Chapter 3

Basic differential algebra

Throughout this chapter we assume that all domains have characteristic 0.

3.1 Differential rings and fields

Definition 3.1.1: Let R be a commutative ring with unity.
A *derivation* $'$ is a map from R to R such that for all $r, s \in R$ we have

$$(r+s)' = r' + s' \quad \text{and} \quad (rs)' = r's + rs' \ .$$

R together with its derivation is called a *differential ring*. □

Lemma 3.1.2: *Let the differential ring R be an integral domain. Then the derivation $'$ extends uniquely to the quotient field K of R.*

Proof: Suppose we can extend the derivation $'$ to K. Take a non-zero $a \in R$; then

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

$$\text{so} \quad (a^{-1})' = \frac{-a'}{a^2} \ .$$

This implies (by the product rule) that for an arbitrary $a/b \in K$

$$\left(\frac{a}{b}\right)' = \frac{ba' - ab'}{b^2} \ . \qquad (*)$$

In fact, $(*)$ defines a derivation on K. □

Definition 3.1.3: Let R be a differential ring.

(a) Since $1' = (1^2)' = 2 \cdot 1 \cdot 1'$, $1' = 0$. Also $0' = 0$. Thus the set $C_R = \{c | c \in R, c' = 0\}$ forms a subring with unity of R, the *ring of constants* of R.

(b) If the differential ring R is actually a field, then R is called a *differential field*. In this case C_R is a subfield of R, the *field of constants*. □

Remark 3.1.4: If n is a positive integer, we can prove by induction that

$$(a^n)' = n \cdot a^{n-1} \cdot a' \ .$$

From the proof of Lemma 3.1.2 we conclude that this property holds for all integers n.

Example 3.1.5: Consider the field M of meromorphic functions on $\mathbb{C}$; i.e., functions which are analytic everywhere except at possibly finitely many isolated singularities which must be poles (limit $\pm\infty$).
C_M is obviously $\mathbb{C}$; but we will be interested in differential subfields of M with possibly smaller fields of constants.

(a) $\mathbb{Q}$: this is the smallest subfield of M. The only derivation on $\mathbb{Q}$ is the trivial one, with $a' = 0$ for all $a \in \mathbb{Q}$. So $C_{\mathbb{Q}} = \mathbb{Q}$.

(b) $\mathbb{Q}(x)$: the field of rational functions in x with $' = d/dx$ is a differential field. The derivative of x is 1, but we would also get a differential fields by setting $x' = 2$.

(c) $\mathbb{Q}(x, \exp(x))$: $\exp(x)$ is transcendental over $\mathbb{Q}(x)$. Notice that this field also contains $\cosh(x) = (\exp(x) + 1/\exp(x))/2$. Antiderivatives may lie outside the field. But something more problematic may happen. E.g., $\int (\exp(x)/x dx$ cannot be written even as a "closed form expression", i.e., cannot be found in a Liouville extension of the field.

Now let us consider extensions of a differential field, both algebraic and transcendental.

Theorem 3.1.6: *Let K be a differential field and $K(\vartheta)$ an algebraic extension of K. Then the derivative $'$ of K extends uniquely to a derivation on $K(\vartheta)$.*

Proof: Let $m(x) \in K[x]$ be the minimal polynomial of ϑ; i.e., $m(x)$ is irreducible and $m(\vartheta) = 0$. So

$$m(\vartheta) = m_n \vartheta^n + \cdots + m_0 = 0 \text{ , with } m_n \neq 0 \ .$$

Consequently also $m(\vartheta)' = 0$; i.e.,

$$\begin{aligned} m(\vartheta)' &= \textstyle\sum_{i=1}^n (m_i' \vartheta^i + i \cdot m_i \vartheta^{i-1} \vartheta') + m_0' \\ &= \vartheta' (\textstyle\sum_{i=1}^n i \cdot m_i \vartheta^{i-1}) + \textstyle\sum_{i=0}^n m_i' \vartheta^i \\ &= 0 \ . \end{aligned}$$

So we get

$$\vartheta' \;=\; \frac{-\sum_{i=0}^{n} m_i' \vartheta^i}{\sum_{i=1}^{n} i \cdot m_i \vartheta^{i-1}} \;.$$

The denominator is non-zero, because m is minimal for ϑ. □

An algebraic extension of the differential field K might contain new constants. For example, $\mathbb{Q}(x)(y)$ with $y^4 - 2x^2 = 0$ contains $\sqrt{2}$ (and $-\sqrt{2}$), since for $t = y^2/x$ we have $t^2 = 2$.

