体上矩阵理论导引

◉ 庄瓦金 著

科学出版社
www.sciencep.com

体上矩阵理论导引

庄瓦金　著

科学出版社

北京

内 容 简 介

体上矩阵是非交换代数研究的基本方向之一. 本书论述了以谢邦杰教授为代表的中国学者自20世纪七八十年代以来在这个研究方向中所取得的一些主要成果. 书中第一章介绍了相关的基础知识;第二至第四章阐述了体上矩阵相抵、相似、合同的基本理论,并论及体上矩阵广义逆、特征值基础;第五章阐述了体上矩阵的 Dieudonné 行列式与谢邦杰行列式,并对四元数矩阵的诸行列式方案作了简析;第六、七章阐述了两个研究专题:四元数矩阵、矩阵偏序. 因此,本书不仅较系统地论述了一般体上矩阵理论,而且也阐述了应用前景广阔的四元数矩阵理论以及更一般的非交换主理想整环上矩阵的某些成果.

本书可作为大学数学系高年级学生选修课教材,也可作为代数相关方向的硕士、博士研究生的教材或其学位论文的主要参考书,还可作为数学、力学、物理学等相关专业的教师、科研人员的参考书.

图书在版编目(CIP)数据

体上矩阵理论导引/庄瓦金著. —北京:科学出版社,2006.6
ISBN 7-03-016979-4

Ⅰ. 体… Ⅱ. 庄… Ⅲ. 矩阵-理论-研究 Ⅳ. O151.21

中国版本图书馆 CIP 数据核字(2006)第016201号

责任编辑:吕 虹 赵彦超/责任校对:鲁 素
责任印制:安春生/封面设计:王 浩

科学出版社 出版
北京东黄城根北街16号
邮政编码:100717
http://www.sciencep.com

天时彩色印刷有限公司印刷

科学出版社编务公司排版制作
科学出版社发行 各地新华书店经销

*

2006年6月第 一 版 开本:B5(720×1000)
2006年6月第一次印刷 印张:19 3/4
印数:1—2 000 字数:375 000

定价:39.00元

(如有印装质量问题,我社负责调换〈环伟〉)

序　言

早在20世纪60年代初，著名数学家华罗庚、万哲先院士在其专著《典型群》[1]序中就明确指出："**体上的矩阵是一个值得注意的对象，因为它是一个不太失去普遍性的抽象事物，但同时又和成果丰富的具体的域上的矩阵距离不远.**"他们在典型群及矩阵几何方向上取得了举世公认的成就. 对体上一般矩阵理论而言，Boulbaki学派发起人之一、著名数学家 Dieudonné 在1943年给出了体上行列式的一种方案. 同年，著名代数学家 N. Jocobson 结合模论方法给出了非交换主理想整环上矩阵的相抵化简[2]；并于1953年出版了"Lectures in Abstract Algebra Vol. Ⅱ—Linear Algerbra"[4]（后列入 Springer 出版社的 Graduate Texts in Mathematics31），应该说这是国际上第一本论述体上线性代数的书，但该书在第三章阐述线性变换化简时便转向域上情形. 究其原因，是体上矩阵相似标准形的唯一性受到破坏，人们还拿不出体上矩阵相似标准形较系统的理论. 与之相伴，体上矩阵的特征值理论、行列式理论也十分艰难，因而使得体上矩阵的研究困难重重. 面对这些困难，著名代数学家 P. M. Cohn 曾长期予以关注，他在1977、1985及1995年的三本专著[5~7]中对体上矩阵的难题都有阐述，可实质性结果甚微. 有幸的是，在20世纪70与80年代之交，吉林大学数学系原主任谢邦杰教授在攻克上述难题方面有所突破[16~27]，得到了体上矩阵相似标准形、相似弱标准形存在定理，给出了体上矩阵特征值的概念，提出了新的行列式方案，因而为一类重要的四元数矩阵——自共轭四元数矩阵的研究打下了基础. 在谢先生工作引路下，一些刚从"文革"噩梦中醒过来的中国高校中青年数学教师也加入到体上矩阵的研究中，并取得一些进展. 本书力图反映中国学者在体上矩阵的一些主要工作，并希望能为进入这一研究方向的青年学者提供一本基础、便捷的入门专著.

全书共分七章，在第一章关于体的若干准备后，第二至四章分别阐述体上矩阵的三大基本关系：相抵（等价）、相似、合同. 注意到非交换主理想整环$\mathbf{R}$嵌入于商体$\mathbf{K}_{\mathbf{R}}$的事实，第二章在阐述$\mathbf{R}$上矩阵相抵化简、秩、满秩分解的基本结果后，重视这些结果对$\mathbf{R}$上右线性方程组、广义逆的应用，并作了较系统的论述. 第三章阐述的绝大部分内容是谢先生的工作，主要是特征矩阵$\lambda I_n - A$的弱法式、法式存在定理及其应用；在此基础上，按照 Cohn 的分类，简要地涉及体上矩阵的特征值问题，完整地阐述了四元数矩阵的右特征值及其 Jordan 标准形（它们分别在20世纪40年代末和50年代中获得解决）[31,32]. 第四章在论及体上自共轭、斜自共轭矩阵的合同化简之后，主要阐述四元数矩阵的酉对角化、酉三角化及酉相抵化简（奇异值分解定理）；同时也阐述了黄礼平最近才得到的可中心化四元数矩阵的自共轭分

解[89]. 第五章介绍 Dieudonné 行列式与谢邦杰行列式，并对四元数非交换行列式作些简析. 第六章专述四元数矩阵，在论及正定性、半正定性刻画及自共轭四元数矩阵的同时合同化简之后，阐述了四元数矩阵的行列式不等式、特征值与奇异值不等式；随后有选择地论及矩阵方程与广义逆. 最后的第七章全部是笔者关于矩阵偏序的工作. 我们从非交换主理想整环上矩阵的减序、左(右)星序、星序的刻画入手，随后阐述四元数矩阵范畴中诸偏序的统一刻画、半正定自共轭四元数矩阵 Löwner 偏序的刻画及其在此偏序下的正定自共轭四元数矩阵的几何均值、半正定自共轭四元数矩阵广义逆的单调性解集；同时，我们也关注诸偏序的泛性，在对 $B^*AB \overset{?}{\leqslant} A$，$A^2 \overset{?}{\leqslant} B^2$ 的考察之后，阐述了四元数矩阵极分解的成套定理，并用之去刻画四元数矩形阵的 GL 偏序，再次将星序、减序、Löwner 偏序联系起来.

