Lecture Notes on Decompositions of Linear Ode’s

Ziming Li
MMRC, Academy of Mathematics and Systems Science
Chinese Academy of Sciences, Beijing 100080, China

Abstract. This note contains Beke’s algorithm for factoring linear homogeneous ode’s and the Eigenring method for factoring completely reducible linear differential factors. It contains a (possibly) new and elementary proof of the correctness of the Eigenring method.

This note grew out of the course Computation Differential Algebra given by the author in the first half of 2000. The author thanks AMSS for the organization, and the listeners of the course for their suggestions and assistance.

1. Ring of linear differential operators

We denote $C(x)$ as $K$. The usual derivation operator $\frac{d}{dx}$ on $K$ will also be denoted by $t$. All conclusions drawn in this section hold for any abstract differential field.

Let $D$ be an indeterminate over $K$. We may regard $K[D]$ as a ring of polynomials in $D$ over $K$. Let us forget the usual commutative multiplication in $K[D]$ and regard merely $K[D]$ as a left $K$-linear space generated by $1, D, D^2, \ldots$. We will define a non-commutative multiplication in $K[D]$, which captures the differentiation of a linear homogeneous ode. To this end, we introduce the following two rules

- Power product rule: $D^n D^m = D^{n+m}$, and
- commutation rule: $Da = aD + a'$.

The power product rule reflects the fact

$$\frac{d^m}{dx^m} \left( \frac{d^n y}{dx^n} \right) = \frac{d^{m+n} y}{dx^{m+n}}$$

The commutation rule reflects the fact that

$$\frac{d}{dx} (ay) = a \frac{dy}{dx} + \frac{da}{dx} y = \left( a \frac{d}{dx} + \frac{da}{dx} \right) y.$$

By the two rules, we define inductively

$$D^n(aD^m) = (D^n a)D^m = D^{n-1}(Da)D^m = D^{n-1}(aD + a')D^m = D^{n-1}aD^{m+1} + D^{n-1}a'D^m$$

where $m, n$ are integers and $a$ is in $K$. Furthermore, define

$$AB = \left( \sum_{i=0}^n a_i D^i \right) \left( \sum_{j=0}^m b_j D^j \right) = \sum_{i=0}^n \sum_{j=0}^m a_i b_j D^{i+j}.$$
A tedious calculation shows that the above-defined multiplication is associative, distributive w.r.t. addition, but non-commutative. The ring $K[D]$ is equipped with the multiplication equivalent to the composition of linear differential operators over $K$. The ring $K[D]$ is then called the ring of linear differential operators over $K$.

**Lemma 1.1** For nonzero $A, B \in K[D]$, we have

1. $\text{lc}(DA) = \text{lc}(A)$
2. $\deg AB = \deg A + \deg B$.

**Proof** Immediate. \(\square\)

Next, we define a right division. For two nonzero $A, B$ in $K[D]$ with respective degrees $m$ and $n$, we construct $Q$ and $R$ in $K[D]$ such that $A = QB + R$ and $\deg R < \deg B$. If $m < n$ then set $Q = 0$ and $R = A$. If $m = n$, then set $Q = \text{lc}(A)/\text{lc}(B)$ and $R = A - QB$. Now, assume that $Q$ and $R$ can be constructed when $m - n < k$. For the case in which $m - n = k$, let

$$\tilde{A} = A - \frac{\text{lc}(A)}{\text{lc}(B)} D^k B.$$ 

Then $\deg \tilde{A} < m$. By induction, there exist $\tilde{Q}$ and $R$ with $\deg R < n$ such that

$$\tilde{A} = \tilde{Q} B + R.$$ 

Combining these two equalities yields

$$A = \frac{\left(\frac{\text{lc}(A)}{\text{lc}(B)} D^k + \tilde{Q}\right)}{\tilde{Q}} B + R.$$ 

Notice that $Q$ and $R$ are unique because of the second assertion of Lemma 1.1. $Q$ and $R$ are called the left quotient and the right remainder of $A$ and $B$, respectively. We denote $Q = \text{quo}(A, B)$ and $R = \text{rem}(A, B)$.

**Definition 1.1** For nonzero $A, B, G \in K[D]$,

1. $G$ is called a right divisor of $A$ if $\text{rem}(A, G) = 0$.
2. $G$ is called a greatest common right divisor (gcrd) of $A$ and $B$ if $G$ is common right divisor of $A$ and $B$ and every common divisor of $A$ and $B$ is a right divisor of $G$.

The existence of the gcrd of $A$ and $B$ is proved by the right Euclidean algorithm given below.

**algorithm** Euclid

**Input:** nonzero $A, B \in K[D]$

**Output:** $G = \text{gcrd}(A, B)$

$A_1 \leftarrow A; A_2 \leftarrow B; i \leftarrow 2$

**while** $A_i \neq 0$ **do** { $i \leftarrow i + 1$ ; $A_i = \text{rem}(A_{i-2}, A_{i-1})$ }

$G \leftarrow A_{i-1}$;

**return**($G$);
The Euclid algorithm generates a (right) polynomial remainder sequence

\[ A_1, A_2, \ldots, A_k, \]

where \( A_k = \text{gcd}(A_1, A_2) \). Note that \( k = i - 1 \) for the last value of \( i \) in the algorithm.

The existence of gcds implies that left ideals in \( K[D] \) are principal.

A fundamental notion in \( K[D] \) is the least common left multiple (lclm).

**Definition 1.2** For nonzero \( A, B \) in \( K[D] \), \( L \in K[D] \) is called the least common left multiple of \( A \) and \( B \) if

- \( \text{rem}(L, A) = \text{rem}(L, B) = 0 \)
- \( \text{rem}(H, A) = \text{rem}(H, B) = 0 \implies \text{rem}(H, L) = 0. \)

A left ideal generated by \( P_1, \ldots, P_m \) in \( K[D] \) is denoted by \((P_1, \ldots, P_m)\). For two nonzero \( A \) and \( B \) in \( K[D] \), \((A) \cap (B) \) is principal, so \((A) \cap (B) = (L) \). It is easy to see that \( L \) is the lcm of \( A \) and \( B \).

Next, we study how to compute lclms. To do this, we introduce some notations: For nonzero \( A \) and \( B \) in \( K[D] \), if \( \text{rem}(A, B) = 0 \), then \( \text{quo}(A, B) \) is denoted by \( AB^{-1} \), and \([A, B]\) denotes the monic lcm of \( A \) and \( B \).

**Lemma 1.2** Let nonzero \( A \) and \( B \) be in \( K[D] \). If \( A = QB + R \), then

\[ [A, B] = \frac{\text{lcm}(R)}{\text{lcm}(A)} [B, R] R^{-1} A. \]

**Proof** Let \([A, B] = HA \). Since \([A, B] = HA = HQB + HR \), \( HR \) is a left common multiple of \( B \) and \( R \). We claim that \( HR \) is an lcm of \( A \) and \( B \). Otherwise, there would exist \( P \) in \( K[D] \) such that \([B, R] = PR \) and \( \text{deg} P < \text{deg} H \). Since

\[ PA = PQB + PR, \]

\( PA \) would be a left common multiple of \( A \) and \( B \). But \( \text{deg} PA < \text{deg} HA \), a contradiction.

