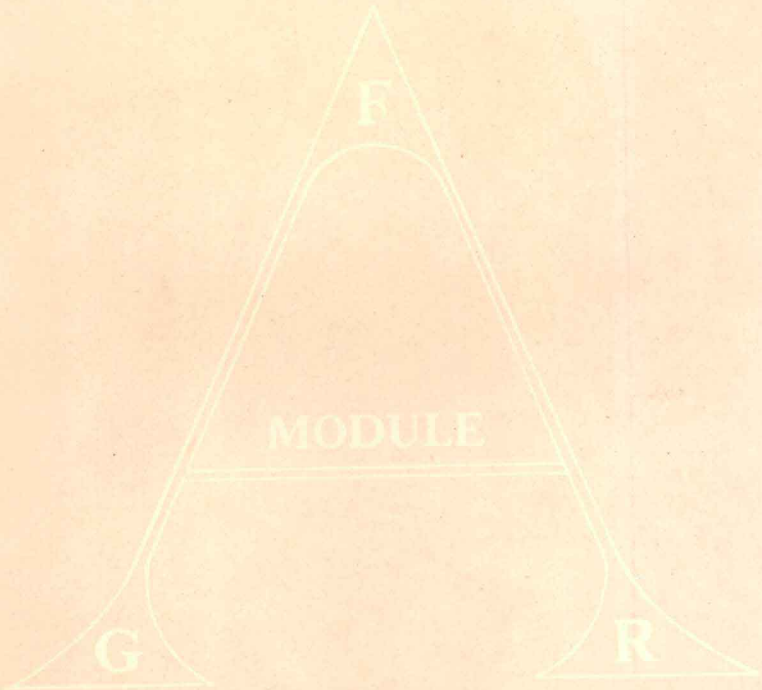
高等学校理科教材

# 近世代數

（第四版）

熊全淹 编著




武汉大学出版社

# 近世代数

（第四版）

熊全淹 编著

武汉大学出版社

一九九一年·武汉

## 内 容 提 要

本书系统地介绍近世代数的基本理论。全书共八章。前四章对群、环、体、模的基础理论作一般的介绍，后四章则作进一步较深入的论述。每节后附有习题，每章后列有参考文献。书末附有习题解答，供读者参考。

本书叙述由浅入深，推理详尽，便于阅读，可作为高等院校数学系大学生和研究生近世代数课的教材或教学参考书，也可供广大教师和数学工作者参考。

近世代数
（第四版）
熊全淹 编著
*
武汉大学出版社出版
（430072 武昌 珞珈山）
新华书店湖北发行所发行
武汉大学印刷厂印刷
*
850×1168毫米 1/32 13.125印张 336千字
1963年10月第1版 1978年8月第2版
1984年9月第8版 1991年12月第4版
1991年12月第4版第1次印刷
印数：1—3000
ISBN 7-307-00856-4/O·74
定价：4.25元

# 第三版前言

本书较系统、全面地介绍近世代数的基本理论。作为高等院校数学系学生的基础读本，在内容选择上，力求简明扼要，避免涉及一些过于难深的问题，以求达到加深基础理论的认识。在次序编排上，大体参照范德瓦尔登著《代数学》一书。

本书自成系统，论述由浅入深，推理详尽，读者不必参考其它书籍就可顺利阅读。每节后附有习题，有些习题提出了一些重要概念和问题，读者宜加注意。书末附有解答，供读者校核。每章后列出了适当的参考文献，其中有些表明近代发展情况，也有不少选自 Amer. Math. Monthly 杂志上的短文；后者内容大都不太困难，读者如有可能，望选择阅读，以加深基本功的训练，增强解决问题的能力。

本书是根据多年来武汉大学数学系的《近世代数讲义》改编而成。1963年第一版和1978年第二版都由上海科学技术出版社出版，此次第三版则由武汉大学出版社出版。它们对本书出版的鼓励和支持，编者表示衷心感谢。

这次改版变动较大，主要是简化了一些定理的证明、添加了一些内容、改正了发现的错误、改写了某些节段，但仍保留了全书的结构。本书屡经修改，质量虽有所提高，但限于编者水平，缺点和错误仍在所难免，敬请读者惠予指正。