值得注意的是，体上矩阵理论属非交换代数，正如著名代数学家 C. Ringel 在 1999 年的《世纪之交的代数》[28]的报告中所指出的：它是 21 世纪代数学研究中极具挑战性的方向。因此，本书也为此做了工作。当然，体上矩阵还有不少专题未被阐述，如矩阵几何、矩阵群、矩阵半群、线性保持问题；又如四元数矩阵的迹……对此，一是本书的容量所限，二是笔者喜好有异. 为弥补此不足，书末收入了较多参考文献，其中也包括实四元数矩阵理论的某些应用[251~258].

谢邦杰教授生前对本书的写作曾予大力支持，他给笔者寄来了自己发表的全部论文. 黄礼平、曹重光、陈建龙、杨忠鹏等教授也给笔者寄来了他们自己论文的题目或文章. 在中国召开的一些矩阵论国际学术会议上，从事体上矩阵研究的同行们也多次对本书的出版表示关心. 因此，本书能如愿出版，是与国内同行们的支持分不开的. 在此，特向上述教授及国内同行们表示衷心的感谢.

本书的出版得到了漳州师院专著出版基金、漳州市科技基金的全额资助，值此特向有关领导、专家表示衷心的感谢. 科学出版社吕虹编审、国家自然科学基金委员会雷天刚博士对本书的出版也给予不少帮助，值此也特向他们表示衷心的谢意.

当然，鉴于本书写作时间紧，笔者学识水平所限，书中定有不少缺点及失误，敬请广大读者批评指正.

庄瓦金

2006 年 1 月

符 号 表

$A \cong B$	矩阵 A 与 B 相抵
$A \simeq B$	矩阵 A 与 B 合同
$A \sim B$	矩阵 A 与 B 相似
$\overline{A}(\overline{a}_{ij})_{mn}$，其中 $A=(a_{ij})_{mn}$	
A'	矩阵 A 的转置
$A^*\overline{A}'$，A 的共轭转置	
A^{ρ}	体上矩阵 A 在对合函数 ρ 作用下的像
A^{d}	体上 n 阶矩阵 A 的 Draain 逆
$A^{\#}$	体上 n 阶矩阵 A 的群逆
A^{+}	矩阵 A 的 Moore-Penrose 逆
$A^{(i,\cdots,j)}$	矩阵 A 的 $(i,\cdots,j)$ 逆
A^{-}	矩阵 A 的(1)逆
$A\{i,\cdots,j\}$	矩阵 A 的 $(i,\cdots,j)$ 逆的全体
$A\{i,\cdots,j;t\}$	$\{X\in A\{i,\cdots,j\} \mid \mathrm{rank}X=t\}$
$\mathrm{Aut}(\mathbf{F})$	域 $\mathbf{F}$ 的自同构群
$\widetilde{A}$	体 $\mathbf{K}$ 上可中心化矩阵 A 的第一种有理弱标准形
$A\begin{pmatrix} i_1 & \cdots & i_t \\ j_1 & \cdots & j_t \end{pmatrix}$	矩阵 A 的第 $i_1,\cdots,i_t$ 行、第 $j_1,\cdots,j_t$ 列交叉处元素所成的 t 阶子矩阵
$A(i\mid j)$	划去矩阵 A 的第 i 行、第 j 列余下的子矩阵
$A_U^{i,\cdots,j}$	四元数矩阵 A 的列西 $(i,\cdots,j)$ 逆
A_c	四元数矩阵 A 的复表示
$A^{1/2}$	n 阶半正定自共轭四元数矩阵 A 的半正定平方根
$A\{i,\cdots,j;\geqslant\}$	$\{X\in A\{i,\cdots,j\} \mid X$ 是半正定自共轭四元数矩阵$\}$
$A\{i,\cdots,j;\geqslant;t\}$	$\{X\in A\{i,\cdots,j;\geqslant\} \mid \mathrm{rank}X=t\}$
$A\{i,\cdots,j;\geqslant,t;\leqslant B\}$	$\{X\in A\{i,\cdots,j;\geqslant;t\} \mid X\overset{L}{\leqslant}B\}$，这里 $B\in \mathbb{H}(n,*)$
$\boldsymbol{A}(A,B)$	正定自共轭四元数矩阵 A 与 B 的算术均值
$\overline{a}\sigma(a)$，σ 是 $\mathbf{K}(\mathbf{R})$ 的对合反自同构	
$\widetilde{B}$	体 $\mathbf{K}$ 上可中心化矩阵 A 的第二种有理弱标准形

