Algebraic Systems Theory

Eva Zerz
Lehrstuhl D für Mathematik
RWTH Aachen

Februar 2006

Contents

Chapter 1

Introduction

Classical linear systems theory studies, e.g., the continuous and discrete models

$$\begin{array}{lrcl} \text{(C)} & \dot{x}(t) & = & Ax(t) + Bu(t) \\ \text{(D)} & x(t+1) & = & Ax(t) + Bu(t) \end{array}$$

where $A \in \mathbb{R}^{n \times n}$ and $B \in \mathbb{R}^{n \times m}$. One calls

$$x : T \to \mathbb{R}^n \quad \text{and} \quad u : T \to \mathbb{R}^m$$

the **state function** and the **input function**, respectively. The set T represents a mathematical model of time, e.g., $T = \mathbb{R}$ or $T = [0, \infty)$ in the continuous case (C), and $T = \mathbb{Z}$ or $T = \mathbb{N}$ in the discrete case (D).

For (C), we additionally require that $u \in \mathfrak{U}$, where $\mathfrak{U}$ is a function space that guarantees the solvability of (C), that is,

$$\forall u \in \mathfrak{U}\ \exists x : \ \dot{x} = Ax + Bu.$$

For example, this is true whenever $\mathfrak{U} \subseteq \mathcal{C}^0(\mathbb{R}, \mathbb{R}^m)$, the set of continuous functions from $T = \mathbb{R}$ to $\mathbb{R}^m$. We will make this assumption for the rest of this chapter. Note that no such condition is needed for (D), which is always recursively solvable, at least for all $t \geq t_0$ if $x(t_0)$ is given. To unify the notation, we put $\mathfrak{U} = (\mathbb{R}^m)^T$ for (D), which is the space of all functions from T to $\mathbb{R}^m$.

Solving (C) and (D) is not a problem (up to numerical issues), because, imposing the initial condition $x(t_0) = x_0$, we have the solution formulas

$$\begin{array}{llcl} \text{(C)} & x(t) & = & e^{A(t-t_0)}x_0 + \int_{t_0}^{t} e^{A(t-\tau)}Bu(\tau)d\tau \\ \text{(D)} & x(t) & = & A^{t-t_0}x_0 + \sum_{\tau=t_0}^{t-1} A^{t-1-\tau}Bu(\tau) \text{ for } t \geq t_0. \end{array}$$

The goal of control theory is not to solve (C) and (D) for a given input function, but rather, to design an input function such that the solution has certain desired properties. For this, one needs to study the structural properties of the underlying system.

One of the most important issues in control theory is the question of **controllability**: Given $x_0, x_1 \in \mathbb{R}^n$ and $t_0, t_1 \in T$ with $t_0 < t_1$, does there exist $u \in \mathfrak{U}$ such that the solution to (C) or (D) with $x(t_0) = x_0$ satisfies $x(t_1) = x_1$? If yes, we say that x_0 can be **controlled** to x_1 in time $t_1 - t_0 > 0$.

Interpretation: One should think of t_0 and x_0 as a given initial time and state, whereas t_1 and x_1 represents a desired terminal time and state. The problem is to find an input function u such that the system goes to state x_1 in finite time $t_1 - t_0 > 0$, when started in state x_0 at time t_0. Without loss of generality, we put $t_0 = 0$ from now on. Then $t_1 > 0$ is the length of the transition period from the initial state $x(0) = x_0$ to the terminal state $x(t_1) = x_1$.

Theorem 1.1 *The following are equivalent:*

1. *There exists* $0 < t_1 \in T$ *such that any* $x_0 \in \mathbb{R}^n$ *can be controlled to any* $x_1 \in \mathbb{R}^n$ *in time* t_1*.*
2. $\operatorname{rank}[B, AB, \ldots, A^{n-1}B] = n$*.*

Proof: We do this only for the discrete case (D), where it is elementary. From $x(t+1) = Ax(t) + Bu(t)$ and $x(0) = x_0$, we get recursively

$$x(t_1) = A^{t_1}x_0 + \sum_{\tau=0}^{t_1-1} A^{t_1-\tau-1}Bu(\tau).$$

Thus the requirement that $x(t_1) = x_1$ is equivalent to

$$x_1 = A^{t_1}x_0 + K_{t_1}v$$

where

$$K_{t_1} = [B, AB, \ldots, A^{t_1-1}B] \quad \text{and} \quad v = \begin{bmatrix} u(t_1-1) \\ \vdots \\ u(0) \end{bmatrix}.$$

The equation $K_{t_1}v = x_1 - A^{t_1}x_0$ has a solution v for any choice of x_0, x_1 if and only if K_{t_1} has full row rank, that is, $\operatorname{rank}(K_{t_1}) = n$. However, the existence of t_1 with $\operatorname{rank}(K_{t_1}) = n$ is equivalent to $\operatorname{rank}(K_n) = n$. This is quite clear for $t_1 < n$, and for all $t_1 \geq n$, we have

$$\operatorname{rank}[B, AB, \ldots, A^{t_1-1}B] = \operatorname{rank}[B, AB, \ldots, A^{n-1}B].$$

This follows from considering the sequence

$$\{0\} \subseteq \operatorname{im}(B) \subseteq \operatorname{im}[B, AB] \subseteq \ldots \subseteq \operatorname{im}[B, AB, \ldots, A^{n-1}B] \overset{\star}{\subseteq} \ldots \subseteq \mathbb{R}^n$$

of subspaces of $\mathbb{R}^n$, which must become stationary. Considering the dimensions of these spaces, one can see that this cannot happen later than at the inclusion marked by a star. □

If assertion 1 from the theorem is true, we say that the system is **controllable**. The matrix $K = K_n = [B, AB, \ldots, A^{n-1}B]$ is called **Kalman controllability matrix** and Theorem 1.1 is sometimes referred to as Kalman controllability criterion.

What can we say about (C)? Let us first give a careful restatement of the theorem.

Theorem 1.2 (Theorem 1.1 restated for (C)) *The following are equivalent:*

1. $\exists t_1 > 0 \ \forall x_0, x_1 \in \mathbb{R}^n \ \exists u \in \mathfrak{U}$ *such that the solution to*

$$\dot{x} = Ax + Bu, \quad x(0) = x_0$$

   satisfies $x(t_1) = x_1$.

2. $\operatorname{rank}[B, AB, \ldots, A^{n-1}B] = n$.

Note that assertion 1 describes an analytic property of the system, whereas assertion 2 is a purely algebraic condition. An immediate question concerns the role of the set $\mathfrak{U}$ which does not appear in assertion 2. For which sets $\mathfrak{U}$ is the theorem valid? It turns out that the theorem holds for a wide range of input function spaces, more precisely, for any $\mathfrak{U}$ with

$$\mathfrak{U} \supseteq \mathcal{O}(\mathbb{R}, \mathbb{R}^m),$$

where $\mathcal{O}$ denotes the analytic functions. Since this condition is met by a lot of relevant function spaces $\mathfrak{U}$, we can say that the theorem is relatively independent of the specific signal space. This contributes to its importance and applicability. It is a prominent example of an algebraic characterization of a systems theoretic property, which is at the heart of algebraic systems theory.

Roughly speaking, the goals of algebraic systems theory are:

- translating analytic properties of systems to algebraic properties and vice versa;
- characterizing the signal spaces for which this is possible.

Chapter 2

Abstract linear systems theory

Let $\mathcal{D}$ be a ring (with unity), let $\mathcal{A}$ be a left $\mathcal{D}$-module, and let q be a positive integer. An **abstract linear system** has the form

$$\mathcal{B} := \{w \in \mathcal{A}^q \mid Rw = 0\},$$

where $R \in \mathcal{D}^{g \times q}$ for some positive integer g.

Interpretation: One should think of $\mathcal{A}$ as the signal set. Our system involves q signals, that is, we have signal vectors in $\mathcal{A}^q$. The set $\mathcal{B}$ tells us which $w \in \mathcal{A}^q$ can occur in the system: namely, those which satisfy the system law $Rw = 0$. This is a linear system of equations, where the entries of R are elements of $\mathcal{D}$. The ring $\mathcal{D}$ should be thought of as a ring of operators acting on $\mathcal{A}$. Since $\mathcal{A}$ is a left $\mathcal{D}$-module, the expression Rw is a well-defined element of $\mathcal{A}^g$. One calls R a representation of $\mathcal{B}$, because in general, there are many different R's that lead to the same $\mathcal{B}$, whereas $\mathcal{B}$ is uniquely determined by R (once $\mathcal{A}$ is fixed). If R has g rows, then g is the number of defining equations in the given representation R of $\mathcal{B}$. Note that in contrast to q, the number g is not an intrinsic system property (for instance, there may be superfluous equations in the chosen representation R). The letter $\mathcal{B}$ comes from the word "behavior" which was introduced by J. C. Willems [20, 24].

Examples: Let $\mathbb{K}$ denote either $\mathbb{R}$ or $\mathbb{C}$.

- Let $\mathcal{D} = \mathbb{K}[\frac{d}{dt}]$. This leads to the class of systems given by linear ordinary differential equations with constant coefficients. Signal sets $\mathcal{A}$ with a $\mathcal{D}$-module structure are, e.g., $\mathcal{A} = \mathcal{C}^\infty(\mathbb{R}, \mathbb{K})$, the space of smooth functions, or $\mathcal{D}'(\mathbb{R}, \mathbb{K})$, the space of distributions etc. For example, the system $\dot{x} = Ax + Bu$ could be written as an abstract linear system by putting

$$w = \begin{bmatrix} x \\ u \end{bmatrix} \quad \text{and} \quad R = \begin{bmatrix} \frac{d}{dt}I - A, & -B \end{bmatrix}.$$

- Let $\mathcal{D} = \mathbb{F}[\sigma]$, where $\mathbb{F}$ is a field, and σ is the shift operator defined by $(\sigma a)(t) = a(t+1)$ for all $a \in \mathcal{A}$. This leads to the class of systems given by linear ordinary difference equations with constant coefficients. Suitable signal sets are $\mathcal{A} = \mathbb{F}^T$, where $T = \mathbb{N}$ or $T = \mathbb{Z}$. For $x(t+1) = Ax(t)+Bu(t)$, one sets
$$w = \begin{bmatrix} x \\ u \end{bmatrix} \quad \text{and} \quad R = \begin{bmatrix} \sigma I - A, & -B \end{bmatrix}.$$

- Let $\mathcal{D} = \mathbb{K}[\frac{d}{dt}, \sigma]$. This leads to the class of linear delay-differential systems with constant coefficients. A signal set is given by $\mathcal{A} = \mathcal{C}^\infty(\mathbb{R}, \mathbb{K})$.

- Let $\mathcal{D} = \mathbb{K}\langle t, \frac{d}{dt}\rangle$. This leads to the class of systems given by linear ordinary differential equations with polynomial coefficients. The signal sets considered in the first example are still suited. The ring $\mathcal{D}$ is known as **Weyl algebra**. In contrast to the other examples, it is non-commutative, because
$$\tfrac{d}{dt} t a = a + t \tfrac{d}{dt} a \quad \text{for all } a \in \mathcal{A}$$
and thus $\frac{d}{dt}t - t\frac{d}{dt} = 1$. Another non-commutative case is given by $\mathcal{D} = K[\frac{d}{dt}]$ where K is a field of functions, e.g., $K = \mathbb{K}(t)$, the field of rational functions, or $K = \mathcal{M}$, the field of meromorphic functions. This leads to linear ordinary differential equations with coefficients in K. We have $\frac{d}{dt}k - k\frac{d}{dt} = k'$. A signal set is given by $\mathcal{A} = K$.

- Let $\mathcal{D} = \mathbb{F}\langle t, \sigma\rangle$. This leads to the class of linear ordinary difference equations with polynomial coefficients. The signals sets $\mathcal{A} = \mathbb{F}^T$ still work.

- Let $\mathcal{D} = \mathbb{K}[\partial_1, \ldots, \partial_n]$. This leads to the class of systems given by linear partial differential equations with constant coefficients. As signal sets, one could take $\mathcal{A} = \mathcal{C}^\infty(\mathbb{R}^n, \mathbb{K})$ or $\mathcal{A} = \mathcal{D}'(\mathbb{R}^n, \mathbb{K})$.

- Finally, $\mathcal{D} = \mathbb{F}[\sigma_1, \ldots, \sigma_n]$ leads to the class of linear partial difference equations with constant coefficients. A signal set is $\mathcal{A} = \mathbb{F}^{T^n}$, the set of all n-fold indexed sequences with values in $\mathbb{F}$. $\diamondsuit$

2.1 Galois correspondences

Let $B \subseteq \mathcal{A}^q$. Define
$$\mathfrak{M}(B) := \{m \in \mathcal{D}^{1\times q} \mid mw = 0 \text{ for all } w \in B\}.$$

Lemma 2.1 *$\mathfrak{M}(B)$ is a left $\mathcal{D}$-submodule of $\mathcal{D}^{1\times q}$.*

Proof: Let $m_1, m_2 \in \mathfrak{M}(B)$, $d_1, d_2 \in \mathcal{D}$. Since $m_1 w = m_2 w = 0$ for all $w \in B$, we have $(d_1 m_1 + d_2 m_2)w = 0$ for all $w \in B$. Thus $d_1 m_1 + d_2 m_2 \in \mathfrak{M}(B)$. □

We call $\mathfrak{M}(B)$ the **module of all equations** satisfied by B. Conversely, let $M \subseteq \mathcal{D}^{1\times q}$. Define

$$\mathfrak{B}(M) := \{w \in \mathcal{A}^q \mid mw = 0 \text{ for all } m \in M\}.$$

Lemma 2.2 *$\mathfrak{B}(M)$ is an (additive) Abelian subgroup of $\mathcal{A}^q$.*

Proof: We have $0 \in \mathfrak{B}(M)$ and if $w, w_1, w_2 \in \mathfrak{B}(M)$, then $-w \in \mathfrak{B}(M)$ and $w_1 + w_2 \in \mathfrak{B}(M)$. □

Note: $\mathfrak{B}(M)$ is not a left $\mathcal{D}$-submodule of $\mathcal{A}^q$, in general.

Example: Let $\mathcal{D} = \mathbb{K}\langle t, \frac{d}{dt}\rangle$, $\mathcal{A} = \mathbb{K}[t]$, and $q = 1$. Take $M = \{\frac{d}{dt}\}$, then

$$\mathfrak{B}(M) = \{w \in \mathcal{A} \mid \tfrac{dw}{dt} = 0\},$$

which clearly consists of all constants. Hence for any $0 \neq c \in \mathbb{K}$, we have $c \in \mathfrak{B}(M)$, but $tc \notin \mathfrak{B}(M)$, showing that $\mathfrak{B}(M)$ is not a left $\mathcal{D}$-module. ♢

Remark: If $\mathcal{D}$ is commutative, then $\mathfrak{B}(M)$ is a (left) $\mathcal{D}$-module. To see this, let $w_1, w_2 \in \mathfrak{B}(M)$ and $d_1, d_2 \in \mathcal{D}$. Since $mw_1 = mw_2 = 0$ for all $m \in M$, we have $m(d_1 w_1 + d_2 w_2) = md_1 w_1 + md_2 w_2 = d_1 m w_1 + d_2 m w_2 = 0$ for all $m \in M$ and hence $d_1 w_1 + d_2 w_2 \in \mathfrak{B}(M)$.

Let $\mathbf{A}$ denote the set of all Abelian subgroups of $\mathcal{A}^q$ and let $\mathbf{M}$ denote the set of all left $\mathcal{D}$-submodules of $\mathcal{D}^{1\times q}$. We have a **Galois correspondence**

$$\begin{array}{rcl} \mathbf{A} & \leftrightarrow & \mathbf{M} \\ B & \rightarrow & \mathfrak{M}(B) \\ \mathfrak{B}(M) & \leftarrow & M. \end{array}$$

The term "Galois correspondence" means that

- $\mathfrak{M}$ and $\mathfrak{B}$ are inclusion-reversing, that is,
  $$B_1 \subseteq B_2 \Rightarrow \mathfrak{M}(B_1) \supseteq \mathfrak{M}(B_2) \quad \text{and} \quad M_1 \subseteq M_2 \Rightarrow \mathfrak{B}(M_1) \supseteq \mathfrak{B}(M_2);$$
- $B \subseteq \mathfrak{B}\mathfrak{M}(B)$ for all B and $M \subseteq \mathfrak{M}\mathfrak{B}(M)$ for all M.

Lemma 2.3 *Let $B_1, B_2 \in \mathbf{A}$ and $M_1, M_2 \in \mathbf{M}$. Then we have*

$$\mathfrak{B}(M_1 + M_2) = \mathfrak{B}(M_1) \cap \mathfrak{B}(M_2) \tag{2.1}$$
$$\mathfrak{M}(B_1 \cap B_2) \supseteq \mathfrak{M}(B_1) + \mathfrak{M}(B_2) \tag{2.2}$$

$$\mathfrak{B}(M_1 \cap M_2) \supseteq \mathfrak{B}(M_1) + \mathfrak{B}(M_2) \tag{2.3}$$
$$\mathfrak{M}(B_1 + B_2) = \mathfrak{M}(B_1) \cap \mathfrak{M}(B_2). \tag{2.4}$$

Moreover, $\mathfrak{B}(0) = \mathcal{A}^q$, $\mathfrak{B}(\mathcal{D}^{1\times q}) = 0$, $\mathfrak{M}(0) = \mathcal{D}^{1\times q}$.

Proof: Let $w \in \mathfrak{B}(M_1 + M_2)$. This means that $(m_1 + m_2)w = 0$ for all $m_1 \in M_1$, $m_2 \in M_2$. Since $0 \in M_i$, this is equivalent to $m_1 w = 0$ and $m_2 w = 0$ for all $m_1 \in M_1$ and all $m_2 \in M_2$. Thus, still equivalently, $w \in \mathfrak{B}(M_1) \cap \mathfrak{B}(M_2)$.

Let $m \in \mathfrak{M}(B_1) + \mathfrak{M}(B_2)$, that is, $m = m_1 + m_2$ with $m_1 w_1 = 0$ for all $w_1 \in B_1$ and $m_2 w_2 = 0$ for all $w_2 \in B_2$. Let $w \in B_1 \cap B_2$, then $mw = m_1 w + m_2 w = 0$. Thus $m \in \mathfrak{M}(B_1 \cap B_2)$.

Let $w \in \mathfrak{B}(M_1) + \mathfrak{B}(M_2)$, that is, $w = w_1 + w_2$ with $m_1 w_1 = 0$ for all $m_1 \in M_1$ and $m_2 w_2 = 0$ for all $m_2 \in M_2$. Let $m \in M_1 \cap M_2$. Then $mw = mw_1 + mw_2 = 0$. Thus $w \in \mathfrak{B}(M_1 \cap M_2)$.

Let $m \in \mathfrak{M}(B_1 + B_2)$. This means that $m(w_1 + w_2) = 0$ for all $w_1 \in B_1$, $w_2 \in B_2$. Since $0 \in B_i$, this is equivalent to $mw_1 = 0$ for all $w_1 \in B_1$ and $mw_2 = 0$ for all $w_2 \in B_2$. Still equivalently, $m \in \mathfrak{M}(B_1) \cap \mathfrak{M}(B_2)$. □

Remark: Note that the three equalities $\mathfrak{B}(0) = \mathcal{A}^q$, $\mathfrak{B}(\mathcal{D}^{1\times q}) = 0$, $\mathfrak{M}(0) = \mathcal{D}^{1\times q}$ are more or less trivial, whereas $\mathfrak{M}(\mathcal{A}^q) = 0$ is not true in general.

Assumption: Let us assume from now on that $\mathcal{D}$ is left Noetherian. This means that the following equivalent conditions are satisfied:

- Every ascending chain $\mathcal{I}_0 \subseteq \mathcal{I}_1 \subseteq \mathcal{I}_2 \subseteq \ldots$ of left ideals in $\mathcal{D}$ must become stationary.
- Every left ideal $\mathcal{I}$ in $\mathcal{D}$ is finitely generated.
- Every non-empty set of left ideals in $\mathcal{D}$ possesses a maximal element (with respect to inclusion).

Note that in all of the examples from above, $\mathcal{D}$ is left Noetherian (if $\mathcal{D}$ is commutative, there is no need to distinguish between left and right Noetherian, and then one simply says "Noetherian"). If $\mathcal{D}$ is left Noetherian, then the finitely generated $\mathcal{D}$-module $\mathcal{D}^{1\times q}$ is a left Noetherian module, which means that the following equivalent conditions are satisfied:

- Every ascending chain $M_0 \subseteq M_1 \subseteq M_2 \subseteq \ldots$ of left submodules of $\mathcal{D}^{1\times q}$ must become stationary.
- Every left submodule of $\mathcal{D}^{1\times q}$ is finitely generated.
- Every non-empty family of left submodules of $\mathcal{D}^{1\times q}$ possesses a maximal element.

Thus every $M \in \mathbf{M}$ is finitely generated, that is, $M = \mathcal{D}^{1\times g}R$ for some suitable integer g and $R \in \mathcal{D}^{g\times q}$. Then

$$\mathfrak{B}(M) = \{w \in \mathcal{A}^q \mid Rw = 0\}.$$

Hence we can characterize $\mathbf{B} := \mathfrak{B}(\mathbf{M})$ as follows: It consists of all $\mathcal{B}$ of the form $\mathcal{B} = \{w \in \mathcal{A}^q \mid Rw = 0\}$, where R is an arbitrary $\mathcal{D}$-matrix with q columns, that is, $\mathbf{B}$ consists of all abstract linear systems.

Thus we have an induced Galois correspondence

$$\begin{array}{rcl} \mathbf{B} & \leftrightarrow & \mathbf{M} \\ \mathcal{B} & \rightarrow & \mathfrak{M}(\mathcal{B}) \\ \mathfrak{B}(M) & \leftarrow & M \end{array} \tag{2.5}$$

with

$$\mathfrak{B}\mathfrak{M}(\mathcal{B}) = \mathcal{B}$$

for all abstract linear systems $\mathcal{B} \in \mathbf{B}$. On the other hand, we only have

$$\mathfrak{M}\mathfrak{B}(M) \supseteq M$$

for $M \in \mathbf{M}$. The module $\mathfrak{M}\mathfrak{B}(M)$ is sometimes called the **(Willems) closure** of M with respect to $\mathcal{A}$, denoted by $\overline{M} := \mathfrak{M}\mathfrak{B}(M)$. This is due to the following properties, which hold for all $M, M_1, M_2 \in \mathbf{M}$:

- $M \subseteq \overline{M}$;
- $\overline{\overline{M}} = \overline{M}$;
- $M_1 \subseteq M_2 \Rightarrow \overline{M_1} \subseteq \overline{M_2}$.

The module M is called **(Willems) closed** with respect to $\mathcal{A}$ if $M = \overline{M}$, or equivalently, if $M \in \mathrm{im}(\mathfrak{M})$.

Using these notions, we can be more specific about the inclusion (2.2).

Lemma 2.4 *Let* $\mathcal{B}_1, \mathcal{B}_2 \in \mathbf{B}$. *Then*

$$\mathfrak{M}(\mathcal{B}_1 \cap \mathcal{B}_2) = \overline{\mathfrak{M}(\mathcal{B}_1) + \mathfrak{M}(\mathcal{B}_2)}.$$

Proof: We have $\mathcal{B}_i = \mathfrak{B}\mathfrak{M}(\mathcal{B}_i)$ and thus

$$\begin{array}{rcl} \mathfrak{M}(\mathcal{B}_1 \cap \mathcal{B}_2) & = & \mathfrak{M}(\mathfrak{B}\mathfrak{M}(\mathcal{B}_1) \cap \mathfrak{B}\mathfrak{M}(\mathcal{B}_2)) \\ & = & \mathfrak{M}\mathfrak{B}(\mathfrak{M}(\mathcal{B}_1) + \mathfrak{M}(\mathcal{B}_2)) \\ & = & \overline{\mathfrak{M}(\mathcal{B}_1) + \mathfrak{M}(\mathcal{B}_2)}, \end{array}$$

where we have used (2.1). □

In what follows, we will study $\mathcal{D}$-modules $\mathcal{A}$ with the property that every $M \in \mathbf{M}$ is closed with respect to $\mathcal{A}$. This is equivalent to $\mathbf{M} = \mathrm{im}(\mathfrak{M})$. Then the Galois correspondence (2.5) will become a pair of inclusion-reversing bijections inverse to each other, and the inclusion (2.2) will become an identity when applied to $\mathcal{B}_1, \mathcal{B}_2 \in \mathbf{B}$. Similarly, we will have $\mathfrak{M}(\mathcal{A}^q) = 0$. This is a good starting point for algebraic systems theory, because it makes it possible to translate statements from the system universe $\mathbf{B}$ to the algebraic setting $\mathbf{M}$ and vice versa. It will turn out that this works for many relevant choices of $\mathcal{D}$-modules $\mathcal{A}$. A counterexample is given next.

Example: Let $\mathcal{D} = \mathbb{K}[\frac{d}{dt}, \sigma]$ and let $\mathcal{A} = \mathcal{C}^\infty(\mathbb{R}, \mathbb{K})$. Let $R = \frac{d}{dt}$ and $M = \mathcal{D}R$. Then $\mathcal{B} = \mathfrak{B}(M)$ consists of all constants functions. However, any constant function a also satisfies

$$a(t+1) = a(t) \quad \text{for all } t \in \mathbb{R}.$$

Thus $\sigma - 1 \in \mathfrak{M}(\mathcal{B}) = \overline{M}$, although $\sigma - 1 \notin M$. This shows that the inclusion $M \subset \overline{M}$ is strict, in general. ♢

Remark: Note that for $M_1, M_2 \in \mathbf{M}$, we have $M_1 \cap M_2, M_1 + M_2 \in \mathbf{M}$. Similarly, for $B_1, B_2 \in \mathbf{A}$, we have $B_1 \cap B_2, B_1 + B_2 \in \mathbf{A}$. This was tacitly used in Lemma 2.3. However, $\mathcal{B}_1, \mathcal{B}_2 \in \mathbf{B}$ implies that $\mathcal{B}_1 \cap \mathcal{B}_2 \in \mathbf{B}$, but $\mathcal{B}_1 + \mathcal{B}_2 \in \mathbf{B}$ is not necessarily true. It turns out that, assuming $\mathbf{M} = \mathrm{im}(\mathfrak{M})$, equality holds in (2.3) if and only if $\mathbf{B}$ is closed under addition. If we have this additional property, then the Galois correspondence (2.5) will become a lattice anti-isomorphism. This situation is the optimal environment for algebraic systems theory. Therefore we will also investigate the question under which conditions $\mathbf{B}$ is closed under addition.

2.2 Property O

Let $\mathcal{D}$ be a left Noetherian ring, let q be a positive integer, and let $\mathbf{M}$ denote the set of all left $\mathcal{D}$-submodules of $\mathcal{D}^{1\times q}$. If $\mathcal{A}$ is a left $\mathcal{D}$-module, we use the notation

$$\mathfrak{B}_{\mathcal{A}}(M) := \{w \in \mathcal{A}^q \mid mw = 0 \text{ for all } m \in M\}$$

for $M \in \mathbf{M}$ and

$$\mathfrak{M}(B) := \{m \in \mathcal{D}^{1\times q} \mid mw = 0 \text{ for all } w \in B\}$$

for $B \subseteq \mathcal{A}^q$. Recall that $\overline{M}^{\mathcal{A}} := \mathfrak{M}\mathfrak{B}_{\mathcal{A}}(M)$ is the closure of M with respect to $\mathcal{A}$. We are interested in $\mathcal{D}$-modules $\mathcal{A}$ with the property that every $M \in \mathbf{M}$ is closed with respect to $\mathcal{A}$. Let us call this **property O** (named after U. Oberst [17]).

Lemma 2.5 *Let $\mathcal{A}_1 \subseteq \mathcal{A}_2$ be two left $\mathcal{D}$-modules. If $\mathcal{A}_1$ has property O, then so has $\mathcal{A}_2$.*

Proof: Let $M \in \mathbf{M}$. Since $\mathcal{A}_1 \subseteq \mathcal{A}_2$, we have $\mathfrak{B}_{\mathcal{A}_1}(M) \subseteq \mathfrak{B}_{\mathcal{A}_2}(M)$. Applying the inclusion-reversing map $\mathfrak{M}$, we obtain

$$\overline{M}^{\mathcal{A}_1} = \mathfrak{M}\mathfrak{B}_{\mathcal{A}_1}(M) \supseteq \mathfrak{M}\mathfrak{B}_{\mathcal{A}_2}(M) = \overline{M}^{\mathcal{A}_2}.$$

If $\mathcal{A}_1$ has property O, then this implies

$$M = \overline{M}^{\mathcal{A}_1} \supseteq \overline{M}^{\mathcal{A}_2}.$$

Since the inclusion $\overline{M}^{\mathcal{A}_2} \supseteq M$ is always true, we obtain $M = \overline{M}^{\mathcal{A}_2}$. Thus $\mathcal{A}_2$ has property O. □

Some signal sets with property O

Theorem 2.6 *Let $\mathcal{D} = \mathbb{K}[\frac{d}{dt}]$. Let $\mathcal{A}$ be the set of all polynomial-exponential functions, that is, all a of the form*

$$a(t) = \textstyle\sum_{i=1}^{k} p_i(t) e^{\lambda_i t} \quad \textit{for all } t \in T = \mathbb{R}$$

where $k \in \mathbb{N}$, $p_i \in \mathbb{C}[t]$ and $\lambda_i \in \mathbb{C}$. Then $\mathcal{A}$ has property O.

Remark: If $\mathbb{K} = \mathbb{R}$, one has to make the additional assumption that for all i with $p_i \neq 0$, there exists j such that $\lambda_j = \overline{\lambda_i}$ and $p_j = \overline{p_i}$ in order to get real-valued signals. In the following, this will be taken for granted tacitly.

Thus all $\mathbb{K}[\frac{d}{dt}]$-modules that contain the polynomial-exponential functions also have property O. This is true for $\mathcal{O}(\mathbb{R}, \mathbb{K})$, $\mathcal{C}^\infty(\mathbb{R}, \mathbb{K})$, and even $\mathcal{D}'(\mathbb{R}, \mathbb{K})$ (using the usual identification between a continuous function and the regular distribution it generates).

The discrete counterpart of the above theorem is stated next.

Theorem 2.7 *Let $\mathcal{D} = \mathbb{K}[\sigma]$. Let $\mathcal{A}$ be the set of all polynomial-exponential functions, that is, all a of the form*

$$a(t) = \textstyle\sum_{i=1}^{k} p_i(t) \lambda_i{}^t \quad \textit{for all } l \leq t \in T = \mathbb{N}$$

where $k, l \in \mathbb{N}$, $p_i \in \mathbb{C}[t]$ and $\lambda_i \in \mathbb{C}$. Then $\mathcal{A}$ has property O.

Remark: Thus the $\mathbb{K}[\sigma]$-module $\mathbb{K}^{\mathbb{N}}$ has property O. Note that Theorem 2.7 is not valid for $T = \mathbb{Z}$. This can be seen from the following example. However, the problem can easily be repaired, see Theorem 2.8 below.

Example: Let $R = \sigma$ and $M = \mathbb{K}[\sigma]R$. Since σ is invertible on $\mathbb{K}^{\mathbb{Z}}$, we obtain $\mathfrak{B}_{\mathcal{A}}(M) = 0$ for $\mathcal{A} = \mathbb{K}^{\mathbb{Z}}$. Thus $\overline{M}^{\mathcal{A}} = \mathbb{K}[\sigma] \neq M$. This shows that no $\mathcal{A} \subseteq \mathbb{K}^{\mathbb{Z}}$ has property O as a $\mathbb{K}[\sigma]$-module. $\Diamond$

Theorem 2.8 *Let $\mathcal{D} = \mathbb{K}[\sigma, \sigma^{-1}]$. Let $\mathcal{A}$ be the set of all polynomial-exponential functions, that is, all a of the form*

$$a(t) = \textstyle\sum_{i=1}^{k} p_i(t)\lambda_i^{\,t} \quad \text{for all } t \in T = \mathbb{Z}$$

where $k \in \mathbb{N}$, $p_i \in \mathbb{C}[t]$ and $\lambda_i \in \mathbb{C} \setminus \{0\}$. Then $\mathcal{A}$ has property O.

Remark: Thus $\mathbb{K}^{\mathbb{Z}}$ has property O when considered as a module over the ring $\mathcal{D} = \mathbb{K}[\sigma, \sigma^{-1}]$.

Theorem 2.9 *Let n be a positive integer and let $\mathcal{D} = \mathbb{K}[\partial_1, \ldots, \partial_n]$. Let $\mathcal{A}$ be the set of all polynomial-exponential functions, that is, all a of the form*

$$a(t) = \textstyle\sum_{i=1}^{k} p_i(t)e^{\lambda_i t} \quad \text{for all } t \in \mathbb{R}^n$$

where $k \in \mathbb{N}$, $p_i \in \mathbb{C}[t_1, \ldots, t_n]$ and $\lambda_i \in \mathbb{C}^{1\times n}$. Then $\mathcal{A}$ has property O.

Remark: Therefore, all $\mathbb{K}[\partial_1, \ldots, \partial_n]$-modules that contain the polynomial-exponential functions also have property O. This is true, e.g., for $\mathcal{O}(\mathbb{R}^n, \mathbb{K})$, $\mathcal{C}^{\infty}(\mathbb{R}^n, \mathbb{K})$, and $\mathcal{D}'(\mathbb{R}^n, \mathbb{K})$.

Also this theorem has discrete counterparts.

Theorem 2.10 *Let $\mathcal{D} = \mathbb{K}[\sigma_1, \ldots, \sigma_n]$. Let $\mathcal{A}$ be the set of all polynomial-exponential functions, that is, all a of the form*

$$a(t) = \textstyle\sum_{i=1}^{k} p_i(t)\lambda_i^{t} \quad \text{for all } l \leq t \in \mathbb{N}^n$$

where $k \in \mathbb{N}$, $l \in \mathbb{N}^n$ ($l \leq t$ means $l_i \leq t_i$ for all i) $p_i \in \mathbb{C}[t_1, \ldots, t_n]$ and $\lambda_i \in \mathbb{C}^{1\times n}$. Here, $\lambda_i^t = \lambda_{i1}^{t_1} \cdots \lambda_{in}^{t_n}$ has to be understood as a multi-index notation. Then $\mathcal{A}$ has property O.

Theorem 2.11 *Let $\mathcal{D} = \mathbb{K}[\sigma_1, \ldots, \sigma_n, \sigma_1^{-1}, \ldots, \sigma_n^{-1}]$. Let $\mathcal{A}$ be the set of all polynomial-exponential functions, that is, all a of the form*

$$a(t) = \textstyle\sum_{i=1}^{k} p_i(t)\lambda_i^{t} \quad \text{for all } t \in \mathbb{Z}^n$$

where $k \in \mathbb{N}$, $p_i \in \mathbb{C}[t_1, \ldots, t_n]$ and $\lambda_i \in (\mathbb{C} \setminus \{0\})^{1\times n}$. Then $\mathcal{A}$ has property O.

Remark: Thus the $\mathbb{K}[\sigma_1, \ldots, \sigma_n]$-module $\mathcal{A} = \mathbb{K}^{\mathbb{N}^n}$ has property O, and the same holds for the $\mathbb{K}[\sigma_1, \ldots, \sigma_n, \sigma_1^{-1}, \ldots, \sigma_n^{-1}]$-module $\mathcal{A} = \mathbb{K}^{\mathbb{Z}^n}$.