本书初版、二版以来，承蒙广大读者爱护，提出了不少宝贵意见，使得本书在修订改版中得以改进，在此一并谨表谢忱。

编　者

1983年10月于珞珈山

武汉大学

# 第四版前言

这次修改主要是充实模的内容，除在新增加的第4章§4.1中系统地介绍外，在其他有关章节也适当补充，目的在介绍模的最基本的概念及性质，供读者看其他代数参考书之用。因为在本书对模的引用不多，所以不作更多的论述。此外简化了某些定义，改写了某些证明，改正了一些错误，还适当增补了一些内容，各章都有变动，大小不一。

新添了第4章，其中第2节是从以前的§4.4搬来的，其它章节仍旧没有变动。这样全书共8章，前4章是群、环、体、模的基本介绍，后4章是它们较深入的论述。

这次改动承副教授谭季伟同志提出了很多宝贵意见，使本书生色不少，附此志谢。

编　者

1990年12月，时年八十

于珞珈山

# 目　录

# 第一章　基本概念

这章简单地介绍集合、映射、分类等基本概念，并且解释记号 $\in$，$\subset$，$\supset$，$\cap$，$\cup$，$\{\cdots\}$等的意义，作为以后各章的准备。

## §1.1 集　　合

数学中讨论的对象，如代数中的数、矩阵，几何中的点、直线等，我们现在统统叫做**元素**，有时就简单地叫做**元**。若干个（有穷个或无穷多个）元的集体，叫做**集合**，或简单地叫做**集**。

我们要知道一个集，必定要知道其中所有的元，也就是说，我们对于任意一个元，要能够判别它是否在这个集中。譬如，所有整数组成一个集，因为我们随便拿一个数来，都可以判别它是否是整数，这个集又叫做**整数集**，我们用 $Z$ 来表示。

一个集都有自己的特性，譬如，整数集中任意元，都有整数这个特性。平面上所有点组成的集与平面上所有圆组成的集都各有各的特性。因此，对于一个集，我们可以用它的特性来判别任意元是否在它里面。

任意一个元 $a$，如果它有集合 $M$ 的特性，也就是说，它是 $M$ 中元时，我们就用记号

$$a \in M$$

来表示。如果它没有集合 $M$ 的特性，也就是说，它不是 $M$ 中元时，我们就用

$$a \overline{\in} M$$

来表示。这时，$a$ 在 $M$ 中我们也说 $a$ 属于 $M$，或者说 $M$ 包含 $a$。同样，$a$ 不在 $M$ 中我们也说 $a$ 不属于 $M$，或者说 $M$ 不包含 $a$。一个集含有限个元，称为有穷集，否则它叫做**无穷集**。一个集所含元的个数，叫做这集的**元数**或**浓度**。有穷集的元数当然是正整数。

集合可以用列举其中所有元来表示，譬如，整数集 $Z$ 可以写成

$$Z=\{0,1,-1,2,-2,\cdots\},$$

或

$$Z=\{\cdots,-2,-1,0,1,2,\cdots\}.$$

一般，假如 $M$ 含元 $a,b,c,\cdots$，我们就用记号表为

$$M=\{a,b,c,\cdots\}.$$

通常一个集都含有一个以上的元，但是当它只含一个元时，这个集就与它所含的那唯一个元常常不加区别。为了叙述方便，我们更假定不包含任何元的也成为一个集，叫做**空集**，它的元数是零。譬如，大于1而小于2的整数集合就是空集。

假如集合 $N$ 中所有元都是集合 $M$ 中元，也就是说，$N$ 是 $M$ 的一部分，或者说，任意一个元，如果它含 $N$ 的特性，它一定也有 $M$ 的特性，那末 $N$ 就叫做 $M$ 的**子集**，$M$ 又叫做 $N$ 的**包含集**。我们用记号 $N\subseteq M$ 或 $M\supseteq N$ 表示。子集与包含集的关系可以用图形（图1.1）来说明。

