高等学校教材

近世代数初步

石生明

高等教育出版社

图书在版编目（CIP）数据

近世代数初步/石生明. —北京：高等教育出版社，2002.6
师范本专科教材
ISBN 7—04—010828—3

Ⅰ.近… Ⅱ.石… Ⅲ.抽象代数—师范大学—教材 Ⅳ.0153

中国版本图书馆CIP数据核字（2002）第037570号

责任编辑 胡乃冏　**封面设计** 柯　鲁　**责任绘图** 李　杰
版式设计 李　杰　**责任校对** 李　杰　**责任印制** 张小强

近世代数初步
石生明

出版发行 高等教育出版社　**购书热线** 010—64054588
社　　址 北京市东城区沙滩后街55号　**免费咨询** 800—810—0598
邮政编码 100009　**网　　址** http://www.hep.edu.cn
传　　真 010—64014048　http://www.hep.com.cn

经　　销 新华书店北京发行所
排　　版 高等教育出版社照排中心
印　　刷 北京市鑫鑫印刷厂

开　　本 787×960　1/16　**版　　次** 2002年7月第1版
印　　张 9.5　**印　　次** 2002年7月第1次印刷
字　　数 150 000　**定　　价** 11.60元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换。

序　言

历来大学数学系近世代数教材主要介绍群、环、域等对象. 书的体系纯粹是介绍数学的逻辑体系,学生不接触背景来源、数学意义及应用情况. 多数学生学完后又没有后续课程来运用这些知识,结果只剩下一些抽象名词,无法用,无处用. 不少学生将基本内容都忘记了.

另一方面由于近代物理、计算机及信息技术的发展,代数基础课中过去没有的一些知识正在受到重视. 例如群论对结晶学和某些组合计算、有限域对编码和密码技术、群表示论对理论物理等的应用等. 但现有的主要近世代数教材几十年来基本内容未变.

再有,现有教材中许多内容的讲法也可以改变,使之更宜于教学.

编者感到以上问题是近世代数教材,特别是大学近世代数的入门教材中必须解决的问题. 在多年的教学实践中编者不断思考这些问题,并坚持内容革新,还将一些革新的想法写成部分讲义在学生中试用. 也向一些同事,同行介绍了这些想法. 学生和同行的反映较好. 这使我增强了改革的信心,并写出这本新教材.

本教材主要给大学教学系,特别是为高等师范院校数学系教学用,也可作为其它理工科大学有关专业师生的参考书.

编者的目标是通过本教材的学习使学生在近世代数的基本概念及其数学意义,初步内容(与传统教材选择的内容相比有不少是不相同了),初等的(但是典型的)应用,以及与其它课程的联系上达到一定的基础. 编者认为这些内容是大学数学系学生在近世代数方面的基本素质要求.

下面介绍各部分内容安排的一些考虑. 本书的核心部分是前三章. (1)引论章. 把引言列为一章是为了强调它的重要性. §1 中讲清代数的研究对象是代数运算系统,为什么要把一些对象组织成运算系统,运算起什么作用. 这个思想要贯穿全教材的各部分内容中. 学生们从各个内容(数学本身的及应用的内容)中弄清和体会了这个思想,在学完近世代数后就不会只剩下群、环、域这几个名词,肯定比纯粹学习抽象系统要留下更多的东西. (2)第一章群论. 以系统的对称性为例引入群的概念,以群在集合上的作用为主线讲述群的各项性质(例如用轨道的概念引出陪集和共轭类,并得出 Lagrange 定理)和应用(一类组合计算),并联系高等代数中的矩阵变换和几何学中 Klein 的 Erlangen 纲领. (3)第二章域与环. 以域扩张为主线讲述域的概念与一般单纯扩域的构造,

用扩域的概念和性质论证了古希腊三大几何作图难题的不可能性.环的概念围绕域扩张展开,讲剩余类域(用以构造有限域或添加多项式的一个根的单扩域),讲整环的分式域.

我们认为这部分是让学生深刻理解代数学的基本概念和基本思想,体现了学生在近世代数方面的基本素质的需要.前面提到的改革思想在这部分体现突出,这部分内容的讲法与以往教材已有很大差别.

下面两章是稍为深入的内容.(4)第三章有限域.讲述有限域及有限域上多项式理论和对周期序列的应用.在计算机和信息技术中这部分内容必不可少,且越见重要.(5)第四章唯一因式分解环和中国剩余定理.前者是以往教材中的重要部分.我们主要讲了有因式分解唯一性的环的几个典型例子.后者是环论对数论中同余方程组的应用,并与中国古代在代数学的成就联系在一起的.过去国内教材中很少提及,而外国教材中却多处讲述,我们把它收入教材之中.

