JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

RACHED MNEIMNÉ

FRÉDÉRIC TESTARD

On products of singular elements

Journal de Théorie des Nombres de Bordeaux, tome 3, nº 2 (1991), p. 337-350

<http://www.numdam.org/item?id=JTNB_1991__3_2_337_0>

Séminaire de Théorie des Nombres,
Bordeaux **3** *(1991), 337-350*

On products of singular elements

by RACHED MNEIMNÉ AND FRÉDÉRIC TESTARD

Some rings, like the ring $M(n, K)$ of square matrices, do not contain irreducible elements: any singular element x can be written as the product $x = yz$ of two singular elements y and z. We shall call these rings S-rings. Our first purpose in this paper is to exhibit some examples of S-rings. For instance, we give a necessary and sufficient condition ensuring that $\mathbb{Z}/n\mathbb{Z}$ is an S-ring.

More generally, let us denote by $S_i(R)$ (or just S_i if no confusion is possible) the set of elements of a ring R, which can be written as the product of i singular elements; the sequence (S_i) is decreasing (we only consider rings where left invertibility is equivalent to right invertibility) and moreover the ring R is an S-ring if and only if $S_1 = S_2$. We denote by S_∞ the intersection of all the S_i; when the sequence (S_i) is stationnary ($S_i = S_k$ whenever $i \geq k$), we have $S_\infty = S_k$ if k is the first index i such that $S_i = S_{i+1}$. There is a natural operation of the group $GL(R)$ of all invertible elements of the ring R on the set S_i defined by: $(g, x) \mapsto gx$ for $g \in GL(R)$ and $x \in S_i$, where gx is the product in R of the two elements g and x. This defines clearly an operation of $GL(R)$ on S_i, hence also on $S_i \setminus S_{i+1}$ (elements of S_i which do not belong to S_{i+1}). Other natural operations could have been considered: $(g, x) \mapsto xg^{-1}$ or $(g, x) \mapsto gxg^{-1}$ or the following operation of $GL(R) \times GL(R)$ on S_i given by $((g_1, g_2), x) \mapsto g_1 x g_2^{-1}$. When the ring R is commutative, these operations bring nothing new. This is the case of the ring $K[A]$ of polynomial expansions of the matrix $A \in M(n, K)$ for which we dispose of a particularly nice description of the orbits of $GL(A)$ $(= GL(K[A]))$-(Part 3).

In part 2, we study in an elementary way the ring $K[A]$ by giving a necessary and sufficient condition in order that the matrix A could be written as $P(A)Q(A)$, where P and Q are polynomials, with $P(A)$ and $Q(A)$ two singular matrices (i.e. $A \in S_2(K[A])$).

Part 4 is devoted to the solution of the following non trivial problem: given any matrix A, what is the maximal number $n(A)$ of singular and

Manuscrit reçu le 23 octobre 1990, version définitive reçue le 29 septembre 1991.

permutable matrices A_i such that $A = A_1 \cdots A_m$? A simple observation allows us to answer the same problem, for A and A_i bistochastic.

1. Examples of S-rings

We begin with an easy criterion

LEMMA 1. *Let E and F be two rings and $E \times F$ be their product ring; then $E \times F$ is an S-ring if and only E and F are S-rings. In particular, any finite product of fields is an S-ring.*

Proof Consider a singular element (x, y) in $E \times F$. For instance, x is not invertible. We can find x_1 and x_2 two singular elements in E so that $x = x_1 x_2$; then $(x, y) = (x_1, y)\cdot(x_2, 1)$ is the product of two singular elements of $E \times F$. Conversely, suppose that $E \times F$ is an S-ring and take x, any singular element in E. There exist two singular couples (x_1, y_1) and (x_2, y_2) so that $(x, 1) = (x_1, y_1)\cdot(x_2, y_2)$. Since $y_1 \cdot y_2 = 1$, x_1 and x_2 are not invertible, and E is an S-ring; the same argument works for F.

LEMMA 2. *Let p be a prime and α be a positive integer. The ring $R = \mathbb{Z}/p^\alpha\mathbb{Z}$ is an S-ring if and only if $\alpha = 1$.*

Proof If $\alpha = 1$, the ring R is a field and there is no problem; otherwise the class of p cannot be the product of two singular classes since it would imply $p - p^2 k = cp^\alpha$ where k and c are integers, which is impossible if $\alpha \geq 2$.

PROPOSITION 1. *Let $R = \mathbb{Z}/n\mathbb{Z}$; the ring R is an S-ring if and only if $n = p_1 \cdots p_k$ where the p_i are distinct primes.*

Proof If $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, the rings R and $\prod_{i=1}^{r} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})$ are isomorphic. The conclusion follows easily from lemmas 1 and 2.

