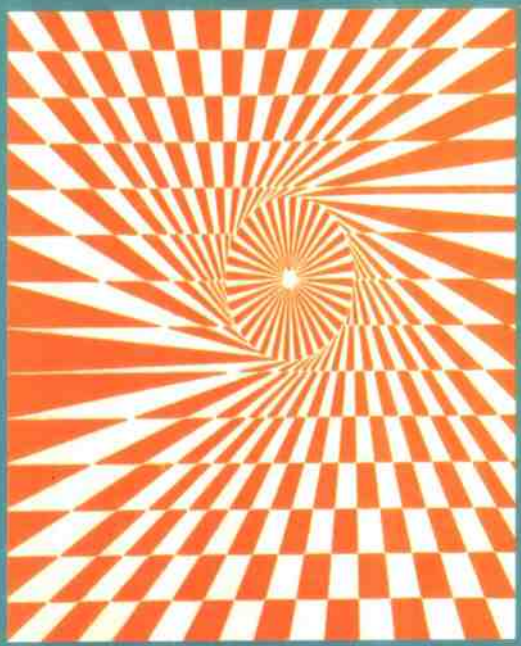
北京大学数学丛书

代数学

上　册

莫宗坚　蓝以中　赵春来 著



北京大学出版社

北京大学教学丛书

代　数　学

上　册

莫宗坚　蓝以中　赵春来　著

北京大学出版社

内 容 提 要

本书分上、下两册出版。

上册主要讲述近代代数的初步知识，内容包括集合论与数论、群论、多项式论、线性代数以及域论。

本书内容丰富，直观性强，推理自然，解释详尽。此书的独到之处是特别注重对于代数学的背景、基本思想以及与其他学科的联系等方面的介绍。书中精选了大量的例题和习题。本书的起点低，由浅入深。具有高等代数基础知识的读者皆可以阅读本书，进而学到现代代数学的较大部分基础知识。

本书可作为高等学校数学系高年级学生以及研究生的教材，也可供数学工作者参考。

书　　名：代数学(上册)
著作责任者：莫宗坚　等著
责 任 编 辑：邱淑清
标 准 书 号：ISBN 7-301-01371-X/O・222
出　版　者：北京大学出版社
地　　址：北京市海淀区中关村北京大学校内　100871
网　　址：http://cbs.pku.edu.cn/cbs.htm
电　　话：出版部 62752015　发行部 62754140　编辑室 62752021
电 子 信 箱：zpup@pup.pku.edu.cn
排　印　者：北京大学印刷厂
印　刷　者：北京大学印刷厂
发　行　者：北京大学出版社
经　销　者：新华书店
850 毫米×1168 毫米　32 开本　12 印张　302 千字
1986 年 10 月第一版　2001 年元月第三次印刷
定　　价：16.00 元

序——献给中国的青年人

这本书是根据我在美国的明尼苏达大学及普度大学的讲义编写而成的。当时的讲授对象是一、二年级的研究生。为了便于课堂讲授及读者自习，我在编写过程中，力求本书能够易于了解、联系各方。我的目标是：

一、抽象与具体结合，理论与应用结合。目前的代数书，常常单线地朝抽象方向发展，使读者——甚至一些数学家们——觉得代数学是抽象概念的游戏。即使代数学能联系实际、解决问题，那也如一些半真半假的电影片的片头语，“如与实际相符，也纯属偶然”。此书是要力矫此弊，希望能通过例题、解说等，阐明代数学与代数几何、代数数论、物理、密码学等等的联系。

各科数学都是人类探索知识、解决问题的钥匙。一般的钥匙只有小部分起开锁的作用，其余部分是防止它开别的锁，这是一般的钥匙的“有害部分”。如果把这些“有害部分”完全取消，就成了百灵钥匙了。我想说明，代数正是这样的百灵钥匙。

