alpha = \delta\alpha\,\alpha^{-1} \in \mathrm{Mat}_K(n)$$

is called the *logarithmic derivative of α with respect to δ*.

Example 5.1.3 If $n = 1$ then, for $\alpha \in \mathrm{GL}_K(1) = K^*$,

$$\ell\delta\alpha = \frac{\delta\alpha}{\alpha}$$

is the logarithmic derivative of the element α with respect to δ.

More generally, if

$$\alpha = \begin{pmatrix} \alpha_1 & & 0 \\ & \ddots & \\ 0 & & \alpha_n \end{pmatrix}$$

is a diagonal matrix then

$$\ell\delta\alpha = \begin{pmatrix} \frac{\delta\alpha_1}{\alpha_1} & & 0 \\ & \ddots & \\ 0 & & \frac{\delta\alpha_n}{\alpha_n} \end{pmatrix}.$$

Example 5.1.4 The additive group K may be identified with the subgroup of $\mathrm{GL}_K(2)$ consisting of matrices of the form

$$\alpha = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}.$$

Then

$$\ell\delta\alpha = \begin{pmatrix} 0 & \delta a \\ 0 & 0 \end{pmatrix}.$$

So we may think of $\ell\delta$ as the mapping $\delta\colon K \to K$.

In both the above examples, $\ell\delta$ is a group homomorphism. In the first example $\ell\delta$ takes the multiplicative group K^* into the additive group K. In the second, it takes the additive group K into itself. However, in general, $\ell\delta$ is not a homomorphism. See Proposition 5.1.6 below.

Example 5.1.5 If $\eta_1, \ldots, \eta_n$ is a fundamental system for

$$L = \delta^n - a_{n-1}\delta^{n-1} - \cdots - a_0$$

then

$$\ell\delta\, W(\eta) = A = \begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & 0 & 1 \\ a_0 & a_1 & \ldots & a_{n-1} \end{pmatrix}$$

is the companion matrix of Section 4.8.

$\mathrm{Mat}_K(n)$ is actually the Lie algebra of the algebraic group $\mathrm{GL}_K(n)$. The bracket is

$$[A, B] = AB - BA.$$

Given an algebraic subgroup G of $\mathrm{GL}_K(n)$ defined over constants, the logarithmic derivative defines a mapping from G into its Lie algebra. For more information see [15, Section 1, p. 584]. We make use of the bracket notation, but not of any other property of Lie algebras.

The multiplicative group $\mathrm{GL}_K(n)$ acts on the additive group $\mathrm{Mat}_K(n)$ by conjugation.

$$\begin{aligned} \tau\colon \mathrm{GL}_K(n) \times \mathrm{Mat}_K(n) &\longrightarrow \mathrm{Mat}_K(n) \\ (\alpha, A) &\longmapsto \mathrm{Ad}_\alpha(A) = \alpha A \alpha^{-1}. \end{aligned}$$

This is called the *adjoint action* (of the algebraic group on its Lie algebra).

Proposition 5.1.6 *Let $\alpha, \beta \in \mathrm{GL}_K(n)$. Then, for each $\delta \in \Delta$,*

$$\ell\delta(\alpha\beta) = \ell\delta\alpha + \alpha\, \ell\delta\beta\, \alpha^{-1},$$

and

$$\ell\delta(\alpha^{-1}) = -\alpha^{-1}\, \ell\delta\alpha\, \alpha.$$

Proof. We compute

$$\begin{aligned} \ell\delta(\alpha\beta) &= \delta(\alpha\beta)(\alpha\beta)^{-1} = \delta\alpha\beta\beta^{-1}\alpha^{-1} + \alpha\delta\beta\beta^{-1}\alpha^{-1} \\ &= \ell\delta\alpha + \alpha\ell\delta\beta\alpha^{-1} \end{aligned}$$

and

$$\ell\delta(\alpha^{-1}) = \delta(\alpha^{-1})\, \alpha = -\alpha^{-1}\delta\alpha\alpha^{-1}\, \alpha = -\alpha^{-1}\, \ell\delta\alpha\, \alpha.$$

q.e.d.

In general, if a multiplicative group G acts on an additive group A and $f\colon G \to M$ satisfies

$$f(gh) = f(g) + g{\cdot}f(h),$$

then f is called a *crossed homomorphism*. Thus $\ell\delta$ is a crossed homomorphism from $\mathrm{GL}_K(n)$ to $\mathrm{Mat}_K(n)$. Of particular interest to us is the kernel of this crossed homomophism. Evidently

$$\ell\delta\alpha = \delta\alpha\alpha^{-1} = 0$$

if and only if $\delta\alpha = 0$, i.e. the entries of α are all constant with respect to δ. So $\ell\delta\alpha = 0$ for *every* $\delta \in \Delta$ if and only if the entries of α are constants.

Definition 5.1.7 The m-tuple

$$\ell\Delta\alpha = (\ell\delta_1\alpha, \ldots, \ell\delta_m\alpha) \in \mathrm{Mat}_K(n)^m$$

is called the *logarithmic derivative of* α.

We often use vector notation for an element of $\mathrm{Mat}_K(n)$, i.e.

$$\mathbf{A} = (A_1, \ldots, A_m).$$

The action of $\mathrm{GL}_K(n)$ on $\mathrm{Mat}_K(n)$ extends to $\mathrm{Mat}_K(n)^m$ coordinate-wise

$$\alpha\mathbf{A}\alpha^{-1} = (\alpha A_1\alpha^{-1}, \ldots, \alpha A_m\alpha^{-1}).$$

Proposition 5.1.8 *Let $\alpha, \beta \in \mathrm{GL}_K(n)$. Then*

$$\ell\Delta(\alpha\beta) = \ell\Delta\alpha + \alpha\,\ell\Delta\beta\,\alpha^{-1},$$

$$\ell\Delta(\alpha^{-1}) = -\alpha^{-1}\,\ell\Delta\alpha\,\alpha.$$

and, if $\alpha \in \mathrm{GL}_K(n)$, then

$$\ell\Delta\alpha = 0 \qquad \textit{if and only if} \qquad \alpha \in \mathrm{GL}_{K^\Delta}(n).$$

Corollary 5.1.9 *Let $\alpha, \beta \in \mathrm{GL}_K(n)$. Then*

$$\ell\Delta\alpha = \ell\Delta\beta$$

if and only if there exists $c \in \mathrm{GL}_{K^\Delta}(n)$ such that

$$\beta = \alpha c.$$

Proof. By the preceding proposition we have

$$\ell\Delta(\alpha^{-1}\beta) = -\alpha^{-1}\ell\Delta\alpha\alpha + \alpha^{-1}\ell\Delta\beta\alpha = 0$$

so

$$\alpha^{-1}\beta \in \mathrm{GL}_{K^\Delta}(n).$$

q.e.d.

Definition 5.1.10 The set of all $\mathbf{A} = (A_1, \ldots, A_m) \in \mathrm{Mat}_K(n)^m$ that satisfy the *integrability conditions*

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

is denoted by $\mathbf{I}_K(n)$.

Note that $\mathbf{I}_K(n)$ has no (a priori) structure other than that of subset of $\mathrm{Mat}_K(n)^m$. (It is not a vector space, as erroneously stated in [18, Definition 5.2].)

