自动控制中的矩阵理论

〔日〕须田信英 等 著

科学出版社

自动控制中的矩阵理论

〔日〕须田信英 児玉慎三 池田雅夫 著

曹长修 译

科学出版社

1979

内 容 简 介

本书是为自动控制工作者编写的关于矩阵理论的长篇讲座．书中除了对矩阵理论的基本内容作了详尽论述外，还以大量篇幅和实例，结合现代控制理论中的基本问题（系统的状态变量表示方法、系统的结构分析、系统反馈、观测器和系统的稳定性等）进行了深入讨论．书后附有大量最新的参考文献．

本书可供自动控制领域内的科技人员及高等院校有关自动化专业的教师、研究生及学生参考．

须田信英　児玉慎三　池田雅夫 著

制御工学者のためのマトリクス理论

日本自动制御协会，1973

自动控制中的矩阵理论

〔日〕须田信英　児玉慎三　池田雅夫　著

曹长修 译

*

科学出版社出版

北京朝阳门内大街137号

湘潭地区印刷厂印刷

新华书店北京发行所发行　各地新华书店经售

*

1979年9月第一版　开本：787×1092 1/16

1979年9月第一次印刷　印张：28 1/2

印数：0001—37,580　字数：657,000

统一书号：15031·237

本社书号：1435·15—8

定 价：2.90 元

译 者 的 话

从1950到1960年，控制系统的分析和设计方法发生了飞跃性变化，在大量生产实践特别是空间技术的基础上，逐渐从经典控制理论发展成为现代控制理论.

在自动调节原理中主要使用的是频率法，即用传递函数及频率特性来分析和设计调节系统，其数学基础是拉普拉斯变换，这种方法只能适应简单的单输入单输出线性调节系统. 但是在现代控制理论中，所研究的对象是多输入多输出系统，系统的表示采用状态变量法，所处理的方程式是矩阵方程式. 采用矩阵写出多输入多输出系统的方程式不但运算时符号简单，可以利用矩阵的各种性质进行深入研究，而且具有适合于在电子数字计算机中处理的特点. 因此，矩阵理论是现代控制理论最重要的数学基础之一.

《自动控制中的矩阵理论》原是一篇在日文《系统与控制》期刊上连续刊载的讲座. 作者们原计划编写I、II、III、IV四个部分，仅其中第I部分就连载四年之久（在1974年才将第I部分刊载完），由于时间拖得太长，后面三个部分没有系统地发表，仅扼要地发表了《多项式矩阵及其应用（基础部分）》和《多项式矩阵及其应用（应用部分）》（1975年第4～5期）. 本书是将已发表的第I部分和上述两部分整理译成.

书中章节编号与一般书籍有所不同，共用了一位英文字母和两位数字. 在编号中P表示预备知识，B表示基础理论，A表示在自动控制中的应用. 第一位数字，0表示绪论部分，1表示第I部分；第二位数字表示章数. 例如，P-0-1表示绪论中预备知识的第1章，B-I-2，表示第I部分中基础理论的第2章，A-I-4表示第I部分中在自动控制中的应用的第4章，等等. 书中没有正式划分节，黑体字的小标题基本上相当于节（书中已整理列于目录）.

本书是为自动控制领域内工作的科学技术人员编写的，为了使广大读者均能阅读此书，内容尽量做到深入浅出. 书中除了对矩阵理论的基本内容作了详尽论述外，还以大量篇幅密切结合现代控制理论中的基本问题：系统的状态变量表示方法、系统的结构分析（可控性、可观测性、典范分解和实现问题）、系统反馈、观测器、系统的稳定性等等，通过读者所熟悉的大量实例进行了深入讨论.

在本书翻译过程中，译者对原文错印和不当之处做了一些修改和注解，但由于水平有限，不当之处在所难免，切望广大读者批评指正.

目　　录

P-0-1 矩阵、矩阵的和及积

有限个标以顺序的元素[1]排列成的矩形称为矩阵 (matrix). 元素的横排称为行 (row), 纵排称为列(column). 行从上数分别称为第1行、第2行……, 第 m 行; 列从左数分别称为第1列、第2列,……, 第 n 列. 位于第 i 行第 j 列的元素称为 (i, j) 元素, 把 i, j 写为下角可表示为 a_{ij}. 因此,典型的矩阵可以表示为

$$\boldsymbol{A}=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \tag{1}$$

为了简便起见,矩阵常用 (i, j) 元素代表,有时也写成

$$\boldsymbol{A}=[a_{ij}] \tag{2}$$

具有 m 行 n 列的矩阵, 称为 m 行 n 列矩阵,或简称为 $m\times n$ 矩阵, 有时写成 $\boldsymbol{A}=m\times n$, 等等. 特别是,把 $\boldsymbol{A}=n\times n$, 即行数和列数相等的矩阵称作方阵 (Square matrix).