Consequences of property O

Let $\mathcal{A}$ be a $\mathcal{D}$-module with property O. Then the Galois correspondence

$$\begin{array}{rcl} \mathbf{B} & \leftrightarrow & \mathbf{M} \\ \mathcal{B} & \to & \mathfrak{M}(\mathcal{B}) \\ \mathfrak{B}(M) & \leftarrow & M \end{array}$$

consists of two inclusion-reversing bijections inverse to each other. Concretely, we have a 1-1 correspondence between $\mathcal{B} = \{w \in \mathcal{A}^q \mid Rw = 0\}$ and $M = \mathcal{D}^{1\times g}R$ for any $R \in \mathcal{D}^{g\times q}$. In particular, we have $\mathfrak{M}(\mathcal{A}^q) = 0$, that is, there is non-zero $m \in \mathcal{D}^{1\times q}$ such that m annihilates all signal vectors $w \in \mathcal{A}^q$, or equivalently, there is no $0 \neq d \in \mathcal{D}$ such that $d\mathcal{A} = 0$.

Moreover, we have for all $\mathcal{B}_1, \mathcal{B}_2 \in \mathbf{B}$ and all $M_1, M_2 \in \mathbf{M}$

$$\begin{array}{rcl} \mathfrak{B}(M_1 + M_2) & = & \mathfrak{B}(M_1) \cap \mathfrak{B}(M_2) \\ \mathfrak{M}(\mathcal{B}_1 \cap \mathcal{B}_2) & = & \mathfrak{M}(\mathcal{B}_1) + \mathfrak{M}(\mathcal{B}_2) \\ \mathfrak{M}(\mathcal{B}_1 + \mathcal{B}_2) & = & \mathfrak{M}(\mathcal{B}_1) \cap \mathfrak{M}(\mathcal{B}_2), \end{array}$$

but the last equation uses that $\mathfrak{M}$ is actually defined on all of $\mathbf{A}$, because $\mathcal{B}_1 + \mathcal{B}_2$ in not necessarily in $\mathbf{B}$. This small flaw can be removed if we assume additionally that $\mathbf{B}$ is closed under addition. Then we also have

$$\mathfrak{B}(M_1 \cap M_2) = \mathfrak{B}(M_1) + \mathfrak{B}(M_2)$$

for all $M_1, M_2 \in \mathbf{M}$, and the Galois correspondence establishes a lattice anti-isomorphism.

An important consequence of property O is the following characterization of the inclusion of abstract linear systems.

Theorem 2.12 *Let R_1, R_2 be two $\mathcal{D}$-matrices with q columns. Let $\mathcal{B}_1, \mathcal{B}_2$ be the corresponding abstract linear systems and let M_1, M_2 be the resulting modules. We have*

$$\mathcal{B}_1 \subseteq \mathcal{B}_2 \quad \Leftrightarrow \quad M_1 \supseteq M_2 \quad \Leftrightarrow \quad \exists X \in \mathcal{D}^{g_2\times g_1} : R_2 = XR_1.$$

As a consequence, we have $\mathcal{B}_1 = \mathcal{B}_2$ if and only if there exist $\mathcal{D}$-matrices X and Y such that $R_2 = XR_1$ and $R_1 = YR_2$. This determines the non-uniqueness of the representation R of an abstract linear system $\mathcal{B}$.

Corollary 2.13 *Let R, $\mathcal{B}$ and M be as above. We have*

$$\begin{array}{lclcl} \mathcal{B} = \mathcal{A}^q & \Leftrightarrow & M = 0 & \Leftrightarrow & R = 0 \quad \textit{and} \\ \mathcal{B} = 0 & \Leftrightarrow & M = \mathcal{D}^{1\times q} & \Leftrightarrow & \exists X \in \mathcal{D}^{q\times g} : I_q = XR. \end{array}$$

2.3 The Malgrange isomorphism

Let $M \in \mathbf{M}$, that is, $M = \mathcal{D}^{1\times g}R$ for some $R \in \mathcal{D}^{g\times q}$, and let $\mathcal{B} = \mathfrak{B}(M) = \{w \in \mathcal{A}^q \mid Rw = 0\}$ be an abstract linear system. In some cases, it is preferable to work with $\mathcal{M} := \mathcal{D}^{1\times q}/M$ instead of M itself. The left $\mathcal{D}$-module $\mathcal{M}$ will be called the **system module** of $\mathcal{B}$. Its relevance is due to the so-called Malgrange isomorphism [14]. To understand it, we need some preparation from algebra.

Hom functors

If $\mathcal{M}$ and $\mathcal{A}$ are left $\mathcal{D}$-modules, we define

$$\mathrm{Hom}_{\mathcal{D}}(\mathcal{M}, \mathcal{A}) := \{\phi : \mathcal{M} \to \mathcal{A} \mid \phi \text{ is } \mathcal{D}\text{-linear}\}.$$

Remark: This is an Abelian group, but in general, not a left $\mathcal{D}$-module. However, if $\mathcal{D}$ is commutative, then $\mathrm{Hom}_{\mathcal{D}}(\mathcal{M}, \mathcal{A})$ is a $\mathcal{D}$-module.

$\mathrm{Hom}_{\mathcal{D}}(\cdot, \mathcal{A})$ is a **contravariant functor**. This means that it assigns to each left $\mathcal{D}$-module $\mathcal{M}$ the Abelian group $\mathrm{Hom}_{\mathcal{D}}(\mathcal{M}, \mathcal{A})$ and to each $\mathcal{D}$-linear map $f : \mathcal{M} \to \mathcal{N}$, where $\mathcal{N}$ is another left $\mathcal{D}$-module, the group homomorphism

$$\mathrm{Hom}_{\mathcal{D}}(f, \mathcal{A}) : \mathrm{Hom}_{\mathcal{D}}(\mathcal{N}, \mathcal{A}) \to \mathrm{Hom}_{\mathcal{D}}(\mathcal{M}, \mathcal{A}), \quad \psi \mapsto \psi \circ f.$$

Let $\mathcal{M}, \mathcal{N}, \mathcal{P}$ be left $\mathcal{D}$-modules and let $f : \mathcal{M} \to \mathcal{N}$ and $g : \mathcal{N} \to \mathcal{P}$ be $\mathcal{D}$-linear maps. We say that

$$\mathcal{M} \xrightarrow{f} \mathcal{N} \xrightarrow{g} \mathcal{P}$$

is **exact** if $\mathrm{im}(f) = \ker(g)$. For example, the sequence $0 \to \mathcal{M} \xrightarrow{f} \mathcal{N}$ is exact if and only if f is injective, and the sequence $\mathcal{M} \xrightarrow{f} \mathcal{N} \to 0$ is exact if and only if f is surjective.

Lemma 2.14 *The functor* $\mathrm{Hom}_{\mathcal{D}}(\cdot, \mathcal{A})$ *is left exact, that is, if*

$$\mathcal{M} \xrightarrow{f} \mathcal{N} \xrightarrow{g} \mathcal{P} \longrightarrow 0$$

is exact, then

$$\mathrm{Hom}_{\mathcal{D}}(\mathcal{M}, \mathcal{A}) \xleftarrow{\mathrm{Hom}_{\mathcal{D}}(f,\mathcal{A})} \mathrm{Hom}_{\mathcal{D}}(\mathcal{N}, \mathcal{A}) \xleftarrow{\mathrm{Hom}_{\mathcal{D}}(g,\mathcal{A})} \mathrm{Hom}_{\mathcal{D}}(\mathcal{P}, \mathcal{A}) \longleftarrow 0$$

is also exact.

The Malgrange isomorphism

Theorem 2.15 *Let $R \in \mathcal{D}^{g\times q}$, $\mathcal{B} = \{w \in \mathcal{A}^q \mid Rw = 0\}$, $M = \mathcal{D}^{1\times g}R$, and $\mathcal{M} = \mathcal{D}^{1\times q}/M$. There is a group isomorphism*

$$\mathcal{B} \cong \mathrm{Hom}_{\mathcal{D}}(\mathcal{M}, \mathcal{A}), \quad w \mapsto \phi_w,$$

where $\phi_w : \mathcal{M} \to \mathcal{A}, [x] = x + M \mapsto \phi_w([x]) := xw$, for all $x \in \mathcal{D}^{1\times q}$. This is the so-called **Malgrange isomorphism**.

Proof: Since $M = \mathcal{D}^{1\times g}R =: \mathrm{im}(\cdot R)$ and $\mathcal{M} = \mathcal{D}^{1\times q}/M$, there is an exact sequence

$$\mathcal{D}^{1\times g} \xrightarrow{\cdot R} \mathcal{D}^{1\times q} \longrightarrow \mathcal{M} \longrightarrow 0.$$

This yields an exact sequence

$$\mathrm{Hom}_{\mathcal{D}}(\mathcal{D}^{1\times g}, \mathcal{A}) \xleftarrow{j} \mathrm{Hom}_{\mathcal{D}}(\mathcal{D}^{1\times q}, \mathcal{A}) \xleftarrow{i} \mathrm{Hom}_{\mathcal{D}}(\mathcal{M}, \mathcal{A}) \longleftarrow 0.$$

The mapping i is injective, and hence its domain $\mathrm{Hom}_{\mathcal{D}}(\mathcal{M}, \mathcal{A})$ is isomorphic to $\mathrm{im}(i)$, which equals $\ker(j)$. We have

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{D}}(\mathcal{D}^{1\times g}, \mathcal{A}) & \xleftarrow{j} & \mathrm{Hom}_{\mathcal{D}}(\mathcal{D}^{1\times q}, \mathcal{A}) \\ \updownarrow & & \updownarrow \\ \mathcal{A}^g & \xleftarrow{k} & \mathcal{A}^q \end{array}$$

where the vertical mappings are isomorphisms expressing the fact that a $\mathcal{D}$-linear map from the free module $\mathcal{D}^{1\times l}$ to $\mathcal{A}$ is uniquely determined by fixing the image of a basis, which amounts to fixing l elements of $\mathcal{A}$. Using the natural basis, denoted by $e_1, \ldots, e_l \in \mathcal{D}^{1\times l}$ we have the explicit version

$$\begin{array}{rcl} \mathcal{A}^l & \cong & \mathrm{Hom}_{\mathcal{D}}(\mathcal{D}^{1\times l}, \mathcal{A}) \\ (\psi(e_1), \ldots, \psi(e_l))^T & \leftarrow & \psi \\ v & \rightarrow & \psi_v : \mathcal{D}^{1\times l} \to \mathcal{A}, x \mapsto xv. \end{array}$$

So far, we have $\mathrm{Hom}_{\mathcal{D}}(\mathcal{M}, \mathcal{A}) \cong \ker(k)$. Let us derive an explicit form for k using the diagram above:

$$\begin{array}{ccc} \psi_w \circ (\cdot R) : \mathcal{D}^{1\times g} \to \mathcal{A}, y \mapsto yRw & \leftarrow & \psi_w : \mathcal{D}^{1\times q} \to \mathcal{A}, x \mapsto xw \\ \downarrow & & \uparrow \\ (e_1Rw, \ldots, e_gRw)^T = Rw & & w \end{array}$$

It turns out that $k(w) = Rw$ for all $w \in \mathcal{A}^q$ and thus $k \equiv R$. Thus

$$\mathrm{Hom}_{\mathcal{D}}(\mathcal{M}, \mathcal{A}) \cong \ker(k) = \{w \in \mathcal{A}^q \mid Rw = 0\} = \mathcal{B}$$

and the explicit form of the isomorphism can be derived along the lines of this proof. Note ϕ_w is well-defined because $[x_1] = [x_2]$ implies $x_1 - x_2 \in M$ and hence $x_1 w = x_2 w$, for $w \in \mathcal{B}$. □

Remark: If $\mathcal{D}$ is commutative, then the Malgrange isomorphism is an isomorphism of $\mathcal{D}$-modules.

The Malgrange isomorphism establishes another correspondence between the analytic object $\mathcal{B}$ and the algebraic object $\mathcal{M}$. The next section shows that for certain choices of $\mathcal{D}$ and $\mathcal{A}$, the Malgrange isomorphism has powerful properties which will fuel the algebraic systems theory machinery.

2.4 Injective cogenerators

A left $\mathcal{D}$-module $\mathcal{A}$ is called **injective** if $\mathrm{Hom}_{\mathcal{D}}(\cdot, \mathcal{A})$ is an exact functor, that is, if exactness of a sequence

$$\mathcal{M} \to \mathcal{N} \to \mathcal{P} \tag{2.6}$$

where $\mathcal{M}, \mathcal{N}, \mathcal{P}$ are left $\mathcal{D}$-modules, implies exactness of

$$\mathrm{Hom}_{\mathcal{D}}(\mathcal{M}, \mathcal{A}) \leftarrow \mathrm{Hom}_{\mathcal{D}}(\mathcal{N}, \mathcal{A}) \leftarrow \mathrm{Hom}_{\mathcal{D}}(\mathcal{P}, \mathcal{A}). \tag{2.7}$$

Note that this requirement is much stronger than left exactness of $\mathrm{Hom}_{\mathcal{D}}(\cdot, \mathcal{A})$ as mentioned in Lemma 2.14.

Let $R \in \mathcal{D}^{g \times q}$ and $v \in \mathcal{A}^g$ be given. Consider the inhomogeneous system $Rw = v$. We would like to know whether there exists a solution $w \in \mathcal{A}^q$. For this, consider $\ker(\cdot R)$ which is finitely generated, being a left submodule of the Noetherian module $\mathcal{D}^{1 \times g}$. Therefore we can write $\ker(\cdot R) = \mathrm{im}(\cdot Z)$ for some $\mathcal{D}$-matrix Z. In other words, we have an exact sequence

$$\mathcal{D}^{1 \times h} \xrightarrow{\cdot Z} \mathcal{D}^{1 \times g} \xrightarrow{\cdot R} \mathcal{D}^{1 \times q}.$$

If $\mathcal{A}$ is injective, then

$$\mathrm{Hom}_{\mathcal{D}}(\mathcal{D}^{1 \times h}, \mathcal{A}) \longleftarrow \mathrm{Hom}_{\mathcal{D}}(\mathcal{D}^{1 \times g}, \mathcal{A}) \longleftarrow \mathrm{Hom}_{\mathcal{D}}(\mathcal{D}^{1 \times q}, \mathcal{A})$$

is also exact, and therefore, so is

$$\mathcal{A}^h \xleftarrow{Z} \mathcal{A}^g \xleftarrow{R} \mathcal{A}^q.$$

This means that $\mathrm{im}_{\mathcal{A}}(R) = \ker_{\mathcal{A}}(Z)$, that is,

$$v \in \mathrm{im}_{\mathcal{A}}(R) \quad \Leftrightarrow \quad \exists w \in \mathcal{A}^q : Rw = v \quad \Leftrightarrow \quad v \in \ker_{\mathcal{A}}(Z) \quad \Leftrightarrow \quad Zv = 0.$$

Thus the solvability condition for $Rw = v$ is another linear system: the right hand side vector v has to satisfy $Zv = 0$. It is clear that this condition is necessary, because $ZR = 0$, but its sufficiency is due to the injectivity of $\mathcal{A}$.

Theorem 2.16 *Let the $\mathcal{D}$-module $\mathcal{A}$ be injective. Let $R \in \mathcal{D}^{g\times q}$ and $Z \in \mathcal{D}^{h\times g}$ be such that* $\ker(\cdot R) = \mathrm{im}(\cdot Z)$*, and let $v \in \mathcal{A}^g$ be given. Then*

$$\exists w \in \mathcal{A}^q : Rw = v \quad \Leftrightarrow \quad Zv = 0.$$

This is known as the **fundamental principle**.

Corollary 2.17 *If the $\mathcal{D}$-module $\mathcal{A}$ is injective, then* $\mathbf{B}$ *is closed under addition.*

Proof: Let $\mathcal{B}_i = \{w_i \in \mathcal{A}^q \mid R_i w_i = 0\}$ for $i = 1, 2$. Then

$$w \in \mathcal{B}_1 + \mathcal{B}_2 \quad \Leftrightarrow \quad \exists w_1, w_2 \in \mathcal{A}^q : \begin{bmatrix} R_1 & 0 \\ 0 & R_2 \\ I & I \end{bmatrix} \begin{bmatrix} w_1 \\ w_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ I \end{bmatrix} w.$$

According to the fundamental principle, there exists a $\mathcal{D}$-matrix R such that $\mathcal{B} := \mathcal{B}_1 + \mathcal{B}_2 = \{w \in \mathcal{A}^q \mid Rw = 0\}$, showing that $\mathcal{B} \in \mathbf{B}$. □

The $\mathcal{D}$-module $\mathcal{A}$ is said to be an **injective cogenerator** if the exactness of (2.6) is equivalent to the exactness of (2.7), for any $\mathcal{M}, \mathcal{N}, \mathcal{P}$.

Lemma 2.18 *If the $\mathcal{D}$-module $\mathcal{A}$ is an injective cogenerator, then it has property O.*

Proof: Let $M = \mathcal{D}^{1\times g}R$ and $M_1 = \mathfrak{M}\mathfrak{B}(M) = \mathcal{D}^{1\times g_1}R_1 \supseteq M$. Then $\mathcal{B} = \mathfrak{B}(M) = \mathcal{B}_1 = \mathfrak{B}\mathfrak{M}\mathfrak{B}(M)$. Let $\mathcal{M}_i = \mathcal{D}^{1\times q}/M_i$ for $i = 1, 2$. Since

$$\mathcal{B}_1 \xrightarrow{\mathrm{id}} \mathcal{B} \longrightarrow 0$$

is exact, so is

$$\mathrm{Hom}_{\mathcal{D}}(\mathcal{M}_1, \mathcal{A}) \longrightarrow \mathrm{Hom}_{\mathcal{D}}(\mathcal{M}, \mathcal{A}) \longrightarrow 0$$

because of the Malgrange isomorphism. The injective cogenerator property implies that

$$\mathcal{M}_1 \xleftarrow{i} \mathcal{M} \longleftarrow 0$$

is also exact. The map i is defined by $i(x + M) = x + M_1$. Since i is injective, we have $M_1 \subseteq M$, and thus $M = M_1 = \mathfrak{M}\mathfrak{B}(M)$. □

If the $\mathcal{D}$-module $\mathcal{A}$ is an injective cogenerator, then the Galois correspondence $\mathbf{B} \leftrightarrow \mathbf{M}$ consists of two inclusion-reversing bijections inverse to each other, and we have a full lattice correspondence

$$\begin{aligned} \mathfrak{B}(M_1 + M_2) &= \mathfrak{B}(M_1) \cap \mathfrak{B}(M_2) \\ \mathfrak{M}(\mathcal{B}_1 \cap \mathcal{B}_2) &= \mathfrak{M}(\mathcal{B}_1) + \mathfrak{M}(\mathcal{B}_2) \end{aligned}$$

$$\begin{aligned} \mathfrak{B}(M_1 \cap M_2) &= \mathfrak{B}(M_1) + \mathfrak{B}(M_2) \\ \mathfrak{M}(\mathcal{B}_1 + \mathcal{B}_2) &= \mathfrak{M}(\mathcal{B}_1) \cap \mathfrak{M}(\mathcal{B}_2) \end{aligned}$$

with $\mathfrak{B}(0) = \mathcal{A}^q$, $\mathfrak{B}(\mathcal{D}^{1\times q}) = 0$, $\mathfrak{M}(0) = \mathcal{D}^{1\times q}$, $\mathfrak{M}(\mathcal{A}^q) = 0$.

The following table lists some $\mathcal{D}$-modules $\mathcal{A}$ that are relevant in systems theory and that are injective cogenerators:

$\mathcal{D}$	$\mathcal{A}$
$\mathbb{K}[\frac{d}{dt}]$	$\mathcal{C}^\infty(\mathbb{R},\mathbb{K}), \mathcal{D}'(\mathbb{R},\mathbb{K})$
$\mathbb{F}[\sigma]$	$\mathbb{F}^{\mathbb{N}}$
$\mathbb{F}[\sigma,\sigma^{-1}]$	$\mathbb{F}^{\mathbb{Z}}$
$\mathbb{K}[\partial_1,\ldots,\partial_n]$	$\mathcal{C}^\infty(\mathbb{R}^n,\mathbb{K}), \mathcal{D}'(\mathbb{R}^n,\mathbb{K})$
$\mathbb{F}[\sigma_1,\ldots,\sigma_n]$	$\mathbb{F}^{\mathbb{N}^n}$
$\mathbb{F}[\sigma_1,\ldots,\sigma_n,\sigma_1^{-1},\ldots,\sigma_n^{-1}]$	$\mathbb{F}^{\mathbb{Z}^n}$

Example: Consider $\mathcal{D} = \mathbb{R}[\partial_1,\partial_2,\partial_3]$ and $\mathcal{A} = \mathcal{C}^\infty(\mathbb{R}^3,\mathbb{R})$. The statements

$$\exists w \in \mathcal{A} : \mathrm{grad}(w) = v \quad \Leftrightarrow \quad \mathrm{curl}(v) = 0$$

and

$$\exists w \in \mathcal{A}^3 : \mathrm{curl}(w) = v \quad \Leftrightarrow \quad \mathrm{div}(v) = 0$$

are two applications of the fundamental principle. Note that gradient, curl, and divergence correspond to

$$R_{\mathrm{grad}} = \begin{bmatrix} \partial_1 \\ \partial_2 \\ \partial_3 \end{bmatrix} \quad R_{\mathrm{curl}} = \begin{bmatrix} 0 & -\partial_3 & \partial_2 \\ \partial_3 & 0 & -\partial_1 \\ -\partial_2 & \partial_1 & 0 \end{bmatrix} \quad R_{\mathrm{div}} = \begin{bmatrix} \partial_1 & \partial_2 & \partial_3 \end{bmatrix}.$$

$\Diamond$

The following criteria make it easier to test whether a $\mathcal{D}$-module $\mathcal{A}$ is an injective cogenerator.

Theorem 2.19 *The $\mathcal{D}$-module $\mathcal{A}$ is injective if and only if for every sequence*

$$0 \to \mathcal{I} \hookrightarrow \mathcal{D},$$

where $\mathcal{I} \subseteq \mathcal{D}$ is a left ideal, the sequence

$$0 \leftarrow \mathrm{Hom}_{\mathcal{D}}(\mathcal{I},\mathcal{A}) \leftarrow \mathrm{Hom}_{\mathcal{D}}(\mathcal{D},\mathcal{A})$$

is exact. This is known as **Baer's criterion** *[12, Ch. 1, §3].*

Theorem 2.20 *Let $\mathcal{A}$ be an injective $\mathcal{D}$-module. Then $\mathcal{A}$ is a cogenerator if and only if*

$$\mathrm{Hom}_{\mathcal{D}}(\mathcal{M},\mathcal{A}) = 0 \quad \Rightarrow \quad \mathcal{M} = 0$$

for every finitely generated $\mathcal{D}$-module $\mathcal{M}$.

Since $\mathcal{D}$ is left Noetherian, a finitely generated $\mathcal{D}$-module $\mathcal{M}$ has the form $\mathcal{M} \cong \mathcal{D}^{1\times q}/\mathcal{D}^{1\times g}R$ for some suitable g, q and $R \in \mathcal{D}^{g\times q}$. To see this, suppose that $\mathcal{M}$ has q generators $m_1, \ldots, m_q \in \mathcal{M}$. Then there exists a surjective $\mathcal{D}$-linear map π from $\mathcal{D}^{1\times q}$ to $\mathcal{M}$ mapping each natural basis element e_i to m_i. The kernel of π is a left $\mathcal{D}$-submodule of $\mathcal{D}^{1\times q}$, and thus, it is also finitely generated, say it has g generators $r_1, \ldots, r_g \in \mathcal{D}^{1\times q}$. Let R be the matrix that contains these elements as rows. Then we have $\mathrm{im}(\cdot R) = \mathcal{D}^{1\times g}R = \ker(\pi)$ and $\mathrm{im}(\pi) = \mathcal{M}$. The homomorphism theorem implies that $\mathcal{D}^{1\times q}/\ker(\pi) \cong \mathrm{im}(\pi)$, that is, $\mathcal{D}^{1\times q}/\mathcal{D}^{1\times g}R \cong \mathcal{M}$. In other words, we have constructed an exact sequence

$$\ldots \longrightarrow \mathcal{D}^{1\times g} \xrightarrow{\cdot R} \mathcal{D}^{1\times q} \longrightarrow \mathcal{M} \longrightarrow 0$$

and this procedure can be iterated, that is, the sequence can be extended to the left. This is called a **free resolution** of $\mathcal{M}$.

Therefore, if $\mathcal{A}$ is injective, the cogenerator property is equivalent to

$$\mathcal{B} = \{w \in \mathcal{A}^q \mid Rw = 0\} = 0 \quad \Rightarrow \quad \mathcal{M} = \mathcal{D}^{1\times q}/\mathcal{D}^{1\times g}R = 0$$

where we have used the Malgrange isomorphism. Note that $\mathcal{M} = 0$ means $\mathcal{D}^{1\times g}R = \mathcal{D}^{1\times q}$, i.e., there exists $X \in \mathcal{D}^{q\times g}$ such that $XR = I$. However, we have already seen in Corollary 2.13 that this implication is a consequence of property O. Combining this with Lemma 2.18, we have the following result.

Theorem 2.21 *Let $\mathcal{A}$ be an injective $\mathcal{D}$-module. Then property O is equivalent to the cogenerator property.*

Remark: Since $\mathcal{D}$ is left Noetherian, Baer's criterion says in particular that it is sufficient to check injectivity for finitely generated modules in (2.6).

The proof of Baer's criterion uses Zorn's lemma which is equivalent to the axiom of choice. If this is to be avoided, an alternative formulation can be used. This is based on the observation that for applications in systems theory, one deals only with sequences (2.6) of finitely generated modules. Thus, instead of requiring $\mathcal{A}$ to be injective (which is equivalent to saying that $\mathrm{Hom}_{\mathcal{D}}(\cdot, \mathcal{A})$ is an exact functor on the category of left $\mathcal{D}$-modules) it suffices, for systems theoretic purposes, to say that $\mathrm{Hom}_{\mathcal{D}}(\cdot, \mathcal{A})$ should be an exact functor on the category of finitely generated left $\mathcal{D}$-modules.

The situation is simpler for the cogenerator property, because Theorem 2.20 does not rely on Zorn's lemma. Its counterpart in the alternative formulation is: Let $\mathrm{Hom}_{\mathcal{D}}(\cdot, \mathcal{A})$ be an exact functor on the category of finitely generated left $\mathcal{D}$-modules. Then $\mathrm{Hom}_{\mathcal{D}}(\cdot, \mathcal{A})$ is faithful (i.e., it reflects exactness) if and only if $\mathrm{Hom}_{\mathcal{D}}(\mathcal{M}, \mathcal{A}) = 0$ implies $\mathcal{M} = 0$ for all finitely generated left $\mathcal{D}$-modules.

Chapter 3

Basic systems theoretic properties

In this chapter, $\mathcal{D}$ is left Noetherian, and the $\mathcal{D}$-module $\mathcal{A}$ is an injective cogenerator. We consider an abstract linear system

$$\mathcal{B} = \{w \in \mathcal{A}^q \mid Rw = 0\}$$

and its system module

$$\mathcal{M} = \mathcal{D}^{1\times q}/\mathcal{D}^{1\times g}R,$$

where $R \in \mathcal{D}^{g\times q}$.

3.1 Autonomy

For $1 \leq i \leq q$, consider the projection of $\mathcal{B}$ onto the i-th component

$$\pi_i : \mathcal{B} \to \mathcal{A}, \quad w \mapsto w_i.$$

We say that w_i is a **free variable** (or: an input) of $\mathcal{B}$ if π_i is surjective. The system $\mathcal{B}$ is called **autonomous** if it admits no free variables.

Interpretation: The surjectivity of π_i means that for an arbitrary signal $a \in \mathcal{A}$, we can always find $q-1$ signals $w_1, \ldots, w_{i-1}, w_{i+1}, \ldots, w_q \in \mathcal{A}$ such that $w := (w_1, \ldots, w_{i-1}, a, w_{i+1}, \ldots, w_q)^T$ belongs to the system $\mathcal{B}$. In this sense, the i-th component of the signal vector $w \in \mathcal{B}$ is "free", i.e., it can be chosen arbitrarily.

Compare this with the solvability condition for $\dot{x} = Ax + Bu$ discussed in the Introduction: There, we required that for all u, there exists x such that $\dot{x} = Ax + Bu$. Using the language from above, this says that u should be an input in $\mathcal{B} = \{[x^T, u^T]^T \mid \dot{x} = Ax + Bu\}$. An autonomous system is a system without inputs, e.g., $\mathcal{B} = \{x \mid \dot{x} = Ax\}$.

Assumption: From now on, let $\mathcal{D}$ be a **domain**, that is, for all $d_1, d_2 \in \mathcal{D}$, we have

$$d_1 d_2 = 0 \quad \Rightarrow \quad d_1 = 0 \text{ or } d_2 = 0.$$

An element $m \in \mathcal{M}$ is called **torsion (element)** if there exists $0 \neq d$ such that $dm = 0$. The module $\mathcal{M}$ is called **torsion (module)** if all its elements are torsion.

Lemma 3.1 *If $\mathcal{M}$ is torsion, then $\mathcal{B}$ is autonomous.*

Proof: If $\mathcal{B}$ is not autonomous, then there exists an exact sequence

$$\mathcal{B} \xrightarrow{\pi_i} \mathcal{A} \longrightarrow 0.$$

Thus

$$\mathcal{M} \xleftarrow{i} \mathcal{D} \longleftarrow 0$$

is also exact. This means that i is injective. Consider $m := i(1) \neq 0$. This is not a torsion element (if $dm = 0$ then $di(1) = i(d) = 0$ which implies $d = 0$ because i is injective). Hence $\mathcal{M}$ is not torsion. $\square$

To obtain the converse direction of the implication of this lemma, we need the following notion. One says that the domain $\mathcal{D}$ has the **left Ore property** if any $0 \neq d_1, d_2 \in \mathcal{D}$ have a left common multiple, that is, there exist $0 \neq c_1, c_2 \in \mathcal{D}$ such that $c_1 d_1 = c_2 d_2$. Inductively, it follows that every finite number of non-zero elements of $\mathcal{D}$ has a left common multiple. The left Ore condition is equivalent to saying that for all $d_1, d_2 \in \mathcal{D}$, there exists $(0,0) \neq (c_1, c_2) \in \mathcal{D}^2$ with $c_1 d_1 = c_2 d_2$.

Remark: If $\mathcal{D}$ is commutative, then it has the Ore property, because we may take $c_1 = d_2$ and $c_2 = d_1$. However, the following theorem says that the assumptions on $\mathcal{D}$ made so far (namely, $\mathcal{D}$ being a left Noetherian domain) are already sufficient to deduce the left Ore property [7, 12].

Theorem 3.2 *If $\mathcal{D}$ is a left Noetherian domain, then it has the left Ore property.*

Proof: Let $0 \neq d_1, d_2 \in \mathcal{D}$. Consider the left ideals

$$\mathcal{I}_n := \sum_{i=0}^{n} \mathcal{D} d_1 d_2^i.$$

Then we have an ascending chain $\mathcal{I}_0 \subseteq \mathcal{I}_1 \subseteq \mathcal{I}_2 \subseteq \ldots$, which has to become stationary according to the Noetherian property. Let n be the smallest integer such that $\mathcal{I}_{n+1} = \mathcal{I}_n$. Then

$$d_1 d_2^{n+1} = \sum_{i=0}^{n} a_i d_1 d_2^i$$

for some $a_i \in \mathcal{D}$. Re-arranging the summands, we obtain

$$a_0 d_1 = (d_1 d_2^n - \sum_{i=1}^{n} a_i d_1 d_2^{i-1}) d_2$$

and hence we have constructed a left common multiple. If the coefficients were zero, we would have

$$d_1 d_2^n = \sum_{i=0}^{n-1} a_{i+1} d_1 d_2^i$$

and thus $\mathcal{I}_n = \mathcal{I}_{n-1}$, contradicting the minimality of n. □

Lemma 3.3 *The following are equivalent:*

1. *$\mathcal{M}$ is torsion.*
2. *$\mathcal{B}$ is autonomous.*

Proof: Since "1 ⇒ 2" follows from the lemma above, it suffices to prove "2 ⇒ 1": Assume that $\mathcal{M}$ is not torsion. We first show that there exists an integer $1 \leq i \leq q$ such that $[e_i]$ is not torsion, where e_i denotes the i-th natural basis vector of $\mathcal{D}^{1\times q}$.

Suppose that all $[e_i]$ were torsion, say $d_i[e_i] = 0$ for some $d_i \neq 0$. Now let $m \in \mathcal{M}$ be given. Then $m = [x]$ for some $x \in \mathcal{D}^{1\times q}$, where $[x]$ denotes the residue class of x modulo $\mathcal{D}^{1\times g} R$. Then

$$m = [x] = [\textstyle\sum_{i=1}^q x_i e_i] = \sum_{i=1}^q x_i [e_i],$$

where $x_i \in \mathcal{D}$. Due to the left Ore property, there exist $b_i, 0 \neq c_i \in \mathcal{D}$ with $b_i d_i = c_i x_i$. Similarly, let $a := a_i c_i \neq 0$ be a left common multiple of all c_i. Then

$$am = \sum a x_i [e_i] = \sum a_i c_i x_i [e_i] = \sum a_i b_i d_i [e_i] = 0.$$

Thus $\mathcal{M}$ is torsion, contradicting the assumption.

Thus there is an exact sequence

$$0 \longrightarrow \mathcal{D} \stackrel{i}{\longrightarrow} \mathcal{M}$$

where $i(1) = [e_i]$. Therefore,

$$0 \leftarrow \mathrm{Hom}_{\mathcal{D}}(\mathcal{D}, \mathcal{A}) \leftarrow \mathrm{Hom}_{\mathcal{D}}(\mathcal{M}, \mathcal{A})$$

is also exact, and thus, using the Malgrange isomorphism, so is

$$0 \longleftarrow \mathcal{A} \overset{p}{\longleftarrow} \mathcal{B}.$$

Thus p is surjective. However, $p \equiv \pi_i$. This shows that $\mathcal{B}$ is not autonomous. □

Theorem 3.4 *The following are equivalent:*

1. *$\mathcal{M}$ is torsion.*
2. *There exists $0 \neq d \in \mathcal{D}$ and $X \in \mathcal{D}^{q\times g}$ such that $dI = XR$.*
3. *$\mathcal{B}$ is autonomous.*

Proof: It suffices to show "1 ⇒ 2 ⇒ 3". If $\mathcal{M}$ is torsion, then all $[e_i]$ are torsion, that is, there exists $0 \neq d_i \in \mathcal{D}$ such that $d_i[e_i] = 0$. This means that $d_i e_i = y_i R$ for some $y_i \in \mathcal{D}^{1\times g}$. Using the left Ore property, let $d = c_i d_i$ be a left common multiple of all d_i. Then $de_i = c_i d_i e_i = c_i y_i R$. Writing these equations in matrix form, we obtain $dI = XR$.

If $dI = XR$, then $\mathcal{B} \subseteq \{w \mid dw = 0\}$, that is, every component w_i of $w \in \mathcal{B}$ satisfies the scalar equation $dw_i = 0$, where $0 \neq d$. However, it is a consequence of property O (which holds since $\mathcal{A}$ is an injective cogenerator) that there is no $0 \neq d \in \mathcal{D}$ with $d\mathcal{A} = 0$, that is, no component of w is free. In other words, $\mathcal{B}$ is autonomous. □

Corollary 3.5 *Let $\mathcal{D}$ be commutative. Then $\mathcal{B} = \{w \in \mathcal{A}^q \mid Rw = 0\}$ is autonomous if and only if R has full column rank, i.e.,* $\mathrm{rank}(R) = q$.

Remark: Over a commutative domain, the rank of a matrix can be defined as usual, that is, as the size of the largest non-singular submatrix. Note that any two representations of $\mathcal{B}$ have the same rank; this follows from Theorem 2.12.

Proof: Since $\mathrm{adj}(S)S = \det(S)I$ holds for any square $\mathcal{D}$-matrix S, and since a full column rank matrix contains a non-singular submatrix of full size, we have: R has full column rank if and only if there exists a $\mathcal{D}$-matrix X and $0 \neq d \in \mathcal{D}$ such that $XR = dI$. The rest follows from the theorem. □

We would like to have a similar result for the non-commutative case as well. However, we cannot work with determinants and adjugate matrices any more. Some preparation is necessary.

