华中师范大学出版基金丛书

抽象代数

CHOUXIANG DAISHU

华中师范大学数学系
《抽象代数》编写组 编

华中师范大学出版社

(鄂)新登字 11 号

图书在版编目(CIP)数据

抽象代数/华中师范大学数学系《抽象代数》编写组 编
—武汉:华中师范大学出版社,2000.8
ISBN 7-5622-2252-5/O·129
Ⅰ.抽… Ⅱ.华… Ⅲ.抽象代数 Ⅳ.O.153

中国版本图书馆 CIP 数据核字(2000)第 66759 号

抽象代数

华中师范大学出版社出版发行
(武昌桂子山 邮编:430079)
新华书店湖北发行所经销 华中科技大学印刷厂印刷

责任编辑:彭守权 封面设计:甘 英
责任校对:张 钟 督 印:方汉江

开本:850×1168 1/32 印张:7.5 字数:186 千字
版次:2000 年 8 月第 1 版 2001 年 9 月第 2 次印刷
印数:1 001-4 000 定价:13.00 元

抽 象 代 数

华中师范大学数学系
《抽象代数》编写组 编

华中师范大学出版社
2000 年 · 武汉

内 容 简 介

本书是积作者以及华中师范大学数学系的同行们多年教学和教改经验而写成的，并且在华中师范大学数学系连续试用. 主要内容有：概述、群、环与域、模、格、范畴与函子等六章，各章的每节都配有习题.

本书可以作为高等院校数学系本科生教材，也可供其他专业师生自学参考.

前　　言

抽象代数是近代数学的一个重要分支.它研究各种代数结构以及代数结构之间的联系.无论是知识本身、还是思想方法,抽象代数的基础知识都是一个师范院校数学系学生所必须了解的.抽象代数在通讯、系统工程、计算机科学、物理、化学等方面都有广泛的应用,因此本书也适用于有关专业.

本书是积作者以及华中师范大学数学系的同行们多年教学和教改的经验而写成的.在取材方面,除了着重介绍群、环、域外,增加了模、格和范畴的内容.在每个知识点上,首先概括总结代数结构的精髓,突出不同代数结构的特点,从具体到抽象,然后再回到具体.读者在经过一个从感性到理性再感性的认识过程,不仅获取了知识,而且掌握了抽象代数的思想方法.为了使读者了解抽象代数的应用,我们选编了几个典型的例子作为阅读材料供读者自学参考.

全书共分六章.第一章"概述",讲述抽象代数的基本概念;第二章"群"、第三章"环与域",分别讨论群、环、域的性质;第四章"模"、第五章"格"、第六章"范畴与函子"分别介绍了有关的基本知识.在本书的编写中,我们始终遵循少而精的原则,讲述知识深入浅出、循序渐进.每节配备有一定数量的习题,帮助初学者消化和巩固所学内容.书中有些打"*"号的内容供读者自由选读,以拓宽知识面.本书作为师范院校数学系本科生教材,也可供其他大专院校师生和相关人员参考.

本书的初稿在数学系本科生中连续试用,并多次进行了修改.书中概述、群、格三章由朱德高副教授编写,环与域、模、范畴与函

子三章以及群、环的阅读材料由李桃生教授编写，全书由李桃生教授进行了适当的调整、修改. 本书的编写、试用、修改直至出版都得到了数学系领导的关心和帮助，数学系的同行们都给予了很大的支持. 从拟订编写大纲到取材，他们都提出了许多重要的、有启发性的意见和建议，在此谨向他们表示诚挚的谢意.

由于我们的水平有限，缺点错误在所难免，诚恳地希望读者批评指正.

作　者

1999 年 4 月于

武汉：华中师范大学

目　录

第一章 概 述

本课程主要使学生了解抽象代数中一些最基本的研究对象与方法. 本章主要是介绍一些基本的概念.

§1 代数运算、代数系

一、 卡氏积

首先我们给出卡氏积的概念.

定义 1 设 A,B 是两个非空集合,则称集合

$$A\times B=\{(a,b)\mid a\in A,b\in B\}$$

为 A 与 B 的卡氏积.

类似地,可以定义有限个非空集合的卡氏积

$$A_1\times A_2\times\cdots\times A_n.$$

注意 一般来说 $A\times B$ 不一定等于 $B\times A$.

二、 代数运算、代数系

下面我们利用集合与映射的概念来定义代数运算,先看几个我们熟悉的代数运算.

