Introduction to Differential Galois Theory

Phyllis J. Cassidy
Richard C. Churchill
Jerald J. Kovacic
William Sit

September 16, 2006

Contents

Chapter 1

Differential rings

In this chapter we record some basic facts from differential algebra. The most comprehensive reference for this material is Kolchin's book (1973). Other references are Kaplansky (1976), Magid (1994) and van der Put and Singer (2003). 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 1.10 and 1.2 we discuss some consequences of this assumption. See also Proposition 1.10.2 and Example 1.10.3.

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.

1.1 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 1.1.1 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 1.1.2 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 1.1.3 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 1.1.4 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 1.1.5 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 1.1.6 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 1.1.7 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 1.1.8 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*.

1.2 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 1.2.1 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 1.6.1, below, to an infinite set of indeterminates), however whenever these appear (in examples only) we assume that they are given the trivial derivation.

Proposition 1.2.2 *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. □

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

Example 1.2.3 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 Okugawa (1962/1963) and more recently by Matzat and van der Put (2003). We will not pursue that theory here.

1.3 Linear Δ-operators

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

Definition 1.3.1 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 1.3.2 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 1.3.3 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 1.3.4 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 ???.

1.4 Δ-subrings and Δ-extensions

Definition 1.4.1 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 1.10.3 why it is useful to restrict our rings to be Ritt algebras.

Definition 1.4.2 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 1.4.3 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 1.9), 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 1.12.

Proposition 1.4.4 *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. □

Corollary 1.4.5 *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 $R = K$. □

1.5 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, Lang (2002, 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 1.5.1 *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. □

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.

1.6 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 1.6.3 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 1.1.5.

Proposition 1.6.1 *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 Bourbaki (1990, 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. □

If $m = \operatorname{card} \Delta > 1$ (partial Δ-fields) the situation is made more complicated by the requirement that the derivations commute. See Example 1.1.8. 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 1.6.2 *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 Bourbaki (1990, 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 $L(x)$. □

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 1.6.3 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 $K[x]$.

1.7 Δ-ideals and Δ-homomorphisms

Definition 1.7.1 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 1.7.2 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 1.7.3 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 1.7.4 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 1.7.5 *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 1.6.2 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. □

Proposition 1.7.6 *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 $\delta a \in \ker\phi$. □

Proposition 1.7.7 *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. □

Using this proposition we can give an alternate proof of Proposition 1.7.5. Indeed ϕ (of Proposition 1.7.5) has kernel (0), which is a Δ-ideal.

Proposition 1.7.8 *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 $\delta a \in \mathfrak{a}$. □

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

Definition 1.7.9 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 $s \in S$.

1.8 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 Zariski and Samuel (1975, 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 Atiyah and Macdonald (1969, p. 24–31) or Lang (2002, 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 Atiyah and Macdonald (1969, 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

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

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

Proposition 1.8.1 *$R \otimes S$ 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

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

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. $\square$

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 1.8.2 *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*

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

are injective.

Proof. The first statement is Lang (2002, 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 $i = 1, \ldots, n$. □

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 **??**.

Proposition 1.8.3 *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, $\tau \in \Sigma$. □

The following proposition is Zariski and Samuel (1975, Theorem 35, p. 184).

Proposition 1.8.4 *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 1.8.5 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

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

1.9 Δ-polynomials

Definition 1.9.1 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 1.9.2 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 1.9.3 Euler's gamma function

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

is Δ-transcendental (Rubel, 1989).

Example 1.9.4 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 $\mathbb{C}(x)$. Rubel (1989) 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 1.9.5 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 1.9.6 *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 1.6.1, 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

$$\delta\delta' X_{\theta j} = \delta X_{\delta'\theta j} = X_{\delta\delta'\theta j} = X_{\delta'\delta\theta j} = \delta' X_{\delta\theta j} = \delta'\delta X_{\theta j}.$$

□

Definition 1.9.7 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 1.9.8 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 $s(P)$.

1.10 Radical and prime Δ-ideals

Δ-rings are rarely Noetherian.

