学校教学用书

抽象代数基础

刘云英
蒋滋梅
卢景波
编

北京师范大学出版社

高等学校教学用书

抽象代数基础

刘云英　蒋滋梅　卢景波　编

高等学校教学用书

抽象代数基础

刘云英　蒋滋梅　卢景波　编

北京师范大学出版社出版
新华书店总店科技发行所发行
中国科学院印刷厂印刷

开本：850×1168　1/32　印张：　6.5　字数：　155千
1990年11月第1版　　1990年11月第1次印刷
印数：1——3 000

ISBN7-303-00985-X/O·135
定价：1.60元

编 委 会

出 版 说 明

北京师范大学是一所具有八十多年历史的老学校，在学科建设和教学实践中积累了一定的经验；将它贯彻到教材中去无疑是有益的。为了加强教材建设，加强与兄弟院校的交流，我社约请北京师范大学数学和数学教育研究所所长严士健教授等组成教材编委会，编写研究出版一套教材。编委会在研究当前教学改革的新情况和过去的教学经验的基础上，同时参照原教育部1984年颁发的中学教师进修大纲，对教材的编写宗旨和要求进行认真地讨论。组织数学系有教学经验的教师进行编写，并且由编委等分工负责对书稿进行审订。

这套教材包括数学分析、解析几何、高等代数、概率论与数理统计、常微分方程、复变函数论、抽象代数基础、高等几何，微分几何、实变函数论与泛函分析、计算方法、理论力学以及高等数学(物理、天文、无线电等专业用)。

这套教材文字通俗易懂、内容由浅入深、循序渐进，便于自学，科学系统性较强。每章有小结，每节(或几节)后配有习题。每章有总复习题，习题安排由易而难，层次清楚。书后附有习题答案或提示，以利于读者自学时检查自己的作业。

为了适应不同层次学校和人员的需要，书中有些内容加了"*"号，它相对独立，如因学时较少，可以删去。

这套教材可供高等师范院校本科生(或专科)、教育学院数学系、函授(数学专业)、在职中学教师进修等使用。

编 者 的 话

本书是根据我们在北京师范大学数学系本科和函授讲授近世代数基础(抽象代数基础)时所选内容和体会，并参照有关的抽象代数基础的教学大纲编写的。它可以作为高等师范院校数学系本科生和函授生，以及中学教师进修的教材，也可以作为自学课本。

抽象代数是数学专业的一门重要基础课程，它的内容和方法不仅深入到数学的各个分支，也深入到其它一些学科。学习抽象代数既可以了解这一学科的特点，也有助于培养学生严格的逻辑思维能力。

本书在编写过程中注意到以下几个方面：

1. 考虑到了高等师范院校数学系本科和函授的特点以及对学生的基本要求，因而在材料的取舍上既要照顾抽象代数作为一门学科必须包括它的基本内容，又要照顾学生的实际接受能力。我们选取了群、环、域的最基本的内容和方法，我们认为取材是比较适中的。

2. 抽象代数的一个特点正象它的名称一样是比较抽象的，这给教与学带来一定的困难。基于这一点，本书在内容上力争由浅入深，在概念的引入和定理的证明力求详尽，同时对用到的预备知识不采取一次集中给出的方式，而是分散到各章节，既可避免学这些知识时感到枯燥，又可以立即看到它们的用处，对一些重要概念，书中给出了较多的例题，特别是给出了若干反例，这样一来可以加深对概念的理解，同时可以得到一些实例，这是学习数学知识的一个常用的方法。在每一节后面都附有适量的习题，大部分

是比较容易的，主要借以巩固所学的内容，只有少量习题比较难。

3. 由于高等师范院校的大部分学生将来都要到中学任教，同时从域论的应用考虑，我们介绍了尺规作图问题，以便使学生对尺规作图的适用范围有所了解，也可消除学生对尺规作图的误解，特别是对三等分任意角的误解，

