Invariant factors of a product of matrices over a principal ideal domain and the product of Schur functions

Olga Azenhas, CMUC, University of Coimbra

based on a 89's joint paper with E. Marques de Sá

Tarde de Álgebra dedicada a Eduardo Marques de Sá
por ocasião do seu 70^{o} aniversário
Coimbra, 2-12-2016

Smith normal form: SNF

- $\mathcal{R}$ a commutative ring with 1.
- A and B $n \times n$ matrices over $\mathcal{R}$.
  A and B are said to be equivalent, $A \sim B$, if $B = PAQ$ for some matrices P and Q in $GL_n(\mathcal{R})$,

Smith normal form: SNF

- $\mathcal{R}$ a commutative ring with 1.
- A and B $n \times n$ matrices over $\mathcal{R}$.
  A and B are said to be equivalent, $A \sim B$, if $B = PAQ$ for some matrices P and Q in $GL_n(\mathcal{R})$,

Definition

A an $n \times n$ matrix over $\mathcal{R}$. If there exist matrices $P, Q \in GL_n(\mathcal{R})$ such that

$$PAQ =: S = diag(d_1, d_1 d_2, d_1 d_2 d_3, \ldots, d_1 d_2 \ldots d_n)$$

with $d_i \in \mathcal{R}$, we then call S a Smith normal form (SNF) of A.

Smith normal form: SNF

- $\mathcal{R}$ a commutative ring with 1.
- A and B $n \times n$ matrices over $\mathcal{R}$.
  A and B are said to be equivalent, $A \sim B$, if $B = PAQ$ for some matrices P and Q in $GL_n(\mathcal{R})$,

Definition

A an $n \times n$ matrix over $\mathcal{R}$. If there exist matrices $P, Q \in GL_n(\mathcal{R})$ such that

$$PAQ =: S = diag(d_1, d_1 d_2, d_1 d_2 d_3, \ldots, d_1 d_2 \ldots d_n)$$

with $d_i \in \mathcal{R}$, we then call S a Smith normal form (SNF) of A.

- $det(A) = u d_1^n d_2^{n-1} \ldots d_{n-1}^2 d_n^1$ with u an unity in $\mathcal{R}$.

Smith normal form: SNF

- $\mathcal{R}$ a commutative ring with 1.
- A and B $n \times n$ matrices over $\mathcal{R}$.
  A and B are said to be equivalent, $A \sim B$, if $B = PAQ$ for some matrices P and Q in $GL_n(\mathcal{R})$,

Definition

A an $n \times n$ matrix over $\mathcal{R}$. If there exist matrices $P, Q \in GL_n(\mathcal{R})$ such that

$$PAQ =: S = diag(d_1, d_1 d_2, d_1 d_2 d_3, \ldots, d_1 d_2 \ldots d_n)$$

with $d_i \in \mathcal{R}$, we then call S a Smith normal form (SNF) of A.

- $det(A) = u d_1^n d_2^{n-1} \ldots d_{n-1}^2 d_n^1$ with u an unity in $\mathcal{R}$.
- Observations
  - Every diagonal matrix over $\mathcal{R}$ admits such a diagonal reduction if and only if every finitely generated ideal is principal (Bézout ring).
  - If every matrix over $\mathcal{R}$ admits such a diagonal reduction, $\mathcal{R}$ is called an elementary divisor ring ($El.Div \subseteq Bez$).

Existence of SNF

- $\mathcal{R} = \mathbb{K}$ a field:
  - By elementary row and column operations (Gaussian elimination), we may compute the SNF of A which is the echelon form

$$diag(\alpha_1, \ldots, \alpha_r, 0, \ldots, 0), \qquad \alpha_i = 1, \quad r = rank(A).$$

- $\mathcal{R} = \mathbb{Z}$.
  - The existence of Euclidean's algorithm guarantees that every unimodular matrix can be written as a product of elementary matrices. By elementary row and column operations we may compute the SNF which is unique up to sign ± 1 of diagonal elements.

$$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, \qquad \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix} \to S = \begin{bmatrix} 1 & 0 \\ 0 & 6 \end{bmatrix}, -2+3=1$$

Existence of SNF continued

- $\mathcal{R} = \mathbb{Z}[x]$ is not an Euclidean ring nor a principal ring (Bézout ring). Not every diagonal matrix has a SNF.