在方阵中, (i, i) 元素如 $(i=1, 2, \cdots, n)$ 称为主对角线元素.

元素全为0的 $m\times n$ 矩阵称作 $m\times n$ 零阵,写成 $\boldsymbol{0}_{m\times n}$, 或简写成 $\boldsymbol{0}$.

仅主对角线元素为1, 而其余元素全为0的 $n\times n$ 方阵, 称为 n 阶单位阵,写成 $\boldsymbol{I}_n$, 或简写成 $\boldsymbol{I}$.

矩阵的和及积

以 $\boldsymbol{A}=[a_{ij}]=m\times n$, $\boldsymbol{B}=[b_{ij}]=m\times n$ 两个矩阵对应元素的和为元素而构成的矩阵, 定义为 $\boldsymbol{A}$、$\boldsymbol{B}$ 的和, 即[2]

$$\boldsymbol{A}+\boldsymbol{B}\triangleq[a_{ij}+b_{ij}]=m\times n \tag{3}$$

设 $\boldsymbol{A}=[a_{ij}]=m\times n$ 和 $\boldsymbol{B}=[b_{ij}]=p\times q$, 当 $\boldsymbol{A}$ 的列数等于 $\boldsymbol{B}$ 的行数(即 $n=p$)时,其积 $\boldsymbol{AB}$ 可定义如下

$$\boldsymbol{AB}\triangleq\left[\sum_{k=1}^{n} a_{ik}b_{kj}\right]=m\times q \tag{4}$$

对于矩阵的积必须注意: (i)在 $n=p$, $m=q$ 均成立的情况下, 可以同时定义乘积 $\boldsymbol{AB}$ 及与其顺序相反的乘积 $\boldsymbol{BA}$, $\boldsymbol{AB}=m\times m$, $\boldsymbol{BA}=n\times n$. 一般, $\boldsymbol{AB}$ 与 $\boldsymbol{BA}$ 是大小不同的矩阵. (ii)仅当 $m=n=p=q$, 即 $\boldsymbol{A}$, $\boldsymbol{B}$ 是大小相同的方阵时, $\boldsymbol{AB}$ 和 $\boldsymbol{BA}$ 才是大小相同的矩阵. (iii)即便在这种情况下,一般 $\boldsymbol{AB}=\boldsymbol{BA}$ 也不成立. (iv)尽管 $\boldsymbol{A}$ 和 $\boldsymbol{B}$ 都不是零阵,但是乘积 $\boldsymbol{AB}$ 有时变成零阵,等等.

数 α 和矩阵 $\boldsymbol{A}=[a_{ij}]=m\times n$ 之积可定义为

$$\alpha\boldsymbol{A}\triangleq[\alpha a_{ij}]=m\times n \tag{5}$$

1) 这里可以将元素理解成实数或复数.

2) $\triangleq$ 意味着根据定义相等.

A-0-1 自动控制和矩阵

大家知道，从1950年下半年到1960年初，自动控制这门科学(自动控制系统中问题的提出、系统的表示、分析和设计等等)得到很大发展，形成所谓的现代控制理论．从它的产生到现在，经历了十年以上的各种考验，显然今后它已是一种肯定的科学，而且和所谓的经典控制理论的关系也逐渐清楚了．

因此可以说，若将现代控制理论和经典控制理论作为两门控制科学，从自动控制的课程设置来说，不掌握经典控制理论就无法学习现代控制理论．根据这个观点，有人把两者结合起来构成一门控制科学的体系．现在已经有一些按照这种观点写成的教科书[1~5]，它们反映了这样一种倾向．

那末，为了掌握按照这种新的体系写成的控制理论，从数学基础来看，除了必须掌握经典控制理论的基础拉普拉斯变换以外，还要求具备线性代数、特别是矩阵理论的知识，这个道理越来越明显．在现代控制理论中，一般都是考虑多变量控制，而不像经典控制理论那样主要是讨论单变量控制．因此，利用矩阵写出多变量系统的方程式，不但运算时符号简便，而且可以利用矩阵的各种性质进行理论上的进一步研究(不利用矩阵是非常困难的)．用矩阵写成的方程式，除了极简单的情况而外，一般不便于手算，而具有适合于在计算机中处理的特点．