Linear algebra over Ore domains

Let $\mathcal{D}$ be a domain. The left Ore property is necessary and sufficient for $\mathcal{D}$ to admit a **field of left fractions** [3, p. 177]

$$\mathcal{K} = \{d^{-1}n \mid d, n \in \mathcal{D}, d \neq 0\}.$$

In fact, the composition $d_1^{-1}n_1d_2^{-1}n_2$ is explained by using the Ore property, which yields $an_1 = bd_2$ for some $a, b \in \mathcal{D}$, $a \neq 0$, and hence one puts

$$d_1^{-1}n_1d_2^{-1}n_2 := (ad_1)^{-1}(bn_2).$$

Of course, one has to show that this does not depend on the specific choice of a, b.

Remark: This is the non-commutative generalization of the fact that every commutative domain $\mathcal{D}$ can be embedded into its quotient field

$$\mathcal{K} = \{\tfrac{n}{d} \mid d, n \in \mathcal{D}, d \neq 0\},$$

for example, $\mathcal{D} = \mathbb{Z}$ with $\mathcal{K} = \mathbb{Q}$, or $\mathcal{D} = \mathbb{K}[t]$ with $\mathcal{K} = \mathbb{K}(t)$.

For $R \in \mathcal{D}^{g\times q}$, consider $V := R\mathcal{K}^q \subseteq \mathcal{K}^g$. This is a vector space over the skew field $\mathcal{K}$, and as such, it has a well-defined dimension

$$\dim(V) =: \operatorname{rank}(R).$$

In fact, we should call this the column rank of R, but since it holds that

$$\dim(R\mathcal{K}^q) = \dim(\mathcal{K}^{1\times g}R)$$

we have equality of row and column rank, just like in the classical case of linear algebra over commutative fields, and therefore it is justified to simply speak of the **rank** of R. If $\mathcal{D}$ is a commutative domain, then this notion coincides with the usual concept of the rank of a matrix.

Remark: The above statement should not be confused with $\operatorname{rank}(R) = \operatorname{rank}(R^T)$ which holds over commutative domains, but not in the non-commutative case, as illustrated by the following example.

Example: Let $a, b \in \mathcal{D}$ be such that $ab \neq ba$. Then the matrix

$$R = \begin{bmatrix} 1 & b \\ a & ab \end{bmatrix}$$

has rank 1 (as it would be in the commutative case), but its transpose

$$R^T = \begin{bmatrix} 1 & a \\ b & ab \end{bmatrix}$$

has rank 2. $\Diamond$

Lemma 3.6 *R has full column rank if and only if there exists a $\mathcal{D}$-matrix X and $0 \neq d \in \mathcal{D}$ such that $XR = dI$.*

Proof: If $XR = dI$ then

$$\mathcal{K}^{1\times q} dI = \mathcal{K}^{1\times q} XR \subseteq \mathcal{K}^{1\times g} R \subseteq \mathcal{K}^{1\times q}.$$

Since the leftmost and the rightmost vector space both have dimension q, we have $\dim(V) = \dim(\mathcal{K}^{1\times g} R) = q$, that is, R has rank q.

Conversely, assume that R has rank q. Let R_1 be R after deletion of the first column. Since $\operatorname{rank}(R_1) = q - 1 < g$, there exists $0 \neq x \in \mathcal{K}^{1\times g}$ such that $xR_1 = 0$. Let $x = [\tilde{d_1}^{-1}\tilde{n}_1, \ldots, \tilde{d_g}^{-1}\tilde{n}_g]$. Using the Ore property, we can write this as $x = \tilde{d}^{-1}[n_1, \ldots, n_g] =: \tilde{d}^{-1} n$ for some $n \in \mathcal{D}^{1\times g}$. Then $nR_1 = 0$ and thus $nR = [d, 0, \ldots, 0]$. There must be at least one choice of x that guarantees that $d \neq 0$, otherwise this would be a contradiction to $\operatorname{rank}(R) = q$. Let n be the first row of a matrix N. Proceeding like this with the remaining columns of R, we obtain $NR = \operatorname{diag}(d_1, \ldots, d_q)$. Exploiting the Ore property once more, we can find a diagonal matrix C such that $CNR = dI$, and we put $X = CN$. □

This lemma is exactly what we need in order to generalize Corollary 3.5 to arbitrary left Noetherian domains. Therefore we have proven the following result.

Theorem 3.7 *$\mathcal{B}$ is autonomous if and only if R has full column rank.*

3.2 Input-output structures

We still assume that $\mathcal{D}$ is a left Noetherian domain.

Let $\mathcal{B} = \{w \in \mathcal{A}^q \mid Rw = 0\}$ and $p := \operatorname{rank}(R)$. Since any two representations of $\mathcal{B}$ possess the same rank, this number does not depend on the choice of the representation R of $\mathcal{B}$, and therefore, it is a property of $\mathcal{B}$, called the **output-dimension** of $\mathcal{B}$.

Then there exist p columns of R that form a basis of $V = R\mathcal{K}^q$. Without loss of generality, we may re-arrange the columns of R such that the last p columns are a basis of V. (This corresponds only to a permutation of the components of $w \in \mathcal{B}$.) Thus

$$R = [-Q, P] \quad \text{with } P \in \mathcal{D}^{g\times p} \text{ and } \operatorname{rank}(P) = \operatorname{rank}(R) = p.$$

This corresponds to a partition of $w \in \mathcal{B}$ according to

$$w = \begin{bmatrix} u \\ y \end{bmatrix}.$$

A partition constructed this way is called an **input-output structure**. Since the columns of Q belong to V, we get

$$Q = PH \quad \text{for some } H \in \mathcal{K}^{p\times m}$$

where $m := q - p$, the **input-dimension** of $\mathcal{B}$. This H is uniquely determined, and it called the **transfer matrix** of $\mathcal{B}$ with respect to the chosen input-output structure (note that in general, there are several input-output structures, corresponding to different choices of the basis of V).

Theorem 3.8 *Let $\mathcal{B} = \{w = [u^T, y^T]^T \in \mathcal{A}^{m+p} \mid Py = Qu\}$ be a system with input-output structure. Then the transfer matrix H depends only on $\mathcal{B}$ and the chosen input-output structure (and not on the representation R). Moreover, we have*

$$\forall u \in \mathcal{A}^m \exists y \in \mathcal{A}^p : Py = Qu$$

and this justifies the term "input-output structure": The vector u consists of free variables of $\mathcal{B}$, and is therefore called an input. Moreover, the associated zero-input system $\mathcal{B}_{u=0} = \{y \in \mathcal{A}^p \mid Py = 0\}$ is autonomous, and therefore, we call y an output.

Proof: Let $R_1 = [-Q_1, P_1]$ and $R_2 = [-Q_2, P_2]$ be two representations of $\mathcal{B}$, and let $Q_1 = P_1H_1$ and $Q_2 = P_2H_2$. Since $R_2 = XR_1$ and $R_1 = YR_2$, this implies $P_1(H_1 - H_2) = 0$ and thus $H_1 = H_2$, because P_1 has full column rank.

Let Z be such that $\ker(\cdot P) = \operatorname{im}(\cdot Z)$. According to the fundamental principle,

$$\exists y \in \mathcal{A}^p : Py = Qu \quad \Leftrightarrow \quad ZQu = 0.$$

However, since $Q = PH$, we have $ZQ = ZPH = 0$ and hence $ZQu = 0$ holds for any $u \in \mathcal{A}^m$. □

Example: Let $\mathcal{D} = \mathbb{K}[\frac{d}{dt}]$ and $\mathcal{A} = \mathcal{C}^\infty(\mathbb{R}, \mathbb{K})$. Consider

$$\mathcal{B} = \{[x^T, u^T]^T \mid \dot{x} = Ax + Bu\},$$

where $A \in \mathbb{K}^{n\times n}$ and $B \in \mathbb{K}^{n\times m}$ are given. Then $R = [\frac{d}{dt}I - A, -B]$ has rank $p = n$, and we may take $P = \frac{d}{dt}I - A$, $Q = B$, and $H = (\frac{d}{dt}I - A)^{-1}B \in \mathbb{K}(\frac{d}{dt})^{p\times m}$.

◊

3.3 Controllability

We still assume that $\mathcal{D}$ is a left Noetherian domain.

An abstract linear system $\mathcal{B} = \{w \in \mathcal{A}^q \mid Rw = 0\}$ is called **controllable** if there exists $L \in \mathcal{D}^{q \times l}$ such that

$$\mathcal{B} = \{w \in \mathcal{A}^q \mid \exists \ell \in \mathcal{A}^l : w = L\ell\}.$$

This is called an **image representation** of $\mathcal{B}$. We will see later on that for certain choices of $\mathcal{D}$ and $\mathcal{A}$, this definition coincides with the intuitive notion of controllability as discussed in the Introduction.

Lemma 3.9 *$\mathcal{B}$ is controllable if and only if R is a left syzygy matrix, that is, there exists a $\mathcal{D}$-matrix L such that* $\mathrm{im}(\cdot R) = \ker(\cdot L)$.

Proof: $\mathcal{B}$ is controllable if and only if there exists L such that

$$Rw = 0 \quad \Leftrightarrow \quad \exists \ell \in \mathcal{A}^l : w = L\ell,$$

that is, $\ker_{\mathcal{A}}(R) = \mathrm{im}_{\mathcal{A}}(L)$. Due to the injective cogenerator property, this is equivalent to $\mathrm{im}(\cdot R) = \ker(\cdot L)$, that is, to R being a left syzygy matrix. □

So far, we have only used the injective cogenerator property. Now we return to our assumption that $\mathcal{D}$ should be domain.

The module $\mathcal{M}$ is called **torsion-free** if it has no torsion elements except zero, that is, for all $d \in \mathcal{D}$, $m \in \mathcal{M}$, we have

$$dm = 0 \quad \Rightarrow \quad d = 0 \text{ or } m = 0.$$

For $\mathcal{M} = \mathcal{D}^{1 \times q}/M$, this means that for all $d \in \mathcal{D}$, $x \in \mathcal{D}^{1 \times q}$,

$$dx \in M \quad \Rightarrow \quad d = 0 \text{ or } x \in M.$$

Lemma 3.10 *If $\mathcal{B}$ is controllable, then $\mathcal{M}$ is torsion-free.*

Proof: Let $0 \neq d \in \mathcal{D}$ and $x \in \mathcal{D}^{1 \times q}$ be such that $dx \in M = \mathrm{im}(\cdot R)$. Since $M = \mathrm{im}(\cdot R) = \ker(\cdot L)$ for some L, we have $RL = 0$ and hence $dxL = 0$. Since $\mathcal{D}$ is a domain, this implies $xL = 0$, that is, $x \in \ker(\cdot L) = M$. □

We need an additional assumption to obtain the converse direction of this implication.

Assumption: From now on, let the domain $\mathcal{D}$ be Noetherian (i.e., both left and right Noetherian).

Theorem 3.11 *The following are equivalent:*

1. *$\mathcal{B}$ is controllable.*

2. *$\mathcal{M}$ is torsion-free.*

3. *R is a left syzygy matrix.*

Proof: Since the equivalence of assertions 1 and 3 and the implication "1 ⇒ 2" follow from the above lemmas, it suffices to show "2 ⇒ 3": Let $\mathcal{M}$ be torsion-free. Consider $W = \ker_{\mathcal{K}}(R) \subseteq \mathcal{K}^q$. This is an m-dimensional $\mathcal{K}$-vector space, where $m = q - \operatorname{rank}(R)$, which has a representation $W = \tilde{L}\mathcal{K}^m$ for some $\tilde{L} \in \mathcal{K}^{q\times m}$. Using the right Ore property, we have $\tilde{L} = L\tilde{d}^{-1}$ for some $L \in \mathcal{D}^{q\times m}$. Since $R\tilde{L} = RL\tilde{d}^{-1} = 0$, we may conclude that $RL = 0$. Consider $\ker(\cdot L) \subseteq \mathcal{D}^{1\times q}$ and let R_c be such that $\operatorname{im}(\cdot R_c) = \ker(\cdot L)$. We will show that $\operatorname{im}(\cdot R) = \operatorname{im}(\cdot R_c)$, which yields the desired result. We have $\operatorname{rank}(R) = \operatorname{rank}(R_c)$ and $R = XR_c$ for some $\mathcal{D}$-matrix X. Thus $\operatorname{im}(\cdot R) \subseteq \operatorname{im}(\cdot R_c)$ and

$$\mathcal{K}^{1\times g}R = \mathcal{K}^{1\times g}XR_c \subseteq \mathcal{K}^{1\times g_c}R_c.$$

Since these vector spaces have the same dimension, they actually coincide, and thus we get $R_c = GR$ for some $\mathcal{K}$-matrix G. Using the left Ore property, we can write $G = d^{-1}N$ and thus $dR_c = NR$. Let x be a row of R_c, then $dx \in M$, and thus, since $\mathcal{M}$ is torsion-free and $d \neq 0$, we must have $x \in M$. Thus $R_c = YR$ for some $\mathcal{D}$-matrix Y. □

Remark: The proof could be shortened considerably if we would use the fact that every finitely generated torsion-free module over a Noetherian domain can be embedded into a finitely generated free module, because then the exact sequence

$$\mathcal{D}^{1\times g} \xrightarrow{\cdot R} \mathcal{D}^{1\times q} \xrightarrow{\pi} \mathcal{M} = \mathcal{D}^{1\times q}/\operatorname{im}(\cdot R)$$

and the embedding $i : \mathcal{M} \to \mathcal{D}^{1\times l}$ would yield an exact sequence

$$\mathcal{D}^{1\times g} \xrightarrow{\cdot R} \mathcal{D}^{1\times q} \xrightarrow{i\circ\pi} \mathcal{D}^{1\times l}$$

and the map $i \circ \pi$ has to take the form $\cdot L$ for some matrix $L \in \mathcal{D}^{q\times l}$.

However, the elementary proof from above gives a constructive method to find L. It also shows that without loss of generality, L has m columns, where m is the input-dimension of the system. Note that alternatively, one could construct L as a matrix whose l columns generate the right $\mathcal{D}$-module $\ker(R) \subseteq \mathcal{D}^q$, which is finitely generated, because $\mathcal{D}$ is right Noetherian; but then we only have $l \geq m$. Anyhow, the matrix R_c from the proof has interesting properties even when $\mathcal{B}$ is not controllable. This is the topic of the next section.

Example: Let $\mathcal{D} = \mathbb{K}[\frac{d}{dt}]$ and $\mathcal{A} = \mathcal{C}^\infty(\mathbb{R}, \mathbb{K})$. Consider

$$\mathcal{B} = \{[x^T, u^T]^T \mid \dot{x} = Ax + Bu\},$$

where $A \in \mathbb{K}^{n\times n}$ and $B \in \mathbb{K}^{n\times m}$ are given. Then $R = [\frac{d}{dt}I - A, -B]$ and

$$\mathcal{M} = \mathcal{D}^{1\times(n+m)}/\mathcal{D}^{1\times n}R.$$

One can show that $\mathcal{M}$ is torsion-free if and only if $\operatorname{rank}[B, AB, \dots, A^{n-1}B] = n$, thus recovering the controllability condition from the Introduction. $\diamondsuit$

3.4 The controllable part of a system

We still assume that $\mathcal{D}$ is a Noetherian domain.

Theorem 3.12 *There exists a uniquely determined largest controllable subsystem $\mathcal{B}_c$ of $\mathcal{B}$, that is, $\mathcal{B}_c \subseteq \mathcal{B}$, $\mathcal{B}_c$ is controllable, and if $\mathcal{B}_1$ is another controllable subsystem of $\mathcal{B}$, then $\mathcal{B}_1 \subseteq \mathcal{B}_c$. The system $\mathcal{B}_c$ is called the* **controllable part** *of $\mathcal{B}$. We have $\mathcal{B} = \mathcal{B}_c$ if and only if $\mathcal{B}$ is controllable.*

Proof: Consider the matrix R_c constructed above and set

$$\mathcal{B}_c = \{w \in \mathcal{A}^q \mid R_c w = 0\}.$$

By construction, $R = XR_c$, that is, $\mathcal{B}_c \subseteq \mathcal{B}$, and R_c is a left syzygy matrix, that is, $\mathcal{B}_c$ is controllable.

Let $\mathcal{B}_1 = \{w \in \mathcal{A}^q \mid R_1 w = 0\}$ be another controllable subsystem of $\mathcal{B}$, then $R = Z_1 R_1$ and $\operatorname{im}(\cdot R_1) = \ker(\cdot L_1)$ for some $\mathcal{D}$-matrices Z_1, L_1. Recall that by construction, $dR_c = NR$ for some $0 \neq d \in \mathcal{D}$ and a $\mathcal{D}$-matrix N. Thus $dR_c L_1 = NRL_1 = NZ_1R_1L_1 = 0$, and since $\mathcal{D}$ is a domain, we may conclude that $R_c L_1 = 0$. Therefore we must have $R_c = Z_2 R_1$, that is, $\mathcal{B}_1 \subseteq \mathcal{B}_c$. $\square$

The **torsion part** $t\mathcal{M}$ of $\mathcal{M}$ is the set of all torsion elements of $\mathcal{M}$, that is,

$$t\mathcal{M} = \{m \in \mathcal{M} \mid \exists 0 \neq d \in \mathcal{D} : dm = 0\}.$$

Theorem 3.13 *$t\mathcal{M}$ is a left submodule of $\mathcal{M}$, the module $\mathcal{M}/t\mathcal{M}$ is torsion-free, and we have the Malgrange isomorphism*

$$\mathcal{B}_c \cong \operatorname{Hom}_{\mathcal{D}}(\mathcal{M}/t\mathcal{M}, \mathcal{A}).$$

In particular, $\mathcal{B}$ is autonomous if and only if $\mathcal{B}_c = 0$.

Proof: Let $m_1, m_2 \in t\mathcal{M}$, that is, $d_1 m_1 = d_2 m_2 = 0$ for some $0 \neq d_1, d_2 \in \mathcal{D}$. Since d_1 and d_2 have a left common multiple $0 \neq d = c_1 d_1 = c_2 d_2$, we obtain $d(m_1 + m_2) = c_1 d_1 m_2 + c_2 d_2 m_2 = 0$, showing that $m_1 + m_2 \in t\mathcal{M}$.

Let $m \in t\mathcal{M}$, say $dm = 0$ for $0 \neq d \in \mathcal{D}$, and consider $m' = d'm$ for some $d' \in \mathcal{D}$. We need to show that m' is torsion. Due to the left Ore property, there exist $c, c' \in \mathcal{D}$, $c' \neq 0$, such that $cd = c'd'$. Thus $0 = cdm = c'd'm = c'm'$, showing that $m' \in t\mathcal{M}$.

Let $0 \neq [m] \in \mathcal{M}/t\mathcal{M}$. If $d[m] = 0$, then $dm \in t\mathcal{M}$, that is, there exists $0 \neq c \in \mathcal{D}$ with $cdm = 0$. Since $0 \neq [m]$, we have $m \notin t\mathcal{M}$ and thus we must have $d = 0$.

For the final statement, we need to prove that $\mathcal{M}/t\mathcal{M}$ is isomorphic to the system module of $\mathcal{B}_c$, that is,

$$\mathcal{D}^{1\times q}/\mathcal{D}^{1\times g_c}R_c \cong \mathcal{M}/t\mathcal{M}.$$

Define $\phi : \mathcal{D}^{1\times q} \to \mathcal{M}/t\mathcal{M}$ via $\phi(x) = [x] + t\mathcal{M}$, where $[x]$ denotes the residue class of x modulo $M = \mathcal{D}^{1\times g}R$. This map is clearly surjective. Therefore, it suffices to show that $\ker(\phi) = M_c := \mathcal{D}^{1\times g_c}R_c$.

For this, recall that $R = XR_c$ and $dR_c = NR$ for some $\mathcal{D}$-matrices X and N and $0 \neq d \in \mathcal{D}$.

If $[x] \in t\mathcal{M}$, there exists $0 \neq c \in \mathcal{D}$ such that $c[x] = 0$, that is, $cx \in M \subseteq M_c$. This implies $x \in M_c$, because $\mathcal{M}_c := \mathcal{D}^{1\times q}/M_c$ is torsion-free.

Conversely, if x is a row of R_c, then $dx \in M$ and thus $d[x] = 0$ showing that $[x] \in t\mathcal{M}$. Since $t\mathcal{M}$ is a left $\mathcal{D}$-module, this implies that $[x] \in t\mathcal{M}$ for any $x \in \operatorname{im}(\cdot R_c) = M_c$. □

Remark: We have an exact sequence

$$0 \to t\mathcal{M} \to \mathcal{M} \to \mathcal{M}/t\mathcal{M} \to 0$$

and thus

$$0 \leftarrow \operatorname{Hom}_{\mathcal{D}}(t\mathcal{M}, \mathcal{A}) \leftarrow \operatorname{Hom}_{\mathcal{D}}(\mathcal{M}, \mathcal{A}) \leftarrow \operatorname{Hom}_{\mathcal{D}}(\mathcal{M}/t\mathcal{M}, \mathcal{A}) \leftarrow 0$$

is also exact. Using the Malgrange isomorphism, this corresponds to

$$0 \leftarrow \mathcal{B}/\mathcal{B}_c \leftarrow \mathcal{B} \leftarrow \mathcal{B}_c \leftarrow 0.$$

Since $t\mathcal{M}$ is a torsion module, the quotient $\mathcal{B}/\mathcal{B}_c$ corresponds to an autonomous system, which is sometimes called the obstruction to controllability. Its significance will become clear in Chapter 5, for a specific choice of $\mathcal{D}$ and $\mathcal{A}$.

Theorem 3.14 *There exists an autonomous system $\mathcal{B}_a$ such that $\mathcal{B} = \mathcal{B}_c + \mathcal{B}_a$. This is known as* **controllable-autonomous decomposition**.

Remark: Note that $\mathcal{B}_a$ is not uniquely determined, and that it is not possible, in general, to choose $\mathcal{B}_a$ such that the sum $\mathcal{B}_a + \mathcal{B}_c$ is direct.

Proof: Choose an input-output structure and set $\mathcal{B} = \{[u^T, y^T]^T \mid Py = Qu\}$, that is $R = [-Q, P] = XR_c$. Partition $R_c = [-Q_c, P_c]$ correspondingly, then this is an input-output structure of $\mathcal{B}_c = \{[u^T, y^T]^T \mid P_c y = Q_c u\}$.

Let $\mathcal{B}_a := \{[u^T, y^T]^T \mid Py = 0, u = 0\}$. This is autonomous and contained in $\mathcal{B}$. Thus $\mathcal{B}_c + \mathcal{B}_a \subseteq \mathcal{B}$.

For the converse, let $[u^T, y^T]^T \in \mathcal{B}$. There exists a solution y_1 to $P_c y_1 = Q_c u$. Write

$$\begin{bmatrix} u \\ y \end{bmatrix} = \begin{bmatrix} u \\ y_1 \end{bmatrix} + \begin{bmatrix} 0 \\ y - y_1 \end{bmatrix}.$$

The first summand is in $\mathcal{B}_c$, and the second is in $\mathcal{B}_a$, because

$$P(y - y_1) = Py - XP_c y_1 = Qu - XQ_c u = Qu - Qu = 0$$

for all u. □

Example: Let $A \in \mathbb{K}^{n \times n}$ and $B \in \mathbb{K}^{n \times m}$. Then there exists a non-singular $T \in \mathbb{K}^{n \times n}$ such that

$$T^{-1}AT = \begin{bmatrix} A_1 & A_2 \\ 0 & A_3 \end{bmatrix} \quad \text{and} \quad T^{-1}B = \begin{bmatrix} B_1 \\ 0 \end{bmatrix}$$

where $A_1 \in \mathbb{K}^{n_1 \times n_1}$, $B_1 \in \mathbb{K}^{n_1 \times m}$, and (A_1, B_1) is controllable, that is,

$$\operatorname{rank}[B_1, A_1 B_1, \ldots, A_1^{n_1 - 1} B_1] = n_1.$$

This is the so-called **Kalman controllability decomposition**. Therefore we may assume without loss of generality that

$$\mathcal{B} = \{[x_1^T, x_2^T, u^T]^T \mid \dot{x}_1 = A_1 x_1 + A_2 x_2 + B_1 u, \dot{x}_2 = A_3 x_2\}.$$

Then

$$\mathcal{B}_c = \{[x_1^T, x_2^T, u^T]^T \mid x_2 = 0, \dot{x}_1 = A_1 x_1 + B_1 u\}$$

and

$$\mathcal{B}_a = \{[x_1^T, x_2^T, u^T]^T \mid u = 0, \dot{x}_1 = A_1 x_1 + A_2 x_2, \dot{x}_2 = A_3 x_2\}.$$

Note that $\mathcal{B}_c \cap \mathcal{B}_a \neq 0$, but in this example, it is possible to find another autonomous system $\mathcal{B}_a'$ such that $\mathcal{B} = \mathcal{B}_c \oplus \mathcal{B}_a'$. ◊

3.5 Observability

Let $\mathcal{B}$ be an abstract linear system in which the representation matrix is partitioned as $R = [R_1, R_2]$. Let the signal vector w be partitioned accordingly. Then

$$\mathcal{B} = \{[w_1^T, w_2^T]^T \in \mathcal{A}^{q_1+q_2} \mid R_1 w_1 + R_2 w_2 = 0\}.$$

One says that w_1 is **observable** from w_2 in $\mathcal{B}$ if w_1 is uniquely determined by w_2 and the fact that $R_1 w_1 + R_2 w_2 = 0$. This means that $R_1 w_1' + R_2 w_2 = 0$ and $R_1 w_1 + R_2 w_2 = 0$ should imply that $w_1 = w_1'$. Equivalently,

$$\mathcal{B}_1 := \{w_1 \in \mathcal{A}^{q_1} \mid R_1 w_1 = 0\} = 0.$$

The following theorem is a direct consequence of Corollary 2.13.

Theorem 3.15 *The subsignal w_1 is observable from w_2 if and only if R_1 is left invertible, that is, there exists a $\mathcal{D}$-matrix X such that $I = XR_1$.*

A **latent variable description** of $\mathcal{B}$ takes the form

$$\mathcal{B} = \{w \in \mathcal{A}^q \mid \exists \ell \in \mathcal{A}^l : Rw = M\ell\}$$

where $R \in \mathcal{D}^{g \times q}$ and $M \in \mathcal{D}^{g \times l}$. According to the fundamental principle, this is indeed an abstract linear system, i.e., we can construct a kernel representation. One is particularly interested in the question whether the latent variables ℓ are observable from the manifest variables w in the associated "full" system

$$\mathcal{B}_f = \{[\ell^T, w^T]^T \in \mathcal{A}^{l+q} \mid M\ell = Rw\}.$$

The theorem above tells us that this is the case if and only if M is left invertible. Then we have

$$\mathcal{B} = \{w \in \mathcal{A}^q \mid \exists! \ell \in \mathcal{A}^l : Rw = M\ell\},$$

which called an observable latent variable description.

Example: Let $\mathcal{D} = \mathbb{K}[\frac{d}{dt}]$ and $\mathcal{A} = \mathcal{C}^\infty(\mathbb{R}, \mathbb{K})$. Consider

$$\mathcal{B} = \{[u^T, y^T]^T \in \mathcal{A}^{m+p} \mid \exists x \in \mathcal{A}^n : \dot{x} = Ax + Bu, y = Cx + Du\}.$$

This is the input-output system associated to the state space system

$$\begin{aligned} \dot{x} &= Ax + Bu \\ y &= Cx + Du, \end{aligned}$$

and the full system consists of all $[x^T, u^T, y^T]^T$ that satisfy these equations. Here, the latent variables correspond to the state x, and the input u and the output y

are considered as manifest variables. Since the state space equations can be rewritten as

$$\begin{bmatrix} B & 0 \\ -D & I \end{bmatrix} \begin{bmatrix} u \\ y \end{bmatrix} = \begin{bmatrix} \frac{d}{dt}I - A \\ C \end{bmatrix} x,$$

we see that observability amounts to the left invertibility of

$$M = \begin{bmatrix} \frac{d}{dt}I - A \\ C \end{bmatrix}$$

which is equivalent to the classical observability criterion, which says that

$$K = \begin{bmatrix} C \\ CA \\ \vdots \\ CA^{n-1} \end{bmatrix}$$

should have rank n. $\Diamond$

Chapter 4

One-dimensional systems

4.1 Ordinary differential equations with rational coefficients

Let $\mathcal{D} = K[\frac{d}{dt}]$, where $K = \mathbb{K}(t)$ is the field of rational functions. Then $\mathcal{D}$ is the ring of linear ordinary differential operators with rational coefficients.

Let $\mathcal{A}$ denote the set of all functions that are smooth except for a finite number of points, that is, for each $a \in \mathcal{A}$ there exists a finite set $\mathbb{E}(a) \subset \mathbb{R}$ such that $a \in \mathcal{C}^\infty(\mathbb{R} \setminus \mathbb{E}(a), \mathbb{K})$. Then $\mathcal{A}$ is a $\mathbb{K}$-vector space and a left $\mathcal{D}$-module. We will identify functions whose values coincide almost everywhere.

Recall that $\mathcal{D}$ is not commutative, because

$$\frac{d}{dt}ta = a + t\frac{d}{dt}a \quad \text{for all } a \in \mathcal{A}$$

and thus $\frac{d}{dt}t = 1 + t\frac{d}{dt}$. More generally, for $k \in K$, we have

$$\frac{d}{dt}k = k' + k\frac{d}{dt}$$

and, proceeding inductively,

$$\frac{d^i}{dt^i}k = \sum_{j=0}^{i} \binom{i}{j} k^{(i-j)} \frac{d^j}{dt^j}.$$

The ring $\mathcal{D}$ is a domain, and any element $0 \neq d \in \mathcal{D}$ can be uniquely written in the form

$$d = a_n(t)\frac{d^n}{dt^n} + \ldots + a_1(t)\frac{d}{dt} + a_0(t)$$

where $n \in \mathbb{N}$, $a_i \in K$, and $a_n \neq 0$. The number n is called the degree of d, and a_n is called the leading coefficient of d. If the leading coefficient equals one, we say that d is monic.

Theorem 4.1 *[7, Ch. 1] The ring $\mathcal{D}$ is simple (that is, the only ideals that are both right and left ideals are the trivial ones, i.e., 0 and $\mathcal{D}$ itself) and it is a left and right principal ideal domain (that is, every left ideal and every right ideal can be generated by one single element).*

Proof: Let $\mathcal{I}$ be a non-zero right and left ideal in $\mathcal{D}$. Let

$$n := \min\{\deg(f) \mid 0 \neq f \in \mathcal{I}\}.$$

Then $\mathcal{I}$ contains an element d of degree n. If $n = 0$, we have $\mathcal{I} = \mathcal{D}$, and we're finished. If $n \geq 1$, consider the element $kd - dk \in \mathcal{I}$, where $k \in K$. We have (writing $D := \frac{d}{dt}$ to simplify the notation)

$$\begin{aligned} kd - dk &= k\sum_{i=0}^{n} a_i D^i - \sum_{i=0}^{n} a_i D^i k \\ &= k\sum_{i=0}^{n} a_i D^i - \sum_{i=0}^{n} a_i \sum_{j=0}^{i} \binom{i}{j} k^{(i-j)} D^j \\ &= k\sum_{i=0}^{n} a_i D^i - \sum_{i=0}^{n} \sum_{j=i}^{n} a_j \binom{j}{i} k^{(j-i)} D^i. \end{aligned}$$

The coefficient at D^n equals $ka_n - a_n k$, which is zero (since K is commutative). Hence the degree of $kd - dk$ is at most $n-1$. However, since n was chosen to be minimal, we must have $kd - dk = 0$. Then the coefficient at D^{n-1} has to vanish. This coefficient is given by $ka_{n-1} - a_{n-1}k - a_n nk' = -a_n nk'$. Thus we have shown that for all $k \in K$, we have $k' = 0$. This is clearly absurd, and thus we have shown that the assumption $n \geq 1$ must be false.

Now let $\mathcal{I}$ be a non-zero left ideal of $\mathcal{D}$. Define n as above, and let $d \in \mathcal{I}$ have degree n. Without loss of generality, let d be monic. We show that $\mathcal{I} = \mathcal{D}d$. Since $\mathcal{D}d \subseteq \mathcal{I}$ is obvious, it suffices to show that $\mathcal{I} \subseteq \mathcal{D}d$. We do this by induction on the degree of $f \in \mathcal{I}$. If $\deg(f) = n$, we consider $f - f_n d$ whose degree is less than n. Thus it must be zero, showing that $f = f_n d \in \mathcal{D}d$. Suppose that we have shown the statement for all $f \in \mathcal{I}$ of degree $n, n+1, \ldots, m-1$. Consider $f \in \mathcal{I}$ with $\deg(f) = m$. Then $f - f_m D^{m-n} d$ has degree less than m. By the inductive hypothesis, it has to be in $\mathcal{D}d$, which implies $f \in \mathcal{D}d$.

The statement for right ideals is proven similarly. □

Remark: In fact, $\mathcal{D}$ is even a left and right Euclidean domain, with means that we have a left and right "division with remainder": For all $0 \neq d \in \mathcal{D}$ and $n \in \mathcal{D}$ there exist $q, r \in \mathcal{D}$ such that $n = qd + r$, where we have either $r = 0$ or $\deg(r) < \deg(d)$. Similarly, we have $n = dq_1 + r_1$.

Anyhow, $\mathcal{D}$ is left and right Noetherian and thus it has the left and right Ore property. Thus it admits a skew field of fractions $\mathcal{K}$, and the rank of a $\mathcal{D}$-matrix is well-defined. A matrix $U \in \mathcal{D}^{g\times g}$ is called unimodular if there exists a matrix $U^{-1} \in \mathcal{D}^{g\times g}$ with $UU^{-1} = U^{-1}U = I$.

Theorem 4.2 (Jacobson form) *[8, Ch. 3], [5, Ch. 8.1] Let $R \in \mathcal{D}^{g\times q}$. Then there exist unimodular matrices U and V such that*

$$URV = \begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix}$$

where $D = \mathrm{diag}(1, \ldots, 1, d) \in \mathcal{D}^{p\times p}$ for some $0 \neq d \in \mathcal{D}$, and $p := \mathrm{rank}(R)$.

Since $\mathcal{D}$ is even a Euclidean domain, the transformation matrices U and V can be obtained by performing elementary row and column operations.

In the following proof, we use the following standard facts from ODE theory: The initial value problem $\dot{x}(t) = A(t)x(t) + b(t)$, $x(t_0) = x_0$, where $A \in \mathcal{C}^\infty(I, \mathbb{K}^{n\times n})$ and $b \in \mathcal{C}^\infty(I, \mathbb{K}^n)$ for some open interval $I \subseteq \mathbb{R}$, has a unique solution for any choice of $t_0 \in I$ and $x_0 \in \mathbb{K}^n$. This solution is defined on all of I and it is smooth, that is, $x \in \mathcal{C}^\infty(I, \mathbb{K}^n)$. The solution set of the associated homogeneous equation $\dot{x}(t) = A(t)x(t)$ is a $\mathbb{K}$-vector space of dimension n.

Moreover, the tests for the injective cogenerator property given in Chapter 2 can be simplified in the case where $\mathcal{D}$ is a left principal ideal domain. A left $\mathcal{D}$-module $\mathcal{A}$ is injective if and only if for all $0 \neq d \in \mathcal{D}$ and all $u \in \mathcal{A}$, there exists $y \in \mathcal{A}$ such that $dy = u$. An injective module is a cogenerator if and only if $\mathrm{Hom}_{\mathcal{D}}(\mathcal{D}/\mathcal{D}d, \mathcal{A}) = 0$ implies $\mathcal{D}/\mathcal{D}d = 0$ for any $d \in \mathcal{D}$. In view of the Malgrange isomorphism, this is equivalent to saying that $\{w \in \mathcal{A} \mid dw = 0\} = 0$ implies that d is left invertible. However, since $\mathcal{D}$ is a domain, left and right invertibility of $d \in \mathcal{D}$ are equivalent. Moreover, in $\mathcal{D} = \mathbb{K}(t)[\frac{d}{dt}]$, an element $d \in \mathcal{D}$ is a unit if and only if $d \in \mathbb{K}(t) \setminus \{0\}$, that is, $\deg(d) = 0$.