Example 1.10.1 Ritt (1932, 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,

$$y^{(n)}y^{(n+1)} = \sum_{i=1}^{n-1} \sum_{j=0}^{t} A_{ij} \left(y^{(i)}y^{(i+1)}\right)^{(j)} \tag{1.10.1}$$

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 1.10.1, 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 Kolchin (1973, p. 122). However our assumption that R is a Ritt algebra (an algebra over $\mathbb{Q}$) permits us to make a simplification.

Proposition 1.10.2 *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 $\delta a \in \sqrt{\mathfrak{a}}$. □

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 1.10.3 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 1.10.4 *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 $[ab]$. □

Proposition 1.10.5 *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 $a \in \sqrt{[T]}$. □

Proposition 1.10.6 *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. □

Corollary 1.10.7 *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. □

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 1.10.8 *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. □

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 Sit (2002).

1.11 Maximal Δ-ideals

Definition 1.11.1 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 1.11.2 As in Example 1.7.2, 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 1.11.3 *Let $\mathfrak{m}$ be a maximal Δ-ideal of R. Then $\mathfrak{m}$ is prime.*

Proof. Proposition 1.10.6 where $\Sigma = \{1\}$. □

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 1.11.4 A Δ-ring R is said to be *Δ-simple* if it has no proper non-zero Δ-ideal.

Proposition 1.11.5 *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 $\mathfrak{m}$. □

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 1.11.6 *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 1.4.4, we need only show that c is algebraic over k. Suppose not, so c is transcendental over k. We know (Atiyah and Macdonald, 1969, 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. □

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 Kolchin (1973, 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 1.11.7 *Assume that $C = k^\Delta$ is algebraically closed. If R is a Δ-simple ring finitely generated over k then*

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

1.12 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 1.12.1 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 1.12.2 *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

$$a_j' = 0, \qquad j = 1, \ldots, n-1.$$

□

We actually use the contrapositive more than the proposition itself.

Corollary 1.12.3 *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 1.12.4 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". Kolchin (1973, 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 1.12.5 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 1.12.6 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 1.12.7 *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 $k = 1, \ldots, m$. □

We use the contrapositive more than the above proposition.

Corollary 1.12.8 *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*

$$\det W_\theta(\eta) \neq 0.$$

1.13 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 Zariski and Samuel (1975, p. 100, bottom).

Proposition 1.13.1 *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. Zariski and Samuel (1975, Theorems 28 and 29, p. 101). □

Corollary 1.13.2 *Let R be an integral domain finitely generated over k. Then every surjective endomorphism is an automorphism.*

Bibliography

Atiyah, M. F. and I. G. Macdonald. 1969. *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. MR 0242802 (39 #4129)

Baider, A. and R. C. Churchill. 1990. *On monodromy groups of second-order Fuchsian equations*, SIAM J. Math. Anal. **21**, no. 6, 1642–1652. MR **1075596 (92d:**33034)

Bourbaki, N. 1990. *Algebra. II. Chapters 4–7*, Elements of Mathematics (Berlin), Springer-Verlag, Berlin. MR **1080964 (91h:**00003)

Bourbaki, Nicolas. 1998. *Commutative algebra. Chapters 1–7*, Elements of Mathematics (Berlin), Springer-Verlag, Berlin. MR **1727221 (2001g:**13001)

Churchill, R. C. 1999. *Two generator subgroups of* $\mathrm{SL}(2, \mathbf{C})$ *and the hypergeometric, Riemann, and Lamé equations*, J. Symbolic Comput. **28**, no. 4-5, 521–545. MR **1731936 (2002a:**34131)

Churchill, R. C. and Jerald J. Kovacic. 2002. *Cyclic vectors*, Differential algebra and related topics (Newark, NJ, 2000), World Sci. Publishing, River Edge, NJ, pp. 191–218. MR **1921700 (2003h:**12007)

Epstein, Marvin P. 1955. *On the theory of Picard-Vessiot extensions*, Ann. of Math. (2) **62**, 528–547. MR 0072868 (17,343a)

Kaplansky, Irving. 1976. *An introduction to differential algebra*, Hermann, Paris. MR 57 #297

Keigher, William F. 1977. *Prime differential ideals in differential rings*, Contributions to algebra (collection of papers dedicated to Ellis Kolchin), pp. 239–249. MR 0485806 (58 #5610)

Kolchin, E. R. 1948. *Algebraic matric groups and the Picard-Vessiot theory of homogeneous linear ordinary differential equations*, Ann. of Math. (2) **49**, 1–42. MR 0024884 (9,561c), reprinted in Kolchin (1999).