Now, we compute the lcm of \( A \) and \( B \). Set \( A_1 = A \) and \( A_2 = B \). Applying the Euclid algorithm to \( A_1 \) and \( A_2 \), we get a polynomial remainder sequence

\[ A_1, A_2, \ldots, A_{k-1}, A_k, \]

where \( A_k = \text{gcd}(A_1, A_2) \). It follows that

\[ A_i = \text{rem}(A_{i-2}, A_{i-1}) \]

where \( i = 3, \ldots, k \) and \( \text{rem}(A_{k-1}, A_k) = 0 \). Set \( l_i = \text{lcm}(A_i) \). We see \([A_{k-1}, A_k] = l_k^{-1} A_{k-1} \).

By Lemma 1.2,

\[ [A_{k-2}, A_{k-1}] = \frac{l_k}{l_{k-1}} [A_{k-1}, A_k] A_k^{-1} A_{k-2} = \frac{l_k}{l_{k-1}} A_{k-1} A_k^{-1} A_{k-2}. \] (1)
Applying Lemma ?? to \( A_{i-1} \) and \( A_i \), for \( i = 2, \ldots, k-2 \), we obtain

\[
[A_{i-1}, A_i] = \frac{l_{i+1}}{l_i} [A_i, A_{i+1}] A_{i+1}^{-1} A_{i-1}.
\]  

(2)

Combining (??) and (??) yields

\[
[A_1, A_2] = a A_{k-2} A_{k-3}^{-1} A_{k-2}^{-1} \cdots A_2 A_1^{-1} A_1,
\]  

(3)

in which \( a \) is a suitable element of \( K \) and the multiplication and exact (right) division are performed from the left to the right. Thus, we have

**Theorem 1.3** Keep the notation introduced above. The \( \text{lclm} \) of \( A_1 \) and \( A_2 \) can be computed by (??), and the degree of \( \text{lclm}(A_1, A_2) \) is equal to \( \deg A_1 + \deg A_2 - \deg \text{gcd}(A_1, A_2) \).

**Proof** By (??) we get

\[
\deg \text{lclm}(A_1, A_2) = (\deg A_{k-2} - \deg A_{k-1}) + (\deg A_{k-3} - \deg A_{k-2}) + \cdots + (\deg A_2 - \deg A_3) + \deg A_1
\]

\[
= \deg A_1 + \deg A_2 - \deg A_k.
\]

The proof is completed. \( \square \)

The reader may prove that, for nonzero \( A, B \in K[D] \),

\[
S(\text{gcd}(A, B)) = S(A) \cap S(B) \text{ and } S(\text{lclm}(A, B)) = S(A) + S(B).
\]

2. Beke’s algorithm for factoring linear differential operators

2.1. Wronskian coefficients

Consider \( A = D^n + a_{n-1} D^{n-1} + \cdots + a_0 \), \( a_i \in \mathbb{C}(x) \). Beke’s algorithm computes an irreducible right factor of \( A \).

Let \( y_1, \ldots, y_n \) be a fundamental set of solutions of \( A(y) \), that is, \( A(y_i) = 0 \), for \( i = 1, \ldots, n \), and \( y_1, \ldots, y_n \) are \( \mathbb{C} \)-linearly independent. First, we study the relation between coefficients \( a_i \) and solutions \( y_i \). Let \((n+1) \times n\) matrix

\[
M = \begin{pmatrix}
y_1 & y_2 & \cdots & y_n \\
y'_1 & y'_2 & \cdots & y'_n \\
\vdots & \vdots & \ddots & \vdots \\
y^{(n-1)}_1 & y^{(n-1)}_2 & \cdots & y^{(n-1)}_n \\
y^{(n)}_1 & y^{(n)}_2 & \cdots & y^{(n)}_n
\end{pmatrix}
\]

Let \( W_i \) be the determinant of \( n \times n \) submatrix obtained from deleting \((i+1)\) row, for \( i = 0, \ldots, n \). Thus, \( W_n \) is the Wronskian of \( y_1, \ldots, y_n \), which is not zero. We call \( W_i \) the \( i \)th Wronskian coefficient of \( A \), for \( i = 0, 1, \ldots, n \).

**Lemma 2.1** \( a_i = (-1)^{n+i} \frac{W_i}{W_n} \), \( i = 0, 1, \ldots, n-1 \), and \( W_i \) is a hyperexponential, \( i = 0, 1, \ldots, n \).
Proof Expanding the determinant
\[
\begin{vmatrix}
  y_1 & y_2 & \cdots & y_n & y \\
  y'_1 & y'_2 & \cdots & y'_n & y' \\
  \cdot & \cdot & \cdots & \cdot & \cdot \\
  y^{(n-1)}_1 & y^{(n-1)}_2 & \cdots & y^{(n-1)}_n & y^{(n-1)} \\
  y^{(n)}_1 & y^{(n)}_2 & \cdots & y^{(n)}_n & y^{(n)} \\
\end{vmatrix}
\]
according to the last row, we get
\[
B(y) = W_n y^{(n)} - W_{n-1} y^{(n-1)} + \cdots + (-1)^n W_0 y.
\]
Since \( W_n \neq 0 \), \( B(y) \) is an \( n \)th order linear ode with a fundamental set of solutions \( \{y_1, \ldots, y_n\} \).
It follows that \( a_i = (-1)^{n+i} W_i/W_n \), for \( i = 0, \ldots, n-1 \). Notice that \( W_{n-1} = W'_n \). Hence, both \( W_n \) and \( W_{n-1} \) are hyperexponentials. Since \( W_i = (-1)^{n+i} a_i W_n \), by differentiation, we find
\[
W'_i = (-1)^{n+i} (a'_i W_n + a_i W'_n).
\]
Thus,
\[
\frac{W'_i}{W_i} = \frac{a'_i}{a_i} + \frac{W'_n}{W_n}.
\]
The proof is complete. \( \square \)

Remark 2.1 \( \frac{W'_n}{W_n} = -a_{n-1} \), or, equivalently, \( W_n = \exp \left( -\int a_{n-1} \right) \) is called Liouville’s formula.

2.2. Associated equations
Assume that
\[
A = \left( \begin{array}{c}
D^{n-m} + b_{n-m-1}D^{n-m-1} + \cdots + b_0 \\
\end{array} \right) \left( \begin{array}{c}
D^{n-m} + b_{n-m-1}D^{n-m-1} + \cdots + b_0 \\
\end{array} \right), \quad (4)
\]
where \( B, F \in K[D] \). Let \( y_1, \ldots, y_m \) be a fundamental set of solutions of \( F \) and set
\[
M = \begin{pmatrix}
  y_1 & y_2 & \cdots & y_m \\
  y'_1 & y'_2 & \cdots & y'_m \\
  \cdot & \cdot & \cdots & \cdot \\
  y^{(n-1)}_1 & y^{(n-1)}_2 & \cdots & y^{(n-1)}_m \\
\end{pmatrix}, \quad (5)
\]
There are \( k = \binom{n}{m} \) \( m \times m \) square submatrices in \( M \). The determinants of these matrices are ordered as
\[ \Delta_1, \Delta_2, \ldots, \Delta_k. \]
Let \( \Delta = \{\Delta_1, \Delta_2, \ldots, \Delta_k\} \). Note that the Wronskian coefficients \( W_m, W_{m-1}, \ldots, W_0 \) of \( F \) are contained in \( \Delta \).

