

MIROSLAV KUREŠ and LADISLAV SKULA

**Smith normal form of a matrix  
of generalized polynomials  
with rational exponents**

**ABSTRACT.** It is proved that generalized polynomials with rational exponents over a commutative field form an elementary divisor ring; an algorithm for computing the Smith normal form is derived and implemented.

**Introduction.** Historically, an important class of optimal control problems conduced to an interest in generalized polynomials over a commutative field  $T$ ; e.g., geometric programming was evolved and it is keeping its practical efficacy. It emerges that it is desirable to study generalized polynomial with rational exponents which can be defined as a map  $P: \mathbb{Q} \rightarrow T$  support of which is a finite set.

Of course, it is necessary to specify properties of generalized polynomials that are analogous to the properties of classical polynomials and investigate those that are different. We emphasize that generalized polynomials with rational exponents over a field do not represent a noetherian ring. In this paper, we have proved that they form an elementary divisor ring (i.e., each matrix with generalized polynomials as entries has a Smith normal form);

---

2000 *Mathematics Subject Classification.* 15A21, 15A54, 15-04, 12Y05.

*Key words and phrases.* Smith normal form, generalized polynomials with rational exponents.

Published results were acquired using the subsidization of the Ministry of Education, Youth and Sports of the Czech Republic, research plan MSM 0021630518 “Simulation modelling of mechatronic systems”.

thus, we have an important example of an elementary divisor ring, which is not a principal ideal ring. Further, we have shown an interesting subclass of elementary divisor rings, so-called EDE-rings, which have an independent theoretical importance.

As a method, we use our original approach, which we have called the transfer of a ring. By this method, we realize an algorithm for computing the Smith normal form of a matrix over generalized polynomials with rational exponents over some field (real, prime finite). We have implemented this algorithm in the computer algebra system Mathematica; examples are enclosed.

**1. Starting points.** In this paper, we use the terminology from the monograph of W. C. Brown, [1]. A ring  $R$  will be always commutative and containing an identity  $1_R \neq 0_R$ ,  $Z(R)$  denotes the set of all zero divisors of  $R$  (including  $0_R$ ) and  $U(R)$  denotes the set of all units of  $R$ , which is a group with respect to the ring multiplication. Further,  $M_{m \times n}(R)$  denotes the set of all  $m \times n$  matrices with entries in  $R$ . By an *elementary transvection*  $V_{ij}(r)$  (of order  $m$ ),  $1 \leq i \neq j \leq m$ ,  $r \in R$ , we mean a matrix  $[a_{\nu\mu}]$  from  $M_{m \times m}(R)$  with

$$a_{\nu\mu} = \begin{cases} 1_R & \text{for } \nu = \mu \\ r & \text{for } \nu = i, \mu = j \\ 0_R & \text{otherwise} \end{cases}$$

and by an *elementary dilation*  $S_i(r)$  (of order  $m$ ),  $1 \leq i \leq m$ ,  $r \in U(R)$ , we mean a matrix  $[a_{\nu\mu}]$  from  $M_{m \times m}(R)$  with

$$a_{\nu\mu} = \begin{cases} 1_R & \text{for } \nu = \mu \neq i \\ r & \text{for } \nu = \mu = i \\ 0_R & \text{otherwise.} \end{cases}$$

Finite products of elementary transvections and elementary dilations (of order  $m$ ) are called ( $m$ -th order) *elementary matrices*. Evidently, elementary matrices (elementary transvections, elementary dilations) are invertible and their inversions are elementary matrices (elementary transvections, elementary dilations, respectively).

**Remark 1.** *Elementary permutations*  $P_{ij}$  are also sometimes considered together with transvections and dilations; however, they represent nothing new, because they can be defined (for  $i \neq j$ ) as

$$P_{ij} = V_{ji}(1_R)S_j(-1_R)V_{ij}(1_R)V_{ji}(-1_R)$$

and their inversions are again elementary permutations.