二、理论的整合与统一。各种数学理论的平行发展，到了代数学中，取得了整合与统一。例如，在第四章中，我们统一了“有限生成的交换群的基本定理”及“矩阵的若当标准式”；在第五章中，我们整合了“几何作图”及“解方程式”；在第八章中，我们用“Dedekind整环”统一了“代数数论”及“仿射曲线论”的讨论，等等。

在这些理论的整合与统一中，我们希望能体现数学的内在规律美。但愿读者们能欣赏数学的“庙堂之美、百官之富”。

对于以上的目标，我自觉作得不够。向前看中国的未来，物质的建设可以速成，精神的建设须要长期的积累，所谓“十年树

木，百年树人”。数学——人类精神活动的最高产物——将促进青年人对真与美的追求，发展对文化的内省力，因此丰裕了精神文化的生活。

本书在完成过程中，得到蓝以中及赵春来两位的协助。他们改正了原稿的许多遗落、误失，与我共同商订了一些名词，并补充了习题，以及写了本书上册的附录(蓝以中)。我们联名出书，正足以纪念我们的共同工作

莫宗坚

序于1984年8月

符号说明

$\cap$	交
$\cup$	并
$\subset$	含于
$\supset$	包含
$\subsetneq$	真含于
$\supsetneq$	真包含
$\in$	属于
$\notin$	不属于
$\varnothing$	空集合
$\sim$	等价
$\overset{\cdot}{\sim}$	相伴
$\overset{D}{\sim}$	在距离D下有共同的极限
$\approx$	同构
$\leqslant$ ($\geqslant$)	不等号或半序
$\langle\ ,\ \rangle$	内积或弱内积
$\boldsymbol{C}$	复数域
$\boldsymbol{N}$	自然数集
$\boldsymbol{Q}$	有理数域
$\boldsymbol{Q}_p$	p-adic数域
$\boldsymbol{R}$	实数域
$\boldsymbol{Z}$	有理整数环
$\boldsymbol{Z}_n$	整数模n的剩余集
$\boldsymbol{Z}_n^*$	整数模n的缩剩余集
$[a]_n$	整数a在$\boldsymbol{Z}_n$中所在的同余集

$a\equiv b(\mathrm{mod}\ m)$	a 与 b 模 m 同余
$a\mid b$	a 整除 b
$a\nmid b$	a 不整除 b
$(a,b)=1$	a 与 b 互素
$\langle a_1,a_2,\cdots\rangle$	由$\{a_1,a_2,\cdots\}$生成的子群或向量空间
$(a_1,a_2,\cdots)$	由$\{a_1,a_2,\cdots\}$生成的理想
$\mathrm{Ann}(S)$	S 的消灭子
(A)	由环的子集 A 生成的理想
A_n	n 个文字的交代群
$\mathrm{Aut}(G)$	群 G 的自同构群
$C(f(x))$	多项式$f(x)$的内涵
$D_\infty(a,b)$	复数a与b之间的距离，即$\lvert a-b\rvert$
$D_p(a,b)$	a 与 b 的 p 距离
deg	次数
$\det A$	矩阵 A 的行列式
$\dim_K V$(或$\dim V$)	K 向量空间 V 的维数
$\mathrm{dis}(f(y))$	多项式$f(y)$的判别式
$\mathrm{Dis}\{w_1,\cdots,w_n\}$	向量空间的一组基$\{w_1,\cdots,w_n\}$的判别式
$F(G)$	群 G 的不变域
$\mathrm{FL}(m,n,K)$	域K上的$m\times n$阶全线性群
$\mathrm{FL}(n,K)$	域K上的$n\times n$阶全线性群
$(G,*)$	集合 G 在运算 $*$ 下构成的群
$G>H$ （或$H<G$）	H 为 G 的子群
$G\rhd H$ （或$H\lhd G$）	H 为 G 的正规子群
$[G:H]$	子群H在群G中的指数
G/H	群 G 对正规子群 H 的商群
$G(L/K)$	域 L 在子域 K 上的伽罗瓦群
$\mathrm{GL}(n,K)$	域 K 上的 n 阶一般线性群
$\mathrm{Hom}_R(M,N)$	R 模 M 到 N 的全体模映射构成的 R 模