Kolchin, E. R. 1973. *Differential algebra and algebraic groups*, Academic Press, New York. MR 58 #27929

Kolchin, E. R. 1974. *Constrained extensions of differential fields*, Advances in Math. **12**, 141–170. MR 0340227 (49 #4982), reprinted in Kolchin (1999).

Kolchin, Ellis. 1999. *Selected works of Ellis Kolchin with commentary*, American Mathematical Society, Providence, RI. MR **2000g:**01042

Kovacic, J. 1969. *The inverse problem in the Galois theory of differential fields*, Ann. of Math. (2) **89**, 583–608. MR 0244218 (39 #5535)

Kovacic, Jerald J. 1986. *An algorithm for solving second order linear homogeneous differential equations*, J. Symbolic Comput. **2**, no. 1, 3–43. MR **839134 (88c:**12011)

Kovacic, Jerald J. 2003. *The differential Galois theory of strongly normal extensions*, Trans. Amer. Math. Soc. **355**, no. 11, 4475–4522 (electronic). MR **1990759 (2004i:**12008)

Kovacic, Jerald J. 2006. *Geometric characterization of strongly normal extensions*, Trans. Amer. Math. Soc. **358**, no. 9, 4135–4157 (electronic). MR 2219014

Lang, Serge. 2002. *Algebra*, Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York. MR **1878556 (2003e:**00003)

McCullough, D. 2005. *Exceptional Subgroups of* $\mathrm{SL}(2, F)$, University of Oklahoma, preprint.

Magid, Andy R. 1994. *Lectures on differential Galois theory*, University Lecture Series, vol. 7, American Mathematical Society, Providence, RI. MR **95j:**12008

Matsumura, Hideyuki. 1989. *Commutative ring theory*, Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, Cambridge. MR **1011461 (90i:**13001)

Matzat, B. Heinrich and Marius van der Put. 2003. *Iterative differential equations and the Abhyankar conjecture*, J. Reine Angew. Math. **557**, 1–52. MR **1978401 (2004d:**12011)

Okugawa, Kôtaro. 1962/1963. *Basic properties of differential fields of an arbitrary characteristic and the Picard-Vessiot theory*, J. Math. Kyoto Univ. **2**, 295–322. MR 0155820 (27 #5754)

Poole, E. G. C. 1960. *Introduction to the theory of linear differential equations*, Dover Publications Inc., New York. MR 0111886 (22 #2746)

Rainville, Earl D., Phillip E. Bedient, and Richard E. Bedient. 1997. *Elementary differential equations*, Prentice Hall Inc., Upper Saddle River, NJ. MR 1442258

Ritt, J. F. 1932. *Differential equations from the algebraic standpoint*, Colloquium Publications, vol. 14, American Mathematical Society, Providence, RI.

Rubel, Lee A. 1989. *A survey of transcendentally transcendental functions*, Amer. Math. Monthly **96**, no. 9, 777–788. MR **1033345 (91b:**12010)

Scanlon, Thomas. 2002. *Model theory and differential algebra*, Differential algebra and related topics (Newark, NJ, 2000), pp. 125–150. MR **1921697 (2003g:**03062)

Seidenberg, A. 1956. *Contribution to the Picard-Vessiot theory of homogeneous linear differential equations*, Amer. J. Math. **78**, 808–818. MR 0081897 (18,463c)

Sit, William Y. 2002. *The Ritt-Kolchin theory for differential polynomials*, Differential algebra and related topics (Newark, NJ, 2000), pp. 1–70. MR **1921694 (2003g:**12010)

Springer, T. A. 1998. *Linear algebraic groups*, Progress in Mathematics, vol. 9, Birkhäuser Boston Inc., Boston, MA. MR **1642713 (99h:**20075)

van der Put, Marius and Michael F. Singer. 2003. *Galois theory of linear differential equations*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 328, Springer-Verlag, Berlin. MR 1 960 772S

Zariski, Oscar and Pierre Samuel. 1975. *Commutative algebra. Vol. 1*, Springer-Verlag, New York. MR 0384768 (52 #5641)

Index