Lemma 2.2 Let \( B_{nm} \) be the \( K \)-linear space generated by \( \Delta \). Then \( B_{nm} \) is closed under differentiation.
Proof Let us denote by $M_{i_1 i_2 \cdots i_m}$ the $m \times m$ submatrices consisting of the $i_1$th, $i_2$th, \ldots, $i_m$th rows of $M$. Assume that $\Delta_j = \det M_{i_1 i_2 \cdots i_m}$. If $0 < i_1 < i_2 < \cdots < i_m < n$, then

$$\Delta'_j = \det M_{i_1 + 1, i_2 \cdots i_m} + \det M_{i_1, i_2 + 1, \cdots i_m} + \cdots + \det M_{i_1, i_2 \cdots i_m + 1}$$

in which the determinants are either 0 or in $\Delta$. Hence $\Delta_j \in \mathcal{B}_{nm}$. If $i_m = n$, then

$$\Delta'_j = \det M_{i_1 + 1, i_2 \cdots i_m} + \det M_{i_1, i_2 + 1, \cdots i_m} + \cdots + \det S$$

where

$$\det S = \begin{vmatrix} y_1^{(i_1-1)} & y_2^{(i_1-1)} & \cdots & y_m^{(i_1-1)} \\ y_1^{(i_2-1)} & y_2^{(i_2-1)} & \cdots & y_m^{(i_2-1)} \\ \vdots & \vdots & \ddots & \vdots \\ y_1^{(n)} & y_2^{(n)} & \cdots & y_m^{(n)} \end{vmatrix} = \begin{vmatrix} y_1^{(i_1-1)} & y_2^{(i_1-1)} & \cdots & y_m^{(i_1-1)} \\ y_1^{(i_1-1)} & y_2^{(i_1-1)} & \cdots & y_m^{(i_1-1)} \\ \vdots & \vdots & \ddots & \vdots \\ -\sum_{l=0}^{n-1} a_l y_1^{(l)} & -\sum_{l=0}^{n-1} a_l y_2^{(l)} & \cdots & -\sum_{l=0}^{n-1} a_l y_m^{(l)} \end{vmatrix}$$

is in $\mathcal{B}_{nm}$. Hence, $\Delta'_j \in \mathcal{B}_{nm}$.

Thus, there exists a $k \times k$ matrix $L_{nm}$ over $K$ such that

$$\begin{pmatrix} \Delta'_1 \\ \Delta'_2 \\ \vdots \\ \Delta'_k \end{pmatrix} = L_{nm} \begin{pmatrix} \Delta_1 \\ \Delta_2 \\ \vdots \\ \Delta_k \end{pmatrix},$$

(6)

which we call the $m$th associated system of $A$.

**Example 2.2** Let $n = 4$. Construct the second associated system of $A$. Assume that $\{y_1, y_2\}$ is a fundamental set of solutions. The matrix

$$M = \begin{pmatrix} y_1 & y_2 \\ y'_1 & y'_2 \\ y''_1 & y''_2 \\ y'''_1 & y'''_2 \end{pmatrix}.$$ 

There are six $2 \times 2$ determinants

$$\Delta_1 = \begin{vmatrix} y_1 & y_2 \\ y'_1 & y'_2 \end{vmatrix}, \quad \Delta_2 = \begin{vmatrix} y_1 & y_2 \\ y''_1 & y''_2 \end{vmatrix}, \quad \Delta_3 = \begin{vmatrix} y'_1 & y'_2 \\ y''_1 & y''_2 \end{vmatrix},$$

$$\Delta_4 = \begin{vmatrix} y_1 & y_2 \\ y'''_1 & y'''_2 \end{vmatrix}, \quad \Delta_5 = \begin{vmatrix} y'_1 & y'_2 \\ y'''_1 & y'''_2 \end{vmatrix}, \quad \Delta_6 = \begin{vmatrix} y''_1 & y''_2 \\ y'''_1 & y'''_2 \end{vmatrix}. $$

A straightforward calculation shows that

$$\begin{pmatrix} \Delta'_1 \\ \Delta'_2 \\ \Delta'_3 \\ \Delta'_4 \\ \Delta'_5 \\ \Delta'_6 \end{pmatrix} = L_{42} \begin{pmatrix} \Delta_1 \\ \Delta_2 \\ \Delta_3 \\ \Delta_4 \\ \Delta_5 \\ \Delta_6 \end{pmatrix},$$

(7)
Since $W_m, W_{m-1}, \ldots, W_0$ belong to $B_{nm}$, so do their derivatives by Lemma ???. Hence, each $W_i$ satisfies a linear ode over $K$ whose order is no more than $k$. Such an ode can be constructed by the associated system, and is called an ode associated with $W_i$.

**Example 2.3** Let $n = 4$ and $m = 2$. Construct respective ode’s associated with $W_2, W_1, W_0$.

Notice that $W_2 = \Delta_1$, $W_1 = \Delta_2$ and $W_0 = \Delta_3$. Let $\Delta = (\Delta_1, \ldots, \Delta_6)^T$ and let $\Delta^{(i)} = L_{42,i} \Delta$. Then $L_{42,1} = L_{42}$ given in (??). By differentiation, we find that $L_{42,i} = L'_{42,i-1} + L_{42,i-1} L_{42,1}$. For $j = 0, 1, 2$, let the $7 \times 6$ matrix $N_{3-j}$ be formed as follows. The first row of $N_{3-j}$ is the vector whose $(3-j)$th coordinate is 1, and others are zero. The $l$th row ($2 \leq l \leq 7$) is the $(3-j)$th row of $L_{42,i-1}$. We then have

\[
\begin{pmatrix}
W_j \\
W'_j \\
W''_j \\
W^{(3)}_j \\
W^{(4)}_j \\
W^{(5)}_j \\
W^{(6)}_j \\
\end{pmatrix} = 
\begin{pmatrix}
\Delta_{3-j} \\
\Delta'_{3-j} \\
\Delta''_{3-j} \\
\Delta^{(3)}_{3-j} \\
\Delta^{(4)}_{3-j} \\
\Delta^{(5)}_{3-j} \\
\Delta^{(6)}_{3-j} \\
\end{pmatrix} = N_{3-j}
\begin{pmatrix}
\Delta_1 \\
\Delta_2 \\
\Delta_3 \\
\Delta_4 \\
\Delta_5 \\
\Delta_6 \\
\end{pmatrix}.
\]  

(8)

Since the rows of $N_{3-j}$ are $K$-linearly dependent, a $K$-linear relation among the rows gives rise to an ode associated with $W_j (= \Delta_{3-j})$.

This example suggests a general way to compute associated equations. Assume that $A$ is given by (??). We want to compute ode’s associated with a right factor of $A$ with degree $m$, that is, $m+1$ linear ode’s, $A_m, A_{m-1}, \ldots, A_0$ in $K[D]$ such that the $j$th Wronskian coefficient of any right factor $A$ with degree $m$ is a solution of $A_j$, for $j = 0, 1, \ldots, m$. We do as follows.