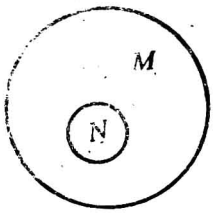


图 1.1

有穷集的子集是有穷集，无穷集的包含集又是无穷集。

为了方便，我们假定任意集都包含空集。再从 $A\subseteq B$ 及 $B\subseteq C$，我们就得到 $A\subseteq C$。

假如 $M$ 中所有元都属于 $N$，同时 $N$ 中所有元又都属于

$M$，即

$$M\subseteq N,\ N\subseteq M,$$

也就是说，$M$ 与 $N$ 的特性完全相同时，我们就说 $M$ 与 $N$ **相等**，用记号

$$M=N$$

表示。假如 $N\subseteq M$，但 $M$，$N$ 不相等，那末 $N$ 就叫做 $M$ 的**真子集**，$M$ 叫做 $N$ 的**真包含集**，用记号

$$N\subset M \text{ 或 } M\supset N$$

表示，这时 $N$ 中所有元都属于 $M$，但 $M$ 中至少有一个元不属于 $N$。

上面，我们介绍了集合的基本概念，现在介绍它的三个结合法。

**定义1** 假如 $M$，$N$ 是两个集，那末属于 $M$ 同时又不属于 $N$ 的所有元形成的集 $D$，叫做 $M$ 与 $N$ 的**差集**，用记号

$$D=M-N$$

表示。

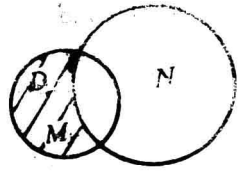



图 1.2

显然，$D$ 是 $M$ 的子集。

$$M-N\neq N-M$$

关于差集的概念，我们可以用图形（图1.2）来说明。

**定义2** 假如 $M$，$N$ 是两个集，那末属于 $M$ 同时又属于 $N$ 的所有元形成的集 $P$，叫做 $M$ 与 $N$ 的**交集**，用记号

$$P=M\cap N$$

表示。

于是 $P$ 是 $M$，$N$ 的子集，并且任何集只要它同时是 $M$，$N$ 的子集，它一定是 $P$ 的子集，因此 $P$ 是包含在 $M$，$N$ 中的**最大集**。关于交集的概念，我们可以用图形（图1.3）来说明。

**定义3** 假如 $M$，$N$ 是两个集，那末属于 $M$ 或者属于 $N$

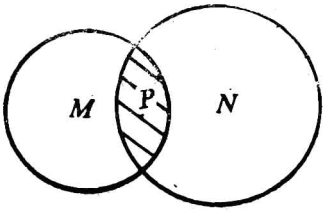



图 1.3

的所有元形成的集 $S$，叫做 $M$ 与 $N$ 的**并集**，用记号

$$S = M \cup N$$

表示。

于是 $S$ 是 $M$，$N$ 的包含集，并且任何集只要它同时是 $M$，$N$ 的**包含集**，它一定也是 $S$ 的**包含集**，因此 $S$ 是包含 $M$，$N$ 的**最小集**。关于并集的概念，我们可以用图形（图1.4）来说明。

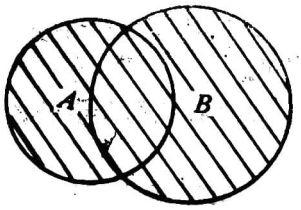



图 1.4

由定义，我们容易得知 $N \cap (M - N)$ 是空集，又

$$M = (M \cap N) \cup (M - N).$$

假如 $A, B, C$ 是三个集，显然

$$(A \cap B) \cap C = A \cap (B \cap C),$$
$$(A \cap B) \cap C = (A \cap C) \cap (B \cap C),$$
$$(A \cup B) \cup C = A \cup (B \cup C),$$
$$(A \cup B) \cup C = (A \cup C) \cup (B \cup C).$$