现代控制理论以所谓的动力学系统的理论为基础，它由线性多变量系统的系统设计、最优控制、状态估计、系统识别及稳定性分析等部分组成．全面地介绍这些内容所涉及到的矩阵理论，作者无论如何也办不到，而且也不是写作本书的目的．因此，这里我们仅选取表1中所列出的一些项目，暂且称其为自动控制中的基本理论，介绍作为其基础的矩阵理论[1)]．

表 1

线性多变量系统	结构理论(可控性、可观测性、实现问题等等)
	控制问题(二次型性能指标的最优控制、模态控制、解耦控制、极点配置、状态反馈的稳定化等等)
	灵敏度分析
	状态估计(观测器、卡尔曼滤波)
	稳定性分析(李亚普诺夫稳定性理论、有界输入-有界输出稳定性)
	响应的数值分析(e^{At}的计算等等)
非线性系统的稳定性分析(李亚普诺夫稳定性理论、频域的稳定性判据、卢里叶问题等)	
线性顺序系统的分析(响应的表示、可控性、可观测性等等)	

1) 除了本书所介绍的内容以外，自动控制中所涉及到的非常重要的矩阵理论，还有数学规划(线性规划、平方规划、共轭梯度法、梯度投影法等等)，读者可以参考文献[11~18]．

虽然表中大部分内容在上述教科书中都有介绍，但是目前还没有一本合适的线性代数参考书，能系统地介绍作为其基础的矩阵理论，而且在自动控制教科书的附录中所能看到的关于矩阵的介绍，大多只限于最基本的内容．从这个角度来说，本书对读者若能有一些帮助，作者也感到安慰．

因为本书的写作对象是从事自动控制工作的工程技术人员，所以在讲述某些数学内容的同时，尽可能结合表1所列出的课题，介绍矩阵理论在自动控制中的应用．

B-0-1 排列和矩阵

我们所运用的数的范围，从自然数开始逐渐扩大成整数、有理数、实数、复数．其中，复数由实部和虚部两个元素组成．将其推广，把更多个(不限于两个)数(整数、有理数、实数、复数)在一定条件下的排列看成更广义的数．矩阵就是这种把有限个数按一定顺序排成m行n列的数，按着这种考虑可以将"数"推广．像这样，可以看成"数的排列 (array)"是矩阵的第一个特点．

但是，这里要注意两点．第一，一谈到数，人们就自然地会认为可以对它进行四则运算(加，减，乘，除)．把这种观点原封不动地拿到作为广义的"数"矩阵，并不完全合适．本书开始部分谈到矩阵的运算，例如在矩阵的乘积$\boldsymbol{AB}$中可以看到，其顺序不一定可以交换，因此就有必要注意与运算有关的性质．因此还有一点，将矩阵$\boldsymbol{A}=[a_{ij}]$看成数的排列，其元素a_{ij}不只限于实数及复数，而可以更自由地考虑，它可以是由实数、复数按照四则运算得到的，例如a_{ij}可以是$(b_nx^n+b_{n-1}x^{n-1}+\cdots+b_0)/(a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0)$这样一个有理数．象这样，可以将矩阵作更广泛的考虑，对于在自动控制中的应用也是很方便的．

为了对上述各点作稍为深入一步的讨论和加以整理，利用代数学中群、环、体的概念是很方便的[1)]．

[定义 1]　当集合G满足下列公理时，称G为群(group)．

a) 对于G的任意两个元α, β, 可以定义某一个运算"$\circ$", $\alpha\circ\beta$作为G中的元唯一确定．(自闭性，唯一性)

b) 对于G的任意三个元α, β, γ, $(\alpha\circ\beta)\circ\gamma=\alpha\circ(\beta\circ\gamma)$成立．(结合律)

c) G中存在元e, 对于G的任意元α, $e\circ\alpha=\alpha\circ e=\alpha$成立．(单位元)

d) 对于G的任意元α, 存在满足$\alpha^{-1}\circ\alpha=\alpha\circ\alpha^{-1}=e$的元$\alpha^{-1}$, 而且$\alpha^{-1}$唯一确定．(逆元)

