近古代史

范云棟　盛德成

西　北　大　学

近世代数

范云棣
盛德成

西北大学

引　言

近世代数在现代数学中的地位和作用已经引起人们的广泛兴趣和重视，它已经成为进入现代数学的阶梯和基础。如果想深入钻研拓扑学、微分几何、同调代数、范畴论等，都需要以近世代数来起步。目前，许多高等院校都已经把近世代数作为数学等专业的一门必修课来开设，为了适应这个需要，我打算写一本介绍近世代数的书。一九七九年夏天，美国维琴尼亚洲诺福克州立大学（NORFOLK STATE UNIVERSITY）数学系范云棣教授（加拿大马基大学数学博士 P. h. D. McGILL UNIVERSITY CANADA）应邀来我校讲学。范教授是著名学者，对近世代数的研究有深的造诣。在西北大学巩重起付校长的支持和鼓励下，我们合作编写了近世代数这本书。

盛德成

一九八〇年十月

序　言

本书共分五章。第一章介绍若干基本概念，它为本书的其余各章提供了一个共同的比较坚实的基础，即使对这一部分内容比较熟悉的读者，再仔细地阅读一下这一部分的内容，也会是有好处的。第二章介绍代数结构——群；第三章介绍代数结构——环与域；第四章介绍格与布尔代数，这四章是基本内容。第四章对于希望从事计算机科学的读者更是需要的。第五章介绍模的概念以及环结构的一些初步知识，起步比较高一些，读起来可能困难些。我们希望它能为愿意在这方面作深入钻研的读者开一个头。除第五章外，几乎每一节后都附有相当数量的难易程度不同的习题，这些习题将使读者加深对基本内容的理解，同时也检验读者对基本内容的掌握程度，有时还对基本内容作了一些补充。本书最后附有中英对照的名词索引。

本书的目的在于为初学近世代数的读者提供一本合适的书，在写法上力求简明，初学者往往苦于概念的高度抽象性，因此本书列入了大量的富有启发性的例题和习题，以引

起和培养读者的学习兴趣。本书在介绍基本内容的同时也考虑到了为读者提供进一步钻研的余地。本书内容偏重于群和环，对域讨论得较少些。

本书在编写过程中，得到了西北大学数学系领导和同事们的大力支持和帮助，我们深表感射。

由于时间仓促，加之我们水平有限，错误之处在所难免，在教学中，如有疑问或意见，欢迎函询西北大学笔者，以便今后更正。不胜感谢。

美国维琴尼亚洲诺福克州立大学　范云棣
中　国　西　北　大　学　盛德成

一九八〇年十月

目　录

第一章　基本概念

近世代数是研究各种代数结构的，比如，群、环、域、格、模等。但这些代数结构的基本成份是集合和集合上的映射，因此，在本书的讨论中常常要用到集合论中的一些概念和结论。为此，在着手研究各种代数结构之前，先对集合论中的一些基本概念作一个简要的讨论。

§1—1 集合、子集、集的运算

集合这个概念是数学中的基本概念。我们对它作如下的说明，集合是由元素组成的。这样，给定了一个集合M，即是给出了M是由哪些元素组成的。

例：三年级一班全体学生的集合。

线性方程组AX=B的解向量的集合。

多项式f(x)的零点的集合。

平面上通过点M(1，4)斜率为3的直线上所有点的集合。

全体偶正整数的集合。

全体自然数的集合。

数域P上所有m行n列的矩阵的集合。

多项式f(x)、g(x)的公因式的集合。

一般以大写字母A，B，C，…，M，N，…表示集合，而以小写字母a，b，c，…表示集合的元素。由此，两个集合M，N相等是指它们是由同样的元素组成的。记为

M = N.

