Geometry of Matrices over Ring

Huang Liping

（环上矩阵几何）

SCIENCE PRESS
Beijing

Huang Liping

Geometry of Matrices over Ring

(环上矩阵几何)

SCIENCE PRESS
Beijing

Responsible Editor: Zhang Yang

Published by Science Press
16 Donghuangchenggen North Street
Beijing 100717, China

Printed in Beijing

ISBN 7-03-016982-4/ O.2461

Supported by National Natural Science
Foundation of China

Preface

We recall the Erlangen Program which was formulated by F. Klein in 1872. It says: "A geometry is the set of properties of figures which are invariant under the nonsingular linear transformations of some group". F. Klein pointed out the intimate relationship of geometry, group and invariants. Thus a fundamental problem in geometry is to characterize the transformation group of the geometry by as few geometric invariants as possible. The answer to this problem is often called the fundamental theorem of the geometry.

In the geometry of matrices, the points of the associated space are a certain kind of matrices, there is an arithmetic distance of two points in this space, and there is a transformation group acting on this space. Two distinct points are said to be adjacent if their arithmetic distance is one or minimal. L.-K. Hua discovered that the invariant "adjacency" alone is sufficient to characterize the group of motions of a certain kind of matrix space. Thus, the fundamental problem of the geometry of matrices is characterize the transformation preserving the adjacency of matrix spaces. The geometry of matrices has applications to algebra, geometry and theory of functions of several complex variables. The fundamental problem of the geometry of matrices can be interpreted as a theorem on graph automorphisms of the graph on a certain kind of matrices, and it also has practical applications in the linear (additive) preserver problems which are the research area in matrix and operator theory.

The study of the geometry of matrices was initiated by L.-K. Hua in the mid forties of the last century. At first, relating to his study of the theory of functions of several complex variables, he began to study four kinds of the geometry of matrices over the complex field, i.e., the geometry of rectangular matrices, symmetric matrices, skew-symmetric matrices and Hermitian matrices. Later he discussed the geometry of symmetric matrices over a field of characteristic not 2 in 1949. In 1951, he studied the geometry of rectangular matrices over a division ring. Hua's work was continued by many mathematicians, and more general results have been obtained. On the geometry of matrices over a field or division ring, one may refer to Z.-X. Wan's book "Geometry of Matrices" [102].

I am interested in the study of the geometry of matrices over some rings. The purpose of this book is to summarize some results obtained by the author and copartners on the geometry of matrices over a division ring or some rings so far. The study of the geometry of matrices over a ring is complicated and difficult, and some problems are expected to be resolved. In order to be as self-contained as possible this book covers some material of ring theory and module theory in Chapter 1, which is necessary for later chapters. Matrices over a ring constitute the main contents of Chapter 2. In Chapter 3, affine geometry and projective geometry over a Bezout domain or a division ring are introduced and studied. Following these chapters, the geometry of rectangular matrices over a Bezout domain, the geometry of Hermitian matrices and skew-Hermitian matrices over a division ring with an involution, the geometry of symmetric matrices over a commutative principal ideal domain, the geometry of block triangular matrices over a division ring, the geometry of matrices over a semisimple ring are discussed in detail in Chapters 4, 5, 6, 7 and 8, respectively. Applications to problems in algebra and geometry are included throughout this book.

I would like to express my thanks to professor Zhe-Xian Wan for his kindest suggestions and encouragement. A great number of friends and colleagues have given their time generously to help me with the manuscript. It is my great pleasure to thank especially professors Chong-Guang Cao, Zhong Yi and Yong-Yu Cai for their valuable comments, suggestions, and corrections. I would also like to express my thanks to my graduate students Kang Zhao, De-Qiong Li, Dan Liu and Tao Ban for their typewriting and carefully checking large parts of the manuscript. This work is supported by the National Natural Science Foundation of China project 10271021. This book is supported by the publishing sustentation fund of Changsha University of Science and Technology.