1. Assume that the differential indeterminates $y_1, y_2, \ldots, y_m$ are $m$ $K$-linearly independent solutions of $A(y) = 0$. Construct the $n \times m$ matrix $M$ given in (??).

2. Pick up all $m \times m$ determinants consisting of rows of $M$ and list them as

$\Delta = \{\Delta_1, \Delta_2, \ldots, \Delta_k\}$

where $k = \binom{n}{m}$.

3. Construct the associated system (??).

4. Construct matrices $L_{nm,i}$, for $i = 1, 2, \ldots, k$ by the recursive formula

$L_{nm,1} = L_{nm}$, $L_{nm,i} = L'_{nm,i-1} + L_{nm,i-1} L_{nm}$.

5. Mark Wronskian coefficients in $\Delta$, say

$W_0 = \Delta_{j_0}, W_1 = \Delta_{j_1}, \ldots, W_m = \Delta_{j_{m-1}}$. 

6. Construct \((k + 1) \times k\) matrices \(N_p\), for \(p = 0, 1, \ldots, m\). The first row of \(N_p\) is \((0, \ldots, 0, 1, 0, \ldots, 0)\) where 1 appears at the \(j_p\)th position, and the \(q\)th row is the \(j_p\)th row in \(L_{nm,q-1}\), for \(q = 2, 3, \ldots, k + 1\). We then have

\[
\begin{pmatrix}
W_p \\
W'_p \\
\vdots \\
W^{(k)}_p
\end{pmatrix} = N_p
\begin{pmatrix}
\Delta_1 \\
\Delta_2 \\
\vdots \\
\Delta_k
\end{pmatrix},
\]

for \(p = 0, 1, \ldots, m\).

7. A \(K\)-linear relation of the rows of \(N_p\) gives rise to an ode associated with \(W_p\), for \(p = 0, 1, \ldots, m\).

Please notice that all steps except the last are done generically.

2.3. A working example

This section contains a working example for Beke’s method. Let us find all second-order right factors of

\[
A = D^4 - 2xD^2 - 2D + x^2.
\]

According to the scheme given in Section ??, we construct the associated system

\[
\begin{pmatrix}
\Delta_1' \\
\Delta_2' \\
\Delta_3' \\
\Delta_4' \\
\Delta_5' \\
\Delta_6'
\end{pmatrix} = L_{42}
\begin{pmatrix}
\Delta_1 \\
\Delta_2 \\
\Delta_3 \\
\Delta_4 \\
\Delta_5 \\
\Delta_6
\end{pmatrix},
\]

by (??). Since \((\frac{4!}{2!}) = 6\), we use the recursion

\[
L_{42,1} = L_{42}, \quad L_{42,i} = L'_{42,i-1} + L_{42,i-1}L_{42}.
\]

to compute

\[
L_{42,2} = \begin{pmatrix}
0 & 0 & 1 & 1 & 0 & 0 \\
2 & 2x & 0 & 0 & 2 & 0 \\
x^2 & 2x & 0 & 0 & 1 \\
& . & . & . & . & . \\
& . & . & . & . & . \\
& . & . & . & . & .
\end{pmatrix}, \quad L_{42,3} = \begin{pmatrix}
2 & 2x & 0 & 0 & 2 & 0 \\
2x^2 & 4 & 6x & 2x & 0 & 2 \\
2x & 2x^2 & 2x & 0 & 2x & 0 \\
& . & . & . & . & . \\
& . & . & . & . & . \\
& . & . & . & . & .
\end{pmatrix},
\]

\[
L_{42,4} = \begin{pmatrix}
2x^2 & 4 & 6x & 2x & 0 & 2 \\
8x & 8x & 6 & 6 & 8x & 0 \\
& . & . & . & . & . \\
2 + 2x^3 & 6x & 6x^2 & 2x^2 & 2 & 2x \\
& . & . & . & . & . \\
& . & . & . & . & .
\end{pmatrix}.
\]
Decompositions of Linear Ode’s

\[ L_{42,5} = \begin{pmatrix}
8x & 8x^2 & 6 & 6 & 8x & 0 \\
20 + 8x^3 & 36x & 24x^2 & 8x^2 & 20 & 8x \\
12x^2 & 8 + 8x^3 & 18x & 10x & 8x^2 & 4 \\
& & & & & \\
& & & & & \\
& & & & & \\
& & & & & \\
& & & & & \\
\end{pmatrix}, \]

and

\[ L_{42,6} = \begin{pmatrix}
20 + 8x^3 & 36x & 24x^2 & 8x^2 & 20 & 8x \\
60x^2 & 56 + 32x^3 & 108x & 52x & 32x^2 & 28 \\
44x + 8x^4 & 60x^2 & 18 + 24x^3 & 18 + 8x^3 & 44x & 8x^2 \\
& & & & & \\
& & & & & \\
& & & & & \\
& & & & & \\
\end{pmatrix}, \]

where "·" represents the data irrelevant to our computation, because \( W_2 = \Delta_1, W_1 = \Delta_2, \) and \( W_0 = \Delta_3. \) By the sixth step of Beke’s scheme, we find

\[ N_0 = \begin{pmatrix}
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
x^2 & 2x^2 & 6x & 6x^2 & 2x^2 & 2 \\
2 + 2x^3 & 6x & 6x^2 & 2x^2 & 2 & 2x \\
12x^2 & 8 + 8x^3 & 18x & 10x & 8x^2 & 4 \\
44x + 8x^4 & 60x^2 & 18 + 24x^3 & 18 + 8x^3 & 44x & 8x^2 \\
\end{pmatrix}, \]

\[ N_1 = \begin{pmatrix}
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 \\
2 & 2x & 0 & 0 & 2 & 0 \\
2x^2 & 4 & 6x & 2x & 0 & 2 \\
8x & 8x^2 & 6 & 6 & 8x & 0 \\
20 + 8x^3 & 36x & 24x^2 & 8x^2 & 20 & 8x \\
60x^2 & 56 + 32x^3 & 108x & 52x & 32x^2 & 28 \\
\end{pmatrix}, \]

and

\[ N_2 = \begin{pmatrix}
0 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 \\
2 & 2x & 0 & 0 & 2 & 0 \\
2x^2 & 4 & 6x & 2x & 0 & 2 \\
8x & 8x^2 & 6 & 6 & 8x & 0 \\
20 + 8x^3 & 36x & 24x^2 & 8x^2 & 20 & 8x \\
\end{pmatrix}, \]

such that

\[ (W_i, W'_i, \ldots, W^{(6)}_i)^T = N_i(\Delta_1, \Delta_2, \ldots, \Delta_6)^T, \]
where \( i = 1, 2, 3 \). The \( K \)-linear dependence of row-vectors of \( N_i \) \((i = 1, 2, 3)\) gives rise to three linear ODE's

\[
H_0 = -\frac{1}{3} x W_0^{(6)} + W_0^{(5)} + \frac{2}{3} \left( \frac{2x - 3}{x} \right) W_0^{(4)} + \frac{2(x^3 + 1)}{x^2} W_0''',
\]

\[
H_1 = W_1^{(4)} - 4x W_1''' - 6W_1',
\]

and

\[
H_2 = W_2^{(5)} - 4x W_2''' - 6W_2''.
\]