Theorem 3.1.7: *Let K be a differential field and $K(\vartheta)$ a transcendental extension of K. Then $\vartheta' = \eta$ induces a derivation on $K(\vartheta)$ for any $\eta \in K(\vartheta)$.*

Proof: Let $a(\vartheta) = a_n\vartheta^n + \cdots + a_0$ be an arbitrary element of $K[\vartheta]$. Define

$$a(\vartheta)' := a_n'\vartheta^n + \sum_{i=1}^{n} (a_{i-1}' + i \cdot a_i\eta)\vartheta^{i-1} \;.$$

Then $'$ is a derivation on the ring $K[\vartheta]$. Since $K(\vartheta)$ is the quotient field of $K[\vartheta]$, Lemma 3.1.2 yields the result. □

Example 3.1.5 (cont.): Both (b) and (c) are applications of Theorem 3.1.7. In (b) we extend by a transcendental element, $\vartheta = x$, and we choose $\eta = 1$. In (c) we extend by a transcendental element, $\vartheta = \exp(x)$, and we choose $\eta = \vartheta$.

Also, whenever we write $K \subseteq L$ for two differential fields we shall mean K to be a differential subfields of L.

Theorem 3.1.8: *Let $K \subseteq L$ be differential fields and let $\vartheta \in L$ such that $\vartheta' \in K$. If there is no element η in K s.t. $\vartheta' = \eta'$, then ϑ is transcendental over K and for the fields of constants we have $C_{K(\vartheta)} = C_K$.*

Proof: Suppose ϑ is algebraic over K; i.e., there exists a monic irreducible polynomial (the minimal polynomial)

$$m(x) = x^n + m_{n-1}x^{n-1} + \cdots + m_0 \;\in K[x]$$

s.t. $m(\vartheta) = 0$. Therefore

$$m(\vartheta)' = (n\vartheta' + m_{n-1}')\vartheta^{n-1} + \cdots = 0 \;.$$

Since $m(x)$ is minimal, $n\vartheta' + m_{n-1}' = 0$, or $\vartheta' = -m_{n-1}'/n \in K$, contradicting our assumption.

Now we prove that $K(\vartheta)$ contains no new constants. First, assume

$$c = c_n\vartheta^n + \cdots + c_0 \in K[\vartheta], \quad n > 0 \text{ and } c_n \neq 0$$

is a new constant; i.e.,

$$c' = c_n'\vartheta^n + (nc_n\vartheta' + c_{n-1}')\vartheta^{n-1} + \cdots = 0 \;.$$

Since ϑ is transcendental, $c_n' = 0 = nc_n\vartheta' + c_{n-1}'$, hence

$$\vartheta' = \frac{-c_{n-1}'}{nc_n} = \frac{-nc_nc_{n-1}' + c_{n-1}nc_n'}{n^2c_n^2} = \Big(\frac{-c_{n-1}}{nc_n}\Big)' .$$

But this contradicts our assumption.

Finally, suppose $f(\vartheta)/g(\vartheta)$ is a new constant, where $f, g \in K[\vartheta]$, $\deg(g) \geq 1$, and $\gcd(f, g) = 1$, g monic. Then we have

$$\Big(\frac{f(\vartheta)}{g(\vartheta)}\Big)' = \frac{f(\vartheta)'g(\vartheta) - f(\vartheta)g(\vartheta)'}{g(\vartheta)^2} = 0 ,$$

and therefore $f(\vartheta)/g(\vartheta) = f(\vartheta)'/g(\vartheta)'$. But $\deg(g(\vartheta)') < \deg(\vartheta))$, which is impossible since f/g is in reduced form. □

Remark 3.1.9: Using this theorem we see that the logarithmic part of the integral of a rational function is transcendental.

