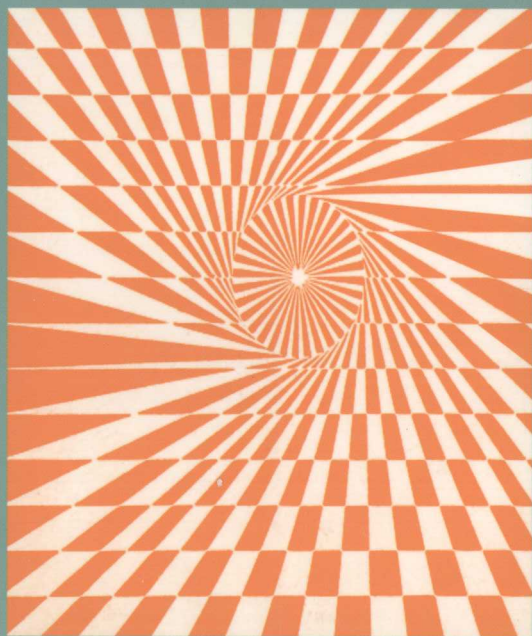


北京大学数学丛书

代 数 学

上 册

莫宗坚 蓝以中 赵春来 著



北京大学出版社

015
18
21

北京大學教學叢書

代 数 学

上 册

莫宗堅 藍以中 趙春來 著

150325021

150325021

電子信箱: zsqp@pub.pku.edu.cn

北京大學印刷廠 印

北京大學印刷廠 印

北京大學出版社 行

北京大學出版社 經

850 毫米×1168 毫米 32 開本 12 印張 302 字

1986 年 10 月第一版 1986 年 7 月第二次印刷

北京大學出版社

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 1999年7月第二次印刷

定 价: 16.00元

《北京大学数学丛书》编委会

主 编：程民德

副主编：江泽培 丁石孙

编 委：钱 敏 丁同仁 姜伯驹 张恭庆 应隆安

责任编辑：邱淑清

说 明

此丛书是以数学、计算数学、概率统计及有关专业的高年级学生、研究生、青年教师及数学研究工作者为读者对象的出版物。丛书特点是内容新颖，力图反映现代数学的新成就；叙述精练，约相当于一学期周学时为3.0的研究生课程的取材。我们编辑出版此丛书的主要目的是为了适应我们国家培养研究生的需要，同时，又可作为数学及有关系科高年级选修课程的参考书，为提高本科生的教学质量贡献一份力量。

我们诚恳地希望：广大读者对于书目的选择，内容的取材提出宝贵意见，作为我们今后出版或再版时的参考。

《北京大学数学丛书》编委会

一九八一年元月

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
\Subset	真含于
\supseteq	真包含
\in	属于
\notin	不属于
\emptyset	空集合
\sim	等价
\sim	相伴
$\underset{D}{\sim}$	在距离 D 下有共同的极限
\cong	同构
$\leq (\geq)$	不等号或半序
\langle, \rangle	内积或弱内积
\mathbb{C}	复数域
\mathbb{N}	自然数集
\mathbb{Q}	有理数域
\mathbb{Q}_p	p -adic 数域
\mathbb{R}	实数域
\mathbb{Z}	有理整数环
\mathbb{Z}_n	整数模 n 的剩余集
\mathbb{Z}_n^*	整数模 n 的缩剩余集
$[a]_n$	整数 a 在 \mathbb{Z}_n 中所在的同余集