$\mathbb{C}$	复数域
C_n	$GL_n(\mathbf{K})$的换位子群
ch$\mathbf{K}$(ch$\mathbf{F}$)	体 $\mathbf{K}$(域 $\mathbf{F}$)的特征
deg$f$	体上多项式 $f(x)$的次数
diag	对角矩阵符号
dim$V$	体上右(左)向量空间 V 的维数
$\widetilde{D}$	体 $\mathbf{K}$ 上可中心化矩阵 A 第一种广义 Jordan 弱标准形
$\det_c A \mid A \mid_c$	n 阶四元数矩阵 A 的陈龙玄行列式
det$A$	$\mathbf{K}$ 上 n 阶矩阵 A 的 Dieudonné 行列式
$D_s(a)$	倍法矩阵
$e_i(0,\cdots,0,\overset{i}{1},0,\cdots,0)'$	
End(V)	向量空间 V 的线性变换环
$\widetilde{E}$	体 $\mathbf{K}$ 上可中心化矩阵 A 第二种广义 Jordan 弱标准形
$\mathbf{F}$	域,形式实域
$\mathbf{F}_q$	含 q 个元素的有限域
$\mathbf{F}_q^*$	$\mathbf{F}_q^*$ 的乘法群
$\mathbf{F}_q^{*2}$	$\mathbf{F}_q^*$ 中平方元素组成的群
$\mathbf{F}(\tau,\sigma)$	域 $\mathbf{F}$ 上的形式 Laurent 级数体
$\mathbf{F}_A$	体 $\mathbf{K}$ 中包含 $\mathbf{F}$ 的由 A 的所有元素生成的子体
$\widetilde{\mathbf{F}}$	体 $\mathbf{K}$ 内域 $\mathbf{F}$ 的取定代数闭域
$\boldsymbol{F}(A,B)$	正定自共轭四元数矩阵 A 与 B 的右谱几何均值
$f(x) \mid g(x)$	体上多项式 $f(x)$左、右整除 $g(x)$
$f(x) \nmid$	$g(x)$体上多项式 $f(x)$不整除 $g(x)$
$GL_n(\mathbf{K})$	体 $\mathbf{K}$ 上的 n 阶完全线性群
GL(V)	向量空间 V 的非奇异线性变换群
$\boldsymbol{G}(A,B)$	正定自共轭四元数矩阵 A 与 B 的(度量)几何均值
$\mathbb{H}$	实四元数体
$\mathbb{H}(n,u)$	n 阶四元数酉矩阵的集合
$\mathbb{H}(n,*)$	n 阶自共轭四元数矩阵的集合
$\mathbb{H}(n,\geqslant)$	n 阶半正定自共轭四元数矩阵的集合
$\mathbb{H}(n,>)$	n 阶正定自共轭四元数矩阵的集合
$\boldsymbol{H}(A,B)$	正定自共轭四元数矩阵 A 与 B 的调和均值
I_n	n 阶单位矩阵
ind$A$	体上 n 阶矩阵 A 的指数

$I_s \otimes P(\lambda)$	I_s 与多项式矩阵 $P(\lambda)$ 的张量积
InA	自共轭四元数矩阵 A 的惯性
$\mathbf{K}$	体(除环)
$\mathbf{K}^*$	体 $\mathbf{K}$ 的非零元素乘法群
$\mathbf{K}_{\mathbf{R}}$	主理想整环 $\mathbf{R}$ 上的商除环
$\mathbf{K}(x)$	体 $\mathbf{K}$ 上关于未定元 x 的有理函数体
$\mathbf{K}_A$	体 $\mathbf{K}$ 中与矩阵 A 的所有元素可交换的元素所成的子体
$\mathbf{K}[x]$	体 $\mathbf{K}$ 上的关于未定元 x 的一元多项式环
$\mathbf{K}^{m\times n}$	体 $\mathbf{K}$ 上 $m\times n$ 矩阵的集合
$\mathbf{K}^n$	体 $\mathbf{K}$ 上 n 维右列空间
$L(\alpha_1,\cdots,\alpha_t)$	由向量 $\alpha_1,\cdots,\alpha_t$ 所生成的子空间
$\mathrm{M}_n(\mathbf{K})$	体 $\mathbf{K}$ 上 n 阶矩阵的集合
M/A	矩阵 M 中子矩阵 A 的 Schur 补
$\mathbf{M}_{\mathbf{K}}$	体 $\mathbf{K}$ 上的矩阵范畴
$\mathbf{M}_{\mathbb{H}}$	实四元数矩阵范畴
$\mathbb{N}$	非负整数集
$\mathbb{N}^*$	自然数集
$N(a)$	实四元数 a 的范数
$N(\alpha)$	n 维四元数列向量 α 的范数
$\mathrm{N}_r(A)$	体上矩阵 A 的右零空间
$\mathrm{N}_l(A)$	体上矩阵 A 的左零空间
P_{st}	互换矩阵
$\boldsymbol{P}(A,B)A/+/B$	n 阶四元数矩阵 A 与 B 的平行和
$\mathbb{Q}$	有理数域
$Q_{\mathbf{F}}$	形式实域 $\mathbf{F}$ 上的四元数体
$\mathbb{R}$	实数域
$\mathbb{R}^+$	正实数的集合
$\mathbf{R}$	非交换主理想整环
$\mathbf{R}\times\mathbf{R}^*$	$\mathbf{R}$ 与 $\mathbf{R}^*$ 的 Descartes 积
Rank$A$	主理想整环 $\mathbf{R}$ 上矩阵 A 的秩
rank$A$	体 $\mathbf{K}$ 上矩阵 A 的秩
$\mathrm{R}_r(A)$	体上矩阵 A 的右列空间
$\mathrm{R}_l(A)$	体上矩阵 A 的左行空间
$\mathbf{R}_+^{m\times n}$	$\mathbf{R}$ 上的有 Moore-Penrose 逆的 $m\times n$ 矩阵的集合
$\mathbf{R}^{m\times n}\{1,3\}$	$\mathbf{R}$ 上的有(1,3)逆的$m\times n$矩阵的集合