  Suppose that the diagonal matrix

  $$A = \begin{bmatrix} 2 & 0 \\ 0 & x \end{bmatrix},$$

  has SNF $S = PAQ$. Then the only possible SNF is $S = diag(1, 2x)$ since $det(S) = \pm 2x$.

  On the other hand, putting $x = 2$ in S gives SNF $diag(1, 4)$ over $\mathbb{Z}$ but putting $x = 2$ in A yields SNF $diag(2, 2)$ over $\mathbb{Z}$.

SNF over a PID

- $\mathcal{R}$ is a PID: an analogue of the fundamental theorem of arithmetic holds; any two elements of a PID have a greatest common divisor although it may not be possible to find it using the Euclidean algorithm; Bézout's identity is satisfied.
- Examples. $\mathbb{K}$ any field; $\mathbb{Z}$ the ring of integers; $\mathbb{K}[x]$ the ring of polynomials in one variable with coefficients in $\mathbb{K}$; $\mathbb{K}[[x]]$ the ring of formal power series in one variable over a field $\mathbb{K}$, more generally any discrete valuation ring.

Proposition

Over a PID the SNF always exists and is unique up to unit multiples,

$$S(A) := PAQ = diag(\alpha_1, \alpha_2, \ldots, \alpha_n), \quad \alpha_1|\alpha_2|\ldots|\alpha_n.$$

The α_i are the invariant factors of A; they are unique up to unit multiples.

For $1 \leq k \leq n$, we have that $\alpha_1\alpha_2\cdots\alpha_k$ is equal to the gcd of all $k \times k$ minors of A, with the convention that if all $k \times k$ minors are 0, then their gcd is 0.

- $\mathcal{R}$-matrices A, B, $n \times n$, $A \sim B$, iff $S(A) = S(B)$.

Gaussian elimination: Elementary row and column operations

- How should one effect the diagonalization on a matrix A over a PID?

  If the ring is Euclidean, elementary row and column operations will do the job.
  In general it relies on the theory of determinantal divisors, the greatest common divisor of all $k \times k$ subdeterminats of A.

Localization

- $\mathcal{R}$ a PID and p a prime element in $\mathcal{R}$.
- $\mathcal{F} \supseteq \mathcal{R}$ the field of fractions of $\mathcal{R}$. The localization of $\mathcal{R}$ with respect to p is

$$\mathcal{R}_p := \{a/b \in \mathcal{F} : (a, b) = 1, p \nmid b\}.$$

  $\mathcal{R}_p$ is the subring of $\mathcal{F}$ generated by $\mathcal{R}$ and the inverses in $\mathcal{F}$ of all elements of $\mathcal{R}$ that are outside of (p).

    - p is the unique prime in $\mathcal{R}_p$ up to multiples of units
    - $f \neq 0 \in \mathcal{R}_p$ is an unit iff $a, b \in \mathcal{R}$ and relatively prime with p.
    - $f \neq 0 \in \mathcal{R}_p$ then $f = \mu p^\nu$ with μ an $\mathcal{R}_p$ unit and ν a non negative integer.
    - $f = 0 := p^\infty$.

- $\mathcal{R}_p$ is a PID and an Euclidean domain whose proper ideals are $(p) \supset (p^2) \supset (p^3) \supset \dots$.
  $\mathcal{R}_p$ is a discrete valuation ring with valuation defined by $\nu \geq 0$.
- Examples. $\mathbb{Z}_p = \{n/m : n, m \in \mathbb{Z} : p \nmid m\}$, for any p prime integer. The ring $K[[x]]$ of formal power series.

SNF over $\mathcal{R}_p$

Proposition

If A is $\mathcal{R}_p$-matrix, its SNF is

$$S_p(A) := diag(p^{\nu_1}, \ldots, p^{\nu_r}, 0, \ldots, 0),$$

for some integers $0 \leq \nu_1 \leq \nu_2 \cdots \leq \nu_r$, r the rank of A. Moreover the group of unimodular matrices over $\mathcal{R}_p$ is generated by the elementary matrices and $S_p(A)$ may be obtained by Gaussian elimination.

Corollary

$S_p(A^t) = S_p(A)$ *and* $A \sim_p A^t$.

- If A is $\mathcal{R}$-matrix with $\mathcal{R}$ invariant factors $\alpha_1|\alpha_2|\ldots$ the p powers contained in $\alpha_1, \alpha_2, \ldots$ constitute the $\mathcal{R}_p$-invariant factors of A as a matrix over the extended $\mathcal{R}_p$,

$$A \sim_p S_p(A)$$

Local global principle

Fix a complete set $\mathcal{P}$ of non associated primes of $\mathcal{R}$.