We need only hyperexponential solutions of the \( H \)'s by Lemma ???. Using the method described in Chapter 1, we find that

\[
W_2 = c_1 + c_2 x, \quad c_1, c_2 \in C.
\]

Thus \( W_1 = c_2 \) by \( W_1 = W_1' \) (and, hence, there is no need to solve \( H_1 \)). Hyperexponential solutions of \( H_0 \) are

\[
W_2 = c_3 + c_4 x + c_5 x^2, \quad c_3, c_4, c_5 \in C.
\]

It follows from Lemma ?? that all second-order right factors of \( A \) are in form

\[
F = (c_1 + c_2 x) D^2 - c_2 D + (c_3 + c_4 x + c_5 x^2), \quad c_1, c_2, c_3 \in C.
\]

The condition \( \text{rem}(A, F) = 0 \) leads to the algebraic system:

\[
\begin{align*}
-2c_2^2c_4 - 8c_2c_1c_5 - 10c_1c_2^3 &= 0 \\
-4c_1c_2c_4 - 4c_1^2c_5 - 8c_1^2c_2 &= 0 \\
2c_2^3c_5 + c_2c_3^2 + c_3^3 &= 0 \\
-2c_1^2c_5 + c_1c_2c_4 + c_1c_2^3 &= 0 \\
-4c_2^2 - 4c_2^3c_5 &= 0 \\
2c_2^2c_3 + 2c_2^3c_5 + 2c_2c_3c_5 + 3c_2^2c_2 + c_2^2c_4 + 2c_1c_4c_5 + 4c_1c_2c_4 &= 0 \\
2c_1c_3c_4 - 2c_2c_1c_5 + c_3^2c_4 + 2c_1^2c_3 + c_2c_3^2 &= 0 \\
2c_2c_3c_4 + c_3^3 + 2c_1c_3c_5 + 2c_1^2c_4 + 4c_1c_2c_3 + c_1c_2^3 &= 0 \\
3c_1c_2^2 + 2c_2c_3c_5 + 4c_2c_1c_5 + 2c_2^2c_4 + c_1c_3^2 &= 0 \\
-2c_2^2c_4 - 2c_3^3 &= 0
\end{align*}
\]

Since \( c_1 \) and \( c_2 \) are not zero simultaneously, we have the solutions

\[
\{c_5 = c_5, c_1 = 0, c_4 = 0, c_3 = 0, c_2 = -c_5\},
\]

where \( c_5 \in C \) with \( c_5 \neq 0 \), or

\[
\{c_3 = c_3, c_1 = c_1, c_4 = -c_1, c_2 = -c_3^2/c_1, c_5 = c_3^2/c_1\},
\]

where \( c_3, c_1 \in C \) with \( c_1 \neq 0 \).
3. Transformation and similarity

Without loss of generality, all operators appearing in this section are assumed to be monic. In particular, for $A, B \in K[D]$, $(A, B)$ and $[A, B]$ denote the monic gcrd and monic lchm of $A$ and $B$, respectively.

Definition 3.1  For nonzero $A, B \in K[D]$, 

$$A_1 = [A, B]B^{-1}$$

is called the transform of $A$ by $B$. The operator $A_1$ is denoted by $BAB^{-1}$.

The next proposition describes the geometric meaning of $A_1$.

Proposition 3.1

$$A_1 = BAB^{-1} \iff B(S(A)) = S(A_1).$$

Proof Assume that $A_1 = BAB^{-1}$. Then $A_1B = [A, B]$. Since $[A, B]$ annihilates all elements of $S(A)$, $B$ maps all elements of $S(A)$ into $S(A)$. It remains to show that $B$ is a subjective from $S(A)$ and $S(A_1)$. Notice that $\ker(B) = S(A) \cap S(B)$, so that $\dim \ker(B) = \deg(A, B)$. Thus, $\dim BS(A) = \deg A - \deg(A, B)$. On the other hand

$$\dim S(A_1) = \deg[A, B] - \deg B = \deg A + \deg B - \deg(A, B) - \deg B = \deg A - \deg(A, B).$$

Hence, $\dim B(S(A)) = \dim S(A_1)$, so $B(S(A)) = S(A_1)$. Conversely, assume that $B(S(A)) = S(A_1)$. Let $[A, B] = LB$. We show $A = L$. Since $LB$ annihilates all elements of $S(A)$, $B(S(A)) \subset S(L)$, that is, $S(A_1) \subset S(A)$. As $\dim S(A) = \deg A - \deg(A, B) = \dim S(L)$, $S(A_1) = S(L)$. Hence $A_1 = L$ because both $A_1$ and $L$ are monic.

The next lemma presents useful properties of transformations

Lemma 3.2  1. $(CB)A(CB)^{-1} = C(BAB^{-1})C^{-1}$.

2. $C[A, B]C^{-1} = [CAC^{-1}, CBC^{-1}]$.

3. $C(AB)C^{-1} = (FAF^{-1})(CBA^{-1})$, where $F = ACA^{-1}$.

Proof Let $A_1 = (CB)A(CB)^{-1}$ and $A_2 = C(BAB^{-1})C^{-1}$. By Proposition ?? we have $CB(S(A)) = S(A_1)$, $B(S(A)) = S(BAB^{-1})$, and $C(S(BAB^{-1})) = S(A_2)$.

Hence, $CB(S(A)) = S(A_2)$. It follows that $S(A_1) = S(A_2)$. This proves that $A_1 = A_2$.

Now, let $A_1 = C[A, B]C^{-1}$ and $A_2 = [CAC^{-1}, CBC^{-1}]$. By Proposition ?? we get

$$C(S(A) + S(B)) = S(A_1).$$

On the other hand,

$$S(A_2) = S(CAC^{-1}) + S(CBC^{-1}) = C(S(A)) + C(S(B)) = C(S(A) + S(B)) = S(A_1).$$

It follows from (??) that $A_1 = A_2$. 

Since $[BA, A] = BA$,
\[
C(BA)C^{-1} = [BA, C]C^{-1} = [[BA, A], C]C^{-1} = [BA, A][C, C^{-1}] = [BA, [A, C]]C^{-1} = L[A, C]C^{-1} = L(CAC^{-1}).
\]
\[
[BA, C]A^{-1} = [BA, [A, C]]A^{-1} = [[BA, C], A]A^{-1} = A[BA, C]A^{-1} = [B, ACA^{-1}].
\]
The last equality holds by the second assertion. Hence, $L[A, C]A^{-1} = L(ACA^{-1}) = [B, ACA^{-1}]$. This shows $L = (ACA^{-1})B(ACA^{-1})^{-1}$.

Lemma 3.3

Let $A_1 = BAB^{-1}$. Then the following statements are equivalent.

1. $(A, B) = 1$.
2. $B$ is a bijective from $S(A)$ to $S(A_1)$
3. $\deg A_1 = \deg A$.

If one of the above conditions holds, then there exists $B_1 \in K[D]$ such that $B_1B = 1_{S(A)}$ and $BB_1 = 1_{S(B)}$.