上面的内容可作为每周四学时的一个学期的教材.如果只有每周三学时,可考虑删掉最后一部分的内容.

作为近世代数教材的改革,编者的上述安排实际是提出一个新的教学方案.它与以往教材虽然有很大差别,但仍然能包含以往教材,特别是师范院校教材(如张禾瑞著《近世代数基础》,高等教育出版社,1978 年修订本)的基本内容(除去域论中的分裂域,可离扩域部分).从这个方面看,它是过去教材的一种发展,并且是互相相容的.另一方面,它作为新的教改方案,只有经过广泛使用之后才能证明是否能用.即使能用,也只有在广泛使用中才能发现缺陷,并加以完善.

欢迎大家试用这个教材,欢迎大家提出批评建议.

石生明
于首都师范大学
2002 年 1 月

目　录

说明 本书中定义、定理、例子等在各章节中是分别编号的.引用时,比如引用第一章§4 命题1,在本节中就说是命题1,在第一章其它节就是§4 命题1,在其它章中则是第一章§4 命题1.

引　论　章

§1　本课程的研究对象

本课程叫近世代数初步，近世代数也常称作抽象代数．抽象代数研究各种代数运算系统的运算性质，并用来解决代数学、其它数学、其它科学以及工程技术中的问题．本课程是介绍抽象代数中三个基本的代数运算系统：域、环、群，介绍它们的运算性质及一些应用．为了初步了解为什么要研究各种代数运算系统的运算性质，我们从下面的例子开始．

例 1　购买了三个苹果共用去 15 元，问平均每个苹果几元？

解　用乘法口诀可知，平均每个 5 元．

例 2　求解下列方程

$$ax = b, \tag{1}$$

其中 a, b 为已知数，x 为未知数．

解　若 $a \neq 0$，用 a^{-1} 乘(1) 的两端，得

$$\text{左边} = a^{-1}(ax) = (a^{-1}a)x = 1 \cdot x = x,$$

$$\text{右边} = a^{-1}b.$$

故　$x = a^{-1}b$.

若 $a = 0$，则不管 x 为何值，(1) 的左边 $= 0$．这时分两种情形：

(i) $b \neq 0$，则不管 x 为何值，(1) 的两边不相等．故(1) 无解．

(ii) $b = 0$，则不管 x 为何值，皆能使(1) 的两边相等．即 x 取任何值皆为 (1) 的解．

例 2 是一个典型的代数问题，从中可以看出两个特点(特别是与例 1 的算术问题相比较)：(1) 代数中是要对一类问题(不只是单个问题) 用统一的方法求得所有可能的解答；(2) 求解代数问题主要是利用数的运算性质．这些特点有普遍性．一般地说，代数问题的特点是对一类问题利用统一的运算性质求出所有可能的解答．

上面谈到了运算性质在解决代数问题中的重要性．在中小学的数学课中，我们一直就是在学习各种运算性质的．开始学整数的加法、乘法，然后是减法，后来是分数的加减乘除，以后是根式、指数的运算，再后来是各种代数式的运算，靠它们的运算性质解决各种问题．这时的代数问题有几何和物理中提出来

的问题，如简单的多项式求根，线性方程组求解等. 到大学高等代数中要研究一般的多项式求根和线性方程组求解的理论. 除了数字运算外，运算对象也不断地扩充，加入了几何向量、多项式、n 元向量、矩阵、一般的线性空间中的向量和线性变换等. 高等代数就是介绍这些对象的运算性质并用以解决各种问题. 从中可以看出代数的发展引起了代数运算系统的扩充和深入研究. 在解决代数问题的过程中，人们常常主动地把与此问题有关的对象（某个有特定关系的集合）组织成一个可运算的系统，研究它的运算性质，并用以解决问题. 我们可以举几个更深刻的例子. (1) 人们为解决 $x^2 + 1 = 0$ 在实数域 $\mathbb{R}$ 中无根的问题，而取实数域 $\mathbb{R}$ 上的二维向量空间，在其上规定了一个加法，一个乘法，可证明它有着与 $\mathbb{R}$ 相同的加减乘除的运算性质（加法和乘法的交换律，结合律，分配律等），并且 $x^2 + 1 = 0$ 在其中有根. 这就是复数域*（注意：复数域是人们构造出来或发现的运算系统）. (2) 在现代通讯中，复杂的信息都是由多个电信号实现. 一般电信号有两个状态："有"、"无"，为了解决信息传输中的纠错和保密等问题，人们要对信息作数学处理. 其手段是把信号的"有"、"无"两个状态看成一个集合，在其上自然地引入加法和乘法运算，它也有着与实数域、复数域"相同"的运算性质，成为一个二元（二个元素）域. 利用它的运算性质就可在信息上进行各种处理**. (3) 更为突出的例子是在研究用根式解多项式方程的问题中，法国天才数学家 Galois 把全体 n 元置换（某个 n 元集合上的一一对应）的集合在变换的乘法下组织成一个代数运算系统"n 元对称群"，利用它的运算性质解决了问题. 他在研究中还引入了许多其它的抽象概念，如子群、正规子群、可解群、域、子域、扩域、分裂域、同构、自同构群等，开创了抽象代数的研究.