Li-Ping Huang
Changsha, Hunan
December, 2005

Notation

$\mathbb{N}$	set of natural numbers (nonnegative integers).
$\mathbb{Z}$	ring of integers.
$\mathbb{Q}$	field of rational numbers.
$\mathbb{R}$	field of real numbers.
$\mathbb{C}$	field of complex numbers.
$\mathbb{F}_2$	the finite field with 2 elements.
$x \in S$	x is a member of the set S.
$A \subseteq B$	A is contained in B.
$A \subset B$	A is a proper subset of B.
$A \cap B$	intersection of sets A and B.
$A \cup B$	union of sets A and B.
$B \setminus A$	set of members of B not in A.
$A \to B$	map from A to B.
$a \mapsto b$	map which takes a to b.
$f \circ g$	composite of maps f and g.
φ^{-1}	the inverse map of bijective map φ
$\operatorname{im} f$	image of the map f.
$\ker f$	kernel of a homomorphism f.
$f^{-1}(T)$	inverse image of set T under map f.
$f\|_A$	the restriction of f to A.
aH	left coset of a in group relation to subgroup H.
$\langle n \rangle$	set of all integers from 1 to n.
$\emptyset$	empty set.
$\|X\|$	cardinal number of the set X.
$\operatorname{char}(R)$	characteristic of ring R.
$Z_R,\ Z$	center of a ring R.
X^*	set of all invertible elements of a subset X of ring.
$R^\times$	set of non-zero elements of a ring R.

1	unit-element of a ring, or identity map.
$F = F(R, -)$	all symmetric elements of ring R with involution $^-$.
$K = K(D, -)$	all skew-symmetric elements of R with involution $^-$.
$\mathrm{Tr}(R)$	trace of a ring R with involution $^-$.
$a \mid b$	a is both left and right divisor of b.
$a \parallel b$	a is a total divisor of b.
δ_{ij}	Kronecker delta.
$\left(\frac{a,b}{Z}\right)$	quaternion division ring over field Z of $\mathrm{char}(Z) \neq 2$.
$\left[\frac{a,b}{Z}\right)$	quaternion division ring over field Z of $\mathrm{char}(Z) = 2$.
$\overline{X}$	subring or submodule spanned by X.
R/I	quotient ring whose elements $a + I$, $a \in R$.
$R[x]$	polynomial ring in an indeterminate x over ring R.
$R[x_1, \cdots, x_n]$	polynomial ring in n indeterminates over ring R.
(X)	an ideal which is generated by X.
$\mathrm{rad} R$	Jacobson radical of ring R.
$R_1 \times \cdots \times R_n$	direct product of the family of rings $\{R_1, \cdots, R_n\}$.
$A \cong B$	module A is isomorphic to module B.
$M_1 + \cdots + M_n$	sum of modules $M_1, \cdots, M_n$.
$\oplus\{M_i : i \in I\}$	internal direct sum of a family of modules.
$\dim_R F$, or $\mathrm{rk}\, F$	dimension of a free module F over a ring R.
$\mathrm{Hom}_{\mathrm{R}}(M, N)$	set of R-modules homomorphisms from M to N.
$[\alpha_1, \cdots, \alpha_r]$	module which is generated by $\alpha_1, \cdots, \alpha_r$.
$[X]$	free submodule of a free module generated by X.
$\langle \alpha_1, \cdots, \alpha_r \rangle$	subspace which is generated by $\alpha_1, \cdots, \alpha_r$, where $\{\alpha_1, \cdots, \alpha_r\}$ is unimodular.
$\overline{[X]}$	subspace of a free module M containing $[X]$.
$M_n(R)$	total matrix ring of degree n over ring R.
$R^{m \times n}$	set of all $m \times n$ matrices over R.
R^n	set of all n-component row vectors over R.
${}^nR$	set of all n-component column vectors over R.
$GL_n(R)$	set of all $n \times n$ invertible matrices over R.
$A_1 \oplus \cdots \oplus A_k$	block diagonal matrin diag $(A_1, \cdots, A_k)$