例 1 设 X 是一个非空集合,X 的所有子集组成的集合记作 $M(X)$,$\forall\ A\in M(X)$,通常称差集 $X-A$ 为 A(在 X 中)的补集,记作 A',那么由 A 求补集 A' 的运算,实际上是 $M(X)$到 $M(X)$的一个映射:

$${}':\quad A\longmapsto A'\qquad\qquad \forall\ A\in M(X).$$

例 2 设 $P^{n\times n}$是数域 P 上的全体 n 阶矩阵组成的集合,$\forall\ A$

$\in P^{n\times n}$,求 A 的行列式 $|A|$ 的代数运算,实际上是 $P^{n\times n}$ 到 P 的一个映射:

$$|\ |:\quad A\mapsto |A| \qquad \forall\ A\in P^{n\times n}.$$

由此我们抽象地给出下面一类代数运算的概念.

定义 2 设 A,B 是两个非空集合,映射 $\sigma:A\to B$ 称为 A 到 B 的代数运算,称 (A,B,σ) 是一个代数系.特别地,当 $A=B$ 时,称 σ 是 A 的一元运算,此时代数系记作 (A,σ).

由定义 2 可知例 1 与例 2 中的 $(M(X),')$ 与 $(P^{n\times n},P,|\ |)$ 都是代数系.例 1 中"$'$"是 $M(X)$ 的一元运算.例 2 中"$|\ |$"是 $P^{n\times n}$ 到 P 的代数运算."$'$"是对 $M(X)$ 的每一个元求补,"$|\ |$"是对 $P^{n\times n}$ 中每一个元求行列式.

进一步我们还可以知道由角 x(弧度数)求 $\sin x$、求 $\cos x$ 都是实数集 $\mathbf{R}$ 的一元运算.即 $(\mathbf{R},\sin)$,$(\mathbf{R},\cos)$ 都是代数系.

下面我们再看几个另外的例子.

例 3 在 $P^{n\times n}$ 中,矩阵的加法与乘法实际上都是 $P^{n\times n}\times P^{n\times n}$ 到 $P^{n\times n}$ 的一个映射:

$$+:\quad (A,B)\mapsto A+B \qquad \forall\ A,B\in P^{n\times n}$$

$$\cdot:\quad (A,B)\mapsto A\cdot B \qquad \forall\ A,B\in P^{n\times n}.$$

而数量乘法实际上是 $P\times P^{n\times n}$ 到 $P^{n\times n}$ 的一个映射:

$$\circ:\quad (k,A)\mapsto kA \qquad \forall\ k\in P,A\in P^{n\times n}.$$

例 4 一般的矩阵乘法可以看作是 $P^{m\times n}\times P^{n\times t}$ 到 $P^{m\times t}$ 的一个映射.

$\forall\ (A_{m\times n},B_{n\times t})\in P^{m\times n}\times P^{n\times t}$.

$$\circ:\quad (A_{m\times n},B_{n\times t})\mapsto A_{m\times n}B_{n\times t},$$

由此我们又给出一类代数运算的概念.

定义 3 设 A,B,C 是三个非空集合.映射

$$\sigma:\quad A\times B\mapsto C$$

称为 $A\times B$ 到 C 的一个代数运算.称 $(A\times B,C,\sigma)$ 是一个代数系.

特别地，当 $B=C$ 时，称 σ 为 A 左乘 B 的代数运算. 当 $A=C$ 时，称 σ 为 B 右乘 A 的代数运算，当 $A=B=C$ 时，称 σ 为 A 的一个二元运算. 此时代数系记作 (A,σ) 或简记作 A.

本书中，代数系 (A,σ) 中的代数运算 σ 通常是 A 的一个二元运算. 此时又称 A 关于代数运算 σ 封闭.

按习惯，$\forall\ a,b\in A$，$\sigma(a,b)$ 记为 ab 或 $a+b$. 否则需加以说明.

若 $\sigma(a,b)=ab$，则称 ab 为 a 与 b 的积.

若 $\sigma(a,b)=a+b$，则称 $a+b$ 为 a 与 b 的和.

由此可知：例 3、例 4 中的集合

$$(P^{n\times n},+),\qquad (P^{n\times n},\cdot),$$
$$(P\times P^{n\times n},P^{n\times n},\cdot),\qquad (P^{m\times n}\times P^{n\times t},P^{m\times t},\cdot)$$

都是代数系.

另外当一个非空集合 A 中定义了多个代数运算时，我们通常将集合 A 连同代数运算一起称为一个代数系. 例如在 $P^{n\times n}$ 中有矩阵加法 $+$，矩阵乘法 $\cdot$，此代数系就记作 $(P^{n\times n},+,\cdot)$，通常称之为(全)矩阵环，可以看到 $(P^{n\times n},+,\cdot)$ 实际上是由两个代数系 $(P^{n\times n},+)$ 与 $(P^{n\times n},\cdot)$ 组合而成，并且"$+$"与"$\cdot$"具有一定联系(例如"$\cdot$"对"$+$"的分配律).