$\mathbf{R}^{m\times n}\{1,4\}$	$\mathbf{R}$ 上的有(1,4)逆的$m\times n$矩阵的集合
$\mathrm{SL}_n(\mathbf{K})$	体 $\mathbf{K}$ 上的 n 阶特殊线性群
$T(a)$	实四元数 a 的迹
$T_{st}(a)$	消法矩阵
$\mathrm{tr}A$	n 阶四元数矩阵 A 的迹
$U_{\perp}$	列酉四元数矩阵 U 的酉正交补
$W_1\cap\cdots\cap W_t$	子空间 $W_1,\cdots,W_t$ 的交
$W_1+\cdots+W_t$	子空间 $W_1,\cdots,W_t$ 的和
$W_1\oplus\cdots\oplus W_t$	子空间 $W_1,\cdots,W_t$ 的直和
$\mathbb{Z}_n$	整数环
$\mathbf{Z}(\mathbf{K})$	体 $\mathbf{K}$ 的中心
1_v	向量空间 V 的恒等变换
$[\mathbf{K}:\ \mathbf{L}]$	体 $\mathbf{K}$ 在其子体$\mathbf{L}$ 上的次数
$(M/A)_{A^{(1)}}$	矩阵 M 中子矩阵 A 关于 $A^{(1)}$ 的广义 Schur 补
$\sigma_r(A)$	体 $\mathbf{K}$ 上矩阵 A 的右谱
$\sigma_l(A)$	体 $\mathbf{K}$ 上矩阵 A 的左谱
$[A,B]AB-BA$,其中 $A,B\in\mathrm{M}_n(\mathbf{R})$	
$\varphi_A(\alpha)$	n 阶四元数矩阵 A 的 Rayleigh 商
$\lvert A\rvert$	实四元数矩阵 AA^* 的半正定平方根
$\lVert A\rVert_n\max\left\{\sum_{i=1}^{n}\lvert a_{ij}\rvert,j=1,\cdots,n\right\}$,其中 $A=(a_{ij})_{nn}\in\mathrm{M}_n(\mathbb{H})$	
$\lVert A\rVert$	$\mathbf{K}$ 上 n 阶可中心化矩阵 A 的谢邦杰行列式
$\lvert A\rvert^{\text{行}}$	n 阶四元数矩阵 A 的谢邦杰行展开式
$\lvert A\rvert_{\text{列}}$	n 阶四元数矩阵 A 的谢邦杰列展开式
$\lvert A\rvert_{\text{列}}^{\text{行}}\frac{1}{2}(\lvert A\rvert^{\text{行}}+\lvert A\rvert_{\text{列}})$	n 阶四元数矩阵 A 的谢邦杰行列展开式
$\lVert A\rVert_c$	$n\times m$ 四元数矩阵 A 的陈龙玄重行列式
$\overset{s}{\prec}$	$\mathbf{K}(\mathbf{R})$上矩阵的空间拟序符号
$\overset{-}{\preccurlyeq}$	$\mathbf{R}$ 上矩阵的减序符号
$\overset{*}{\preccurlyeq}$	$\mathbf{R}$ 上矩阵的星序符号
$*\preccurlyeq$	$\mathbf{R}$ 上矩阵的左星序符号
$\preccurlyeq *$	$\mathbf{R}$ 上矩阵的右星序符号
$\preceq$	四元数矩阵的 Banksalary-Hauke 偏序符号
$\overset{L}{\preccurlyeq}$	自共轭四元数矩阵的 Löwner 偏序符号
$\overset{\mathrm{GL}}{\preccurlyeq}$	四元数矩形阵的 GL 偏序符号

目　录

第一章　体的若干准备

本章先概述体(除环)的例子,体上多项式、体上右(左)向量空间的基本事实;同时,随之也介绍非交换主理想整环的基本概念,为以后各章作些准备.

1.1　四元数体

在历史上,第一个非交换的体是 W. R. Hamilton 在 1843 年给出的,叫做**实四元数体**,在同构意义下其矩阵形式可表述为

$$\mathbb{H} = \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \middle| \alpha, \beta \in \mathbb{C} \right\}, \tag{1}$$

这里$\mathbb{C}$是复数域,$\bar{\alpha}$是α的共轭复数. 因此,实四元数体$\mathbb{H}$是$\mathbb{C}$上的二阶全矩阵环的子体. 当然,这里需要验证集合$\mathbb{H}$关于矩阵加、乘运算是一个体. 例如,若

$$A = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \neq 0, \quad \text{即} |\alpha| + |\beta| \neq 0,$$

则容易证明A非奇异,且

$$A^{-1} = (|\alpha|^2 + |\beta|^2)^{-1} \begin{pmatrix} \bar{\alpha} & -\beta \\ \bar{\beta} & \alpha \end{pmatrix} \in \mathbb{H}.$$

设$\mathbb{R}$是实数域,记 $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \boldsymbol{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \boldsymbol{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \boldsymbol{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$,这里$i$是虚数单位,则

$$\mathbb{H} = \{a1 + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k} \mid a, b, c, d \in \mathbb{R}\}, \tag{1'}$$

且$1, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}$的乘法表如右下表所示. 因此,易见$\mathbb{H}$是实数域$\mathbb{R}$上的可除代数. 由同构嵌入定理知道,每个数域都是体$\mathbb{H}$的子域,因而$\mathbb{H}$的元素可表为$\alpha = a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}$,其中$a, b, c, d \in \mathbb{R}$.

	1	$\boldsymbol{i}$	$\boldsymbol{j}$	$\boldsymbol{k}$
1	1	$\boldsymbol{i}$	$\boldsymbol{j}$	$\boldsymbol{k}$
$\boldsymbol{i}$	$\boldsymbol{i}$	-1	$\boldsymbol{k}$	$-\boldsymbol{j}$
$\boldsymbol{j}$	$\boldsymbol{j}$	$-\boldsymbol{k}$	-1	$\boldsymbol{i}$
$\boldsymbol{k}$	$\boldsymbol{k}$	$\boldsymbol{j}$	$-\boldsymbol{i}$	-1

注　$\mathbb{H}$上多项式根的存在性问题,已有肯定解答[169],但个数问题却较为复杂. 例如,二次多项式$x^2 + 1$,在$\mathbb{H}$上有无穷多个根,因为$x = b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}$(其中$b^2 + c^2 + d^2 = 1$)都是它的根.

定义 1.1.1　设 **K** 是一个体,命

$$\mathbf{Z}(\mathbf{K}) = \{a \in \mathbf{K} \mid ax = xa, \forall x \in \mathbf{K}\},$$

叫做体 **K** 的**中心**.

容易证明

命题 1.1.1　体 $\mathbf{K}$ 的中心 $\mathbf{Z}(\mathbf{K})$ 是它的一个子域；特别地，$\mathbf{Z}(\mathbb{H}) = \mathbb{R}$.