Theorem 4.3 *The left $\mathcal{D}$-module $\mathcal{A}$ is an injective cogenerator.*

Proof: For injectivity, we need to prove: For every $0 \neq d \in \mathcal{D}$ and every $u \in \mathcal{A}$, there exists $y \in \mathcal{A}$ such that $dy = u$. Let $d = a_n(t)\frac{d^n}{dt^n} + \ldots + a_0(t)$ be given, with $a_n \neq 0$. If $n = 0$, there is nothing to prove, so let us assume that $n \geq 1$. Since K

is a field, one may assume that $a_n = 1$. Then $dy = u$ can be rewritten as a first order system

$$\dot{x}(t) = A(t)x(t) + Bu(t),$$

where $x = [y, \dot{y}, \dots, y^{(n-1)}]^T$ and

$$A = \begin{bmatrix} 0 & 1 & & \\ \vdots & & \ddots & \\ 0 & & & 1 \\ -a_0 & \cdots & \cdots & -a_{n-1} \end{bmatrix} \in K^{n \times n} \quad \text{and} \quad B = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix} \in \mathbb{K}^n.$$

Let $\mathbb{E}(d)$ be the finite set of all poles of the rational coefficients a_i of d. Let $\mathbb{E}(y) := \mathbb{E}(u) \cup \mathbb{E}(d) = \{t_1, \dots, t_k\}$ with $t_1 < \dots < t_k$. On every interval $I \subseteq \mathbb{R}$ of the form (t_i, t_{i+1}) or $(-\infty, t_1)$ or (t_k, ∞), it holds that $A|_I$ and $u|_I$ are smooth. Therefore, there exists a smooth solution $x_I : I \to \mathbb{K}^n$ to $\dot{x} = Ax + Bu$ on each of these intervals. By concatenating them (i.e., by setting $x|_I := x_I$), one gets a solution $x \in \mathcal{A}^n$ and thus $y = x_1 \in \mathcal{A}$.

For the cogenerator property, it has to be shown that if for some $d \in \mathcal{D}$, the equation $dy = 0$ possesses only the zero solution, then $d \in K \setminus \{0\}$. Assume conversely that $\deg(d) = n \geq 1$. The one can rewrite $dy = 0$ as $\dot{x}(t) = A(t)x(t)$. On each of the intervals I from above, the solution set of this is an n-dimensional subspace of $\mathcal{C}^\infty(I, \mathbb{K}^n)$, in particular, there exist non-zero solutions. Concatenating them, we obtain a non-zero solution $x \in \mathcal{A}^n$. If $y = x_1$ were identically zero, then $x = [y, \dot{y}, \dots, y^{(n-1)}]^T$ would also be identically zero, a contradiction. □

4.2 Rationally time-varying systems

Let $R \in \mathcal{D}^{g \times q}$ be given. The abstract linear system

$$\mathcal{B} = \{w \in \mathcal{A}^q \mid Rw = 0\}$$

is the solution space of the linear system of rational-coefficient ordinary differential equations $Rw = 0$.

Let

$$URV = \begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix}$$

be the Jacobson form of R, and let $W := V^{-1} \in \mathcal{D}^{q \times q}$. Since $Rw = 0$ is equivalent to $URw = URVWw = 0$, there is an isomorphism of Abelian groups

$$\begin{array}{rcl} \mathcal{B} & \cong & \tilde{\mathcal{B}} := \{\tilde{w} \in \mathcal{A}^q \mid [D, 0]\tilde{w} = 0\} \\ w & \mapsto & \tilde{w} := Ww \end{array} \tag{4.1}$$

where

$$\tilde{\mathcal{B}} = \{\tilde{w} \in \mathcal{A}^q \mid \tilde{w}_1 = \ldots = \tilde{w}_{p-1} = 0, d\tilde{w}_p = 0\} \tag{4.2}$$

is fully decoupled, since $D = \text{diag}(1, \ldots, 1, d)$.

Consider the system module $\mathcal{M} = \mathcal{D}^{1\times q}/\mathcal{D}^{1\times g}R$. According to the Jacobson form, there is an isomorphism of left $\mathcal{D}$-modules

$$\begin{array}{rcl} \mathcal{M} & \cong & \tilde{\mathcal{M}} = \mathcal{D}^{1\times q}/\mathcal{D}^{1\times p}[D, 0] \\ {[x]} & \mapsto & [xV] \end{array}$$

where $[\cdot]$ denotes the residue class of an element of $\mathcal{D}^{1\times q}$ in $\mathcal{M}$ or $\tilde{\mathcal{M}}$, respectively. Thus we have

$$\mathcal{M} \cong \mathcal{D}/\mathcal{D}d \times \mathcal{D}^{1\times m} = \mathcal{D}/\mathcal{D}d \oplus \mathcal{D}^{1\times m} \tag{4.3}$$

where $m := q-p$ and $p = \text{rank}(R)$. The module $\mathcal{D}/\mathcal{D}d$ is isomorphic to the torsion submodule $t\mathcal{M}$ of $\mathcal{M}$. The module $\mathcal{M}/t\mathcal{M} \cong \mathcal{D}^{1\times m}$ is not only torsion-free, but even free.

The decomposition (4.3) induces an isomorphism of Abelian groups

$$\mathcal{B} \cong \{y \in \mathcal{A} \mid dy = 0\} \oplus \mathcal{A}^m, \tag{4.4}$$

because

$$\text{Hom}_{\mathcal{D}}(\mathcal{D}/\mathcal{D}d, \mathcal{A}) \cong \{y \in \mathcal{A} \mid dy = 0\}$$

according to the Malgrange isomorphism, and

$$\text{Hom}_{\mathcal{D}}(\mathcal{D}^{1\times m}, \mathcal{A}) \cong \mathcal{A}^m.$$

Of course, the existence of the isomorphism (4.4) can also be seen directly from (4.1) and (4.2). The details of this decomposition will be investigated in Theorem 4.11 below.

Existence of full row rank representations

Corollary 4.4 *Let $\mathcal{B} = \{w \in \mathcal{A}^q \mid Rw = 0\}$ for some $R \in \mathcal{D}^{g\times q}$. Then $\mathcal{B}$ can be represented by a matrix with full row rank.*

Proof: Without loss of generality, let $R \neq 0$ (the system $\mathcal{B} = \mathcal{A}^q$ can be represented by the empty matrix, which has full row rank by convention). Let

$$URV = \begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix}$$

be the Jacobson form of R. Partition

$$W = V^{-1} = \begin{bmatrix} W_1 \\ W_2 \end{bmatrix} \tag{4.5}$$

according to the partition of the Jacobson form. Since U is unimodular, $Rw = 0$ is equivalent to $URw = 0$. Thus $\tilde{R} := DW_1$ also represents $\mathcal{B}$, and it has full row rank. □

Equivalence of representations

Corollary 4.5 *Let R_1, R_2 be two $\mathcal{D}$-matrices with the same number of columns, and let $\mathcal{B}_1, \mathcal{B}_2$ be the associated systems. We have $\mathcal{B}_1 \subseteq \mathcal{B}_2$ if and only if $R_2 = XR_1$ for some $\mathcal{D}$-matrix X. If $\mathcal{B}_1 = \mathcal{B}_2$, then R_1 and R_2 have the same rank. If R_1 and R_2 have full row rank, then $\mathcal{B}_1 = \mathcal{B}_2$ if and only if $R_2 = UR_1$ for some unimodular matrix U.*

Proof: It suffices to show the final statement. If $\mathcal{B}_1 = \mathcal{B}_2$, then $R_2 = XR_1$ and $R_1 = YR_2$, which shows that R_1 and R_2 have the same rank. If additionally, R_1 and R_2 both have full row rank, then they have the same number of rows, which implies that X and Y are square, and in fact, we must have $X = Y^{-1}$ showing that the matrices are unimodular. □

Elimination of latent variables

Corollary 4.6 *Consider*

$$\mathcal{B} = \{w \in \mathcal{A}^q \mid \exists \ell \in \mathcal{A}^l : Rw = M\ell\}$$

where $R \in \mathcal{D}^{g\times q}$ and $M \in \mathcal{D}^{g\times l}$. Then there exists a kernel representation of $\mathcal{B}$.

Proof: This follows from the fundamental principle. □

Input-output structures and autonomy

Let $R \in \mathcal{D}^{p\times q}$ be a full row rank representation of $\mathcal{B}$. Then there exists a $p \times p$ submatrix P of R of full rank. Without loss of generality, arrange the columns of R such that $R = [-Q, P]$. Let $w = [u^T, y^T]^T$ be partitioned accordingly. This is called an input-output structure of $\mathcal{B}$, and $H = P^{-1}Q \in \mathcal{K}^{p\times m}$ is called its transfer matrix. The term input-output structure is justified by the fact that

$$\forall u \in \mathcal{A}^m \exists y \in \mathcal{A}^p : Py = Qu.$$

Note that the exactness of

$$0 \longrightarrow \mathcal{D}^{1\times p} \xrightarrow{\cdot P} \mathcal{D}^{1\times p}$$

implies the exactness of

$$0 \longleftarrow \mathcal{A}^p \xleftarrow{P} \mathcal{A}^p$$

which says that $P : \mathcal{A}^p \to \mathcal{A}^p$ is even surjective, i.e., for all $v \in \mathcal{A}^p$ there exists $y \in \mathcal{A}^p$ such that $Py = v$. In particular, this is true for $v = Qu$. Then one says that u is a vector of free variables of $\mathcal{B}$. Recall that a system without free variables is called autonomous.

Corollary 4.7 *The following are equivalent:*

1. *$\mathcal{B}$ is autonomous.*
2. *$\mathcal{B}$ can be represented by a square matrix of full rank.*
3. *$\mathcal{M}$ is torsion.*

Proof: The equivalence of assertions 1 and 3 is known from the previous chapter. We also know that these two assertions are equivalent to the fact that any representation matrix has full column rank. Therefore it suffices to show that "1 $\Rightarrow$ 2": However, since representations with full row rank do always exist, a representation of an autonomous system can be assumed to have both full row and full column rank. Then it must be square of full rank. $\square$

Now we can give an analytic interpretation of autonomy.

Theorem 4.8 *The following are equivalent:*

1. *$\mathcal{B}$ is autonomous.*
2. *There exists a finite set $\mathbb{E} \subset \mathbb{R}$ such that for all open intervals $I \subseteq \mathbb{R} \setminus \mathbb{E}$, and all $w \in \mathcal{B}$ that are smooth on I, we have*

$$w|_J = 0 \quad \Rightarrow \quad w|_I = 0$$

for all open intervals $J \subseteq I$.

Proof: If $\mathcal{B}$ is autonomous, then $\mathcal{B} \cong \{y \in \mathcal{A} \mid dy = 0\}$ for some $0 \neq d \in \mathcal{D}$. If $d \in K$, then $\mathcal{B} = 0$ and the result follows. Otherwise, set $\mathbb{E} := \mathbb{E}(d)$ and let $I \subseteq \mathbb{R} \setminus \mathbb{E}$. Similarly as above, the equation $dy = 0$ can be rewritten as $\dot{x}(t) = A(t)x(t)$, where $x = [y, \ldots, y^{(n-1)}]^T$, and A is smooth on I. If y is smooth on I, then so is x. If $y|_J = 0$ for some open interval $J \subseteq I$, then $x|_J = 0$, and thus the solution x of the homogeneous equation $\dot{x} = Ax$ must be identically zero on all of I (due to the uniqueness of the solution of the initial value problem $\dot{x} = Ax$, $x(t_0) = 0$, where $t_0 \in J$), and hence this holds also for $y = x_1$.

If $\mathcal{B}$ is not autonomous, then it contains free variables. Therefore $w|_J = 0$ does not imply the vanishing of w on a larger set I, because the free variables can be chosen arbitrarily, in particular, they can take non-zero values arbitrarily close to J. $\square$

Examples:

- Consider $R = t\frac{d}{dt} + 1$, which corresponds to the differential equation

  $$\dot{w}(t) + \tfrac{1}{t}w(t) = 0.$$

  On every open interval $I \subset \mathbb{R} \setminus \{0\}$ on which w is smooth, it holds that $w(t) = \frac{c}{t}$ for some $c \in \mathbb{K}$. Thus every solution has a singularity at zero, that is, $0 \in \mathbb{E}(w)$ for all $w \in \mathcal{B}$.

  In spite of its singularity at zero, the function $w(t) = \frac{1}{t}$, defined on $\mathbb{R} \setminus \{0\}$, can be interpreted as a distribution on $\mathbb{R}$, that is, there exists $W \in \mathcal{D}'(\mathbb{R}, \mathbb{K})$ such that W and the regular distribution generated by w on $\mathbb{R} \setminus \{0\}$ assign the same value to each test function whose support is in $\mathbb{R} \setminus \{0\}$.

- Consider $R = t^3\frac{d}{dt} + 1$, which corresponds to

  $$\dot{w}(t) + \tfrac{1}{t^3}w(t) = 0.$$

  On every open interval $I \subset \mathbb{R} \setminus \{0\}$ on which w is smooth, we have $w(t) = ce^{\frac{1}{2t^2}}$ for some $c \in \mathbb{K}$. Again, we have $0 \in \mathbb{E}(w)$ for all solutions w.

  In contrast to the previous example, it is known that there exists no distribution $W \in \mathcal{D}'(\mathbb{R}, \mathbb{K})$ that coincides with the regular distribution generated by $w(t) = e^{\frac{1}{2t^2}}$ on $\mathbb{R} \setminus \{0\}$. This shows that the set of distributions is not an injective cogenerator as a $K[\frac{d}{dt}]$-module (however, it is if K is replaced by the field of constants $\mathbb{K}$).

- Consider $R = t\frac{d}{dt} - 1$. Any w of the form $w(t) = ct$, $c \in \mathbb{K}$, solves the resulting equation $Rw = 0$. Therefore, there exist solutions that are smooth on all of $\mathbb{R}$ (that is, $\mathbb{E}(w) = \emptyset$), but also any function of the form

  $$w(t) = \begin{cases} c_1 t & \text{for } t < 0 \\ c_2 t & \text{for } t > 0 \end{cases}$$

where $c_1, c_2 \in \mathbb{K}$ is a solution to $Rw = 0$ in $\mathcal{A}$ (and if $c_1 \neq c_2$, then $0 \in \mathbb{E}(w)$).

- Consider $R = t^3 \frac{d}{dt} - 1$. Here we have solutions of the form $w(t) = ce^{-\frac{1}{2t^2}}$ for $c \in \mathbb{K}$. These solutions are smooth on all of $\mathbb{R}$, even if we select different values of the constant c for $t > 0$ and $t < 0$.

- Consider $R = (1 - t^2)^2 \frac{d}{dt} + 2t$. A solution is given by

$$w(t) = \begin{cases} e^{-\frac{1}{1-t^2}} & \text{for } -1 < t < 1 \\ 0 & \text{otherwise} \end{cases}$$

which happens to be smooth on all of $\mathbb{R}$. This example shows that the autonomous equation $Rw = 0$ possesses non-zero solutions of compact support (which is impossible in the constant coefficient case). $\diamondsuit$

Image representations and controllability

Theorem 4.9 *The following are equivalent:*

1. *$\mathcal{B}$ admits an image representation.*
2. *$\mathcal{B}$ admits a right invertible kernel representation matrix.*
3. *$\mathcal{M}$ is torsion-free, or equivalently, free.*

Proof: The system $\mathcal{B} = \mathcal{A}^q$ with its module $\mathcal{M} = \mathcal{D}^{1\times q}$ satisfies all three conditions, if we use that it can be represented by the empty matrix, which we declare right invertible, as a convention. Therefore, assume that $\mathcal{B} \neq \mathcal{A}^q$, that is, $R \neq 0$.

It follows from the decomposition (4.3) that $\mathcal{M}$ is torsion-free if and only if it is free. Thus the equivalence of the first and third condition is known from the previous chapter.

Therefore it suffices to prove: Provided that R has full row rank, $\mathcal{M}$ is torsion-free if and only if R is right invertible. For a full row rank matrix R, the Jacobson form is $URV = [D, 0]$, where $D = \text{diag}(1, \ldots, 1, d)$, with $d \neq 0$. It is easy to see that R is right invertible if and only if its Jacobson form is right invertible, and for the Jacobson form, right invertibility is equivalent to $d \in K$. On the other hand, this is precisely the criterion for the vanishing of the torsion part $t\mathcal{M} \cong \mathcal{D}/\mathcal{D}d$ of $\mathcal{M}$. $\square$

Remark: The assertions of the theorem are equivalent to the statement that the element $0 \neq d$ that appears in the Jacobson form of a kernel representation R of $\mathcal{B}$ has degree zero, that is, $d \in K$. Note that since $t\mathcal{M} \cong \mathcal{D}/\mathcal{D}d$, the degree of d corresponds to the K-dimension of $t\mathcal{M}$, and therefore, it is uniquely determined by $\mathcal{M}$, or $\mathcal{B}$, equivalently. If $0 \neq d \in K$, we may put $d = 1$, without loss of generality, and then the Jacobson form of a full row rank representation $R \in \mathcal{D}^{p \times q}$ of $\mathcal{B}$ takes the form $URV = [I, 0]$.

Now we can give an interpretation of the controllability notion from the previous chapter (namely, the existence of an image representation) in terms of a concatenation property of the system trajectories.

The system $\mathcal{B}$ is called **concatenable** if for all $w_1, w_2 \in \mathcal{B}$ and all but finitely many $t_0 \in \mathbb{R}$, there exists $w \in \mathcal{B}$, an open interval $t_0 \in I \subseteq \mathbb{R}$ such that w_1, w_2, w are smooth on I, and $\tau > 0$ with $t_0 + \tau \in I$ such that

$$w(t) = \begin{cases} w_1(t) & \text{if } t < t_0 \\ w_2(t) & \text{if } t > t_0 + \tau \end{cases}$$

for all $t \in I$.

Theorem 4.10 *$\mathcal{B}$ is concatenable if and only if it is controllable.*

Proof: Let $\mathcal{B} = \{w \in \mathcal{A}^q \mid \exists \ell \in \mathcal{A}^l : w = L\ell\}$ and let $w_1 = L\ell_1, w_2 = L\ell_2 \in \mathcal{B}$ be given. Let t_0 be in $\mathbb{R} \setminus (\mathbb{E}(\ell_1) \cup \mathbb{E}(\ell_2) \cup \mathbb{E}(L))$. Then there exists an open interval $t_0 \in I \subseteq \mathbb{R}$ such that ℓ_1, ℓ_2 and w_1, w_2 are smooth on I. Choose $\tau > 0$ and let ℓ be a smooth function on I with

$$\ell(t) = \begin{cases} \ell_1(t) & \text{if } t < t_0 \\ \ell_2(t) & \text{if } t > t_0 + \tau. \end{cases}$$

Then $w := L\ell$ has the desired property. This direction of the proof can also be seen directly from the fact that if $\mathcal{B}$ has an image representation, then $\mathcal{B} \cong \mathcal{A}^m$, and $\mathcal{A}^m$ has the required concatenability property.

For the converse, it suffices to show that $\mathcal{B}_a = \{w \in \mathcal{A} \mid dw = 0\}$, where $d \in \mathcal{D} \setminus K$, is not concatenable. Let w_1 be the zero solution, and let w_2 be a non-zero solution. Then there exists an open interval $J \subseteq \mathbb{R} \setminus \mathbb{E}(d)$ on which w_2 is smooth and does not vanish. Let $t_0 \in J$. Suppose that w were a connecting trajectory. Then w is smooth on some open neighborhood $I \subseteq J$ of t_0. On the other hand, since $\mathcal{B}_a$ is autonomous, $w(t) = w_1(t) = 0$ for all $t \in I$ with $t < t_0$ implies that $w(t) = 0$ for all $t \in I$. This contradicts $w(t) = w_2(t) \neq 0$ for all $t \in I$ with $t > t_0 + \tau$. □

Theorem 4.11 *There exists a largest controllable subsystem $\mathcal{B}_c$ of $\mathcal{B}$, and $\mathcal{B}$ can be decomposed into a direct sum*

$$\mathcal{B} = \mathcal{B}_a \oplus \mathcal{B}_c$$

where $\mathcal{B}_a$ is autonomous.

This decomposition corresponds to (4.3). Note that

$$\mathcal{B}_a \cong \mathrm{Hom}_{\mathcal{D}}(t\mathcal{M}, \mathcal{A}) \cong \mathrm{Hom}_{\mathcal{D}}(\mathcal{D}/\mathcal{D}d, \mathcal{A}) \cong \{y \in \mathcal{A} \mid dy = 0\}$$

and

$$\mathcal{B}_c \cong \mathrm{Hom}_{\mathcal{D}}(\mathcal{M}/t\mathcal{M}, \mathcal{A}) \cong \mathrm{Hom}_{\mathcal{D}}(\mathcal{D}^{1\times m}, \mathcal{A}) \cong \mathcal{A}^m.$$

Proof: Let R be a full row rank representation of $\mathcal{B}$, and let $URV = \begin{bmatrix} D & 0 \end{bmatrix}$ be the Jacobson form of R. Let $W = V^{-1}$ be partitioned as in (4.5). Then

$$w \in \mathcal{B} \quad \Leftrightarrow \quad \begin{bmatrix} D & 0 \end{bmatrix} Ww = DW_1 w = 0.$$

Let $V = [V_1, V_2]$ be partitioned accordingly and set

$$\begin{aligned} \mathcal{B}_c &= \{w \in \mathcal{A}^q \mid W_1 w = 0\} \\ &= \{w \in \mathcal{A}^q \mid \exists \ell \in \mathcal{A}^m : w = V_2 \ell\}. \end{aligned}$$

The second equality follows from $W = V^{-1}$, which implies $W_1 V_2 = 0$ and $V_1 W_1 + V_2 W_2 = I$, from which one can conclude that $\mathrm{im}(\cdot W_1) = \ker(\cdot V_2)$. Then $\mathcal{B}_c \subseteq \mathcal{B}$ is controllable. If $\mathcal{B}_1$ is another controllable subsystem of $\mathcal{B}$, then $\mathcal{B}_1 \subseteq \mathcal{B}_c$. Define

$$\mathcal{B}_a = \{w \in \mathcal{A}^q \mid DW_1 w = 0 \text{ and } W_2 w = 0\}.$$

Then $\mathcal{B}_a \subseteq \mathcal{B}$ is autonomous, and $\mathcal{B} = \mathcal{B}_a \oplus \mathcal{B}_c$, where the decomposition is given by $w = V_1 W_1 w + V_2 W_2 w$. □

Observability

Let $R = [R_1, R_2]$ and let $w = [w_1^T, w_2^T]^T$ be partitioned accordingly. One says that w_1 is observable from w_2 in $R_1 w_1 + R_2 w_2 = 0$ if w_1 is uniquely determined by w_2. Due to linearity, this is equivalent to

$$\mathcal{B}_1 := \{w_1 \in \mathcal{A}^{q_1} \mid R_1 w_1 = 0\} = 0.$$

Theorem 4.12 *Let $\mathcal{B}$ be given by $Rw = R_1 w_1 + R_2 w_2 = 0$. Then w_1 is observable from w_2 if and only if R_1 is left invertible.*

4.3 Time-invariant case

All the results of Section 4.2 hold also for the constant coefficient case, that is, $\mathcal{D} = \mathbb{K}[\frac{d}{dt}]$ and $\mathcal{A} = \mathcal{C}^\infty(\mathbb{R}, \mathbb{K})$, with some slight modifications of the proofs where necessary. The main difference is that the matrix D from the Jacobson form (which is then the Smith form) has the form $D = \text{diag}(d_1, \ldots, d_p)$. Thus the torsion submodule $t\mathcal{M}$ of $\mathcal{M}$ is isomorphic to $\mathcal{D}/\mathcal{D}d_1 \oplus \cdots \oplus \mathcal{D}/\mathcal{D}d_p$. Still, the characterizations of Theorem 4.9 are equivalent to $D = I$. Similarly, $\mathcal{B}_a$ is isomorphic to $\{y \in \mathcal{A}^p \mid d_i y_i = 0 \text{ for } 1 \leq i \leq p\}$. The quotient field of $\mathcal{D}$ is the field of rational functions $\mathcal{K} = \mathbb{K}(\frac{d}{dt})$, and thus transfer matrices are rational.

The concepts of autonomy and controllability, formulated in terms of the trajectories, become simpler:

- $\mathcal{B}$ is autonomous if for all $w \in \mathcal{B}$ and all open intervals $J \subseteq \mathbb{R}$, we have
$$w|_J = 0 \quad \Rightarrow \quad w = 0.$$
- $\mathcal{B}$ is controllable if for all $w_1, w_2 \in \mathcal{B}$, and all $t_0 \in \mathbb{R}$, there exists $w \in \mathcal{B}$ and $\tau > 0$ such that
$$w(t) = \begin{cases} w_1(t) & \text{if } t < t_0 \\ w_2(t) & \text{if } t > t_0 + \tau \end{cases}$$
for all $t \in \mathbb{R}$. Here, we can put $t_0 = 0$ without loss of generality.

Chapter 5

Multi-dimensional systems

In this chapter,

$$\mathcal{D} = \mathbb{K}[\partial_1, \ldots, \partial_n] \quad \text{and} \quad \mathcal{A} = \mathcal{C}^\infty(\mathbb{R}^n, \mathbb{K}),$$

that is, we deal with systems of linear partial differential equations with constant coefficients (note that linear ordinary differential equations with constant coefficients are included as the special case $n = 1$) and their smooth solutions.

The ring $\mathcal{D}$ is a commutative Noetherian domain, and the $\mathcal{D}$-module $\mathcal{A}$ is an injective cogenerator. Therefore the theory of Chapter 3 is directly applicable. However, $\mathcal{D}$ is not a principal ideal domain (unless $n = 1$), and therefore, there exists no analogue of the Smith form for $n \geq 2$. Thus the results of the previous chapter do not translate to this setting, for example, not every system has a full row rank representation.

5.1 Interpretation of autonomy and controllability

Let $\mathcal{B} = \{w \in \mathcal{A}^q \mid Rw = 0\}$, where $R \in \mathcal{D}^{g \times q}$.

Lemma 5.1 *Let $\mathcal{B}$ be autonomous. If $w \in \mathcal{B}$ has compact support, then $w = 0$.*

Proof: Let $\mathcal{B} = \{w \in \mathcal{A}^q \mid Rw = 0\}$ be autonomous. This means that R has full column rank. Let $w \in \mathcal{B}$ have compact support. Then w has a well-defined Fourier transform $\hat{w} := \mathcal{F}w$, defined by

$$\hat{w}(\xi) = \int_{\mathbb{R}^n} w(x) e^{-i\langle x, \xi \rangle} dx,$$

where $\langle x, \xi \rangle = \sum_{i=1}^{n} x_i \xi_i$, and $\hat{w}$ is an analytic function of $\xi \in \mathbb{R}^n$. The Fourier transform of $Rw = 0$ yields $R(i\xi)\hat{w}(\xi) = 0$. This can be interpreted as a linear equation over the field of meromorphic functions. Since $R(i\xi)$ has full column rank, we obtain $\hat{w} = 0$, and hence, using the inverse Fourier transform, $w = 0$. □

Theorem 5.2 *The following are equivalent [19]:*

1. *$\mathcal{B}$ is controllable, i.e., it possesses an image representation.*
2. *For all open sets $U_1, U_2 \subset \mathbb{R}^n$, with $\overline{U}_1 \cap \overline{U}_2 = \emptyset$, and for all $w_1, w_2 \in \mathcal{B}$, there exists $w \in \mathcal{B}$ such that*
$$w(x) = \begin{cases} w_1(x) & \text{if } x \in U_1 \\ w_2(x) & \text{if } x \in U_2. \end{cases}$$
3. *For all $0 < r_1 < r_2$ and for all $w_1, w_2 \in \mathcal{B}$, there exists $w \in \mathcal{B}$ such that*
$$w(x) = \begin{cases} w_1(x) & \text{if } x \in U_1 \\ w_2(x) & \text{if } x \in U_2, \end{cases}$$
where
$$U_1 = \{x \in \mathbb{R}^n \mid \|x\| < r_1\} \quad \text{and} \quad U_2 = \{x \in \mathbb{R}^n \mid \|x\| > r_2\},$$
and $\|\cdot\|$ denotes the Euclidean norm.

Proof: "1 ⇒ 2": Suppose that $\mathcal{B}$ possesses an image representation
$$\mathcal{B} = \{w \in \mathcal{A}^q \mid \exists \ell \in \mathcal{A}^l : w = L\ell\}.$$
Let U_i and $w_i = L\ell_i$ for $i = 1, 2$ be given. It is a fundamental property of $\mathcal{A} = \mathcal{C}^\infty(\mathbb{R}, \mathbb{K})$ that for any open sets U_1, U_2 whose closures are disjoint, there exists a smooth function χ with [23, §1, VIII]
$$\chi(x) = \begin{cases} 1 & \text{if } x \in U_1 \\ 0 & \text{if } x \in U_2. \end{cases}$$
Set $\ell := \chi\ell_1 + (1 - \chi)\ell_2 \in \mathcal{A}^l$. Then
$$\ell(x) = \begin{cases} \ell_1(x) & \text{if } x \in U_1 \\ \ell_2(x) & \text{if } x \in U_2. \end{cases}$$
Set $w := L\ell$, then $w \in \mathcal{B}$ has the desired properties.

Since assertion 3 is obviously a special case of assertion 2, it suffices to show that "3 ⇒ 1": If $\mathcal{B}$ is not controllable, then $\mathcal{B}_c \subsetneq \mathcal{B}$, that is, there exists $w_0 \in \mathcal{B}$ with

$v_0 := R_c w_0 \neq 0$, but $dv_0 = 0$ (recall that $dR_c = NR$ for some $0 \neq d \in \mathcal{D}$ and some $\mathcal{D}$-matrix N). Let x_0 be such that $v_0(x_0) \neq 0$. Choose $r_2 > r_1 > \|x_0\|$ and let U_1, U_2 be the corresponding sets from assertion 3. We show that there exists no $w \in \mathcal{B}$ such that

$$w(x) = \begin{cases} w_0(x) & \text{if } x \in U_1 \\ 0 & \text{if } x \in U_2. \end{cases}$$

Indeed, if this were the case, then $v := R_c w$ would be a non-zero compact support element of the autonomous system $\{v \in \mathcal{A} \mid dv = 0\}$, which is impossible according to the lemma above. □

Lemma 5.3 *If $\mathcal{B} \neq 0$ is controllable, then it contains a non-zero trajectory with compact support.*

Proof: Let $0 \neq w_0 \in \mathcal{B}$. Let x_0 be such that $w_0(x_0) \neq 0$. Let $r_2 > r_1 > \|x_0\|$ and let U_1, U_2 be as defined above. By controllability, there exists $w \in \mathcal{B}$ such that

$$w(x) = \begin{cases} w_0(x) & \text{if } x \in U_1 \\ 0 & \text{if } x \in U_2. \end{cases}$$

Then w is non-zero and it has compact support. □

Theorem 5.4 *The following are equivalent:*

1. *$\mathcal{B}$ is autonomous.*

2. *If $w \in \mathcal{B}$ has compact support, then $w = 0$.*

Proof: In view of the previous lemma, it suffices to prove "2 ⇒ 1": Assume that $\mathcal{B} = \{w \in \mathcal{A}^q \mid Rw = 0\}$ is not autonomous, that is, $\mathcal{B}_c \neq 0$. By the previous lemma, $\mathcal{B}_c$ contains a non-zero trajectory with compact support, and therefore, so does $\mathcal{B} \supseteq \mathcal{B}_c$. □

Now we can give an interpretation to the obstruction to controllability $\mathcal{B}/\mathcal{B}_c$ introduced earlier. We say that w_1 and $w_2 \in \mathcal{B}$ are **concatenable**, written $w_1 \sim w_2$, if for all U_1, U_2 as above, there exists $w \in \mathcal{B}$ such that $w = w_i$ on U_i. This defines an equivalence relation on $\mathcal{B}$.

Theorem 5.5 *We have*

$$\mathcal{B}/\!\sim\; \cong\; \mathcal{B}/\mathcal{B}_c$$

that is, $w_1 \sim w_2$ if and only if $w_1 - w_2 \in \mathcal{B}_c$.

This justifies the term "obstruction to controllability": each residue class $[w]$ in $\mathcal{B}/\mathcal{B}_c$ corresponds to an equivalence class with respect to concatenability. The system $\mathcal{B}$ is controllable if and only if all $w_1, w_2 \in \mathcal{B}$ are concatenable, i.e., there is only one equivalence class, or equivalently, $\mathcal{B} = \mathcal{B}_c$, that is, the obstruction to controllability vanishes. On the other hand, an autonomous system is one in which every trajectory can only be concatenated with itself (because the controllable part of an autonomous system is zero).

Proof: It suffices to show that $w \sim 0$ if and only if $w \in \mathcal{B}_c$. If $w \in \mathcal{B}_c$, then the image representation of $\mathcal{B}_c$ can be used in order to concatenate w with zero as explained above.

Conversely, if $w \notin \mathcal{B}_c$, then we have $dR_c w = 0$, but $R_c w \neq 0$, and we have seen above that w cannot be concatenated with zero. □

Examples:

- Let $n = 3$ and consider
$$R = \begin{bmatrix} 0 & -\partial_3 & \partial_2 \\ \partial_3 & 0 & -\partial_1 \\ -\partial_2 & \partial_1 & 0 \end{bmatrix}.$$
Then $\mathcal{B} = \{w \in \mathcal{A}^3 \mid Rw = 0\}$ consists of all vector fields whose curl is zero. Since R is a left syzygy matrix, this $\mathcal{B}$ is controllable. An image representation $\mathcal{B} = \{w \in \mathcal{A}^3 \mid \exists \ell \in \mathcal{A} : w = L\ell\}$ is given by
$$L = \begin{bmatrix} \partial_1 \\ \partial_2 \\ \partial_3 \end{bmatrix}.$$
Algebraically speaking, this means that $\ker(\cdot L) = \operatorname{im}(\cdot R)$, and analytically, it reflects the fact that w is the gradient of some scalar potential ℓ if and only if the curl of w vanishes.

- Now consider
$$R = \begin{bmatrix} 0 & -\partial_3 & \partial_2 \\ \partial_3 & 0 & -\partial_1 \end{bmatrix}.$$
The resulting system is not controllable, in fact, its controllable part is precisely the system from above. A trajectory w is concatenable with zero if and only if $\partial_1 w_2 - \partial_2 w_1 = 0$.

- The system $\mathcal{B} = \{w \in \mathcal{A}^3 \mid \operatorname{div}(w) = 0\}$ is represented by $R = [\partial_1, \partial_2, \partial_3]$ and it is controllable. An image representation is given by the curl operator, reflecting the fact that w is the curl of some $\ell \in \mathcal{A}^3$ if and only if the divergence of w vanishes.

- Let us consider
$$\mathcal{B} = \{w_1 \in \mathcal{A}^3 \mid R_1 w_1 = 0\} + \{w_2 \in \mathcal{A}^3 \mid R_2 w_2 = 0\}$$
where R_1 is the curl operator from above, and $R_2 = [\partial_1, \partial_2, \partial_3]$ is the divergence operator. Using the image representation matrices L_1, L_2 of the two summands, it is clear that $L = [L_1, L_2]$ is an image representation matrix of $\mathcal{B}$. However,
$$L = \begin{bmatrix} \partial_1 & 0 & -\partial_3 & \partial_2 \\ \partial_2 & \partial_3 & 0 & -\partial_1 \\ \partial_3 & -\partial_2 & \partial_1 & 0 \end{bmatrix}$$
has full row rank. From this, we conclude that $\mathcal{B} = \mathcal{A}^3$. Thus we have shown that any w in $\mathcal{A}^3$ can be written in the form $w = w_1 + w_2$, where the curl of w_1 vanishes, and the divergence of w_2 vanishes. This is known as the Helmholtz-Hodge decomposition.

