Discussiones Mathematicae
General Algebra and Applications 26(2006) 21–43

UNIQUE PRIME FACTORIZATION IN A PARTIAL SEMIGROUP OF MATRIX-POLYNOMIALS

Michael Kaltenbäck and Harald Woracek

Institute for Analysis and Scientific Computing
Vienna University of Technology
Wiedner Hauptstr. 8–10/101, A–1040 Wien, Austria

e-mail: michael.kaltenbaeck@tuwien.ac.at
e-mail: harald.woracek@tuwien.ac.at

Abstract

We establish a unique factorization result into irreducibel elements in the partial semigroup of 2×2-matrices with entries in $K[x]$ whose determinant is equal to 1, where K is a field, and where multiplication is defined as the usual matrix-multiplication if the degrees of the factors add up. This investigation is motivated by a result on matrices of entire functions.

Keywords: partial semigroup, unique prime factorization.

2000 Mathematics Subject Classification: 20M10, 08A55, 15A23.

1. Introduction

Let K be a field. We consider divisability and factorization into irreducibel elements in the partial semigroup of 2×2-matrices with entries in $K[x]$ and determinant 1, where multiplication is defined as matrix-multiplication if the degrees of the factors add up, cf. Section 2. Our aim is to establish a unique factorization result, cf. Theorem 3.1.

Although our considerations are purely algebraic and in fact quite elementary, they should be seen in connection with some results of complex analysis. Let us explain this motivation: Let $W(z) = (w_{ij}(z))_{i,j=1,2}$ be a 2×2-matrix function whose entries are entire functions, i.e. are defined and holomorphic in the whole complex plane.

We say that W belongs to the class $\mathcal{M}_\kappa$ where κ is a nonnegative integer, if $w_{ij}(\overline{z}) = \overline{w_{ij}(z)}$, $W(0) = I$, $\det W(z) = 1$, and if the kernel

$$K_W(w,z) := \frac{W(z)JW(w)^* - J}{z - \overline{w}}$$

has κ negative squares. There by

$$J := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

The latter condition means that for every choice of $n \in \mathbb{N}$, $z_1, \dots, z_n \in \mathbb{C}$, $a_1, \dots, a_n \in \mathbb{C}^2$, the quadratic form

$$Q(\xi_1, \dots, \xi_n) := \sum_{l,k=1}^{n} \Big(K_W(z_k, z_l)a_l, a_k \Big)_{\mathbb{C}^2} \xi_l \overline{\xi_k}$$

has at most κ negative squares and that this bound is actually attained for some choice of n, z_l, a_l.

The following result lies at the core of the theory of L. de Branges on Hilbert spaces of entire functions [1] and its generalization to the Pontryagin space setting [4, 5, 6].

Maximal Chain Theorem:
Let $W \in \mathcal{M}_\kappa$ be given. Then there exists a (essentially unique) family $(W_i)_{i\in\mathcal{I}}$ of entire 2×2-matrix functions, where the index set $\mathcal{I}$ is of the form $\mathcal{I} = [0,1] \setminus \{\sigma_1, \dots, \sigma_n\}$, $\sigma_i \in (0,1)$, such that

(i) $W_0 = I$, $W_1 = W$.

(ii) $W_i \in \mathcal{M}_{\kappa(i)}$ and $\kappa(i)$ is a nondecreasing function of i which is constant on each connected component of $\mathcal{I}$.

(iii) If $i, j \in \mathcal{I}$, $i \le j$, then $W_i^{-1} W_j \in \mathcal{M}_{\kappa(j)-\kappa(i)}$.

(iv) If $j \in \mathcal{I}$ and $M \in \mathcal{M}_\nu$, $\nu \le \kappa(j)$, is such that $M^{-1}W_j \in \mathcal{M}_{\kappa(j)-\nu}$, then $M = W_i$ for some $i \in \mathcal{I}$, $i \le j$.

This result tells us, in particular, that the family $(W_i)_{i\in\mathcal{I}}$ gives all possible factorizations $W = M \cdot \hat{M}$ so that the number of negative squares add up ($\hat{M} = M^{-1}W$).

If $W(z)$ is a 2×2-matrix function whose entries are polynomials with real coefficients, $W(0) = I$ and $\det W(z) = 1$, then the number of negative squares of K_W is finite, in fact it is less than or equal to the maximal degree of an entry of W, cf. [4]. The simplest example is a matrix polynomial with degree 1. Due to the conditions $W(0) = I$ and $\det W(z) = 1$ those matrix polynomials are of the form ($l \in \mathbb{R}, \phi \in [0, \pi)$)

$$W_{(l,\phi)} := \begin{pmatrix} 1 - lz \sin\phi\cos\phi & lz\cos^2\phi \\ -lz\sin^2\phi & 1 + lz\sin\phi\cos\phi \end{pmatrix} .$$

For a matrix polynomial W the chain $(W_i)_{i\in\mathcal{I}}$ given by the Maximal Chain Theorem is of a particularly simple form: There exist unique matrix polynomials M_k, $k = 1, \ldots, n$, with $M_k \in \mathcal{M}_{\nu_k}$, values $\phi_k \in [0, \pi)$ and indices $i_k \in \mathcal{I}$ with $i_k < i_{k+1}$, such that

(i)
$$M_1 \cdot \ldots \cdot M_k = W_{i_k},\ k = 1, \ldots, n\,,$$
$$i_n = 1,\ \text{i.e.}\ M_1 \cdot \ldots \cdot M_n = W\,.$$

(ii) If $i_{k-1} \le i \le i_k$ then for some $l, l' \in \mathbb{R}$,
$$W_i^{-1} W_{i_k} = W_{(l,\phi_k)},\ W_{i_{k-1}}^{-1} W_i = W_{(l',\phi_k)}.$$

There by $k = 1, \ldots, n$ and we have put $i_0 := 0$.