id	恒同映射
$\mathrm{im}(\rho)$	映射 ρ 的象
$\mathrm{Inn}(G)$	群 G 的内自同构群
$\ker(\rho)$	映射 ρ 的核
K^*	域 K 的非零元素乘法群
$K_{\mathfrak{L}}$	域 K 在扩域 L 中的代数闭包
K_L	域 K 在扩域 L 中的可离代数闭包
$K[a_1,a_2,\cdots]$	域 K 上添加 $a_1,a_2,\cdots$ 所得到的环
$K(a_1,a_2,\cdots)$	域 K 上添加 $a_1,a_2,\cdots$ 所得到的域
$l(G)$	群 G 的长度
$[L:K]$	代数扩域 L 在 K 上的扩张次数
M^T	矩阵 M 的转置
$\mathrm{N}_{L/K}$(简记 N)	由域 L 到 K 的范数
$o(G)$	群 G 的阶
$o(a)$	群的元素 a 的阶
ord	阶，阶数
$\mathrm{Orb}(s)$	集合的元素 s 在变换群作用下的轨道
p.i.d	主理想整环
$\mathrm{Res}_y(f(y),g(y))$	多项式 $f(y)$ 与 $g(y)$ 的结式
R/I	环 R 对理想 I 的商环
$R[a_1,a_2,\cdots]$	环 R 上添加 $a_1,a_2,\cdots$ 所得到的多项式环
$\mathrm{SL}(n,K)$	域 K 上的 n 阶特殊线性群
$\mathrm{SL}(n,\boldsymbol{Z})$	n 阶整数特殊线性群
S_n	n 个文字的对称群
$\mathrm{Stab}(T)$	子集 T 的稳定群
$<S>$	由集合 S 生成的群或向量空间
$S\backslash T$	集合 T 在集合 S 中的补集
$\mathrm{tr\ deg}(L/K)$	域 L 对域 K 的超越次数
$\mathrm{Tr}_{L/K}$(简记Tr)	由 L 到子域 K 的迹

$\mathscr{V}(I)$	理想 I 的代数多样体，或包含 I 的所有素理想的集合
1_S	集合 S 上的恒同映射
$\varphi(\ )$	尤拉 φ 函数
$\varphi_n(x)$	n 次割圆多项式
$\rho: S\to T$	由集合 S 到 T 的映射 ρ
$\prod_{i\in I} S_i$	S_i $(i\in I)$的直积
$\bigoplus_{i\in I} S_i$	S_i $(i\in I)$的直和
∎	定理、系、引理证明完毕，或与下文可能混淆的例及讨论的结束

上册目录

第一章　集合论与数论

§1 集　合　论

我们假定读者已熟悉集合论的基本概念，如**交集**、**并集**、**子集**、**包含**及**映射**等。请参考前面的“符号说明”。

定义1.1　设S及T为集合，$\rho: S\to T$是由S到T的映射。任取S中的二元素s_1及s_2，如果$\rho(s_1)=\rho(s_2)$时，必有$s_1=s_2$，则称ρ为**一一映射**，或**单射**。如果对于T中任意元素t，必有$s\in S$，使$\rho(s)=t$，则称ρ为S到T**上的映射**，或**满射**。如果ρ同时为单射及满射，则称ρ为**单满映射**。