在上面定义中对于运算"$\circ$"没有假定交换律成立，当下列交换律

e) 对于G的任意两个元α, β, $\alpha\circ\beta=\beta\circ\alpha$成立．

成立时，该群称为可换群[2)](阿贝尔群)．

当运算"$\circ$"是加法时，满足上面 a)～e)的群称为加群(即关于加法的可换群)．在加群中，单位元e写成0，叫做零元，而且将α^{-1}写成$-\alpha$．当运算"$\circ$"是乘法时，满足 a)～e)的群称作关于乘法的可换群，这时单位元e可以写成1．此外，通常将$\alpha\circ\beta$写成$\alpha\beta$．

---

1) 关于代数学，除了传统性的[6,7]以外，K. L. 加多纳著的《近代代数学的发现》(ダイヤモント社出版)也是一本很好的入门参考书．

2) 使用逻辑符号$\forall$(对于所有的…)和表示所属关系的符号$\in$(属于…)，上述定义可以写成

$$\forall\alpha,\ \beta\in G,\ \text{可以定义}\ \alpha\circ\beta$$

a) $\alpha\circ\beta\in G$

b) $(\alpha\circ\beta)\circ\gamma=\alpha\circ(\beta\circ\gamma)$, $\forall\alpha,\ \beta,\ \gamma\in G$

c) G中存在元e, $e\circ\alpha=\alpha\circ e=\alpha$, $\forall\alpha\in G$

d) 对于$\forall\alpha\in G$, 有满足$\alpha^{-1}\circ\alpha=\alpha\circ\alpha^{-1}=e$的元$\alpha^{-1}\in G$存在

e) $\alpha\circ\beta=\beta\circ\alpha$, $\forall\alpha,\ \beta\in G$

[例 1] 实数的集合 R 是加群，R 中除掉 0 后的集合，变成关于乘法的可换群.

[定义 2] 当集合 $\tilde{R}$ 满足下列公理时，称 $\tilde{R}$ 为环(ring).

a) 对于 $\tilde{R}$ 的任意两个元 α, β，可以定义加法＋和乘法·，而且 $\alpha+\beta$、$\alpha\beta$ 皆唯一确定，

$$\alpha+\beta\in\tilde{R},\quad \alpha\beta\in\tilde{R},\quad {}^{\forall}\alpha,\ \beta\in\tilde{R}$$

b) $\tilde{R}$ 是加群.

c) 对于乘法·，结合律成立.

$$(\alpha\beta)\gamma=\alpha(\beta\gamma),\quad {}^{\forall}\alpha、\beta,\ \gamma\in\tilde{R}$$

d) 对于加法和乘法都满足分配律

$$\alpha(\beta+\gamma)=\alpha\beta+\alpha\gamma\quad {}^{\forall}\alpha,\ \beta,\ \gamma\in\tilde{R}$$

$$(\alpha+\beta)\gamma=\alpha\gamma+\beta\gamma\quad {}^{\forall}\alpha,\ \beta,\ \gamma\in\tilde{R}$$

在上述环的定义中，根据条件 b)，$\alpha+\beta=\beta+\alpha$. 但不要求关于乘法的可换性. 作为附加条件，把满足乘法交换律的环叫做可换环.

[例 2] 全体整数的集合 $Z\{0, \pm1, \pm2, \cdots\}$，是关于普通加法、乘法的可换环. 偶数的集合 $Z_e\{0, \pm2, \pm4, \cdots\}$ 也是同样.

[例 3] 设 $\tilde{R}$ 为任意环，将 $\tilde{R}$ 中的元排列成 n 行 n 列方阵

$$\boldsymbol{A}=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

等，$\boldsymbol{A}$ 称为环 $\tilde{R}$ 上的矩阵. 当 n 固定时，这样的矩阵全体的集合，我们用 $\tilde{R}^{n\times n}$ 表示. 在 $\tilde{R}^{n\times n}$ 中应用 P-0-1 中(3)，(4)式定义的加法、乘法，可以证明 $\tilde{R}^{n\times n}$ 也是环(试证明)，也叫做矩阵环. 当然，既使 $\tilde{R}$ 是可换环，一般 $\tilde{R}^{n\times n}$ 也不一定是可换环.

[定义 3] 当集合 F 满足下列公理时，称 F 为体(field).

a) F 是可换环.

b) F 中除 0 以外的元，对乘法构成可换群.

虽然体和环、群有关，可如上定义，但因体是今后经常用到的重要的概念，现再将其条件反复列举如下.

[定义 3′] 以 $\alpha, \beta, \gamma\cdots$ 为元的集合 F，当满足下列公理时，称 F 为体.