The factorization $W = M_1 \cdot \ldots \cdot M_n$ has the property that degrees add up: For a matrix polynomial P denote by δP the maximal degree of one of its entries. Then

$$\delta W = \delta M_1 + \ldots + \delta M_n\,.$$

In fact, it is characterized by this property: If $W = \hat{M}_1 \cdot \ldots \cdot \hat{M}_m$ is any factorization of W into matrix polynomials with $\hat{M}_i(0) = I$, $\det \hat{M}_i(z) = 1$, such that $\delta W = \delta \hat{M}_1 + \ldots + \hat{M}_m$, then $n = m$ and $\hat{M}_i = M_i$, $i = 1, \ldots, n$. We conclude in particular that the following result holds true:

Unique Factorization Theorem:
Let W be a 2×2-matrix polynomial with real coefficients, $W(0) = I$ and $\det W(z) = 1$. Then there exists a unique number $n \in \mathbb{N}$ and unique 2×2-matrix polynomials $M_1, \ldots, M_n$ with real coefficients, $M_i(0) = I$ and $\det M_i(z) = 1$, such that

$$W = M_1 \cdot \ldots \cdot M_n, \ \delta W = \delta M_1 + \ldots + \delta M_n \,,$$

and no M_i can be further decomposed.

It was noted by A. Dijksma (personal communication, see also [3]) that this fact can also be proved without employing the deep machinery of L. de Branges theory and the Maximal Chain Theorem. In fact, the desired factorization of a matrix polynomial can be constructed with the help of the so-called Schur algorithm, first invented by I. Schur in the study of some classical interpolation and moment problems.

Although the proof of the stated Maximal Chain Theorem relies heavily on the theory of analytic functions, it seems to be promising to try to generalize the Maximal Chain Theorem to matrix functions with values in fields different to the complex number field, e.g. in a locally compact field. Of course then in particular a similar Unique Factorization Theorem would have to hold. It is therefore a noteworthy fact that the Unique Factorization Theorem actually is true for 2×2-matrix polynomials over arbitrary fields. It is the aim of this note to establish this result.

We give a purely algebraic and elementary proof of the Unique Factorization Theorem for 2×2-matrix polynomials with coefficients in an arbitrary field K based on the euclidean algorithm in the polynomial ring $K[x]$. It is seen that the Unique Factorization Theorem boils down to the fact that the greatest common divisor of two polynomials a, b can be written as a linear combination of a and b and that the coefficients of this linear combination can be constructed explicitly from the factors and remainders in the euclidean algorithm.

In the particular case $K = \mathbb{R}$ our result gives another proof of the above stated Unique Factorization Theorem. It is worth to be noted that the previous approaches to factorization in the case $K = \mathbb{R}$, via the theory of de Branges spaces or via the Schur algorithm, involve deep methods of complex analysis, whereas the proof obtained as a specialization of the present Theorem 3.1 is completely elementary.

A possible direction of future work is also motivated from recent developments in the theory of the Schur algorithm. In fact a factorization result for rational matrix functions with real coefficients which is obtained via the Schur algorithm was recently communicated to the authors by Aad Dijksma. It seems a promising task to find a similar factorization theorem for rational matrix functions over arbitrary fields. Another direction of future development could be motivated from [2] where a factorization theorem for a certain class of rational matrix functions over the complex field is given. There by this class of functions is related to the unit circle in a similar way as the class of real matrix functions is related to the real axis. Thus it seems likely that the present result can be carried over.

2. The partial semigroup $(\mathcal{S}, \cdot)$

Let K be a field and let $\mathcal{M}(2, K[x])$ be the ring of 2×2-matrices whose entries are elements of the polynomial ring $K[x]$. For $p \in K[x]$ denote by $\deg p$ the degree of p where we put $\deg 0 := -\infty$. We will use in the sequel that the function $\deg : K[x] \to \mathbb{N}_0 \cup \{-\infty\}$ satisfies

$$\deg(p_1 + p_2) \leq \max\{\deg p_1, \deg p_2\},$$

where strict inequality can hold only if $\deg p_1 = \deg p_2$, and that

$$\deg(p_1 \cdot p_2) = \deg p_1 + \deg p_2,$$

where $-\infty + n = n + (-\infty) = -\infty + (-\infty) = -\infty$.

Let $A \in \mathcal{M}(2, K[x])$ and write

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

We define the degree δA of A as

$$\delta A := \max\{\deg a, \deg b, \deg c, \deg d\}\,.$$

Note that δA is nothing else but the degree of A if we identify $\mathcal{M}(2, K[x])$ canonically with $\mathcal{M}(2, K)[x]$. We clearly have

$$\delta(AB) \le \delta A + \delta B,\ \ A, B \in \mathcal{M}(2, K[x])\,.$$

Consider the set $\mathcal{S} := \{A \in \mathcal{M}(2, K[x]) : \det A = 1\}$. Then $\mathcal{S}$ is closed with respect to matrix multiplication and, by Cramers rule, with respect to taking inverses. We will endow $\mathcal{S}$ with the partially defined binary operation

$$\cdot : \begin{cases} \mathcal{D} \subseteq \mathcal{S} \times \mathcal{S} & \to & \mathcal{S} \\ (A, B) & \mapsto & AB \end{cases}$$

where

$$\mathcal{D} := \{(A, B) \in \mathcal{S} \times \mathcal{S} :\ \delta(AB) = \delta A + \delta B\}\,.$$

For further reference let us collect a couple of elementary properties of $(\mathcal{S}, \cdot)$.