Proposition 5.1.11 *Let $\alpha \in \mathrm{GL}_K(n)$. Then*

$$\ell\Delta\alpha \in \mathbf{I}_K(n).$$

Proof. We compute

$$\begin{aligned}\delta_i(\ell\delta_j\alpha) - \delta_j(\ell\delta_i\alpha) &= \delta_i\delta_j(\alpha)\,\alpha^{-1} - \delta_j(\alpha)\,\alpha^{-1}\delta_i(\alpha)\alpha^{-1} \\ &\qquad - \delta_j\delta_i(\alpha)\,\alpha^{-1} + \delta_i(\alpha)\,\alpha^{-1}\delta_j(\alpha)\alpha^{-1} \\ &= -\ell\delta_j\alpha\,\ell\delta_i\alpha + \ell\delta_i\alpha\,\ell\delta_j\alpha \\ &= [\ell\delta_i\alpha,\, \ell\delta_j\alpha].\end{aligned}$$

q.e.d.

5.2 Existence

In Section 4.2 we showed the a Δ-operator has a fundamental system that does not introduce new constants. In this section we prove the analogous result for matrix equations. Another way of saying this is that $\ell\Delta$ is surjective, in the sense of the following proposition. Compare it with Proposition 4.2.2.

Proposition 5.2.1 *Let $\mathbf{A} \in \mathbf{I}_k(n)$. Then there exists a Δ-extension field K of k and $\alpha \in \mathrm{GL}_K(n)$ such that $\ell\Delta\alpha = \mathbf{A}$.*

Proof. Let $X = (X_{jk})_{1 \leq j,k \leq n}$ be indeterminates (not Δ-indeterminates) over k and consider

$$k[X] = k[(X_{j,k})_{1 \leq j,k \leq n}].$$

By Proposition 3.6.1 there is a unique structure of *ordinary* Δ-ring on $k[X]$ such that

$$\delta_i X = A_i X.$$

i.e.

$$\delta_i X_{jk} = \sum_l (A_i)_{jl} X_{lk}.$$

To show that $k[X]$ is a Δ-ring we need to prove that δ_i commutes with δ_j. Set

$$D = \delta_i \circ \delta_j - \delta_j \circ \delta_i$$

This is the trivial derivation on k and

$$DX = \delta_i(A_jX) - \delta_j(A_iX) = \delta_iA_jX + A_jA_iX - \delta_jA_iX - A_iA_jX = 0$$

because $\mathbb{A} \in \mathbf{I}_k(n)$. Thus D is trivial on $k[X]$ and hence δ_i and δ_j commute.

Thus $k[X]$ is a Δ-ring, it is an integral domain (even a polynomial algebra over k) and

$$\det X \neq 0$$

since X_{jk} are indeterminates (algebraically independent over k). Set $K = k(X)$. Then

$$X \in \mathrm{GL}_K(n)$$

and

$$\ell\delta_i X = A_i.$$

q.e.d.

We could have used a more direct proof involving Δ-ideals, as we did for Proposition 4.2.2, however the analogue of Lemma 4.2.1 is slightly more complicated for partial Δ-rings.

Just as in Section 4.2, we do not have uniqueness. We could choose any prime Δ-ideal $\mathfrak{p}$ of $k[X]$ that does not contain any power of $\det X$, let $K = \mathrm{qf}(k[X]/\mathfrak{p})$ and let α be the image of X in K. Then one also has

$$\ell\Delta\alpha = \mathbf{A}.$$

Alternatively we might consider the Δ-ring

$$k[X, \tfrac{1}{\det X}] = k[X, X^{-1}]$$

and consider a Δ-ideal $\mathfrak{m}$ of $k[X, X^{-1}]$. Again $K = \mathrm{qf}(k[X, X^{-1}]/m)$ and α is the image of X in K. Note that in both these cases

$$K = k(\alpha) = k\langle\alpha\rangle.$$

Compare the following with Proposition 4.2.4.

Proposition 5.2.2 *With the notation above, the following conditions are equivalent.*

1. $\mathfrak{p}$ *is a* Δ*-ideal that is maximal with respect to the condition that it not contain any power of* $\det X$*.*
2. $\mathfrak{m}$ *is a maximal* Δ*-ideal.*
3. $k[\alpha, \alpha^{-1}]$ *is* Δ*-simple.*
4. $k\langle\alpha\rangle^{\Delta} = C$*.*

Proof. $1 \Leftrightarrow 2$ is Proposition **??**, $2 \Leftrightarrow 3$ is Proposition 3.11.5, and $3 \Rightarrow 4$ is Corollary 3.11.7. That leaves $4 \Rightarrow 3$ and the proof is almost identical with that of Proposition 4.2.4. We sketch it here, see Proposition 4.2.4 to fill in the details.

Let

$$R = k\{\alpha, \alpha^{-1}\} = k[\alpha, \alpha^{-1}] \qquad \text{and} \qquad K = k\langle\alpha\rangle.$$

Suppose that $\mathfrak{a} \subset R$ is a proper Δ-ideal, we need to show that $\mathfrak{a} = (0)$. Choose a maximal Δ-ideal $\mathfrak{m} \subset K \otimes R$ containing $K \otimes \mathfrak{a}$ (which is proper by Proposition 3.8.4) and consider the canonical homomorphism

$$\pi\colon K \otimes R \to S = (K \otimes R)/\mathfrak{m}.$$

Identify K with its image in S. If β is the image of $1 \otimes \alpha$, then

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

Note that S is finitely generated over $\pi_K(K)$ and Δ-simple (since $\mathfrak{m}$ is a maximal Δ-ideal), so, by Corollary 3.11.7,

$$\operatorname{qf}(S)^\Delta = K^\Delta = C.$$

We have

$$\ell\Delta\alpha = \mathbf{A} = \ell\Delta\beta$$

so, by Corollary 5.1.9, there is an invertible matrix

$$c \in GL_C(n)$$

with

$$\beta = \alpha c$$

Therefore

$$\pi(R) = k[\beta, \beta^{-1}] = k[\alpha, \alpha^{-1}].$$

This shows that

$$\pi\colon R \to k[\alpha, \alpha^{-1}] \approx R.$$

is surjective. It also shows that the transcendence degree of R over k is the same as $\pi(R)$. By Proposition 3.13.1, π is an isomorphism and therefore $\mathfrak{a} = (0)$. **q.e.d.**

It is the last condition that is traditionally used in the definition of a Picard-Vessiot extension. Recall that a Δ-extension field K of k has *has no new constants* if $K^\Delta = C$.

Proposition 5.2.3 *Given $\mathbf{A} \in \mathbf{I}_k(n)$, there exists a Δ-extension field K of k and $\alpha \in \mathrm{GL}_K(n)$ such that*

1. $\ell\Delta\alpha = \mathbf{A}$,
2. $k\langle\alpha\rangle^\Delta = C$.

Proof. Choose $\mathfrak{p} \in k[X]$ maximal with respect to the condition that no power of $\det X$ is in $\mathfrak{p}$. Set $K = \mathfrak{k}[X]/\mathfrak{p}$ and let α be the image of X in K. **q.e.d.**

Note that

$$k\langle\alpha\rangle = k(\alpha)$$

because of the first condition. If $k\langle\alpha\rangle^\Delta = C$ we often say that α introduces *no new constants*.

As discussed at the end of Section 4.2 the assumption that C is algebraically closed is required for this proposition. See also Section 4.6.

5.3 Uniqueness

Compare the following with Proposition 4.3.1.

Proposition 5.3.1 *Let $\mathbf{A} \in \mathbf{I}_k(n)$. Suppose that $\alpha \in \mathrm{GL}_K(n)$ and $\beta \in \mathrm{GL}_L(n)$, where K and L are Δ-extension fields of k, satisfy*

1. *$\ell\Delta\eta = \mathbf{A} = \ell\Delta\beta$, and*
2. *$k\langle\alpha\rangle^\Delta = C = k\langle\beta\rangle^\Delta$.*

Then

$$k\{\alpha, \alpha^{-1}\} \qquad \textit{and} \qquad k\{\beta, \beta^{-1}\}$$

are isomorphic over k.