Proof

Since $\gcd(A, B) = 1$ iff $\deg[A, B] = \deg A + \deg B$, the first and third statements are equivalent. If $B$ is a bijective from $S(A)$ to $S(A_1)$, then $\dim S(A) = \dim S(A_1)$. Hence, $\deg A = \deg A_1$. Conversely, if $\deg A = \deg A_1$, then $\dim S(A) = \dim S(A_1)$. Hence, $B$ is a bijective by Proposition 3.3.

Assume now that one of the equivalent conditions holds. Then $(A, B) = 1$. By the Euclid algorithm we find $B_1, F \in K[D]$ such that
\[
B_1B + FA = 1.
\]
Applying $B_1B$ to $S(A)$ is equivalent to applying $1 - FA$ to $S(A)$. $1 - FA$ is the identity mapping of $S(A)$. Thus $B_1B = 1_{S(A)}$. Since $B$ is a bijective, $BB_1$ is the identity mapping of $S(A_1) = B(S(A))$.

Definition 3.2

Two operators $A_1$ and $A_2$ in $K[D]$ are similar if there exists $B \in K[D]$ with $(A, B) = 1$ such that $A_1 = BAB^{-1}$. This relation is denoted by $A_1 \sim A_2$.

Lemma 3.4

1. Let $P \in K[D]$ be irreducible. If $A \sim P$, then $A$ is irreducible too.
2. Let $Q, P_1, \ldots, P_k \in K[D]$. If $Q$ and the product $P_kP_{k-1}\cdots P_1$ are relatively prime, then there are $Q_k, Q_{k-1}, \ldots, Q_1 \in K[D]$ such that
\[
Q(P_kP_{k-1}\cdots P_1)Q^{-1} = (Q_kP_kQ_k^{-1})(Q_{k-1}P_{k-1}Q_{k-1}^{-1})\cdots (Q_1P_1Q_1^{-1})
\]
and $P_i \sim Q_iP_iQ_i^{-1}$.  

Example 4.1 obviously holds. Assume that the assertion holds for \( k \) and \( \deg C < \deg P \). Hence, \( r \) to show that \( (P, P_1) Q^{-1} = FPF^{-1}(QP_1Q^{-1}) \) by Lemma ???. Since \((Q, P_1) = 1\), \( P_1 \sim QP_1Q \). It remains to show that \((F, P) = 1 \). We notice that

\[
\deg(QPP_1Q^{-1}) = \deg P + \deg P_1 \quad \text{and} \quad \deg(QP_1^{-1}Q^{-1}) = \deg P.
\]

Hence, \( \deg(FPP^{-1}) = \deg P \), and so \((F, P) = 1 \) by Lemma ???. The lemma then follows from induction.

4. Resultants

Let nonzero \( A \) and \( B \) be in \( K[D] \) with respective degrees \( m \) and \( n \). The resultant of \( A \) and \( B \), denoted by \( \text{res}(A, B) \), is defined to be the \((m + n) \times (m + n)\) determinant \( |r_{ij}| \), where \( r_{ij} \) is the coefficient of \( D^{m+n-j} \) in \( D^{n-i}A \) for \( i \geq n \), and that in \( D^{m+n-i}B \) if \( i > n \).

Example 4.1 If \( A = a_2D^2 + a_1D + a_0 \) and \( B = b_2D^2 + b_1D + b_0 \), then

\[
DA = a_2D^3 + (a_2' + a_1)D^2 + (a_1' + a_0)D + a_0'
\]

and

\[
DB = b_2D^3 + (b_2' + b_1)D^2 + (b_1' + b_0)D + b_0'.
\]

Hence,

\[
\text{res}(A, B) = \begin{vmatrix}
a_2 & a_2' + a_1 & a_1' + a_0 & a_0' \\
0 & a_2 & a_1 & a_0 \\
b_2 & b_2' + b_1 & b_1' + b_0 & b_0' \\
0 & b_2 & b_1 & b_0
\end{vmatrix}.
\]

The next theorem presents two useful properties of resultants

Theorem 4.1 Let nonzero \( A \) and \( B \) be in \( K[D] \) with respective degrees \( m \) and \( n \).

1. There are \( F, G \in K[D] \) with \( \deg F < n \) and \( \deg G < m \) such that

\[
FA + GB = \text{res}(A, B).
\]

2. \( \text{gcd}(A, B) = 1 \iff \text{res}(A, B) \neq 0 \).

Proof By the definition of resultants we see that the last column of the determinant can be replaced by

\[
(D^{n-1}A, D^{n-1}A, \ldots, A, D^{m-1}B, D^{m-2}B, \ldots, B)^\tau.
\]

Expanding the determinant according to the last column yields the first assertion. (Note: although the last column consists of non-commutative polynomials, such an expansion still makes sense when we put all the minors (w.r.t. the last column) to the left hand-side of any element of the last column).

By the first assertion we find that \( \text{gcd}(A, B) \) is a right divisor of \( \text{res}(A, B) \). Hence, \( \text{res}(A, B) \neq 0 \) implies that \( \text{gcd}(A, B) = 1 \). Conversely, if \( \text{res}(A, B) = 0 \), then \( FA \) is a left common multiple of \( A \) and \( B \) by the first assertion. Since \( \deg FA < m + n \), so is the degree of \( \text{lcm}(A, B) \). Thus, the degree of \( \text{gcd}(A, B) \) is greater than 0 by Theorem ???.
5. Eigenring method

Given nonzero \( A \) in \( K[D] \), a linear operator \( X \) in \( K[D] \) is called an eigenroot of \( A \) if \( \text{rem}(AX, A) = 0 \). The geometric meaning of eigenroots is

**Proposition 5.1** Let \( A \) and \( X \) be in \( K[D] \). \( X \) is an eigenroot of \( A \) iff \( X \) is a linear mapping from \( S(A) \) to itself.

**Proof** Assume that \( X \) is an eigenroot of \( A \). Then there exists \( Q \in K[D] \) such that \( AX = QA \). Hence, \( AX \) annihilates all elements of \( S(A) \), that is, \( X(S(A)) \subseteq S(A) \). Conversely, if \( X(S(A)) \subseteq S(A) \), then \( AX \) annihilates all elements of \( S(A) \). Hence, \( \text{rem}(AX, A) = 0 \). \( \square \)

If \( X \) is an eigenroot of \( A \), then \( X \) and \( \text{rem}(X, A) \) represent the same linear mapping of \( S(A) \). Thus, we only need to consider eigenroots whose degrees are less than \( \deg A \). Denote by \( \mathcal{E}_A \) all eigenroots of \( A \) with degrees less than \( \deg A \). We have

**Theorem 5.2** The set \( \mathcal{E}_A \) is a finite-dimensional \( C \)-algebra whose multiplication is defined as \( X_1X_2 = \text{rem}(X_1X_2, A) \).