Lemma 2.1. *We have*

(i) *If $A \in \mathcal{S}$ then $\delta A \ge 0$.*

(ii) *If $A, B, C \in \mathcal{S}$ and $B \cdot C$ as well as $A \cdot (B \cdot C)$ are defined, then also $A \cdot B$ and $(A \cdot B) \cdot C$ are defined and*

$$A \cdot (B \cdot C) = (A \cdot B) \cdot C.$$

(iii) *Denote by I the 2×2-identity matrix. Then for all $A \in \mathcal{S}$ we have $(A, I), (I, A) \in \mathcal{D}$ and*

$$A \cdot I = I \cdot A = A.$$

(iv) *Put* $\mathcal{S}^\times := \{U \in \mathcal{S} : (U, U^{-1}) \in \mathcal{D}\}$. *Then* $\mathcal{S}^\times = \{U \in \mathcal{S} : \delta U = 0\}$. *If* $U \in \mathcal{S}^\times$, *then for all* $A \in \mathcal{S}$ *we have* $(U, A), (A, U) \in \mathcal{D}$. *Hence* $(\mathcal{S}^\times, \cdot)$ *is a (totally defined) subgroup of* $\mathcal{S}$, *the subgroup of units of* $(\mathcal{S}, \cdot)$.

(v) *If* $A, B, C \in \mathcal{S}$, $(A, C), (B, C) \in \mathcal{D}$, *and* $A \cdot C = B \cdot C$, *then* $A = B$. *Similarly the left-cancellation law holds.*

Proof.

Ad (i): Obvious, since $0 \notin \mathcal{S}$.

Ad (ii): By assumption

$$\delta[A(BC)] = \delta A + \delta(BC) = \delta A + \delta B + \delta C.$$

It follows that

$$\delta[A(BC)] = \delta[(AB)C] \leq \delta(AB) + \delta C \leq$$

$$\leq \delta A + \delta B + \delta C = \delta[A(BC)].$$

Hence $\delta(AB) = \delta A + \delta B$ and $\delta[(AB)C] = \delta(AB) + \delta C$.

Ad (iii): Obvious.

Ad (iv): If $(U, U^{-1}) \in \mathcal{D}$, then $0 = \delta I = \delta(UU^{-1}) = \delta U + \delta(U^{-1})$. This is only possible if $\delta U = 0$. Conversely, assume that $\delta U = 0$. Then also $\delta U^{-1} = 0$ and we obtain

$$0 = \delta I = \delta U + \delta(U^{-1}).$$

Let $A \in \mathcal{S}$, $U \in \mathcal{S}^\times$. Then

$$\delta A = \delta[(AU)U^{-1}] \leq \delta(AU) + \delta\left(U^{-1}\right) =$$

$$= \delta(AU) \leq \delta A + \delta U = \delta A\,,$$

and hence $\delta(AU) = \delta A + \delta U$. The fact that $(U, A) \in \mathcal{D}$ follows in the same way.

Ad (v): Obvious, since $\mathcal{S}$ contains only invertible matrices. ■

Remark 2.2. Note that $(A, B) \in \mathcal{D}$ not necessarily implies $(B, A) \in \mathcal{D}$, as is seen from the example

$$A = \begin{pmatrix} 1+x^2 & x \\ x & 1 \end{pmatrix} \ , \ B = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \ .$$

Notational Convention:
We agree that, whenever we use the notation $A \cdot B$, this implies that $(A, B) \in \mathcal{D}$.

The following property plays a technically important role: We say that a matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{S} \tag{2.1}$$

satisfies the property (D) , if $\deg b > \deg a$.

Lemma 2.3. *Let $A \in \mathcal{S}$ be written as in* (2.1).

(i) *Assume that $a, b, c, d \neq 0$. Then*

$$\deg d - \deg c = \deg b - \deg a \tag{2.2}$$

(ii) *Assume that $\delta A > 0$. Then A satisfies* (D) *if and only if* $\deg d > \deg c$.

Proof.
Ad (i): If $\delta A = 0$, the desired relation trivially holds true. Hence assume that $\delta A > 0$. Since $a, b, c, d \neq 0$, in this case at least one of $\deg(ad)$ and $\deg(bc)$ is greater than 0. It follows from $ad - bc = \det A = 1$ that $\deg(ad) = \deg(bc)$, and hence that (2.2) holds.

Ad (ii): Assume that A satisfies (D) . If $a = 0$, we have $-bc = 1$, and hence $\deg b = \deg c = 0$. Since $\delta A > 0$, we obtain $\deg d > 0$, and thus $\deg d > \deg c$. If $c = 0$, we have $ad = 1$, and hence $\deg a = \deg d = 0$. Thus also in this case $\deg d > \deg c$. It remains to consider the case that $a, c \neq 0$. Then, by (D) , $\deg b > 0$ and hence also $\deg(bc) > 0$. Since $ad - bc = 1$, and hence the desired conclusion follows, in fact (2.2) holds.