随着代数学的发展，就像上面例子中的情况一样，引入了许多运算系统，开始是单个地，独立地研究各个具体的运算系统. 逐渐地发现，很多运算系统有相同的运算性质. 我们可以抽象出来进行讨论. 抽象地讨论而得的结果适用于各个具体的运算系统. 这种抽象出共同本质后进行统一处理的方法是事半功倍的，因而是代数学研究以及数学研究中最常用的手段. 代数学中抽象的代数运算系统也是很多的，但最基本的，最重要的就是域、环、群.

§2 域、环、群的定义与简单性质

我们在高等代数中学习抽象线性空间的定义时，其方式是给定一个非空的集合 V 和一个数域 F，在 V 上有一个加法运算，在 F 的元素和 V 的元素之

* 第 2 章 §1 例 3.
** 第 2 章 §1 例 4.

间有一个数量乘积，又满足必要的一些性质，就称 V 是 F 上的线性空间. 抽象的代数运算系统的定义方式也是如此. 给定一个抽象的集合，在其中定义一些运算，满足一些运算法则. 这些称为公理，一组公理就定义一种**代数运算系统**，然后在这些公理的基础上来研究代数运算系统的运算性质.

定义和研究代数运算系统离不开集合及映射的概念和性质，这在很多高等代数教材中都有讲述(例如可参考张禾瑞、郝炳新编《高等代数》(第四版)，高等教育出版社，1998 年). 关于集合上的代数运算，我们见过数的加法、乘法；多项式的加法、乘法；矩阵的乘法；变换的乘法 …，把它们的共同点概括起来：集合 A 上的代数运算是一个对应法则，对于 A 中的任意一对元素 a,b，按这个法则都有 A 中唯一一个元素 c 与其对应，再抽象一步就是

定义 1 A 是一个非空集合，**集合积** $A\times A=\{(a,b)\mid a,b\in A\}$ 到 A 的一个映射就称为 A 的一个**代数运算**. 也常称为 A 的一个**二元运算**，或简称为 A 的一个运算.

下面依次定义域、环、群. 将数域这个代数运算系统直接推广就得

定义 2 设 F 是至少包含两个元素的集合，在 F 中有一个代数运算，称作加法：这就是说，对 F 中任意两个元素 a,b，有 F 中唯一一个元素 c 与之对应，称为 a 与 b 的**和**，并记为 $c=a+b$*. 在 F 中还有另一个代数运算叫做乘法，即对 F 中任意两个元素 a,b，在 F 中都有唯一的一个元素 d 与之对应，称为 a 与 b 的**积**，并记为 $d=ab$. 如果 F 的这两个运算还满足

Ⅰ. 1. 加法交换律 $a+b=b+a,\quad \forall a,b\in F.$

2. 加法结合律 $(a+b)+c=a+(b+c),\quad \forall a,b,c\in F.$

3. F 中有一个**零元素** 0 满足 $a+0=a,\quad \forall a\in F.$

4. 对 F 中任一元素 a，有 F 的元素 b，使得 $a+b=0$，b 称为 a 的一个**负元素**.

Ⅱ. 1. 乘法交换律 $ab=ba,\quad \forall a,b\in F.$

2. 乘法结合律 $(ab)c=a(bc),\quad \forall a,b,c\in F.$

3. F 中有一个**单位元素** 1，满足 $1a=a,\quad \forall a\in F.$

4. 对 F 中任意非零元素 a，有 F 的元素 b，使得 $ab=1$，称 b 为 a 的一个**逆元素**.

Ⅲ. 乘法对加法的分配律 $a(b+c)=ab+ac,\forall a,b,c\in F.$

这时我们称 F 为一个**域**.

把整数环、多项式环、n 阶方阵的运算的共同点抽象出来，就是

定义 3 设 R 是非空集合，在 R 上有两个代数运算，分别称为加法和乘

---

* 这儿的等号表示集合相等，即等号两边的元素相同.

法.如果加法满足定义 2 中 Ⅰ 的全部 4 条性质,Ⅱ 中的性质 2 及 3,而性质 Ⅲ 则改为

Ⅲ′. $a(b+c)=ab+ac$ 及 $(b+c)a=ba+ca$, $\forall a,b,c\in R$.

