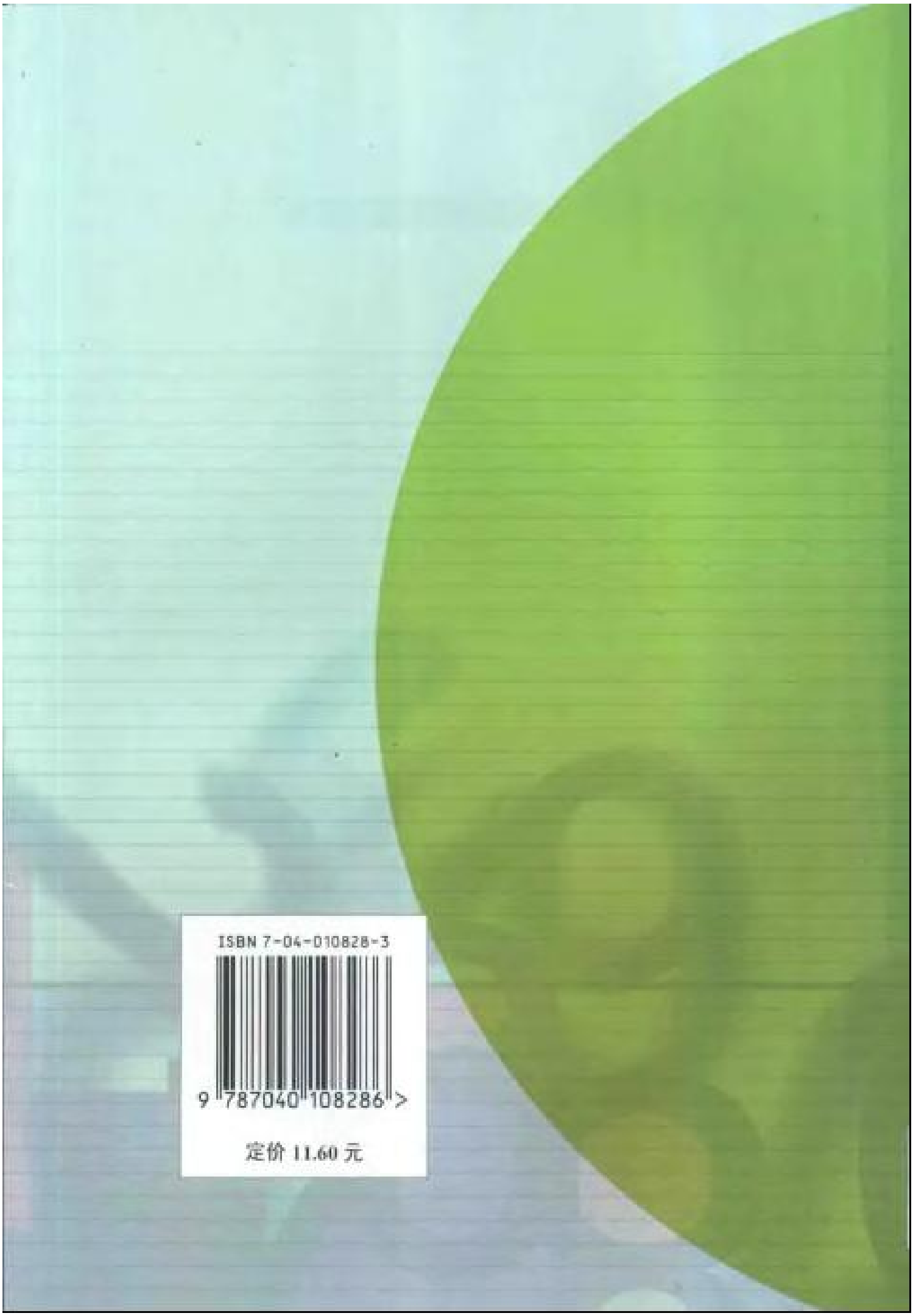
高等学校教材

近世代数初步

石生明

高等教育出版社



ISBN 7-04-010828-3

9 787040 108286 >

定价 11.60 元

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 胡乃冈　**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 $a_1 \cdots a_n$ 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 $U_n = \left\{ \varepsilon_k = e^{k\frac{2\pi}{n}i} \mid k = 0,1,\cdots,n-1 \right\}$. 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 $O_n(V)$.

例 9 平面上绕某定点按同一方向旋转$\frac{2\pi}{n}k$角，$k=0,1,\cdots,n-1$的n个旋转变换的集合在变换的乘法下成为群.

(注意:旋转角为2π的旋转变换把平面上每个点送回原处,即每个点仍保持不动.它与旋转角为0的旋转变换一样都是平面的恒等变换).

例 10 平面(作为点集合)上全体正交变换*在变换的乘法下成为一个群,称为平面的**正交变换群**.同样有空间的正交变换群.

习 题

1. 平面取定坐标系Oxy,则平面仿射(点)变换$\varphi:(x,y)^{\mathrm{T}}\longrightarrow(x',y')^{\mathrm{T}}$(这里T是矩阵的转置,$(x,y)^{\mathrm{T}}$是一列的矩阵,即列向量)可写为

$$\begin{aligned} x' &= a_{11}x + a_{12}y + b_1, \\ y' &= a_{21}x + a_{22}y + b_2, \end{aligned} \tag{1}$$

其中行列式

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \neq 0.$$

证明平面上全体仿射变换对于变换的乘法成一个群,称为平面的**仿射变换群**.(可以把(1)写成矩阵形式,再进行证明).

2. 平面上取定直角坐标系Oxy,则平面正交(点)变换$\varphi:(x,y)^{\mathrm{T}}\longrightarrow(x',y')^{\mathrm{T}}$可写为

$$\begin{aligned} x' &= a_{11}x + a_{12}y + b_1, \\ y' &= a_{21}x + a_{22}y + b_2, \end{aligned}$$

其中矩阵

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

是正交矩阵.证明平面上全体正交变换对于变换的乘法成为一个群,称为平面的正交变换群.

3. 平面上三个(不同的)点$(x_0,y_0)^{\mathrm{T}},(x_1,y_1)^{\mathrm{T}},(x_2,y_2)^{\mathrm{T}}$(在习题1中同一坐标系$Oxy$下)共线当且仅当有实数$l$,使$(x_2-x_0,y_2-y_0)^{\mathrm{T}}=l(x_1-x_0,y_1-y_0)^{\mathrm{T}}$.证明在习题1中的仿射变换$\varphi$下,有$(x'_2-x'_0,y'_2-y'_0)^{\mathrm{T}}=l(x'_1-x'_0,y'_1-y'_0)^{\mathrm{T}}$,故变换后的三点$(x'_0,y'_0),(x'_1,y'_1),(x'_2,y'_2)$也

* 平面上正交变换是保持点之间距离和直线间夹角的变换.

共线.

4. 平面上二点$(x_1,y_1)^{\mathrm{T}},(x_2,y_2)^{\mathrm{T}}$(在习题2中直角坐标系$Oxy$下)的距离为$|x_2-x_1,y_2-y_1|=\sqrt{(x_2-x_1)^2+(y_2-y_1)^2}$.证明:在习题2中的正交变换$\varphi$下,变换前后两点的距离不变.注:只要证明$(x_2-x_1)^2+(y_2-y_1)^2=(x'_2-x'_1)^2+(y'_2-y'_1)^2$.除直接计算外还可利用矩阵工具.实际上

$$\begin{pmatrix}x'_2-x'_1\\y'_2-y'_1\end{pmatrix}=\begin{pmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{pmatrix}\begin{pmatrix}x_2-x_1\\y_2-y_1\end{pmatrix}.$$

又若把一个数看成1×1矩阵,则有

$$\begin{aligned}&(x_2-x_1)^2+(y_2-y_1)^2\\=&(x_2-x_1,y_2-y_1)(x_2-x_1,y_2-y_1)^{\mathrm{T}}\end{aligned}$$

及

$$\begin{aligned}&(x'_2-x'_1)^2+(y'_2-y'_1)^2\\=&(x'_2-x'_1,y'_2-y'_1)(x'_2-x'_1,y'_2-y'_1)^{\mathrm{T}}.\end{aligned}$$

5. 所有形为

$$\begin{pmatrix}a&b\\0&a\end{pmatrix},$$

$a\neq0,a,b$皆为复数,的矩阵对于矩阵的乘法成为一个群.

6. 令G是全部实数对$(a,b),a\neq0$,的集合.在G上定义乘法为$(a,b)(c,d)=(ac,ad+b),e=(1,0)$,验证$G$是一个群.

7. 设G是一个幺半群.若G的每个元a有右逆元,即有$b\in G$,使$ab=e$,则G是一个群.

8. 设G是一个群.若$\forall a,b$皆有$(ab)^2=a^2b^2$,则G是交换群.

9. 设群G的每个元素a都满足$a^2=e$,则G是交换群.

10. $G=\{z\in\mathbb{C}(\text{复数域})\mid|z|=1\}$对于复数的乘法成群.

11. $K=\left\{\begin{pmatrix}\alpha&\beta\\-\bar{\beta}&\bar{\alpha}\end{pmatrix}\middle|\alpha,\beta\in\mathbb{C},\text{不同时为}0\right\}$,其中$\bar{\alpha},\bar{\beta}$是$\alpha,\beta$的共轭复数,则$K$在矩阵的乘法下成群.

12. 设G是非空的有限集合,G上的乘法满足:$\forall a,b,c\in G$有

1) $(ab)c=a(bc)$;

2) $ab=ac\Rightarrow b=c$;

3) $ac=bc\Rightarrow a=b$;

则G是群.

13. 证明(1)群中元$a,a^2=e$当且仅当$a=a^{-1}$.(2)偶数个元素的群都含有一个元$a\neq e$,使得$a^2=e$.

14. 证明任一个群G不能是两个不等于G的子群的并集.

15. 以 $\mathbb{Q}_p$ 记分母与某素数 p 互素的全体有理数组成的集合，证明它对于数的加法成为一个群.

16. 以 $\mathbb{Q}^{p^i}$ 记分母皆为 $p^i, i \geqslant 0, p$ 素数，的全体有理数的集合，证明它对数的加法成为群.

17. 令

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}, \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 6 & 4 \end{pmatrix},$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 1 & 3 & 5 & 4 \end{pmatrix},$$

计算 $\rho\sigma, \sigma\tau, \tau\rho, \sigma^{-1}, \sigma\rho\sigma^{-1}$.

18. 设

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

问

$$\sigma = \begin{pmatrix} \tau(1) & \tau(2) & \cdots & \tau(n) \\ ? & ? & \cdots & ? \end{pmatrix}, \tau^{-1} = \begin{pmatrix} ? & ? & \cdots & ? \\ i_1 & i_2 & \cdots & i_n \end{pmatrix},$$

及

$$\tau\sigma\tau^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ ? & ? & \cdots & ? \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} \begin{pmatrix} ? & ? & \cdots & ? \\ 1 & 2 & \cdots & n \end{pmatrix}$$
$$= ?$$

§2 对称性变换与对称性群 晶体对称性定律

群是刻画事物对称性的工具. 它可以刻画图形的对称性，也可以刻画多个变量的函数的对称性，甚至可以刻画物理系统的对称性. 我们先来考察图形的对称性是如何刻画的. 为简单起见，考虑平面图形.

例 1 证明图 1 的等腰三角形的两个底角相等.

这是平面几何中的典型问题. 其证法之一是：作 AD 平分 $\angle A$，即 $\angle 1 = \angle 2$. 然后绕 AD 翻转 $\triangle ABD$，由于 $\angle 1 = \angle 2$，可将 AB 落下与直线 AC 重合. 又因是等腰三角形，$AB = AC$，这时 B 正好落到 C 上. 于是经翻转可使 $\triangle ABD$ 与 $\triangle ACD$ 重合. 于是

$$\angle ABD = \angle ACD.$$

证毕.

上面的证明中实际上是实现下述操作：把 $\triangle ABC$ 整个图形绕 AD 翻转，当 AB 转到与 AC 重合时，AC 也与 AB 重合，即把 $\triangle ABC$ 翻转到与原来位置

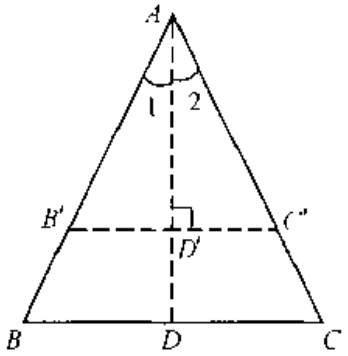


图 1

重合.这个翻转引起 $\triangle ABC$ 所在平面的一个正交变换,称为对于直线或轴 AD 的反射.

$\triangle ABC$ 经此反射后仍与原图形重合的性质叫做 $\triangle ABC$ 对于 AD 是对称的,或称对于轴 AD 的反射是 $\triangle ABC$ 的一个**对称性变换**.

定义 1 平面上(或空间中)的一个图形 Γ.若平面上(空间中)的一个正交变换将 Γ 变成与自己重合,则称此变换是 Γ 的**对称性变换**.

上面的讨论说明图形 Γ 的对称性变换反映了 Γ 的某种对称性.更有意义的是下面的

命题 1 图形 Γ 的全体对称性变换在变换的乘法下成为一个群.我们称它为 Γ 的**对称性群**.

证明 首先设 T_1, T_2 是 Γ 的两个对称性变换.它们都是正交变换,于是它们的乘积也是正交变换.它们都把 Γ 变成与自己重合,故它们的乘积也把 Γ 变得与自己重合.这说明它们的乘积是对称性变换,也即全体对称性变换在变换的乘法下是封闭的.T_1 是正交变换,它的逆变换也是正交变换,且也把 Γ 变成与自己重合,即 T_1 的逆变换也是对称性变换.

又恒等变换是对称性变换,它是单位元,而变换的乘法满足结合律.故 Γ 的全体对称性变换作成一个群.

有了这个命题可知图形的全部对称性是由它的对称性群所刻画的.它必受到定义中条件的制约.正是基于这一点再经过复杂的推理论证,人们得出了晶体的所有可能的对称性群(参见本节最后).

例 2 正四边形 $A_0A_1A_2A_3$ 的中心是 O,则绕 O 点旋转 0°,90°,180°,270° 以及对图上直线 l_1, l_2, l_3, l_4 的反射都是它的对称性变换.实际上它只有这 8 个对称性变换.为此只要证明正四边形 $A_0A_1A_2A_3$ 的对称性变换不超过 8 个就行了.

设 T_0, T_1, T_2, T_3 分别是绕 O 转 0°,90°,180°,270° 的旋转.T 是任一个对

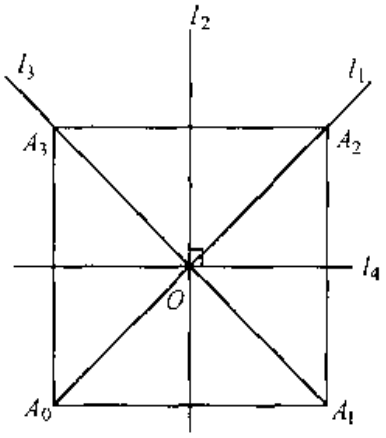


图 2

称性变换，设它将 A_0 变到 A_i，则 $T_i^{-1}T$ 是对称性变换，它使 A_0 不动. 又 O 点在任何对称性变换下不动，故 $T_i^{-1}T$ 使直线 l_1 上每一点不动，$T_i^{-1}T$ 这个对称性变换只有两种可能性：$T_i^{-1}T = T_0$（恒等变换）及 $T_i^{-1}T =$ 对直线 l_1 的反射，记为 S_1. 于是 $T = T_iT_0$ 或 $T = T_iS_1$. 因 $i = 1,2,3,4$ 有 4 个可能，故 T 只有 8 种可能.

上面计算出 $\square A_0A_1A_2A_3$ 的对称性群的 8 个元素是 T_0, T_1, T_2, T_3 及 S_1, S_2, S_3, S_4（S_i 是对直线 l_i 的反射）. 它们也可写成 $T_0, T_1, T_2, T_3, T_0S_1, T_1S_1, T_2S_1, T_3S_1$. 这个群记作 D_4（正四边形的对称性群）.

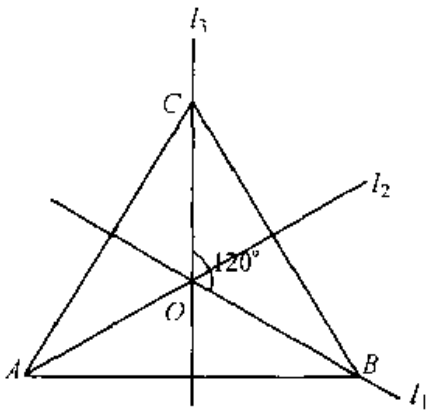


图 3

例 3　正三角形 $\triangle ABC$（中心在 O）的全体对称性变换由绕 O 旋转 0°，120°，240° 的旋转 T_0, T_1, T_2 及对直线 l_1, l_2 和 l_3 的反射 S_1, S_2, S_3 组成. 这 6 个元素的集合也能写成 $\{T_0, T_1, T_2, T_0S_1, T_1S_1, T_2S_1\} = D_3$. $\triangle ABC$ 的对称性群就是 D_3.

上面两个例子中，在求所有对称性变换时已经用到了群的运算：逆元素和

乘积.这说明了有运算的好处.运算在解决各种问题中起的作用就好像力学中杠杆的作用.

下面再来看多变量函数的对称性.

我们在根与系数关系的公式中学习过 n 个文字的初等对称多项式

$$x_1 + x_2 + \cdots + x_n,$$

$$x_1x_2 + x_2x_3 + \cdots + x_1x_n + x_2x_3 + \cdots + x_2x_n + \cdots + x_{n-1}x_n,$$

$$\cdots\cdots$$

$$x_1x_2x_3\cdots x_n.$$

现来考察一下对称的涵义是什么?

首先对 $1,2,\cdots,n$ 的任一置换

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}, \sigma(k) = i_k, k = 1,2,\cdots,n,$$

它引起 n 个文字 $x_1,\cdots,x_n$ 的一个置换

$$\begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ x_{i_1} & x_{i_2} & \cdots & x_{i_n} \end{pmatrix}.$$

进而引起某域上任一多项式 $f(x_1,\cdots,x_n)$ 中 $x_1,\cdots,x_n$ 的置换,面将 $f(x_1,\cdots,x_n)$ 变成 $f(x_{i_1},\cdots,x_{i_n})$.为简便计,我们仍记为

$$\sigma(f(x_1,\cdots,x_n)) = f(x_{i_1},\cdots,x_{i_n}) = f(x_{\sigma(1)},\cdots,x_{\sigma(n)}).$$

例如令

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

及 $f(x_1,x_2,x_3) = x_1^3 + x_2x_3$,则 $\sigma(x_1^3 + x_2x_3) = x_2^3 + x_3x_1$.

但是容易看出对任意 σ,

$$\sigma(x_1 + \cdots + x_n) = x_{i_1} + \cdots + x_{i_n} = x_1 + \cdots + x_n;$$

$$\sigma(x_1x_2 + \cdots + x_1x_n + x_2x_3 + \cdots + x_2x_n + \cdots + x_{n-1}x_n)$$

$$= x_{i_1}x_{i_2} + \cdots + x_{i_1}x_{i_n} + x_{i_2}x_{i_3} + \cdots + x_{i_2}x_{i_n} + \cdots + x_{i_{n-1}}x_{i_n}$$

$$= x_1x_2 + \cdots + x_1x_n + x_2x_3 + \cdots + x_2x_n + \cdots + x_{n-1}x_n;$$

$$\cdots\quad\cdots$$

$$\sigma(x_1x_2\cdots x_n) = x_{i_1}x_{i_2}\cdots x_{i_n} = x_1x_2\cdots x_n.$$

这说明对任意置换 σ,在任一初等对称多项式的各个文字的脚标上进行置换 σ 后,该多项式完全不变.

定义 2 设 $f(x_1,x_2,\cdots,x_n)$ 是某域 F 上的 n 元多项式.对 $1,2,\cdots,n$ 的任一置换 σ,若在 $f(x_1,x_2\cdots,x_n)$ 的各文字的脚标上进行置换 σ 后,该多项式

完全不变,则称它是域 F 上的一个 n 元**对称多项式**.

但是域 F 上一般的 n 元多项式就不一定是对称多项式.例如 $f(x_1,x_2,x_3,x_4)=x_1x_2+x_3x_4$ 对置换

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

有

$$\begin{aligned}\sigma f(x_1,x_2,x_3,x_4)&=\sigma(x_1x_2+x_3x_4)\\&=x_3x_2+x_1x_4\neq f(x_1,x_2,x_3,x_4).\end{aligned}$$

它就不是对称多项式.

定义 3 设 $f(x_1,x_2,\cdots,x_n)$ 是域 F 上 n 元多项式.若 n 元置换 σ 满足 $\sigma f(x_1,\cdots,x_n)=f(x_1,\cdots,x_n)$,则称 σ 是 $f(x_1,\cdots,x_n)$ 的一个**对称性变换**.

类似于图形的对称性变换,容易证明 $f(x_1,\cdots,x_n)$ 的全体对称性变换对于置换的乘法也作成一个群.我们称它为多项式 $f(x_1,x_2,\cdots,x_n)$ 的**对称性群**.

任一 n 元置换都是 n 元对称多项式的对称性变换,而它的对称性群就是 n 元对称群 S_n.

例 4 $f(x_1,x_2,x_3,x_4)=x_1x_2+x_3x_4$ 的全部对称性变换为

$$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},$$
$$\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}.$$

共有 8 个元素,它们组成 $x_1x_2+x_3x_4$ 的对称性群.

问题:用 S_4 的全部置换去变 $x_1x_2+x_3x_4$ 共能变出几个多项式?把它们都写出来.

实际答案有三个多项式.S_4 有 24 个元素,$x_1x_2+x_3x_4$ 的对称性群有 8 个元.用 S_4 的全部置换去变 $x_1x_2+x_3x_4$ 共能变出 3 个多项式,且有关系式 $24=8\cdot 3$.这个关系不是偶然的,这是群论中的一个基本性质的反映.我们将在讨论有限群作用下的轨道长的 §6 中论证它,这个关系是群的运算性质的良好表现.

以上我们用了两节篇幅讲了群的很多例子,下面介绍一个应用.历史上引入群的定义后不久,群就用于刻画晶体的对称性.下面我们先证明所谓晶体对称性定律,然后介绍反映晶体对称结构的群论结果.

实验证明晶体是由原子、分子或分子团排成的格(子)点阵.抽象地可用空间的无限格点阵来代表晶体结构.在数学上可如下地表述空间点阵:取空间中一坐标系 $[O,\vec{a}_1,\vec{a}_2,\vec{a}_3]$,则空间取整数坐标的全部点的集合就是一个空间点阵,以 Γ 记任一空间点阵.实际上坐标原点 O 可换成 Γ 中的任一点 O',$[O',$

$\vec{a}_1,\vec{a}_2,\vec{a}_3]$,决定同一点阵.我们还称向量 $l_1\vec{a}_1+l_2\vec{a}_2+l_3\vec{a}_3$,其中 l_1,l_2,l_3 是整数,为 Γ 的**格向量**.

晶体对称性定律 Γ 是空间中由坐标系$[O,\vec{a}_1,\vec{a}_2,\vec{a}_3]$ 确定的点阵.过 Γ 上一点,不妨就设为原点 O(因坐标原点可取 Γ 上任一点),有直线 L.若绕 L 的某旋转使 Γ 不变,则旋转角只有 $0,\pm\frac{\pi}{3},\pm\frac{\pi}{2},\pm\frac{2\pi}{3},\pi$ 这几种可能.

证明 设绕 L(过原点 O)旋转 θ 角的转动为 $\mathbb{T}$,可选 L 轴为 z 轴,原点仍为 O,建立一个直角坐标系 $Oxyz$,则 $\mathbb{T}$ 在新坐标下的矩阵为

$$T_0=\begin{pmatrix}\cos\theta & -\sin\theta & 0\\ \sin\theta & \cos\theta & 0\\ 0 & 0 & 1\end{pmatrix}.$$

又 $\mathbf{T}$ 使 Γ 不动,于是将坐标向量 $\vec{a}_1,\vec{a}_2,\vec{a}_3$ 变成 Γ 中的格向量.故$(\mathbf{T}\vec{a}_1,\mathbf{T}\vec{a}_2,\mathbf{T}\vec{a}_3)=(\vec{a}_1,\vec{a}_2,\vec{a}_3)T$,$T$ 是整数矩阵.T 与 T_0 这两个矩阵是相似的,于是有相同的迹.设整数矩阵 T 的迹是整数 m,而矩阵 T_0 的迹是$1+2\cos\theta$,故 $1+2\cos\theta=$ 整数 m.因此

$$\cos\theta=\frac{m-1}{2}=\text{整数之半}.$$

又$|\cos\theta|\leqslant 1$,就得出 $\cos\theta$ 可能取的值为$0,\pm\frac{1}{2},\pm 1$.而 θ 可能取值是$\pm\frac{\pi}{3},\pm\frac{\pi}{2},\pm\frac{2}{3}\pi,0,\pi$.这就证明了晶体对称性定律.

如果将绕某轴旋转角为$0,\pm\frac{\pi}{3},\pm\frac{\pi}{2},\pm\frac{2}{3}\pi,\pi$的旋转分别记为 $T_1,T_6,T_6^{-1},T_4,T_4^{-1},T_3,T_3^{-1},T_2$,则易知这几个旋转能组成五个群:

$$C_1=\{T_1\},$$
$$C_2=\{T_2,T_2^2=T_1\},$$
$$C_3=\{T_3,T_3^2=T_3^{-1},T_3^3=T_1\},$$
$$C_4=\{T_4,T_4^2=T_2,T_4^3=T_4^{-1},T_4^4=T_1\},$$
$$C_6=\{T_6,T_6^2=T_3,T_6^3=T_2,T_6^4=T_3^{-1},T_6^5=T_6^{-1},T_6^6=T_1\}.$$

我们把点阵 Γ 的固定 Γ 上某点的对称性变换组成的群叫做**点群**.我们证明了任一空间点阵的点群若只由绕一固定轴的旋转组成,则这种点群只有 C_1,C_2,C_3,C_4,C_6 五种.

晶体的对称性定律先是在实验上发现的.这里利用空间点阵的结构从数学上证明了它.还可以证明空间点阵可能的点群也只有 32 种(这时点群中可以有绕过一点的多个轴的旋转对称性变换,和中心对称、镜面反射 …… 等形

式的对称性变换，所有这些旋转、中心对称、镜面反射 …… 只有 32 种组合能作成群）. 以上还未考虑空间点阵在平移变换下的对称性. 全面反映空间点阵对称性的对称性群叫**空间群**. 19 世纪末费多罗夫(1885)、熊夫利(1891)、巴罗(1895)各自独立地导出了空间群恰好是230种，完成了晶体结构对称性理论. 20 世纪后实验上证实了上述理论的正确性. 230 种空间群的导出是群论对结晶学也是对自然科学的重要应用，它也推动了群论本身的发展.

习 题

1. 计算下列图形的对称性群：

(1) 正五边形；

(2) 不等边矩形；

(3) 圆.

2. 用 S_4 的全部变换去变 $x_1x_2 + x_3x_4$，把变到的所有可能的多项式写出来.

3. 用 S_3 去变 $x_1^3x_2^2x_3$ 能变出几个多项式，把它们全写出来. 以 $x_1^3x_2^2x_3$ 为其中一项作出一个和，使它是对称多项式，并使其项数最少.

4. 写出 S_3 中全体元素

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ i_1 & i_2 & i_3 \end{pmatrix},$$

$i_1i_2i_3$ 是 1,2,3 的偶排列. 证明所有这些元素在置换的乘法下成为群，记为 A_3.

5. S_4 中下列 4 个元素

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix},$$

在置换乘法下成为一个群，记为 V_4.

6. 求出正四面体 $A_1A_2A_3A_4$ 的对称性群.

§3 子群，同构，同态

本节涉及的是群结构中的几个基本概念.

定义 1 群 G 中若有无限多个元素，则称为**无限群**. 若仅有有限个元素则称为**有限群**. 有限群 G 中元素的数目称为 G 的**阶**，记为 $|G|$.

例如本章 §1 例 2 中的 U_n 的阶 $|U_n| = n$. 例 6 中 n 元对称群 S_n 的阶为 $n!$.

定义 2 H 是群 G 的非空子集,如果 H 对于 G 的乘法也成为群,则称 H 为 G 的**子群**.

本章 §1 的例 1 中,$\mathbb{R}^*$ 是非零实数的乘法群 $\mathbb{R}\setminus\{0\}$ 的子群.例 3 中域 F 上行列式为 1 的 $n\times n$ 阵的群 $SL_n(F)$ 是域 F 上 $n\times n$ 可逆矩阵的群 $GL_n(F)$ 的子群.例 2 中 U_n 是非零复数的乘法群的有限子群.

由定义,G 的非空子集 H 是 G 的子群当且仅当:(1)H 对 G 的乘法是封闭的;(2)H 自身有单位元;(3)H 的每个元在 H 中有逆元.(结合律自然成立).

容易验证 H 的单位元 e' 就是 G 的单位元 e.实际上,e 是 G 的单位元,故有 $ee'=e'$.e' 是 H 的单位元,自然有 $e'e'=e'$.于是 $ee'=e'e'$,用消去律,$e=e'$.

同样可证,对 $h\in H$,h 在 G 中的逆元与 h 在 H 中的逆元(如果有的话)是相等的.因此说明 H 的元素 h 在 H 中有逆元当且仅当 h 在 G 中的逆元属于 H.由此有

命题 1 H 是群 G 的非空子集.H 是 G 的子群当且仅当:(1)H 对于 G 的乘法是封闭的;(2)G 的单位元属于 H;(3)$\forall h\in H$,h 在 G 中的逆元属于 H.

命题 2 设 H 是 G 的非空子集.H 是 G 的子群的充分必要条件是 $\forall a,b\in H$,有 $ab^{-1}\in H$.

证明 只要证明"充分性".取 $b\in H$,则 $e=bb^{-1}\in H$.即 H 中有单位元.由 $e,b\in H$,有 $eb^{-1}=b^{-1}\in H$,故 H 的任一元 b 的逆在 H 中.对 $a,b\in H$,则 $a,b^{-1}\in H$.于是 $ab=a(b^{-1})^{-1}\in H$.即 H 对于 G 的乘法是封闭的.又 H 的乘法自然有结合律,故 H 是 G 的子群.

推论 设 G 是加群,则它的非空子集 H 是 G 的子群当且仅当对 $\forall a,b\in H$,有 $a-b\in H$.

设 $H_1,\cdots,H_k,\cdots$ 是群 G 的子群,则 $\bigcap\limits_{k=1}^{\infty}H_k$ 是 G 的子群(留作习题).

定义 3 设 S 是群 G 的一个非空子集,G 的含 S 的所有的子群的交仍是 G 的一个子群.这个子群称为 G 的由 S **生成的子群**.记为 $\langle S\rangle$.

注意,G 就是含 S 的一个子群,因此定义 3 中 G 的含有 S 的所有子群的交是有意义的.而且,$\langle S\rangle$ 就是 G 中含 S 的最小的子群.

若 S 仅由一个元素 a 组成时,$\langle S\rangle=\langle a\rangle$,我们称 $\langle a\rangle$ 为 G 的循环子群.可证 $\langle a\rangle$ 由 a 的全部方幂组成,$\langle a\rangle=\{a^m\mid m\in\mathbb{Z}\}$(留作习题).若有 $a\in G$,使 $G=\langle a\rangle$,则称 G 为**循环群**.

定义 4 两个群 G_1 及 G_2,若有 G_1 到 G_2 的映射 σ,它保持乘法,即对 $\forall g_1,g_2\in G_1$,有 $\sigma(g_1g_2)=\sigma(g_1)\sigma(g_2)$,则称 σ 是 G_1 到 G_2 的**同态**.若 σ 还是 G_1 到 G_2 的双射(有的书上叫一一对应),则称 σ 是 G_1 到 G_2 的**同构**.通常用

$G_1 \cong G_2$ 表示 G_1 与 G_2 同构. 群 G 到自身的同构叫 G 的**自同构**.

先看看同构的意义. 设 σ 是 G_1 到 G_2 的一个同构, $\forall g_1, g_2 \in G_1$,

$$g_1 \overset{\sigma}{\longmapsto} \sigma(g_1),$$

$$g_2 \overset{\sigma}{\longmapsto} \sigma(g_2),$$

则 $\sigma(g_1g_2) = \sigma(g_1)\sigma(g_2)$ 就是

$$g_1g_2 \overset{\sigma}{\longmapsto} \sigma(g_1)\sigma(g_2).$$

也即在映射 σ 下 G_1 中元素 g_1 和 g_2 的积 g_1g_2 映射到 G_2 中, 对应的象元 $\sigma(g_1g_2)$ 是 $\sigma(g_1)$ 和 $\sigma(g_2)$ 的积 $\sigma(g_1)\sigma(g_2)$. 这就是映射 σ 保持乘法.

由于 σ 是双射, 当 g_1 取遍 G_1 时, $\sigma(g_1)$ 取遍 G_2, 且不相重. 因此若把 g_1 与 $\sigma(g_1)$ 看成等同(实际上 $\sigma(g_1)$ 是 g_1 在 σ 下的象)时, G_1 与 G_2 也看成等同(G_2 是 G_1 的象), 且它们的乘法也是一样的, 因而是同样的代数运算系统. 换句话说, G_1 与 G_2 除了记号不同外运算结构是一样的. 代数学中主要是研究运算的一般性质, 而对于承载运算的集合是不注意的. 因此同构的群作为代数运算系统是看作一样的. 从同构的群中选择任一个群来研究它的运算性质, 就能得出其他群的运算性质.

下面看一些群同构的例子.

例 1 本章 §1 的例 7 中, V 是域 F 上 n 维性空间, V 上全体可逆线性变换的群 $GL(V)$ 及例 3 中域 F 上全体 $n \times n$ 可逆矩阵的群 $GL_n(F)$ 是同构的.

这是因为任给 V 的一组基, V 中的可逆线性变换与 F 上 $n \times n$ 可逆矩阵是一一对应的. 即 $GL(V)$ 到 $GL_n(F)$ 上有双射. 由线性代数还知道, 在这个双射之下, 可逆线性变换的乘积对应于相应的可逆矩阵的乘积, 故是同构.

例 2 令 $\mathbb{R}^+$ 是正实数的乘法群, $\mathbb{R}$ 是实数加法群. 任一正实数 a 可以表成 $10^{a'}$ (10 的方幂). 由数学分析知道这定义了一个映射

$$\mathbb{R}^+ \xrightarrow{\log} \mathbb{R}$$

$$a \longmapsto a', \text{其中 } a = 10^{a'},$$

而且是双射. 这个映射中学里学过, 它是对 a 取以 10 为底的对数, $a' = \log a = \log_{10} a$. 设 $a, \beta \in \mathbb{R}^+$, $a \mapsto a'$, $\beta \mapsto \beta'$, 即有 $a = 10^{a'}$, $\beta = 10^{\beta'}$. 于是 $a\beta = 10^{a'+\beta'}$, 即 $a\beta \mapsto a' + \beta'$. 这说明对数映射保持运算(注意, $\mathbb{R}^+$ 中是乘法, $\mathbb{R}$ 中是加法). 故取对数 log 这个映射是 $\mathbb{R}^+$ 到 $\mathbb{R}$ 的同构映射.

由于有这个同构, 在求 $\mathbb{R}^+$ 中两个元素的乘积时, 一般地乘法比加法计算量大, 我们先对这两个元素取对数(就映到了 $\mathbb{R}$ 中)将它们的对数相加, 然后再通过 log 的逆映射(取反对数)得到它们的乘积. 利用取对数将求两个正数

的乘积化为求两个实数的和.这在中学时已学过,这里只是指出了对数的理论基础(也是中学时讲过的)在代数上的意义是群同构.

下面的定理说明任意一个抽象群都与某集合上的一个变换群(集合 M 上全变换群 S_M 的子群都称为此集合的**变换群**)同构.

定理 3 (Cayley) 任何一个群 G 都同构于 G 上(作为集合)的一个变换群.

证明 首先对任一元 $g \in G$,将 g 从左边遍乘 G 的全部元素就得到 G 的一个变换 σ_g:

$$G \xrightarrow{\sigma_g} G$$

$$a \longmapsto ga.$$

即对于所有 $a \in G, \sigma_g(a) = ga$.全体 $\sigma_g, \forall g \in G$,的集合记为

$$G_L = \{\sigma_g \mid g \in G\}.$$

下面来证 G_L 对变换的乘法成为群,于是 G_L 是 G 上的一个变换群.

由于 G 非空,$\{\sigma_g \mid g \in G\}$ 也就非空.对 $g_1, g_2 \in G, (\sigma_{g_1}\sigma_{g_2})(a) = g_1(g_2a) = (g_1g_2)a = \sigma_{g_1g_2}(a), \forall a \in G$.故 $\sigma_{g_1}\sigma_{g_2} = \sigma_{g_1g_2}$.即 G_L 对变换的乘法是封闭的.

若 e 是 G 的单位元,则有 $\sigma_e(a) = ea = a, \forall a \in G$.故 σ_e 是 G 上恒等变换,它是 G_L 的单位元.

又 $\forall g \in G$,

$$\sigma_g\sigma_{g^{-1}}(a) = \sigma_{gg^{-1}}(a) = \sigma_e(a),$$

$$\sigma_{g^{-1}}\sigma_g(a) = \sigma_{g^{-1}g}(a) = \sigma_e(a), \forall a \in G.$$

这即说明 G_L 中任一元 σ_g 有逆变换,且逆变换是 $\sigma_{g^{-1}}$.

这就证明了 G_L 是一个群,且是 G 上的变换群.

作映射

$$G \longrightarrow G_L$$

$$g \longmapsto \sigma_g.$$

由于 $\sigma_g(e) = g$,故 $g \neq g'$ 时,$\sigma_g \neq \sigma_{g'}$.即这个映射是单的(有的书上称1 - 1的).由 G_L 的定义,上述映射是满的(有的书上称为映上的),因而是双射.又 $\forall g_1, g_2 \in G, g_1g_2 \longmapsto \sigma_{g_1g_2} = \sigma_{g_1}\sigma_{g_2}$,故该映射保持乘法,又是双射,因而是同构.这就证明了定理.

同态是同构的推广,它有更广泛的例子.下一节的群作用是同态的例子.这儿也举几个例子.

例 3 整数加法群 $\mathbb{Z}, n \in \mathbb{Z}$,记 $n\mathbb{Z} = \{kn \mid k \in \mathbb{Z}\}$.也即 $n\mathbb{Z} = \langle n \rangle$($\mathbb{Z}$ 中

由 n 生成的循环子群是由 n 的一切倍数构成的). 作映射

$$\begin{aligned}\mathbb{Z} &\longrightarrow \langle n\rangle\\ k &\longmapsto kn.\end{aligned}$$

易知这是群同态.

例 4 整数加法群 $\mathbb{Z}$ 及任一乘法循环群 $G=\langle a\rangle$. 作映射

$$\begin{aligned}\mathbb{Z} &\longrightarrow G\\ k &\longmapsto a^k.\end{aligned}$$

这也是群同态. 在 §10 中讲完同态基本定理后,应用此映射可以使循环群的结构更清楚.

例 5 对 $A\in GL_n(F)$,以 $|A|$ 记 A 的行列式. 作映射

$$\begin{aligned}GL_n(F) &\xrightarrow{\sigma} F^*=F\setminus\{0\}\\ A &\longmapsto |A|.\end{aligned}$$

$\forall A,B\in GL_n(F)$,有 $|AB|=|A||B|$,即 $\sigma(AB)=\sigma(A)\sigma(B)$. 故 σ 是群同态.

设 σ 是群 G 到 G' 的同态. 对 G 的子集 S,令 $\sigma(S)=\{\sigma(a)\mid a\in S\}$. 它是 G' 的子集,称为 S 在 σ 下的**象**. 易验证 $\sigma(e)$ 是 G' 的单位元 e';对 $g\in G$, $\sigma(g^{-1})$ 是 $\sigma(g)$ 的逆元;设 H 是 G 的子群,则 $\sigma(H)$ 是 G' 的子群. 对于 G 的象 $\sigma(G)$ 的子集 H',令 $\sigma^{-1}(H')=\{g\in G\mid\sigma(g)\in H'\}$,称为 H' 的**原象**. 若 H' 是 $\sigma(G)$ 中子群,则 $\sigma^{-1}(H')$ 是 G 中子群. 特别 $\sigma^{-1}(e')$ 是 G 的子群,称为同态 σ 的**核**,记为 $\mathrm{Ker}\,\sigma$. 如果 G 在 σ 下的象 $\sigma(G)=G'$,即 σ 是满射,则称 σ 是**满同态**. 如同态 σ 是单射,则称 σ 为**单同态**. σ 为单同态当且仅当 $\mathrm{Ker}\,\sigma=\{e\}$. 这些都请读者自行验证.

习 题

1. 四个复数 $1,-1,\mathrm{i},-\mathrm{i}$ 的集合 U_4 构成非零复数的乘法群的子群.

2. $H_1,H_2,\cdots,H_k,\cdots$ 都是群 G 的子群. 证明

(1) $H_1\cap H_2$ 是子群.

(2) $\bigcap\limits_{i=1}^{\infty}H_i$ 是子群.

(3) 若 $H_1\subset H_2\subset\cdots\subset H_k\subset H_{k+1}\subset\cdots$,则 $\bigcup\limits_{i=1}^{\infty}H_i$ 是子群.

3. 设 G 是群. 令 $Z(G)=\{a\in G\mid ag=ga,\forall g\in G\}$,则 $Z(G)$ 是 G 的子群. 称为 G 的**中心**.

4. G 是群,S 是 G 的非空子集. 令

$$C_G(S) = \{a \in G \mid as = sa, \forall s \in S\},$$

$$N_G(S) = \{a \in G \mid aSa^{-1} = S\},$$

则它们都是 G 的子群,其中 $aSa^{-1} = \{asa^{-1} \mid \forall s \in S\}$. $C_G(S)$ 和 $N_G(S)$ 分别称为 S 在 G 中的**中心化子和正规化子**.

5. 设 G 是群,H 是 G 的子群.(1)$a \in G$,则 aHa^{-1} 也是子群.(2)τ 是 G 的自同构,则 $\tau(H)$ 也是子群.

6. 证明 §2 中习题 5 中 V_4 与上面习题 1 中 U_4 不同构.

7. 证明正三角形 $A_1A_2A_3$ 的对称性群与 S_3 同构(将每个对称性变换与它引起的顶点的置换相对应)

8. 利用 Cayley 定理证明具有给定阶 n 的有限群只有有限个.

9. 令

$$L = \left\{ \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \middle| 0 \leqslant \theta < 2\pi \right\}, M = \left\{ \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix} \middle| 0 \leqslant \theta < 2\pi \right\}.$$

它们都在矩阵的乘法下成为群,并且相互同构.

10. 证明群 G 是交换群当且仅当映射 $x \mapsto x^{-1}$ 是 G 的自同构.

11. 实数域 $\mathbb{R}$ 到习题 9 中群 L 的映射 φ:

$$\mathbb{R} \longrightarrow L$$

$$x \longmapsto \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix},$$

其中 $x = 2k\pi + \theta, 0 \leqslant \theta < 2\pi$,是 $\mathbb{R}$ 的加群到群 L 的同态.

12. G 是群,S 是 G 的非空子集.令

$$H = \{t_1 \cdots t_i \cdots t_k \mid \forall k \text{ 是正整数}, t_i \text{ 或 } t_i^{-1} \in S\}.$$

证明 H 是子群且 $H = \langle S \rangle$.

13. 整数加法群 $\mathbb{Z}$ 的子群一定是 $n\mathbb{Z}$,某 $n \in \mathbb{Z}$.

14. 证明有理数加法群 $\mathbb{Q}$ 的任何有限生成的子群是循环群.

15. $G = \{$全体 2×2 整数元素的可逆矩阵$\}$,对矩阵乘法是否成为群?全体正实数元素的 2×2 可逆矩阵对矩阵乘法是否成为群?

16. 群 G 的全部自同构在 G 上变换的乘法下成为群,称为 G 的**自同构群**,记为 Aut G.

§4　群在集合上的作用,定义与例子

群在集合上的作用是群论中的重要概念,也是数学中(例如在微分几何、李群、多复变函数论中)的重要概念,甚至在物理,化学中也有重要应用.

我们仍从本章 §2 中对称性群的例子开始.实际上,在讨论平面上正多边形的对称性群时已先有平面上全体正交变换的群(包括旋转、反射、平移 …).进行每个正交变换时把平面上每个点变动了位置,于是平面上所有图形(它们是平面点集的子集)也随之变动了位置,变到了另一个图形.因此每个正交变换引起平面上全体图形的集合上的一个变换.一个图形的对称性群只是全体正交变换的群的一个子群,它是把这个图形变成与自己重合的那些正交变换组成的.因此在图形的对称性群的背景中都以下述事实作前提:(1) 有平面上全体图形的集合.(2) 有平面上全体正交变换的群.(3) 这个群中每个元素都引起平面上全体图形的集合的一个变换.

我们用数学语言来表述上面事实.令平面上全体正交变换的群为 G,平面上全体图形的集合为 M,M 上可逆变换的群为 S_M.任意 $g \in G$ 引起 M 中的变换 $T(g)$.连续两次进行正交变换 g_2, g_1,其结果在 M 上也是连续两次进行 $T(g_2), T(g_1)$.这说明 G 中元素的积 g_2g_1 引起 M 上相应变换的积 $T(g_2)T(g_1)$,即 $T(g_2g_1) = T(g_2)T(g_1)$,显然恒等正交变换引起 M 的恒等变换,g^{-1} 在 M 中引起 $T(g)$ 的逆变换,故 $T(g)$ 是 M 的可逆变换,即 $T(g) \in S_M$.严格写出来,即有 G 到 S_M 的映射 T:

$$G \longrightarrow S_M$$
$$g \longmapsto T(g),$$

满足 $T(g_1g_2) = T(g_1)T(g_2), \forall\, g_1, g_2 \in G$.

即 T 把平面上每个正交变换 g 映成 M 中的可逆变换 $T(g)$,这就作成了平面上全体正交变换群 G 到平面上全体图形集合 M 上可逆变换的群 S_M 的同态.

按上述事实进行抽象就得到下面的

定义 1 设群 G 到某集合 M 的可逆变换的群 S_M 有一同态 T.将群 G 的任一元 g 对应于 S_M 的变换 $T(g)$,而对 M 进行变换,就说 g **作用于** M 上.且称该同态 T 是群 G 在集合 M 上的一个**群作用**.

实际上,当群作用 T 明确时,记号上常进行简化.对 $g \in G$ 及 $\forall\, m \in M$,记 $T(g)m = g \circ m$.令**集合积** $G \times M = \{(g, m) \mid g \in G, m \in M\}$,则群作用确定了一个映射 $\circ$:

$$G \times M \longrightarrow M$$
$$(g, m) \longmapsto g \circ m.$$

对给定 $g \in G, \forall\, m \in M, g \circ m$ 定义了 M 上的一个可逆变换,且

$$(g_2g_1) \circ m = g_2 \circ (g_1 \circ m).$$

更进一步,我们证明下面的命题,它给出更简明的充要条件来判断

$G \times M$ 到 M 的映射。是否引起群 G 在 M 上的群作用.

命题 1 下述映射

$$G \times M \dashrightarrow M$$
$$(g, m) \longmapsto g \circ m$$

能确定群 G 在 M 上的一个群作用的充分必要条件为

1) $g_2 \circ (g_1 \circ m) = (g_2 g_1) \circ m$,

2) $e \circ m = m$,

$\forall g_1, g_2 \in G, \forall m \in M$.

证明 先证"充分性".对固定 $g \in G, \forall m \in M, g \circ m$ 定义了 M 中的变换,记为 $T(g)$.由 1),2),

$$T(g^{-1})T(g)m = g^{-1} \circ (g \circ m) = (g^{-1}g) \circ m = e \circ m = m,$$

同样 $T(g)T(g^{-1})m = e \circ m = m$.这说明 $T(g)$ 是 M 中可逆变换,$T(g) \in S_M$.

由 $g_2 \circ (g_1 \circ m) = (g_2 g_1) \circ m$,即有 $T(g_2)T(g_1) = T(g_2 g_1), \forall g_1, g_2 \in G$.这说明

$$G \xrightarrow{T} S_M$$
$$g \longmapsto T(g): T(g)m = g \circ m$$

是 G 到 S_M 的同态.即 T 是 G 在 M 上的群作用.

"必要性"是明显的.

注意:上述满足条件 1),2) 的 $G \times M$ 到 M 的映射与 G 在 M 上的群作用 T 是互为决定的关系,但映射本身不是 T,不是群作用,它只是能给出 T,使 T 是 G 到 M 的可逆变换群 S_M 的一个同态.

例 1 令 S_n 是 n 个数字 $1,2,\cdots,n$ 上的 n 元对称群.M 为域上 F 上 n 元多项式 $f(x_1, x_2, \cdots, x_n)$ 的全体.作映射:$S_n \times M \longrightarrow M$,

$$\text{对 } \sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix},$$
$$(\sigma, f(x_1, \cdots, x_n)) \longmapsto \sigma \circ f(x_1, \cdots, x_n),$$

其中

$$\sigma \circ f(x_1, x_2, \cdots, x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \cdots, x_{\sigma(n)}).$$

易知,当 σ 是恒等置换 e 时,$e \circ f(x_1, x_2, \cdots, x_n) = f(x_1, x_2, \cdots, x_n)$.对任意 $\tau, \sigma \in S_n$,又有

$$(\tau\sigma) \circ (f(x_1, \cdots, x_n))$$
$$= f(x_{(\tau\sigma)(1)}, \cdots, x_{(\tau\sigma)(n)}) = f(x_{\tau(\sigma(1))}, \cdots, x_{\tau(\sigma(n))})$$

$$= \tau \circ (f(x_{\sigma(1)}, \cdots, x_{\sigma(n)})) = \tau \circ (\sigma \circ f(x_1, \cdots, x_n)).$$

故得到 S_n 在 M 上的群作用.

