高等学校教材

近世代数

(第二版)

杨子胥　编著

高等教育出版社

内容提要

本书是作者在长期教学实践的基础上，参考国内外大量相关教材、专著、文献并吸纳个人一些科研成果编写而成的。本次修订是在《近世代数》(第一版,杨子胥编著)的基础上，作了较大的修改：去掉了一些定理，减少了深度和难度；适当增加了例题；习题作了较大的变动；改正了部分错误；增强了本书的可读性、适用性和灵活性。内容包括基本概念、群、正规子群和群的同态与同构、环与域、惟一分解整环、域的扩张等。

本书由万哲先、王梓坤二位院士推荐出版，并由刘绍学教授撰写序言。

本书可作为综合大学理科数学类专业、高等师范院校数学类专业近世代数课程的教材。

图书在版编目(CIP)数据

近世代数/杨子胥编著．—2版．—北京：高等教育出版社，2003.12

ISBN 7-04-012948-5

Ⅰ.近… Ⅱ.杨… Ⅲ.抽象代数-高等学校-教材 Ⅳ.0153

中国版本图书馆CIP数据核字(2003)第089335号

出版发行 高等教育出版社 ■ 购书热线 010-64054588

社 址 北京市西城区德外大街4号 免费咨询 800-810-0598

邮政编码 100011 网 址 http://www.hep.edu.cn

总 机 010-82028899 http://www.hep.com.cn

经 销 新华书店北京发行所

印 刷

开 本 850×1168 1/32 版 次 2000年5月■第1版

印 张 9.625 年 月■第2版

字 数 240■000 印 次 年 月第 次印刷

定 价 14.70元

策划编辑　李　蕊
责任编辑　胡乃
封面设计　王　睢
责任绘图　郝　林
版式设计　张　岚
责任校对　康晓燕
责任印制

序　言

近世代数(或抽象代数)是大学数学系的重要基础课之一，主要介绍群、环、域(以及模)的基本概念和基本理论．在这里人们将受到良好的代数训练，并为进一步学习数学得到一个扎实的代数基础．

我们知道，数、多项式和矩阵的出现是为了刻画一些物理量和几何量，诸如长度、面积、速度、物理定律、空间中点的位置、平面的运动和几何变换等．它们的表现能力是很强的，使用数、多项式和矩阵足以刻画许多我们遇到的物理量和几何量．然而当人们企图刻画对称性——无论是物理现象中，还是数学世界中(尤其是在几何图形中)的对称性时，都无法用单个的数、多项式或矩阵去刻画．为了刻画对称这一概念，人们发现了群．现在我们知道，群是研究对称性的有力工具．由于物理、几何、数学中对称这一概念的特殊重要性，因而使群成为近代数学极其深刻极其重要的概念之一．

类似地，环、域、模也是刻画物理量和几何量的数学工具．

因而研究群、环、域、模的方式可分为两大类．一类是紧密结合其背景去研究，如晶体群，群与量子力学等；另一类是对群、环、域、模作理论上的研究．当然两者有着相互的联系．这样，自然地在介绍群、环、域、模的书中也有两种不同的倾向．

本书则是介绍群、环、域的基本概念和基本理论．本书作者

写的另一本书《正交表的构造》则是以群、环、域为基本工具，讲述正交表的构造原理和方法．

杨子胥教授从事于高校代数教学与科研工作数十年，经验丰富，成果不断．他编写的这本《近世代数》一书，是他在长期教学实践的基础上，经过反复修改提炼整理而成的．本书取材广泛，内容丰富且紧扣大纲，前后呼应，非常紧凑．其中一个概念的引入，一种思想的建立或一个定理的证明，都字斟句酌一丝不苟，既保持严格的科学性和系统性，又自然明快易于接受．

近世代数是比较抽象的一门学科，但本书所举正反例子较多，涉及面广，尽量把抽象的概念和问题具体化．而且还特别注意同高等代数的联系，每节所配备的习题的数量和难易程度适当，尤其是文句叙述和表达自然流畅，读来引人入胜，确实不失为一本好的近世代数教材．

第二版前言

本书修订版主要的变动有如下四个方面:

一、更正了一些错误，改动了个别定理的证明方法，特别是去掉了一些不很必要的内容 .

二、增加了传递群、单群、可解群和幂集环等概念和相应的一些定理和例子 . 此外还增加了少数交换图、一些研究对象的历史背景介绍以及“ 本书所用符号 ”和“ 参考文献 ”等 .

三、对习题作了较大调整，去掉了少数题，每节题量减少，难度降低 . 但在每章最后一节的习题中却增加题目较多，题量稍大一些 . 其主要目的是，可通过这些习题对本章内容起一个复习巩固的作用；当然，其中也有少数题目难度稍大一些，可供学生参考或习作 .

四、个别章节顺序作了调整，有的章节和个别定理打上星号“ * ”，这些内容可略讲或不讲 .

由于各校情况不同，因此在使用本书时应灵活掌握，不可千篇一律 . 例如上面已谈到，对于打 * 号的章节可略讲或不讲 . 比如 Sylow 定理，它是群论特别是有限群论中经典结论之一，尤其是它的证明几乎涉及到了前三章中群理论的所有概念，不仅如此，由 Sylow 定理还可以很容易地推演出大量有关一些群的重要结论和结构定理 . 因此，若课时不够，即使不讲定理证明但介绍一下 Sylow 定理本身的内容和意义也是很有价值的 .

据知，有些高校只讲前四章，其实这也是可以的，因为这四章可以说涵盖了近世代数最基本的内容．当然，如果条件允许，也可以简略介绍一下主理想整环和欧氏环以及第六章的前三节．

对于习题，一般而言，每节选 3 至 5 个题做作业即可．而对余下的题目，特别是每章最后一节中的习题，可让学有余力和考研同学课下自行练习．

我将编写《近世代数学习辅导与习题选解》(高等教育出版社出版)，几乎包含了本书所有习题的解答，因此可作为高校师生学习参考之用．但这里应提醒读者的是，对任何题解都不可产生太大的依赖性．这如同身体不适服药一样，适当用药有益健康，过量服用则有损肌体．正确的方法应该是，对于一个题目要尽量自己先动脑去想，实在做不出时再参阅题解．这样用辅导书可能效果会更好一些．

在本书这次修订中，山东大学张顺华教授、陕西师大雷天德教授、潍坊学院王新民教授、解放军信息工程大学马传贵教授以及曲阜师大、济南大学和山东师大等校有关老师，都提出了不少宝贵意见，我表示衷心的感谢！

这次修订虽主观力求完善，但仍难免还有不妥之处，希望读者多多指正．

杨子胥

2003 年 6 月于济南

前　言

本书是作者在长期教学实践的基础上，参考国内外大量相关教材、专著、文献并吸纳个人一些科研成果，编写而成．

全书共六章，可大致分为三个部分：

第一部分，包括引言和第一章基本概念，它是全书的基础，在以后各章都要用到，应予以充分重视；

第二部分，包括第二、三两章，介绍含一个代数运算的群的理论．其中第二章介绍群的最基本的知识；第三章则进一步介绍正规子群和群的同态与同构，以及和它们相关联的群论中最基本最重要的定理，如群的同态和同构定理，共轭、正规化子和中心化子，Sylow 定理和有限交换群基本定理等等；

第三部分，包括第四、五、六三章，介绍含有两个代数运算的环与域的理论．其中第四章介绍环的基本知识；第五章介绍环论中一个特殊问题——惟一分解整环内的因子分解理论，并由此介绍了两种特殊的环类，即主理想整环和欧氏环；第六章介绍域，一种加强条件的环，并且主要介绍代数扩域，特别是有限次扩域和有限域．

本书取材广泛，有的高校若教学时间不够，有些内容，例如多项式环、环的直和、非交换环、惟一分解整环的多项式扩张、可离扩域或其它内容，可粗讲或不讲，或只详述结论而略去证明．本书每节都配备有习题，其题量和难度比较适中，个别稍难

题目都有提示，各校可根据不同情况择题而作 .

本书承蒙我国数学家、中科院院士万哲先研究员和我国数学家、中科院院士王梓坤教授推荐出版，并承蒙我国数学家、北京师范大学博士生导师刘绍学教授撰写序言，作者由衷地对他们表示最诚挚的感谢！

作者才疏学浅，书中错误和疏漏之处恐在所难免，恳请读者批评指正 .

作 者

1999 年 5 月

目　　录

引　言

代数学是数学的一个古老分支，有着悠久的历史．但是，近一百年来，随着数学的发展和应用的需要，代数学的研究对象和研究方法发生了巨大的变化，一系列新的代数领域被建立起来，大大地扩充了代数学的研究范围，形成了所谓的近世代数学．

大家知道，数是我们研究数学的最基本的对象，数的最基本的运算是加、减、乘、除．但是，数并不是我们研究数学的惟一对象，而且我们所遇到的许多运算也不全是数的普通加、减、乘、除．例如，向量、力以及多项式、函数、矩阵和线性变换等等，它们虽然都不是数，但却也可以类似于数那样来进行运算．特别是，尽管这些研究对象千差万别，各有自己的特性，但是从运算的角度看却有着很多共同的性质．于是，从一般的集合出发，研究各种运算的种种性质，就具有非常重要的意义．因为它的结论和方法不仅可以渗透到数学的各个部门，而且在其他学科，例如在物理、化学、正交试验设计和编码等理论中都有重要应用．

一个集合，如果有一种或数种代数运算，我们就笼统地称它是一个代数系统．简言之，近世代数就是研究各种代数系统的一门学科．在近世代数中，尽管有时，特别是在举例时，也讲具体的集合和具体的运算，但其最根本的任务是研究各种抽象的代数系统．也就是说，一般讲，不仅集合是抽象的，而且所说的运算

也是抽象的．因此，常把近世代数也叫做抽象代数．

由于代数系统中运算个数以及对运算所要求的附加条件的不同，从而产生了各种各样的不同的代数系统，这就形成了近世代数中各个不同的分支．其中最基本、最重要的分支是群、环和域，它们所研究的内容极为丰富和广泛．实践已经证明，这些理论不仅对数学本身产生重要影响并有重要应用，而且对其他学科也有重要影响和应用．这样一来，古老的代数学在新的基础上又以全新的面貌和更加旺盛的活力飞速地向前发展着．

本课程的任务是，介绍近世代数中最基本的代数系统——群、环、域的最基本的概念和性质．

第一章　基■本■概■念

本章所介绍的内容，是在以后各章中都要用到的基本概念．它们是：集合、映射与变换、代数运算、运算律、同态与同构、等价关系与集合的分类，等．

§1　集　　合

我们在讨论问题时，在一定范围内所说的对象，例如，数、向量、多项式、矩阵、点、直线，甚或书架上的书，桌子上的茶杯、钢笔、铅笔等等，都笼统地称为__素　元__．

若干个(有限个或无限个)固定元素的全体，叫做一个__合__，或简称为__集__．

集合常用大写拉丁字母 A，B，C，…，G，R，F，…等表示；集合中的元素常用小写拉丁字母 a，b，c，…，x，y，…来表示．

如果 x 是集合 A 中的一个元素，就说 x 属于集合 A 或集合 A 包含 x，记为 $x\in A$ 或 $A\ni x$；如果 x 不是集合 A 中的元素，就说 x 不属于集合 A 或集合 A 不包含 x，记为 $x\notin A$ 或 $A\not\ni x$．

不包含任何元素的集合称为__空集合__，记为　　．

今后常用 $\mathbf{Z}$ 表示整数集，$\mathbf{Z}^*$ 表示非零整数集；用 $\mathbf{Q}$ 表示有理数集，$\mathbf{Q}^*$ 表示非零有理数集．

要指明一个集合是由哪些元素构成的，可以用列举法，例如

$$A=\{1,3,5\},\quad B=\{\text{东},\text{西}\},$$

$$C=\left\{1,\frac{1}{2},\frac{1}{3},\frac{1}{4},\cdots\right\};$$

有时也可以用描述法，例如

$$E=\{\text{全体自然数}\},\quad F=\{x\mid x\text{是实数且}x^2<1\}.$$

定义 1 如果集合 A 的每个元素都属于集合 B，则称 A 是 B 的一个__集__，记为 $A\quad B$.

如果 A 是 B 的一个子集，又 B 中有元素不在 A 中，则称 A 是 B 的一个__真子集__，记为 $A\quad B$.

空集合被认为是任意集合的一个子集.

当集合 A 不是集合 B 的子集或真子集时，分别记为 $A\ \check{n}\ B$ 或 $A\ \grave{a}\ B$.

显然，$A\quad B$ 意味着 $A\quad B$ 或 $A=B$(即 A 与 B 是由完全相同的元素作成的集合). 一个虽然简单但却非常重要的事实是:

$$A=B\ \text{当且仅当}\ A\quad B\ \text{且}\ B\quad A.$$

因此，要证两个集合 A 与 B 相等，常需证明 $A\quad B$ 且 $B\quad A$, 即 A 与 B 互相包含. 这个事实虽然简单，但它却是贯穿到整个近世代数中的一个一般方法.

如果把集合 A 的每一个子集当成一个元素，则 A 的所有子集(包括空集)也作成一个集合,称为 A 的__集__,记为 $P(A)$.

如果集合 A 包含无限多个元素，则记为 $|A|=\infty$; 如果 A 包含 n 个元素，则记为 $|A|=n$. 于是易知，当 $|A|=n$ 时有

$$|P(A)|=2^n.$$

定义 2 由集合 A 和集合 B 的所有公共元素构成的集合，记为 $A\cap B$, 叫做 A 与 B 的__集__，简称 A 与 B 的__交__.

例如，集合 $A=\{0,1,2,3\}$与集合 $B=\{0,2,4\}$的交为

$$A\cap B=\{0,2\}.$$

但是，集合 A 与集合 $C=\{4,5,6\}$ 的交为空集合，即

$$A\cap C=\quad .$$

定义 3　由属于集合 A 或集合 B 的所有元素作成的集合，记为 $A\cup B$，叫做 A 与 B 的__集__，简称 A 与 B 的__并__．

例如，集合 $A=\{0,1,2,3\}$ 与集合 $B=\{0,1,-2,-3\}$ 的并为

$$A\cup B=\{-3,-2,0,1,2,3\}\ .$$

对于两个以上甚至无穷多个集合，也可以类似地定义其交与并．

容易推出，集合的交与并有以下性质：

1) $A\cap A=A$，　$A\cup A=A$；　(幂等性)

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

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

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

习题　1.1

1. 证明本节的等式 4)．

2. 若 $A\cap B=A\cap C$，问：是否 $B=C$？把 $\cap$ 改成 $\cup$ 时又如何？

3. 设 A 是有限集合，且 $|A|=n$．证明：

$$|P(A)|=2^n\ .$$

4. 设 A，B 是两个有限集合．证明：

$$|A\cup B|+|A\cap B|=|A|+|B|\ .$$

5. 设 A，B 是两个集合．称集合

$$A-B=\{a\,|\,a\in A,a\mid B\}$$

为 A 与 B 的__集__．特别，当 $Y\quad X$ 时，用 Y' 表示 $X-Y$，并称为 Y 在 X 中的__集__．证明德·摩根(A .De Morgan，1806～1871)律：若 A，$B\quad X$，则

$$(A\cup B)'=A'\cap B',\ (A\cap B)'=A'\cup B'.$$

§2 映射与变换

通过映射与变换来研究代数系统，这是近世代数中最重要的方法之一．

定义 1 设 X 与 Y 是两个集合．如果有一个法则 ϕ，它对于 X 中每个元素 x，在 Y 中都有一个惟一确定的元素 y 与它对应，则称 ϕ 为集合 X 到集合 Y 的一个__射__．这种关系常表示成

$$\phi: \quad x \quad y \quad \text{或} \quad y = \phi(x),$$

并且把 y 叫做 x 在映射 ϕ 之下的__象__，而把 x 叫做 y 在映射 ϕ 之下的__象__ __象__．

例 1 设 X 为有理数集，Y 为实数集，则法则

$$\phi: \quad x \quad \frac{1}{x-1}, \quad \text{即} \quad \phi(x) = \frac{1}{x-1}$$

不是 X 到 Y 的映射．因为，虽然 ϕ 对于任何不等于 1 的有理数 x 在 Y 中都有惟一确定的象，但是有理数 1 没有确定的象．

例 2 设 X 与 Y 都是有理数集，法则

$$\phi: \quad \frac{a}{b} \quad a+b, \quad \text{即} \ \phi\frac{a}{b} = a+b$$

不是 X 到 Y 的映射．因为，例如对于 $\frac{1}{2} = \frac{2}{4}$，却有

$$\phi\frac{1}{2} = 1+2 = 3, \quad \phi\frac{2}{4} = 2+4 = 6,$$

即 X 中相等的元素在 Y 中的象不惟一．但映射必须要求 X 中相等的元素在 Y 中的象也相等．

例 3 设 $X = \{1,2,3\}$, $Y = \{2,4,8,16\}$，则法则

$$\phi: \quad x \quad 2x, \quad \text{即} \ \phi(x) = 2x$$

也不是 X 到 Y 的映射．因为，虽然 ϕ 对 X 中每个元素都有一个惟一确定的象，但 3 的象 6 却不属于 Y．

这就是说，集合 X 到集合 Y 的一个法则 ϕ，在满足以下三

个条件时才是一个映射:

1) φ对于 X 中每个元素都必须有确定的象;

2) X 中相等元素的象也必须相等，亦即 X 中每个元素的象是惟一的;

3) X 中每个元素的象都必须属于 Y .

例 4 设 $X=\{1,2,3\}$, $Y=\{0,4,9,10\}$, 则法则

$$\varphi:\quad 1\quad 0,\quad 2\quad 0,\quad 3\quad 9,$$

即 $\varphi(1)=\varphi(2)=0$, $\varphi(3)=9$ 是 X 到 Y 的一个映射 .

例 5 设 X 为数域 F 上全体 n 维向量作成的集合, 则法则

$$\varphi:\quad (a_1,a_2,\cdots,a_n)\qquad a_1\quad (a_i\in F)$$

即 $\varphi((a_1,a_2,\cdots,a_n))=a_1$ 是 X 到 F 的一个映射 .

例 6 设 $X=\{1,2,3,\cdots\}$, Y 为有理数集, 则法则

$$\varphi:\quad x\qquad x^2,\quad \text{即}\quad \varphi(x)=x^2$$

也是 X 到 Y 的一个映射 .

映射是通常函数概念的一种推广，集合 X 相当于定义域 . 不过应注意，集合 Y 包含值域，但不一定是值域 . 就是说，在映射 φ之下不一定 Y 中每个元素都有逆象 . 例如，例 6 就属于这种情形 .

定义 2 设 φ是集合 X 到集合 Y 的一个映射 . 如果在 φ之下 Y 中每个元素在 X 中都有逆象，则称 φ为 X 到 Y 的一个____，或 X 到 Y 上的一个映射 .

设 φ是集合 X 到集合 Y 的一个映射，又 $X_1\quad X$, $Y_1\quad Y$. 则用 $\varphi(X_1)$ 表示 X_1 中所有元素在 φ之下全体象作成的集合, 称为 X_1 在 φ之下的象, 它是 Y 的一个子集; 类似地, 用 $\varphi^{-1}(Y_1)$ 表示 Y_1 中所有元素在 φ之下全体逆象作成的集合，称为 Y_1 在 φ之下的逆象，它是 X 的一个子集 .

显然，X 到 Y 的映射 φ是满射当且仅当 $\varphi(X)=Y$.

定义 3 设 φ是集合 X 到 Y 的一个映射 . 如果在 φ之下，X

中不相等的元素在 Y 中的象也不相等，则称 ϕ 为 X 到 Y 的一个__射__，或 X 到 Y 里的__一一映射__.

我们不难检查上面所举的例子中，哪些是满射，哪些是单射.

定义 4 集合 X 到 Y 的一个映射，如果既是单射又是满射，则称它为 X 到 Y 的一个__射__(或 X 到 Y 上的一一映射).

例 7 设 $X=\{1,2,3,\cdots\}$，$Y=\{2,4,6,\cdots\}$，则法则

$$\phi:\quad x\quad 2x \quad \text{即}\ \phi(x)=2x$$

显然是 X 到 Y 的一个双射.

例 8 设 X 是数域 F 上全体 n 阶方阵作成的集合，$Y=\{0,1,\cdots,n\}$，又用 $r(A)$ 表示 F 上 n 阶方阵 A 的秩，则法则

$$\phi:\quad A\quad r(A)$$

是 X 到 Y 的一个满射. 但不是单射，因为不同的方阵显然可能有相同的秩. 因此，ϕ 不是 X 到 Y 的双射.

定理 1 设 ϕ 是集合 X 到集合 Y 的一个映射. 则 ϕ 是 X 到 Y 的一个双射，当且仅当 ϕ 为“双方单值”，即 ϕ 对 X 中每个元素在 Y 中只有一个象，且对 Y 中每个元素在 X 中有且只有一个逆象.

证 1) 设 ϕ 对 X 中每个元素在 Y 中只有一个象，且对 Y 中每个元素在 X 中只有一个逆象，则 ϕ 当然是 X 到 Y 的一个满射.

又设 x_1，$x_2\in X$，且 $\phi(x_1)=y_1$，$\phi(x_2)=y_2$. 如果 $y_1=y_2$，则由于其逆象惟一，故 $x_1=x_2$. 即 ϕ 为 X 到 Y 的单射，从而 ϕ 为 X 到 Y 的一个双射.

2) 设 ϕ 为 X 到 Y 的一个双射，则当然对 X 中每个元素在 Y 中只能有一个象. 由于 ϕ 是满射，故 ϕ 对 Y 中每个元素都有逆象；又由于 ϕ 是单射，因此 ϕ 对 Y 中每个元素只能有一个逆象.

(证毕)

设 ϕ 为集合 X 到集合 Y 的一个双射，且 $\phi(x)=y$，则显然法则

$$\varphi^{-1}: \quad y \quad x, \quad \text{即} \quad \varphi^{-1}(y) = x$$

便是集合 Y 到 X 的一个双射．我们称 φ^{-1} 为 φ 的逆映射．

显然，φ^{-1} 的逆映射就是 φ，即 $(\varphi^{-1})^{-1} = \varphi$.

对两个有限集合 X 与 Y 来说，显然它们间能建立双射的充要条件是 $|X| = |Y|$，即二者包含的元素个数相等．特别有

定理 2 设 X 与 Y 是两个有限集合且 $|X| = |Y|$，则 X 到 Y 的映射 φ 是满射当且仅当 φ 是单射．

证 设 $|X| = |Y| = n$, 且

$$X = \{x_1, x_2, \cdots, x_n\}, \quad Y = \{y_1, y_2, \cdots, y_n\},$$

又

$$\varphi: \quad x_i \quad y_{k_i} \quad (i = 1, \cdots, n; 1 \leq k_i \leq n)$$

是 X 到 Y 的一个映射．

若 φ 是满射，则由 $x_1 \neq x_2$，必有 $y_{k_1} \neq y_{k_2}$:

因若 $y_{k_1} = y_{k_2}$，则

$$\varphi(X) = \{y_{k_2}, y_{k_3}, \cdots, y_{k_n}\}$$

最多有 $n-1$ 个元素，因此 $\varphi(X) \neq Y$, 这与 φ 是满射矛盾．这种讨论对 X 中任二元素都成立，因此 φ 是单射．

反之，设 φ 是单射，则由于 X 中不同元素的象也不同，故

$$|\varphi(X)| = n = |Y| .$$

但是 $\varphi(X) \quad Y$，故 $\varphi(X) = Y$，即 φ 是满射．

(证毕)

本定理的一个直接结果是以下

推论 如果 X 与 Y 是两个所含元素个数相等的有限集合，则 X 到 Y 的映射 φ 是双射当且仅当 φ 是满(单)射．

下面来介绍映射的相等与映射的合成．

定义 5 设 σ 与 τ 都是集合 X 到 Y 的映射．如果对 X 中每个元素 x 都有

$$\sigma(x) = \tau(x),$$

则称 σ与τ是 X 到 Y 的两个相等的映射，记为

$$\sigma = \tau .$$

设 τ是集合 M_1 到 M_2 的一个映射，又 σ是集合 M_2 到 M_3 的一个映射，则显然

$$x \quad \sigma(\tau(x)) \quad (\forall\ x \in M_1)$$

是 M_1 到 M_3 的一个映射．我们把这个映射记为 στ，即

$$\sigma\tau(x) = \sigma(\tau(x)), \quad (\forall\ x \in M_1),$$

并称其为__射的合成__ __射的乘法__，而称 στ 为映射 τ与σ的__乘积__．

映射合成的这种关系可用右图表示出来．这种图在代数学中常称为__交换图__．

本节最后，我们来介绍一种特殊的映射——变换．

定义 6 集合 X 到自身的映射，叫做集合 X 的一个__ 换__．

同样可定义满射变换、单射变换和双射变换．X 的双射变换也称为 X 的一个__一一变换__．

集合 X 中每个元素与自身对应的变换，是 X 的一个双射变换，称为集合 X 的__恒等变换__．

例 9 设 $X = \{1,2,3,\cdots\}$，则

$$\phi: \quad x \quad x^2, \quad \text{即 } \phi(x) = x^2$$

是 X 的一个单射变换．但不是满射变换，因为例如正整数 2 在 X 中就没有逆象．

又法则

$$\sigma: \quad 1 \quad 2, \quad 2 \quad 1, \quad n \quad n \ (n = 3,4,\cdots)$$

显然是正整数集 X 的一个双射变换．

例 10 设 X 为数域 F 上全体 n 阶方阵作成的集合．则变换

$$\phi(A) = A^{\mathrm{T}} \quad \text{及} \quad \tau(A) = CAC^{-1}$$

都是 X 的双射变换，其中 A^{T} 为 A 的转置矩阵，而 C 为 F 上任

意一个固定的 n 阶满秩方阵 .

