抽象代数

辛未 编

河南大学出版社

抽 象 代 数

辛 未 编

责任编辑 程 庆

河南大学出版社出版
（开封市明伦街85号）
河南省新华书店发行
中国科学院开封印刷厂印刷

开本：850×1168毫米 1/32 印张：7.875 字数：199千字
1988年11月第1版 1988年11月第1次印刷

印数1—3000 定价：1.90元

ISBN7-81018-115-7/O·6

内 容 提 要

本书根据1980年8月原教育部颁发的综合大学数学专业《抽象代数教学大纲》编写，全书共分四章，内容为集合、群、环、域和模。

本书取材适当，条理清晰，讲述细致，适宜于高等院校数学专业近世代数课教材及自学使用。

前　言

1．本书是根据原教育部委托北京大学草拟，1980年5月在上海举行的高等学校理科数学、力学、天文学教材编审委员会扩大会议讨论、修改，并经编委会审订，于1980年8月由原教育部颁发的综合大学数学专业《抽象代数教学大纲》及我系教学实践经验编写的．主要内容为群、环、域和模．

2．考虑到学时有限，大纲中有些内容没有编入．它们是：自然数，数学归纳法；整数，整数的可除性；偏序，Zorn引理介绍以及群论中的共轭类、Sylow子群等．

3．编写时力求做到条理清晰，深入浅出，易读易懂，不因抽象而不得要领．故本书适宜于自学．

4．抽象代数(即近世代数)是学习现代数学的一门基础课程．本书力图使读者可以获得所需的近世代数基础知识与良好的基本训练．

5．每节末都配有精心选择的练习题，这些练习题都是最基本的．其中有些是为了更好地理解、掌握基本知识而设置的，有些则是重要结论(即定理)或反例．因而习题是正文的补充，望读者留心．

6．为了方便教学，书末附有习题解答与提示，供读者查对与参考．既然是提示，当然是"点到为止"．完整的解答应由读者自己完成．希望这些提示不会束缚读者解题的思路，愿读者能找到更好的解法．

7．本书名词采用尽量与大纲一致．第二章中monoid一词在大纲中使用的就是原文，至今尚无统一译名．如需翻译，编者认为叫做"幺半群"较好．

8．师范院校每周4节一学期讲完前三章是绰绰有余的．

9. 本书初稿经姚伯华、高建国二同志审阅，修改稿先后经杨绍忠、高建国、胡长流、王秀琴等同志使用，习题解答与提示部分经杨绍忠同志逐题审订．他们都提出了很好的修改意见．谨此一一致谢．

10. 编者水平有限，书中错误与不当之处，在所难免．真诚希望读者批评指正

编　者

1987 年 5 月

目　录

第一章 集 合

抽象代数以群、环、域、模等代数系统为其基本内容. 它对高等代数中出现的数环、数域、多项式、矩阵、线性空间等概念进一步概括，具有抽象的特点，适宜于培养抽象思维和逻辑推理的能力. 它是学习现代数学的一门必修的基础课程. 它在自然科学的许多部门中都有重要的应用.

所谓代数系统，就是带有运算的集合. 做为全书的序篇，本章简单介绍本书将用到的有关集合的一些基本知识和一些基本概念，主要是集合、映射(包括代数运算)和分类.

§1.1 集合及其运算

所谓集合，就是若干个(有限或无限多个)特定事物(对象)的全体. 我们用大写字母表示集合，如 $A, B, C, \cdots$. 下列集合各有它们的专用符号：

全体自然数组成的集合(自然数集) 记做 $\mathbf{N}$ (本书中所谓自然数，采用较新的提法，就是非负整数：0，1，2，…)；

全体整数组成的集合(整数集)记做 $\mathbf{Z}$；

全体有理数组成的集合(有理数集)记做 $\mathbf{Q}$；

全体实数组成的集合(实数集)记做 $\mathbf{R}$；

全体复数组成的集合(复数集)记做 $\mathbf{C}$.

全体正整数组成的集合 (正整数集) 记做 $\mathbf{Z}^+$. 同样，正有理数集可记做 $\mathbf{Q}^+$ 等等.

组成集合的每个事物(对象)叫做一个元素. 元素用小写字母

表示，如 $a,b,c,\cdots$. 元素 a 是集合 A 的一个元素记做 $a\in A$，读做“a 属于 A”. 元素 a 不是集合 A 的元素时，记做 $a\notin A$，读做“a 不属于 A”.