Proposition

Let A, B over $\mathcal{R}$.

- $S(A) = \prod_{p \in \mathcal{P}} S_p(A)$.
- $A \sim B$ *iff* $A \sim_p B$ *for all* $p \in \mathcal{P}$.
- $(|A|, |B|) = 1$ *then* $S(AB) = S(A)S(B)$.

Invariant factors of a product of matrices over a PID

- Which $\alpha = (\alpha_i)$, $\beta = (\beta_i)$, $\gamma = (\gamma_i)$ in $\mathcal{R}^n$ can be invariant factors of $n \times n$ non-singular $\mathcal{R}$-matrices A, B and C if $C = AB$?

Localization of a matrix product

A matrix product over $\mathcal{R}$ is *localizable* in the following sense: we wish to construct matrices A,B and $C = AB$ over $\mathcal{R}$ with given invariant factors. First we work out in $\mathcal{R}_p$, for $p \in \mathcal{P}$, then we stick together our local constructs and obtain a product $AB = C$ inside $\mathcal{R}$ with the desired invariant factors.

Localization of a matrix product

A matrix product over $\mathcal{R}$ is *localizable* in the following sense: we wish to construct matrices A,B and $C = AB$ over $\mathcal{R}$ with given invariant factors. First we work out in $\mathcal{R}_p$, for $p \in \mathcal{P}$, then we stick together our local constructs and obtain a product $AB = C$ inside $\mathcal{R}$ with the desired invariant factors.

Theorem

(A. and Marques de Sá, 90) *Let $\alpha_1, \ldots, \alpha_n$, $\beta_1, \ldots, \beta_n$, and $\gamma_1, \ldots, \gamma_n$, be 3n elements of $\mathcal{R}$, such that $\alpha_i | \alpha_{i+1}$, $\beta_i | \beta_{i+1}$ and $\gamma_i | \gamma_{i+1}$, for $i = 1, \ldots, n-1$. The following conditions are pairwise equivalent:*

(a) *There exist $n \times n$ matrices over $\mathcal{R}$, say A, B and C with invariant factors (α_i), (β_i) and γ_i) resp. such that $AB = C$.*

(b) *For each prime $p \in \mathcal{P}$, there exist $n \times n$ matrices over $\mathcal{R}_p$ say A_p, B_p and C_p with $\mathcal{R}_p$-invariant factors (α_i), (β_i) and (γ_i) resp. such that $A_p B_p = C_p$.*

(c) *For each prime $p \in \mathcal{P}$, there exist $n \times n$ matrices over $\mathcal{R}$ say $\bar{A}_p$, $\bar{B}_p$ and $\bar{C}_p$ whose $\mathcal{R}$-invariant factors are the powers of p contained in (α_i), (β_i) and γ_i) resp. such that $\bar{A}_p \bar{B}_p = \bar{C}_p$.*

Matrix localization continued

R.C. Thompson, 1985, shows $(a) \Leftrightarrow (c)$, that is, the product is localizable inside of $\mathcal{R}$. We work in the extended $\mathcal{R}_p$. We prove $(b) \Rightarrow (c)$ and $(c) \Rightarrow (a)$.

Lemma

(R.C.Thompson, 82) *Given $n \times n$ matrices A, B and $C = AB$ over $\mathcal{R}_p$, we may assume that:*

(i) *A is upper triangular with p powers along the diagonal,*

(ii) *B is diagonal with p-powers along the diagonal,*

(iii) *C is upper triangular with p-powers along the diagonal.*

$(b) \Rightarrow (c)$ Let $\mu_j \in \mathcal{R}$ be a least common multiple of the denominators of the entries in the j-th column of A. Define $d_j := \mu_1 \mu_2 \cdots \mu_j$ and the $\mathcal{R}_p$-unimodular matrix

$$\Delta := diag(d_1, d_2, \ldots, d_n).$$

Put $\bar{A} := \Delta^{-1} A \Delta$, $\bar{B} := B$, and $\bar{C} := \Delta^{-1} C \Delta$; $\mathcal{R}$-matrices and $\bar{A}\bar{B} = \bar{C}$.
The $det(\bar{A})$ is a power of p thus the $\mathcal{R}$-invariant factors of $\bar{A}$ are powers of p.
Similarly for $\bar{C}$ the $\mathcal{R}$- invariant factors of $\bar{C}$ are powers of p.
This proves (c) because $\bar{A} \sim_p A$ and $\bar{B} \sim_p B$ and $\bar{C} \sim_p C$.