The converse implication follows in the same way. ∎

The validity of (D) can always be achieved by multiplying with units:

Lemma 2.4. *Let $A \in \mathcal{S}$, $\delta A > 0$, be given. Then there exist $U, V \in \mathcal{S}^\times$ such that VAU satisfies* (D) *. Let A be written as in* (2.1)*. If $b \neq 0$, we can choose $V = I$. If $c = 0$, we can choose $U = V = I$. If $b = 0$, we can choose $V = U = J$, where*

$$J := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Assume that A satisfies (D) *and $U \in \mathcal{S}^\times$. Then AU satisfies* (D) *if and only if U is upper triangular.*

Proof. If $c = 0$, we have $\deg a = \deg d = 0$, and since $\delta A > 0$, this implies that $\deg b > 0$. Thus A satisfies (D) . If $b = 0$, the same argument yields $\deg a = \deg d = 0$ and $\deg c > 0$. Hence

$$JAJ = \begin{pmatrix} -d & c \\ 0 & -a \end{pmatrix}$$

satisfies (D).

It remains to consider the case that $b, c \neq 0$.

Case 1. $\deg b > \deg a$ or $\deg d > \deg c$: Then we can, by Lemma 2.3,(ii), choose $U = V = I$.

Case 2. $\deg b < \deg a$ or $\deg d < \deg c$: Then Case 1 can be applied to the matrix

$$AJ = \begin{pmatrix} b & -a \\ d & -c \end{pmatrix}$$

and we see that we can choose $V = I$, $U = J$.

Case 3. $\deg b = \deg a$ and $\deg d = \deg c$: Choose $\lambda \in K$ such that $\deg(a + \lambda b) < \deg a = \deg b$. Then

$$A\begin{pmatrix}1 & 0\\ \lambda & 1\end{pmatrix} = \begin{pmatrix}a+\lambda b & b\\ c+\lambda d & d\end{pmatrix}$$

satisfies (D) , i.e. we can choose $V = I$ and

$$U = \begin{pmatrix}1 & 0\\ \lambda & 1\end{pmatrix}.$$

We come to the proof of the uniqueness statement. Write $U \in \mathcal{S}^\times$ as

$$U = \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}.$$

Then

$$AU = \begin{pmatrix}\alpha a+\gamma b & \beta a+\delta b\\ \alpha c+\gamma d & \beta c+\delta d\end{pmatrix}.$$

Hence in order that AU satisfies (D) it is necessary and sufficient that $\gamma = 0$.

■

The next statement is an important step towards factorization results.

Proposition 2.5. *Let $A \in \mathcal{S}$. Assume that for some $p \in K[x]$, $\deg p > 0$, and $A_1 \in \mathcal{S}$ the matrix A can be factorized as*

$$A = A_1 \cdot \begin{pmatrix}1 & p\\ 0 & 1\end{pmatrix}. \tag{2.3}$$

Then A satisfies (D) *and $\delta A > 0$. Conversely, if A satisfies* (D) *and $\delta A > 0$, then there exists a unique polynomial p with $p(0) = 0$, and a unique element $A_1 \in \mathcal{S}$, such that A factorizes as in* (2.3).

Proof. Assume that A factorizes as in (2.3). Clearly $\delta A > 0$. The relation (2.3) writes explicitly as

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a_1 & pa_1 + b_1 \\ c_1 & pc_1 + d_1 \end{pmatrix}.$$

Since

$$\delta A = \delta A_1 + \deg p > \delta A_1 \geq \max\{\deg a_1, \deg c_1\}$$

we have either $\deg b > \deg a$ or $\deg d > \deg c$, and hence see that A satisfies (D), cf. Lemma 2.3, (ii) .

Let A be given, $\delta A > 0$, such that (D) holds. We show existence of a factorization (2.3).

Case 1. $c = 0$: Then $\deg a = \deg d = 0$, $\deg b = \delta A > 0$, and thus

$$A = \begin{pmatrix} a & b(0) \\ 0 & d \end{pmatrix} \cdot \begin{pmatrix} 1 & \frac{b-b(0)}{a} \\ 0 & 1 \end{pmatrix}$$

is a factorization of the desired form.

Case 2. $a = 0$: Apply Case 1 to the matrix

$$JA = \begin{pmatrix} -c & -d \\ 0 & b \end{pmatrix}$$

to obtain

$$JA = A_1 \cdot \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}.$$

Then

$$A = (-JA_1) \cdot \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}$$

is a factorization of A of the desired form (2.3).

Case 3. $a, c \neq 0$: Choose $p, r \in K[x]$ with $p(0) = 0$, $\deg r \leq \deg a$, such that $b = pa + r$. Define

$$A_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} := A \begin{pmatrix} 1 & -p \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & r \\ c & d - pc \end{pmatrix}.$$

It follows that $\deg(d - pc) \leq \deg c$: For if $\deg(d - pc) = 0$, this relation is true since $c \neq 0$, and if $\deg(d - pc) > 0$, we must have $r \neq 0$ and by Lemma 2.3, (i) ,

$$\deg(d - pc) - \deg c = \deg r - \deg a \leq 0\,.$$

We conclude that

$$\delta A_1 = \max\{\deg a, \deg c\}\,.$$

Since

$$\deg(b - pa) = \deg r \leq \deg a < \deg b$$

we must have $\deg b = \deg(pa)$. Similarly, $\deg(d - pc) \leq \deg c < \deg d$, cf. Lemma 2.3, (ii) , and thus $\deg d = \deg(pc)$. Alltogether, we conclude that

$$\delta A_1 + \deg p = \max\{\deg a, \deg c\} + \deg p$$

$$= \max\{\deg(pa), \deg(pc)\} = \max\{\deg b, \deg d\} = \delta A.$$

Hence, A_1 and p yield a factorization of the desired form.