Proof. Let

$$R = k\{\alpha, \alpha^{-1}\} \qquad \text{and} \qquad S = k\{\beta, \beta^{-1}\},$$

and consider the tensor product

$$R \otimes S = R \otimes_k S.$$

Choose a maximal Δ-ideal $\mathfrak{m}$ of $R \otimes S$ and let

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

be the canonical Δ-homomorphism. Note that

$$\pi_R = \pi \,|\, R \colon R \to T \quad \text{and} \quad \pi_S = \pi \,|\, S \colon S \to T$$

are injective because R and S, by Proposition 5.2.2, are Δ-simple. But T is also Δ-simple and finitely generated over k, hence

$$\mathrm{qf}(T)^\Delta = k^\Delta = C.$$

By Corollary 5.1.9 there is an invertible matrix $c \in GL_C(n)$ with

$$\pi_S(\beta) = \pi_R(\alpha)c.$$

Therefore

$$\operatorname{im} \pi_R = \operatorname{im} \pi_S.$$

Since π_R and π_S are both injective. R and S Δ-isomorphic. **q.e.d.**

5.4 Picard-Vessiot extensions

Definition 5.4.1 Let K be a Δ-extension field of k. We say that K is a *Picard-Vessiot extension (of k)* if there exists $\alpha \in \mathrm{GL}_K(n)$ such that

1. $\ell\Delta\alpha = \mathbf{A} \in \mathrm{Mat}_k(n)$,
2. $K = k\langle\alpha\rangle$, and

3. $K^{\Delta} = C$.

The first condition says that α is an invertible solution of the system of matrix Δ-equations

$$\delta_i Y = A_i Y$$

where $A_1, \ldots, A_m$ are matrices with coefficients in k that satisfy the integrability conditions. The second condition is the same as

$$K = k(\alpha)$$

because $\ell\Delta\alpha \in \mathrm{Mat}_k(n)$. The third condition simply says that α introduces no new constants.

Note that our definition emphasizes the Δ-field K, not the system of Δ-equations. It is quite conceivable that K also is $k\langle\beta\rangle$ where $\beta \in \mathrm{GL}_K(r)$ and $\ell\Delta\beta \in \mathbf{I}_k(r)$.

Definition 5.4.2 Let K be a Picard-Vessiot extension. Then the group of all Δ-automorphisms of K over k is called the *Galois group* of K over k and is denoted by

$$\mathrm{Gal}(K/k).$$

The group operation is composition of automorphisms. The Galois group can be embedded into $\mathrm{GL}_C(n)$, however, not canonically. Let K be a Picard-Vessiot extension for L and choose a matrix $\alpha \in \mathrm{GL}_K(n)$ with $K = k\langle\alpha\rangle$ and $\ell\Delta\alpha \in I_k(n)$. (It is this choice that makes our embedding non-canonical.) Let $\sigma \in \mathrm{Gal}(K/k)$, i.e. σ is a Δ-automorphism of K over k. Then

$$\ell\Delta(\sigma\alpha) = \sigma(\ell\Delta\alpha) = \ell\Delta\alpha,$$

so, by Corollary 5.1.9, there is a matrix

$$c(\sigma) \in \mathrm{GL}_C(n)$$

with

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

Proposition 5.4.3 *With the notation above,*

$$c\colon\ \mathrm{Gal}(K/k) \longrightarrow \mathrm{GL}_C(n)$$

is an injective homomorphism of groups.

Proof. We first show that c is a homomorphism. Let $\sigma, \tau \in \mathrm{Gal}(K/k)$. Recall that $c(\tau)$ is a matrix with coefficients in $C = k^{\Delta}$, so σ will leave that matrix fixed. Therefore

$$\alpha c(\sigma\tau) = \sigma\tau(\alpha) = \sigma\big(\alpha c(\tau)\big) = \alpha c(\sigma)c(\tau).$$

Now suppose that $c(\sigma) = 1$. Then

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

Thus σ leaves α fixed and therefore leaves all of K fixed, i.e. is the identity automorphism. **q.e.d.**

In the next chapter we will prove the fundamental theorems of Galois theory. The following result is a consequence of the first fundamental theorem, however we need the result now and it is easy to prove.

Proposition 5.4.4 *Let $a \in K$. If $\sigma a = a$ for every $\sigma \in \mathrm{Gal}(K/k)$, then $a \in k$.*

Proof. We use a device that we have used several times before, in Propositions 4.2.4, 4.3.1, Proposition 5.2.2, and 5.3.1. Consider the tensor product

$$K \otimes_k K.$$

This ring is reduced (has no non-zero nilpotents) by [34, Corollary, p. 196]. Therefore no power of

$$d = a \otimes 1 - a \otimes a$$

is 0. Hence the ring of fractions

$$R = (K \otimes_k K)[1/d]$$

is not the 0 ring. Let $\mathfrak{m}$ be a maximal Δ-deal of R. Therefore

$$R/\mathfrak{m}$$

is Δ-simple. Let

$$\pi \colon R \to R/\mathfrak{m}$$

be the canonical homomorphism and define

$$\begin{aligned} &\pi_1 \colon K \to R/\mathfrak{m}, \qquad \pi_1(b) = \pi(b \otimes 1), \textit{and} \\ &\pi_1 \colon K \to R/\mathfrak{m}, \qquad \pi_1(b) = \pi(1 \otimes b). \end{aligned}$$

Both these mappings are injective (since K is a field). Also

$$\ell\Delta\pi_1(\alpha) = \pi_1(\ell\Delta\alpha) = \pi_2(\ell\Delta\alpha) = \ell\Delta\pi_2(\alpha),$$

since $\ell\Delta\alpha \in \mathrm{Mat}_k(n)$. By Corollary 5.1.9, there exists $c \in \mathrm{GL}(n)$ with entries in $(R/\mathfrak{m})^\Delta$ such that

$$\pi_2(\alpha) = \pi_1(\alpha)c.$$

It follows that

$$\pi_1(K) = \pi_2(K).$$

Let

$$\sigma \colon K \to K, \qquad \sigma = \pi_2^{-1} \circ \pi_1.$$

Then $\sigma \in \mathrm{Gal}(K/k)$, and

$$\pi_2(\sigma a - a) = \pi(a) - \pi_2(a) = \pi(a \otimes 1 - 1 \otimes a) = \pi(d) \neq 0.$$

q.e.d.

5.5 Examples

The next proposition show that the examples of Section 4.5 all apply here as well.

Proposition 5.5.1 *Suppose that k is an ordinary Δ-field and let K be a Δ-field extension of k. Then K is a Picard-Vessiot extension in the sense of Definition 4.4.1 if and only if it a Picard-Vessiot extension in the sense of Definition 5.4.1.*

Proof. In both definitions we must have $K^\Delta = k$. Suppose that K is a Picard-Vessiot extension in the sense of Definition 4.4.1 then there is a Δ-operator

$$L = \delta^n - a_{n-1}\delta^{n-1} - \cdots - a_0$$

and a fundamental system

$$\eta = (\eta_1, \ldots, \eta_n)$$

such that $K = k\langle\eta\rangle$ and $K^\Delta = C$. Set

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

Then

$$\ell\delta\alpha = A = \begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & 0 & 1 \\ a_0 & a_1 & \ldots & a_{n-1} \end{pmatrix}$$

is in $\mathrm{Mat}_k(n)$. Therefore K is a Picard-Vessiot extension in the sense of Definition 5.4.1.

Let $\alpha \in \mathrm{GL}_K(n)$ satisfy

1. $K = k\langle\alpha\rangle$, and
2. $\ell\delta\alpha = A \in \mathrm{Mat}_k(n)$.