三、 运算表

有限集的代数运算常用一个表来表示.

例 5 设 $A=\{a_1,a_2\}$，"$\cdot$"是 A 的乘法运算，则运算表如下：

$\cdot$	a_1	a_2
a_1	a_1a_1	a_1a_2
a_2	a_2a_1	a_2a_2

注意 如果表中横线以下，竖线以右的元全部都在 A 中，则 A 关于 $\cdot$ 封闭. 即 $(A,\cdot)$ 是一个代数系. 这里 a_ia_j 表示 a_i、a_j 相乘

后所得的结果．若 a_ia_j 等于元素 a_1 或 a_2 时，$(A,\cdot)$是代数系．

四、 基本运算律

1. 结合律

定义 4 设$(A,\cdot)$是一个代数系，如果

$$(ab)c=a(bc), \qquad \forall\, a,b,c\in A$$

则称二元运算"·"是结合的或称二元运算"·"满足结合律.

$(A,\cdot)$是由 n 个元素组成的代数系，要验证乘法"·"是否满足结合律，必须验证 n^3 个等式成立. 这是一件很困难的事. 但是只要有了结合律，A 中任意 m 个元相乘 $a_1a_2\cdots a_m$ 就有意义. 这里需约定

$$a_1a_2\cdots a_m=(a_1\cdots a_{m-1})a_m,$$

也就是

定理 1 如果 $(A,\cdot)$ 的乘法满足结合律，那么，$\forall\, a_1, a_2, \cdots, a_m\in A$ $(m>2)$，给 $a_1a_2\cdots a_m$ 任意添括号得出的结果都等于 $(a_1a_2\cdots a_{m-1})a_m$.

这个定理可用数学归纳法证明.

2. 交换律

定义 5 设$(A,\cdot)$是一个代数系，如果 $a,b\in A$，有

$$a\cdot b=b\cdot a$$

则称 a,b 是可交换的. 若对 A 中任意两个元都可交换，则称代数运算"·"满足交换律.

事实上，数域中的加法与乘法运算都满足结合律与交换律. 而减法与非零数间的除法都不满足结合律与交换律. $P^{n\times n}$中矩阵乘法满足结合律但不满足交换律.

在实数集 $\mathbf{R}$ 中由 $\mathbf{R}\times\mathbf{R}$ 到 $\mathbf{R}$ 的映射

$$(a,b)\longmapsto|a-b|$$

定义了一个满足交换律但不满足结合律的二元运算.

有限集的二元运算是否满足交换律，可以从运算表看出来，如

果运算表从左上角到右下角的对角线称为主对角线,则二元运算满足交换律的充要条件是运算表关于主对角线对称.

定理 2 如果$(A,\cdot)$的乘法满足结合律与交换律,$\forall\, a_1,a_2,\cdots,a_n\in A$,令$i_1,i_2,\cdots,i_n$是$1,2,\cdots,n$的一个排列,则

$$a_{i_1}a_{i_2}\cdots a_{i_n}=a_1a_2\cdots a_n.$$

读者可用数学归纳法证明.

3. 分配律

定义 6 设$(A,+,\circ)$是一个代数系.如果

$$a\cdot(b+c)=(a\cdot b)+(a\cdot c)\qquad \forall\, a,b,c\in A,$$

则称“$\cdot$”对“$+$”满足左分配律.如果

$$(b+c)\cdot a=(b\cdot a)+(c\cdot a)\qquad \forall\, a,b,c\in A,$$

则称“$\cdot$”对“$+$”满足右分配律.如果左、右分配律均满足,则称为满足分配律.

由于这里没有约定先乘除后加减,因此先进行的运算必须用括号括起来.

这种例子有$(P^{n\times n},+,\cdot)$,$(\mathbf{Z},+,\cdot)$,其中$\mathbf{Z}$是整数集合.

读者仍然可以用数学归纳法证明.

定理 3 设$(A,+,\cdot)$是代数系,“$+$”满足结合律,“$\cdot$”对“$+$”满足左分配律,则$\forall\, a,b_1,\cdots,b_n\in A$,有

$$a\cdot(b_1+b_2+\cdots+b_n)=ab_1+ab_2+\cdots+ab_n.$$

关于右分配律;也有相类似的结论.