定理 3 含 n 个元素的任意集合共有 $n!$ 个双射变换 .

证 设 $M=\{1,2,\cdots,n\}$, 则对 M 的每个双射变换 ϕ, 都能确定元素 1, 2, …, n 的一个全排列

$$\phi(1)\phi(2)\cdots\phi(n) .$$

反之,元素 $1,2,\cdots,n$ 的任意一个全排列都确定 M 的一个双射变换;而且不同的排列确定不同的双射变换 .因此,这 n 个元素有多少个全排列, M 就有多少个双射变换 .由于 n 个元素共有 $n!$ 个全排列,故 M 共有 $n!$ 个双射变换 .

(证毕)

对有限集合的双射变换 ϕ, 常用以下特殊符号表示:

$$\phi=\begin{matrix}1 & 2 & \cdots & n\\ \phi(1) & \phi(2) & \cdots & \phi(n)\end{matrix},$$

并称其为一个 n 次置换 .

例如, 当 $n=3$ 时, 集合 $M=\{1,2,3\}$ 共有 $3!=6$ 个 3 次置换, 它们是

$$\phi_1=\begin{matrix}1&2&3\\1&2&3\end{matrix},\quad \phi_2=\begin{matrix}1&2&3\\1&3&2\end{matrix},\quad \phi_3=\begin{matrix}1&2&3\\2&1&3\end{matrix},$$

$$\phi_4=\begin{matrix}1&2&3\\2&3&1\end{matrix},\quad \phi_5=\begin{matrix}1&2&3\\3&1&2\end{matrix},\quad \phi_6=\begin{matrix}1&2&3\\3&2&1\end{matrix}.$$

应该注意的是, 同一个 n 次置换可以有 $n!$ 种不同的写法 . 例如, 上面的 3 次置换 ϕ_4 的 6 种写法是:

$$\phi_4=\begin{matrix}1&2&3\\2&3&1\end{matrix}=\begin{matrix}1&3&2\\2&1&3\end{matrix}=\begin{matrix}2&1&3\\3&2&1\end{matrix}$$

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

在下一节, 特别在下一章中, 我们还将详细地讨论 n 次置换 .

习题 1.2

1. 设 $X=\{1,2,3,4,5\}$, $Y=\{0,2,4,6,8,10\}$.试给出 X 到 Y 的两个单射.

2. 设 X 是数域 F 上全体 $n(n>1)$阶方阵作成的集合.问:

$$\varphi: A \quad |A|$$

是否为 X 到 F 的一个映射?其中 $|A|$为 A 的行列式.是否为满射或单射?

3. 设 A 与 B 是数域 F 上两个 n 阶相似方阵,$F[A]$为系数属于 F 的关于 A 的一切多项式作成的集合.问:法则

$$\varphi: f(A) \quad f(B)$$

是否为 $F[A]$到 $F[B]$的映射?其中 $f(x)$是系数属于 F 的任意多项式.又 φ 是否为单射或满射.

4. 对本节中给出的 3 次置换,求出下列各元素:

1) $\varphi_3(\varphi_3(\varphi_1(1)))=$?

2) $\varphi_2(\varphi_4(\varphi_2(2)))=$?

5. 给出整数集的两个不同的双射.

§3 代■数■运■算

我们说过,近世代数的主要任务是研究各种抽象的代数系统.所谓代数系统,就是指带有运算的集合.这一节我们要严格指出,所谓“带有运算”究竟是什么意思.

定义 1 设 M 是一个集合.如果有一个法则,它对 M 中任意两个有次序的元素 a 与 b,在 M 中都有一个惟一确定的元素 d 与它们对应,则称这个法则是集合 M 的一个<u>代数运算</u>.

如果我们用记号“ ”表示本定义中所说的法则,则平常把 a 与 b 通过 所确定的元素 d 记为

$$a \quad b=d.$$

就是说,对 M 中任二元素 a, b, 通过所规定的法则“ ”,“算”出一个元素 d 来,而 d 必须属于 M.

这正是通常的加法和乘法运算所共有的最本质的属性.因

此，代数运算就是通常加法与乘法运算在最一般情况下的一种自然推广．

例 1 普通加法、减法与乘法都是整数集、有理数集、实数集和复数集的代数运算．

例 2 普通的减法不是正整数集的代数运算，因为例如正整数 1 减 2 得 - 1，但 - 1 不是正整数．

类似地，普通除法 $a \quad b = \frac{b}{a}$ 也不是有理数集的代数运算，因为，尽管对任何有理数 b 及任何非零有理数 a 来说，$\frac{b}{a}$ 是确定的有理数，但是

$$0 \quad b = \frac{b}{0}$$

却无意义．

例 3 法则

$$a \quad b = \quad a^2 + b^2$$

不是整数集的代数运算．因为，尽管对任二整数 a, b 来说，$a^2 + b^2$ 是惟一确定的实数，但却不一定是整数，例如

$$1 \quad 2 = \quad 1^2 + 2^2 = \quad 5$$

就不是一个整数．

例 4 法则

$$a \quad b = ab + 1 \quad \text{或} \quad a \quad b = a + b - 10$$

都是整数集的代数运算，而且前者还是自然数集的一个代数运算．

例 5 法则

$$A \quad B = |A| B$$

是数域 F 上全体 n 阶方阵的集合的一个代数运算．

下面来讨论变换的运算，它在下一章群的讨论里起重要作用．

设 M 是任意一个非空集合，用 $T(M)$ 表示 M 的全体变换作成的集合．任取 $\sigma,\ \tau\in T(M)$，则根据映射的合成知，乘积 $\sigma\tau$ 即

$$\sigma\tau(x)=\sigma(\tau(x))\quad(\forall\ x\in M)$$

也是 M 的一个变换，故 $\sigma\tau\in T(M)$．我们称其为__变换的乘法__．它是 $T(M)$ 的一个代数运算．

若用 ε 表示集合 M 的恒等变换，则对任意 $\sigma\in T(M)$ 都有

$$\sigma\varepsilon(x)=\varepsilon\sigma(x)=\sigma(x),\quad(\forall\ x\in M),$$

从而

$$\varepsilon\sigma=\sigma\varepsilon=\sigma,$$

即在变换的乘法中，恒等变换起着数 1 在数的普通乘法中相同的作用．

令 $S(M)$ 表示集合 M 的全体双射变换作成的集合，于是

$$S(M)\quad T(M),$$

即 $S(M)$ 是 $T(M)$ 的一个子集．可以证明，变换乘法也是 $S(M)$ 的一个代数运算，即 M 的任意两个双射变换的乘积仍是 M 的一个双射变换．

事实上，设 $\sigma,\ \tau\in S(M)$，$a\in M$，则由于 σ 是 M 的双射变换，故存在 $b\in M$，使

$$\sigma(b)=a;$$

又因为 τ 也是 M 的双射变换，故存在 $c\in M$ 使

$$\tau(c)=b.$$

从而 $\sigma\tau(c)=a$，即乘积 $\sigma\tau$ 是 M 的满射变换．

又若 $a_1\neq a_2$，则 $\tau(a_1)\neq\tau(a_2)$，从而

$$\sigma\tau(a_1)\neq\sigma\tau(a_2),$$

即 $\sigma\tau$ 又是 M 的单射变换．

因此，$\sigma\tau$ 是 M 的一个双射变换，即 $\sigma\tau\in S(M)$．

例如，设 $M=\{1,2,3\}$，则由上节知

$$S(M)=\{\varphi_1,\varphi_2,\varphi_3,\varphi_4,\varphi_5,\varphi_6\},$$

而变换的乘法是它的一个代数运算．例如

$$\varphi_3\varphi_1(1)=\varphi_3(\varphi_1(1))=\varphi_3(2)=1,$$
$$\varphi_3\varphi_1(2)=\varphi_3(\varphi_1(2))=\varphi_3(3)=3,$$
$$\varphi_3\varphi_1(3)=\varphi_3(\varphi_1(3))=\varphi_3(1)=2,$$

即

$$\varphi_3\varphi_1=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=\varphi .$$

对有限集合的代数运算，常直观地列成一个表．例如，设

$$M=\{a_1,a_2,\cdots,a_n\},$$

而 $a_i\ \ a_j=a_{ij}\in M(i,j=1,2,\cdots,n)$是 M 的一个代数运算，则对此可列成下表：

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

常称这种表为 M 的“乘法表”.

习题 1.3

1. 设 M 是正整数集，下列各法则哪些是 M 的代数运算？

1) $a\ \ b=a^b$; 2) $a\ \ b=a+b-2$; 3) $a\ \ b=a$.

2. 设 及 $\bar{}$ 是集合 M 的两个代数运算，如果在 M 中存在元素 a，b 使

$$a\ \ b\neq a\ \bar{}\ b,$$

则称 与 $\bar{}$ 是 M 的两个不同的代数运算．

如果 $|M|=n$，问：可以为 M 规定出多少种不同的代数运算？

3. 试对数域 F 上全体 n 阶方阵的集合规定两个(异于矩阵普通运算)不同的代数运算．

4. 设 $M=\{1,2,3\}$，问：$|T(M)|=?\ |S(M)|=?$ 再列出 $S(M)$ 的乘法表．

5. 设 M 为正整数集合，试给出 M 的两个双射变换 σ,τ，使得 $\sigma\tau\neq\tau\sigma$.

§4 运 算 律

近世代数虽然是讨论具有代数运算的集合,但并不是讨论对代数运算不加任何限制的集合.事实上,数、多项式、矩阵、函数等的普通运算,一般都满足通常所熟悉的运算规则,诸如结合律、分配律或交换律等.近世代数在研究各种代数系统时,也不能脱离开这些运算律.

定义 1 设 M 是一个有代数运算 $\circ$ 的集合,如果对 M 中任意元素 a, b, c 都有

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

则称 M 的这个代数运算 $\circ$ 满足结合律.

当然,数、多项式、矩阵及函数等对通常的加法与乘法都满足结合律.但是,一般的代数运算不一定满足结合律.

例 1 设 M 是自然数集.则 M 的代数运算

$$a \circ b = ab + 1$$

不满足结合律.

证 因为

$$(a \circ b) \circ c = abc + c + 1, \quad a \circ (b \circ c) = abc + a + 1,$$

而一般 $abc + c + 1 \neq abc + a + 1$,即 $(a \circ b) \circ c \neq a \circ (b \circ c)$,除非 $a = c$.例如,取 $a = 1$, $b = 1$, $c = 2$ 时得

$$(a \circ b) \circ c = 5, \quad a \circ (b \circ c) = 4.$$

例 2 变换的乘法满足结合律.

证 任取 σ, τ, $\varphi \in T(M)$, $x \in M$,则根据变换乘法有

$$[(\sigma\tau)\varphi](x) = (\sigma\tau)(\varphi(x)) = \sigma[\tau(\varphi(x))],$$

$$[\sigma(\tau\varphi)](x) = \sigma[(\tau\varphi)(x)] = \sigma[\tau(\varphi(x))],$$

从而 $[(\sigma\tau)\varphi](x) = [\sigma(\tau\varphi)](x)$.再由于 x 是 M 中的任意元素,故 $(\sigma\tau)\varphi = \sigma(\tau\varphi)$.

今后我们主要讨论满足结合律的代数运算.下面将看到,具

有这种性质的代数运算会对元素的运算带来什么影响.

设集合 M 有代数运算 $\circ$，现在从 M 中任取四个元素 a，b，c，d，则写法

$$a \circ b \circ c \circ d$$

应该说是毫无意义的.因为，代数运算每次只能对两个元素进行运算，四个元素只能采取加括号的方法逐步加以计算.但易知，这四个元素共有以下五种加括号的方法:

$$[(a \circ b) \circ c] \circ d,\quad a \circ [(b \circ c) \circ d],$$
$$[a \circ (b \circ c)] \circ d,\quad a \circ [b \circ (c \circ d)],$$
$$(a \circ b) \circ (c \circ d),$$

其中每一个都是 M 中一个确定的元素.一般来说，这五个确定的元素不一定相等.但是当 $\circ$ 满足结合律时，下面将知道这五种加括号方法的所得结果是相等的，即它们是 M 中同一个元素.这时便可以不加括号，而把这个共同的元素记为

$$a \circ b \circ c \circ d.$$

在这种规定下，写法 $a \circ b \circ c \circ d$ 才有确定的意义.

对任意有限个元素可以作完全类似的规定.

一般，对 M 中 n 个元素 a_1，a_2，…，a_n，可以证明(例如可参看书末参考文献[2])共有

$$s = \frac{(2n-2)!}{n! \cdot (n-1)!}$$

种加括号方法，分别表示成

$$\Pi_1(a_1 \circ a_2 \circ \cdots \circ a_n),\quad \Pi_2(a_1 \circ a_2 \circ \cdots \circ a_n),\quad \cdots,$$
$$\Pi_s(a_1 \circ a_2 \circ \cdots \circ a_n).$$

定理 1 若集合 M 的代数运算 $\circ$ 满足结合律，则对 M 中任意 $n(n \geq 3)$ 个元素无论怎样加括号，其结果都相等.

证 对元素个数 n 用数学归纳法.

由于代数运算 $\circ$ 满足结合律，故当 $n=3$ 时定理当然成立.

假定对元素个数 $\leq n-1$ 时定理成立，则任取

$$\Pi_j(a_1\ a_2\ \cdots\ a_n),\quad 1\leq j\leq s,$$

不管其怎样加括号，其最后一步总是 M 中两个元素结合，设为

$$\Pi_j(a_1\ a_2\ \cdots\ a_n)=b_1\ b_2,$$

且设 b_1 是 a_1，a_2，…，a_n 中前 $k(1\leq k<n)$ 个元素结合所得的结果，b_2 是后 $n-k$ 个元素结合所得的结果，由归纳假设，它们都是惟一确定的，故

$$\begin{aligned}\Pi_j(a_1\ a_2\ \cdots\ a_n)&=b_1\ b_2\\&=(a_1\ a_2\ \cdots\ a_k)\ (a_{k+1}\ \cdots\ a_n)\\&=[a_1\ (a_2\ \cdots\ a_k)]\ (a_{k+1}\ \cdots\ a_n)\\&=a_1\ [(a_2\ \cdots\ a_k)\ (a_{k+1}\ \cdots\ a_n)]\\&=a_1\ [(a_2\ \cdots\ a_k)\ (a_{k+1}\ \cdots\ a_n)]\\&=a_1\ (a_2\ \cdots\ a_n).\end{aligned}$$

由归纳假设，由于 $a_2\ \cdots\ a_n$ 是 M 中惟一确定的元素，从而 $a_1\ (a_2\ \cdots\ a_n)$ 是 M 中惟一确定的元素.因此，每个 $\Pi_j(a_1\ a_2\ \cdots\ a_n)$ 都等于这个确定的元素，从而

$$\Pi(a_1\ a_2\ \cdots\ a_n)=\cdots=\Pi_s(a_1\ a_2\ \cdots\ a_n).$$

(证毕)

根据这个定理，对于满足结合律的代数运算来说，任意 n 个元素只要不改变元素的前后次序，就可以任意结合而不必再加括号.

由于数、多项式、矩阵和线性变换的普通加法与乘法都满足结合律，从而在对这些对象进行这两种运算时便可以任意结合，而不必加括号.这一结论不仅在中学数学中，而且在高等代数或其他课程中从未证明过，甚至从未提及过，而现在则由定理 1 全部统一解决了.这一点充分说明，正是由于近世代数所讨论的代数系统具有抽象性，从而决定了其具有较广泛的应用范围.

下面再讨论交换律.

定义 2 如果集合 M 的代数运算 $\circ$ 对 M 中任意元素 a，b 都有

$$a \quad b = b \quad a,$$

则称 M 的这个代数运算满足交换律.

满足结合律和交换律的代数运算有以下重要意义.

定理 2 若集合 M 的代数运算 既满足结合律又满足交换律，则对 M 中任意 n 个元素进行运算时可以任意结合和交换元素的前后次序，其结果均相等.

证 对元素的个数 n 用数学归纳法.

当 $n=2$ 时，结论当然成立. 假定对元素个数为 $n-1$ 时结论成立，下证对 n 也成立.

在 M 中任取 n 个元素 a_1，a_2，…，a_n，并设

$$a_{i_1}，\ a_{i_2}，\ \cdots，\ a_{i_n}$$

是它的任意一个排列，且令 $a_{i_k} = a_1$，则由于代数运算 满足结合律和交换律，故

$$\begin{aligned} a_{i_1} \quad a_{i_2} \quad \cdots \quad a_{i_n} &= [(a_{i_1} \quad \cdots \quad a_{i_{k-1}}) \quad a_1] \quad (a_{i_{k+1}} \quad \cdots \quad a_{i_n}) \\ &= [a_1 \quad (a_{i_1} \quad \cdots \quad a_{i_{k-1}})] \quad (a_{i_{k+1}} \quad \cdots \quad a_n) \\ &= a_1 \quad [(a_{i_1} \quad \cdots \quad a_{i_{k-1}}) \quad (a_{i_{k+1}} \quad \cdots \quad a_{i_n})] \\ &= a_1 \quad (a_2 \quad \cdots \quad a_n) \\ &= a_1 \quad a_2 \quad \cdots \quad a_n . \end{aligned}$$

即对 n 个元素无论怎样加括号和交换，其结果都是相等的.

(证毕)

最后再讨论分配律.

定义 3 设集合 M 有两个代数运算 及 . 如果对 M 中任意元素 a，b，c，都有

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

则称运算 对 满足左分配律；如果

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

则称运算 对 满足右分配律.

定理 3 设集合 M 有两个代数运算 及 ，其中 满足结合律，而 对 满足左分配律，则对 M 中任意元素 a 及 b_1，b_2，

…, b_n 有

$$a(b_1 b_2 \cdots b_n) = (a b_1) \cdots (a b_n).$$

证 对 n 用数学归纳法即可得证.

对右分配律有类似结论, 不再赘述.

习题 1.4

1. 设 M 为实数集. 问:

$$a \ b = 2a + 3b \quad (a, b \in M)$$

是否满足结合律和交换律?

2. 下列各集合对所规定的代数运算是否满足结合律和交换律?

1) M 为整数集, $a \ b = a^2 + b^2$;

2) M 为有理数集, $a \ b = a + b - ab$.

3. 设 $M = \{1, 2, 3\}$. 试为 M 规定一个满足结合律和交换律的代数运算; 再规定一个满足交换律但不满足结合律的代数运算.

4. 数域 F 上全体非零多项式的集合对于

$$f(x) \ g(x) = (f(x), g(x))$$

是否满足结合律和交换律? 其中 $(f(x), g(x))$ 表示 $f(x)$ 与 $g(x)$ 的首系数是 1 的最高公因式.

5. 证明本节定理 3.

§5 同态与同构

由于近世代数主要研究具有代数运算的集合, 因此, 近世代数很少考察一般的映射, 而主要考察与代数运算发生联系的映射, 这就是同态映射和同构映射. 它是近世代数中非常重要的概念.

定义 1 设集合 M 与 [illegible] 各有代数运算 [illegible] 及 [illegible], 且 φ 是 M 到 [illegible] 的一个映射. 如果 φ 满足以下条件: 对 M 中任意元素 a, b, 在 φ 之下由

$$a \quad [illegible], \quad b \quad [illegible]$$

总有

$$a \quad b \qquad \text{珑} \ \bar{} \ \text{珑},$$

亦即$\overline{a \quad b} = \text{珑} \ \bar{} \ \text{珑}$或$\phi(a \ b) = \phi(a) \ \bar{} \ \phi(b)$，则称$\phi$为$M$到$\overline{M}$的一个<u>同态映射</u>.

如果M到$\overline{M}$存在同态满射时，则简称M与$\overline{M}$<u>同态</u>，记为$M \sim \overline{M}$.

例1 令M是数域F上全体n阶方阵作成的集合，代数运算是方阵的普通乘法；再令$\overline{M} = F$，代数运算是数的普通乘法. 则

$$\phi: \qquad A \qquad |A|$$

是M到$\overline{M}$的一个同态映射，且是一个满射.

事实上，ϕ是M到$\overline{M}$的映射是显然的；又任取$a \in \overline{M}$，则

$$A = \begin{matrix} a & & \\ & 1 & \\ & & \ddots \\ & & & 1 \end{matrix} \in M,$$

且$\phi(A) = |A| = a$，即ϕ是满射.

又由于$|AB| = |A| \cdot |B|$，即有

$$\phi(AB) = \phi(A) \cdot \phi(B),$$

故ϕ是M到$\overline{M}$的一个同态满射.

定理1 设集合M与$\overline{M}$分别有代数运算 与 ，且$M \sim \overline{M}$，则

1) 当 满足结合律时， 也满足结合律；

2) 当 满足交换律时， 也满足交换律.

证 用ϕ表示M到$\overline{M}$的一个同态满射.

1) 任取 珑, 珑, 珑$\in \overline{M}$，由于ϕ是满射，可令

$$a \qquad \text{珑}, \qquad b \qquad \text{珑}, \qquad c \qquad \text{珑},$$

又由于ϕ是同态映射，故

$$(a \ b) \ c \qquad \overline{(a \ b)} \ \bar{} \ \text{珑} = (\text{珑} \ \bar{} \ \text{珑}) \ \bar{} \ \text{珑}$$

$$a\ (b\ c)\quad \text{璔}\ (\overline{b\ c})=\text{璔}\ (\text{璔}\ \text{璒}).$$

但 满足结合律，故$(a\ b)\ c=a\ (b\ c)$，从而

$$(\text{璔}\ \text{璔})\ \text{璒}=\text{璔}\ (\text{璔}\ \text{璒}),$$

即 也满足结合律．

2) 类似地，任取 璔, 璔$\in\overline{M}$，且设

$$a\quad \text{璔},\qquad b\quad \text{璔},$$

则有

$$a\quad b\quad \text{璔}\ \text{璔},\qquad b\quad a\quad \text{璔}\ \text{璔}.$$

当 满足交换律时，$a\quad b=b\quad a$，故亦有

$$\text{璔}\ \text{璔}=\text{璔}\ \text{璔},$$

即 也满足交换律．

(证毕)

定理 2 设集合 M 有代数运算 及 ，集合$\overline{M}$有代数运算 及 ；又 φ是 M 到$\overline{M}$的一个满射，且对 与 以及 与 同态，则当 对 满足左(右)分配律时， 对 也满足左(右)分配律．

这个定理的证明方法同定理 1 完全类似，不再重复．

定义 2 设 φ是 M 到$\overline{M}$的一个(关于代数运算 及)同态满射．如果 φ又是单射时，则称 φ是 M 到$\overline{M}$的一个<u>同构映射</u>．

如果集合 M 到$\overline{M}$存在同构映射，就说 M 与$\overline{M}$<u>同构</u>，记为 $M\cong\overline{M}$.否则，即若 M 到$\overline{M}$不存在任何同构映射时，则称 M 与$\overline{M}$<u>不同构</u>．

M 到自身的同态映射，称为 M 的<u>同态映射</u>，或简称 M 的<u>自同态</u>．同样，M 到自身的同构映射，叫做 M 的<u>同构映射</u>，简称为 M 的<u>自同构</u>．

例 2 设 M 是整数集，$\overline{M}$是偶数集，则映射

$$\varphi:\quad n\quad 2n$$

对 M 与$\overline{M}$的普通加法来说，是 M 到$\overline{M}$的一个同构映射，但对于数的普通乘法来说，φ不是 M 到$\overline{M}$的同构映射．

例 3 令 M 是正有理数集，代数运算为普通乘法，则法则

$$\varphi: \quad a \quad \frac{1}{a}$$

是 M 的一个自同构．但对普通加法来说，φ 不是 M 的自同构，因为例如

$$\varphi(2+3)=\varphi(5)=\frac{1}{5},$$

然而 $\varphi(2)+\varphi(3)=\frac{1}{2}+\frac{1}{3}=\frac{5}{6}\neq\frac{1}{5}$，即

$$\varphi(2+3)\neq\varphi(2)+\varphi(3).$$

同构映射是比较两个代数系统的最有力的工具，它在整个近世代数中起着非常重要的作用．

对任意代数系统 M，因为 M 的恒等映射总是 M 到 M 的一个同构映射，即 M 的自同构，故总有 $M\cong M$．其次易知，若代数系统 M_1 与 M_2 同构，且

$$\varphi: \quad x \quad y, \quad \text{即 } \varphi(x)=y \quad (\forall\, x\in M_1)$$

是 M_1 到 M_2 的一个同构映射，则易知 φ 的逆映射

$$\varphi^{-1}: \quad y \quad x, \quad \text{即 } \varphi^{-1}(y)=x \quad (\forall\, y\in M_2)$$

便是 M_2 到 M_1 的一个同构映射．因此，M_2 与 M_1 同构．

又若 M_1 与 M_2 同构，M_2 又与 M_3 同构，且分别设 τ，σ 为它们间的同构映射，则根据映射的合成知，乘积 $\sigma\tau$ 即

$$\sigma\tau(x)=\sigma(\tau(x)) \qquad (\forall\, x\in M_1)$$

是 M_1 到 M_3 的映射且易知是 M_1 到 M_3 的同构映射．因此，$M_1\cong M_3$．

由于同构映射首先是一个双射，因此，相互同构的代数系统有相同的势．特别，当这些代数系统有限时，它们包含的元素个数必相等．

最后，再特别强调一下代数系统同构的意义．

设 $M=\{a,b,c,\cdots\}$ 是一个有代数运算 $\circ$ 的代数系统，而 $\overline{M}=$

{琠,琡,琱,…}是另一个有代数运算 ˉ 的代数系统．如果 $M \cong \overline{M}$，且在这个同构之下如果

$$a \quad 琠, \quad b \quad 琠, \quad c \quad 琱, \quad \cdots$$

则根据同构的定义，$a \quad b = c$ 当且仅当琠 ˉ 琠= 琱. 这就是说，除去元素本身的性质和代数运算名称与所用符号的不同外，从运算的性质看，M 与 $\overline{M}$ 并没有任何实质性的差别．更具体地说，就是由 M 仅根据代数运算所推演出来的一切性质和结论，都可以自动地全部转移到与 M 同构的一切代数系统上去．因此，在近世代数中常把同构的代数系统等同起来，甚至有时候不加区分．这正表现出这门学科所研究的问题的实质所在．

以上的同态映射与同构映射是只对有一个代数运算的代数系统来说的，实际上也可以类推到有两个或两个以上的代数运算的代数系统上去．对此不再赘述．

习题 1.5

1. 设 M 为实数集，代数运算是普通乘法．问：以下各映射是否为 M 的自同态映射？是否为自同态满射和自同构映射？说明理由．

1) $x \quad |x|$, 3) $x \quad x^2$,

2) $x \quad 2x$, 4) $x \quad -x$.