Matrix localization continued

$(c) \Rightarrow (a)$

Lemma

(Commutation property) Let $X_1, X_2, \ldots, X_t$ be any $n \times n$ matrices over $\mathcal{R}$. Given $\sigma \in \mathfrak{S}_t$, there exist $\mathcal{R}$-matrices $X_1', X_2', \ldots, X_t'$ $\mathcal{R}$-equivalent to $X_1, X_2, \ldots, X_t$ respectively such that

$$X_1X_2 \ldots X_t = X'_{\sigma(1)}X'_{\sigma(2)} \ldots X'_{\sigma(t)}.$$

$t = 2$

$$X_1^t \sim X_1, \quad X_2^t \sim X_2, \quad X_1X_2 \sim (X_1X_2)^t$$

$$X_1X_2 = U(X_1X_2)^t V = UX_2^t X_1^t V = (UU_2X_2V_2)(U_1X_1V_1V) = X_2'X_1',$$

for some $\mathcal{R}$-unimodular matrices $U, U_1,\ U_2,\ V, V_1,\ V_2$.

Matrix localization continued

$(c) \Rightarrow (a)$
Let $p_1, \dots, p_m$ be the distinct primes of α_i's, β_i's and γ_i's. For each $k \in \{1, \dots, m\}$, let $\bar{A}_{p_k}$, $\bar{B}_{p_k}$, $\bar{C}_{p_k}$ be the $\mathcal{R}$-matrices whose $\mathcal{R}$-invariant factors are the powers of p_k contained in (α_i), (β_i) and $\gamma_i)$ resp. such that $\bar{A}_{p_k}\bar{B}_{p_k} = \bar{C}_{p_k}$.

- Put $\bar{A}_k := \bar{A}_{p_k}$, $\bar{B}_k := \bar{B}_{p_k}$, $\bar{C}_k := \bar{C}_{p_k}$.
- Define $C := C_1 C_2 \cdots C_m = A_1 B_1 A_2 B_2 \cdots A_m B_m$.
- By the commutation property, for each k there exist $\mathcal{R}$-matrices A'_k, B'_k equivalent to A_k , B_k respect. such that

$$C = A'_1 A'_2 \cdots A'_m B'_1 B'_2 \cdots B'_m.$$

- Define $A := A'_1 A'_2 \cdots A'_m$ and $B := B'_1 B'_2 \cdots B'_m$. Therefore, over the ring $\mathcal{R}$, A,B, and C have invariant factors (α_i), (β_i) and (γ_i) respect.

Invariant factors of a product of matrices over $\mathcal{R}_p$

- Which $\alpha = (\alpha_i)$, $\beta = (\beta_i)$, $\gamma = (\gamma_i)$ in $\mathcal{R}_p^n$ can be invariant factors of $n \times n$ non-singular $\mathcal{R}_p$-matrices A, B and C if $C = AB$?

Proposition

Let A be an $n \times n$ nonsingular $\mathcal{R}_p$. There exist a partition $a = (a_1, \ldots, a_n)$ such that

$$S_p(A) = diag(p^{\alpha_1}, p^{\alpha_2}, \ldots, p^{\alpha_n}).$$

The sequence $\alpha = (\alpha_1, \ldots, \alpha_n)$ of exponents by decreasing order in the SNF of A is called the invariant partition of A.

- Which $\alpha = (\alpha_i)$, $\beta = (\beta_i)$, $\gamma = (\gamma_i)$ partitions of length $\leq n$, can be invariant partitions of $n \times n$ non-singular $\mathcal{R}_p$-matrices A, B and C if $C = AB$?

Schur polynomials

Let $x = (x_1, x_2, \ldots, x_n)$ be a sequence of indeterminates. For each partition γ of $\ell(\gamma) \le n$, there exists a Schur function $s_\gamma(x)$ which is a homogeneous symmetric polynomial in x of total degree $|\gamma|$. These Schur functions $s_\gamma(x)$ for all such γ form a linear basis of the ring Λ_n of symmetric polynomials in x. It follows that

$$s_\alpha(x)\ s_\beta(x) = \sum_\gamma c_{\alpha\beta}^\gamma\ s_\gamma(x),$$

where the $c_{\alpha\beta}^\gamma$ are *non-negative integers* called Littlewood–Richardson coefficients.

