Graduate Texts in Mathematics

216

Matrices

Springer-Verlag

Denis Serre

Matrices

Theory and Applications

Springer

Denis Serre
Ecole Normale Supérieure de Lyon
UMPA
Lyon Cedex 07, F-69364
France
Denis.SERRE@umpa.ens-lyon.fr

Mathematics Subject Classification (2000): 15-01

Library of Congress Cataloging-in-Publication Data
Serre, D. (Denis)
[Matrices. English.]
Matrices : theory and applications / Denis Serre.
p. cm.—(Graduate texts in mathematics ; 216)
Includes bibliographical references and index.
ISBN 0-387-95460-0 (alk. paper)
1. Matrices I. Title. II. Series.
QA188 .S4713 2002
512.9′434—dc21 2002022926

ISBN 0-387-95460-0 Printed on acid-free paper.

Translated from *Les Matrices: Théorie et pratique*, published by Dunod (Paris), 2001.

Printed in the United States of America.

9 8 7 6 5 4 3 2 1 SPIN 10869456

Typesetting: Pages created by the author in LaTeX2e.

www.springer-ny.com

Springer-Verlag New York Berlin Heidelberg
A member of BertelsmannSpringer Science+Business Media GmbH

To Pascale and Joachim

Preface

The study of matrices occupies a singular place within mathematics. It is still an area of active research, and it is used by every mathematician and by many scientists working in various specialities. Several examples illustrate its versatility:

- Scientific computing libraries began growing around matrix calculus. As a matter of fact, the discretization of partial differential operators is an endless source of linear finite-dimensional problems.
- At a discrete level, the maximum principle is related to nonnegative matrices.
- Control theory and stabilization of systems with finitely many degrees of freedom involve spectral analysis of matrices.
- The discrete Fourier transform, including the fast Fourier transform, makes use of Toeplitz matrices.
- Statistics is widely based on correlation matrices.
- The generalized inverse is involved in least-squares approximation.
- Symmetric matrices are inertia, deformation, or viscous tensors in continuum mechanics.
- Markov processes involve stochastic or bistochastic matrices.
- Graphs can be described in a useful way by square matrices.

- Quantum chemistry is intimately related to matrix groups and their representations.
- The case of quantum mechanics is especially interesting: Observables are Hermitian operators, their eigenvalues are energy levels. In the early years, quantum mechanics was called "mechanics of matrices," and it has now given rise to the development of the theory of large random matrices. See [23] for a thorough account of this fashionable topic.

This text was conceived during the years 1998–2001, on the occasion of a course that I taught at the École Normale Supérieure de Lyon. As such, every result is accompanied by a detailed proof. During this course I tried to investigate all the principal mathematical aspects of matrices: algebraic, geometric, and analytic.

In some sense, this is not a specialized book. For instance, it is not as detailed as [19] concerning numerics, or as [35] on eigenvalue problems, or as [21] about Weyl-type inequalities. But it covers, at a slightly higher than basic level, all these aspects, and is therefore well suited for a graduate program. Students attracted by more advanced material will find one or two deeper results in each chapter but the first one, given with full proofs. They will also find further information in about the half of the 170 exercises. The solutions for exercises are available on the author's site `http://www.umpa.ens-lyon.fr/~serre/exercises.pdf`.

This book is organized into ten chapters. The first three contain the basics of matrix theory and should be known by almost every graduate student in any mathematical field. The other parts can be read more or less independently of each other. However, exercises in a given chapter sometimes refer to the material introduced in another one.

This text was first published in French by Masson (Paris) in 2000, under the title *Les Matrices: théorie et pratique*. I have taken the opportunity during the translation process to correct typos and errors, to index a list of symbols, to rewrite some unclear paragraphs, and to add a modest amount of material and exercises. In particular, I added three sections, concerning alternate matrices, the singular value decomposition, and the Moore–Penrose generalized inverse. Therefore, this edition differs from the French one by about 10 percent of the contents.

Acknowledgments. Many thanks to the Ecole Normale Supérieure de Lyon and to my colleagues who have had to put up with my talking to them so often about matrices. Special thanks to Sylvie Benzoni for her constant interest and useful comments.