加法：

a) 对于 F 的任意两个元 α, β，α 和 β 的和可以唯一定义，$\alpha+\beta\in F$

b) $\alpha+\beta=\beta+\alpha,\ {}^{\forall}\alpha,\ \beta\in F$(加法的交换律)

c) $\alpha+(\beta+\gamma)=(\alpha+\beta)+\gamma,\ {}^{\forall}\alpha,\ \beta,\ \gamma\in F$(加法的结合律)

d) F中存在 0 元，$\alpha+0=\alpha,\ {}^{\forall}\alpha\in F$ 成立.

e) 对于任意的 $\alpha\in F$，在 F 中存在 $-\alpha$ 元，$\alpha+(-\alpha)=0$成立.

乘法：

f) 对于 F 中的任意两个元 α, β，α 和 β 的积 $\alpha\beta$ 可唯一定义，$\alpha\beta\in F$

g) $\alpha\beta=\beta\alpha,\ {}^{\forall}\alpha,\ \beta\in F$(乘法的交换律)

h) $\alpha(\beta\gamma)=(\alpha\beta)\gamma,\ {}^{\forall}\alpha,\ \beta,\ \gamma\in F$(乘法的结合律)

i) F 中存在单位元 1，$\alpha 1=\alpha,\ {}^{\forall}\alpha\in F$ 成立.

j) 对于 F 中的任意 $\alpha\neq0$ 的元，在 F 中有用 α^{-1} 表示的逆元存在，$\alpha\alpha^{-1}=\alpha^{-1}\alpha=1$ 成立.

对于加法和乘法还满足下列分配律

k) $\alpha(\beta+\gamma)=\alpha\beta+\alpha\gamma$, $^{\forall}\alpha, \beta, \gamma\in F$(分配律)

[例 4] 全体有理数的集合,对于普通加法、乘法构成体.

[例 5] 全体实数的集合 R, 复数的集合 C 均构成体.

(问题 1) 试证明体 F 中加法的单位元 0 及乘法的单位元 1 均唯一确定.

由定义 3′ 可见, 体就是可以任意地对其元做有限次加减乘除的集合. 只知道自然数的儿童不会做由 2 减去 5, 用 3 除尽 2 而感到不自由, 这是因为自然数或整数不能构成体. 另方面,在有理数、实数、复数等体上, 我们随心所欲地用惯了四则运算, 而对于矩阵的运算也感到不自由(不满足乘法的交换律,逆矩阵不一定存在,等等),如例 3 所示,这是因为矩阵最多只能构成环.

(问题 2) 试证明例 3 中的方阵改成 m 行 n 列的长方矩阵($m\neq n$)时又如何?

(问题 3) 在例 3 中将环 $\tilde{R}$ 换成体 F, 将 F 的元排列成 n 行 n 列的方阵, 这些矩阵的全体用 $F^{n\times n}$ 表示,试证明 $F^{n\times n}$ 关于矩阵的加法、乘法能否构成体.

群、环、体的概念不仅与上述的数有关, 而且有更为广泛的应用. 下面结合经常用到的重要的部分举几个例子.

[例 6] 设 F 为任意体,由该体的元 a_k 和变量 s 组成的多项式

$$a_0+a_1s+\cdots+a_ns^n=\sum_{i=0}^{n}a_is^i \tag{1}$$

的全体,用 $P(s, F)$ 表示.

对于两个多项式

$$f(s)=\sum_{i=0}^{n}a_is^i,\quad g(s)=\sum_{i=0}^{n}b_is^i,$$

在定义其和

$$f(s)+g(s)\triangleq\sum_{i=0}^{n}(a_i+b_i)s^i \tag{2}$$

及积

$$f(s)g(s)\triangleq\sum_{i=0}^{2n}c_is^i,\quad c_i\triangleq\sum_{\substack{j+k=i\\ j,k\leq n}}a_ib_i \tag{3}$$

时, $P(s, F)$ 便构成环.

[例 7] 设 F 为任意体,由 F 的元 a_k, b_k 和变量 s 构成有理式.

$$\frac{b_0+b_1s+\cdots+b_ns^m}{a_0+a_1s+\cdots+a_ns^n}=\frac{n(s)}{d(s)} \tag{4}$$

的全体,用 $Q(s, F)$ 表示,当定义两个有理函数的和及积

$$\frac{n_1(s)}{d_1(s)}+\frac{n_2(s)}{d_2(s)}\triangleq\frac{n_1(s)d_2(s)+n_2(s)d_1(s)}{d_1(s)d_2(s)} \tag{5}$$

$$\frac{n_1(s)}{d_1(s)}\cdot\frac{n_2(s)}{d_2(s)}\triangleq\frac{n_1(s)n_2(s)}{d_1(s)d_2(s)} \tag{6}$$

时, $Q(s, F)$ 构成体.