Definition 3.1.10: Consider the differential field extension $K \subset L$. Let $\vartheta \in L \setminus K$.

(a) If there exists an $\eta \in K$ s.t. $\vartheta' = \eta$ we call the extension $K(\vartheta)$ an extension of K by an *integral*, and we call ϑ *primitive* over K. We write $\vartheta = \int \eta$.

(b) If $\vartheta' = \frac{\eta'}{\eta}$ for some $\eta \in K \setminus \{0\}$, then we call $K(\vartheta)$ an extension of K by a *logarithm* and write $\vartheta = \log\eta$. Obviously, extensions by logarithms are extensions by integrals.

(c) If $\frac{\vartheta'}{\vartheta} = \eta$ for some $\eta \in K$, we call $K(\vartheta)$ an extension of K by an *exponential of an integral*. We write $\vartheta = \exp(\int \eta)$.

(d) If $\frac{\vartheta'}{\vartheta} = \eta'$ for some $\eta \in K$, we call $K(\vartheta)$ an extension of K by an *exponential* and we write $\vartheta = \exp\eta$. Obviously, extensions by exponentials are extensions by exponentials of integrals.

(e) ϑ is *elementary* over K if
- ϑ is algebraic over K, or
- $\vartheta = \log\eta$ for some $\eta \in K$, or
- $\vartheta = \exp\eta$ for some $\eta \in K$.

(f) ϑ is an (*elementary*) *monomial* over K if $\vartheta = \log\eta$ or $\vartheta = \exp\eta$ for some $\eta \in K$ and ϑ is transcendental over K with $C_{K(\vartheta)} = C_K$. □

Definition 3.1.11: Let $K \subseteq L$ be a differential field extension. L is an *elementary extension* or *Liouville extension* of K if there are $\vartheta_1, \ldots, \vartheta_n$ in L s.t. $L = K(\vartheta_1, \ldots, \vartheta_n)$ and ϑ_i is elementary over $K(\vartheta_1, \ldots, \vartheta_{i-1})$ for $1 \leq i \leq n$.

L is a *regular* elementary extension of K if L is an elementary extension of K, and all the intermediate transcendental extensions are extensions by elementary monomials.

We say that $f \in K$ *has an elementary integral over* K if there exists an elementary extension E of K and $g \in E$ s.t. $g' = f$.

An *elementary function* is an element of an elementary extension of $(\mathbb{C}, d/dx)$. $\square$

Example 3.1.12: We shall take the liberty of nesting extensions by simply listing them, so for example

$$K(\exp\eta_1, \log\eta_2) = (K(\exp\eta_1))(\log\eta_2) \ .$$

(a) $\mathbb{Q}(x, \exp(x), \log(\exp(x)+1), \exp(x)^{2/3})$ is a regular elementary extension of $\mathbb{Q}(x)$. But we cannot prove this here.

(b) $\mathbb{Q}(x, \exp(x), \exp(2x+1))$ is an elementary extension of $\mathbb{Q}(x)$. But it is not regular, since

$$\exp(2x+1) \ / \ \exp(x)^2 \ = \ \exp(1) \ ,$$

and thus a new transcendental constant is introduced.

(c) $\mathbb{Q}(x, \log(x), \exp(\log(x)/3))$ is not an extension by a monomial of $\mathbb{Q}(x, \log(x))$, because

$$\exp(\log(x)/3) \ = \ x^{1/3}$$

is algebraic over this field. $\square$

Without proof we quote the strong version of Liouville's Theorem on integration. This theorem can be found in [Bro97] as Theorem 5.5.3, where it is fully proved.