这时称 R 为一个**环**.

注意:(1) 环中不要求有多于二个元素;(2) 环中乘法不要求满足交换律;(3) 我们的定义中规定环中一定有乘法单位元;(4) 环中即使有乘法单位元,也不一定对每个非零元都有逆元素.

例如,R 由单独一个数 0 组成,在通常数的加法和乘法下就作成一个环,称这个环为**零环**.又如全体 n 阶方阵在方阵的加法和乘法下成为环.它正是注意中所说的情况(2),(4).

域和环是有两个代数运算的运算系统,下面是具有一个代数运算的运算系统.

定义 4 设 G 是非空集合,在 G 上有一个代数运算,叫做乘法,对 G 的任意两个元 a,b,其运算的结果 c 称为 a 与 b 的积,记为 $c=ab$,如果还满足

1. 结合律:$(ab)c=a(bc)$, $\forall a,b,c\in G$.

2. 有**单位元** e,使得 $ea=ae=a$, $\forall a\in G$.

3. 对每个 $a\in G$,有 $b\in G$,使 $ab=ba=e$,b 称为 a 的一个**逆元素**,则称 G 为一个**群**.

当群 G 的运算满足交换律时,称 G 为**交换群**.这时也常把其运算记成加法,并称它是一个加(法)群.注意,加群中零元素相当于乘法群中的单位元素,而负元素相当于乘法群中的逆元素.

下面考察群的一些简单性质,首先设 G 是群,则群 G 中的单位元是唯一的.设 e,及 e' 皆为 G 的单位元,由单位元的定义有

$$e'=ee' \text{ 及 } e=ee',$$

故 $e'=e$,即单位元唯一.

对任意 $a\in G$,a 的逆元素也是唯一的.设 b 及 b' 是 a 的逆元素.由逆元的定义有

$$ba=e, ab'=e.$$

于是 $b'=(ba)b'=b(ab')=b$.即 a 的逆元唯一.

如 G 是加群,就知道 G 的零元素唯一,任一元素的负元素唯一.

对群 G 有下述**消去律**:设 $a,b,c\in G$,若 $ab=ac$ 或 $ba=ca$,则有 $b=c$.实际上用 a^{-1} 乘第一式的两端得 $a^{-1}(ab)=(a^{-1}a)b=eb=b$ 及 $a^{-1}(ac)=(a^{-1}a)c=ec=c$,即有 $b=c$.对第二式同样能得 $b=c$.对加群 G,它有**加法消去律**:$\forall a,b,c\in G$,若 $a+b=a+c$,则 $b=c$.

对域 F,用上面同样的方法可知 F 的零元素、负元素、单位元及逆元素都

有唯一性. 加法有消去律，乘法的消去律则须修改成：设 $a,b,c \in F$，$ab = ac$，若还有 $a \neq 0$，则 $b = c$.

同样对环 R，它的加法零元素、负元素都有唯一性，对于乘法单位元，也有唯一性. R 中有加法消去律. 但没有乘法消去律. 例如 n 阶矩阵中有 A,B 皆为非零的矩阵，但可以有 $AB = 0$，读者自己举出例子. 又显然 $A0 = 0$（这里 0 是零矩阵），于是 $AB = A0$，虽然 $A \neq 0$，但 $B \neq 0$，故乘法消去律不成立.

定义 5 R 是环，$a \in R, a \neq 0$，若有 $b \neq 0$，使 $ab = 0$（或 $ba = 0$），则称 a 是 R 中的一个左（或右）**零因子**.

对于域 F，它是没有零因子的. 实际上若 $a,b \in F, a \neq 0, b \neq 0$，则 $ab \neq 0$. 否则设 $ab = 0, a \neq 0$，由消去律有 $b = 0$，矛盾. 这一事实说明集合 $F^* = F \setminus \{0\}$ 的元素在 F 的乘法运算下仍在 F^* 中（我们说 F^* 在 F 的乘法下是封闭的）(*). 对比一下定义 2 与定义 4，我们就得到

命题 1 F 是域，则 F 对于自身的加法成为一个交换群，而 $F^* = F \setminus \{0\}$ 对于 F 的乘法运算也成为一个交换群.

由此看出群是比域更基本的代数运算系统. 我们进一步用群的概念来描述域的概念：

F 是非空集合，F 上有两个代数运算，一个称为加法，F 对于加法成为交换群；另一个称为乘法，这个乘法限制到 $F^* = F \setminus \{0\}$ 上使 F^* 也成为交换群. 并且在 F 上乘法对于加法满足分配律，则 F 是一个域.