§2 中定义过多项式 $x_1x_2 + x_3x_4$ 的对称性群,实际上是 S_4 的子群,它是 S_4 作用在域 F 上 x_1, x_2, x_3, x_4 的全体多项式的集合上时,能保持 $x_1x_2 + x_3x_4$ 不变的全体元素所成的子群.

从上面两个例子看出,在对称性群的概念形成的时候,群作用的概念就同时蕴含其中.因此群作用的概念是十分基本和重要的.在我们以前学过的解析几何和代数中已经接触过这种现象,下面举出若干例子介绍它们.

例 2 取 $G = GL_n(\mathbb{C})$,$\mathbb{C}$ 是复数域.$M = \mathbb{C}$ 上全体 n 阶方阵.令映射

$$G \times M \longrightarrow M$$
$$(C, A) \longmapsto C \circ A = CA(\text{方阵的乘积}).$$

当 C 是单位阵 E 时,$E \circ A = EA = A$,且对 $C_1, C_2 \in G$ 有

$$C_2 \circ (C_1 \circ A) = C_2(C_1A) = (C_2C_1)A = (C_2C_1) \circ A.$$

故它定义了群 $GL_n(\mathbb{C})$ 在 M 上的群作用.这个群作用是用可逆矩阵 C 左乘 A,相当于对 A 进行一系列初等行变换.

例 3 取 G, M 同上例.$C \in GL_n(\mathbb{C})$,$A \in M$.用 C 右乘 A 是否是群作用呢?先试试看:设 $C \circ A = AC$,则

$$C_2 \circ (C_1 \circ A) = (AC_1)C_2 = A(C_1C_2) = (C_1C_2) \circ A,$$

右边与 $(C_2C_1) \circ A$ 不一定相等.故这样定义的映射不一定能成为群作用.只要做如下修改就能使右乘成为群作用,作映射

$$G \times M \longrightarrow M$$
$$(C, A) \longmapsto C \circ A = AC^{-1}.$$

当 C 是单位阵 E 时,$E \circ A = AE = A$,且对 $C_1, C_2 \in G$,有

$$C_2 \circ (C_1 \circ A) = (AC_1^{-1})C_2^{-1} = A(C_1^{-1}C_2^{-1})$$
$$= A(C_2C_1)^{-1} = (C_2C_1) \circ A,$$

故决定一个群作用.这个群作用是用可逆矩阵 C^{-1} 右乘 A,相当于对 A 作一系列初等列变换.

例 4 取 $G = GL_n(\mathbb{C})$,$M = \mathbb{C}$ 上全体 n 阶对称阵.作映射

$$G \times M \longrightarrow M$$
$$(C, A) \longrightarrow C \circ A = CAC', \text{这里 } C' \text{ 是 } C \text{ 的转置}.$$

当 C 是单位阵 E 时,$E \circ A = EAE' = A$.又对 $C_1, C_2 \in G$,有

$$C_2 \circ (C_1 \circ A) = C_2(C_1AC'_1)C'_2$$
$$= (C_2C_1)A(C_2C_1)' = (C_2C_1) \circ A,$$

故得到 G 在 M 上的群作用.这个群作用是对 A 作合同变换.

例 5 $G = GL_n(\mathbb{C}), M = \mathbb{C}$ 上 n 阶方阵.作映射

$$G \times M \dashrightarrow M$$
$$(C, A) \longmapsto C \circ A = CAC^{-1}.$$

易验证,由这映射可得到 G 在 M 上的群作用.这个群作用是对 A 作相似变换.

例 6 令 $M = \mathbb{C}$ 上 $s \times n$ 矩阵的全体,$G_1 = GL_s(\mathbb{C})$ 及 $G_2 = GL_n(\mathbb{C})$. 取 $P_1 \in G_1, P_2 \in G_2$,可对 M 作变换:$\forall A \in M, A \longrightarrow P_1AP_2$.这相当于对 A 两边都作了一系列初等变换.这是否可解释为群作用呢?

定义 2 设 G_1, G_2 是任给的两个群.作集合积

$$G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}.$$

在其上定义乘法为 $(g_1, g_2)(g_1', g_2') = (g_1g_1', g_2g_2'), \forall g_1, g_1' \in G_1, g_2, g_2' \in G_2$. 这个乘法自然地有结合律,它的乘法单位元素为 (e_{G_1}, e_{G_2}). 任意 $(g_1, g_2) \in G_1 \times G_2$,其逆元素为 (g_1^{-1}, g_2^{-1}).因此在这个乘法下,$G_1 \times G_2$ 成为一个群.仍记为 $G_1 \times G_2$,称为群 G_1 与 G_2 的**直积**.

作直积是从已知群来构造新的群的一种方法.现在我们把上面的变换解释成 $(P_1, P_2^{-1}) \circ A = P_1AP_2$,于是就有映射

$$(G_1 \times G_2) \times M \longrightarrow M$$
$$((P_1, P_2), A) \longmapsto (P_1, P_2) \circ A = P_1AP_2^{-1}.$$

显然当 P_1 是 s 阶单位阵 E_s,P_2 是 n 阶单位阵 E_n 时,

$$(E_s, E_n) \circ A = E_sAE_n^{-1} = A.$$

又对 $P_1, Q_1 \in G_1, P_2, Q_2 \in G_2, \forall A \in M$ 有

$$\begin{aligned}&(P_1, P_2) \circ ((Q_1, Q_2) \circ A)\\ =&(P_1, P_2) \circ (Q_1AQ_2^{-1}) = P_1Q_1AQ_2^{-1}P_2^{-1} = P_1Q_1A(P_2Q_2)^{-1}\\ =&(P_1Q_1, P_2Q_2) \circ A = ((P_1, P_2)(Q_1, Q_2)) \circ A,\end{aligned}$$

故上述映射给出 $G_1 \times G_2$ 在 M 上的群作用.

在线性代数中,我们对以上矩阵变换还引入了相关的等价关系以及标准形等概念,并讨论各自等价的充分必要条件.既然这些矩阵变换都统一地归入群作用的范围,自然地我们应该在群作用中引入一些相关的概念来统一地表达它们.后者与几何概念接近,比原来的说法更"形象"些.在下一节中我们就做这件事.这就是关于群作用的轨道和不变量等内容.

我们再举出一些群作用的例子.下面两例是 G 在自身上的群作用.群论中,特别是有限群论中一些重要的定理就是这些群作用性质的表现.

例 7 群 G 及其子群 H.我们证明用 H 的元素来左乘 G 的元素是 H 在

G 上的群作用.作映射

$$H \times G \longrightarrow G$$
$$(h, g) \longmapsto h \circ g = hg.$$

易知 $e_H \circ g = e_G \circ g = g$ 及 $h_2 \circ (h_1 \circ g) = (h_2 h_1) \circ g$.故是 H 在 G 上的群作用.

当 $H = G$ 时,以上就是群 G 在作为集合的 G 上的左乘作用,它正是 §3 定理 3 中群 G 到 G 上变换群 G_L 的同态.并且该定理 3 证明了这个群同态还是群同构.

类似地,H 的元素右乘 G 的元素也是 H 在 G 上的群作用.不过这时的映射是

$$H \times G \longrightarrow G$$
$$(h, g) \longmapsto h \circ g = gh^{-1}.$$

下面对群 G 的元 a 来引人 G 上的一个变换 I_a:对 $\forall g \in G$,令

$$I_a(g) = aga^{-1}.$$

易知 I_{e_G} 是 G 上恒等变换,且 I_a 的逆变换是 I_a^{-1}.故 I_a 是 G 上可逆变换.又有

$$I_a(g_1 g_2) = ag_1 g_2 a^{-1} = ag_1 a^{-1} ag_2 a^{-1} = I_a(g_1) I_a(g_2),$$

故 I_a 是 G 的一个自同构.称 I_a 为 a 对应的**内自同构**,或 a 在 G 上引起的**共轭变换**.

共轭变换可引起 G 的任意子群 H(包括 G)在 G 上的群作用,如下面例子所示.

例 8 群 G 及其子群 H.作映射

$$H \times G \longrightarrow G$$
$$(h, g) \longmapsto h \circ g = I_h(g) = hgh^{-1}.$$

易知 $e_H \circ g = e_G \circ g = g$.又对 $h_1, h_2 \in H$, $\forall g \in K$ 有

$$h_2 \circ (h_1 \circ g) = h_2(h_1 g h_1^{-1}) h_2^{-1} = (h_2 h_1) g (h_2 h_1)^{-1} = (h_2 h_1) \circ g.$$

故得到 H 在 G 上的群作用.称为 H 在 G 上的**共轭作用**.

习 题

1. V 是某域 F 上 n 维线性空间,$GL(V)$ 是 V 上全线性变换群.令 M 为 V 的全部子空间的集合.证明 G 在 M 上有群作用.

2. G 是群.K, H 是 G 的子群.作群直积 $K \times H$.定义映射 $\circ$:

$$(K \times H) \times G \longrightarrow G$$

$$((k,h),g)\longmapsto(k,h)\circ g = kgh^{-1}.$$

证明映射。决定了群 $K\times H$ 在集合 G 上的作用.

3. G 是正四面体 $A_1A_2A_3A_4$ 的对称性群. 令 $M_1=|$四面体的顶点的集合$|$, $M_2=|$四面体的四个面的集合$|$, $M_3=|$四面体的六条棱的集合$|$, 则 G 在 M_1,M_2,M_3 上分别有群作用.

4. 令 G 是 $n\times n$ 实正交矩阵的群, M 是 $n\times n$ 实对称矩阵的集合. 证明下述对应是一个映射

$$G\times M\longrightarrow M$$
$$(P,A)\longmapsto P\circ A = PAP^{-1},$$

且决定 G 在 M 上的群作用.

5. 写域 F 上多项式 $f(x,y,z)=f(\boldsymbol{r})$, 其中 $\boldsymbol{r}=(x,y,z)^{\mathrm{T}}$, 取 M 为 F 上全部 x,y,z 的多项式的集合. G 为群 $GL_3(F)$. 对 $A\in G$, 令 $\boldsymbol{r}'=(x',y',z')^{\mathrm{T}}=A(x,y,z)^{\mathrm{T}}=A\boldsymbol{r}$. 证明下述对应

$$(A,f)\longmapsto A\circ f = f(\boldsymbol{r}') = f(A\boldsymbol{r})$$

是 $G\times M\longrightarrow M$ 的一个映射, 且决定 G 在 M 上的群作用.

6. G 是群, K 及 H 是 G 的子群. M 是 G 中 H 的左陪集的集合. 用 K 的元素对 M 的元素进行左乘, 得下列映射：

$$K\times M\longrightarrow M$$
$$(k,tH)\longmapsto k\circ(tH) = ktH,$$

证明这决定了 K 在 M 上的一个群作用.

§5　群作用的轨道与不变量，集合上的等价关系

先看几何空间中的轨道. 取空间中的一直线 l, 空间绕 l 的所有旋转作成一个群 G, $G=|$绕 l 按定向转 θ 角的旋转$|0\leqslant\theta<2\pi|$, 它直接作用于空间所有点的集合. 任取空间一点 x, 用 G 的所有旋转来变动它, 就得到点集$|gx\,|g\in G|$. 这个点集是一个圆, 它在垂直于 l 的平面上, 中心在 l 上, 又过 x 点. 这就是 x 在 G 作用下得到的一条轨道.

类比这个几何形象, 我们给出下述

定义 1　群 G 作用于集合 M 上, 对 $x\in M$, 称集合

$$O_x=|g\circ x\,|g\in G|$$

为 x 在 G 作用下的轨道, 或简称过 x 的轨道.

形象地想, 下面三件事是易于接受的：(1) x 在过 x 的轨道上, (2) 若 x 在过 y 的轨道上, 则 y 也在过 x 的轨道上, (3) 若 x 在过 y 的轨道上, y 在过 z 的

轨道上，则 x 也在过 z 的轨道上. 只要清楚记住：m 在过 x 的轨道上，即为有 $g \in G$，使 $m = g \circ x$，则上述三点是容易验证的. 我们写成下列引理.

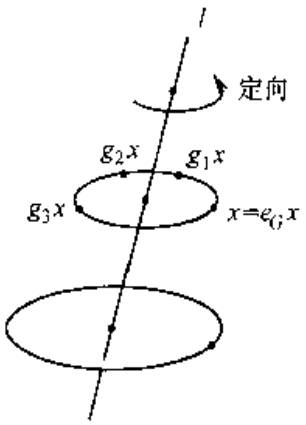


图 1

引理 1 (1) $x \in O_x$，

(2) 若 $y \in O_x$，则 $x \in O_y$，

(3) 若 $z \in O_y, y \in O_x$ 则 $z \in O_x$.

定理 2 设群 G 在 M 上有群作用，则

(1) 若 $y \in O_x$，那么 $O_x = O_y$，

(2) O_x 与 O_y 或重合或不相交，

(3) 在 M 的每一条轨道上取一个元素组成 M 的一个子集 I，称为 M **的轨道的代表元集**，则

$$M = \bigcup_{x \in I} O_x,$$

且此中各 O_x 互不相交.

证明 (1) 对 $z \in O_y$，因 $y \in O_x$ 及由引理 1，得 $z \in O_x$，故 $O_y \subset O_x$. 反之，由 $y \in O_x$ 及引理 1，有 $x \in O_y$. 对 $z \in O_x$，再用引理 1 得 $z \in O_y$，故 $O_x \subset O_y$. 这证明了 $O_x = O_y$

(2) 任两个 O_x, O_y 若相交，设 $z \in O_x \cap O_y$. 由(1)就有 $O_x = O_z = O_y$. 否则它们不相交.

(3) 由于 $\bigcup_{x \in I} O_x$ 含 M 的任一条轨道，而 M 的任一元必属于某一轨道，故 $M \subset \bigcup_{x \in I} O_x$. 反包含是显然的. 故 $M = \bigcup_{x \in I} O_x$. 由于此中各 O_x 互不相同，由(2)，必互不相交.

上面所说的 M 中两个元素在一条轨道上，实际上是 M 上的一种关系，并且是一种等价关系. 在高等代数中矩阵的合同及矩阵的相似也是这样的等价关系. 在此我们要定义任意集合 M 上的一般的等价关系. 类似于定理 2 也有结果：M 是等价类的无交并.

定义 2 设 M 是一个集合，R 是涉及 M 中任意两个元素的有序对的一个法则. 若对于 M 中任意两个元素 a, b 的有序对 (a, b)，均能确定 (a, b) 是否适合 R，则称 R 是 M 上的一个二元关系. 常以 aRb 表示 (a, b) 适合 R.

定义 3 设 M 是一个集合，R 是 M 上的一个二元关系. 若 R 还满足

(1) 反身性：$\forall\, a \in M$，aRa 成立，

(2) 对称性：$\forall\, a, b \in M$，若 aRb 成立，则 bRa 成立，

(3) 传递性：$\forall\, a, b, c \in M$，若 aRb 及 bRc 成立，则 aRc 成立.

则称此二元关系 R 为 M 上的一个**等价关系**. 这时，若有 aRb 成立，也称 a 与 b 关于 R **等价**.

定义 4 设 R 是 M 上的一个等价关系. $a \in M$,令

$$\bar{a} = \{b \in M \mid aRb \text{ 成立}\},$$

称 $\bar{a}$ 为 a 的关于 R 的等价类.简称为 a 的**等价类**.

定理 3 设 R 是集合 M 上的一个等价关系,则

(1) 若 $b \in \bar{a}$,那么 $\bar{b} = \bar{a}$;

(2) $\bar{a}$ 与 $\bar{b}$ 或重合或不相交;

(3) 在 M 的每个等价类中取一个元素组成 M 的一个子集 I,称为 M 的等价类的代表元集,则

$$M = \bigcup_{a \in I} \bar{a},$$

且此中各 $\bar{a}$ 互不相交.

定理 3 的证明完全可仿照定理 2,请读者自己作出.

在代数中会多次碰到集合上的等价关系的例子,因而定理 3 很有用.

现在可用轨道的观点来回顾线性代数中矩阵的一些等价关系,即考察前一节中例 2 到例 6.

例 4 中,$B = C \circ A = CAC'$.即两个复对称方阵 A,B 在一条轨道上当且仅当 A,B 合同.

例 5 中,$B = C \circ A = CAC^{-1}$.即两个复方阵 A,B 在一条轨道上当且仅当 A,B 相似.

例 2 中,$B = C \circ A = CA$. A,B 在一条轨道上当且仅当可用初等行变换化 A 为 B.

例 6 中,$B = (P_1, P_2) \circ A = P_1 A P_2^{-1}$. A,B 在一条轨道上当且仅当可用初等(行及列)变换化 A 为 B.

线性代数中我们还学过:复对称矩阵合同当且仅当它们有相同的秩.相似的矩阵有相同的特征多项式、相同的行列式. A 与 B 可用初等(行及列)变换互变当且仅当它们有相同的秩.我们可用群作用的语言来描述这些性质.

定义 2 设 $G \times M \longrightarrow M$ 的映射 $\circ$ 能决定一个群作用.若 M 上取值于另一集合(域,或复数域,或这些域上多项式的集合)的某个函数 F,满足 $F(x) = F(g \circ x)$, $\forall x \in M$, $\forall g \in G$ 成立,则称 F 是该群作用下的一个**不变量**.

此定义是说 M 上的一个函数 F,它在任一条轨道上都取常值,就是不变量.

前一节例 4 中,矩阵的秩是该作用的不变量.例 5 中,矩阵的特征多项式和行列式是该作用的不变量.例 6 中,矩阵的秩是不变量.线性代数中还研究矩阵合同、相似的充要条件.比如复对称矩阵合同当且仅当它们有相同的秩.这就是说矩阵的秩不但是不变量,而且它是保证两个矩阵在一条轨道上的充

要条件.我们有下面的

定义 3 设 G 在 M 上有群作用.M 上的一组函数 $F_1, F_2, \cdots, F_l$ 称为 M 在 G 作用下的**不变量的一个完全组**,如果对 $\forall x, y \in M$,x 与 y 在同一轨道上当且仅当 $F_i(x) = F_i(y), i = 1, 2, \cdots, l$.

这样在前一节例 4 中的群作用下,矩阵的秩一个不变量就构成不变量的一个完全组.例 6 中的群作用下矩阵的秩一个不变量也组成不变量的一个完全组.对例 5,情况要复杂些.我们知道两个复矩阵相似当且仅当有相同的行列式因子组 $D_1, \cdots, D_n$(或不变因子组 $d_1, d_2, \cdots, d_n$,或初等因子组,而初等因子组写起来更麻烦些).因此,这个群作用下的不变量的完全组可取 $D_1, \cdots, D_n$(或 $d_1, d_2, \cdots, d_n$).

在线性代数中还考虑矩阵的各种等价关系下的标准形问题.像前一节例 2 到例 6 中的等价关系下的等价类,正是某些群作用下的轨道.在等价类中找标准形的问题就是在轨道中选择有特点的,相对简单的元素作代表元.

这样我们就把线性代数中各种矩阵变换的标准形问题用群作用的统一观点加以概括和描述了.群作用的这种观点在几何、分析中已有广泛应用.

注意:上面用不变量以及不变量的完全组来刻画群作用的轨道的方法多在无限群 G 的情形,这时轨道中的元素一般有无限多个.能用有限个不变量刻画轨道那是非常优美的数学性质,这说明能用有限个量来掌握无限个元素的集合.当群 G 是有限群时,轨道中只有有限个元,完全可以列举出来,通常没必要用不变量来刻画轨道.

在本节的最后,我们介绍几何中一个例子,用群作用的思想来分类各种几何学.这就是 Klein 提出的几何学的 Erlangen 纲领.它把欧氏几何、仿射几何、射影几何等几何学用这种观点统一起来.

先看欧氏几何.三维空间中有正交点变换的群 G,它是由空间中保持任意两点距离的所有变换组成的群.把空间所有的图形作成集合 M,当空间进行正交变换时,引起空间图形间的变换,因而 G 可作用在 M 上.欧氏几何就是研究空间图形有哪些性质在 G 作用下保持不变,即研究空间图形在正交变换下的不变性.

例如欧氏几何中证明了两个三角形能在 G 作用下互变(即几何中所说的两个三角形全等)的充要条件是这两个三角形的两边及相应的夹角相等(或三边相等或两角及相应的夹边相等).我们看到欧氏几何书中列出了很多这种不变性.

仍将空间所有图形作成集合 M.空间中将任何共面的四点变成共面的四点的可逆变换叫做仿射变换,所有仿射变换组成群 G.这个群叫作空间的仿射变换群.任一仿射变换引起空间每一图形的变换.这就得到 G 在 M 上的作

用.仿射变换下图形有可能改变大小甚至形状.但也有很多性质不变:直线变成直线,平行直线变成平行直线,平面变成平面,直线上两个线段之比值不变,平面上封闭图形面积之比不变,三角形变成三角形,二次曲线变成二次曲线,保持二次曲线的中心和直径不变…….仿射几何就是研究图形在仿射变换下不变的性质.

射影空间中建立齐次坐标后,四个变数的齐次满秩线性变换叫射影变换,全体射影变换作成射影变换群.射影变换群作用在射影空间的"图形"上.也有许多不变性质:如保持四个点的交比不变,将射影直线变成射影直线,射影平面变成射影平面;它保持关联关系,即将线性相关的点(用齐次坐标表示,是四元向量)变成线性相关的点,将线性无关的点变成线性无关的点.射影几何就是研究射影空间的"图形"有哪些性质在射影变换群作用下保持不变,也即研究在射影变换群作用下不变的几何性质.

Klein 总结了以上例子及当时的其它几何学,想到要刻画各种几何学的共同特征.他是从各个几何学要完成的目标的角度来刻画的.1872 年他在进入 Erlangen 大学教授会时作了题为"近代几何研究的比较评述"的讲演.这个讲演中所表达的观点后来以几何学的 Erlangen 纲领闻名于世.其基本观点是:"每种几何都由变换群所刻画,并且每种几何要做的事实际就是在这种变换群下考察其不变性".按照 Klein 的观点,一种变换群下的不变性质的全体(表述为许多定理)就是一门几何学.不同的变换群就得到不同的几何学.

几何学的 Erlangen 纲领是对几何学的一种看法.在 1872 年时,它能概括当时的大多数几何学,后来还有增加,如拓扑学,它是研究在空间的同胚变换(连续的可逆变换)群下图形的不变性质.但是这个看法也不能把所有的几何学包括进去.例如当时的微分几何,现在的代数几何就不能归入.

Klein 的几何分类思想指引几何学发展达 50 年.他强调的变换群下的不变性质的思想更超出了数学范围而达到力学和物理中.物理中很多系统以某些变换群为对称性群,物理系统的对称性群下的不变性使得群表示论用于量子力学以至场论中.

习　题

1. §4 习题 1 中的群作用有几条轨道?找出群作用的不变量与不变量的完全组.

2. 找出 §4 习题 4 中群作用的不变量和不变量的完全组.

3. (联系 §4 习题 2 中的群作用)令 $t \in G$,称 $KtH = \{kth \mid k \in K, h \in H\}$ 为 G 的一个(K,H)双陪集,则 G 的两个(K,H)双陪集或重合或不

相交,且 G 是全部(K,H)双陪集的无交并.

§6 陪集,Lagrange 定理,稳定化子,轨道长

这一节利用有限群 G 在自身上的几个群作用,即 §4 中例 7、例 8 中的群作用来得到有限群的一些性质.

本节和下节都只考虑有限群.设 H 是有限群 G 的子群.考察 H 在 G 上的左乘作用及右乘作用(§4 中例 7).

定义 1 令 H 在 G 上作左乘作用.对 $x \in G$,这个群作用下过 x 的轨道

$$Hx = \{h \circ x = hx \mid h \in H\}$$

称为 H 在 G 中的一个**右陪集**.而 H 在 G 上右乘作用下过 x 的轨道

$$xH = \{x \circ h^{-1} = xh \mid h \in H\}$$

称为 H 在 G 中的**左陪集**.

由 §5 定理 2 知,若 G 在 M 上有群作用,则 M 是群作用的若干不相交的轨道的并集.设 $Hg_1, Hg_2, \cdots, Hg_s$ 是 H 在 G 中的全部不同(也就互不相交)的右陪集(H 在 G 上左乘作用的全部轨道),而 $g'_1H, g'_2H, \cdots, g'_tH$ 是 H 在 G 中的全部不同(也就互不相交)的左陪集(H 在 G 上右乘作用的全部轨道),则

$$G = \bigcup_{i=1}^{s} Hg_i = \bigcup_{j=1}^{t} g'_jH. \tag{1}$$

易知任意右陪集 Hg_i 中元素数目,同样地任意左陪集 g'_jH 中元素数目皆为 $|H|$.比较(1)中第二个等号两端元素的数目,就有 $s|H| = t|H|$.故 $s = t$,即 H 在 G 中的左,右陪集的数目相等.

定义 2 子群 H 在 G 中左(右)陪集的数目称为子群 H 在 G 中的**指数**,记为$[G:H]$.(1)中第一(二)个等号后面的式子称为子群 H 对于 G 的右(左)**陪集分解**.

由(1)式,我们计算 G 的元素的数目,得到

定理 1 (Lagrange) G 是有限群,H 是 G 的子群,则

$$|G| = [G:H]|H|.$$

这是有限群的最基本的性质.

下面我们来分析群作用下的轨道长.

定义 3 设群 G 作用子 M.对 $x \in M$,令

$$\mathrm{Stab}_G(x) = \{g \in G \mid g \circ x = x\},$$

称它为群 G 作用下 x 的**稳定化子**.

易证 $\mathrm{Stab}_G(x)$ 是 G 的子群.

考虑平面上正交变换的群在平面所有图形的集合上的群作用.给定一个图形(例如正 n 边形),它的稳定化子,就是保持该图形不变的全体正交变换所成的子群.在引入群的概念时我们称它为图形的对称性群.不过在群作用下考虑时,我们采用稳定化子这个名词.

定理 2 G 是有限群,G 在 M 上有群作用.对 $x \in M$,令 O_x 是过 x 的轨道,$O_x = \{g \circ x \mid g \in G\}$ 是有限集.设 $O_x = \{x_1, x_2, \cdots, x_k\}$,其中 $x_1 = x$.且设 $g_1, \cdots, g_k \in G$ 使 $x_i = g_i \circ x$,$i = 1, 2, \cdots, k$,则

$$G = \bigcup_{i=1}^{k} g_i \mathrm{Stab}_G(x) \tag{2}$$

是 $\mathrm{Stab}_G(x)$ 对 G 的左陪集的无交并.

证明 设 $g \in G$ 使 $g \circ x = x_i$,则

$$g_i^{-1} \circ (g \circ x) = g_i^{-1} \circ (g_i \circ x) = (g_i^{-1} g_i) \circ x = x.$$

而等式左端为 $(g_i^{-1} g) \circ x$,故 $(g_i^{-1} g) \circ x = x$,即有 $g_i^{-1} g \in \mathrm{Stab}_G(x)$.于是 $g \in g_i \mathrm{Stab}_G(x)$,而有 $G \subseteq \bigcup_{i=1}^{k} g_i \mathrm{Stab}_G(x)$.反包含是显然的,这就证明了(2).

再证 $i \neq j$ 时,$g_i \mathrm{Stab}_G(x)$ 与 $g_j \mathrm{Stab}_G(x)$ 无交.实际上这时 $x_i \neq x_j$.若有 $g \in g_i \mathrm{Stab}_G(x) \cap g_j \mathrm{Stab}_G(x)$.由 $g \in g_i \mathrm{Stab}_G(x)$,得 $g \circ x = x_i$,由 $g \in g_j \mathrm{Stab}_G(x)$,得 $g \circ x = x_j$,矛盾.这就证明了(2)是无交并.

推论 1 **轨道长** $|O_x|$ 满足公式 $|G| = |\mathrm{Stab}_G(x)| |O_x|$ 或 $|O_x| = [G : \mathrm{Stab}_G(x)]$.

定义 4 设 G 在 M 上有群作用.若 M 只有一条轨道,即 M 自身构成一条轨道,则称 G 在 M 上的作用是**传递的**.

推论 2 若有限群 G 在 M 上的群作用是传递的,则

$$|M| = [G : \mathrm{Stab}_G(x)],$$

这里 x 是 M 中任意一个元素.

下面讲两个应用定理 2 的例子.

例 1 决定立方体(如下图)的对称性群 G.

我们把立方体的 6 个面作成集合 M.把上、下两底面分别记为 1,3;前后两面为 2,4;而左右两侧面为 6,5.G 在 M 上引起群作用,并且传递地作用在 M 上.将立方体绕 Ox 轴旋转 0°,90°,180°,270° 就把面 1 分别变到面 1,面 2,面 3,面 4;绕 Oy 轴转 90° 和 270° 就把面 1 变到面 5 和面 6(以上旋转都是按右手旋转).把这 6 个旋转依次记为 T_i($i = 1, \cdots, 6$).易知 G 在面 1 处的稳定化子 $\mathrm{Stab}_G(1)$ 有 8 个元素:四个绕 Oz 轴的旋转及分别对于 xOz 面、AOz 面、yOz 面及 BOz 面的镜面反射.由定理 2 知道

$$G = \bigcup_{i=1}^{6} T_i \mathrm{Stab}_G(1).$$

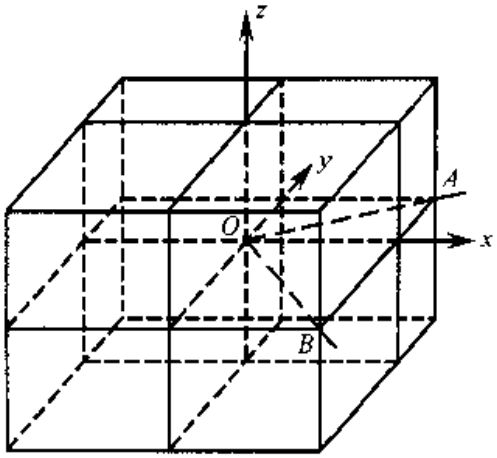


图 1

由此知 G 是由 48 个元素组成的.

上面决定立方体的对称性群的方法不是靠观察去找出它的全部对称性变换,而是用了定理 2 的结果.这不需要高超的观察技巧,它说明了抽象研究的力量.

例 2　回答 §2 的例 4 中提出的问题:用 S_4 去变

$$f(x_1,x_2,x_3,x_4) = x_1x_2 + x_3x_4 \tag{3}$$

能变出几个元素?

这个数目正是轨道长 $|O_f|$.这时是群 S_4 作用在域 F 上 x_1,x_2,x_3,x_4 的全部多项式的集合上.(3) 中 $f(x_1,x_2,x_3,x_4)$ 的稳定化子正是它的对称性群 S_f.在 §2 中已经计算过它有 8 个元素.定理 2 的推论说明

$$|O_f| = [S_4:S_f] = |S_4| \div |S_f| = 24 \div 8 = 3.$$

这正是 §2 的例 4 中给出过的答案.

我们取

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

则

$$x_1x_2 + x_3x_4,$$

$$\sigma \circ (x_1x_2 + x_3x_4) = x_1x_3 + x_2x_4,$$

$$\tau \circ (x_1x_2 + x_3x_4) = x_1x_4 + x_2x_3$$

是 O_f 中的全部元素.

上面关于 S_4 在过 $x_1x_2 + x_3x_4$ 的轨道的结果可用来解决下述已知一根求多项式方程的问题.

例 3 设 x_1,x_2,x_3,x_4 是域 F 上多项式 $x^4+a_1x^3+a_2x^2+a_3x+a_4$ 的四个根,求 F 上的一个多项式以 $x_1x_2+x_3x_4$ 为一个根.

解 由根与系数的关系知

$$\begin{cases} x_1+x_2+x_3+x_4=-a_1 \\ x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_3x_4=a_2 \\ x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4=-a_3 \\ x_1x_2x_3x_4=a_4. \end{cases} \tag{4}$$

S_4 作用在 $x_1x_2+x_3x_4$ 上所得轨道由

$$x_1x_2+x_3x_4=a_1,\quad x_1x_3+x_2x_4=a_2,\quad x_1x_4+x_2x_3=a_3$$

组成.作多项式

$$\begin{aligned}&(x-a_1)(x-a_2)(x-a_3)\\ &=x^3-(a_1+a_2+a_3)x^2+(a_1a_2+a_1a_3+a_2a_3)x-a_1a_2a_3,\end{aligned}$$

易计算出

$$\begin{aligned}&a_1+a_2+a_3=a_2,\\ &a_1a_2+a_1a_3+a_2a_3=a_1a_3-4a_4,\\ &a_1a_2a_3=a_3^2+a_1^2a_4-4a_2a_4,\end{aligned}$$

故得

$$\begin{aligned}&(x-a_1)(x-a_2)(x-a_3)\\ &=x^3-a_2x^2+(a_1a_3-4a_4)x-(a_3^2+a_1^2a_4-4a_2a_4)\end{aligned}$$

是 F 上三次多项式,它以 $x_1x_2+x_3x_4$ 为一个根.

一般地,设 F 上 n 次多项式 $f(x)$ 有 n 个根 $a_1,\cdots,a_n$.取 F 上 n 元多项式 $\rho(x_1,\cdots,x_n)$.设 S_n 作用在 $\rho(x_1,\cdots,x_n)$ 上所得轨道 O_ρ 的长度为 k,其元素 $\rho_1(x_1,\cdots,x_n)=\rho(x_1,\cdots,x_n),\rho_2(x_1,\cdots,x_n),\cdots,\rho_k(x_1,\cdots,x_n)$,则

$$(x-\rho_1(a_1,\cdots,a_n))(x-\rho_2(a_1,\cdots,a_n))\cdots(x-\rho_k(a_1,\cdots,a_n))$$

是 F 上的一个 k 次多项式,它以 $\rho(a_1,\cdots,a_n)$ 为根.有兴趣的读者可自己证明这一结论(证明中要用到高等代数中对称多项式的基本定理).

下面再来考察有限群 G 在自身上的共轭作用(§4 例 8).

定义 5 群 G 在自身上作共轭作用的轨道叫做 G 的一个**共轭类**.

由 §5 定理 2 式知,G 是它的全部不同(也就互不相交)的共轭类的并.记 G 的含元素 x 的共轭类为 C_x,而 G 的全部共轭类为 $C_{x_1},\cdots,C_{x_n}$,则

$$G=\bigcup_{i=1}^{n}C_{x_i}. \tag{5}$$

定义 6 G 的元素 x 在 G 的共轭作用下的稳定化子称为 x 在 G 中的**中**

心化子，记为 $C_G(x)$，

$$C_G(x) = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid xg = gx\}.$$

定理 3（类长与类方程） G 中含 x 的共轭类中的元素数目即类长 $|C_i|$ 等于 $[G:C_G(x)]$. 设 $C_{x_1}, \cdots, C_{x_n}$ 是 G 的全部共轭类，也即 $(x_1, \cdots, x_n)$ 是 G 的全体共轭类的一组代表元，则

$$|G| = \sum_{i=1}^{n} [G:C_G(x_i)]. \tag{6}$$

证明 由定理 2 的推论及(5)式得出.

设共轭类 C_i 仅有一个元素，则 $\forall g \in G, gxg^{-1} = x$ 或 $gx = xg$. 即 x 与 G 的所有元素都交换.

定义 7 令 $Z(G)$ 是与 G 的全部元素都交换的全体元素的集合，即

$$Z(G) = \{g \in G \mid gxg^{-1} = x, \forall x \in G\}.$$

称 $Z(G)$ 为 G 的中心.

中心是 G 的子群(读者自证).

设 G 中元素多于一个的全部共轭类为 $C_{y_1}, \cdots, C_{y_m}$，$Z(G)$ 中的每个元素组成一个元素的共轭类，则类方程(6)可改写成

$$|G| = |Z(G)| + \sum_{i=1}^{m} [G:C_G(y_i)]. \tag{7}$$

当 G 是交换群时，$G = Z(G)$. G 中每个共轭类中只有一个元素.

小结 从 §4 到 §6 我们介绍了群在集合上的作用的概念及初步应用. 群在集合上的作用是一种群同态. 我们介绍了在几何，线性代数中的群作用一些例子. 群作用将集合划分成轨道的无交并，用到有限群的左(或右)乘作用上就得到有限群中基本的 Lagrange 定理. 介绍了稳定化子的概念，用到有限群的群作用上可得轨道长的公式. 用到有限群的共轭作用上就得到共轭类长的公式和有限群类长的方程. 从这三节内容可见群作用的基本重要性.

习 题

1. G 是群，H 是 G 的子群. $x, y \in G$，则 x, y 属于 H 的同一左陪集当且仅当 $x^{-1}y \in H$.

2. 群 G 作用于集合 M 上，$x \in M$. 证明：(1) 稳定化子 $\mathrm{Stab}_G(x)$ 是子群. (2) 设 $g_1, g_2 \in G$，则 $g_1 \circ x = g_2 \circ x$ 当且仅当 g_1, g_2 属于 $\mathrm{Stab}_G(x)$ 的同一左陪集.

3. V 是域 F 上 n 维线性空间，取定 V 的一组基 $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n$. V 上任一可逆线性变换 $\mathbb{A}$，设它在 $\varepsilon_1, \cdots, \varepsilon_n$ 下矩阵为 A，则建立起 $GL(V)$ 到 $GL_n(F)$ 的

同构，$\mathbb{A}\dashrightarrow A$. 于是群 $GL_n(F)$ 通过 $GL(V)$ 可作用于空间 V 上，进而可作用于 V 的子空间的集合 M 上.

(1) $GL_n(F)$ 在 ε_1 处的稳定化子由哪些元素组成?

(2) 令 W 是由 $\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_k$，$k\leqslant n$，生成的子空间，$GL_n(F)$ 在 W 处的稳定化子由哪些元素组成?

4. 正四面体 $A_1A_2A_3A_4$ 的对称性群 G 可作用在它的顶点的集合和它的面的集合上，也作用在它的棱的集合上. (1) 试决定 G 在顶点 A_1 处的稳定化子；(2) 求 G 在面 $A_2A_3A_4$ 处的稳定化子；(3) 求 G 在棱 A_1A_2 处的稳定化子.

5. 把正四面体 $A_1A_2A_3A_4$ 的对称性群用顶点的置换表出. 利用 §6 定理 2 中公式(2) 写出它的对称性群的全部元素. 再回到四面体上考察每个置换代表什么正交变换.

6. 试决定 §5 习题 5 中群作用过 tH 的轨道及在 tH 处的稳定化子. 并证明 $|KtH| = [K:K\cap tHt^{-1}]|H|$.

7. S_3 中 $C_3=\{e,(1\,2\,3),(1\,3\,2)\}$ 组成 S_3 的子群. 写出 S_3 中 C_3 的全部左陪集和全部右陪集.

8. S_4 中写出子群 $S_3=\left\{\begin{pmatrix}1&2&3&4\\ i_1&i_2&i_3&4\end{pmatrix}\middle|\, i_1i_2i_3 \text{是}1\,2\,3\text{的全部排列}\right\}$ 的全部左陪集.

9. G 是群，H 是子群. 当 G 是交换群时，H 的任一左陪集都是一个右陪集.

10. 写出 $\mathbb{Z}$ 中子群 $3\mathbb{Z}=\{3k\mid k\in\mathbb{Z}\}$ 的全部左陪集.

11. 证明任意 $l,k\in\mathbb{Z}$ 属于 $n\mathbb{Z}$ 在 $\mathbb{Z}$ 中同一陪集的充分必要条件为 $l\equiv k(\mathrm{mod}\ n)$. 写出 $\mathbb{Z}$ 中 $n\mathbb{Z}$ 的全部陪集.

12. S_3 作用在域 F 上全部多项式 $f(x_1,x_2,x_3)$ 的集合上. 求 S_3 在 $x_1^3x_2^2x_3$ 和 $x_1x_2+x_2x_3$ 处的稳定化子及 S_3 作用下分别过 $x_1^3x_2^2x_3$ 和 $x_1x_2+x_2x_3$ 的轨道.

13. 有限群 G 称为 p 群，如果它的阶是素数 p 的方幂. 证明 G 的非单位元子群的阶能被 p 除尽，及 G 对于其真子群(即不等于 G 的子群) 的指数也被 p 除尽.

14. 有限群 G 为 p 群，则 G 的中心 $Z(G)\neq\{e\}$. (利用改进的类方程(7)).

15. $G=S_3$ 共轭作用于自身. 求中心化子 $C_G(\sigma)$，其中 σ 分别是 $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ 和 $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$.

16. 求 S_3 的含上题中 $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ 和 $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$ 的共轭类.

17. G 是素数 p 阶的群,则(1) G 除本身和单位元群以外没有其它子群. (2) $G = \langle a\rangle$, $\forall a \neq e$. 即 G 是循环群.(见 §3 定义 4 前一段).

18. G 作用在集合 M 上. $x \in M$, $g \in G$, 及 $g \circ x = y$, 则 $\mathrm{Stab}_G(y) = g\mathrm{Stab}_G(x)g^{-1}$.

19. G 是有限群, $H \subset K$ 皆是 G 的子群, 则 $[G:H] = [G:K][K:H]$.

20. 有限群 G 是 p 群, $p \nmid m$. G 在 M 上有群作用, 且 $|M| = m$, 则 G 在 M 上有不动元.

§7 循环群与交换群

循环群与交换群是最简单的群. 我们来研究它们的结构与性质.

定理 1 设 G 是群, $a \in G$. 当 a 的任意两个方幂皆不相等时,

$$\langle a\rangle = \{\cdots a^{-m}, a^{-(m-1)}, \cdots, a^{-1}, a^0 = e, a, \cdots, a^{m-1}, a^m, \cdots\}$$

有无限个元. 当 a 有两个幂相等时, 必有 n 为正整数, 使 $\langle a\rangle = \{a, a^2, \cdots, a^n = e\}$, 其中任意两个幂互不相同. 这时 $\langle a\rangle$ 的阶为 n, 称为 a 的**阶**, 记作 $o(a)$, 故 $o(a) \mid |G|$.

证明 前半部的结论是显然的.

当 a 有两个幂相等时, 设 $a^k = a^l$, $l > k$, 则 $a^{l-k} = e$, $l - k > 0$. 取最小的正整数 n, 使 $a^n = e$. 对 a 的任一幂 a^k, 令 $k = ln + s$, $0 \leqslant s < n$. 则

$$a^k = a^{ln+s} = (a^n)^l \cdot a^s = a^s \in \{a, a^2, \cdots, a^{n-1}, e = a^n\}.$$

故 $\langle a\rangle = \{a, a^2, \cdots, a^{n-1}, e = a^n\}$. 对其中任意两个幂 a^k 及 a^l, 设 $l > k > 0$, 则 $n > l - k > 0$. 故 $a^{l-k} \neq e$, 即 $a^l \neq a^k$.

由 Lagrange 定理(§6 定理 1) 知 $|\langle a\rangle| \mid |G|$, 即 $o(a) \mid |G|$.

推论 设 G 为有限群, 则最小的使 $a^n = e$ 的正整数 n 是 a 的阶, 且 $a^k = e$ 当且仅当 $n \mid k$. 特别地, $a^{|G|} = e$.

证明 由定理 1 得第一个结论, 进而当 $n \mid k$ 时, $a^k = e$. 特别地, $a^{|G|} = e$. 现设 $a^k = e$, 令 $k = tn + s$, $0 \leqslant s < n$. 若 $s \neq 0$, 则

$$a^s = a^{k-tn} = a^k \cdot (a^n)^{-t} = e.$$

而 $s < n$, 这与 n 是使 $a^n = e$ 成立的最小正整数矛盾. 故 $s = 0$, $n \mid k$.

命题 2 无限阶循环群 G 与整数加法群 $\mathbb{Z}$ 同构. 两个有限循环群 G_1, G_2 同构当且仅当 $|G_1| = |G_2|$.

证明 设 $G = \langle a\rangle = \{a^k \mid k \in \mathbb{Z}\}$ 是无限阶群, 作映射

$$G \xrightarrow{\varphi} \mathbb{Z}$$
$$a^k \longmapsto k.$$

由于 a 的任何两个幂不相等，故 φ 有定义，且是一一对应. 又

$$\varphi(a^m \cdot a^n) = \varphi(a^{m+n}) = m + n = \varphi(a^m) + \varphi(a^n),$$

故 φ 保持运算，因而是同构.

对有限循环群 G_1, G_2，若它们同构，显然 $|G_1| = |G_2|$. 令 $G_i = \langle a_i \rangle$.

现设 $|G_1| = |G_2| = n$，则由定理 1 可知

$$G_i = \langle a_i \rangle = \{a_i, a_i^2, \cdots, a_i^{n-1}, a_i^n = e_{G_i}\} \quad (i = 1,2),$$

其中 a_i 的各个幂 a_i^k，$1 \leqslant k \leqslant n$，是不同的，$i = 1,2$. 作映射

$$G_1 \xrightarrow{\varphi} G_2$$
$$a_1^k \longmapsto a_2^k, \qquad k = 1,2,\cdots,n.$$

φ 是一一对应. 又对 $\forall k \in \mathbb{Z}$，显然也有 $\varphi(a_1^k) = a_2^k$，故：$\forall m, l \in \mathbb{Z}$，

$$\varphi(a_1^m \cdot a_1^l) = \varphi(a_1^{m+l}) = a_2^{m+l} = a_2^m \cdot a_2^l = \varphi(a_1^m) \cdot \varphi(a_1^l).$$

φ 保持运算，这证明了 G_1 与 G_2 同构.

下面要定出循环群 G 的全部子群.

定理3 循环群 $G = \langle a \rangle$ 的子群是循环群. 若 $\langle a \rangle$ 是无限群，则除 $\{e\}$ 外，其它的子群皆为无限群，其形式为 $\langle a^s \rangle$，s 为大于零的整数. 若 $\langle a \rangle$ 是 n 阶群，则它的子群的阶为 n 的因子，且对 n 的每个因子 q，有且仅有一个 q 阶子群，其形式为 $\langle a^{\frac{n}{q}} \rangle$.

证明 设 $\{e\} \neq H$ 是 $\langle a \rangle$ 的子群，则有 $m \neq 0, a^m \in H$. 又 $(a^m)^{-1} = a^{-m} \in H$，故可设 m 为正整数，使 $a^m \in H$. 取最小的有这种性质的正整数，记为 s. 我们证任意 $a^m \in H$，必有 $s \mid m$. 写 $m = sq + t$，$0 \leqslant t < s$. 若 $t > 0$，则 $a^m = a^{sq+t} = (a^s)^q \cdot a^t$，即有 $a^t = a^m \cdot (a^s)^{-q} \in H$. 但 $0 < t < s$，与 s 的最小性矛盾. 因此 $t = 0$，$s \mid m$. 于是 $a^m = (a^s)^q$. 这就证明了 $H = \langle a^s \rangle$.

当 $\langle a \rangle$ 是无限群时，a 的任何两个幂皆不同，因此

$$\langle a^s \rangle = \{\cdots, a^{-ks}, a^{-(k-1)s}, \cdots, a^{-s}, a^0, a^s, \cdots, a^{(k-1)s}, a^{ks}, \cdots\}$$

有无限个元，是无限群.

当 $|\langle a \rangle| = n$ 时，对 $q \mid n$，令 $s = \dfrac{n}{q}$，作

$$H = \langle a^s \rangle = \{a^s, a^{2s}, \cdots, a^{(q-1)s}, a^{qs} = e\},$$

因 $|\langle a \rangle| = n = sq$，由定理 1，$\{a^s, a^{2s}, \cdots, a^{(q-1)s}, a^{qs} = e\}$ 中任何两个幂不相等. 故 H 是一个 q 阶子群.

又设 H_1 是 q 阶子群. 令 s 是最小正整数，使 $a^s \in H_1$. 在第一部分中已证

了 $H_1 = \langle a^s \rangle$，且对任意正整数 m，若 $a^m \in H_1$，则 $s \mid m$. 特别取 m 为 a 的阶 n，则 $a^n = e \in H_1$，即有 $s \mid n$. 令 $n = ls$，则 $\{a^s, a^{2s}, \cdots, a^{(l-1)s}, a^{ls} = a^n = e\}$ 中元素两两不同(定理 1)，即 l 是使 $(a^s)^l = e$ 的最小的正整数. 因此 l 是 a^s 的阶，也即 $H_1 = \langle a^s \rangle$ 的阶，故 $l = q$. 这样 $H_1 = \langle a^{\frac{n}{q}} \rangle$，即 $\langle a \rangle$ 只有一个 q 阶子群.

在 §10 中讲了同态基本定理以后，我们还要进一步考察循环群的构造.

在循环群之后，最简单的群要数交换群. 这里不能详细讨论交换群的构造，我们只研究有限交换群能成为循环群的条件.

对有限群 G，任意元 $a \in G$，满足 $a^{|G|} = e$. 我们对满足这种关系的最小正整数引入下列定义.

定义 1 G 是有限群，使所有 $a \in G$ 满足 $a^t = e$ 的最小正整数 t，称为 G 的**方次数**，记为 $\exp(G)$.