**Proof** It is easy to see that all constants are eigenroots of any operators and that any \( C \)-linear combination of eigenroots of \( A \) are eigenroots. Hence \( \mathcal{E}_A \) is a \( C \)-linear space. If \( X_1, X_2 \in \mathcal{E}_A \) represent the same mapping of \( S(A) \), then \( X_1 - X_2 \) annihilates all elements of \( S(A) \), so that \( X_1 = X_2 \) as elements in \( K[D] \) because \( \deg(X_1 - X_2) < \deg A \). Thus, \( \mathcal{E}_A \) can be regarded as a subspace of the \( C \)-linear space consisting of all linear mappings of \( S(A) \). Thus, \( \mathcal{E}_A \) is a finite-dimensional linear space over \( C \). It remains to show that \( \mathcal{E}_A \) is a ring. It is clear that \( 0, 1 \in \mathcal{E}_A \). The addition of \( \mathcal{E}_A \) is the addition in \( \mathcal{E}_A \). We need only to verify the multiplication. This is easy because \( X_1X_2 \) represents the composition of the mappings \( X_1 \circ X_2 \).

Computing \( \mathcal{E}_A \) amounts to finding \( r_{n-1}, \ldots, r_1, r_0 \) in \( K \) such that

\[
\text{rem}(A(r_{n-1}D^{n-1} + \cdots + r_1D + r_0), A) = 0.
\]

This equation gives rise to a linear differential system in \( r_{n-1}, \ldots, r_1, r_0 \). Since a solution of this system corresponds to a linear mapping of \( S(A) \), \( r_i \) must satisfy a linear ode, which can be computed by elimination. Hence, all rational solutions of the linear differential system can be determined.

**Example 5.1** Let \( A = D^2 + \frac{1}{2}D - \left( 1 + \frac{1}{2} \right) \). Compute \( \mathcal{E}_A \). For \( r_1, r_0 \in C(x) \), the equation

\[
\text{rem}(A(r_1D + r_0), A) = 0
\]

gives rise to the system

\[
\begin{cases}
-x^2r_1' + 2x^3r_0' + xr_1 + x^3r_1'' = 0 \\
x^2r_0' + 2x^3r_1' + 2x^2r_1' + x^3r_0'' - xr_1 = 0
\end{cases}
\]

which implies

\[
\begin{aligned}
&\frac{4}{x} - \frac{2(1 + 4x)}{4x^2 + 2x + 1} \right) r_0'' + \left( -4 + \frac{2}{x^2} - \frac{10}{4x^2 + 2x + 1} \right) r_0' + \left( -8 + \frac{16(-1 + 2x)}{4x^2 + 2x + 1} \right) r_0 = 0.
\end{aligned}
\]

Thus, \( r_1 = 0 \) and \( r_0 \) is a complex number. Hence \( \mathcal{E}_A = C \).
Example 5.2 Let $A = (1 + x^2)D^2 + (-x + x^3)D + 1 - x^2$. Compute $E_A$. For $r_1, r_0 \in \mathbb{C}(x)$, the equation
\[ \text{rem}(A(r_1 D + r_0), A) = 0 \]
gives rise to the system
\[
\begin{cases}
(3x^4 + 3x^2 + 1 + x^6)r''_0 + (-x - x^3 + x^2 + x^5)r'_0 \\
\quad + (-2 + 2x^4 - 2x^2 + 2x^6)r'_1 + (4x + 4x^3)r_1 = 0 \\
(2 + 6x^4 + 2x^6 + 6x^2)r'_0 + (3x^4 + 3x^2 + 1 + x^6)r''_0 \\
\quad + (-x^5 + x + x^3 - x^7)r'_1 + (-5x^4 + 1 - 3x^2 - x^6)r_1 = 0
\end{cases}
\]
which implies
\[
\begin{align*}
(-x^4 + 3x^4 + 10x^4 - x^8 + 3 + 10x^6)r^{(4)}_0 + (8x^7 + 40x^5 - 40x^3 + 24x)r''_0 \\
\quad + (x^{12} + x^{10} - 6x^8 - 42x^6 - 75x^4 + 45x^2 + 36)r''_0 \\
\quad + (x^{11} - x^9 - 78x^7 + 42x^5 - 105x^3 - 45x)r'_0 = 0 \\
(-x^6 - 3x^4 - 3x^2 - 3x^2 - 1)r''_1 + (x^{8} + 5x^6 + 13x^4 + 3x^2 - 6)r'_1 + (3x^3 + x^7 + 21x - x^3)r_1 = 0
\end{align*}
\]
Thus,
\[ r_0 = \frac{c_1 + c_2x^2}{1 + x^2}, \quad r_1 = \frac{(c_2 - c_1)x}{1 + x^2}. \]
Hence,
\[ E_A = \left\{ \left( \frac{(c_2 - c_1)x}{1 + x^2}D + \frac{c_1 + c_2x^2}{1 + x^2} \right)| c_1, c_2 \in \mathbb{C} \right\}. \]
The next theorem links eigenrings and factorization.

Theorem 5.3 Let $A$ be in $\mathbb{C}(x)[D]$, where $\mathbb{C}$ is the field of the complex numbers. If $A$ is irreducible over $\mathbb{C}$, then $E_A$ is $\mathbb{C}$. Assume further that $A$ is completely reducible over $K$. Then $E_A$ is irreducible over $\mathbb{C}$ if $E_A$ is $\mathbb{C}$.

Proof Assume that $X$ belongs to $E_A$ with deg $X > 0$. Regard $X$ as a linear mapping of $S(A)$. Let $c \in \mathbb{C}$ be a characteristic set of $X$. Then $X - c$ annihilates a nonzero element of $S(A)$. It follows that $A$ and $X - c$ has a nontrivial gcrd whose degree less than deg $A$. This gcrd is a nontrivial right factor of $A$.

Assume further that $A$ is completely reducible. We show that $E_A = \mathbb{C}$ implies that $A$ is irreducible. Suppose the contrary. Then $A = [F, G]$ where $F, G \in K[D]$ such that gcrd$(F, G) = 1$. Hence, there are $P, Q \in K[D]$ with deg $P < \text{deg } G$ and deg $Q < \text{deg } F$ such that $PF + QG = 1$. Note that $0 < \text{deg } PF < \text{deg } F + \text{deg } G = \text{deg } A$. We claim that $PF$ is an eigenroot of $A$. Clearly, $\text{rem}(FPF, F) = 0$ since $GPF = G(1 - QG) = (1 - GQ)G$ and $\text{rem}(PF, G) = 0$. Thus, $[F, G]PF$ is a left multiple of $F$ and $G$, hence $[F, G]PF$ is right divisible by $[F, G]$. Our claim is proved. Since $0 < \text{deg } PF < \text{deg } A$, $E_A$ is not $\mathbb{C}$, a contradiction.

The operator $A$ in Example ?? factors into $\left( D + \left(1 + \frac{1}{2} \right) \right)^2$. But its eigenring is $\mathbb{C}$. Thus, $A$ is not completely reducible.

This theorem implies an algorithm for factoring completely reducible factors. We proceed as follows to factor $A$.

1. compute a finite basis $X_1, \ldots, X_k$ for $E_A$
2. If $k = 1$, then $A$ is irreducible. Otherwise, pick up an $X_i$ with $\deg X_i > 0$.

3. Regard $X_i$ as a linear mapping of $S(A)$ and compute a characteristic root of $X_i$.

4. Compute $G = \gcd(A, X_i - c)$. $G$ is a nontrivial factor of $A$.

5. Compute $F$ such that $A = \text{lcm}(F, G)$, and apply the same method to both $F$ and $G$.

We need to study how to compute $E_A$, a characteristic root of $X_i$ and $F$. Among them, the easiest one is to compute a characteristic root of a linear mapping $X$ of $S(A)$.