PROPOSITION 2. *Let X be a topological space and $R = C(X, \mathbb{R})$ be the ring of all continuous mappings from X to $\mathbb{R}$. Then R is an S-ring.*

Proof The function f is singular in R if and only if it vanishes at some point of X. When it happens, the same is true for the two continuous mappings $f_1 = f^{1/3}$ and $f_2 = f^{2/3}$ and $f = f_1 f_2$.

PROPOSITION 3. *Let R be the ring of all germs of C^∞ real functions on a neighbourhood of zero. Then $f \in S_i \Leftrightarrow f(0) = f'(0) = \cdots = f^{(i-1)}(0) = 0$.*

Proof Let us recall that a germ is an equivalence class with respect to the relation: $f \mathcal{R} g \Leftrightarrow f = g$ on a neighbourhood of zero. An element f of R is singular if and only if $f(0) = 0$ and a straightforward application of Leibniz's derivation rule shows that if $f = f_1 \cdots f_i$ is the product of i singular elements, the function f and its $i-1$ first derivatives vanish at 0. Conversely, if this is true, Taylor's formula gives, for x small enough:

$$f(x) = \frac{x^i}{(i-1)!} \int_0^1 (1-t)^{i-1} f^{(i)}(tx)dt \text{ and the conclusion follows.}$$

Remark 1: This result provides an exemple of a ring where the sequence S_i is not stationnary and does not "converge" to 0. Indeed the well known C^∞-function $f(x) = \exp(-1/x^2)$ whenever $x \neq 0$, clearly belongs to all the S_i without being 0. The explanation lies in the fact that the ring R of germs of C^∞ functions which is a local ring (S_1 is an ideal, hence the unique maximal ideal) is not noetherian: indeed, in a local noetherian ring, the intersection $\bigcap S_i$ is equal to $\{0\}$ as it results trivially from Krull's theorem (see e.g. Atiyah-Macdonald: Introduction to Commutative Algebra p.110 - Addison-Wesley 1969).

PROPOSITION 4. *Let K be a field and $R = M(n, K)$ be the ring of square matrices $n \times n$ with coefficients in K. Then R is an S-ring.*

Proof Let $A \in R$ be a singular matrix and $r < n$ be the rank of A. We know that A is equivalent to the matrix $J_r = \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$ where I_r denotes the identity matrix of order r, i.e. there exist two invertible matrices P and Q such that $A = PJ_rQ$. Since $J_r^2 = J_r$, we get $A = XY$ where $X = PJ_r$ and $Y = J_rQ$ are singular matrices.

COROLLARY 1. *The ring of bistochastic matrices of order n is an S-ring.*

Proof Recall that a matrix $M = (a_{i,j})$ is bistochastic if there exists d in K such that $\forall i, \sum_j a_{ij} = d$ and $\forall j, \sum_i a_{ij} = d$. It is easy to prove that M is bistochastic if and only if $M(H) \subset H$ and $M(D) \subset D$ where H denotes the hyperplane of K^n equipped with its canonical basis $\{e_1 \ldots, e_n\}$, of equation $\sum_i x_i = 0$ and D is the one dimensional subspace generated by $\sum_i e_i$. Hence, there exists an invertible matrix P, independent of M, satisfying $M = P \begin{bmatrix} A & 0 \\ 0 & \lambda \end{bmatrix} P^{-1}$; where A is an element of $M(n-1, K)$. This defines an isomorphism between the ring of bistochastic matrices and $M(n-1, K) \times K$ and the conclusion follows from lemma 1.

2. Singular polynomial decompositions of matrices

From now on, A will denote a square matrix, P and Q will be polynomials.

PROPOSITION 5. *The singular matrix A can be written as $P(A)Q(A)$, where $P(A)$ and $Q(A)$ are singular if and only if 0 is a simple root of the minimal polynomial of A.*

Proof Let us recall that the minimal polynomial of A is the unitary generator π of the ideal of all polynomials which vanish at A. The roots of π in the field K are the eigenvalues of A in K. In particular, 0 is a root of π since A is singular.

The sufficient condition is easy to prove: one can write, $0 = \pi(A) = \lambda A + AQ(A)$ with $\lambda \neq 0$, Q being a polynomial vanishing at 0; so that $A = (-A/\lambda)Q(A)$ and the conclusion follows, since $Q(A)$ is singular ($Q(A)$ admits $Q(0) = 0$ as an eigenvalue). Conversely, if $A = P(A)Q(A)$, the minimal polynomial of A divides the polynomial $X - P(X)Q(X)$: it is enough to prove that 0 is a simple root of $X - P(X)Q(X)$. Let us first remark that the equality $A = P(A)Q(A)$ remains true for any matrix B similar to A, so that, considering an upper triangular matrix B similar to A, (we could need to extend the ground field) we get $\lambda_i = P(\lambda_i)Q(\lambda_i)$ for any eigenvalue λ_i of A this implies that if $\lambda_i \neq 0, P(\lambda_i) \neq 0$ and $Q(\lambda_i) \neq 0$, so necessarily, since $P(A)$ and $Q(A)$ are singular, $P(0) = Q(0) = 0$ and the required conclusion follows easily.