引理 4 G 是有限交换群，$g, h \in G$，满足 $(o(g), o(h)) = 1$，则

$$o(gh) = o(g)o(h).$$

证明 令 $r = o(gh), m = o(g), n = o(h)$. 由于

$$(gh)^{mn} = g^{mn}h^{mn} = e,$$

从定理 1 的推论得 $r \mid mn$. 又 $e = (gh)^r = g^r h^r$，得 $h^r = g^{-r}$. 由

$$e = (g^m)^{-r} = (g^{-r})^m = (h^r)^m = h^{mr}.$$

定理 1 的推论断言 $n = o(h) \mid mr$. 由 $(m, n) = 1$，故 $n \mid r$. 同样可证 $m \mid r$. 再由 $(m, n) = 1$，知 $mn \mid r$. 前面已证 $r \mid mn$，因此 $r = mn$.

引理 5 设 G 为有限交换群，g 是 G 的有最大阶的元，则

$$\exp(G) = o(g).$$

证明 要证 $\forall h \in G, h^{o(g)} = e$. 设

$$o(g) = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}, o(h) = p_1^{f_1} p_2^{f_2} \cdots p_s^{f_s},$$

$e_i, f_i \geqslant 0$，及 p_i 是不同的素数，$i = 1, 2, \cdots, s$. 若设有 $f_i > e_i$，某 i. 不妨设 $i = 1$. 作 $g_1 = g^{p_1^{e_1}}, h_1 = h^{p_2^{f_2} \cdots p_s^{f_s}}$. $(g_1)^{p_2^{e_2} \cdots p_s^{e_s}} = g^{p_1^{e_1} \cdots p_s^{e_s}} = e$，且对任意正整数 $n < p_2^{e_2} \cdots p_s^{e_s}$，必有

$$p_1^{e_1} \cdot n < p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s} = o(g),$$

而不能有 $(g_1)^n = g^{p_1^{e_1} \cdot n} = e$. 故 $o(g_1) = p_2^{e_2} \cdots p_s^{e_s}$. 同样可证 $o(h_1) = p_1^{f_1}$.

由引理 4 知，

$$o(g_1 h_1) = p_1^{f_1} p_2^{e_2} \cdots p_s^{e_s} > p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s} = o(g)$$

与 $o(g)$ 是最大阶矛盾，故 $f_i \leqslant e_i, i = 1, 2, \cdots, s$. 于是 $h^{o(g)} = (h^{p_1^{f_1} \cdots p_s^{f_s}})^{p_1^{e_1 - f_1} \cdots p_s^{e_s - f_s}} = e$. 即有 $o(g) = \exp(G)$.

定理 6 设 G 是交换群，则 G 是循环群当且仅当 $\exp(G) = |G|$.

证明 设 G 是循环群，则有 $g \in G, G = \langle g \rangle$，则 $|G| = o(g) = \exp(G)$. 反之，设 $G = \exp(G)$，由于引理 5，有 $g \in G, o(g) = \exp(G)$. 于是 $|\langle g \rangle| = o(g) = |G|$，知 $\langle g \rangle = G$. 即 G 是循环群.

下面的定理是很美妙的结果，是域的重要性质.

定理 7 域 F 中的乘法有限子群 G 皆为循环群.

证明 设 $|G| = n$. 若 $n > \exp(G) = m$，则任意 $g \in G$ 满足方程 $g^m = 1$，或 G 中任一元是 $x^m - 1 = 0$ 的根. 即域 F 上的 m 次多项式 $x^m - 1$ 在 F 中至少有 n 个不同的根. 于是域 F 上多项式 $x^m - 1$ 的不同的根的数目 $\geqslant n$ > 它的次数 m. 这是不可能的. 又 $|G| = n$ 总是大于或等于 $\exp(G) = m$ 的，故 $|G| = \exp(G)$. 由定理 6 知，G 是循环群.

习 题

1. G 是 n 阶循环群，$m \mid n$，则方程 $x^m = e$ 在 G 中恰有 m 个解.

2. 循环群的同态象是循环群.

3. G 有 n 阶循环子群当且仅当 G 有 n 阶元. 再证：

(1) G 是素数 p 阶群，则 G 是循环群.

(2) G 是 $2p$ 阶非交换群，p 素数，则 G 必有 p 阶子群.

4. G 是交换群，$g, h \in G$. $o(g) = m, o(h) = n, (m, n) = 1$. 证明：

(1) g, h 生成的子群 $\langle g, h \rangle = \langle gh \rangle$.

(2) $\langle g \rangle \cap \langle h \rangle = e$ 且 $\langle gh \rangle \cong \langle g \rangle \times \langle h \rangle$.

5. $G = \langle a \rangle$ 是 n 阶循环群，则

(1) $\langle a^m \rangle = \langle a \rangle$ 当且仅当 $(m, n) = 1$.

(2) 当 $(m, n) = d$ 时，$\langle a^m \rangle = \langle a^d \rangle$.

6. G 的阶是 p 的方幂，p 是素数，则 G 中有 p 阶元.

7. G 是交换群，则 G 中有限阶元素的集合组成 G 的子群.

8. G 是群，则 $o(a) = o(a^{-1}), o(ab) = o(ba), \forall c \in G, o(a) = o(cac^{-1})$.

9. $l\mathbb{Z} \cap k\mathbb{Z} = [l, k]\mathbb{Z}, l\mathbb{Z} + k\mathbb{Z} = (l, k)\mathbb{Z}$，其中 $[l, k]$ 为 l, k 的最小公倍数.

§8 正规子群和商群

设 G 是一个群，H 是它的一个子群. 令 I 是 G 的全部左陪集的代表元集，

则

$$G = \bigcup_{g \in I} gH$$

是 G 的全部左陪集的无交并. 提出下列问题:能否在全体左陪集的集合上建立一个乘法运算使它成为一个群呢?

实际上在群 G 的子集之间是有自然的乘法的.

定义 1 K, L 是群 G 的两个非空子集,称集合

$$KL = \{kl \mid k \in K, l \in L\}$$

为 K 与 L 的**集合乘积**.

易知,这个乘法有结合律,即 $K(LM) = (KL)M$. 问题是这个乘法对于左陪集的集合是否封闭呢?即任给两个左陪集合 g_1H 及 g_2H,它们的乘积是否是一个左陪集呢?由于 g_1H 中有 g_1,g_2H 中有 g_2,因此 $(g_1H)(g_2H)$ 中有元素 g_1g_2. 于是若要 $(g_1H)(g_2H)$ 等于一个左陪集,就必须是 g_1g_2 所在的左陪集 $(g_1g_2)H$.

命题 1 G 是群,H 是 G 的一个子群,则 $\forall g_1, g_2 \in G, (g_1H)(g_2H) = g_1g_2H$ 当且仅当 $\forall g_2 \in G, Hg_2 = g_2H$,或当且仅当 $\forall g_2 \in G, g_2^{-1}Hg_2 = H$.

证明 首先设 $\forall g_1, g_2 \in G$,有 $(g_1H)(g_2H) = (g_1g_2)H$,则用 g_1^{-1} 乘两端,就得 $Hg_2H = g_2H$. 左端 $= \bigcup_{h \in H} Hg_2h = g_2H$. 在中间项中取 $h = e$,则 $Hg_2e = Hg_2 \subseteq g_2H$. 即 $\forall g_2 \in G$,有 $Hg_2 \subseteq g_2H$. 同样 $\forall g_2^{-1} \in G$,有 $Hg_2^{-1} \subseteq g_2^{-1}H$. 于是 $g_2H \subseteq Hg_2$,就得 $g_2H = Hg_2$.

反之,设 $\forall g_2 \in G, Hg_2 = g_2H$. 由于 H 是子群,$HH = H$. 故 $Hg_2H = g_2HH = g_2H$. 进而 $\forall g_1 \in G$,用 g_1 左乘它的两端,则 $\forall g_1, g_2 \in G$,$(g_1H)(g_2H) = (g_1g_2)H$.

第二个当且仅当是显然的.

定义 2 G 是群,H 是 G 的子群. 若 $\forall g \in G$,有 $g^{-1}Hg = H$,则称 H 为 G 的**正规子群**. 记为 $H \lhd G$.

由命题 1,对 H 是正规子群,它的任一个左陪集也是右陪集,我们简称为 G 的陪集. 而且 G 的子集间的乘法对于陪集的集合是封闭的以及 $\forall g_1, g_2 \in G, (g_1H)(g_2H) = g_1g_2H$.

命题 2 设 G 是群,$H \lhd G$. 记 H 对 G 的陪集的集合为

$$\frac{G}{H} = \{gH \mid g \in G\},$$

则 $\frac{G}{H}$ 对于陪集的乘积成为一个群,称为 G 对 H 的**商群**.

证明 首先$\frac{G}{H}$对于上述乘法是封闭的，且已知这乘法满足结合律.

陪集 $H = eH$ 是它的单位元，$eHgH = egH = gH$，$\forall g \in H$. 又任意 gH，有 $g^{-1}Hgh = eH = gHg^{-1}H$. 即 $g^{-1}H$ 是 gH 的逆元. 这就完成了证明.

当 H 在上下文中是给定时，我们也常写$\frac{G}{H}$为$\bar{G}$，而元素 gH 写为$\bar{g}$. 注意，不同的 g, g' 可以有$\bar{g} = \bar{g'}$. 这时表示 $gH = g'H$，即 g, g' 在 H 的同一陪集中. 由于 $g_1Hg_2H = g_1g_2H$，故 $g_1\bar{g}_2 = \overline{g_1g_2}$.

例 1 单位元群$\langle e\rangle$及群 G 本身都是 G 的正规子群. 当 G 是交换群时，它的任一子群都是正规子群.

例 2 对整数加法群 $\mathbb{Z}$，它的任一子群为$\langle n\rangle$（§7 定理 3），也即 $n\mathbb{Z}$. 加群的陪集形为 $k + n\mathbb{Z}$. $\mathbb{Z}$ 的对于子群 $n\mathbb{Z}$ 的商群为

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \cdots, (n-1) + n\mathbb{Z}\}.$$

$k + n\mathbb{Z}$ 是 $\mathbb{Z}$ 中用 n 去除，其余数与 k 的余数相同的全体整数的集合. 故 $\mathbb{Z}$ 对 $n\mathbb{Z}$ 的陪集也常称为模 n 的**同余类或剩余类**. $\frac{\mathbb{Z}}{n\mathbb{Z}}$是 $\mathbb{Z}$ 的模 n 的剩余类的加法群.

例 3 $F[x]$ 是域 F 上多项式环，考虑它的加法群. 任取 $f(x) \in F[x]$，作 $F[x]$ 的加法子群 $f(x)F[x]$（$F[x]$ 中 $f(x)$ 的全体多项式倍数），它也是正规子群，则可作商群$\frac{F[x]}{f(x)F[x]}$. 设 $f(x)$ 为 n 次多项式，则对任一陪集 $p(x) + f(x)F[x]$，作 $p(x)$ 被 $f(x)$ 除所得余式 $r(x)$. 由 $p(x) = q(x)f(x) + r(x)$，而有

$$p(x) + f(x)F[x] = r(x) + f(x)F[x].$$

$p(x) + f(x)F[x]$ 是 $F[x]$ 中用 $f(x)$ 去除，其余式与 $p(x)$ 的余式相同的多项式的全体. 故也称 $F[x]$ 对 $f(x)F[x]$ 的陪集为模 $f(x)$ 的**同余类或剩余类**. $\frac{F[x]}{f(x)F[x]}$ 是 $F[x]$ 的模 $f(x)$ 的剩余类的加法群. 易知

$$\frac{F[x]}{f(x)F[x]} = \{a_0x^{n-1} + a_1x^{n-2} + \cdots + a_{n-2}x + a_{n-1} \mid a_i \in F\}.$$

通过商群可以反映原群的一些性质. 例如，有限群 $G, H \lhd G$. 设 $[G:H] = s$. $\forall g \in G, \bar{g} \in G = \frac{G}{H}$. 因 $|\bar{G}| = s$，$\bar{g}^s = \overline{g^s} = \bar{e}$，又由于 $(gH)^s = g^sH$ 及 §7 定理 1 的推论，故 $g^s \in H$. 这个性质通过商群就很容易得到证明. 这种方法是群论中常用的.

例 4 令 C_p 是素数 p 阶循环群. 比如 C_p 是平面绕点 O 旋转 $n \cdot \frac{2\pi}{p}$ 角，

$0 \leqslant n \leqslant p-1$,的全体旋转所成的群.绕 O 转 $\frac{2\pi}{p}$ 角的旋转 T 是它的生成元. $C_p = \{T^n \mid 0 \leqslant n \leqslant p-1\}$. C_p 的子群的阶 q 必须满足 $q \mid p$. p 是素数,故 $q = 1$ 或 p.即 C_p 除了单位元素的群和自身外没有其它的子群,更没有其它的正规子群.

这时 C_p 只可以作出两个商群:

$$\frac{C_p}{C_p} = \{e \cdot C_p\} \cong \langle e \rangle,$$

$$\frac{C_p}{\langle e \rangle} = \{T^n \langle e \rangle \mid 0 \leqslant n \leqslant p-1\} \cong C_p.$$

一般说来,商群比原群简单些(至少商群元素的数目比较少,而乘法运算是原群的乘法运算的继承).像 C_p 这样的群,由于没有非平凡的正规子群,作不出非平凡的商群.从结构上看是不太好"化简"的群.

定义 3 若群 G 没有非平凡的正规子群(即除 G 和 $\langle e \rangle$ 外没有其它的正规子群),就称为**单群**.

素数阶循环群 C_p 就是一类单群.任意单群只是从商群方式不能化简其结构的群,并不表示其结构简单.实际上从 Galois 那时就知,A_5(5 次交错群)就是 60 阶单群.以后就逐步知道了更多的有限阶单群.经过一百多年成百位数学家的努力,目前公认为已经找出了所有的**有限单群**.用数学术语说是完成了有限单群的分类.可惜的是这个证明太长(要用若干本书),至今还未完全写出来.但可以看出有限单群的结构也是非常复杂的.有限群论中有一种理论叫群扩张,是通过商群去构造原群.和用砖造房子相比,在这种理论中有限阶单群就好比是有限群论中的"建筑块".

习 题

1. G 的指数为 2 的子群 H 是正规子群.

2. G 的中心 $Z(G)$ 是正规子群.

3. 证明 S_3 中的子群 $\left\{e, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\right\}$ 不是正规子群, $\left\{e, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right\}$ 是正规子群.

4. 证明 S_4 中 V_4(见 §2 习题 5)是正规子群.

5. $GL_n(F)$ 中子群 $SL_n(F)$ 是正规子群及全部 $n \times n$ 数量矩阵的集合组成正规子群.

6. G 是群，$H_1, H_2, \cdots, H_k, \cdots$ 皆为 G 的正规子群，则 $\bigcap_{i=1}^{\infty} H_k$ 是 G 的正规子群.

7. G 是群，H 是子群，则 $\bigcap_{x \in G} xHx^{-1}$ 是 G 的正规子群.

8. 证明 S_3 是唯一的非交换 6 阶群.

9. S_4 中 $\left\{e, \begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 1 & 4\end{pmatrix}, \begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 1 & 2 & 4\end{pmatrix}\right\}$ 是正规子群吗?

10. 设 G 是有限群，$n \mid |G|$，且 G 中仅有一个 n 阶子群 H，则 H 是 G 的正规子群.

11. 确定 $\frac{\mathbb{Z}}{3\mathbb{Z}}, \frac{\mathbb{Z}}{6\mathbb{Z}}$ 的加法表. 写出 $\frac{\mathbb{Z}}{n\mathbb{Z}}$ 的全部元素.

12. F_2 是二元域，确定 $\frac{F_2[x]}{(x^2+1)}, \frac{F_2[x]}{(x^3+x^2+x+1)}$ 的加法表. $f(x)$ 是域 F 上 n 次多项式，写出 $\frac{F_2[x]}{f(x)}$ 的全部元素.

13. F 是域，写出 $\frac{GL_n(F)}{SL_n(F)}$ 的全部元素.

14. $G = \{(a,b) \mid a, b \in \mathbb{R}, a \neq 0\} = \mathbb{R}^* \times \mathbb{R}$，其中 $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$，对乘法 $(a,b)(c,d) = (ac, ad+b)$ 成为群（§1 习题 6）. 证明

$$K = \{(1,b) \mid b \in \mathbb{R}\}$$

是 G 的正规子群，且 $\frac{G}{K} \cong \mathbb{R}^*$ 的乘法群.

15. G 是群，H 是子群. $C_G(H)$ 及 $N_G(H)$ 分别是 H 的中心化子及正规化子.（见 27 页习题 4）证明：

(1) $C_G(H)$ 是 $N_G(H)$ 的正规子群.

(2) $N_G(H)$ 到 H 的自同构群 Aut H 有同态映射

$$N_G(H) \longrightarrow \text{Aut } H$$

$$n \longmapsto \tau_n: \quad \tau_n(h) = nhn^{-1}, \forall\, h \in H.$$

(3) $\forall\, n_1, n_2 \in N_G(H)$，$\tau_{n_1} = \tau_{n_2}$ 当且仅当 $n_2 \in n_1 C_G(H)$.

(4) 映射

$$N_G(H)/C_G(H) \longrightarrow \text{Aut } H$$

$$nC_G(H) \longmapsto \tau_n$$

是群的单同态.

16. $G = \langle a \rangle$ 是 n 阶循环群，$\mathbb{Z}$ 是整数加法群. 证明：

(1) 映射

$$\mathbb{Z} \xrightarrow{\tau} G$$

$$m \longmapsto a^m$$

是群同态.

(2) $\forall k, m \in \mathbb{Z}, \tau(k) = \tau(m)$ 当且仅当 $k \in m + n\mathbb{Z}$.

(3) 映射

$$\frac{\mathbb{Z}}{n\mathbb{Z}} \to G = \langle a \rangle$$

是群同构.

17. G 是 p^2 阶群，p 是素数，则 G 是交换群. 进而证明只有两个(不同构的) p^2 阶的群. (提示：若 $G \neq Z(G)$，则有 $g \in Z(G)$，使 $G = \bigcup_{i=1}^{p} g^i Z(G)$).

18. 若 $\frac{G}{Z(G)}$ 是循环群，则 G 是交换群.

19. G 是群，H 是循环子群且在 G 中正规，则 H 的子群在 G 中都正规.

20. 令 D_n 是平面上正 n 边形的对称性群. 当 n 为奇数时，$Z(D_n)$ 为 $\{e\}$，当 n 为偶数时，$Z(D_n)$ 为 2 阶群.

21. G 是群，$H_1, H_2, \cdots, H_k, \cdots$ 是 G 的子群. K 是 G 的正规子群，$K \subset H_k, k = 1, 2, \cdots$，则

$$\bigcap_{k=1}^{\infty} \left(\frac{H_k}{K}\right) = \frac{\left(\bigcap_{k=1}^{\infty} H_k\right)}{K}.$$

§9　n 元交错群 A_n，A_n，$n \geqslant 5$，的单性

n 元交错群 A_n，当 $n \geqslant 5$ 时是有限单群. 这一节的目标就是定义 A_n，并证明上述结论. A_n 是 n 元对称群 S_n 中全部所谓偶置换组成的子群. 我们先来建立偶置换的定义.

定义 1　下述 n 元置换

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & i & \cdots & j & \cdots & n \\ 1 & 2 & \cdots & j & \cdots & i & \cdots & n \end{pmatrix}$$

称为一个**对换**，它仅把 $i \to j, j \to i$，即 i, j 互换而其它元素不动. 我们把这个置换简记为 (ij).

命题 1　设 n 元置换

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ l_1 & l_2 & \cdots & l_n \end{pmatrix}.$$

若将排列 $l_1 l_2 \cdots l_i \cdots l_j \cdots l_n$ 进行一个对换，使 l_i 与 l_j 互换位置，则

$$\begin{pmatrix} 1 & 2 & \cdots & i & \cdots & j & \cdots & n \\ l_1 & l_2 & \cdots & l_j & \cdots & l_i & \cdots & l_n \end{pmatrix}$$

$$(i_j l_j)\begin{pmatrix}1 & 2 & \cdots & i & \cdots & j & \cdots & n\\ l_1 & l_2 & \cdots & l_i & \cdots & l_j & \cdots & l_n\end{pmatrix}.$$

证明 按置换乘积的定义.

推论 任一 n 元置换 σ 可表成若干个对换的乘积，σ 的每一种这样的表示方法中的对换数目可以不同，但数目的奇偶性由 σ 唯一决定. 设

$$\sigma = \begin{pmatrix}1 & 2 & \cdots & n\\ l_1 & l_2 & \cdots & l_n\end{pmatrix},$$

则 σ 的奇偶性与排列 $l_1 l_2 \cdots l_n$ 的逆序数的奇偶性一样.

证明 令

$$\tau = \begin{pmatrix}1 & 2 & \cdots & n\\ 1 & 2 & \cdots & n\end{pmatrix}.$$

由高等代数中知道可用一系列对换，将排列 $1\,2\cdots n$ 变成 $l_1 l_2 \cdots l_n$. 设所用的对换依次为 $(i_1 j_1), \cdots, (i_k j_k)$. 由命题 1 有

$$\sigma = (i_k j_k)\cdots(i_1 j_1)\tau = (i_k j_k)\cdots(i_1 j_1),$$

就将 σ 表成为若干对换的乘积. 设有另一种表示法

$$\sigma = (m_s n_s)\cdots(m_1 n_1) = (m_s n_s)\cdots(m_1 n_1)\tau.$$

仍由命题 1，这些对换将排列 $1\,2\cdots n$ 变成 $l_1 \cdots l_n$. 由高等代数知道 s 与 k 有相同的奇偶性，并与排列 $l_1 \cdots l_n$ 的逆序数的奇偶性一样.

定义 2 n 元置换

$$\sigma = \begin{pmatrix}1 & 2 & \cdots & n\\ l_1 & l_2 & \cdots & l_n\end{pmatrix}$$

中排列 $l_1 \cdots l_n$ 是奇排列(有奇数个逆序)时称为**奇置换**，是偶排列时(有偶数个逆序)称为**偶置换**.

定理 2 n 元对称群 S_n 中的全部偶置换组成 S_n 的一个子群称为 n 元**交错群**，记为 A_n，并且 $A_n \lhd S_n$.

证明 偶置换是偶数个对换的乘积. 设 $\sigma = (i_{2k} j_{2k})\cdots(i_1 j_1)$ 是偶置换，于是

$$\sigma^{-1} = (i_1 j_1)^{-1}\cdots(i_{2k} j_{2k})^{-1}$$
$$= (i_1 j_1)\cdots(i_{2k} j_{2k})$$

(注意：对换的逆元就是自身)，故 σ^{-1} 也是偶置换. 任给 $\sigma, \tau \in A_n$，由 σ, τ^{-1} 都是偶数个对换的乘积，于是 $\sigma\tau^{-1}$ 也是偶数个对换的乘积，因而 $\sigma\tau^{-1} \in A_n$. 由 §3 命题 1 知，A_n 是 S_n 的子群.

又任给 $\tau \in S_n$，$\sigma \in A_n$. τ 及 τ^{-1} 可表成相同数目的对换的乘积，而 σ 是偶数个对换的乘积，故 $\tau^{-1}\sigma\tau$ 可表成偶数个对换的乘积. 因此 $\forall\, \tau \in S_n$，$\tau^{-1}\sigma\tau$

$\in A_n$ 及 $\tau^{-1}A_n\tau \subseteq A_n$. 这证明了 $A_n \lhd S_n$.

还可证 S_n 对于 A_n 的陪集分解中只有两个陪集，故 $[S_n : A_n] = 2$（留作习题）.

为了证明 A_n，$n \geqslant 5$ 时是单群，需介绍置换的轮换表示法，它在置换的运算中也是一种重要的表示方法. 先看一个例子.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 5 & 4 & 6 \end{pmatrix},$$

其中 1 变成 3，3 变成 2，2 又变成 1；4 变成 5，5 又变成 4；6 变成 6. 这种循环变换关系使我们能把 σ 记为

$$\sigma = (1\ \ 3\ \ 2)(4\ \ 5)(6).$$

每个括弧表示一个循环变换关系，叫做一个**轮换**. 虽然 $(1\ \ 3\ \ 2)$ 只在 1，3，2 上作循环变换，它仍是 $\{1,2,\cdots,6\}$ 上的一个置换

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 5 & 6 \end{pmatrix}.$$

将 $(4\ \ 5)$，(6) 也看成 $\{1,2,\cdots,6\}$ 上的置换，则 $(1\ \ 3\ \ 2)(4\ \ 5)(6)$ 也就可看成 $\{1,2,\cdots,6\}$ 上三个置换的乘积，且这三个置换各自变动的元素集合是互不相交的. 它们的置换作用是互相独立的，于是它们的乘积可任意交换次序. 例如

$$(1\ \ 3\ \ 2)(4\ \ 5)(6) = (6)(4\ \ 5)(1\ \ 3\ \ 2).$$

命题 3 任意 n 元置换可表成若干不相交的（的子集上的）轮换的乘积，且除去在乘积中的次序外这些轮换是唯一决定的.

证明 对 n 元置换 σ，任取 $\alpha_1 \in \{1,2,\cdots,n\}$，用 σ 连续作用它得序列

$$\sigma(\alpha_1) = \alpha_2, \sigma(\alpha_2) = \alpha_3, \cdots, \alpha_i \in \{1,2,\cdots,n\}.$$

这个序列中的元不能永远不同. 设第一次重复前面元素的元是 α_j，而与前面的元 α_i，$i < j$，相同，$\alpha_i = \alpha_j$. 而 $\alpha_1, \cdots, \alpha_{j-1}$ 各不相同. 若 $i > 1$，则 $\sigma(\alpha_{i-1}) = \alpha_i = \alpha_j$ 及 $\sigma(\alpha_{j-1}) = \alpha_j$. 由于 σ 是双射，则 $\alpha_{i-1} = \alpha_{j-1}$，矛盾. 故 $i = 1$. 即

$$\sigma(\alpha_1) = \alpha_2, \sigma(\alpha_2) = \alpha_3, \cdots, \sigma(\alpha_{j-1}) = \alpha_1.$$

考察

$$\{1,2,\cdots,n\} = \{\alpha_1, \alpha_2, \cdots, \alpha_{j-1}\} \cup (\{1,2,\cdots,n\} \setminus \{\alpha_1, \alpha_2, \cdots, \alpha_{j-1}\})$$
$$= \{\alpha_1, \alpha_2, \cdots, \alpha_{j-1}\} \cup I.$$

σ 将 $\{\alpha_1, \alpha_2, \cdots, \alpha_{j-1}\}$ 变到自己. 由于 σ 是双射，σ 不能将 I 的元变到 $\{\alpha_1, \alpha_2, \cdots, \alpha_{j-1}\}$ 中. 故 σ 在 I 上引起置换，对置换的元素的数目作归纳法，可知能将 I 分成几个不相交的子集的并集

$$\{\alpha_j, \cdots, \alpha_{l-1}\} \cup \cdots \cup \{\alpha_r, \cdots, \alpha_n\},$$

其中 $j < l < \cdots < r \leqslant n$. σ 在每个子集上是循环变换. 于是 $\{1,2,\cdots,n\}$ 分成几个不相交的子集的并集

$$\{\alpha_1,\alpha_2,\cdots,\alpha_{j-1}\} \cup \{\alpha_j,\cdots,\alpha_{l-1}\} \cup \cdots \cup \{\alpha_r,\cdots,\alpha_n\},$$

其中 $1 < j < l < \cdots < r \leqslant n$. σ 在每个子集上是循环变换. 可将 σ 记成

$$\sigma = (\alpha_1\alpha_2\cdots\alpha_{j-1})(\alpha_j\cdots\alpha_{l-1})\cdots(\alpha_r\cdots\alpha_n).$$

每个括弧代表一个循环变换, 也叫做一个轮换. 每个轮换也是 $\{1,2,\cdots,n\}$ 上的一个置换. 因此上式也是表示一些置换的乘积. 由于每个轮换作用于一个子集, 这些子集是互不相交的, 我们称这些轮换为不相交的. 这些置换的作用就是互相独立的了, 它们的乘积就可任意交换次序.

以上我们就证明了: 任意一个 n 元置换可表成若干个互不相交的轮换的乘积.

再证表法的唯一性: 若有另一分解, 则它的含有 α_1 的轮换反映了 σ 作用在 α_1 上形成的循环变换序列, 这是由 σ 唯一决定的, 故两个分解中含 α_1 的轮换应完全相同. 类似地其它轮换也相同. 这就证明了唯一性.

用置换的轮换表示可很容易地将置换表成对换的乘积. 以前我们用记号 (ij) 表示对换. 对换 (ij) 正是二元子集 $\{i,j\}$ 上的轮换. 对换的记号 (ij) 也正是它的轮换表示. 容易验证

$$(\alpha_1\ \alpha_2\cdots\alpha_k) = (\alpha_1\ \alpha_2)(\alpha_2\ \alpha_3)\cdots(\alpha_{k-2}\alpha_{k-1})(\alpha_{k-1}\alpha_k),$$

即一个 k 元轮换是 $k-1$ 个对换的乘积. 现设

$$\begin{aligned}\sigma &= (\alpha_1\cdots\alpha_{r_1})(\alpha_{r_1+1}\cdots\alpha_{r_1+r_2})\cdots(\alpha_{r_1+\cdots+r_{l-1}+1}\cdots\alpha_n)\\ &= (\alpha_1\ \alpha_2)\cdots(\alpha_{r_1-1}\alpha_{r_1})(\alpha_{r_1+1}\alpha_{r_1+2})\cdots(\alpha_{r_1+r_2-1}\alpha_{r_1+r_2})\\ &\quad\cdots(\alpha_{r_1+\cdots+r_{l-1}+1}\alpha_{r_1+\cdots+r_{l-1}+2})\cdots(\alpha_{n-1}\alpha_n),\end{aligned}$$

则 σ 中偶级轮换的数目的奇偶性决定 σ 的奇偶性.

下面用 S_n 中的元素 ρ 对元素 σ 作共轭, 计算其结果. 设

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

则

$$\begin{aligned}&\rho\sigma\rho^{-1}\\ &= \begin{pmatrix}\sigma(1) & \sigma(2) & \cdots & \sigma(n)\\ \rho(\sigma(1)) & \rho(\sigma(2)) & \cdots & \rho(\sigma(n))\end{pmatrix}\begin{pmatrix}1 & 2 & \cdots & n\\ \sigma(1) & \sigma(2) & \cdots & \sigma(n)\end{pmatrix}\\ &\quad\cdot\begin{pmatrix}\rho(1) & \rho(2) & \cdots & \rho(n)\\ 1 & 2 & \cdots & n\end{pmatrix}\\ &= \begin{pmatrix}\rho(1) & \rho(2) & \cdots & \rho(n)\\ \rho(\sigma(1)) & \rho(\sigma(2)) & \cdots & \rho(\sigma(n))\end{pmatrix}.\end{aligned}$$

特别地，$\rho(\alpha_1\alpha_2\cdots\alpha_r)\rho^{-1}=(\rho(\alpha_1)\rho(\alpha_2)\cdots\rho(\alpha_r))$. 即一个 r 级轮换被 ρ 对其作共轭作用，其结果仍是一个 r 级轮换. 且任一个用互不相交轮换的乘积表示的置换

$$(\alpha_1\cdots\alpha_{r_1})(\alpha_{r_1+1}\cdots\alpha_{r_1+r_2})\cdots(\alpha_{r_1+\cdots+r_{s-1}+1}\cdots\alpha_{n-1}\alpha_n),$$

被 ρ 作用后变为

$$(\rho(\alpha_1)\cdots\rho(\alpha_{r_1}))(\rho(\alpha_{r_1+1})\cdots\rho(\alpha_{r_1+r_2}))\cdots(\rho(\alpha_{r_1+\cdots+r_{s-1}+1})\cdots\rho(\alpha_{n-1})\rho(\alpha_n)),$$

仍是不相交的轮换的乘积.

定义 3 设 $n=r_1+\cdots+r_s$，且 $0<r_1\leqslant r_2\leqslant\cdots\leqslant r_s$，则称正整数组 $(r_1,r_2,\cdots,r_s)$ 为 n 的一个划分. 设 n 元置换 σ 表成互不相交的轮换的乘积

$$\sigma=(\alpha_1\cdots\alpha_{r_1})(\alpha_{r_1+1}\cdots\alpha_{r_1+r_2})\cdots(\alpha_{r_1+\cdots+r_{s-1}+1}\cdots\alpha_{r_1+\cdots+r_s}),$$

其中 $(r_1,\cdots,r_s)$ 是 n 的一个划分，则称它是由 σ 确定的划分.

例如，6 元置换 $(1\ \ 2\ \ 3)(4\ \ 5)(6)$ 确定的划分是 $(1,2,3)$.

命题 3 S_n 中两个置换 σ,τ 共轭当且仅当它们确定的划分相同.

证明 我们已证过了 σ 与 τ 共轭，它们确定相同的划分. 现在设它们确定相同的划分，故可设

$$\sigma=(\alpha_1\cdots\alpha_{r_1})\cdots(\alpha_{r_1+\cdots+r_{s-1}+1}\cdots\alpha_{r_1+\cdots+r_s}),$$

$$\tau=(\beta_1\cdots\beta_{r_1})\cdots(\beta_{r_1+\cdots+r_{s-1}+1}\cdots\beta_{r_1+\cdots+r_s}).$$

令

$$\rho=\begin{pmatrix}\alpha_1 & \alpha_2 & \cdots & \alpha_n\\ \beta_1 & \beta_2 & \cdots & \beta_n\end{pmatrix},$$

则

$$\begin{aligned}\rho\sigma\rho^{-1}&=(\rho(\alpha_1)\cdots\rho(\alpha_{r_1}))\cdots(\rho(\alpha_{r_1+\cdots+r_{s-1}+1})\cdots\rho(\alpha_{r_1+\cdots+r_s}))\\&\quad(\beta_1\cdots\beta_{r_1})\cdots(\beta_{r_1+\cdots+r_{s-1}+1}\cdots\beta_{r_1+\cdots+r_s})\\&=\tau.\end{aligned}$$

现在我们可以证明 A_n，当 $n\geqslant 5$ 时是单群了.

引理 4 每个偶置换是三轮换的积，因而 A_n 可由全体三轮换来生成.

证明 只要证二个对换的积(因而偶数个对换的积)是三轮换的积. 只有以下三种情形：

(i) $(i\ j)(i\ j)=$ 恒等置换 $=(1\ 2\ 3)(3\ 2\ 1)$;

(ii) $(i\ j)(i\ l)=(i\ l\ j)$. 其中 $l\neq j$;

(iii) $(i\ j)(k\ l)=(i\ j)(j\ k)(j\ k)(k\ l)=(j\ k\ i)(k\ l\ j)$,

故引理的前半部分成立.

又 A_n 中的子群 H 若包含所有三轮换，则 H 包含所有偶置换，只能有

$H = A_n$.

定理 5 A_n,当 $n \geqslant 5$ 时是单群.

证明 设 $|e| \neq H \lhd A_n$,来证 $H = A_n$.

首先证明在 $A_n (n \geqslant 5)$ 中所有三轮换在 A_n 中是互相共轭的.令 $(i_1 i_2 i_3)$ 和 $(j_1 j_2 j_3)$ 是两个三轮换.由于 $n \geqslant 5$,在 j_1, j_2, j_3 以外能取到二个文字 l, m. 于是令

$$(l\ m)\begin{pmatrix} i_1 & i_2 & i_3 \\ j_1 & j_2 & j_3 \end{pmatrix} = \rho_1, \quad 及 \quad \begin{pmatrix} i_1 & i_2 & i_3 \\ j_1 & j_2 & j_3 \end{pmatrix} \rho_2,$$

就满足

$$\rho_2 (i_1 i_2 i_3) \rho_2^{-1} = \begin{pmatrix} i_1 & i_2 & i_3 \\ j_1 & j_2 & j_3 \end{pmatrix} (i_1\ i_2\ i_3) \begin{pmatrix} i_1 & i_2 & i_3 \\ j_1 & j_2 & j_3 \end{pmatrix}^{-1} = (j_1\ j_2\ j_3),$$

及

$$\begin{aligned} \rho_1 (i_1\ i_2\ i_3) \rho_1^{-1} \quad & (l\ m) \rho_2 (i_1\ i_2\ i_3) \rho_2^{-1} (l\ m)^{-1} \\ &= (l\ m)(j_1\ j_2\ j_3)(l\ m) \\ &= (j_1\ j_2\ j_3). \end{aligned}$$

ρ_1, ρ_2 中必有一个是偶置换,故任意两个三轮换在 A_n 中共轭.

由于 $H \lhd A_n, \forall \tau \in A_n, \tau H \tau^{-1} \subseteq H$.故若能在 H 中找到一个三轮换 σ,则任何三轮换必为某 $\tau \sigma \tau^{-1}, \tau \in A_n$,于是 $\tau \sigma \tau^{-1} \in \tau H \tau^{-1} \subseteq H$,则 H 包含全部三轮换,必有 $H = A_n$.

下面就来证 H 中必有三轮换.对置换 σ 及文字 i,若 $\sigma(i) = i$,则称 i 为 σ 的不动元.我们取 H 中不动元最多的非单位元置换为 τ. τ 不可能恰有 $n-1$ 个不动元,这时 τ 就不动所有的元,因而是单位元.也不能恰有 $n-2$ 个不动元,这时 τ 是对换,是奇置换,不在 H 中.故 τ 最多有 $n-3$ 个不动元.若恰有 $n-3$ 个不动元,它在其它三个文字上就是一个三轮换,定理就能得证.现设 τ 的不动元的数目小于 $n-3$,我们来证出矛盾.把 τ 分解成互不相交的轮换的乘积.有两种情形:(i) τ 中有长度 $\geqslant 3$ 的轮换 $(\alpha_1 \alpha_2 \alpha_3 \cdots)$;(ii) $\tau = (\alpha_1 \alpha_2)(\alpha_3 \alpha_4) \cdots$.

在情形(i), τ 的不动元的数目不能为 $n-4$,否则 $\tau = (\alpha_1 \alpha_2 \alpha_3 \alpha_4)$,是奇置换.于是 τ 的不动元的数目 $\leqslant n-5$.换句话说,除 $\alpha_1, \alpha_2, \alpha_3$ 外还有两个文字 α_4, α_5 被变动了.现在对情形(i)及(ii)都令 $\varphi = (\alpha_3 \alpha_4 \alpha_5)$,并作 $\varphi \tau \varphi^{-1}$.在情形(i), $\varphi \tau \varphi^{-1} = (\alpha_1 \alpha_2 \alpha_4 \cdots) \cdots$.在情形(ii), $\varphi \tau \varphi^{-1} = (\alpha_1 \alpha_2)(\alpha_4 \alpha_5) \cdots$.再作 $\tau^{-1} \varphi \tau \varphi^{-1} = \tau_1$.这时对情形(i)有 $\tau_1(\alpha_1) = \alpha_1$,而 $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$ 以外的文字中,原来 τ 的不动元仍是 τ_1 的不动元.可是 τ 的不动元全在 $\alpha_1, \alpha_2, \cdots, \alpha_5$ 以外的文字中.这样 τ_1 的不动元比 τ 的不动元要多.在情形(ii), $\tau_1(\alpha_1) = \alpha_1$, $\tau_1(\alpha_2) = \alpha_2$.在 $\alpha_1, \alpha_2, \cdots, \alpha_5$ 以外的文字中 τ 与 τ_1 的不动元是相同的.在 α_1,

$\alpha_2,\cdots,\alpha_5$ 中 τ 最多不动 α_5，而 τ_1 不动 α_1 及 α_2. τ_1 的不动元也比 τ 的不动元多. 而 $\tau_1 = \tau^{-1}\varphi\tau\varphi^{-1} \in H$，就与 τ 有最少数目的不动元相矛盾. 故 H 中必有三轮换，从而 $H = A_n$. 定理得证.

以上证明了 $A_n, n \geqslant 5$ 时是单群. 它们都是非交换单群. 又 $A_2 = \{e\}$, $A_3 = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$ 是交换群. A_4 中的 $V_4 = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ 是它的非平凡的正规子群，故 A_4 不是单群.

习 题

1. 将下列置换分解成不相交的轮换的乘积：

$$\begin{pmatrix}1&2&3&4&5&6&7\\7&1&2&6&5&4&3\end{pmatrix}, \begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\2&4&5&9&7&10&8&3&1&6\end{pmatrix}.$$

然后再分解成对换的乘积，说明是奇或偶置换.

2. 确定置换

$$\sigma = \begin{pmatrix}1&2&\cdots&n-1&n\\n&n-1&\cdots&2&1\end{pmatrix}$$

的奇偶性.

3. 把(1 4 7)(7 8 10)(3 10 9)(9 4 2)(3 5 6) 表成不相交的轮换的乘积.

4. 证明 S_n 可由 $(1\ 2), (1\ 3), \cdots, (1\ n)$ 生成，也可由 $(1\ 2), (2\ 3), \cdots, (n-1\ n)$ 生成.

5. (1) 求(1 2), (3 4 5) 在 S_7 中的中心化子.

(2) 证明 $\sigma = (1\ 2\ 3\cdots n)$ 在 S_n 中的中心化子是 $\langle\sigma\rangle$ 及 σ 所在的共轭类中元素数目为 $(n-1)!$.

(3) 求(1 2)(3 4 5)(6) 在 S_6 中的中心化子的阶及其所在共轭类元素数目.

6. G 是 S_n 的子群，则 G 中全部偶置换组成一个正规子群 H. 若 G 中有奇置换，则 $[G:H] = 2$.

7. G 是 $2k$ 阶群，k 奇数，则 G 中有一个 k 阶的正规子群(提示：由 §3 定理 3(Cayley 定理)，G 同构于 S_{2k} 的一个子群. 又由 §1 习题 13，这个子群有一个元 $a \neq e, a^2 = e$. 分析这个置换的奇偶性).

8. 证明 $n \geqslant 3$ 时，S_n 的中心为 e.

9. 重新证明 A_5 是单群.

10. 证明 A_4 中没有 6 阶子群.

11. 求 A_4 的全部共轭类及 S_4 的全部共轭类.

§10 同态基本定理

前面已讲过群 G 在集合上的作用，这是群 G 的一种特殊的同态. 给定 G 的一个正规子群 N，可以作商群 $\bar{G}=\frac{G}{N}=\{gN=\bar{g}\mid g\in G\}$. $\bar{G}$ 上乘法运算定义成

$$\bar{g}_1\bar{g}_2=(g_1N)(g_2N)=g_1g_2N=\overline{g_1g_2}.$$

从这个乘法可以作出 G 到 $\bar{G}$ 的一个同态.

命题 1 G 是群，N 是 G 的正规子群，则下列映射

$$\begin{aligned} G &\xrightarrow{\eta}\bar{G}=\frac{G}{N}\\ g &\longmapsto \bar{g}\end{aligned}$$

作成 G 到商群 $\bar{G}$ 的满同态，称为 G 到商群 $\bar{G}$ 的**自然同态**.

证明 首先 $\forall g_1,g_2\in G,\bar{g}_1\bar{g}_2=\overline{g_1g_2}$ 表明 $\eta(g_1)\eta(g_2)=\eta(g_1g_2)$. 即 η 保持乘法，故是同态. 它显然是满同态.

上面证明了 G 的任一个商群是 G 的某个同态象. 实际上这个结论的逆也成立，即 G 的任一个同态象也是(同构于) G 的某个商群. 这就是下面的

定理 2(同态基本定理) 设 $G,\bar{G}$ 是两个群及 π 是群同态 $G\to\bar{G}$，且是满同态. 令

$$K=\{g\in G\mid \pi(g)=e_{\bar{G}}\}=\operatorname{Ker}\pi$$

是同态 π 的核，则 K 是 G 的正规子群，且商群 $\frac{G}{K}$ 与 $\bar{G}$ 同构.

证明 对 $\forall g_1,g_2\in K$，由 π 是同态得 $\pi(g_1g_2)=\pi(g_1)\pi(g_2)=e_{\bar{G}}$，$\pi(g_1^{-1})=\pi(g_1)^{-1}=e_{\bar{G}}^{-1}=e_{\bar{G}}$ 及 $\pi(e_G)=e_{\bar{G}}$，就得出 $g_1g_2\in K,g_1^{-1}\in K$，$e_G\in K$. 故 K 是 G 的子群. 又对 $\forall g\in G,k\in K$，

$$\pi(gkg^{-1})=\pi(g)e_{\bar{G}}\pi(g)^{-1}=e_{\bar{G}},$$

故 $gkg^{-1}\in K$. 即 $gKg^{-1}=K$，K 是 G 的正规子群.

作映射

$$\begin{aligned} \frac{G}{K} &\xrightarrow{\pi_1}\bar{G}\\ gK &\longmapsto \pi(g).\end{aligned}$$

若有 $g_1K=gK$，则有 $k\in K$ 使 $g_1=gk$，

$$\pi(g_1)=\pi(g)\pi(k)=\pi(g)e_{\bar{G}}=\pi(g),$$

即 $\pi_1(g_1K)=\pi_1(gK)$. 故上述映射 π_1 是有定义的.

由于

$$\pi_1(g_1Kg_2K)=\pi_1(g_1g_2K)=\pi(g_1g_2)$$
$$=\pi(g_1)\pi(g_2)\quad\pi_1(g_1K)\pi_1(g_2K),$$

故 π_1 是同态.因为 π 是满射,π_1 也就是满射.

再设 $\pi_1(g_1K)=\pi_1(g_2K)$,则 $\pi(g_1)=\pi(g_2)$.两边乘以 $\pi(g_2^{-1})$,则得

$$\pi(g_2^{-1}g_1)=\pi(g_2^{-1})\pi(g_1)=\pi(g_2^{-1})\pi(g_2)=e_G.$$

于是 $g_2^{-1}g_1\in K$,即 $g_1\in g_2K$ 或 $g_1K=g_2K$.这说明 π_1 是单射(或 1-1 的).

以上就证明了 π_1 是所要的同构.

定理1之所以称为同态基本定理,是它找出了群 G 的所有可能的同态象.从同构的意义看,群 G 的全部的同态象就是全部的商群.

§7命题2中证明了无限循环群 G 与整数加法群 $\mathbb{Z}$ 同构.而两个有限循环群 G_1 与 G_2 同构当且仅当 $|G_1|=|G_2|$.§8例2中我们对任意 n,构造了 n 阶循环群 $\frac{\mathbb{Z}}{n\mathbb{Z}}$.因此任意 n 阶循环群 G 与 $\frac{\mathbb{Z}}{n\mathbb{Z}}$ 同构.这两件事可统一地利用同态基本定理来阐明.这样又从另一个侧面观察了循环群的构造.

设 $G=\langle a\rangle=\{a^k\mid k\in\mathbb{Z}\}$.作映射

$$\mathbb{Z}\xrightarrow{\varphi}G$$
$$k\longmapsto a^k.$$

这是满射,且 $\varphi(k+l)=a^{k+l}=a^ka^l=\varphi(k)\varphi(l)$.故 φ 是同态,因此是满同态.由同态基本定理,$\frac{\mathbb{Z}}{\mathrm{Ker}\varphi}\cong G$.这里重要的是要决定 $\mathrm{Ker}\varphi$ 可能的结构.

实际上 $\mathrm{Ker}\varphi$ 是无限循环(加法)群的子群.由 §7定理3已经得到无限循环群的全部子群.只要把那里对乘法循环群写出的结果转换成加法循环群的情形,就知 $\mathrm{Ker}\varphi$ 有两种可能:

(i) $\mathrm{Ker}\varphi=0$.这时 $\mathbb{Z}$ 与 G 同构.

(ii) $\mathrm{Ker}\varphi=n\mathbb{Z}$.这时 $\frac{\mathbb{Z}}{n\mathbb{Z}}$ 与 G 同构.

第一种情形 G 是无限循环群,它与 $\mathbb{Z}$ 同构.第二种情形下,$\frac{\mathbb{Z}}{n\mathbb{Z}}$ 与 G 都是 n 阶循环群,n 阶循环群 G 与 $\frac{\mathbb{Z}}{n\mathbb{Z}}$ 同构.

习 题

1. F 是域.试证明 $\frac{GL_n(F)}{SL_n(F)}\cong F$.

2. S_4 有正规子群 $V_4 = \{(1),(1\,2)(3\,4),(1\,3)(2\,4),(1\,4)(2\,3)\}$. 试写出 $\frac{S_4}{V_4}$ 的全部元素并建立一个同构映射

$$\frac{S_4}{V_4} \longrightarrow S_3.$$

3. G 是群，$Z(G)$ 是 G 的中心，则 $\frac{G}{Z(G)}$ 同构于 Aut G 的子群. 进而，若 G 非交换，则 Aut G 非循环群.

4. $\mathbb{C}^*$ 是非零复数的乘法群. $U = \{e^{i\theta} \mid \theta \text{ 实数}\}$ 是 $\mathbb{C}^*$ 中绝对值等于 1 的复数的子群，则 $\frac{\mathbb{C}^*}{U}$ 同构于正实数的乘法群.

5. $\mathbb{R}$ 是实数加法群，$\mathbb{Z}$ 是它的加法子群. 则 $\frac{\mathbb{R}}{\mathbb{Z}}$ 同构于绝对值为 1 的复数的乘法群.

6. 设群 G 到群 $\bar{G}$ 有满同态 f. 令 $N = \mathrm{Ker} f$. 记 $f^{-1}(K)$ 为 $\bar{G}$ 的子集 $\bar{K}$ 对于 f 的原象. 证明：

(1) 若 $\bar{K}$ 是 G 的子群，则 $N \subset f^{-1}(\bar{K})$.

(2) $\{G \text{ 的包含 } N \text{ 的子群}\} \xrightarrow{\varphi} \{\bar{G} \text{ 的子群}\}$

$$H \longmapsto f(H)$$

是双射，且保持包含关系.