注意以上描述的 F 中，由于 $F^* = F \setminus \{0\}$ 是非空集合，F 至少有两个元素.

对 R 是环时，R 对于自身的加法成为交换群、由于不要求 R 中的元素有逆元素，$R^* = R \setminus \{0\}$ 对乘法不一定成群. 但是可建立下列

定义 6 非空集合 S 上有一个代数运算称为乘法，适合结合律，就称为**半群**. 若此运算有单位元，则称 S 为**幺半群**.

半群与幺半群在数学中是日渐重要的概念，不过本课程中不准备去讨论它们了.

用群和半群可以将环 R 的概念描述成：

R 是非空集合，R 上有两个代数运算. 一个称为加法，R 对于加法成为交换群；另一个称为乘法，对这个乘法，R 成为一个幺半群；并且 R 的乘法对于加法满足定义 3 中 Ⅲ′ 形式的分配律，则 R 是一个环.

域当然是环，域又有单位元素，故域在其乘法下成为幺半群.

---

* 一般地，设一个非空集合 G 上有一代数运算，H 是它的非空子集. 若 G 的运算限制到 H 上是 H 的代数运算，即 H 的任一对元素在 G 的运算下仍是 H 的元素，就称 H 在 G 的**运算下是封闭的**.

对加群、域、环中任意元 a，其负元素唯一，我们以 $-a$ 记 a 的负元素. 对乘法群的任意元 a，或域中非零元 a，其逆元唯一，我们以 a^{-1} 记 a 的逆元. 在加群中和域中可定义减法. 对其中任意两元 a, b. 令 $a - b = a + (-b)$. 对方程 $a + x = b$，这时有唯一解，$x = (-a) + b = b - a$. 对负元素有 $-(-a) = a$. 对乘法群的任意元 a 及域中任意非零元 a，可以去除群中或域中任意元 b，即定义 $b \div a = ba^{-1}$. 方程 $ax = b$ 有唯一解 $x = a^{-1}b$. 逆元素还有性质 $(a^{-1})^{-1} = a$.

域、环、群以及半群中的加法和乘法都满足结合律. 即有性质 $(a + b) + c = a + (b + c)$，$(ab)c = a(bc)$. 若有 n 个元素 $a_1, \cdots, a_n$ 的序列 $(n \geqslant 3)$，对这个序列组合多次二元运算，可作出很多乘积或和. 例 $n = 4$ 时，就有如下的各个可能的积：

$$((a_1a_2)a_3)a_4, (a_1(a_2a_3))a_4,$$
$$(a_1a_2)(a_3a_4), a_1(a_2a_3)a_4, a_1(a_2(a_3a_4)).$$

或和：

$$((a_1 + a_2) + a_3) + a_4, (a_1 + (a_2 + a_3)) + a_4, (a_1 + a_2) + (a_3 + a_4),$$
$$a_1 + (a_2 + a_3) + a_4, a_1 + (a_2 + (a_3 + a_4)).$$

实际上能证明其结果是相同的. 我们用 $a_1 \cdots a_m$ 表示 $((a_1a_2)a_3 \cdots)a_m$，则有下列**广义结合律**：

命题 2 设 S 是一个半群. $a_1, a_2, \cdots, a_n$ 是 S 中 n 个元的一个序列. 对这个序列组合多次乘法运算所得到的乘积是相等的.

证明 设 $\varphi(a_1, a_2, \cdots, a_n)$ 是任意一个这样的积. 我们来证明

$$\varphi(a_1, \cdots, a_n) = a_1a_2 \cdots a_n.$$

我们对 n 作归纳法，$n = 1$，显然成立. 设对任意 $m < n$ 上述结论已经成立. 对 $\varphi(a_1, \cdots, a_n)$ 这个乘积的最后一次乘法一定是对某个 $m < n$，由 $a_1, \cdots, a_m$ 的某个这样的乘积 $\varphi_1(a_1, \cdots, a_m)$ 和 $a_{m+1}, \cdots, a_n$ 的某个这样的乘积 $\varphi_2(a_{m+1}, \cdots, a_n)$ 作乘积，即

$$\varphi(a_1, \cdots, a_n) = \varphi_1(a_1, \cdots, a_m)\varphi_2(a_{m+1}, \cdots, a_n).$$

由归纳假设

$$\varphi_1(a_1, \cdots, a_m) = a_1 \cdots a_m, \varphi_2(a_{m+1}, \cdots, a_n) = a_{m+1} \cdots a_n.$$

如 $m + 1 = n$，则

$$\varphi_1(a_1, \cdots, a_m)\varphi_2(a_{m+1}, \cdots, a_n)$$
$$= (a_1 \cdots a_m)a_n = a_1a_2 \cdots a_n.$$