一个集合说是已知的(或确定的)，应能(且只要求能)判断任一元素属于它或不属于它. 对于集合中的元素，应能区分其异同. 若 a，b 表示同一元素，则记做 $a=b$；若 a，b 表示不同元素，则记做 $a\neq b$. 例如用 A 表示方程 $(x-1)^2=0$ 的全体实根组成的集合，则 A 中只有一个元素 1，除此以外，A 中不含异于 1 的任何元素. 只含一个元素的集合叫做**单元集**.

1.1.1 **定义** 不含任何元素的集合叫做**空集**，记做 $\varnothing$ (读做空集).

例如方程 $x^2+1=0$ 的全体实根的集合就是一个空集.

两个集合 A 与 B 说是**相等**的，当且仅当它们含有相同的元素. 具体说，就是 A 的任一元素都属于 B，B 的任一元素也都属于 A. A 与 B 相等记做 $A=B$，否则，记做 $A\neq B$.

一个集合如果只含有限多个元素，叫做**有限集合**；否则，叫做**无限集合**.

给出一个集合，通常是把它的全部元素放在括号{ }内.“全部元素”可有两种方式来描述. 一是列举每个元素，例如含 n 个元素 a_1，a_2，…，a_n 的集合可记做

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

对于无限集合有时也可采取这种形式，例如

$$\mathbf{N}=\{0,1,2,3,\cdots\},$$

$$\mathbf{Z}=\{0,\pm1,\pm2,\pm3,\cdots\},$$

用…表示未被列出的其余的无穷多个元素，而它们是什么样的元素则应是显而易见的. 二是给出这个集合的元素所具有的性质，其形式为

$$A=\{x\mid\cdots\},$$

表示 A 为由满足条件…的一切元素 x 组成. 例如方程 $(x-1)^2=0$ 的所有实根的集合可记做

$$\{x \mid x\in \mathbf{R},\ (x-1)^2=0\},$$

也可以记做

$$\{x\in \mathbf{R} \mid (x-1)^2=0\}.$$

由集合相等的规定易知

$$\{x\in \mathbf{R} \mid (x-1)^2=0\}=\{1\}.$$

1.1.2 定义 说集合 B 是集合 A 的**子集**，如果 B 的每个元素都属于 A. B 是 A 的子集记做 $B\subseteq A$(读做 B 包含于 A)，也可以记做 $A\supseteq B$ (读做 A 包含 B). B 不是 A 的子集记做 $B\subsetneq A$(或 $A\supsetneq B$). 于是我们有

$$B\subseteq A(\text{或 } A\supseteq B)\Longleftrightarrow(x\in B\Rightarrow x\in A).$$

$$B\subsetneq A(\text{或 } A\supsetneq B)\Longleftrightarrow(\exists\, x\in B\ni x\notin A).$$

由子集定义及集合相等的规定，易知

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

空集被认为是任何集合的子集.

1.1.3 定义 若 $B\subseteq A$ 并且 $B\neq A$，则说 B 是 A 的**真子集**，记做 $B\subsetneq A$.

1.1.4 定义 一个集合 A 的所有子集组成的集合 $P(A)$ 叫做 A 的**幂集**，即

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

例如 $A=\{1,2,3\}$，则 A 的幂集 $P(A)$ 恰含

$$\binom{3}{0}+\binom{3}{1}+\binom{3}{2}+\binom{3}{3}=2^3=8\text{ 个元素(子集)：}$$

$$\varnothing;\{1\},\ \{2\},\ \{3\};\ \{1,2\},\ \{1,3\},\ \{2,3\};$$

$$\{1,2,3\}=A.$$

一般地，如果 $S=\{1,2,\cdots,n\}$ 含 n 个元素，则 S 的幂集 $P(S)$ 中含

$$\binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\cdots+\binom{n}{n}=2^n$$

个元素.

对于任意集合 A，总有 $\varnothing\in P(A)$ 及 $A\in P(A)$.

1.1.5 **定义** 由集合 A 及集合 B 的所有共同元素组成的集合叫做集合 A 与 B 的**交集**(简称**交**)，记做 $A\cap B$，即

$$A\cap B=\{x\mid x\in A\ \wedge\ x\in B\}.$$

显然有

$$A\cap B\subseteq A,\quad A\cap B\subseteq B.$$

1.1.6 **定义** 由一切属于 A 或属于 B 的元素做成的集合叫做集合 A 与 B 的**并集**(简称**并**)，记做 $A\cup B$，即

$$A\cup B=\{x\mid x\in A\ \vee\ x\in B\}.$$

显然有

$$A\cup B\supseteq A,\quad A\cup B\supseteq B.$$

1.1.7 **命题** 集合的交与并适合以下诸律：对于任意集合 A, B, C，有

(1) $A\cap A=A$, $A\cup A=A$, (幂等律)