All invertible matrices of order  $n$  with entries in  $R$  form a group with respect to the multiplication; this is the well-known general linear group  $GL_n(R)$ . Of course, all elementary matrices of order  $n$  with entries in  $R$

form its subgroup; it is denoted by  $\text{GE}_n(R)$ . It is clear that  $\text{GL}_1(R) = \text{GE}_1(R) (= \text{U}(R))$  for every  $R$ . If for any  $n \in \mathbb{N}$  and a ring  $R$ , the equality  $\text{GL}_n(R) = \text{GE}_n(R)$  is satisfied, we say  $R$  is a  $\text{GE}_n$ -ring. If a ring  $R$  is  $\text{GE}_n$ -ring for all  $n \in \mathbb{N}$ , then  $R$  is called the  $\text{GE}$ -ring or the *generalized euclidean ring*. Fields, euclidean rings and semilocal rings are known examples of generalized euclidean rings. On the other hand, they are known rings, for which  $\text{GE}_2(R)$  is a proper subgroup of  $\text{GL}_2(R)$ . The example of such a ring is the ring  $\mathbb{Z} \left[ \frac{1+\sqrt{-19}}{2} \right]$  of algebraic integers of  $\mathbb{Q} [\sqrt{-19}]$ . The example of a second order non-elementary invertible matrix with entries in  $\mathbb{Z} \left[ \frac{1+\sqrt{-19}}{2} \right]$  is

$$\begin{bmatrix} 3 - \frac{1+\sqrt{-19}}{2} & 2 + \frac{1+\sqrt{-19}}{2} \\ -3 - 2\frac{1+\sqrt{-19}}{2} & 5 - 2\frac{1+\sqrt{-19}}{2} \end{bmatrix}.$$

Another example of a ring, for which  $\text{GE}_2(R)$  is a proper subgroup of  $\text{GL}_2(R)$  is e.g., the ring  $T[x, y]$  of polynomials in two indeterminates over a field  $T$ . The second order non-elementary invertible matrix with entries in this ring is

$$\begin{bmatrix} 1 + xy & x^2 \\ -y^2 & 1 - xy \end{bmatrix}.$$

(Nevertheless, it is known, that  $\text{GE}_n(R) = \text{GL}_n(R)$  is satisfied for all natural  $n$  in the ring  $T[x_1, \dots, x_m]$  of polynomials in  $m \geq 3$  indeterminates.) For more detail see e.g., papers of P. M. Cohn [3] and A. A. Suslin [13].

Let  $A \in M_{m \times n}(R)$ . A diagonal matrix  $S = \text{Diag}(s_1, \dots, s_r) \in M_{m \times n}(R)$  is called the *Smith normal form* of  $A$  if  $A \approx S$  (i.e., there exist invertible matrices  $U \in M_{m \times m}(R), V \in M_{n \times n}(R)$  with  $UAV = S$ ) and  $s_1 | s_2 | \dots | s_r$  in  $R$  (i.e., the element  $s_i$  divides the element  $s_{i+1}$  in  $R$  for each  $1 \leq i \leq r-1$ ). If each matrix with entries in  $R$  has a Smith normal form, then  $R$  is called an *elementary divisor ring*. We say about the mentioned matrix  $S$  that it is *in the Smith normal form*. In an elementary divisor ring, every finitely generated ideal is principal. Nevertheless, the opposite implication is not true in general. For an explanation, we can define the *adequate ring* as a ring  $R$  in which every finitely generated ideal is principal and for which the following condition is satisfied: for every  $a, b \in R, a \neq 0_R$ , the element  $a$  may be written as  $a = rs$  with  $(r, b) = (1_R)$  and  $(t, b) \neq (1_R)$  for every nonunit divisor  $t$  of  $s$ . (As usual,  $(a_1, \dots, a_k)$  denotes the ideal generated by  $a_1, \dots, a_k$ .) Now, we can recall Helmer's theorem (see [7], [6]): if a ring  $R$  is adequate and  $Z(R) = \{0_R\}$  (i.e.,  $R$  is an integral domain), then  $R$  is an elementary divisor ring.

**2. EDE-rings.** We introduce additional concepts and formulate a little bit familiar assertions. If  $F$  is an automorphism of  $R$  (we shall write  $F \in \text{Aut } R$ )

and  $A = [a_{\mu\nu}] \in M_{m \times n}(R)$ , then we put

$$\tilde{F}(A) = [F(a_{\mu\nu})] \in M_{m \times n}(R).$$

Certainly,  $\tilde{F}$  is a bijection of  $M_{m \times n}(R)$  onto itself. We have (for suitable types of matrices and  $r \in R$ ) the following identities:

$$\begin{aligned}\tilde{F}(A + B) &= \tilde{F}(A) + \tilde{F}(B), \\ \tilde{F}(AB) &= \tilde{F}(A)\tilde{F}(B), \\ \tilde{F}(rA) &= F(r)\tilde{F}(A).\end{aligned}$$

Thus, we have easily two useful assertions.