$\mathrm{diag}(a_1, \cdots, a_n)$	matrix with $a_1, \cdots, a_n$ on the main diagonal and all other entries zero.
$E_{ij}^{(m\times n)}, E_{ij}$	$m \times n$ matrix whose (i,j)-entry is 1 and all other entries are 0's.
$\mathrm{rank}(A)$	inner rank of matrix A over a ring.
I_r	$r \times r$ identity matrix.
$0^{(r)}$	$r \times r$ zero matrix.
${}^tA$	transpose of matrix A.
A^σ	the image of matrix A under the map σ.
${}^t\overline{P}$	involution transpose matrix of matrix P over ring R with involution $^-$.
A^{-1}	inverse matrix of matrix A.
A^-	g-inverse of matrix A.
$\mathcal{H}_n(D,-)$	set of $n \times n$ Hermitian matrices over a ring D with involution $^-$.
$\mathcal{H}_n[\alpha]$	all Hermitian matrices of the form $\sum_{1\leqslant s,t\leqslant r} x_{i_s i_t} E_{i_s i_t}^{(n)}$ where $\alpha = \{i_1, \cdots, i_r\} \subseteq \langle n \rangle$.
$\mathcal{S}_n(R)$	set of $n \times n$ symmetric matrices over commutative ring R.
$\mathcal{K}_n(F)$	set of $n \times n$ alternate matrices over a field F.
$\mathcal{SH}_n(D)$	set of $n \times n$ skew-Hermitian matrices over a ring D with involution.
$T_{(m_i,n_i,k)}(D)$	set of $k \times k$ block triangular matrices over ring D.
$T_{(n_i,k)}(D)$	$= T_{(n_i,n_i,k)}(D)$.
$A \cong B, A \to B$	matrices A and B are equivalent (associated).
$A \approx B$	Hermitian matrices A, B are cogradient.
$\|A\|$, $\det(A)$	determinant of matrix A over commutative ring.
$AG(V)$	left (right) affine geometry on a left (right) free module or an affine flat V.
$\overline{[\alpha_0 - \alpha_1] + \alpha_1}$	line passing through two distinct points α_0 and α_1.
$\dim(AG(V))$	dimension of left (right) affine geometry $AG(V)$.
$\mathrm{aff}\,\mathcal{E}$	intersection of all affine flats of $AG(V)$ containing $\mathcal{E}$.
$\mathrm{P}(M)$	left (right) projective geometry on a free module M.
$S \cup T$	join of two affine flats or projective flats S and T.

$\mathrm{pdim}(M)$	projective dimension of $\mathrm{P}(M)$.
$PGL_n(R)$	projective general linear group of degree n.
$W^{\perp}$	dual flat of projective flat W.
$\mathrm{P}(M,k)\setminus H$	generalized left (right) affine geometry.
$\mathrm{ad}(A,B)$	arithmetic distance between points A and B.
$\mathrm{d}(A,B)$	distance between points A and B.
$A\sim B$	point A is adjacent to point B.
$\mathcal{P}^{l}_{m+n-1,m-1}(R)$	left Grassmann space of $(m-1)$-flats in $\mathrm{P}(R^{m+n})$.
$\mathcal{PM}_{m\times(m+n)}(R)$	projective space of $m\times(m+n)$ matrices over R.
$D_{ij}(x)$	$D_{ij}(x)=xE_{ij}+\overline{x}E_{ji}$, $j\neq i$.
D_{ij}	$D_{ij}=E_{ij}+E_{ji}$, $j\neq i$.
$\mathcal{M}_i$	maximal set of rank 1 in $R^{m\times n}$ or $\mathcal{H}_n(D)$.
$\mathcal{N}_j$	maximal set of rank one in $R^{m\times n}$.
$\mathcal{M}_{1j}$	maximal set of rank 1 in $\mathcal{H}_n(D)$.
$\mathcal{L}_i$	maximal set of rank 2 in $R^{m\times n}$ or $\mathcal{H}_n(D)$.
$\mathcal{L}_{1j}$	maximal set of rank 2 in $\mathcal{H}_n(D)$.
$J(\mathcal{H}_n(D,-))$	Jordan ring of $n\times n$ Hermitian matrices over division ring D with involution $^{-}$.
$\perp$	null system (or symplectic polarity) of $\mathrm{P}(D^{2n})$.
$S^{\perp}$	$\{x\in D^{2n}: xJ\,{}^t\overline{S}=0\}$, where $S\in\mathcal{H}_n(D)$.
$U_{2n}(D,J)$	unitary group of degree $2n$ over D with respect to J.
$\mathcal{PH}_n(D)$	projective space of $n\times n$ Hermitian matrices over D.
$\mathcal{PS}_n(F)$	projective space of $n\times n$ symmetric matrices over field F (or space of the null system $\perp$).
A^{+}	$A^{+}=(a'_{ij})\in D^{n\times m}$, where $A=(a_{ij})\in D^{m\times n}$ and $a'_{ij}=a_{m+1-j,n+1-i}$.
$\psi^{(r)}_{A_r}(X)$	map of the form $X+X\begin{pmatrix}0 & A_r\\ 0 & 0\end{pmatrix}X$, $X\in T_{(n_i,k)}$.
$\mathcal{R}_i$	maximal set of rank 1 of the form $\mathcal{M}_i\cap T_{(n_i,k)}$.
$\mathcal{C}_j$	maximal set of rank 1 of the form $\mathcal{N}_j\cap T_{(n_i,k)}$.
X_D	D-representation matrix of a matrix X over semisimple Artinian ring.
$\mathcal{D}_{(m_i,n_i,r)}$	$\{\mathrm{diag}(X_1,\cdots,X_r): X_i\in D_i^{m_i\times n_i}\}$, where $D_1,\cdots,D_r$ are r division rings.
$\mathcal{D}_{(n_i,r)}$	$=\mathcal{D}_{(n_i,n_i,r)}$.