集合论中最有意义的概念之一是“基数”。我们有如下的定义：

定义1.2　设S及T为集合。如有一单满映射$\rho: S\to T$，则称S与T**同基数**。

讨论　1）如集合S与整数集合$\{1,2,\cdots,n\}$同基数，则称S为**有限集**，而称其基数为n。反之则称之为**无限集**。设S及T为同基数的有限集，$\rho: S\to T$为一映射，则易证：如ρ为单射，则ρ必为满射。反之，如ρ为满射，则ρ必为单射。此一命题可谓之**鸽笼定理**，即设想S为一群鸽子，T为等数的鸽笼，则上命题即：如果每一鸽子已一一进笼，则鸽笼必无空者；反之，如鸽笼皆无空者，则必然每一笼中仅有一只鸽子。

2）如集合S与正整数集合$\{1,2,3,\cdots,n,\cdots\}$同基数，则称$S$为**可数无限集**。有限集与可数无限集统称**可数集**。除此之外，皆称为**不可数集**。

3）对所有的无限集而言，鸽笼定理皆不成立，然而证法比较

复杂，远离本书的趣旨，请读者参考集合论的专书。现在我们仅举一例以说明此种现象，即所谓的“希尔伯特的旅馆”：设一旅馆有可数无限个房间$\{1,2,\cdots,n,\cdots\}$，已住满房客。如同时又来了可数无限个新房客$\{g_1,g_2,\cdots,g_n,\cdots\}$，则一个简易的安排方法是令原住$n$号房间的老房客移入$2n$号房间，于是空出$\{1,3,5,\cdots,2n+1,\cdots\}$所有奇数号房间。令新房客依序住入即可，也即令新房客g_n住入$2n-1$号房间。从此例中，可以看出单射不一定必是满射。反之，如令头两个人挤一间房，其余的人依序住入空出的房间，则满射又不一定是单射了。

定理1.1 有理数集$\boldsymbol{Q}$是可数无限集。

证明 我们采用所谓“三角数法”。考虑正有理数的集合$\boldsymbol{Q}_+$。把$\boldsymbol{Q}_+$中的元素按分母大小排成如下的无限矩阵：

$$\boldsymbol{Q}_+=\begin{pmatrix}\frac{1}{1} & \frac{2}{1} & \frac{3}{1} & \cdots\cdots\\ \frac{1}{2} & \frac{2}{2} & \frac{3}{2} & \cdots\cdots\\ \frac{1}{3} & \frac{2}{3} & \frac{3}{3} & \cdots\cdots\\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots\\ \frac{1}{n} & \frac{2}{n} & \frac{3}{n} & \cdots\cdots\\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots\end{pmatrix},$$

然后我们把整个矩阵的元素，按箭头所指的顺序，依次对应到所有正的偶数，自然，已经出现过的有理数则略去。例如，

$$\frac{1}{1}\to 2,\ \frac{1}{2}\to 4,\ \frac{2}{1}\to 6,\ \frac{1}{3}\to 8,\ \frac{3}{1}\to 10,$$

等等。这样就把$\boldsymbol{Q}_+$对应到了正偶数集。同法，我们可以把负有理数集$\boldsymbol{Q}_-$对应到大于1的正奇数集。再把0对应到1。不难看出，这个对应是由$\boldsymbol{Q}$到正整数集$\boldsymbol{N}=\{1,2,\cdots,n,\cdots\}$的单满映射。

于是Q是可数无限集。∎

系 设有可数集$S_i=\{s_{i1},s_{i2},\cdots,s_{in},\cdots\}$，$i\in$可数集$I$。则这些可数个$S_i$的并集$\bigcup_{i\in I}S_i$也是可数集。

证明 利用三角数法。∎

定理1.2 实数集R为不可数集。

证明 假设R为可数集，则所有实数可以排成一行：$\{r_1,r_2,\cdots,r_n,\cdots\}$。我们用“对角线法”来证明这是不可能的。

把$r_1,r_2,\cdots,r_n,\cdots$用十进小数写出如下：

$$r_1=a_1.b_{11}b_{12}\cdots b_{1n}\cdots,$$
$$r_2=a_2.b_{21}b_{22}\cdots b_{2n}\cdots,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$r_n=a_n.b_{n1}b_{n2}\cdots b_{nn}\cdots,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