Remark 2: An equivalent way to characterize such matrices is the following: 0 is a simple root of the minimal polynomial if and only if $\ker(A) = \ker(A^2)$.

Remark 3: Let R be the ring $K[A]$; it results from the proof of proposition 5 that if $A \in S_2$, then $A \in S_i, \forall i$ (once we have written $A = (-A/\lambda)Q(A)$, we obtain $A = (A/\lambda^2)Q(A)Q(A)$, and so on). We will understand the situation much better in the following section (see Remark 8).

COROLLARY 2. *For $A = B^k$, there exist polynomials P and Q so that $A = P(A)Q(A)$ with $P(A)$ and $Q(A)$ singular matrices if and only if 0 is a root of the minimal polynomial of B of order $\leq k$.*

Proof This is an easy consequence of the fact already noticed in remark 2, that the order of 0 in the minimal polynomial of a matrix M is the first step where the increasing sequence $\ker(M^i)$ becomes stationnary: we have $\ker(B^k) = \ker(A) \subset \ker(B^{k+1}) \subset \cdots \subset \ker(B^{2k}) = \ker(A^2)$.

3. The ring $K[A]$ for itself

In this section it will be assumed that the field K is algebraically closed, although most results can be stated in a more general context; let us recall that the ring $R = K[A] = \{P(A),\ P \in K[X]\}$ is isomorphic to the quotient ring $K[X]/(\pi)$, where (π) denotes the principal ideal generated by the minimal polynomial of A. Writing π in the form $\pi(X) = \prod_i (X-\lambda_i)^{\alpha_i}$ $(\lambda_i \in K, \alpha_i \in \mathbb{N}^\star)$ it follows from the chinese remainder theorem (or from an adequate computation of the dimension of the underlying vector spaces) that $K[A]$ is isomorphic to the product ring $\prod_i K[X]/(X-\lambda_i)^{\alpha_i}$, so that we obtain, as for the ring $\mathbb{Z}/n\mathbb{Z}$, a first result:

PROPOSITION 6. *The ring $K[A]$ is an S-ring if and only if A is diagonalisable.*

Proof This is again a straightforward consequence of lemma·1, once we know that a matrix A can be reduced to the diagonal form if and only if the minimal polynomial of A has simple roots.

Remark 4: If K is no more algebraically closed, we can replace the statement of proposition 6 by the more general one: the ring $K[A]$ is an S-ring if and only if A is semisimple (i.e. diagonalisable over an extension K' of K).

Remark 5: It is not worthless to note that an element $M = P(A)$ of the ring $R = K[A]$ is invertible if and only if $\det(M) \neq 0$ or still, if and only if $P(X)$ and $\pi(X)$ are coprime: the first criterion results for instance, from a direct application of Cayley-Hamilton theorem; as for the second it is, in view of the isomorphism $K[A] \cong K[X]/(\pi)$, a consequence of Bezout theorem.

Before we start the study of the sets S_i for the ring $K[A]$, together with their $GL(A)$-action, we give a general lemma which can be more easily stated if the underlying set of the group $GL(R)$ of a ring R is denoted by $S_0(R)$:

LEMMA 3. *Let E and F be two rings and $E \times F$ be their product ring. Then, for $n \geq 1$*

$$S_n(E \times F) = \bigcup S_i(E) \times S_j(F) \text{ the union being taken over } i + j \geq n.$$

Proof Let $x = x_1 \cdots x_i$ be an element of $S_i(E)$ and $y = y_1 \cdots y_j$ an element of $S_j(F)$ where all the (x_k, y_k) are singular unless $i = 0$ or $j = 0$. We write $(x,y) = (x_1, 1) \cdots (x_i, 1)(1, y_1) \cdots (1, y_j)$; the element (x,y)

belongs to $S_{i+j}(E \times F) \subset S_n)$, since $i+j \geq n \geq 1$. Conversely, let $(x, y) = (x_1, y_1) \cdots (x_n, y_n)$ be an element of $S_n(E \times F)$ where all the couples (x_i, y_i) are singular. We write $(x, y) = (x_1 \cdots x_n, y_1 \cdots y_n)$ and we denote by i the number (possibly equal to 0) of x_k which are singular in E, so there are $(n-i)$ elements x_k which are invertible; the corresponding y_k are necessarily singular, so that at least $j \geq n-i$ elements among the y_k are singular and $y \in S_j(F)$; the result then follows from the hypothesis $x \in S_i(E)$.

Remark 6: The lemma can be easily extended by induction to the case of a finite product of rings $E_1, \ldots, E_t$.

Remark 7: For $n \geq 2$, the indexation in lemma 3 could be replaced by $i+j=n$. (For $n=1$, this is no more true because the factor $S_1 \times S_1$ cannot be taken into account). In the case of k rings, we get the same for $n \geq k$.