- What does $c_{\alpha\beta}^\gamma$ count?

Theorem

The Littlewood-Richardson (LR) rule (D.E. Littlewood and A. Richardson, M. P-Schützenberger, G. Thomas).

$$c_{\alpha\beta}^\gamma = \#\{\textit{ballot SSYT of shape } \gamma/\alpha \textit{ and content } \beta\}.$$

$U = \begin{array}{|c|c|c|c|} \hline & & 1 & 2 \\ \hline & 1 & 3 & \\ \hline 1 & 2 & & \\ \hline \end{array}$ is not ballot, $T = \begin{array}{|c|c|c|c|} \hline & & 1 & 1 \\ \hline & 1 & 2 & \\ \hline 2 & 3 & & \\ \hline \end{array}$ 112132, is ballot

Invariant factors of a product of matrices over $\mathcal{R}_p$

- Which α, β, γ partitions of length $\leq n$ can be invariant partitions of $\mathcal{R}_p$-matrices A, B and C if $C = AB$?

(P. Hall, J.A. Green 1956, T. Klein, 1968)

Theorem

Fora any discrete valuation ring $\mathcal{R}$ ($\mathcal{R}_p$) a triple (α, β, γ) of partitions of length $\leq n$ occurs as invariant factors of A, B and $C = AB$ if and only if $c^{\gamma}_{\alpha,\beta} = c^{\bar{\gamma}}_{\bar{\alpha},\bar{\beta}} > 0$.

Theorem

(Klein's Theorem, 68) Suppose that $c^{\gamma}_{\alpha,\beta} = c^{\bar{\gamma}}_{\bar{\alpha},\bar{\beta}} > 0$ and let $T = (\bar{\alpha}^0, \bar{\alpha}^1, \ldots, \bar{\alpha}^t)$ be an LR tableau of skew shape $\bar{\gamma}/\bar{\alpha}$ and content $\bar{\beta}$. Then there exist $n \times n$ nonsingular $\mathcal{R}_p$-matrices $A_0, B_1, \ldots, B_t$ such that
(i) For each $r = 0, 1, \ldots, t$, the matrix $A_r := A_0 B_1 B_2 \cdots B_r$ has invariant fact α^r.
(ii) The matrix $B := B_1 B_2 \cdots B_t$ has invariant partition $\beta = (\beta_1, \ldots, \beta_t)$.
(iii) For each $r \in \{1, \ldots, t\}$, B_r has invariant factor $(1, \ldots, 1)$ of length β_r.

Our contribution, 1990

- We explicitly provide a matrix proof of Klein's theorem:
  We explicitly construct an $\mathcal{R}_p$-matrix realization of a given LR tableau T.
  We give a simple matrix proof that each $\mathcal{R}_p$-matrix triple $(A, B, C = AB)$ gives rise to an unique LR tableau despite the various factorizations of the matrix B as aforesaid $B = B_1 B_2 \cdots B_t$.

1. O. Azenhas, E. Marques de Sá, Matrix realizations of Littlewood-Richardson sequences, Linear and Multilinear Algebra, 27 (1990) 229 242.
2. L. J. Gerstein, A local approach to matrix equivalence, LAA, 16,221–232, 1977.
3. I. Kaplansky, Elementary divisors and modules, Trans. Amer. Math. Soc. 66 (1949), 464491.
4. T. Klein, The multiplication of Schur functions and extensions of *p*-modules, Journal of the London Mathematical Society, 43:280-284, 1968.
5. D. E. Littlewood and A. R. Richardson, Group characters and algebra, Philos. Trans. London Ser. A 233:99-141, 1934.
6. D. Lorenzini, Elementary divisor domains and Bézout domains, J. Algebra 371 (2012), 609619.
7. R. Stanley, Smith normal form in Combinatorics, arXiv:1602.00166v2 [math.CO] 2 Apr 2016.
8. R. C. Thompson, An inequality for invariant factors, Proceedings of the American Mathematical Society, 86:9-11, 1982.
9. R. C. Thompson, Smith invariants of a product of integral matrices, in Linear Algebra and its Role in Systems Theory, Contemporary Mathematics, 47:401-435, AMS, 1985.