本书共分四章，第一章由卢景波执笔初稿，第二、四章由蒋滋梅执笔，第三章由刘云英执笔。由于我们水平有限，错误是难免的，敬希读者多多指正。

在编写本书过程中得到我们教研室的诸位老师和出版社的编辑同志的大力支持和鼓励，特别是吴品三教授仔细阅读了初稿，提了很多宝贵意见，给予了极大的帮助，仅此致谢。

目　录

抽象代数(近世代数)是一门以研究各种代数系统结构的性质为中心的数学学科。从19世纪20年代至今，它已发展成为整个现代数学科学的主体部分之一。近几十年来，一些代数系统与数学的其它分支相结合产生了新的数学学科，使得抽象代数已经成了现代大部分数学的通用语言。

本书主要介绍抽象代数中典型的代数系统——群、环、域等，介绍它们的基本概念及基本性质。掌握这些内容不仅对于数学工作者和数学教师来说是必要的，而且对于其它专业的科技工作者来说也是有益的。

第一章 群论基础

§1. 代数运算

关于数的运算我们早已熟悉，然而无论从数学理论本身的发展还是从数学在其它学科中的应用来说，仅仅研究数的运算是不够的。在高等代数中，我们曾定义了多项式的加法与乘法运算；矩阵的加法与乘法运算。显然多项式和矩阵不是数，这说明运算不仅可以在数之间进行，而且可以在数以外的其它对象之间进行。下面我们将引进抽象的代数运算的概念，为此需要先简述一下集合及映射等概念。

作为我们讨论问题的起点，集合可以认为是原始(不定义)的

术语；可以认为它是一定事物的集体，组成集合的事物叫做这个集合的元素。我们常用大写拉丁字母 A、B、C … 表示集合；用小写拉字丁母 a、b、c …表示集合里的元素。

设 S 是一个集合，如果 x 是 S 的一个元素，就说 x 属于 S，记作 $x \in S$；或说 S 包含 x，记作 $S \ni x$。如果 x 不是 S 的元素，就说 x 不属于 S，记作 $x \notin S$，或说 S 不包含 x；记作 $S \not\ni x$。

如果集合 S 由所有适合命题 $P(x)$ 的元素构成，我们记作

$$S = \{x|P(x)\}.$$

例如 $S_1 = \{x|x$ 是平面上的点$\}$；

$S_2 = \{x|x$是平面上位于坐标轴上的点$\}$；

$S_3 = \{x|x$ 是实数且 $x^2 = 9\}$；

$S_4 = \{x|x$ 是实数且 $|x| = 3\}$。

如果集合 A 的每个元素都是集合 B 的元素，就说 A 是 B 的一个子集，记作

$$A \subseteq B \text{ 或 } B \supseteq A.$$

设 A、B 是两个集合，如果 $A \subseteq B$ 并且 $B \supseteq A$，即 A 是 B 的子集并且 B 也是 A 的子集，就说 A 与 B 相等，记作

$$A = B.$$

如果集合 A 是集合 B 的子集，并且 $A \neq B$，就说 A 是 B 的真子集，记作

$$A \subsetneqq B.$$

如果集合 A 不是 B 的子集，则记作 $A \not\subseteq B$。

我们用符号 ϕ 表示空集合（不包含任何元素的集合），并且约定 ϕ 是任意集合 A 的子集，即 $\phi \subseteq A$。

在前面的例子中可见：

$$S_2 \subsetneqq S_1,\ S_3 = S_4,\ S_3 \not\subseteq S_2.$$

如果集合 A 的元素个数是一个有限数，就说 A 是一个有

限集。否则，就说 A 是一个无限集。

例如前面的例子中的 S_3 是有限集，而 S_1, S_2 均为无限集。

设 A、B 是两个集合（A 与 B 可以相等）。现在，我们介绍集合 A 与 B 的并、交、差三种运算。

（一）由 A 的所有元素与 B 的所有元素构成的集合叫做集合 A 与 B 的并集，记作 $A \cup B$。即

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

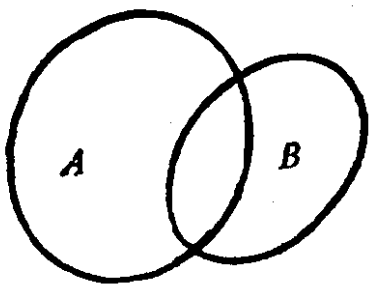
（二）由 A 与 B 的所有公共元素构成的集合叫做集合 A 与 B 的交集，记作 $A \cap B$。即