(3) 若 $\bar{K}$ 是 $\bar{G}$ 的正规子群，则 $f^{-1}(\bar{K})$ 是 G 的含 N 的正规子群. 于是

$$\{G \text{ 的包含 } N \text{ 的正规子群}\} \xrightarrow{\varphi} \{\bar{G} \text{ 的正规子群}\}$$

$$K \longmapsto f(K)$$

是双射.

(4) 设 $\bar{H}$ 是 $\bar{G}$ 的正规子群，则有同构

$$\frac{G}{f^{-1}(\bar{H})} \cong \frac{\bar{G}}{\bar{H}}.$$

(5) G 是群，N 是正规子群. 令 $\bar{G} = \frac{G}{N}$. π 是自然同态

$$G \xrightarrow{\pi} \frac{G}{N} = \bar{G},$$

则 π 建立了 $\{G \text{ 的含 } N \text{ 的子群}\}$ 到 $\{G \text{ 的子群}\}$ 上的双射：$\pi(H) = \bar{H} = \frac{H}{N}$. 且保持包含关系. 同时建立了 $\{G \text{ 的含 } N \text{ 的正规子群}\}$ 到 $\{\bar{G} \text{ 的正规子群}\}$ 上的双射. 且有同构

$$\frac{G}{H} \cong \frac{\bar{G}}{\bar{H}} \quad \text{即} \quad \frac{\frac{G}{N}}{\frac{H}{N}}.$$

以上的结论称为**第二同构定理**.

7. G 是群,H 是子群,$[G:H]=n$. 令 G 中 H 的左陪集的集合 $M=\{x_iH \mid i=1,2,\cdots,n,x_i\in G\}$. 证明:

(1) $g\in G, gx_iH=x_iH, i=1,2,\cdots,n$ 当且仅当 $g\in\bigcap_{i=1}^{n}x_iHx_i^{-1}$.

(2) $\bigcap_{i=1}^{n}x_iHx_i^{-1}=\bigcap_{x\in G}xHx^{-1}$ 是 G 的正规子群.

(3) 映射 $G\xrightarrow{\varphi}S_n$($M$ 中 n 个元的置换群)

$$g\longrightarrow\varphi(g):\ x_iH\longmapsto gx_iH,\quad i=1,2,\cdots,n,$$

是群同态.

(4) $\forall g_1,g\in G,\varphi(g)=\varphi(g_1)$ 当且仅当 $g_1\in g(\bigcap_{x\in G}xHx^{-1})$.

(5) 映射:

$$\frac{G}{\bigcap_{x\in G}xHx^{-1}}\longrightarrow S_n$$

$$g\bigcap_{x\in G}xHx^{-1}\longmapsto\varphi(g)$$

是群的单同态. 即 $\dfrac{G}{\bigcap_{x\in G}xHx^{-1}}$ 与 S_n 的一个子群同构.

(6) H 包含一个正规子群,它在 G 中的指数是 $n!$ 的因子.

8. G 是有限群,p 是 $|G|$ 的最小素因子. 证明 G 的指数为 p 的任意子群皆为正规子群.

§11 轨道数的定理及其在计数问题中的应用

在某些计数问题中,群在集合上作用的思想和结果起着关键的作用. 在本章的最后这一节我们来介绍计算轨道数的 Burnside 定理,并用于计数问题中.

先看一个例子.

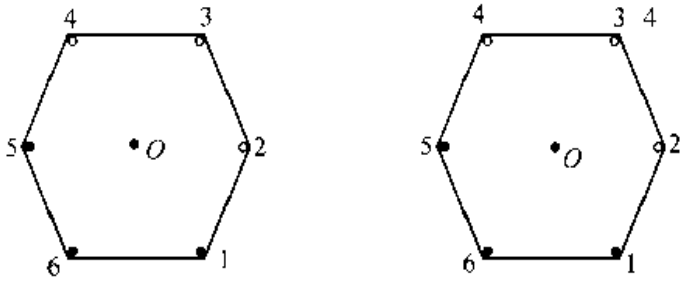


图 1

例 1 上图是正六角形瓷砖的正面. 在六个顶点上分别有三个染白色,有

三个染黑色.问:可以作出几种瓷砖图案?

分析　上面两图从染色的方法看是不同的,但它们都表示了同一种瓷砖图案.只要把右面的瓷砖绕 O 点转 120°(反时针旋转),则它就与左面瓷砖的染色方法一致了.故这两种染色方法是同一种图案.

实际上对于正六角形瓷砖的两种染色法,只要在瓷砖绕 O 反时针旋转 0°,60°,120°,180°,240°,300° 的任一个旋转的变换下将其中一个染色法变成另一种染色法,这两种染色法就提供同一种图案.

正六角形瓷砖按前面要求来染色,共有 $C_6^3=\frac{6\cdot5\cdot4}{3\cdot2\cdot1}=20$ 种染色法,它们作成一个集合 M.将绕 O 反时针转 0°,60°,120°,180°,240°,300° 的旋转分别记成 T_0,T_1,T_2,T_3,T_4,T_5.它们对变换的乘法作成一个群 G.G 的任一旋转引起M中的一个变换,于是 G 在M 上有群作用.按前面的讨论,两种染色法表示同一图案当且仅当这两种染色法在 G 的元素的作用下互变,也即当且仅当这两种染色法作为 M 的元素属于G 作用下的同一轨道.故不同的图案的数目恰是 M 在 G 作用下的轨道的数目.

下面的定理给出群作用下的轨道数的一种计算方法.

定理 1 (Burnside)　设有限群 G 作用于有限集 M 上.对 $g\in G$,令 M 中被 g 固定的元素(下面称为 g 的不动元)的集合为 $\mathrm{Fix}(g)$,则 M 在 G 的作用下的轨道数是

$$\frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g)|.$$

证明　$\sum\limits_{g\in G}|\mathrm{Fix}(g)|$ 是 G 的全体元素的不动元素的总数,这个数也可以换一个数法:对任一 $m\in M$,G 中能固定它的元素的集合恰是 $\mathrm{Stab}_G(m)$,于是 $\sum\limits_{m\in M}|\mathrm{Stab}_G(m)|$ 就和它相等.

设 G 作用于M 上有 k 条轨道 $O_1,O_2,\cdots,O_k$.设 x,y 是任一轨道 O_i 中的两个元,由 §6 定理 2 的推论 1,

$$|G|=|\mathrm{Stab}_G(x)||O_i|=|\mathrm{Stab}_G(y)||O_i|,$$

故 $|\mathrm{Stab}_G(x)|=|\mathrm{Stab}_G(y)|$.因此

$$\frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g)|=\frac{1}{|G|}\sum_{m\in M}|\mathrm{Stab}_G(m)|=\frac{1}{|G|}\sum_{i=1}^{k}\sum_{m\in O_i}|\mathrm{Stab}_G(m)|$$

$$=\frac{1}{|G|}\sum_{i=1}^{k}|O_i||\mathrm{Stab}_G(m)|=\frac{1}{|G|}\sum_{i=1}^{k}|G|=k.$$

上述结果表明轨道数 k 是 G 的元素的不动元的数目的平均值.这个结果对一些计数问题指出了一种算法.后来发展成组合数学中的 Polya 计数定理.

现在用这个定理来计算本节开头例子中的轨道数.这需要计算 G 的每个元素在 M 上的不动元的数目.

T_0:旋转 0°,它是恒等变换,固定 M 中全部 20 种染色法.

T_1:旋转 60°,它把正六角形的每个顶点变到下一个顶点.T_1 把一种染色法变成新染色法时,原先染色法中某顶点的颜色与新染色法中在下一个顶点的颜色一样.若原染色法在 T_1 变换下不动.即原染色法在下一个顶点的颜色与新染色法在下一个顶点的颜色一样.于是原染色法在每顶点的颜色与下一顶点的颜色相同.因而被 T_1 不动的染色法在各个顶点上有相同颜色.这不是 M 中的染色法.故 M 中 T_1 的不动元数目为零.

T_2:旋转 120°,它把每个顶点在六角形的顶点位置上下移两位.被 T_2 固定的染色法在这样顶点上有相同颜色.即顶点 1,3,5 上和顶点 2,4,6 上应分别有相同颜色.M 中有两个这样的染色法:即顶点 1,3,5 上染白色,顶点 2,4,6 上染黑色,这是一种;而顶点 1,3,5 上染黑色,顶点 2,4,6 上染白色是第二种.T_2 在 M 中就有这两个不动元.

T_3:旋转 180°,它把顶点 1,4 互变,2,5 互变,3,6 互变.若某种染色法被 T_3 固定,则顶点 1,4 上,顶点 2,5 上,顶点 3,6 上的颜色相同.共有黑白两色,因此每种颜色在偶数个顶点上出现.它不在 M 中,故 M 中没有 T_3 的不动元.

T_4:旋转 240°(反时针)相当于顺时针旋转 120°.与 T_2 类似,被 T_4 固定的染色法中,顶点 1,5,3 上和顶点 2,6,4 上分别有相同的颜色.T_4 在 M 中有两个不动元.

T_5:旋转 300°(反时针)相当于顺时针旋转 60°.与 T_1 类似,可证 T_5 在 M 中没有不动元.

由定理 1,G 在 M 上作用的轨道数也即瓷砖的不同图案的数目是

$$\frac{1}{6}(20+0+2+0+2+0)=4.$$

上面 6 角形顶点染色看成瓷砖面上图案时共有四种不同的图案.现把它看成一个手镯,上面串着三个白珠子,三个黑珠子,问有几种串法?这个问题中从图上看有 20 种串法.但是对于手镯而言,它们中有些是对应手镯的同一个式样,如何区分出不同的式样?请读者分析.

例 2 上述类型的计数问题在化学中有类似的应用.化学中的某类化合物,它由六个碳原子排成六边形,每个碳原子上可任意附属着 CH_3 或 H(图 2 是该类化合物的一种情形).问可得多少种化合物?

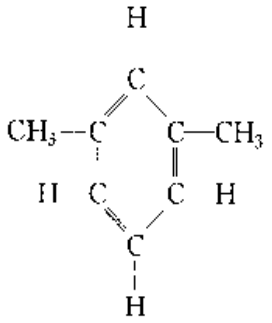
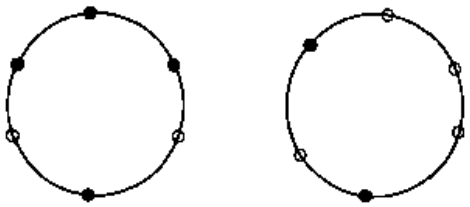


图 2

这个计算留给读者.

习　题

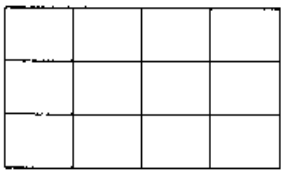
1.在一个圆手镯上串上六粒珠子,珠子可任意染白色或黑色.问能作出几种式样的手镯?(下图中列出两种式样的例子)



2.在一个正四面体的顶点上任意染黑色或白色,能作出几种式样?

3.将课文例 2 中的问题计算出答案.

4.下面图中,矩形板上有 12 个同样的矩形格子.将其中 5 个染红色,7 个染黄色.问能作出几种图板?若矩形板换成白布.将格子的正反面都染成同一颜色,五个染红色,7 个染黄色.问能染成几种图样?



5.把 3 个红球,4 个白球,2 个兰球共 10 个球分成三堆,问有多少种分法?

第二章　域　和　环

§1　域的例子，复数域及二元域的构造，对纠一个错的码的应用

例 1　数域是域.

高等代数中讲过复数域 $\mathbb{C}$，实数域 $\mathbb{R}$，有理数域 $\mathbb{Q}$，及 $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$，这些都是数域.

例 2　设 P 是数域，x 是一个文字，所有形式为

$$\frac{a_m x^n + a_{n-1} x^{n-1} + \cdots + a_0}{b_m x^m + b_{m-1} x^{m-1} + \cdots b_0}$$

的式子，其中 $a_i, b_i \in P$，且分母不为零多项式，在通常分式运算下成为一个域，称为系数在 P 中的有理分式域，记为 $P(x)$.

例 3　复数域的构造.

在实数域 $\mathbb{R}$ 上负数是没有平方根的，即 $x^2 + a = 0$，a 是正实数，这方程在 $\mathbb{R}$ 中无解. 但实际上从 16 世纪开始就有数学家引入形如 $a + b\sqrt{-1}$ 的数，其中 a, b 为实数，并且认为它也适合实数所适合的运算规则. 这样所有负数的平方根可通过 $\sqrt{-1}$ 来表达，且能对形如 $a + b\sqrt{-1}$ 的数进行加减乘除四则运算. $a + b\sqrt{-1}$ 这种形式的数称为复数. 其后，人们证明了三次和四次复系数多项式（包括实系数多项式）的根能够通过系数的加减乘除和根式运算的某种公式来求得. 即使是实系数多项式，其根的公式中也不能避免出现 $a + b\sqrt{-1}$ 形式的复数. 尽管如此，由于 $\sqrt{-1}$ 记号的引入及运算缺乏严格的基础，许多数学家仍认为这种形式的数是“虚”的，“想象”的数，称为虚数. 历史上，虚数的支持者与反对者的斗争经历了 300 年. 到 19 世纪经过 Gauss 和 Hamilton 在平面的点集上严格定义了四则运算，检验了运算规则才得到严格意义下的复数. 中学课程中我们虽讲了复数，但也不是严格的构造. 这里我们严格地介绍复数的构造.

命题 1　令 $\mathbb{R}$ 为实数域，$\mathbb{C} = \{(a, b) \mid a, b \in \mathbb{R}\}$. 令

$$(a, b) + (c, d) = (a + c, b + d),$$

$$(a, b)(c, d) = (ac - bd, ad + bc),$$

则 $\mathbb{C}$ 对于上述加法和乘法成为一个域，称为**复数域**（读者自己验证一下）.

$\mathbb{C}$ 有下列性质:

i) $\mathbb{C}$ 中子集 $\{(a,0)\mid a\in\mathbb{R}\}$ 对于 $\mathbb{C}$ 的加法和乘法成为一个子域*.一个自然的对应 $(a,0)\to a$ 建立了这个子域与 $\mathbb{R}$ 之间的一个域同构*.我们干脆记它为 $\mathbb{R}$.这即说明 $\mathbb{C}$ 包含实数域 $\mathbb{R}$.

$\mathbb{C}$ 自然地是 $\mathbb{R}$ 上二维向量空间:任意 $(c,0)\in\mathbb{R}$,$(c,0)$ 对 (a,b) 的数量乘积就是它们在 $\mathbb{C}$ 中的乘积,$(c,0)(a,b)=(ca,cb)$.于是有 $(a,b)=(a,0)+(b,0)(0,1)$.干脆将 $(a,0)$,$(b,0)$ 写成 a,b,则 $(a,b)=a+b(0,1)$.

ii) $\mathbb{C}$ 的乘法单位元是 $(1,0)=1$.由乘法规则 $(0,1)^2+1=(0,1)^2+(1,0)=0$.故 $\mathbb{C}$ 中元素 $(0,1)$ 满足 $x^2+1=0$,或 $x^2=-1$.它是 -1 的平方根.如将它记成 $\sqrt{-1}$(或 i),则 $\mathbb{C}$ 就由 $a+b\sqrt{-1}$(或 $a+bi$)组成.

iii) $\mathbb{C}$ 中任意含 $\mathbb{R}$ 的子域 K 在(i)中规定的数量乘法下自然成为 $\mathbb{C}$ 的子空间(域 $\mathbb{R}$ 上的).因 $\mathbb{C}$ 是二维的,若 K 不等于 $\mathbb{C}$,则必为 $\mathbb{R}$.故 $\mathbb{C}$ 中没有真子域 K 既含 R 又使 K 中有 -1 的平方根 $\sqrt{-1}$.

从命题 1 看出,虚数、复数的引入,不是想象的或虚的,其数学实质是把实数域 $\mathbb{R}$ 进行扩充得到一个更大的域*,使得 $x^2+1=0$ 在大域中有根.

例 4 二元域的一种构造及对编码的应用.

现在是信息时代,世界上时刻有大量的信息在传输.如电话、电报、电视、传真、计算机中数据送入内外存贮器或送到运算器、打印机、*VCD* 机、*CD* 机等.现在技术上多采用电信号,一般有两个状态:"有""无"或"高""低".工程上常用 1,0 来代表这两个状态.通常用一组 0,1 信号来代表一个信息.例如明码电报中北京是编成0554,0079,再用国际第二种5单位电码方法编为8个0,1五元序列

01101 00001 00001 01010 01101 01101 11100 00011.

又如图像传输中,把照片分成很多小方格,每格上的明暗程度用 0 到 63 共 64 个等级来标出.这恰可用 6 位二进数表出.把图片用 0,1 信号表示后,卫星上拍的照片就可传送到地球上.

由于机器、电路、大气层对信号的干扰,会引起信号局部改变,由 0 变 1 或由 1 变 0,于是接收到的信息中有部分是错误的.因此人们希望在接收后能用一定的方法纠正错误,恢复正确信息.怎样来实现这个想法呢?人们想让承载信息的各 0,1 序列(或说码集合)是具有某种特定结构的序列的集合.有错误时,结构就遭破坏,我们能恢复其特定的结构,就纠正了错误.0,1 序列上的特定结构最好是数学结构,于是人们想到把 0,1 这两个元素的集合记成 F_2,像

* 这里涉及到子域、扩域、域的同构的概念,读者应该能自己给出其定义.以后在 §2 和 §4 中会给出严格的叙述.

数域一样地组织成一个可运算的系统. F_2 上有很自然的加法和乘法如下：

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

(1)

容易验证 F_2 在这样的加法和乘法下成为一个域，称为**二元域**. 将 F_2 作成一个域以后，0,1 序列就是 F_2 上的向量. 例如前面代表北京的 8 个代码都是 5 元 0,1 向量. 我们想到要对一组 n 元 0,1 向量附加上特定的结构，最易实现的是取它们为域 F_2 上某固定方程组的解. 这就想到要检验一下对于数域成立的线性方程组理论和矩阵理论还有多少结论对 F_2 成立. 检验的结果很鼓舞人心，这些理论全部有效. 在引论章的最后一段，我们已把这些总结成为定理了. 在此基础上人们想出了许多纠错码的方案. 下面举一个例子，即一个最简单的纠错方案，看看它是如何实现纠错的.

作 F_2 上 4×15 矩阵

$$H=\begin{pmatrix}0&0&0&0&0&0&0&1&1&1&1&1&1&1&1\\0&0&0&1&1&1&1&0&0&0&0&1&1&1&1\\0&1&1&0&0&1&1&0&0&1&1&0&0&1&1\\1&0&1&0&1&0&1&0&1&0&1&0&1&0&1\end{pmatrix}_{4\times 15}, \tag{2}$$

实际上将十进位数 1,2,…,15 变成四位二进位数后，把它们看成 F_2 上的 4 元向量，依次排在第 1 列，第 2 列，…，第 15 列，就得到上面的 H.

以 H 为系数矩阵作 F_2 上的齐次方程组

$$H_{4\times 15}X_{15\times 1}=0. \tag{3}$$

我们取方程组(3)的解集合，它是 F_2 上 15 元向量的一个集合，用以作为承载各个信息的 0,1 向量的集合，这在编码理论中称为码集合，其中的每一个向量都是一个码字. 前面说的特定结构就是它的向量都是(3)的解，或满足方程组(3). 我们看看这个结构为何能用以纠错.

这个码具有纠一个错的能力. 任一个码字

$$\alpha=\begin{pmatrix}a_1\\a_2\\\vdots\\a_{15}\end{pmatrix},\qquad a_i\in F_2,$$

是(3)的解，即满足 $H\alpha=0$. 假设它在传输时受到干扰，有一位发生改变，设在第 i 位发生改变，即第 i 位由 0 变 1 或由 1 变 0. 由 F_2 的运算，这相当于第 i 位上加上 1. 令

$$e_i = \begin{vmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{vmatrix} \cdots\cdots i \text{ 位},$$

则接收到的向量为 $\beta = \alpha + e_i$.用 H 乘它,$H\beta = H\alpha + He_i = 0 + He_i = He_i$.由矩阵乘法知,$He_i$ 是 H 的第 i 列的列向量.因此对接收到的向量 β,若 $H\beta$ 是 H 的第 i 列的列向量,则 β 错在第 i 位.只要将 β 再加上 e_i,就恢复了发出的码字 α.

若 α 虽受干扰,但未发生错误,则接收的向量 $\beta = \alpha$ 满足 $H\beta = 0$.

因此若这个码集合的一个码字在传输过程中最多有一位错,则对接收到的向量 β 来计算 $H\beta$ 就能断定发出的码字是谁.但错位有两个以上时就不能判定发出的码字(读者试验证这句话),故我们说这个码是纠一个错的码.

作为对 F_2 的运算的练习.我们仿造数域的情形先来解方程组(3),求出它的一般解.然后我们取一个特解来作为一个码字.故意破坏它的某一位后,再用上面提供的方法来纠错.

写出方程组(3),$HX = 0$,即

$$\begin{cases} x_8 + x_9 + x_{10} + x_{11} + x_{12} + x_{13} + x_{14} + x_{15} = 0 \\ x_4 + x_5 + x_6 + x_7 + 0 + 0 + 0 + 0 + x_{12} + x_{13} + x_{14} + x_{15} = 0 \\ x_2 + x_3 + 0 + 0 + x_6 + x_7 + 0 + 0 + x_{10} + x_{11} + 0 + 0 + x_{14} + x_{15} = 0 \\ x_1 + 0 + x_3 + 0 + x_5 + 0 + x_7 + 0 + x_9 + 0 + x_{11} + 0 + x_{13} + 0 + x_{15} = 0. \end{cases} \tag{4}$$

解之,得一般解

$$\begin{cases} x_1 = x_3 + x_5 + x_7 + x_9 + 0 + x_{11} + 0 + x_{13} + 0 + x_{15} \\ x_2 = x_3 + x_6 + x_7 + x_{10} + x_{11} + x_{14} + x_{15} \\ x_4 = x_5 + x_6 + x_7 + x_{12} + x_{13} + x_{14} + x_{15} \\ x_8 = x_9 + x_{10} + x_{11} + x_{12} + x_{13} + x_{14} + x_{15}, \end{cases} \tag{5}$$

其中 $x_3, x_5, x_6, x_7, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}$ 为自由未知量、取所有自由量为 1,得解

$$X = (1,1,1,1,1,1,1,1,1,1,1,1,1,1,1)^{\mathrm{T}}.$$

将 X 的第 6 位变为 0,得

$$Y = (1,1,1,1,1,0,1,1,1,1,1,1,1,1,1)^{\mathrm{T}}.$$

若我们不知它是由 X 改变第 6 位而得,只知道它与方程组(4)的一个解最多

有一位不同，来恢复 X.

现在作 HY. 也即将 Y 代入(4)的各式的左端得

$$1+1+1+1+1+1+1+1=0,$$

$$1+1+0+1+0+0+0+0+1+1+1+1=1,$$

$$1+1+0+0+0+1+0+0+1+1+0+0+1+1=1,$$

$$1+0+1+0+1+0+1+0+1+0+1+0+1+0+1=0,$$

即

$$HY=\begin{pmatrix}0\\1\\1\\0\end{pmatrix}$$

是 H 的第6列(这个四位二进位数换算成十进位数为6). 故 Y 与原解在第6位差了1，将 Y 的第6位加1就得原解了. 这正是我们预先设定的 X.

方程组(3)中 H 的秩是4，未知数有15个，故(3)的解空间是 F_2 上 $15-4=11$ 维空间. 因 F_2 只有2个元素，故解空间中有 2^{11} 个向量. 即这个码集合中有 2^{11} 个码字. 我们称这个码的容量是 2^{11}. 又每个码字(即每个解向量)中，自由未知量有11个. 即码字中仅有11位是用以代表信息的，还有4位从表示信息的角度看完全是多余的，它的作用是赋以码字的特定结构，在我们的情况中就是使它是 $HX=0$ 的解. 特定结构的作用是为了有纠错的能力.

有的信息传输，很少发生错误，例如计算机中的数据传输，用纠一个错的码就足够了. 但计算机中表达信息(数据)的码字要用更多的位数，15位肯定是不够的；有的信息传输过程中，可能发生较多的错位，例如从卫星上发送信息(比如照片)到地球上就是这样，于是纠一个错就不符合需要了. 因此需要有新的编码方法，其中不但要用到 F_2 上线性方程组、矩阵、向量空间的理论，还要用到 F_2 上多项式的理论. 20世纪60年代美国人造卫星发送火星、土星的照片到地球上，虽然一个信息(一个小方格上的明暗程度)只需6位0,1向量，但实践上却用32位的0,1向量来表示它，其中26位多余位数是用来附加它的特定结构. 这样做出来的码叫 Reed-Solomon 码，它有纠7个错的能力. 这个码至今已用到 CD(及 VCD)盘上，即使 CD(及 VCD)盘上附有灰尘和脏物，或有些擦伤，仍能让你欣赏此中的音乐(读者常会在电视中看到这样的广告：×× VCD，强纠错能力). 这说明一个多世纪以来(从19世纪30年代 Galois 开始)发展起来的抽象的代数运算系统(上面的有限域 F_2 只是一个例子)已进入了我们的生活之中.

从上面的例子我们可以看出人们为了数学上、工程上或其它方面的一定的需要，主动扩充老的运算系统(例如把实数域 $\mathbb{R}$ 扩充为复数域 $\mathbb{C}$)，甚至创造

出新的运算系统(比如 F_2).由于与某些老的运算系统有共同的运算性质(例如 F_2 与数域),于是有一些共同的数学理论(例如 F_2 上也有线性方程组理论、矩阵理论、向量空间理论等)对新的运算系统(一般域)成立,因而在新的运算系统中能应用这些理论.这就是扩充域或造新域的好处与目的.

即使这样,数域的有些理论,比如二次型的理论就不是对于所有的域都成立.实际上,任意二次型用非退化线性替换化为平方项的和的配方法对 F_2 就不成立.例如在 F_2 上,二次型 $x_1^2 + x_1x_2 + x_2^2$ 就不能用非退化线性替换化成平方项的和(留作习题).

F_2 与任意数域 P 有一重要的区别是:在 F_2 中有 $1 + 1 = 0$,而数域 P 中对任意正整数 n,$n \cdot 1 = \underbrace{1 + 1 + \cdots + 1}_{n\text{个}} \neq 0$.对任意域 F,设 m 是使 $m \cdot 1 = 0$ 的最小正整数,因 $1 \neq 0$,故 $m > 1$.我们来证明 m 必为素数.用反证法,若 $m = m_1m_2$,m_1,m_2 是两个比 m 小的正整数,于是 $m1 = (m_1 1)(m_2 1) = 0$,由于域 F 中没有零因子,故必须 $m_1 1 = 0$ 或 $m_2 1 = 0$,这都与 m 的最小性矛盾,故 m 为素数.

定义 1　设 F 是一个域.若对任何正整数 m,都有 $m1 \neq 0$,就称 F 是**特征为 0 的域**;若 m 是使 $m1 = 0$ 的最小的正整数,则称 F 是**特征为 m 的域**,这时 m 必为素数.

数域的特征为 0,而 F_2 的特征为 2.若 F 是一个有限个元的域,可证它的特征是某个素数.这只要证有某个正整数 m,使 $m1 = 0$.考察 $1, 2 \cdot 1, 3 \cdot 1, \cdots, n \cdot 1, \cdots$ 它们都是 1 的倍数,都属于 F.因 F 中仅有有限个元,上述倍数中必有两个是相同的.设 $k1 = l1$ 且 $k > l$.于是 $(k - l)1 = 0$,而 $k - l$ 是正整数.故 F 以某个素数为特征.

上面讲了如何构作复数域以及 F_2.以后在我们讲了环的基本概念后还要介绍模某个理想的剩余类环和剩余类域,以及对整环来构造它的分式域,并介绍它们的用途.

在介绍这些之前,在 §2 中我们先讨论域扩张的基本性质.作为应用,在 §3 中我们对古希腊著名的三大几何作图难题的否定答案给出论证.

习　题

1.令

$$\mathbb{C}_0 = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| a, b \in \mathbb{R} \right\},$$

则(1)$\mathbb{C}_0$ 对矩阵的加法和乘法成为域.

(2)$\mathbb{C}_0$ 中 $\mathbb{R}_0=\left\{\begin{pmatrix}a&0\\0&a\end{pmatrix}\middle|a\in\mathbb{R}\right\}$ 是同构于 $\mathbb{R}$ 的子域.

(3) 干脆将 $\mathbb{R}_0$ 与 $\mathbb{R}$ 等同,将 $\begin{pmatrix}a&0\\0&a\end{pmatrix}$ 写成 a,则可写

$$\begin{pmatrix}a&b\\-b&a\end{pmatrix}=\begin{pmatrix}a&0\\0&a\end{pmatrix}+\begin{pmatrix}b&0\\0&b\end{pmatrix}\begin{pmatrix}0&1\\-1&0\end{pmatrix}=a+b\begin{pmatrix}0&1\\-1&0\end{pmatrix}.$$

作映射

$$\mathbb{C}\xrightarrow{\varphi}\mathbb{C}_0,\quad a+bi\longmapsto a+b\begin{pmatrix}0&1\\-1&0\end{pmatrix},\quad \forall a,b\in\mathbb{R},$$

则 φ 是域同构.

以下 2 – 6 题出现的运算是 F_2 中元素的运算.

2. 计算

$$\begin{pmatrix}1&1&1&1&0&0&1\\0&1&0&1&1&0&1\\0&0&1&0&1&1&1\\1&1&1&0&1&1&0\end{pmatrix}\begin{pmatrix}1&1&1\\1&0&1\\1&0&0\\1&1&1\\0&1&0\\0&0&1\\1&1&0\end{pmatrix}.$$

3. 求

$$\begin{pmatrix}1&1&1&1\\0&0&1&1\\1&1&0&1\\0&1&1&1\end{pmatrix}^{-1}.$$

4. 解方程组

$$\begin{cases}x_1+x_2+x_3+x_4+x_5+x_6=1\\x_3+x_4+0+x_6=0\\x_1+x_2+0+x_4=1\\x_2+x_3+x_4=0.\end{cases}$$

5. 计算

$$(x^4+x^3+x+1)^2,(x^3+x^2+1)(x^5+x^2+x+1).$$

6. (1) 以 x^2+x+1 除 $x^6+x^4+x^3+1$,求商及余式.

(2) 求 x^2+x+1 与 $x^6+x^4+x^3+1$ 的最大公因式 $d(x)$.

(3) 求 $u(x),v(x)$,使

$$u(x)(x^2+x+1)+v(x)(x^6+x^4+x^3+1)=d(x).$$

7. 求作一个 13 位 0,1 序列的码集合，其容量为 2^9，有纠一个错的能力.

8. F 为特征 p 的域，$a, b, a_1, \cdots, a_n \in F$，则

(1) $(a+b)^p = a^p + b^p$，进而不管 p 为奇偶皆有 $(a-b)^p = a^p - b^p$.

(2) $(a+b)^{p^k} = a^{p^k} + b^{p^k}$.

(3) $(a_1 + a_2 + \cdots + a_n)^{p^k} = a_1^{p^k} + a_2^{p^k} + \cdots + a_n^{p^k}$.

(参见引论章习题 6)

(4) 映射　$F \xrightarrow{\varphi} F$，

$a \longmapsto a^p$

是 F 的自同态. 且 φ 是同构当且仅当方程 $x^p - b = 0$ 对所有 $b \in F$ 都有解.

§2　域的扩张，扩张次数，单扩张的构造

令 E 是域，$F \subset E$，若 F 在 E 的运算下也成为域，则称 F 为 E 的**子域**，而 E 称为 F 的**扩域**.

扩域的用处常常表现在：子域 F 中的某些数学问题只在 F 中考虑就不能解决或是不能简单地得到解决，而在扩域中就容易解决.

例 1　对有理数域 $\mathbb{Q}$ 上的矩阵

$$A = \begin{pmatrix} 1 & 5 \\ 1 & 1 \end{pmatrix},$$

求 A^k 的迹.

解　如果想先求出 A^k，再求出它的迹这将是很难的. 但如我们先把 A^k 的特征值求出来，立即就能求出迹. 我们知道 A^k 的特征值是 A 的特征值的 k 次幂. 而

$$|\lambda I - A| = \begin{vmatrix} \lambda - 1 & -5 \\ -1 & \lambda - 1 \end{vmatrix} = (\lambda - 1)^2 - 5$$

$$= (\lambda - 1 + \sqrt{5})(\lambda - 1 - \sqrt{5}).$$

在 $\mathbb{Q}$ 中是算不出 A 的特征值的. A 的两个特征值是 $1 \pm \sqrt{5}$，属于实数域 $\mathbb{R}$. 而 A^k 的两个特征值是 $(1+\sqrt{5})^k$ 及 $(1-\sqrt{5})^k$，于是

$$\mathrm{Tr}(A^k) = (1+\sqrt{5})^k + (1-\sqrt{5})^k.$$

例 2　在实可微函数范围内求下列微分方程的通解：

$$y'' + a^2 y = 0, \qquad a \text{ 是实数} > 0.$$

令 $y = e^{\lambda x}$，代入方程，则 $\lambda^2 e^{\lambda x} + a^2 e^{\lambda x} = 0$. 所以 $\lambda^2 + a^2 = 0$，$\lambda = \pm ai$. 故 $y = c_1 e^{iax} + c_2 e^{-iax}$ 是通解. 但它不全为实值函数. 考察 $e^{\pm iax}$ 的实部 $\cos ax$ 和

虚部 $\sin ax$ 也是方程的解，且是线性无关的.故实函数的通解是

$$y = c_1\cos ax + c_2\sin ax, \quad c_1, c_2 \in \mathbb{R}.$$

上面两个例子中都表现出即使在子域中有解答的数学问题，要求出这个解答，比较简单的方法却是在它的扩域中进行的.这是引进扩域的一个好处.

先来考察下述问题：设 E 是域 F 的扩域，任取 $\alpha \in E$，问用 F 的元素及 α 尽可能多次地进行加减乘除运算，能作出一个什么样的集合？记这个集合为 $F(\alpha)$.可证

$$F(\alpha) = \left\{ \frac{f_1(\alpha)}{f_2(\alpha)} \middle| f_1(x), f_2(x) \in F[x], f_2(\alpha) \neq 0 \right\}, \tag{1}$$

其中 $F[x]$ 是 F 上多项式的集合.

实际上，每个 $\dfrac{f_1(\alpha)}{f_2(\alpha)}$ 皆可由 F 的元素和 α 经多次加减乘除来得到，故(1)的右端 $\subseteq$ (1) 的左端.

反之，用 F 的元素和 α 经多次加减乘(没有除)其结果必是某 $f(\alpha), f(x) \in F[x]$.作一次除法就是(1)式右端的形式的元素.而(1)式右端的元素再进行加减乘除，其结果仍为这种形式.故(1)的左端 $\subseteq$ (1) 的右端，(1)式成立.

可以把一个元 α 推广到 E 中的一个子集 S，而得

命题 1 设 $F \subset E$ 是域扩张及 S 是 E 的一个子集.令

$$F(S) = \left\{ \frac{f_1(\alpha_1, \cdots, \alpha_k)}{f_2(\alpha_1, \cdots, \alpha_k)} \middle| \begin{array}{l} \forall \text{ 正整数 } k, \forall \alpha_1, \alpha_2, \cdots, \alpha_k \in S, \\ \forall f_i(x_1, x_2, \cdots, x_k) \in F[x_1, x_2, \cdots, x_k], \\ i = 1, 2, f_2(\alpha_1, \alpha_2, \cdots, \alpha_k) \neq 0 \end{array} \right\}, \tag{2}$$

则 $F(S)$ 是用 F 的元素和 S 中元素尽可能多次地加减乘除得到的元素的集合.它是 E 的子域，且是 E 中含 F 及 S 的最小的域.

证明 用上一段对 $F(\alpha)$ 的类似的讨论，(2)式同样成立.并且 $F(S)$ 对加减乘除都封闭.故 $F(S)$ 是 E 的子域.

又对 E 的任一子域 I，若它含有 F 及 S，则含有由 F 及 S 的元素尽可能多次地经加减乘除后所得的集合 $F(S)$.故 $F(S)$ 是 E 的含 F 及 S 的最小的子域.

定义 1 E 是 F 的扩域，$S \subset E$，称域 $F(S)$ 为 F **添加** S **而成的扩域**.

命题 2 E 为 F 的扩域，$S_1, S_2 \subset E$，则 $F(S_1)(S_2) = F(S_1 \cup S_2)$.

证明 显然 $F, S_1, S_2 \subset F(S_1)(S_2)$，故由命题 1 有

$$F(S_1 \cup S_2) \subset F(S_1)(S_2).$$

又 $F(S_1 \cup S_2)$ 包含 $F(S_1)$ 及 S_2，仍由命题 1 有

$$F(S_1 \cup S_2) \supset F(S_1)(S_2).$$

这就证明了命题.

特别当 S 为有限集合，$S=\{\alpha_1,\cdots,\alpha_n\}$ 时，记 $F(S)=F(\alpha_1,\cdots,\alpha_n)$. 它可以按 $\alpha_1,\cdots,\alpha_n$ 的任何次序，从 F 起逐个地添加进去成为 $F(\alpha_1,\cdots,\alpha_n)$.

定义 2 E 是 F 的扩域，$\alpha,S\subset E$，则称 $F(\alpha)$ 为 F 的**单扩域**，而当 S 为有限集时，称 $F(S)$ 为 F 的**有限生成的扩域**.

上面讲了一类扩域，它是由添加一组元素而得. 下面描述扩域的一个重要性质.

设 E 是 F 的扩域. E 有加法，又有乘法，把 F 对 E 的乘法看成域 F 对 E 的数量乘积，则 E 自然地成为 F 上的线性空间*（关于线性空间的其他运算规则是自然成立的）.

定义 3 设 E 是 F 的扩域. 以 $[E:F]$ 表示 E 作为 F 上线性空间的维数，称为 E 对 F 的**扩张次数**. 若 $[E:F]=\infty$，则称为**无限次扩域**；若 $[E:F]=n$，则称为**有限次（n 次）扩域**.

定理 3 设 $F\subset H\subset E$ 是域的扩张，则 $[E:F]=[E:H][H:F]$.

证明 先设 $[E:H]=n$，$[H:F]=m$. 设 $e_1,\cdots,e_n$ 是 E 作为 H 上线性空间的一组基，$h_1,\cdots,h_m$ 是 H 作为 F 上线性空间的一组基. 故 E 的任意元素 e 可表成 $e=\sum_{i=1}^{n}l_ie_i$，$l_i\in H$，而 l_i 可表成 $l_i=\sum_{j=1}^{m}f_{ij}h_j$，$i=1,\cdots,n$，$f_{ij}\in F$. 于是

$$e=\sum_{i=1}^{n}l_ie_i=\sum_{i=1}^{n}\Big(\sum_{j=1}^{m}f_{ij}h_j\Big)e_i=\sum_{i=1}^{n}\sum_{j=1}^{m}f_{ij}e_ih_j$$

是 $\{e_ih_j\mid i=1,\cdots,n;j=1,\cdots,m\}$ 的线性组合，系数在 F 上. 我们要证明它是 E 作为 F 上线性空间的一组基. 这只要证明 $\{e_ih_j,i=1,\cdots,n;j=1,\cdots,m\}$ 是 F 上线性无关的. 设有 $\sum_{i=1}^{n}\sum_{j=1}^{m}l_{ij}e_ih_j=0$，$l_{ij}\in F$，$i=1,\cdots,n;j=1,\cdots,m$. 于是 $\sum_{j=1}^{m}l_{ij}h_j\in H$，$i=1,\cdots,n$，而得 H 上的一个线性关系：$\sum_{i=1}^{m}\Big(\sum_{j=1}^{m}l_{ij}h_j\Big)e_i=0$. 但 $e_1,\cdots,e_n$ 是 H 上线性无关的，故

$$\sum_{j=1}^{m}l_{ij}h_j=0,\qquad i=1,2,\cdots,n.$$

又由于 $l_{ij}\in F$ 及 $h_1,\cdots,h_m$ 是 F 上线性无关的，故 $l_{ij}=0$，$i=1,\cdots,n;j=1,\cdots,m$. 故 $\{e_ih_j\ i=1,\cdots,n;j=1,\cdots,m\}$ 在 F 上线性无关，因而是 E 作为 F 上线性空间的基. 这就证明了 $[E:F]=mn=[E:H][H:F]$.

现设 $[E:H]$，$[H:F]$ 有一个为 ∞，若 $[H:F]=\infty$，则对任意正整数 m，

---

* 很多书上称为 F 上向量空间.

H 中有 m 个 F 上线性无关的元素 $h_1,\cdots,h_m$. 由 $H\subset E$,这也是 E 中 m 个 F 上线性无关的元素,于是 E 对 F 的维数大于任意正整数 m,故 $[E:F]=\infty=[E:H][H:F]$.

对 $[E:H]=\infty$ 的情形. 对任意正整数 m,E 中有 m 个 H 上线性无关的元素,由于 $F\subset H$. 这当然也是 F 上线性无关的元素. 故 E 对 F 的维数大于任意正整数 m,因此 $[E:F]=\infty=[E:H][H:F]$. 证毕.

推论 设 $F\subset H\subset E$ 为域扩张. 若都是有限次扩张,则有

$$[H:F]\mid[E:F].$$

定义 4 $F\subset E$ 为域扩张,$\alpha\in E$. 若 α 是 F 上某一非零多项式的根,则称 α 为 F 上**代数元**. 而 $F(\alpha)$ 称为 F 上**单代数扩张**. 若 $\alpha\in E$ 不是 F 上代数元,则称为 F 上**超越元**. $F(\alpha)$ 称为 F 上**单超越扩张**. 若 E 中每个元都是 F 上代数元,则称 E 是 F 上**代数扩张**.

例 1 $\sqrt{2},\sqrt[3]{2}$ 皆为 $\mathbb{Q}$ 上代数元. π,e 是 $\mathbb{Q}$ 上超越元.

下面的定理给出了单扩张的构造及单扩张的次数.

定理 4 $F\subset E$ 是域扩张. $\alpha\in E$ 是 F 上代数元当且仅当有 F 上不可约多项式 $f(x)$ 以 α 为根. 这样的 $f(x)$ 是 F 上以 α 为根的最低次多项式. 设 $\partial(f(x))=n$,则 $[F(\alpha):F]=n$,且 $1,\alpha,\cdots,\alpha^{n-1}$ 是 $F(\alpha)$ 作为 F 上线性空间的基. 若 $\alpha\in E$ 是 F 上超越元,则 $[F(\alpha):F]=\infty$.

证明 设 $\alpha\in E$ 是 F 上代数元,故有 $p(x)\in F[x]$,使 $p(\alpha)=0$. 将 $p(x)$ 分解成 $F[x]$ 中不可约多项式的乘积,$p(x)=p_1(x)\cdots p_s(x)$,则 $p(\alpha)=p_1(\alpha)\cdots p_s(\alpha)=0$. 由于 E 中无零因子,故必有某 i,$p_i(\alpha)=0$. 这个 $p_i(x)$ 即为定理中所要的不可约多项式 $f(x)$. 反之,若有 F 上不可约多项式以 α 为根,当然 α 是 F 上代数元.

又设 $m(x)$ 是 F 上满足 $m(\alpha)=0$ 的多项式. 作除法算式

$$m(x)=q(x)f(x)+r(x),$$

这里 $r(x)$ 或为零或 $\partial(r(x))<\partial(f(x))$. 代入 α,由 $f(\alpha)=m(\alpha)=0$,知 $r(\alpha)=0$. 若 $r(x)\neq 0$,$\partial(r(x))<\partial(f(x))$. 由 $f(x)$ 不可约得 $r(x),f(x)$ 互素. 故有 $u(x),v(x)$ 为 F 上多项式使 $u(x)f(x)+v(x)r(x)=1$. 再用 α 代入,左端为零与右端为 1,矛盾. 故 $r(x)=0$.

以上证明了 F 上任何以 α 为根的多项式 $m(x)$ 都是 $f(x)$ 的倍数. 因此 $f(x)$ 是 F 上最低次的以 α 为根的多项式.

再来看

$$F(\alpha)=\left\{\frac{f_1(\alpha)}{f_2(\alpha)}\,\middle|\,\forall f_1(x),f_2(x)\in F[x],f_2(\alpha)\neq 0\right\}.$$

我们能进一步简化这个集合的结构.

首先对任何 $f_2(x)$,若 $f_2(\alpha)\neq 0$,则显然 $f(x)\nmid f_2(x)$.又 $f(x)$ 不可约,得 $f(x),f_2(x)$ 互素,有 $u(x),v(x)\in F[x]$ 使

$$u(x)f(x)+v(x)f_2(x)=1.$$

将 α 代入,由 $f(\alpha)=0$,得到

$$v(\alpha)f_2(\alpha)=1.$$

但是 $f_2(\alpha)\neq 0$,故 $v(\alpha)=\dfrac{1}{f_2(\alpha)}$.这样 $F(\alpha)$ 的任一元 $\dfrac{f_1(\alpha)}{f_2(\alpha)}$ 必有形式 $f_1(\alpha)v(\alpha)$.它是以 F 的元为系数的 α 的多项式.令 $M(x)=f_1(x)v(x)\in F[x]$.作除法算式

$$M(x)=q(x)f(x)+r(x),$$

可知

$$r(x)=a_0\cdot 1+a_1\cdot x+\cdots+a_{n-1}x^{n-1},a_i\in F,i=0,1,\cdots,n-1.$$

于是 $M(\alpha)=a_0\cdot 1+a_1\cdot\alpha+\cdots+a_{n-1}\alpha^{n-1}$.这就说明 $F(\alpha)$ 的任一元是 $1,\alpha,\cdots,\alpha^{n-1}$ 的 F 上的线性组合.

下面再证 $1,\alpha,\cdots,\alpha^{n-1}$ 在 F 上是线性无关的.设 $a_0,a_1,\cdots,a_{n-1}\in F$,使得 $a_0\cdot 1+a_1\cdot\alpha+\cdots+a_{n-1}\alpha^{n-1}=0$.令

$$r(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}\in F[x],$$

则 $r(\alpha)=0$.上面已证 $f(x)$ 是以 α 为根的 F 上最低次多项式,其次数为 n.而 $r(x)$ 以 α 为根,若不为 0,则次数 $\leqslant n-1$ 与 $f(x)$ 的次数最低矛盾.故 $r(x)=0$,于是 $a_0,a_1,\cdots,a_{n-1}$ 全为 0.因此 $1,\alpha,\cdots,\alpha^{n-1}$ 在 F 上线性无关.

这样我们就证明了 $F(\alpha)$ 作为 F 上线性空间以 $1,\alpha,\cdots,\alpha^{n-1}$ 为一组基.当然有 $[F(\alpha):F]=n$.

当 α 为 F 上超越元时.对任意 m,若有 $a_0,a_1,\cdots,a_{n-1}\in F$,使

$$a_0\cdot 1+a_1\cdot\alpha+\cdots+a_{n-1}\alpha^{n-1}=0.$$

即有 F 上多项式 $a_0+a_1x+\cdots+a_{n-1}x^{n-1}$ 以 α 为根,由于 α 是 F 上超越元,这只能是零多项式,即有 $a_0=a_1=\cdots=a_{n-1}=0$.故对任意 n,$1,\alpha,\cdots,\alpha^{n-1}$ 在 F 上线性无关.故 $F(\alpha)$ 中有任意多个 F 上线性无关的元素,即 $[F(\alpha):F]=\infty$.

定义 5 $F\subset E$ 是域扩张,$\alpha\in E$ 为 F 上代数元.F 上以 α 为根的次数最低的多项式称为 α **的极小多项式**.

推论 $F\subset E$ 为域扩张,$\alpha\in E$ 为 F 的代数元,则 F 上以 α 为根的不可约多项式就是 α 的极小多项式.且 F 上任意以 α 为根的多项式以极小多项式为其因式,于是最多差一个倍数,极小多项式是唯一的.

证明 分析定理 4 的证明过程可得到结论.

例 2 计算$[\mathbb{Q}(\sqrt{5}):\mathbb{Q}]$.

解 $\sqrt{5}$ 满足 $\mathbb{Q}$ 上多项式方程 $x^2-5=0$,且 x^2-5 在 $\mathbb{Q}$ 上不可约,故 $[\mathbb{Q}(\sqrt{5}):\mathbb{Q}]=2$.

例 3 计算$[\mathbb{Q}(\pi):\mathbb{Q}]$.

解 由数学分析中知道,π 是 $\mathbb{Q}$ 上超越元,故$[\mathbb{Q}(\pi):\mathbb{Q}]=\infty$.

习 题

1. $F\subset E$ 是域扩张.

(1) $\alpha_1,\alpha_2,\cdots,\alpha_s\in E$,则

$$F(\alpha_1,\alpha_2,\cdots,\alpha_s)=\left\{\frac{f_1(\alpha_1,\cdots,\alpha_s)}{f_2(\alpha_1,\cdots,\alpha_s)}\middle|\ f_1,f_2\in F[x_1,\cdots,x_s],f_2(\alpha_1,\cdots,\alpha_s)\neq 0\right\}.$$

(2) $S\subset E$,则

$$F(S)=\bigcup_{\substack{S_0\subset S\\ S_0\text{有限}}}F(S_0).$$

2. 计算$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]$,$[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}]$.证明

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}].$$

3. $F\subset E$ 是域扩张,且$[E:F]=p$ 是素数,则任意 $\alpha\in E\setminus F$,有 $E=F(\alpha)$.

4. $E\supset F$ 为域扩张,$\alpha_1,\alpha_2,\cdots,\alpha_t\in E$,$[F(\alpha_i):F]=n_i$,$i=1,2,\cdots,t$,则$[F(\alpha_1,\cdots,\alpha_t):F]\leqslant n_1n_2\cdots n_t$.