仿上，设 $\mathbf{F}$ 是一个域，命

$$Q_{\mathbf{F}} = \{a1 + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k} \mid a,b,c,d \in \mathbf{F}\}, \tag{2}$$

其中 $1,\boldsymbol{i},\boldsymbol{j},\boldsymbol{k}$ 的乘法表如上所述. $Q_{\mathbf{F}}$ 中元素的加、乘运算也同$\mathbb{H}$情形. 如乘法，设 $\alpha = a_1 1 + a_2\boldsymbol{i} + a_3\boldsymbol{j} + a_4\boldsymbol{k}, \beta = b_1 1 + b_2\boldsymbol{i} + b_3\boldsymbol{j} + b_4\boldsymbol{k}$，规定

$$\begin{aligned}\alpha\beta = {} & (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4)1 \\ & + (a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3)\boldsymbol{i} \\ & + (a_1b_3 + a_3b_1 - a_2b_4 + a_4b_2)\boldsymbol{j} \\ & + (a_1b_4 + a_4b_1 + a_2b_3 - a_3b_2)\boldsymbol{k},\end{aligned} \tag{3}$$

那么不难验证 $Q_{\mathbf{F}}$ 是一个具有单位元 1 的非交换环. $Q_{\mathbf{F}}$ 可以是一个非交换体吗？

定义 1.1.2　一个域 $\mathbf{F}$ 叫做**形式实域**，如果在 $\mathbf{F}$ 中关系式 $\sum_{t=1}^{n} a_t^2 = 0$ 仅当 $a_t = 0 (t = 1,2,\cdots,n)$ 时成立.

命题 1.1.2　设 $\mathbf{F}$ 是一个形式实域，则如(2)所示的 $Q_{\mathbf{F}}$ 关于上述加、乘运算是一个非交换体.

证　设 $\alpha = a_1 1 + a_2\boldsymbol{i} + a_3\boldsymbol{j} + a_4\boldsymbol{k}$ 是 $Q_{\mathbf{F}}$ 中的任一非零元，则 $N(\alpha) = a_1^2 + a_2^2 + a_3^2 + a_4^2 \neq 0$. 于是 $\beta = N(\alpha)^{-1}a_1 1 - N(\alpha)^{-1}a_2\boldsymbol{i} - N(\alpha)^{-1}a_3\boldsymbol{j} - N(\alpha)^{-1}a_4\boldsymbol{k} \in Q_{\mathbf{F}}$. 直接计算知道 $\alpha\beta = \beta\alpha = 1$. 因此，$Q_{\mathbf{F}}$ 是一个非交换体. □

令

$$\begin{aligned}\sigma : \mathbf{F} &\to Q_{\mathbf{F}} \\ a &\mapsto a1 + 0\boldsymbol{i} + 0\boldsymbol{j} + 0\boldsymbol{k}, \quad \forall a \in \mathbf{F},\end{aligned}$$

则 σ 是一个单射. 因此，称 $Q_{\mathbf{F}}$ 是**由 $\mathbf{F}$ 所嵌入的四元数体**，简称为 **$\mathbf{F}$ 上的四元数体**. 于是，由同构嵌入定理，$Q_{\mathbf{F}}$ 的元素也可表示为 $a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}$，其中 $a,b,c,d \in \mathbf{F}$.

考虑命题 1.1.2 的逆命题，注意到 $\forall \alpha = a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k} (\neq 0) \in Q_{\mathbf{F}}$，则

$$\alpha\bar{\alpha} = a^2 + b^2 + c^2 + d^2 \neq 0.$$

因而易见 $\mathbf{F}$ 是一个形式实域. 于是，再注意到命题 1.1.2，则有

定理 1.1.1　设 $\mathbf{F}$ 是一个域，则如(2)所示的 $Q_{\mathbf{F}}$ 关于相应的加、乘运算是 $\mathbf{F}$ 上的一个四元数体的充分且必要条件为 $\mathbf{F}$ 是一个形式实域.

命题 1.1.3　设 $\mathbf{F}$ 是一个形式实域，则 $\mathbf{Z}(Q_{\mathbf{F}}) = \mathbf{F}$.

证　在同构意义下，由(3)显然有 $\mathbf{F} \subseteq \mathbf{Z}(Q_{\mathbf{F}})$. 设 $\alpha = a_1 + a_2\boldsymbol{i} + a_3\boldsymbol{j} + a_4\boldsymbol{k} \in \mathbf{Z}(Q_{\mathbf{F}})$，则 $\alpha\boldsymbol{i} = \boldsymbol{i}\alpha$，于是

$$a_2 + a_1\boldsymbol{i} + a_4\boldsymbol{j} - a_3\boldsymbol{k} = a_2 + a_1\boldsymbol{i} - a_4\boldsymbol{j} + a_3\boldsymbol{k}.$$

注意到 $Q_{\mathbf{F}}$ 的特征 $\mathrm{ch}Q_{\mathbf{F}} = 0$，则有 $a_3 = a_4 = 0$. 再由 $\alpha\boldsymbol{j} = \boldsymbol{j}\alpha$ 得 $a_2 = 0$. 因此 $\alpha = a_1 \in \mathbf{F}$，故 $\mathbf{Z}(Q_{\mathbf{F}}) = \mathbf{F}$. □

定理 1.1.2　设 $\mathbf{F}_1,\mathbf{F}_2$ 都是形式实域，则 $Q_{\mathbf{F}_1} \cong Q_{\mathbf{F}_2}$ 的充分且必要条件是 $\mathbf{F}_1 \cong \mathbf{F}_2$.

证 充分性. 设 $\mathbf{F}_1 \overset{\sigma}{\cong} \mathbf{F}_2$, 命

$$\tau: a_1 + a_2\boldsymbol{i} + a_3\boldsymbol{j} + a_4\boldsymbol{k} \mapsto \sigma(a_1) + \sigma(a_2)\boldsymbol{i} + \sigma(a_3)\boldsymbol{j} + \sigma(a_4)\boldsymbol{k},$$

显然有 $Q_{\mathbf{F}_1} \overset{\tau}{\cong} Q_{\mathbf{F}_2}$.