- Let $n = 4$. The Maxwell equations are given by
$$\begin{aligned} \mathrm{div}(B) &= 0 \\ \mathrm{curl}(E) + \partial_t B &= 0. \end{aligned}$$
Setting $w = [B_1, B_2, B_3, E_1, E_2, E_3]^T$, a kernel representation is given by
$$R = \begin{bmatrix} \partial_1 & \partial_2 & \partial_3 & 0 & 0 & 0 \\ \partial_t & 0 & 0 & 0 & -\partial_3 & \partial_2 \\ 0 & \partial_t & 0 & \partial_3 & 0 & -\partial_1 \\ 0 & 0 & \partial_t & -\partial_2 & \partial_1 & 0 \end{bmatrix}.$$
The resulting system, consisting of all pairs of magnetic and electric fields that satisfy the Maxwell equations, is controllable. An image representation is given by
$$L = \begin{bmatrix} 0 & -\partial_3 & \partial_2 & 0 \\ \partial_3 & 0 & -\partial_1 & 0 \\ -\partial_2 & \partial_1 & 0 & 0 \\ -\partial_t & 0 & 0 & -\partial_1 \\ 0 & -\partial_t & 0 & -\partial_2 \\ 0 & 0 & -\partial_t & -\partial_3 \end{bmatrix}.$$
This means that any B, E that satisfy the Maxwell equations can be written as
$$\begin{aligned} B &= \mathrm{curl}(A) \\ E &= -\partial_t A - \mathrm{grad}(\phi) \end{aligned}$$
for some $\ell = [A_1, A_2, A_3, \phi]^T$. These equations are well-known in physics, where A is called the magnetic vector potential, and ϕ is the scalar electric potential. $\diamondsuit$

5.2 The dimension of a system

Facts from dimension theory

Let $\mathcal{D}$ be a commutative ring (with unity). Let $\mathcal{M}$ be a $\mathcal{D}$-module. One defines

$$\operatorname{ann}(\mathcal{M}) := \{d \in \mathcal{D} \mid d\mathcal{M} = 0\},$$

which is an ideal in $\mathcal{D}$. The **dimension** of $\mathcal{M} \neq 0$ is defined by

$$\dim(\mathcal{M}) := \dim(\operatorname{ann}(\mathcal{M})).$$

The **dimension of an ideal** $\mathcal{I} \neq \mathcal{D}$ in $\mathcal{D}$ is defined as the **Krull dimension** of the ring $\mathcal{D}/\mathcal{I}$, that is, $\dim(\mathcal{I}) := \text{Krull-dim}(\mathcal{D}/\mathcal{I}) :=$

$$\sup\{n \in \mathbb{N} \mid \exists \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n, \mathfrak{p}_i \text{ prime ideal in } \mathcal{D}/\mathcal{I}\ \forall i\}.$$

The surjective ring homomorphism $\mathcal{D} \to \mathcal{D}/\mathcal{I}$ induces an inclusion-preserving bijection between the ideals in $\mathcal{D}/\mathcal{I}$ and the ideals in $\mathcal{D}$ that contain $\mathcal{I}$. Since the primeness of an ideal is preserved under this correspondence, we have

$$\dim(\mathcal{I}) = \sup\{n \in \mathbb{N} \mid \exists \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n, \mathfrak{p}_i \text{ prime ideal in } \mathcal{D}, \mathfrak{p}_i \supseteq \mathcal{I}\ \forall i\}.$$

In particular, for a prime ideal $\mathfrak{p}$ in $\mathcal{D}$, we obtain

$$\dim(\mathfrak{p}) = \sup\{n \in \mathbb{N} \mid \exists \mathfrak{p} = \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n, \mathfrak{p}_i \text{ prime ideal in } \mathcal{D}\ \forall i\}.$$

The **height** of $\mathfrak{p}$ is defined by

$$\operatorname{ht}(\mathfrak{p}) := \sup\{m \in \mathbb{N} \mid \exists \mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \ldots \subsetneq \mathfrak{q}_m = \mathfrak{p}, \mathfrak{q}_i \text{ prime ideal in } \mathcal{D}\ \forall i\}.$$

Therefore, we have

$$\operatorname{ht}(\mathfrak{p}) + \dim(\mathfrak{p}) \leq \text{Krull-dim}(\mathcal{D})$$

for any prime ideal $\mathfrak{p}$ in $\mathcal{D}$. This implies that for any ideal $\mathcal{I} \neq \mathcal{D}$, we have

$$\operatorname{ht}(\mathcal{I}) + \dim(\mathcal{I}) \leq \text{Krull-dim}(\mathcal{D}),$$

since

$$\dim(\mathcal{I}) = \sup\{\dim(\mathfrak{p}) \mid \mathfrak{p} \text{ prime ideal in } \mathcal{D} \text{ and } \mathfrak{p} \supseteq \mathcal{I}\}.$$

Similarly,

$$\operatorname{ht}(\mathcal{I}) := \inf\{\operatorname{ht}(\mathfrak{p}) \mid \mathfrak{p} \text{ prime ideal in } \mathcal{D} \text{ and } \mathfrak{p} \supseteq \mathcal{I}\}.$$

Coming back to the module $\mathcal{M}$, suppose that $\mathcal{M} = \mathcal{D}^{1\times q}/\mathcal{D}^{1\times g}R$. Then

$$\operatorname{ann}(\mathcal{M}) = \{d \in \mathcal{D} \mid \exists X \in \mathcal{D}^{q\times g} : dI = XR\}.$$

This should be compared with Theorem 3.4. Indeed, if $\mathcal{D}$ is commutative, then the condition given there is equivalent to $\text{ann}(\mathcal{M}) \neq 0$.

The **Fitting invariant** $\mathcal{F}(\mathcal{M})$ of $\mathcal{M}$ is defined as the ideal generated by the $q \times q$ subdeterminants of R, which is called the q-th **determinantal ideal** [16, Ch. 1.4] of R, and which is denoted by $J_q(R)$. One can show that $\mathcal{F}(\mathcal{M})$ does not depend on the specific choice of the presentation matrix R of $\mathcal{M}$ with q columns. We have [6, Ch. 20.2]

$$\text{ann}(\mathcal{M})^q \subseteq \mathcal{F}(\mathcal{M}) \subseteq \text{ann}(\mathcal{M}),$$

which implies that $\text{ann}(\mathcal{M})$ and $\mathcal{F}(\mathcal{M})$ have the same radical, and hence any prime ideal that contains one of them also contains the other. We conclude that the two ideals have the same height and the same dimension. Therefore,

$$\dim(\mathcal{D}^{1\times q}/\mathcal{D}^{1\times g}R) = \dim(J_q(R)).$$

Now let $\mathcal{D} = \mathbb{K}[\partial_1, \ldots, \partial_n]$. Then we have

$$\text{ht}(\mathcal{I}) + \dim(\mathcal{I}) = \text{Krull-dim}(\mathcal{D}) = n$$

for any ideal $\mathcal{I} \neq \mathcal{D}$. As a convention, we set

$$\text{ht}(\mathcal{D}) := n + 1 \quad \text{and} \quad \dim(\mathcal{D}) := -1.$$

Therefore, the dimension of any ideal $\mathcal{I}$ in $\mathcal{D}$ is an integer between -1 and n, where $\dim(\mathcal{I}) = -1$ is equivalent to $\mathcal{I} = \mathcal{D}$, and $\dim(\mathcal{I}) = n$ is equivalent to $\mathcal{I} = 0$. More generally, we have

$$\mathcal{I} \subseteq \mathcal{J} \quad \Rightarrow \quad \dim(\mathcal{I}) \geq \dim(\mathcal{J}).$$

This is counter-intuitive at first sight, but the reason is that, when defined this way, the dimension of $\mathcal{I}$ coincides with the dimension of its algebraic variety

$$\mathfrak{V}(\mathcal{I}) = \{v \in \mathbb{C}^n \mid f(v) = 0 \text{ for all } f \in \mathcal{I}\},$$

and thus, the dimension of an ideal has a neat geometric interpretation.

Examples:

- Let $n = 2$. The ideal $\mathcal{I} = \langle \partial_1 \rangle$ has dimension one (its variety is a line), whereas the ideal $\mathcal{J} = \langle \partial_1, \partial_2 \rangle$ has dimension zero (its variety is a point).

- Let $n = 3$. The ideal $\mathcal{I} = \langle \partial_1 \rangle$ has dimension two (its variety is a plane). Comparing this with the previous example, we see that the dimension of an ideal depends on the polynomial ring into which we embed it. The height, however, is independent of this embedding (we have $\text{ht}(\mathcal{I}) = 1$ in any $\mathbb{K}[\partial_1, \ldots, \partial_n]$). Similarly, the ideal $\mathcal{J} = \langle \partial_1, \partial_2 \rangle$ has dimension one, and the ideal $\mathcal{L} = \langle \partial_1, \partial_2, \partial_3 \rangle$ has dimension zero. $\Diamond$

For $\mathcal{D} = \mathbb{K}[\partial_1, \ldots, \partial_n]$, we also have the following characterization of the dimension of an ideal $\mathcal{I} \neq \mathcal{D}$ [1, Ch. 6.3]: Let $J \subseteq \{1, \ldots, n\}$ and let $\mathcal{D}_J$ be the polynomial ring (with coefficients in $\mathbb{K}$) in the variables ∂_j, $j \in J$. Clearly, $\mathcal{D}_J$ is a subring of $\mathcal{D}$, and we put $\mathcal{D}_\emptyset = \mathbb{K}$. Then

$$\dim(\mathcal{I}) = \max\{|J| \mid \mathcal{I} \cap \mathcal{D}_J = 0\}.$$

For example, $\dim(\mathcal{I}) < 1$ means that for all $1 \leq i \leq n$, we have $\mathcal{I} \cap \mathbb{K}[\partial_i] \neq 0$, that is, there exists $0 \neq d_i \in \mathcal{I}$ which depends only on the i-th variable.

Application to systems

Let $\mathcal{B} = \{w \in \mathcal{A}^q \mid Rw = 0\}$ and let $\mathcal{M} = \mathcal{D}^{1\times q}/\mathcal{D}^{1\times g}R$. The **dimension** of $\mathcal{B}$ is defined as the dimension of $\mathcal{M}$. As outlined above, this is both equal to the dimension of the ideal $\mathrm{ann}(\mathcal{M})$ and equal to the dimension of $J_q(R)$, which is the ideal generated by the $q \times q$ minors of R.

Lemma 5.6 *The following are equivalent:*

1. $\dim(\mathcal{B}) = -1$.
2. $\mathcal{B} = 0$.

Proof: We have $\mathcal{B} = 0$ if and only if $\mathcal{M} = 0$. However, $\mathcal{M} = 0$ is equivalent to $\mathrm{ann}(\mathcal{M}) = \mathcal{D}$, which is true if and only if $\dim(\mathcal{B}) = \dim(\mathrm{ann}(\mathcal{M})) = -1$. □

Lemma 5.7 *The following are equivalent:*

1. $\dim(\mathcal{B}) < n$.
2. *$\mathcal{B}$ is autonomous.*

Proof: We have $\dim(\mathcal{B}) = n$ if and only if $J_q(R) = 0$. This means that all the $q \times q$ minors of R are zero, or equivalently, R does not have full column rank, which means that $\mathcal{B}$ is not autonomous. □

Therefore, the dimension of a system $\mathcal{B}$ is always an integer between -1 and n, where $\dim(\mathcal{B}) = -1$ corresponds to $\mathcal{B} = 0$, and $\dim(\mathcal{B}) = n$ corresponds to $\mathcal{B}$ having free variables. The dimensions between 0 and $n-1$ yield a refinement of the concept of autonomy.

5.3 Autonomy degrees

We say that $\mathcal{B}$ has **autonomy degree** at least r if

$$\dim(\mathcal{B}) < n - r.$$

Clearly, autonomy degree at least zero corresponds to autonomy itself. In what follows, we will give analytic interpretations of the autonomy degrees close to the extreme cases.

Autonomy degree at least n

The system $\mathcal{B}$ has autonomy degree at least n if and only if $\dim(\mathcal{B}) < 0$, which means that $\mathcal{B} = 0$, a very strong form of autonomy indeed.

Autonomy degree at least $n-1$

Theorem 5.8 *The following are equivalent:*

1. *$\mathcal{B}$ has autonomy degree at least $n-1$.*
2. *$\mathcal{B}$ is finite-dimensional as a $\mathbb{K}$-vector space.*

Proof: We first observe that

$$\operatorname{ann}(\mathcal{B}) := \{d \in \mathcal{D} \mid d\mathcal{B} = 0\} = \operatorname{ann}(\mathcal{M}).$$

To see this, recall that for any $d \in \operatorname{ann}(\mathcal{M})$, there exists X such that $dI = XR$, and thus $Rw = 0$ implies $dw = 0$. Conversely, if $dw = 0$ for all $w \in \mathcal{B}$, we must have $dI = XR$ for some X, since $\mathfrak{MB}(\mathcal{D}^{1\times g}R) = \mathcal{D}^{1\times g}R$ because of the injective cogenerator property of $\mathcal{A}$.

Now if $\dim(\mathcal{B}) < 1$, then $\operatorname{ann}(\mathcal{M})$ contains, for each $1 \le i \le n$, an element $0 \ne d_i \in \mathbb{K}[\partial_i]$. Thus every component of $w \in \mathcal{B}$ satisfies n scalar ordinary differential equations (one for each independent variable). Since the solution spaces of autonomous ordinary differential equations are finite-dimensional over $\mathbb{K}$ according to the lemma below, we obtain that $\mathcal{B}$ must be finite-dimensional as a $\mathbb{K}$-vector space, too.

Conversely, let $\mathcal{B}$ be finite-dimensional over $\mathbb{K}$, and let $w_1, \ldots, w_r$ be a $\mathbb{K}$-basis. For each $1 \le i \le n$ and each $1 \le j \le r$, consider the $\mathbb{K}$-vector space spanned by

$\partial_i^k w_j \in \mathcal{B}$, where $k \in \mathbb{N}$. As a subspace of $\mathcal{B}$, this space must be finite-dimensional, too. Thus there exists $0 \neq d_{ij} \in \mathbb{K}[\partial_i]$ such that $d_{ij} w_j = 0$. But then we have $d_i w = 0$ for all $w \in \mathcal{B}$ for $d_i := d_{i1} \cdots d_{ir}$. This way, we can construct elements $0 \neq d_i \in \mathrm{ann}(\mathcal{M}) \cap \mathbb{K}[\partial_i]$, showing that $\dim(\mathrm{ann}(\mathcal{M})) < 1$. □

Lemma 5.9 *Let $n = 1$. Then $\mathcal{B}$ is autonomous if and only if it is finite-dimensional as a $\mathbb{K}$-vector space.*

Proof: If $\mathcal{B}$ contains free variables, then it is certainly not finite-dimensional over $\mathbb{K}$, because the $\mathbb{K}$-vector space $\mathcal{A} = \mathcal{C}^\infty(\mathbb{R}, \mathbb{K})$ has infinite dimension. Conversely, if $\mathcal{B}$ is autonomous, then $\mathcal{B} \cong \{y \in \mathcal{A}^p \mid d_i y_i = 0 \text{ for } 1 \leq i \leq p\}$ for some $0 \neq d_i \in \mathcal{D}$, due to the Smith form. Each scalar ordinary differential equation $d_i y_i = 0$ has a solution space whose $\mathbb{K}$-dimension equals the degree of d_i. Therefore $\mathcal{B}$ is also finite-dimensional over $\mathbb{K}$. □

For $n \geq 2$ however, autonomy and finite $\mathbb{K}$-dimension are no longer equivalent; autonomy is a weaker property. For example, $\mathcal{B} = \{w \in \mathcal{C}^\infty(\mathbb{R}^2, \mathbb{K}) \mid \partial_1 w = 0\}$ is autonomous, but not finite-dimensional (any smooth function depending only on the second variable belongs to $\mathcal{B}$).

Examples:

- The system given by $\mathcal{B} = \{w \in \mathcal{A} \mid \mathrm{grad}(w) = 0\}$ has the kernel representation
$$R = \begin{bmatrix} \partial_1 \\ \vdots \\ \partial_n \end{bmatrix}.$$
Thus $J_1(R) = \langle \partial_1, \ldots, \partial_n \rangle$ which has dimension zero for all n. Therefore its solution space is finite-dimensional. Of course, this can also be seen directly, because $\mathcal{B}$ consists of all constant functions in this example, and therefore $\mathcal{B} \cong \mathbb{K}$, which is a one-dimensional $\mathbb{K}$-vector space.

- Let $n = 2$ and $\mathbb{K} = \mathbb{R}$. Consider $\mathcal{B} = \{w \in \mathcal{A} \mid \partial_1^2 w = \partial_2 w, \partial_2^2 w = w\}$. Then $J_1(R) = \langle \partial_1^2 - \partial_2, \partial_2^2 - 1 \rangle$, which has dimension zero, because it contains the elements $\partial_1^4 - 1 = (\partial_1^2 + \partial_2)(\partial_1^2 - \partial_2) + (\partial_2^2 - 1)$ and $\partial_2^2 - 1$. If we set $x(t) := w(t_1, t)$, considering t_1 as a parameter, the equation $\partial_2^2 w = w$ becomes
$$\ddot{x} = x.$$
The solutions are of the form
$$x(t) = ae^t + be^{-t}.$$

Thus

$$w(t_1, t_2) = a(t_1)e^{t_2} + b(t_1)e^{-t_2}.$$

Now the equation $\partial_1^2 w = \partial_2 w$ implies

$$\ddot{a} = a \quad \text{and} \quad \ddot{b} = -b,$$

and thus

$$a(t_1) = c_1 e^{t_1} + c_2 e^{-t_1} \quad \text{and} \quad b(t_1) = c_3 \cos(t_1) + c_4 \sin(t_1).$$

Finally, we have

$$w(t_1, t_2) = c_1 e^{t_1} e^{t_2} + c_2 e^{-t_1} e^{t_2} + c_3 \cos(t_1) e^{-t_2} + c_4 \sin(t_1) e^{-t_2},$$

showing that the solution space is four-dimensional over $\mathbb{K} = \mathbb{R}$. ◊

Remark: Systems with finite $\mathbb{K}$-dimension can be solved by iteratively solving ordinary differential equations. Therefore, they behave very much like autonomous one-dimensional ($n = 1$) systems. For instance, they have only polynomial-exponential trajectories (with complex exponents admitted, which explains the appearance of sine and cosine in the previous example).

In fact, the $\mathbb{K}$-vector space isomorphism $\mathcal{M} \cong \mathbb{K}^N$ can be used to construct pairwise commuting matrices $A_i \in \mathbb{K}^{N \times N}$ and a matrix $C \in \mathbb{K}^{q \times N}$ such that

$$\mathcal{B} = \{w \in \mathcal{A}^q \mid \exists x \in \mathcal{A}^N : \partial_i x = A_i x \text{ for } 1 \leq i \leq n \text{ and } w = Cx\}$$

which can also be written as

$$\mathcal{B} = \{w \in \mathcal{A}^q \mid \exists x_0 \in \mathbb{K}^N : w(t_1, \ldots, t_n) = Ce^{A_1 t_1 + \ldots + A_n t_n} x_0\}.$$

These are generalizations of one-dimensional autonomous systems, which after reduction to first order, take the form $\dot{x} = Ax$, $w = Cx$, or equivalently, $w(t) = Ce^{At}x_0$.

Autonomy degree at least 1

A system has autonomy degree at least one if and only if it is **over-determined** [18, Ch. 8]. This means that any smooth function v, defined on a neighborhood of

$$\overline{U} = \{x \in \mathbb{R}^n \mid \|x\| \geq r\},$$

where $r > 0$, and satisfying the local system law $Rv = 0$ there, can be uniquely extended to an element $w \in \mathcal{B}$, that is, there exists a unique $w \in \mathcal{B}$ (i.e., w is defined on all of $\mathbb{R}^n$ and satisfies $Rw = 0$ everywhere) such that $w(x) = v(x)$ for all x in a neighborhood of $\overline{U}$.

We do not give the full proof, but only an overview of its main ingredients.

Theorem 5.10 *1. If* $\dim(\mathcal{B}) < n-1$*, then* R *is a right syzygy matrix, that is,* $\mathrm{im}(R) = \ker(L)$ *for some* $\mathcal{D}$*-matrix* L*.*

2. If

$$\mathcal{D}^q \xrightarrow{R} \mathcal{D}^g \xrightarrow{L} \mathcal{D}^l$$

is exact, then so is

$$\mathcal{A}_0^q \xrightarrow{R} \mathcal{A}_0^g \xrightarrow{L} \mathcal{A}_0^l$$

where $\mathcal{A}_0 := \mathcal{C}_0^\infty(\Omega, \mathbb{K})$*, and* $\Omega = \{x \in \mathbb{R}^n \mid \|x\| < r\}$ *for some* $r > 0$*.*

The space $\mathcal{A}_0$ consists of all smooth functions defined on Ω and having a compact support $K \subset \Omega$. We identify

$$\mathcal{A}_0 = \{a \in \mathcal{A} \mid \mathrm{supp}(a) \subset \Omega\}.$$

Let $\mathcal{B}$ have autonomy degree at least one. We show that $\mathcal{B}$ is over-determined.

The lemma above implies that R is a right syzygy matrix, say of L. Then the sequences of the theorem are both exact. Now let v as above be given. Since v is smooth on a neighborhood of $\overline{U}$, there exists $\bar{v} \in \mathcal{A}^q$ such that $\bar{v}(x) = v(x)$ for all x in a neighborhood of $\overline{U}$. Since $Rv = 0$ on a neighborhood of $\overline{U}$, we obtain that $R\bar{v}$ is zero in a neighborhood of $\overline{U}$, that is, $R\bar{v} \in \mathcal{A}_0^g = \mathcal{C}_0^\infty(\Omega, \mathbb{K})^g$, where

$$\Omega = \{x \in \mathbb{R}^n \mid \|x\| < r\} = \mathbb{R}^n \setminus \overline{U}.$$

We need to construct w with $Rw = 0$ and $w(x) = v(x)$ for all x in a neighborhood of $\overline{U}$. The theorem above implies that the inhomogeneous equation $R\phi = R\bar{v}$ possesses a solution $\phi \in \mathcal{A}_0^q$ (because the right hand side is annihilated by L due to $LR = 0$, and thus $R\bar{v} \in \ker_{\mathcal{A}_0}(L) = \mathrm{im}_{\mathcal{A}_0}(R)$). Thus we are finished by putting $w := \bar{v} - \phi$. By construction, this w satisfies $Rw = 0$ and, since ϕ vanishes on a neighborhood of $\overline{U}$, w coincides with $\bar{v}$, and thus with v, on a neighborhood of $\overline{U}$. This shows the existence of an extension w of v. Its uniqueness follows from the autonomy of $\mathcal{B}$: If w_1, w_2 were two different extensions of v, then their difference would be a non-zero compact support element of $\mathcal{B}$. Lemma 5.1 shows that this is impossible.

Examples:

- The system given by $\mathrm{grad}(w) = 0$ is over-determined for all $n \geq 2$.
- The Cauchy-Riemann equations for functions of one complex variable (corresponding to $n = 2$ real variables) have the kernel representation

$$R = \begin{bmatrix} \partial_1 & -\partial_2 \\ \partial_2 & \partial_1 \end{bmatrix}.$$

We have $J_2(R) = \langle \partial_1^2 + \partial_2^2 \rangle$ which has dimension one. Thus the resulting system is autonomous, but not over-determined. Indeed, the function $f(z) = \frac{1}{z}$ is analytic on any $\{z \in \mathbb{C} \mid |z| > \rho\}$, where $\rho > 0$, and hence its real and imaginary parts satisfy the Cauchy-Riemann equations. If f were extendable to an analytic function on all of $\mathbb{C}$, this would be a contradiction to the uniqueness of analytic continuation.

- The Cauchy-Riemann equation for functions of two complex (corresponding to $n = 4$ real) variables have the kernel representation

$$R = \begin{bmatrix} \partial_1 & -\partial_2 \\ \partial_2 & \partial_1 \\ \partial_3 & -\partial_4 \\ \partial_4 & \partial_3 \end{bmatrix}.$$

We have $J_2(R) = \langle \partial_1^2 + \partial_2^2, \partial_1\partial_4 - \partial_2\partial_3, \partial_1\partial_3 + \partial_2\partial_4, \partial_3^2 + \partial_4^2 \rangle$ which has dimension two. Thus the system is over-determined. $\diamondsuit$

Remark: Similarly as with autonomy, one can introduce controllability degrees [21, 22], but this is mathematically more involved. The lowest controllability degree corresponds to controllability itself, and higher controllability degrees will give various stronger versions of the controllability concept. In the next section, we study systems whose controllability degree is as large as possible, that is, a class of systems with the strongest possible controllability properties.

5.4 Free systems

Controllability of $\mathcal{B}$, that is, the existence of an image representation, amounts to $\mathcal{M}$ being torsion-free. A strong form of controllability is obtained when $\mathcal{M}$ is even free (we will see below that this is equivalent to the existence of an observable image representation). This property is called "strong controllability" of $\mathcal{B}$ by some authors. However, since the term "strong controllability" is also used with a different meaning in the literature, it is preferable to speak of "free systems" (corresponding to the fact that the system module is free).

We say that $\mathcal{B}$ has an **observable image representation** if there exists L such that

$$\mathcal{B} = \{w \in \mathcal{A}^q \mid \exists! \ell \in \mathcal{A}^l : w = L\ell\}$$

that is, the latent variable ℓ is uniquely determined by the manifest variable w. In other words, ℓ is observable from w in the associated full system

$$\mathcal{B}_f = \{[\ell^T, w^T]^T \in \mathcal{A}^{l+q} \mid L\ell = w\}.$$

This means that L must be left invertible. Thus we can conclude: $\mathcal{B}$ has an observable image representation if and only if its kernel representation R is a left syzygy matrix of a left invertible matrix.

Lemma 5.11 *The following are equivalent:*

1. *$\mathcal{B}$ possesses an observable image representation.*
2. *$\mathcal{M}$ is free, that is, $\mathcal{M} \cong \mathcal{D}^{1\times l}$ for some $l \in \mathbb{N}$. Equivalently, $\mathcal{B} \cong \mathcal{A}^l$.*

Proof: If R is a left syzygy matrix of a left invertible matrix L, there is an exact sequence

$$\mathcal{D}^{1\times g} \xrightarrow{\cdot R} \mathcal{D}^{1\times q} \xrightarrow{\cdot L} \mathcal{D}^{1\times l} \longrightarrow 0.$$

On the other hand, there is the exact sequence

$$\mathcal{D}^{1\times g} \xrightarrow{\cdot R} \mathcal{D}^{1\times q} \longrightarrow \mathcal{M} \longrightarrow 0.$$

From this, one can construct an isomorphism between $\mathcal{M}$ and $\mathcal{D}^{1\times l}$ as follows: Define $\phi : \mathcal{M} \to \mathcal{D}^{1\times l}$ by $\phi([x]) := xL$, where $x \in \mathcal{D}^{1\times q}$ and $[x]$ is its residue class in $\mathcal{M}$. This is well-defined, because $x = yR$ implies $xL = yRL = 0$. It is injective, because conversely $xL = 0$ implies that $x = yR$ for some y. Finally, the surjectivity of ϕ follows from the surjectivity of $\cdot L$.

Conversely, if $\mathcal{M}$ is free, one can replace $\mathcal{M}$ by some $\mathcal{D}^{1\times l}$ without losing exactness in the sequence above. The resulting map from $\mathcal{D}^{1\times q}$ to $\mathcal{D}^{1\times l}$ can be identified with $\cdot L$ for some $L \in \mathcal{D}^{q\times l}$. Since $\cdot L$ is surjective, the matrix L is left invertible. Thus R is a left syzygy matrix of a left invertible matrix. □

Remark: The number l that appears in the second condition coincides with the input-dimension of $\mathcal{B}$. To see this, note that if

$$\mathcal{D}^{1\times g} \xrightarrow{\cdot R} \mathcal{D}^{1\times q} \xrightarrow{\cdot L} \mathcal{D}^{1\times l}$$

is exact, then $\operatorname{rank}(R) + \operatorname{rank}(L) = q$. Similarly, if L is left invertible (that is, if $\cdot L$ is surjective), we must have $l = \operatorname{rank}(L)$. Combining these equations, we obtain $l = \operatorname{rank}(L) = q - \operatorname{rank}(R) = m$, which is the input-dimension of $\mathcal{B}$.

In Chapter 4, we have seen that controllability is also equivalent to $\mathcal{B}$ admitting a right invertible kernel representation. This equivalence does not hold in general, as can be seen from the system

$$\mathcal{B} = \{w \in \mathcal{A}^3 \mid \operatorname{curl}(w) = 0\}$$

discussed above: This system is controllable, but it cannot be represented by a right invertible matrix (or any matrix of full row rank). Still, the existence of right invertible kernel representations is an interesting property also for multidimensional systems.

Theorem 5.12 (Quillen-Suslin) *Let $R \in \mathcal{D}^{g\times q}$. The following are equivalent:*

1. *R is right invertible.*
2. *R can be embedded into a unimodular matrix, that is, there exists a $\mathcal{D}$-matrix N such that*
$$\begin{bmatrix} R \\ N \end{bmatrix} \in \mathcal{D}^{q\times q}$$
is unimodular.

Remark: This theorem has quite a remarkable history [11]: In 1955, J.-P. Serre raised the question whether projective modules over the polynomial ring $\mathcal{D}$ were free. (A module is projective if it is a direct summand of a free module.) Some years later, Serre himself was able to reduce the problem to the statement of the theorem above, but he did not succeed in proving it. Thus, the problem became known as Serre's conjecture. In 1976, it was solved by D. Quillen and A. Suslin, independently of each other, thus giving a positive answer to Serre's original question.

Let R be a right invertible matrix, and let N be a matrix according to the Quillen-Suslin theorem. Set

$$\begin{bmatrix} R \\ N \end{bmatrix}^{-1} = \begin{bmatrix} X & L \end{bmatrix}.$$

Then $RX = I$ and $NL = I$, showing that L is left invertible. Moreover, $RL = 0$ and $XR + LN = I$, implying that $\ker(\cdot L) = \mathrm{im}(\cdot R)$. This shows that any right invertible matrix is a left syzygy matrix (and thus, any system represented by a right invertible matrix will be controllable), and moreover, it is a left syzygy matrix of a left invertible matrix.

Conversely, the transposed version of the Quillen-Suslin theorem (L is left invertible if and only if it can be embedded into a unimodular matrix $[X, L]$), shows that any left invertible matrix possesses a left syzygy matrix that is right invertible. These considerations prove the following extension of the lemma above.

Theorem 5.13 *The following are equivalent:*

1. *$\mathcal{B}$ admits a right invertible kernel representation.*
2. *$\mathcal{B}$ possesses an observable image representation.*
3. *$\mathcal{M}$ is free, that is, $\mathcal{M} \cong \mathcal{D}^{1\times l}$ for some $l \in \mathbb{N}$. Equivalently, $\mathcal{B} \cong \mathcal{A}^l$.*

Control of free systems

Suppose that $\mathcal{B}$ is a free system, and let L, N be as above. Let $w \in \mathcal{B}$. Then

$$w = L\ell \quad \Leftrightarrow \quad \ell = Nw.$$

This can be used in order to compute connecting trajectories: Suppose that $w_1, w_2 \in \mathcal{B}$ and U_1, U_2 are given. Compute $\ell_i = Nw_i$. Find a smooth function ℓ that coincides with ℓ_1 on U_1, and with ℓ_2 on U_2. Then $w = L\ell$ is a connecting trajectory, i.e., it coincides with w_1 on U_1 and with w_2 on U_2. This procedure is known as "flatness-based control", and ℓ is called a "flat output" of the system.

Free systems are also very convenient for **controller design**. Let $\mathcal{B}$ be a given system, and let $\mathcal{B}_d \subset \mathcal{B}$ be a subset containing certain desirable functions. The task is to design a controller $\mathcal{C}$ such that

$$\mathcal{B} \cap \mathcal{C} = \mathcal{B}_d \quad \text{and} \quad \mathcal{B} + \mathcal{C} = \mathcal{A}^q.$$

The first requirement says that if the system laws $Rw = 0$ are additionally constrained by the controller laws $Cw = 0$, then the controlled system, which is represented by $[R^T, C^T]^T$ will only have desirable solutions. According to the following lemma, the second statement is equivalent to $\text{rank}(R) + \text{rank}(C) = \text{rank}[R^T, C^T]^T$ which means that the controller laws should be independent of the system laws (otherwise $\mathcal{C} = \mathcal{B}_d$ would always be a trivial solution).

Lemma 5.14 *Let $\mathcal{B}_i = \{w \in \mathcal{A}^q \mid R_i w = 0\}$ for some $R_i \in \mathcal{D}^{g_i \times q}$, where $i = 1, 2$. The following are equivalent:*

1. $\mathcal{B}_1 + \mathcal{B}_2 = \mathcal{A}^q$.
2. $\text{rank}(R_1) + \text{rank}(R_2) = \text{rank}[R_1^T, R_2^T]^T$.

Proof: The input-dimension (idim) of $\mathcal{B}_i$ equals the dimension of $\ker_{\mathcal{K}}(R_i)$, where $\mathcal{K}$ is the quotient field of $\mathcal{D}$, that is, the field of rational functions. Thus

$$\text{idim}(\mathcal{B}_i) = q - \text{rank}(R_i).$$

If $\mathcal{B}_1 + \mathcal{B}_2 = \mathcal{A}^q$, then we have

$$\begin{aligned} q &= \text{idim}(\mathcal{A}^q) = \text{idim}(\mathcal{B}_1 + \mathcal{B}_2) = \text{idim}(\mathcal{B}_1) + \text{idim}(\mathcal{B}_2) - \text{idim}(\mathcal{B}_1 \cap \mathcal{B}_2) \\ &= (q - \text{rank}(R_1)) + (q - \text{rank}(R_2)) - (q - \text{rank}[R_1^T, R_2^T]^T). \end{aligned}$$

This yields the desired result. Conversely, assume that assertion 2 is true. We need to show that $\mathcal{B}_1 + \mathcal{B}_2 = \mathcal{A}^q$. By the fundamental principle, this is true if in any left syzygy matrix $[X, Y, Z]$ of

$$R := \begin{bmatrix} R_1 & 0 \\ 0 & R_2 \\ I & I \end{bmatrix}$$

the matrix Z must be zero. However, if $[X, Y, Z]$ is a left syzygy matrix of R, then $XR_1 = YR_2 = -Z$. This means that the rows of Z belong to $\mathrm{im}(\cdot R_1) \cap \mathrm{im}(\cdot R_2)$. However, this module is zero, because

$$\begin{aligned} \mathrm{rank}[R_1^T, R_2^T]^T &= \dim \mathrm{im}_{\mathcal{K}} \cdot [R_1^T, R_2^T]^T = \dim(\mathrm{im}_{\mathcal{K}}(\cdot R_1) + \mathrm{im}_{\mathcal{K}}(\cdot R_2)) \\ &= \dim \mathrm{im}_{\mathcal{K}}(\cdot R_1) + \dim \mathrm{im}_{\mathcal{K}}(\cdot R_2) - \dim(\mathrm{im}_{\mathcal{K}}(\cdot R_1) \cap \mathrm{im}_{\mathcal{K}}(\cdot R_2)) \\ &= \mathrm{rank}(R_1) + \mathrm{rank}(R_2) - \dim(\mathrm{im}_{\mathcal{K}}(\cdot R_1) \cap \mathrm{im}_{\mathcal{K}}(\cdot R_2)) \end{aligned}$$

yields $\dim(\mathrm{im}_{\mathcal{K}}(\cdot R_1) \cap \mathrm{im}_{\mathcal{K}}(\cdot R_2)) = 0$, which implies $\mathrm{im}_{\mathcal{K}}(\cdot R_1) \cap \mathrm{im}_{\mathcal{K}}(\cdot R_2) = 0$, and thus $\mathrm{im}(\cdot R_1) \cap \mathrm{im}(\cdot R_2) = 0$, since $\mathcal{D} \subset \mathcal{K}$. □

Remark: Using the language of Chapter 2, we have $\mathcal{B}_1 + \mathcal{B}_2 = \mathcal{A}^q$ if and only if

$$\mathfrak{M}(\mathcal{B}_1) \cap \mathfrak{M}(\mathcal{B}_2) = \mathfrak{M}(\mathcal{B}_1 + \mathcal{B}_2) = \mathfrak{M}(\mathcal{A}^q) = 0.$$

However, $\mathfrak{M}(\mathcal{B}_i) = \mathrm{im}(\cdot R_i)$, showing that $\mathcal{B}_1 + \mathcal{B}_2 = \mathcal{A}^q$ is equivalent to

$$\mathrm{im}(\cdot R_1) \cap \mathrm{im}(\cdot R_2) = 0.$$

Then any equation of the form $X_1 R_1 + X_2 R_2 = 0$ implies that the summands are individually zero, that is, $X_i R_i = 0$.