5. $F\subset E$ 为有限次域扩张,则必为代数扩张.

6. $F\subset E$ 为有限次域扩张,则有 $\alpha_1,\cdots,\alpha_t\in E$,使得 $E=F(\alpha_1,\cdots,\alpha_t)$.

7. $F\subset E$ 为域扩张,$S\subset E$ 且 S 中每个元皆是 F 上代数元,则 $F(S)$ 是 F 上代数扩张.进而,E 中全部代数元作成 F 的一个扩域.

8. 令 $E=\mathbb{Q}(u)$.

(1) 设 $u^3-u^2+u+2=0$.试把$(u^2+u+1)(u^2-u)$ 和$(u-1)^{-1}$ 表成 au^2+bu+c 的形式,$a,b,c\in\mathbb{Q}$.

(2) 若 $u^3-2=0$,把$\dfrac{u+1}{u-1}$ 表成 au^2+bu+c 的形式,$a,b,c\in\mathbb{Q}$.

9. 令 $E=F(u)$,u 是极小多项式为奇数次的代数元.证明 $E=F(u^2)$.

10. 求$\sqrt[3]{2}+\sqrt{5}$ 在 $\mathbb{Q}$ 上的极小多项式.

11. $E\supset F$,E 是环,F 是域.$s\in E$ 是 F 上代数元,则 s 可逆当且仅当有 F 上多项式 $f(x)$,其常数项不为零使 $f(s)=0$.并且 $s^{-1}=g(s)$,$g(x)$ 是 F 上多项式.

12. E 是 F 上的代数扩张，则 E 的含 F 的子环都是子域.

13. 设 $[E:F]=n$，则不存在子域 G，使 $E\supset G\supset F$ 及 $[G:F]$ 与 n 互素.

14. $\mathbb{R}$(实数域) 上任意代数扩张 E 若不为 $\mathbb{R}$，则同构于 $\mathbb{C}$. 特别地，$\mathbb{R}$ 上除二次扩域外没有其它有限次扩域.(这正是 Hamilton 等数学家找不到“三维复数”的原因).

§3　古希腊三大几何作图难题的否定

在学习“平面几何”课程时，我们做过很多作图题，即用圆规和直尺(没有刻度的直尺，只能划直线) 作出要求的几何量或几何图形. 如平分给定的任意角，任意等分一个线段 …… . 在古希腊几何学的研究中，曾提出了几个耐人寻味的“难题”. 要求只用圆规和直尺解决下列问题：

(1) 三等分任意角问题；

(2) 倍立方问题：从一个给定的立方体，求作另一个立方体，其体积是原体积的两倍. 亦即给定长度 u，求作另一长度 $\sqrt[3]{2}u$；

(3) 化圆为方问题：求作一个正方形，其面积等于一给定半径的圆的面积. 即已知半径 r，求作一个长度 a，使 $a=r\sqrt{\pi}$.

对问题(1)，任意给定单位长度 OA，已知一个角 θ 等同于知道长度 $OB=\cos\theta$(见图 1).

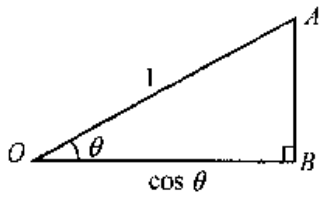


图 1

这是因为用圆规和直尺可以作出直角三角形 OAB，其中 $OB=\cos\theta$. 于是求作角 $\frac{1}{3}\theta$ 就等于求作量 $\cos\frac{1}{3}\theta$.

上面的三个问题最后都是否定的答案. 即只用圆规、直尺来作图是不能达到目的的. 下面我们逐步给以分析，关键步骤中利用了域的扩张的概念及扩张次数的性质，即前一节中定理 3、定理 4 中的结论.

第一步我们对能用圆规和直尺作图(当然实践上是有限步作图) 作出的量作一番分析. 作图能作出一些线段的长度和一些角. 由于角的正弦、余弦又表现为长度，因此我们只须分析能作出一些什么样的长度. 为此，在平面上取

一个直角坐标系(取定某已知线段的长度作单位长).

几何作图中先给定一些已知量,按上面的所说,即有一些已知线段及其长度,以已知线段的长度作坐标可得一些已知点.解析几何中已知

(α) 以定点(x_0,y_0)为中心,R为半径的方程是

$$(x-x_0)^2+(y-y_0)^2=R^2.$$

(β) 过点(x_1,y_1)和(x_2,y_2)的直线的方程是

$$(y_2-y_1)(x-x_1)-(x_2-x_1)(y-y_1)=0.$$

(γ) 两点$(x_1,y_1),(x_2,y_2)$之间的距离为

$$d=\sqrt{(x_2-x_1)^2+(y_2-y_1)^2}.$$

用圆规和直尺作图就是作圆,作直线,画出它们的交点以及截取两点间线段的长度.当$(\alpha),(\beta)$中的$(x_i,y_i),i=0,1,2$,及R是已知量或已作出的量时,就可作出交点.作出的交点的两个坐标以及两个点的距离就是作图能作出的新量.从代数上看每一次交点就是(α)中或(β)中的两个方程,或是(α)中一个方程和(β)中一个方程的联立方程组的求解.截取两点之间的距离是计算平方根.这些量可由已知量(或已作出的量),及某已知量(或某已作出的量)的平方根经加减乘除来得到(读者验证一下).自然地我们想到用域的扩张的手段来描述作图求出的量究竟在什么范围内.

作图是逐步进行的,第一次作图前,有一些已知量.因单位长度是给定的,故1是已知的.由1经多次加减乘除可得任何有理数,我们知道作图可实现加减乘除,故可设任何有理数是已知的.令$\mathbb{Q}$为有理数域,若还有些已知量为非有理数$a_1,a_2,\cdots,a_k$,则有$\mathbb{Q}$的扩域$E_0=\mathbb{Q}(a_1,a_2,\cdots,a_k)$.$E_0$中的量可由$\mathbb{Q}$的量及$a_1,a_2,\cdots,a_k$经加减乘除得到,因此可用作图来实现.仍可称$E_0$的量为已知量.因此在作图前有一个已知量作成的数域$E_0$.第一次作图的结果可由已知量及某一已知量的平方根$a_1$(也许仍在$E_0$中)经加减乘除运算表示出来.记$E_1=E_0(a_1)$,则作图的结果属于域$E_1$.同样地第二次作图的结果属于域$E_2=E_1(a_2)=E_0(a_1,a_2)$,其中$a_2$是$E_1$中某个元的平方根,……,第$k$次作图的结果属于域$E_k=E_{k-1}(a_k)=E_0(a_1,a_2,\cdots,a_k)$,其中$a_k$是$E_{k-1}=E_0(a_1,\cdots,a_{k-1})$中某个元的平方根.仅用圆规、直尺来作图经过$k$步后所得的结果必须落在某个域$E_0(a_1,\cdots,a_k)$中.

我们还能估计扩张次数$[E_0(a_1,\cdots,a_k):E_0]$.实际上$a_i$是$E_{i-1}$中某个元的平方根即$a_i^2\in E_{i-1},i=1,2,\cdots,k$.若$a_i\notin E_{i-1}$,则$a_i$是$E_{i-1}$上不可约多项式$x^2-a_i^2$的根.由$E_i=E_{i-1}(a_i)$,及§2定理4及推论,得$[E_i:E_{i-1}]=2$;若$a_i\in E_{i-1}$,则$[E_i:E_{i-1}]=1$.于是

$$[E_0(a_1,a_2,\cdots,a_k):E_0]$$

$$= [E_0(\alpha_1,\alpha_2,\cdots,\alpha_k):E_0(\alpha_1,\cdots,\alpha_{k-1})][E_0(\alpha_1,\cdots,\alpha_{k-1}):E_0(\alpha_1,\cdots,\alpha_{k-2})]$$
$$\cdots[E_0(\alpha_1):E_0]$$
$$= [E_k:E_{k-1}][E_{k-1}:E_{k-2}]\cdots[E_1:E_0] = 2^l, \quad 0 \leqslant l \leqslant k.$$

这即说从 E_0 出发用圆规直尺作图所得的量必在 E_0 的某个有限次扩域中，并且这个扩域对 E_0 的扩张次数是 2 的幂.

经过上面对出几何作图所得的几何量的一番代数上的分析后，我们可以来回答前面的三个作图难题了.

(1) 三等分任意角问题.

此问题中是已知有理数域 $\mathbb{Q}$ 及已知某角的余弦 $\cos\theta$，求作 $\cos\frac{1}{3}\theta$. 由三角恒等式 $\cos\theta = 4\cos^3\frac{1}{3}\theta - 3\cos\frac{1}{3}\theta$. 例如 $\theta = 60°$，则 $\cos60° = \frac{1}{2}$，$E_0 = \mathbb{Q}(\cos60°) = \mathbb{Q}$. 而 $\cos20°$ 满足 $4x^3 - 3x - \frac{1}{2} = 0$. 易检验它没有有理根，因此它的左端是 $\mathbb{Q} = E_0$ 上不可约多项式(读者试证明之). 故 $[E_0(\cos20°):E_0] = 3$(§2 定理 4 及推论). 若 $\cos20°$ 能用圆规和直尺作图得到，则必存在于 E_0 的某扩域 E 中，且 $[E:E_0] = 2$ 的幂. 于是由

$$[E:E_0] = [E:E_0(\cos20°)][E_0(\cos20°):E_0],$$

就有 $3|[E:E_0]$ 2 的幂，矛盾. 故 $\cos20°$ 不能从 $\mathbb{Q}(\cos60°)$ 的量出发用圆规和直尺作图作出它. 自然用圆规、直尺作图不能将 $60°$ 角三等分.

注 三等分任意角问题的答案是并非任何角都能用圆规直尺作图将它三等分，例如 $60°$ 角就不能. 但有些角例如 $90°, 180°\cdots$ 还是可以作到的. 又注意，某个角不能用圆规、直尺作图进行三等分，并不排除可用别的数学方法将它三等分.

(2) 倍立方问题.

此问题中已知 $\mathbb{Q}$ 及一个量 u，求作 $\sqrt[3]{2}u$. 这时 $E_0 = \mathbb{Q}(u)$，而 $\sqrt[3]{2}u$ 满足 $x^3 - 2u^3 = 0$. 取 $u = 1$，这时 $E_0 = \mathbb{Q}$. 易知 $x^3 - 2$ 是 $\mathbb{Q}$ 中不可约多项式，故 $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3$. 与第(1)问题中一样，$\sqrt[3]{2}$ 不能从 $\mathbb{Q}$ 出发用圆规、直尺作图作出来.

(3) 化圆为方.

这时已知 $\mathbb{Q}$ 及半径 R，求作 $\sqrt{\pi}R$. 可取 $R = 1$，则 $E_0 = \mathbb{Q}(R) = \mathbb{Q}$，而 $E_0(\sqrt{\pi}) = \mathbb{Q}(\sqrt{\pi})$. 易知 $\pi \in \mathbb{Q}(\sqrt{\pi})$，故

$$[\mathbb{Q}(\sqrt{\pi}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{\pi}):\mathbb{Q}(\pi)][\mathbb{Q}(\pi):\mathbb{Q}].$$

由于 π 是 $\mathbb{Q}$ 上的超越元，$[\mathbb{Q}(\pi):\mathbb{Q}] = \infty$，故 $[\mathbb{Q}(\sqrt{\pi}):\mathbb{Q}] = \infty$. 这样 $\sqrt{\pi}$ 不能含在 $\mathbb{Q}$ 上的任何有限次扩域中. 故不能从 $\mathbb{Q}$ 出发用圆规、直尺作图来得到它.

至此,我们论证了古希腊的三大作图难题的答案是:不可能.

习 题

1. 设已知量 a,b 及 r 皆大于0且 $a>b$. 试用圆规直尺来作出 $a\pm b, ab, \frac{a}{r}, \sqrt{r}$.

2. 下列哪些量可以用圆规直尺来作出:

(1) $\sqrt[4]{5+2\sqrt{6}}$ (2) $\dfrac{2}{1+\sqrt{7}}$

(3) $1-\sqrt[5]{27}$

3. 下列多项式中哪些多项式的实根可用圆规直尺作出:

(1) $x^2-7x-13$ (2) x^4-5

(3) x^3-10x^2+1 (4) x^5-9x^3+3

(5) x^4-2x-3

4. 证明:实数 α 可用圆规直尺作出当且仅当有实数的域的序列 $E_0\subset E_1\subset\cdots\subset E_{n-1}\subset E_n$,使 $\alpha\in E_n$,且 $[E_i:E_{i-1}]=2, 1\leqslant i\leqslant n$,其中 E_0 是已知量的域.

§4 环的例子,几个基本概念

本节先介绍环的几种典型例子,然后介绍子环、同态、理想、商环(也称剩余类环)、同态基本定理. 这些基本概念是群中有关的概念在环中的推广,在某些情形下商环是域,这就提供了一种构造新域的方法. 用此方法可以造出有限个元的域,也可对于某域 F 上的多项式造出该域的一个扩域,使得此扩域中有元素是该多项式的根. 我们知道在整数环上作所有的分式就可得有理数域,推广到一般整环也能构造它的分式域.

读者可以看出本节虽是讲环的内容,但主要目的还是介绍造扩域、造新域的一些方法. 环论的一些重要内容如因式分解唯一性定理、中国剩余定理等将在本书的最后一章中讨论.

回忆引论章中环 R 的定义:R 是非空集合,有两个代数运算,称为加法和乘法. R 对于加法成为交换群. $R^*=R\setminus\{0\}$ 对于乘法成为幺半群. R 的乘法对于加法有分配律.

与有些书上不同,本书的环要求含有乘法单位元1.

例1 以 $\mathbb{Z}$ 表全体整数的集合. 它对于数的加法、减法和乘法是封闭的.

但除法不封闭,整数在 $\mathbb{Z}$ 中一般没有乘法逆元素.$\mathbb{Z}$ 是一个环.

例 2 域 F 上全体多项式的集合 $F[x]$,在多项式的加法、减法和乘法下是封闭的.多项式在 $F[x]$ 中一般没有乘法逆元素.$F[x]$ 是一个环.

例 3 全体偶数的集合对于数的加法、减法和乘法是封闭的.该集合不但除法不封闭,而且没有乘法单位元.它不是一个环.

($F[x]$ 中有这样的集合吗?)

例 4 域 F 上全体 $n \times n$ 矩阵的集合 $M_n(F)$ 在矩阵的加法、减法、乘法下是封闭的.但不是每个 $n \times n$ 矩阵都有逆矩阵,更有甚者,矩阵的乘法没有交换律.但 $M_n(F)$ 是环.

定义 1 设 R 是环,若它的乘法满足交换律,则称为**交换环**.

定义 2 R 是环.S 是 R 的子集,它含有 R 的乘法单位元 1,且对于 R 的运算仍成为环,则称 S 为 R 的**子环**.

注意,我们的定义要求环 R 与子环有同一个乘法单位元素.

例 5 域 F 是环.若它的子环 S 是域,则 S 是 F 的子域.

定义 3 设 R, R' 是两个环,φ 是从 R 到 R' 的映射,如果

1) φ 保持加法,即 $\forall x, y \in R$,有 $\varphi(x+y) = \varphi(x) + \varphi(y)$,

2) φ 保持乘法,即 $\forall x, y \in R$,有 $\varphi(xy) = \varphi(x)\varphi(y)$,

3) $\varphi(1_R) = 1_{R'}$,

则称 φ 为环 R 到环 R' 的**同态**.若 φ 还是双射,则称 φ 为 R 到 R' 的**同构**.称 φ 是域 F 到域 F' 的同态(或同构),若它是 F 和 F' 作为环的同态(或同构).

回想群同态的象和核的定义,我们对环也有

定义 4 设 φ 是环 R 到 R' 的同态.令

$$\varphi(R) = \{\varphi(x) \mid x \in R\},$$

称为 R 在 φ 下的**象**.若 $\varphi(R) = R'$,则称为**满同态**.令

$$\mathrm{Ker}\varphi = \{x \in R \mid \varphi(x) = 0 \in R'\},$$

称为 R 在 φ 下的**核**.

命题 1 对环 R 到环 R' 的同态 φ 有

(1) 对 $\forall r \in R$,有 $r(\mathrm{Ker}\varphi) \subseteq \mathrm{Ker}\varphi$ 及 $(\mathrm{Ker}\varphi)r \subseteq \mathrm{Ker}\varphi$.

(2) φ 是单射当且仅当 $\mathrm{Ker}\varphi = \{0\}$.

证明 (1) 对 $\forall r \in R, \forall x \in \mathrm{Ker}\varphi$,

$$\varphi(rx) = \varphi(r)\varphi(x) = \varphi(r) \cdot 0 = 0.$$

故 $rx \in \mathrm{Ker}\varphi$,即 $r\mathrm{Ker}\varphi \subseteq \mathrm{Ker}\varphi$.同样还能证 $(\mathrm{Ker}\varphi)r \subseteq \mathrm{Ker}\varphi$.

(2) 对任意 $x, y \in R, x \neq y$,即 $x - y \neq 0$.

当 $\mathrm{Ker}\varphi = 0$ 时,$\varphi(x-y) \neq 0$,即 $\varphi(x) - \varphi(y) \neq 0$.也即 φ 为单射.

当 φ 为单射时,设 $x \neq 0$,则 $\varphi(x) \neq \varphi(0) = 0$.这即说明 $x \notin \mathrm{Ker}\varphi$,故

$\mathrm{Ker}\varphi = 0$.

$\mathrm{Ker}\varphi$ 是 R 到 R' 的环同态的核. R 与 R' 又是加群,这时 φ 当然也是加群同态. 而 $\mathrm{Ker}\varphi$ 是加群同态的核,必是 R 的加法子群. $\mathrm{Ker}\varphi$ 的这些性质使我们给出

定义 5 R 是环,S 是 R 的加法子群,且对 $\forall r \in R$ 有 $Sr \subseteq S$ 及 $rS \subseteq S$,则称 S 为 R 的一个**理想**.

对于群 G 及 G 的正规子群 H,我们已经在 H 对 G 的陪集上定义了运算:

$$(aH)(bH) = (ab)H,$$

使它成为一个群,即 G 对 H 的商群 $\frac{G}{H}$.

对环 R 如何作**商环**呢?就要利用 R 的理想 S. 这时 R 的加法群是交换群,它的理想 S 是 R 的加法子群,当然是正规子群. 自然有加法商群 $\frac{R}{S}$,这是对于 S 的剩余类 $a + S$ 的集合的加法群. 即

$$\frac{R}{S} = \{a + S \mid a \in R\},$$

其加法为

$$(a + S) + (b + S) = (a + b) + S, \quad \forall a, b \in R.$$

在 $\frac{R}{S}$ 上如能自然地定义乘法,才可使其成为商环. 为此我们对环 R 中的集合 K, L 规定集合乘积

$$KL = \{kl \mid k \in K, l \in L\}.$$

易知这个乘积有结合律.

来看两个剩余类 $a + S, b + S$ 的集合乘积,有

$$(a + S)(b + S) = \{ab + as_2 + s_1 b + s_1 s_2 \mid s_1, s_2 \in S\} \subset ab + S, \quad (1)$$

上式最后的包含关系用到了 S 是理想这个性质. 这个包含关系说明 $a + S$ 中任一元 a' 与 $b + S$ 中任一元 b' 的积 $a'b'$ 与 ab 属于同一剩余类. 即有

$$a'b' + S = ab + S.$$

由此可证

$$\frac{R}{S} \times \frac{R}{S} \xrightarrow{\varphi} \frac{R}{S},$$

$$(a + S, b + S) \longmapsto ab + S$$

是一个映射. 实际上若 $a + S = a' + S, b + S = b' + S$,则

$$\varphi((a' + S, b' + S)) = a'b' + S = ab + S = \varphi((a + S, b + S)).$$

我们把这映射作为 $\frac{R}{S}$ 上的另一代数运算:乘法,写成

$$(a + S)(b + S) = ab + S. \quad (2)$$

注意,(1) 与(2) 具有完全不同的意义.(1) 式是 R 中的集合乘积的一个关系式,(2) 式是 $\frac{R}{S}$ 上的代数运算.

这样,$\frac{R}{S}$ 作为 R 的加法群的商群已有加法:

$$(a+S)+(b+S)=(a+b)+S. \tag{3}$$

又有乘法(2).$\frac{R}{S}$ 对于加法已是一个群.$1+S$ 是 $\frac{R}{S}$ 的乘法单位元.由

$$\begin{aligned}&[(a+S)+(b+S)](c+S)\\&=(a+b)c+S=(a+S)(c+S)+(b+S)(c+S),\\&(c+S)[(a+S)+(b+S)]\\&=c(a+b)+S=(c+S)(a+S)+(c+S)(b+S),\\&[(a+S)(b+S)](c+S)\\&=(ab)c+S=a(bc)+S=(a+S)[(b+S)(c+S)],\end{aligned}$$

知 $\frac{R}{S}$ 的乘法对加法有分配律,乘法有结合律.故 $\frac{R}{S}$ 成为一个环,称为 R 对 S 的**商环**.

与群同态一样,也有

定理 2(环的同态基本定理)

(1) R 是环,S 是它的理想,则 R 到商环 $\frac{R}{S}$ 有满同态 $\eta:\eta(a)=a+S,\forall a\in R$,称为 R 到 $\frac{R}{S}$ 的**自然同态**.

(2) R,R' 是环.φ 是环 R 到环 R' 的满同态.令 $K=\mathrm{Ker}\varphi$,则商环 $\frac{R}{K}$ 与环 R' 同构.

证明 (1) $\eta(a+b)=a+b+S=(a+S)+(b+S)=\eta(a)+\eta(b)$,

$\eta(ab)=ab+S=(a+S)(b+S)=\eta(a)\eta(b),\eta(1)=1+S.$

故 η 保持加法和乘法,且把单位元映成单位元,它是同态.又

$$\eta(R)=\{\eta(a)\mid a\in R\}=\{a+S\mid a\in R\}=\frac{R}{S},$$

即 η 是满同态.

(2) 首先 $\varphi(a+K)=\varphi(a)$.这是因为 K 中任一元 k 在 φ 下的象为零,则

$$\varphi(a+k)=\varphi(a)+\varphi(k)=\varphi(a)+0=\varphi(a).$$

由此有 $\frac{R}{K}$ 到 R' 的映射

$$\frac{R}{S} \xrightarrow{\psi} R'$$

$$a + K \longmapsto \varphi(a + K) - \varphi(a).$$

又

$$\begin{aligned}
&\psi(a + K) + \psi(b + K)\\
&= \varphi(a) + \varphi(b) = \varphi(a + b) = \psi(a + b + K)\\
&= \psi((a + K) + (b + K)),\\
&\psi(a + K)\psi(b + K)\\
&= \varphi(a)\varphi(b) = \varphi(ab) = \psi(ab + K)\\
&= \psi((a + K)(b + K)). \quad \psi(1_R + K) = \varphi(1_R) = 1_{R'},
\end{aligned}$$

故 ψ 是 $\frac{R}{K}$ 到 R' 的环同态. 又 R 到 R' 的环的满同态 φ, 只看 R 与 R' 的加群结构是加群的满同态. 而 $K = \mathrm{Ker}\varphi$ 是加群同态的核. 由群的同态基本定理, ψ 是 $\frac{R}{K}$ 到 R' 的加群同构, 即 ψ 是双射. 故 ψ 是环同构.

以上我们一连串地把群中的基本概念与性质推广到环中, 其中理想这概念是从正规子群推广过来的. 我们举几个典型的环, 考察这些环中的理想都是什么样子.

例 7 任意环 R 中, 零元素构成的集合和 R 本身都是 R 的理想.

例 8 域 F 中, 只有零元构成的理想和 F 本身这两个理想.

实际上设 S 是 F 的一个非零理想, $s \in S$ 是它的非零元, 则 $s^{-1}s = 1 \in S$. 于是 $\forall a \in F, a \cdot 1 \in S$. 故 $S = F$.

例 9 对整数环 $\mathbb{Z}$, 设 H 是它的非零理想, 则 H 是循环加群 $\mathbb{Z} = 1 \cdot \mathbb{Z}$ 的子群. 由第一章 §7 定理 3 知, $H = n\mathbb{Z}$, n 为某正整数. 显然 $n\mathbb{Z}$ 是 $\mathbb{Z}$ 的理想. 故整数环 $\mathbb{Z}$ 的全部理想为 $n\mathbb{Z}, n = 0, 1, 2, \cdots$ (包括零元构成的理想).

例 10 R 是交换环, $a \in R$, 则 aR 是 R 的理想. 我们称它为 R 的**主理想**, 更详细一点说, 是 R 中由 a 生成的理想, aR 常记成 (a). (注意群 G 中由元 a 生成的群记成 $\langle a \rangle$)

例 11 设 $r, s \in \mathbb{Z}$, 皆不为零. 作

$$H = \{lr + ms \mid l, m \in \mathbb{Z}\},$$

则 H 是 $\mathbb{Z}$ 的理想. 由例 10 知 $H = n\mathbb{Z} = (n)$, n 为某正整数. 易证这个 n 是 r 和 s 的最大公因数.

例 12 F 是域, $F[x]$ 是 F 上多项式环, N 是 $F[x]$ 的非零理想, 则有非零多项式 $m(x)$, 使 $N = m(x)F[x] = (m(x))$.

证明 取 N 中次数最低的多项式为 $m(x)$. 任取 $f(x) \in N$, 作除法算式

$$f(x) = q(x)m(x) + r(x),$$

这里 $r(x) = 0$ 或 $\partial(r(x)) < \partial(m(x))$. 若 $r(x) \neq 0$, 则 $\partial(r(x)) < \partial(m(x))$. 由于 N 是理想, $q(x)m(x) \in N$, 又 $f(x) \in N$, 故

$$r(x) = f(x) - q(x)m(x) \in N.$$

这与 $m(x)$ 是 N 中最低次多项式矛盾. 因此 $r(x) = 0$, $f(x) = m(x)q(x)$. 这就证明了 $N = m(x)F[x]$.

例 10 及例 12 证明了整数环 $\mathbb{Z}$ 和域 F 上多项式环 $F[x]$ 的每个理想都是主理想.

下面的例子讨论非交换环 $M_n(F)$(域 F 上 $n \times n$ 方阵的环) 的理想.

例 13 $M_n(F)$ 只有零元的理想和自身两个理想.

证明 设 N 是 $M_n(F)$ 的非零理想. 记 e_{ij} 为第 i 行第 j 列的元素为 1, 其余位置上元素为零的 F 上 $n \times n$ 方阵. F 上任意 $n \times n$ 方阵 $A = (a_{ij})$, 可写成 $A = \sum_{i,j=1}^{n} a_{ij}e_{ij}$. 现设 $0 \neq A \in N$, 则有 $a_{lk} \neq 0$, 某 l, k. 于是 $e_{il}Ae_{kk} = \sum_{i,j=1}^{n} a_{ij}e_{il}e_{ij}e_{kk} = a_{lk}e_{ik} \in N$. 对任 i, j, 作 $a_{lk}^{-1}e_{il}(a_{lk}e_{lk})e_{kj} = e_{ij}$, 则 $e_{ij} \in N$. 于是任意 $\sum_{i,j=1}^{n} b_{ij}e_{ij} = \sum_{i,j=1}^{n} (b_{ij}e_{ii})e_{ij} \in N$. 这就证明了 $N = M_n(F)$.

定义 6 设 R 是环, 若 R 除零理想和 R 本身外没有其他理想, 则称 R 为**单环**.

上面已证明域 F 和 $M_n(F)$ 都是单环.

在证明域 F 没有其它理想时主要用到每个非零元有乘法逆元素. 实际上 $F^* = F \setminus \{0\}$ 是乘法交换群. 是否有这样的环, 它除了乘法交换律以外, 具有域的其它所有的性质呢?

定义 7 设 R 是环, $R^* = R \setminus \{0\}$ 是乘法群, 但不满足交换律, 则称 R 为**除环**.

例 14 除环是单环.

其证明与例 8 中类似.

例 15 我们来构造除环的一个例子, 它是代数学历史上有重要地位的**四元数环**. 令

$$H = \left\{ \begin{pmatrix} a + b\mathrm{i} & c + d\mathrm{i} \\ -(c - d\mathrm{i}) & a - b\mathrm{i} \end{pmatrix} \middle| a + b\mathrm{i}, c + d\mathrm{i} \in \mathbb{C} \right\}.$$

这是 $M_n(\mathbb{C})$ 的非空子集. 易知:

(1) H 显然是 $M_n(\mathbb{C})$ 的加法子群.

(2) 单位矩阵

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\in H.$$

(3) 对

$$\begin{pmatrix} a+b\mathrm{i} & c+d\mathrm{i}\\ -(c-d\mathrm{i}) & a-b\mathrm{i}\end{pmatrix},\begin{pmatrix} a'+b'\mathrm{i} & c'+d'\mathrm{i}\\ -(c'-d'\mathrm{i}) & a'-b'\mathrm{i}\end{pmatrix}\in H,$$

作它们的积,令 $\alpha=a+b\mathrm{i},\beta=c+d\mathrm{i},\gamma=a'+b'\mathrm{i},\delta=c'+d'\mathrm{i}$,则

$$\begin{aligned}\begin{pmatrix}\alpha & \beta\\ -\bar{\beta} & \bar{\alpha}\end{pmatrix}\begin{pmatrix}\gamma & \delta\\ -\bar{\delta} & \bar{\gamma}\end{pmatrix}&=\begin{pmatrix}\alpha\gamma-\beta\bar{\delta} & \alpha\delta+\beta\bar{\gamma}\\ -\beta\gamma-\alpha\bar{\delta} & -\bar{\beta}\bar{\delta}+\bar{\alpha}\bar{\gamma}\end{pmatrix}\\ &=\begin{pmatrix}\alpha\gamma-\beta\bar{\delta} & -\alpha\delta+\beta\bar{\gamma}\\ \overline{\alpha\delta+\beta\bar{\gamma}} & \overline{\alpha\gamma-\beta\bar{\delta}}\end{pmatrix}\in H,\end{aligned}$$

故 H 对乘法封闭.

这说明 H 是 $M_n(\mathbb{C})$ 的子环.再证 H 的每个非零元是可逆矩阵,且其逆仍属于 H.非零矩阵

$$\begin{pmatrix}\alpha & \beta\\ -\bar{\beta} & \bar{\alpha}\end{pmatrix},\quad \alpha,\beta\text{ 不全为零}$$

的行列式

$$\begin{vmatrix}\alpha & \beta\\ -\bar{\beta} & \bar{\alpha}\end{vmatrix}=\alpha\bar{\alpha}+\beta\bar{\beta}=|\alpha|^2+|\beta|^2\neq 0,$$

其逆矩阵为

$$\begin{pmatrix}\alpha & \beta\\ -\bar{\beta} & \bar{\alpha}\end{pmatrix}=\frac{1}{|\alpha|^2+|\beta|^2}\begin{pmatrix}\alpha & -\beta\\ \bar{\beta} & \alpha\end{pmatrix}.$$

故它的逆矩阵属于 H.

H 还是实数域上四维空间,任一元素

$$\begin{aligned}A&=\begin{pmatrix} a+b\mathrm{i} & c+d\mathrm{i}\\ -(c-d\mathrm{i}) & a-b\mathrm{i}\end{pmatrix}\\ &=a\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}+b\begin{pmatrix}\mathrm{i} & 0\\ 0 & -\mathrm{i}\end{pmatrix}+c\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}+d\begin{pmatrix}0 & \mathrm{i}\\ \mathrm{i} & 0\end{pmatrix},\end{aligned}$$

于是 $A=0$ 当且仅当 $a+b\mathrm{i}=0$ 及 $c+d\mathrm{i}=0$ 当且仅当 $a=b=c=d=0$.故

$$E=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\quad I=\begin{pmatrix}\mathrm{i} & 0\\ 0 & -\mathrm{i}\end{pmatrix},\quad J=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix},\quad K=\begin{pmatrix}0 & \mathrm{i}\\ \mathrm{i} & 0\end{pmatrix}$$

是 H 的一组基.基元素之间的积为

$$I^2=J^2=K^2=-E,$$

$$IJ=K=-JI,\quad JK=I=-KJ,\quad KI=J=-IK.$$

可以看到 H 的乘法不满足交换律,它是一个除环.

历史上把平面点集构成复数域后，人们想把实数域上三维空间构造成实数域的扩域，这即为“三维复数”的寻找问题. Hamilton 研究此问题达数十年，发现必须在条件上作出两个让步：一是维数由 3 变 4，一是不要求乘法有交换律. 这样他造出了四元数除环. 他的研究促进了各种代数运算系统的构作，对抽象代数学科的形成有积极的影响.

现在提出一个问题：设 R 是交换环，K 是 R 的理想，问何时商环 $\frac{R}{K}$ 是域?

定义 8　设 R 是环，M 是 R 的理想，但不等于 R. 对 R 的任何包含 M 的理想 N，若 $N \neq M$，则 $N = R$. 这时称 M 为 R 的**极大理想**.

定理 3　设 R 是交换环，K 是 R 的理想，则 $\frac{R}{K}$ 是域的充分必要条件是 K 为 R 的极大理想.

证明　必要性. 设 $\frac{R}{K}$ 是域及 N 是 R 的理想且 $N \supseteq K$. 若 $N \neq K$，则有 $a \in N \setminus K$. 显然 $\bar{N} = \{n + K \mid n \in N\}$ 是 $\frac{R}{K}$ 的理想. $a + K \in \bar{N}$，又 $a + K \neq \bar{0}$. 故 $\bar{N}$ 是域 $\frac{R}{K}$ 的非零理想，必有 $\bar{N} = \frac{R}{K}$. 故对任 $r \in R$，有 $r + K \in N$，则有 $n \in N, k \in K$ 使 $r = n + k$. 但 $k \in K \subseteq N$，则 $r \in N$. 于是 $N = R$，这就证明了 K 是 R 的极大理想.

充分性，设 K 是 R 的极大理想. 于是 $\frac{R}{K} \neq \bar{0}$ 是至少有两个元素的交换环. 只要证 $\frac{R}{K}$ 的任何非零元有乘法逆元素，则 $\frac{R}{K}$ 是域.

设 $a + K \neq \bar{0}$，即 $a \notin K$. 作 $\{ra + m \mid r \in R, m \in K\} = \langle a, K \rangle$. 易知它是 R 的理想，包含 K 又不等于 K. 由 K 的极大性知 $\langle a, K \rangle = R$. 于是有 $r \in R$ 及 $k \in K$ 使 $ra + k = 1$. 就有 $(r + K)(a + K) = 1 + K$. 故 $r + K$ 是 $a + K$ 的逆. 定理得证.

习　题

1. 举出 $\frac{\mathbb{Z}}{6\mathbb{Z}} = \mathbb{Z}_6$ 中的零因子的例子.

2. 令 $\mathbb{Z}[\mathrm{i}] = \{a + b\mathrm{i} \mid a, b \in \mathbb{Z}\}$，它是整环. $2\mathbb{Z}[\mathrm{i}] = \{2a + 2b\mathrm{i}\}$ 是 $\mathbb{Z}[\mathrm{i}]$ 的主理想. 问 $\frac{\mathbb{Z}[\mathrm{i}]}{2\mathbb{Z}[\mathrm{i}]}$ 中是否有零因子?

3. 写出下列商环的全部元素、加法表和乘法表.

(i) $\mathbb{Z}_2 = \frac{\mathbb{Z}}{2\mathbb{Z}}$，检查它与 F_2 是否同构.

(ii) $\mathbb{Z}_3 = \frac{\mathbb{Z}}{3\mathbb{Z}}$,检查是否是域.

(iii) $\frac{F_2[x]}{(x^2+x+1)}$,检查是否有零因子.

(iv) $\frac{\mathbb{Z}_3[x]}{(x^2+x+2)}$,检查是否是域.

4. R 是环.若 R 的加群是循环群,则(i)R 是交换环;(ii)R 的子环只有 R;(iii) 当 R 的元素是无限多个时,它的任一理想也是无限多个元;(iv) 当 R 的元素有限时,设 I 为它的理想,则 $|I|\,||R|$;(v) R 的加法子群都是 R 的理想.

5.找出 $\mathbb{Z}_6,\mathbb{Z}_8$ 的全部理想.哪些是极大理想?对所有极大理想 K,写出 $\frac{\mathbb{Z}_6}{K}$ 及 $\frac{\mathbb{Z}_8}{K}$ 的全部元素、加法表和乘法表.

6.设 K 为交换环,M 是它的理想,M 作为 K 的加法子群满足 $[K:M]$ = 素数,则商环 $\frac{K}{M}$ 是域.

7.设 $f(x) = f_1(x)f_2(x)\cdots f_k(x)$ 是域 F 上的不可约多项式的乘积,且 $f_1(x),\cdots,f_k(x)$ 互不相同.令 $R = \frac{F[x]}{(f(x))}$ 是商环.

(i) 求出 R 的全体理想.

(ii) 这些理想中哪些是极大理想?

(iii) 设 $\overline{K}$ 是 R 的理想,K 是 $\overline{K}$ 在 $F[x]$ 中的原象.检验 $\frac{F[x]}{K} \cong \frac{R}{\overline{K}}$.

8.试将第一章 §10 习题 8 中关于群同态的结论推广到环同态的情形.

9.证明 $\frac{\mathbb{Z}[i]}{(1+i)}$ 是域.

§5 整数模 n 的剩余类环,素数 p 个元素的域

我们在 §4 例 9 中已指出整数环 $\mathbb{Z}$ 的全部理想是 $(n) = n\mathbb{Z}, n = 0,1,2,\cdots$.任取一个 $n\mathbb{Z}, n \neq 0$,作商环

$$\frac{\mathbb{Z}}{(n)} = \frac{\mathbb{Z}}{n\mathbb{Z}} = \{\overline{0} = 0 + n\mathbb{Z}, \overline{1} = 1 + n\mathbb{Z}, \cdots, \overline{n-1} = (n-1) + n\mathbb{Z}\}.$$

它称为整数模 n 的剩余类的环.这是 n 个元素的交换环.也记它为 $\mathbb{Z}_n$.

命题 1 $\mathbb{Z}$ 的理想 (n) 为极大理想的充分必要条件是 n 为素数.

证明 必要性.设 (n) 为极大理想.若 n 不是素数,则 $n = n_1n_2$, $1 < n_1, n_2 < n$.考察理想 (n_1).因 $n_1 \mid n$.故

$$(n) = \{na \mid a \in \mathbb{Z}\} \subseteq \{n_1a \mid a \in \mathbb{Z}\} = (n_1).$$

又 $n_1 \in (n)$，$1 \in (n_1)$，故 $(n) \neq (n_1) \neq \mathbb{Z}$. 这与 (n) 为极大理想矛盾. 故 n 必须为素数.

充分性. 设 n 为素数. 若有正整数 n_1，使 $(n_1) \supseteq (n)$，则 $n \in (n_1) = \{n_1 k \mid k \in \mathbb{Z}\}$，即有 $n_1 \mid n$. 由 n 为素数，$n_1 = 1$ 或 n. 这时 $(n_1) = (1) = \mathbb{Z}$ 或 $(n_1) = (n)$，证明了 (n) 是 $\mathbb{Z}$ 的极大理想.

推论　$\dfrac{\mathbb{Z}}{(n)}$ 是 n 个元素的域当且仅当 n 是素数.

证明　由 §4 定理 3 和上面命题 1.

上面的推论告诉了构造素数个元素的有限域的方法. 以后在第三章中，我们将构造出 p^k 个元素的有限域，p 是素数. 可证明有限域的元素的数目一定是素数的方幂，且元素数目相同的有限域是同构的.

我们知道 $\mathbb{Z}$ 到 $\mathbb{Z}_p$ 有环同态，它能引起 $\mathbb{Z}[x]$ 到 $\mathbb{Z}_p[x]$ 的同态. 利用这同态以及 $\mathbb{Z}_p[x]$ 的性质可反映出 $\mathbb{Z}[x]$ 的性质.

命题 2　下述映射

$$\mathbb{Z}[x] \xrightarrow{\varphi} \mathbb{Z}_p[x]$$

$$\sum_{i=0}^{k} a_i x^i \longmapsto \sum_{i=0}^{k} \bar{a}_i x^i$$

是环同态. 其中 $\bar{a}_i = a_i + p\mathbb{Z} \in \mathbb{Z}_p$.

证明　由 $\overline{a+b} = \bar{a} + \bar{b}$，$\forall a, b \in \mathbb{Z}$，易知

$$\varphi\Big(\sum_{i=0}^{k} a_i x^i + \sum_{i=0}^{k} b_i x^i\Big) = \sum_{i=0}^{k} \overline{(a_i + b_i)} x^i = \sum_{i=0}^{k} \bar{a}_i x^i + \sum_{i=0}^{k} \bar{b}_i x^i$$

$$= \varphi\Big(\sum_{i=0}^{k} a_i x^i\Big) + \varphi\Big(\sum_{i=0}^{k} b_i x^i\Big),$$

即 φ 保持加法.

又设

$$(a_0 + a_1 x + \cdots + a_k x^k)(b_0 + b_1 x + \cdots + b_l x^l)$$

$$= c_0 + c_1 x + \cdots + c_{k+l} x^{k+l},$$

这里

$$c_i = \sum_{m+n=i} a_m b_n,$$

就有

$$\bar{c}_i = \sum_{m+n=i} \bar{a}_m \bar{b}_n.$$

因此

$$\varphi\Big(\sum_{i=0}^{k} a_i x^i\Big)\varphi\Big(\sum_{i=0}^{l} b_i x^i\Big) = \Big(\sum_{i=0}^{k} \bar{a}_i x^i\Big)\Big(\sum_{i=0}^{l} \bar{b}_i x^i\Big)$$

$$\sum_{i=0}^{k+l}\bar{c}_i x^i = \varphi\Big(\sum_{i=0}^{k+l} c_i x^i\Big) = \varphi\Big(\sum_{i=0}^{k} a_i x^i \sum_{i=0}^{l} b_i x^i\Big).$$

这证明了 φ 保持乘法，故是环同态.

应用举例.

例 1 证明 $x^3 + 13x + 121$ 在 $\mathbb{Z}[x]$ 上是不可约的.

解 对它模 2，成为 $x^3 + \bar{1}\cdot x + \bar{1}$（即将 $x^3 + 13x + 121$ 同态映射到 $\mathbb{Z}_2[x]$ 中），$\bar{0}$ 及 1 都不是它的根. 也即在 $\mathbb{Z}_2[x]$ 中它没有一次因式，因而它在 $\mathbb{Z}_2[x]$ 中不可约. 由于环同态保持乘法，若 $x^3 + 13x + 121$ 在 $\mathbb{Z}[x]$ 中可约，则 $x^3 + \bar{1}\cdot x + \bar{1}$ 也可约，矛盾. 故 $x^3 + 13x + 121$ 不可约.

例 2 我们用模 p（即 $\mathbb{Z}[x]$ 到 $\mathbb{Z}_p[x]$ 上的同态）方法重证一下高等代数中的**爱森斯坦判别法**：

设 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$. 若存在一个素数 p，满足

(a) $p \mid a_0, \cdots, a_{n-1}$；

(b) $p \nmid a_n$；

(c) $p^2 \nmid a_0$，

则 $f(x)$ 在 $\mathbb{Z}[x]$ 上不能分解成两个比 $f(x)$ 次数都低的多项式的乘积（因而 $f(x)$ 在 $\mathbb{Q}[x]$ 中不可约）.

证明 用反证法. 设

$$f(x) = g(x)h(x), \tag{1}$$

$g(x), h(x) \in \mathbb{Z}[x]$，且 $\partial(g(x)), \partial(h(x)) < \partial(f(x))$. 设

$$g(x) = b_m x^m + \cdots + b_0,$$

$$h(x) = c_l x^l + \cdots + c_0,$$

其中 $1 \leqslant m, l < n$. 对(1)式两边都模 p，由假设中条件(a)及(1)式得

$$\bar{a}_n x^n + \cdots + \bar{a}_0 = a_n x^n = (\bar{b}_m x^m + \cdots + \bar{b}_0)(\bar{c}_l x^l + \cdots + c_0). \tag{2}$$

因 $p \nmid a_n$，有 $\bar{a}_n \neq \bar{0}$. 又 $\bar{a}_n = \bar{b}_m \bar{c}_l$，故 $\bar{b}_m \neq \bar{0}, \bar{c}_l \neq \bar{0}$. 由(1)，$a_0 = b_0 c_0$. 但 $p^2 \nmid a_0$，故 p 不能同时除尽 b_0 及 c_0. 不妨设 $p \nmid c_0$，则 $\bar{c}_0 \neq 0$. 于是 $a_n x^n$ 与 $\bar{c}_l x^l + \cdots + \bar{c}_0$ 互素. 这与(2)式矛盾. 推出(1)式不能成立. 爱森斯坦判别法成立.

当 p 是素数时，$\mathbb{Z}_p$ 是域，$\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{\bar{0}\}$ 就是有限乘法群. $\mathbb{Z}_p$ 的每个非零元素都可逆. 对 $\mathbb{Z}_n$，一般 n 时，我们有下列结论：

命题 3 设 $\bar{0} \neq \bar{k} \in \mathbb{Z}_n$，则 $\bar{k}$ 是 $\mathbb{Z}_n$ 中乘法可逆元当且仅当 $(k, n) = 1$. (k, n 互素)

证明 先设 $\bar{0} \neq \bar{k}$ 是可逆元，则有 $l \in \mathbb{Z}_n$，使 $\bar{k}\bar{l} = 1$. 即有 $tn \in n\mathbb{Z}$，使 $kl + tn = 1$. 因此 $(k, n) = 1$（k, n 互素）.

又上面的证明完全可以反推回去，即由 $(k, n) = 1$ 推出 $\bar{k}$ 是可逆元.

推论　$\mathbb{Z}_n$ 中所有可逆元组成乘法群，它的阶是 $1,2,\cdots,n-1$ 中与 n 互素的元素的数目.

定义 1　对于任意正整数 n，令 $\varphi(n)$ 是 $1,2,\cdots,n-1$ 中与 n 互素的元素的数目，称为**欧拉函数**.

把有限群的阶与元素阶的关系用到 $\mathbb{Z}_n$ 中可逆元的乘法群可得到数论上的一些关系式.

定理 4（欧拉 - 费尔马）　设 $(a,n)=1, N=\varphi(n)$，则

$$a^N \equiv 1 (\mathrm{mod}\ n).$$

证明　$\mathbb{Z}_n$ 中可逆元素的乘法群的阶是 N. $(a,n)=1$，则 $\bar{a}$ 是该群的元. 由第一章 §7 定理 1 的推论知，$\bar{a}^N=\bar{1}$. 由此 $\overline{a^N}=\bar{1}$，即 $a^N \equiv 1(\mathrm{mod}\ n)$.

推论　当 p 是素数，而 $p \nmid a$ 时有

$$a^{p-1} \equiv 1 (\mathrm{mod}\ p).$$

证明　$\mathbb{Z}_p$ 中任一非零元 $\bar{a}$，有 $p \nmid a$. 因 p 是素数，$(p,a)=1$. 即 $\mathbb{Z}_p$ 中每个非零元是可逆元，于是 $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{\bar{0}\}$ 对乘法成为群，其阶为 $p-1$. 任意 a，若 $p \nmid a$，则 a 是 $\mathbb{Z}_p^*$ 中元，仍由第一章 §7 定理 1 的推论，得 $a^{p-1}=\bar{1}$. 由此知 $\bar{a}^{p-1}=\bar{1}$，即 $a^{p-1} \equiv 1(\mathrm{mod}\ p)$.

欧拉函数是数论中的重要函数. 我们列出 $\varphi(n)$ 的值，但略去证明（见第四章 §5 习题 4）.

设 $n=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$ 是 n 按素因子的分解，其中 $p_1,\cdots,p_r$ 为不同素数，$e_i \geqslant 1, i=1,\cdots,r$，则

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right),\cdots,\left(1-\frac{1}{p_r}\right).$$

特别当 n 是素数 p 时

$$\varphi(p)=p-1.$$

习　题

1. 求出 $\mathbb{Z}_8$ 中可逆元的群及其乘法表.

2. 求出 $\mathbb{Z}_9$ 中可逆元的群及其乘法表.

3. 写出 $\dfrac{\mathbb{Z}_3[x]}{(x^2+1)}$ 的全部元素. 求出 $\overline{x+1}$ 与全部元素的乘积以及它的逆元素.

4. $4^{27} \equiv ?(\mathrm{mod}\ 3)$　　$7^{123} \equiv ?(\mathrm{mod}\ 5)$　　$8^{27} \equiv ?(\mathrm{mod}\ 6)$

5. p 是素数，则域 $\mathbb{Z}_p$ 中全部元素是方程 $x^p-x=0$ 的全部根. 因而映射

$$\mathbb{Z}_p \longrightarrow \mathbb{Z}_p$$
$$a \longmapsto a^p$$

是恒等自同构.

§6 $F[x]$模某个理想的剩余类环，添加一个多项式的根的扩域

设F是域，在§4例12中已指出$F[x]$的全部理想都是主理想$(f(x)) = f(x)F[x]$，$f(x)$是$F[x]$中任意多项式.设$\partial(f(x)) = n$.作商环$\frac{F[x]}{(f(x))}$，则

$$\frac{F[x]}{(f(x))} = \frac{F[x]}{f(x)F[x]} = \{a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0 + (f(x))\}$$
$$= \{\overline{a_{n-1}x^{n-1} + \cdots + a_0}\}$$
$$= \{\bar{a}_{n-1}\bar{x}^{n-1} + \cdots + \bar{a}_0\}.$$

这里，一个多项式$r(x)$上面加一杠成$\overline{r(x)}$是表示

$$\overline{r(x)} = r(x) + (f(x)),$$

它是模$f(x)$的剩余类.有性质

$$\overline{r_1(x)} + \overline{r_2(x)} = \overline{r_1(x) + r_2(x)},$$
$$\overline{r_1(x)} \cdot \overline{r_2(x)} = \overline{r_1(x)r_2(x)}.$$

$\frac{F[x]}{(f(x))}$是交换环，何时它成为域？这和$\frac{\mathbb{Z}}{(n)}$的讨论是类似的.