[例 8] 设 S 为任意集合, $\tilde{R}$ 为任意环, 并设定义在 S 上而在 $\tilde{R}$ 上取值的函数的全体为 Φ. 对于 $\varphi_1(t)$, $\varphi_2(t)\in\Phi$, 当定义其和及积

$$(\varphi_1+\varphi_2)(t)\triangleq\varphi_1(t)+\varphi_2(t) \tag{7}$$

$$(\varphi_1\varphi_2)(t)\triangleq\varphi_1(t)\varphi_2(t) \tag{8}$$

时，Φ 构成环.

在实轴上定义的连续(分段连续)实函数的全体，对于上述运算也构成环.

到此为止，以上所讨论的集合均具有无限个元. 具有无限个元的体叫做无限体(infinite field). 与此相应，仅由有限个元构成的体叫做有限体 (finite field). 下面举一些大家最熟悉的例子.

[例 9] 在集合 $\{0, 1\}$ 上，将加法和乘法定义为：$0+0=0$, $0+1=1+0=1$, $1+1=0$, $0\cdot0=0\cdot1=1\cdot0=0$, $1\cdot1=1$, 则 $\{0, 1\}$ 构成体.

设 p 为质数，有限集合 $\{0, 1, \cdots, p-1\}$ 一般用 $GF(p)$ 表示. 在 $GF(p)$ 上定义 mod p 运算(即当 $\alpha-\beta$ 是 p 的倍数时，认为 $\alpha=\beta$)时，$GF(p)$ 构成体，该体称为伽罗瓦体(Galois field).

[例 10] 在 $GF(3)$ 上的 mod 3 加法和乘法如下

加 法

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

乘 法

	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

由此可见，$GF(3)$ 构成体.

(问题 4) 在 $GF(p)$ 上定义 mod p 运算，当 p 不是质数时，试以 $p=4$ 验证 $GF(p)$ 不是体.

容易看到，环和体的重要区别是在乘法运算方面. 一般来说，环除了不满足乘法的交换律以外，乘法的单位元也不一定存在[1](例如例 2 中的 Z_e). 既使假定单位元存在，对于任意 $\alpha\neq0$ 的元，使 $\alpha^{-1}\alpha=\alpha\alpha^{-1}=1$ 成立的 α^{-1} 也不一定定义在该环上[2]. 在例 2 的 Z 上，若 $\alpha=+1$, -1, 则 α^{-1} 分别为 $+1$, -1, 是环 Z 上的元，但是对于 Z 上的其它元，例如 $\alpha=2$ 时，α^{-1} 为 $1/2$, 它不是 Z 上的元. 环 Z 上的 $+1$, -1, 其 α^{-1} 是 Z 上的元，这种元叫做可逆元. 在环 $P(s, F)$ 上(例 6)，除了零次多项式(即体 F 的 0)以外，其余的元均为可逆元.

根据例 3，将环 $\tilde{R}$ 中的元排列成 n 行 n 列方阵，该方阵的全体 $\tilde{R}^{n\times n}$ 也构成环，下面简单讲一下该环的性质. 如果 $\tilde{R}$ 中存在单位元 1，则 $\tilde{R}^{n\times n}$ 中也存在类似的单位元，即存在主对角线元素均为 1，而其它元素均为 0 的 n 阶方阵. 环 $\tilde{R}^{n\times n}$ 中*一定存在乘法的单位元. 在这里考虑 $\tilde{R}$ 为可换环，而且为了简单起见，令 $n=2$，我们来讨论一下 $\tilde{R}^{2\times2}$. 对于 $\boldsymbol{A}\triangleq[a_{ij}]\in\tilde{R}^{2\times2}$，若定义

$$\tilde{A}\triangleq\begin{bmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{bmatrix}\in\tilde{R}^{2\times2}$$

$$\Delta\triangleq a_{11}a_{22}-a_{21}a_{12}\in\tilde{R},$$

1) 有理数、实数、复数构成体是显然的，关于有理函数的集合 $Q(s, F)$ 及有限集合 $GF(p)$ 构成体的证明，在文献[10]中讲得很详细.

2) 若存在则唯一确定.

* 原文误为环 $F^{n\times n}$ 中. ——译者注