Lyon, France
December 2001

Denis Serre

List of Symbols

Contents

1
Elementary Theory

1.1 Basics

1.1.1 Vectors and Scalars

Fields. Let $(K, +, \cdot)$ be a field. It could be $\mathbb{R}$, the field of real numbers, $\mathbb{C}$ (complex numbers), or, more rarely, $\mathbb{Q}$ (rational numbers). Other choices are possible, of course. The elements of K are called *scalars*.

Given a field k, one may build larger fields containing k: algebraic extensions $k(\alpha_1, \dots, \alpha_n)$, fields of rational fractions $k(X_1, \dots, X_n)$, fields of formal power series $k[[X_1, \dots, X_n]]$. Since they are rarely used in this book, we do not define them and let the reader consult his or her favorite textbook on abstract algebra.

The digits 0 and 1 have the usual meaning in a field K, with $0 + x = 1 \cdot x = x$. Let us consider the subring $\mathbb{Z}1$, composed of all sums (possibly empty) of the form $\pm(1 + \cdots + 1)$. Then $\mathbb{Z}1$ is isomorphic to either $\mathbb{Z}$ or to a field $\mathbb{Z}/p\mathbb{Z}$. In the latter case, p is a prime number, and we call it the *characteristic* of K. In the former case, K is said to have characteristic 0.

Vector spaces. Let $(E, +)$ be a commutative group. Since E is usually not a subset of K, it is an abuse of notation that we use $+$ for the additive laws of both E and K. Finally, let

$$\begin{array}{ccc} (a, x) & \mapsto & ax, \\ K \times E & \to & E, \end{array}$$

be a map such that

$$(a+b)x = ax + bx, \quad a(x+y) = ax + ay.$$

One says that E is a *vector space* over K (one often speaks of a K-vector space) if moreover,

$$a(bx) = (ab)x, \quad 1x = x,$$

hold for all $a, b \in K$ and $x \in E$. The elements of E are called *vectors*. In a vector space one always has $0x = 0$ (more precisely, $0_K x = 0_E$).

When $P, Q \subset K$ and $F, G \subset E$, one denotes by PQ (respectively $P + Q, F{+}G, PF$) the set of products pq as (p, q) ranges over $P{\times}Q$ (respectively $p{+}q, f{+}g, pf$ as p, q, f, g range over P, Q, F, G). A subgroup $(F, +)$ of $(E, +)$ that is stable under multiplication by scalars, i.e., such that $KF \subset F$, is again a K-vector space. One says that it is a *linear subspace* of E, or just a subspace. Observe that F, as a subgroup, is nonempty, since it contains 0_E. The intersection of any family of linear subspaces is a linear subspace. The sum $F + G$ of two linear subspaces is again a linear subspace. The trivial formula $(F + G) + H = F + (G + H)$ allows us to define unambiguously $F + G + H$ and, by induction, the sum of any finite family of subsets of E. When these subsets are linear subspaces, their sum is also a linear subspace.

Let I be a set. One denotes by K^I the set of maps $a = (a_i)_{i \in I} : I \to K$ where only finitely many of the a_i's are nonzero. This set is naturally endowed with a K-vector space structure, by the addition and product laws

$$(a+b)_i := a_i + b_i, \quad (\lambda a)_i := \lambda a_i.$$

Let E be a vector space and let $i \mapsto f_i$ be a map from I to E. A *linear combination* of $(f_i)_{i \in I}$ is a sum

$$\sum_{i \in I} a_i f_i,$$

where the a_i's are scalars, only finitely many of which are nonzero (in other words, $(a_i)_{i \in I} \in K^I$). This sum involves only finitely many terms. It is a vector of E. The family $(f_i)_{i \in I}$ is *free* if every linear combination but the trivial one (when all coefficients are zero) is nonzero. It is a *generating* family if every vector of E is a linear combination of its elements. In other words, $(f_i)_{i \in I}$ is free (respectively generating) if the map

$$\begin{aligned} K^I &\to E, \\ (a_i)_{i \in I} &\mapsto \sum_{i \in I} a_i f_i, \end{aligned}$$

is injective (respectively onto). Last, one says that $(f_i)_{i \in I}$ is a *basis* of E if it is free and generating. In that case, the above map is bijective, and it is actually an isomorphism between vector spaces.