Theorem 3.1.13 (Liouville's Theorem – strong version): *Let K be a differential field, C the field of constants of K, and $f \in K$.*
If there exists an elementary extension E of K and $g \in E$ s.t. $g' = f$, then there are $v \in K$, $c_1, \ldots, c_n \in \overline{C}$, and $u_1, \ldots, u_n \in K(c_1, \ldots, c_n)^*$ such that

$$f \ = \ v' + \sum_{i=1}^{n} ci \frac{u_i'}{u_i} \ .$$

So if f has an elementary integral over K, then $\int f$ is something in K plus a sum of logarithms.

3.2 Differential polynomials

The following definitions and facts can be found in Chapter 1 of [Ritt50].

Definition 3.2.1: Let $(R,')$ be a differential ring. Consider the polynomial ring in infinitely many variables

$$R\{y\} \;=\; R[y^{(0)}, y^{(1)}, y^{(2)}, \ldots] \;=\; R[y, y', y'', \ldots] \;.$$

The derivation $'$ on R can be extended to the following derivation δ on $R\{y\}$:

$$\delta\Big(\sum_i a_i y^{(i)}\Big) = \sum_i (a_i' y^{(i)} + a_i y^{(i+1)}) \;.$$

So $(R\{y\}, \delta)$ is a differential ring, the *ring of differential polynomials* over R. We call y a *differential variable.* Often we also write $'$ for δ. □

Similarly, this construction can be extended to several indeterminates. In this case there may be several derivations. The differential ring is called *ordinary* if it is equipped with only one derivation.

Definition 3.2.2: Let (R, δ) be an ordinary differential ring. An ideal I of R is called a *differential ideal* iff I is closed under the derivation δ; i.e., for all $a \in I$ we have $\delta(a) \in I$.

Let B be a set of differential polynomials in R. The *differential ideal generated by* B, denoted by $[B]$, is the ideal generated by all elements in B and their derivatives. The *radical differential ideal generated by* B, denoted by $\{B\}$, is the radical of $[B]$. □

Example 3.2.3: Consider the differential ring $R = \mathbb{Q}[x]$ with the usual derivation $'$. Then the ring of differential polynomials in y over R contains, for example, the differential polynomials

$$p(y) = 3xy''' - (2x^2 + 5)y' - 7, \quad q(y) = (2x^3 + x - 1)y'' + 3x^2 y \;.$$

The derivation of p is

$$p'(y) = 3xy^{(4)} + 3y''' - (2x^2 + 5)y'' - 4xy' \;.$$

Observe that $R\{y\}$ is a non-Noetherian ring. The ideal

$$< y, y', y'', \ldots >$$

does not have a finite basis. But as a differential ideal $[y, y', y'', \ldots]$ it has a finite basis, namely it can be written as $[y]$. □

Definition 3.2.4: Let I be a differential ideal in the differential ring $R = (K\{y\}, \delta)$, where K is a differential field. Let L be a differential extension field of K. An element $\xi \in L$ is called a *zero* of I iff for all $p(y) \in I$ we have $p(\xi) = 0$.

The *defining differential ideal* of ξ in R is $\{p(y) \in R \mid p(\xi) = 0\}$.
A point $\xi \in L$ is called a *generic zero* of I iff I is the defining differential ideal of ξ in R. $\square$

Remark 3.2.5: In commutative algebra every prime ideal in $K[x_1, \ldots, x_n]$ has a generic zero in a suitable extension of K. Similarly in differential algebra every prime differential ideal has a generic zero in a suitable differential extension of K.

For example, the prime differential ideal generated by

$$y'^2 + 3y' - 2y - 3x \in \mathbb{Q}(x)\{y\}$$

has the generic zero $((x + c)^2 + 3c)/2$, where c is a transcendental constant. The corresponding differential equation

$$y'^2 + 3y' - 2y - 3x = 0$$

has the general solution $y(x) = ((x + c)^2 + 3c)/2$. $\square$

3.3 Linear differential operators

Definition 3.3.1: Let (R, δ) be a differential integral domain; δ is also written as $'$. We consider the non-commutative *ring of linear differential operators* $R[\partial]$, where the rule for the multiplication of ∂ by an element of $r \in R$ is

$$\partial r = r\partial + r' \ .$$

The *application* of an operator

$$A = \sum_{i=0}^{m} a_i \partial^i$$

to an element of the differential ring $r \in R$ is defined as

$$A(r) = \sum_{i=0}^{m} a_i r^{(i)} \ .$$

Here $r^{(i)}$ denotes the i-fold application of $'$ to r.
If $a_m \neq 0$, the *order* of A is m and a_m is the *leading coefficient* of A.
The application of A can naturally be extended to the quotient field K of R, and to any field extension of K. If $A(\eta) = 0$, with η in R, K or any extension of K, we call η a *root* of the linear differential operator A. □