(2) $A\cap B=B\cap A$, $A\cup B=B\cup A$, (交换律)

(3) $A\cap(B\cap C)=(A\cap B)\cap C$,
$A\cup(B\cup C)=(A\cup B)\cup C$, (结合律)

(4) $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$,
$A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$, (分配律)

(5) $A\cap(A\cup B)=A\cup(A\cap B)=A$, (吸收律)

(6) 若 $A\subseteq C$，则
$A\cup(B\cap C)=(A\cup B)\cap C$, (模律)

(7) $A\cap\varnothing=\varnothing$, $A\cup\varnothing=A$.

证 作为例子，我们证明(4)中第一个等式(交对并的分配律)，其余留作练习.

设 $x\in A\cap(B\cup C)$，则 $x\in A$ 并且 $x\in B\cup C$. 由 $x\in B\cup C$ 知 $x\in B$ 或者 $x\in C$. 再由 $x\in A$ 知

$$x\in A\cap B \quad 或 \quad x\in A\cap C,$$

即

$$x\in(A\cap B)\cup(A\cap C).$$

这就证明了

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

另一方面，若 $y\in(A\cap B)\cup(A\cap C)$，则有

$$y\in A\cap B \quad 或 \quad y\in A\cap C,$$

即 $y\in A$ 并且 $y\in B$，或者 $y\in A$ 并且 $y\in C$，也即 $y\in A$，并且 $y\in B$ 或者 $y\in C$，即

$$y\in A\cap(B\cup C).$$

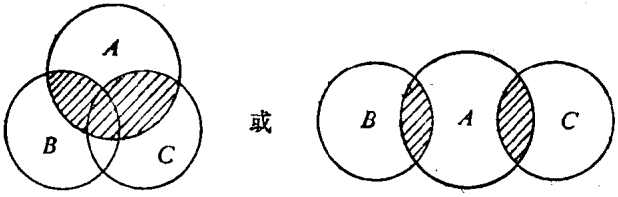
这样又得到

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

由集合相等的规定便有

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

等式两边的集合，可用下图中的阴影部分表示：



若 $A\cap B=\varnothing$，则说 A 与 B **不相交**.

两个集合的交与并的概念也可以推广到任意多个集合上去. 设有一个集合簇 $\{A_i\mid i\in I\}$，可定义这个集合簇的**交为**

$$\bigcap_{i\in I}A\triangleq\{x\mid \forall i\in I,\ x\in A_i\}.$$

当足标集 $I=\{1,2,\cdots,n\}$ 为有限集时，其交可记做 $\bigcap_{i=1}^{n}A_i$.

集合簇 $\{A_i\mid i\in I\}$ 的并定义为

$$\bigcup_{i\in I} A_i \triangleq \{x \mid \exists i \in I \ni x \in A_i\}.$$

当 $I=\{1,2,\cdots,n\}$时，可记 $\bigcup_{i\in I} A_i$ 为 $\bigcup_{i=1}^{n} A_i$.

最后，我们介绍集合的笛卡儿积集(或加氏积)，这是利用给定的一些集合构造新集合常用的方法. 设 A_1, A_2, …, A_n 为给定的 n 个集合，记

$$A_1\times A_2\times\cdots\times A_n \triangleq \{(a_1,a_2,\cdots,a_n) \mid a_i\in A_i,\ i=1,2,\cdots,n\},$$

称集合 $A_1\times A_2\times\cdots\times A_n$ 为集合 $A_1, A_2, \cdots, A_n$ 的**笛卡儿积集(或加氏积)**. 这个集合中两个元素 $(a_1,a_2,\cdots,a_n)$ 与 $(b_1,b_2,\cdots,b_n)$ 说是相等的，当且仅当对每个 $i(i=1,2,\cdots,n)$，$a_i=b_i$ (即对应分支相等). $A_1\times A_2\times\cdots\times A_n$ 也可以记做 $\prod_{i=1}^{n} A_i$.

例如 $\mathbf{R}\times\mathbf{R}=\{(x,y) \mid x\in\mathbf{R},\ y\in\mathbf{R}\}$. 它的每个元素 (x, y) 对应于取定坐标系的平面中的一个点，而集合 $\mathbf{R}\times\mathbf{R}$ 则对应于整个平面.