Contents

Chapter 1

Rings and Modules

The basic facts regarding ring theory and module theory can be found in many textbooks, e.g. [67, 75, 16, 17, 18, 69]. In order to be as self-contained as possible this chapter covers some material of ring theory and module theory which is necessary for later chapters. We state them but omit all proofs. The reader who already knows these basic concepts can immediately start with section 1.5. From sections 1.1 to section 1.4, we give a short introduction into ring theory and module theory. For further concepts and results reader may refer to the bibliography of this book. In section 1.5, we introduce some results of rings having an involution, and study the weak automorphisms of division ring with involution.

Throughout this book, all rings are associative, with a unit element 1 which is preserved by homomorphisms, inherited by subrings. Usually our rings are *nontrivial*, i.e., $1 \neq 0$.

1.1 Rings

Throughout this book, let $|X|$ be the cardinal number (cardinality) of the set X, $\mathbb{F}_2 = \{0, 1\}$ the finite field of two elements.

Let $f : A \to B$ and $g : B \to C$ be maps. The *composite* of f and g is the map $A \to C$ given by $a \mapsto g(f(a))$, $a \in A$. The composite map is denoted by $g \circ f$ or simply gf. If $T \subset B$, the *inverse image of* T under f, denoted by $f^{-1}(T)$, is the set $\{a \in A : f(a) \in T\}$. Map f is said to be *injective* (or *one-to-one*) provided for all $a, a' \in A$, $a \neq a' \Rightarrow f(a) \neq f(a')$; alternatively, f is injective if and only if for all $a, a' \in A$, $f(a) = f(a') \Rightarrow a = a'$. f is said to be *surjective* (or *onto*) provided $f(A) = B$; f is said to be *into* provided $f(A) \subset B$; f is said to be *bijective* (or a *bijection* or a *one-to-one correspondence*) if it is both injective and surjective.

If $f : A \to B$ is a map and $S \subset A$, then the map from S to B given by $a \mapsto f(a)$, for $a \in S$, is called the *restriction* of f to S and is denoted by $f|_S : S \to B$. If A is any set, the *identity map* on A (denoted by $1_A : A \to A$) is the map given by $a \mapsto a$. The symbol 1 is also used to denote the identity map $R \to R$. In the context this usage will not be ambiguous.

For $A_1, A_2 \subseteq A$, the following facts can be easily verified:

$$f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2), \tag{1.1.1}$$

$$f(A_1 \cup A_2) = f(A_1) \cup f(A_2), \tag{1.1.2}$$

$$f(A_1 \cap A_2) = f(A_1) \cap f(A_2), \text{ if } f \text{ is injective.} \tag{1.1.3}$$

Definition 1.1.1 *A ring is a nonempty set R together with two binary operations (usually denoted as addition (+) and multiplication) such that:*
(i) *$(R,+)$ is an abelian group (use the additive notation);*
(ii) *$(ab)c = a(bc)$ for all $a, b, c \in R$ (associative multiplication);*
(iii) *$a(b+c) = ab+ac$, $(a+b)c = ac+bc$ (left and right distributive laws);*
(iv) *there exists an identity element $1 \in R$ such that $1a = a1 = a$ for all $a \in R$.*

If R is a ring, and $ab = ba$ for all $a, b \in R$, then R is said to be a commutative ring.