五、 半群、子半群与幂

定义 7 设$(A,\cdot)$是一个代数系.如果“$\cdot$”满足结合律,则称$(A,\cdot)$是一个半群.如果又满足交换律则称之为交换半群.否则称之为非交换半群.

由定义可知$(\mathbf{Z},+)$,$(\mathbf{Z},\cdot)$,$(\mathbf{Q},+)$,$(\mathbf{Q},\cdot)$,$(\mathbf{Q}^*,\cdot)$,$(\mathbf{R},+)$,$(\mathbf{R},\cdot)$,$(P^{n\times n},+)$等都是交换半群.$(P^{n\times n},\cdot)$是非交

换半群. 这里 $\mathbf{Q}$ 是有理数集合,$\mathbf{R}$ 是实数集合,$\mathbf{Q}^* = \mathbf{Q} - \{0\}$.

在半群$(A, \cdot)$中,$\forall\ n \in \mathbf{N}$($\mathbf{N}$ 是自然数集合),定义

$$a^1 = a, a^{n+1} = a^n \cdot a. \qquad \forall\ a \in A,$$

则 a^n 称为 a 的 n 次幂.

显然

$$a^m a^n = a^{m+n}, (a^m)^n = a^{mn}, \quad \forall\ a \in A, \quad m, n \in \mathbf{N}$$

注意 在一般情况下,$(ab)^n \neq a^n b^n$. 只有当 $ab = ba$ 时,才有 $(ab)^n = a^n b^n$, ($\forall\ n \in \mathbf{N}$).

如果将交换半群改写为$(A, +)$,类似定义倍数

$$1 \cdot a = a, (n+1)a = na + a, \qquad \forall\ a \in A,$$

且有

$$ma + na = (n+m)a,$$

$$m(na) = (mn)a, \qquad \forall\ a \in A, m, n \in \mathbf{N},$$

又因为 $a + b = b + a$,则

$$n(a+b) = na + nb, \qquad \forall\ n \in \mathbf{N}.$$

在研究代数系时,往往从内部进行探讨,因此给出子系、子半群的概念.

定义 8 设$(A, \circ)$是一个代数系(或半群). A 的一个非空子集 B 关于 A 的运算也是一个代数系(或半群),则称 B 是 A 的子系(或子半群).

例如:$(\mathbf{Z}, +)$ 是 $(\mathbf{Q}, +)$ 的子系(也是子半群). $(\mathbf{Z}, +)$还是$(\mathbf{R}, +)$的子系(子半群).

由于代数系与其子系的代数运算相同,因此子系(或子半群)具有反身性与传递性. 即

(1) 代数系(半群)$(A, \cdot)$是其自身的子系(或子半群).

(2) 若 B 是 A 的子系(或子半群),C 是 B 的子系(或子半群),则 C 是 A 的子系(或子半群).

下面给出子半群的判定定理.

定理 4 A 是半群，则 B 是 A 的子半群的充要条件是：B 是 A 的子系.

证 “$\Rightarrow$” 显然.

“$\Leftarrow$” 设 B 是 A 的子系，则 B 关于 A 的代数运算成一个代数系. 又 $\forall\ b_1, b_2, b_3 \in B$，因为 $B \subseteq A$，所以 $b_1, b_2, b_3 \in A$，由 A 是半群，代数运算满足结合律，$b_1(b_2b_3) = (b_1b_2)b_3$，即 B 的代数运算也满足结合律. 因此 B 关于 A 的代数运算成一个半群，得 B 是 A 的子半群.

定义 9 $(A, \cdot)$ 是半群. 如果有 $e \in A$，使得对任意 $a \in A$，恒有 $ea = ae = a$，则称 e 是 A 的单位元又称幺元. $(A, \cdot)$ 就称为含幺半群. 如果 A 又有交换律，则称 A 为交换幺半群，对于交换幺半群，有时把二元运算记作加法. 此时幺元素记作 0，即称零元素. 含幺半群中，单位元唯一.（读者自证）.

例如 $(\mathbf{R}, \cdot)$ 与 $(\mathbf{Z}, \cdot)$ 都是含幺半群，其幺元都是 1. $(\mathbf{R}, +)$ 与 $(\mathbf{Z}, +)$ 也都是含幺半群，其幺元称为零元是 0. 这里“$+$”、“$\cdot$”是普通数的加法与乘法.

定义 10 $(A, \cdot)$ 是幺半群. e 是单位元，$a \in A$，如果有 $b \in A$，使得 $ab = ba = e$，则称 b 是 a 的逆元（当乘法改为加法时，b 称为 a 的负元）.

在 $(\mathbf{R}, \cdot)$ 中所有非零元都有逆元，0 无逆元. 而 $(\mathbf{Z}, +)$ 中所有元都有逆元，n 的逆元是 $-n$.