Choose a maximal subset of the entries α_{ij} of α that are linearly independent over C, say

$$\eta = (\eta_1, \ldots, \eta_r).$$

Here r may be as large as n^2. Evidently

$$K = k\langle\eta_1, \ldots, \eta_r\rangle.$$

We would like to find a linear homogeneous Δ-equation with coefficients in k for which η is a fundamental system. This would prove that K is a Picard-Vessiot extension in the sense of Definition 4.4.1.

Finding a linear homogeneous Δ-equation for which η is a fundamental system is easy, simply take

$$L(y) = \det W(\eta, y) = \det \begin{pmatrix} \eta_1 & \dots & \eta_r & y \\ \eta_1' & \dots & \eta_r & y' \\ \vdots & & \vdots & \\ \eta_1^{(r} & \dots & \eta_r^{(r)} & y^{(r)} \end{pmatrix}.$$

Then $L(\eta_i) = 0$ since the determinant has equal columns. We claim that

$$M(y) = \frac{1}{\det W(\eta)} L(y)$$

has coefficients in k. To prove this we shall use Proposition 5.4.4.

Let $\sigma \in \mathrm{Gal}(K/k)$. Then, as seen in Proposition 5.4.3, there is a matrix $c \in \mathrm{Gal}_C(n)$ with

$$\sigma\alpha = \alpha c.$$

Because $\eta_1, \dots, \eta_r$ is a maximal subset of the entries of α that are linearly independent over C, there is a matrix $d \in \mathrm{GL}_C(r)$ with

$$\sigma\eta_j = \sum_i \eta_i d_{ij}.$$

Therefore

$$\sigma W(\eta) = W(\eta) d.$$

If we let σ act trivially on y we have

$$\sigma W(\eta, y) = W(\eta, y) \left(\begin{array}{ccc} & d & \vdots \\ & & 0 \\ \cdots & \cdots & \cdots \\ & 0 & \vdots \\ & & 1 \end{array} \right) = W(\eta, y) D$$

Therefore

$$\sigma M(y) = \frac{1}{\det(W(\eta) d)} \det(W(\eta, y) D) = M(y).$$

If follows, from Proposition 5.4.4, that $M(y)$ has coefficients in k. **q.e.d.**

An alternative proof uses the cyclic vector theorem [6] in the case k does not consist of constants alone and then ad hoc arguments if $k = C$.

Example 5.5.2 Suppose that K is a finite normal algebraic extension of k. Then K is a Picard-Vessiot extension of k. Let Γ be the Galois group of K over k. Choose $a_1, \dots, a_s$ with

$$K = k(a_1, \dots, a_s).$$

(In fact we can always choose $s = 1$ but we do not need to for this argument.) Let

$$\eta = (\eta_1, \dots, \eta_n)$$

be a maximal subset of

$$\{\gamma a_j \mid \gamma \in \Gamma, j = 1, \ldots, s\}$$

that is linearly independent over C. By Corollary 3.12.8 there is an n-tuple

$$\theta = (\theta_1, \ldots, \theta_n),$$

where $\theta_i \in \Theta$ has order $< i$, such that

$$\alpha = W_\theta(\eta) \in \mathrm{GL}_K(n).$$

For each $\gamma \in \Gamma$ and $j = 1, \ldots, n$,

$$\gamma\eta_j = \sum_{i=1}^{n} c_{ij}\eta_i$$

for some $c = (c_{ij}) \in \mathrm{GL}_C(n)$. It follows that

$$\gamma\alpha = \alpha c.$$

By Proposition 3.7.5, γ is a Δ-homomorphism, therefore

$$\gamma\ell\Delta\alpha = \ell\Delta(\gamma\alpha) = \ell\Delta(\alpha c) = \ell\Delta\alpha.$$

Each entry of $\ell\Delta\alpha$ is invariant under the Galois group Γ and hence is in k. I.e.

$$\ell\Delta\alpha \in \mathrm{Mat}_k(n)$$

so K is a Picard-Vessiot extension of k.

5.6 Constants of a certain tensor product

In this section K is a Picard-Vessiot extension of k. We fix a matrix $\alpha \in \mathrm{GL}_K(n)$ with

1. $\ell\Delta\alpha = \mathbf{A} \in \mathrm{Mat}_k(n)$,
2. $K = k\langle\alpha\rangle = k(\alpha)$, and
3. $K^\Delta = k^\Delta = C$.

Let

$$R = k\{\alpha\} = k[\alpha].$$

Eventually we shall show that R is independent of the choice of α, but we need to develop properties of R first.

Proposition 5.6.1 *R is Δ-simple.*

Proof. Proposition 5.2.2. **q.e.d.**

Some of the tools that we use are various tensor products

$$K \otimes_k K, \qquad K \otimes_k R \qquad \text{and} \qquad R \otimes_k R.$$

As we shall see, these all have similar properties, so our choice is based on convenience of the moment. Since K is a Δ-field, one might hope that $K \otimes_k K$ is a Δ-field, or at least an integral domain. However that is not the case.

Example 5.6.2 Let $k = \mathbb{C}(x)$ and $K = k(\sqrt{x})$. Then

$$(\sqrt{x} \otimes 1 - 1 \otimes \sqrt{x})(\sqrt{x} \otimes 1 + 1 \otimes \sqrt{x}) = x \otimes 1 - 1 \otimes x = 0.$$

It is precisely algebraic extensions that give rise to this phenomenon. By [34], $K \otimes K$ is an integral domain if k is (relatively) algebraically closed in K (but not a field).

Definition 5.6.3 Let K be a Picard-Vessiot extension of k. Then we define

$$D = D(K/k) = (K \otimes_k K)^{\Delta}.$$

This definition appears to come "out of the blue". In fact it is a very important "invariant" associated with a Picard-Vessiot extension. It turns out to be a Hopf algebra in a natural way, hence $\operatorname{Spec} D$ is a affine group scheme which turns out to be canonically isomorphic to $\operatorname{Gal}(K/k)$. We will discuss this in Section **??**.

Proposition 5.6.4 *With the notation above,*

$$D = (K \otimes_k K)^{\Delta} = (K \otimes_k R)^{\Delta} = (R \otimes_k R)^{\Delta}.$$

Proof. Let $c \in D$ and define

$$\mathfrak{b} = \{b \in R \mid (1 \otimes b)c \in K \otimes_k R\}.$$

This is the set of "denominators" of the right factor of c and is immediately seen to be an ideal. It is a Δ-ideal because c is a constant. It is non-zero since $K = \operatorname{qf}(R)$. However R is Δ-simple, therefore

$$\mathfrak{b} = R.$$

But then $1 \in \mathfrak{a}$ and $c = (1 \otimes 1)c \in K \otimes_k R$.

Similarly

$$\mathfrak{a} = \{a \in R \mid (a \otimes 1)c \in R \otimes_k R\}$$

equals R. Therefore

$$D \subset (R \otimes_k R)^{\Delta} \subset (K \otimes_k R)^{\Delta} \subset (K \otimes_k K)^{\Delta} = D.$$

q.e.d.