If $\mathcal{G} \subset E$, one often identifies $\mathcal{G}$ and the associated family $(g)_{g\in\mathcal{G}}$. The set G of linear combinations of elements of $\mathcal{G}$ is a linear subspace E, called the linear subspace *spanned* by $\mathcal{G}$. It is the smallest linear subspace E containing $\mathcal{G}$, equal to the intersection of all linear subspaces containing $\mathcal{G}$. The subset $\mathcal{G}$ is generating when $G = E$.

One can prove that every K-vector space admits at least one basis. In the most general setting, this is a consequence of the axiom of choice. All the bases of E have the same cardinality, which is therefore called the *dimension* of E, denoted by $\dim E$. The dimension is an upper (respectively a lower) bound for the cardinality of free (respectively generating) families. In this book we shall only use finite-dimensional vector spaces. If F, G are two linear subspaces of E, the following formula holds:

$$\dim F + \dim G = \dim F \cap G + \dim(F + G).$$

If $F \cap G = \{0\}$, one writes $F \oplus G$ instead of $F + G$, and one says that F and G are in *direct sum*. One has then

$$\dim F \oplus G = \dim F + \dim G.$$

Given a set I, the family $(\mathbf{e}^i)_{i\in I}$, defined by

$$(\mathbf{e}^i)_j = \begin{cases} 0, & j \neq i, \\ 1, & j = i, \end{cases}$$

is a basis of K^I, called the *canonical basis*. The dimension of K^I is therefore equal to the cardinality of I.

In a vector space, every generating family contains at least one basis of E. Similarly, given a free family, it is contained in at least one basis of E. This is the *incomplete basis theorem.*

Let L be a field and K a subfield of L. If F is an L-vector space, then F is also a K-vector space. As a matter of fact, L is itself a K-vector space, and one has

$$\dim_K F = \dim_L F \cdot \dim_K L.$$

The most common example (the only one that we shall consider) is $K = \mathbb{R}$, $L = \mathbb{C}$, for which we have

$$\dim_{\mathbb{R}} F = 2 \dim_{\mathbb{C}} F.$$

Conversely, if G is an $\mathbb{R}$-vector space, one builds its *complexification* $G^{\mathbb{C}}$ as follows:

$$G^{\mathbb{C}} = G \times G,$$

with the induced structure of an additive group. An element (x, y) of $G^{\mathbb{C}}$ is also denoted $x + iy$. One defines multiplication by a complex number by

$$(\lambda = a + ib, z = x + iy) \mapsto \lambda z := (ax - by, ay + bx).$$

One verifies easily that $G^{\mathbb{C}}$ is a $\mathbb{C}$-vector space, with

$$\dim_{\mathbb{C}} G^{\mathbb{C}} = \dim_{\mathbb{R}} G.$$

Furthermore, G may be identified with an $\mathbb{R}$-linear subspace of $G^{\mathbb{C}}$ by

$$x \mapsto (x, 0).$$

Under this identification, one has $G^{\mathbb{C}} = G + iG$. In a more general setting, one may consider two fields K and L with $K \subset L$, instead of $\mathbb{R}$ and $\mathbb{C}$, but the construction of G^L is more delicate and involves the notion of tensor product. We shall not use it in this book.

One says that a polynomial $P \in L[X]$ *splits* over L if it can be written as a product of the form

$$a \prod_{i=1}^{r} (X - a_i)^{n_i}, \quad a, a_i \in L, \quad r \in \mathbb{N}, n_i \in \mathbb{N}^*.$$

Such a factorization is unique, up to the order of the factors. A field L in which every nonconstant polynomial $P \in L[X]$ admits a root, or equivalently in which every polynomial $P \in L[X]$ splits, is *algebraically closed.* If the field K' contains the field K and if every polynomial $P \in K[X]$ admits a root in K', then the set of roots in K' of polynomials in $K[X]$ is an algebraically closed field that contains K, and it is the smallest such field. One calls K' the *algebraic closure* of K. Every field K admits an algebraic closure, unique up to isomorphism, denoted by $\overline{K}$. The fundamental theorem of algebra asserts that $\overline{\mathbb{R}} = \mathbb{C}$. The algebraic closure of $\mathbb{Q}$, for instance, is the set of *algebraic* complex numbers, meaning that they are roots of polynomials $P \in \mathbb{Z}[X]$.