Finally, let us prove uniqueness. If $p \in K[x]$, $p(0) = 0$, and $A_1 \in \mathcal{S}$, are such that A factorizes as in (2.3), then $a_1 = a$, $c_1 = c$, $b = pa_1 + b_1$, $d = pc_1 + d_1$.

We have $\delta A = \max\{\deg b, \deg d\}$. Say $\delta A = \deg b$; the case $\delta A = \deg d$ can be treated in the same way. Then

$$\deg b = \delta A = \delta A_1 + \deg p \geq \deg b_1 + \deg p\,.$$

Hence $\deg b > \deg b_1$, and we see that $\deg b = \deg(pa_1)$. In particular, $a_1 \neq 0$. Moreover,

$$\deg p + \deg a_1 = \deg b \geq \deg b_1 + \deg p\,,$$

and hence $\deg b_1 \leq \deg a_1$. Thus $p \in K[x]$, is such that $p(0) = 0$ and $\deg(b - pa) \leq \deg a$. By this condition, however, p is determined uniquely. Clearly with p also A_1 is determined uniquely. ∎

3. The unique factorization theorem

An element $B \in \mathcal{S}$, $\delta B > 0$, is called irreducible if for all $A, A' \in \mathcal{S}$ with $B = A \cdot A'$ we must have $A \in \mathcal{S}^\times$ or $A' \in \mathcal{S}^\times$. This amounts to saying that for any $A, A' \in \mathcal{S}$ with $B = AA'$ and $\delta B = \delta A + \delta A'$ necessarily $\delta A = 0$ or $\delta A' = 0$.

Let us define a relation $\sim$ on $\mathcal{S}$ by

$$A \sim B : \iff \exists\, U, V \in \mathcal{S}^\times : A = U \cdot B \cdot V.$$

By Lemma 2.1, $\sim$ is an equivalence relation. Clearly, the set of all irreducible elements is saturated with respect to the relation $\sim$.

In the following theorem, which basically follows from the euclidean algorithm in $K[x]$, we characterize the set of irreducible elements (up to $\sim$) and show that every element of $\mathcal{S}$ can be factorized uniquely (up to $\sim$) into irreducibles. There by item (iii) is exactly the general version of the Unique Factorization Theorem mentioned in the introduction.

Theorem 3.1. *We have*

(i) *An element $B \in \mathcal{S}$ is irreducible if and only if there exists $p \in K[x]$, $p(0) = 0$, such that*

$$B \sim \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}.$$

(i) *Let $A \in \mathcal{S}$, $\delta A > 0$. Then there exist $n \in \mathbb{N}$ and $W_1, \ldots, W_n$, $\delta W_i > 0$, irreducible in $\mathcal{S}$, such that*

$$A = W_1 \cdot \ldots \cdot W_n.$$

If $A = \hat{W}_1 \cdot \ldots \cdot \hat{W}_m$ is another factorization of A into irreducibles in $\mathcal{S}$, $\delta\hat{W}_i > 0$, then $n = m$ and $W_i \sim \hat{W}_i$, $i = 1, \ldots, n$.

(i) *Assume that $A \in \mathcal{S}$, $\delta A > 0$, $A(0) = I$. Then there exists a unique number $n \in \mathbb{N}$ and unique irreducible elements W_i, $i = 1, \ldots, n$, $\delta W_i > 0$, $W_i(0) = I$, such that $A = W_1 \cdot \ldots \cdot W_n$.*

For the sake of completeness let us remark that the case of matrices A or B with $\delta A = 0$ or $\delta B = 0$, respectively, is trivial.

The rest of this section is devoted to the proof of Theorem 3.1, which will be carried out in several steps.

Proof. (of (i), sufficiency) We show that whenever $p \in K[x]$, $\deg p > 0$, the matrix

$$B := \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}$$

is irreducible.

Assume on the contrary that $B = AA'$ where $(A, A') \in \mathcal{D}$ and $\delta A, \delta A' > 0$. From $\delta B = \delta A + \delta A'$ it thus follows that $\delta A, \delta A' < \delta B$. Write

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \ A' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$$

so that

$$B = \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}.$$

First note that

$$c' = c'(cb' + dd') - d'(ca' + dc') = c(c'b' - d'a') = -c$$

and that

$$d = d(aa' + bc') - b(ca' + dc') = a'(da - bc) = a'.$$

Next let us exclude the cases that one of the entries of A or A' is equal to 0.

Assume that $b = 0$. Then $\deg a = \deg d = 0$ and $p = ab'$. Thus $\delta B = \deg p = \deg b' \leq \delta A'$, and we have reched a contradiction. The cases that either of a, b' or d' vanishes can be excluded in the same way.

Assume that c, and with it also c', is equal to 0. Then a, d, a', d' are nonzero constants. Hence

$$\delta B = \deg p = \deg(ab' + bd') \leq \max\{\deg b', \deg b\} \leq$$

$$\leq \max\{\delta A', \delta A\} < \delta B\,,$$

and again we obtained a contradiction. The case that d, and with it also a', vanishes is treated in the same way.

If $U \in \mathcal{S}^\times$, then

$$B = (AU^{-1}) \cdot (UA')$$

is again a factorization with $\delta(AU^{-1}), \delta(UA') > 0$.

From the above elaborations and the Lemmata 2.3, 2.4, we conclude that it can be assumed without loss of generality that all entries of A and A' are nonzero and that

$$\deg b - \deg a = \deg d - \deg c > 0.$$

In particular then $\deg b, \deg d > 0$.