命题1 $F[x]$的理想$(f(x))$是$F[x]$的极大理想的充分必要条件是$f(x)$为$F[x]$中的不可约多项式.

证明 必要性.设$(f(x))$是极大理想.若$f(x)$可约，则$f(x) = f_1(x)f_2(x)$，$f_i(x) \in F[x]$，且$1 < \partial(f_i(x)) < \partial(f(x))$，$i = 1,2$.考察$(f_2(x))$.由于$f_2(x) \mid f(x)$，有

$$(f(x)) \subseteq (f_2(x)) = \{f_2(x)g(x) \mid g(x) \in F[x]\}.$$

但$1 \notin (f_2(x))$，$(f_2(x)) \neq F[x]$.$f_2(x) \in (f(x))$，故$(f_2(x)) \neq (f(x))$.这与$(f(x))$是极大理想矛盾.故$f(x)$是不可约的.

充分性.设$f(x)$是不可约多项式，若有$(f_1(x)) \supseteq (f(x))$，则$f(x) \in \{f_1(x)g(x) \mid g(x) \in F[x]\}$.即有$f_1(x) \mid f(x)$.由于$f(x)$不可约，$f_1(x) = r$或$rf(x)$，这里$0 \neq r \in F$.于是$(f_1(x)) = F[x]$或$(f(x))$.即$(f(x))$是极大理想.

推论 $\dfrac{F[x]}{(f(x))}$是域当且仅当 $f(x)$ 是不可约多项式.

证明 由 §4 定理 3 及上面命题 1.

下面转向研究多项式求根的一个问题.在 §1 中我们介绍了复数域 $\mathbb{C}$ 的严格构造.这实际上是在实数域 $\mathbb{R}$ 上添加方程 $x^2+1=0$ 的一个根 $\sqrt{-1}$ 面得的扩域,$\mathbb{C}=\mathbb{R}(\sqrt{-1})$.这里我们对任意域 F 及 F 上的任意一个不可约多项式 $p(x)$,要造出 F 的一个扩域 F_1,使得 $p(x)$ 在 F_1 中至少有一个根 a.如 F_1 能作出,则 $F(a)\subset F_1$,$F(a)$ 也是这样的域.下面就提供一个一般的方法来构造域 $F(a)$,a 是 $p(x)$ 的一个根.这是商环性质的重要应用.

现设 $\partial(p(x))=n$,$p(x)=a_nx^n+\cdots+a_1x+a_0$.由于 $p(x)$ 不可约,上面推论中指出商环 $\dfrac{F[x]}{(p(x))}$ 是域.我们有下述定理.

定理 2 F 是域,$p(x)$ 是 $F[x]$ 中不可约多项式,$\partial(p(x))=n$,则

(1) 域 $\dfrac{F[x]}{(p(x))}$ 可看成 F 的扩域,这时 $\bar{x}=x+(p(x))\in\dfrac{F[x]}{(p(x))}$ 是 $p(x)$ 的根.

(2) 设 $E=F(a)$,a 是 $p(x)$ 的一个根,则 $E=F(a)\cong\dfrac{F[x]}{(p(x))}$.

证明 $\dfrac{F[x]}{(p(x))}=\{r(x)+(p(x))\mid r(x)=0\text{ 或 }\partial(r(x))<n\}$.在这个域中令

$$\bar{F}=\{\bar{a}=a+(p(x))\mid a\in F\},$$

它是子域,且易知 $\bar{F}\cong F$.干脆写 $\bar{F}$ 为 F,任意 $a\in F$,$\bar{a}$ 也写成 a,则 $\dfrac{F[x]}{(p(x))}$ 可看成是 F 的扩域.于是

$$\begin{aligned}p(\bar{x})&=a_n\bar{x}^n+a_{n-1}\bar{x}^{n-1}+\cdots+a_0\\&=\bar{a}_n\bar{x}^n+\bar{a}_{n-1}\bar{x}^{n-1}+\cdots+\bar{a}_0\\&=\overline{(a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0)}\\&=\overline{p(x)}=\bar{0}=0.\end{aligned}$$

故 $\bar{x}$ 是 $p(x)$ 的一个根.

(2) 作映射

$$\begin{aligned}F[x]&\xrightarrow{\varphi}F(a)\\f(x)&\longmapsto f(a).\end{aligned}$$

易知这是环同态.$\operatorname{Ker}\varphi=\{f(x)\mid f(a)=0\}$.因 $p(x)$ 不可约及 $p(a)=0$,由 §2 定理 4 及推论,$\operatorname{Ker}\varphi$ 中任一多项式 $f(x)$ 是 $p(x)$ 的倍数.于是 $\operatorname{Ker}\varphi=(p(x))$.由环的同态基本定理知 $\dfrac{F[x]}{(p(x))}=\dfrac{F[x]}{\operatorname{Ker}\varphi}\cong F(a)$.这里虽是环同

构,但两者都是域,故是域同构.

在 §1 例 3 中,我们叙述了复数域的一种构造方法.现在定理 1 的方法既具有一般性,又突出了方法的实质.用现在的方法造出域$\frac{\mathbb{R}[x]}{(x^2+1)}$是 $\mathbb{R}$ 的扩域,它等于 $\mathbb{R}(\bar{x})$,且 $x^2+1=0$.定理证明了 $\mathbb{R}(\bar{x}) \cong \mathbb{R}(\sqrt{-1}) = \mathbb{C}$,其同构对应是 $a+bx \longmapsto a+b\sqrt{-1}$,$\forall a,b \in \mathbb{R}$.说明了复数域构造的唯一性.

推论 域 F 上不可约多项式 $p(x)$ 在某扩域 E 中若有两个根 a_1,a_2,则有域同构 $F(a_1) \cong F(a_2)$,且在 F 上是恒等映射.

习 题

1. $\mathbb{Z}_3[x]$ 中计算 $(x^2+x+1)(x^3+2x+1)$ 及 $(x^4+2x+1)(x^3+x+1)$.

2. 证明 x^2+1, x^3+2x+1 是 $\mathbb{Z}_3[x]$ 中不可约多项式.问 $\frac{\mathbb{Z}_3[x]}{(x^2+1)}$,$\frac{\mathbb{Z}_3[x]}{(x^3+2x+1)}$ 分别是几个元素的域.

3. 写出 $\frac{\mathbb{Z}_3[x]}{((x^2+1)(x^3+2x+1))}$ 中的全部理想和极大理想.

4. 证明 $\frac{\mathbb{Q}[x]}{(x^2-2)}$ 与 $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$ 都是域,且互相同构.

§7 整环的分式域,素域

整数的比就是分数,也即有理数.把整数环扩充成分数的集合,在分式的加法和乘法运算下就成为有理数域 $\mathbb{Q}$.多项式环扩充成分式的集合,在分式的加法和乘法下为有理分式域.我们问,对一般的环 R,是否也能类似地扩充成域呢?如果能,则 R 包含在某域中,域是乘法交换的,故 R 必须是交换的;域中也无零因子,故 R 中也无零因子.这是 R 能扩充成域的先决条件.

定义 1 设 R 是有非零元素的环,若它是交换环且无零因子,则称 R 为**整环**.

整数环 $\mathbb{Z}$,域上多项式环 $F[x]$ 都是整环.域也是整环.

对一般整环我们能建立分式域.回忆在 $\mathbb{Z}$ 中,一个分数形为 $\frac{r}{s}$,$r,s \in \mathbb{Z}$,$s \neq 0$.两个分数 $\frac{r}{s}$ 及 $\frac{l}{m}$ 是相等的当且仅当 $rm = ls$.现在对整环 R 引入集合

$$\{(r,s) \mid r \in R, s \in R \setminus \{0\}\} = R \times (R \setminus \{0\}).$$

在此集合上引入关系 $\sim$:$(r,s)\sim(l,m)$ 当且仅当 $rm=ls$. 易知这关系满足:

(1) 反身性:$(r,s)\sim(r,s)$.

(2) 对称性:若$(r,s)\sim(l,m)$,则$(l,m)\sim(r,s)$.

(3) 传递性:若$(r,s)\sim(l,m),(l,m)\sim(t,n)$ 则,$(r,s)\sim(t,n)$.

故它是等价关系. 于是 $R\times(R\setminus\{0\})$ 按此关系划分成一些等价类,这些等价类之间互不相交(见一章 §5 定理 3). 把$(r,s)\in R\times(R\setminus\{0\})$ 所在的等价类也记成$\frac{r}{s}$. 于是像整数环$\mathbb{Z}$中分数一样:$\frac{r}{s}=\frac{l}{m}$ 当且仅当$rm=ls$. 易知,若 $t\neq0$,则$\frac{r}{s}=\frac{rt}{st}$.

记这些等价类的集合为

$$F=\left\{\frac{r}{s}\mid(r,s)\in R\times(R\setminus\{0\})\right\}.$$

在 F 上定义加法乘法如下:$\forall\ \frac{a}{b},\frac{c}{d}\in F$,令

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd},$$

$$\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}.$$

首先上面的运算与$\frac{a}{b},\frac{c}{d}$ 的写法无关. 设$\frac{a}{b}=\frac{a'}{b'},\frac{c}{d}=\frac{c'}{d'}$,即有 $ab'=a'b,cd'=c'd$,则

$$\begin{aligned}\frac{a'}{b'}+\frac{c'}{d'}&=\frac{a'd'+b'c'}{b'd'}=\frac{ba'd'+bb'c'}{bb'd'}\\&=\frac{ab'd'+bb'c'}{bb'd'}=\frac{ad'+bc'}{bd'}=\frac{dad'+dbc'}{dbd'}\\&=\frac{d'ad+bd'c}{dbd'}=\frac{ad+bc}{db}=\frac{a}{b}+\frac{c}{d}.\end{aligned}$$

同样易证

$$\frac{a'}{b'}\cdot\frac{c'}{d'}=\frac{a}{b}\cdot\frac{c}{d}$$

这说明两个运算是有定义的.

在 F 上$\frac{0}{d}=\{(0,d)\mid d\in R\setminus\{0\}\}$ 显然是加法零元素. $\frac{a}{b}$ 的负元素是 $\frac{-a}{b}$. F 上的乘法单位元是$\frac{1}{1}=\{(a,a)\mid a\in R\setminus\{0\}\}$. F 上非零元$\frac{a}{b},a\neq0$, $b\neq0$,的乘法逆元素为$\frac{b}{a}$. 又 F 上的加法交换律和结合律、乘法的交换律和结

合律、乘法对加法的分配律都是成立的(读者可自己验证).故 F 是一个域.

又 F 中含有一个子环 $R' = \left\{ \frac{a}{1} \middle| a \in R \right\}$,易知它与 R 是同构的.将 $\frac{a}{1}$ 干脆记成 a,则可将 R' 与 R 等同起来.即 F 是 R 的扩域.

F 中元素 $\frac{a}{b} = \frac{a}{1} \cdot \frac{1}{b} = \frac{a}{1} \cdot \left(\frac{b}{1}\right)^{-1}$.即 F 中元素可写成 R 中元素的商.

至此我们证明了下述定理.

定理 1 设 R 是整环,则有一个域 F,它以 R 为子环且 F 中元都是 R 的元素的商.

定义 2 设 R 是整环,称具有定理 1 中性质的域 F 为 R 的**分式域**.

下面还能证明整环 R 的分式域在同构意义下还是唯一的.实际上设 F 是整环 R 的一个分式域,则 $F = \{ab^{-1} \mid a, b \in R, b \neq 0\}$.我们写 ab^{-1} 为 $\frac{a}{b}$.易知有(请读者自行验证)

(1) $\frac{a}{b} = \frac{c}{d}$ 当且仅当 $ad = bc$.

(2) $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$.

(3) $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.

定理 2 设整环 R_1 与 R_2 同构,它们分别有分式域 F_1 与 F_2,则 F_1 与 F_2 是同构的域.

证明 因 R_1 与 R_2 有同构映射,为简单起见,我们把 $a \in R$ 在这映射下的象记为 a'.于是

$$F_1 = \left\{ \frac{a}{b} \middle| a, b \in R_1, b \neq 0 \right\},$$

$$F_2 = \left\{ \frac{a'}{b'} \middle| a', b' \in R_2, b' \neq 0 \right\},$$

于是由上面的(1),有

$$\frac{a}{b} = \frac{c}{d} \text{ 当且仅当 } ad = bc,$$

(由于 R_1, R_2 环同构)当且仅当 $a'd' = b'c'$,当且仅当 $\frac{a'}{b'} = \frac{c'}{d'}$.这样就有双射

$$F_1 \longrightarrow F_2$$

$$\frac{a}{b} \longmapsto \frac{a'}{b'}.$$

由于 R_1, R_2 环同构,上述双射下,

$$\frac{ad+bc}{bd} \text{ 的象为} \frac{a'd'+b'c'}{b'd'},$$

$$\frac{ac}{bd} \text{ 的象为} \frac{a'c'}{b'd'},$$

由前面的(2),(3)知

$$\frac{a}{b}+\frac{c}{d} \text{ 的象是} \frac{a'}{b'}+\frac{c'}{d'},$$

$$\frac{a}{b}\cdot\frac{c}{d} \text{ 的象是} \frac{a'}{b'}\cdot\frac{c'}{d'}.$$

这说明上述映射保持加法和乘法,故 F_1 与 F_2 是同构的域.

推论 整环 R 的分式域在同构意义下是唯一的.

当 $R=\mathbb{Z}$ 时,它的分式域就是有理数域 $\mathbb{Q}$. 当 $R=F[x]$(域 F 上多项式环)时,它的分式域称为 F 上有理分式域,通常记为 $F(x)$. 注意:设 E 是 F 的扩域及 $\alpha\in E$,若 α 是 F 上的超越元,则 $F[x]$ 与 $F[\alpha]$(F 上 α 的全体多项式)是环同构的. $F(x)$ 和 $F(\alpha)$ 分别是它们的分式域,也是同构的.

在这一节的最后,我们还要讲到有理数域 $\mathbb{Q}$ 和 p 个元素的域 $\mathbb{Z}_p$ 的一个性质:任何域必包含(在同构意义下)$\mathbb{Q}$ 或 $\mathbb{Z}_p$ 作为子域.

定理 3 设 F 是域.

(i) 当 F 的特征为 0 时,F 中必含有一个子域与 $\mathbb{Q}$ 同构;

(ii) 当 F 的特征为 p(素数)时,F 中必含有一个子域与 $\mathbb{Z}_p$ 同构.

证明 (i) 设 F 的特征为零,则 F 的单位元 1 的非零倍数 $m\cdot 1\neq 0$. 令

$$\mathbb{Z}_0=\{m\cdot 1\mid m\in\mathbb{Z}\},$$

易知 $\mathbb{Z}_0$ 是 F 的子环,它与整数环 $\mathbb{Z}$ 同构. 再令

$$\mathbb{Q}_0=\left\{(m\cdot 1)(n\cdot 1)^{-1}=\frac{m\cdot 1}{n\cdot 1}\,\middle|\, m,n\in\mathbb{Z},n\neq 0\right\}.$$

$\mathbb{Q}_0$ 中元素的加法和乘法为以下的分式运算:

$$\frac{m\cdot 1}{n\cdot 1}+\frac{k\cdot 1}{l\cdot 1}=\frac{(lm+nk)\cdot 1}{(nl)\cdot 1},$$

$$\frac{m\cdot 1}{n\cdot 1}\cdot\frac{k\cdot 1}{l\cdot 1}=\frac{(mk)\cdot 1}{(nl)\cdot 1},$$

因此 $\mathbb{Q}_0$ 对 F 的加法、乘法是封闭的,进一步可知它是 F 的子域. 由分式域的定义知 $\mathbb{Q}_0$ 是 $\mathbb{Z}_0$ 的分式域.

由于 $\mathbb{Z}$ 同构于 $\mathbb{Z}_0$,用定理 2,它们的分式域 $\mathbb{Q}$ 和 $\mathbb{Q}_0$ 同构.

(ii) 设 F 的特征是 p. 作映射

$$\begin{aligned}\mathbb{Z} &\xrightarrow{\varphi} F\\ n &\longmapsto n\cdot 1.\end{aligned}$$

由倍数的性质这是环同态.由于 F 的特征是 p,$\mathrm{Ker}\ \varphi = p\mathbb{Z} = (p)$.由环同态基本定理,

$$\mathbb{Z}_p = \frac{\mathbb{Z}}{(p)} = \frac{\mathbb{Z}}{\mathrm{Ker}\ \varphi} \cong \varphi(\mathbb{Z}) \subseteq F.$$

$\mathbb{Z}_p$ 与 $\varphi(\mathbb{Z})$ 是环同构,$\mathbb{Z}_p$ 又是域,故 $\varphi(\mathbb{Z})$ 也是域.这就证明了(ii).

定义 3 域 F 称为**素域**,若它不含有其它的子域.

$\mathbb{Z}_p$ 的子域须含单位元的任意整倍数,只能是 $\mathbb{Z}_p$ 自身.$\mathbb{Q}$ 的子域含所有整数,也就含有所有分数(分数是两个整数的商),也只能是 $\mathbb{Q}$ 自身.故 $\mathbb{Z}_p$,$\mathbb{Q}$ 是素域.定理3指出特征为0的域含有与 $\mathbb{Q}$ 同构的素域,特征为 p 的域含有与 $\mathbb{Z}_p$ 同构的素域.

习 题

1.证明:有限整环是域.

2. R 是交换环,P 是 R 的理想,则 $\frac{R}{P}$ 是整环当且仅当 P 有性质:若 a,$b \in R$ 满足 $ab \in P$,则 $a \in P$ 或 $b \in P$.有这种性质的理想 P 称为**素理想**.

3. R 是交换环,则 R 的极大理想必为素理想.

4. $\mathbb{Z}$ 中主理想 $(n) = n\mathbb{Z}$ 是素理想当且仅当 n 是素数.

5.设 R 是一个域,则 R 的分式域就是自身.

6.令 $\mathbb{Z}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$,$\mathbb{Q}(\sqrt{2}) = \{\alpha + \beta\sqrt{2} \mid \alpha, \beta \in \mathbb{Q}\}$.证明 $\mathbb{Q}(\sqrt{2})$ 是 $\mathbb{Z}(\sqrt{2})$ 的分式域.

7.令 $\mathbb{Z}[\mathrm{i}] = \{a + b\mathrm{i} \mid a, b \in \mathbb{Z}\}$,$\mathbb{Q}[\mathrm{i}] = \{\alpha + \beta\mathrm{i} \mid \alpha, \beta \in \mathbb{Q}\}$.证明 $\mathbb{Q}[\mathrm{i}]$ 是 $\mathbb{Z}[\mathrm{i}]$ 的分式域.

8.域 F 上多环式环 $F[x]$ 中主理想 $(f(x))$ 是素理想当且仅当 $f(x)$ 是不可约多项式.

第三章　有限域及其应用

我们已学过 p(素数)个元素的有限域的构造.这一章来讨论一般的**有限域**的构造、性质以及有限域上多项式的性质.由于计算机和信息科学的发展,离散的数学结构(对比于连续的数学结构)的研究日渐重要.有限域在很多离散数学问题中,例如在纠错码、密码学、试验设计、有限群、有限几何等问题中担任重要角色.这一章中我们除了讲一些一般的理论外,还介绍了在编码、线性移位寄存器中的简单应用.

§1　有限域的基本构造

命题 1　任意有限域 F 都是特征为 p 的,p 是与 F 有关的素数.

证明　只要证 F 不是特征为零就行.反证法.设 F 的特征为零,则任意 $m, n \in \mathbb{Z}, m \neq n$,有 $(m-n)\cdot 1 \neq 0$,于是 $m\cdot 1 \neq n\cdot 1$.因而 F 中有无限个不同的元素,矛盾.命题得证.

定理 2　(1) 特征为 p 的有限域 F 的元素的数目一定是 p^n,n 是某正整数.

(2) p^n 个元素的有限域 F 的全部元素恰是 F 上多项式方程 $x^{p^n}-x=0$ 的全部根,且 $F\setminus\{0\}$ 是乘法循环群.

证明　(1) F 的特征为 p,由第二章 §7 定理 3,F 含有一个子域与 $\mathbb{Z}_p$ 同构.为简便计,就令这个子域为 $\mathbb{Z}_p$.于是 F 是 $\mathbb{Z}_p$ 上的线性空间.因 F 只有有限个元,它的维数必有限.设其基为 $\varepsilon_1, \cdots, \varepsilon_n$,则 F 的全部元素为 $\{l_1\varepsilon_1 + l_2\varepsilon_2 + \cdots + l_n\varepsilon_n \mid l_1, l_2, \cdots, l_n \in \mathbb{Z}_p\}$.每个 l_i 可在 $\mathbb{Z}_p$ 中独立取 p 个值,故 $l_1, l_2, \cdots, l_n$ 有 p^n 个可能的取法.即 F 有 p^n 个元素.

(2) 由第一章 §7 定理 7,域 F 的乘法有限子群是循环群.现在 F 是有限域,$F\setminus\{0\}$ 当然是乘法有限子群,因而是循环群.

$F\setminus\{0\}$ 是 p^n-1 阶乘法群,任意 $a \in F\setminus\{0\}$ 有 $a^{p^n-1}=1$,也就有 $a^{p^n}=a$.F 的零元 0 也满足 $0^{p^n}=0$.这说明 F 的全部元满足 F 上方程 $x^{p^n}-x=0$.又方程 $x^{p^n}-x=0$ 最多有 p^n 个不同的根,故 F 的全部元是它的全部根.

定理 3　对任何素数 p 及正整数 n,必存在 p^n 个元素的域,它还是 $\mathbb{Z}_p$ 上的单扩张.并且任何两个 p^n 个元素的域互相同构,即在同构意义下 p^n 个元的

域是唯一的.

证明 我们对任意域 F 上任意多项式 $f(x)$ 来证明:有 F 的扩域 E,使得 $f(x)$ 在 E 中分解成一次因式的乘积.对 $f(x)$ 的次数 k 作归纳法.

任取 $f(x)$ 的一个不可约因式 $p(x)$.由第二章 §6 定理 2,我们可造出 F 的一个扩域 $F(\alpha_1)$,其中 α_1 是 $p(x)$ 的一个根.于是在域 $F(\alpha_1)$ 中 $f(x)$ 有分解:$f(x)=(x-\alpha_1)f_1(x)$.此时 $f_1(x)$ 为 $F(\alpha_1)$ 上 $k-1$ 次多项式.用归纳法知有 $F(\alpha_1)$ 的扩域,也是 F 的扩域 E,$f_1(x)$ 在 E 上,因而 $f(x)$ 在 E 上分解成一次因式的乘积.

现在对 $\mathbb{Z}_p$ 上多项式 $x^{p^n}-x$,设其在某域 E 上分解成一次因式的乘积.由于 $(x^{p^n}-x)'$(导数)为 -1 与 $x^{p^n}-x$ 互素,故 $x^{p^n}-x$ 无重根.因而它在 E 中有 p^n 个根.我们证明这 p^n 个根构成 E 的一个子域,它正是 p^n 个元素的域.

令 $x^{p^n}-x$ 的这 p^n 个根的集合为 F.对 $\alpha,\beta\in F$,即有 $\alpha^{p^n}=\alpha$,$\beta^{p^n}=\beta$.为证明 F 对加法封闭,需用到特征为 p 的域 F 中有(见二章 §1 习题 8)

$$(\alpha+\beta)^{p^n}=\alpha^{p^n}+\beta^{p^n}=\alpha+\beta,$$

即 F 对加法封闭.又易知

$$(\alpha\beta)^{p^n}=\alpha^{p^n}\beta^{p^n}=\alpha\beta,$$

$$(-\alpha)^{p^n}=((-1)\alpha)^{p^n}=(-1)\alpha=-\alpha,$$

$$(\alpha^{-1})^{p^n}=(\alpha^{p^n})^{-1}=\alpha^{-1}.$$

故 F 是 E 的子域,具有 p^n 个元素.

再证唯一性.设 F,F' 皆是 p^n 个元的域.因 $F\setminus\{0\}$ 是循环群,设 α 是它的生成元.由零元及 $F\setminus\{0\}=\langle\alpha\rangle$ 皆属于 $\mathbb{Z}_p(\alpha)$,得 $F\subseteq\mathbb{Z}_p(\alpha)$.再由 $\mathbb{Z}_p(\alpha)$ 是含 $\mathbb{Z}_p$ 及 α 的最小的域,就得到 $F=\mathbb{Z}_p(\alpha)$.又 α 是 $x^{p^n}-x$ 的根,设 $x^{p^n}-x$ 在 $\mathbb{Z}_p$ 上的分解中的不可约因式 $p(x)$ 以 α 为根.由第二章 §6 定理 2 知,$F=\mathbb{Z}_p(\alpha)\cong\dfrac{\mathbb{Z}_p[x]}{(p(x))}$.

由定理 2 知,F' 也是 $\mathbb{Z}_p$ 上多项式 $x^{p^n}-x$ 的全部根,故 F' 中有 $p(x)$ 的根,任取一个设为 α',则 $\mathbb{Z}_p(\alpha')\cong\dfrac{\mathbb{Z}_p[x]}{(p(x))}$.但右端有 p^n 个元,故 $\mathbb{Z}_p(\alpha')$ 有 p^n 个元.而 $\mathbb{Z}_p(\alpha')\subseteq F'$,右端也是 p^n 个元,故 $\mathbb{Z}_p(\alpha')=F'$.这就证明了 $F\cong F'$.

推论 1 对任意素数 p 和正整数 n,$\mathbb{Z}_p$ 上有 n 次不可约多项式存在.且 $\mathbb{Z}_p$ 上任意 n 次不可约多项式是 $x^{p^n}-x$ 的因式,也能在 p^n 个元的域中完全分解成一次因式的积.

证明　由定理3,有 p^n 个元素的域 F 存在.并且定理中证明唯一性时,已得到 $\mathbb{Z}_p$ 上不可约多项式 $p(x)$,使 $F \cong \mathbb{Z}_p(\alpha)$,$\alpha$ 是 $p(x)$ 的根.若 $p(x)$ 为 k 次,由第二章 §2 定理4,右端是 $\mathbb{Z}_p$ 上 k 维线性空间,因而有 p^k 个元素.但左端有 p^n 个元,故 $n = k$.即 $\mathbb{Z}_p$ 上有 n 次不可约多项式.

现设 $q(x)$ 是 $\mathbb{Z}_p$ 上 n 次不可约多项式.在域 $\frac{\mathbb{Z}_p[x]}{(q(x))}$ 中 $\bar{x} = x + (q(x))$ 是不可约多项式 $q(x)$ 的根.这个域有 p^n 个元,故由定理2,$\bar{x}$ 也是 $x^{p^n} - x$ 的根.由第二章 §2 定理4 的推论,$q(x)$ 是以 $\bar{x}$ 为根的极小多项式(可能差一倍数),$x^{p^n} - x$ 以它为因式.又 $x^{p^n} - x$ 在 p^n 个元的域能完全分解,故 $q(x)$ 也能.

推论2　特征为 p 的任何域若含有多项式 $x^{p^n} - x$ 的全部根,则这 p^n 个根组成该域的一个子域.

证明　定理3的证明中已蕴含了这个结论.

以后我们常记 p^n 个元素的域(在同构意义下是唯一的)为 F_{p^n}.下面来讨论它的子域.

定理4　(1) F_{p^n} 的子域一定为 F_{p^m},且 $m \mid n$.

(2) 对每个 $m \mid n$,一定有 F_{p^n} 的唯一的子域 F_{p^m}.

证明　(1) 设 F_{p^n} 有一个子域 F,F_{p^n} 是特征为 p 的,F 也是.又 F 是有限域,由命题1,F 有 p^m 个元.即 $F = F_{p^m}$(同构意义下).

再由 $[F_{p^n} : \mathbb{Z}_p] = [F_{p^n} : F_{p^m}][F_{p^m} : \mathbb{Z}_p]$,$[F_{p^n} : \mathbb{Z}_p] = n$ 及 $[F_{p^m} : \mathbb{Z}_p] = m$,就推得 $m \mid n$.

(2) 设 $m \mid n$,则 $x^{p^m} - x \mid x^{p^n} - x$.$F_{p^n}$ 有 $x^{p^n} - x$ 的全部根,也就有 $x^{p^m} - x$ 的全部根.定理3的推论2断言,F_{p^n} 中 $x^{p^m} - x$ 的全部 p^m 个根作成它的 p^m 个元的子域.

又 F_{p^n} 中的 p^m 个元的任一子域的元都是 $x^{p^m} - x$ 的根.而 $x^{p^m} - x$ 在 F_{p^n} 中仅有 p^m 个根,故 F_{p^n} 中仅有一个 p^m 个元的子域.

用有限域 $F = F_{p^n}$ 可以构成很多矩阵群,它们都是有限群的典型例子.例如

$GL(s,F)$ 为 F 上 $s \times s$ 可逆方阵的群,$SL(s,F)$ 为 F 上行列式为1的 $s \times s$ 方阵的群,作

$$PSL(n,F) = \frac{SL(s,F)}{Z(SL(s,F))},$$

$Z(SL(s,F))$ 是群 $SL(s,F)$ 的中心.$PSL(s,F)$ 称为 F 上射影幺模群,除了 $s = 2$,$p^n = 2,3$ 而外都是有限单群.

习 题

1. 验证 x^2+1 及 x^2+x+2 皆为 $\mathbb{Z}_3[x]$ 上不可约多项式. 写出下列两域

$$\frac{\mathbb{Z}_3[x]}{(x^2+1)} \text{ 及} \frac{\mathbb{Z}_3[x]}{(x^2+x+2)}$$

的加法表和乘法表. 找出这两个域之间的同构对应.

2. 作出 $\mathbb{Z}_2[x]$, $\mathbb{Z}_3[x]$ 中所有的二次、三次、四次不可约多项式. 作出 2^2, 2^3, 2^4 个元的域.

3. $f_1(x)$, $f_2(x)$ 都是 $\mathbb{Z}_p[x]$ 上 m 次不可约多项式, 则

$$\frac{\mathbb{Z}_p[x]}{(f_1(x))} \cong \frac{\mathbb{Z}_p[x]}{(f_2(x))}.$$

4. 作出一个 3^4 个元的域, 并在其中找出一个 3^2 个元的子域.

5. 设 $d \mid m$, 证明

(1) $p^d-1 \mid p^m-1$.

(2) $x^{p^d}-x \mid x^{p^m}-x$.

6. 设 $F_{p^n}=\mathbb{Z}_p(\alpha)$. 问 α 是乘法群 $F_{p^n}^*=F_{p^n}\setminus\{0\}$ 的生成元吗?

§2 有限域上不可约多项式及其周期, 本原多项式及其对纠错码的应用

首先有限域上多项式性质服从一般域上多项式理论, 前面的讨论中我们已多次应用了这个理论. 这一节是讨论它的一些与有限域有关的性质. 下面都记 p^n 为 q, 于是 F_{p^n} 记成 F_q.

命题1 $f(x)$ 是域 F_q 上的多项式, 则 $f(x^p)=g(x)^p$, $g(x)$ 是 F_q 上的一个多项式.

证明 在 F_q 上建立映射

$$\begin{aligned} F_q &\xrightarrow{\sigma} F_q \\ a &\longmapsto a^p. \end{aligned}$$

由于 $a^q=a^{p^n}=a$, 即 $\sigma^n(a)=a$. 故 $\sigma(\sigma^{n-1}(F_q))=F_q$, 当然有 $\sigma(F_q)=F_q$, 即 σ 是满射*.

* 实际上 σ 是 F_q 上自同构.

现设 $f(x)=a_kx^k+a_{k-1}x^{k-1}+\cdots+a_0$, $a_i\in F_q$. 由 σ 是满射,有 $b_i\in F_q$, 使得 $a_i=\sigma(b_i)=b_i^p$, $i=0,1,\cdots,k$. 于是

$$\begin{aligned}f(x^p)&=a_k(x^p)^k+a_{k-1}(x^p)^{k-1}+\cdots+a_0\\&=b_k^p(x^k)^p+b_{k-1}^p(x^{k-1})^p+\cdots+b_0^p\\&=(b_kx^k)^p+(b_{k-1}x^{k-1})^p+\cdots+b_0^p\\&=(b_kx^k+b_{k-1}x^{k-1}+\cdots+b_0)^p.\end{aligned}$$

令 $g(x)=b_kx^k+b_{k-1}x^{k-1}+\cdots+b_0$, 则 $f(x^p)=g(x)^p$.

推论 若 $h(x)$ 是 F_q 上不可约多项式,则不能有 F_q 上 $f(x)$ 使得 $h(x)=f(x^p)$.

定理 2 (1) F_q 上有任意 m 次不可约多项式,且存在 F_q 的扩域 F_{q^m}.

(2) F_q 上任意 m 次不可约多项式都是 $x^{q^m}-x$ 的因式,且它在 F_q 的一个扩域 F_{q^m} 上完全分解成一次因式的乘积.

(3) $F_q[x]$ 上的不可约多项式 $f(x)$ 是 $x^{q^m}-x$ 的因式当且仅当 $f(x)$ 的次数 r 满足 $r\mid m$.

证明 (1) 与(2) 的证明类似于 §1 中定理 3 及推论的证明,只要把 p 换成 q, n 换成 m, $\mathbb{Z}_p$ 换成 F_q, p^n 换成 q^m,就可照搬过来.

(3) 设 $f(x)$ 是 F_q 上不可约多项式,次数 r, $r\mid m$. 由此知,

$$x^{q^r}-x\mid x^{q^m}-x.$$

由(2) 知 $f(x)\mid x^{q^r}-x$,则 $f(x)\mid x^{q^m}-x$.

再设 $f(x)$ 在 F_q 上不可约,次数 r 以及 $f(x)\mid x^{q^m}-x$. 取 q^m 个元的域 F_{q^m}. 因 F_{q^m} 由 $x^{q^m}-x$ 的全部根组成,它含有 x^q-x(是 $x^{q^m}-x$ 的因式) 的 q 个根. 由 §1 定理 3 的推论 2 知,这 q 个根组成域 F_q. 故 $F_q\subset F_{q^m}$. 又 $f(x)\mid x^{q^m}-x$,故可取 F_{q^m} 中的元 β 使其为 $f(x)$ 的根. $F_q(\beta)$ 是 F_{q^m} 的子域,且 $F_q(\beta)\cong\dfrac{F_q[x]}{(f(x))}$,于是 $F_q(\beta)$ 有 q^r 个元. 再由 $m=[F_{q^m}:F_q]=[F_{q^m}:F_q(\beta)][F_q(\beta):F_q]$ 及 $[F_q(\beta):F_q]=r$,得 $r\mid m$.

推论 $x^{q^m}-x$ 等于 F_q 上所有次数除尽 m 的不可约多项式的乘积.

证明 令 M 为 F_q 上所有次数除尽 m 的不可约多项式的集合. 再令

$$x^{q^m}-x=p_1(x)p_2(x)\cdots p_s(x),\tag{1}$$

$p_i(x)$ 皆为 F_q 上不可约多项式. 由于 $x^{q^m}-x$ 无重因式, $p_1(x),p_2(x),\cdots,p_s(x)$ 互不相同. 由定理 2 知

$$M = \{p_1(x), p_2(x), \cdots, p_s(x)\},$$

再由(1)式，$x^{q^m} - x$ 等于 M 中所有多项式的乘积.

下面我们引进 F_q 上 $f(x)$ 的周期的概念.它在实际应用中很重要.

由于 $F_{q^m} \setminus \{0\}$ 是 $q^m - 1$ 阶乘法循环群.对 F_q 上任意 m 次不可约多项式 $f(x)$，$F_{q^m} \cong \dfrac{F_q[x]}{(f(x))}$.若 $x = x + (f(x)) \neq 0$，即 $x \neq f(x)$，则 $\bar{x}^{q^m-1} = \bar{1}$.这推出 $x^{q^m-1} - 1 \equiv 0 (\mathrm{mod}\ f(x))$ 或 $f(x) \mid x^{q^m-1} - 1$.设 $\bar{x}$ 在 $F_{q^m} \setminus \{0\}$ 的乘法群的阶为 e，e 即为最小正整数使 $\bar{x}^e = \bar{1}$ 或 $f(x) \mid x^e - 1$.又 $F_{q^m} \setminus \{0\}$ 的阶为 $q^m - 1$，而 $\bar{x}$ 的阶为 e，必然有 $e \mid q^m - 1$.引入下述

定义 1 设 $f(x)$ 是 F_q 上不可约多项式及 $f(x) \neq x$.称满足 $f(x) \mid x^e - 1$ 的最小正整数 e 为 $f(x)$ 的**周期**.

前面的讨论可写成

命题 1 设 $f(x) \neq x$ 是 F_q 上不可约多项式，则 $f(x)$ 的周期 e 就是 $\bar{x} = x + (f(x))$ 在乘法群 $\dfrac{F_q(x)}{(f(x))} \setminus \{\bar{0}\}$ 中的阶.因而 $e \mid q^m - 1$.

又 $F_{q^m} \setminus \{0\}$ 是 $q^m - 1$ 阶循环群.设它的一个生成元为 α，则 α 的阶为 $q^m - 1$.F_{q^m} 的元都是 $x^{q^m} - x$ 的根，α 也是.于是 α 是 $x^{q^m} - x$ 的 F_q 上某不可约因式 $f(x)$ 的根.由 $F_{q^m} \setminus \{0\} = \langle \alpha \rangle$ 及 $0 \in F_q$，推出 $F_{q^m} = F_q(\alpha)$.于是 $F_q(\alpha) \cong \dfrac{F_q(x)}{(f(x))}$.写 $\bar{x} = x + (f(x))$ 及 $\dfrac{F_q[x]}{(f(x))} = F_q(\bar{x})$，则 $F_q(\alpha) \cong F_q(\bar{x})$.因 $\alpha \neq 0$，所以 $\bar{x} \neq 0$，即 $x \neq f(x)$.

这样，对任意 m 我们可得到 F_q 上 m 次的不可约多项式 $f(x)$，$f(x) \neq x$，并且 $f(x)$ 的周期也即 $\bar{x} = x + (f(x))$ 的阶为 $q^m - 1$.

定义 2 设 $f(x) \neq x$ 是 F_q 上 m 次不可约多项式.若它的周期是 $q^m - 1$，则称为**本原多项式**.

前面的讨论说明 F_q 上任意 m 次本原多项式一定存在.

例 验证 $F_2[x]$ 上 $g(x) = x^4 + x + 1$ 是否本原多项式.

首先证它是 F_2 上不可约的.F_2 上一次和二次不可约多项式只有 x，$x + 1$，$x^2 + x + 1$.经计算它们都不是 $g(x)$ 的因式.因此 $g(x)$ 在 F_2 上不可约.

再证它的本原性.$2^4 - 1 = 15$，故 $g(x) \mid x^{15} - 1$.$g(x)$ 的周期是 15 的因子，只可能是 1，3，5，15，显然 $g(x)$ 不是 $x - 1$，$x^3 - 1$，$x^5 - 1$ 的因子.故 $g(x)$ 的周期为 15，是 F_2 上本原多项式.

下面介绍本原多项式的一点应用.利用本原多项式来构造纠一个错的码.

对 F_2 上任意 15 元向量 $(a_1, a_2, \cdots, a_{15})$，将它与 F_2 上一个多项式对应：

$f(x)=a_1x^{14}+a_2x^{13}+\cdots+a_{15}$. 取定一个4次本原多项式 $g(x)$,规定码集合为

$$M=\{(a_1,a_2,\cdots,a_{15})\mid f(x)\text{ 是 }g(x)\text{ 的倍数}\}.$$

由于 $F_2[x]$ 中$\leqslant 14$次的多项式*的集合作成 $F_2[x]$ 的子空间,它是15维的,取基底 $x^{14},x^{13},\cdots,x,1$,则 $f(x)=a_1x^{14}+a_2x^{13}+\cdots+a_{15}$ 与$(a_1,a_2,\cdots,a_{15})$的对应是向量与坐标向量的对应. 它保持加法和与 F_2 中元素的数量乘法. 我们干脆等同它们,把 M 中码子所对应的多项式也叫做码子. 因此一个多项式 $f(x)$ 是码子当且仅当 $f(x)=g(x)h(x)$,其中 $h(x)$ 是 F_2 上$\leqslant 10$次的多项式**. 我们也写码集合为

$$M=\{f(x)\in F_2[x]\mid f(x)=g(x)h(x),\partial(h(x))\leqslant 10\},$$

M 有基$\{x^{10}g(x),x^9g(x),\cdots,g(x)\}$,故是 $F_2[x]$ 的11维子空间.

设 M 的一个码子 $f(x)$ 经传输后,收到的向量 $f_1(x)$ 至多只有一位错. 数学上看是下述情况:

(i) 传输中没出错,$f_1(x)=f(x)$,则 $g(x)\mid f_1(x)$.

(ii) 错在第 i 项. 写 $f(x)=\sum_{j=1}^{15}a_jx^{15-j}$. 第 i 项系数a_i,由0变成1或由1变成0. 也即变成 a_i+1(F_2 中的加法). 于是 $f_1(x)=\sum_{j=1}^{15}a_jx^{15-j}+x^{15-i}=f(x)+x^{15-i}$. 若用 $g(x)$ 去除 $f_1(x)$,其余式正是用 $g(x)$ 去除 x^{15-i} 所得的余式. 因 $g(x)\nmid f_1(x)$,其余式不为零.

如何由余式定出 x^{15-i}. 这需要15个单项式 $x^{14},x^{13},\cdots,x,1$ 被 $g(x)$ 除所得的余式(皆不为零)皆不相同. 这个性质可通过 $\frac{F[x]}{(g(x))}$ 的元素来表达. 即 $\bar{x}^{14}=x^{14}+(g(x)),\bar{x}^{13}=x^{13}+(g(x)),\cdots,\bar{x}=x+(g(x)),\bar{1}=1+(g(x))$ 是 $\frac{F_2[x]}{(g(x))}$ 的15个不同的非零元. 它们组成的乘法群$\langle\bar{x}\rangle$是15阶群,正是 $\frac{F[x]}{(g(x))}$ 的全部非零元的乘法群. 这等价于 $g(x)$ 是 F_2 上的本原多项式. 因此当 $g(x)$ 选为本原多项式以后,用 $g(x)$ 去除 $x^{14},x^{13},\cdots,x,1$ 得到15个余式 $r_1(x),r_2(x),\cdots,r_{14}(x),r_{15}(x)$ 互不相同,且 $\overline{r_i(x)}=\bar{x}^{15-i}$.

现在可以进行纠错了.

(i) $g(x)\mid f_1(x)$,$f_1(x)$ 就是 $f(x)$.

(ii) $g(x)\nmid f_1(x)$. 用 $g(x)$ 去除 $f_1(x)$ 得余式 $r(x)\neq 0$. 计算 $xr(x)$,

* 包括零多项式

** 包括零多项式.

$x^2r(x),\cdots,x^{14}r(x),x^{15}r(x)$ 被 $g(x)$ 除的余式. 由于 $\overline{x}\,\overline{r(x)},\overline{x^2}\,\overline{r(x)},\cdots,\overline{x^{15}}\,\overline{r(x)}$ 是 $\dfrac{F_2[x]}{(g(x))}$ 中 15 个不同的非零元,只有一个为 $\overline{1}$. 设 $\overline{x^i}\,\overline{r(x)}=\overline{1}$,则 $x^ir(x)$ 被 $g(x)$ 除的余式为 1. 由于 $r(x)$ 是某 x^{15-i} 的余式,于是 $\overline{x^j}\,\overline{r(x)}=\overline{x^jx^{15-i}}=\overline{1}$. 但 $\overline{x}\,\overline{r(x)},\overline{x^2}\,\overline{r(x)},\cdots,\overline{x^{15}}\,\overline{r(x)}$ 中仅能有一个为 $\overline{1}$. 因而 $i=j$. 即若 $f_1(x)$ 只错了一位,就只能错在 x^{15-i} 的这位置上. 结果是 $f(x)=f_1(x)+x^{15-i}$.

习 题

1. 验证 $\dfrac{\mathbb{Z}_3[x]}{(x^2+1)}$ 的非零元乘法群是循环群,找出生成元. x^2+1 是否本原多项式?

2. x^3+x+1,x^4+x+1 是否 $\mathbb{Z}_2[x]$ 中的本原多项式?

3. 证明映射

$$F_{p^m}\longrightarrow F_{p^m}$$
$$a\longrightarrow a^p$$

是 F_{p^m} 的自同构且保持 F_{p^m} 中的素子域 F_p 中的元素不动.

4. $f(x)$ 是 $\mathbb{Z}_p$ 上 m 次不可约多项式. 设 $\alpha\in F_{p^m}$ 是 $f(x)$ 的一个根,则 $\alpha,\alpha^p,\cdots,\alpha^{p^{m-1}}$ 是 $f(x)$ 的全部 m 个根.

5. 设 $\beta\in F_{p^m}$,β 在 $\mathbb{Z}_p$ 上的极小多项式 $f(x)$ 是 d 次的,则(1)β 属于 F_{p^m} 中的一个 p^d 个元的子域. (2) $d\mid m$.

6. 证明 F_{p^m} 中元素 β 与 β^p 在 $\mathbb{Z}_p$ 上有相同的极小多项式.

7. 设 α 是 $\mathbb{Z}_3[x]$ 中多项式 x^4+x+2 的一个根. 把 $\mathbb{Z}(\alpha)$ 中全部元素用 $1,\alpha,\alpha^2,\alpha^3$ 的线性组合表示出来. 并算出 $\dfrac{1+\alpha+\alpha^3}{1+\alpha^2+\alpha^3}+\alpha+\alpha^2$.

8. 把 $x^{2^4}-x,x^{2^3}-x$ 分解成 $\mathbb{Z}_2[x]$ 上不可约多项式的乘积,把 $x^{3^3}-x$,$x^{3^2}-x$ 分解成 $\mathbb{Z}_3[x]$ 上不可约多项式的乘积.

9. 取 $\mathbb{Z}_2[x]$ 中本原多项式 x^3+x+1. 在多项式 $\sum_{i=1}^{6}a_ix^{7-i}=a_1x^6+a_2x^5+\cdots+a_6x+a_7$ 与向量 $(a_1,a_2,\cdots,a_n)$ 等同的约定下,作码集合

$$M=\{(x^3+x+1)(b_1x^3+b_2x^2+b_3x+b_4)\mid b_i\in\mathbb{Z}_2\}.$$

(i) 取 $f(x)=x^6+x^4+c_1x^2+c_2x+c_3$,试决定 c_1,c_2,c_3 使 $f(x)$ 属于码集合 M.

(ii) 设 $f_1(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ 是接受到的向量，并设传输过程中最多错一位，试进行译码.

§3 线性移位寄存器序列

线性移位寄存器序列，特别是最长周期的移位寄存器序列(简称为 m 序列)是一类应用广泛的0,1序列.例如在连续波雷达中可作为测距信号，在遥控信号系统中作遥控信号，还可作噪声源，在保密通讯中起加密作用，在多址通讯中用作地址信号等.线性移位寄存器序列所以能有很广泛的应用，主要是它有许多优美的性质.这些性质全都可借助有限域理论来得到.这一节只介绍线性移位寄存器序列有关周期性方面的性质.从讨论中看到抽象代数的重要作用.正是引进了二元域(有限域)，研究了有关的理论，才能把线性移位寄存器序列的讨论归结为数学问题，并利用数学方法来解决问题.

如下的框图表示了线性移位寄存器的逻辑功能:(我们不讨论它的物理构造)

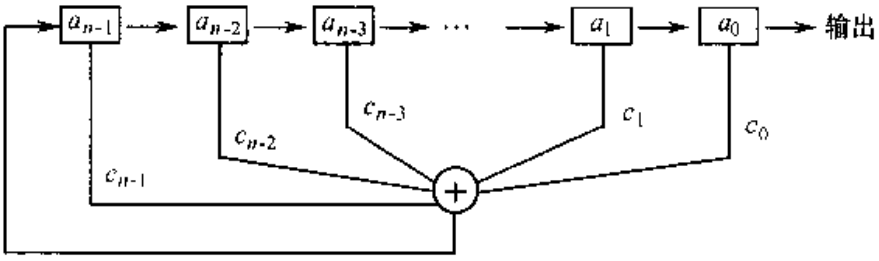


图 1

图中每个方框是一个寄存器，它只有两个状态，正好表示存放的是0或1这两个元.整个移位寄存器的最初状态是在各寄存器中已分别给定了 a_{n-1}, $a_{n-2}, \cdots, a_1, a_0$，它们都是0或1.开始工作是给各寄存器同时加一个移位脉冲，于是各寄存器把所存的"数"都向右移给下一个寄存器，而最后(即最右)一个寄存器的内容 a_0 就输出.同时将全部移位寄存器的内容按下面公式在 F_2 中进行加法得 a_n，

$$a_n = c_{n-1}a_{n-1} + c_{n-2}a_{n-2} + \cdots + c_0 a_0, \tag{1}$$

并把它反馈回第一个(最左边)寄存器中，这就完成了第一步工作.完成后移位寄存器的状态如图2.

注意:要实现(1)中的运算，图中各寄存器与加法器的连线情况应随各 c_i 来决定.因 c_i 只能为0或1，若为1，则(1)中加了一项 a_i，这时图1中相应于 a_i 的寄存器与加法器就用线连接.若 $c_i = 0$，则不连接.