PROPOSITION 7. *Let $R = K[A]$ and $\pi(X) = \prod_i (X-\lambda_i)^{\alpha_i}, i = 1, \ldots, r$ the minimal polynomial of A, then $S_\infty = S_\rho$ where $\rho = \sum_i(\alpha_i - 1) + 1$.*

Proof Since the sets S_i behave well under ring isomorphisms, we look at the problem in the ring $R = \prod_i R_i$, where R_i denotes the quotient ring $K[X]/(X-\lambda_i)^{\alpha_i}$. Let $x = (x_1, \ldots, x_r)$ belong to $S_\rho(R)$; we shall prove that one of the components of x is zero, this will imply clearly that $x \in S_\infty$. From lemma 3, we have $x_j \in S_{\beta_j}(R_j)$, where $\sum_j \beta_j \geq \rho$, so that one of the β_i, say β_k is $\geq \alpha_k$ (otherwise, we would have $\sum_j \beta_j \leq \sum_j(\alpha_j - 1) < \rho$) which ensures $x_k \in S_{\alpha_k}(R_k) = \{0\}$. To end the proof, we notice that the element $x = ((X-\lambda_1)^{\alpha_1 - 1}, \ldots, (X-\lambda_r)^{\alpha_r - 1})$ is in $S_{\rho-1}$ but not in S_ρ (no component of x is equal to zero !)

Again Lemma 3 will be of use to establish the following criterion:

PROPOSITION 8. *An element $P(A)$ in the ring $R = K[A]$ belongs to S_2 if and only if P vanishes at at least two eigenvalues not necessary distinct of A or at an eigenvalue of order one in the minimal polynomial of A.*

Proof We keep the notation introduced in the precedent proof; the isomorphism between the ring $R = K[A]$ and the ring $\prod R_i$ is given by $P(A) \mapsto P_i$ where P_i denotes the class of the polynomial $P(X)$ in the quotient R_i. Hence, the element $P(A)$ belongs to S_2 if and only if one among the P_i belongs to $S_2(R_i)$ or at least two among the P_i, say P_t and P_s, belong to $S_1(R_t)$ and $S_1(R_s)$ respectively, the second alternative implies clearly that the polynomial P is divisible by $(X-\lambda_t)$ and by $(X-\lambda_s)$, the first alternative means that P is divisible by $(X-\lambda_i)^2$ if $\alpha_i \geq 2$ or $P_i = 0$ if $\alpha_i = 1$.

Remark 8: We understand now better the proposition 5 and the remark 3: to say that A belongs to S_2 means that the polynomial X (which cannot vanish at two eigenvalues of A !) vanishes at an eigenvalue of order 1 in π_A; since 0 is its only root, this means that 0 is a simple root of π_A. The image in the product $\prod R_i$ has one of its components 0 so, belongs to S_∞.

Remark 9: A necessary and sufficient condition in order that an element $P(A)$ belongs to S_3 could be stated: the polynomial must vanish at at least three roots, or must be divisible by $(X-\lambda)^2$ where λ is a root of order 2 of π_A, or vanish at a simple root of π_A The proof is left to the reader.

Our purpose until the end of this section will be the study of the orbits of $GL(A)$ on the S_i. We begin with the case $\pi(X) = (X-\lambda)^\alpha$ (i.e. $A = \lambda I + N$, N nilpotent). In this case $S_\alpha = \{0\} \subset S_{\alpha-1} \subset \cdots \subset S_1$ (strict inclusions). For $i = 1, \ldots, \alpha-1$, an element of $R = K[X]/(X-\lambda)^\alpha$ belongs to $S_i \setminus S_{i+1}$ if and only if it can be written as $(X-\lambda)^i Q(X), Q$ and π being mutually prime, which means in view of remark 5, that it belongs to the orbit of $(X-\lambda)^i$. This proves that the $S_i \setminus S_{i+1}$ along with S_α are the orbits of $GL(R)$ acting on S_1; in particular, there are α orbits.

The following lemma will permit us to compute the number of orbits in the general case:

LEMMA 4. *Let G_i denotes the group of invertible elements of the ring E_i, $i = 1, \ldots, k$ and let E be the product ring. Then $GL(E)$ is isomorphic to the product $\prod GL(E_i)$. Moreover, if α_i is the number of orbits of G_i acting on $S_1(E_i)$, then the number of orbits of $GL(E)$ on $S_1(E)$ is given by $(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_r+1)-1$.*

Proof The assertion concerning $GL(E)$ is trivial. As for the second, we begin with the case $n = 2$. Considering the action of $G_1 \times G_2$ on the set of singular elements of $R_1 \times R_2$, we can divide the orbits in three kinds: orbits of elements (x, y) where x and y are singular, orbits of elements (x, y) where x is singular and y is invertible and finally, orbits of those elements (x, y) where x is invertible and y singular. There are clearly $\alpha_1\alpha_2$ orbits of the first kind, α_1 of the second type and α_2 of the third, which gives $\alpha_1\alpha_2 + \alpha_1 + \alpha_2 = (\alpha_1+1)(\alpha_2+1)-1$, first and last. An induction argument will do with the general case.