It follows from $1 = aa' + bc'$ and $1 = cb' + dd'$ that

$$\deg a + \deg a' = \deg b + \deg c'\,,\ \deg c + \deg b' = \deg d + \deg d'\,.$$

Summing up and using that $c' = -c$, $d = a'$, we obtain

$$\deg a + \deg b' = \deg b + \deg d'\,.$$

We obtain a contradiction:

$$\delta B = \deg p = \deg(ab' + bd') \leq \max\{\deg(ab'), \deg(bd')\}$$

$$= \deg a + \deg b' < \deg b + \deg b' \leq \delta A + \delta A'\,.$$

■

Proof. (of (ii), existence) In fact the existence of a factorization of A into irreducibles is clear, either by a descending chain argument or by inductive

application of Proposition 2.5. However, we shall establish an algorithmic way to obtain a factorization of a specific form.

Let $A \in \mathcal{S}$ be given and write A as in (2.1). Since $\det A = 1$, we have $\gcd\{a, b\} = 1$. Define $n \in \mathbb{N}$ and polynomials $r_{-1}, r_0, \dots, r_n$, $p_1, \dots, p_n$ by carrying out the euclidean algorithm for (a, b):

$$r_{-1} := b,\ r_0 := a\,,$$

$$r_{k-2} = p_k r_{k-1} + r_k,\ k = 1, \dots, n\,,$$

where $\deg r_k < \deg r_{k-1}$, $k = 1, \dots, n$. There by let $n \in \mathbb{N}$ be such that r_n is the first vanishing remainder, so that we have $\deg r_{n-1} = 0$.

Define matrices V_k, D_k, $k = 1, \dots, n$, by

$$V_k := \begin{cases} \begin{pmatrix} 1 & -p_k \\ 0 & 1 \end{pmatrix}, & k \text{ odd} \\ \\ \begin{pmatrix} 1 & 0 \\ -p_k & 1 \end{pmatrix}, & k \text{ even} \end{cases}$$

$$D_k := A \cdot V_1 \cdot \ldots \cdot V_k\,.$$

We show that for all $k = 1, \dots, n$

$$(1, 0)D_k = \begin{cases} (r_{k-1}, r_k)\,, & k \text{ odd} \\ (r_k, r_{k-1})\,, & k \text{ even.} \end{cases}$$

For $k = 1$ we have

$$(1, 0)D_1 = (1, 0)AV_1 = (a, b)\begin{pmatrix} 1 & -p_1 \\ 0 & 1 \end{pmatrix}$$

$$= (r_0, r_{-1})\begin{pmatrix} 1 & -p_1 \\ 0 & 1 \end{pmatrix} = (r_0, -p_1 r_0 + r_{-1}) = (r_0, r_1).$$

Let $1 < k \leq n$ be given and assume that the assertion for $(1,0)D_{k-1}$ has already been proved.

Case k odd: Then $k-1$ is even and we obtain

$$(1,0)D_k = (1,0)D_{k-1}V_k = (r_{k-1}, r_{k-2}) \begin{pmatrix} 1 & -p_k \\ 0 & 1 \end{pmatrix}$$

$$= (r_{k-1}, -p_k r_{k-1} + r_{k-2}) = (r_{k-1}, r_k)\,.$$

Case k even: Then $k-1$ is odd and thus

$$(1,0)D_k = (1,0)D_{k-1}V_k = (r_{k-2}, r_{k-1}) \begin{pmatrix} 1 & 0 \\ -p_k & 1 \end{pmatrix}$$

$$= (r_{k-2} - p_k r_{k-1}, r_{k-1}) = (r_k, r_{k-1})\,.$$

Consider the matrix D_n. Since $\det D_n = 1$, we must have

$$D_n = \begin{cases} \begin{pmatrix} r_{n-1} & 0 \\ q & \dfrac{1}{r_{n-1}} \end{pmatrix}, & n \text{ odd} \\ \begin{pmatrix} 0 & r_{n-1} \\ -\dfrac{1}{r_{n-1}} & q \end{pmatrix}, & n \text{ even} \end{cases}$$

for some polynomial q.

We have found a factorization of A in $\mathcal{M}(2, K[x])$, in fact

$$A = D_n V_n^{-1} \cdot \ldots \cdot V_1^{-1}. \tag{3.1}$$

We can write

$$D_n = U \begin{pmatrix} 1 & -\dfrac{q}{r_{n-1}} \\ 0 & 1 \end{pmatrix} U'$$

with

$$U := -J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ U' := \begin{cases} \begin{pmatrix} 0 & -\dfrac{1}{r_{n-1}} \\ r_{n-1} & 0 \end{pmatrix}, & n \text{ odd} \\ \begin{pmatrix} \dfrac{1}{r_{n-1}} & 0 \\ 0 & r_{n-1} \end{pmatrix}, & n \text{ even} \end{cases}$$

Moreover,

$$V_k^{-1} = \begin{cases} \begin{pmatrix} 1 & p_k \\ 0 & 1 \end{pmatrix}, & k \text{ odd} \\ U \begin{pmatrix} 1 & -p_k \\ 0 & 1 \end{pmatrix} U', & k \text{ even} \end{cases}$$

where $U = U' = J$.