**Lemma 1.** *The matrix  $U \in M_{m \times m}(R)$  is invertible (elementary) if and only if  $\tilde{F}(U)$  is invertible (elementary, respectively).*

**Lemma 2.** *The matrix  $S \in M_{m \times m}(R)$  is in a Smith normal form if and only if  $\tilde{F}(S)$  is in a Smith normal form.*

Now, we define special elementary divisor rings. Let for each matrix  $A \in M_{m \times n}(R)$  with entries in  $R$  there exist elementary matrices  $U \in M_{m \times m}(R), V \in M_{n \times n}(R)$  with  $UAV = S$ , where  $S \in M_{m \times n}(R)$  is in the Smith normal form. Then we call  $R$  an  $\text{EDE}_{m,n}$ -ring. If a ring  $R$  is  $\text{EDE}_{m,n}$ -ring for all  $m, n \in \mathbb{N}$ , then  $R$  is called the  $\text{EDE}$ -ring.

**Proposition 1.** *Let  $R$  be an elementary divisor ring  $R$ . Then  $R$  is an  $\text{EDE}$ -ring if and only if  $R$  is a  $\text{GE}$ -ring.*

**Proof.** Let us suppose  $R$  is an  $\text{EDE}$ -ring. We present that every invertible square matrix over  $R$  is elementary: let  $n \in \mathbb{N}$  and let  $A \in M_{n \times n}(R)$  be invertible. Then, there exist  $U \in M_{n \times n}(R), V \in M_{n \times n}(R)$  with  $UAV = S$ , where  $S = \text{Diag}(s_1, \dots, s_n) \in M_{n \times n}(R)$  is in a Smith normal form. The matrix  $S$  is invertible, and thus  $s_i \in U(R)$  for  $1 \leq i \leq n$ . It follows  $S$  is elementary. As  $U^{-1}, V^{-1}$  are also elementary, the matrix  $A = U^{-1}SV^{-1}$  is elementary. The proof in an opposite direction is trivial.  $\square$

**Lemma 3.** *Let  $R$  be an  $\text{EDE}_{m,n}$ -ring. Then  $R$  is also an  $\text{EDE}_{n,m}$ -ring.*

**Proof.** Let  $A \in M_{m \times n}(R), U \in \text{GE}_m(R), V \in \text{GE}_n(R), UAV = S$  in the Smith normal form. Then

$$S^T = (UAV)^T = V^T A^T U^T$$

and  $S^T$  is in the Smith normal form. Evidently,  $V^T$  and  $U^T$  are elementary matrices as the mere change of row and column operations.  $\square$

**Remark 2.** It follows from the proof of Proposition 1 that an elementary divisor ring is an  $\text{EDE}_{n,n}$ -ring if and only if it is  $\text{GE}_n$ -ring. It is also clear, that if an elementary divisor ring  $R$  is simultaneously  $\text{GE}_m$ -ring and  $\text{GE}_n$ -ring, then  $R$  is  $\text{EDE}_{m,n}$ -ring,  $\text{EDE}_{n,m}$ -ring,  $\text{EDE}_{m,m}$ -ring, and  $\text{EDE}_{n,n}$ -ring.

**3. Transfer of a ring.** Let  $R$  be a subring of a ring  $P$ . We say that  $P$  transfers to  $R$ , if for every  $N \in \mathbb{N}$  and every  $\sigma_1, \dots, \sigma_N \in P$  there exists a unit  $\epsilon \in U(P)$  and an automorphism  $F \in \text{Aut } P$  of the ring  $P$  such that

$$F(\epsilon\sigma_i) \in R \quad \text{for every } 1 \leq i \leq N.$$

**Proposition 2.** *Let a ring  $P$  transfers to its subring  $R$ . If  $R$  is an elementary divisor ring (an EDE-ring), then  $P$  is an elementary divisor ring (an EDE-ring), too.*