$$A \cap B = \{x \mid x \in A \text{ 且 } x \in B\}$$

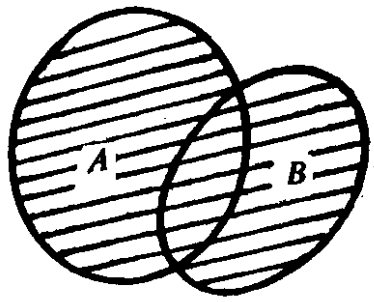
（三）由属于 A 而不属于 B 的所有元素构成的集合叫做集合 A 与 B 的差，记作 $A \setminus B$ 即

$$A \setminus B = \{x \mid x \in A \text{ 且 } x \notin B\}$$

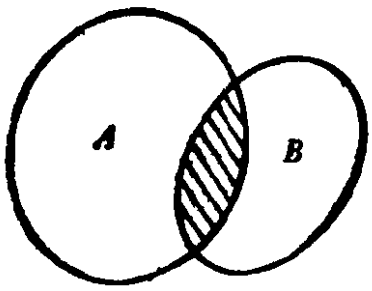
我们可用以下图形来直观示意两集合的并、交、差。



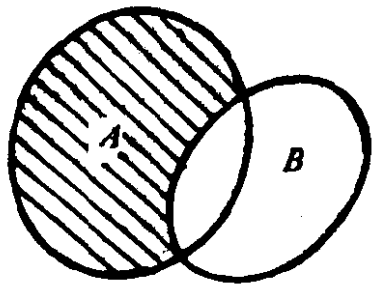
（a）两集合 A 与 B



（b）阴影部分是 $A \cup B$



（c）阴影部分是 $A \cap B$



（d）阴影部分是 $A \setminus B$

例1 设 $A=[-4,4]$，则

$$A\cup A=[-4,4]=A,$$

$$A\cap A=[-4,4]=A,$$

$$A\backslash A=\phi.$$

例2 设 $S=\{a\mid a$ 是整数且 $\sqrt{2}<a<10\}$；

$T=\{b\mid b$是方程 x^2-3x+2的根$\}$则

$$S\cup T=\{1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9\};$$

$$S\cap T=\{2\};$$

$$S\backslash T=\{3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9\};$$

$$T\backslash S=\{1\}.$$

例3 设 $P_1=\{(x,y)\mid x^2+y^2\leqslant 1\}$；

$P_2=\{(x,y)\mid x^2+y^2\geqslant 1\}$，则

$$P_1\cup P_2=\{\text{平面上全体点 }(x,y)\};$$

$$P_1\cap P_2=\{(x,y)\mid x^2+y^2=1\};$$

$$P_1\backslash P_2=\{(x,y)\mid (x,y)\text{ 是圆}x^2+y^2=1\text{ 内的点}\}$$

同样，我们可以定义任意多个集合的交与并。

设 I 是一个非空集合，如果对于 I 的每一个元素 i，对应一个集合 X_i，此时称 I 是足标集合，我们定义

$$\bigcup_{i\in I}X_i=\{x\mid x\in X_i,\ \text{对某个 } i\in I\},$$

$$\bigcap_{i\in I}X_i=\{x\mid x\in X_i,\text{对每个 } i\in I,\}$$

即 $x\in\bigcup_{i\in I}X_i$ 当且仅当存在某个 $i_0\in I$ 使得 $x\in X_{i_0}$ $x\in\bigcap_{i\in I}X_i$ 当且仅当对每个 $i\in I$ 均有 $x\in X_i$。

设 A,B 是两个非空集合（A 与 B 可以相等），集合$\{(a,b)\mid a\in A,b\in B\}$叫做 A 与 B 的卡氏积，记作 $A\times B$。