Suppose that $A, B \in \mathrm{Mat}_K(n)$. We then define

$$A \otimes B \in \mathrm{Mat}_{K \otimes_k K}(n)$$

by the formula

$$(A \otimes B)_{ij} = \sum_{k=1}^{n} A_{ik} \otimes B_{kj}.$$

Another way of writing this is

$$A \otimes B = \begin{pmatrix} A_{11} \otimes 1 & \dots & A_{1n} \otimes 1 \\ \vdots & & \vdots \\ A_{n1} \otimes 1 & \dots & A_{nn} \otimes 1 \end{pmatrix} \begin{pmatrix} 1 \otimes B_{11} & \dots & 1 \otimes B_{1n} \\ \vdots & & \vdots \\ 1 \otimes B_{n1} & \dots & 1 \otimes B_{nn} \end{pmatrix}$$

i.e.

$$A \otimes B = (A \otimes 1)(1 \otimes B)$$

but be careful,

$$A \otimes B \neq (1 \otimes B)(A \otimes 1).$$

From the first formula we get

$$\delta(A \otimes B) = \delta A \otimes B + A \otimes \delta B.$$

Also

$$\det(A \otimes B) = \det A \otimes \det B.$$

Therefore $A \otimes B$ is invertible if both A and B are, however

$$(A \otimes B)^{-1} \neq A^{-1} \otimes B^{-1}.$$

Proposition 5.6.5 *Let*

$$\gamma = \alpha^{-1} \otimes \alpha.$$

Then

$$\gamma \in \mathrm{Mat}_D(n).$$

Proof. For $\delta \in \Delta$,

$$\begin{aligned} \delta\gamma &= -\alpha^{-1}\delta\alpha\alpha^{-1} \otimes \alpha + \alpha^{-1} \otimes \delta\alpha \\ &= -\alpha^{-1}\ell\delta\alpha \otimes \alpha + \alpha^{-1} \otimes \ell\delta\alpha\alpha \\ &= 0 \end{aligned}$$

since $\ell\delta\alpha \in \mathrm{Mat}_k(n)$. **q.e.d.**

Proposition 5.6.6 $D = C[\gamma, \gamma^{-1}]$.

Proof. The preceding proposition says that γ has entries in D. γ^{-1} must also have entries in D (e.g. by Kramer's Rule). Therefore

$$C[\gamma, \gamma^{-1}] \subset D.$$

Observe that

$$1 \otimes \alpha = (\alpha \otimes 1)(\alpha^{-1} \otimes \alpha) = (\alpha \otimes 1)\gamma.$$

Therefore

$$K \otimes_k R = K \otimes_k k[\alpha, \alpha^{-1}] \subset (K \otimes 1)[\gamma, \gamma^{-1}].$$

Any element $c \in D$ can be written in the form

$$c = \sum_{i=1}^{r} (a_i \otimes 1) d_i$$

where $a_i \in K$ and $d_i \in C[\gamma, \gamma^{-1}]$. We may assume that $d_1, \ldots, d_r$ are linearly independent over $K \otimes 1$. For each $\delta \in \Delta$,

$$0 = \delta c = \sum_{i=1}^{r} (\delta a_i \otimes 1) d_i,$$

so $\delta a_i = 0$ for $i = 1, \ldots, r$. Hence $c \in C[\gamma, \gamma^{-1}]$. **q.e.d.**

In this section we choose α and constructed γ from it, so, a priori, the ring $C[\gamma, \gamma^{-1}]$ depends on the choice of α. However $D = (K \otimes_k K)^{\Delta}$ does not. Therefore, the preceding proposition shows that $C[\gamma, \gamma^{-1}]$ is also independent of the choice of α.

5.7 Picard-Vessiot ring

In this section K is a Picard-Vessiot extension of k. In the previous section, we fixed an element $\alpha \in \mathrm{GL}_K(n)$ with $K = k\langle\alpha\rangle = K(\alpha)$. The Δ-ring

$$R = k\{\alpha, \alpha^{-1}\} = k[\alpha, \alpha^{-1}]$$

played an important role. In this section we show that this ring is independent of the choice of α. To simplify the notation we write Gal rather than $\mathrm{Gal}(K/k)$. First we need a few preliminary results. The first proposition is reminiscent of the Wronskian condition (Proposition 3.12.7.

Proposition 5.7.1 *$a_1, \ldots, a_n \in K$ are linearly dependent over k if and only if*

$$\det(\sigma_i a_j) = 0, \qquad 1 \leq i, j \leq n,$$

for every choice of $\sigma_1, \ldots, \sigma_n \in \mathrm{Gal}$.

Proof. Suppose that $a_1, \ldots, a_n$ are linearly dependent over k, say

$$\sum_{j=1}^{n} k_j a_j = 0, \qquad k_j \in k.$$

For any $\sigma_1, \ldots, \sigma_n \in \mathrm{Gal}$,

$$\sum_{j=1}^{n} k_j \sigma a_j = 0,$$

so the columns of

$$\begin{pmatrix} \sigma_1 a_1 & \ldots & \sigma_1 a_n \\ \vdots & & \vdots \\ \sigma_n a_1 & \ldots & \sigma_n a_n \end{pmatrix}$$

are linearly dependent over k (and hence over K). Therefore the determinant of this matrix is 0.

For the converse, we use induction on n. The case $n = 1$ is trival. Let $\sigma_1, \ldots, \sigma_{n-1} \in \mathrm{Gal}$. If

$$\det(\sigma_i a_j) = 0, \qquad (1 \le i, j \le n-1)$$

then, by the induction hypothesis, $a_1, \ldots, a_{n-1}$ are linearly dependent over k and we are done. So we assume that

$$\det(\sigma_i a_j) \neq 0, \qquad (1 \le i, j \le n-1)$$

but

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

for every $\sigma \in \mathrm{Gal}$. The columns of the matrix are linearly dependent over K so there exist $b_1, \ldots, b_n \in K$, not all 0, with

$$\begin{aligned} b_n \sigma_i a_n &= \sum_{j=1}^{n-1} b_j \sigma_i a_j \qquad \text{for } i = 1, \ldots, n-1, \text{ and} \\ b_n \sigma a_n &= \sum_{j=1}^{n-1} b_j \sigma a_j. \end{aligned} \tag{5.7.1}$$

The first set of equations, in matrix form, is

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

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

For any $\tau \in \mathrm{Gal}$ we may successively set $\sigma = \tau^{-1}\sigma_i$, $i = 1, \ldots, n-1$, to get

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

Therefore

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

This implies that $\tau b_j = b_j$ for every $\tau \in \mathrm{Gal}$, therefore, by Proposition 5.4.4, $b_j \in k$. Since $b_1 = 1$, the last equation of (5.7.1), with $\sigma = \mathrm{id}$, gives

$$a_n = \sum_{j=1}^{n-1} b_j a_j.$$

q.e.d.

Definition 5.7.2 Let $a \subset K$. Then

$$k[\Theta]a$$

denotes the k-vector subspace of K generated by

$$\{L(a) \mid \text{where } L \in k[\Theta]\}.$$

In general $k[\Theta]a$ has infinite dimension, but we are interested in the case where the dimension is finite. If k is an ordinary Δ-field and $k[\Theta]a$ has dimension d, then

$$a, a', \ldots, a^{(d)}$$

are linearly dependent over k, i.e. a satisfies a linear homogeneous Δ-equation of order d. If k is a partial Δ-field, for *every* choice of $\theta_1, \ldots, \theta_{d+1} \in \Theta$,

$$\theta_1 a, \ldots, \theta_{d+1} a$$

are linearly dependent over k. So a satisfies an over-determined system of linear homogeneous Δ-equations.

Definition 5.7.3 By a *Picard-Vessiot element* of K is meant an element a of K such that $k[\Theta]a$ has finite dimension over k.

We will show that the set of all Picard-Vessiot elements is a Δ-ring and equals $\mathfrak{k}[\alpha, \alpha^{-1}]$. This will give a characterization of that ring which is independent of the choice of α.

Definition 5.7.4 Let $a \in K$. Then

$$C[\mathrm{Gal}]a$$

denotes the C-vector subspace of K generated by

$$\{\sigma a \mid \sigma \in \mathrm{Gal}\}.$$

In general $C[\mathrm{Gal}]a$ has infinite dimension, but we are interested in the case where the dimension is finite.