必要性. 设 $Q_{\mathbf{F}_1} \overset{\varphi}{\cong} Q_{\mathbf{F}_2}$, $a \in \mathbf{F}_1$, $\alpha_2 \in Q_{\mathbf{F}_2}$, 记 $a_2 = \varphi(a)$, α 满足 $\varphi(\alpha) = \alpha_2$, 那么由 $a\alpha = \alpha a$ 得

$$a_2\alpha_2 = \varphi(a)\varphi(\alpha) = \varphi(a\alpha) = \varphi(\alpha a) = \varphi(\alpha)\varphi(a) = \alpha_2 a_2.$$

于是 $a_2 \in \mathbf{F}_2$, 从而有 $\varphi(\mathbf{F}_1) \subseteq \mathbf{F}_2$. 由于 φ^{-1} 存在, 因而有 $\mathbf{F}_1 \subseteq \varphi^{-1}(\mathbf{F}_2)$. 但类似地有 $\varphi^{-1}(\mathbf{F}_2) \subseteq \mathbf{F}_1$. 因此 $\mathbf{F}_1 = \varphi^{-1}(\mathbf{F}_2)$, 故 $\mathbf{F}_1 \cong \mathbf{F}_2$. □

显然, 实数域 $\mathbb{R}$ 及其子域都能嵌入四元数体, 因而 $Q_{\mathbf{F}}$ 是一类非交换体. 由此, 人们自然会问及: 在同构意义下的最小四元数体为何?

定义 1.1.3 由有理数域所嵌入的四元数体叫做**有理四元数体**.

定理 1.1.3 有理四元数体是最小的四元数体.

证 设 $Q_{\mathbf{F}}$ 是任意的一个四元数体, 因 $\mathrm{ch}Q_{\mathbf{F}} = 0$, 则 $Q_{\mathbf{F}}$ 包含一个与有理数域同构的子域 $\mathbf{F}_0$. 显然 $\mathbf{F}_0 \subseteq Q_{\mathbf{F}}$, 从而 $Q_{\mathbf{F}_0} \subseteq Q_{\mathbf{F}}$. 但有理四元数体与 $Q_{\mathbf{F}_0}$ 同构, 因而存在有理四元数体到 $Q_{\mathbf{F}}$ 的单射, 故知它是最小的四元数体. □

1.2 体上多项式环

设 $\mathbf{K}$ 是一个体, x 是一个未定元, 如域上情形, 形式表达式

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n, \tag{1}$$

其中 $a_0, a_1, \cdots, a_n \in \mathbf{K}$, 叫做 $\mathbf{K}$ 上的一个一元多项式, 简记作 $f(x) = \sum_{t=0}^{n} a_t x^t$. 若 $a_n \neq 0$, 则称 n 为 $f(x)$ 的**次数**, 记作 $\deg f$. $\mathbf{K}$ 上所有一元多项式的集合记作 $\mathbf{K}[x]$.

设 $f(x) = \sum_{s=0}^{m} a_s x^s$, $g(x) = \sum_{t=0}^{n} b_t x^t$, 则多项式的加法、乘法依次定义为

$$f(x) + g(x) = \sum_{s} (a_s + b_s)x^s,$$

$$f(x)g(x) = \sum_{r=0}^{m+n} c_r x^r, \quad \text{其中 } c_r = \sum_{s+t=r} a_s b_t.$$

不难证明, $\mathbf{K}[x]$ 是一个环, 叫做**体 $\mathbf{K}$ 上的一元多项式环**.

容易证明

命题 1.2.1 设 $\mathbf{Z}$ 是 $\mathbf{K}$ 的中心, 则 $\mathbf{Z}[x]$ 是 $\mathbf{K}[x]$ 的中心.

命题 1.2.2 设 $f(x), g(x) \in \mathbf{K}[x] - \{0\}$, 则

1) $f(x)g(x) \neq 0$, 且 $\deg fg = \deg f + \deg g$;

2) 若 $f(x) + g(x) \neq 0$, 则 $\deg(f+g) \leqslant \max\{\deg f, \deg g\}$.

由 1) 知道 $\mathbf{K}[x]$ 是一个无零因子环. 再注意到 $\mathbf{K}$ 中元素乘积未必可交换, 类

似域上的证明可得如下的左、右带余除法定理：

命题 1.2.3　设 $f(x),g(x)\in\mathbf{K}[x],g(x)\neq 0$，则存在 $q_s(x),r_s(x)\in\mathbf{K}[x]$，$s=1,2$，使得

$$f(x)=g(x)q_1(x)+r_1(x)=q_2(x)g(x)+r_2(x),$$

这里 $r_1(x)=0$ 或 $\deg r_1<\deg g$；$r_2(x)=0$ 或 $\deg r_2<\deg g$.

定义 1.2.1　设 $\mathbf{R}$ 是一个无零因子环，$\mathbb{N}$ 是非负整数集. 如果存在

$$\sigma:\mathbf{R}\to\mathbb{N}$$
$$r\mapsto\sigma(r),\quad\forall r\in\mathbf{R}$$

满足以下条件：

1) $\sigma(ab)\geqslant\max\{\sigma(a),\sigma(b)\}$，$\forall a,b\in\mathbf{R}^*=\mathbf{R}-\{0\}$，

2) 若 $a,b\in\mathbf{R},b\neq 0$，则存在 $q_s,r_s\in\mathbf{R},s=1,2$，使得

$$a=bq_1+r_1,r_1=0\text{ 或 }\sigma(r_1)<\sigma(b)$$
$$=q_2b+r_2,r_2=0\text{ 或 }\sigma(r_2)<\sigma(b),$$

那么称 $\mathbf{R}$ 是一个(非交换)Euclid **环**.

这里说的 Euclid 环未必可交换，如体 $\mathbf{K}$ 上的一元多项式环 $\mathbf{K}[x]$ 就是 Euclid 环.

定义 1.2.2　设 $f(x),g(x)\in\mathbf{K}[x]$.