若元素a是集合A的元素，用符号$a \in A$表示；若元素a不是集合A的元素，用符号$a \notin A$表示。给出一个集合M 通常有两种方式，一种是列出集合M的全部元素。比如：

$M = \{1, 2, 3\}$, $N = \{a, b\}$

另一种方式是给出这个集合的定义性质，这时集合M用如下的记号表示，

$$M = \{a \mid P(a)\}$$

它表示所有使命题P(a)为真的元素a的集合。比如：

f(x)，g(x)的所有公因式的集合M可以表示为

$$M = \{d(x) \mid d(x) \mid f(x),\ d(x) \mid g(x)\}$$

这儿$d(x) \mid f(x)$表示d(x)是f(x)的因式。给出一个集合的这一方式特别重要，因为当一个集合由无限多个元素组成时，要列出它们是困难的。

空集合ϕ是指一个元素也没有的集合。比如

$$M = \{x \mid x\text{是实数}, x^2 + 1 = 0\}$$

就是一个空集合，即$M = \phi$。空集合的引入可以使我们在谈到一个集合时不必事先论证这个集合至少含有一个元素。

在本书中经常用到的几个集合，常用下述记号表示：

N = 所有自然数的集合。

Z = 所有整数的集合。

Q = 所有有理数的集合。

R = 所有实数的集合。

C = 所有复数的集合。

设A、B是两个集合，若

$b \in \beta \Longrightarrow b \in A$，（即由$b \in B$推出$b \in A$）

则称B为A的子集，记为$B\subseteq A$或$A\supseteq B$.

这样，容易看到

$$A=B\Longleftrightarrow A\subseteq B,\ B\subseteq A.$$

由此，当我们要证明$A=B$时，我们常常去证明

$$x\in A\Longrightarrow x\in B\text{以及}x\in B\Longrightarrow x\in A.$$

例：全体偶数的集合E是Z的子集。又显然地对任何集合A有$\phi\subseteq A$，$A\subseteq A$。

设A是一个给定的集，令

$$P(A)=\{B\mid B\subseteq A\}$$

它是A的所有子集的集合，叫做A的幂集。

例：若$A=\{1,2,3\}$，则

$$P(A)=\{\phi,\{1\},\{2\},\{3\},\{1,2\},\{2,3\},\{1,3\},\{1,2,3\}\}.$$

这儿应该注意，a与$\{a\}$是不同的，$a\in A$而$\{a\}\in P(A)$.

设A，B是两个集合，令

$$A\cap B=\{c\mid c\in A,c\in B\}$$

叫做集合A与B的交.

例：设$A=\{(x,y)\mid 2x-y=2\}$是方程$2x-y=2$的解向量的集合，$B=\{(x,y)\mid x-2y=2\}$是方程$x-2y=2$的解向量的集合，则$A\cap B$是方程组

$$\begin{cases}2x-y=2\\ x-2y=2\end{cases}$$

的解向量的集合。类似地，设有集簇$\{A_i\}$，令

$$\bigcap A_i=\{c\mid \text{对每一}i\text{有}c\in A_i\}$$

叫做$\{A_i\}$的交。

若 $A \cap B = \phi$，即A，B 无公共元素，则说A，B 不相交。

令 $A \cup B = \{ c \mid c \in A$ 或 $c \in B \}$

叫做A 与B的并。

例：设 $A = \{ 1, 2, 3 \}$；$B = \{ 2, 4, 5 \}$，则 $A \cup B = \{ 1, 2, 3, 4, 5 \}$，而 $A \cap B = \{ 2 \}$。

类似地，设有集簇 $\{ A_i \}$，令

$$\bigcup A_i = \{ c \mid \text{存在一个 } i \text{ 使 } c \in A_i \}$$

叫做 $\{ A_i \}$ 的并。

练习 1—1

一、下述诸集合中，哪些是相等的？

$A = \{ x \mid x$ 是＜10的偶正整数 $\}$

$B = \{ x \mid x \in N, x^2 < 90 \}$

$C = \{ 2, 4, 6, 8 \}$

$D = \{ 1, 2, 3, 4, 5, 6, 7, 8, 9 \}$

二、下述命题哪些是对的，哪些是错的？

1、$\phi \in \{ \phi \}$

2、$\phi \in \phi$

3、$\phi \in \{ 0 \}$

4、$0 \in \phi$

5、$\phi \in \{ \{ \phi \} \}$

6、$\{ 1, 2 \} \in \{ \{ 1 \}, \{ 2 \}, \{ 1, 2 \}, \{ \{ 1, 2 \} \} \}$

7、$2 \in \{ \{ 1 \}, \{ 2 \}, \{ 1, 2 \}, \{ \{ 1, 2 \} \} \}$

三、对任何集A，完成下述等式

$A \cup \phi =$ ；$A \cap A =$ ；

$A \cap \phi =$ ；$A \cup A =$ 。

四、设$A=\{1, 3, 5\}$，$B=\{3, 7\}$，$C=\{x \mid x \in N, x \geqslant 9\}$，$D=\{x \mid x \in N, x<45\}$，$E=\{x \mid x \in N, 2<x<50\}$，确定下列集合