应该注意，加氏积 $A_1\times A_2\times\cdots\times A_n$ 中元素 $(a_1,a_2,\cdots,a_n)$ 的各个分支 a_i 的排列顺序必须与它们所在集合的顺序一致，即加氏积中每个元素是于集合 $A_1, A_2, \cdots, A_n$ 中各取一个且只取一个元素，按给定集合的顺序排列而成. 例如 $A=\{a_1,a_2\}$, $B=\{b\}$，则 $A\times B$ 中只含两个元素 (a_1,b) 与 (a_2,b)，而 (a_1,a_2), (b,a_1) 等都不是 $A\times B$ 中的元素. 易知若 A 含有 p 个元素，B 含有 q 个元素，则 $A\times B$ 含有 pq 个元素.

习 题 1.1

1. 证明 $A\subseteq B\Longleftrightarrow A\cap B=A\Longleftrightarrow A\cup B=B$.

2. 证明命题 1.1.7 中各律.

3. $A=\{1,2,3,4\}$, $P(A)=$?

4. 若用加氏积 $\mathbf{R}\times\mathbf{R}$ 中元素 (x, y) 表示笛卡儿坐标平面上点 (x, y)，则 $\mathbf{R}\times\mathbf{R}$ 的下列各子集确定的点的集合是平面上什么图形?

(1) $F_1=\{(x,x)\mid x\in\mathbf{R}\}$.

(2) $F_2=\{(x,ax+b)\mid x\in\mathbf{R}\}$, 其中 a,b 为给定的两个实数, $a\neq 0$.

(3) $F_3=\{(x,\sin x)\mid x\in\mathbf{R}\}$.

(4) $F_4=\{(x,y)\mid x\in\mathbf{R},y\in\mathbf{R},x^2+y^2=1\}$.

(5) $F_5=\{(x,y)\mid x,y\in\mathbf{R},x^2+y^2<1\}$.

(6) $F_6=\{(x,y)\mid x,y\in\mathbf{R},|x|\leqslant 1,|y|\leqslant 1\}$.

(7) 若记 $A\backslash B=\{x\mid x\in A,\ x\notin B\}$, 则 $F_1\backslash F_2=$? $F_6\backslash F_5=$? $F_6\backslash(F_5\cup F_4)=$? $F_5\backslash F_6=$?

§1.2 映射 代数运算

映射是现代数学中一个重要的概念, 在我们的课程中起着重要的作用.

1.2.1 **定义** 设 A,B 是给定的两个集合. A 与 B 的元素间的一个对应法则 φ 叫做 A 到 B 的一个**映射**, 如果对于 A 的每个元素 a 按照法则 φ 都有唯一确定的元素 $a'\in B$ 与之对应. 称 a' 为 a 在 φ 下的**象**, 记做 $\varphi(a)$. 称 a 为 a' 的一个**原象**(或**逆象**).

φ 是 A 到 B 的映射, 并且 φ 使 a 对应 a' 时, 常记做

$$\varphi:\ \begin{matrix}A\longrightarrow B\\ a\mapsto a'\end{matrix}\quad\text{或}\quad \begin{matrix}A\xrightarrow{\varphi} B.\\ a\mapsto a'\end{matrix}$$

通过 $a\mapsto a'$ (即 $\varphi(a)=a'$) 来描述具体的对应法则, 当然, 这里的 a 应能表示 A 中的每个元素.

1.2.2 **定义** 两个映射

$$\varphi:\ A\to B,\qquad \psi:\ A'\to B'$$

说是**相等**的(记做 $\varphi=\psi$), 当且仅当 $A=A'$, $B=B'$, 并且对每个 $a\in A$, 均有 $\varphi(a)=\psi(a)$.

例 1 $A=\{a,b,c\}$, $B=\mathbf{Z}^+=\{1,2,3,\cdots\}$, 法则

$$\varphi_1:\ a\mapsto 1,\quad b\mapsto 1,\quad c\mapsto 1,$$

$$\varphi_2:\ a\mapsto 1,\quad b\mapsto 2,\quad c\mapsto 3.$$

都是 A 到 B 的映射. 显然 $\varphi_1\neq\varphi_2$, 因为存在 $b\in A$ 使得 $\varphi_1(b)=1\neq 2=\varphi_2(b)$.

法则 φ_1 可简记成

$$\varphi_1:\ \begin{matrix}A\longrightarrow B\\ x\mapsto 1\end{matrix}$$

意即 $\forall x\in A,\ \varphi_1(x)=1$.

例 2 $A=\mathbf{R}$, $B=\{x\in\mathbf{R}\mid x\geqslant 0\}$, 法则

$$\varphi_1:\ a\mapsto |a|,$$

$$\varphi_2:\ a\mapsto\sqrt{a^2}$$

都是 A 到 B 的映射, 并且 $\varphi_1=\varphi_2$, 因为对于任意实数 a, 总有 $\sqrt{a^2}=|a|$.