若 $m + 1 < n$，则

$$\varphi_1(a_1, \cdots, a_m)\varphi_2(a_{m+1}, \cdots, a_n) = (a_1 \cdots a_m)(a_{m+1} \cdots a_n)$$

$$= (a_1\cdots a_m)((a_{m+1}\cdots a_{n-1})a_n)$$
$$\overset{(1)}{=\!=} ((a_1\cdots a_m)(a_{m+1}\cdots a_{n-1}))a_n$$
$$\overset{(2)}{=\!=} (a_1\cdots a_{n-1})a_n = a_1\cdots a_{n-1}a_n.$$

其中等号(1)是由 S 中乘法有结合律，等号(2)是对$(a_1,\cdots,a_m)(a_{m+1},\cdots,a_{n-1})$使用了归纳假设.以上就完成了归纳法.

由命题2就知道域、环、群中的乘法和加法都有广义结合律.

对群 G 中任意一个元素a，及任意一个正整数 n，我们可自然地定义 a 的方幂：

$$a^n = \underbrace{aa\cdots a}_{n个}.$$

我们再定义

$$a^0 = 1, a^{-n} = \underbrace{a^{-1}a^{-1}\cdots a^{-1}}_{n个}.$$

由广义结合律易知对任意整数 m,n 都有性质：

$$a^{m+n} = a^m a^n;$$
$$(a^m)^n = a^{mn};$$
$$(a^m)^{-1} = a^{-m}.$$

对于加法群 G，则方幂就成为倍数.对 $a \in G$，及任意一个正整数 n，可定义

$$na = \underbrace{a + a + \cdots + a}_{n个},$$
$$(-n)a = \underbrace{(-a) + \cdots + (-a)}_{n个},$$
$$0a = 0.$$

同样对任意整数 m,n 都有

$$ma + na = (m+n)a, m(na) = (mn)a, -(ma) = m(-a).$$

对域和环中元素，上面关于倍数的性质都成立.对域中元素，前面关于方幂的性质都成立.对环中元素，没有负方幂，其余关于幂的性质成立.

到现在，我们已经讨论了群、域、环的一些基本的运算性质，以后就可以自由运用这些性质了.特别地对于域，它基本上继承了数域的运算性质.说是“基本上”，是指到现在为止还未发现域中元素的运算性质与数域中元素的运算性质有不同的地方.当然以后我们会讨论到有些域的“特征”是素数，而数域的“特征”是零(见二章 §1 定义1).

小结 在引论这一章中我们做了以下几件事：

(1) 了解了代数运算在解决代数问题中的重要性，在代数学的发展中扩

展了运算对象,作出了许许多多的代数运算系统,这是代数学的研究对象.

(2) 讲了域、环、群的定义,建立了它们的基本的运算性质,零元、单位元、负元、逆元的唯一性,加法和乘法的消去律,广义结合律,方幂和倍数的运算性质等.

(3) 群是一个代数运算的运算系统,用它可描述域、环的概念,域和环的各种运算性质大多是它们的加法群和乘法群的运算性质的反映.群是最基本的运算系统.本课程以后的内容中我们先讲群,后讲域和环.因为域和环的某些性质可以由群的性质推出来.

(4) 正由于一般域 F 和数域的运算性质基本相同,我们自然地提出,一般域 F 上能否有行列式理论、多项式理论、线性方程组理论、矩阵运算及理论、F 上线性空间和线性变换理论以及 F 上二次型理论呢?重复高等代数中的讨论,除了二次型理论而外,其它理论同样成立.我们不去重复写出这些讨论了,而直接写出下面的

定理 设 F 是一个域,则关于数域上的行列式理论、多项式理论(包括除法算式、整除性、最大公因式、因式分解唯一性定理等)、线性方程组理论、矩阵运算及理论、线性空间和线性变换的理论在域 F 上都成立.

实际上,我们构造一些新的域的目的就是为了在新域上应用上面提到的一些理论,在本教材中我们将在任意域中自由地使用上述定理.

注:上述定理中关于多项式的理论,并没提到任意域中必有多项式存在.我们将在第四章 §3 中讲清这个问题.

习 题

1. 判断下列哪些是集合 A 上的代数运算.

(1) A = 所有实数,A 上的除法.

(2) A 是平面上全部向量,用实数和 A 中向量作数量乘法(倍数).

(3) A 是空间全部向量,A 中向量的向量积(或外积,叉乘).

(4) A = 所有实数,A 上的一个二元实函数.