2. 证明本节定理 2．

3. 设 **Q** 是有理数集，代数运算是普通加法．试给出 **Q** 的一个除恒等变换以外的自同构．

4. 设集合 M 有代数运算 ，集合 $\overline{M}$ 有代数运算 ˉ，且 $M \sim \overline{M}$．问：当 ˉ 满足结合律时， 如何？

5. 设 M_1，M_2，M_3 是三个代数系统．证明：

1) 若 $M_1 \cong M_2$，则 $M_2 \cong M_1$；

2) 若 $M_1 \cong M_2$，$M_2 \cong M_3$，则 $M_1 \cong M_3$．

§6 等价关系与集合的分类

研究代数系统，除去同态与同构外，还有另一个经常要用到

的一般方法，就是把代数系统分成若干个子集来加以讨论，这就是集合的分类．它与另一个概念——集合的等价关系有密切的联系．

定义 1　设 M 是一个集合．如果有一个法则 R，它对 M 中任二元素 a，b 可以确定“是”或“不是”符合这个法则，则称此法则 R 为 M 的元素间的一个关系，简称 M 的一个关系．

当元素 a 与 b 符合这一法则时记为 aRb；否则记为 a 与 b 不满足关系 R，记为 $a\not R b$．

例 1　设 M 是有理数集，规定

$$aRb \quad \text{当且仅当} \quad a+b \text{是整数}.$$

这是 M 的一个关系，因为任意两个有理数的和是不是整数，是完全确定的．例如，

$\because 2+\frac{1}{3}=\frac{7}{3}$ 不是整数，　$\therefore 2$ 与 $\frac{1}{3}$ 不满足关系 R；

$\because 2+3=5$ 是整数，　$\therefore 2\ R\ 3$；

$\because \frac{1}{2}+\frac{3}{2}=2$ 是整数，　$\therefore \frac{1}{2}\ R\ \frac{3}{2}$，等等．

例 2　设 M 是实数集，规定

$$aRb \quad \text{当且仅当} \quad a<b.$$

这是 M 的一个关系．例如，

$\because 2<3$，　$\therefore 2\ R\ 3$；

$\because 3\not<2$，　$\therefore 3$ 与 2 不满足关系 R；

$\because 2\not<2$，　$\therefore 2$ 与 2 不满足关系 R，等等．

例 3　设 M 是整数集，规定

$$aRb \quad \text{当且仅当} \quad \frac{a}{b}>0.$$

这不是 M 的一个关系，因为当 $b=0$ 时，$\frac{a}{b}$ 无意义，即不能确定 a 与 0 是或不是符合这一法则．

例 4　设 M 是正有理数集，规定

$$\frac{b}{a} R \frac{d}{c} \qquad \frac{b+d}{a+c} < 1 .$$

这不是 M 的一个关系，因为例如由于

$$\frac{1+3}{2+2} = \frac{4}{4} = 1,$$

故 $\frac{1}{2}$ 瓗 $\frac{3}{2}$. 但是，$\frac{1}{2} = \frac{2}{4}$，而

$$\frac{2+3}{4+2} = \frac{5}{6} < 1,$$

故又有 $\frac{2}{4} R \frac{3}{2}$，即又有 $\frac{1}{2} R \frac{3}{2}$.

这就是说，$\frac{1}{2}$ 与 $\frac{3}{2}$ 是不是符合所规定的法则，是不确定的 .

下面要讨论一种特殊的关系，叫做等价关系 .

定义 2 如果集合 M 的一个关系 R 满足以下条件:

1° 对 M 中任意元素 a 都有 aRa; (反身性)

2° 如果 aRb, 必有 bRa; (对称性)

3° 如果 aRb, bRc, 必有 aRc, (传递性)

则称这个关系是 M 的一个等价关系 .

等价关系常用符号～表示 . 当 $a \sim b$ 时，称 a 与 b 等价 .

由上节末直接可知，同构关系就是所有代数系统间的一个等价关系 .

例 5 法则

$$aRb \qquad a \mid b$$

虽是整数集 Z 的一个关系，但不是等价关系 . 因为虽然反身性与传递性都成立，但对称性不成立，例如 $2 \mid 6$，但 6 8 2 . 即 $2 R 6$，但 6 瓗 2 .

例 6 令 M 为全校学生的集合，规定

$$aRb \qquad a \text{ 与 } b \text{ 同在一系 .}$$

这显然是 M 的一个等价关系 .

例 7 令 Z 是整数集，任意取定一个正整数 n，并规定

$$aRb \qquad a\equiv b(\bmod n),$$

即 a 与 b 同用 n 除其余数相等，这显然是 Z 的一个等价关系 .

定义 3 若把集合 M 的全体元素分成若干互不相交的子集 (即任二互异子集都无公共元素)，则称每个这样的子集叫做 M 的一个类；类的全体叫做 M 的一个 类 .

集合的分类与集合的等价关系间有密切的联系 .

定理 1 集合 M 的一个分类决定 M 的一个等价关系 .

证 对集合 M 的元素规定以下关系：

$$aRb \qquad a \text{ 与 } b \text{ 同在一类} .$$

这显然是 M 的一个等价关系 .

定理 2 集合 M 的一个等价关系决定 M 的一个分类 .

证 下面利用 M 的等价关系～来作出 M 的一个分类 .

任取 $a\in M$，与 a 等价的一切元素作成 M 的一个子集，这个子集记为珚. 由于 $a\sim a$，故

$$a\in 珚;$$

因此，M 中每个元素都一定属于一个类 .

下面再证每个元素只属于一个类 .

设 $a\in 珚$，$a\in 瑚$，则

$$a\sim b,\quad a\sim c .$$

任取 $x\in 珚$，则 $x\sim b$. 于是由上可得

$$b\sim a,\qquad a\sim c,$$

从而 $x\sim c$，即 $x\in 瑚$. 于是珚 瑚.

同理可证瑚 珚. 因此，珚=瑚.

这样，便把 M 的全体元素分成了互不相交的子集，因此，这是 M 的一个分类 .

(证毕)

例 8 求由等价关系

$$aRb \qquad a \equiv b(\mathrm{mod}\ 4)$$

所决定的整数集 Z 的分类.

解 由于任何整数用 4 除所得余数只能是 0, 1, 2, 3, 故由此可得 Z 的一个分类. 它把 Z 分成四个类, 它们是

$$\{\cdots, -8, -4, 0, 4, 8, \cdots\},$$

$$\{\cdots, -7, -3, 1, 5, 9, \cdots\},$$

$$\{\cdots, -6, -2, 2, 6, 10, \cdots\},$$

$$\{\cdots, -5, -1, 3, 7, 11, \cdots\}.$$

如果用 $\bar{r}$ 表示整数 m 所在的类, 则以上四个类可表示成

$$\bar{0},\ \bar{1},\ \bar{2},\ \bar{3},$$

称它们是 4 为模的剩余类(或同余类). 显然, 两个整数 a 与 b 同在一类, 即 $\bar{a}=\bar{b}$ 当且仅当 4 整除 a 与 b 的差.

更一般的, 可讨论以任意正整数 n 为模的剩余类.

这种剩余类在以后各章还将作进一步讨论.

习题 1.6

1. 设 M 为整数集, 规定

$$aRb \qquad 4 \mid a+b.$$

问: R 是否为 M 的一个关系? 是否满足反身性、对称性和传递性?

2. 设 M 是实数集. 问以下各关系是否为 M 的等价关系?

1) $aRb \qquad a \leq b;$ 3) $aRb \qquad a = b;$

2) $aRb \qquad ab \geq 0;$ 4) $aRb \qquad a^2 + b^2 \geq 0.$

3. 试指出上题中等价关系所决定的分类.

4. 分别举出三个例子各满足等价关系中的两个条件, 而另一个条件不满足.

5. 设 M 是任意非空集合, 并令

$$R = \{(a, b) \mid a, b \in M\}.$$

证明：M 的一个关系决定 R 的一个子集；反之，R 的任一个子集决定 M 的一个关系，且不同的关系决定 R 的两个不同的子集．

6. 设 A，B 为集合 M 的任二非空子集，A' 与 B' 分别为 A 与 B 在 M 中的余集．证明：

1) $A - B = A \cap B'$；

2) $(A \cup B) - (A \cap B) = (A - B) \cup (B - A)$

$= (A \cup B) \cap (A' \cup B')$．

7. 设 φ 是集合 X 到集合 Y 的任意一个映射，A 与 B 分别为 X 与 Y 的非空子集．证明：

1) $\varphi^{-1}(\varphi(A)) \quad A$，且当 φ 为单射时等号成立；

2) $\varphi(\varphi^{-1}(B)) \quad B$，且当 φ 为满射时等号成立．

8. 设 φ 是集合 X 到集合 Y 的一个映射，而 A 与 B 是 X 的任二非空子集．证明：

1) $\varphi(A \cup B) = \varphi(A) \cup \varphi(B)$；

2) $\varphi(A \cap B) \quad \varphi(A) \cap \varphi(B)$．

9. 设 σ 与 τ 分别为集合 A 到 B 以及集合 B 到 C 的映射．证明：

1) 若 σ，τ 都是单射，则 $\tau\sigma$ 是单射；反之，若 $\tau\sigma$ 是单射，则 σ 是单射；

2) 若 σ，τ 都是满射，则 $\tau\sigma$ 是满射；反之，若 $\tau\sigma$ 是满射，则 τ 是满射．

10. 设 σ 是集合 A 到集合 B 的一个映射．证明：

1) σ 是单射 存在 B 到 A 的映射 τ，使 $\tau\sigma = 1_A$；

2) σ 是满射 存在 B 到 A 的映射 τ，使 $\sigma\tau = 1_B$．其中 1_A，1_B 分别为集合 A，B 的恒等映射．

11. 设 σ 是集合 A 到集合 B 的一个映射．证明：

1) σ 是单射 对任意集合 X 到 A 的任意映射 τ_1，τ_2，若有 $\sigma\tau_1 = \sigma\tau_2$，必有 $\tau_1 = \tau_2$；

2) σ 是满射 对任意集合 Y 与 B 到 Y 的任意映射 τ_1，τ_2，若有 $\tau_1\sigma = \tau_2\sigma$，必有 $\tau_1 = \tau_2$．

12. 设 A 是一个非空集合，$P(A)$ 是 A 的幂集，即由 A 的一切子集作

成的集合．证明：在 $P(A)$ 与 A 间不存在双射．

提示：反证法．若有双射 φ，可考虑

$$A_1 = \{\varphi(M) \mid M \in P(A), \varphi(M) \notin M\}.$$

第二章　群

群论有着悠久的历史,现在已发展成为一门范围广泛和内容十分丰富的数学分支,在近世代数和整个数学中占有重要地位.

在19世纪初,数学中一个长达三世纪之久而未能解决的难题,即五次和五次以上代数方程的根式解问题,被挪威青年数学家阿贝尔(N.H.Abel,1802～1829)和法国青年数学家伽罗瓦(E.Galois,1811～1832)所彻底解决.从而推动了数学的发展,其重要意义是不言而喻的.但更重要的是,他们在解决这一问题时引入了一种新概念和新思想,即置换群的理论,它对今后数学的发展,特别是代数学的发展起着巨大的关键性的作用.因此可以说,阿贝尔和伽罗瓦是群论和近世代数的真正创始人.

在阿贝尔和伽罗瓦之后,人们逐渐发现,对于这一理论中大多数的本质问题来说,用以构成群的特殊材料——置换——并不重要,重要的只是在于对任意集合里所规定的代数性质的研究,即对于我们上一章所说的代数系统的研究.这样一个现在看起来似乎很平凡的发现,实际上是一个很大的突破,它的重要意义在于把置换群的研究推进到了更一般的抽象群的研究上去.这样便把群的研究建立在公理化的基础上,使它的理论变得更加严谨和清晰,从而为这一理论的进一步蓬勃发展开辟了广阔的前景.

在群的抽象化理论中做出贡献的数学家，主要有凯莱(A．Cayley,1821～1895)、弗罗宾纽斯(F．G．Frobenius,1849～1917)以及柯西(A．L．Cauchy,1785～1857)、若尔当(C Jordan,1838～1922)和西罗(L．Sylow,1832～1918)等人．

这一章主要介绍群的定义、例子、基本性质和一些特殊群类．

§1　群的定义和初步性质

定义1　设 G 是一个非空集合，　是它的一个代数运算，如果满足以下条件：

Ⅰ．结合律成立，即对 G 中任意元素 a，b，c 都有

$$(a\ \ b)\ \ c=a\ \ (b\ \ c);$$

Ⅱ．G 中有元素 e，叫做 G 的左单位元，它对 G 中每个元素 a 都有

$$e\ \ a=a;$$

Ⅲ．对 G 中每个元素 a，在 G 中都有元素 a^{-1}，叫做 a 的左逆元，使

$$a^{-1}\ \ a=e;$$

则称 G 对代数运算　作成一个群．

如果对群 G 中任二元素 a，b 均有

$$a\ \ b=b\ \ a,$$

即 G 的代数运算满足交换律，则称 G 为交换群(可换群)或 Abel 群．否则称 G 为非交换群(非可换群)或非 Abel 群．

例如，显然全体非零有理数以及全体正有理数对于数的普通乘法都作成群，分别称其为　零有理数乘群　　有理数乘群．

但应注意，整数集 **Z** 对于数的普通乘法不能作成群．因为，尽管普通乘法是 **Z** 的代数运算，并且满足结合律，也有左单位元1，但是，除去 ±1 外其他任何整数在 **Z** 中都没有左逆

元．

又显然，数域 F 上全体 n 阶满秩方阵对矩阵的普通乘法(或 F 上 n 维线性空间的全体满秩线性变换对线性变换的乘法)作成一个群，通常称其为 F 上的一般线性群或 F 上的 n 阶线性群，并用 $GL_n(F)$ 表示．

下面再举一些别的例子．

例 1 设 G 为整数集．问：G 对运算

$$a \circ b = a + b + 4$$

是否作成群？

解 由于对任意整数 a，b，显然 $a+b+4$ 为由 a 与 b 惟一确定的整数，故所给运算 $\circ$ 是 G 的一个代数运算．其次，有

$$(a \circ b) \circ c = (a+b+4) \circ c$$
$$= (a+b+4) + c + 4 = a + b + c + 8.$$

同理有 $a \circ (b \circ c) = a + b + c + 8$．因此，对 G 中任意元素 a，b，c 有

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

即代数运算 $\circ$ 满足结合律．

又因为对任意整数 a 均有

$$(-4) \circ a = -4 + a + 4 = a,$$

故 -4 是 G 的左单位元．

最后，由于

$$(-8-a) \circ a = -8 - a + a + 4 = -4,$$

故 $-8-a$ 是 a 的左逆元．

因此，整数集 G 对代数运算 $\circ$ 作成一个群．

例 2 问：由全体正整数作成的集合 G 对运算

$$a \circ b = a^b$$

是否作成群？

解 所给运算显然是全体正整数集合的一个代数运算．但是结合律不成立，因为例如

$$(2\ 1)\quad 2=2^{1}\quad 2=2^{2}=4,$$

$$2\quad (1\ 2)=2\quad 1^{2}=2^{1}=2,$$

从而$(2\ 1)\ 2\neq 2\quad (1\ 2)$.因此,全体正整数集合对这个代数运算不作成群.

对于一个集合,要考察它是否作成群,不仅要注意它的元素是什么,更应注意它的代数运算是什么.因为同一个集合,对这个代数运算可能作成群,而对另一个代数运算却不一定作成群;即使对两个不同的代数运算同时都作成群,那么一般来说,也被认为是两个不同的群.

我们知道,一个群的代数运算叫什么名称或用什么符号表示,这是非本质的.因此,在不致发生混淆时,有时为了方便,也常把群的代数运算叫做"乘法",并且往往还把 $a\ b$ 简记为 $a\cdot b$ 或 ab.

一个群如果只包含有限个元素,则称为有限群;否则称为无限群.

如果一个有限群 G 中所含的元素个数为 n,则称 n 为群 G 的阶,并记为 $|G|=n$.无限群的阶称为无限,被认为是大于任意的正整数.例如,$|G|>1$ 就意味着 G 可能是阶大于 1 的有限群,也可能是无限群.

我们前面所提到的一切群都是无限群,下面再举几个有限群的例子.

例 3　全体 n 次单位根对于数的普通乘法作成一个群.这个群记为 U_n,并称为 n 次单位根群.

事实上,由于任二 n 次单位根的乘积以及 n 次单位根的逆均仍为 n 次单位根,又 1 是 n 次单位根,故 U_n 作成群,而且是一个 n 阶有限交换群.

以后将知道,n 次单位根群是一种很重要的群.

例 4　令

$$G=\{1,i,j,k,-1,-i,-j,-k\},$$

并规定 G 的乘法如下:

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

$$(-x)y=x(-y)=-xy,$$
$$-(-x)=x,$$

其中 $x,\ y\in\{1,i,j,k\}$.

显然 G 对这个乘法封闭(即 G 中任二元素之积仍属于 G),因此,此乘法是 G 的一个代数运算;又 1 是左单位元;每个元素的左逆元也是明显的:因为,1 与 -1 的左逆元均为自身,i 与 $-i$(j 与 $-j$ 以及 k 与 $-k$)互为左逆元 .

因此,要证明 G 对此乘法作成一个群,关键在于验算结合律成立 . 但由乘法表知,因为 i, j, k 三个元素在乘法中地位相当,故只用验算以下诸等式成立即可:

$$(ii)i=i(ii),\quad (ii)j=i(ij),$$
$$(ji)i=j(ii),\quad (ij)i=i(ji),$$
$$(ij)k=i(jk)\ .$$

不难验算这五个等式都成立,故 G 对所规定的乘法作成一个群 . 它是一个 8 阶非交换群 . 通常称这个群为<u>四元数群</u> .

这个群我们以后还要讨论 .

下面来讨论群的一些基本性质 .

定理 1 群 G 的元素 a 的左逆元 a^{-1} 也是 a 的一个右逆元,即有

$$a^{-1}a=aa^{-1}=e\ .$$

证 因为 $a^{-1}\in G$,故 a^{-1} 在 G 中也有左逆元,设为 a',即

$$a'a^{-1}=e\ .$$

由此可得

$$aa^{-1}=e(aa^{-1})=(a'a^{-1})(aa^{-1})$$

$$= a'[(a^{-1}a)a^{-1}] = a'(ea^{-1})$$
$$= a'a^{-1} = e,$$

从而

$$a^{-1}a = aa^{-1} = e.$$

(证毕)

以后称 a^{-1} 为 a 的逆元.

定理 2 群 G 的左单位元 e 也是 G 的一个右单位元，即对群 G 中任意元素 a 均有

$$ea = ae = a.$$

证 因为 $ae = a(a^{-1}a) = (aa^{-1})a = ea = a$，故

$$ea = ae = a.$$

(证毕)

以后称 e 为群 G 的单位元.

定理 3 群 G 的单位元及每个元素的逆元都是惟一的.

证 设 e 与 e' 都是 G 的单位元，则根据单位元的定义，有

$$ee' = e' = e.$$

其次，设 a^{-1} 及 a' 都是 a 的逆元，即有

$$a^{-1}a = aa^{-1} = e,$$
$$a'a = aa' = e.$$

由此进一步得

$$a' = a'e = a'(aa^{-1})$$
$$= (a'a)a^{-1} = ea^{-1} = a^{-1},$$

即 $a' = a^{-1}$，a 的逆元是惟一的.

(证毕)

推论 1 在群中消去律成立，即

$$ab = ac \qquad b = c,$$
$$ba = ca \qquad b = c.$$

这个推论的证明是显然的，因为只需用 a^{-1} 分别从左、右乘二等式两端即得.

下面介绍一种同群有密切关系但比群更广泛的代数系统.

定义 2 设 S 是一个非空集合. 如果它有一个代数运算满足结合律, 则称 S 是一个半群.

如果 S 中有元素 e, 它对 S 中任意元素 a 都有

$$ea = a,$$

则称 e 为半群 S 的一个左单位元; 如果在 S 中有元素 e', 它对 S 中任意元素 a 都有

$$ae' = a,$$

则称 e' 为 S 的一个右单位元.

如果半群 S 有单位元(既是左单位元又是右单位元), 则称 S 为有单位元的半群, 或简称幺半群(monoid).

在一个半群中, 可能既没有左单位元, 也没有右单位元; 可能只有左单位元, 而没有右单位元; 也可能只有右单位元, 而没有左单位元. 但是, 如果既有左单位元又有右单位元, 则二者必相等, 它就是半群的惟一的单位元.

例 5 正整数集对普通乘法作成一个半群, 而且是一个幺半群, 1 是它的单位元.

例 6 正整数集对普通加法作成一个半群, 它既没有左单位元也没有右单位元.

例 7 设 S 是任一非空集合, 对 S 中任意元素 a, b, 规定

$$a \quad b = b$$

则 S 作成一个半群, 而且 S 中每个元素都是左单位元. 但是当 $|S| > 1$ 时, S 没有右单位元.

本节最后介绍两个定理, 它实际上是群定义的另两种形式.

定理 4 设 G 是一个半群, 则 G 作成群的充分与必要条件是:

1) G 有右单位元 e: 即对 G 中任意元素 a 都有

$$ae = a;$$

2) G 中每个元素 a 都有右逆元 a^{-1}：

$$aa^{-1} = e .$$

证　利用定理 1 及定理 2 的结果以及此二定理的类似证法，立即可得．

这个定理说明，在群的定义里，可同时将左单位元改为右单位元并把左逆元改成右逆元．

定理 5　设 G 是一个半群，则 G 作成群的充要条件是，对 G 中任意元素 a，b，方程

$$ax = b,\quad ya = b$$

在 G 中都有解．

证　设 G 作成群，则

$$x = a^{-1}b,\quad y = ba^{-1}$$

显然分别为两个方程的解．

反之，设对 G 中任意元素 a，b，所给两个方程在 G 中都有解．则对 G 中任意一个固定元素 b，设方程 $yb = b$ 在 G 中的解用 e 表示，即有

$$eb = b .$$

再任取 $a \in G$，设方程 $bx = a$ 在 G 中的解为 c，即有

$$bc = a .$$

于是

$$\begin{aligned} ea &= e(bc) = (eb)c \\ &= bc = a, \end{aligned}$$

即 e 是 G 的左单位元．

最后，对 G 中任意元素 a，由于方程

$$ya = e$$

在 G 中有解，即 a 在 G 中有左逆元．

因此，G 作成一个群．

(证毕)

显然，在群中方程 $ax = b$ 与 $ya = b$ 的解都是惟一的．

推论 2 有限半群 G 作成群的充分与必要条件是，在 G 中两个消去律成立．

证 必要性显然，下证充分性，

设 $|G| = n$，且 $G = \{a_1, a_2, \cdots, a_n\}$．今在 G 中任取元素 a，b．由于半群 G 满足消去律，从而易知

$$G = \{aa_1, aa_2, \cdots, aa_n\} \ni b.$$

于是在 G 中必有某 $aa_j = b(1 \leq j \leq n)$，即方程 $ax = b$ 在 G 中有解．

同理可证方程 $ya = b$ 在 G 中也有解．故由定理 5 知 G 作成群．

(证毕)

在推论 2 中，要求半群 G 有限是必要的，因为例如正整数集对乘法作成半群，消去律也成立，但显然它并不作成群．

如果一个交换群 G 的代数运算用加号“ + ”表示时，我们常称其为一个<u>加群</u>．这时的单位元改用 0 表示，并称为 G 的<u>零元</u>；元素 a 的逆元用 $-a$ 表示，并称为 a 的<u>负元</u>．

例如，全体整数对数的普通加法作成一个加群，常称其为<u>整数加群</u>；又如全体有理数，更一般地，任意数环或数域对数的普通加法都作成加群．

但应注意，在一般情况下，我们今后讨论抽象群时，其代数运算不管是否满足交换律却仍用通常的乘号表示或省略这个乘号，并仍称为乘法．

习题 2.1

1. 证明：对群中任意元素 a，b 有

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

又问：$(ab\cdots c)^{-1} = ?$

2. 问：自然数集 N 对运算

$$a \quad b = a + b + ab$$

是否作成半群、幺半群或群？为什么？

3. 令

$$O_n(R) = \{A \mid A \text{ 为 } n \text{ 阶实正交方阵}\}.$$

证明：$O_n(R)$ 对于方阵的普通乘法作成一个群（此群常称为实正交群）.