其中诸a_i为整数，b_{ij}为0,1,2,…,9之一。现取一实数

$$r=0.c_1c_2\cdots c_n\cdots$$

如下：如果$b_{nn}\neq 5$，则取$c_n=5$，否则取$c_n=4$ $(n=1,2,\cdots)$。显然$r\neq r_n$ $(\forall n=1,2,\cdots)$。故r不在集合$\{r_1,r_2,\cdots,r_n,\cdots\}$之中。由此知$R$为不可数集。∎

在代数学中，经常应用构造“直积”、“商集”的方法。我们有如下定义。

定义1.3 设I为一个集合。如果对每一个$i\in I$，都有一个集合S_i，则S_i的**直积**$\prod_{i\in I}S_i$定义为

$$\{(s_i)_{i\in I}:\ s_i\in S_i\},$$

即I到$\bigcup_{i\in I}S_i$的所有映射s，而且能适合$s(i)=s_i\in S_i$者。如I为可数集时，$\prod_{i\in I}S_i$中的元素常写成一行$(s_1,s_2,\cdots,s_n,\cdots)$。

定义1.4 设T为一集合。如果T为一些分离的子集的并集，

即$T=\bigcup_{j\in J}T_j$，并且不同的子集T_j的交集为空集，则这些子集T_j的集合$\{T_j: j\in J\}$称为T的一个**商集**。

讨论 1) 设T为所有中国人民的集合，按照某种法定年龄的标准，T可以划分为T_1=未成年人的集合和T_2=成年人的集合。则$\{T_1,T_2\}$构成T的一个商集。此商集中仅有两个元素。

2) 设$\{T_j: j\in J\}$为T的一个商集，则可在T中定义一个相应的“等价关系”～如下：

$$a\sim b \iff a,b\text{属于同一个}T_j。$$

一般言之，任意关系“～”如具有下列三条性质，则称为一个**等价关系**：

(a) 反身性：$a\sim a$；

(b) 对称性：如果$a\sim b$，则$b\sim a$；

(c) 传递性：如果$a\sim b$，$b\sim c$，则$a\sim c$。 ∎

我们也可以用等价关系来定义商集如下。

定义1.4* 设～为集合T上的等价关系。令

$$T_a=\{b: b\in T,\ b\sim a\},$$

则$\{T_a: a\in T\}$是T的一个商集，称之为**关于等价关系～的商集**，T_a称为一个**等价子集**。

讨论 为说明定义1.4*中的$\{T_a\}$确实是商集，我们仅须验证两点：1) $T=\bigcup_{a\in T}T_a$；2) 如果$T_a\cap T_c\neq\varnothing$，则$T_a=T_c$。1)是显然的，这因为$a\sim a$，所以$a\in T_a$；关于2)，设$b\in T_a\cap T_c$，令$d$为$T_c$中任意元素，则有

$$a\sim b\sim c\sim d,\quad a\sim c\sim d,\quad a\sim d。$$

即$d\in T_a$。所以$T_c\subset T_a$。同法可得出$T_a\subset T_c$，于是$T_a=T_c$。 ∎

下面的“数学归纳法”是正整数集N的公理之一，其详情请见附录中正整数的“皮诺公理”。

数学归纳法 设对每个正整数m，有命题$P(m)$。如能证明：

1) $P(1)$是正确的；

2) 设n是任意大于1的正整数。如对所有小于n的正整数l，$P(l)$都是正确的，则$P(n)$是正确的，

那么所有的命题$P(m)$皆是正确的。

讨论 这个数学归纳法不能从更简明的公理系统导出，然而可以从下面的讨论中理解其合理性：根据1)，已知$P(1)$是正确的。运用2)，令$n=2$，则知$P(2)$是正确的。再运用2)，令$n=3$，则知$P(3)$是正确的。如此反复运用2)，则知所有的命题$P(m)$皆是正确的。|