We have $\delta(V_k^{-1}) = \deg p_k$ and in the euclidean algorithm

$$\max\{\deg a, \deg b\} = \deg p_1 + \ldots + \deg p_n\,.$$

Since (with appropriate $\hat{c}, \hat{d}$)

$$V_n^{-1} \cdot \ldots \cdot V_1^{-1} = D_n^{-1} A = \begin{cases} \begin{pmatrix} \dfrac{1}{r_{n-1}} a & \dfrac{1}{r_{n-1}} b \\ \hat{c} & \hat{d} \end{pmatrix}, & n \text{ odd} \\ \begin{pmatrix} -\hat{c} & -\hat{d} \\ \dfrac{1}{r_{n-1}} a & \dfrac{1}{r_{n-1}} b \end{pmatrix}, & n \text{ even} \end{cases} \tag{3.2}$$

we obtain

$$\max\{\deg a, \deg b\} \le \delta(V_n^{-1} \cdot \ldots \cdot V_1^{-1}) \le \deg(V_n^{-1}) + \ldots + \delta(V_1^{-1})$$

$$= \deg p_n + \ldots + \deg p_1 = \max\{\deg a, \deg b\}\,.$$

This means that the product $V_n^{-1} \cdot \ldots \cdot V_1^{-1}$ is defined in $\mathcal{S}$. Moreover, $\delta(D_n^{-1}A) = \max\{\deg a, \deg b\}$, and hence in (3.2)

$$\max\{\deg \hat{c}, \deg \hat{d}\} \le \max\{\deg a, \deg b\}.$$

We have

$$A = D_n(D_n^{-1}A) = \begin{cases} \begin{pmatrix} r_{n-1} & 0 \\ q & \dfrac{1}{r_{n-1}} \end{pmatrix} \begin{pmatrix} \dfrac{1}{r_{n-1}}a & \dfrac{1}{r_{n-1}}b \\ \hat{c} & \hat{d} \end{pmatrix}, & n \text{ odd} \\ \begin{pmatrix} 0 & r_{n-1} \\ -\dfrac{1}{r_{n-1}} & q \end{pmatrix} \begin{pmatrix} -\hat{c} & -\hat{d} \\ \dfrac{1}{r_{n-1}}a & \dfrac{1}{r_{n-1}}b \end{pmatrix}, & n \text{ even} \end{cases}$$

$$= \begin{pmatrix} a & b \\ \dfrac{qa}{r_{n-1}} + \dfrac{\hat{c}}{r_{n-1}} & \dfrac{qb}{r_{n-1}} + \dfrac{\hat{d}}{r_{n-1}} \end{pmatrix}.$$

It follows that $\delta A = \delta D_n + \max\{\deg a, \deg b\} = \delta D_n + \delta(D_n^{-1}A)$. Hence the factorization (3.1) is actually a factorization in $\mathcal{S}$.

Since in the euclidean algorithm $\deg r_k < \deg r_{k-1}$ for $k = 1, \ldots n$, we have $\deg p_k > 0$ for $k = 2, \ldots, n$. Hence, for $k = 2, \ldots, n$ the matrices V_k^{-1} are irreducible in $\mathcal{S}$. The matrices V_1^{-1} and D_n are either irreducible or belong to $\mathcal{S}^\times$, depending whether $\deg p_1 > 0$ or $\deg p_1 \le 0$ ($\deg q > 0$ or $\deg q \le 0$, respectively).

We have proved that A admits a factorization

$$A = W_1 \cdot \ldots \cdot W_{n'}\,, \tag{3.3}$$

where W_i are irreducible elements of $\mathcal{S}$ of the form

$$W_i = U_i \begin{pmatrix} 1 & q_i \\ 0 & 1 \end{pmatrix} U_i' = U_i \begin{pmatrix} 1 & q_i - q_i(0) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & q_i(0) \\ 0 & 1 \end{pmatrix} U_i'$$

with appropriate $q_i \in K[x]$, $\deg q_i > 0$, and $U_i, U_i' \in \mathcal{S}^\times$. ∎

Proof. (of (i), necessity) Assume that $B \in \mathcal{S}$ is irreducible. Then in the factorization (3.3) only one factor can appear, i.e. $B = W_1$, and hence B is of the desired form. ∎

Proof. (of (iii), existence) Let A, $A(0) = I$, be given. Choose any factorization $A = W_1 \cdot \ldots \cdot W_n$ into irreducible elements and define

$$\begin{aligned} V_n &:= W_n(0)^{-1} W_n \\ V_{n-1} &:= W_n(0)^{-1} W_{n-1}(0)^{-1}\, W_{n-1}\, W_n(0) \\ &\vdots \\ V_1 &:= W_n(0)^{-1} \cdots W_1(0)^{-1}\, W_1\, W_2(0) \cdots W_n(0) = W_1\, W_2(0) \cdots W_n(0). \end{aligned}$$

Then $V_i \sim W_i$ and $V_i(0) = I$. Moreover,

$$V_1 \cdot \ldots \cdot V_n = W_1 \cdot \ldots \cdot W_n = A.$$

∎

Proof. (of (iii), uniqueness) We use induction on the minimum number n such that A admits a factorization $A = W_1 \cdot \ldots \cdot W_n$ with W_i irreducible, $W_i(0) = I$.

Assume that $n = 1$. Then A can be written as $A = W_1$ and thus is irreducible. Hence in any other factorization $A = \hat{W}_1 \cdot \ldots \cdot \hat{W}_m$ we must have $m = 1$ and $W_1 = \hat{W}_1$.