PROPOSITION 9. *The action of $GL(A)$ on the set of singular elements of $K[A]$ determines $\prod_i(\alpha_i+1)-1$ orbits, $i = 1, \ldots, r$ if the minimal polynomial is given by $\prod_i(X-\lambda_i)^{\alpha_i}$.*

Proof it is an immediate consequence of lemma 4 and the discussion before.

COROLLARY 3. *The non empty sets $S_i \setminus S_{i+1}$, along with S_∞ are exactly the orbits of $GL(A)$ acting on $K[A]$ if and only if the matrix A can be written $A = \lambda I + N$, where $\lambda \in K$ and N nilpotent.*

Proof We have already established the sufficient condition. Conversely, our hypothesis implies that, in view of proposition 7 and 8,

$$\sum_i (\alpha_i - 1) + 1 = \prod_i (\alpha_i + 1) - 1$$

which is possible only if $r = 1$, that is $A = \lambda I + N$.

COROLLARY 4. *Let A have r distinct eigenvalues, then A is diagonalisable if and only if the number of orbits on the set of singular elements is $2^r - 1$.*

Proof This is clear since the condition is equivalent to $\alpha_i = 1, \forall i$.

PROPOSITION 10. *Let $S_\infty = S_\rho$ in the ring $R = K[A]$ and suppose that $K[A]$ is not an S-ring (i.e. $\rho \geq 2$), then the number of orbits of $GL(A)$ acting on the non-empty set $S_1 \setminus S_2$ is exactly the number of multiple roots of the minimal polynomial π_A. Moreover, the non-empty set $S_{\rho-1} \setminus S_\rho$ is exactly an orbit in the singular set.*

Proof We keep use of the isomorphism $R \cong \prod_i R_i$ with its $GL(A) \cong \prod_i GL(R_i)$ action; an element $(x_1, \dots, x_r)$ belongs to $S_1 \setminus S_2$ if and only if all the x_i but one, say x_k are invertible and x_k belongs to $S_1(R_k) \setminus S_2(R_k)$; this set is hence non empty and a $GL(R_k)$-orbit. We get so a correspondence between the orbit of the element $(x_1, \dots, x_r)$ and the necessary multiple eigenvalue α. As for the second assertion, we first make use of lemma 3: the element $(x_1, \dots, x_r)$ belongs to $S_{\rho-1} \setminus S_\rho$ if $x_i \in S_{\beta i}(R_{\beta i})$ and $\sum_i \beta_i \geq \rho - 1$ and no x_i is zero (cf. proof of proposition 7), that is $\beta_i \leq \alpha_i - 1$; since $\rho - 1 = \sum_i (\alpha_i - 1)$, we get $\beta_i = \alpha_i - 1$, for every i. But each $S_{\alpha_i - 1}(R_i) \setminus S_{\alpha_i}(R_i)$ is an orbit (even if $\alpha_i = 1$; see our convention of notation preceding lemma 3), the conclusion follows.

Remark 10: More generally, it is not difficult to establish that there is a one-to-one correspondence between the orbits in $S_k \setminus S_{k-1}$ and the r-uples $(a_1, \dots, a_r)$ for which $a_1 + \cdots + a_r = k$ and $0 \leq a_i \leq \alpha_i - 1$ for every i. This gives for example in the case of a matrix A with minimal polynomial $\pi_A(X) = X^3(X+1)^4(X-1)^3$ (here $\rho = (2+3+2)+1 = 8$ and the number of orbits is 79) exactly 3 orbits in $S_1 \setminus S_2$, 6 orbits in $S_2 \setminus S_3$, 8 orbits in

$S_3 \setminus S_4$, 8 orbits in $S_4 \setminus S_5$, 6 orbits in $S_5 \setminus S_6$, 3 orbits in $S_6 \setminus S_7$, one orbit in $S_7 \setminus S_8$ and 44 orbits in S_8.

Computing all the orbits in $S_1 \setminus S_\rho$, we need to know all the $(a_1, \ldots, a_r)$ such that $\forall i\ 0 \leq a_i \leq \alpha_i - 1$ and $1 \leq a_1 + \cdots + a_r \leq \rho - 1$. This last inequality is a consequence of the first r inequalities, so there are $(\alpha_1 \cdots \alpha_r - 1)$ orbits in $S_1 \setminus S_\infty$ and by substraction $\prod(\alpha_i + 1) - (\alpha_1 \cdots \alpha_r)$ orbits in S_∞ (result which is valid even if $\rho = 1$). It is now easy to solve the following:

Exercise 1: Prove that if A has exactly k distinct roots with $k \geq 2$, then A is diagonalisable if and only if there are $2^k - 1$ orbits of $GL(A)$ on S_∞. (Compare with corollary 4).