4. 设 G 是一个群，而 u 是 G 中任意一个固定的元素. 证明：G 对新运算

$$a \quad b = aub$$

也作成一个群.

5. 设 $G = \{(a, b) \mid a, b \text{ 为实数且 } a \neq 0\}$，并规定

$$(a, b) \quad (c, d) = (ac, ad + b).$$

证明：G 对此运算作成一个群. 又问：此群是否为交换群？

6. 证明：如果群 G 的每个元素都满足方程 $x^2 = e$，则 G 必为交换群.

提示：G 中每个元素 $a = a^{-1}$.

§2　群中元素的阶

设 G 是一个群. 由于 G 对乘法满足结合律，因此由第一章可知，在 G 中任意取定 n 个元素 a_1，a_2，…，a_n 后，不管怎样加括号，其结果都是相等的，所以

$$a_1 a_2 \cdots a_n$$

总有意义，它是 G 中一个确定的元素.

下面我们对群中元素引入指数的概念.

任取 $a \in G$，n 是一个正整数，规定

$$a^0 = \mathbf{e}, \quad a^n = \underbrace{aa \cdots a}_{n},$$

$$a^{-n} = (a^{-1})^n = \underbrace{a^{-1} a^{-1} \cdots a^{-1}}_{n}.$$

由此不难推出通常熟知的指数运算规则在群中也成立：

$$a^m a^n = a^{m+n}, \quad (a^m)^n = a^{mn},$$

其中 m，n 为任意整数.

定义 1 设 a 为群 G 的一个元素，使

$$a^n = e$$

的最小正整数 n，叫做元素 a 的阶．

如果这样的 n 不存在，则称 a 的阶为无限(或称是零)．

元素 a 的阶常用 $|a|$ 表示．

由此可知，群中单位元的阶是 1，而其他任何元素的阶都大于 1．

例 1 $G=\{1, -1, i, -i\}$(i 是虚单位)关于数的普通乘法作成一个群，即 4 次单位根群．其中 1 的阶是 1，-1 的阶是 2，i 与 $-i$ 的阶都是 4．

例 2 在正有理数乘群 Q^+ 中，除单位元的阶是 1 外，其余元素的阶均无限．

例 3 在非零有理数乘群 Q^* 中，1 的阶是 1，-1 的阶是 2，其余元素的阶均无限．

定理 1 有限群中每个元素的阶均有限．

证 设 G 为 n 阶有限群，任取 $a\in G$，则

$$a,\ a^2,\ \cdots,\ a^n,\ a^{n+1}$$

中必有相等的．设 $a^s = a^t$，$1 \leq t < s \leq n+1$，则

$$a^{s-t} = e,$$

从而 a 的阶有限．

(证毕)

应注意，无限群中元素的阶可能无限，也可能有限，甚至可能都有限．

例 4 设 U_i(i 是正整数)是全体 i 次单位根对普通乘法作成的群，即 i 次单位根群．现在令

$$U = \bigcup_{i=1}^{\infty} U_i,$$

则由于一个 m 次单位根与一个 n 次单位根的乘积必是一个 mn 次单位根，故 U 对普通乘法作成一个群，而且是一个无限交换群．

这个无限群中每个元素的阶都有限．

定义 2　若群 G 中每个元素的阶都有限，则称 G 为周期群；若 G 中除 e 外，其余元素的阶均无限，则称 G 为无扭群；既不是周期群又不是无扭群的群称为混合群．

由定理 1 知，有限群都是周期群．又例 4 中的群 U 是无限周期群；例 2 中的正有理数乘群 Q^+ 为无扭群，例 3 中的非零有理数乘群 Q^* 为混合群．

定理 2　设群 G 中元素 a 的阶是 n，则

$$a^m = e \qquad n \mid m .$$

证　设 $a^m = e$ 并令

$$m = nq + r,\ 0 \leq r < n . \tag{1}$$

则由于 $a^n = e$，故

$$\begin{aligned} a^m &= a^{nq+r} = (a^n)^q a^r \\ &= a^r = e . \end{aligned}$$

但 $|a| = n$，且 $0 \leq r < n$，故必 $r = 0$．从而由 (1) 知，$n \mid m$．

反之，设 $n \mid m$，且令 $m = nq$，则因 a 的阶是 n，故

$$a^m = (a^n)^q = e .$$

(证毕)

定理 3　若群中元素 a 的阶是 n，则

$$|a^k| = \frac{n}{(k, n)},$$

其中 k 为任意整数．

证　设 $(k, n) = d$，且

$$n = dn_1,\ k = dk_1,\ (n_1, k_1) = 1 . \tag{2}$$

则由于 $|a| = n$，故有

$$\begin{aligned} (a^k)^{n_1} &= a^{kn_1} = a^{nk_1} \\ &= (a^n)^{k_1} = e . \end{aligned}$$

即 $(a^k)^{n_1} = e$．

其次，设 $(a^k)^m = e$，则 $a^{km} = e$．于是由定理 2 知，

$$n \mid km,\ n_1 \mid k_1 m .$$

但$(n_1, k_1) = 1$，故 $n_1 \mid m$．因此，a^k 的阶是 n_1，故由(2)知：

$$|a^k| = n_1 = \frac{n}{(k, n)}.$$

(证毕)

由定理 3 可立得以下二推论．

推论 1 在群中设 $|a| = st$，则 $|a^s| = t$，其中 s，t 是正整数．

证 因为 $|a| = st$，故由定理 3 知，a^s 的阶是

$$\frac{st}{(s, st)} = t,$$

即 $|a^s| = t$．

推论 2 在群中设 $|a| = n$，则

$$|a^k| = n \qquad (k, n) = 1.$$

定理 4 若群中元素 a 的阶是 m，b 的阶是 n，则当 $ab = ba$ 且 $(m, n) = 1$ 时，

$$|ab| = mn.$$

证 首先，由于 $|a| = m$，$|b| = n$，$ab = ba$，故

$$(ab)^{mn} = (a^m)^n (b^n)^m = e;$$

其次，若有正整数 s 使 $(ab)^s = e$，则

$$(ab)^{sm} = (a^m)^s b^{sm}$$

$$= b^{sm} = e,$$

但是 $|b| = n$，故 $n \mid sm$．又因 $(m, n) = 1$，故

$$n \mid s.$$

同理可得 $m \mid s$．再根据 $(m, n) = 1$，故

$$mn \mid s.$$

从而 $|ab| = mn$．

(证毕)

应该十分注意这个定理中的条件 $ab = ba$，因为当 $ab \neq ba$ 时，a 与 b 乘积的阶会出现各种各样的情况．例如，在有理数域上二

阶线性群 $GL_2(Q)$中，易知

$$a=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix},\quad b=\begin{pmatrix}0 & 1\\ -1 & -1\end{pmatrix}$$

的阶都有限，且分别为 4，3，但其乘积

$$ab=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$$

的阶却为无限．这也说明，一般来说一个群 G 的全体有限阶元素对 G 的乘法并不封闭．

又例如，仍在群 $GL_2(Q)$中，易知

$$c=\begin{pmatrix}1 & 2\\ 0 & -2\end{pmatrix},\quad d=\begin{pmatrix}1 & 0\\ 0 & \frac{1}{2}\end{pmatrix}$$

的阶都无限，但其乘积

$$cd=\begin{pmatrix}1 & 1\\ 0 & -1\end{pmatrix}$$

的阶却有限，是 2．

至于定理 4 中的条件$(m, n)=1$，则是明显必要的，因为易知群中任何元素 a 与其逆元 a^{-1} 有相同的阶，但其乘积 e 的阶则是 1．

由此可见，当元素 a 与 b 不满足定理 4 中的假设条件时，其乘积 ab 的阶将无法根据 a，b 的阶来做出判断．

下面再介绍交换群中元素阶的一个性质．

定理 5　设 G 为交换群，且 G 中所有元素有最大阶 m，则 G 中每个元素的阶都是 m 的因数．从而群 G 中每个元素均满足方程 $x^m=e$．

证　设 G 中元素 a 的阶是 m，b 为 G 中任意一个元素，阶为 n．如果 $n\nmid m$，则必存在素数 p 满足以下等式：

$$m=p^k m_1,\quad p\nmid m_1,$$

$$n=p^t n_1,\quad t>k.$$

由于 $|a|=m$，$|b|=n$，故由上面推论 1 知，$|a^{p^k}|=m_1$，$|b^{n_1}|=p^t$．又由于

$$(m_1, p^t)=1,$$

且 G 是交换群，故由定理 4 知：

$$|a^{p^k}b^{n_1}|=p^t m_1 > p^k m_1 = m.$$

这与 m 是 G 中所有元素的最大阶矛盾，因此，$n \mid m$．从而由定理 2 知，群 G 中每个元素都满足方程 $x^m=e$．

（证毕）

本定理中要求 G 为交换群是必要的，因为例如在后面 §6 将看到三次对称群 S_3 就不满足这个定理（S_3 中元素的最大阶是 3，而它有 2 阶元素）．

习题 2.2

1．证明：群中以下每组中的元素有相同的阶：

1）a，a^{-1}，cac^{-1}；2）ab，ba；

3）abc，bca，cab．

2．在有理数域上二阶满秩方阵作成的乘群中，给出元素 a，b 分别满足：

1）$|a|=\infty$，$|b|$ 有限，$|ab|=\infty$；

2）$|a|=\infty$，$|b|$ 有限，$|ab|$ 有限．

3．设 G 是群，且 $|G|>1$．证明：若 G 中除 e 外其余元素的阶都相同，则这个相同的阶不是无限就是一个素数．

4．证明：

1）在一个有限群里，阶数大于 2 的元素的个数一定是偶数．

2）偶数阶群中阶等于 2 的元素的个数一定是奇数．

5．设群 G 中元素 a 的阶为 n．证明：

$$a^s=a^t \qquad n \mid (s-t).$$

6．设群 G 中元素 a 的阶是 mn，$(m,n)=1$．证明：在 G 中存在元素 b，c 使

$$a=bc=cb,\ \text{且}\ |b|=m,\ |c|=n,$$

并且这样的 b, c 还是惟一的.

提示: 利用 $ms+nt=1$, 并令 $b=a^{nt}$.

§3 子 群

子群的概念是群论中一个基本概念, 群论的全部内容都在不同程度上和子群有联系. 特别, 有时要根据子群的各种特征来对群进行分类, 即根据子群来研究群, 这也是研究群的重要方法之一.

定义 1 设 G 是一个群, H 是 G 的一个非空子集. 如果 H 本身对 G 的乘法也作成一个群, 则称 H 为群 G 的一个子群.

如果 $|G|>1$, 则 G 至少有两个子群, 一个是只由单位元 e 作成的子群 $\{e\}$ (以后常简记为 e), 另一个是 G 本身. 这两个子群我们称为 G 的平凡子群. 别的子群, 如果存在的话, 叫做 G 的非平凡子群或真子群.

当 H 是群 G 的子群时, 简记为 $H\leqslant G$; 若 H 是 G 的真子群, 则简记为 $H<G$.

例 1 全体偶数或全体 3 的整倍数, 更一般的, 全体 n 的整倍数 (n 是一个固定整数)

$$\{\cdots,-3n,-2n,-n,0,n,2n,3n,\cdots\}$$

都是整数加群的子群.

例 2 数域 F 上全体 n 阶满秩对角矩阵的集合 G_1 是 F 上一般线性群 $GL_n(F)$ 的一个子群; F 上一切纯量矩阵 aE ($0\neq a\in F$, E 为 n 阶单位方阵.) 的集合 G_2 又是 G_1 的一个子群, 当然也是群 $GL_n(F)$ 的一个子群.

定理 1 设 G 是群, $H\leqslant G$. 则子群 H 的单位元就是群 G 的单位元, H 中元素 a 在 H 中的逆元就是 a 在 G 中的逆元.

证 设 e' 是子群 H 的单位元, e 是群 G 的单位元, 则

$$e'e'=e'=e'e,$$

于是由消去律知，$e'=e$.

同样，若 a'是 a 在 H 中的逆元，a^{-1}是 a 在 G 中的逆元，则

$$a'a=a^{-1}a=e,$$

于是 $a'=a^{-1}$.

(证毕)

要看群的一个子集是不是作成一个子群，由下面定理可知，不必验算群定义中的所有条件 .

定理 2 群 G的一个非空子集 H 作成子群的充分与必要条件是:

1) $a,\ b\in H \qquad ab\in H;$

2) $a\in H \qquad a^{-1}\in H$.

证 设 $H\leq G$, 则 G 的代数运算也是 H 的代数运算，因此，当 $a,\ b\in H$ 时有 $ab\in H$.

其次，当 $a\in H$ 时由定理 1 知，$a^{-1}\in H$.

反之，设 1) 与 2) 两个条件满足，则 1) 说明 G 的代数运算也是 H 的代数运算; 结合律在 G 中成立当然在 H 中也成立; 又根据 2)，当 $a\in H$ 时 $a^{-1}\in H$, 从而再由 1) 得

$$aa^{-1}=e\in H,$$

即 H 中有单位元 e, 且每个元素都有逆元 . 从而 H 是 G 的一个子群 .

(证毕)

我们还可以进一步将定理 2 的两个条件合并成一个条件 .

定理 3 群 G的非空子集 H 作成子群的充分与必要条件是

$$a,\ b\in H \qquad ab^{-1}\in H .$$

证 设 $H\leq G$, 则当 $a,\ b\in H$ 时由定理 2 知，$b^{-1}\in H$, 从而

$$ab^{-1}\in H .$$

反之，设当 $a,\ b\in H$ 时 $ab^{-1}\in H$. 则若 $a\in H$，便有

$$aa^{-1}=e\in H,\quad ea^{-1}=a^{-1}\in H.$$

于是当 $a,\ b\in H$ 时有 $a,\ b^{-1}\in H$，从而

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

故由定理 2 知，$H\leq G$.

(证毕)

这个定理中的条件

$$a,\ b\in H\qquad ab^{-1}\in H$$

显然也可以改写成

$$a,\ b\in H\qquad a^{-1}b\in H.$$

由于消去律在 G 中成立，自然也在 H 中成立，因此由本章§1 推论 2 知，群 G 的有限子集 H 作成子群的充分与必要条件是，H 对 G 的乘法封闭，即

$$a,\ b\in H\qquad ab\in H.$$

例 3 令 G 为数域 F 上行列式等于 1 的全体 n 阶方阵作成的集合．由于

$$|A|=|B|=1\qquad |AB^{-1}|=1,$$

即由 $A,\ B\in G$ 可得 $AB^{-1}\in G$，故 G 作成数域 F 上一般线性群 $GL_n(F)$ 的一个子群．

这个子群常记为 $SL_n(F)$，并称为 F 上的特殊线性群．

定义 2 令 G 是一个群，G 中元素 a 如果同 G 中每个元素都可换，则称 a 是群 G 的一个中心元素．

群 G 的单位元 e 总是群 G 的中心元素，除 e 外可能还有别的中心元素．若群 G 的中心元素只有 e 时，称 G 为无中心群．

交换群的每个元素都是中心元素．另外易知，数域 F 上一般线性群 $GL_n(F)$ 除去单位元外还有别的中心元素(例如纯量矩阵)，但当 $n>1$ 时显然也有非中心元素．

定理 4 群 G 的全体中心元素作成的集合 $C(G)$ 是 G 的一个子群，称为群 G 的中心．

证 因为 $e\in C(G)$，故 $C(G)$ 非空．又设 a，$b\in C(G)$，则对 G 中任意元素 x 都有

$$ax = xa,\quad bx = xb,$$

从而又有 $b^{-1}x = xb^{-1}$．于是有

$$\begin{aligned}(ab^{-1})x &= a(b^{-1}x) = a(xb^{-1})\\ &= (ax)b^{-1} = (xa)b^{-1} = x(ab^{-1}),\end{aligned}$$

故 $ab^{-1}\in C(G)$，从而 $C(G)\leq G$．

（证毕）

群 G 的中心显然是 G 的一个交换子群；又显然 G 是交换群当且仅当 $C(G) = G$．

群 G 的中心在不发生混淆时也常简记为 C．

定义 3 设 A，B 是群 G 的任二非空子集，规定

$$AB = \{ab \mid a\in A, b\in B\},$$

$$A^{-1} = \{a^{-1} \mid a\in A\},$$

并分别称 AB 为 A 与 B 的<u>乘积</u>，A^{-1} 为 A 的<u>逆</u>．

由此易知，对群的任意三个非空子集 A，B，C 均有

$$(AB)C = A(BC),\qquad A(B\cup C) = AB\cup AC$$

$$(AB)^{-1} = B^{-1}A^{-1},\qquad (A^{-1})^{-1} = A.$$

另外，由定理 2 和定理 3 可直接得到以下两个推论．

推论 1 群 G 的非空子集 H 作成子群的充分与必要条件是：

$$HH = H \quad 且 \quad H^{-1} = H.$$

证 设 $H\leq G$，则 $HH = H$ 显然．又若 $a\in H$，则必 $a^{-1}\in H$，从而

$$a = (a^{-1})^{-1}\in H^{-1},$$

故 $H\quad H^{-1}$．类似可证 $H^{-1}\quad H$，故 $H^{-1} = H$．

反之设 $HH = H$，$H^{-1} = H$．则由 $HH = H$ 知 H 对 G 的乘法封闭．另外，若 $a\in H$，则 $a\in H^{-1}$．于是有 $b\in H$ 使

$$a = b^{-1},\qquad a^{-1} = b\in H.$$

于是由定理 2 知，$H \leq G$.

(证毕)

类似有

推论 2 群 G 的一个非空子集 H 作成子群的充分与必要条件是:

$$HH^{-1} = H.$$

特别，群 G 的非空有限子集 H 作成子群的充分与必要条件是:

$$HH = H.$$

以后将会看到，一个群的两个子群的乘积一般不再是子群．但在一定条件下可以是子群．

定理 5 设 H，K 是群 G 的两个子群，则

$$HK \leq G \qquad HK = KH.$$

证 1) 设 $HK \leq G$，则由推论 1 知

$$(HK)^{-1} = HK.$$

但由于 $H^{-1} = H$，$K^{-1} = K$，$(HK)^{-1} = K^{-1}H^{-1} = KH$，从而

$$HK = KH.$$

2) 设 $HK = KH$，则有

$$(HK)(HK)^{-1} = HK \cdot K^{-1}H^{-1} = HKKH$$
$$= HKH = HHK = HK.$$

从而由推论 2 知，$HK \leq G$.

(证毕)

应该注意的是，本定理中的条件 $HK = KH$ 是两个集合的相等，并不是说 H 中的任何元素与 K 中任何元素相乘时可以交换．当然，对于交换群则另当别论．因此，交换群的任二子群之积必仍为子群．

习题 2.3

1. 证明：群 G 的任意个子群的交仍是 G 的一个子群．

2. 设 H 是群 G 的一个非空子集，且 H 中每个元素的阶都有限．证明：$H \leq G$ 当且仅当 H 对 G 的乘法封闭．

3. 证明：交换群中所有有限阶元素作成一个子群．又，对非交换群如何？

4. 证明：一般线性群 $GL_n(F)$ 的中心是一切纯量矩阵 $aE(0 \neq a \in F)$ 作成的子群．

5. 设 G 是群，$H \leq G$，$a \in G$，a^m，$a^n \in H$．证明：若 $(m, n) = 1$，则 $a \in H$．

6. 设 G 是一个阶数大于 2 的群，且 G 的每个元素都满足方程 $x^2 = e$．证明：G 必含有 4 阶子群．

提示：可利用定理 5 及习题 2.1 第 6 题．

7. 证明：任何群都不能是两个真子群的并．

提示：利用反证法．

§4 循 环 群

循环群是一种很重要的群，也是一种已经被完全解决了的一类群．就是说，这种群的元素表达方式和运算规则，以及在同构意义下这种群有多少个和它们子群的状况等等，都完全研究清楚了．

设 M 是群 G 的任意一个非空子集，G 中包含 M 的子群总是存在的，例如 G 本身就是一个．当然，一般来说，G 中可能还有别的子群也包含 M．现在用 $\blacksquare M \blacksquare$ 表示 G 中包含 M 的一切子群的交，则 $\blacksquare M \blacksquare$ 仍是 G 中包含 M 的一个子群，而且 G 中任何一个子群只要包含 M，就必然包含 $\blacksquare M \blacksquare$．所以 $\blacksquare M \blacksquare$ 是群 G 中包含 M 的最小子群．

定义 1 称 $\blacksquare M \blacksquare$ 为群 G 中由子集 M 生成的子群，并把 M 叫做这个子群的生成系．

一个群或子群可能有很多的生成系，甚至可能有无限多个生

成系 .

例如，设 Z 是整数加群，又

$$M=\{-8,4,6,10\},$$

则易知■ M■是偶数加群，而且

$$\{4,6\},\ \{-8,4,10\},\ \{2\},$$

$$\{10,12\},\ \{6,8,10,12,14,\cdots\}$$

等等都是■ M■的生成系 .

当 M 本身是一个子群时，显然■ M■ = M .

下面进一步考察■ M■中的元素是些什么样子 .

任取 $a_i\in M$，由于 M ■ M■，而■ M■是子群，故对任意整数 k_i，必有

$$a_i^{k_i}\in\blacksquare M\blacksquare\ .$$

从而对任意正整数 n，■ M■包含如下的一切元素:

$$a_1^{k_1}\ a_2^{k_2}\cdots a_n^{k_n},\quad a_i\in M,\quad n=1,\ 2,\ \cdots .$$

另一方面，一切这样的元素显然作成一个包含 M 的子群，因此

$$\blacksquare M\blacksquare=\{a_1^{k_1}\ a_2^{k_2}\cdots a_n^{k_n}\mid a_i\in M,\ k_i\in Z,\ n=1,2,\cdots\}\ .$$

集合 M 中的元素可以是无限个，也可以是有限个 . 当

$$M=\{a_1,a_2,\cdots,a_n\}$$

时，把■ M■简记为■ $a_1,a_2,\cdots,a_n$■ . 特别，当 $M=\{a\}$时有

$$\blacksquare M\blacksquare=\blacksquare a\blacksquare\ .$$

定义 2 如果群 G 可以由一个元素 a 生成，即 $G=\blacksquare a\blacksquare$，则称 G 为由 a 生成的一个<u>循环群</u>，并称 a 为 G 的一个<u>生成元</u> .

于是■ a■是由一切形如

$$a^k\quad (k\text{是任意整数})$$

的元素作成的群，亦即

$$\blacksquare a\blacksquare=\{\cdots,a^{-3},a^{-2},a^{-1},a^0,a^1,a^2,a^3,\cdots\}\ .$$

易知，循环群必是交换群 .

若群的代数运算用加号表示时，则由 a 生成的循环群应表为

$$\blacksquare a\blacksquare = \{\cdots, -3a, -2a, -a, 0, a, 2a, 3a, \cdots\}.$$

例 1 整数加群 Z 是无限循环群.

事实上，$1 \in Z$，又对任意整数 n，有

$$n = n \cdot 1,$$

故 $Z = \blacksquare 1\blacksquare$. 即 Z 是一个无限循环群，1 是它的一个生成元. 另易知，-1 也是它的一个生成元.

例 2 n 次单位根乘群 U_n 是一个 n 阶循环群.

事实上，设 ε 是一个 n 次原根，则 ε 是 U_n 的一个生成元，且

$$U_n = \blacksquare \varepsilon\blacksquare = \{1, \varepsilon, \varepsilon^2, \cdots, \varepsilon^{n-1}\}.$$

这 n 个复数是互异的，而对任意整数 k，ε^k 必与这 n 个复数中的一个相等.

定理 1 设群 $G = \blacksquare a\blacksquare$. 则

1) 当 $|a| = \infty$ 时，由 $s \neq t$ 可得 $a^s \neq a^t$，即

$$\cdots, a^{-2}, a^{-1}, e, a^1, a^2, \cdots$$

是 $\blacksquare a\blacksquare$ 的全体互异的元素;

2) 当 $|a| = n$ 时，$\blacksquare a\blacksquare$ 是 n 阶群且

$$\blacksquare a\blacksquare = \{e, a, a^2, \cdots, a^{n-1}\}.$$

证 1) 设 $|a| = \infty$. 则若 $a^s = a^t$，且 $s > t$，便有

$$a^{s-t} = e,$$

这与 $|a| = \infty$ 矛盾.