**Proof.** Let  $A = [a_{ij}] \in M_{m \times n}(S)$ . As  $P$  transfers to its subring  $R$ , then there is  $\epsilon \in U(P)$  and an automorphism  $F \in \text{Aut } P$  such that  $F(\epsilon a_{ij}) \in R$  for all  $1 \leq i \leq m, 1 \leq j \leq n$ . There exist invertible (elementary) matrices  $\tilde{U} \in M_{m \times m}(R), \tilde{V} \in M_{n \times n}(R)$  such that

$$\tilde{U}\tilde{F}(\epsilon A)\tilde{V} = \tilde{S},$$

where  $\tilde{S} \in M_{m \times n}(R)$  is in the Smith normal form. Let

$$U = \widetilde{F^{-1}}(\tilde{U}), \quad V = \widetilde{F^{-1}}(\tilde{V}), \quad S = \widetilde{F^{-1}}(\tilde{S}).$$

Then  $U \in M_{m \times m}(P)$  and  $V \in M_{n \times n}(P)$  are invertible (elementary) matrices and  $S \in M_{m \times n}(P)$  is in the Smith normal form (in  $P$ ). Further,  $U\epsilon AV = S$ , thus  $UAV = \epsilon^{-1}S$ . However,  $\epsilon^{-1}D \in M_{m \times n}(P)$  is in the Smith normal form (in  $P$ ), and the proposition is proved.  $\square$

Let  $T$  be a field. A *generalized polynomial with rational exponents* can be defined as a map

$$P: \mathbb{Q} \rightarrow T$$

support of which is a finite set. Formally, such polynomials can be written in the form

$$P(q_1)Z^{q_1} + \dots + P(q_k)Z^{q_k},$$

where  $Z$  is an indeterminate;  $q_1, \dots, q_k \in \mathbb{Q}$  are called *exponents* and  $P(q_1), \dots, P(q_k) \in T$  are called *coefficients*. Such generalized polynomials were studied by numerous authors and sometimes named *signomials* (with rational exponents), see e.g., [4]. We define operations  $+$  and  $\cdot$  by usual way (as on the ring  $T[Z]$  of polynomials over  $T$ ). Then, evidently, the set of all generalized polynomials with rational exponents is a commutative ring with unit: this ring will be denoted by  $T^{\mathbb{Q}}[Z]$ . Moreover,  $T^{\mathbb{Q}}[Z]$  is an integral domain containing  $T[Z]$  as its own subdomain. An element of  $T^{\mathbb{Q}}[Z]$  (denoting by  $E$ ) belongs to  $U(T^{\mathbb{Q}}[Z])$  if and only if its support is singleton. Let  $n \in \mathbb{N}$  and  $P \in T^{\mathbb{Q}}[Z]$ . We define the map

$$R_n: T^{\mathbb{Q}}[Z] \rightarrow T^{\mathbb{Q}}[Z], \quad R_n: P \mapsto Q,$$

where  $Q \in T^{\mathbb{Q}}[Z]$  is defined by

$$Q(\alpha) = P\left(\frac{\alpha}{n}\right)$$

(for all  $\alpha \in \mathbb{Q}$ ). The map  $R_n$  is an automorphism of  $T^{\mathbb{Q}}[Z]$ ; i.e.,  $R_n \in \text{Aut } T^{\mathbb{Q}}[Z]$ , for more details see the monographical work of J. Karásek and J. Šlapal, [10].

**Proposition 3.** *The ring  $T^{\mathbb{Q}}[Z]$  transfers to its subring  $T[Z]$  of polynomials in one indeterminate over  $T$ .*

**Proof.** Let  $N \in \mathbb{N}$  and  $S_1, \dots, S_N \in T^{\mathbb{Q}}[Z]$  be maps with non-empty support. Let  $\text{supp } S_i = \{u_{i0} > u_{i1} > \dots > u_{in_i}\}$  for  $1 \leq i \leq N$ , where  $n_i \in \mathbb{N} \cup \{0\}$  and  $u_{ij} \in \mathbb{Q}$ . Then, there exists  $u \in \mathbb{Q}$  such that  $u_{ij} + u \geq 0$  for all  $1 \leq i \leq N$ ,  $0 \leq j \leq n_i$ . Let  $E \in T^{\mathbb{Q}}[Z]$ , where  $E(u) = 1_T$  and  $E(q) = 0_T$  for all  $q \in \mathbb{Q} - \{u\}$ . Then  $E = Z^u \in U(T^{\mathbb{Q}}[Z])$  and  $\text{supp } ES_i = \{v_{i0} > v_{i1} > \dots > v_{in_i}\}$   $1 \leq i \leq N$ , where  $v_{ij} = u_{ij} + u \geq 0$  for  $1 \leq i \leq N$ ,  $0 \leq j \leq n_i$ .