Remark 1.1.2 *Throughout this book, all rings occurring are associative, but not generally commutative. Every ring has an identity element, denoted by 1, which is preserved by homomorphisms, inherited by subrings. Usually our rings are nontrivial or non-zero, i.e., $1 \neq 0$.*

The additive identity element of a ring is called the zero element and denoted 0. If R is a ring, $a \in R$ and $n \in \mathbb{Z}$, then na has its usual meaning for additive groups.

Let R be a ring and S a nonempty subset of R that is closed under the operations of addition and multiplication in R. If S is itself a ring under these operations then S is called a *subring* of R. An element a in a ring R is said to be left (resp. right) invertible if there exists $c \in R$ (resp. $b \in R$) such that $ca = 1$ (resp. $ab = 1$). The element c (resp. b) is called a left (resp. right) inverse of a. An element $a \in R$ that is both left and right invertible is said to be *invertible* or to be a *unit.* The set of all units in a ring R is denoted by R^*.

Throughout this book, let $R^\times = R \setminus \{0\}$ be the set of all non-zero elements of a ring R. If S is a subset of a ring R, let S^* be the set of all units (invertible elements) of S. Let

$$Z_R = \{a \in R : ax = xa, \ \forall x \in R\}$$

be the *center* of ring R (Z for short), Z is a commutative subring of R.

If R is a ring, we define the *opposite ring* R° as the ring whose additive group is the same as that of R, but with the multiplication defined by $x \cdot y =$

yx $(x, y \in R)$. Generally speaking, if we have a result for rings "on the right", then we can obtain an analogous result "on the left" by applying the known result to opposite rings.

An element of a ring is called an *atom*, or *irreducible*, if it is a non-unit which can not be written as a product of two non-units.

A non-zero element a in a ring R is said to be a *left* (*resp. right*) *zero divisor* if there is a non-zero $b \in R$ such that $ab = 0$ (resp. $ba = 0$). A *zero divisor* is an element of R which is both a left and a right zero divisor. An element that is neither 0 nor a left or right zero-divisor is called *regular.*

A non-zero ring R which has no left (or right) zero divisors is called a *domain.* A commutative domain is also called an *integral domain.*

A non-zero ring D in which every non-zero element is a unit is called a *division ring* or *skew field.* A *field* is a commutative division ring. Every domain or every division ring has at least two elements (namely 0 and 1). A ring R is a division ring if and only if the non-zero elements of R form a group under multiplication. Every division ring D is a domain.

Definition 1.1.3 *Let R and S be rings. A map $f : R \to S$ is called a* homomorphism of rings *if for all $a, b \in R$,*

$$f(a + b) = f(a) + f(b) \quad \text{and} \quad f(ab) = f(a)f(b).$$

If there exists a homomorphism $f : R \to S$, then we call that R and S are homomorphic rings.

Consequently the same terminology is used: a *monomorphism of rings* (resp. *epimorphism of rings* , *isomorphism of rings*) is a homomorphism of rings which is an injective (resp. surjective, bijective) map. A monomorphism of rings $R \to S$ is sometimes called an *embedding of R in S.* An isomorphism from R to itself is called an *automorphism of ring R.*

The *kernel of a homomorphism* of rings $f : R \to S$ is its kernel as a map of additive groups; that is, $\ker f = \{r \in R : f(r) = 0\}$. Similarly the *image of f*, denoted by $\mathrm{im} f$, is $\{s \in S : s = f(r) \text{ for some } r \in R\}$.