2) 设 $|a| = n$. 任取 $a^m \in \blacksquare a\blacksquare$，令

$$m = nq + r, \quad 0 \leq r < n.$$

则

$$a^m = a^{nq+r} = (a^n)^q a^r = a^r.$$

从而 $\blacksquare a\blacksquare = \{e, a, a^2, \cdots, a^{n-1}\}$，且易知这 n 个元素是互异的.

(证毕)

推论 1 n 阶群 G 是循环群 $\Leftrightarrow$ G 有 n 阶元素.

证 设 $G = \blacksquare a\blacksquare$ 是 n 阶循环群，则由定理 1 知，生成元 a

的阶是 n.

反之，设 G 有 n 阶元素 a，则易知

$$H=\{e, a, \cdots, a^{n-1}\}$$

是 G 的一个 n 阶子群．但 G 的阶也是 n，故

$$G=H=\langle a\rangle .$$

(证毕)

由此推论可知，n 阶循环群的一个元素是不是生成元，就看这个元素的阶是不是 n.

定理 2 无限循环群 $\langle a\rangle$ 有两个生成元，即 a 与 a^{-1}；n 阶循环群有 $\varphi(n)$ 个生成元，其中 $\varphi(n)$ 为 Euler 函数．

证 当 $|a|=\infty$ 时，$\langle a\rangle$ 只有两个生成元 a 与 a^{-1} 是显然的．

当 $|a|=n$ 时，元素 $a^k\ (0<k<n)$ 是 $\langle a\rangle$ 的生成元当且仅当 a^k 的阶也是 n，亦即 $(k, n)=1$．从而 $\langle a\rangle$ 有 $\varphi(n)$ 个生成元．

(证毕)

例如，4，5，6 阶循环群分别有

$$\varphi(4)=2,\quad \varphi(5)=4,\quad \varphi(6)=2$$

个生成元．

定理 3 设 $\langle a\rangle$ 是任意一个循环群．

1) 若 $|a|=\infty$，则 $\langle a\rangle$ 与整数加群 Z 同构；

2) 若 $|a|=n$，则 $\langle a\rangle$ 与 n 次单位根群 U_n 同构．

证 1) 设 $|a|=\infty$，则当 $m\neq n$ 时 $a^m\neq a^n$，于是

$$\varphi:\quad a^m\quad\quad m$$

是循环群 $\langle a\rangle$ 到整数加群 Z 的一个双射；又由于

$$a^m\cdot a^n=a^{m+n}\quad\quad \langle m+n,$$

故 φ 是 $\langle a\rangle$ 到 Z 的一个同构映射，因此 $\langle a\rangle\cong Z$.

2) 设 $|a|=n$，则

$$\langle a\rangle=\{e, a, a^2, \cdots, a^{n-1}\}.$$

于是易知

τ: a^m ■ε^m (ε为 n次原根)

是循环群■a■到 n 次单位根群 U_n = ■ε■的一个同构映射，因此

■a■ ■ε■ .

(证毕)

由于群间的同构关系具有反身性、对称性和传递性，故此定理说明，凡无限循环群都彼此同构，凡有限同阶循环群都彼此同构．而不同阶的群，由于不能建立双射，当然不能同构．

这样，抽象地看，即在同构意义下，循环群只有两种，即整数加群和 n 次单位根群，这里 n 是任意正整数．

本节最后，我们来讨论循环群的子群．

定理 4 循环群的子群仍为循环群．

证 设 H 是循环群■a■的任一子群．若 $H=\{e\}$，H 当然是循环群．下设 $H\neq\{e\}$．

由于当 $a^m\in H$ 时 $a^{-m}\in H$，故可设 a^m 为 H 中 a 的最小正幂，于是

■a^m■ H .

另一方面，任取 $a^s\in H$，令

$$s=mq+r,\quad 0\leq r<m .$$

则由于 a^s，$a^m\in H$，故

$$a^r = a^{s-mq}$$
$$= a^s\cdot(a^m)^{-q}\in H .$$

但 a^m 是 H 中 a 的最小正幂，故 $r=0$．从而

$$a^s=(a^m)^q\in\blacksquare a^m\blacksquare ,$$

于是又有 H ■a^m■．因此

$$H=\blacksquare a^m\blacksquare ,$$

即子群 H 也是循环群．

(证毕)

定理 5 无限循环群有无限多个子群；当■ a ■为 n 阶循环群时，对 n 的每个正因数 k，■ a ■有且只有一个 k 阶子群，这个子群就是■ $a^{\frac{n}{k}}$ ■ .

证 1) 设 $|a| = \infty$，则易知

$$■e■,\ ■a■,\ ■a^2■,\ \cdots$$

是■ a ■的全部互不相同的子群 . 且除■ e ■外都是无限循环群，从而彼此同构 .

2) 设 $|a| = n$，$k | n$ 且

$$n = kq, \tag{1}$$

则 $|a^q| = k$，从而■ a^q ■是■ a ■的一个 k 阶子群 .

又设 H 也是■ a ■的一个 k 阶子群，则由定理 4，设 $H = ■a^m■$，则 $|a^m| = k$. 但由 §2 知，a^m 的阶是 $\frac{n}{(m, n)}$，故

$$\frac{n}{(m, n)} = k,\quad n = k(m, n) . \tag{2}$$

由(1)式与(2)式得 $q = (m, n)$，$q | m$. 从而

$$a^m \in ■a^q■,\ ■a^m■ \quad ■a^q■ .$$

但由于■ a^q ■与■ a^m ■的阶相同，故

$$H = ■a^q■,$$

即■ a ■的 k 阶子群是惟一的 .

(证毕)

设 n 是大于 1 的整数，且

$$n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$$

为 n 的标准分解式 . 易知 n 共有

$$T(n) = (k_1 + 1)(k_2 + 1)\cdots(k_m + 1)$$

个正因数，这里 $T(n)$ 是 n 的正因数的个数于是由以上定理直接可得以下

推论 2 n 阶循环群有且仅有 $T(n)$ 个子群 .

例如，4，5，6 阶循环群分别有 3，2，4 个子群 .

这样，通过以上两个定理，对循环群的子群的情况，我们也是了解得很清楚的．

习题 2.4

1. 设 $G=\blacksquare a\blacksquare$ 为 6 阶循环群．给出 G 的一切生成元和 G 的所有子群．

2. 设群中元素 a 的阶无限．证明：

$$\blacksquare a^s\blacksquare=\blacksquare a^t\blacksquare \qquad s=\pm t .$$

3. 设群中元素 a 的阶是 n．证明：

$$\blacksquare a^s\blacksquare=\blacksquare a^t\blacksquare \qquad (s,n)=(t,n) .$$

4. 设 a, b 是群 G 中两个有限阶元素且

$$ab=ba,\ (|a|,|b|)=1 .$$

证明：$\blacksquare a,b\blacksquare=\blacksquare ab\blacksquare$．

提示：利用本章§2 定理 4．

5. 设 p 是一个素数，$G_p=\bigcup_{i=1}^{\infty}U_{p^i}$，其中 U_{p^i} 是 p^i 次单位根群．证明：

1) G_p 关于数的普通乘法作成一个群；

2) G_p 的真子群只有 U_{p^i}，$i=1,2,\cdots$．

6. 设 H 是群 G 的一个子群，且 $H\neq G$．又 $M=G-H$ 是 G 关于 H 的余集．证明：$G=\blacksquare M\blacksquare$．

提示：H 中元素可表为 M 中元素之积．

7. 证明：$1,\frac{1}{2},\frac{1}{3!},\cdots,\frac{1}{n!},\cdots$ 是有理数加群的一个生成系．

提示：$\frac{b}{a}=\frac{(a-1)!b}{a!}$．

§5 变 换 群

本节介绍一种同任何群都有密切联系，从而具有广泛意义的群．

设 M 是任意一个非空集合，则由第一章可知，M 的全体变换关于变换的乘法作成一个半群．我们将较为深入地讨论这个半

群的一些重要的子群．

定义 1 设 M 是一个非空集合．则由 M 的若干个变换关于变换的乘法所作成的群，称为 M 的一个变换群；由 M 的若干个双射变换关于变换的乘法作成的群，称为 M 的一个双射变换群；由 M 的若干个非双射变换关于变换的乘法作成的群，称为 M 的一个非双射变换群．

当然，M 的双射变换群与非双射变换群都是 M 的变换群．

例 1 设 $|M|>1$，并取定 $a\in M$．则易知

$$\tau:\quad x\quad \blacksquare a\quad (\forall\, x\in M)$$

是 M 的一个非双射变换，并且 $\tau^2=\tau$．从而 $G=\{\tau\}$ 作成 M 的一个非双射变换群．

至于 M 的双射变换群当然也是存在的．

定理 1 设 M 为任一非空集合，$S(M)$ 为由 M 的全体双射变换作成的集合．则 $S(M)$ 关于变换的乘法作成一个群．

由第一章知道，这个定理的证明是显然的，因为 M 的恒等变换是这个群的单位元，而 M 的任一双射变换 σ 的逆变换 σ^{-1} 也是 M 的双射变换，它是 σ 的逆元．

定义 2 称集合 M 的双射变换群 $S(M)$ 为 M 上的对称群．当 $|M|=n$ 时，其上的对称群用 S_n 表示，并称为 n 次对称群．

显然，M 的任何双射变换群都是 M 上对称群 $S(M)$ 的一个子群，即 M 上的对称群是 M 的最大的双射变换群．另外由第一章可知，n 次对称群 S_n 是一个阶为 $n!$ 的有限群．

定理 2 设 G 是非空集合 M 的一个变换群．则 G 是 M 的一个双射变换群的充分与必要条件是，在 G 中含有 M 的单(满)射变换．

证 必要性显然，下证定理的充分性．

设有 M 的单射变换 $\tau\in G$．因为 G 是群，故必有单位元，用 ε 表示，于是在群 G 中有

$$\varepsilon\tau=\tau\varepsilon=\tau .$$

这样，对 M 中任意元素 a 均有

$$\tau(\varepsilon(a))=\tau\varepsilon(a)=\tau(a) .$$

但 τ 是单射变换，故

$$\varepsilon(a)=a, \qquad (\forall\, a\in M) .$$

因此，ε 是 M 的恒等变换 .

再在 G 中任取元素 σ，因 G 是群，σ 在 G 中有逆元，用 σ^{-1} 表示，它是 M 的一个变换，于是在群 G 中有

$$\sigma\sigma^{-1}=\sigma^{-1}\sigma=\varepsilon .$$

由此可得：若 $\sigma(a)=\sigma(b)\,(a,\ b\in M)$，则有

$$\sigma^{-1}(\sigma(a))=\sigma^{-1}(\sigma(b)),\ \ \varepsilon(a)=\varepsilon(b),$$

从而 $a=b$. 即 σ 是 M 的单射变换 .

又由于 $\sigma(\sigma^{-1}(a))=\varepsilon(a)=a$，即 M 中任意元素 a 在 σ 之下都有逆象 .亦即 σ 又是 M 的满射变换 .因此 σ 是 M 的一个双射变换 . 从而 G 是 M 的双射变换群 .

当 G 含有 M 的满射变换时，可类似证明 .

（证毕）

由此定理显然直接可得

推论 1 设 G 是集合 M 的一个变换群 .则 G 或是 M 的双射变换群（其单位元必是恒等变换），或是 M 的非双射变换群 .

这就是说，在 M 的任意一个变换群中，不可能既含有 M 的双射变换又含有 M 的非双射变换 .

由此显然可知，如果 $|M|>1$，则集合 M 的全体变换的集合 $T(M)$ 只能作成幺半群而不能作成群 .

例 2 设 $M=\{1,2,3,4\}$. 则 M 的以下二变换

$$\alpha=\begin{pmatrix}1&2&3&4\\1&1&3&4\end{pmatrix},\quad \beta=\begin{pmatrix}1&2&3&4\\1&1&4&3\end{pmatrix}$$

作成 M 的一个非双射变换群 .

证 令 $G=\{\alpha,\beta\}$，则易知

$$\alpha^2 = \beta^2 = \alpha,\quad \alpha\beta = \beta\alpha = \beta.$$

因此，G 关于变换的乘法封闭，且 α 是 G 的单位元，α 与 β 的逆元均为自身，故 G 作成群．

又因为 α 与 β 都是 M 的非双射变换，故 G 是 M 的一个非双射变换群．

这是有限集合上的一个非双射变换群．下面再举一个无限集合上的非双射变换群．

例 3 令 $M=\{(x,y)\mid x,\ y$ 为实数$\}$，且对任意实数 a 规定

$$\tau_a:\quad (x,y)\quad (x+a,0),\quad (\forall (x,y)\in M)$$

则 $G=\{\tau_a \mid a$ 为实数$\}$作成 M 的一个非双射变换群．

证 τ_a 显然是 M 的一个非双射变换．又易知

$$\tau_a\tau_b = \tau_{a+b},$$

τ_0 是 G 的单位元，且 τ_a 的逆元是 τ_{-a}，故 G 作成群，从而是 M 的一个非双射变换群．

例 4 设 M 为整数集．现对任意整数 n 规定

$$\tau_n:\quad x\quad x+n\quad (\forall x\in M),$$

并令 $G=\{\tau_n \mid n\in M\}$．则 G 是 M 的一个双射变换群，但非 M 上的对称群．

证 首先易知 τ_n 是 M 的双射变换，故 $G \subset S(M)$．

其次，由于对任意整数 $s,\ t$ 有

$$\tau_s\tau_t(x) = \tau_s(x+t) = x+s+t\quad (\forall x\in M),$$

故 $\tau_s\tau_t = \tau_{s+t}\in G$．又因为

$$\tau_n\tau_{-n}(x) = \tau_{-n}\tau_n(x) = x,$$

故 $\tau_n\tau_{-n} = \tau_{-n}\tau_n = \varepsilon$，即 $\tau_n^{-1} = \tau_{-n}\in G$，故 G 为 M 上对称群 $S(M)$ 的一个子群．从而 G 是 M 的一个双射变换群．

再由于例如 $\tau:\ x\quad -x$ 是 M 的一个双射变换，但易知 $\tau\notin G$，故 G 不是 M 上的对称群．

(证毕)

最后来建立抽象群同变换群之间的联系.

定理 3 (A.Cayley, 1821～1895)任何群都同一个(双射)变换群同构.

证 设 G 是任意一个给定的群，任取 $a\in G$，并令

$$\tau_a: \quad x \quad \blacksquare ax \quad (\forall\, x\in G),$$

则易知 τ_a 是 G 的一个双射变换.

现在令

$$\overline{G}=\{\tau_a \mid a\in G\},$$

则显然

$$\phi: \quad a \quad \blacksquare \tau_a,$$

即 $\phi(a)=\tau_a$ 是 G 到 $\overline{G}$ 的一个双射. 又由于对 G 中任意元素 x 来说，有

$$\begin{aligned}\tau_{ab}(x) &= (ab)x = a(bx)\\ &= a\cdot\tau_b(x) = \tau_a\tau_b(x),\end{aligned}$$

故 $\tau_{ab}=\tau_a\tau_b$，即有

$$\phi(ab)=\phi(a)\phi(b),$$

因此，$G\cong\overline{G}$. 由于 G 是群，故 $\overline{G}$ 也是群，即 G 与双射变换群 $\overline{G}$ 同构.

(证毕)

由这个定理可立即得以下

推论 2 任何 n 阶有限群都同 n 次对称群 S_n 的一个子群同构.

变换群，特别是 n 次对称群，是一种相对具体的群. 以上定理及推论表明，任何一个抽象群都可以找到一个具体的群与它同构. 而同构的群，我们曾说过，除了元素的差别外，就其代数性质，即由代数运算而产生的性质来说，则是完全一致的.

尽管如此，但实践表明，研究这种相对具体的群有时并不比研究一些抽象群来得简单.

习题 2.5

1. 设 $M=\{1,2,3,4\}$，$H=\{\tau,\sigma\}$，其中

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

问：H 关于变换乘法是否作成有单位元半群？是否作成群？

2. 设 M 为正整数集，而

$$\tau:1\quad 1,\ n\quad \blacksquare\ n-1(n>1);\quad \sigma:n\quad \blacksquare\ n+1(n\in M).$$

问：$\tau\sigma$ 与 $\sigma\tau$ 各为何？是否相等？

3. 设 M 为有理数集，又令

$$\tau_{(a,b)}:\ x\quad \blacksquare\ ax+b,\qquad (a,\ b,\ x\in M,\ \text{但}\ a\neq 0).$$

问：$G=\{\tau_{(a,b)}\mid 0\neq a,\ b\in M\}$ 关于变换乘法是否作成群？是 M 的双射变换群还是非双射变换群？

4. 设 $|M|>1$．证明：集合 M 的全体非双射变换关于变换的乘法不能作成群．

5. 证明：对任何固定的正整数 n，互不同构的 n 阶群只有有限个．

提示：利用 Cayley 定理．

§6 置 换 群

置换群是群论中很重要的一类群，前已说过，群论最早就是从研究置换群开始的．利用这种群，伽罗瓦成功地解决了代数方程是否可用根式求解的问题．伽罗瓦在这方面的工作，现在已发展成为代数学中一种专门的理论——伽罗瓦理论．

置换群之所以重要，不仅因为它是最早研究的一类群，而且它是一类重要的非交换群，特别是由上节知，每个有限的抽象群都与一个置换群同构．

这一节我们来讨论这种群的基本性质．

定义 1 n 次对称群 S_n 的任意一个子群，都叫做一个 n 次置换群．简称置换群．

我们在研究有限集合的置换时，这个有限集合中的元素是什

么是无关紧要的．因此，为方便起见，这个集合中的元素常用数码 1，2，…，n 表示，并且一般都假设 $n>1$．

定义 2 一个置换 σ 如果把数码 i_1 变成 i_2，i_2 变成 i_3，…，i_{k-1} 变成 i_k，又把 i_k 变成 i_1，但别的元素(如果还有的话)都不变，则称 σ 是一个 k-循环置换，简称为 k-循环或 环，并表示成

$$\sigma=(i_1\ i_2\cdots i_k)=(i_2\ i_3\cdots i_k\ i_1)=\cdots=(i_k\ i_1\cdots i_{k-1}).$$

例如

$$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=(132)=(321)=(213),$$

$$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=(13)=(31)，\text{等等}.$$

为方便起见，把恒等置换叫做 1-循环，记为

$$(1)=(2)=\cdots=(n).$$

2-循环简称为对换，无公共元素的循环称为不相连循环．

定理 1 不相连循环与不相连循环相乘时可以交换．

证 设 $\sigma=(i_1\ i_2\cdots i_k)$ 与 $\tau=(j_1\ j_2\cdots j_s)$ 为两个不相连的循环，则由变换乘法知，乘积 τσ 与 στ 都是集合 $\{1,2,\cdots,n\}$ 的以下变换：

$$i_1\to i_2，\ i_2\to i_3，\ \cdots，\ i_{k-1}\to i_k，\ i_k\to i_1，$$

$$j_1\to j_2，\ j_2\to j_3，\ \cdots，\ j_{k-1}\to j_k，\ j_k\to j_1，$$

别的元素不动．

因此，$\tau\sigma=\sigma\tau$．

(证毕)

定理 2 每个(非循环)置换都可表为不相连循环之积；每个循环都可表为对换之积，因此，每个置换都可表为对换之积．

证 1) 任何一个置换都可以把构成一个循环的所有元素按连贯顺序紧靠在一起，而把不动的元素放在最后．举例说，例如

$$\begin{pmatrix}1&2&3&4&5&6&7\\3&5&6&4&2&1&7\end{pmatrix}=\begin{pmatrix}1&3&6&2&5&4&7\\3&6&1&5&2&4&7\end{pmatrix}$$

$$=(136)(25).$$

一般的，对任意置换 σ 有

$$\sigma = \begin{matrix} i_1\ i_2 \cdots i_k & \cdots & j_1\ j_2 \cdots j_s & a \cdots b \\ i_2\ i_3 \cdots i_1 & \cdots & j_2\ j_3 \cdots j_1 & a \cdots b \end{matrix}$$

$$= (i_1\ i_2 \cdots i_k) \cdots (j_1\ j_2 \cdots j_s),$$

即置换 σ 表成了不相连循环的乘积。

2) 由置换乘法知：$(1) = (12)(12)$，又

$$(i_1\ i_2 \cdots i_k) = (i_1\ i_k)(i_1\ i_{k-1}) \cdots (i_1\ i_3)(i_1\ i_2).$$

从而定理得证．

(证毕)

用循环和循环的乘积来表示置换，在书写时非常简便．

例 1 S_3 的 6 个元素用循环表示出来就是：

(1)，(12)，(13)，(23)，(123)，(132)．

例 2 S_4 的 24 个元素用循环或循环的乘积表示出来就是：

(1)；

(12)，(13)，(14)，(23)，(24)，(34)；

(123)，(124)，(132)，(134)，(142)，(143)，(234)，(243)；

(1234)，(1243)，(1324)，(1342)，(1423)，(1432)；

$(12)(34)$，$(13)(24)$，$(14)(23)$．

应注意，把一个置换表示成对换的乘积时，表示法不是惟一的．例如

$$\begin{aligned} (132) &= (12)(13) \\ &= (12)(23)(23)(13); \\ (1432) &= (34)(13)(23) \\ &= (23)(12)(14) \\ &= (23)(13)(23)(13)(14). \end{aligned}$$

但是，同一个置换虽然有不同的对换分解，而各分解中对换个数的奇偶性必然相同．

定理 3 每个置换表成对换的乘积时，其对换个数的奇偶性

不变.

证 设置换 σ 可表为 m 个对换 σ_1, σ_2, …, σ_m 之积:

$$\sigma=\sigma_1\sigma_2\cdots\sigma_m,$$

则因为 σ 将排列 $12\cdots n$ 变成排列

$$\sigma(1)\sigma(2)\cdots\sigma(n). \tag{1}$$

又由于 $\sigma=\sigma_1\sigma_2\cdots\sigma_m$, 故连续施用对换 σ_1, σ_2, …, σ_m 于 $12\cdots n$ 也得排列(1). 但由高等代数知, 每施行一次对换都改变排列的奇偶性, 而 $12\cdots n$ 是偶排列, 故 m 与排列(1)的奇偶性一致. 但不论 σ 表示成多少个对换之积, 排列(1)的奇偶性是完全确定的, 因此对换个数 m 的奇偶性不变.

(证毕)

定义 3 一个置换若分解成奇数个对换的乘积时, 称为<u>奇置换</u>; 否则称为<u>偶置换</u>.

由定理 3 知, σ 是奇(偶)置换当且仅当 $\sigma(1)\sigma(2)\cdots\sigma(n)$ 是奇(偶)排列, 即其反序数是奇(偶)数.

由于任何奇置换乘上一个对换后变为偶置换, 而偶置换乘上一个对换后变为奇置换, 故 $n!$ 个 n 次置换中奇偶置换各半, 各为 $\frac{n!}{2}$ 个.

恒等置换是偶置换, 又任二偶置换之积仍为偶置换, 因此, S_n 中全体偶置换作成一个 $\frac{n!}{2}$ 阶的子群, 记为 A_n, 称为<u>n 次交代(交错)群</u>.

n 次对称群 S_n 中的奇、偶置换各占一半, 而交代群 A_n 中的置换全为偶置换. 更一般地, 其实任何置换群中的置换在奇、偶性上均有此特征.

例 3 证明: 一个 n 次置换群中的置换或者全是偶置换, 或者奇、偶置换各占一半.

证 设 G 为任意一个 n 次置换群. 因为 G 必包含恒等置换,

而恒等置换是偶置换，从而 G 必包含有偶置换．

如果 G 中的置换全是偶置换，结论已对；如果 G 含有奇置换，任取其一，设为 σ．并令 A，B 分别为 G 中全体奇、偶置换作成的集合，则由于 σ 与 σ^{-1} 都是奇置换，从而易知

$$\varphi:\ \tau \longmapsto \tau\sigma \quad (\forall\, \tau \in A)$$

是 A 到 B 的一个双射．因此，$|A| = |B|$，即 G 中奇、偶置换的个数相等，各占一半(从而还可知，此时阶 $|G|$ 是偶数)．

(证毕)

例 4 证明：

$$K_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$$

作成交代群 A_4 的一个交换子群．这个群(以及与其同构的群)称为 Klein(C. L. Klein，1849～1925)四元群．

证 显然 K_4 中的置换全为偶置换，而且除恒等置换外其余三个置换的阶都是 2，而且其中任二个相乘等于第三个，即 K_4 对置换的乘法封闭．从而 K_4 是 A_4 的一个子群，且显然是一个交换子群．

(证毕)

关于置换的阶，有以下更一般的判别方法．

定理 4 k-循环的阶为 k；不相连循环乘积的阶为各因子的阶的最小公倍．

证 由直接验算知，当 $1 \leq m < k$ 时有

$$(i_1\ i_2 \cdots i_k)^m = (i_1\ i_{m+1} \cdots) \neq (1),$$

而 $(i_1\ i_2 \cdots i_k)^k = (1)$，故 $(i_1\ i_2 \cdots i_k)$ 的阶是 k．

其次，设 σ_1，σ_2，…，σ_s 分别是阶为 k_1，k_2，…，k_s 的不相连循环，且

$$t = [k_1, k_2, \cdots, k_s],$$

则由于 $k_i \mid t$ 且不相连循环相乘时可以交换，故

$$(\sigma_1\sigma_2\cdots\sigma_s)^t = \sigma_1^t\sigma_2^t\cdots\sigma_s^t = (1)\ .$$

另一方面，设若

$$(\sigma_1\sigma_2\cdots\sigma_s)^r = (1),$$

则同样有

$$\sigma_1^r\sigma_2^r\cdots\sigma_s^r = (\sigma_1\sigma_2\cdots\sigma_s)^r = (1),$$

这只有

$$\sigma_i^r = (1),\quad i=1,\ 2,\ \cdots,\ s.$$

否则由于 σ_1^r，σ_2^r，$\cdots$，σ_s^r 仍是不相连的循环，而不相连循环的乘积不能是(1).