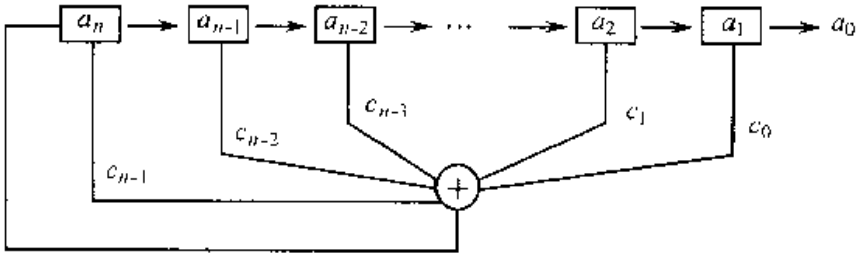


图 2

对移位寄存器的图 2 状态，再加一个移位脉冲，就重复第一次的工作流程，不断地加移位脉冲，则有不断的输出．于是输出一个序列 $a_0, a_1, a_2, \cdots$．记它为

$$\boldsymbol{a} = (a_0, a_1, a_2, \cdots). \tag{2}$$

每一步工作流程都作一次反馈，就有与(1) 相应的关系．对第 $k+1$ 步的反馈，就是关系

$$a_{k+n} = c_{n-1}a_{k+(n-1)} + c_{n-2}a_{k+(n-2)} + \cdots + c_0 a_k, \tag{3}$$

$$k = 0, 1, 2, \cdots.$$

(第一步相应于 $k = 0$)．序列 $\boldsymbol{a}$ 就叫做**线性移位寄存器序列**．由于递推关系式(3) 的右端是线性函数，故在移位寄存器前面加了“线性”二字．

序列(2) 完全由初始状态 $(a_0, a_1, \cdots, a_{n-1})$ 及递推关系(3) 所决定．

还须指出，在实用中线性移位寄存器序列都是有限长的，且各种用途中所用的序列的长度也是不一样的．为了在数学上便于统一讨论，我们才把线性移位寄存器序列看成(2) 那样的无限序列．

下面的讨论中我们其实只要以(2) 和(3) 作为出发点，完全抽象地进行研究．暂时不必与移位寄存器联系了．在抽象的讨论中我们给出

定义 1 域 F_2 上的无限序列(2)，若满足递推公式(3)，就称为一个**线性递归序列**．

例如，无限序列

$$(0, 1, 1, 0, 1, 1, \cdots)$$

是由 0，1，1，无限重复而组成的序列．它适合

$$a_{k+2} = a_{k+1} + a_k, k = 0, 1, 2, \cdots.$$

故它是一个线性递归序列．

F_2 上全体无限序列的集合记作 $V(F_2)$．$V(F_2)$ 上可定义加法及数量乘法．

设 $\boldsymbol{a} = (a_0, a_1, a_2\cdots)$ 及 $\boldsymbol{b} = (b_0, b_1, b_2\cdots) \in V(F_2), c \in F_2$，令

$$\boldsymbol{a} + \boldsymbol{b} = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \cdots), c\boldsymbol{a} = (ca_0, ca_1, ca_2, \cdots).$$

易验证，$V(F_2)$ 在上面运算下成为 F_2 上线性空间. $V(F_2)$ 中的零元素是零序列

$$(0,0,0,\cdots),$$

我们常简记它为 0.

下面我们要用 $V(F_2)$ 中向量和线性变换的运算将关系式(3)换一个等价的写法.

对 $\boldsymbol{a}=(a_0,a_1,a_2,\cdots)$，定义 $V(F_2)$ 中的一个变换 L：

$$L\boldsymbol{a}=(a_1,a_2,a_3,\cdots).$$

这是 $\boldsymbol{a}$ 中的左移变换. 易知它是 $V(F_2)$ 上线性变换.(读者自己验证一下). 显然

$$L^2\boldsymbol{a}=L(L\boldsymbol{a})=(a_2,a_3,a_4,\cdots).$$

一般地

$$L^r\boldsymbol{a}=(a_r,a_{r+1},a_{r+2},\cdots).$$

比较 $L^n\boldsymbol{a}$ 和 $\sum_{i=0}^{n-1}c_iL^i\boldsymbol{a}$ 的任意第 $k+1$ 位的分量，这正是关系式(3)的左端与右端. 当 $k=0,1,2,\cdots$ 时，(3)的左端与右端都相等，就是下面两个序列相等，

$$L^n\boldsymbol{a}=\sum_{i=0}^{n-1}c_iL^i\boldsymbol{a}$$

或

$$L^n\boldsymbol{a}+\sum_{i=0}^{n-1}c_iL^i\boldsymbol{a}=0(\text{全零序列}). \tag{4}$$

令

$$f(x)=x^n+c_{n-1}x^{n-1}+\cdots+c_1x+c_0, \tag{5}$$

于是

$$f(L)=L^n+c_{n-1}L^{n-1}+\cdots+c_1L+c_0I.$$

这里 I 是 $V(F_2)$ 中的恒等变换. 由(4)就有

$$f(L)\boldsymbol{a}=0. \tag{6}$$

按(5)定义 $f(x)$ 后，关系式(3)与(6)是等价的. 于是我们可说：给定 $f(x)\neq 0$，无限序列 $\boldsymbol{a}$ 若满足 $f(L)\boldsymbol{a}=0$，就称为一个线性递归序列.

例 1 $(0,1,1,0,1,1,\cdots)=\boldsymbol{a}$，其中 0,1,1 无限重复. 它适合关系 $a_{k+2}=a_{k+1}+a_k, k=0,1,\cdots$. 令 $f(x)=x^2+x+1$，则

$$f(L)\boldsymbol{a}=L^2\boldsymbol{a}+L\boldsymbol{a}+\boldsymbol{a}=0.$$

又易发现 $\boldsymbol{a}$ 为是周期为3的序列. 即 $\boldsymbol{a}$ 满足：$a_{k+3}=a_k, k=0,1,2,\cdots$. 这关系等价于 $L^3\boldsymbol{a}=\boldsymbol{a}$.

例 2 由上例的启发，试问 F_2 上无限序列 $\boldsymbol{a}$ 何时是周期序列？答案也易

得到:$\boldsymbol{a}$ 是周期序列当且仅当有 $k \geqslant 1$,使 $L^k\boldsymbol{a} = \boldsymbol{a}$.

实际上,后者等价于有 $k \geqslant 1$,使 $a_{k+l} = a_l, l = 0,1,2,\cdots$.

现在我们转入这一节的主题,研究线性递归序列的周期性问题.我们的目标不是介绍这个问题的完全彻底的答案.而是通过典型的情形展示线性递归序列的一些优美的结果.也看到有限域理论是多么巧妙地被应用到线性递归序列的问题中.这个人们事先演绎出来的理论就像是为它订制的,对它是多么合用.我们看到了抽象代数的魅力和威力.

由例 1 可发现,一个线性递归序列 $\boldsymbol{a}$ 可能满足多个递推关系.例 1 中的 $\boldsymbol{a}$ 就满足

$$a_{k+2} + a_{k+1} + a_k = 0, \text{及 } a_{k+3} + a_k = 0, k = 0,1,2,\cdots.$$

用多项式来表达就有 $f(x) = x^2 + x + 1$ 及 $g(x) = x^3 + 1$ 使得 $f(L)\boldsymbol{a} = 0$ 及 $g(L)\boldsymbol{a} = 0$.对于所有这样的多项式的集合有什么特点呢?我们有

命题 1 设 $f(x)$ 是 F_2 上的非零多项式,$\boldsymbol{a}$ 是满足关系式(6)的一个线性递归序列,令

$$A(\boldsymbol{a}) = \{g(x) \in F_2(x) \mid g(L)\boldsymbol{a} = 0\},$$

则 $A(\boldsymbol{a})$ 是 $F_2[x]$ 中的非零理想,$A(\boldsymbol{a}) = (m(x)), m(x) \neq 0$.特别地,当 $\boldsymbol{a} \neq 0$ 且 $f(x)$ 是不可约多项式时,$A(\boldsymbol{a}) = (f(x))$.

证明 我们有

(1) 因 $f(x) \in A(\boldsymbol{a})$,故 $A(\boldsymbol{a})$ 中有非零多项式.

(2) 若 $h(x), g(x) \in A(\boldsymbol{a})$,则 $h(x) + g(x) \in A(\boldsymbol{a})$.这是显然的.

(3) 若 $g(x) \in A(\boldsymbol{a}), h(x) \in F_2[x]$,则 $h(x)g(x) \in A(\boldsymbol{a})$.

这是因为 $h(L)g(L)\boldsymbol{a} = h(L)(g(L)\boldsymbol{a}) = h(L)0 = 0$,故 $h(x)g(x) \in A(\boldsymbol{a})$.

于是 $A(\boldsymbol{a})$ 是 $F_2[x]$ 中的一个非零理想.而 $F_2[x]$ 是主理想环,就有 $m(x) \in F_2[x], m(x) \neq 0$,使 $A(\boldsymbol{a}) = (m(x))$.因 $f(x) \in A(\boldsymbol{a})$,而有 $m(x) \mid f(x)$.若 $f(x)$ 不可约,则 $m(x) = cf(x)$ 或 $m(x) = c$,c 是 F_2 中非零常数,只能为 1.又 $\boldsymbol{a} \neq 0$,若 $m(x) = 1$,则 $m(L)\boldsymbol{a} = I\boldsymbol{a} = \boldsymbol{a} \neq 0$,这不可能.故 $m(x) = cf(x)$ 及 $A(\boldsymbol{a}) = (f(x))$.

这样对线性递归序列 $\boldsymbol{a}$,若 $A(\boldsymbol{a}) = (m(x)), m(x)$ 是 $A(\boldsymbol{a})$ 中次数最低的,设为 n 次,则 $\boldsymbol{a}$ 所满足的反馈关系(3)中,右端最少的为 n 项.

定义 2 $\boldsymbol{a}$ 是线性递归序列,设 $A(\boldsymbol{a}) = (m(x)), m(x)$ 是 n 次的,则称 $\boldsymbol{a}$ 为 n 级线性递归序列.

由命题 1 知道,若 $\boldsymbol{a}$ 是满足 $f(L)\boldsymbol{a} = 0$ 的线性递归序列,$\boldsymbol{a} \neq 0$,及 $f(x)$ 是 F_2 上 n 次不可约多项式,则 $\boldsymbol{a}$ 是 n 级线性递归序列.

现在给出周期的定义.

定义 3 F_2 上的一个无限序列

$$\boldsymbol{a} = (a_0, a_1, a_2, \cdots).$$

如果有正整数 l 存在，使得

$$a_{k+l} = a_k, k = 0, 1, 2, \cdots, \tag{7}$$

则称 $\boldsymbol{a}$ 为一个周期序列，具有长为 l 的周期性，并将满足(7)的最小正整数 l 称为 $\boldsymbol{a}$ 的**周期**，记为 $p(\boldsymbol{a})$.

由例2中的分析，并回忆 §2 命题1关于多项式 $f(x)$ 的周期的结果，我们可证

定理 2 设 $f(x) \neq x$ 是 F_2 上不可约多项式，则满足关系式(6)的非零的线性递归序列 $\boldsymbol{a}$ 是周期序列，且 $f(x)$ 的周期就是 $\boldsymbol{a}$ 的周期.

证明 由 §2 命题1(注意，定理中假设 $f(x) \neq x$，正是 §2 命题1中所必须的)，$f(x)$ 有周期 e，即有 $f(x) \mid x^e - 1$. 于是有 $h(x) \in F_2[x]$ 使，$x^e - 1 = h(x)f(x)$. 移项后得 $x^e = h(x)f(x) + 1$. 用 L 代入，则有 $L^e = h(L)f(L) + I$，I 为 $V(F_2)$ 上恒等变换. 再来变换 $\boldsymbol{a}$，得到

$$L^e\boldsymbol{a} = h(L)f(L)\boldsymbol{a} + \boldsymbol{a} = h(L)(f(L)\boldsymbol{a}) + \boldsymbol{a} = h(L)0 + \boldsymbol{a} = \boldsymbol{a}.$$

用分量写出来就是 $a_{e+k} = a_k, k = 0, 1, 2, \cdots$. 由定义3得 $p(\boldsymbol{a}) \leqslant e$.

另一方面，$\boldsymbol{a}$ 的周期为 $p(\boldsymbol{a})$，即有 $L^{p(\boldsymbol{a})}\boldsymbol{a} = \boldsymbol{a}$，于是 $(L^{p(\boldsymbol{a})} + I)\boldsymbol{a} = 0$. 令 $h(x) = x^{p(\boldsymbol{a})} + 1$，则 $h(L)\boldsymbol{a} = 0$，这样 $h(x) = x^{p(\boldsymbol{a})} + 1 \in A(\boldsymbol{a})$. 因 $f(x)$ 不可约，由命题1，$A(\boldsymbol{a}) = (f(x))$. 因此 $x^{p(\boldsymbol{a})} + 1$ 是 $f(x)$ 的倍数. 因 $f(x)$ 的周期为 e，故 $f(x)$ 的形为 $x^k + 1 = x^k - 1$ 的倍数中次数最小的是 e. 所以 $e \leqslant p(\boldsymbol{a})$. 与前面已证的 $p(\boldsymbol{a}) \leqslant e$ 合起来就是 $p(\boldsymbol{a}) = e$. 定理得证.

现在引入记号：对 F_2 上多项式 $f(x)$，令

$$G(f) = \{\boldsymbol{a} \in V(F_2) \mid f(L)\boldsymbol{a} = 0\}.$$

上面定理说，若 $f(x) \neq x$ 是 F_2 上 n 次不可约多项式，则 $G(f)$ 中所有非零序列的周期相同. 皆等于 $f(x)$ 的周期.

推论 1 设 $f(x) \neq x$ 是 F_2 上 n 次不可约多项式，则 $G(f)$ 中每个非零序列 $\boldsymbol{a}$ 的周期 $p(\boldsymbol{a})$ 满足 $p(\boldsymbol{a}) \mid 2^n - 1$.

证明 由定理1及 §2 命题1.

推论 2 $f(x) \neq x$ 是 F_2 上不可约多项式，$\boldsymbol{a}, \boldsymbol{b}$ 是 $G(f)$ 中两个不同的序列，则 $\boldsymbol{a} + \boldsymbol{b}$ 的周期仍与 $f(x)$ 的周期相同.

证明 由 $G(f)$ 的定义知，$\boldsymbol{a} + \boldsymbol{b} \in G(f)$. $\boldsymbol{a} \neq \boldsymbol{b}$ 得出 $\boldsymbol{a} + \boldsymbol{b} \neq 0$. 再由定理2得结论.

推论 3 设 $f(x)$ 是 F_2 上 n 次本原多项式，则 $G(f)$ 中非零序列 $\boldsymbol{a}$ 的周期为 $2^n - 1$.

证明 由定理 2 及 §2 中本原多项式的定义 2.

在所有 n 次不可约多项式 $f(x) \neq x$ 中,本原多项式作出的 $G(f)$ 中非零序列 $\boldsymbol{a}$ 的极小周期最长(比较推论 1,3).

定义 4 n 级线性递归序列的周期若是 $2^n - 1$,则称为 ***m* 序列**.

推论 3 说,由本原多项式 $f(x)$ 作出的 $G(f)$ 中的非零序列是 m 序列.

这一章到此就结束了.以上关于有限域理论和一点应用的介绍展示了这个"人为"的理论还是真有用呢?实际上近年来在计算机和信息科学中的许多离散的数学问题中它起的作用越来越大.

习 题

1. F_p(p 为素数)上首项系数为 1 的 m 次本原多项式的个数为 $\varphi(p^m - 1)/m$,这里 φ 是欧拉函数(参见二章 §5).并算出 $\mathbb{Z}_2$,$\mathbb{Z}_3$ 上二次、四次本原多项式的数目.

2. 作出 $\mathbb{Z}_2$ 上二个周期为 7 的 m 序列(写出 2 个周期的长度).

3. 设 F_2 上序列 $\boldsymbol{a} = (a_0, a_1, a_2, \cdots)$ 的周期为 e.证明

(i) 若有 e' 使 $a_{k+e'} = a_k, k = 0,1,2,\cdots$,则 $e \mid e'$.

(ii) 若令 $S_0 = (a_0, \cdots, a_{e-1}), S_1 = (a_1, \cdots, a_e), \cdots, S_{e-1} = (a_{e-1}, \cdots, a_{2e-2})$,则它们两两不同.

4. 设 $f(x)$ 是 F_2 上 n 次不可约多项式,则

(i) $G(f)$ 是 F_2 上向量空间.

(ii) 对任意 $\boldsymbol{a} \in G(f)$.令 $S_{\boldsymbol{a}} = (a_0, a_1, \cdots, a_{n-1})$,称为 $\boldsymbol{a}$ 的初始状态向量,则 $\forall \boldsymbol{a}, \boldsymbol{b} \in G(f)$,$\boldsymbol{a} = \boldsymbol{b}$ 当且仅当 $S_{\boldsymbol{a}} = S_{\boldsymbol{b}}$.

(iii) $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_k, \boldsymbol{a} \in G(f), l_1, \cdots, l_k \in F_2$,则

$$\boldsymbol{a} = l_1\boldsymbol{a}_1 + \cdots + l_k\boldsymbol{a}_k \text{ 当且仅当 } S_{\boldsymbol{a}} = l_1 S_{\boldsymbol{a}_1} + \cdots + l_k S_{\boldsymbol{a}_k}.$$

于是 $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_k$ 线性相关当且仅当 $S_{\boldsymbol{a}_1}, \cdots, S_{\boldsymbol{a}_k}$ 线性相关.

(iv) $G(f)$ 是 F_2 上 n 维空间.

5. 设 $f(x)$ 是 $F_2[x]$ 中 n 次本原多项式,$\boldsymbol{a}$ 是 $G(f)$ 中非零序列,即 m 序列,则

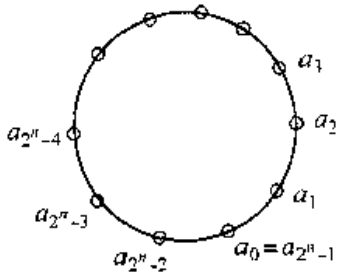
$$\boldsymbol{a} = \boldsymbol{a}_0, L\boldsymbol{a} = \boldsymbol{a}_1, \cdots, L^{2^n-2}\boldsymbol{a} = \boldsymbol{a}_{2^n-2}$$

是 $G(f)$ 中全部非零序列.进一步 $S_{\boldsymbol{a}_0}, S_{\boldsymbol{a}_1}, \cdots, S_{\boldsymbol{a}_{2^n-2}}$ 全不相同,它们是 F_2 上 n 元向量空间中全部非零向量.

6. 设

$$\boldsymbol{a} = (a_0, a_1, a_2, \cdots)$$

是 F_2 上周期为 2^n-1 的 m 序列.将 a 的一个周期 $(a_0,a_1,\cdots,a_{2^n-2})$ 中的元



依次排在圆周上,并使 a_{2^n-2} 与 $a_0=a_{2^n-1}$ 相邻,则 F_2 上的任一 k 元组 $(1\leqslant k\leqslant n)$,

$$(b_1,b_2,\cdots,b_k)$$

在上述圆周中出现的次数为

$$\begin{cases}2^{n-k}, & \text{若}(b_1,b_2,\cdots,b_k)\neq(0,0,\cdots,0),\\ 2^{n-k}-1, & \text{若}(b_1,b_2,\cdots,b_k)=(0,0,\cdots,0).\end{cases}$$

(考察有多少个 S_{a_r} 的前 k 个元正是 $b_1,b_2,\cdots,b_k$).

7. a 为 F_2 上周期为 2^n-1 的 m 序列,则在 a 的一个周期中 1 的数目为 2^{n-1},0 的数目为 $2^{n-1}-1$.

8. 对习题 2 中作出的 F_2 上周期为 7 的两个 m 序列的一个周期排成圆圈如习题 6,数出 1,0,01,10,101,110,出现的次数.

第四章　有因式分解唯一性的环，中国剩余定理

在第二章中我们介绍了环的一些基本概念.在那里主要是为第二章的中心内容"域"服务，用环论方法来造一些新的域(当然也造出一些新的环).这一章继续介绍环的内容，有两个方面：一是深入讨论整环中的因式分解问题.对整数环及域上多项式环已有因式分解唯一性定理.这两个环的直接抽象是有除法算式和辗转相除法(也叫欧几里得算法)的环，称为欧几里得环，简称欧氏环.因式分解唯一性定理对欧氏环依然成立，连证明方法也是直接推广.欧氏环有一重要性质：它的任何理想都是主理想(见第二章 §4 例10).我们把具有这种性质的整环叫做主理想(整)环.利用主理想性质，不依赖除法算式也可证明因式分解唯一性定理对主理想环成立.于是就有下述环类的包含关系：

欧氏环 $\subseteq$ 主理想环 $\subseteq$ 唯一因式分解环.

可证这些关系还是真包含关系.这是本章的第一方面的内容.第二方面是介绍中国剩余定理.这是中国古代数学书"孙子算经"中一个成果(亦被叫作孙子定理)的现代推广.

§1　整环的因式分解

回忆整环是有1的无零因子的交换环.以 R 表示一个整环.先对 R 建立有关整除和因式分解的概念.

$a, b \in R$，称 a **整除** b(或 b 可被 a 整除，也说 b 是 a 的倍数)，如果有 $c \in R$，使 $b = ac$.记为 $a \mid b$.这时也说 a 是 b 的**因子**.若 a 不能整除 b，记为 $a \nmid b$.

若 $b = ac$ 且 c 是 R 中可逆元(即 c 在 R 中有逆元素)，则称 a 与 b 为**相伴元**(这时 $a = bc^{-1}$).

我们知道在 $\mathbb{Z}$ 中 n 与 $-n$ 是相伴的，在 $F[x]$ 中(F 是域) $f(x)$ 与 $cf(x)$ 是相伴的，其中 $0 \neq c \in F$.

非零元素 $p \in R$ 称为**不可约元**，如果 p 不是可逆元且不能写成 $p = ab$ 的形式，其中 a, b 皆非可逆元.显然，$p \in R$ 与其相伴元同时是或不是不可约元.

$\mathbb{Z}$ 中的素数 p 和 $F[x]$ 中的不可约多项式都是不可约元的例子.

R 中整除有以下性质：

(i) 若 $a|b$，且 $b\ c$ 则 $a|c$.

由假设有 $b = ab'$ 及 $c = bc'$，$b', c' \in R$. 因此 $c = bc' = (ab')c' = a(b'c')$，即 $a|c$.

(ii) 若 $c|a$ 且 $c|b$，则 $c|(a \pm b)$.

因为 $a = ca'$ 及 $b = cb'$，就有 $(a \pm b) = c(a' \pm b')$.

(iii) 若 $a|b$，则 $a|bc$.

因 $b = ab'$，则 $bc = a(b'c)$.

结合(ii)和(iii)则有

(iv) 设 $b_1, \cdots, b_m \in R$，若每个 b_i 都被 $a \in R$ 整除，则它们的任意线性组合 $b_1c_1 + b_2c_2 + \cdots + b_mc_m$ 也能被 a 整除，其中 $c_1, 2, \cdots, c_m$ 为 R 中任意元素.

(v) a 与 b 相伴当且仅当 $a|b$ 且 $b|a$.

设 a 与 b 相伴，则 $a = bc$，$b = ad$，其中 c, d 皆为 R 中可逆元. 故 $b|a$，$a|b$.

反之设 $a|b$ 及 $b|a$. 于是 $a = bc$，$b = ad$，得到 $b = bcd$. 因此 $b(1 - cd) = 0$. 若 $b = 0$，易知 $a = 0$，当然 a 与 b 相伴. 当 $b \neq 0$，由 R 无零因子知，$1 - cd = 0$. $cd = 1$，说明 c, d 皆为可逆元. 故 a, b 相伴.

现在可给出唯一因式分解环的定义了.

定义 1 设 R 是整环，(i)若对 R 中任意非零且非可逆的元 a 都可表示为

$$a = up_1p_2\cdots p_r, \tag{1}$$

其中 $r \geqslant 1$，u 为可逆元，$p_1, \cdots, p_r$ 为 R 中不可约元(可以有相伴的). (ii)且若有另外一个这样的表达式

$$a = vq_1\cdots q_s,$$

其中 v 为 R 中可逆元，$q_1, \cdots, q_s$ 为 R 中不可约元，则一定有 $r = s$. 若有必要，在适当改排 $q_1, \cdots, q_s$ 的脚标后，可使 p_i 与 q_i 成对地相伴，也即有 R 的可逆元 u_i，使 $p_i = u_iq_i$，$i = 1, 2, \cdots, r$. 我们称这样的整环 R 为**唯一因式分解环**.

定义中的(i)说明 R 中非零且不可逆的元能表成不可约因子的乘积. (ii)为表示法的唯一性.

定理 1 设 R 是一个整环，它的任一非零且非可逆的元都有因式分解(1)，则 R 是唯一因式分解环当且仅当 R 的任一不可约元 p 若整除乘积 ab，$a, b \in R$，则 p 一定整除 a 或 b.

证明 设 R 是唯一因式分解环，$p \in R$ 是不可约元且 $p|ab$，$a, b \in R$. 于是有 $c \in R$，使 $ab = pc$. 设 a, b 中有一个是零，比如 $a = 0$，则 $p|a$. 若 a, b 中有一个是可逆元，比如 a 是可逆元，则 $b = pca^{-1}$. 也得 $p|b$. 现在设 a, b

都是非零的不可逆元.R 是整环,故 $c \neq 0$.若 c 为可逆元,则

$$p = (ab)c^{-1} = a(bc^{-1}).$$

b 非可逆,c^{-1} 可逆,得(bc^{-1})非可逆.又 a 非可逆,于是与 p 不可约矛盾.这样 a,b,c 皆非零且非可逆.设

$$a = a_1a_2\cdots a_r, b = b_1b_2\cdots b_s, c = c_1c_2\cdots c_t$$

分别是 a,b,c 的不可约因子的乘积,则

$$a_1a_2\cdots a_rb_1b_2\cdots b_s = pc_1c_2\cdots c_t.$$

由 R 是唯一因式分解环,p 必与 a_i,b_j 之一相伴.设 $up = a_i$,则有 $a = a_1a_2\cdots up\cdots a_r$.可得 $p|a$.若 $up = b_j$,类似地得到 $p|b$.

反之,对任意不可约元 $p \in R$,若 $p|ab, a,b \in R$,则 $p|a$ 或 $p|b$.设 $c \in R$ 是非零且非可逆的元.且

$$\begin{aligned} c &= p_1\cdots p_r \\ &= q_1\cdots q_s \end{aligned} \tag{2}$$

是 c 的不可约因子的两个乘积.为证明表示法的唯一性我们对 r 作归纳法.

$r = 1$.这时 $c = p_1$ 不可约.q_1 已不可逆,若 $s > 1$,令 $u = q_2\cdots q_s$,$p_1 = q_1u$,u 必为可逆元.于是 $u^{-1}q_2\cdots q_s = 1$,这样每个 $q_2,\cdots,q_s$ 皆可逆,与它们是不可约元矛盾.故 $s = 1$.于是 $c = p_1 = q_1$,证明了表示法的唯一性.

设不可约因子数$\leqslant r-1$的乘积的表示法已有唯一性.来证不可约因子数为 r 时的乘积的表示法有唯一性.假设 $c \in R$ 有如(2)的两种表示法,并且 $r > 1$.因 $q_s|(p_1\cdots p_{r-1})p_r$,由定理的条件

$$q_s|p_r \text{ 或 } q_s|p_1\cdots p_{r-1}.$$

如是后者,可继续作下去.两者都可推出 $q_s|p_i$,i 是 $1,2,\cdots,r$ 中之一.于是有 $a \in R$,使 $q_sa = p_i$.因 p_i 不可约,a 必为可逆元,即 q_s 与 $p_1,\cdots,p_r$ 之一的 p_i 相伴.重排 $p_1,\cdots,p_r$ 的脚标使该 p_i 为 p_r,则由 $p_r = aq_s$ 有

$$p_1p_2\cdots p_r = q_1q_2\cdots q_s = q_1\cdots(a^{-1}q_{s-1})(aq_s).$$

用消去律得

$$p_1p_2\cdots p_{r-1} = q_1q_2\cdots(a^{-1}q_{s-1}). \tag{3}$$

(3)是不可约因子的两个乘积,左端乘积中元素数目为 $r-1$.可用归纳法,知 $r-1 = s-1$,即 $r = s$.而且经脚标的重排后 p_i 与 q_i 相伴,$i = 1,2,\cdots,r-1$.上而已证 p_r 与 q_r 相伴.这样就证明了唯一性.

定义 2 设 R 是整环,$p \in R$ 是非零的不可逆元.若 $p|ab, a,b \in R$,都有 $p|a$ 或 $p|b$,则称 p **为素元**.

在整环 R 中素元都是不可约元(留作习题),反之不一定.为此我们写出整环 R 成为唯一因式分解环的条件(iii):

(iii) R 是整环，R 的不可约元都是素元.

定理 1 将唯一因式分解环的定义中的条件(i)及(ii)换成了条件(i)和(iii).比较而言，在很多情形下，验证条件(iii)比验证条件(ii)容易操作.

例 1 $\mathbb{Z}$ 中素数既是不可约元也是素元.

例 2 $F[x]$(F 是域)中不可约多项式既是不可约元也是素元.

例 3 $\mathbb{Z}(\sqrt{-5}) = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ 对复数的加法和乘法成为环.令 $N(a + b\sqrt{-5}) = (a + b\sqrt{-5})\overline{a + b\sqrt{-5}} = |a + b\sqrt{-5}|^2 = a^2 + 5b^2$.即它是取复数模的平方.由于 $|\alpha||\beta| = |\alpha\beta|$.故 $N(\alpha)N(\beta) = N(\alpha\beta)$.它有性质：(i)$N(\alpha) = 0$ 当且仅当 $\alpha = 0$,(ii)$\alpha \in \mathbb{Z}(\sqrt{-5})$,$N(\alpha)$ 为非负整数，$\alpha \neq 0$ 时是正整数,(iii)$\alpha, \beta \in \mathbb{Z}(\sqrt{-5})$,若 $\alpha \mid \beta$,则 $N(\alpha) \mid N(\beta)$,(iv)$\alpha \in \mathbb{Z}(\sqrt{-5})$ 为可逆元当且仅当 $\exists \beta \in \mathbb{Z}(\sqrt{-5})$ 使 $\alpha\beta = 1$ 当且仅当 $\exists \beta \in \mathbb{Z}(\sqrt{-5})$ 使 $N(\alpha\beta) = N(\alpha)N(\beta) = 1$ 当且仅当 $\alpha = \pm 1$.于是 α 不可逆时，$N(\alpha) > 1$.

考察 $\mathbb{Z}(\sqrt{-5})$ 中 9 的两种因子分解：

$$9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5}). \tag{4}$$

$3, 2 + \sqrt{-5}, 2 - \sqrt{-5}$ 这三个元素的复数模平方都是 9.令其中任意一个为 α.又设 $\alpha = \alpha_1\alpha_2$,$\alpha_1\alpha_2$ 皆不可逆，则 $N(\alpha_1), N(\alpha_2) > 1$ 及 $9 = N(\alpha) = N(\alpha_1)N(\alpha_2)$.由此只能 $N(\alpha_1) = N(\alpha_2) = 3$,但 $a^2 + 5b^2 = 3$ 是无解的.这样，上面三个元素皆是 $\mathbb{Z}(\sqrt{-5})$ 中不可约元.

又由于 $\mathbb{Z}(\sqrt{-5})$ 中只有 ± 1 为可逆元.故上面三个元素是互不相伴的.由此看出 $\mathbb{Z}(\sqrt{-5})$ 中元素 9 有两种不可约因子的分解，它们不符合定义 2 中表示法唯一性的条件(ii).也看出

$$3 \mid (2 + \sqrt{-5})(2 - \sqrt{-5}), (2 \pm \sqrt{-5}) \mid 3 \cdot 3,$$

但 $3 \nmid 2 \pm \sqrt{-5}$,$2 \pm \sqrt{-5} \nmid 3$.故它们都是不可约元，但不是素元.

$\mathbb{Z}(\sqrt{-5})$ 提供了不是唯一因式分解环的整环的例子.

下面介绍最大公因子的概念，我们会看到它的性质在因式分解唯一性中起重要作用.

定义 3 R 是整环，$c, a_1, \cdots, a_n \in R$.若 $c \mid a_i, i = 1, 2, \cdots, n$，则称 c 是 $a_1, \cdots, a_n$ 的**公因子**.若 d 是 $a_1, \cdots, a_n$ 的公因于，且 $a_1, \cdots, a_n$ 的任一个公因子都是 d 的因子，则称 d 是 $a_1, \cdots, a_n$ 的**最大公因子**.

设 d, d' 皆为 $a_1, \cdots, a_n$ 的最大公因子，则 $d \mid d'$ 及 $d' \mid d$，故 d 与 d' 是相伴的.

唯一因式分解环 R 中的两个元 a, b 一定有最大公因子.

首先若 a, b 中有零，比如 a 是零，则 b 是 a, b 的最大公因子.

若 a,b 中有可逆元，比如 a 是可逆元，则 a,b 的最大公因子是 a.

若 a,b 皆非零且非可逆的元.将它们分解成不可约元的乘积：

$$a = p_1\cdots,p_r,b = q_1\cdots q_s,$$

p_i,q_j 皆不可约.把 $p_1,\cdots,p_r,q_1\cdots q_s$，中互相相伴的元中各选一个代表，其全部代表为 $r_1,\cdots,r_t$，它们互不相伴，且 $p_1\cdots,p_r,q_1\cdots q_s$ 皆与其中之一相伴，则 a,b 可写为

$$a = ur_1^{l_1}\cdots r_t^{l_t},b = vr_1^{n_1}\cdots r_t^{n_t}, \tag{5}$$

其中 l_i,n_j 皆为非负整数，u,v 为可逆元.

命题 2 R 是唯一因式分解环.设 a,b 为非零且非可逆的元，有分解如(5)，则

(i) $a|b$ 当且仅当 $l_i \leqslant n_i,i = 1,\cdots,t$.

(ii) 令 $s_i = \min(l_i,n_i),i = 1,\cdots,t$，则 $d = r_1^{s_1}\cdots r_t^{s_t}$ 是 a,b 的最大公因子.

证明 (i) 当 $l_i \leqslant n_i$ 时，显然有 $a|b$.反之，设 $b = ac$.若 c 可逆，由因式分解的唯一性知 $l_i = n_i,i = 1,2,\cdots,t$.若 c 非可逆，又不为零，令 $c = p'_1p'_2\cdots p'_s$ 是不可约因子的分解.于是 $vr_1^{n_1}\cdots r_t^{n_t} = ur_1^{l_1}\cdots r_t^{l_t}p'_1\cdots p'_s$ 是不可约因式的两种分解.由分解唯一性，知 p'_i 与 $r_1\cdots r_t$ 之一相伴.于是 $c = wr_1^{m_1}\cdots r_t^{m_t}$，$w$ 为可逆元，m_i 为非负整数.就得到 $vr_1^{n_1}\cdots r_t^{n_t} = uwr_1^{l_1+m_1}\cdots r_t^{l_t+m_t}$.再由分解唯一性得 $n_i = l_i + m_i$，故 $l_i \leqslant n_i,i = 1,2,\cdots,t$.

(ii) 由假设及(i)有 $d|a$ 及 $d|b$.又设 d' 为 a,b 的一个公因子，若为非可逆元，如(i)中所证，令 $d' = w'r_1^{m'_1}\cdots r_t^{m'_t}$，则 $m'_i \leqslant \min(l_i,n_i)$.故 $d'|d$.若 d' 为可逆元，显然也有 $d'|d$.因此 d 是最大公因子.

若 a,b 的最大公因子为可逆元，则称 a,b 为**互素**.

命题 3 若整环 R 中任一对互素的元 a,b 都有 $u,v \in R$ 使 $ua + vb = 1$，则 R 的不可约元都是素元.

证明 首先证，若 $p|ab$ 且 p,b 互素，则 $p|a$.实际上有 $u,v \in R$，$up + vb = 1$.两端乘以 a，则有 $a = upa + vab$.而 p 整除右端的任一项，故 $p|a$.

再设 p 是不可约元，且 $p|ab$.令 p,b 的最大公因子为 d，则 $p = dc$.因 p 不可约，d 及 c 之一必为可逆元.若 c 可逆，则 p 与 d 相伴，$p|d$，又 $d|b$，故 $p|b$.若 d 可逆，则 p,b 互素，由上面所证得 $p|a$.

定理 4 设 R 为整环，且满足(i)R 的每个非零且非可逆的元都是一些不可约元的乘积.(ii)R 的任一对互素的元素 a,b 都有 $u,v \in R$，使 $ua + vb = 1$，则 R 是唯一因式分解环.

证明 由命题3,定义2及定理1.

在§2和§3中将介绍几类典型的唯一因式分解环.实际上这一章的一个重点就是学习这几类典型的环(欧氏环,主理想环,…)的性质.

习 题

1. 试说明整环中的零元,可逆元不能是不可约元的乘积.

2. R 是整环,则它的素元是不可约元.

3. R 是整环,则 $a \in R$ 是素元当且仅当主理想 $(a) = aR$ 是素理想(二章§7习题2).

4. 令整环

$$M = \{a + b\sqrt{3}\mathrm{i} \mid a, b \in \mathbb{Z}\}.$$

求出 M 的全部可逆元.证明它没有因式分解唯一性(举反例,有 M 中非零的不可逆元 a,它没有分解唯一性).

5. 证明在环 $\mathbb{Z}(\sqrt{-5})$ 中 $3(2+\sqrt{5}\mathrm{i})$ 和 9 没有最大公因子.

6. R 为唯一因式分解环.a, b 不同时为零,$a = a_1 d, b = b_1 d$,则 d 是 a, b 的最大公因子当且仅当 a_1, b_1 互素.

7. 设 M 是形为 $\frac{m}{2^k}$(m 任意整数,k 非负整数)的全部有理数的集合,则它是 Q 的子环.找出 M 的全部可逆元和不可约元.

8. R 是唯一因式分解环.d 是 R 中非零元,则 R 中只有有限个不同的素理想包含 (d)(提示:$(d) \subset (k) \Rightarrow k \mid d$).

9. R 是唯一因式分解环.$a, b \in R$ 是互素的,且 $a \mid bc$,则 $a \mid c$.

§2 欧氏环,主理想整环

我们在高等代数中已学过,整数环及域上多项式环 $F[x]$ 都有因式分解及唯一性定理.其证明步骤都是相仿的.首先它们都有除法算式.对 $\mathbb{Z}$ 中 a,及 $b, b \neq 0$,则有 $q, r \in \mathbb{Z}$,使

$$a = qb + r,$$

满足 $r = 0$ 或 $|r| < |b|$.

对 $F[x]$ 中 $f(x)$ 及 $g(x), g(x) \neq 0$,则有 $q(x), r(x) \in F[x]$,使

$$f(x) = q(x)g(x) + r(x),$$

满足 $r(x) = 0$ 或 $\partial(r(x)) < \partial(g(x))$.

$\mathbb{Z}$ 中 $|\ \ |$,当 $a \neq 0$ 时,满足

$$|ab| \geqslant |b|.$$

而 $F[x]$ 中 $\partial(\ \ )$，满足

$$\partial(f(x)g(x)) \geqslant \partial(f(x)).$$

用上面性质，就证明了 $\mathbb{Z}$ 及 $F[x]$ 中每个非零的非可逆元是有限个不可约元(在 $\mathbb{Z}$ 中是素数，在 $F[x]$ 中是不可约多项式) 的乘积.

$\mathbb{Z}$ 及 $F[x]$ 都有辗转相除法求最大公因子，且由此证得：$\mathbb{Z}$(或 $F[x]$) 中两元 a,b 若互素，则必有 $\mathbb{Z}$(或 $F[x]$) 中元 u,v，使 $ua + vb = 1$. 由此证明了有因式分解唯一性定理. §1 中关于一般整环的定理 1，命题 3 和定理 4 的证明实际是仿照 $\mathbb{Z}$ 及 $F[x]$ 中的证明. 将 $\mathbb{Z}$ 和 $F[x]$ 的特性进行抽象，就是

定义 1 设 R 是整环，有 $R \setminus \{0\} = R^*$ 到非负整数集 $\mathbb{Z}'$ 的一个函数 δ，满足

(i) $\forall a,b \in R^*, \delta(ab) \geqslant \delta(a)$,

(ii) $\forall a,b \in R, b \neq 0$，都有 $q,r \in R$，使得

$$a = qb + r, \text{且 } r = 0 \text{ 或 } \delta(r) < \delta(b).$$

我们称这样的环为**欧几里得环**，简称**欧氏环**.

与 $\mathbb{Z}, F[x]$ 一样在欧氏环中可用下面所谓辗转相除法(也称欧几里得算法) 来计算两个非零元素的最大公因子. 逐次用(ii) 中的步骤，我们可得

$$\begin{aligned}
a &= q_1 b + r_1, \delta(r_1) < \delta(b),\\
b &= q_2 r_1 + r_2, \delta(r_2) < \delta(r_1),\\
r_1 &= q_3 r_2 + r_3, \delta(r_3) < \delta(r_2),\\
&\cdots\cdots\\
r_{k-2} &= q_k r_{k-1} + r_k, \delta(r_k) < \delta(r_{k-1}).
\end{aligned}$$

若 r_k 不为零，则可继续做下去. 但 $\delta(b) > \delta(r_1) > \cdots > \delta(r_k)$ 是非负整数序列，不能无限减小. 必有某 $k, r_{k+1} = 0$. 于是 $r_{k-1} = q_{k+1} r_k$. 由此可推出 r_k 是 a, b 的最大公因数，并可推出(实际可递推地算出) 有 $u,v \in R$ 使 $ua + vb = r_k$. 当 a,b 互素时，$ua + vb = 1$.(这完全是重复 $\mathbb{Z}$ 或 $F[x]$ 时的情况).

这样，当 R 是欧氏环时，§1 定理 4 中的条件(ii) 已具备.

下面再说明欧氏环 R 的非零非可逆元 a 能表成有限个不可约元的乘积. 若 a 不可约，则 a 是一个不可约元的乘积. 若 a 不是不可约，则 $a = bc$，其中 b,c 皆非零非可逆. 由欧氏环的定义条件(i)，$\delta(b) \leqslant \delta(bc) = \delta(a)$. 若 $\delta(b) = \delta(a)$. 由定义条件(ii)，有 $q,r \in R$ 使 $b = qa + r$，且 $r = 0$ 或 $\delta(r) < \delta(a)$. 若 $r = 0$，则 $a = bc$ 及 $b = aq$ 推出 $a = aqc$. 于是 $qc = 1$ 与 c 非可逆矛盾. 故 $\delta(r) < \delta(a)$. 又 c 非可逆，有 $1 - qc \neq 0$.

$$\delta(a) = \delta(b) \leqslant \delta(b(1 - qc)) = \delta(b - qa) = \delta(r) < \delta(a).$$

矛盾.故 $\delta(b) < \delta(a)$.

现设 $a = a_1a_2\cdots a_r$，a_i 皆非可逆.于是每个 i，$a_i(a_{i+1}\cdots a_r)$ 是两个非可逆元之积.由上面所证

$$\delta(a) = \delta(a_1a_3\cdots a_r) > \delta(a_2a_3\cdots a_r) > \delta(a_3\cdots a_r) > \cdots > \delta(a_r) \geqslant 0$$

是个严格减少的非负整数序列，故序列的长度 $r \leqslant \delta(a) + 1$.但 $\delta(a)$ 是个定数，这个序列不能任意加长，故 a 表成非可逆元的乘积中有最长的一个.设仍记为 $a = a_1a_2\cdots a_r$，a_i 非可逆.若 a_i 中有可约元，则这个乘积仍可加长，就与最长的要求矛盾.故 a_i 都是不可约元，即 a 表成了有限个不可约元的乘积.

这样，欧氏环对于定理 3 中的两个条件都具备.

定理 1 欧氏环是唯一因式分解环.

证明 上面的论述已是证明.其实这些也完全是模仿 $\mathbb{Z}$ 和 $F[x]$ 情形的证明.

除了 $\mathbb{Z}$ 和 $F[x]$ 是欧氏环外，我们提供下面的新例子.

例 1 **高斯整数环** $\mathbb{Z}[\mathrm{i}] = \mathbb{Z}[\sqrt{-1}]$，其中

$$\mathbb{Z}[\mathrm{i}] = \{a + b\mathrm{i} \mid a, b \in \mathbb{Z}\}.$$

它是复数域的子集，显然是子环.取 δ 为复数 $a + b\mathrm{i}$ 的模的平方，$\delta(a + b\mathrm{i}) = |a + b\mathrm{i}|^2 = a^2 + b^2$.下面证明 δ 满足定义 1 中各项要求，首先

$$\delta: \mathbb{Z}[\mathrm{i}]^* \longrightarrow \mathbb{Z}^+ \text{（非负整数集）}.$$

其次，任意 $\alpha \in \mathbb{Z}[\mathrm{i}]^*$，$\delta(\alpha) \geqslant 1$.由模的性质得

(i) $\delta(\alpha\beta) = \delta(\alpha)\delta(\beta) \geqslant \delta(\alpha)$，$\forall\, \alpha, \beta \in \mathbb{Z}[\mathrm{i}]$.

对 $\alpha \in \mathbb{Z}[\mathrm{i}]$，$\beta \in \mathbb{Z}[\mathrm{i}]^*$，写 $\alpha\beta^{-1} = a + b\mathrm{i}$，这里 $a, b \in \mathbb{Q}$.选最接近 a，b 的整数 k 和 l，使 $a = k + \nu$，$b = l + \mu$，这里 $|\mu| \leqslant \frac{1}{2}$，$|\nu| \leqslant \frac{1}{2}$，则

$$\alpha = \beta[(k + \nu) + \mathrm{i}(l + \mu)] = \beta(k + \mathrm{i}l) + \beta(\nu + \mathrm{i}\mu).$$

令 $q = k + \mathrm{i}l \in \mathbb{Z}[\mathrm{i}]$ 及 $\gamma = \alpha - \beta q = \beta(\nu + \mathrm{i}\mu) \in \mathbb{Z}[\mathrm{i}]$，则 $\alpha = q\beta + \gamma$ 且

$$\delta(\gamma) = |\gamma|^2 = |\beta|^2|\nu + \mathrm{i}\mu|^2 = |\beta|^2(\nu^2 + \mu^2) \leqslant |\beta|^2\left(\frac{1}{4} + \frac{1}{4}\right)$$

$$= \frac{1}{2}\delta(\beta) < \delta(\beta).$$

这样又验证了 $\mathbb{Z}[\mathrm{i}]$ 对欧氏环的条件(ii)也成立.故 $\mathbb{Z}[\mathrm{i}]$ 是欧氏环.

第二章 §4 例 10 到例 13 中看到 $\mathbb{Z}$ 及 $F[x]$ 的每个理想都是主理想.这个性质对一般欧氏环同样成立.

命题 2 欧氏环 R 的任何理想都是主理想.

证明 设 J 是 R 的理想.若 J 只由零元组成，$J = 0 \cdot R$ 是主理想.若 J 中有非零元 x.选 J 中 $\delta(x)$ 最小的元 x.任意 $a \in J$，令 $a = qx + r$.

若 $r \neq 0$,则 $\delta(r) < \delta(x)$. 且由 a 及 $qx \in J$,得 $r = a - qx \in J$. 与 $\delta(x)$ 最小矛盾. 因此 $r = 0, a = qx$. 故 $J \subset xR$. 又 $x \in J, xR \subset J$. 所以 $J = xR$ 是主理想环.

定义 2 设 R 是整环. 若它的每个理想都是主理想,则称 R 为**主理想整环**,简称**主理想环**.

命题 2 说明欧氏环是主理想环. 文献中(见习题 8)举出过例子,有些环是主理想环但非欧氏环. 例如 $R_1 = \{\frac{1}{2}a + \frac{1}{2}b\sqrt{19}\mathrm{i} \mid a, b \in \mathbb{Z}\}$ 是主理想环但不是欧氏环.

对于主理想环 R 中的两个元 a, b,关于它们的最大公因子有下列命题 3. 在欧氏环中同样的命题是靠辗转相除法得到的.

命题 3 对主理想环 R 中的两个元 a, b 必有 R 中 u, v,使 $ua + vb$ 是它们的最大公因子.

证明 作 $aR + bR$,易知它是 R 的理想,故必为主理想. 于是有 $d \in aR + bR$,使 $aR + bR = dR$. $a, b \in dR$,因而是 d 的倍数,故 d 是 a, b 的公因子. 又 $d \in aR + bR$,故有 u, v,使 $d = ua + vb$. 显然,a 和 b 的公因子是 d 的因子. 这就证明了 d 是 a, b 的最大公因子.

命题 3 是利用主理想的特性来证明的. 比欧氏环中用辗转相除要简单. 但是这里只是证明了 u, v 的存在,而辗除相除法却可算出 u, v.

命题 3 证明了 §1 中定理 4 的条件(ii)对主理想环成立. 下面来证明条件(i)也成立. 因而主理想环也是唯一因式分解环.

定理 4 主理想环是唯一因式分解环.

证明 现在只需证明 §1 中定理 4 的条件(i)对主理想环成立,即证明主理想环 R 中任一非零的非可逆元都是有限个不可约元的乘积.