2. 给定集合 $F_2 = \{1,0\}$,定义 F_2 上两个代数运算加法和乘法,用下面的加法表,乘法表来表示:

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

例如,$0+1=1$,在加法表中 + 号下的 0 所在的行与 + 号右边的 1 所在的列相交处的元就是 1;$1\times 0=0$,在乘法表中 × 号下的 1 所在的行与 × 号右边的 0 所在的列相交处的元是 0.

试验证上述加法、乘法都有交换律、结合律,且乘法对于加法有分配律.

3. 设 R 是环. 证明下述性质: $\forall a,b,c\in R$,

(1) $a+b=a$,则 $b=0$,　　(2) $-(a+b)=(-a)-b$,

(3) $-(a-b)=(-a)+b$,　　(4) $a-b=c$,则 $a=c+b$,

(5) $a0=0$,　　(6) $-(ab)=(-a)b=a(-b)$,

(7) $a(b-c)=ab-ac$.

4. R 是环,$a_1,a_2,\cdots,a_m,b_1,b_2,\cdots,b_n\in R$,则

$$\left(\sum_{i=1}^{m}a_i\right)\left(\sum_{j=1}^{n}b_j\right)=\sum_{i=1}^{m}\sum_{j=1}^{n}a_ib_j.$$

5. R 是环,验证:对所有非负整数 m,n,$\forall a,b\in R$,有

$$a^{m+n}=a^ma^n,(a^m)^n=a^{mn}.$$

若 a,b 交换,则 $(ab)^m=a^mb^m$.

6. R 是环,$a,b\in R$,a,b 交换,证明二项定理:

$$(a+b)^n=a^n+\binom{n}{1}a^{n-1}b+\cdots+\binom{n}{k}a^{n-k}b^k+\cdots+b^n,$$

其中

$$\binom{n}{k}=C_k^n=\frac{n(n-1)\cdots(n-k+1)}{1\cdot 2\cdots k}.$$

7. R 是环,$a_1,a_2,\cdots,a_m\in R$,分别有乘法逆元素 $a_1^{-1},\cdots,a_m^{-1}$,则 $a_1\cdots a_m$ 的逆元素为 $a_m^{-1}a_{m-1}^{-1}\cdots a_2^{-1}a_1^{-1}$. 若 $a_1,\cdots,a_m$ 两两交换,则 $a_1a_2\cdots a_m$ 有逆元素的充要条件是 $a_1,\cdots,a_m$ 皆有逆元素.

8. R 是环,$a,b\in R$. 证明

$$c(1-ab)=(1-ab)c=1\Rightarrow(1-ba)d=d(1-ba)=1,$$

其中 $d=1+bca$. 即若 $1-ab$ 在 R 内可逆,则 $1-ba$ 也可逆. 元素 $1+adb$ 等于什么?

8. $M_n(F)$ 为域 F 上全体 $n\times n$ 阵作成的环. 举出其中零因子的例子.

第一章　群

这一章我们介绍群，特别是有限个元素的群的一些基本知识. 群不仅是域、环构造的基础，它还广泛出现在代数学、几何学、组合学以及理论物理学和化学中. 这一章中除了介绍群本身的一些基础知识外，也介绍了群论在以上方面应用的几个简单例子.

§1　群的例子

例 1　全体正实数 $\mathbb{R}^+$ 对于实数的乘法成为一个交换群.

首先正实数的积仍为正实数，故 $\mathbb{R}^+$ 对实数的乘法是封闭的，也即实数的乘法是 $\mathbb{R}^+$ 的代数运算. 其次 $\mathbb{R}^+$ 对乘法满足结合律. 又 $\mathbb{R}^+$ 中 1 是乘法单位元，正实数的逆元素仍为正实数. 故 $\mathbb{R}^+$ 对实数的乘法满足群的定义的全部要求. 实数乘法有交换律，故 $\mathbb{R}^+$ 是交换群.

例 2　令 $U_n = \left\{ \varepsilon_k = e^{k\frac{2\pi}{n}i} \middle| k = 0,1,\cdots,n-1 \right\}$. 这是 n 个复数的集合. 因 $\varepsilon_k^n = 1 = \varepsilon_0$，故 $\varepsilon_0,\cdots,\varepsilon_{n-1}$ 恰是方程 $x^n = 1$ 的 n 个根. 我们称 $\varepsilon_0,\cdots,\varepsilon_{n-1}$ 为 1 的 n 次根或 n **次单位根**.