下面是关于交集与并集的两个分配律。

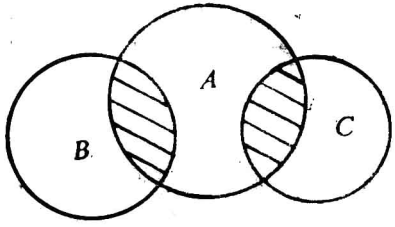



图 1.5

**定理** $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$。

用图形说明如左：

**证明** 首先因为

$$B \subseteq B \cup C$$

所以 $A \cap B \subseteq A \cap (B \cup C)$。

同样 $A \cap C \subseteq A \cap (B \cup C)$

因此 $$(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C).$$

再假如 $a\in A\cap(B\cup C)$，那末 $a\in A$，$a\in B\cup C$ 于是 $a\in B$ 或 $a\in C$. 从前者言，$a\in A\cap B$；从后者言，$a\in A\cap C$. 因此 $a\in(A\cap B)\cup(A\cap C)$，这就是说

$$A\cap(B\cup C)\subseteq(A\cap B)\cup(A\cap C),$$

所以定理成立.

同样我们有

$$A\cup(B\cap C)=(A\cup B)\cap(A\cup C).$$

为了区别，由元组成的集，叫做**第一层集**，把第一层集当作元组成的集，叫做**第二层集**. 第二层集又常叫做**系**.

若干个集的交集与并集可以按两个集的情形同样定义. 假定 $L$ 是由集 $A, B, C, \cdots$ 组成的系，我们用

$$A\cap B\cap C\cap\cdots$$

表示 $L$ 的交集，用

$$A\cup B\cup C\cup\cdots$$

表示 $L$ 的并集. 要注意的是 $L$ 虽然是第二层集，但它的交集、并集却都是第一层集.

## 习 题 1.1

1. 任意两个集是否都有交集与并集？
2. 假定 $A\subseteq B$，那末 $A\cup B=$？$A\cap B=$？
3. 假定 $A, B, C$ 是三个集，试证

   (i) $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$；

   (ii) $(A-B)\cup(B-A)=(A\cup B)-(A\cap B)$.
4. 假定 $A, B, C$ 是三个集，如果它们的乘法规定是

$$AB=(A\cup B)-(A\cap B),$$

试证

$$(AB)C=A(BC).$$

5. 假定 $M$ 是元数为 $n$ 的有穷集，$L$ 是 $M$ 的所有子集组成的系，试证 $L$ 的元数是 $2^n$.

## §1.2 映射、分类

我们知道，近世代数中集合的元是抽象的，因此，两个集合如何进行比较是一个重要问题．映射这个概念主要用途之一就是用来解决这个问题，它是近世代数中最基本的工具．

下面是一些最基本概念．

对于集 $M$ 中每一个元 $a$，如果根据某种规则，我们可以使它与集 $N$ 中唯一个元对应，那末这对应叫做 $M$ 射到 $N$ 的**映射**，那个与 $a$ 对应的元，叫做 $a$ 的**象**，$a$ 又叫做它的象的**象源**．这时 $M$ 中任意元在 $N$ 中都有象，但 $N$ 中任意元在 $M$ 中不一定都有象源．如果 $N$ 中元在 $M$ 中不都有象源，那末这映射叫做 $M$ 射到 $N$ **内的映射**．如果 $N$ 中任意元在 $M$ 中都有象源，那末这映射叫做 $M$ 射到 $N$ **上的映射**．有时又叫做**满射**．

假如 $M$ 射到 $N$ 的映射用 $\sigma$ 来表示，那末 $a$ 的象，我们就用 $\sigma(a)$来表示，有时这映射又表为 $a\to\sigma(a)$．映射这个概念与数学分析中函数的概念一致，因此 $\sigma(a)$又常叫做 $a$ 的**函数**．

显然，$M$ 射到 $N$ 内的映射就是 $M$ 射到 $N$ 中某个子集上的映射．譬如在整数集 $Z$ 中，根据自乘这个规则，把任意整数 $a$ 与它的自乘 $a^2$ 对应，即 $a\to a^2$，那末这对应是 $Z$ 射到自己内的映射，也是 $Z$ 射到由所有整数平方组成的子集上的映射．