Lemma 5.7.5 *Let $a \in K$ and suppose that $C[\mathrm{Gal}]a$ has finite dimension over C with basis*

$$a_1, \ldots, a_n.$$

Then there is an n-tuple $\theta = (\theta_1, \ldots, \theta_n)$ of derivative operators such that

$$\alpha = (\theta_i a_j) \in \mathrm{GL}_K(n)$$

and

$$\ell\Delta\alpha \in \mathrm{Mat}_k(n).$$

Proof. α is a Wronskian of $a_1, \ldots, a_n$, the existence of which is Corollary 3.12.8. For each $\sigma \in \mathrm{Gal}(K/k)$,

$$\sigma\alpha = \alpha c$$

for some $c \in \mathrm{GL}_C(n)$ so

$$\sigma(\ell\Delta\alpha) = \ell\Delta(\sigma\alpha) = \ell\Delta(\alpha c) = \ell\Delta\alpha$$

hence, by Proposition 5.4.4,

$$\ell\Delta\alpha \in \mathrm{Mat}_k(n).$$

q.e.d.

Recall from Definition 5.6.3 that

$$D = (K \otimes K)^{\Delta}.$$

Proposition 5.7.6 *For $a \in K$ the following are equivalent.*

1. *a is a Picard-Vessiot element,*
2. *$k[\Theta]a$ has finite dimension over k.*
3. *$C[\mathrm{Gal}]a$ has finite dimension over C.*
4. *$1 \otimes a \in (K \otimes 1)[D]$.*

Proof. $1 \Leftrightarrow 2$ is Definition 5.7.3.

$2 \Rightarrow 3$. Suppose that $k[\Theta]a$ has dimension $n-1$. If $(\theta_1, \ldots, \theta_n)$ is any n-tuple of derivative operators then

$$\theta_1 a, \ldots, \theta_n a$$

are linearly dependent over k and therefore, by Proposition 5.7.1,

$$\det(\sigma_i \theta_j a) = 0 \qquad (1 \leq i, j \leq n)$$

for every choice of $\sigma_1, \ldots, \sigma_n \in \mathrm{Gal}$. By the Wronskian condition (Proposition 3.12.7),

$$\sigma_1 a, \ldots, \sigma_n a$$

are linearly dependent over C. Thus $C[\mathrm{Gal}]a$ has dimension no bigger than $n-1$.

$3 \Rightarrow 2$. Suppose that $C[\mathrm{Gal}]a$ has dimension $n-1$. Then, for any $\sigma_1, \ldots, \sigma_n \in \mathrm{Gal}$,

$$\sigma_1 a, \ldots, \sigma_n a$$

are linearly dependent over C. By Proposition 3.12.7

$$det(\theta_i \sigma_j a) = 0, \qquad 1 \leq i, j \leq n,$$

for every choice of $\theta_1, \ldots, \theta_n \in \Theta$. By Proposition 5.7.1

$$\theta_1 a, \ldots, \theta_n a$$

are linearly dependent over k. Thus $k[\Theta]a$ has dimension no bigger than $n-1$.

$3 \Rightarrow 4$. Let $a_1, \ldots, a_n$ be a basis of $C[\mathrm{Gal}]a$ with $a_1 = a$. Choose $\theta_1, \ldots, \theta_n \in \Theta$ satisfying the conditions of Lemma 5.7.5. Thus

1. $\alpha = (\theta_i a_j)$, $1 \leq i, j \leq n$,
2. $\alpha \in \mathrm{GL}_K(n)$,
3. $\ell\Delta\alpha \in \mathrm{Mat}_k(n)$.

By replacing α with $\sigma_1^{-1}\alpha$, we have that $\sigma_1 = \mathrm{id}$. Then

$$a = \alpha_{11}.$$

By Proposition 5.6.5

$$\gamma = \alpha^{-1} \otimes \alpha \in \mathrm{Mat}_D(n),$$

hence

$$1 \otimes a = 1 \otimes \alpha_{11} = ((\alpha \otimes 1)\gamma)_{11} \in (K \otimes 1)[D].$$

$4 \Rightarrow 3$. For any $\sigma \in \mathrm{Gal}$ we define

$$\overline{\sigma} \colon K \otimes_k K \to K$$

by the formula

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

Evidently $\overline{\sigma}$ is a Δ-homomorphism, and therefore

$$\overline{\sigma}(D) \subset K^{\Delta} = C.$$

Now suppose that

$$1 \otimes a = \sum_{i=1}^{n} (a_i \otimes 1) c_i \in (K \otimes 1)[D].$$

Then

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

Hence σa is in the C-vector space spanned by $a_1, \ldots, a_n$. **q.e.d.**

Proposition 5.7.7 *The set of all Picard-Vessiot elements of K is a Δ-ring containing k.*

Proof. This is immediate from Condition 4 of the previous proposition. **q.e.d.**

Definition 5.7.8 The Δ-ring of all Picard-Vessiot elements of K is called the Picard-Vessiot ring of K. We denote it by $P = P(K/k)$.

Proposition 5.7.9 *If $K = k(\alpha)$ where $\alpha \in \mathrm{GL}_K(n)$ and $\ell\Delta\alpha \in \mathrm{Mat}_k(n)$, then $k[\alpha, \alpha^{-1}]$ is the Picard-Vessiot ring of K.*

Proof. Let $R = k[\alpha, \alpha^{-1}]$. We know, by Proposition 5.6.5 that

$$\gamma = \alpha^{-1} \otimes \alpha \in D,$$

so

$$1 \otimes \alpha = (\alpha \otimes 1)\gamma \in (K \otimes 1)[D], \qquad \text{and}$$
$$1 \otimes \alpha^{-1} = (\alpha^{-1} \otimes 1)\gamma^{-1} \in (K \otimes 1)[D].$$

Therefore $R \subset P$.

By Proposition 5.6.6, $D = k[\gamma, \gamma^{-1}]$. Therefore we have

$$(K \otimes 1)[D] \subset K \otimes R \subset K \otimes P \subset (K \otimes 1)[D].$$

The last inclusion comes from Condition 4 of Proposition 5.7.6. It follows that

$$K \otimes R = K \otimes P$$

and therefore, by Proposition 3.8.3, $R = P$. **q.e.d.**

This proposition shows that the ring $k[\alpha, \alpha^{-1}]$ is independent of the choice of α.

Corollary 5.7.10 *P is Δ-simple and $D = (P \otimes P)^{\Delta}$.*

Proof. Propositions 5.6.1 and 5.6.4. **q.e.d.**

Chapter 6

Fundamental theorems

In this chapter we prove the main theorems about Picard-Vessiot extensions. In the first section we discuss a basic isomorphism, which should be thought of as the main structure theorem for Picard-Vessiot extensions. Next we recall the definition of a linear algebraic group. Our approach is classical, in Chapter ??? we shall discuss the scheme-theoretic approach. Next we show that the Galois group of a Picard-Vessiot extension is a linear algebraic group. After this we prove the two fundamental theorems of Galois theory.

Throughout this chapter (and this book), k is a Δ-field of characteristic 0 with algebraically closed field of constants $C = k^{\Delta}$. K is a Picard-Vessiot extension of k (Section **??**). The Galois group of all Δ-automorphisms of K over k is denoted by

$$\mathrm{Gal} = \mathrm{Gal}(K/k).$$

As in Section **??**,

$$D = D(K/k) = (K \otimes_k K)^{\Delta}.$$

As in Section **??**

$$P = P(K/k)$$

is the Picard-Vessiot ring of K.

6.1 The main isomorphism

The main result of this section is perhaps the most important theorem about Picard-Vessiot theory. Later we will use it to show that Picard-Vessiot theory is a special case of both Hopf-Galois theory and the Galois theory of categories.