定理 5 幺半群 $(A, \cdot)$ 中的元 a 有逆元，则逆元唯一.

证 设 b_1, b_2 都是 a 的逆元，e 是单位元，则

$$b_1a = ab_1 = e,\ b_2a = ab_2 = e$$

所以

$$b_1 = b_1e = b_1(ab_2) = (b_1a)b_2 = eb_2 = b_2.$$

由于 a 的逆元唯一，通常将 a 的逆元记作 a^{-1}（a 的负元记作 $-a$）. 且有 $(a^{-1})^{-1} = a$. 即 a 与 a^{-1} 互为逆元.

如果 a,b 都可逆，则 ab 也可逆，且 $(ab)^{-1}=b^{-1}a^{-1}$.

这是因为

$$(ab)(b^{-1}a^{-1})=a(bb^{-1})a^{-1}=(ae)a^{-1}=aa^{-1}=e.$$

类似可证 $(b^{-1}a^{-1})(ab)=e$.

所以

$$(ab)^{-1}=b^{-1}a^{-1}.$$

习题 1.1

1. 证明定理 1.

2. 证明定理 2.

3. 设 A 由 m 个元素组成，在 A 中可以定义多少个 A 的二元运算？

4. 下列法则是不是有理数集 **Q** 的代数运算？如果是代数运算，它是否满足结合律？

1) $a\circ b=\dfrac{a+b}{2}$;

2) $a\circ b=a+2b$;

3) $a\circ b=10^{a+b}$;

4) $a\circ b=ab+1$;

5) $a\circ b=a-b$;

6) $a\circ b=\dfrac{ab}{2}$.

5. 自然数集 **N** 与正偶数集 2**N**，对于数的加法成半群，且 2**N** 是 **N** 的子半群.

6. 在 **Z** 中定义二元运算“$\circ$”为

$$a\circ b=a+b-ab \qquad \forall\, a,b\in \mathbf{Z},$$

则

1) **Z** 是关于“$\circ$”的一个幺半群；

2) 求 $(\mathbf{Z},\circ)$ 的幺元；

3) $2,5,-1$ 在 $(\mathbf{Z},\circ)$ 中是否可逆？可逆时，求其逆元.

7. 在幺半群 **A** 中，单位元唯一.

§2 关系、等价关系与同余关系

一、 关系、等价关系与分类

1. 关系

为了介绍关系与等价关系,先看一下我们熟悉的例子.

$\forall A,B\in P^{n\times n}$,如果 A 与 B 相似,即 $A\sim B$,我们称 A 与 B 有相似关系.如果 A 与 B 不相似,则称 A 与 B 没有相似关系,将所有有相似关系的 A,B 作成有序元素对 (A,B),这些有序元素对作成一个集合

$$\sim=\{(A,B)\mid A,B\in P^{n\times n},A\sim B\}.$$

则 $P^{n\times n}$ 的相似关系 $\sim$ 可以用 $P^{n\times n}\times P^{n\times n}$ 的一个子集 $\sim$ 来刻画.

由此我们给出关系的一般定义.

定义 1 集合 $A\times A$ 的一个子集 R,称为 A 的一个关系.$\forall a,b\in A$,若 $(a,b)\in R$,则称 a 与 b 有关系 R,记作 aRb.若 $(a,b)\notin R$,则称 a 与 b 无关系 R.记作 $a\overline{R}b$.

由定义 1 知在 $P^{n\times n}$ 中,矩阵的相似是 $P^{n\times n}$ 的一个关系.矩阵的合同也是 $P^{n\times n}$ 的一个关系 R:

$$R=\{(A,B)\mid A,B\in P^{n\times n},\exists\text{ 可逆矩阵 }C\in P^{n\times n},\text{使 }C'AC=B\}.$$

例 1 $R=\{(a,b)\mid a,b\in \mathbf{Z},a>b\}$ 是整数集 $\mathbf{Z}$ 的大于关系,具体写出来就是

$$R=\{(n,n-i)\mid n\in\mathbf{Z},i\in\mathbf{N}\}.$$

即 $\forall n\in\mathbf{Z},i\in\mathbf{N}$,恒有 $nR(n-i)$,将 R 记作 $>$,即 $n>n-i$.

2. 等价关系

定义 2 集合 A 的关系 R 若满足下列条件

1) 反身性: $aRa,\forall a\in A$;

2) 对称性: 若 aRb,则 $bRa,\forall a,b\in A$;

3) 传递性: 若 aRb,bRc,则 $aRc,\forall a,b,c\in A$,