$a \equiv b \pmod{m}$	a 与 b 模 m 同余
$a b$	a 整除 b
$a \nmid b$	a 不整除 b
$(a, b) = 1$	a 与 b 互素
$\langle a_1, a_2, \dots \rangle$	由 $\{a_1, a_2, \dots\}$ 生成的子群或向量空间
(a_1, a_2, \dots)	由 $\{a_1, a_2, \dots\}$ 生成的理想
$\text{Ann}(S)$	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
$\text{Aut}(G)$	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 $ a - b $
$D_p(a, b)$	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
$\text{dis}(f(y))$	多项式 $f(y)$ 的判别式
$\text{Dis}\{w_1, \dots, w_n\}$	向量空间的一组基 $\{w_1, \dots, w_n\}$ 的判别式
$F(G)$	群 G 的不变域
$\text{FL}(m, n, K)$	域 K 上的 $m \times n$ 阶全线性群
$\text{FL}(n, K)$	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
$G \triangleright H$ (或 $H \triangleleft G$)	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
$\text{GL}(n, K)$	域 K 上的 n 阶一般线性群
$\text{Hom}_R(M, N)$	R 模 M 到 N 的全体模映射构成的 R 模

id	恒同映射
$\text{im}(\rho)$	映射 ρ 的象
$\text{Inn}(G)$	群 G 的内自同构群
$\text{ker}(\rho)$	映射 ρ 的核
K^*	域 K 的非零元素乘法群
K_L	域 K 在扩域 L 中的代数闭包
K_L^s	域 K 在扩域 L 中的可离代数闭包
$K[a_1, a_2, \dots]$	域 K 上添加 a_1, a_2, \dots 所得到的环
$K(a_1, a_2, \dots)$	域 K 上添加 a_1, a_2, \dots 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
$N_{L/K}$ (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
$\text{Orb}(s)$	集合的元素 s 在变换群作用下的轨道
p.i.d	主理想整环
$\text{Res}_y(f(y), g(y))$	多项式 $f(y)$ 与 $g(y)$ 的结式
R/I	环 R 对理想 I 的商环
$R[a_1, a_2, \dots]$	环 R 上添加 a_1, a_2, \dots 所得到的多项式环
$\text{SL}(n, K)$	域 K 上的 n 阶特殊线性群
$\text{SL}(n, \mathbf{Z})$	n 阶整数特殊线性群
S_n	n 个文字的对称群
$\text{Stab}(T)$	子集 T 的稳定群
$\langle S \rangle$	由集合 S 生成的群或向量空间
$S \setminus T$	集合 T 在集合 S 中的补集
$\text{tr deg}(L/K)$	域 L 对域 K 的超越次数
$\text{Tr}_{L/K}$ (简记 Tr)	由 L 到子域 K 的迹

$\mathcal{Z}(I)$	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
$\rho: S \rightarrow T$	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

符号说明	(i)
第一章 集合论与数论	(1)
§ 1 集合论	(1)
§ 2 唯一分解定理	(7)
§ 3 同余式	(15)
§ 4 中国剩余定理	(22)
§ 5 复整数集	(26)
§ 6 p -adic 数与赋值	(37)
第二章 群论	(50)
§ 1 群的定义	(50)
§ 2 集合上的变换群	(57)
§ 3 子群	(63)
§ 4 内自同构及正规子群	(72)
§ 5 自同构群	(82)
§ 6 p 群及西洛定理	(87)
§ 7 若当-荷德定理	(93)
§ 8 对称群 S_n	(102)
第三章 多项式	(110)
§ 1 域与环	(110)
§ 2 多项式环及比域	(117)
§ 3 多项式环的唯一分解定理	(126)
§ 4 对称式, 结式及判别式	(141)
§ 5 理想	(157)

第四章 线性代数.....(175)

§ 1 向量空间.....(175)

§ 2 基及维数.....(180)

§ 3 线性变换及矩阵.....(191)

§ 4 模及主理想环上的模.....(206)

§ 5 若当标准式.....(226)

§ 6 内积及正交坐标.....(246)

§ 7 谱论.....(260)

第五章 一元多项式的解及域论.....(269)

§ 1 C 的代数封闭性.....(269)

§ 2 代数扩域.....(275)

§ 3 代数闭包.....(291)

§ 4 特征数及有限域.....(296)

§ 5 可离代数扩域.....(304)

§ 6 伽罗瓦理论.....(314)

§ 7 用根式解方程式.....(330)

§ 8 域多项式及判别式.....(343)

§ 9 超越扩张.....(349)

附 录 自然数的皮诺公理系.....(357)