**Lemma 5.4** Let nonzero $X$ be in $K[D]$, where $K = \mathbb{C}(x)$. If $X(S(A)) \subset S(A)$, then the characteristic roots of the linear mapping $A$ are exactly the roots of $\text{content}(\text{res}(A, X - c), x)$.

**Proof** A complex number $c$ is a characteristic root of $X$ if and only if $\gcd(A, X - c)$ is of positive degree if and only if $\text{res}(A, X - c) = 0$.

**Example 5.3** Let $A$ be the same as in Example 5.2. The operator $A$ has nontrivial eigenroots. Pick up one eigenroot

$$X = -\frac{1}{x^2 + 1}(xD - 1).$$

The content (w.r.t. $x$) of $\text{res}(A, X - c)$ is $c(c - 1)$. Hence $\gcd(A, X) = X$ and $\gcd(A, X - 1) = X - 1$ are two right factors of $A$.

The last problem can be addressed as follows.

Let $A$ be a linear differential operator in $K[D]$. Assume that $A = LR$ is a nontrivial factorization over $K$. Decide if there is $S \in K[D]$ such that $\gcd(R, S) = 1$ and $\text{lcm}(R, S) = A$; produce such an $S$ if existent.

**Theorem 5.5** Let $A$, $L$ and $R$ be given as above. Then there exists $S$ such that $\gcd(R, S) = 1$ and $\text{lcm}(R, S) = A$ if and only if there is a linear differential operator $r \in K[D]$ such that $\text{rem}(Rr, L) = 1$.

**Proof** Since $\gcd(R, S) = 1$, there are $r$ and $s$ in $K[D]$ such that

$$rR + sS = 1. \quad (11)$$

Since $V(A) = V(R) \oplus V(S)$, any $v_A \in V(A)$ can be written as a sum $v_R + v_S$, where $v_R \in V(R)$ and $v_S \in V(S)$. Applying $sS$ (as an operator) to $v_A$, we find that

$$sS(v_a) = sS(v_R + v_S) = sS(v_R) = (1 - rR)(v_R) = v_R.$$

Thus

$$rR(v_a) = (1 - sS)(v_a) = v_a - v_R = v_S.$$

It follows that $rR$ acts as the identity on $V(S)$. Now, $R$ is a linear mapping from $V(A)$ to $V(L)$ whose kernel is $V(R)$. Thus $R$ is surjective since

$$\dim_{\mathbb{C}_K} V(A)/V(R) = \dim_{\mathbb{C}_K} V(S) = \deg S = \deg L = \dim_{\mathbb{C}_K} V(L).$$
Hence, $R$ is a linear bijection between $V(S)$ and $V(L)$. It follows that $r$ is the inverse of bijection of $R$, so that $Rr$ acts as the identity on $V(L)$. It follows that $(Rr - 1)$ acts as the null mapping on $V(L)$. Thus $\text{rem}(Rr - 1, L) = 0$, or, equivalently, $\text{rem}(Rr, L) = 1$.

Conversely, if $\text{rem}(Rr, L) = 1$, then there exists $l \in K[D]$ such that $Rr + lL = 1$. Thus $Rr$ acts on $V(L)$ as the identity. Thus $r$ is a bijection from $V(L)$ to $rV(L)$. We now construct a linear differential operator $S$ such that $rV(L) = V(S)$. Let $H_i \text{ be } \text{rem}(X^i r, L)$, for $i = 0, \ldots, \deg L = n$. Then $H_0, \ldots H_n$ are linearly dependent over $K$. Hence there are $b_n, \ldots, b_0$ in $K$, not all 0, such that $\sum_i b_i H_i = 0$. Let $S = b_nX^n + \cdots + b_0$.

Then $Sr + qL = 0$ for some $q \in K[D]$. Thus $Sr$ acts on $V(L)$ as the null mapping, so that $rV(L) \subseteq V(S)$. Since $r$ is a bijection from $V(L)$ to $rV(L)$, we find that $\dim_{C_K}(V(S)) \geq n$. As $\deg S \leq n$, we have $\dim_{C_K}(V(S)) = n$, $\deg S = n$ and $rV(L) = V(S)$. As $Rr$ acts as the identity on $V(L)$, $R$ is a bijection from $V(S)$ to $V(L)$, so $rR$ acts as the identity on $V(S)$, so that $\gcd(R, S) = 1$. If $v_S \in V(S)$, then $R(v_S) \in V(L)$, and hence $LR(v_S) = 0$. That is to say $S$ is a right divisor of $A$. Since $\text{lcm}(S, L)$ has degree $\deg R + \deg S$, which equals $\deg R + \deg L$. $A = \text{lcm}(S, L)$.

\textbf{Remark 5.4} Let $L$ and $r$ be in $K[D]$. We can find $S$ in $K[D]$ such that $V(S) = rV(L)$ by the formula

$$S = \text{lcm}(r, L)r^{-1}.$$  

The proof is as follows. Let $G = \gcd(L, r)$ be of degree $d$. Then the dimension of $rV(L)$ is $\deg L - d$, which is the degree of $S$. So, to prove $V(S) = rV(L)$, it suffices to prove that $rV(L) \subseteq rV(S)$. Note that $\text{lcm}(L, r) = Sr = UL$, for some $U \in K[D]$. For any solution $y$ of $L, Sr(y) = UL(y) = 0$. Thus, $rV(L) \subseteq rV(S)$.

\textbf{Example 5.5} For $A$ given in Example ??, we set

$$R = X = -\frac{1}{x^2 + 1}(xD - 1).$$

Then

$$L = -(1 + x^2)^2 \left(\frac{1}{x} D + 1\right)$$

is the left quotient of $A$ and $R$, that is, $A = LR$. Consider the mixed equation

$$\text{rem}(Rr_0, L) = 1.$$  

We find that

$$(x^3 + x)r'_0 + (-x^4 - 2x^2 - 1)r_0 + 1 + 2x^2 + x^4 = 0$$

whose only rational solution is $1$. Thus, $S = [L, 1]/1 = L$. We get $A = [R, L]$.  

6. Bibliographic notes

The materials in Section ?? are a special case of skew polynomials studied by Ore [?], which is an extension of his results about linear differential operators [?, ?]. A good introduction to basic operations on linear differential operators is the book by Poole [?]. The efficient algorithms for computing gcrds and lclms are described in [?, ?]. Beke’s algorithm was invented by Beke [?]. Modern presentations and improvements are given in [?, ?], respectively. A generalization of Beke’s algorithm to skew polynomials is made by Bronstein and Petkovsek in [?]. Factoring linear differential operators modulo a prime is studied by van der Put [?]. The notion of differential resultants is proposed by Berkovich and Tsirulik [?], and Chardin [?]. Resultants of skew polynomials are defined in [?]. The notion of completely reducible operators may be found in [?], in which solving mixed equations plays an important role. The eigenring method for factoring completely reducible factors is proposed by Singer [?], and the method for computing rational solutions of mixed equations is given by van Hoeji [?].

References