4. Permutable decompositions of singular matrices

If A is a singular matrix, we define $n(A)$ as the upper bound of the numbers m of singular permutative matrices A_i such that $A = A_1 \cdots A_m$. In order to compute the number $n(A)$ for a given matrix A, we need to introduce a special class of operators characterized by the following:

PROPOSITION 11. *For a given matrix acting on the finite dimensional vector space $E = K^n$, it is equivalent to say:*

a) $\dim \ker(A^2) = 2 \dim \ker(A)$

b) the Jordan cells of A associated with the eigenvalue 0 *are of order* ≥ 2

c) $\ker(A) \subset \operatorname{im}(A)$

d) the matrix A is similar to a matrix $\begin{bmatrix} 0 & X \\ 0 & Y \end{bmatrix}$ *written with respect to a direct decomposition of* $E = \ker(A) \oplus G$ *where the linear operators*

$$X : G \xrightarrow{A} E \xrightarrow{pr_1} \ker(A) \qquad Y : G \xrightarrow{A} E \xrightarrow{pr_2} G$$

satisfy $(\alpha) \ker(X) \oplus \ker(Y) = G$ *and* (β) *X is onto.*

Proof The equivalence between a) and b) results from the classical Jordan decomposition; the one between a) and c) is a direct consequence of the Frobenius injection $\varphi : \ker(A^2)/\ker(A) \to \ker(A)$ given by $\overline{x} \mapsto A(x)$; thus a) is equivalent to say that φ is surjective, which is exactly c). We prove now $a) \Rightarrow d)$: let C_1 be a complementary subspace of $\ker(A)$ in $\ker(A^2)$ and C_2 be a complementary subspace of $\ker(A^2)$ in E and write $G = C_1 \oplus C_2$ -we have already noticed that the restriction of A to C_1 is an isomorphism between C_1 and $\ker(A)$; the same is true for the restriction of X to C_1, since these restrictions are equal. It follows that X is onto and that C_1 and $\ker(X)$ are complementary in G. We need only to prove that $C_1 = \ker(Y)$; it is clear that $C_1 \subset \ker(Y)$, moreover, if A^+ denotes the restriction of A to G, A^+ is one-to-one so $\dim(C_1) + \dim(C_2) = rk(A^+) = rk \begin{bmatrix} X \\ Y \end{bmatrix} = rk([X \quad Y]) = rk(X) + rk(Y) = \dim(C_1) + rk(Y)$ and we are done.

Finally let us prove $d) \Rightarrow a)$: the matrix A^2 is similar to $\begin{bmatrix} 0 & XY \\ 0 & Y^2 \end{bmatrix}$ and with respect to the direct decomposition $E = \ker(A) \oplus G$, to say that the vector column $\begin{bmatrix} u \\ v \end{bmatrix}$ is in $\ker(A^2)$ means that $v \in \ker(Y^2) \cap \ker(XY)$ and u is arbitrary in $\ker(A)$; but $\ker(Y) = \ker(Y^2) \cap \ker(XY)$ if $\ker(X) \cap \ker(Y) = \{0\}$ (easy) so that $v \in \ker(Y)$. We end the proof by noting that since X is onto and $G = \ker(X) \oplus \ker(Y)$, we have in fact $\dim\ker(Y) = \dim\ker(A)$.

We are able to state the main result of this section:

PROPOSITION 12. *The number $n(A)$ is finite if and only if A satisfies the equivalent properties given in proposition 11. In which case $n(A) = \dim\ker(A)$.*

Proof The matrix A is similar to a matrix B of the form:

$B = \begin{bmatrix} B_0 & & & \\ & B_1 & 0 & \\ & 0 & \ddots & \\ & & & B_k \end{bmatrix}$, the matrix B_0 being invertible and each of the matrices B_i being a Jordan cell associated to the eigenvalue 0 (obviously, $k = \dim\ker(A)$ and moreover B_0 is absent if A is nilpotent). If one of the B_i is of order 0, the matrix A is similar to $B = \begin{bmatrix} B' & 0 \\ 0 & 0 \end{bmatrix}$ and $B = B_1 \times B_2 \times \cdots \times B_p$, with $B_1 = B$, $B_2 = \cdots = B_p = \begin{bmatrix} I_{n-1} & 0 \\ 0 & 0 \end{bmatrix}$ (with evident notation), all these matrices are singular and permutative, and we can choose p as large as we want: $n(A) = \infty$. When $\dim\ker(A^2) = 2\dim\ker(A)$, we have $B = B'_1 \times \cdots \times B'_k$ where $B'_1 = \begin{bmatrix} B_0 & & & \\ & B_1 & & 0 \\ & & Id & \\ & 0 & & \ddots \\ & & & & Id \end{bmatrix}$ (the blocks B_0 and B_1 kept unchanged and the others replaced by Id) and for $i = 2, \ldots, k$, $B'_i = \begin{bmatrix} Id & & & \\ & \ddots & & 0 \\ & & B_i & \\ 0 & & \ddots & \\ & & & Id \end{bmatrix}$ (we replace all the blocks B_j by Id, except B_i which remains unchanged); again these matrices are singular and permutative so $n(A) \geq k = \dim\ker(A)$.