在代数学里，经常应用“Zorn引理”。此引理等同于“选择公理”及“良序原理”，是集合论的公理之一。为了讨论Zorn引理，我们先引入“序”与“半序”的概念。

定义1.5 设S为一集合。S的一个关系“$\geqslant$”如适合下列条件，则称之为一个**半序**：

1) $s_1 \geqslant s_1$，$\forall s_1 \in S$；

2) $s_1 \geqslant s_2$，$s_2 \geqslant s_3 \Longrightarrow s_1 \geqslant s_3$，$\forall s_1, s_2, s_3 \in S$；

3) $s_1 \geqslant s_2$，$s_2 \geqslant s_1 \Longrightarrow s_1 = s_2$，$\forall s_1, s_2 \in S$。

定义1.6 设S为一集合，$\geqslant$为S的半序。如果适合下列条件，则称$\geqslant$为S的**序**：

4) 对任意的$s_1, s_2 \in S$，总有$s_1 \geqslant s_2$或$s_2 \geqslant s_1$。

定义1.7 设$\geqslant$为S的半序，T为S的子集。如果S的一个元素s，适合$s \geqslant t$ ($\forall t \in T$)，则称s为T的一个**上限**。如果s具有如下性质：$\forall s_1 \in S$，只要$s_1 \geqslant s$，必有$s_1 = s$，则称s为S的**一个极大元素**。

定义1.8 设S为一集合，$\geqslant$为S的半序，T为S的子集。如果局限于T中$\geqslant$是一个序，则称T为一**链**。

Zorn引理 设S为一非空集合，$\geqslant$为S的半序。如果任意链皆有上限，则S有一极大元素。

讨论 1) 在集合论中，已经证明了Zorn引理实际上是一个

公理，所以不可能从其它较简单的公理系统中导出。

2）利用Zorn引理可以简化许多证明，也可以证明一些除此之外的其它方法不能证明的结果。例如，我们可以证明平面上的任何有界区域D内皆有极大的开圆盘，证法如下：（a）令S为D内所有开圆盘构成的集合，用包含$\subset$定义半序$\leqslant$；（b）由于D内至少有一个开圆盘，所以S是非空的；（c）如果一些开圆盘构成的集合$\{D_i: i\in I\}$成为一链，则$\bigcup_{i\in I} D_i$也显然是D的一个开圆盘，它是此链的上限；（d）于是根据Zorn引理，有界区域D内必有极大的开圆盘。

习　题

1. 设ρ为集合S到集合T的映射。证明ρ是一个单射的充要条件是下列两条件中任一条成立：

（1）存在T到S的映射τ，使$\tau\rho = 1_S$；

（2）不存在某集合U到S的两个不同映射τ_1, τ_2，使

$$\rho\tau_1 = \rho\tau_2.$$

2. 设ρ为集合S到集合T的映射。证明ρ是一个满射的充要条件是下列两条件中任一条成立：

（1）存在T到S的映射τ，使$\rho\tau = 1_T$；

（2）不存在T到某集合U的两个不同映射τ_1, τ_2，使

$$\tau_1\rho = \tau_2\rho.$$

3. 设S是一基数为$n(n\geqslant 1)$的有序集。证明在S中存在一个元素a，使$\forall b\in S$，有$a\leqslant b$。举例说明无限的有序集不一定具有此性质。

4. 设ρ是集合S到集合T的映射，A, B是S的子集。证明

$$\rho(A\cup B) = \rho(A)\cup\rho(B), \quad \rho(A\cap B)\subset\rho(A)\cap\rho(B).$$

举例说明$\rho(A\cap B)$不一定等于$\rho(A)\cap\rho(B)$。

5. 设ρ是集合S到集合T的映射，A是S的子集。证明在