Theorem 5.15 *$\mathcal{B}$ is a free system if and only if there exists $\mathcal{B}_1$ such that*

$$\mathcal{B} \oplus \mathcal{B}_1 = \mathcal{A}^q.$$

Proof: If $\mathcal{B}$ is free, it has a right invertible image representation. Let N be a matrix according to the Quillen-Suslin theorem, then $\mathcal{B}_1 := \{w \in \mathcal{A}^q \mid Nw = 0\}$ has the desired property.

Conversely, if $\mathcal{B} \oplus \mathcal{B}_1 = \mathcal{A}^q$ for some $\mathcal{B}_1 = \{w \in \mathcal{A}^q \mid Nw = 0\}$, then the matrix

$$\begin{bmatrix} R \\ N \end{bmatrix}$$

has a left inverse, say $[X, L]$ (this follows from $\mathcal{B} \cap \mathcal{B}_1 = 0$), and the rank of $[R^T, N^T]^T$ equals $\mathrm{rank}(R) + \mathrm{rank}(N)$ (this follows from $\mathcal{B} + \mathcal{B}_1 = \mathcal{A}^q$). The equation $XR + LN = I$ yields $(RX - I)R + RLN = 0$, and hence, by the previous remark, we must have $RXR = R$. Then we have, for the system module $\mathcal{M} = \mathcal{D}^{1\times q}/\mathcal{D}^{1\times g}R$, an isomorphism

$$\mathcal{D}^{1\times q} \cong \mathcal{M} \oplus \mathcal{D}^{1\times g}R, \quad x \mapsto ([x], xXR).$$

The surjectivity of this map follows from

$$\mathcal{D}^{1\times g}R = \mathcal{D}^{1\times g}RXR \subseteq \mathcal{D}^{1\times q}XR \subseteq \mathcal{D}^{1\times g}R$$

which implies that these modules are actually equal. For injectivity, suppose that $[x] = 0$ and $xXR = 0$. Then $x = yR$ for some y, and $0 = yRXR = yR$, which yields $x = 0$. This isomorphism shows that $\mathcal{M}$ is a direct summand of a free $\mathcal{D}$-module, that is, $\mathcal{M}$ is projective. As remarked above, it is a consequence of the Quillen-Suslin theorem that projective $\mathcal{D}$-modules are free. □

Remark: The "only if" direction could also be proved without using the Quillen-Suslin theorem. Indeed, if $\mathcal{M}$ is free, then it is also projective. This is equivalent to the existence of X with $RXR = R$ (similarly as in the proof of the "if" direction). Then

$$\ker_{\mathcal{A}}(R) \oplus \operatorname{im}_{\mathcal{A}}(XR) = \mathcal{A}^q$$

and thus we may put $\mathcal{B}_1 := \operatorname{im}_{\mathcal{A}}(XR)$.

Using the complementary system $\mathcal{B}_1$, the controller design problem for a free system $\mathcal{B}$ can easily be solved by putting

$$\mathcal{C} = \mathcal{B}_1 + \mathcal{B}_d.$$

Then

$$\mathcal{B} + \mathcal{C} = \mathcal{B} + \mathcal{B}_1 + \mathcal{B}_d = \mathcal{A}^q$$

and

$$\mathcal{B} \cap \mathcal{C} = \mathcal{B} \cap (\mathcal{B}_1 + \mathcal{B}_d) = (\mathcal{B} \cap \mathcal{B}_1) + \mathcal{B}_d = \mathcal{B}_d$$

where we have used the modular law

$$\mathcal{B}_d \subseteq \mathcal{B} \quad \Rightarrow \quad \mathcal{B} \cap (\mathcal{B}_1 + \mathcal{B}_d) = (\mathcal{B} \cap \mathcal{B}_1) + \mathcal{B}_d.$$

Appendix A

Background material

A.1 Kalman controllability criterion

In this section, we prove Theorem 1.2.

Let $A \in \mathbb{R}^{n\times n}$ and $B \in \mathbb{R}^{n\times m}$. Let $\mathfrak{U}$ be such that

$$\mathcal{C}^0(\mathbb{R},\mathbb{R})^m \supseteq \mathfrak{U} \supseteq \mathcal{O}(\mathbb{R},\mathbb{R})^m,$$

where $\mathcal{C}^0$ denotes the continuous functions and $\mathcal{O}$ denotes the analytic functions.

Then $\dot{x} = Ax + Bu$, $x(0) = x_0$ has the unique solution

$$x(t) = e^{At}x_0 + \int_0^t e^{A(t-\tau)}Bu(\tau)d\tau.$$

Lemma A.1.1 (Identity theorem for analytic functions) *Let $f:\mathbb{R}\to\mathbb{R}^{1\times m}$ be an analytic function. Then*

$$f \equiv 0 \quad \Leftrightarrow \quad f^{(i)}(0) = 0 \text{ for all } i \in \mathbb{N}.$$

Lemma A.1.2 *All powers A^i of A, where $i \in \mathbb{N}$, are $\mathbb{R}$-linear combinations of $A^0 = I, A^1 = A, \ldots, A^{n-1}$.*

Proof: This follows from the Hamilton-Cayley theorem: $\chi_A(A) = 0$, where χ_A is the characteristic polynomial of A, a polynomial of degree n. □

Lemma A.1.3 *Let $t > 0$ and*

$$K := [B, AB, \ldots, A^{n-1}B] \quad \text{and} \quad W_t := \int_0^t e^{A\tau}BB^Te^{A^T\tau}d\tau.$$

Then $\operatorname{rank}(K) = \operatorname{rank}(W_t)$.

In particular, the following are equivalent:

1. $\operatorname{rank}(K) = n$.
2. W_t *is non-singular.*

Proof: Let $t > 0$ and $\xi \in \mathbb{R}^{1\times n}$. Note that W_t is symmetric and positive semi-definite. Hence we have $\xi W_t = 0 \Leftrightarrow \xi W_t \xi^T = 0 \Leftrightarrow$

$$\int_0^t \|\xi e^{A\tau} B\|^2 d\tau = 0$$

$\Leftrightarrow f \equiv 0$, where $f(t) = \xi e^{At} B \Leftrightarrow f^{(i)}(0) = \xi A^i B = 0$ for all $i \in \mathbb{N} \Leftrightarrow \xi K = 0$. Thus $\ker(\cdot W_t) = \ker(\cdot K)$, and thus $\dim(\ker(\cdot W_t)) = n - \operatorname{rank}(W_t) = \dim(\ker(\cdot K)) = n - \operatorname{rank}(K)$. □

Theorem A.1.4 *The following are equivalent:*

1. $\exists t_1 > 0\ \forall x_0, x_1 \in \mathbb{R}^n$: x_0 *can be controlled to* x_1 *in time* t_1, *that is,* $\exists u \in \mathfrak{U}$ *such that the solution to*

   $$\dot{x} = Ax + Bu, \quad x(0) = x_0$$

   satisfies $x(t_1) = x_1$.
2. $\operatorname{rank}(K) = n$, *where* $K = [B, AB, \ldots, A^{n-1}B]$.

Proof: $1 \Rightarrow 2$: Assume that $\operatorname{rank}(K) < n$. Then there exists $0 \neq \xi \in \mathbb{R}^{1\times n}$ such that $\xi K = 0$. This means that $\xi A^i B = 0$ for $0 \leq i \leq n-1$. According to the lemma, this implies

$$\xi A^i B = 0 \quad \text{for all } i \in \mathbb{N}.$$

Consider the analytic function $f(t) = \xi e^{At} B$. We have $f^{(i)}(0) = 0$ for all $i \in \mathbb{N}$ and hence $f \equiv 0$.

If $x_0 = 0$ can be controlled to x_1 in time t_1, then

$$x_1 = \int_0^{t_1} e^{A(t_1-\tau)} B u(\tau) d\tau$$

and then $\xi x_1 = 0$. Since this does not hold for all x_1, assertion 1 is not true.

$2 \Rightarrow 1$: Let $\operatorname{rank}(K) = n$. Let x_0, x_1 be given. Let $t_1 > 0$ be arbitrary. Set

$$u(t) = B^T e^{A^T(t_1-t)} W_{t_1}^{-1} (x_1 - e^{At_1} x_0).$$

This is an analytic function and hence it belongs to $\mathfrak{U}$. The solution of $\dot{x} = Ax + Bu$ satisfies

$$\begin{aligned} x(t_1) &= e^{At_1}x_0 + \int_0^{t_1} e^{A(t_1-\tau)}BB^T e^{A^T(t_1-\tau)}d\tau W_{t_1}^{-1}(x_1 - e^{At_1}x_0) \\ &= e^{At_1}x_0 + W_{t_1}W_{t_1}^{-1}(x_1 - e^{At_1}x_0) \\ &= x_1 \end{aligned}$$

and hence we have the desired result. □

In fact, the proof shows more than originally claimed: $\text{rank}(K) = n$ is equivalent to the following stronger version of assertion 1:

$\forall t_1 > 0$ and $\forall x_0, x_1$ there exists $u \in \mathfrak{U}$ such that the solution to $\dot{x} = Ax + Bu$, $x(0) = x_0$ satisfies $x(t_1) = x_1$.

In other words, if x_0 can be controlled to x_1 at all, then this can be done in an arbitrarily small time $t_1 > 0$. This feature, which has no analogue in discrete time, is counter-intuitive at first sight: In a "real world" system, it certainly takes "some time" to change from one state to another. The reason is that we admit arbitrarily large input values here, i.e., we make the optimistic assumption that we can put as much "energy" as we like into the system. In a real world system, there are constraints which limit the size of the admissible inputs, and this has the consequence that the transition from one state to another cannot be done arbitrarily fast in practice.

Theorem A.1.5 *Let $\dot{x} = Ax + Bu$ be controllable, and let u be an input function that controls $\dot{x} = Ax + Bu$ from $x(0) = 0$ to $x(t_1) = x_1$, where $t_1 > 0$. Then*

$$E(u) := \int_0^{t_1} \|u(t)\|^2 dt \geq E_{\min}(t_1, x_1) := x_1^T W_{t_1}^{-1} x_1$$

and equality is achieved for the input function

$$u(t) = B^T e^{A^T(t_1-t)} W_{t_1}^{-1} x_1. \tag{A.1}$$

In other words, the input function from (A.1) is optimal in the sense that its **energy** $E(u)$ is minimal among the energies of all u that steer the system from $x(0) = 0$ to $x(t_1) = x_1$. This minimal energy is given by $E_{\min}(t_1, x_1) = x_1^T W_{t_1}^{-1} x_1$. This shows that the smaller t_1 is, the more energy is needed to do the transition from 0 to x_1 in time t_1. More precisely, if $0 < s < t$, then $W_t > W_s$ (this notation means that $W_t - W_s$ is positive definite), which implies, using some linear algebra, $W_s^{-1} > W_t^{-1}$, and hence

$$E_{\min}(s, x) = x^T W_s^{-1} x > x^T W_t^{-1} x = E_{\min}(t, x) \quad \text{for all } x \neq 0.$$

This explains the trade-off between the speed of control on the one hand and the energy consumption of control on the other.

Proof: Define

$$V(t,x) := x^T W_t^{-1} x.$$

Let us look at the change of $V(t,x(t))$ along a trajectory x of our system. We have

$$\begin{aligned}\tfrac{d}{dt}V(t,x(t)) &= \tfrac{d}{dt}x(t)^T W_t^{-1} x(t) \\ &= \dot{x}(t)^T W_t^{-1} x(t) + x(t)^T (\tfrac{d}{dt}W_t^{-1}) x(t) + x(t)^T W_t^{-1} \dot{x}(t).\end{aligned}$$

Note that for any matrix-valued function W,

$$\tfrac{d}{dt}W_t^{-1} = -W_t^{-1}\dot{W}_t W_t^{-1}.$$

Moreover, we plug in $\dot{x} = Ax + Bu$ and we obtain (omitting the argument t in $x(t)$ and $u(t)$ for simplicity)

$$\begin{aligned}\tfrac{d}{dt}V(t,x) &= (Ax+Bu)^T W_t^{-1} x - x^T W_t^{-1}\dot{W}_t W_t^{-1} x + x^T W_t^{-1}(Ax+Bu) \\ &= x^T (A^T W_t^{-1} + W_t^{-1}A - W_t^{-1}\dot{W}_t W_t^{-1}) x + 2u^T B^T W_t^{-1} x.\end{aligned}$$

Consider the matrix

$$X_t := A^T W_t^{-1} + W_t^{-1} A - W_t^{-1}\dot{W}_t W_t^{-1}.$$

We have

$$\begin{aligned}W_t X_t W_t &= W_t A^T + A W_t - \dot{W}_t \\ &= \int_0^t (e^{A\tau}BB^T e^{A^T\tau}A^T + Ae^{A\tau}BB^T e^{A^T\tau})d\tau - \dot{W}_t \\ &= e^{A\tau}BB^T e^{A^T\tau}\Big|_{\tau=0}^{\tau=t} - \dot{W}_t \\ &= e^{At}BB^T e^{A^T t} - BB^T - \dot{W}_t.\end{aligned} \tag{A.2}$$

Noting that by the definition of W,

$$\dot{W}_t = e^{At}BB^T e^{A^T t}$$

we obtain

$$W_t X_t W_t = -BB^T \tag{A.3}$$

and hence $X_t = -W_t^{-1}BB^T W_t^{-1}$. We use this to rewrite our expression for $\frac{d}{dt}V(t,x)$ and obtain

$$\begin{aligned}\tfrac{d}{dt}V(t,x) &= -x^T W_t^{-1}BB^T W_t^{-1} x + 2u^T B^T W_t^{-1} x \\ &= -\|B^T W_t^{-1} x\|^2 + 2\langle u, B^T W_t^{-1} x\rangle \\ &= \|u\|^2 - \|u - B^T W_t^{-1} x\|^2.\end{aligned}$$

Let's integrate this from 0 to t_1, exploiting that $x(0) = 0$ and $x(t_1) = x_1$. Then

$$V(t_1, x_1) - V(0, 0) = \int_0^{t_1} \|u(t)\|^2 dt - \int_0^{t_1} \|u(t) - B^T W_t^{-1} x(t)\|^2 dt$$

or

$$x_1^T W_{t_1}^{-1} x_1 = E(u) - \int_0^{t_1} \|u(t) - B^T W_t^{-1} x(t)\|^2 dt \le E(u). \tag{A.4}$$

This shows that

$$E(u) \ge E_{\min}(t_1, x_1) := x_1^T W_{t_1}^{-1} x_1.$$

Equality is achieved if and only if the integral in (A.4) vanishes, i.e., if

$$u(t) = B^T W_t^{-1} x(t). \tag{A.5}$$

Plugging that into $\dot{x} = Ax + Bu$, we get

$$\dot{x}(t) = (A + BB^T W_t^{-1}) x(t).$$

Since we know that $x(t_1) = x_1$, the solution of this linear time-varying ODE is uniquely determined for all $t > 0$. This solution is given by

$$\xi(t) = W_t e^{A^T(t_1 - t)} W_{t_1}^{-1} x_1.$$

This can easily be checked: We have $\xi(t_1) = x_1$ and

$$\dot{\xi}(t) = (\dot{W}_t - W_t A^T) e^{A^T(t_1 - t)} W_{t_1}^{-1} x_1.$$

Combining (A.2) with (A.3), we see that

$$\dot{W}_t = W_t A^T + A W_t + BB^T.$$

This implies

$$\begin{aligned} \dot{\xi}(t) &= (AW_t + BB^T) e^{A^T(t_1 - t)} W_{t_1}^{-1} x_1 \\ &= (A + BB^T W_t^{-1}) W_t e^{A^T(t_1 - t)} W_{t_1}^{-1} x_1 \\ &= (A + BB^T W_t^{-1}) \xi(t) \end{aligned}$$

as desired. Thus $x = \xi$ is the optimal state trajectory. Then, according to (A.5),

$$u(t) = B^T W_t^{-1} \xi(t) = B^T e^{A^T(t_1 - t)} W_{t_1}^{-1} x_1$$

is the minimum energy control function that steers the system from 0 to x_1 in time t_1. □

A.2 Galois correspondences

A **partial order** on a set X is a relation $\leq$ with the properties:

- $x \leq x$ (reflexivity);
- $x_1 \leq x_2$ and $x_2 \leq x_3 \Rightarrow x_1 \leq x_3$ (transitivity);
- $x_1 \leq x_2$ and $x_2 \leq x_1 \Rightarrow x_1 = x_2$ (antisymmetry).

The term "partial" refers to the fact that there may be elements $x_1, x_2 \in X$ such that neither $x_1 \leq x_2$ nor $x_2 \leq x_1$ is true.

Let X and Y be partially ordered sets and let $f : X \to Y$ and $g : Y \to X$ be two maps. The mappings f and g are called a **Galois correspondence** if

1. f and g are order-reversing, that is,
$$x_1 \leq x_2 \Rightarrow f(x_1) \geq f(x_2) \quad \text{and} \quad y_1 \leq y_2 \Rightarrow g(y_1) \geq g(y_2);$$
2. $x \leq g(f(x))$ for all $x \in X$ and $y \leq f(g(y))$ for all $y \in Y$.

Lemma A.2.1 *We have $gfg \equiv g$ and $fgf \equiv f$. Thus there are order-reversing bijections*

$$\begin{array}{rcl} \mathrm{im}(g) & \leftrightarrow & \mathrm{im}(f) \\ x & \to & f(x) \\ g(y) & \leftarrow & y \end{array}$$

that are inverse to each other.

Proof: Due to property 2, we have $f(g(y)) \geq y$ and $g(f(g(y))) \geq g(y)$. Applying the order-reversing mapping g to the first inequality, we obtain $g(f(g(y)) \leq g(y)$. Combining these inequalities, we obtain $g(f(g(y))) = g(y)$. Since this holds for all $y \in Y$, we have $gfg \equiv g$. The second statement is analogous.

We show that the map $f_1 : \mathrm{im}(g) \to \mathrm{im}(f),\ x \mapsto f(x)$ is a bijection. For injectivity, let $f(x_1) = f(x_2)$ for some $x_1, x_2 \in \mathrm{im}(g)$, that is, $x_i = g(y_i)$ for some $y_1, y_2 \in Y$. Thus
$$f(g(y_1)) = f(g(y_2)).$$
Applying g and using $gfg \equiv g$, we obtain
$$x_1 = g(y_1) = g(f(g(y_1))) = g(f(g(y_2))) = g(y_2) = x_2.$$

Secondly, we show that f_1 is surjective: Let $y \in \mathrm{im}(f)$ be given, that is, $y = f(x)$ for some $x \in X$. Using $fgf \equiv f$, we have $y = f(x) = f(g(f(x)))$ and thus, with $\tilde{x} := g(f(x)) \in \mathrm{im}(g)$, we have $y = f(\tilde{x})$.

Similarly, one shows that $g_1 : \mathrm{im}(f) \to \mathrm{im}(g)$, $y \mapsto g(y)$ is a bijection.

It remains to be shown that f_1 and g_1 are inverse to each other: However, we have, for $x = g(y)$: $g(f(x)) = g(f(g(y))) = g(y) = x$ and similarly, the other way round. □

Define $\overline{x} := gf(x)$ for all $x \in X$. Then

- $x \leq \overline{x} = gf(x)$;
- $\overline{\overline{x}} = gfgf(x) = gf(x) = \overline{x}$;
- if $x_1 \leq x_2$, then $f(x_1) \geq f(x_2)$, and thus $\overline{x_1} = gf(x_1) \leq gf(x_2) = \overline{x_2}$.

This shows that gf is a **closure operation**. We say that x is closed if $\overline{x} = x$. This is true if and only if $x \in \mathrm{im}(g)$. Analogous statements can be shown if we set $\overline{y} := fg(y)$ for all $y \in Y$.

Note that if only the left hand side X of the Galois correspondence is restricted to $\mathrm{im}(g) \subseteq X$, we have order-reversing maps

$$\begin{array}{rcl} \mathrm{im}(g) & \to & Y \\ x & \to & f(x) \\ g(y) & \leftarrow & y \end{array}$$

with

$$\overline{x} = g(f(x)) = x \quad \text{for all } x \in \mathrm{im}(g)$$

and

$$\overline{y} = f(g(y)) \geq y \quad \text{for all } y \in Y.$$

This was used in Chapter 2 for $X = \mathbf{A}$, $Y = \mathbf{M}$, $f \equiv \mathfrak{M}$, $g \equiv \mathfrak{B}$. Then $\mathrm{im}(g) = \mathbf{B}$. The partial order is given by inclusion.

Here are two other prominent examples of Galois correspondences, where the partial order is also given by inclusion:

- Let X be the set of all subsets of $\mathbb{C}^n$ and let Y be the set of all ideals in $\mathbb{K}[s_1, \ldots, s_n]$. Let $f \equiv \mathfrak{I}$ be defined by

$$\mathfrak{I}(V) = \{f \in \mathbb{K}[s_1, \ldots, s_n] \mid f(v) = 0 \text{ for all } v \in V\}$$

and let $g \equiv \mathfrak{V}$ be defined by

$$\mathfrak{V}(\mathcal{I}) = \{v \in \mathbb{C}^n \mid f(v) = 0 \text{ for all } f \in \mathcal{I}\}.$$

Then $\mathfrak{V}\mathfrak{I}(V) \supseteq V$ is called the Zariski closure of V, and V is called an algebraic variety if it is Zariski closed. Thus $\mathrm{im}(\mathfrak{V})$ is the set of all algebraic varieties, and $\mathfrak{I}\mathfrak{V}(\mathcal{I}) = \mathrm{Rad}(\mathcal{I}) := \{f \in \mathbb{K}[s_1, \ldots, s_n] \mid \exists l \in \mathbb{N} : f^l \in \mathcal{I}\}$ by Hilbert's Nullstellensatz. The ideal $\mathrm{Rad}(\mathcal{I}) \supseteq \mathcal{I}$ is the closure of $\mathcal{I}$ with respect to this correspondence.

- Let $X = Y$ be the set of all subspaces of $\mathbb{R}^n$, and let $f = g$ be defined by $f(V) = V^\perp$, the orthogonal complement of V with respect to the standard scalar product $\langle x, y\rangle = x^T y$. In this case the Galois correspondence consists already of order-reversing bijections inverse to each other.

A **lattice** is a partially ordered set X in which any two elements $x_1, x_2 \in X$ possess an infimum $x_1 \wedge x_2 \in X$ and a supremum $x_1 \vee x_2 \in X$, that is

- $x_1 \wedge x_2 \leq x_i$ for $i = 1, 2$; and $x \leq x_i$ for $i = 1, 2$ implies $x \leq x_1 \wedge x_2$;
- $x_1 \vee x_2 \geq x_i$ for $i = 1, 2$; and $x \geq x_i$ for $i = 1, 2$ implies $x \geq x_1 \vee x_2$.

For example, let X be the power set of a given set. This is partially ordered by inclusion, and it becomes a lattice by taking the union as the supremum, and the intersection as the infimum.

Similarly, the set X of all subspaces of a given vector space is partially ordered by inclusion, and we take the sum as the supremum, and the intersection as the infimum.

The set $\mathbf{M}$ of all left $\mathcal{D}$-submodules of $\mathcal{D}^{1\times q}$ becomes a lattice in the same way.

Note that the set $\mathbf{B}$ of all abstract linear systems becomes a lattice if we can show that it is closed under addition.

Let X, Y be two lattices and let $f : X \to Y$ be an order-reversing bijection with order-reversing inverse. Then we call f a lattice anti-isomorphism and we have

$$\begin{aligned} f(x_1 \wedge x_2) &= f(x_1) \vee f(x_2) \\ f(x_1 \vee x_2) &= f(x_1) \wedge f(x_2) \end{aligned}$$

for all $x_1, x_2 \in X$.

A.3 Property O for 1-d time-invariant systems

In this section, we prove Theorem 2.6.

The commutative ring $\mathcal{D} = \mathbb{K}[\frac{d}{dt}]$ is a Euclidean domain, that is, we have a "division with remainder": For all $0 \neq d \in \mathcal{D}$ and all $n \in \mathcal{D}$, there exist $q, r \in \mathcal{D}$ such that $n = qd + r$, where the "remainder" r satisfies either $r = 0$ or $\deg(r) < \deg(d)$. It is known that Euclidean domains are principal ideal domains, that is, every ideal in $\mathcal{D}$ can be generated by one single element. A matrix $U \in \mathbb{K}[s]^{g\times g}$ is called **unimodular** if there exists $U^{-1} \in \mathbb{K}[s]^{g\times g}$. Equivalently, $\det(U) \in \mathbb{K}\setminus\{0\}$.

Lemma A.3.1 (Smith form) *For every $R \in \mathbb{K}[s]^{g\times q}$, there exist unimodular matrices $U \in \mathbb{K}[s]^{g\times g}$ and $V \in \mathbb{K}[s]^{q\times q}$ such that*

$$URV = \begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix}$$

where $D = \operatorname{diag}(d_1, \ldots, d_p)$ for some $0 \neq d_i \in \mathbb{K}[s]$ and $d_1|d_2|\ldots|d_p$. Here, $p = \operatorname{rank}(R)$.

Moreover, since $\mathcal{D}$ is Euclidean, the unimodular transformation matrices U and V can be obtained by performing elementary row and column operations. By an elementary operation, we mean one of the following matrix transformations:

- interchanging two rows (columns) of a matrix;
- adding a multiple of one row (column) to another row (column);
- multiplying a row (column) by a unit, that is, an element of $\mathbb{K} \setminus \{0\}$.

It is easy to see that these operations correspond to multiplication by unimodular matrices from the left and right.

Proof: Without loss of generality, let $R \neq 0$. It is sufficient to show that by elementary operations, R can be brought into the form

$$R' = \begin{bmatrix} a & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & Q & \\ 0 & & & \end{bmatrix} \tag{A.6}$$

where a divides all entries of Q. Then one applies the same procedure to Q, and the result follows inductively.

Case 1: There exists i, j such that R_{ij} divides all entries of R. By a suitable interchange of rows and columns, this element can be brought into the (1,1) position of the matrix. Therefore without loss of generality, R_{11} divides all entries of R. Now perform the following elementary operations: for all $i \neq 1$, put ith row minus R_{i1}/R_{11} times 1st row; for all $j \neq 1$, put jth column minus R_{1j}/R_{11} times 1st column. Then we are finished.

Case 2: There is no i, j such that R_{ij} divides all entries of R. Let

$$\delta(R) := \min\{\deg(R_{ij}) \mid R_{ij} \neq 0\}.$$

Without loss of generality, $\deg(R_{11}) = \delta(R)$. We show that by elementary operations, we can transform R into $R^{(1)}$ with $\delta(R^{(1)}) < \delta(R)$. Then we obtain a strictly decreasing sequence $\delta(R) > \delta(R^{(1)}) > \delta(R^{(2)}) > \ldots \geq 0$. After finitely many steps, we arrive at zero, i.e., we obtain a matrix which has a unit as an entry, and thus we are in Case 1.

Case 2a: R_{11} does not divide all R_{1j}, R_{i1}, say, it does not divide R_{1k}. By the Euclidean algorithm, we can write

$$R_{1k} = R_{11}q + r$$

where $r \neq 0$ and $\deg(r) < \deg(R_{11})$. Perform the elementary operation: kth column minus q times 1st column. Then the new matrix $R^{(1)}$ has r in the $(1, k)$ position and thus $\delta(R^{(1)}) < \delta(R)$ as desired.

Case 2b: R_{11} divides all R_{1j}, R_{i1}. Similarly as in Case 1, we can transform, by elementary operations, R into the form (A.6). If a divides all entries of Q, then we are finished. If there exists i, j such that a does not divide Q_{ij}, then we perform the elementary operation: 1st row plus $(i+1)$st row. (Note that the $(i+1)$st row of R' corresponds to the ith row of Q.) The new matrix has Q_{ij} in the $(1, j+1)$ position and therefore we are in Case 2a. □

Theorem A.3.2 *Let $\mathcal{D} = \mathbb{K}[\frac{d}{dt}]$ and let $\mathcal{A}$ consist of all polynomial-exponential functions. Then $\mathcal{A}$ has property O.*

Proof: We need to show that $M = \mathfrak{M}\mathfrak{B}(M)$ for all $M = \mathcal{D}^{1\times g}R$ for some $R \in \mathcal{D}^{g\times q}$. Due to the Smith form, it suffices to consider the case where $g = q = 1$.

Thus let $R \in \mathcal{D}$. If $R = 0$, then $M = 0$ and $\mathfrak{B}(M) = \mathcal{A}$. The only linear constant-coefficient ordinary differential equation which has all $a \in \mathcal{A}$ as solutions is the trivial equation. Therefore, $\mathfrak{M}\mathfrak{B}(M) = 0 = M$. If R is a non-zero constant, then $M = \mathcal{D}$ and $\mathfrak{B}(M) = 0$ and thus $\mathfrak{M}\mathfrak{B}(M) = \mathcal{D} = M$.

Let us assume that R is not constant, and let $M = \mathcal{D}R$. By the fundamental theorem of algebra, there exists a representation

$$R = c\prod_{i=1}^{k}(\tfrac{d}{dt} - \lambda_i)^{\mu_i} \tag{A.7}$$

where $c \in \mathbb{K}$, k and μ_i are positive integers, and $\lambda_i \in \mathbb{C}$. From the theory of linear constant-coefficient ordinary differential equations, it is known that $\mathcal{B} = \mathfrak{B}(M)$ consists of all functions of the form

$$w(t) = \sum_{i=1}^{k} p_i(t)e^{\lambda_i t}$$

where $p_i \in \mathbb{C}[t]$ is an arbitrary polynomial of degree $\mu_i - 1$. On the other hand, the only elements of $\mathcal{D}$ that annihilate all these w are the multiples of R. Hence $\mathfrak{M}(\mathcal{B}) = \mathfrak{M}\mathfrak{B}(M) = \mathcal{D}R = M$. □

The discrete counterpart given in Theorem 2.7 is proven similarly (using the Smith form and some basic facts about the solutions of linear constant-coefficient difference equations). However, the proof of the multivariate versions, that is, Theorems 2.9 and 2.10, is much harder, because $\mathcal{D} = \mathbb{K}[\partial_1, \ldots, \partial_n]$ is not a principal ideal domain, and therefore there exists no analogue of the Smith form, for $n \geq 2$.

A.4 Left-exactness of the Hom-functor

In this section, we prove Lemma 2.14, which is restated below.

Let $\mathcal{D}$ be a ring, and let $\mathcal{A}$ be a left $\mathcal{D}$-module. For a left $\mathcal{D}$-module $\mathcal{M}$, we set

$$\mathrm{Hom}_{\mathcal{D}}(\mathcal{M}, \mathcal{A}) = \{\phi : \mathcal{M} \to \mathcal{A} \mid \phi \text{ is } \mathcal{D}\text{-linear}\}.$$

If $\mathcal{N}$ is another left $\mathcal{D}$-module, and if $f : \mathcal{M} \to \mathcal{N}$ is a $\mathcal{D}$-linear map, then

$$\mathrm{Hom}_{\mathcal{D}}(f, \mathcal{A}) : \mathrm{Hom}_{\mathcal{D}}(\mathcal{N}, \mathcal{A}) \to \mathrm{Hom}_{\mathcal{D}}(\mathcal{M}, \mathcal{A}), \quad \psi \mapsto \psi \circ f.$$

Lemma A.4.1 *The functor* $\mathrm{Hom}_{\mathcal{D}}(\cdot, \mathcal{A})$ *is left exact, that is, if*

$$\mathcal{M} \stackrel{f}{\longrightarrow} \mathcal{N} \stackrel{g}{\longrightarrow} \mathcal{P} \longrightarrow 0$$

is exact, where $\mathcal{M}, \mathcal{N}, \mathcal{P}$ *are left* $\mathcal{D}$*-modules, and* f, g *are* $\mathcal{D}$*-linear maps, then*

$$\mathrm{Hom}_{\mathcal{D}}(\mathcal{M}, \mathcal{A}) \stackrel{\mathrm{Hom}_{\mathcal{D}}(f,\mathcal{A})}{\longleftarrow} \mathrm{Hom}_{\mathcal{D}}(\mathcal{N}, \mathcal{A}) \stackrel{\mathrm{Hom}_{\mathcal{D}}(g,\mathcal{A})}{\longleftarrow} \mathrm{Hom}_{\mathcal{D}}(\mathcal{P}, \mathcal{A}) \longleftarrow 0$$

is also exact.

Proof: We first show that $\mathrm{Hom}_{\mathcal{D}}(g, \mathcal{A})$ is injective. Suppose that $\mathrm{Hom}_{\mathcal{D}}(g, \mathcal{A})\varphi = \varphi \circ g = 0$ for some $\varphi \in \mathrm{Hom}_{\mathcal{D}}(\mathcal{P}, \mathcal{A})$. This means that $\varphi(g(n)) = 0$ for all $n \in \mathcal{N}$. Since g is surjective, this implies $\varphi(p) = 0$ for all $p \in \mathcal{P}$, and thus $\varphi = 0$.

Secondly, we have that $\mathrm{Hom}_{\mathcal{D}}(f, \mathcal{A}) \circ \mathrm{Hom}_{\mathcal{D}}(g, \mathcal{A}) = \mathrm{Hom}_{\mathcal{D}}(g \circ f, \mathcal{A}) = 0$, since $g \circ f = 0$. Therefore $\ker(\mathrm{Hom}_{\mathcal{D}}(f, \mathcal{A})) \supseteq \mathrm{im}(\mathrm{Hom}_{\mathcal{D}}(g, \mathcal{A}))$.

Finally, we prove that $\ker(\mathrm{Hom}_{\mathcal{D}}(f, \mathcal{A})) \subseteq \mathrm{im}(\mathrm{Hom}_{\mathcal{D}}(g, \mathcal{A}))$. For this, let $\psi \in \mathrm{Hom}_{\mathcal{D}}(\mathcal{N}, \mathcal{A})$ be such that $\psi \circ f = 0$. We need to show that $\psi = \varphi \circ g$ for some $\varphi \in \mathrm{Hom}_{\mathcal{D}}(\mathcal{P}, \mathcal{A})$. Let $p \in \mathcal{P}$ be given. Since g is surjective, there exists $n \in \mathcal{N}$ such that $g(n) = p$. We put $\varphi(p) := \psi(n)$. This is well-defined, because $g(n_1) = g(n_2) = p$ implies $n_1 - n_2 \in \ker(g) = \mathrm{im}(f)$ and hence $\psi(n_1) = \psi(n_2)$. The map φ satisfies $\varphi(g(n)) = \psi(n)$ for all $n \in \mathcal{N}$, and thus $\psi = \varphi \circ g$ as desired. To see that φ is $\mathcal{D}$-linear, let $p_1, p_2 \in \mathcal{P}$ and $d_1, d_2 \in \mathcal{D}$. Note that $g(n_i) = p_i$ for $i = 1, 2$ implies $g(d_1 n_1 + d_2 n_2) = d_1 p_1 + d_2 p_2$ and thus

$$\varphi(d_1 p_1 + d_2 p_2) = \psi(d_1 n_1 + d_2 n_2) = d_1 \psi(n_1) + d_2 \psi(n_2) = d_1 \varphi(p_1) + d_2 \varphi(p_2),$$

where we have used the linearity of g and ψ. □

A.5 Baer's criterion

In this section, we prove the alternative version of Baer's criterion which does not rely on the axiom of choice; see e.g. [12, Ch. 1, §3] for the classical version.