Recall that Recall that, by Proposition **??**,

$$D = (K \otimes_k K)^{\Delta} = (P \otimes_k P)^{\Delta}.$$

Therefore we may define a Δ-homomorphism

$$\phi\colon P \otimes_C D \longrightarrow P \otimes_k P$$

by

$$\phi(a \otimes_C d) = (a \otimes_k 1)d.$$

(Contrary to normal usage, we have put subscripts $\otimes$ to emphasize the base field.) The goal of this section is to show that ϕ is an isomorphism.

Lemma 6.1.1 *ϕ is injective.*

Proof. Let $a \in P \otimes_C D \neq 0$ be in the kernel of ϕ. We may write

$$a = \sum_{i=1}^{n} a_i \otimes_C d_i$$

where $a_p \in P$ and $d_i \in D$. Among all non-zero elements of the kernel we choose one with shortest representation in the above form, i.e. with n minimal. This implies that $d_1, \ldots, d_n$ are linearly independent over C and therefore $1 \otimes_C d_1, \ldots, 1 \otimes_C d_n$ are linearly independent over $R \otimes_C 1$.

For each $\delta \in \Delta$

$$\delta a = \sum_{i=1}^{n} \delta a_i \otimes_C d_i$$

is also in the kernel. And so is

$$a_n \delta a - \delta a_n a = \sum_{i=1}^{n-1} (a_n \delta a_i - a_i \delta a_n) \otimes_c d_i.$$

But this is shorter and therefore must be 0. Hence

$$a_n \delta a_i - a_i \delta a_n = 0 \qquad \text{for all } i = 1, \ldots, n \text{ and } \delta \in \Delta.$$

Therefore

$$c_i = \frac{a_i}{a_n} \in K^{\Delta} = C$$

and

$$a = \sum_{i=1}^{n} \Big(a_n c_i \otimes_C d_i \Big) = a_n \otimes_C \Big(\sum_{i=1}^{n} c_i d_i \Big) = a_n \otimes_C d.$$

By Proposition **??**, P is Δ-simple so

$$1 \in [a_n],$$

i.e. there is a linear differential operator $L \in R[\Theta]$ with

$$1 = L(a_n).$$

But then

$$1 \otimes_C d = L(a_n \otimes_C d) \in \ker \phi.$$

Since $\phi(1 \otimes_C d) = d$, $d = 0$ and therefore $a = 0$. **q.e.d.**

Theorem 6.1.2 *The Δ-homomorphism*

$$\begin{aligned}\phi\colon R \otimes_C D &\longrightarrow P \otimes_k P\\ a \otimes_C d &\longmapsto (a \otimes_k 1)\, d\end{aligned}$$

is an isomorphism.

Proof. By the lemma, ϕ is injective. To prove the theorem we need to show that

$$P \otimes_k P = (P \otimes_k 1)[D].$$

Suppose that $K = k(\alpha)$ where $\alpha \in \mathrm{GL}_K(n)$ and $\ell\Delta\alpha \in \mathrm{Mat}_k(n)$. Then, by Proposition **??**,

$$P = k[\alpha, \alpha^{-1}] = k[\alpha, \tfrac{1}{\det \alpha}]$$

and, if $\gamma = \alpha^{-1} \otimes_k \alpha$, then

$$D = k[\gamma, \gamma^{-1}] = k[\gamma, \tfrac{1}{\det \gamma}].$$

Also, by ???,

$$\tfrac{1}{\det \gamma} = \det \alpha \otimes_k \tfrac{1}{\det \alpha}.$$

Therefore

$$1 \otimes_k \alpha = (\alpha \otimes_k 1)\gamma \in (P \otimes_k 1)[D]$$

and

$$1 \otimes_k \tfrac{1}{\det \alpha} = \left(\tfrac{1}{\det \alpha} \otimes_k 1\right) \tfrac{1}{\det \gamma}.$$

q.e.d.

6.2 Algebraic groups

In this section we give a quick review of definition of an algebraic group.

TO DO

6.3 The Galois group

In this section K is a Picard-Vessiot extension of k. As before, $C = k^\Delta$ is algebraically closed. We start with a choice of fundamental matrix α, thus

1. $\alpha \in \mathrm{GL}_K(n)$,
2. $\ell\Delta\alpha \in \mathbf{I}_k(n)$,
3. $K = k(\alpha)$,
4. $K^\Delta = C$.

Then there is a injective homomorphism

$$\begin{aligned} c\colon \operatorname{Gal}(K/k) &\longrightarrow \mathrm{GL}_C(n) \\ \sigma &\longmapsto \alpha^{-1}\sigma\alpha. \end{aligned}$$

Proposition ??? asserts that c is an injective homomorphism. Let

$$G = \operatorname{im} c = c(\operatorname{Gal}(K/k)) \subset \mathrm{GL}_C(n).$$

The goal of this section is to show that the image of G is an algebraic subgroup of $\mathrm{GL}_C(n)$, i.e. is the intersection with $\mathrm{GL}_C(n)$ of a closed set in the Zariski topology. In Section ??? we shall get a more intrinsic description of $\operatorname{Gal}(K/k)$, one that is independent of the choice of α.

Recall from Section 5.6 that we defined

$$D = D(K/k) = (K \otimes_k K)^{\Delta}.$$

In Proposition 5.6.6 we proved that

$$D = C[\gamma, \gamma^{-1}] = C[\gamma, \tfrac{1}{\det \gamma}].$$

where $\gamma = \alpha^{-1} \otimes \alpha$, i.e.

$$\gamma_{ij} = \sum_{k=1}^{n} (\alpha^{-1})_{ik} \otimes \alpha_{kj}.$$

Let $X = (X_{ij})_{1 \le i,j \le n}$ be a family of indeterminates over C and consider the substitution homomorphism

$$\begin{aligned} \phi\colon c[X] &\longrightarrow C[\gamma] \\ X_{ij} &\longmapsto \gamma_{ij} \end{aligned}$$

and set $\mathfrak{a} = \ker \phi$. Although we will not make use of the fact, $\mathfrak{a}$ is a radical ideal because $C[\gamma] \subset K \otimes_k K$, which is a reduced ring by [34].

Theorem 6.3.1 *G is an algebraic subgroup of $\mathrm{GL}_C(n)$ defined by $\mathfrak{a}$, i.e.*

$$G = \{g \in \mathrm{GL}_C(n) \mid P(g) = 0 \quad \textit{for every } P \in \mathfrak{a}\}.$$

Proof. Assume that $g \in \mathrm{GL}_C(n)$ satisfies $P(g) = 0$ for every $P \in \mathfrak{a}$ and let

$$\begin{aligned} \psi\colon C[X] &\longrightarrow C \\ X &\longmapsto g \end{aligned}$$

be the substitution homomorphism. By hypothesis, $\mathfrak{a} \subset \ker \psi$. Therefore there is a homomorphism $\overline{\sigma}$ that makes the following diagram commute.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker\psi & \longrightarrow & C[X] & \xrightarrow{\psi} & C & \longrightarrow & 0 \\ & & \uparrow & & \| & & \uparrow{\scriptstyle \overline{\sigma}} & & \\ 0 & \longrightarrow & \mathfrak{a} & \longrightarrow & C[X] & \xrightarrow{\phi} & C[\gamma] & \longrightarrow & 0 \end{array}$$

Evidently $\gamma \mapsto g$. Since g is invertible, $\overline{\sigma}$ extends to

$$\overline{\sigma}\colon C[\gamma, \gamma^{-1}] = D \to C.$$

We now use Proposition ??? to define a Δ-homomorphism

$$\sigma\colon K \to K$$

by

$$\begin{array}{rccccl} \sigma\colon K & \longrightarrow & K \otimes_k K & \approx & K \otimes_C D & \longrightarrow K \\ a & \longmapsto & 1 \otimes a & & a \otimes d & \longmapsto a\psi(d) \end{array}$$

Note that, at this stage of the argument, we do not know that σ is an automorphism of K, i.e. we do not know that σ is surjective. Nonetheless we can compute $\sigma(\alpha)$.

$$\begin{array}{ccccc} K & \longrightarrow & K \otimes_k K & \longrightarrow & K \otimes_C D \longrightarrow K \\ \alpha & \longmapsto & 1 \otimes_k \alpha & \longmapsto & \alpha \otimes_C \gamma \longmapsto \alpha\psi(\gamma) = \alpha g. \end{array}$$

It follows that σ is surjective so that $\sigma \in \mathrm{Gal}(K/k)$ and $c(\sigma) = g$.