设 $a \in R$ 是非零的非可逆元. 且设它不是有限个不可约元的乘积. 首先它不是不可约的,故有 $a = d_1 d_1', d_1, d_1'$ 皆非可逆元. 于是 $d_1, d_1' \mid a$,但 $a \nmid d_1, d_1'$. 因 a 不是有限个不可约元的乘积,d_1, d_1' 中至少有一个不是,不妨设 d_1 不是有限个不可约元的乘积. 于是 $d_1 = d_2 d_2', d_2, d_2'$ 皆非可逆元. d_2, d_2' 中至少有一个不是有限个不可约元的乘积. 不妨设为 d_2,同样 $d_2 \mid d_1$,但 $d_1 \nmid d_2$. 如此可无限地作下去,得到一个序列:

$a = d_0, d_1, d_2, \cdots$. 对每个 i,有 $d_i \mid d_{i-1}$ 但 $d_{i-1} \nmid d_i$. 由此得理想的包含序列

$$d_0 R \subset d_1 R \subset d_2 R \subset \cdots.$$

作所有这些理想的并集

$$I = \bigcup_{i=0}^{\infty} d_i R.$$

易知 I 也是 R 的理想. R 是主理想环,故有 $d \in I$,使 $dR = I$. 由并集的定义,有 i, $d \in d_i R$. 这样 $d_i | d$. 又 $d_i \in I = dR$,得 $d | d_i$. 故 d_i 与 d 相伴,这就有 $d_i R = dR$.

对 $d_{i+1} R$,即有 $d_i R \subset d_{i+1} R$. 又有 $d_{i+1} R \subset I = dR = d_i R$. 故 $d_i R \subset d_{i+1} R \subset d_i R$,则它们是相等的,即 $d_i R = d_{i+1} R$. 而 $d_{i+1} \in d_i R$ 表明 $d_i | d_{i+1}$,与 $d_i \nmid d_{i+1}$ 矛盾. 故 a 必须能表成有限个不可约元的乘积.

按常理,有了定理4,定理1可作为推论不必去重复证明. 我们这样作是为了能看出欧氏环、主理想环这些概念以及因式分解唯一性定理的证明的发展过程.

习　题

1. 主理想环的商环是主理想环.

2. R 是主理想环, a 为 R 中不可约元,则

(i) (a) 为极大理想; (ii) a 为素元;

(iii) 每个非0素理想(见二章 §7 习题2)是极大理想;

(iv) $\dfrac{R}{(a)}$ 是域.

3. 证明 $M = \{a + b\sqrt{2}i \mid a, b \in \mathbb{Z}\}$ 是欧氏环(仿例1).

4. p 是素数. 令 $R = \left\{ \dfrac{a}{b} \,\middle|\, a, b \in \mathbb{Z}, (b, p) = 1 \right\}$.

(i) 证明 R 是整环;

(ii) 求出 R 的所有可逆元;

(iii) 证明 R 的所有非可逆元组成 R 的唯一极大理想;

(iv) 上述极大理想是主理想;

(v) 求出 R 的全部理想.

5. 找出高斯整数环 $\mathbb{Z}[\mathrm{i}] = \{a + b\mathrm{i} \mid a, b \in \mathbb{Z}\}$ 的全部可逆元.

6. 高斯整数环的元素 a 满足 $\delta(a) =$ 素数,则 a 为不可约元.

7. R 是欧氏环,求证

(i) 若 $\varepsilon \in R^* = R \setminus \{0\}$,则 ε 是 R 中可逆元当且仅当 $\forall a \in R^*$ 有 $\delta(\varepsilon) \leqslant \delta(a)$.

(ii) 设 $a \in R^*$, a 不可逆. 若对所有不可逆元 $b \in R^*$ 都有 $\delta(a) \leqslant \delta(b)$,则 a 是 R 中不可约元.

8. $R=\left\{\frac{1}{2}a+\frac{1}{2}b\sqrt{19}\mathrm{i}\,\middle|\,a,b\in\mathbb{Z}\right\}$，则 R 是主理想环但不是欧氏环（参看 Motzkin, The Euclidean algorithm, Bull. Amer. Math. Soc. 55. 1142 – 1146(1949)）.

§3 交换环上多项式环

这一节我们要证明：若 R 是唯一因式分解环，则 R 上多项式环 $R[x]$ 也是唯一因式分解环.

但是有个事实到现在还未论证过：对一般交换环，甚至对一般域有没有多项式环？我们从数域 P 上多项式的定义谈起. P 上的一个多项式是一个形式的表达式

$$a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0, \tag{1}$$

这里 $a_0,a_1,\cdots,a_n$ 是 P 中元，x 是一个文字或叫不定元. 多项式(1)是零当且仅当所有 $a_i=0, i=0,1,2,\cdots,n$. 在多项式规定的加法和对 P 的元素作数量乘积之下，P 上全体多项式的集合 $P[x]$ 已经是 P 上线性空间. 上述关于零多项式的规定表明对任意 n，$\{1,x,\cdots,x^n\}$ 在 P 上是线性无关的. 再加上多项式的乘法运算，$P[x]$ 构成多项式环，它是域 P 上的扩环. 文字 x 并没指明有什么具体意义，有时也叫不定元. 只要有 P 的扩环 R，R 中有一个元 x，对任何 n，$\{1,x,\cdots,x^n\}$ 在 P 上都是线性无关的，就可作成多项式环 $P[x]$. 对数域 P 来讲这样的扩环和这样的元是存在的. 举两个例子.

例 1 数域 P 上的全部函数（复数值的）在函数的加法和乘法下成 P 上函数环. P 上的全部常数函数

$$\{f(x)=a\mid\forall a\in P\}$$

组成一个子域，就与数域 P 同构. 干脆将它与 P 等同，则 P 上函数环是 P 的扩环. P 的自变量函数 x 就满足下述条件：对任意 n，

$$a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0=0, a_0,a_1,\cdots,a_n\in P, \tag{*}$$

当且仅当 $a_0=a_1=\cdots=a_n=0$. 这时作成的 $P[x]$ 就是符合需要的多项式环.

例 2 实数域 $\mathbb{R}$ 是有理数域 $\mathbb{Q}$ 的扩环. 超越数 e, π 等都满足：对任意 n，当 $x=$ e 或 π 时，

$$a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0=0, a_0,a_1,\cdots,a_n\in\mathbb{Q},$$

当且仅当 $a_0=a_1=\cdots=a_n=0$.

用 x 记 e 或 π. 则作成的 $P[x]$ 也是符合需要的多项式环.

从例子看出 $\mathbb{Q}[x]$ 中的 x 叫作文字或不定元的原因是对于不同的具体情

况，x 有不同的意义.只要 x 满足(*)条件，就能作成多项式环 $P[x]$，且它们的理论是一样的.以上说明数域 P 是有具体的多项式环存在的，其关键是 P 上不定元存在.

定义1 R 是交换环，若有 R 的交换扩环 R_0 及 R_0 中的一个元素 x，使得对任何 n，有

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0, a_0, a_1, \cdots, a_n \in R,$$

当且仅当 $a_0 = a_1 = \cdots = a_n = 0$，则称 x 是 R 上的一个文字或**不定元**.

但是对一般交换环，特别像有限域就不能简单地模仿例1、例2的方法来找不定元.实际上这也行不通.于是人们构思了另外的方法.

命题1 R 是交换环，则有 R 上的文字或未定元存在.

证明 令

$$R_0 = \{(a_0, a_1, \cdots, a_n, \cdots) \mid a_0, a_1, \cdots \in R, \text{且只有限个 } a_i \neq 0\}.$$

在 R_0 上引进加法和乘法为：

$$(a_0, a_1, \cdots, a_n, \cdots) + (b_0, b_1, \cdots, b_n, \cdots) = (a_0 + b_0, a_1 + b_1, \cdots),$$

$$(a_0, a_1, \cdots, a_n, \cdots)(b_0, b_1, \cdots, b_n, \cdots) = (c_0, c_1, c_2, \cdots, c_n, \cdots),$$

这里

$$c_k = \sum_{i+j=k} a_i b_j, k = 0, 1, 2, \cdots.$$

易知这样的加法和乘法是 R_0 上的代数运算.且易知 R_0 对加法成交换群，其零元素为 $(0,0,0,\cdots)$，记为 0.

乘法显然适合交换律.现在来验算乘法结合律.令

$$[(a_0, a_1, a_2, \cdots)(b_0, b_1, b_2, \cdots)](c_0, c_1, c_2, \cdots) = (d_0, d_1, d_2, \cdots),$$

$$(a_0, a_1, a_2, \cdots)[(b_0, b_1, b_2, \cdots)(c_0, c_1, c_2, \cdots)] = (e_0, e_1, e_2, \cdots),$$

易计算

$$d_n = \sum_{m+k=n} \Big(\sum_{i+j=m} a_i b_j \Big) c_k = \sum_{i+j+k=n} a_i b_j c_k,$$

$$e_n = \sum_{i+m=n} a_i \Big(\sum_{j+k=m} b_j c_k \Big) = \sum_{i+j+k=n} a_i b_j c_k,$$

故两者相等，乘法有结合律.又令

$$(a_0, a_1, a_2, \cdots)[(b_0, b_1, b_2, \cdots) + (c_0, c_1, c_2, \cdots)] = (d_0, d_1, d_2, \cdots)$$

$$(a_0, a_1, a_2, \cdots)(b_0, b_1, b_2, \cdots) + (a_0, a_1, a_2, \cdots)(c_0, c_1, c_2, \cdots)$$

$$= (e_0, e_1, e_2, \cdots).$$

则

$$d_k = \sum_{i+j=k} a_i (b_j + c_j) = \sum_{i+j=k} a_i b_j + \sum_{i+j=k} a_i c_j = e_k.$$

故乘法对加法有分配律.又 R_0 有乘法单位元

$$1 = (1,0,0,\cdots).$$

故 R_0 是交换环.它的子集

$$R' = \{(a,0,\cdots,0,\cdots) \mid a \in R\}$$

构成 R_0 的子环,并且与 R 同构.于脆将 R' 等同于 R,把 R' 的元$(a,0,0,\cdots)$就记成 a,则 R_0 就是 R 的扩环.再令 R_0 的元

$$x = (0,1,0,0,\cdots),$$

则

$$x^2 = (0,0,1,0,0,\cdots), x^3 = (0,0,0,1,0,0,\cdots),\cdots,$$
$$x^k = (\underbrace{0,0,\cdots,0}_{k\text{个}},1,0,0,\cdots)\cdots.$$

易验证:对任何 n,若

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0, a_0, a_1, a_2, \cdots, a_n \in R.$$

其左端正好等于

$$(a_0, a_1, a_2, \cdots, a_n, 0, 0, \cdots, 0, \cdots),$$

右端为

$$(0,0,0,\cdots,0,\cdots),$$

故 $a_0 = a_1 = \cdots = a_n = 0$.这就证明了 x 是 R 的不定元.

R_0 中任一元$(a_0, a_1, \cdots, a_k, \cdots)$,只有有限个 $a_i \neq 0$.设足标最大的非零的 a_i 的 i 为 n.则它是$(a_0, a_1, \cdots, a_n, 0, 0, \cdots)$,它就等于 $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$.

定义 2 R 为交换环.上面作出的交换环 R_0 正是

$$R[x] = \left\{ a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \;\middle|\; \begin{array}{l} \forall\, n \text{ 为非负整数} \\ \forall\, a_n, a_{n-1}, \cdots, a_0 \in R \end{array} \right\},$$

称为 R 上**多项式环**.

显然在 $R[x]$ 中的两个多项式

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0$$

当且仅当 $a_i = b_i, i = 0,1,2,\cdots,n$.

多项式的加法和乘法是

$$(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0) + (b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0)$$
$$= (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_0 + b_0), \tag{1}$$

及

$$(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0)(b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0)$$
$$= c_{m+n}x^{m+n} + c_{m+n-1}x^{m+n-1} + \cdots + c_0. \tag{2}$$

其中

$$c_{m+n}=a_nb_m,c_{m+n-1}=a_nb_{m-1}+a_{n-1}b_m,\cdots,$$
$$c_k=\sum_{i+j=k}a_ib_j,\cdots,c_1=a_1b_0+a_0b_1,c_0=a_0b_0. \tag{3}$$

称多项式

$$a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0,\text{其中 } a_n\neq 0,$$

的**次数**为 n. 记多项式 $f(x)\neq 0$ 的次数为 $\partial(f(x))$. 零多项式没有次数. 次数有性质(当下面式子中出现的多项式皆不为零时):

(i) $\partial(f(x)+g(x))\leqslant\min(\partial(f(x)),\partial(g(x)))$.

(ii) $\partial(f(x)g(x))\leqslant\partial(f(x))+\partial(g(x))$.

命题 2 设 R 是整环,则 $R[x]$ 也是整环,且

$$\partial(f(x)g(x))=\partial(f(x))+\partial(g(x)).$$

证明 设(2)中左端两个多项式,记为 $f(x)$ 及 $g(x)$,皆不为零,且 $a_n\neq 0$ 及 $b_m\neq 0$. 于是 $a_nb_m\neq 0$(R 中无零因子). 由(3)知,(2)的右端不为零,即左端乘积不为零. 故 $R[x]$ 是整环.

由 $a_n\neq 0$ 及 $b_m\neq 0$,知 $\partial(f(x))=n,\partial(g(x))=m$. 而由 $c_{m+n}=a_nb_m\neq 0$,知 $\partial(f(x)g(x))=m+n$. 这证明了命题.

设 R 是交换环,R_1 是 R 的交换扩环. 对任一元 $u\in R_1$ 及 $R[x]$ 中的多项式 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$,我们令 $f(u)=a_nu^n+a_{n-1}u^{n-1}+\cdots+a_0$. 这即是以前学过的将值 u 代入 $f(x)$. 这个代入有性质:对 $f(x),g(x)\in R[x]$,令 $f(x)+g(x)=h(x),f(x)g(x)=I(x)$,则

$$f(u)+g(u)=h(u),$$
$$f(u)g(u)=I(u).$$

这是容易验证的.

进一步地,令

$$R(u)=\{f(u)\mid f(x)\in R[x]\},$$

则 $R(u)$ 是 R_1 的子环,而且下列映射

$$R[x]\longrightarrow R(u)$$
$$f(x)\longrightarrow f(u)$$

是环同态.

有了一元多项式就可以作出多元多项式. 可采取逐次作出. 设 R 是交换环. 我们已经会作 $R[x_1],x_1$ 是 R 上不定元. $R[x_1]$ 是交换环,有 $R[x_1]$ 上不定元 x_2,作出 $R[x_1][x_2],\cdots$,对任意 k 可作出 $R[x_1][x_2]\cdots[x_k]$.

命题 3 $R[x_1][x_2]\cdots[x_k]$ 中元素具有形式

$$\sum_{i_1,\cdots,i_k}a_{i_1\cdots i_k}x_1^{i_1}\cdots x_k^{i_k},\quad a_{i_1\cdots i_k}\in R.$$

且 $\sum_{i_1\cdots i_k} a_{i_1\cdots i_k} x_1^{i_1}\cdots x_k^{i_k} = 0$ 当且仅当所有 $a_{i_1\cdots i_k} = 0$.

证明 对 k 作归纳法. $k = 1$ 时，$R[x_1]$ 中元是 $\sum_{i_1} a_{i_1} x_1^{i_1}$. 命题正确. 设 $k - 1$ 时命题已对. 即 $R[x_1]\cdots[x_{k-1}]$ 中元素具有形式 $\sum_{i_1\cdots i_{k-1}} a_{i_1\cdots i_{k-1}} x_1^{i_1}\cdots x_{k-1}^{i_{k-1}}$. 当 k 时，$R[x_1]\cdots[x_{k-1}][x_k]$ 中元素有形式 $\sum_{i_k} b_{i_k} x_k^{i_k}$，其中 $b_{i_k} \in R[x_1]\cdots[x_{k-1}]$. $k - 1$ 时归纳假设命题正确，故 b_{i_k} 为 $\sum_{i_1\cdots i_{k-1}} d_{i_1\cdots i_{k-1}} x_1^{i_1}\cdots x_{k-1}^{i_{k-1}}$ 形状. 但这表达式与 i_k 有关，故应设 $d_{i_1\cdots i_{k-1}}$ 为 $a_{i_1\cdots i_{k-1}i_k}$. 于是

$$b_{i_k} = \sum_{i_1\cdots i_{k-1}} a_{i_1\cdots i_{k-1}i_k} x_1^{i_1}\cdots x_{k-1}^{i_{k-1}}.$$

就有

$$\sum_{i_k} b_{i_k} x_k^{i_k} = \sum_{i_k}\Big(\sum_{i_1\cdots i_{k-1}} a_{i_1\cdots i_k} x_1^{i_1}\cdots x_{k-1}^{i_{k-1}}\Big) x_k^{i_k} = \sum_{i_1 i_2\cdots i_k} a_{i_1\cdots i_k} x_1^{i_1}\cdots x_{k-1}^{i_{k-1}} x_k^{i_k}.$$

命题的第一部分得证. 证第二部分，仍对 k 作归纳法. 设 $k - 1$ 时已对，现设 $\sum_{i_1\cdots i_k} a_{i_1\cdots i_k} x_1^{i_1}\cdots x_k^{i_k} = 0$，则

$$\sum_{i_1\cdots i_k} a_{i_1\cdots i_k} x_1^{i_1}\cdots x_k^{i_k} = \sum_{i_k}\Big(\sum_{i_1\cdots i_{k-1}} a_{i_1\cdots i_k} x_1^{i_1}\cdots x_{k-1}^{i_{k-1}}\Big) x_k^{i_k} = 0.$$

由于 x_k 是 $R[x_1]\cdots[x_{k-1}]$ 上的不定元. 故 $\forall\, i_k$ 有

$$\sum_{i_1\cdots i_k} a_{i_1\cdots i_k} x_1^{i_1}\cdots x_{k-1}^{i_{k-1}} = 0.$$

又归纳假设 $k - 1$ 时已对，故 $\forall\, i_1\cdots i_{k-1} i_k$，$a_{i_1 i_2\cdots i_k} = 0$. 命题证毕.

将命题 3 的第二部分的性质抽象出来，我们给出

定义 3 R 是交换环. R_0 是 R 的交换扩环，$x_1, x_2, \cdots, x_k \in R_0$ 满足：对任意的表达式

$$\sum_{i_1 i_2\cdots i_k} a_{i_1\cdots i_k} x_1^{i_1}\cdots x_k^{i_k} = 0, a_{i_1\cdots i_k} \in R,$$

都有 $\forall_{i_1\cdots i_k}$，$a_{i_1\cdots i_k} = 0$，则称 $x_1, x_2, \cdots, x_k$ 为 R 上无关的不定元.

记

$$R[x_1, x_2, \cdots, x_k] = \Big\{\sum_{i_1\cdots i_k} a_{i_1\cdots i_k} x_1^{i_1}\cdots x_k^{i_k} \,\Big|\, i_1, \cdots, i_k \text{ 可取任意非负整数}, a_{i_1\cdots i_k} \in R\Big\},$$

则它构成 R_0 的子环，称为 R 上不定元 $x_1, \cdots, x_k$ 的多项式环.

从集合 $R[x_1, x_2, \cdots, x_k]$ 的构成易见，$R[x_1, \cdots, x_k]$ 中 $x_1, \cdots, x_k$ 换一个次序仍表示同一集合. 此外，易见 $R[x_1, x_2, \cdots, x_k] = R[x_1]\cdots[x_k]$. 由命题

2得

命题4 设 R 是整环，则多项式环 $R[x_1,\cdots,x_k]$ 是整环.

证明 $R[x_1,\cdots,x_k]=R[x_1][x_2]\cdots[x_k]$. 由命题2，从 R 是整环，知 $R[x_1]$ 为整环，于是 $R[x_1][x_2]$ 是整环，然后 $R[x_1][x_2][x_3],\cdots$，$R[x_1][x_2]\cdots[x_k]$ 都是整环.

在这一节的最后，再说一下这一节内容的重要性. 我们教材中有些内容是以多项式环的存在作前提的. 例如第二章 §6 关于构造添加任意域 F 上某多项式的一个根的扩域. 其方法是作 $F[x]$，模它的一个主理想作剩余类域. 又第三章 §1 中造 p^n 个元素数的有限域，$n>1$ 时也是利用 $\mathbb{Z}_p[x]$ 模某理想的剩余类域. 若 $F[x]$，$\mathbb{Z}_p[x]$ 的存在性得不到证明，这些结论就没有根据了.

习 题

1. R 是整环，则 $R[x]$ 中可逆元一定是 R 中可逆元.

2. 设 R 是有限域. 令

$$R_1=\{R\text{ 到 }R\text{ 的全部映射的集合}\}.$$

R_1 上有加法和乘法：$f_1,f_2\in R_1$，令 $\forall a\in R$，

$$(f_1+f_2)(a)=f_1(a)+f_2(a),$$
$$(f_1\cdot f_2)(a)=f_1(a)f_2(a).$$

易知 R_1 在这两个运算下成环. 其单位元 e 为：$\forall a\in R, e(a)=1$.

对 $\forall r\in R$，作 R_1 中映射 $f_{(r)}$：$f_{(r)}(a)=ra$，$\forall a\in R$. 它们组成 R_1 的子环，并与 R 同构. 干脆记成 R，于是 R_1 是 R 的扩环，并将 $f_{(r)}$ 记成 r.

令 u 是 R 的恒等映射：$u(a)=a$，$\forall a\in R$. 证明 u 不是 R 上不定元.

3. $\mathbb{Z}$ 是整数环，则 $a+bi, a,b\in\mathbb{Z}$，不是 $\mathbb{Z}$ 上不定元.

§4 唯一因式分解环上的多项式环

这一节主要是证明，若 R 是唯一因式分解环，则 $R[x]$ 也是唯一因式分解环.

在高等代数中证明过 $\mathbb{Z}[x]$ 中的正次数多项式 $f(x)$，若在 $\mathbb{Z}[x]$ 中不可约，则它在 $\mathbb{Q}[x]$ 中不可约. 这个结果可以推广成：设 R 是唯一因式分解环，$f(x)\in R[x]$，$\partial(f(x))>0$. 若 $f(x)$ 在 $R[x]$ 中不可约，则在 $Q(R)[x]$ 中也不可约，其中 $Q(R)$ 是 R 的分式域. 它的证明是模仿 $\mathbb{Z}[x]$，$\mathbb{Q}[x]$ 情况的证明，利用了高斯的本原多项式的概念和性质. 用这个推广的结果才能推出本节

开头叙述的主要结果.

本节中始终设 R 是唯一因式分解环,$f(x) \in R[x]$.若 $f(x)$ 的各系数的最大公因子是 1(也可以是可逆元),则称 $f(x)$ 为 R 上**本原多项式***.

引理 1 $R[x]$ 中任一非零多项式 $f(x)$ 恒可写成一个常数 d 和一个本原多项式 $f_1(x)$ 的乘积,而且 d 和 $f_1(x)$ 在相伴的意义下由 $f(x)$ 唯一决定.

证明 设 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$. 取 $a_0, a_1, \cdots, a_n$ 的最大公因子是 d, $a_i = a_i' d$, $f_1(x) = a_n' x^n + a_{n-1}' x^{n-1} + \cdots + a_0'$. 于是 $f(x) = df_1(x)$, $f_1(x)$ 为本原多项式.设 $f(x) = ef_2(x)$, $f_2(x)$ 也为本原多项式,$e \in R$.令 $f_2(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0$.我们要证 e 也是 $f(x)$ 的各系数的最大公因子.首先 e 显然是各系数的公因子.而 d 是各系数的最大公因子,故有 $e \mid d$.我们若能证 $d \mid e$,于是 e 与 d 相伴,有可逆元 u 使 $e = du$.因此 $f(x) = ef_2(x) = d(uf_2(x)) = df_1(x)$.故有 $uf_2(x) = f_1(x)$, $f_1(x)$ 与 $f_2(x)$ 是相伴的.

现来证明 $d \mid e$.我们已有 $e \mid d$.令 $d = ef$.若 f 是可逆元,则 $e = df^{-1}$,即有 $d \mid e$.

若 f 为非可逆元,取 f 的不可约因子 p,则 $pe \mid d$.因 d 是 $f(x)$ 的各系数的公因子,pe 也是.$f(x) = ef_2(x)$ 的各系数是 $eb_n, eb_{n-1}, \cdots, eb_0$.故 $pe \mid eb_i$, $i = 0, 1, \cdots, n$,从而 $p \mid b_i$, $i = 0, 1, \cdots, n$. p 是非可逆元,与 $f_2(x)$ 的本原性矛盾.即 f 必为可逆元,引理得证.

引理 2 (高斯引理) $f(x), g(x) \in R[x]$ 皆为本原多项式,则 $f(x)g(x)$ 也是本原多项式.

证明 反设 $f(x)g(x)$ 非本原,必有一个非可逆元 f 是它的各系数的公因子.取 f 的一个不可约的因子 p,则 p 整除 $f(x)g(x)$ 的各个系数.设

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0,$$

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0, a_i, b_i \in R.$$

现作 $\overline{R} = \dfrac{R}{(p)}$. $a \in R$ 在 $\overline{R}$ 中的象为 $\overline{a} = a + (p)$.易知映射

$$R[x] \longrightarrow \overline{R}[x]$$

$$h(x) = \sum_{i=1}^{k} l_i x^i \longmapsto \overline{h(x)} = \sum_{i=1}^{k} \overline{l_i} x^i$$

是环同态.故有

$$\overline{f(x)g(x)} = \overline{f(x)}\,\overline{g(x)}.$$

由于 p 整除 $f(x)g(x)$ 的各系数,故 $\overline{f(x)g(x)} = \overline{0}$.但 $f(x), g(x)$ 皆本原,

---

* 第三章 §2 定义 2 和这里的本原多项式是不同的概念,但在其他书和文献中都用了同一名称.我们也只好这样处理.好在这两个概念只分别在第三章,第四章中使用.用了同一名词也不会混淆.

即有$\overline{f(x)}\neq 0,\overline{g(x)}\neq\bar{0}$.若我们能证明$R$是整环,由§3命题2,$\bar{R}[x]$是整环.于是$\overline{f(x)}\,\overline{g(x)}\neq 0$,矛盾.就证明了$f(x)g(x)$是本原的.

现反设R非整环,则有$\bar{a}\neq\bar{0},\bar{b}\neq\bar{0}$,使$\overline{ab}=a\cdot b\quad\bar{0}$.由$\bar{R}$的定义推出$p\nmid a,p\nmid b$及$p\mid ab$.但$p$为不可约元必为素元(见§1定理1及定义2),由$p\mid ab$,必能使$p$至少整除$a,b$中的一个,矛盾.

引理得证.

定理1 若$R[x]$中的一个正次数多项式$f(x)$在$R[x]$中不能分解成两个正次数的多项式的乘积,则$f(x)$在$Q(R)[x]$中不可约,其中$Q(R)$是R的分式域.

证明 设$f(x)=f_1(x)f_2(x),f_i(x)\in Q(R)[x]$,且都是正次数.用$f_i(x)$的各系数分母的最小公倍数$b_i$乘以$f_i(x)$,则$b_if_i(x)\in R[x]$.它可写成$b_if_i(x)=a_ig_i(x),a_i\in R,g_i(x)$是本原的.又$f(x)\in R[x]$,可写成$f(x)=cg(x),c\in R,g(x)$是本原的.于是

$$b_1b_2cg(x)=(b_1f_1(x))(b_2f_2(x))=a_1a_2g_1(x)g_2(x).$$

因$g_1(x)g_2(x)$本原(高斯引理),$g(x)$本原及$b_1b_2c,a_1a_2\in R$,用引理1,b_1b_2c与a_1a_2在R中相伴,则$(b_1b_2)^{-1}a_1a_2$与c在R中相伴.于是$(b_1b_2)^{-1}a_1a_2\in R$.得到

$$f(x)=cg(x)=\left(\frac{a_1a_2}{b_1b_2}\right)g_1(x)g_2(x),$$

$g_1(x),g_2(x)\in R[x]$,它们皆正次数.与$f(x)$在$R[x]$中不能分解相矛盾.故$f(x)$在$Q(R)[x]$中也不可约.

定理2 R是唯一因式分解环,则$R[x]$也是唯一因式分解环.

证明 对于$f(x)\in R[x]$,先证它是$R[x]$中有限个不可约元的乘积.令$f(x)=df_0(x),d\in R,f_0(x)$是$R[x]$中本原多项式.若$d$在$R[x]$中可分解,$d=g_1(x)g_2(x)$.由于$R[x]$是整环(§3命题2),

$$\partial(d)\quad\partial(g_1(x)g_2(x))=\partial(g_1(x))+\partial(g_2(x)).$$

但d的次数为零,故$\partial(g_1(x))=\partial(g_2(x))=0$.$g_1(x),g_2(x)$皆是常数,属于$R$.于是$d$在$R[x]$的不可约因子就是$d$在$R$中的不可约因子.因$R$是唯一因式分解环,故$d$是$R$中,也是$R[x]$中有限个不可约元的乘积,$d=p_1\cdots p_r$.又设$f_0(x)=f_1(x)f_2(x),f_i(x)\in R[x]$.$R[x]$是整环,故$\partial(f_0(x))=\partial(f_1(x))+\partial(f_2(x))$.由$f_0(x)$的本原性,用归纳法可证$f_0(x)$是有限个$R[x]$中正次数不可约元乘积,$f_0(x)=q_1(x)\cdots q_s(x)$.于是$f(x)$分解成$R[x]$中不可约元的乘积

$$f(x)=p_1\cdots p_rq_1(x)\cdots q_s(x).\tag{1}$$

由 $f_0(x)$ 本原及 $f_0(x) = q_1(x)\cdots q_s(x)$,每个 $q_i(x)$ 也本原.

下面证唯一性.设

$$f(x) = p_1'\cdots p_t' q_1'(x)\cdots q_u'(x)$$

为另一分解,其中 p_i' 是 R 中不可约元,$q_i'(x)$ 是 $R[x]$ 中正次数不可约多项式.易知 $q_i'(x)$ 是本原的.否则设 $q_i'(x) = d_i q_i''(x)$, $d_i \in R$, $q_i''(x)$ 本原.若 d_i 是 R 中非可逆元,则 d_i 也是 $R[x]$ 中非可逆元.否则设有 $q(x) \in R[x]$,使 $d_i q(x) = 1$.比较次数,$q(x)$ 的次数也是零次,$q(x) \in R$.与 d_i 在 R 中非可逆矛盾.这样 $q'_i(x)$ 是 $R[x]$ 中两个非可逆元 d_i 与 $q''_i(x)$ 的乘积,与它是不可约元矛盾.故 d_i 是 R 中可逆元,$q'_i(x)$ 为本原多项式.由高斯引理 $q'_1(x)\cdots q'_u(x)$ 是本原多项式.由引理 1,有

$$p_1 p_2\cdots p_r = \omega p_1' p_2'\cdots p_t' \text{ 及 } q_1(x)q_2(x)\cdots q_s(x) = \nu q_1'(x)\cdots q_u'(x),$$

其中 ω,ν 皆为 R 中可逆元.由 R 是唯一因式分解环,$r = t$,且适当改变 p_i' 的脚标后 p_i 与 p'_i 是相伴的,$i = 1,2,\cdots,r$.将上面第二个式子放到 $Q(R)[x]$ 中考虑.由定理 1,$q_i(x)$,$q_i'(x)$ 是 $Q(R)[x]$ 中不可约多项式.$Q(R)[x]$ 是欧氏环,有因式分解唯一性,因此 $s = u$,且适当改变 $q'_i(x)$ 的脚标后 $q_i(x)$ 与 $q_i'(x)$ 在 $Q(R)[x]$ 中相伴,即有

$$q_i(x) = \frac{a_i}{b_i} q_i'(x), a_i, b_i \in R, i = 1,2,\cdots,s.$$

由上式有 $b_i q_i(x) = a_i q_i'(x)$.前面证明中已指出 $q_i(x)$ 及 $q_i'(x)$ 皆是 $R[x]$ 中本原多项式,由引理 1,$q_i(x)$ 与 $q'_i(x)$ 在 $R[x]$ 中相伴.

以上证明了 $R[x]$ 中 $f(x)$ 的因式分解的唯一性.故 $R[x]$ 是唯一因式分解环.

推论 R 是唯一因式分解环,则多元多项式环 $R[x_1,x_2,\cdots,x_n]$ 也是唯一因式分解环.

证明 由定理 2,$R[x_1]$ 是唯一因式分解环.逐次用定理 2,$R[x_1][x_2]$,$R[x_1][x_2][x_3]$,$\cdots$,$R[x_1][x_2]\cdots[x_n]$ 都是唯一因式分解环.于是 $R[x_1,\cdots,x_n] = R[x_1]\cdots[x_n]$ 是唯一因式分解环.

这样定理 2 又提供了唯一因式分解环的新例子.它们中有些还不是主理想环.

例 1 考察环 $\mathbb{Q}[x]$ 和 $\mathbb{Z}[x]$.

我们知道 $\mathbb{Q}[x]$ 是欧氏环,当然是主理想环.对 $\mathbb{Z}[x]$,取 $\mathbb{Z}[x]$ 中理想 $2\mathbb{Z}[x] + x\mathbb{Z}[x]$.我们将证明这个理想不是主理想.

反证法.设它是主理想,令

$$2\mathbb{Z}[x] + x\mathbb{Z}[x] = p(x)\mathbb{Z}[x]. \tag{2}$$

由 $2 \in p(x)\mathbb{Z}[x]$ 及 $x \in p(x)\mathbb{Z}[x]$,$p(x)|2$ 及 $p(x)|x$.即 $p(x)$ 是 2 和

x 的公因子，只能是 $\mathbb{Z}[x]$ 的可逆元. 于是

$$p(x)\mathbb{Z}[x] = \mathbb{Z}[x], 2\mathbb{Z}[x] + x\mathbb{Z}[x] = \mathbb{Z}[x].$$

因 $1 \in \mathbb{Z}[x]$，就有 $u(x), v(x) \in \mathbb{Z}[x]$，使

$$2 \cdot u(x) + xv(x) = 1.$$

设 $u(x) = a_0 + a_1x + \cdots + a_nx^n$，计算上述两端的零次项，则

$$2a_0 = 1.$$

但 $u(x) \in \mathbb{Z}[x]$，a_0 为整数，上式不能成立. 故 $2\mathbb{Z}[x] + x\mathbb{Z}[x]$ 不是主理想.

由此知 $\mathbb{Z}[x]$ 不是主理想环. 但由定理 2，$\mathbb{Z}[x]$ 是唯一因式分解环.

我们还知道有主理想环但不是欧氏环的例子（§2 定义 2 的下方）. 至此我们已弄清了下述包含关系：

$$\text{欧氏环} \subseteq \text{主理想环} \subseteq \text{唯一因式分解环},$$

而且每一个都是真包含关系.

习　　题

下面的环 R 都是唯一因式分解环.

1. $R[x]$ 的正次数多项式若是不可约元，一定是本原多项式.

2. $f(x), g(x) \in R[x]$. $g(x)$ 的首项系数为 1，则有 $q(x), r(x) \in R[x]$，使

$$f(x) = g(x)q(x) + r(x),$$

其中 $r(x)$ 或者为零或者 $\partial(r(x)) < \partial(g(x))$.

3. $f(x) \in R[x], c \in R$ 是 $f(x)$ 的一个根，则 $(x - c) \mid f(x)$.

4. $R[x]$ 中的 n 次多项式 $f(x)$ 在 R 中最多有 n 个不同的根. 于是 $f(x) = a_nx^n + \cdots + a_0$ 在 R 中若有多于 $n + 1$ 个根，必是零多项式.

§5　环的直和与中国剩余定理

《孙子算经》（中国古代数学著作，成书于公元 5 – 6 世纪(?)）中写过一个数学问题，“物不知其数问题”：今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？

用现代数学语言表述，就是求整数 n，使得

$$n \equiv 2 \pmod 3,$$
$$n \equiv 3 \pmod 5,$$
$$n \equiv 2 \pmod 7.$$

这是一个同余方程组问题，《孙子算经》中给出了它的解法.

它可推广成一般的同余方程组求解.其结果是:设 $m_1, m_2, \cdots, m_r$ 是两两互素的正整数.任给正整数 $a_1, a_2, \cdots, a_r$,必有正整数 x,使

$$x \equiv a_i (\mathrm{mod}\ m_i), i = 1,2,\cdots,r.$$

若令 $m = m_1 m_2 \cdots m_r$,则 $x(\mathrm{mod}\ m)$ 是唯一的.

物不知其数问题在欧洲是一个知名问题.19 世纪初高斯给出了它的一般性定理.因此国际上称《孙子算经》中的问题为中国剩余定理.近世代数对此有几种形式的推广.一种是用与环的直和有关的环同构来表示的,仍称为中国剩余定理.这一节就是介绍这个结果.

先介绍环的(外)直和的概念.

定义 1 $R_1, R_2, \cdots, R_n$ 都是环.又设 $R = R_1 \times R_2 \times \cdots \times R_n$ 是它们作为集合的集合积

$$R = R_1 \times R_2 \times \cdots \times R_n = \{(x_1, x_2, \cdots, x_n) \mid x_i \in R_i, i = 1,2,\cdots,n\}.$$

在 R 上按对应分量相加和相乘的方法引入

$$(x_1, x_2, \cdots, x_n) + (y_1, y_2, \cdots, y_n) = (x_1 + y_1, x_2 + y_2, \cdots, x_n + y_n),$$

$$(x_1, x_2, \cdots, x_n)(y_1, y_2, \cdots, y_n) = (x_1 y_1, x_2 y_2, \cdots, x_n y_n).$$

在这加法和乘法下,R 成为一个环,称为环 $R_1, R_2, \cdots, R_n$ 的**外直和**.记为 $R = R_1 \oplus \cdots \oplus R_n$.

定义 2 在环 R 的理想的集合上定义如下的运算

和:$J_1 + J_2 = \{x_1 + x_2 \mid x_i \in J_i\}$.

交:$J_1 \cap J_2 = \{x \mid x \in J_1 \text{ 且 } x \in J_2\}$.

乘积:$J_1 J_2 = \left\{ \sum_i x_{1i} x_{2i} \,\middle|\, \begin{matrix} x_{ki} \in J_k \\ k = 1,2 \end{matrix} \right\} \subseteq J_1 \cap J_2$.

$k = 1,2$.

由于能验证 R 的理想的和、交及乘积仍是 R 的理想,才能说和、交及乘积是理想集合上的运算.这个验证留给读者.

当然还可以定义有限多个理想的和、乘积或交.

命题 1 如果环 R 中理想 $J_1, J_2, \cdots, J_n$ 满足等式

$$J + J_k = R, k = 1,2,\cdots,n,$$

则下面等式也成立:

$$J + J_1 \cap J_2 \cap \cdots \cap J_n = R = J + J_1 J_2 \cdots J_n.$$

证明 因 $J_1 J_2 \cdots J_n \subseteq J_1 \cap J_2 \cap \cdots \cap J_n$,故只要证后一个等式 $J + J_1 J_2 \cdots J_n = R$ 就够了.对 n 作归纳法.若 $n = 1$,按命题中的假设它已成立.现设 $J + J_1 \cdots J_{n-1} = R$.又题设有 $J + J_n = R$.这两个式子右端取 1,则有 $x_1, x_2 \in J$,$y_1 \in J_1 \cdots J_{n-1}$,$y_2 \in J_n$,使得 $1 = x_1 + y_1 = x_2 + y_2$.故

$$1=(x_1+y_1)(x_2+y_2)=y_1y_2+(x_1y_2+y_1x_2+x_1x_2)$$
$$\in J_1J_2\cdots J_n+J.$$

$J_1J_2\cdots J_n+J$ 是 R 的理想,又含有 1,就得

$$J_1J_2\cdots J_n+J=R.$$

中国剩余定理 设 R 是环,$J_1,J_2,\cdots,J_n$ 是 R 的理想,满足

$$J_i+J_j=R,1\leqslant i,j\leqslant n,i\neq j,$$

(称为 $J_1,J_2,\cdots,J_n$ 间两两互素),则有环同构:

$$\frac{R}{J_1\cap\cdots\cap J_n}\cong\frac{R}{J_1}\oplus\cdots\oplus\frac{R}{J_n}.$$

证明 作映射

$$R\xrightarrow{\varphi}\frac{R}{J_1}\oplus\cdots\oplus\frac{R}{J_n}$$
$$x\longmapsto(x+J_1,\cdots,x+J_n).$$

这是环同态(读者自己验证).再证 φ 是满射.由假设和命题 1 有,$J_i+\bigcap\limits_{\substack{j=1\\j\neq i}}^{n}J_j=R$.于是有 $a_i\in J_i,b_i\in\bigcap\limits_{\substack{j=1\\j\neq i}}^{n}J_j$,使 $1=a_i+b_i$,或写成 $b_i\equiv 1(\mathrm{mod}\ J_i)$.当 $k\neq i$ 时,$b_k\in\bigcap\limits_{\substack{j=1\\j\neq k}}^{n}J_j$,乘积中有 J_i,故 $b_k\in J_i$.或写成 $b_k\equiv 0(\mathrm{mod}\ J_i)$.现对 $(x_1+J_1,\cdots,x_n+J_n)$,令 $x=\sum\limits_{k=1}^{n}x_kb_k$.由于

$$x_ib_i+J_i-(x_i+J_i)(b_i+J_i)=(x_i+J_i)(1+J_i)=x_i+J_i.$$

$k\neq i$ 时,

$$x_kb_k+J_i=(x_k+J_i)(b_k+J_i)=(x_k+J_i)(0+J_i)=0+J_i.$$

故

$$x+J_i=\sum_{k=1}^{n}(x_kb_k+J_i)=x_i+J_i,$$

即

$$\varphi(x)=(x+J_1,x+J_2,\cdots,x+J_n)=(x_1+J_1,x_2+J_2,\cdots,x_n+J_n).$$

这证明了 φ 是满同态.

计算 $\mathrm{Ker}\ \varphi$.$\varphi(x)=0$ 当且仅当 $x\in J_i,\forall i$.当且仅当 $x\in J_1\cap J_2\cap\cdots\cap J_n$.由此 $\mathrm{Ker}\ \varphi=J_1\cap J_2\cap\cdots\cap J_n$.

最后由环同态基本定理得

$$\frac{R}{J_1\cap J_2\cap\cdots\cap J_n}\cong\frac{R}{J_1}\oplus\cdots\oplus\frac{R}{J_n}.$$

回到前面一般的同余方程组的求解. 在那里，环是 $\mathbb{Z}$，理想是 $m_1\mathbb{Z}, m_2\mathbb{Z}, \cdots, m_n\mathbb{Z}$. $m_1, m_2, \cdots, m_n$ 中两两互素，即 $m_i\mathbb{Z} + m_j\mathbb{Z} = 1 \cdot \mathbb{Z} = \mathbb{Z}$，$m_1 m_2 \cdots m_n\mathbb{Z} = m_1\mathbb{Z} \cap m_2\mathbb{Z} \cap \cdots \cap m_n\mathbb{Z}$. 中国剩余定理断言有环同构：

$$\frac{\mathbb{Z}}{m_1 m_2 \cdots m_n\mathbb{Z}} \cong \frac{\mathbb{Z}}{m_1\mathbb{Z}} \oplus \frac{\mathbb{Z}}{m_2\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{m_n\mathbb{Z}}.$$

给定同余方程组

$$n \equiv a_i \pmod{m_i}.$$

为求解它. 要求 $b_i \in \prod_{\substack{k=1 \\ k \neq i}}^{n} m_k\mathbb{Z} = \left(\prod_{\substack{k=1 \\ k \neq i}}^{n} m_k\right)\mathbb{Z} = \frac{m}{m_i}\mathbb{Z}$，$m = m_1 \cdots m_n$，使 $b_i \equiv 1 \pmod{m_i}$. 可写 $b_i = k_i \frac{m}{m_i}$. 令

$$n = \sum_{i=1}^{n} k_i \frac{m}{m_i} a_i. \tag{1}$$

则 n 满足要求，并且模 $m = m_1 m_2 \cdots m_n$ 是唯一的.

例　“物不知其数问题”中是要解同余方程组

$$n \equiv 2 \pmod 3,$$
$$n \equiv 3 \pmod 5,$$
$$n \equiv 2 \pmod 7.$$

解　求 k_1，使 $k_1 \cdot \frac{3 \cdot 5 \cdot 7}{3} \equiv 1 \pmod 3$. 求出 $k_1 = 2$. ($2 \cdot 5 \cdot 7 = 70 \equiv 1 \pmod 3$).

求 k_2，使 $k_2 \cdot \frac{3 \cdot 5 \cdot 7}{5} \equiv 1 \pmod 5$. 求出 $k_2 = 1$ ($1 \cdot 3 \cdot 7 = 21 \equiv 1 \pmod 5$)

求 k_3，使 $k_3 \cdot \frac{3 \cdot 5 \cdot 7}{7} \equiv 1 \pmod 7$. 求出 $k_3 = 1$ ($1 \cdot 3 \cdot 5 = 15 \equiv 1 \pmod 7$).

于是求出解为

$$n = 2 \cdot 5 \cdot 7 \cdot 2 + 1 \cdot 3 \cdot 7 \cdot 3 + 1 \cdot 3 \cdot 5 \cdot 2 = 140 + 63 + 30 = 233.$$

取 $n - 2 \cdot 3 \cdot 5 \cdot 7 = 233 - 210 = 23$. 这是满足方程组的最小正整数解.

在《孙子算经》中没有(1)中各 k_i 的具体算法. 宋代秦九韶在《数书九章》中第一次详细地、完整地阐述了求解一次同余方程组的算法. 他称此算法为“大衍总数术”，其中包括求 k_i 的一种机械化算法——大衍求一术. 这是中国古代数学的光辉成就.

习　题

1. 解同余方程组.

(i) $\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 7 \\ x \equiv 4 \pmod 9 \end{cases}$　　(ii) $\begin{cases} x \equiv 5 \pmod 7 \\ x \equiv 4 \pmod 6 \end{cases}$

2. 韩信点兵问题:有兵一队,若列 5 列纵队,则末行 1 人,成 6 列纵队,则末行 5 人,成 7 列纵队,则末行 4 人,成 11 列纵队,则末行 10 人.求兵数.

3. $R_1, \cdots, R_s$ 是环. $U_1, \cdots, U_s$ 分别是它们的可逆元的群. 证明 $R_1 \oplus \cdots \oplus R_s$ 的可逆元群 $U = U_1 \times U_2 \times \cdots \times U_s$.

4. 设 $n = m_1 m_2 \cdots m_s$, m_i 两两互素. 令 $U(\mathbb{Z}_m)$ 表 $\mathbb{Z}_m$ 的可逆元群,则 $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ 的可逆元群同构于 $U(\mathbb{Z}_{m_1}) \times \cdots \times U(\mathbb{Z}_{m_s})$. 进而有, $\varphi(n) = \varphi(m_1)\varphi(m_2)\cdots\varphi(m_s)$. 这里 $\varphi(n)$ 是欧拉函数. 当 $n = p_1^{e_1} \cdots p_s^{e_s}$, p_i 为不同素数时, $\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_s}\right)$.

参考书目

供进一步学习的近世代数教材：

(1) 刘绍学. 近世代数基础. 北京：高等教育出版社，1999

(2) 聂灵沼，丁石孙. 代数学引论. 北京：高等教育出版社，1993

(3) 阿·伊·柯斯特利金. 代数学引论(上，下). (译自英文版，原为俄文). 北京：高等教育出版社，1988

(4) T W Hungerford. 代数学(译自英文). 长沙：湖南教育出版社，1985

(5) N Jacobson. Basic Algebra Ⅰ，Ⅱ. San Francisco: W H Freeman Company, 1974, 1980

(6) S Lang. Algebra(第二版). Menlo Park: Addison-Weeley Publishing Company, Inc., 1984

以下是几本与近世代数应用有关的书：

(1) 俞文海. 晶体结构的对称群. 合肥：中国科学技术大学出版社，1991

(2) J H van 林特. 编码理论导引(译自英文). 北京：科学出版社，1988

(3) 冯登国，裴定一. 密码学导引. 北京：科学出版社，1999

(4) I Tomescu. 组合学引论(译自英文版). 北京：高等教育出版社，1985

(5) W J Gilbert. Modern Algebra with Applications. New York: John Wiley & Sons, 1976

(6) 张端明，钟志成. 应用群论导引. 武汉：华中理工大学出版社，2001

符 号 表

$\mathbb{C}$ 复数域

$\mathbb{R}$ 实数域

$\mathbb{R}^*$ 非零实数集

$\mathbb{R}^+$ 正实数集

$\mathbb{Q}$ 有理数域

$\mathbb{Z}$ 整数环

$\mathbb{Z}_n$ 整数模 n 剩余类环

F_q q 个元素的域

$[E:F]$ F 的扩域 E 的扩张次数

$GL_n(F)$ F 上 $n\times n$ 可逆矩阵的群

$SL_n(F)$ F 上 $n\times n$ 行列式为 1 的矩阵的群

$PSL(n,F)$ 射影幺模群

$GL(V)$ 线性空间 V 上可逆线性变换的群

$O_n(\mathbb{R})$ $\mathbb{R}$ 上 $n\times n$ 正交矩阵的群

$O_n(V)$ n 维欧氏空间上正交变换的群

S_M 集合 M 上可逆变换的群

S_n n 元对称群

A_n n 元交错群

$|G|$ 群 G 的阶

$[G:H]$ G 的子群 H 的指数

$o(a)$ 群元素 a 的阶

$\exp(G)$ G 的方次数

$\langle S\rangle$ 由群的子集 S 生成的群

$C_G(x)$ x 在 G 中的中心化子

$C_G(H)$ H 在 G 中的中心化子

$N_G(H)$ H 在 G 中的正规化子

$\mathrm{Stab}_G(x)$ G 在 x 处的稳定化子

$\mathrm{Ker}\varphi$ 同态 φ 的核

$\varphi(n)$ 欧拉函数

Aut G 自同构群

名词索引(按汉语拼音的首字母次序排列)