$T = \mathrm{Hom}_{\mathcal{D}}(\cdot, \mathcal{A})$ is an exact functor on the category of left $\mathcal{D}$-modules if, for every exact sequence

$$\mathcal{M} \xrightarrow{f} \mathcal{N} \xrightarrow{g} \mathcal{P}$$

of left $\mathcal{D}$-modules, the sequence

$$T\mathcal{M} \xleftarrow{Tf} T\mathcal{N} \xleftarrow{Tg} T\mathcal{P}$$

is also exact. This is equivalent to saying that $\mathcal{A}$ is injective.

Lemma A.5.1 $T = \mathrm{Hom}_{\mathcal{D}}(\cdot, \mathcal{A})$ *is exact if and only if it turns every exact sequence of the form*

$$0 \to \mathcal{N} \hookrightarrow \mathcal{P}$$

into an exact sequence

$$0 \leftarrow T\mathcal{N} \leftarrow T\mathcal{P}.$$

Proof: The condition is clearly necessary. For sufficiency, let

$$\mathcal{M} \xrightarrow{f} \mathcal{N} \xrightarrow{g} \mathcal{P}$$

be a given exact sequence. Consider

$$\mathcal{M} \xrightarrow{f} \mathcal{N} \xrightarrow{g_1} \operatorname{im}(g) \longrightarrow 0.$$

Using the fact that the Hom-functor is left exact, this yields an exact sequence

$$T\mathcal{M} \leftarrow T\mathcal{N} \leftarrow T\operatorname{im}(g) \leftarrow 0.$$

We need to show that

$$T\mathcal{M} \xleftarrow{Tf} T\mathcal{N} \xleftarrow{Tg} T\mathcal{P}$$

is exact, that is, for $\varphi \in \operatorname{Hom}_{\mathcal{D}}(\mathcal{N}, \mathcal{A})$, we have to prove that

$$\varphi \circ f = 0 \quad \Leftrightarrow \quad \exists \psi \in \operatorname{Hom}_{\mathcal{D}}(\mathcal{P}, \mathcal{A}) : \varphi = \psi \circ g.$$

The implication "$\Leftarrow$" is trivial, because $g \circ f = 0$. For "$\Rightarrow$", note that $\varphi \circ f = 0$ implies that there exists $\theta \in \operatorname{Hom}_{\mathcal{D}}(\operatorname{im}(g), \mathcal{A})$ such that $\varphi = \theta \circ g_1$. However,

$$0 \to \operatorname{im}(g) \hookrightarrow \mathcal{P}$$

is exact, and therefore, using the assumption,

$$0 \leftarrow \operatorname{Hom}_{\mathcal{D}}(\operatorname{im}(g), \mathcal{A}) \leftarrow \operatorname{Hom}_{\mathcal{D}}(\mathcal{P}, \mathcal{A})$$

is also exact, which means that θ can be extended to a map $\psi \in \operatorname{Hom}_{\mathcal{D}}(\mathcal{P}, \mathcal{A})$, that is, $\psi|_{\operatorname{im}(g)} = \theta$. Therefore $\varphi = \theta \circ g_1 = \theta \circ g = \psi \circ g$. □

Now let $\mathcal{D}$ be left Noetherian, and consider T as a functor on the category of finitely generated left $\mathcal{D}$-modules, that is, T is exact if it turns every exact sequence of finitely generated left $\mathcal{D}$-modules into an exact sequence.

Theorem A.5.2 $T = \operatorname{Hom}_{\mathcal{D}}(\cdot, \mathcal{A})$ *is exact if and only if for every sequence*

$$0 \to \mathcal{I} \hookrightarrow \mathcal{D},$$

where $\mathcal{I}$ *is a left ideal in* $\mathcal{D}$*, the sequence*

$$0 \leftarrow \operatorname{Hom}_{\mathcal{D}}(\mathcal{I}, \mathcal{A}) \leftarrow \operatorname{Hom}_{\mathcal{D}}(\mathcal{D}, \mathcal{A})$$

is also exact.

Proof: The condition is clearly necessary. For sufficiency, let

$$0 \to \mathcal{N} \hookrightarrow \mathcal{P}$$

be a given exact sequence. We need to show that $0 \leftarrow T\mathcal{N} \leftarrow T\mathcal{P}$ is exact, that is, for $\varphi \in \mathrm{Hom}_{\mathcal{D}}(\mathcal{N},\mathcal{A})$, we have to prove that there exists $\psi \in \mathrm{Hom}_{\mathcal{D}}(\mathcal{P},\mathcal{A})$ such that $\varphi = \psi|_{\mathcal{N}}$. Let φ be given.

Consider the set of all submodules $\mathcal{N} \subseteq \mathcal{Q} \subseteq \mathcal{P}$ with the property that there exists $\psi \in \mathrm{Hom}_{\mathcal{D}}(\mathcal{Q},\mathcal{A})$ with $\varphi = \psi|_{\mathcal{N}}$. Since $\mathcal{D}$ is left Noetherian, this non-empty family of left submodules of the finitely generated module $\mathcal{P}$ possesses a maximal element, say $\mathcal{Q}_1$. Let $\psi_1 \in \mathrm{Hom}_{\mathcal{D}}(\mathcal{Q}_1,\mathcal{A})$ be such that $\varphi = \psi_1|_{\mathcal{N}}$. We are finished if we can show that $\mathcal{P} \subseteq \mathcal{Q}_1$.

Assume conversely that $x \in \mathcal{P} \setminus \mathcal{Q}_1$. Set

$$\mathcal{I} := \{d \in \mathcal{D} \mid dx \in \mathcal{Q}_1\}.$$

This is a left ideal in $\mathcal{D}$. Define $\phi \in \mathrm{Hom}_{\mathcal{D}}(\mathcal{I},\mathcal{A})$ via

$$\phi(d) := \psi_1(dx).$$

By assumption, there exists $\theta \in \mathrm{Hom}_{\mathcal{D}}(\mathcal{D},\mathcal{A})$ such that $\theta|_{\mathcal{I}} = \phi$. The map θ is uniquely determined be $a := \theta(1) \in \mathcal{A}$, via $\theta(d) = d\theta(1) = da$, and thus

$$\phi(d) = da$$

for all $d \in \mathcal{I}$. Now let $\mathcal{Q}_2 := \mathcal{Q}_1 + \mathcal{D}x$. Since $x \notin \mathcal{Q}_1$, this is a proper supermodule of $\mathcal{Q}_1$. Set

$$\psi_2(q_2) := \psi_2(q_1 + dx) := \psi_1(q_1) + da.$$

To see that this is well-defined, let $q_2 = q_1 + dx = q_1' + d'x$. Then $q_1 - q_1' = (d' - d)x$, and thus $d' - d \in \mathcal{I}$. Hence $\phi(d' - d) = (d' - d)a$. On the other hand, $\phi(d' - d) = \psi_1((d' - d)x) = \psi_1(q_1 - q_1') = \psi_1(q_1) - \psi_1(q_1')$. Thus $\psi_1(q_1) + da = \psi_1(q_1') + d'a$.

Moreover, ψ_2 is $\mathcal{D}$-linear, because

$$\begin{aligned} \psi_2(q_2 + q_2') &= \psi_2(q_1 + q_1' + dx + d'x) = \psi_1(q_1 + q_1') + (d + d')a \\ &= \psi_1(q_1) + da + \psi_1(q_1') + d'a = \psi_2(q_2) + \psi_2(q_2') \end{aligned}$$

and

$$\psi_2(d'q_2) = \psi_2(d'q_1 + d'dx) = \psi_1(d'q_1) + d'da = d'\psi_1(q_1) + d'da = d'\psi_2(q_2).$$

Finally, we show that $\psi_2|_{\mathcal{N}} = \varphi$: Since $\mathcal{N} \subseteq \mathcal{Q}_1$, we have

$$\psi_2(n) = \psi_1(n) = \varphi(n)$$

for all $n \in \mathcal{N}$. Thus we have a contradiction to the maximality of $\mathcal{Q}_1$. □

A.6 Criterion for the cogenerator property

In this section, we prove Theorem 2.20.

First, we recall the definition of a (co-)generator [10, p. 53]. Let $\mathcal{D}$ be a ring (with unity), and let $\mathcal{A}$ be a left $\mathcal{D}$-module. One calls $\mathcal{A}$ a **generator** if for all left $\mathcal{D}$-modules $\mathcal{N}$, one has

$$\mathcal{N} = \sum_{\varphi \in \mathrm{Hom}_{\mathcal{D}}(\mathcal{A},\mathcal{N})} \mathrm{im}(\varphi)$$

and $\mathcal{A}$ is said to be a **cogenerator** if for all left $\mathcal{D}$-modules $\mathcal{N}$, we have

$$0 = \bigcap_{\varphi \in \mathrm{Hom}_{\mathcal{D}}(\mathcal{N},\mathcal{A})} \ker(\varphi).$$

Lemma A.6.1 *The following are equivalent:*

1. *$\mathcal{A}$ is a cogenerator.*
2. *If* $\mathrm{Hom}_{\mathcal{D}}(f, \mathcal{A}) = 0$*, then* $f = 0$.

In the second assertion, $f : \mathcal{M} \to \mathcal{N}$ is an arbitrary $\mathcal{D}$-linear map between two arbitrary left $\mathcal{D}$-modules $\mathcal{M}, \mathcal{N}$.

Proof: "1 ⇒ 2": Assume conversely that $f : \mathcal{M} \to \mathcal{N}$ is not identically zero, that is, $f(m_0) \neq 0$ for some $m_0 \in \mathcal{M}$, but $\mathrm{Hom}_{\mathcal{D}}(f, \mathcal{A}) = 0$, that is, $\varphi \circ f = 0$ for all $\varphi \in \mathrm{Hom}_{\mathcal{D}}(\mathcal{N}, \mathcal{A})$. This means that $\varphi(f(m_0)) = 0$ for all $\varphi \in \mathrm{Hom}_{\mathcal{D}}(\mathcal{N}, \mathcal{A})$, and hence $f(m_0) \neq 0$ is contained in the intersection of all kernels of $\varphi \in \mathrm{Hom}_{\mathcal{D}}(\mathcal{N}, \mathcal{A})$.

"2 ⇒ 1": Let $\mathcal{N}$ be such that there exists $0 \neq n_0 \in \mathcal{N}$ with $n_0 \in \ker(\varphi)$ for all $\varphi \in \mathrm{Hom}_{\mathcal{D}}(\mathcal{N}, \mathcal{A})$. Consider the map $f : \mathcal{D} \to \mathcal{N}$ defined by $f(1) = n_0$, that is, $f(d) = dn_0$ for all $d \in \mathcal{D}$. Then f is not identically zero, but $\mathrm{Hom}_{\mathcal{D}}(f, \mathcal{A})$ is, because

$$\varphi(f(d)) = \varphi(dn_0) = d\varphi(n_0) = 0$$

for all $d \in \mathcal{D}$, and hence $\varphi \circ f = 0$ for all $\varphi \in \mathrm{Hom}_{\mathcal{D}}(\mathcal{N}, \mathcal{A})$. □

In the following, we will see that if $\mathcal{A}$ is injective (which means that the functor $\mathrm{Hom}_{\mathcal{D}}(\cdot, \mathcal{A})$ is exact, i.e., it preserves exactness), then the cogenerator property is equivalent to saying that the functor $\mathrm{Hom}_{\mathcal{D}}(\cdot, \mathcal{A})$ is faithful (i.e., it reflects exactness).

Let T be a contravariant additive functor from the left $\mathcal{D}$-modules to the (additive) Abelian groups, that is, T assigns to each left $\mathcal{D}$-module $\mathcal{M}$ an Abelian group $T\mathcal{M}$, and to each $\mathcal{D}$-linear map $f : \mathcal{M} \to \mathcal{N}$ a group homomorphism $Tf : T\mathcal{N} \to T\mathcal{M}$ with

1. $T\mathrm{id}_{\mathcal{M}} = \mathrm{id}_{T\mathcal{M}}$;
2. $T(g \circ f) = Tf \circ Tg$;
3. $T(f + g) = Tf + Tg$;
4. If $f = 0$, then $Tf = 0$.

Note that conditions 1 and 4 imply: If $\mathcal{M} = 0$, then $T\mathcal{M} = 0$.

A typical example for such a functor is $T = \mathrm{Hom}_{\mathcal{D}}(\cdot, \mathcal{A})$. Additionally, assume that T is exact, that is, if

$$\mathcal{M} \xrightarrow{f} \mathcal{N} \xrightarrow{g} \mathcal{P}$$

is exact, then so is

$$T\mathcal{M} \xleftarrow{Tf} T\mathcal{N} \xleftarrow{Tg} T\mathcal{P}.$$

For $T = \mathrm{Hom}_{\mathcal{D}}(\cdot, \mathcal{A})$, exactness means injectivity of $\mathcal{A}$.

Lemma A.6.2 *The following are equivalent:*

1. *If* $T\mathcal{M} = 0$, *then* $\mathcal{M} = 0$.
2. *If* $Tf = 0$, *then* $f = 0$.

For $T = \mathrm{Hom}_{\mathcal{D}}(\cdot, \mathcal{A})$, *this means that* $\mathcal{A}$ *is a cogenerator.*

Proof: "2 $\Rightarrow$ 1": Let $\mathcal{M} \neq 0$. Then $\mathrm{id}_{\mathcal{M}} \neq 0$. By assertion 2, $T\mathrm{id}_{\mathcal{M}} \neq 0$. Since $T\mathrm{id}_{\mathcal{M}} = \mathrm{id}_{T\mathcal{M}}$, it follows that $T\mathcal{M} \neq 0$.

"1 $\Rightarrow$ 2": Let $f : \mathcal{M} \to \mathcal{N}$ be given. We have $f = i \circ f_1$, where $f_1 : \mathcal{M} \to \mathrm{im}(f)$ and $i : \mathrm{im}(f) \hookrightarrow \mathcal{N}$. Then $Tf = Tf_1 \circ Ti$. Suppose that $Tf = 0$. Since f_1 is surjective, Tf_1 is injective. Thus $Ti = 0$. On the other hand, since i is injective, Ti is surjective. Thus $\mathrm{im}(Ti) = T\mathrm{im}(f) = 0$. Using assertion 1, we have $\mathrm{im}(f) = 0$, that is, $f = 0$. □

Theorem A.6.3 *The following are equivalent:*

1. *If* $T\mathcal{M} = 0$, *then* $\mathcal{M} = 0$.
2. *If* $T\mathcal{M} \leftarrow T\mathcal{N} \leftarrow T\mathcal{P}$ *is exact, then so is* $\mathcal{M} \to \mathcal{N} \to \mathcal{P}$.

If the second assertion is true, one says that T *is faithful, or that* T *reflects exactness. Again, for* $T = \mathrm{Hom}_{\mathcal{D}}(\cdot, \mathcal{A})$, *this means that* $\mathcal{A}$ *is a cogenerator.*

Proof: "2 $\Rightarrow$ 1": Let $T\mathcal{M} = 0$. Then $0 \leftarrow T\mathcal{M} \leftarrow 0$ is exact. By assertion 2, $0 \to \mathcal{M} \to 0$ is exact, which means that $\mathcal{M} = 0$.

"1 $\Rightarrow$ 2": Let

$$\mathcal{M} \xrightarrow{f} \mathcal{N} \xrightarrow{g} \mathcal{P}$$

be not exact. We need to show that

$$T\mathcal{M} \xleftarrow{Tf} T\mathcal{N} \xleftarrow{Tg} T\mathcal{P}$$

is not exact.

Case 1: $g \circ f \neq 0$. Then, using the lemma, $T(g \circ f) \neq 0$, that is, $Tf \circ Tg \neq 0$, and we're finished.

Case 2: $g \circ f = 0$, that is, $\operatorname{im}(f) \subsetneq \ker(g)$. Then $T(g \circ f) = Tf \circ Tg = 0$, that is $\operatorname{im}(Tg) \subseteq \ker(Tf)$. We need to show that this inclusion is strict. Define

$$\sigma : \ker(g) \hookrightarrow \mathcal{N} \quad \text{and} \quad \pi : \mathcal{N} \to \mathcal{N}/\operatorname{im}(f).$$

Then

$$\ker(g) \xrightarrow{\sigma} \mathcal{N} \xrightarrow{g} \mathcal{P} \quad \text{and} \quad \mathcal{M} \xrightarrow{f} \mathcal{N} \xrightarrow{\pi} \mathcal{N}/\operatorname{im}(f)$$

are both exact. Therefore

$$T\ker(g) \xleftarrow{T\sigma} T\mathcal{N} \xleftarrow{Tg} T\mathcal{P} \quad \text{and} \quad T\mathcal{M} \xleftarrow{Tf} T\mathcal{N} \xleftarrow{T\pi} T(\mathcal{N}/\operatorname{im}(f))$$

are also exact. Thus

$$\ker(T\sigma) = \operatorname{im}(Tg) \subseteq \ker(Tf) = \operatorname{im}(T\pi).$$

The fact that $\operatorname{im}(f) \subsetneq \ker(g)$ means that $\pi \circ \sigma \neq 0$, and hence $T\sigma \circ T\pi \neq 0$. This shows that the above inclusion must be strict. $\square$

Corollary A.6.4 *Let $T = \operatorname{Hom}_{\mathcal{D}}(\cdot, \mathcal{A})$ with $\mathcal{A}$ injective. The following are equivalent:*

1. *If $T\mathcal{M} = 0$, then $\mathcal{M} = 0$.*
2. *If $T\mathcal{M} = 0$ and $\mathcal{M}$ is finitely generated, then $\mathcal{M} = 0$.*
3. *If $T\mathcal{M} = 0$ and $\mathcal{M}$ is generated by one single element, then $\mathcal{M} = 0$.*
4. *$\mathcal{A}$ is a cogenerator.*

Proof: The equivalence of assertions 1 and 4 was shown in a lemma above. Since "1 ⇒ 2 ⇒ 3" is obvious, it suffices to show "3 ⇒ 1". Let $\mathcal{M} \neq 0$. We need to show that $\mathrm{Hom}_{\mathcal{D}}(\mathcal{M}, \mathcal{A}) \neq 0$, that is, there exists a non-zero $\mathcal{D}$-linear map from $\mathcal{M}$ to $\mathcal{A}$. Let $0 \neq m \in \mathcal{M}$. Then $0 \neq \mathcal{D}m \subseteq \mathcal{M}$ and there is an exact sequence

$$0 \to \mathcal{D}m \hookrightarrow \mathcal{M}.$$

Since $\mathcal{A}$ is injective, the sequence

$$0 \leftarrow \mathrm{Hom}_{\mathcal{D}}(\mathcal{D}m, \mathcal{A}) \leftarrow \mathrm{Hom}_{\mathcal{D}}(\mathcal{M}, \mathcal{A})$$

is also exact, and by condition 3, $\mathrm{Hom}_{\mathcal{D}}(\mathcal{D}m, \mathcal{A}) \neq 0$, that is, there exists a non-zero $\mathcal{D}$-linear map $\psi : \mathcal{D}m \to \mathcal{A}$. However, the exactness of the last sequence says that there exists a $\mathcal{D}$-linear map $\phi : \mathcal{M} \to \mathcal{A}$ with $\phi|_{\mathcal{D}m} = \psi$. Thus $\phi \neq 0$. □

If $\mathcal{D}$ is left Noetherian, we can proceed analogously with the category of finitely generated left $\mathcal{D}$-modules. (Note that we need the Noetherian property to guarantee that kernels and images of $\mathcal{D}$-linear maps between finitely generated $\mathcal{D}$-modules are again finitely generated.) Then we obtain the following alternative version of Theorem 2.20.

Theorem A.6.5 *Let $T = \mathrm{Hom}_{\mathcal{D}}(\cdot, \mathcal{A})$ be an exact functor on the category of finitely generated left $\mathcal{D}$-modules. The following are equivalent:*

1. *If $T\mathcal{M} = 0$, then $\mathcal{M} = 0$.*
2. *T is faithful, i.e., it reflects exactness.*
3. *$\mathcal{A}$ is a cogenerator.*

A.7 Injective cogenerator property for 1-d time-invariant systems

Theorem A.7.1 *Let $\mathcal{D} = \mathbb{K}[\frac{d}{dt}]$ and $\mathcal{A} = \mathcal{C}^\infty(\mathbb{R}, \mathbb{K})$. Then $\mathcal{A}$ is an injective cogenerator.*

Proof: Using Baer's criterion, we need to prove that

$$0 \leftarrow \mathrm{Hom}_{\mathcal{D}}(\mathcal{I}, \mathcal{A}) \leftarrow \mathrm{Hom}_{\mathcal{D}}(\mathcal{D}, \mathcal{A})$$

is exact, that is, for every $\mathcal{D}$-linear map $\psi : \mathcal{I} \to \mathcal{A}$ there exists a $\mathcal{D}$-linear map $\phi : \mathcal{D} \to \mathcal{A}$ such that $\phi|_{\mathcal{I}} = \psi$. This is trivial if $\mathcal{I} = 0$, so assume otherwise.

Every ideal in $\mathcal{D}$ can be generated by one single element (principal ideal domain). Thus $\mathcal{I} = \mathcal{D}d$ for some $0 \neq d \in \mathcal{D}$ and $\psi : \mathcal{D}d \to \mathcal{A}$ is uniquely determined by fixing an element $u := \psi(d) \in \mathcal{A}$. In order to extend ψ to all of $\mathcal{D}$, we need to find an element $y := \phi(1) \in \mathcal{A}$ such that $\phi(d) = d\phi(1) = dy = \psi(d) = u$.

Therefore we need to show: Provided that $d \neq 0$, we have

$$\forall u \in \mathcal{A} \exists y \in \mathcal{A} : dy = u.$$

This property of $\mathcal{A}$ is called divisibility. If $d \in \mathbb{K}$, this is trivial. Suppose that d has degree at least one. It is a standard fact from ODE theory that every scalar linear constant-coefficient ordinary differential equation with a smooth right hand side possesses a smooth solution.

For the cogenerator property we need to show: If $Rw = 0$ has only the zero solution (that is, $\mathrm{Hom}_{\mathcal{D}}(\mathcal{M}, \mathcal{A}) \cong \mathcal{B} = 0$), then R must be left invertible (that is, $\mathcal{M} = 0$). Since $\mathcal{D}$ is a principal ideal domain, it suffices to consider the case where R is a scalar. Therefore, we need to prove: If $dy = 0$ has only the zero solution, then d is a non-zero constant, that is, $d \in \mathbb{K} \setminus \{0\}$.

However, if d is not a non-zero constant, then the fundamental theorem of algebra implies that there exists $\lambda \in \mathbb{C}$ such that $d(\lambda) = 0$. Then $de^{\lambda t} = d(\lambda)e^{\lambda t} = 0$, showing that $dy = 0$ has not only the zero solution. Of course, $e^{\lambda t}$ will be complex-valued in general. However, if $\mathbb{K} = \mathbb{R}$, then $\mathrm{Re}(e^{\lambda t}) = e^{\mathrm{Re}(\lambda)t} \cos(\mathrm{Im}(\lambda)t)$ is a non-zero solution to $dy = 0$. □

A.8 Ore domains and fields of fractions

Let $\mathcal{D}$ be a domain. The following theorem can be found in [3, p. 177].

Theorem A.8.1 *$\mathcal{D}$ admits a field of left fractions*

$$\mathcal{K} = \{d^{-1}n \mid d, n \in \mathcal{D}, d \neq 0\}$$

if and only if $\mathcal{D}$ has the left Ore property.

Proof: If $\mathcal{D}$ admits a field of left fractions $\mathcal{K}$, then $\mathcal{K}$ contains all $n = 1^{-1}n$ and all $d^{-1} = d^{-1}1$ for $n, d \in \mathcal{D}$, $d \neq 0$. Therefore it also contains nd^{-1}. This has to be left fraction again, that is $nd^{-1} = d_1^{-1}n_1$ or equivalently,

$$d_1 n = n_1 d$$

for some $d_1, n_1 \in \mathcal{D}$, $d_1 \neq 0$. Thus we have shown that all $n, d \in \mathcal{D}$, $d \neq 0$ possess a left common multiple. If we know additionally that $n \neq 0$ then this implies $n_1 \neq 0$. Thus we have the left Ore property.

Conversely, let $\mathcal{D}$ be a left Ore domain, and let $\mathcal{D}^* := \mathcal{D} \setminus \{0\}$. We define a relation on $\mathcal{D}^* \times \mathcal{D}$ via

$$(d_1, n_1) \sim (d_2, n_2) \quad \Leftrightarrow \quad c_1 d_1 = c_2 d_2 \text{ implies } c_1 n_1 = c_2 n_2.$$

This is an equivalence relation: Reflexivity and symmetry are obvious. For transitivity, let $(d_1, n_1) \sim (d_2, n_2)$ and $(d_2, n_2) \sim (d_3, n_3)$ and $c_1 d_1 = c_3 d_3 \neq 0$. Due to the left Ore property, there exist $0 \neq c, c_2$ such that $cc_1 d_1 = cc_3 d_3 = c_2 d_2$. This implies both $cc_1 n_1 = c_2 n_2$ and $c_2 n_2 = cc_3 n_3$ which yields $c(c_1 n_1 - c_3 n_3) = 0$ and hence $c_1 n_1 = c_3 n_3$.

We set $\mathcal{K} := (\mathcal{D}^* \times \mathcal{D}) / \sim$. The multiplication on $\mathcal{K}$ is defined by

$$[(d_1, n_1)] \cdot [(d_2, n_2)] := [(ad_1, bn_2)]$$

where $an_1 = bd_2$, $a \neq 0$. To see that this is well-defined, let $(d_1, n_1) \sim (d_1', n_1')$ and $(d_2, n_2) \sim (d_2', n_2')$ and $a'n_1' = b'd_2'$. We need to show that $(ad_1, bn_2) \sim (a'd_1', b'n_2')$. For this let $cad_1 = c'a'd_1'$. Then $can_1 = c'a'n_1'$. Equivalently, $cbd_2 = c'b'd_2'$. This implies $cbn_2 = c'b'n_2'$.

Let $0_{\mathcal{K}} := [(1, 0)] = [(d, 0)]$ for all $d \neq 0$, and $1_{\mathcal{K}} := [(1, 1)] = [(d, d)]$ for all $d \neq 0$. We have $0_{\mathcal{K}} \cdot k = k \cdot 0_{\mathcal{K}} = 0_{\mathcal{K}}$ and $1_{\mathcal{K}} \cdot k = k \cdot 1_{\mathcal{K}} = k$ for all $k \in \mathcal{K}$. All $0_{\mathcal{K}} \neq [(d, n)] \in \mathcal{K}$ are invertible, because

$$[(d, n)] \cdot [(n, d)] = [(n, d)] \cdot [(d, n)] = [(1, 1)] = 1_{\mathcal{K}}.$$

To define the addition on $\mathcal{K}$, it suffices to explain $k + 1_{\mathcal{K}}$ for all $k \in \mathcal{K}$, because then the sum of arbitrary elements of $\mathcal{K}$ can be defined via

$$k + l = \begin{cases} k & \text{if } l = 0_{\mathcal{K}} \\ l(l^{-1}k + 1_{\mathcal{K}}) & \text{if } l \neq 0_{\mathcal{K}}. \end{cases}$$

We set

$$[(d, n)] + [(1, 1)] = [(d, n + d)].$$

Thus $\mathcal{K}$ becomes a field, and we have an injective ring homomorphism

$$\mathcal{D} \to \mathcal{K}, \quad d \mapsto [(1, d)].$$

Identifying $\mathcal{D}$ with its image under this map, we have for all $d \neq 0$

$$d^{-1}n = [(1, d)]^{-1} \cdot [(1, n)] = [(d, 1)] \cdot [(1, n)] = [(d, n)]$$

which shows that an element of $\mathcal{K}$ as constructed can be identified with a left fraction of elements of $\mathcal{D}$. □

Remark: Let $\mathcal{D}$ be a left Ore domain and let $\mathcal{K}$ be its field of left fractions. Any $H \in \mathcal{K}^{p\times m}$ has a representation $H = d^{-1}N$ where $0 \neq d \in \mathcal{D}$ and $N \in \mathcal{D}^{p\times m}$.

For this let $H_{ij} = d_{ij}^{-1}\tilde{n}_{ij}$ and let d be a left common multiple of all d_{ij}, say $d = a_{ij}d_{ij}$ for all i, j. Then $H_{ij} = d^{-1}a_{ij}\tilde{n}_{ij}$ and we set $N_{ij} := a_{ij}\tilde{n}_{ij}$.

A.9 Linear algebra over skew fields

Let $\mathcal{K}$ be a skew (i.e., non-commutative) field.

Let V be a finitely generated right $\mathcal{K}$-module with generators $v_1, \ldots, v_q$. Then

$$V = \sum_{i=1}^{q} v_i\mathcal{K}.$$

Since $\mathcal{K}$ is a field, one also says that V is a right $\mathcal{K}$-vector space. Note that we may assume without loss of generality that $v_i \neq 0$ for all i.

Lemma A.9.1 *There exists a set $J \subseteq \{1, \ldots, q\}$ such that*

$$V = \bigoplus_{j\in J} v_j\mathcal{K}.$$

The directness of the sum says that v_j, $j \in J$ are (right) $\mathcal{K}$-linearly independent, that is,

$$\sum_{j\in J} v_jk_j = 0 \quad \Rightarrow \quad k_j = 0 \text{ for all } j \in J.$$

If $V = \oplus_{j\in J}v_j\mathcal{K}$, then we say that $\{v_j \mid j \in J\}$ is a **basis** of V. Thus the lemma says that every finitely generated right $\mathcal{K}$-vector space has a basis.

Proof: Consider the sets $I \subseteq \{1, \ldots, q\}$ for which the sum $\sum_{i\in I} v_i\mathcal{K}$ is direct. Among these sets, choose one whose cardinality is maximal, say J. Set $V_J := \oplus_{j\in J}v_j\mathcal{K}$. We need to show that $V_J = V$. For this, it suffices to show that $v_i \in V_J$ for all $i \notin J$. Let $W_i := V_J \cap v_i\mathcal{K}$ for $i \notin J$. This is a right $\mathcal{K}$-submodule of $v_i\mathcal{K}$.

Case 1: $W_i = 0$. Then $V_J + v_i\mathcal{K} = V_J \oplus v_i\mathcal{K}$, contradicting the maximality of J.

Case 2: $W_i \neq 0$. Let $0 \neq w_i \in W_i$. Then $w_i = v_ik$ for some $0 \neq k \in \mathcal{K}$, and hence $w_ik^{-1} = v_i$, showing that $v_i\mathcal{K} \subseteq w_i\mathcal{K} \subseteq W_i \subseteq v_i\mathcal{K}$. Thus $W_i = v_i\mathcal{K}$. This means that $v_i\mathcal{K} \subseteq V_J$, hence $v_i \in V_J$. □

Let $R \in \mathcal{K}^{g\times q}$ and let $V = R\mathcal{K}^q$. Then V is generated by the columns of R. The lemma says that we have (after a suitable permutation of the columns) a representation $R = [-Q, P]$ where the columns of P are linearly independent, and $Q = PH$ for some $\mathcal{K}$-matrix H.

Theorem A.9.2 *Let $W = \oplus_{i=1}^m w_i\mathcal{K} \subseteq V = \oplus_{i=1}^n v_i\mathcal{K}$. Then $m \leq n$ and there exists a set $J \subseteq \{1, \ldots, n\}$ of cardinality $n - m$ such that $W \oplus W' = V$, where $W' = \oplus_{j\in J} v_j\mathcal{K}$. In particular, $V = W$ if and only if $n = m$.*

Proof: The proof is by induction on m. If $m = 0$, there is nothing to prove. Assume that we have proven the statement for $m - 1$. Consider

$$W = \oplus_{i=1}^{m-1} w_i\mathcal{K} \oplus w_m\mathcal{K} \subseteq V.$$

By the inductive hypothesis, $m - 1 \leq n$, and we can choose $n - m + 1$ elements from the basis of V, say $v_m, \ldots, v_n$, such that $B := \{w_1, \ldots, w_{m-1}, v_m, \ldots, v_n\}$ is a basis of V. Now if $m - 1 = n$, then we have $B = \{w_1, \ldots, w_{m-1}\}$. But this cannot be a basis of V, because $w_m \in V$ cannot be generated by these elements (by the assumed linear independence of $w_1, \ldots, w_m$). Therefore, we must have $m \leq n$.

Since B is a basis of V, there exists a representation

$$w_m = \sum_{i=1}^{m-1} w_i a_i + \sum_{j=m}^{n} v_j b_j$$

for some $a_i, b_j \in \mathcal{K}$. If all b_j were zero, then this would again contradict the linear independence of $w_1, \ldots, w_m$. Therefore at least one of the b_j is non-zero. Without loss of generality, let $b_m \neq 0$. Then v_m is a linear combination of $B' := \{w_1, \ldots, w_m, v_{m+1}, \ldots, v_n\}$. Since B generates V, so does $B \cup \{w_m\}$, and by the previous argument, $B' = B \cup \{w_m\} \setminus \{v_m\}$ is also a generating set for V. We are finished if we can show that B' is a basis of V. For this, we have to show that the elements of B' are linearly independent. Assume that

$$\sum_{i=1}^{m} w_i a_i + \sum_{j=m+1}^{n} v_j b_j = 0.$$

Case 1: $a_m \neq 0$. Then we can write w_m as a linear combination of $B' \setminus \{w_m\}$. Thus $B' \setminus \{w_m\} \subsetneq B$ is already a generating system of V. This contradicts the fact that B is a basis of V.

Case 2: $a_m = 0$. Then

$$\sum_{i=1}^{m-1} w_i a_i + \sum_{j=m+1}^{n} v_j b_j = 0$$

which implies that all a_i and all b_i must be zero, because $B' \setminus \{w_m\} \subseteq B$ and hence its elements are linearly independent. $\square$

Thus the cardinality of a basis is an invariant of a finitely generated $\mathcal{K}$-module V and we call it the **dimension** of V. If $V = R\mathcal{K}^q \subseteq \mathcal{K}^g$, we set $\operatorname{columnrank}(R) := \dim(V)$.