例 3 $A=\mathbf{R}$, $B=\mathbf{R}^+$(正实数集), 法则 $\varphi: a\mapsto |a|$ 不是 $\mathbf{R}$ 到 $\mathbf{R}^+$ 的映射, 因为 $|0|=0\notin\mathbf{R}^+$.

例 4 取 $A=B=\mathbf{C}$, 法则 $\varphi: a\mapsto\sqrt{a}$ 不是 $\mathbf{C}$ 到 $\mathbf{C}$ 的映射, 因为当 $a\neq 0$ 时 $\sqrt{a}$ 表示两个不同的数.

例 5 设 S 为任一集合, 法则

$$\mathrm{id}_S: a\mapsto a\quad(\forall a\in S)$$

是 S 到 S 本身的一个映射, 这个映射叫做集合 S 的**恒等映射**(或**单位映射**).

映射有单射与非单射, 满射与非满射之分.

1.2.3 定义 映射 $\varphi: A\to B$ **说是满的**(或叫**满射**), 如果 B 中每个元素都是 A 中某个元素的象, 满射记做 $\varphi: A\twoheadrightarrow B$. 这样,

$$\varphi: A\twoheadrightarrow B\Longleftrightarrow(\forall b\in B,\ \exists a\in A\ni\varphi(a)=b).$$

映射 $\varphi: A\to B$ **说是单的**(或叫**单射**), 如果 A 中不同元素的

象总是 B 中不同的元素. 单射记做 $\varphi: A\rightarrowtail B$. 这样,

$$\varphi: A\rightarrowtail B\Longleftrightarrow(a_1\neq a_2\Rightarrow\varphi(a_1)\neq\varphi(a_2),(\forall a_1,a_2\in A))$$

$$\Longleftrightarrow(\varphi(a_1)=\varphi(a_2)\Rightarrow a_1=a_2.\ (\forall a_1,a_2\in A))$$

映射 $\varphi: A\to B$ 如果既是满的，又是单的，则称之为**双射**(或**满单射、一一映射**)，此时，可用符号 $\varphi: A\leftrightarrow B$ 表示.

前面例 1 中的 φ_1 与 φ_2 都不是满射，φ_1 不是单射而 φ_2 是单射. 例 2 中的 $\varphi_1=\varphi_2$ 是满射，但不是单射，因为 $a\neq 0$ 时有 $\varphi(-a)=\varphi(a)$，而 $-a\neq a$. 例 5 中的 id_A 显然是双射.

设 φ 是 A 到 B 的映射，$S\subseteq A$，记

$$\varphi(S)\triangleq\{\varphi(s)\mid s\in S\},$$

称 $\varphi(S)$ 为 S 在 φ 下的**象**. 显然 $\varphi(S)\subseteq B$. 当 $S=\varnothing$ 时，$\varphi(S)=\varnothing$. 当 $S=A$ 时 $\varphi(S)=\varphi(A)$，特称之为**映射 φ 的象**，记做 $\mathrm{Im}\varphi$:

$$\mathrm{Im}\varphi=\varphi(A).$$

易知，当且仅当 $\mathrm{Im}\varphi=B$ 时，φ 是满射.

任何映射 $\varphi: A\to B$ 都导出一个满射

$$\varphi^+: A\twoheadrightarrow\mathrm{Im}\varphi,\quad a\mapsto\varphi(a)$$

当且仅当 φ 是满射时，$\varphi^+=\varphi$.

反之，若 $T\subseteq B$，记

$$\varphi^{-1}(T)\triangleq\{x\in A\mid\varphi(x)\in T\},$$

则 $\varphi^{-1}(T)$ 是 A 的子集，称之为 T 在 φ 下的**完全原象**. 当 $T=\{t\}$ 为单元集时，记 $\varphi^{-1}(\{t\})$ 为 $\varphi^{-1}(t)$. 显然有

$$\varphi^{-1}(T)=\bigcup_{t\in T}\varphi^{-1}(t).$$

若 φ 为 A 到 B 的映射，称 A 为 φ 的**定义域**，B 为 φ 的**值域**. 以 A 为定义域，B 为值域的映射的全体组成一集合，记做 B^A. 设 $A=\{a_1,a_2,\cdots,a_m\}$，$B=\{b_1,b_2,\cdots,b_n\}$，则 B^A 中共含 n^m 个元素(映射)，因为对于每个 $a_i\in A$，在 B 中取象的方法都