1) 若存在 $f_1(x)(f_2(x))$ 使 $f(x)=g(x)f_1(x)(=f_2(x)g(x))$，则称 $g(x)$ 是 $f(x)$ 的一个**左(右)因式**，或 $g(x)$ **左(右)整除** $f(x)$.

2) 若 $g(x)$ 既左整除 $f(x)$，又右整除 $f(x)$，则称 $g(x)$ **整除** $f(x)$，记作 $g(x)\mid f(x)$. 否则，记 $g(x)\nmid f(x)$.

定义 1.2.3　设 $f(x),g(x),d(x)\in\mathbf{K}[x]$. 若 $d(x)$ 分别是 $f(x)$、$g(x)$ 的左因式，即 $f(x)$ 与 $g(x)$ 的**左公因式**；并且对于 $f(x)$ 与 $g(x)$ 的任意一个左公因式 $d_1(x)$，都有 $d_1(x)$ 是 $d(x)$ 的一个左因式，那么称 $d(x)$ 是 $f(x)$ 与 $g(x)$ 的一个**最大左公因式**.

类似地可定义两个多项式的最大右公因式的概念.

定义 1.2.4　设 $f(x),g(x)\in\mathbf{K}[x]$. 若 $f(x)$ 与 $g(x)$ 的左、右最大公因式皆是零次的，则称 $f(x)$ 与 $g(x)$ **互素**.

下面，证明体 $\mathbf{K}$ 上多项式的一些性质，并总假设 $\mathbf{F}=\mathbf{Z}(\mathbf{K})$，即为 $\mathbf{K}$ 的中心.

命题 1.2.4　设 $f(x)\in\mathbf{K}[x],x-a_i\in\mathbf{F}[x],i=1,2,\cdots,m$，且诸 a_i 互异，$n_1,\cdots,n_m\in\mathbb{N}^*$，这里 $\mathbb{N}^*$ 是自然数集. 如果 $(x-a_i)^{n_i}\mid f(x),i=1,2,\cdots,m$，则

$$(x-a_1)^{n_1}(x-a_2)^{n_2}\cdots(x-a_m)^{n_m}\mid f(x).$$

证　由 $(x-a_i)^{n_i}\mid f(x)$ 知道有

$$f(x)=(x-a_1)^{n_1}f_1(x)=(x-a_2)^{n_2}f_2(x)=\cdots=(x-a_m)^{n_m}f_m(x).\tag{2}$$

显然 $f(a_i)=0$，特别地 $f(a_2)=(a_2-a_1)^{n_1}f_1(a_2)=0$. 因 $a_1-a_2\neq 0$，故 $f_1(a_2)=0$，从而有 $(x-a_2)\mid f_1(x)$. 设

$$f_1(x)=(x-a_2)^n\varphi(x),(x-a_2)\nmid\varphi(x),$$

代入(2)，得

$$f(x) = (x-a_1)^{n_1}(x-a_2)^{n}\varphi(x) = (x-a_2)^{n_2}f_2(x). \tag{3}$$

假如 $n < n_2$，则因 $\mathbf{K}[x]$ 满足消去律，且 $(x-a_1)^{n_1}(x-a_2)^{n} = (x-a_2)^{n}(x-a_1)^{n_1}$，于是从(3)的两边消去 $(x-a_2)^{n}$，得

$$(x-a_1)^{n_1}\varphi(x) = (x-a_2)^{n_2-n}f_2(x), n_2 - n \geqslant 1.$$

由此得 $(a_2-a_1)^{n_1}\varphi(a_2) = 0, \varphi(a_2) = 0$，与 $(x-a_2) \nmid \varphi(x)$ 矛盾. 故必有 $n \geqslant n_2$，即由(3)得

$$f(x) = (x-a_1)^{n_1}(x-a_2)^{n_2}\varphi_1(x), \varphi_1(x) = (x-a_2)^{n-n_2}\varphi(x).$$

再代入 $x = a_3$ 得 $\varphi(a_3) = 0$. 仿上可证必有

$$f(x) = (x-a_1)^{n_1}(x-a_2)^{n_2}(x-a_3)^{n_3}\varphi_2(x).$$

如此继续下去，即可得

$$f(x) = (x-a_1)^{n_1}(x-a_2)^{n_2}\cdots(x-a_m)^{n_m}\varphi_{m-1}(x). \qquad \square$$

在命题 1.2.4 中，若 $a_i \notin \mathbf{F}$，则结论不真. 如在实四元数体中，有

$$x^2+1 = (x-\boldsymbol{i})(x+\boldsymbol{i}) = (x-\boldsymbol{j})(x+\boldsymbol{j}) = (x-\boldsymbol{k})(x-\boldsymbol{k}),$$

从而有

$$(x-\boldsymbol{i})^2 \mid (x^2+1)^2, (x+\boldsymbol{i})^2 \mid (x^2+1)^2, (x-\boldsymbol{j})^2 \mid (x^2+1)^2,$$

但从次数看显然有

$$(x-\boldsymbol{i})^2(x+\boldsymbol{i})^2(x-\boldsymbol{j})^2 \nmid (x^2+1)^2.$$

这也说明命题 1.2.4 并非显而易见的. 若用 $g_i(x) \in \mathbf{F}[x]$ 代换 $(x-a_i)$，且 $g_1(x), \cdots, g_m(x)$ 两两互素，则命题 1.2.4 的结论真确.

命题 1.2.5 设 $f(x), g(x) \in \mathbf{K}[x]$，$(x-a) \in \mathbf{F}[x]$. 如果 $(x-a)^n \mid f(x)g(x)$，$(x-a)^n \nmid f(x)$，其中 $n \geqslant 1$，则 $(x-a) \mid g(x)$.