我们知道，对于映射 $\sigma$，象源 $a$ 固然只有唯一的象 $\sigma(a)$，但是象 $\sigma(a)$就不一定只有一个象源 $a$，它可能有一个以上的象源．任意象只有一个象源的映射，又叫做**一对一的映射**；有时叫做**单射**，不是一对一的映射，又叫做**多对一的映射**．假如 $\sigma$ 是 $M$ 射到 $N$ 的映射，$B$ 是 $N$ 的子集，$A$ 是 $M$ 中所有这样元组成的子集，它们的象都在 $B$ 中，那末 $A$ 叫做 $B$ 对于映射 $\sigma$ 的**完全象源**．

$M$ 射到 $N$ 的映射 $\sigma$，当 $a_1 \neq a_2$ 时，$\sigma(a_1) \neq \sigma(a_2)$，也就是说，当 $\sigma(a_1) = \sigma(a_2)$ 时，$a_1 = a_2$，那末 $\sigma$ 就是单射。单射又是满射时，有时叫做**双射**。

集合 $M$ 射到 $N$ 的双射 $\sigma$ 又叫做**可逆映射**，用记号

$$a \leftrightarrow \sigma(a)$$

表示。这时 $N$ 中元 $b$ 的象源用 $\sigma^{-1}(b)$ 来表示。显然 $b \to \sigma^{-1}(b)$ 是 $N$ 射到 $M$ 上的映射，我们叫它做 $\sigma$ 的**逆映射**，用记号 $\sigma^{-1}$ 表示。因此，任意可逆映射都有唯一个逆映射，这逆映射也是可逆映射。假如 $\sigma$ 是可逆映射，那末它的逆映射 $\sigma^{-1}$ 的逆映射就是 $\sigma$，这就是说

$$(\sigma^{-1})^{-1} = \sigma.$$

譬如，在整数集 $Z$ 中，我们把偶数与0对应，奇数与1对应，这样就得到 $Z$ 射到集合 $\{0, 1\}$ 上的映射，这映射是多对一的，0的完全象源是所有偶数，1的完全象源是所有奇数，它们都没有唯一的象源。假如我们把整数 $n$ 与 $2n$ 对应，即 $n \to 2n$，那就得到 $Z$ 射到偶数集上的映射，这映射是单射，因此它是可逆映射，它的逆映射就是 $2n \to n$。

假如有一个单射把两个集 $M$、$N$ 中的一个，譬如说 $M$，射到另一个 $N$ 上，那末这两个集就叫做**有相等的浓度，或元数**。显然 $Z$ 与偶数集有相等的浓度，因此一个集的浓度也可以与它的真子集的浓度相等，这是无穷集的一个重要性质。任意有穷集是没有这个性质的。与正整数集或它的子集有相等浓度的集，叫做**可数集**。一个集如果不是可数集，就叫做**不可数集**。任一可数集中元可以用正整数做标号来排列，于是任意可数集 $M$ 可以写成

$$M = \{a_1, a_2, \cdots, a_n, \cdots\}.$$

有穷集是可数集，正整数集是可数集，整数集 $Z$ 也是可数集。再可数个可数集的并集又是可数集，因此有理数集是可数集。

假定 $M=N$，那末 $M$ 射到 $N$ 的映射，就叫做 $M$ 射到**自己的映射**，$M$ 射到 $N$ 上（内）的映射，就叫做 $M$ 射到**自己上（内）的映射**。$M$ 射到自己双射即 $M$ 的可逆映射，有时又叫做 $M$ 的**变换**。对于 $M$ 中任意元使自身与它对应，也就是说，不使 $M$ 中任意元变动，是 $M$ 射到自己的双射，叫做 $M$ 的**恒等映射**，用 $I$ 表示，即 $I(a)=a$。很多重要的映射都是射到自己上的映射，譬如，平面上的旋转就可以看成为平面上的点集射到自己上的映射。要注意的是 $M$ 射到自己内的映射有时是单射，而 $M$ 射到自己上的映射却有时不是单射。譬如，$n\to 2n$ 就是 $Z$ 射到自己内的单射，$2n\to n$，$2n+1\to 2n+1$ 是 $Z$ 射到自己上的多对一的映射。