例如，当 $A=B=$ 实数集 R（全体实数组成的集合），则 $R\times R=\{(a,b)\mid a,\ b\in R\}$，即 $R\times R$ 表示由全体实数对组成的集合或表示坐标平面上所有点 (x,y) 组成的集合。

设 X 和 Y 是两个非空集合（X 与 Y 可以相等），X 到 Y 的一个映射（函数）指的是满足以下条件的法则 f，即对集合 X 的每个元素 x，通过这个法则 f，有集合 Y 的一个唯一确定的元素（记作 $f(x)$）与之对应。

现在定义集合 A 上的代数运算如下：

定义1 设 A 是一个非空集合，则称 $A\times A$ 到 A 的一个映射 f 为集合 A 的一个代数运算。此时也称在 A 上定义了一个代数运算 f.

设 f 是集合 A 上的一个代数运算，那么对任意 a、$b\in A$，都有唯一确定的元素 $c\in A$ 使得 $f(a,b)=c$。为了方便，我们把 $f(a,b)$ 记作 $a\circ b$，读作 a 与 b 的积，于是有 $a\circ b=c$。应该注意，这里的“$\circ$”并不是指普通的数的乘法，因为 a 与 b 是集合 A 的元素，一般来说，它们不一定是数，即使 A 是一个数集时，在 A 上定义的代数运算也未必仅只有乘法。总之，“$\circ$”是代表在 A 上定义的一个代数运算，通过它可以对 A 中任意元素 a、b 算出一个唯一确定的积 $a\circ b$。

例4 设 Z 全体整数的集合。规定

f：$(a,b)\longmapsto a+b$，对任意 $a,b\in Z$

用定义中约定的记法，即

$$a\circ b=a+b.$$

这就是通常的整数加法，也就是说在 Z 上定义了一个加法运算。

例5 设 Z 是全体整数的集合。规定

$$f(a,\ b)=a\circ b=0,\ \text{对任意}\ a,\ b\in Z$$

易见 f 也是 Z 的一个代数运算。

由例4，例5可以看出同一个集合上可以定义不同的代数运算。

例6 设 Q 是全体有理数的集合，规定

$$a\circ b = a+b-ab,\quad \text{对任意 } a,b\in Q.$$

易见"$\circ$"是 Q 的一个代数运算。

设有限集 $A=\{a_1,a_2,\cdots,a_n\}$，则 A 的代数运算"$\circ$"可以用下面的表给出：

$\circ$	a_1	a_2	$\cdots$	a_n
a_1	c_{11}	c_{12}	$\cdots$	c_{1n}
a_2	c_{21}	c_{22}	$\cdots$	c_{2n}
$\vdots$	$\vdots$	$\vdots$		$\vdots$
a_n	c_{n1}	c_{n2}		c_{nn}

这个表的最左面的一列和最上面的一行由 A 的全体元素构成；表的左上角符号"$\circ$"表示集合 A 的代数运算；表中的 c_{ij} ($1\leqslant i\leqslant n$，$1\leqslant j\leqslant n$，$c_{ij}\in A$) 表示 $a_i\circ a_j$。有了这个表我们就很容易计算 A 中任意两个元素的积。例如我们要计算 $a_2\circ a_1$，先在表的最左面一列找到 a_2，再在表的最上面一行找到 a_1，那么元素 a_2 所在第 2 行与元素 a_1 所在的第 1 列交叉位置的元素 c_{21} 就是 $a_2\circ a_1$。又如我们要计算 $a_1\circ a_2$ 先在表的最左面一列找到 a_1，再在表的最上面一行找到 a_2，那么元素 a_1 所在的第 1 行与元素 a_2 所在的第 2 列交叉位置的元素 c_{12} 就是 $a_1\circ a_2$。一般说来 $a_1\circ a_2\neq a_2\circ a_1$。用列表的方法表示有限集的代数运算既方便又简练，以后我们将会看到列表的方法还有其它一些优点。