证 由假设知 $f(x)g(x) = (x-a)^n\varphi(x)$，且可设

$$f(x) = (x-a)^r f_1(x), 0 \leqslant r < n, (x-a) \nmid f_1(x).$$

于是

$$(x-a)^r f_1(x)g(x) = (x-a)^n\varphi(x),$$

两边消去 $(x-a)^r$ 得 $f_1(x)g(x) = (x-a)^{n-r}\varphi(x)$，$n-r \geqslant 1$，从而 $f_1(a)g(a) = 0$. 但是 $(x-a) \nmid f_1(x)$，有 $f_1(a) \neq 0$，故 $g(a) = 0$，从而 $(x-a) \mid g(x)$. $\square$

命题 1.2.6 设 $p(x) \in \mathbf{F}[x]$. 如果在 $\mathbf{K}[x]$ 中有 $p(x) = p_1(x)p_2(x)$，则 $p_1(x)p_2(x) = p_2(x)p_1(x)$.

证 因为 $p_2(x)p_1(x)p_2(x) = p_2(x)p(x) = p(x)p_2(x) = p_1(x)p_2(x)p_2(x)$，所以由消去律知本命题成立. $\square$

命题 1.2.7 设 $p(x) \in \mathbf{F}[x]$，$q(x), \varphi(x) \in \mathbf{K}[x]$；$p(x) \mid q(x)\varphi(x)$. 如果 $p_1(x) \in \mathbf{K}[x]$ 是 $p(x)$ 与 $\varphi(x)$ 的最大左公因式，且 $p(x) = p_1(x)p_2(x)$，则 $q(x) = q_2(x)p_2(x)$.

证 由 $p(x) \mid q(x)\varphi(x)$ 得 $q(x)\varphi(x) = p(x)h(x)$. 由 $p_1(x)$ 是 $p(x)$ 与

$\varphi(x)$的最大左公因式知道有 $f(x),g(x)\in \mathbf{K}[x]$，使

$$p_1(x)=p(x)f(x)+\varphi(x)g(x),$$

两边左乘以 $q(x)$，并注意到命题 1.2.6，则有

$$\begin{aligned}q(x)p_1(x)&=q(x)p(x)f(x)+q(x)\varphi(x)g(x)\\&=q(x)f(x)p(x)+h(x)g(x)p(x)\\&=(q(x)f(x)+h(x)g(x))p_2(x)p_1(x).\end{aligned}$$

记 $q_2(x)=q(x)f(x)+h(x)g(x)$，则由消去律得 $q(x)=q_2(x)p_2(x)$. □

命题 1.2.8　设在 $\mathbf{K}[\lambda]$ 中有 $\varphi_1(x)\mid\varphi_2(x)\mid\cdots\mid\varphi_t(x)$，$p(x)\in\mathbf{F}[x]$；且有 $q_1(x),\cdots,q_t(x)\in\mathbf{K}[x]$，使 $p(x)\mid q_i(x)\varphi_i(x)(i=1,\cdots,t)$；$p_1(x)$ 是 $p(x)$ 与 $\varphi_1(x)$ 的最大左公因式，则有

$$p(x)=p_1(x)p_2(x)\cdots p_t(x)p_0(x),\tag{4}$$

使 $p_1(x)\cdots p_i(x)$ 恰为 $p(x)$ 与 $\varphi_i(x)$ 的最大左公因式，$i=1,2,\cdots,t$；$q_i(x)=h_i(x)p_{i+1}(x)\cdots p_t(x)p_0(x),i=1,\cdots,t-1$；$q_t(x)=h_t(x)p_0(x)$.

证　对 t 用数学归纳法证明命题的前半部分.

当 $t=1$ 时，此即命题 1.2.7，结论成立. 假设结论对 $t-1$ 成立，那么对于 t 的情形，先设 $d(x)$ 是 $p(x)$ 与 $\varphi_2(x)$ 的一个最大左公因式，则有 $f(x),g(x)\in\mathbf{K}[x]$，使

$$d(x)=p(x)f(x)+\varphi_2(x)g(x).$$

因为 $\varphi_1(x)\mid\varphi_2(x)$，所以可设 $\varphi_2(x)=\varphi_1(x)l(x)$. 因为 $p_1(x)$ 是 $p(x)$ 与 $\varphi_1(x)$ 的一个最大左公因式，所以可设 $p(x)=p_1(x)m(x),\varphi_1(x)=p_1(x)s(x)$. 因此

$$d(x)=p_1(x)(m(x)f(x)+s(x)l(x)g(x))=p_1(x)p_2(x),$$

其中 $p_2(x)=m(x)f(x)+s(x)l(x)g(x)$. 令 $\mu_2(x)=d(x)=p_1(x)p_2(x),\mu_i(x)=\varphi_i(x),i=3,\cdots,t$. 由已知，则有 $q_i(x)\in\mathbf{K}[x]$，使 $p(x)\mid q_i(x)\mu_i(x),i=3,\cdots,t$；且注意到命题 1.2.7，有

$$p(x)=d(x)r(x)=\mu_2(x)r(x)=r(x)\mu_2(x).$$

因 $\mu_2(x)$ 是 $p(x)$ 与 $\varphi_2(x)$ 的最大左公因式，所以由归纳假设有

$$p(x)=g_2(x)g_3(x)\cdots g_t(x)g_0(x),g_2(x)=p_1(x)p_2(x),$$

使 $g_2(x)\cdots g_i(x)$ 为 $p(x)$ 与 $\mu_i(x)$ 的最大左公因式. 设 $g_i(x)=p_i(x),i\neq 1,2$，则有(4)式成立，且使 $p_1(x)\cdots p_i(x)$ 是 $p(x)$ 与 $\varphi_i(x)$ 的最大左公因式，$i=1,\cdots,t$，归纳法完成.

又 $p(x)\mid q_i(x)\varphi_i(x)$，利用(4)与命题 1.2.7 知本命题的后半部分成立. □

命题 1.2.9　设 $g_1(x),\cdots,g_m(x)\in\mathbf{F}[x]$，且两两互素，$\varphi(x)\in\mathbf{K}[\lambda]$. 如果

$$(g_i(x))^{n_i}\mid\varphi(x),n_i\geqslant 1,\qquad i=1,\cdots,m,$$

则 $\prod_{i=1}^{m}(g_i(x))^{n_i}\mid\varphi(x)$.

证　由已知有