$C \cap D =$

$C \cup D =$

$C \cup E =$

$D \cap E =$

$C \cap D \cap E =$

$(C \cap D) \cup E =$

$\{x \mid x \in N, x^2 \in B\} =$

五、设$A=\{a, \square, \triangle, *\}$，写出$P(A)$的全部元素。

六、对于给定的集合A，考察幂集$P(A)$，此时常称A为全集合，对$B \in P(A)$，称$B'=\{x \in A \mid x \notin B\}$为B的余集合。试证下述De Morgan定理：

$$(B_1 \cup B_2)' = B_1' \cap B_2'$$

$$(B_1 \cap B_2)' = B_1' \cup B_2'$$

§1—2 笛卡尔积集，映射

1° 笛卡尔积集

设S、T是两个集合，令

$$S \times T = \{(s, t) \mid s \in S, t \in T\}$$

$S \times T$中的两个元素(s_1, t_1)与(s_2, t_2)叫做相等的，是指$s_1 = s_2$和$t_1 = t_2$，称$S \times T$为S与T的笛卡尔积。这儿并不要求S与T不相同。若S有m个元素，T有n个元素，则显

然S×T有m·n个元素。以后我们约定以|S|表示S中元素的个数，则|S×T| = |S| |T|.

例：设S={1，2}，T={1，2，3}，则

S×T={(1，1)，(1，2)，(1，3)，(2，1)，(2，2)，(2，3)}

例：设S为平面上x－轴上的点的集合，T为y－轴上的点的集合，则S×T为整个平面上的点的集合。

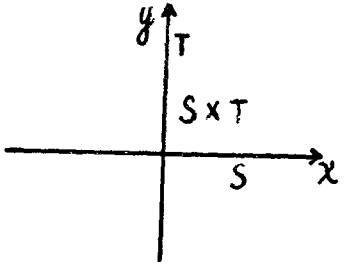

图 1－2－1

一般地，S_1，S_2，…，S_r是任意r个集合，则称所有r－有序组$(s_1, s_2, \cdots s_r)$，$s_i \in S_i$，的集合为S_1，S_2，…，S_r的笛卡尔积，记为$S_1 \times S_2 \times \cdots \times S_r$，从而

$$S_1 \times S_2 \times \cdots \times S_r = \{(s_1, s_2, \cdots, s_r) \mid s_i \in S_i,\ i = 1, 2, \cdots, r\}.$$

2° 映射

定义1－2－1：集合S到集合T中的一个映射是有序三组〈S，T，μ〉，这儿μ是一个对应法则，依此，对每一$s \in S$有唯一的$t \in T$与之对应，记t为$t = s\mu$，集合S叫做该映射的区域，T叫做余区域。

映射〈S，T，μ〉常常记为$\mu: S \longrightarrow T$，或$S \xrightarrow{\mu} T$。当在上下文中S，T是清楚的时候，可以简单地说映射μ。对于映射$\mu: S \longrightarrow T$，若$t = s\mu$，则t叫做s关于μ的象，而s叫做t关于μ的前象。

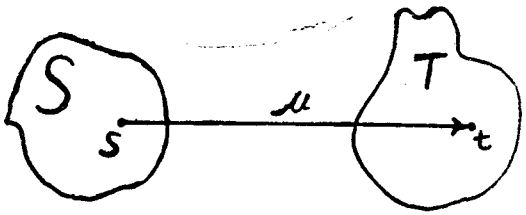

图 1—2—2

例 1 考察μ：Z⟶R，其中xμ = 2x，它是一个映射。

例 2 设S是数域P上的n阶方阵的集合，T = P，则μ：S⟶T，xμ = |x| 是矩阵x的行列式，是一个映射。

例 3 给定S、T及$t_0 \in T$，命μ是这样一个对应，对任何$s \in S$，$s\mu = t_0$。则μ：S⟶T是一个映射。

例 4 对给定的S，考察T = S，并令μ是这样的对应，对任何$s \in S$，有$s\mu = s$，则μ：S⟶S是一个映射，它叫做S上的恒等映射，记为I_S。