任意 $(\varepsilon_{k_1}\varepsilon_{k_2})^n = \varepsilon_{k_1}^n\varepsilon_{k_2}^n = 1$，故 $\varepsilon_{k_1}\varepsilon_{k_2} \in U_n$. 即 U_n 对复数的乘法是封闭的. U_n 中 $\varepsilon_0 = 1$ 是乘法单位元. $\varepsilon_0^{-1} = \varepsilon_0$，而 $1 \leqslant k \leqslant n-1$ 时，$\varepsilon_k \cdot \varepsilon_{n-k} = e^{k\frac{2\pi}{n}i}e^{(n-k)\frac{2\pi}{n}i} = e^{(k+(n-k))\frac{2\pi}{n}i} = e^{2\pi i} = 1$. 它们是互逆的，且 $\varepsilon_k, \varepsilon_{n-k} \in U_n$. 故 U_n 中任一元 ε_k 在 U_n 中有逆元. 又 U_n 中乘法满足结合律. 以上说明了 U_n 在复数乘法下成一个群.

例 3　域 F 上全体 $n \times n$ 可逆矩阵对矩阵乘法成为群，记为 $GL_n(F)$，称为 F 上 n 阶**一般线性群**.

又 $GL_n(F)$ 中行列式为 1 的矩阵成为一个群，记为 $SL_n(F)$，称为 F 上 n 阶**特殊线性群**.

例 4　实数域 $\mathbb{R}$ 上 $n \times n$ 正交矩阵的全体对矩阵乘法成为群，记为 $O_n(\mathbb{R})$，称为 n 阶**正交群**.

例 5　非空集合 M 上的变换有自然的乘法. 两个变换 φ, ψ 的乘积 $\varphi\psi$ 表示先作变换 ψ，后作变换 φ 合成而得的变换. M 上全体**一一对应(可逆变换)**

对于变换的乘法成为一个群.称为集合 M 的**全变换群**.记为 S_M.

例 6 设集合 M 有 n 个元素,不妨就用 $1,2,\cdots,n$ 表示这 n 个元素.σ 是 M 上的一个一一对应当且仅当 $\sigma(1),\sigma(2),\cdots,\sigma(n)$ 是 $1,2,\cdots,n$ 的一个排列.$M=\{1,2,\cdots,n\}$ 上的一一对应(或可逆变换)称为 $1,2,\cdots,n$ 的一个**置换**(注意 $1,2,\cdots,n$ 的排列与 $1,2,\cdots,n$ 的置换的不同含义).也称一个 n **元置换**.我们常以其对应关系来表示置换 σ,即写

$$\sigma=\begin{pmatrix}1 & 2 & \cdots & n\\ \sigma(1) & \sigma(2) & \cdots & \sigma(n)\end{pmatrix}.$$

表示中还可打乱各列的次序.当重排 $1,2,\cdots,n$ 为 $l_1,\cdots,l_n$ 时,也写

$$\sigma=\begin{pmatrix}l_1 & l_2 & \cdots & l_n\\ \sigma(l_1) & \sigma(l_2) & \cdots & \sigma(l_n)\end{pmatrix}.$$

例如三元置换 $\sigma:\sigma(1)=2,\sigma(2)=3,\sigma(3)=1$.可写成

$$\sigma=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}=\begin{pmatrix}2 & 3 & 1\\ 3 & 1 & 2\end{pmatrix}.$$

反之,任给 $1,2,\cdots,n$ 的一个排列 $i_1\cdots i_n$.记号

$$\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix}$$

表示一个置换 $\sigma,\sigma(k)=i_k,k=1,2,\cdots,n$.于是上面的记号表出了全部的置换.由于共有 $n!$ 个排列,故共有 $n!$ 个置换.

置换的乘法是变换的乘法,对于两个置换 τ,σ,有 $(\tau\sigma)(i)=\tau(\sigma(i))$.(变换 τ,σ 的积 $\tau\sigma$ 是先进行 σ 再进行 τ 的合成的结果.)例如取

$$\tau=\begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 2 & 4 & 1\end{pmatrix},\quad \sigma=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix}$$

则 $\tau\sigma:1\longrightarrow 2\longrightarrow 2;2\longrightarrow 1\longrightarrow 3;3\longrightarrow 4\longrightarrow 1;4\longrightarrow 3\longrightarrow 4.$

即

$$\tau\sigma=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 1 & 4\end{pmatrix}.$$

由于 $M=\{1,2,\cdots,n\}$ 上的全体一一对应在变换的乘法下成为群,故全体 n 元置换($1,2,\cdots,n$ 的全体置换)在置换的乘法下成为一个群称为 n **元对称群**,记为 S_n.

n 元对称群是群论的重要对象,后面我们还要讨论它.

例 7 域 F 上 n 维线性空间 V 上全体可逆线性变换在变换的乘法下成为群,记为 $GL(V)$.

例 8 (实数域上)n 维欧氏空间 V 中全体正交变换对变换的乘法成为群,记为 $O_n(V)$.