Conversely assume that $\sigma \in \mathrm{Gal}(K/k)$ and let $g = c(\sigma)$. We must show that $P(g) = 0$ for every $P \in \mathfrak{a}$. Define

$$\begin{array}{rcl} \overline{\sigma}\colon K \otimes_k K & \longrightarrow & K \\ a \otimes_k b & \longmapsto & a\sigma b. \end{array}$$

Then

$$\overline{\sigma}(\gamma) = \overline{\sigma}(\alpha^{-1} \otimes_k \alpha) = \alpha^{-1}\sigma\alpha = c(\sigma) = g.$$

For any $P \in \mathfrak{a}$, $P(\gamma) = 0$ and therefore

$$0 = \overline{\sigma}(P(\gamma)) = P(\overline{\gamma}) = P(g).$$

q.e.d.

Bibliography

[1] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass., 1969. MR0242802 (39 #4129)

[2] A. Baider and R. C. Churchill, On monodromy groups of second-order Fuchsian equations, SIAM J. Math. Anal. **21** (1990), no. 6, 1642–1652. MR1075596 (92d:33034)

[3] N. Bourbaki, *Algebra. II. Chapters 4–7*, Translated from the French by P. M. Cohn and J. Howie, Springer, Berlin, 1990. MR1080964 (91h:00003)

[4] N. Bourbaki, *Commutative algebra. Chapters 1–7*, Translated from the French, Reprint of the 1989 English translation, Springer, Berlin, 1998. MR1727221 (2001g:13001)

[5] R. C. Churchill, Two generator subgroups of $\mathrm{SL}(2, \mathbf{C})$ and the hypergeometric, Riemann, and Lamé equations, J. Symbolic Comput. **28** (1999), no. 4-5, 521–545. MR1731936 (2002a:34131)

[6] R. C. Churchill and J. J. Kovacic, Cyclic vectors, in *Differential algebra and related topics (Newark, NJ, 2000)*, 191–218, World Sci. Publ., River Edge, NJ. MR1921700 (2003h:12007)

[7] E. A. Coddington and N. Levinson, *Theory of ordinary differential equations*, McGraw-Hill Book Company, Inc., New York, 1955. MR0069338 (16,1022b)

[8] M. P. Epstein, On the theory of Picard-Vessiot extensions, Ann. of Math. (2) **62** (1955), 528–547. MR0072868 (17,343a)

[9] I. Kaplansky, *An introduction to differential algebra*, Second edition, Hermann, Paris, 1976. MR0460303 (57 #297)

[10] W. F. Keigher, Prime differential ideals in differential rings, in *Contributions to algebra (collection of papers dedicated to Ellis Kolchin)*, 239–249, Academic Press, New York. MR0485806 (58 #5610)

[11] E. R. Kolchin, Algebraic matric groups and the Picard-Vessiot theory of homogeneous linear ordinary differential equations, Ann. of Math. (2) **49** (1948), 1–42. MR0024884 (9,561c) reprinted in [14].

[12] E. R. Kolchin, *Differential algebra and algebraic groups*, Academic Press, New York, 1973. MR0568864 (58 #27929)

[13] E. R. Kolchin, Constrained extensions of differential fields, Advances in Math. **12** (1974), 141–170. MR0340227 (49 #4982) reprinted in [14].

[14] E. Kolchin, *Selected works of Ellis Kolchin with commentary*, Amer. Math. Soc., Providence, RI, 1999. MR1677530 (2000g:01042)

[15] J. Kovacic, The inverse problem in the Galois theory of differential fields, Ann. of Math. (2) **89** (1969), 583–608. MR0244218 (39 #5535)

[16] J. J. Kovacic, An algorithm for solving second order linear homogeneous differential equations, J. Symbolic Comput. **2** (1986), no. 1, 3–43. MR0839134 (88c:12011)

[17] J. J. Kovacic, The differential Galois theory of strongly normal extensions, Trans. Amer. Math. Soc. **355** (2003), no. 11, 4475–4522 (electronic). MR1990759 (2004i:12008)

[18] J. J. Kovacic, Geometric characterization of strongly normal extensions, Trans. Amer. Math. Soc. **358** (2006), no. 9, 4135–4157 (electronic). MR2219014

[19] S. Lang, *Algebra*, Revised third edition, Springer, New York, 2002. MR1878556 (2003e:00003)

[20] D. McCullough, *Exceptional Subgroups of* $\mathrm{SL}(2, F)$, University of Oklahoma, 2005-06, preprint.

[21] A. R. Magid, *Lectures on differential Galois theory*, Amer. Math. Soc., Providence, RI, 1994. MR1301076 (95j:12008)

[22] H. Matsumura, *Commutative ring theory*, Translated from the Japanese by M. Reid, Second edition, Cambridge Univ. Press, Cambridge, 1989. MR1011461 (90i:13001)

[23] B. H. Matzat and M. van der Put, Iterative differential equations and the Abhyankar conjecture, J. Reine Angew. Math. **557** (2003), 1–52. MR1978401 (2004d:12011)

[24] K. Okugawa, Basic properties of differential fields of an arbitrary characteristic and the Picard-Vessiot theory, J. Math. Kyoto Univ. **2** (1962/1963), 295–322. MR0155820 (27 #5754)

[25] E. G. C. Poole, *Introduction to the theory of linear differential equations*, Dover, New York, 1960. MR0111886 (22 #2746)

[26] E. D. Rainville, P. E. Bedient and R. E. Bedient, *Elementary differential equations*, Eighth edition, Prentice Hall, Upper Saddle River, NJ, 1997. MR1442258

[27] J. F. Ritt, *Differential equations from the algebraic standpoint*, Colloquium Publications, Volume 14, American Mathematical Society, Providence, RI, 1932.

[28] L. A. Rubel, A survey of transcendentally transcendental functions, Amer. Math. Monthly **96** (1989), no. 9, 777–788. MR1033345 (91b:12010)

[29] T. Scanlon and Model theory and differential algebra, in *Differential algebra and related topics (Newark, NJ, 2000)*, 125–150, World Sci. Publ., River Edge, NJ. MR1921697 (2003g:03062)

[30] A. Seidenberg, Contribution to the Picard-Vessiot theory of homogeneous linear differential equations, Amer. J. Math. **78** (1956), 808–818. MR0081897 (18,463c)

[31] W. Y. Sit, The Ritt-Kolchin theory for differential polynomials, in *Differential algebra and related topics (Newark, NJ, 2000)*, 1–70, World Sci. Publ., River Edge, NJ. MR1921694 (2003g:12010)

[32] T. A. Springer, *Linear algebraic groups*, Second edition, Birkhäuser Boston, Boston, MA, 1998. MR1642713 (99h:20075)

[33] M. van der Put and M. F. Singer, *Galois theory of linear differential equations*, Springer, Berlin, 2003. MR1960772 (2004c:12010)

[34] O. Zariski and P. Samuel, *Commutative algebra. Vol. 1*, Corrected reprinting of the 1958 edition, Springer, New York, 1975. MR0384768 (52 #5641)

Index