Let $A = W_1 \cdot \ldots \cdot W_n = \hat{W}_1 \cdot \ldots \cdot \hat{W}_m$, $1 < n \leq m$, be given. Choose $U, U' \in \mathcal{S}^\times$ according to Lemma 2.4 such that $U'AU$ satisfies (D), and let p be the unique polynomial as in Proposition 2.5. It follows from the already established item (i) of the present theorem that we can write

$$W_n = V^{-1} \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} V$$

with appropriate q, $\deg q > 0$, $q(0) = 0$, and $V \in \mathcal{S}^\times$. Thus

$$U'AU = U'W_1 \cdot \ldots \cdot W_{n-1} \cdot V^{-1} \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} VU$$

and hence by Proposition 2.5 and Lemma 2.4

$$VU = \begin{pmatrix} \alpha & \beta \\ 0 & \frac{1}{\alpha} \end{pmatrix} = \begin{pmatrix} 1 & \alpha\beta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha & 0 \\ 0 & \frac{1}{\alpha} \end{pmatrix}.$$

It follows that

$$U'AU = U'W_1 \cdot \ldots \cdot W_{n-1} V^{-1} \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \alpha\beta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha & 0 \\ 0 & \frac{1}{\alpha} \end{pmatrix}$$

$$= U'W_1 \cdot \ldots \cdot W_{n-1} V^{-1} \begin{pmatrix} 1 & \alpha\beta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha & 0 \\ 0 & \frac{1}{\alpha} \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{\alpha} & 0 \\ 0 & \alpha \end{pmatrix} \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha & 0 \\ 0 & \frac{1}{\alpha} \end{pmatrix}$$

$$= U'W_1 \cdot \ldots \cdot W_{n-1} U \begin{pmatrix} 1 & \frac{q}{\alpha^2} \\ 0 & 1 \end{pmatrix}.$$

We conclude from Proposition 2.5 that $\frac{q}{\alpha^2} = p$ and hence that

$$A' := AU \begin{pmatrix} 1 & -p \\ & \\ 0 & 1 \end{pmatrix} U^{-1} = W_1 \cdot \ldots \cdot W_{n-1}.$$

The same argument starting from $A = \hat{W}_1 \cdot \ldots \cdot \hat{W}_m$ yields that $A' = \hat{W}_1 \cdot \ldots \cdot \hat{W}_{m-1}$. Our inductive hypothesis applied to A' now implies that $n-1 = m-1$ and

$$W_i = \hat{W}_i, \ i = 1, \ldots, n-1\,.$$

Thus also $W_n = \hat{W}_n$. ∎

Proof. (of (ii), uniqueness) Let A be given and assume that $A = W_1 \cdot \ldots \cdot W_n$ and also $A = \hat{W}_1 \cdot \ldots \cdot \hat{W}_m$. By the proof of item (iii) , existence, we find $V_1, \ldots, V_n$ and $\hat{V}_1, \ldots, \hat{V}_m$ such that

$$V_i \sim W_i,\, V_i(0) = I, \ i = 1, \ldots, n\,,$$

$$\hat{V}_i \sim \hat{W}_i,\, \hat{V}_i(0) = I, \ i = 1, \ldots, m\,,$$

$$AA(0)^{-1} = V_1 \cdot \ldots \cdot V_n = \hat{V}_1 \cdot \ldots, \cdot \hat{V}_m\,.$$

By the already established item (iii) , uniqueness, it follows that

$$n = m, \ V_i = \hat{V}_i, \ i = 1, \ldots, n\,.$$

Thus also $W_i \sim \hat{W}_i$, $i = 1, \ldots, n$. ∎

To conclude let us note that the euclidean algorithm or -better to say- its corollary that the greatest common divisor of two polynomials a, b can be written as a linear combination of a and b, can be viewed as a solution of the following completion problem:

Remark 3.2. Let $a, b \in K[x]$ with $\gcd\{a, b\} = 1$ be given.

(i) There exists a matrix $A \in \mathcal{S}$ such that

$$(1,0)A = (a,b). \tag{3.4}$$

The matrix A can be chosen such that, with $(c,d) := (0,1)A$,

$$\deg c \le \deg a,\ \deg d \le \deg b. \tag{3.5}$$

(ii) Let $A_0 \in \mathcal{S}$ be fixed such that (3.4) and (3.5) hold. Then a matrix $A \in \mathcal{S}$ satisfies (3.4) if and only if there exists $p \in K[x]$ such that

$$A = \begin{pmatrix} 1 & 0 \\ p & 1 \end{pmatrix} A_0.$$

References

[1] L. de Branges, Hilbert spaces of entire functions Prentice-Hall, London 1968.

[2] D. Alpay, Ya. Azizov, A. Dijksma and H. Langer, *The Schur algorithm for generalized Schur functions III: J-unitary matrix polynomials on the circle*, Linear Algebra Appl. **369** (2003), 113–144.

[3] D. Alpay, A. Dijksma and H. Langer, *Factorization of J-unitary matrix polynomials on the line and a Schur algorithm for generalized Nevanlinna functions,* Linear Algebra Appl. **387** (2004), 313–342.

[4] M. Kaltenbäck and H. Woracek, *Pontryagin spaces of entire functions I,* Integral Equations Operator Theory **33** (1999), 34–97.

[5] M. Kaltenbäck and H. Woracek, *Pontryagin spaces of entire functions II,* Integral Equations Operator Theory **33** (1999), 305–380.

[6] M. Kaltenbäck and H. Woracek, *Pontryagin spaces of entire functions III,* Acta Sci. Math. (Szeged) **69** (2003), 241–310.

Received March 2004
Revised November 2005