假如 $\sigma_1,\sigma_2$ 都是 $M$ 射到 $N$ 的映射，如果对于 $M$ 中任意元 $a$，有 $\sigma_1(a)=\sigma_2(a)$，我们就说这两个映射**相等**，用记号 $\sigma_1=\sigma_2$ 表示。假如 $\sigma$ 是 $A$ 射到 $B$ 的映射，$\tau$ 是 $B$ 射到 $C$ 的映射，$\sigma(a)=b$，$\tau(b)=c$，即 $a\to b$，$b\to c$，我们容易证明，对应 $a\to c$ 就是 $A$ 射到 $C$ 的映射，叫做映射 $\tau$，$\sigma$ 的**积**，用记号 $\tau\sigma$ 表示，即

$$\tau\sigma(a)=\tau(\sigma(a)).$$

这就是说，$\tau\sigma$ 是先施行 $\sigma$，后施行 $\tau$ 得到的映射。

要注意的是，同一个集的任意两个映射的积是存在的，但一般对于不同集的两个映射不一定有积，假如有积，其积也不只一个。譬如 $\sigma$ 是 $M$ 射到 $N$ 的映射，$\tau$ 是 $N$ 射到 $M$ 的映射，这时，$\tau\sigma,\sigma\tau$ 都有意义，但前者是 $M$ 射到自己的映射，而后者则是 $N$ 射到自己的映射，两者显然不一致。即令 $M=N$，一般 $\tau\sigma$ 与 $\sigma\tau$ 也不一定相等，即 $\tau\sigma\neq\sigma\tau$，也就是说，映射的乘法不适合交换律。象这样的例子，我们在几何上是常见的。再假如 $\sigma$ 是可逆映射，那末 $\sigma^{-1}\sigma(a)=a$，因此 $\sigma^{-1}\sigma=I$，这就是说，$\sigma^{-1}\sigma$ 是恒等映射。同样，$\sigma\sigma^{-1}$ 也是恒等映射。再假如 $\sigma$，$\tau$ 都是可逆映射，那末 $\tau\sigma$，$\sigma\tau$ 又都

是可逆映射．显然 $\sigma^{-1}\tau^{-1}$，$\tau^{-1}\sigma^{-1}$ 就分别是它们的逆 映射．

为了方便映射等式 $\gamma=\tau\sigma$有时用**交换图**（图1.6）来表示.同

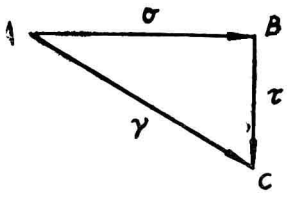



图 1.6

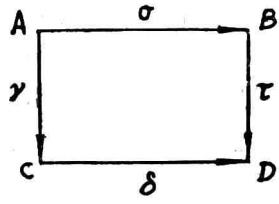



图 1.7

样，交换图（图1.7）表示 $\tau\sigma=\delta\gamma$．这里所谓的交换是指在图中从一个始点沿着每一条路线到达一个终点所得到的映射都是相等的．

假定对于集 $M$ 中任意两元 $a, b$，根据某个规则，我们可 以把 $a, b$ 与某集中唯一的一个元 $c$ 对应，那末这对应，我们 叫 做 $M$ 的**结合法**，有时又叫做 $M$ 的**代数运算**．这时我们又常常说，根据这结合法，可以把 $a$，$b$ 结合得到元 $c$，因此我们又说 $M$ 有一个结合法．譬如，对于整数集 $Z$中任意两数 $a, b$，我们命$a+b$ 与它们对应，那末这对应就是 $Z$ 的结合法，它就是普通的加法．同样，对于 $a, b$，我们命 $a\cdot b$ 与它们对应，这对应也是 $Z$ 的结合法，它就是普通的乘法．

一个集，假如它具有适合某些法则的结合法，或代数运算，就叫做**代数系**．象上面所示，整数集 $Z$ 是代数系，因为它 的 加法，乘法两个结合法适合交换律、结合律、分配律等法则．近世代数的目的就是讨论某些基本代数系关于结合法的性质，也就是代数性质．因此可以说，近世代数是研究某些基本代数系的理论学科．