Now, there also exists  $n \in \mathbb{N}$  for which  $nv_{ij} = c_{ij} \in \mathbb{N} \cup \{0\}$  for all  $1 \leq i \leq N$ ,  $0 \leq j \leq n_i$ . We put  $F = R_n$ . Let  $1 \leq i \leq N$  be fixed;  $P = ES_i$  and  $Q = F(P) = F(ES_i) = R_n(P)$ . Then

$$\begin{aligned} Q(c_{ij}) &= P\left(\frac{c_{ij}}{n}\right) = P(v_{ij}) \neq 0 && \text{for } 0 \leq j \leq n_i \\ Q(q) &= 0 && \text{for } q \in \mathbb{Q} - \{c_{ij}; 0 \leq j \leq n_i\}. \end{aligned}$$

Hence  $Q = F(ES_i) \in T[Z]$ . □

Propositions 2 and 3 give the following results immediately:

**Proposition 4.** *The ring  $T^{\mathbb{Q}}[Z]$  is an EDE-ring.*

**Proof.** Of course,  $T[Z]$  is an EDE-ring and the assertion is an application of the mentioned Propositions. □

**Remark 3.** The ring  $T^{\mathbb{Q}}[Z]$  is not noetherian, see e.g., [10], thus we have an example of an elementary divisor ring (even EDE-ring!), which is not a principal ideal ring.

**4. Algorithm for computing the Smith normal form of a matrix over  $T^{\mathbb{Q}}[Z]$ .** There are many algorithms for computing the Smith normal form over integer and polynomial matrices, see e.g., [2], [8], [14]. It is known that they can be realized in polynomial time. So, the task is the implementation of the transfer of the ring  $T^{\mathbb{Q}}[Z]$  described above and using of an algorithm over polynomial matrices. We have announced our approach in [11]; it can be presented by the following way.

INPUT: Generalized polynomials are entered as a list of ordered couples with the exponent as the first term and the coefficient as the second. The matrix of generalized polynomials is entered as a list of  $m$  ordered  $n$ -tuples.

Thus, the input has a form

$$A = [ [((q_{11,1}, P_{11}(q_{11,1})), \dots, (q_{11,k_{11}}, P_{11}(q_{11,k_{11}}))), \\ \dots, \\ ((q_{1n,1}, P_{1n}(q_{1n,1})), \dots, (q_{1n,k_{1n}}, P_{1n}(q_{1n,k_{1n}}))), \\ \dots, \\ (((q_{m1,1}, P_{11}(q_{m1,1})), \dots, (q_{m1,k_{m1}}, P_{m1}(q_{m1,k_{m1}}))), \\ \dots, \\ ((q_{mn,1}, P_{mn}(q_{mn,1})), \dots, (q_{mn,k_{mn}}, P_{mn}(q_{mn,k_{mn}}))) ] ] .$$

STEP 1. THE ARRANGEMENT OF INPUT. In general, a certain exponent can occur in the input of a polynomial several times (possibly in different forms) and coefficients can vanish. Thus, entered couples are ordered and unnecessary couples are removed. From now, we assume

$$q_{ij,1} < \dots < q_{ij,k_{ij}}$$

and

$$P_{ij}(q_{ij,1}) \neq 0, \dots, P_{ij}(q_{ij,k_{ij}}) \neq 0$$

for every non-zero generalized polynomial ( $i = 1, \dots, m, j = 1, \dots, n$ ).

STEP 2. EXPONENTS ARE TRANSFORMED TO NON-NEGATIVE. We take

$$\gamma = -\min\{q_{ij,k_{ij}}; i = 1, \dots, m, j = 1, \dots, n\}$$

and set

$$r_{ij,\kappa_{ij}} = \gamma + q_{ij,\kappa_{ij}}$$

for all  $i = 1, \dots, m, j = 1, \dots, n$  and all  $\kappa_{ij} = 1, \dots, k_{ij}$ . The exponents  $q_{ij,\kappa_{ij}}$  are replaced with  $r_{ij,\kappa_{ij}}$ .

STEP 3. EXPONENTS ARE TRANSFORMED TO NON-NEGATIVE INTEGERS. We find the least common denominator of all  $r_{ij,\kappa_{ij}}$  ( $i = 1, \dots, m, j = 1, \dots, n, \kappa_{ij} = 1, \dots, k_{ij}$ ) and denote it by  $\rho$ . Then we realize the following transformation:

$$\tilde{q}_{ij,\kappa_{ij}} = \rho r_{ij,\kappa_{ij}}$$

for all  $i = 1, \dots, m, j = 1, \dots, n$  and all  $\kappa_{ij} = 1, \dots, k_{ij}$ . The exponents  $r_{ij,\kappa_{ij}}$  are replaced with  $\tilde{q}_{ij,\kappa_{ij}}$ .