We proceed to prove the opposite inequality (in due course we shall need two lemmas). Suppose that $M = \begin{bmatrix} 0 & X \\ 0 & Y \end{bmatrix}$ given by proposition 11 can be written as a product $N_1 \cdots N_{k+1}$, where the N_i are permutable matrices; we shall show that one of the N_i must be invertible.

Let us write $N_i = \begin{bmatrix} S_i & D_i \\ R_i & C_i \end{bmatrix}$ according to the decomposition of M. The first remark is $R_i = 0$. Indeed, since N_i and M commute, $N_i(\ker(M)) \subset \ker(M)$, that is $R_i = 0$. It follows that the S_i are permutative and that $S_1 \times S_2 \cdots \times S_{k+1} = 0$.

LEMMA 5. *Let $S_1, \ldots, S_{k+1}$ be permutative matrices of order k satisfying $S_1 \times S_2 \times \cdots \times S_{k+1} = 0$, then after reindexation $S_1 \times S_2 \times \cdots \times S_k = 0$.*

Proof By induction. The result is trivial for $k = 1$; if S_{k+1} is invertible, the conclusion is clear since we may multiply on the right by its inverse. We may then suppose that the dimension d of the image subspace $\mathrm{im}(S_{k+1})$ is strictly smaller than n. If S'_i, $i = 1, \ldots, n$, denotes the restriction (everything commute with S_{k+1}) of S_i to the subspace $\mathrm{im}(S_{k+1})$, we have $S'_1 \times S'_2 \times \cdots \times S'_k = 0$. This last expression can be thought (by grouping if necessary some operators toghether) as the null product of $d + 1$ commuting operators in a $d-$dimensional space. By induction hypothesis, we get (after possible reindexation, and reinserting of some possible operators) $S'_1 \times S'_2 \times \cdots \times S'_{k-1} = 0$, and conclude that at the level of the hole space $S_1 \times S_2 \times \cdots \times S_{k-1} \times S_{k+1} = 0$.

Accordingly, we may suppose that $S_1 \times \cdots \times S_k = 0$ and that, denoting the product $N = N_1 \cdots N_k$ by $\begin{bmatrix} 0 & H \\ 0 & U \end{bmatrix}$ and N_{k+1} by $\begin{bmatrix} R & S \\ 0 & T \end{bmatrix} = 0$,

$X = HT = RH + SU$ (i)

$Y = UT = TU$ (ii), since $M = NN_{k+1} = N_{k+1}N$.

The last step of the proof will consist of proving that R and T are invertible.

(i) and (ii) imply that $\ker(T) \subset \ker(X)$ and $\ker(T) \subset \ker(Y)$ so that $\ker(T) = \{0\}$: T is invertible. Now since T is invertible, again (ii) shows that $\ker(U) = \ker(Y)$ and (i) shows that $rk(H) = rk(X)$.

Keeping the notations of proposition 11, we assert that $G = \ker(X) \oplus \ker(U)$ and $G = \ker(H) \oplus \ker(U)$; the first equality is now clear, the second will be established if $\ker(H) \cap \ker(U) = \{0\}$, but this is easy since $\ker(H) \cap \ker(U) \subseteq \ker(U) = \ker(Y)$ and by (i) $\ker(H) \cap \ker(U) \subset \ker(X)$. We get now the invertibility of R from the following lemma:

LEMMA 6. *Consider the diagram:*

$$\begin{tikzcd} & G \arrow[r, "u"] \arrow[dl, "h"'] \arrow[d, "x"] & G \arrow[dl, "s"] \\ F \arrow[r, "r"] & F & \end{tikzcd}$$

and suppose that $x = r \circ h + s \circ u$ *together with* $\ker(h)$ *and* $\ker(x)$ *in direct summand with* $\ker(u)$ *in* G, *then* r *induces an isomorphism between the images of* h *and* x.

Proof This is immediate as soon as we consider the restrictions to $\ker(u)$ of the mappings given on G.

COROLLARY 5. *If* $n(A^k)$ *is finite then* $n(A^k) = k \cdot n(A)$.