但 σ_i 的阶是 k_i，故 $k_i \mid r$，$i=1,\ 2,\ \cdots,\ s$. 从而

$$t \mid r,$$

即 $\sigma_1\sigma_2\cdots\sigma_s$ 的阶是 $t=[k_1, k_2, \cdots, k_s]$.

（证毕）

根据这个定理，我们可以很容易地来判断一个具体置换的阶是多少. 例如

(24)的阶是 2，　　(153)的阶是 3，

$(24)(153)$的阶是 6，　　$(12)(34)$的阶是 2，

而

$$\begin{matrix}1&2&3&4&5&6\\2&1&4&5&6&3\end{matrix} = (12)(3456)$$

的阶是 4，等等.

定理 5　设有 n 次置换 $\tau=\begin{matrix}1&2&\cdots&n\\i_1&i_2&\cdots&i_n\end{matrix}$，则对任意 n 次置换 σ，有

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

从而当 τ 表成循环的乘积时，把出现在 τ 中各循环中的数码 i 换成 $\sigma(i)$ 后即得 $\sigma\tau\sigma^{-1}$.

证　由于

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

故

$$\sigma\tau=\begin{matrix}1 & 2 & \cdots & n\\ \sigma(1) & \sigma(2) & \cdots & \sigma(n)\end{matrix}\begin{matrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{matrix}$$

$$=\begin{matrix}1 & 2 & \cdots & n\\ \sigma(i_1) & \sigma(i_2) & \cdots & \sigma(i_n)\end{matrix}$$

但是

$$\begin{matrix}\sigma(1) & \sigma(2) & \cdots & \sigma(n)\\ \sigma(i_1) & \sigma(i_2) & \cdots & \sigma(i_n)\end{matrix}\sigma$$

$$=\begin{matrix}\sigma(1) & \sigma(2) & \cdots & \sigma(n)\\ \sigma(i_1) & \sigma(i_2) & \cdots & \sigma(i_n)\end{matrix}\begin{matrix}1 & 2 & \cdots & n\\ \sigma(1) & \sigma(2) & \cdots & \sigma(n)\end{matrix}$$

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

故

$$\sigma\pi\sigma^{-1}=\begin{matrix}\sigma(1) & \sigma(2) & \cdots & \sigma(n)\\ \sigma(i_1) & \sigma(i_2) & \cdots & \sigma(i_n)\end{matrix}.$$

(证毕)

例 5 设 $\sigma=(14)(235)$，$\tau=(153)(24)$．求 $\sigma\pi\sigma^{-1}=?$

解 由定理 5 可知

$$\sigma\pi\sigma^{-1}=(\sigma(1)\sigma(5)\sigma(3))(\sigma(2)\sigma(4))$$

$$=(425)(31).$$

下面来讨论 n 次对称群的中心．

由于一次和二次对称群 S_1 与 S_2 都是交换群，故其中心均为自身．但当 $n\geq 3$ 时，情况就不同了．

定理 6 当 $n\geq 3$ 时，n 次对称群 S_n 的中心为恒等置换，即 S_n 是一个无中心群．

证 设 π 是任意一个 n 次置换且 $\pi\neq(1)$，则必有数码 i 使

$$\pi(i)=j\neq i.$$

又由于 $n\geq 3$，故必有数码 $k\in\{1,2,\cdots,n\}$ 使 $k\neq i$，$k\neq j$．于是令 $\sigma=(jk)$，则

$$\pi\sigma(i)=j,\qquad \sigma\pi(i)=k,$$

即 $\pi\sigma(i)\neq\sigma\pi(i)$，因此 $\pi\sigma\neq\sigma\pi$．亦即任何异于恒等置换的置换都不是 S_n 的中心元素，故 S_n 是一个无中心群．

（证毕）

本节最后，我们来介绍在置换群理论中占特殊地位的一类群——传递群．

定义 4 设 G 是集合 $M=\{1,2,\cdots,n\}$ 上的一个置换群．如果对 M 中任意两组 k 个互异数码 i_1，i_2，$\cdots$，i_k 与 j_1，j_2，$\cdots$，j_k $(1\leq k\leq n)$，在 G 中都有置换 τ 使

$$\tau(i_1)=j_1,\qquad \tau(i_2)=j_2,\quad\cdots,\quad \tau(i_k)=j_k,$$

则称 G 为一个 k 重传递（可迁）群．

1 重传递群，即对 M 中任意数码 i 与 j 在 G 中都有置换 τ 使

$$\tau(i)=j$$

时，则简称 G 为传递群或可迁群．

显然，一个 k 重传递群 $(2\leq k\leq n)$ 必是一个 $k-1$ 重传递群．

又显然 S_n 为 n 重传递群，Klein 四元群 K_4 为传递群．但是，4 次置换群

$$H=\{(1),(14)\}$$

不是传递群，因为例如在 H 中没有置换把数码 1 变为数码 2．

定理 7 $M=\{1,2,\cdots,n\}$ 上置换群 G 是 $k(1\leq k\leq n)$ 重传递群的充要条件是，对 M 中任意 k 个互异的数码 j_1，j_2，$\cdots$，j_k 在 G 中有置换 τ 使

$$\tau(1)=j_1,\quad \tau(2)=j_2,\quad\cdots,\quad \tau(k)=j_k\ .\qquad (2)$$

证 必要性显然，下证充分性．

设条件成立．则对 M 中任意 k 个互异数码 i_1，i_2，$\cdots$，i_k 在 G 中有置换 σ 使

$$\sigma(1)=i_1,\quad \sigma(2)=i_2,\quad\cdots,\quad \sigma(k)=i_k\ .\qquad (3)$$

从而 $\tau\sigma^{-1}\in G$ 且由式(2)与式(3)知:

$$\tau\sigma^{-1}(i_1)=j_1,\quad \tau\sigma^{-1}(i_2)=j_2,\quad \cdots,\quad \tau\sigma^{-1}(i_k)=j_k.$$

因此，G 为 k 重传递群.

(证毕)

在本定理中，显然可把(2)式中的 1，2，…，k 换成 M 中任意 k 个固定的数码.

当 $k=1$ 时由定理 7 即得

推论 M 上置换群 G 是传递群，当且仅当对 M 中任意数码 j 有 $\tau\in G$ 使

$$\tau(1)=j.$$

例 6 当 $n\geq 3$ 时，交代群 A_n 是一个 $n-2$ 重传递群.

证 在 $M=\{1,2,\cdots,n\}$ 中任取 $n-2$ 个互异数码 j_1，j_2，…，j_{n-2}，则由于对换改变排列的奇偶性，因此总可以在 M 中选取数码 j_{n-1}，j_n 使

$$\tau=\begin{matrix}1 & 2 & \cdots & n-2 & n-1 & n\\ j_1 & j_2 & \cdots & j_{n-2} & j_{n-1} & j_n\end{matrix}$$

为偶置换，即 $\tau\in A_n$ 且显然有:

$$\tau(1)=j_1,\quad \tau(2)=j_2,\quad \cdots,\quad \tau(n-2)=j_{n-2}.$$

因此，A_n 是一个 $n-2$ 重传递群.

(证毕)

多重传递群是置换群理论中重要研究课题之一. 除去 S_n 和 A_n 外，有大量的 2 重和 3 重传递群早已为人们所熟知. 1861 年及 1873 年法国数学家马提厄(E. Mathieu, 1835～1890)发现了四个 4 重传递群，后人称为马提厄群，并分别用 M_{11}，M_{12}，M_{23}，M_{24} (M_{11} 表示为 11 次置换群, 其余同)表示，其中

$$|M_{11}|=7920,$$

而其余三个的阶更大. 另外，M_{12} 和 M_{24} 还是两个 5 重传递群，而且也是仅有的两个已知的(除 S_n, A_n 以外)5 重传递群. 1981 年有限单群分类问题解决后，利用这些结果不仅弄清楚了全部的

2 重传递群，而且还证明了上述的四个马提厄群是除 S_n，A_n 以外的全部 4 重传递群．但是，已经证明没有 6 重传递群(除 S_n，A_n 外)，从而也没有 6 重以上的传递群．

习题 2.6

1. 给出三次对称群 S_3 的所有真子群，并利用§3 推论 2 和本节例 3 说明理由．

2. 1) 设置换 $\sigma=\sigma_1\sigma_2\cdots\sigma_k$(每个 σ_i 都是对换)．问：$\sigma^{-1}=?$ 再由此说明置换 σ 与 σ^{-1} 有相同的奇偶性．

2) 证明：循环 $(i_1\ i_2\cdots i_k)$ 的奇偶性与 k 的奇偶性相反．

3. 证明：

1) $(i_1\ i_2\cdots i_k)^{-1}=(i_k i_{k-1}\cdots i_2\ i_1)$；

2) $\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix}^{-1}=\begin{pmatrix}i_1 & i_2 & \cdots & i_n\\ 1 & 2 & \cdots & n\end{pmatrix}$．

4. 试求下列各置换的阶：

$$\tau_1=(1378)(24);\qquad \tau_2=(1372)(234);$$

$$\tau_3=\begin{pmatrix}1&2&3&4&5&6\\6&4&1&5&2&3\end{pmatrix};\qquad \tau_4=\begin{pmatrix}1&2&3&4&5&6&7\\5&7&6&3&1&4&2\end{pmatrix}.$$

5. 设 $\tau=(327)(26)(14)$，$\sigma=(134)(57)$．试求

$$\sigma\tau\sigma^{-1}=?\qquad \sigma^{-1}\tau\sigma=?$$

6. 证明：$H=\{(1),(12),(34),(12)(34)\}\leq S_4$．又问：$H$ 是否为传递群？

7. 先用循环或循环之积写出 6 阶循环群 $G=\blacksquare(123456)\blacksquare$ 的全部元素，再指出 G 是一个传递群但不是 2 重传递群．

§7 陪集、指数和 Lagrange 定理

陪集和指数是群的理论中最基本的概念，它们和群的阶之间有着密切的联系，这就是著名的 Lagrange 定理．

定义 1 设 H 是群 G 的一个子群，$a\in G$．则称群 G 的子集

$$aH=\{ax\mid x\in H\}$$

为群 G 关于子群 H 的一个左陪集．而称

$$Ha=\{xa\mid x\in H\}$$

为群 G 关于子群 H 的一个右陪集．

由此可知，不管是左陪集或右陪集，它们都是群的一种特殊的子集．也就是这种特殊的子集在群的讨论中占着很重要的地位．

例如，$H=\{(1),(12)\}$ 是三次对称群 S_3 的一个子群，而

$$(13)H=\{(13),(123)\},\qquad (23)H=\{(23),(132)\}$$

是 H 的两个左陪集；又

$$H(13)=\{(13),(132)\},\qquad H(23)=\{(23),(123)\}$$

是 H 的两个右陪集．

从这里还可以看出，左陪集 aH 与右陪集 Ha 一般并不相等．但有时也可能相等，特别当 G 是交换群时一定相等．

我们下面只讨论左陪集，对右陪集可作类似的讨论．

左陪集有以下一些今后经常用到的重要性质．

1) $a\in aH$．

证　因为 H 是子群，$e\in H$，故

$$a=ae\in aH.$$

2) $a\in H\quad\Leftrightarrow\quad aH=H$．

证　设 $aH=H$．则由 1) 知，$a\in aH$，故 $a\in H$．

反之，设 $a\in H$．任取 $ax\in aH$，$x\in H$，但 H 是子群，故 $ax\in H$．从而 $aH\subseteq H$；

又任取 $x\in H$．由于 $a\in H$，故 $a^{-1}x\in H$，且

$$x=a(a^{-1}x)\in aH.$$

从而又有 $H\subseteq aH$．因此

$$aH=H.$$

3) $b\in aH\quad\Leftrightarrow\quad aH=bH$．

证 设 $b\in aH$. 令 $b=ax(x\in H)$, 则由 2) 有

$$bH=axH=aH.$$

反之, 设 $aH=bH$. 则因 $b\in bH$, 故

$$b\in aH.$$

4) $aH=bH$, 即 a 与 b 同在一个左陪集中 $a^{-1}b\in H$ (或 $b^{-1}a\in H$).

证 设 $aH=bH$, 则

$$a^{-1}aH=a^{-1}bH,\quad H=a^{-1}bH.$$

于是由 2) 知, $a^{-1}b\in H$.

反之, 若 $a^{-1}b\in H$, 则依上倒推回去即得 $aH=bH$.

应注意, 把 3)与 4)两条合起来,就是

$b\in aH$, 即 a, b 属于同一个左陪集 $aH=bH$

$$a^{-1}b\in H(b^{-1}a\in H)$$

5) 若 $aH\cap bH\neq$, 则 $aH=bH$.

证 设 $c\in aH\cap bH$, 则 $c\in aH$, $c\in bH$. 于是由 3)知

$$aH=bH=cH.$$

这个性质表明, 对任二左陪集来说, 要么相等, 要么无公共元素(即其交为空集).

这样, 群 G 中每个元素必属于一个左陪集(即 1)), 而且不能属于不同的左陪集(即 5)). 因此, G 的全体不同的左陪集构成群 G 的元素的一个分类, 而且两个元素 a 与 b 同在一类当且仅当 $a^{-1}b\in H$.

如果用 aH, bH, cH, …表示子群 H 在群 G 中的所有不同的左陪集, 则有等式

$$G=aH\cup bH\cup cH\cup\cdots,$$

称其为群 G 关于子群 H 的左陪集分解. 而称$\{a,b,c,\cdots\}$为 G 关于 H 的一个左陪集代表系.

应注意, 子群 H 本身是 G 的一个左陪集, 但 G 的任何别的左陪集由于都没有单位元, 当然都不是 G 的子群.

同样可讨论群 G 的右陪集和群的右陪集分解．但应注意，性质 4)对于右陪集应改为：

4′) $Ha = Hb$ $ab^{-1} \in H$(或 $ba^{-1} \in H$)．

群 G的左陪集和右陪集有以下关系．

定理 1 设 H 是群 G 的一个子群，又令

$$L = \{aH \mid a \in G\}, \quad R = \{Ha \mid a \in G\}.$$

则在 L 与 R 之间存在一个双射，从而左、右陪集的个数或者都无限或者都有限且个数相等．

证 在 L 与 R 之间建立映射：

$$\varphi: \quad aH \quad Ha^{-1}.$$

如果 $aH = bH$，则 $a^{-1}b \in H$，即 $a^{-1}(b^{-1})^{-1} \in H$，从而由 4′)知，

$$Ha^{-1} = Hb^{-1}.$$

反之，若 $Ha = Hb$，可同样推出 $a^{-1}H = b^{-1}H$．即 φ为双方单值，从而为双射．

(证毕)

根据此定理的证明可知，由 G的左陪集分解

$$G = aH \cup bH \cup cH \cup \cdots$$

可立即得到 G的一个相应的右陪集分解：

$$G = Ha^{-1} \cup Hb^{-1} \cup Hc^{-1} \cup \cdots.$$

这就是说，当$\{a, b, c, \cdots\}$是 G 关于 H 的一个左陪集代表系时，则$\{a^{-1}, b^{-1}, c^{-1}, \cdots\}$必然是 G 关于 H 的一个右陪集代表系．

例 1 取 S_3 的子群 $H = \{(1), (12)\}$，则

$(1)H = \{(1), (12)\}$, $H(1) = \{(1), (12)\}$,

$(13)H = \{(13), (123)\}$, $H(13) = \{(13), (132)\}$,

$(132)H = \{(132), (23)\}$, $H(123) = \{(123), (23)\}$.

于是

$$S_3 = H \cup (13)H \cup (132)H$$

$$= H \cup H(13) \cup H(123),$$

它们分别是 S_3 关于子群 H 的左、右陪集分解．而$\{(1),(13),(132)\}$与$\{(1),(13),(123)\}$分别为 S_3 关于 H 的左、右陪集代表系．但显然

$$H \cup (13)\, H \cup (132)\, H \neq H \cup H(13) \cup H(132)\ .$$

定义 2 群 G 中关于子群 H 的互异的左(或右)陪集的个数，叫做 H 在 G 里的指数，记为

$$(G : H)\ .$$

例如，在例 1 中有$(S_3 : H) = 3$．

定理 2 设 H，K 是群 G 的两个子群．则群 G 关于交 $H \cap K$ 的所有左陪集，就是关于 H 与 K 的左陪集的所有非空的交．

证 设 $c(H \cap K)$ 为 G 关于交 $H \cap K$ 的任一左陪集，则易知

$$c(H \cap K) = cH \cap cK\ .$$

故关于交 $H \cap K$ 的任一左陪集都是关于 H 与 K 的二左陪集的交．

反之，任取 H 与 K 的二左陪集 aH 与 bK，且

$$aH \cap bK \neq \quad .$$

令 $c \in aH \cap bK$，则 $c \in aH$，$c \in bK$，于是由陪集性质 3)知：

$$aH = cH, \qquad bK = cK\ .$$

从而

$$aH \cap bK = cH \cap cK = c(H \cap K)\ .$$

这样，关于交 $H \cap K$ 的所有左陪集就是关于 H 与 K 的左陪集的所有非空的交．

(证毕)

从这个定理直接可知，当$(G : H)$与$(G : K)$都有限时，不仅$(G : H \cap K)$有限，而且有

$$(G : H \cap K) \leq (G : H) \cdot (G : K)\ .$$

于是有

推论 1 (J.H.Poincar，1854～1912) 设 H，K 是群 G 的

两个子群，则当指数$(G:H)$与$(G:K)$都有限时，指数$(G:H\cap K)$也有限．

利用数学归纳法，不难把定理 2 和推论 1 推广到有限个子群的情形上去．

关于子群的阶、指数和群的阶之间，存在着如下极其重要的关系．

定理 3　(J.L.Lagrange, 1736～1813)　设 H 是有限群 G 的一个子群，则

$$|G| = |H|(G:H).$$

从而任何子群的阶和指数都是群 G 的阶的因数．

证　令$(G:H)=s$，且

$$G = a_1H \cup a_2H \cup \cdots \cup a_sH \tag{1}$$

是 G 关于 H 的左陪集分解．由于易知

$$\phi: \quad a_ih \qquad a_jh \qquad (h\in H)$$

是左陪集 a_iH 到 a_jH 的一个双射，从而

$$|a_iH| = |a_jH|.$$

于是

$$|a_1H| = \cdots = |a_sH| = |H|.$$

因此由(1)式知，$|G| = |H|\cdot s$，即

$$|G| = |H|(G:H).$$

(证毕)

推论 2　有限群中每个元素的阶都整除群的阶．

证　设 a 是有限群 G 的一个 n 阶元素，则

$$H = \{e, a, \cdots, a^{n-1}\}$$

是 G 的一个 n 阶子群，故由定理 3 知，$n \mid |G|$．

(证毕)

例 2　由于$|S_3| = 6$，故三次对称群 S_3 的子群及元素的阶都是 6 的因数．例如，子群

$$H=\{(1),(12)\}$$

的阶是 2，指数是 3，且有 $|S_3|=|H|(S_3:H)$，即 $6=2\cdot 3$．

子群的指数还有以下重要的基本关系．

定理 4 设 G 是一个有限群，又 $K\leq H\leq G$，则

$$(G:H)(H:K)=(G:K)\ . \tag{2}$$

证 由 Lagrange 定理知

$$|G|=|H|\cdot(G:H)=|K|\cdot(G:K),$$

且 $|H|=|K|\cdot(H:K)$．将此代入上式并消去 $|K|$，即得(2)．

(证毕)

在此定理中，当 $K=\{e\}$ 时即得 Lagrange 定理．因此，公式(2)可视为 Lagrange 定理的一种推广．另外，若当 G 为无限群而且 $A=\{a_1,a_2,\cdots\}$ 与 $B=\{b_1,b_2,\cdots\}$ 分别为 G 关于 H 和 H 关于 K 的左陪集代表系时，则可以证明

$$AB=\{a_ib_j\mid a_i\in A,b_j\in B\}$$

是 G 关于 K 的一个左陪集代表系．因此，$(G:K)$ 无限当且仅当 $(G:H)$ 与 $(H:K)$ 中至少有一个是无限的．这样，此时也可以认为公式(2)是正确的．

作为陪集分解的一个应用，我们来证明

定理 5 设 H，K 是群 G 的两个有限子群，则

$$|HK|=\frac{|H|\cdot|K|}{|H\cap K|}\ .$$

证 由于 $H\cap K\leq H$，设 $\dfrac{|H|}{|H\cap K|}=m$，且

$$H=h_1(H\cap K)\cup h_2(H\cap K)\cup\cdots\cup h_m(H\cap K),$$

$$h_i\in H,\qquad h_i^{-1}h_j\notin K,\quad i\neq j\ .$$

易知

$$HK=h_1K\cup h_2K\cup\cdots\cup h_mK,$$

$$h_iK\cap h_jK=\quad,\quad i\neq j,$$

从而 $|HK|=m|K|$，即

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

(证毕)

应该注意的是，尽管有以上等式，但乘积 HK 仍然不一定是子群.

由此定理可知，当且仅当子群 H 与 K 的交是单位元时才有

$$|HK| = |H| \cdot |K|.$$

推论 3　设 p，q 是两个素数且 $p < q$，则 pq 阶群 G 最多有一个 q 阶子群.

证　设 H，K 都是 G 的 q 阶子群，则由定理 5 知，

$$|HK| = \frac{q^2}{|H \cap K|},$$

但 $|H \cap K|$ 整除 q，而 q 是素数，故

$$|H \cap K| = 1 \text{ 或 } q.$$

若 $|H \cap K| = 1$，则由 $q > p$ 知：$|HK| = q^2 > pq = |G|$，不可能. 故 $|H \cap K| = q$，从而 $H = K$.

(证毕)

以后将知道，这样的群必有 q 阶子群. 从而这样的群有且仅有一个 q 阶子群.

由此推论知，6 阶群最多有一个 3 阶子群(实际是有且仅有一个 3 阶子群)，10 与 15 阶群都最多有一个 5 阶子群(实际上也是有且仅有一个 5 阶子群)，等等.

另外，尽管这种群的 q 阶子群有且仅有一个，然而其 p 阶子群却可能有很多个. 例如，$|S_3| = 2 \cdot 3$，但群 S_3 的 2 阶子群却有三个.

习题　2.7

1. 设 G 为 n 阶有限群. 证明：G 中每个元素都满足方程 $x^n = e$.

2. 写出三次对称群 S_3 关于子群 $H = \{(1), (23)\}$ 的所有左陪集和所有

右陪集.

3. 设 H, K 分别为群 G 的两个 m 与 n 阶子群. 证明: 若 $(m, n) = 1$, 则 $H \cap K = \{e\}$.

4. 证明: p^m (p 是素数, m 为正整数) 阶群必含有 p 阶元, 而且 p 阶元的个数是 $p - 1$ 的倍数.

5. 设 G 是群, $K \leq H \leq G$, 又 $A = \{a_1, a_2, \cdots\}$ 与 $B = \{b_1, b_2, \cdots\}$ 分别为 G 关于 H 和 H 关于 K 的左陪集代表系. 证明: $AB = \{a_i b_j \mid a_i \in A, b_j \in B\}$ 是 G 关于 K 的一个左陪集代表系.

6. 试给出三次对称群 S_3 的所有子群, 并利用 Lagrange 定理说明理由.

7. 证明: 四元数群的真子群只有 4 个:

$$\langle -1 \rangle, \quad \langle i \rangle, \quad \langle j \rangle, \quad \langle k \rangle.$$

8. 设 A, B, C 是群 G 的三个子集. 证明:

$$A(B \cup C) = AB \cup AC.$$

问: $A(B \cap C) = AB \cap AC$ 是否成立? 当 A, B, C 都是子群时又如何?

9. 设 G 是群, 且 $|G| = p^t m$, p 是素数, $p \nmid m$. 又 H, K 分别是 G 的 p^t, p^s ($0 < s \leq t$) 阶子群且 $K \not\subseteq H$. 证明: HK 不是 G 的子群.

提示: 反证法并利用 §7 定理 5.

10. 设 G 是数域 F 上某些 n 阶方阵对于方阵的普通乘法作成的群. 证明: G 中的方阵或者全是满秩的, 或者全是降秩的.

提示: 可利用 §1 定理 5.