Note that ∂r, which denotes the operator product of ∂ and r, is distinct from $\partial(r)$, the application ∂ to r, namely r'.
The application of an operator a of order 0, i.e. an element a of R considered as an operator, to $r \in R$ is $a(r) = a \cdot r$.

Proposition 3.3.1. *For $n \in N$: $\partial^n r \ = \ \sum_{i=0}^{n} \binom{n}{i} r^{(n-i)} \partial^i$.*

Proof: For $n = 0$ this obviously holds.
Assume the fact holds for some $n \in \mathbb{N}$. Then

$$\begin{aligned}
\partial^{n+1} r &= \partial(\partial^n r) \ = \ \partial\left(\sum_{i=0}^{n} \binom{n}{i} r^{(n-i)} \partial^i\right) \\
&= \sum_{i=0}^{n} \binom{n}{i} \partial r^{(n-i)} \partial^i \ = \ \sum_{i=0}^{n} \binom{n}{i} [r^{(n-i)}\partial + r^{(n-i+1)}] \partial^i \\
&= \sum_{i=0}^{n} \binom{n}{i} r^{(n-i)} \partial^{i+1} \ + \ \sum_{i=0}^{n} \binom{n}{i} r^{(n-i+1)} \partial^i \\
&= \sum_{i=1}^{n+1} \binom{n}{i-1} r^{(n+1-i)} \partial^i \ + \ \sum_{i=0}^{n} \binom{n}{i} r^{(n-i+1)} \partial^i \\
&= \binom{n}{n} r^{(0)} \partial^{n+1} \ + \ \sum_{i=1}^{n} [\binom{n}{i-1} + \binom{n}{i}] r^{(n+1-i)} \partial^i \ + \ \binom{n}{0} r^{(n+1)} \partial^0 \\
&= \sum_{i=0}^{n+1} \binom{n+1}{i} r^{(n+1-i)} \partial^i .
\end{aligned}$$ □

From a linear homogeneous ODE $f(y) = 0$, with $f(y) \in R\{y\}$, we can extract a linear differential operator $A = \mathcal{O}(f)$ such that the given ODE can be written as

$$A(y) = 0,$$

in which y is regarded as an unknown element of R, K or some extension of K. Such a linear homogeneous ODE always has the trivial solution $y = 0$; so a linear differential operator always has the trivial root 0.

In [Chardin:91] it is stated that $K[\partial]$ is left-Euclidean, and a few brief remarks are provided by way of proof.

Since the concept of a left-Euclidean ring is not as widely known as that of Euclidean ring, it may be helpful to recall its definition here.

Definition 3.3.2. *A (potentially non-commutative) ring R is* left-Euclidean *if there exists a function $d : R^* \to \mathbb{N}$ such that for all a, b in R, with $b \neq 0$, there exist q and r in R such that $a = qb + r$, with $d(r) < d(b)$ or $r = 0$.* □

If one wishes to provide a complete proof of the claim that $K[\partial]$ is left-Euclidean (in which we take $d(A)$ to be the order of A), Proposition 3.3.1 above is useful. For example, by way of proof hint, Chardin claims that the operator $A - (a/b)\partial^{m-n}B$ is of order less than m, where a and b are the leading coefficients of A and B, respectively, and m and n are their orders, with $m \geq n$ assumed. To show this claim, it suffices to show that the term $(a/b)\partial^{m-n}B$ consists of $a\partial^m$ plus terms of order less than m. This follows by applications of Proposition 3.3.1, putting $n = m - n$ and r equal to each coeficient of operator B in turn.