1.1.2 Matrices

Let K be a field. If $n, m \geq 1$, a matrix of size $n \times m$ with entries in K is a map from $\{1, \dots, n\} \times \{1, \dots, m\}$ with values in K. One represents it as an array with n rows and m columns, an element of K (an *entry*) at each point of intersection of a row an a column. In general, if M is the name of the matrix, one denotes by m_{ij} the element at the intersection of the ith row and the jth column. One has therefore

$$M = \begin{pmatrix} m_{11} & \dots & m_{1m} \\ \vdots & \ddots & \vdots \\ m_{n1} & \dots & m_{nm} \end{pmatrix},$$

which one also writes

$$M = (m_{ij})_{1 \leq i \leq n, 1 \leq j \leq m}.$$

In particular circumstances (extraction of matrices or minors, for example) the rows and the columns can be numbered in a different way, using nonconsecutive numbers. One needs only two finite sets, one for indexing the rows, the other for indexing the columns.

The set of matrices of size $n \times m$ with entries in K is denoted by $\mathbf{M}_{n\times m}(K)$. It is an additive group, where $M + M'$ denotes the matrix M'' whose entries are given by $m''_{ij} = m_{ij} + m'_{ij}$. One defines likewise multiplication by a scalar $a \in K$. The matrix $M' := aM$ is defined by $m'_{ij} = am_{ij}$. One has the formulas $a(bM) = (ab)M$, $a(M + M') = (aM) + (aM')$, and $(a+b)M = (aM) + (bM)$, which endow $\mathbf{M}_{n\times m}(K)$ with a K-vector space structure. The zero matrix is denoted by 0, or 0_{nm} when one needs to avoid ambiguity.

When $m = n$, one writes simply $\mathbf{M}_n(K)$ instead of $\mathbf{M}_{n\times n}(K)$, and 0_n instead of 0_{nn}. The matrices of sizes $n \times n$ are called *square* matrices. One writes I_n for the *identity* matrix, defined by

$$m_{ij} = \delta_i^j = \begin{cases} 0, & \text{if } i \neq j, \\ 1, & \text{if } i = j. \end{cases}$$

In other words,

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}.$$

The identity matrix is a special case of a *permutation matrix*, which are square matrices having exactly one nonzero entry in each row and each column, that entry being a 1. In other words, a permutation matrix M reads

$$m_{ij} = \delta_i^{\sigma(j)}$$

for some permutation $\sigma \in \boldsymbol{S}_n$.

A square matrix for which $i < j$ implies $m_{ij} = 0$ is called a *lower triangular* matrix. It is *upper* triangular if $i > j$ implies $m_{ij} = 0$. It is *strictly* upper triangular if $i \geq j$ implies $m_{ij} = 0$. Last, it is *diagonal* if m_{ij} vanishes for every pair (i, j) such that $i \neq j$. In particular, given n scalars $d_1, \ldots, d_n \in K$, one denotes by $\operatorname{diag}(d_1, \ldots, d_n)$ the diagonal matrix whose diagonal term m_{ii} equals d_i for every index i.

When $m = 1$, a matrix M of size $n \times 1$ is called a *column vector*. One identifies it with the vector of K^n whose ith coordinate in the canonical basis is m_{i1}. This identification is an isomorphism between $\mathbf{M}_{n\times 1}(K)$ and K^n. Likewise, the matrices of size $1 \times m$ are called *row vectors*.

A matrix $M \in \mathbf{M}_{n\times m}(K)$ may be viewed as the ordered list of its columns $M^{(j)}$ $(1 \leq j \leq m)$. The dimension of the linear subspace spanned by the $M^{(j)}$ in K^n is called the *rank* of M and denoted by $\operatorname{rk} M$.