例 5 设f为定义在实数集R上的通常的函数，则f：R⟶R是一个映射。

例 6 考察实数集R，对每一$x \in R$，令$x\mu = \frac{1}{x}$，则〈R，R，μ〉不是一个映射，因为0μ不存在。

例 7 设S是所有有理数的集合，T为整数集合，对$s \in S$，令sμ为把s写成分数$s = \frac{q}{p}$时的分母，则〈S_1，T，μ〉不是映射，因为sμ不唯一。比如：$s = \frac{2}{3} = \frac{4}{6}$，从而

$\frac{2}{3}\mu = 3$， $\frac{2}{3}\mu = 6$，……

例 8，考察μ：$R \longrightarrow N$，$x\mu = |x|$是x的绝对值，它不是一个映射，比如$3.5\mu = 3.5 \notin N$.

两个映射$\alpha_1 : S_1 \longrightarrow T_1$，$\alpha_2 : S_2 \longrightarrow T_2$叫做相等的，是指$S_1 = S_2$，$T_1 = T_2$，对任何$s \in S_1$有$s\alpha_1 = s\alpha_2$。

3° 映射的图形。

定义 1－2－2：设有映射$\mu : S \longrightarrow T$，称

$$G(\mu) = \{(s, t) \mid t = s\mu, s \in S\} \subseteq S \times T$$

为该映射的图形。

从定义，立即得到$G(\mu)$具有下述性质：

1　对任何$s \in S$，存在$t \in T$，使 $(s, t) \in G(\mu)$

2　$(s, t_1) \in G(\mu), (s, t_2) \in G(\mu) \Longrightarrow t_1 = t_2$。

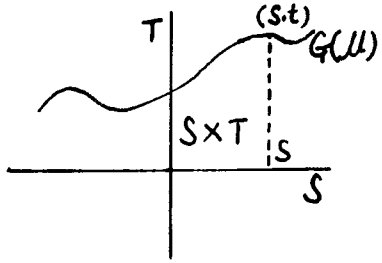

图 1－2－3

这两条性质完全刻划了$S \times T$中的一个子集能作为某一映射的图形的条件。事实上，若$G \subseteq S \times T$具有上述性质 1，2，则可定义映射μ：$S \longrightarrow T$如下：对$s \in S$，由性质1，存在$t \in T$使 $(s, t) \in G$，又由性质 2，这种t是唯一的，

令$s\mu = t$，从而得到了映射μ：$S \longrightarrow T$，而且正好有$G = G(\mu)$。

从而，我们也可以把映射定义为有序三组$\langle S, T, G\rangle$，其中$G \subseteq S \times T$具有上述性质1、2。

容易看到，若α_1：$S_1 \longrightarrow T_1$

α_2：$S_2 \longrightarrow T_2$

则$\langle S_1, T_1, \alpha_1\rangle = \langle S_2, T_2, \alpha_2\rangle \Longleftrightarrow S_1 = S_2$，$T_1 = T_2$，$G(\alpha_1) = G(\alpha_2)$。

4° 几种特殊的映射。

定义1—2—3：映射μ：$S \longrightarrow T$叫做内射或1—1的，是指$s_1 \neq s_2 \Longrightarrow s_1\mu \neq s_2\mu$。

由此，若μ：$S \longrightarrow T$是内射，$t \in T$若有前象，则是唯一的，反之亦然。

定义1—2—4：映射μ：$S \longrightarrow T$叫做满射或到上的，是指对任何$t \in T$，都存在$s \in S$使$t = s\mu$。即T中的每一个元素都有前象，也就是说，T中的每一个元素都是S中某个元素的象。

定义1—2—5：映射μ：$S \longrightarrow T$叫做双射或1—1到上，是指它既是内射又是满射。

按定义，本节中的

例1 是内射但不是满射。

例2 不是内射但是满射。

例3 不是内射也不是满射。

例4 是双射。

一般地，