Definition 1.1.4 *Let R and S be rings. A map $f : R \to S$ is called an* anti-homomorphism *of rings if for all $a, b \in R$,*

$$f(a + b) = f(a) + f(b) \quad \text{and} \quad f(ab) = f(b)f(a).$$

If there exists an anti-homomorphism $f : R \to S$, then we call that R and S are anti-homomorphic. *An* anti-isomorphism *of rings is an anti-homomorphism of rings which is a bijective map. An anti-isomorphism from R to itself is called an* anti-automorphism *of R.*

Definition 1.1.5 *Let R and R' be two rings. A bijective map (resp. map) σ from R to R' is called a* ring semi-isomorphism *(resp.* ring semi-homomorphism*) if $(a+b)^\sigma = a^\sigma + b^\sigma$, $(aba)^\sigma = a^\sigma b^\sigma a^\sigma$, $1^\sigma = 1$, for all $a, b \in R$.*

Theorem 1.1.6 (Hua, [47]) *Let R be a ring and R' be a domain. Then every ring semi-homomorphism from R to R' is either a ring homomorphism or a ring anti-homomorphism.*

Proof [47]. Let σ be a ring semi-homomorphism from R to R'. For $a, b, c \in R$, we have

$$\begin{aligned}(abc+cba)^\sigma &= [(a+c)b(a+c) - aba - cbc]^\sigma \\ &= (a^\sigma + c^\sigma)b^\sigma(a^\sigma + c^\sigma) - a^\sigma b^\sigma a^\sigma - c^\sigma b^\sigma c^\sigma \\ &= a^\sigma b^\sigma c^\sigma + c^\sigma b^\sigma a^\sigma.\end{aligned} \tag{1.1.4}$$

By $(aba)^\sigma = a^\sigma b^\sigma a^\sigma$ and (1.1.4), we have

$$\begin{aligned}&[(ab)^\sigma - a^\sigma b^\sigma][(ab)^\sigma - b^\sigma a^\sigma] \\ =&[(ab)^\sigma]^2 + a^\sigma (b^\sigma)^2 a^\sigma - [a^\sigma b^\sigma (ab)^\sigma + (ab)^\sigma b^\sigma a^\sigma] \\ =&[(ab)^2 + ab^2a - ab(ab) - (ab)ba]^\sigma = 0.\end{aligned} \tag{1.1.5}$$

Since R' is a domain, $(ab)^\sigma = a^\sigma b^\sigma$ or $(ab)^\sigma = b^\sigma a^\sigma$.

Without loss of generality, we assume that $(ab)^\sigma = a^\sigma b^\sigma \neq b^\sigma a^\sigma$, we can prove that

$$(xb)^\sigma = x^\sigma b^\sigma, \ \forall\, x \in R. \tag{1.1.6}$$

In fact, suppose that $(xb)^\sigma = b^\sigma x^\sigma \neq x^\sigma b^\sigma$, we have $a^\sigma b^\sigma + b^\sigma x^\sigma = (ab)^\sigma + (xb)^\sigma = [(a+x)b]^\sigma = (a^\sigma + x^\sigma)b^\sigma$ or $b^\sigma(a^\sigma + x^\sigma)$, a contradiction. Similarly, we have

$$(ay)^\sigma = a^\sigma y^\sigma, \ \forall\, y \in R. \tag{1.1.7}$$

We assert that σ is a ring homomorphism, i.e.,

$$(xy)^\sigma = x^\sigma y^\sigma, \ \forall\, x, y \in R. \tag{1.1.8}$$

Suppose that there are two $c, d \in R$ such that $(cd)^\sigma = d^\sigma c^\sigma \neq c^\sigma d^\sigma$. Similarly, we can prove that $(ad)^\sigma = d^\sigma a^\sigma$, $(cb)^\sigma = b^\sigma c^\sigma$. By (1.1.6) and (1.1.7), we have $a^\sigma b^\sigma + a^\sigma d^\sigma + c^\sigma b^\sigma + d^\sigma c^\sigma = [(a+c)(b+d)]^\sigma = (a^\sigma + c^\sigma)(b^\sigma + d^\sigma)$ or $(b^\sigma + d^\sigma)(a^\sigma + c^\sigma)$, a contradiction. □

Let R be a ring. Denote by $M_n(R)$ (or $R^{n\times n}$) the set of all $n \times n$ matrices over R. By the addition and multiplication of matrices, $M_n(R)$ is a ring, which will be called the *total matrix ring of degree n over R*.