汉英名词索引.....(362)

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， $\rho: S \rightarrow T$ 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 $\rho: S \rightarrow T$ ，则称 S 与 T 同基数。

讨论 1) 如集合 S 与整数集合 $\{1, 2, \dots, n\}$ 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， $\rho: S \rightarrow T$ 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 $\{1, 2, 3, \dots, n, \dots\}$ 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 $\{1, 2, \dots, n, \dots\}$ ，已住满房客。如同时又来了可数无限个新房客 $\{g_1, g_2, \dots, g_n, \dots\}$ ，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 $\{1, 3, 5, \dots, 2n+1, \dots\}$ 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 \mathbf{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 \mathbf{Q}_+ 。把 \mathbf{Q}_+ 中的元素按分母大小排成如下的无限矩阵：

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

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，

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

等等。这样就把 \mathbf{Q}_+ 对应到了正偶数集。同法，我们可以把负有理数集 \mathbf{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 \mathbf{Q} 到正整数集 $\mathbf{N} = \{1, 2, \dots, n, \dots\}$ 的单满映射。

于是 \mathbb{Q} 是可数无限集。|

系 设有可数集 $S_i = \{s_{i1}, s_{i2}, \dots, s_{in}, \dots\}$, $i \in$ 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 \mathbb{R} 为不可数集。

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

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

$$r_1 = a_1 . b_{11} b_{12} \dots b_{1n} \dots,$$

$$r_2 = a_2 . b_{21} b_{22} \dots b_{2n} \dots,$$

$$\dots \dots \dots$$

$$r_n = a_n . b_{n1} b_{n2} \dots b_{nn} \dots,$$

$$\dots \dots \dots$$

其中诸 a_i 为整数, b_{ij} 为 $0, 1, 2, \dots, 9$ 之一。现取一实数

$$r = 0 . c_1 c_2 \dots c_n \dots$$

如下: 如果 $b_{nn} \neq 5$, 则取 $c_n = 5$, 否则取 $c_n = 4$ ($n = 1, 2, \dots$)。显然 $r \neq r_n$ ($\forall n = 1, 2, \dots$)。故 r 不在集合 $\{r_1, r_2, \dots, r_n, \dots\}$ 之中。由此知 \mathbb{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, $\prod_{i \in I} S_i$ 中的元素常写成一排 $(s_1, s_2, \dots, s_n, \dots)$ 。

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 $T = \bigcup_{i \in I} T_j$, 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” \sim 如下:

$$a \sim b \iff a, b \text{ 属于同一个 } T_j.$$

一般言之, 任意关系“ \sim ”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 $a \sim c$ 。 |

我们也可以利用等价关系来定义商集如下。

定义 1.4* 设 \sim 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 \sim 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 $T_a \cap T_c \neq \emptyset$, 则 $T_a = T_c$ 。 |

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“ \geq ”如适合下列条件, 则称之为一个半序:

$$1) s_1 \geq s_1, \quad \forall s_1 \in S;$$

$$2) s_1 \geq s_2, s_2 \geq s_3 \implies s_1 \geq s_3, \quad \forall s_1, s_2, s_3 \in S;$$

$$3) s_1 \geq s_2, s_2 \geq s_1 \implies s_1 = s_2, \quad \forall s_1, s_2 \in S.$$

定义1.6 设 S 为一集合, \geq 为 S 的半序。如果适合下列条件, 则称 \geq 为 S 的序:

$$4) \text{对任意的 } s_1, s_2 \in S, \text{ 总有 } s_1 \geq s_2 \text{ 或 } s_2 \geq s_1.$$

定义1.7 设 \geq 为 S 的半序, T 为 S 的子集。如果 S 的一个元素 s , 适合 $s \geq t$ ($\forall t \in T$), 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 $s_1 \geq s$, 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, \geq 为 S 的半序, T 为 S 的子集。如果局限于 T 中 \geq 是一个序, 则称 T 为一链。

Zorn引理 设 S 为一非空集合, \geq 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