Proof Write $\{0\} \subset \ker(A) \subset \ker(A^2) \subset \cdots \subset \ker(A^k) \subset \ker(A^{k+1}) \subset \cdots \subset \ker(A^{2k})$. Since $\dim\ker(A^{2k}) = 2\dim\ker(A^k)$, the Frobenius inequalities:

$\dim\ker(A^{k+1}) - \dim\ker(A^k) \leq \dim\ker(A^k) - \dim\ker(A^{k-1})$ are in fact equalities so $\dim\ker(A^k) = k \cdot \dim\ker(A)$.

Remark 11: The preceding corollary shows in particular that if $n(A)$ is odd, the matrix A has no square root.

PROPOSITION 13. *Suppose* $n(A) < \infty$, *and let* $A = X_1 \cdots X_m$ *a permutative singular maximal decomposition of* A ($m = n(A)$), *then* $\forall i,\ n(X_i) < \infty$ *and is* $= 1$.

Proof We have $\ker(X_i) \subset \ker(A) \subset \operatorname{im}(A) \subset \operatorname{im}(X_i)$, since the X_i commute. So $n(X_i)$ is finite. We proceed, for proving $n(X_i) = 1$, by induction on $m = \dim\ker(A)$; the case $m = 1$ is trivial. Write $A = X_1 \cdot B$ where $B = X_2 \cdots X_m$; as for X_i, we prove that $n(B)$ is finite, but B is already written as $m-1$ permutative singular matrices, hence $n(B) \geq m-1$. Remember now that $\ker(B) \subset \ker(A)$ so either $\dim\ker(B) = m-1$ or m; we prove that it is not m: otherwise, the inclusion $\operatorname{im}(A) \subset \operatorname{im}(B)$ would in fact be an equality. Write now: $\operatorname{im}(B) = \operatorname{im}(A) = X_1(\operatorname{im}(B))$. This means that X_1 leaves $\operatorname{im}(B)$ invariant, and its restriction to $\operatorname{im}(B)$ is surjective, and hence $\ker(X_1) \cap \operatorname{im}(B) = \{0\}$. But $\ker(X_1) \subset \ker(A) \subset \operatorname{im}(A) = \operatorname{im}(B)$, so X_1 is bijective which is false. We have in fact $\dim\ker(B) = m-1$, and $n(X_j) = 1\ \forall j \geq 2$ by induction hypothesis. Since we could have chosen $B = X_1 \cdots X_{m-1}$, the fact $n(X_i) = 1$ is clear.

The next result is a simple application of proposition 12 to permutative decomposition of singular bistochastic matrices: if A is such a matrix we define $n_s(A)$ as the upper bound of the number m of singular permutative bistochastic matrices A_i such that $A = A_1 \cdots A_m$.

PROPOSITION 14. *For a bistochastic matrix,* $n_s(A) = n(A)$.

Proof We make again use of the isomorphism between the ring of bistochastic matrices and the product ring $M_{n-1}(K) \times K$, and may suppose $A = \begin{bmatrix} A_1 & 0 \\ 0 & \lambda \end{bmatrix}$ (see the proof of corollary 1); if $\lambda = 0$, $n_s(A) = n(A) = \infty$; and if $n(A) < \infty$ the scalar λ is different from 0 (proposition 11 b)) and $n(A) = n(A_1)$ the conclusion follows easily.

We look in this final paragraph to the upper bound $m(A)$ of numbers k such that $A = A_1 \cdots A_k$ where the A_i are singular and quasi-commutative (i.e. $A_iA_j - A_jA_i$ is nilpotent).

PROPOSITION 15. $m(A) = \infty, \forall A$.

Proof The problem behaves well under base change, and a simple argument similar to the one given at the beginning of the proof of proposition 12, shows that we only need to consider the case when A is a Jordan cell J_n associated to the zero eigenvalue. But if $B = \begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & 0 \end{bmatrix}$, we have for every m, $B^mJ_n = BJ_n = J_n$; we get the result by noting that two triangular matrices are quasi-commutative.

Exercises: 2 - Given an arbitrary matrix A, prove that there exists an invertible matrix P, such that $n(PA) < \infty$.

3 - Prove that if $n(A \otimes B) < \infty$, where $A \otimes B$ is the tensor

product of A and B, then either A or B is invertible.

4 - Prove that if $p \geq 2$, then $n(\Lambda^p A) = \infty$. (We have denoted by $\Lambda^p A$ the p^{th} exterior power of A).

5 - Prove that the ring of upper triangular matrices is an S-ring. Use this fact to give another proof of proposition 15.

References

[1] GLAZMAN-LIUBITCH, *Analyse linéaire dans les espaces de dimension finie*, Editions Mir, Moscou (1972).

[2] JACOBSON N, *Lectures in abstract algebra II- Linear algebra*, D. Van Nostrand New-York, (1953).

Université de Paris VII
Département de Mathématiques
Tour 45.55, 5e étage
2, place Jussieu
75251 PARIS Cedex 05

and

Université de NICE
Parc Valrose
06034 NICE Cedex.