例 7 设 $A=\{e,a,b,c\}$，A 的代数运算由下表给出：

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

例 8 设 $M=\{0,1,2\}$，M 的代数运算由下表给出：

$\circ$	0	1	2
0	1	2	2
1	1	1	1
2	0	0	0

应该注意，这里的0、1、2是表示集合的元素的符号，并不一定是普通的整数。

设“$\circ$”是非空集合 A 的一个代数运算，$a\circ b\circ c(a,b,\ c\in A)$ 没有意义。因为由代数运算定义知，代数运算只对 A 的两个元素如何进行运算作出规定，当然 $(a\circ b)\circ c$ 及 $a\circ(b\circ c)$ 是有意义的，但一般地。

$$(a\circ b)\circ c\neq a\circ(b\circ c).$$

因此，如果 A 的代数运算“$\circ$”具性质：对于 A 中任意三个元素 a，b，c均有

$$(a\circ b)\circ c = a\circ(b\circ c),$$

那么，我们可以用 $a\circ b\circ c$ 来代表这三个元素按任意不同方式加括号所得的唯一结果，此时称 A 的代数运算适合结合律。

定义2 设“$\circ$”是非空集合 A 的一个代数运算，如果对于 A 中任意元素 a、b、c 都有

$$(a\circ b)\circ c = a\circ(b\circ c),$$

则称 A 的代数运算“$\circ$”适合结合律。

例9 设 A 及 A 的代数运算如例7，证明“$\circ$”适合结合律。

证 任取 $x\in A$，则有 $e\circ x = x\circ e = x$，故取 A 中三个元素 u、v、w，如果其中有一个元素是 e，则必有 $(u\circ v)\circ w = u\circ(v\circ w)$。如果三个元素中有两个相等，设 $u = v$，此时仍有 $(u\circ u)\circ w = u\circ(u\circ w) = w$，或 $(w\circ u)\circ u = w\circ(u\circ u) = w$，或 $(u\circ w)\circ u = u\circ(u\circ w) = u\circ(w\circ u)$。如果三个元素互不相等且都不等于 e，则有 $u\circ(v\circ w) = u\circ u = e$ 且$(u\circ v)\circ w = w\circ w = e$，

综上所述，证得 A 的代数运算“$\circ$”适合结合律。

例10 设 M 及 M 的代数运算如例 8，证明“$\circ$”不适合结合律。

证 由于 $0\circ(1\circ 2)=0\circ 2$，而 $(0\circ 1)\circ 2=2\circ 2=0$，所以 M 的代数运算“$\circ$”不适合结合律。

我们知道，有理数集的减法不适合结合律，全体非零有理数组成的集合的除法也不适合结合律。

设集合 A 上定义的代数运算“$\circ$”适合结合律，a_1，a_2，a_3，$a_4\in A$，此时式子

$$a_1\circ a_2\circ a_3\circ a_4$$

仍没有意义，因为它可以有以下几种加括号的方法

$$[(a_1\circ a_2)\circ a_3]\circ a_4,$$

$$[a_1\circ(a_2\circ a_3)]\circ a_4,$$

$$a_1\circ[(a_2\circ a_3)\circ a_4],$$

$$a_1\circ[a_2\circ(a_3\circ a_4)],$$

$$(a_1\circ a_2)\circ(a_3\circ a_4).$$

但由于“$\circ$”适合结合律，故可以证明上述几个式子所得结果都相等，也就是说上述几种加括号方法所得结果都相等，那么我们可以用 $a_1\circ a_2\circ a_3\circ a_4$ 来代表这四个元素按任意不同方式加括号所得的唯一的结果。一般地，A 的任意 n 个元素 a_1，a_2，…，a_n，进行运算时，其加括号的方法只有有限种，下面将要证明，由“$\circ$”适合结合律，则 A 的 n 个元素按任意不同方式加括号所得结果均相等，为此，我们用符号 $\pi(a_1,a_2,\cdots,a_n)$ 表示 a_1，a_2，…，a_n 的某一种加括号的方法。于是有

定理 1.1.1 设集合 A 的代数运算“$\circ$”（叫做乘法）适合结合律，则对于 A 的任意 $n(n\geqslant 2)$ 个元素 a_1，a_2，…，a_n，其各种加括号方式所得结果由元素 a_1，a_2，…，a_n 及它们的排列次序唯一确定。