It follows from the left-Euclidean property that every left-ideal $_K I$ of the form $_K I = (A, B)$ is principle, and is generated by the right-gcd of A and B. As remarked in [Chardin:91], any linear differential operator of positive order has a root in some extension of K. We state this result precisely.

Theorem 3.3.3. (Ritt-Kolchin). *Assume that the differential field K has characteristic 0 and that its field C of constants is algebraically closed. Then, for any linear differential operator A over K of positive order n, there exist n roots $\eta_1, \ldots, \eta_n$ in a suitable extension of K, such that the η_i are linearly independent over C. Moreover, the field $K\langle\eta_1, \ldots, \eta_n\rangle$ contains no constant not in C.*

This result is stated and proved in [Kolchin:48b] using results from [Kolchin:48a] and [Ritt:32]. The field $K\langle\eta_1, \ldots, \eta_n\rangle$ associated with A is known as a *Picard-Vessiot extension* of K (for A). Henceforth assume the hypotheses of Theorem 3.3.3.

It follows from Theorem 3.3.3 that if the operators $A, B \in K[\partial]$ have a common factor F of positive order on the right, i.e.,

$$A = \overline{A} \cdot F, \quad \text{and } B = \overline{B} \cdot F, \tag{3.1}$$

then they have a non-trivial common root in a suitable extension of K. For by Theorem 3.3.3, F has a root $\eta \neq 0$ in an extension of K. We have $A(\eta) = \bar{A}(F(\eta)) = \bar{A}(0) = 0$ and similarly $B(\eta) = 0$.

On the other hand, if A and B have a non-trivial common root η in a suitable extension of K, we show that they have a common right factor of positive order in

$K[\partial]$. Let F be a nonzero differential operator of lowest order s.t. $F(\eta) = 0$. Then F has positive order. Because the ring of operators is left-Euclidean, F is unique up to multiplication of non-zero elements of K. This F is a right divisior of both A and B. To see this, apply division in the left-Euclidean ring $K[\partial]$:

$$A = Q \cdot F + R,$$

with the order of R less than the order of F, or $R = 0$. Apply both sides of this equation to η:

$$A(\eta) = (Q \cdot F)(\eta) + R(\eta).$$

Since $A(\eta) = 0$ and $F(\eta) = 0$, $R(\eta) = 0$. Therefore, by minimality of F, $R = 0$. Hence F is a right divisor of A. We see that F is a right divisor of B similarly. We summarize our result in the following theorem.

Theorem 3.3.4. *Assume that K has characteristic 0 and that its field of constants is algebraically closed. Let A, B be differential operators of positive orders in $K[\partial]$. Then the following are equivalent:*

(i) *A and B have a common non-trivial root in an extension of K,*

(ii) *A and B have a common factor of positive order on the right in $K[\partial]$.*

In the following chapter we will investigate the existence of a non-trivial factor, and we will see that (3.1) is equivalent to the existence of a non-trivial order-bounded linear combination

$$CA + DB = 0 \;, \tag{3.2}$$

with $\text{order}(C) < \text{order}(B)$ and $\text{order}(D) < \text{order}(A)$, and $(C, D) \neq (0, 0)$.
This will lead to the concept of a differential resultant.

References

[Chardin:91] Chardin, M., Differential resultants and subresultants. In *Proc. Fundamentals of Computation Theory 1991*, *LNCS Vol. 529*, Springer-Verlag, 1991.

[Kolchin:48a] Kolchin, E.R., Algebraic matric groups and the Picard-Vessiot theory of homogeneous linear ODEs. *Ann. of Math. 49*, 1–42, 1948.

[Kolchin:48b] Kolchin, E.R., Existence theorems connected with the Picard-Vessiot theory of homogeneous linear ODEs. *Bull. Amer. Math. Soc. 54*, 927–932, 1948.

[Ritt:32] Ritt, J. F., *Differential Equations from the Algebraic Standpoint.* AMS Coll. Publ. Vol. 14, New York, 1932.