11. 证明: 分式的集合

$$G = \left\{ x, \ \frac{1}{x}, \ 1 - x, \ \frac{1}{1 - x}, \ \frac{x - 1}{x}, \ \frac{x}{x - 1} \right\}$$

对运算

$$a \circ b = \text{把 } b \text{ 代入 } a \text{ 中的 } x \qquad (\forall\, a, b \in G)$$

作成一个群.

12. 设 a, b 是群 G 中阶分别为 m 与 n 的两个元素. 证明: 若 $ab = ba$, 则

$$|ab| \mid [m, n],$$

且 G 中有阶为 $[m, n]$ (m 与 n 的最小公倍) 的元素.

提示: 给出 m, n 的标准分解式并利用 §2 定理 4.

13. 设■a^s■与■a^t■是循环群■a■的两个子群，s与t为自然数，证明：

1) ■a^s■∩■a^t■ = ■$a^{[s,t]}$■；

2) ■a^s■■a^t■ = ■$a^{(s,t)}$■ .

其中$[s,t]$是s，t的最小公倍，(s,t)是s，t的最大公约 .

14. 证明：群G是有限群当且仅当G只有有限个子群 .

15. 设H，K是群G的子群，证明：

1) $(H:H\cap K)\leq(G:K)$；

2) 当$(G:K)$有限时，则$(H:H\cap K)=(G:K)$当且仅当$G=HK$.

提示：$h(H\cap K)$　　$hK(h\in H)$是单射 .

16. 设G是一个$2n$阶有限交换群，其中n是一个奇数 . 证明：G有且只有一个2阶元素 .

17. 设H是群G的一个周期子群，且$(G:H)$有限 . 证明：G是周期群 .

提示：考虑元素a，a^2，a^3，… .

18. 证明：15阶交换群必为循环群 .

19. 设e是幺半群S的单位元，又a，$b\in S$. 证明：a是以b为逆元的可逆元当且仅当

$$aba=a,\qquad ab^2a=e .$$

20. 证明：无限循环群的非e子群的指数均有限 .

21. 举出一个无限群，其任何真子群的指数均无限 .

22. 证明：四次交代群A_4无6阶子群 .

23. 设G是$M=\{1,2,\cdots,n\}$上的一个置换群，又$i\in M$. 令

$$G_i=\{\tau\mid\tau\in G,\tau(i)=i\},\qquad G(i)=\{\tau(i)\mid\tau\in G\} .$$

证明：1) $G_i\leq G$；

2) 若s，$t\in G(i)$，则有$\sigma\in G$使$\sigma(s)=t$；

3) $|G|=|G_i|\cdot|G(i)|$.

24. 设G,M如上题 .又令A　M且

$$G_A=\{\tau\mid\tau\in G,\text{对每个 }i\in A\text{ 都有 }\tau(i)=i\},$$

$$G^A=\{\tau\mid\tau\in G,\text{对每个 }i\in A\text{ 都有 }\tau(i)\in A\} .$$

证明：$G_A\leq G^A\leq G$.

25. 证明：以下的 M_1 与 M_2 都是 n 次对称群 S_n 的生成系：

1) $M_1=\{(12),(13),\cdots,(1n)\}$；

2) $M_2=\{(12),(12\cdots n)\}$.

提示：令 $\tau=(12)$，$\sigma=(12\cdots n)$，则可证：

$\sigma^k\tau\sigma^{-k}=(k+1,k+2)$或$(j,j-1)(j-1,j-2)\cdots(i+2,i+1)\in\langle\tau,\sigma\rangle$；

再指出$\langle\tau,\sigma\rangle$包含所有对换.

26. 设有一正三角形$\triangle ABC$，中心为 O，现使它在空间中运动，但运动之前后仍占有同一空间位置. 问：这样的运动(包括正三角形不动的运动)共有多少个？它与 $M=\{A,B,C\}$ 上的三次对称群有何关系？

第三章　正规子群和群的同态与同构

正规子群是一种特殊的子群，它在整个群的讨论中起着非常重要的作用．把正规子群与群的同态和同构结合起来，可以得到群论中最基本最重要的一些结果．

本章还介绍在有限群论中占有重要地位的 Sylow 定理和有限交换群基本定理．

§1　群同态与同构的简单性质

我们在研究群时，经常需要对不同的群来进行比较．群的同态，特别是同构，是比较群的最重要最有力的方法．

群是具有一个代数运算的代数系统，因此，在第一章里所介绍的有关代数系统的同态与同构的概念，自然可以转移到群的同态与同构上去．但是，为了强调这一概念在群的讨论中的重要性，我们有必要对这些概念再作重新的回忆和强调．

设 G 与 $\bar{G}$ 是两个群．如果有一个 G 到 $\bar{G}$ 的映射 φ 满足

$$\varphi(ab)=\varphi(a)\varphi(b)\qquad(\forall\ a,b\in G),$$

则称 φ 为群 G 到群 $\bar{G}$ 的一个同态映射．

当 φ 又是满射时，则称群 G 与 $\bar{G}$ 同态，记为 $G\sim\bar{G}$．

当 φ是一个双射时，称 φ为群 G 到瑏的一个同构映射．如果群 G到群瑏存在同构映射，就称群 G 与瑏同构，记为

$$G\tilde{u}\ \text{瑏}.$$

群 G到自身的同态映射与同构映射，分别称为群 G 的自同态映射和自同构映射，简称为 G的自同态　自同构．

定理 1　设 G 是一个群，瑏是一个有代数运算(也称为乘法)的集合．如果 $G\sim$瑏，则瑏也是一个群．

证　因为 $G\sim$瑏，G 是群，其乘法满足结合律，故由第一章知，瑏的乘法也满足结合律．

设 e是群 G 的单位元，瑎是瑏的任一元素，又设 φ是 G 到瑏的满同态，且在 φ之下

$$e\quad \text{瑏},\quad a\quad \text{瑎},$$

于是

$$ea\quad \text{瑏瑎}.$$

但是 $ea=a$，故瑏瑎=瑎．即瑏是瑏的单位元．

又设

$$a^{-1}\quad \overline{a^{-1}},$$

则

$$a^{-1}a\quad \overline{a^{-1}}\text{瑎}.$$

但是 $a^{-1}a=e$，故$\overline{a^{-1}}$瑎=瑏，即$\overline{a^{-1}}$是瑎的逆元．

因此瑏也是一个群．

(证毕)

应注意，本定理中的同态映射 φ必须是满射．因为，例如设 G是正有理数乘群，瑏是全体正偶数对 $a\quad b=2$ 作成的半群．则显然

$$\varphi:\ x\quad 2\quad (\forall\ x\in G)$$

是 G到瑏的一个同态映射(但不是满射)．G 是群，但瑏并不是

群．

由定理 1 可得以下推论．

推论　设 φ是群 G 到群瑏瑏的一个同态映射(不一定是满射)．则群 G 的单位元的象是群瑏瑏的单位元；G 的元素 a 的逆元的像是 a 的像的逆元，即

$$\overline{a^{-1}}=瑏瑎^{-1}\quad 或\quad \varphi(a^{-1})=\varphi(a)^{-1}.$$

证　设 e 是群 G 的单位元，且在 φ之下

$$e\qquad 瑏瑏.$$

由于 φ是同态映射，故在 φ之下有

$$e=e^2\qquad 瑏瑏=瑏瑏.$$

但瑏瑏是群，故由瑏瑏=瑏瑏可知，瑏瑏是瑏瑏的单位元．

至于 $\varphi(a^{-1})=\varphi(a)^{-1}\ (a\in G)$ 则是定理 1 证明中的直接结果．

(证毕)

还应注意，如果集合 G 与瑏瑏各有一个代数运算，且 $G\sim$瑏瑏，则当瑏瑏为群时，G 却不一定是群．

例 1　令 $G=\{$全体正负奇数$\}$，代数运算为数的普通乘法；又瑏瑏$=\{1,-1\}$关于数的普通乘法作成群，令

$$\varphi:\ 正奇数\qquad 1,$$

$$负奇数\qquad -1.$$

则易知 φ是 G 到瑏瑏的一个同态满射，故 $G\sim$瑏瑏．瑏瑏是群，但 G 却不是群．

当然，若 G 与瑏瑏为各有一个代数运算的代数系统，且 $G\tilde{}$瑏瑏，则当 G 与瑏瑏中有一个是群时，另一个必然也是群．

定理 1 的意义在于，要验证一个集合 G 对所指的代数运算作成群，可找一个已知群，并通过同态来实现．

例 2　证明：瑏瑏$=\{0,1,2,3\}$对代数运算

$$a\ \ b=r\qquad (r\text{ 为 }a+b\text{ 用 }4\text{ 除所得余数})$$

作成一个群．

证　令 Z 是整数加群，则易知

$$\varphi: \quad x \quad x' \quad (\forall x \in Z)$$

是 Z 到□的一个同态满射，其中 x' 为整数 x 用 4 除所得余数．

由于 Z 是群，故由定理 1 知，□也是群．

（证毕）

这样，在证明□是一个群时，可以减少一些麻烦的验算过程．

定理 2　设 φ 是群 G 到群□的一个同态映射（不一定是满射），则

1）当 $H \leq G$ 时，有 $\varphi(H) \leq$□，且 $H \sim \varphi(H)$；

2）当□$\leq$□时，有 φ^{-1}（□）$\leq G$，且在 φ 之下诱导出 φ^{-1}（□）到□的一个同态映射．

证　1）任取□，□$\in \varphi(H)$，且在 φ 之下令

$$a \quad \square, \quad b \quad \square,$$

其中 $a, b \in H$．由于 $H \leq G$，故 $ab \in H$，且

$$ab \quad \square\square,$$

从而□$\in \varphi(H)$，即 $\varphi(H)$ 对□的乘法封闭，且

$$H \sim \varphi(H)．$$

但 H 是子群，从而 $\varphi(H)$ 也是群且是□的子群．

2）当□$\leq$□时，由于 φ^{-1}（□）显然非空，任取 $a, b \in \varphi^{-1}$（□），且在 φ 之下令

$$a \quad \square, \quad b \quad \square.$$

则

$$ab^{-1} \quad \square\square^{-1},$$

其中□，□$\in$□，而□$\leq$□，故□$\square^{-1} \in$□，从而

$$ab^{-1} \in \varphi^{-1}(\square)．$$

即 $\varphi^{-1}(\text{琀})\leq G$，且显然 φ诱导出 $\varphi^{-1}(\text{琀})$到 琀的一个同态映射．(证毕)

定理 3　群 G到群珺的同态映射 φ是单射的充分与必要条件是，群珺的单位元瑚的逆象只有 e．

证　必要性显然，下证充分性．

设 φ是群 G到群珺的任一同态映射，且在 φ之下瑚的逆象只有 e．又设在 φ之下

$$a \quad \text{琀}, \quad b \quad \text{琀},$$

当 $a\neq b$时，必 琀≠琀．因若 琀=琀，则由于

$$ab^{-1} \quad \text{琀}\text{琀}^{-1}=\text{瑚},$$

故 $ab^{-1}=e$，$a=b$，矛盾．因此，φ是单射．

(证毕)

例 3　设 6 阶群 G不是循环群．证明：

$$G\tilde{\cong} S_3.$$

证　因为 G不是循环群，故 G没有 6 阶元．从而由 Lagrange 定理知，G必有 2 阶元或 3 阶元．

除 e外 G中元素不能都是 2 阶元：若不然，则由习题 2.1 第 6 题知，G为交换群．于是在 G中任取互异的 2 阶元 a，b，则易知

$$H=\{e, a, b, ab\}\leq G.$$

这与 Lagrange 定理矛盾．

又除 e外 G中元素不能都是 3 阶元：若不然，则在 G中任取 3 阶元 a，b，可知 G有子群

$$K=\{e, a, a^2\}, \qquad N=\{e, b, b^2\} \quad (\text{其中 } b\notin K),$$

且 $K\cap N=\{e\}$．于是

$$|KN|=\frac{|K|\cdot|N|}{|K\cap N|}=9,$$

这与 $|G|=6$ 矛盾．

因此，G 必有 2 阶元 a 和 3 阶元 b.由此可知：

$$G=\{e, a, b, b^2, ab, ab^2\},$$

且易知

$$\varphi: \quad e \quad (1), \quad a \quad (12), \quad b \quad (123),$$

$$ab \quad (23), \quad b^2 \quad (132), \quad ab^2 \quad (13)$$

是 G 到对称群 S_3 的一个同构映射，故 $G\cong S_3$.

(证毕)

这个例子说明，在同构意义下 6 阶群只有两个：一个是 6 阶循环群，另一个是三次对称群 S_3 .

习题 3.1

1. 设 H 是群 G 的一个子群，$a\in G$. 证明：

$$aHa^{-1}\leq G, \quad \text{且 } H\cong aHa^{-1} .$$

2. 在群的同态映射下，一个元素与其象的阶是否一定相等？在同构映射下如何？

3. 问：$\varphi(A)=A^{\mathrm{T}}$ (A 的转置方阵)是否为一般线性群 $GL_n(F)$ 的自同构？又 $\sigma(A)=(A^{-1})^{\mathrm{T}}$ 呢？

4. 先证明本节例 3 中 6 阶群 G 的元素 $ba=ab^2$，再各给出 G 与 S_3 的乘法表，并由此指出 φ 是群 G 到三次对称群 S_3 的同构映射 .

5. 证明：4 阶群 G 若不是循环群则必与 Klein 四元群同构 .

6. 设 G 是正有理数乘群，$\mathbb{Z}$ 为整数加群 . 证明：

$$\varphi: \quad 2^n\frac{b}{a} \quad n$$

是 G 到 $\mathbb{Z}$ 的一个同态满射 . 其中 a 与 b 是互素的奇数，n 是整数 .

§2 正规子群和商群

正规子群是群论中最重要概念之一 . 本节主要介绍：①正规子群定义和简单性质，其中包括子群作成正规子群的条件，在同

态映射下的正规子群以及正规子群相乘的状况(定理 1、2、3)；②商群及商群的一个应用(定理 4、5)；③与正规子群密切相关的哈密顿群和单群．

由上一章知道，对于群 G 的一个子群 H 来说，左陪集 aH 不一定与右陪集 Ha 相等．但也有些子群对 G 中任意元素 a 都有 $aH = Ha$．具有这种性质的子群，在群论的研究中特别重要．

定义 1　设 N 是群 G 的一个子群，如果对 G 中每个元素 a 都有

$$aN = Na, \quad \text{即 } aNa^{-1} = N,$$

则称 N 是群 G 的一个__规子群(或不变子群)__

就是说，正规子群的任何一个左陪集都是一个右陪集，因此可以简称为__集__．

若 N 是群 G 的一个正规子群，则简记为 $N \quad G$；若 N 不是 G 的正规子群，则记为 $N \quad G$．

若 $N \quad G$ 且 $N \neq G$，则记为 $N \quad G$．

交换群的子群当然都是正规子群．因此，正规子群这一概念主要对非交换群才具有真正意义．

设 $N \quad G$，又 $N \leq H \leq G$，则显然 N 也是 H 的一个正规子群．

群 G 的平凡子群 e 与 G 显然都是 G 的正规子群，称其为群 G 的__凡正规子群__．G 的其它正规子群，如果存在的话，称为 G 的__平凡正规子群__．

显然，群 G 的中心是 G 的一个正规子群．

例 1　$N = \{(1), (123), (132)\}$ 是三次对称群 S_3 的一个正规子群．但是，S_3 的三个子群

$$H_1 = \{(1), (12)\}, \quad H_2 = \{(1), (13)\}, \quad H_3 = \{(1), (23)\}$$

都不是 S_3 的正规子群．

证　由上一章§6 定理 5 知，对 S_3 中任意元素 σ 有

$$\sigma N\sigma^{-1} = \{(1), \sigma(123)\sigma^{-1}, \sigma(132)\sigma^{-1}\} = N,$$

故 $N \quad S_3$.

但由于 $(13)\ H_1 \neq H_1\ (13)$, 故 $H_1 \quad S_3$.类似可证 H_2 与 H_3 也不是 S_3 的正规子群 .

(证毕)

定理 1 设 G 是群, $N \leq G$. 则

$$N \quad G \qquad aNa^{-1} \quad N \quad (\forall\ a \in G) .$$

证 设 $N \quad G$, 则对 G 中任意元素 a 有

$$aNa^{-1} = N,$$

当然有 $aNa^{-1} \quad N$.

反之, 设对 G 中任意 a 有 $aNa^{-1} \leq N$, 则有

$$aNa^{-1}a \quad Na, \quad \text{即 } aN \quad Na;$$

又由 $a^{-1}Na \quad N$ 可得 $Na \quad Na$. 因此

$$aN = Na, \quad \text{即 } N \quad G .$$

(证毕)

本定理显然也可以改述为: 设 G 是群, $N \leq G$, 则

$$N \quad G \qquad axa^{-1} \in N \qquad (\forall\ a \in G, x \in N) .$$

例 2 n 次交代群 A_n 是 n 次对称群 S_n 的一个正规子群 .

证 由于任意 n 次置换 σ 与其逆 σ^{-1} 有相同的奇偶性, 从而易知 $\sigma A_n \sigma^{-1} \quad A_n$, 故

$$A_n \quad S_n .$$

(证毕)

例 3 证明: Klein 四元群

$$K_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$$

是 S_4 的一个正规子群, 因而也是交代群 A_4 的一个正规子群 .

证 因为 K_4 中除单位元外的三个元素是 S_4 中仅有的阶为 2 的偶置换, 现任取其中一个, 设为 x, 则对任意 4 次置换 σ, 乘积 $\sigma x \sigma^{-1}$ 显然仍是一个阶为 2 的偶置换, 从而

$$\sigma x \sigma^{-1} \in K_4 ,$$

故 $K_4 \quad S_4$. 于是也有 $K_4 \quad A_4$.

(证毕)

又由于 K_4 是交换群，故

$$B_4 = \{(1),(12)(34)\} \quad K_4 .$$

从而有 $B_4 \quad K_4 \quad S_4$. 但是 $B_4 \quad S_4$: 因为易知

$$(13)B_4 \neq B_4(13) .$$

这说明，正规子群的正规子群不一定是原群的正规子群. 亦即正规子群不具有传递性 .

下面讨论在同态映射下正规子群的状况，以及正规子群相乘时的情形 .

定理 2 设 ϕ 是群 G 到群 $\bar{G}$ 的一个同态满射，则在 ϕ 之下 G 的正规子群的象是 $\bar{G}$ 的一个正规子群，$\bar{G}$ 的正规子群的逆象是 G 的一个正规子群 .

证 1) 设 $N \quad G$. 则由上节定理 2 知，

$$\phi(N) \leq \bar{G} .$$

再任取 $\bar{a} \in \phi(N)$，$\bar{a} \in \bar{G}$，则由于 ϕ 是同态满射，可令

$$a \quad \bar{a}, \quad n \quad \bar{a},$$

其中 $a \in G$, $n \in N$, 于是

$$ana^{-1} \quad \bar{a}\bar{a}\bar{a}^{-1} .$$

但是 $N \quad G$, $ana^{-1} \in N$, 故 $\bar{a}\bar{a}\bar{a}^{-1} \in \phi(N)$, 从而

$$\bar{a}\phi(N)\bar{a}^{-1} \quad \phi(N), \quad \phi(N) \quad G .$$

2) 若 $\bar{H} \quad \bar{G}$，则可类似证明 $\phi^{-1}(\bar{H}) \quad G$.

(证毕)

定理 3 群 G 的一个正规子群与一个子群的乘积是一个子群；两个正规子群的乘积仍是一个正规子群 .

证 1) 设 $N \quad G$, $H \leq G$, 任取

$$nh \in NH, \quad (n \in N, h \in H)$$

由于 $hN = Nh$, 故

$$nh \in Nh = hN \quad HN,$$

从而 $NH \quad HN$.

同理可得 $HN \quad NH$. 因此 $NH = HN$, 从而由上一章§3定理5知,

$$NH \leq G.$$

2) 设 $N \quad G$, $K \quad G$. 则由上知, $NK \leq G$.

又对任意 $a \in G$, 有

$$\begin{aligned} a(NK) &= (aN)K = (Na)K \\ &= N(aK) = N(Ka) = (NK)a, \end{aligned}$$

故 $NK \quad G$.

(证毕)

正规子群之所以重要, 其根本原因在于这种子群的全体陪集对于子集的乘法又可以作成一个新的群.

设 N 是群 G 的一个正规子群, 则任取二陪集 aN 与 bN, 有

$$\begin{aligned} (aN)(bN) &= a(Nb)N = a(bN)N \\ &= (ab)NN = (ab)N, \end{aligned}$$

即 $(aN)(bN) = (ab)N$. 我们称此为 集的乘法.

陪集的乘法, 实际上就是在条件 $aN = Na$ (a 为群中任意元素) 之下群中子集的乘法, 但其乘积仍是一个左陪集. 因此, 当 $N \quad G$ 时, 陪集的乘法是全体陪集的一个代数运算.

进一步还有

定理4 群 G 的正规子群 N 的全体陪集对于陪集的乘法作成一个群, 称为 G 关于 N 的 群, 记为 $G \quad N$.

证 由于群中子集的乘法满足结合律, 故陪集的乘法也满足结合律. 又陪集 N 显然是关于陪集乘法的单位元. 最后, 由于

$$(a^{-1}N)(aN) = a^{-1}aN = N,$$

故 $a^{-1}N$ 是 aN 的逆元, 即 $(aN)^{-1} = a^{-1}N$. 因此 $G \quad N$ 作成一个群.

(证毕)

由此定理可知，对任意整数 m 和群 G 中任意元素 a，都有

$$(aN)^m = a^m N .$$

另外，由于商群 G/N 中的元素就是 N 在 G 中的陪集，因此

$$|G/N| = (G:H) .$$

又根据 Lagrange 定理，对有限群 G 有

$$|G| = |N|(G:H),$$

从而有

$$|G/N| = \frac{|G|}{|N|} .$$

作为商群的一个应用，我们证明以下

定理 5 (A.L.Cauchy) 设 G 是一个 pn 阶有限交换群，其中 p 是一个素数，则 G 有 p 阶元素，从而有 p 阶子群 .

证 对 n 用数学归纳法 .

当 $n=1$ 时，G 是 p 阶循环群，则 G 的生成元就是一个 p 阶元，定理成立 .

假定定理对阶为 $pk(1 \leq k < n)$ 的交换群成立，下证对阶为 pn 的交换群 G 定理成立 .

在 G 中任取 $a \neq e$. 若 $p \mid |a|$，令

$$|a| = ps,$$

则 $|a^s| = p$, 定理成立 .

若 $p \nmid |a|$，令 $|a| = m \neq 1$, 则 $(m, p) = 1$.由于

$$m \mid pn,$$

故 $m \mid n$.令 $H = \blacksquare a \blacksquare$, 则由于 G 是交换群, 故

$$|G/H| = p \cdot \frac{n}{m}, \quad 1 \leq \frac{n}{m} < n .$$

于是由归纳假设, 群 G/H 有 p 阶元, 任取其一, 设为 bH, 且 $|b| = r$, 则

$$(bH)^r = b^r H = H,$$

从而 $p \mid r$. 令 $r = pt$, 则 $\mid b^t \mid = p$.

(证毕)

在后面§6将看到, 当 G 是非交换群时, 这个定理仍成立.

推论　pq(p, q为互异素数)阶交换群必为循环群.

证　设 G 为 pq 阶交换群, 由定理5, G 有 p 阶元素 a 与 q 阶元素 b. 又因为 p 和 q 是互异素数, 故 $|ab| = pq = |G|$, 从而 G 为循环群.

本节最后,我们来介绍由正规子群所界定的两类群——哈密顿群和单群.

定义2　设 G 是一个非交换群. 如果 G 的每个子群都是 G 的正规子群,则称 G 是一个<u>哈密顿群</u>.

这是由于哈密顿(瑜.R.Hamilton, 1805～1865)首先研究此种群而得名.

例4　四元数群

$$G = \{1, i, j, k, -1, -i, -j, -k\}$$

是一个哈密顿群.

证　首先, G 是非交换群显然. 其次, 由上一章习题2.7知, G 的真子群只有

$$\blacksquare -1\blacksquare,\ \blacksquare i\blacksquare,\ \blacksquare j\blacksquare,\ \blacksquare k\blacksquare.$$

而$\blacksquare -1\blacksquare$　G 显然. 又令

$$N = \blacksquare i\blacksquare,\quad x \in G,$$

则由于 $N = \{1, -1, i, -i\}$, 故易知

$$\{x, -x, xi, -xi\} = \{x, -x, ix, -ix\},$$

即 $xN = Nx$, 从而$\blacksquare i\blacksquare$　G.

同理可证$\blacksquare j\blacksquare$与$\blacksquare k\blacksquare$也是 G 的正规子群. 因此, G 是一个哈密顿群.