Consider the right $\mathcal{K}$-linear map

$$R : \mathcal{K}^q \longrightarrow \mathcal{K}^g, \quad x \mapsto Rx.$$

Its image equals $\operatorname{im}(R) = R\mathcal{K}^q$, and its kernel is a right $\mathcal{K}$-submodule of $\mathcal{K}^q$. Thus $\ker(R)$ is also finitely generated (if it were not, we could construct an infinite sequence $x_1, x_2, \ldots$ of linearly independent elements of $\ker(R)$, and hence of $\mathcal{K}^q$, in particular, we would have $\oplus_{i=1}^{q+1} x_i\mathcal{K} \subseteq \mathcal{K}^q = \oplus_{i=1}^{q} e_i\mathcal{K}$, a contradiction). There is an induced isomorphism

$$\mathcal{K}^q / \ker(R) \cong \operatorname{im}(R)$$

which shows that

$$\dim(\mathcal{K}^q / \ker(R)) = \dim(\operatorname{im}(R)) = \operatorname{columnrank}(R).$$

However, there exists a finitely generated right $\mathcal{K}$-vector space W' such that $\ker(R) \oplus W' = \mathcal{K}^q$, where $\dim(W') = q - \dim(\ker(R))$. Since $\mathcal{K}^q / \ker(R) \cong W'$, we have

$$q - \dim(\ker(R)) = \operatorname{columnrank}(R).$$

Similarly, one considers

$$\cdot R : \mathcal{K}^{1\times g} \longrightarrow \mathcal{K}^{1\times q}, \quad x \mapsto xR$$

which is a left $\mathcal{K}$-linear map, and we obtain $\operatorname{im}(\cdot R) = \mathcal{K}^{1\times g}R$ and $\ker(\cdot R)$ which are left $\mathcal{K}$-modules. Then

$$g - \dim(\ker(\cdot R)) = \dim(\mathcal{K}^{1\times g}R) =: \operatorname{rowrank}(R).$$

Theorem A.9.3 *For any $\mathcal{K}$-matrix R, we have* $\operatorname{rowrank}(R) = \operatorname{columnrank}(R)$.

For this, we need the concept of the dual vector space: For a finitely generated right $\mathcal{K}$-module V, we set

$$V^* = \operatorname{Hom}_{\mathcal{K}}(V, \mathcal{K})$$

which contains all right-linear maps $\varphi : V \to \mathcal{K}$, that is, $\varphi(vk) = \varphi(v)k$. Then V^* is a left $\mathcal{K}$-module. Indeed, for $l \in \mathcal{K}$, the map $l\varphi$, defined by $(l\varphi)(v) := l\varphi(v)$, is again in V^*. Since a $\mathcal{K}$-linear map is uniquely determined by the image of a basis, we have

$$V^* \cong \mathcal{K}^{1\times d},$$

where $d = \dim(V)$. In particular, $(\mathcal{K}^d)^* \cong \mathcal{K}^{1\times d}$. More explicitly, this isomorphism is given by

$$\phi : \mathcal{K}^{1\times d} \to (\mathcal{K}^d)^*, \quad x \mapsto \phi(x)$$

where $\phi(x) : \mathcal{K}^d \mapsto \mathcal{K}$, $y \mapsto xy$. The following proof can be found in [13].

Proof: We have a commutative diagram

$$\begin{array}{ccc} \mathcal{K}^{1\times g} & \xrightarrow{\cdot R} & \mathcal{K}^{1\times q} \\ \downarrow & & \downarrow \\ (\mathcal{K}^g)^* & \xrightarrow{R^*} & (\mathcal{K}^q)^* \end{array}$$

where the vertical arrows are given by the isomorphism ϕ. Thus

$$\dim(\ker(R^*)) = \dim(\ker(\cdot R)) = g - \text{rowrank}(R).$$

On the other hand, the exact sequence

$$\mathcal{K}^q \xrightarrow{R} \mathcal{K}^g \longrightarrow \mathcal{K}^g/\text{im}(R) \longrightarrow 0$$

implies, due to the left exactness of $\text{Hom}_{\mathcal{K}}(\cdot, \mathcal{K})$, that

$$(\mathcal{K}^q)^* \xleftarrow{R^*} (\mathcal{K}^g)^* \longleftarrow (\mathcal{K}^g/\text{im}(R))^* \longleftarrow 0$$

is also exact, and thus

$$\ker(R^*) \cong (\mathcal{K}^g/\text{im}(R))^*$$

which implies that

$$\dim(\ker(R^*)) = g - \dim(\text{im}(R)) = g - \text{columnrank}(R).$$

Combining this with the equation above, we have the desired result. □

Remark: $\text{Hom}_{\mathcal{K}}(\cdot, \mathcal{K})$ is an exact and faithful functor from the category of finitely generated right $\mathcal{K}$-modules to the category of finitely generated left $\mathcal{K}$-modules (and the same holds, of course, if "left" and "right" are interchanged).

A.10 Controllability and observability for 1-d time-invariant systems

Controllability

In this section, we show that a classical state space system $\dot{x} = Ax + Bu$ is controllable in the sense of the Introduction if and only if its system module is torsion-free. This shows that the notion of controllability proposed in Section 3.3 coincides with the classical concept when applied to systems of this form.

Let $\mathcal{D} = \mathbb{K}[\frac{d}{dt}]$, let $R \in \mathcal{D}^{g\times q}$ and consider $\mathcal{M} = \mathcal{D}^{1\times q}/\mathcal{D}^{1\times g}R$. Since $\mathcal{D}$ is a principal ideal domain, we have the following result.

Lemma A.10.1 *$\mathcal{M}$ is torsion-free if and only if it is free, that is, $\mathcal{M}\cong\mathcal{D}^{1\times l}$ for some integer l. Indeed, we have $l = q - \mathrm{rank}(R)$.*

Proof: This can be shown using the Smith form. Let

$$URV = \begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix}$$

where $D = \mathrm{diag}(d_1, \dots, d_p)$ for some $0 \neq d_i \in \mathcal{D}$. Without loss of generality, let the d_i be monic polynomials. Then

$$\mathcal{M} \cong \mathcal{D}/\mathcal{D}d_1 \times \cdots \times \mathcal{D}/\mathcal{D}d_p \times \mathcal{D}^{1\times(q-p)}.$$

The module $\mathcal{D}/\mathcal{D}d_i$ is torsion-free if and only if $d_i = 1$. Thus $\mathcal{M}$ is torsion-free if and only if $\mathcal{M} \cong \mathcal{D}^{1\times(q-p)}$, where $p = \mathrm{rank}(R)$. □

Note that in general, a torsion-free module is not necessarily free, whereas the implication "free ⇒ torsion-free" is always true when $\mathcal{D}$ is a domain.

Lemma A.10.2 *Let R have full row rank, that is, $\mathrm{rank}(R) = g$. Then $\mathcal{M}$ is free if and only if there exists $X \in \mathcal{D}^{q\times g}$ such that $RX = I$.*

Proof: Let R have full row rank, that is, $p = g$. Then the Smith form takes the form $URV = [D, 0]$. By the previous lemma, $\mathcal{M}$ is free if and only if we have $URV = [I, 0]$. Then

$$URV \begin{bmatrix} I \\ 0 \end{bmatrix} = I$$

which implies (multiplying by U^{-1} from the left, and by U from the right)

$$RV \begin{bmatrix} I \\ 0 \end{bmatrix} U = I$$

that is, we have found X with the desired property. Conversely, if $RX = I$, then $URVV^{-1}XU^{-1} = I$. Thus there exists a $\mathcal{D}$-matrix Y such that $DY = I$, and thus $d_i y_{ii} = 1$ for all i. This implies that $d_i = 1$ for all i, that is, $D = I$. □

Lemma A.10.3 *There exists X such that $RX = I$ if and only if $R(\lambda)$ has full row rank for all $\lambda \in \mathbb{C}$.*

Proof: If $RX = I$, then $R(\lambda)X(\lambda) = I$ and hence $R(\lambda)$ has full row rank. Conversely, if $\operatorname{rank}(R(\lambda)) = g$ for all $\lambda \in \mathbb{C}$, the $g \times g$ minors m_i of R have no common zero, i.e., they are coprime and hence there exists a Bézout identity

$$\sum d_i m_i = 1.$$

Since there exist X_i with $RX_i = m_i I$, we obtain with $X := \sum d_i X_i$

$$RX = \sum d_i R X_i = \sum d_i m_i I = I.$$

□

Let $A \in \mathbb{K}^{n \times n}$ and $B \in \mathbb{K}^{n \times m}$ and set

$$R = [\tfrac{d}{dt} I - A, -B] \in \mathcal{D}^{n \times (n+m)}.$$

Then $g = n$, $q = n + m$ and $p = n$.

Lemma A.10.4 *Let $0 \neq V \subseteq \mathbb{K}^{1 \times n}$ be an A-invariant vector space, that is, $v \in V$ implies $vA \in V$. Then V contains a left eigenvector of A, that is, there exists $0 \neq v \in V$ with $vA = \lambda v$ for some $\lambda \in \mathbb{C}$.*

Proof: Let $\dim(V) = d$, and let $v_1, \ldots, v_d$ be a basis of V. Collecting these basis vectors into a matrix $W \in \mathbb{K}^{d \times n}$, we have $V = \operatorname{im}(\cdot W)$ and $\operatorname{rank}(W) = d$. The A-invariance of V means that $WA = CW$ for some $C \in \mathbb{K}^{d \times d}$. Let x be a left eigenvector of C, that is, $xC = \lambda x$ for some $\lambda \in \mathbb{C}$. Then $xWA = xCW = \lambda xW$. Set $v := xW \in V$. Since $x \neq 0$ and since W has full row rank, we have $v \neq 0$ and thus it has the desired properties. □

Corollary A.10.5 *The following are equivalent:*

1. *There exists $0 \neq \xi \in \mathbb{K}^{1 \times n}$ such that $\xi A^i B = 0$ for all $i \in \mathbb{N}$, or equivalently, for all $0 \leq i \leq n - 1$.*
2. *There exists a left eigenvector v of A with $vB = 0$, that is, there exists $\lambda \in \mathbb{C}$ and $0 \neq v \in \mathbb{K}^{1 \times n}$ such that*

$$vR(\lambda) = v[\lambda I - A, -B] = 0.$$

Proof: "1 ⇒ 2": Apply the previous lemma to

$$V = \bigcap_{i \in \mathbb{N}} \ker(\cdot A^i B) = \bigcap_{i=0}^{n-1} \ker(\cdot A^i B).$$

"2 $\Rightarrow$ 1": If $vR(\lambda) = 0$, we obtain inductively $vB = 0$, $vAB = \lambda vB = 0$, $vA^2B = \lambda vAB = 0$ etc. □

Now we obtain the desired result, which shows that the two controllability concepts coincide.

Theorem A.10.6 *$\mathcal{M}$ is torsion-free if and only if* $\mathrm{rank}(K) = n$*, where*

$$K = [B, AB, \ldots, A^{n-1}B].$$

Proof: By the lemmas from above, $\mathcal{M}$ is torsion-free if and only if $RX = I$ for some $\mathcal{D}$-matrix X, which is in turn equivalent to $R(\lambda)$ having full row rank for all $\lambda \in \mathbb{C}$. Still equivalently, there exists no $\xi \neq 0$ with $\xi A^i B = 0$ for all i. In other words, $\mathrm{rank}(K) = n$. □

The equivalence

$$\mathrm{rank}(K) = n \quad \Leftrightarrow \quad \mathrm{rank}(R(\lambda)) = n \text{ for all } \lambda \in \mathbb{C}$$

is known as the **Hautus test**.

Observability

In this section we show that in a state space system

$$\begin{aligned} \dot{x} &= Ax + Bu \\ y &= Cx + Du, \end{aligned}$$

the latent variables x are observable from the manifest variables u and y if and only if the system is observable in the classical sense, which means that

$$K = \begin{bmatrix} C \\ CA \\ \vdots \\ CA^{n-1} \end{bmatrix}$$

has rank n. Recall that x is observable from u, y if and only if $u = 0$ and $y = 0$ imply $x = 0$, that is,

$$\dot{x} = Ax \text{ and } Cx = 0 \quad \Rightarrow \quad x = 0.$$

In other words,

$$\mathcal{B}_{unobs} = \{x \in \mathcal{A}^n \mid \dot{x} = Ax, Cx = 0\} = 0.$$

Since $\mathcal{B}_{unobs}$ has the kernel representation

$$M = \begin{bmatrix} \frac{d}{dt}I - A \\ C \end{bmatrix} \in \mathcal{D}^{(n+p)\times n},$$

this amounts to saying that M is left invertible. Therefore it suffices to prove the following lemma.

Lemma A.10.7 *The following are equivalent:*

1. *The matrix M is left invertible.*
2. $\operatorname{rank}(M(\lambda)) = n$ *for all* $\lambda \in \mathbb{C}$.
3. $\operatorname{rank}(K) = n$.

Proof: The equivalence of the first two conditions is analogous to the statement of Lemma A.10.3, and the equivalence of the second and third assertion is analogous to Corollary A.10.5. □

A.11 Jacobson form

Let $\mathcal{D}$ be a right and left principal ideal domain.

An element $a \in \mathcal{D}$ is called a **right divisor** of $b \in \mathcal{D}$ if there exists $x \in \mathcal{D}$ such that $xa = b$ or equivalently, if $\mathcal{D}b \subseteq \mathcal{D}a$. Similarly, a is a **left divisor** of b if $ay = b$ for some y, which means that $b\mathcal{D} \subseteq a\mathcal{D}$. Finally, a is said to be a **total divisor** of b if

$$\mathcal{D}b\mathcal{D} \subseteq a\mathcal{D} \cap \mathcal{D}a.$$

Note that this implies that a is both a right and a left divisor of b, but "total divisor" is a stronger property than "right and left divisor": for instance, a is not necessarily a total divisor of a.

Although the given definition of a total divisor is appealing due to its symmetry, it is important to note that it is actually redundant, as shown in the following lemma.

Lemma A.11.1 *If $\mathcal{D}b\mathcal{D} \subseteq a\mathcal{D}$, then a is a total divisor of b. Analogously, the condition $\mathcal{D}b\mathcal{D} \subseteq \mathcal{D}a$ is also sufficient for a being a total divisor of b.*

Proof: It suffices to show the first statement. Let the non-zero two-sided ideal $\mathcal{D}b\mathcal{D}$ be generated, as a left ideal, by c, and, as a right ideal, by c'. We first show that without loss of generality, we may assume that $c = c'$. Indeed, if

$$\mathcal{D}b\mathcal{D} = \mathcal{D}c = c'\mathcal{D},$$

then $c = c'u$ and $c' = vc$ for some $u, v \in \mathcal{D}$, which yields $c' = vc'u$. Since $vc' \in \mathcal{D}b\mathcal{D}$, we have $vc' = c'u'$ for some u', and hence $c' = c'u'u$. Since $c' \neq 0$ by assumption, we obtain $u'u = 1$, that is, u is a unit. This implies $c\mathcal{D} = c'\mathcal{D}$ and hence

$$\mathcal{D}b\mathcal{D} = \mathcal{D}c = c\mathcal{D}.$$

Now let $0 \neq \mathcal{D}b\mathcal{D} = c\mathcal{D} \subseteq a\mathcal{D}$. We need to show that $\mathcal{D}b\mathcal{D} = \mathcal{D}c \subseteq \mathcal{D}a$. For this, consider the left ideal $\mathcal{D}a + \mathcal{D}c$, which can be generated by one single element, say by d, that is,

$$\mathcal{D}a + \mathcal{D}c = \mathcal{D}d.$$

Then $d = ka + lc$ for some $k, l \in \mathcal{D}$. On the other hand, we have $c = ay$ for some $y \in \mathcal{D}$ by assumption. Combining this, we get

$$dy = kay + lcy = kay + ly'c = kay + ly'ay = (k + ly')ay,$$

where we have used $c\mathcal{D} = \mathcal{D}c$, that is, $cy = y'c$ for some y'. Since $y \neq 0$ by assumption, this implies $d = (k + ly')a$, and hence $\mathcal{D}d \subseteq \mathcal{D}a$. From this, we obtain $\mathcal{D}c \subseteq \mathcal{D}a$ as desired. □

From now on, let $\mathcal{D} = K[D]$, where $D = \frac{d}{dt}$, and K denotes the rational functions.

Theorem A.11.2 *$\mathcal{D}$ is a left and right Euclidean domain.*

Proof: We first observe that for any $d, n \in \mathcal{D}$, $d \neq 0$, with $\deg(n) \geq \deg(d)$ there exists $f \in \mathcal{D}$ such that

$$\deg(n - fd) < \deg(n).$$

Indeed, if $n = a_\mu D^\mu + \ldots + a_0$ and $d = b_\nu D^\nu + \ldots + b_0$ with $a_\mu, b_\nu \neq 0$ and $\mu \geq \nu$, we may take $f = a_\mu D^{\mu-\nu} b_\nu^{-1}$.

Now let $n, d \in \mathcal{D}$, $d \neq 0$ be given. If d is a right divisor of n, we have $n = qd$ for some $q \in \mathcal{D}$ and we are finished by putting $r = 0$. Otherwise, define

$$\delta := \min\{\deg(n - fd) \mid f \in \mathcal{D}\}.$$

Let $q \in \mathcal{D}$ be such that $\deg(n - qd) = \delta$.

Case 1: $\deg(n - qd) \geq \deg(d)$. Then there exists f such that

$$\deg(n - qd - fd) < \deg(n - qd) = \delta.$$

This contradicts the minimality of δ.

Case 2: $\deg(n - qd) < \deg(d)$. Then we are finished by putting $r := n - qd$, that is, we have constructed a representation $n = qd + r$ with $\deg(r) < \deg(d)$ as desired.

The right division with remainder is constructed similarly. □

Theorem A.11.3 (Jacobson form) *For every $R \in \mathcal{D}^{g\times q}$, there exist unimodular matrices U, V such that*

$$URV = \begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix}$$

where $D = \operatorname{diag}(d_1, \dots, d_p)$, $0 \neq d_i \in \mathcal{D}$, $p = \operatorname{rank}(R)$, and each d_i is a total divisor of d_{i+1} for $1 \leq i \leq p-1$.

Recalling that the ring $\mathcal{D}$ is simple, the two-sided ideal $\mathcal{D}b\mathcal{D}$ can only be the zero ideal or $\mathcal{D}$ itself. This means that a is a total divisor of b if and only if either $b = 0$ or a is a unit (and then without loss of generality, $a = 1$). Therefore we may conclude that $d_1 = \ldots = d_{p-1} = 1$. Note that except for this observation, the proof given below holds for arbitrary right and left Euclidean domains.

Proof: Without loss of generality, let $R \neq 0$. It is sufficient to show that by elementary operations, R can be brought into the form

$$R' = \begin{bmatrix} a & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & Q & \\ 0 & & & \end{bmatrix} \tag{A.8}$$

where a is a total divisor of all entries of Q. Then one applies the same procedure to Q, and the result follows inductively.

Case 1: There exists i, j such that R_{ij} is a total divisor of all entries of R. By a suitable interchange of rows and columns, this element can be brought into the (1,1) position of the matrix. Therefore without loss of generality, R_{11} is a total divisor of all entries of R. This means, in particular, that $x_i R_{11} = R_{i1}$ and $R_{11} y_j = R_{1j}$. Now perform the following elementary operations: for all $i \neq 1$, put ith row minus x_i times 1st row (i.e., the first row is being multiplied by x_i from the left); for all $j \neq 1$, put jth column minus 1st column times y_j (i.e., the first column is being multiplied by y_j from the right). Then we are finished.

Case 2: There is no i, j such that R_{ij} is a total divisor of all entries of R. Let

$$\delta(R) := \min\{\deg(R_{ij}) \mid R_{ij} \neq 0\}.$$

Without loss of generality, $\deg(R_{11}) = \delta(R)$. We show that by elementary operations, we can transform R into $R^{(1)}$ with $\delta(R^{(1)}) < \delta(R)$. Then we obtain a strictly decreasing sequence $\delta(R) > \delta(R^{(1)}) > \delta(R^{(2)}) > \ldots \geq 0$. After finitely many steps, we arrive at zero, i.e., we obtain a matrix which has a unit as an entry, and thus we are in Case 1.

Case 2a: R_{11} is not a left divisor of all R_{1j}, say, it is not a left divisor of R_{1k}. By the Euclidean algorithm, we can write

$$R_{1k} = R_{11}q + r$$

where $r \neq 0$ and $\deg(r) < \deg(R_{11})$. Perform the elementary operation: kth column minus 1st column times q. Then the new matrix $R^{(1)}$ has r in the $(1, k)$ position and thus $\delta(R^{(1)}) < \delta(R)$ as desired.

Case 2a': R_{11} is not a right divisor of all R_{i1}. Proceed analogously as in Case 2a.

Case 2b: R_{11} is a left divisor of all R_{1j}, and a right divisor of all R_{i1}. Similarly as in Case 1, we can transform, by elementary operations, R into the form (A.8). If a is a total divisor of all entries of Q, then we are finished. If there exists i, j such that a is not a total divisor of $b := Q_{ij}$, then there exists c such that a is not a left divisor of cb. (Assume conversely that a is a left divisor of cb for all c, then $a\mathcal{D} \supseteq \mathcal{D}b$, and thus $a\mathcal{D} \supseteq \mathcal{D}b\mathcal{D}$, which implies that a is a total divisor of b according to the lemma.) We perform the elementary operation: 1st row plus c times $(i+1)$st row. (Note that the $(i+1)$st row of R' corresponds to the ith row of Q.) The new matrix has cb in the $(1, j+1)$ position and therefore we are in Case 2a. □

Example: Let $D = \frac{d}{dt}$ and

$$R = \begin{bmatrix} D+t & -1 & 1 \\ 0 & D - \frac{1}{t} & t \end{bmatrix} \in \mathcal{D}^{2\times 3},$$

where $\mathbb{K} = \mathbb{R}$. The Jacobson form is given by

$$URV = \begin{bmatrix} 1 & 0 & 0 \\ 0 & D + t - \frac{1}{t} & 0 \end{bmatrix},$$

where we may take

$$U = \begin{bmatrix} 1 & 0 \\ -t & 1 \end{bmatrix} \quad \text{and} \quad V = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & t \\ 1 & 1 & -D \end{bmatrix}.$$

Since R has the form $R = [DI - A, B]$ for some K-matrices A, B, we write $w = [x_1, x_2, -u]^T$; then the system $Rw = 0$ takes the form

$$\dot{x} = A(t)x(t) + B(t)u(t), \quad \text{where } A(t) = \begin{bmatrix} -t & 1 \\ 0 & \frac{1}{t} \end{bmatrix} \text{ and } B(t) = \begin{bmatrix} 1 \\ t \end{bmatrix}.$$

Since $d = D + t - \frac{1}{t}$ has degree one, this system is not controllable. Indeed, this can also be verified directly, because these equations imply

$$d(x_2 - tx_1) = 0,$$

which is an autonomous equation for $x_2 - tx_1$, in particular, it is fully decoupled from the input u. (To construct such relations systematically, note that $x_2 - tx_1 = [-t, 1, 0]w$, and $\xi = [-t, 1, 0]$ is the second row of $W = V^{-1}$. Thus $\xi \notin \mathrm{im}(\cdot R)$, but $d\xi \in \mathrm{im}(\cdot R)$, that is, $[\xi]$ is a torsion element of the system module $\mathcal{M}$.) Thus, on every interval I on which x_1, x_2 are smooth, we have

$$x_2(t) - tx_1(t) = cte^{-\frac{1}{2}t^2}$$

for some $c \in \mathbb{R}$. This shows that there exists a non-trivial relation between x_1 and x_2, which makes it intuitively clear that the system cannot be controllable (because not every configuration of x_1 and x_2 can be reached).

However, for every fixed $t_0 \in \mathbb{R} \setminus \{0\}$, the matrix pair $A = A(t_0) \in \mathbb{R}^{2\times 2}$, $B = B(t_0) \in \mathbb{R}^2$ is controllable, because its Kalman matrix is

$$K = \begin{bmatrix} 1 & 0 \\ t_0 & 1 \end{bmatrix}$$

which has rank 2 for any t_0. This corresponds to the fact that the Smith form of

$$R(t_0) = \begin{bmatrix} D + t_0 & -1 & 1 \\ 0 & D - \frac{1}{t_0} & t_0 \end{bmatrix} \in \mathbb{R}[D]^{2\times 3}$$

equals $[I, 0]$ for any $0 \neq t_0 \in \mathbb{R}$. This shows that the "snapshots" of a time-varying system (i.e., the time-invariant systems that result from "freezing" the system at some fixed t_0) will not provide sufficient information about the underlying time-varying system, in general. ◊

A.12 The tensor product

Let $\mathcal{D}$ be commutative, and let $\mathcal{M}$ and $\mathcal{A}$ be $\mathcal{D}$-modules. The tensor product is defined as

$$\mathcal{M} \otimes \mathcal{A} = \{\textstyle\sum_{i=1}^{k} m_i \otimes a_i \mid k \in \mathbb{N}, m_i \in \mathcal{M}, a_i \in \mathcal{A}\}$$

together with the laws

$$\begin{aligned}(m_1+m_2)\otimes a &= m_1\otimes a + m_2\otimes a\\ m\otimes(a_1+a_2) &= m\otimes a_1 + m\otimes a_2\\ dm\otimes a &= d(m\otimes a)\\ m\otimes da &= d(m\otimes a).\end{aligned}$$

Thus $\mathcal{M}\otimes\mathcal{A}$ becomes a $\mathcal{D}$-module. Similarly, if $f:\mathcal{M}\to\mathcal{N}$ is a $\mathcal{D}$-linear map between two $\mathcal{D}$-modules, we define

$$f\otimes\mathcal{A}:\mathcal{M}\otimes\mathcal{A}\to\mathcal{N}\otimes\mathcal{A},\quad \sum m_i\otimes a_i\mapsto\sum f(m_i)\otimes a_i.$$

Thus the tensor product becomes a covariant functor; see [3, Ch. II, §3] for more details.

Theorem A.12.1 *The tensor product is right exact, that is, if*

$$\mathcal{M}\stackrel{f}{\longrightarrow}\mathcal{N}\stackrel{g}{\longrightarrow}\mathcal{P}\longrightarrow 0$$

is an exact sequence of $\mathcal{D}$-modules, then

$$\mathcal{M}\otimes\mathcal{A}\stackrel{f\otimes\mathcal{A}}{\longrightarrow}\mathcal{N}\otimes\mathcal{A}\stackrel{g\otimes\mathcal{A}}{\longrightarrow}\mathcal{P}\otimes\mathcal{A}\longrightarrow 0$$

is also exact.

Proof: It is easy to see that $g\otimes\mathcal{A}$ is surjective: Let $\sum p_i\otimes a_i$ be given, then we have $p_i=g(n_i)$ for some n_i because of the surjectivity of g, and thus

$$\sum p_i\otimes a_i=\sum g(n_i)\otimes a_i=(g\otimes\mathcal{A})(\sum n_i\otimes a_i).$$

Also, the fact that $g\circ f=0$ implies that $(g\otimes\mathcal{A})\circ(f\otimes\mathcal{A})=0$, and hence we have $\operatorname{im}(f\otimes\mathcal{A})\subseteq\ker(g\otimes\mathcal{A})$. It remains to prove the converse inclusion. For this, consider

$$G:(\mathcal{N}\otimes\mathcal{A})/\operatorname{im}(f\otimes\mathcal{A})\to\mathcal{P}\otimes\mathcal{A},\quad [x]\mapsto(g\otimes\mathcal{A})(x)$$

where $x\in\mathcal{N}\otimes\mathcal{A}$ and $[x]$ is its residue class modulo the image of $f\otimes\mathcal{A}$. The map G is well-defined and surjective. We are finished if we can show that it is injective. For this, consider

$$H:\mathcal{P}\otimes\mathcal{A}\to(\mathcal{N}\otimes\mathcal{A})/\operatorname{im}(f\otimes\mathcal{A}),$$

which maps an element $\sum p_i\otimes a_i$ to $[\sum n_i\otimes a_i]$, where n_i is chosen such that $g(n_i)=p_i$. For well-definedness, we need to show: If $g(n_i^{(1)})=g(n_i^{(2)})=p_i$, then $[\sum n_i^{(1)} \otimes a_i] = [\sum n_i^{(2)} \otimes a_i]$. It suffices to show that $g(n) = 0$ implies $n \otimes a \in \mathrm{im}(f \otimes \mathcal{A})$. However, this follows from the exactness of the original sequence, which says that $g(n) = 0$ implies $n = f(m)$ and thus $n \otimes a = f(m) \otimes a = (f \otimes \mathcal{A})(m \otimes a) \in \mathrm{im}(f \otimes \mathcal{A})$. Finally, we have

$$H(G([\sum n_i \otimes a_i])) = H((g \otimes \mathcal{A})(\sum n_i \otimes a_i)) = H(\sum g(n_i) \otimes a_i) = [\sum n_i \otimes a_i]$$

which shows that $H \circ G$ is the identity map. This yields the desired result. □

Since we have $\mathcal{D} \otimes \mathcal{A} \cong \mathcal{A}$, or more generally, $\mathcal{D}^k \otimes \mathcal{A} \cong \mathcal{A}^k$, we have just shown that the exactness of

$$\mathcal{D}^q \xrightarrow{R} \mathcal{D}^g \xrightarrow{L} \mathcal{D}^l \longrightarrow 0$$

implies the exactness of

$$\mathcal{A}^q \xrightarrow{R} \mathcal{A}^g \xrightarrow{L} \mathcal{A}^l \longrightarrow 0.$$

The module $\mathcal{A}$ is called **flat** [2, Ch. I] if the tensor product $- \otimes \mathcal{A}$ is exact, that is, if the exactness of

$$\mathcal{M} \to \mathcal{N} \to \mathcal{P}$$

implies the exactness of

$$\mathcal{M} \otimes \mathcal{A} \to \mathcal{N} \otimes \mathcal{A} \to \mathcal{P} \otimes \mathcal{A}.$$

Theorem A.12.2 *$\mathcal{A}$ is flat if and only if for any exact sequence*

$$0 \to \mathcal{N} \hookrightarrow \mathcal{P}$$

the sequence

$$0 \to \mathcal{N} \otimes \mathcal{A} \to \mathcal{P} \otimes \mathcal{A}$$

is exact, that is, if the tensor product turns injections into injections.

Proof: The condition is clearly necessary. For sufficiency, let an exact sequence

$$\mathcal{M} \xrightarrow{f} \mathcal{N} \xrightarrow{g} \mathcal{P}$$

be given. Then the sequence

$$\mathcal{M} \xrightarrow{f} \mathcal{N} \xrightarrow{g_1} \mathrm{im}(g) \longrightarrow 0$$

is exact. The right exactness of the tensor product implies that

$$\mathcal{M} \otimes \mathcal{A} \xrightarrow{f \otimes \mathcal{A}} \mathcal{N} \otimes \mathcal{A} \xrightarrow{g_1 \otimes \mathcal{A}} \mathrm{im}(g) \otimes \mathcal{A} \longrightarrow 0$$

is exact. On the other hand, we have an exact sequence

$$0 \to \mathrm{im}(g) \hookrightarrow \mathcal{P}.$$

By assumption,

$$0 \to \mathrm{im}(g) \otimes \mathcal{A} \to \mathcal{P} \otimes \mathcal{A}$$

is also exact. Thus

$$\mathcal{M} \otimes \mathcal{A} \xrightarrow{f \otimes \mathcal{A}} \mathcal{N} \otimes \mathcal{A} \xrightarrow{g \otimes \mathcal{A}} \mathcal{P} \otimes \mathcal{A}$$

is also exact. □

It can be shown that the space of smooth functions with compact support

$$\mathcal{A}_0 = \mathcal{C}_0^\infty(\mathbb{R}^n, \mathbb{K})$$

is a flat $\mathcal{D}$-module, that is, the tensor product $- \otimes \mathcal{A}_0$ transforms injections into injections. The result of Lemma 5.1 is an example for this: If $R \in \mathcal{D}^{g \times q}$ has full column rank (that is, the map $\mathcal{D}^q \to \mathcal{D}^g$, $x \mapsto Rx$ is injective), then $Rw = 0$ has no non-zero solutions with compact support (that is, the map $\mathcal{A}_0^q \to \mathcal{A}_0^g$, $w \mapsto Rw$ is injective).

Since $\mathcal{A}_0$ is a flat module, the exactness of

$$\mathcal{D}^q \xrightarrow{R} \mathcal{D}^g \xrightarrow{L} \mathcal{D}^l$$

implies the exactness of

$$\mathcal{A}_0^q \xrightarrow{R} \mathcal{A}_0^g \xrightarrow{L} \mathcal{A}_0^l,$$

as stated in Theorem 2. In fact, $\mathcal{A}_0$ is even **faithfully flat**, that is, the exactness of the two sequences is actually equivalent. The same holds for $\mathcal{C}_0^\infty(\Omega, \mathbb{R})$, where $\Omega = \{x \in \mathbb{R}^n \mid \|x\| < r\}$ for some $r > 0$. This was needed for the interpretation of over-determined systems, that is, systems whose autonomy degree is at least one.

Let us summarize the categorical language used in this course: The contravariant Hom-functor $\mathrm{Hom}_{\mathcal{D}}(\cdot, \mathcal{A})$ is always left exact. It is exact if and only if $\mathcal{A}$ is injective. This can be reduced to showing that injections are transformed into surjections. If exactness is not only preserved, but also reflected, then $\mathcal{A}$ is an injective cogenerator.

For the sake of completeness, note that the covariant Hom-functor $\mathrm{Hom}_{\mathcal{D}}(\mathcal{M}, \cdot)$ is also left exact. It is exact if and only if $\mathcal{M}$ is projective. For this, the crucial point is to show that surjections become surjections under this functor. If exactness is not only preserved, but also reflected, then $\mathcal{M}$ is a projective generator.

Finally, the tensor product $- \otimes \mathcal{A}$ is a covariant functor which is always right exact. We call $\mathcal{A}$ flat if it is exact, and for this, we need to show that injections are turned into injections. If exactness is not only preserved, but also reflected, then $\mathcal{A}$ is called faithfully flat.

Bibliography

[1] T. Becker, V. Weispfenning. Gröbner Bases. Springer, 1993.

[2] N. Bourbaki. Commutative Algebra. Hermann, 1972.

[3] N. Bourbaki. Algebra. Hermann, 1974.

[4] F. Chyzak, A. Quadrat, D. Robertz. Linear Control Systems over Ore Algebras. *Proceedings of the IFAC Workshop on Time-Delay Systems* (2003).

[5] P. M. Cohn. Free Rings and their Relations. Academic Press, 1971.

[6] D. Eisenbud. Commutative Algebra with a View Toward Algebraic Geometry. Springer, 1995.

[7] K. R. Goodearl, R. B. Warfield, Jr. An Introduction to Noncommutative Noetherian Rings. Cambridge University Press, 1989.

[8] N. Jacobson. The Theory of Rings. American Mathematical Society, 1943.

[9] J. P. Jans. Rings and Homology. Holt, Rinehart and Winston, 1964.

[10] F. Kasch. Moduln und Ringe. Teubner, 1977.

[11] T. Y. Lam. Serre's Conjecture. Springer, 1978.

[12] T. Y. Lam. Lectures on Modules and Rings. Springer, 1999.

[13] T. Y. Lam. On the Equality of Row Rank and Column Rank. *Expositiones Mathematicae* 18, 161–163 (2000).

[14] B. Malgrange. Systèmes Différentiels à Coefficients Constants. *Séminaire Bourbaki* 15, No. 246 (1964).

[15] D. G. Northcott. A First Course of Homological Algebra. Cambridge University Press, 1973.

[16] D. G. Northcott. Finite Free Resolutions. Cambridge University Press, 1976.

[17] U. Oberst. Multidimensional Constant Linear Systems. *Acta Applicandae Mathematicae* 20, 1–175 (1990).

[18] V. P. Palamodov. Linear Differential Operators with Constant Coefficients. Springer, 1970.

[19] H. K. Pillai, S. Shankar. A Behavioral Approach to Control of Distributed Systems. *SIAM J. Control Optim.* 37, 388–408 (1999).

[20] J. W. Polderman, J. C. Willems. Introduction to Mathematical Systems Theory. Springer, 1998.

[21] J.-F. Pommaret, A. Quadrat. Algebraic Analysis of Linear Multidimensional Control Systems. *IMA J. Math. Control Inf.* 16, 275–297 (1999).

[22] J.-F. Pommaret, A. Quadrat. Equivalences of Linear Control Systems. *Proceedings of the Symposium on Mathematical Theory of Networks and Systems* (2000).

[23] W. Walter. Einführung in der Theorie der Distributionen. B. I. Wissenschaftsverlag, 1974.

[24] J. C. Willems. Paradigms and Puzzles in the Theory of Dynamical Systems. *IEEE Trans. Autom. Control* 36, 259–294 (1991).