STEP 4. SMITH NORMAL FORM IS COMPUTED. Now, our input has a form

$$\tilde{A} = [ [((\tilde{q}_{11,1}, P_{11}(q_{11,1})), \dots, (\tilde{q}_{11,k_{11}}, P_{11}(q_{11,k_{11}}))), \\ \dots, \\ ((\tilde{q}_{1n,1}, P_{1n}(q_{1n,1})), \dots, (\tilde{q}_{1n,k_{1n}}, P_{1n}(q_{1n,k_{1n}}))), \\ \dots, \\ (((\tilde{q}_{m1,1}, P_{11}(q_{m1,1})), \dots, (\tilde{q}_{m1,k_{m1}}, P_{m1}(q_{m1,k_{m1}}))), \\ \dots, \\ ((\tilde{q}_{mn,1}, P_{mn}(q_{mn,1})), \dots, (\tilde{q}_{mn,k_{mn}}, P_{mn}(q_{mn,k_{mn}}))) ] ]$$

and represents a matrix with entries in (standard) polynomial ring  $\mathbb{R}[Z]$ . Thus, usual Smith normal form  $\tilde{S}$  and factors  $\tilde{U}, \tilde{V}$  are computed (for  $\tilde{A}$ ).

STEP 5. THE REVERSE OF STEP 3. We denote by  $\tilde{s}_{ij, \kappa_{ij}}, \tilde{u}_{ij, \kappa_{ij}}$  and  $\tilde{v}_{ij, \kappa_{ij}}$  the exponents in matrices  $\tilde{S}, \tilde{U}$  and  $\tilde{V}$ , respectively. Then we realize the following transformation:

$$\begin{aligned} s_{ij, \kappa_{ij}} &= \frac{1}{\rho} \tilde{s}_{ij, \kappa_{ij}} \\ w_{ij, \kappa_{ij}} &= \frac{1}{\rho} \tilde{u}_{ij, \kappa_{ij}} \\ v_{ij, \kappa_{ij}} &= \frac{1}{\rho} \tilde{v}_{ij, \kappa_{ij}} \end{aligned}$$

( $i = 1, \dots, m, j = 1, \dots, n, \kappa_{ij} = 1, \dots, k_{ij}$ ).

STEP 6. THE REVERSE OF STEP 2. We finish:

$$u_{ij, \kappa_{ij}} = -\gamma + w_{ij, \kappa_{ij}}$$

( $i = 1, \dots, m, j = 1, \dots, n, \kappa_{ij} = 1, \dots, k_{ij}$ ). (Likewise, the second factor  $V$  can be modified by this way.)

OUTPUT: The required matrices  $S, U$  and  $V$  are matrices with exponents  $s_{ij, \kappa_{ij}}, u_{ij, \kappa_{ij}}$  and  $v_{ij, \kappa_{ij}}$  respectively.

**5. Examples for  $T = \mathbb{R}$  and for  $T = F_p$ .** Packages of Mathematica commands for finding the Smith normal form of a matrix with entries in polynomials are universally available. Usually, they provide commands for transforming matrices as well.

The new package `SmithFormGP.m` extends power of the package `SmithForm.m`. The package `SmithForm.m` is actively used; we employ the package [12] programmed by A. Pascoletti. In particular, the command

$$\{\mathbf{S}, \{\mathbf{U}, \mathbf{V}\}\} = \text{SFGP}[\mathbf{A}, \mathbf{Z}]$$

yields the Smith normal form  $S$  of the matrix  $A$  with entries in  $\mathbb{R}^{\mathbb{Q}}[Z]$  (or  $\mathbb{Q}^{\mathbb{Q}}[Z]$ ) together with the factors  $U, V, S = UAV$ ;  $Z$  is an indeterminate. Further, the command

$$\{\mathbf{S}, \{\mathbf{U}, \mathbf{V}\}\} = \text{SFGPN}[\mathbf{A}, \mathbf{Z}, \mathbf{p}]$$

yields the Smith normal form  $S$  of the matrix  $A$  with entries in  $F_p^{\mathbb{Q}}[Z]$  together with the factors  $U, V$ , where  $p$  is a prime and  $F_p$  is the prime finite field. For the matrix

$$A = \begin{bmatrix} Z & 0 & 2Z^3 \\ \frac{2}{Z} & 0 & 3Z \\ 0 & Z^4 + 5\sqrt{Z} & 0 \end{bmatrix},$$



we have obtained the following Smith normal forms as outputs of our commands `SFGP[A,Z]`, `SFGPN[A,Z,2]`, `SFGPN[A,Z,3]`, `SFGPN[A,Z,5]`, `SFGPN[A,Z,7]`:

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & Z^{\frac{3}{2}} & 0 \\ 0 & 0 & Z^{\frac{15}{2}} + 5Z^4 \end{bmatrix}, \begin{bmatrix} Z^{\frac{3}{2}} & 0 & 0 \\ 0 & Z^2 & 0 \\ 0 & 0 & Z^{\frac{11}{2}} + Z^2 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & Z^{\frac{3}{2}} & 0 \\ 0 & 0 & Z^{\frac{15}{2}} + 2Z^4 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & Z^4 & 0 \\ 0 & 0 & Z^5 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & Z^{\frac{3}{2}} & 0 \\ 0 & 0 & Z^{\frac{15}{2}} + 5Z^4 \end{bmatrix},$$

respectively. A number of examples of a use of the command `SFGP[A,Z]` including also non-square matrices, irrational coefficients of polynomials, etc., is in [11].

#### REFERENCES

- [1] Brown, W. C., *Matrices over Commutative Rings*, Marcel Dekker, 1993.
- [2] Cohen, H., *Hermite and Smith normal form algorithms over Dedekind domains*, *Math. Comp.* **65** (1996), 1681–1699.
- [3] Cohn, P. M., *On the structure of  $GL_2$  of a ring*, *Publications Mathématiques de l'I.H.É.S.* **30** (1966), 5–53.
- [4] Delzell, C. N., *Extension of Pólya's theorems to signomials with rational exponents*, Preprint available on <http://www.math.lsu.edu/~preprint/>.
- [5] Gantmacher, F. R., *The Theory of Matrices, Vol.1*, AMS Chelsea Publishing, Providence, RI, 1998.
- [6] Gillman, L., Henriksen, M., *Some remarks about elementary divisor rings*, *Trans. Am. Math. Soc.* **82** (1956), 362–365.
- [7] Helmer, O., *The elementary divisor theorem for certain rings without chain condition*, *Bull. Am. Math. Soc.* **49** (1943), 225–236.
- [8] Kannan, A., Bachem, A., *Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix*, *SIAM J. Comput.* **8** (1979), 499–507.
- [9] Kaplansky, I., *Elementary divisors and modules*, *Trans. Am. Math. Soc.* **66** (1949), 464–491.
- [10] Karásek, J., Šlapal, J., *Polynomials and Generalized Polynomials in Control Theory*, (Czech), CERM Academic Publishing Brno, 2007.
- [11] Kureš, M., *On the computation of Smith normal form of a matrix of generalized polynomials with rational exponents*, in: *Aplimat 2007, Proceedings of the International Conference Aplimat, Bratislava, Slovakia, February 6–9, 2007*, Slovak University of Technology, 2007, pp. 103–108.
- [12] Pascolletti, A.: `SmithForm.m`, version 1.0 (2005). The Mathematica package available on <http://library.wolfram.com/infocenter/MathSource/682/>.
- [13] Suslin, A. A., *On the structure of the special linear group over polynomial rings*, *Math. USSR, Izv.* **11** (1977), 221–238.
- [14] Villard, G., *Computation of the Smith normal form of polynomial matrices*, in: *ISSAC '93, Proceedings of the 1993 international symposium on Symbolic and algebraic computation*, Kiev, Ukraine, July 6–8, 1993, ACM Press Baltimore, 1993, pp. 209–217.

Miroslav Kureš  
Institute of Mathematics  
Brno University of Technology  
Technická 2, 61669 Brno  
Czech Republic  
e-mail: [kures@fme.vutbr.cz](mailto:kures@fme.vutbr.cz)

Ladislav Skula  
Institute of Mathematics  
Brno University of Technology  
Technická 2, 61669 Brno  
Czech Republic  
e-mail: [skula@fme.vutbr.cz](mailto:skula@fme.vutbr.cz)

Received February 8, 2008