(证毕)

1、2、3、5、7阶群都是循环群, 从而都不是哈密顿群; 又

由上节例 3 和习题 6 以及本节例 1 可知，4 与 6 阶群也都不是哈密顿群．因此由例 4 可知，四元数群(8 阶)是阶数最小的哈密顿群．

关于哈密顿群的研究有很多深入的结果．例如，哈密顿群必为周期群即每个元素的阶都有限，哈密顿群的任何非交换子群都含有四元数群(在同构意义下)为其子群以及有限非交换群为哈密顿群的充要条件，等等．这些内容都超出本书范围，不再详述．

下面介绍单群．

定义 3 阶大于 1 且只有平凡正规子群的群，称为__群__．

例如，素数阶群显然都是单群；而由例 1 知，三次对称群不是单群．

另外，由例 3 可知交代群 A_4 不是单群．又 A_2 是单位元群，而 A_3 显然是单群．特别当 $n\geq 5$ 时，可以证明 A_n 是单群，对此，本书不再证明了．

利用 $n\geq 3$ 但 $n\neq 4$ 时 A_n 是单群这一事实，顺便指出 $S_n\ (n\neq 4)$ 的正规子群除去 $\{(1)\}$ 与 S_n 外只有 A_n．

事实上，设 $N \quad S_n$，则 $N\cap A_n \quad A_n$．但 A_n 是单群，故

$$N\cap A_n = A_n \quad \text{或} \quad N\cap A_n = \{(1)\}.$$

当 $N\cap A_n = A_n$ 时，$A_n \quad N$．由于置换群不是全由偶置换组成就是含奇、偶置换各半，故

$$N = A_n \quad \text{或} \quad N = S_n.$$

当 $N\cap A_n = \{(1)\}$ 时，则必 $N = \{(1)\}$：因若不然，设 $N > \{(1)\}$，则同上理由，N 只能再包含一个奇置换，设为 τ．于是

$$N = \{(1), \tau\} \quad S_n.$$

从而对 S_n 中任意 σ，必 $\sigma N\sigma^{-1} = N$，即

$$\sigma\tau\sigma^{-1} = \tau, \quad \text{或} \quad \sigma\tau = \tau\sigma.$$

亦即 τ 是 S_n 的中心元．但当 $n\geq 3$ 时 S_n 为无中心群，即中心元只有(1)，故 $\tau = (1)$，矛盾．故此时 $N = \{(1)\}$．

因此，$S_n\ (n\neq 4)$ 的正规子群只有：

$$\{(1)\},\quad A_n,\quad S_n\ .$$

有限交换单群的情况比较简单，因为有以下

定理 6　有限交换群 G 为单群的充分与必要条件是，$|G|$ 为素数．

证　设 $|G|$ 为素数，则 G 是一个素阶循环群，从而 G 显然是一个单群．

反之，设 G 是单群且 $|G| = n > 1$．在 G 中任取元素 $a \neq e$．若 $|a| < n$，则由于 G 是交换群，故

$$e \quad \blacksquare a \blacksquare \quad G\ .$$

这与 G 是单群矛盾．因此必 $|a| = n$，从而 $G = \blacksquare a \blacksquare$ 为 n 阶循环群．再由循环群的定理 5 可知，n 必为素数．

（证毕）

有限单群是一类重要的群，它长期是群论研究的中心问题之一．有限单群分为四大类：素数阶群、交代群 $A_n\ (n \geq 5)$、有限李型单群和 26 个零散单群．每个有限单群都同其中的一个单群同构．在零散单群中，阶数最大的一个其阶数约为 10^{54}，常称为怪物群或　群．置换群一节中所说的马提厄群都属于零散单群．在马提厄后约一百年的 1965 年，数学家简科(Z Janko)又发现了另一个新的零散单群．尔后，人们又陆续地发现了所有的零散单群．

20 世纪初，伯恩赛德(W .S .Burnside)关于 $p^s q^t\ (p, q$ 为素数)阶群必为可解群(可解群定义参本节习题第 8 题)的定理，是有限单群分类问题早期最重要的工作．1942 年至 1954 年间，布劳尔(R .D .Brauer)关于有限单群的研究又创造出新方法，标志着这一工作的新起点，他堪称近代有限单群分类工作的先驱．1962 年，费特(瑜 .Feit)和汤普森(J .G .Thompson)关于奇数阶群必为可解群的结论是单群分类中最重要的一个定理，它标志着有限单群分类的重大突破．1972 年，戈朗斯坦(D .Gorenstein)以及世界上众多数学家经过 40 多年的不懈努力，关于有限单群

的完全分类(即找出有限单群所有的同构类)，终于在 1981 年得到解决．这是 20 世纪世界数学史上一个非凡的成就．

习题　3.2

1. 证明：群 G 的任意个正规子群的交还是 G 的一个正规子群．

2. 证明：指数是 2 的子群必是正规子群．

3. 证明：若群 G 的 n 阶子群有且只有一个，则此子群必为 G 的正规子群．

4. 设 $H \quad G$，且 $(G : H) = m$．证明：对群 G 中任意元素 a 有 $a^m \in H$．

5. 设 H，K 是群 G 的两个正规子群，且二者的交为 $\{e\}$．证明：H 与 K 中的元素相乘时可换．

6. 设 H 是包含在群 G 的中心内的一个子群．证明：当 G/H 是循环群时，G 是交换群．

7. 设 G 是群，$N \quad G$．证明：如果 N 及商群 G/N 都是周期群，则 G 也是周期群．

8. 设 G 是群，$G_i\ (0 \leq i \leq k)$ 为其子群且

$$e = G_0 \quad G_1 \quad \cdots \quad G_{k-1} \quad G_k = G, \tag{1}$$

则称此为群 G 的<u>正规群列</u>．若群 G 有正规群列 (1) 且诸商群

$$G_1/G_0, \quad G_2/G_1, \quad \cdots, \quad G_k/G_{k-1}$$

又都是交换群时，则称 G 为<u>可解群</u>．证明：对称群 S_2，S_3 及 S_4 都是可解群．

提示：参本节例 3．

§3　群同态基本定理

在正规子群、商群以及同态与同构映射之间，存在着一些极为重要的内在联系．通过这些联系，我们将看到正规子群和商群在群论研究中的重要作用．

定理 1　设 N 是群 G 的任一正规子群，则

$$G \sim G/N,$$

即任何群均与其商群同态.

证 在群 G 与商群 G/N 间建立以下映射:

$$\tau:\quad a \longrightarrow aN. \quad (\forall a\in G)$$

这显然是 G 到 G/N 的一个满射.

又任取 $a, b\in G$, 则有

$$ab \longrightarrow (ab)N = (aN)(bN),$$

即 τ 是 G 到 G/N 的一个同态满射, 故 $G\sim G/N$.

(证毕)

今后称群 G 到商群 G/N 的这个同态满射 τ 为 G 到商群 G/N 的自然同态.

下面将证明, 在一定意义下定理 1 的逆定理也成立. 为此, 先给出以下定义.

定义 设 ϕ 是群 G 到群 $\bar{G}$ 的一个同态映射, $\bar{G}$ 的单位元在 ϕ 之下所有逆象作成的集合, 叫做 ϕ 的核, 记为 $\mathrm{Ker}\phi$.

群 G 中所有元素在 ϕ 之下的象作成的集合 $\phi(G)$, 称为 ϕ 的象集, 记为 $\mathrm{Im}\phi$.

显然, 核 $\mathrm{Ker}\phi$ 是群 G 的子群, 象集 $\mathrm{Im}\phi$ 是群 $\bar{G}$ 的子群.

又易知, 定理 1 中的同态映射 τ 的核就是 N.

进一步有

定理 2 (群同态基本定理) 设 ϕ 是群 G 到群 $\bar{G}$ 的一个同态满射. 则 $N=\mathrm{Ker}\phi \lhd G$, 且

$$G/N\cong \bar{G}.$$

证 首先, 由于 $\bar{G}$ 的单位元是 $\bar{G}$ 的一个正规子群, 故由上节定理 2 知, 其所有逆象的集合, 即 ϕ 的核 $N=\mathrm{Ker}\phi$ 也是 G 的一个正规子群.

其次, 设

$$\phi:\quad a \longrightarrow \bar{a} \quad (a\in G, \bar{a}\in \bar{G}),$$

则在 G/N 与 $\bar{G}$ 间建立以下映射:

$\sigma: aN \mapsto \phi(a)$.

1) 设 $aN = bN$, 则 $a^{-1}b \in N$. 于是

$$\phi(a^{-1}b) = \overline{a^{-1}b} = \bar{1}, \quad \phi(a)^{-1}\phi(b) = \bar{1},$$

即 G/N 中的每个陪集在 σ 之下在 $\bar{G}$ 中只有一个象, 因此, σ 确为 G/N 到 $\bar{G}$ 的一个映射;

2) 任取 $\phi(a) \in \bar{G}$, 则因 ϕ 是满射, 故有 $a \in G$ 使 $\phi(a) = \phi(a)$. 从而在 σ 之下元素 $\phi(a)$ 在 G/N 中有逆象 aN, 即 σ 为 G/N 到 $\bar{G}$ 的一个满射;

3) 又若 $aN \neq bN$, 则 $a^{-1}b \notin N$, 从而 $\phi(a)^{-1}\phi(b) \neq \bar{1}$, $\phi(a) \neq \phi(b)$. 即 σ 为 G/N 到 $\bar{G}$ 的一个单射.

因此, σ 是 G/N 到 $\bar{G}$ 的一个双射.

又由于有

$$(aN)(bN) = abN \quad \overline{ab} = \phi(a)\phi(b),$$

故 σ 为同构映射, 从而 $G/N \cong \bar{G}$.

(证毕)

由定理 1 和定理 2 知:

$$G \xrightarrow{\phi} \bar{G}$$
$$a \mapsto \phi(a);$$

又

$$G \xrightarrow{\tau} G/N \xrightarrow{\sigma} \bar{G}$$
$$a \mapsto aN \mapsto \phi(a),$$

其中 $N = \mathrm{Ker}\phi$. 因此, $\phi = \sigma\tau$, 即右图为交换图.

定理 1 表明, 任何群都同它的商群同态; 定理 2 表明, 如果一个群 G 同另一个群 $\bar{G}$ 同态, 则这个群 $\bar{G}$ 在同构意义下是 G 的一个商群. 因此, 在同构意义下, 定理 1 与定理 2 的意思是:

每个群能而且只能同它的商群同态.

这是群论中最基本最重要的结论之一, 在很多场合下, 都要经常用到这个事实.

另外，由定理 2 的证明知，若 $G\sim$珂，且同态核是 N，则珂中每个元素的全体逆象恰好都是关于 N 的一个陪集．珂中元素与陪集的这种对应不仅是一个双射，而且是一个同构映射．

推论 1　设 G 与珂是两个有限群．如果 $G\sim$珂，则

$$|\text{珂}| \mid |G| \ .$$

证　因为 $G\sim$珂，设此同态核为 N，则由定理 2 知，

$$G/N \cong \text{珂},$$

从而 $|\text{珂}| = |G/N|$．但是 $|G/N|$ 整除 $|G|$，故 $|\text{珂}|$ 整除 $|G|$．

(证毕)

本节最后，再来讨论循环群的同态象以及在同态映射下两个群的子群间的一些关系．

定理 3　设 G 与珂是两个群且 $G\sim$珂．若 G 是循环群，则珂也是循环群．

证　设 $G=(a)$．由于 $G\sim$珂，设在此同态下 G 的生成元 a 在珂中的象是琯，下证珂 $=(\text{琯})$．

事实上，显然 $(\text{琯}) \subseteq$ 珂；另一方面，任取 $\text{珂} \in$珂，并令

$$x \mapsto \text{珂} \quad (x \in G=(a)),$$

且 $x=a^m$，但由于在所说的同态之下

$$a^m \mapsto \text{琯}^m,$$

故珂 $=\text{琯}^m \in (\text{琯})$，从而又有珂 $\subseteq (\text{琯})$．因此珂 $=(\text{琯})$，即珂也是循环群．

(证毕)

由以上证明可知，在同态映射下，循环群的生成元的象也是生成元．

由于任何群都与其商群同态，于是由定理 3 可立得以下推论．

推论 2　循环群的商群也是循环群．

为讨论在群同态映射之下两个群的子群间的关系，先证以下引理.

引理 设 ϕ 是群 G 到群 $\bar{G}$ 的一个同态映射，又 $H \leq G$. 如果 $H \supseteq \mathrm{Ker}\phi$，则

$$\phi^{-1}[\phi(H)] = H.$$

证 首先，由习题 1.6 知

$$H \subseteq \phi^{-1}[\phi(H)];$$

其次，任取 $x \in \phi^{-1}[\phi(H)]$，则 $\phi(x) \in \phi(H)$. 于是有 $h \in H$ 使

$$\phi(h) = \phi(x), \quad \phi(h^{-1}x) = \bar{1},$$

从而 $h^{-1}x \in \mathrm{Ker}\phi \subseteq H$，故

$$h^{-1}x \in H, \quad x \in H.$$

即又有

$$\phi^{-1}[\phi(H)] \subseteq H.$$

因此，$\phi^{-1}[\phi(H)] = H$.

(证毕)

定理 4 设 ϕ 是群 G 到群 $\bar{G}$ 的一个同态满射，核是 K. 则 G 的含 K 的所有子群与 $\bar{G}$ 的所有子群间可建立一个保持包含关系的双射.

证 设 M 是 G 的含 K 的所有子群作成的集合，$\bar{M}$ 是 $\bar{G}$ 的所有子群的集合，则易知

$$f: \quad H \quad \phi(H)$$

是 M 到 $\bar{M}$ 的一个映射；其次任取 $\bar{H} \in \bar{M}$，并令 $H = \phi^{-1}(\bar{H})$，则由 §1 定理 2 知，H 是 G 的一个子群且包含核 K，故 $H \in M$. 再由于 ϕ 是满同态，故由引理知：

$$\phi(H) = \phi[\phi^{-1}(\bar{H})] = \bar{H},$$

即 f 是 M 到 $\bar{M}$ 的一个满射.

最后，任取 $H_1, H_2 \in M$，若 $f(H_1) = f(H_2)$，即

$$\phi(H_1) = \phi(H_2),$$

则 $\phi^{-1}[\phi(H_1)] = \phi^{-1}[\phi(H_2)]$. 于是由引理知, $H_1 = H_2$. 即 f 是单射.

因此, f 是 M 到 $\bar{M}$ 的一个双射.

又显然对 M 中的 H_1 与 H_2, 有 $H_1 \subseteq H_2$ 当且仅当有 $\phi(H_1) \subseteq \phi(H_2)$, 即双射 f 还保持 M 与 $\bar{M}$ 中子群间的包含关系.

(证毕)

习题 3.3

1. 设群 $G \sim \bar{G}$, 且同态核是 K. 证明: G 中二元素在 $\bar{G}$ 中有相同的象, 当且仅当它们在 K 的同一陪集中.

2. 证明: 单群的同态象是单群或单位元群(即只含一个元素的群).

3. 设 N 是群 G 的一个正规子群, 又 $N \subseteq H \leq G$. 证明: H 在自然同态

$$G \sim G/N$$

之下的像是 H/N.

4. 证明:

1) 无限循环群与任何循环群同态;

2) 两个有限循环群 G 与 $\bar{G}$ 同态, 当且仅当 $|\bar{G}| \mid |G|$.

5. 证明: 有理数加群 Q_+ 与非零有理数乘群 Q^* 不同构.

提示: 用反证法并考虑单位元.

§4 群的同构定理

本节介绍群的三个同构定理. 这三个定理在群论研究中都很重要, 它们的证明有多种方法, 其中有的与群同态基本定理有直接的关系.

定理 1 (第一同构定理) 设 ϕ 是群 G 到群 $\bar{G}$ 的一个同态满射, 又 $\mathrm{Ker}\phi \subseteq N \subseteq G$, $\bar{N} = \phi(N)$, 则

G/N 的子群.

证 为配合本定理证明并增强记忆，先画以下示意图(其中双直线 表示下方为上方的正规子群):

因为 $N \trianglelefteq G$，又 φ 是满同态，故 $\bar{N} = \varphi(N)$ 是 $\bar{G}$ 的子群. 现在令

$$\tau: G/N \to \bar{G}, \quad xN \mapsto \varphi(x)\varphi(N) \quad (\forall x \in G).$$

下证 τ 是商群 G/N 到子群 $\bar{N}$ 的一个同构映射.

1) τ 是映射: 设 $aN = bN$ $(a, b \in G)$，则 $a^{-1}b \in N$. 但由于 φ 是同态满射，故

$$\varphi(a)^{-1} \cdot \varphi(b) = \varphi(a^{-1}b) \in \varphi(N) = \bar{N}.$$

从而 $\varphi(a)\bar{N} = \varphi(b)\bar{N}$，即 τ 是 G/N 到子群 $\bar{N}$ 的映射;

2) τ 是满射: 任取 $\bar{a}\bar{N} \in$ 子群 $\bar{N}$ $(\bar{a} \in$ 子群$)$，则因 φ 是满同态，故有 $a \in G$ 使 $\varphi(a) = \bar{a}$. 从而在 τ 之下 $\bar{a}\bar{N}$ 有逆象 aN，即 τ 是满射.

3) τ 是单射: 设 $\varphi(a)\bar{N} = \varphi(b)\bar{N}$，则

$$\varphi(a^{-1}b) = \varphi(a)^{-1}\varphi(b) \in \bar{N}.$$

但 φ 为满同态且 $\bar{N} = \varphi(N)$，故有 $c \in N$ 使

$$\varphi(a^{-1}b) = \varphi(c) \quad 或 \quad \varphi(c^{-1}a^{-1}b) = \bar{1},$$

其中 $\bar{1}$ 是子群的单位元. 于是 $c^{-1}a^{-1}b \in \mathrm{Ker}\varphi$. 但是 $\mathrm{Ker}\varphi \trianglelefteq N$，故

$$a^{-1}b = c \cdot c^{-1}a^{-1}b \in N.$$

从而 $aN = bN$，即 τ 是单射.

因此，τ是双射．又因为显然在τ之下有

$$aN \cdot bN = abN \to \phi(ab) = \phi(a)\phi(b) = \phi(a) \cdot \phi(b),$$

故τ是 G/N 到 $\phi(G)$ 的同构映射．因此

$$G/N \cong \phi(G).$$

(证毕)

以上的同构当然也可以写成

$$G/N \cong \phi(G)/\phi(N).$$

但应注意，定理1中的φ必须是满同态而且 N 必须是 G 的包含核 Kerφ的正规子群．

另外也可证明：$G \sim \phi(G)$，且此同态核为 N．从而由同态基本定理可给出第一同构定理的另一证法．

推论 设 H，N 是群 G 的两个正规子群，且 $N \triangleleft H$，则

$$G/H \cong (G/N)/(H/N).$$

证 因为自然同态

$$G \sim G/N$$

的核为 $N \triangleleft H$，而 H 在这个同态下的象为 H/N，故由定理1得

$$G/H \cong (G/N)/(H/N).$$

(证毕)

例1 设 H，K 是群 G 的两个正规子群．证明：

$$G/HK \cong (G/H)/(HK/H). \quad (1).$$

证 因为 $H \triangleleft G$，$K \triangleleft G$，故 $HK \triangleleft G$．又显然 $H \triangleleft HK$，故直接由以上推论知，(1)式成立．

(证毕)

定理2 (第二同构定理) 设 G 是群，又 $H \leq G$，$N \triangleleft G$．则 $H \cap N \triangleleft H$，并且

$$HN/N \cong H/(H \cap N). \quad (2)$$

证 因为 $H \leq G$，$N \triangleleft G$，故 $HN \leq G$，且 $N \triangleleft HN$．又易知

$$\varphi:\quad x\quad xN\quad (\forall x\in H)$$

是子群 H 到商群 HN/N 的同态满射，且核为 $H\cap N$，故由群同态基本定理知：

$$H/(H\cap N)\cong HN/N.$$

从而(2)成立．

(证毕)

例 2　设 S_3，S_4 分别为三、四次对称群，K_4 为 Klein 四元群．证明：

$$S_4/K_4\cong S_3.$$

证　因为 $S_3\leq S_4$ (把 S_3 中每个置换 τ 视为 $\tau(4)=4$)，又 $K_4\quad S_4$，故

$$K_4\quad S_3K_4\leq S_4. \tag{3}$$

再由于 S_3 中每个置换把 4 变为 4，故 $S_3\cap K_4=\{(1)\}$．从而

$$|S_3K_4|=\frac{|S_3|\cdot|K_4|}{|S_3\cap K_4|}=\frac{6.4}{1}=24.$$

但是 $|S_4|=24$，故由(3)知，$S_4=S_3K_4$．于是由定理 2 得

$$S_4/K_4=S_3K_4/K_4\cong S_3/(S_3\cap K_4)\cong S_3.$$

因此，$S_4/K_4\cong S_3$．

(证毕)

定理 3　(第三同构定理)　设 G 是群，又 $N\quad G$，$H\leq G$ N 则

1) 存在 G 的惟一子群 $H\quad N$，且 $H=H/N$；

2) 又当 $H\quad G$ 时，有惟一的 $H\quad G$ 使

$$H=H/N\quad 且\quad G/H\cong G/N/H/N.$$

证　1) 设在自然同态

$$\sigma:\quad G\sim G/N$$

之下 H 的逆象为 H．则 $N\quad \sigma^{-1}(H)=H\leq G$，且因 σ 是满同态，故由习题 1.6 知：

$$\sigma(H)=\sigma[\sigma^{-1}(H)]=H.$$

但由习题 3.3 第 3 题知，$\sigma(H)=H/N$，故

$$珔H=H/N;$$

再由上节定理 4，由于 G 中含 N 的不同子群其象也不同，故可知这样的 H 也是惟一的．

2) 当 $珔H$ 是 G/N 的正规子群时，由 1) 及 §1 定理 2 知，G 有惟一正规子群 $H\supset N$ 使 $珔H=H/N$．又由于在自然同态

$$G\sim G/N$$

之下有 $H\supset N$，且 H 的象是 H/N，故由第一同构定理知，

$$G/H\cong(G/N)/(H/N).$$

(证毕)

此定理表明，商群 G/N 的子群仍为商群，且呈 H/N 形，其中 H 是 G 的含 N 的子群；又 H 是 G 的正规子群当且仅当 H/N 是 G/N 的正规子群．

习题 3.4

1. 设群 $G\sim$□，□ $\supset$ □，N 是□的逆像．证明：

$$G/N\cong□.$$

2. 设 H，K 是群 G 的两个子群，$K'\supset K$．证明：

1) $H\cap K'\supset H\cap K$;

2) $H\cap K'/H\cap K$ 与 K'/K 的一个子群同构．

3. 设 G 是群，又 $K\leq H\subset G$，$K\subset G$．证明：若 G/K 是交换群，则 G/H 也是交换群．

4. 题设如定理 1．证明：$\sigma: x\to\phi(x)$ □是群 G 到商群□的满同态，且其核 $\mathrm{Ker}\sigma=N$．从而 $G/N\cong$□.

5. 设 G 是一个群，又 $H_1\leq G$，$H_2\subset G$，$N\subset G$．证明：如果 $|H_1|$，$|H_2|$ 与 $(G:N)$ 均有限，且

$$(|H_i|,(G:N))=1,\quad i=1,2.$$

则 $H_1H_2\leq N$．

提示：利用第二同构定理．

6. 设 G 是群，$N \quad G$．如果当 $N \leq H \quad G$ 时必有 $N = H$，则称 N 是 G 的一个 大正规子群．证明：

N 是 G 的极大正规子群　　G/N 是单群．

提示：利用第三同构定理．

§5　群的自同构群

本节讨论由群的全体自同构作成的群．为此，先讨论更一般的代数系统的自同构群．

定理 1　设 M 是一个有代数运算(叫做乘法)的集合．则 M 的全体自同构关于变换的乘法作成一个群，称为 M 的自同构群．

证　设 σ, τ 是 M 的任意两个自同构，则对 M 中任二元素 a，b 有

$$\begin{aligned}\sigma\tau(ab) &= \sigma[\tau(ab)] \\ &= \sigma[\tau(a)\tau(b)] = \sigma\tau(a) \cdot \sigma\tau(b),\end{aligned}$$

即乘积 $\sigma\tau$ 也是 M 的一个自同构．

又因为对 M 中任意元素 x 有

$$\sigma\sigma^{-1}(x) = \sigma^{-1}\sigma(x) = x,$$

故

$$\begin{aligned}\sigma^{-1}(ab) &= \sigma^{-1}[\sigma\sigma^{-1}(a) \cdot \sigma\sigma^{-1}(b)] \\ &= \sigma^{-1}[\sigma(\sigma^{-1}(a) \cdot \sigma^{-1}(b))] \\ &= \sigma^{-1}(a) \cdot \sigma^{-1}(b),\end{aligned}$$

即 σ^{-1} 也是 M 的自同构．因此，M 的全体自同构作成 M 上的对称群 $S(M)$(M 的全体双射变换作成的群)的一个子群．

(证毕)

推论 1　群 G 的全体自同构关于变换的乘法作成一个群．这个群称为群 G 的自同构群，记为 $\mathrm{Aut}G$．

例 1　求 Klein 四元群

$$K_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$$

的自同构群．

解　把 K_4 的四个元素依次记为 e，a，b，c．再令 x，y，z 代表 a，b，c 中三个不同的元素，则 xyz 是 a，b，c 的任意一个排列．由于自同构把单位元变成单位元，故根据 K_4 中元素的乘法易知，置换

$$\begin{matrix} e & a & b & c \\ e & x & y & z \end{matrix}$$

是 K_4 的一个自同构．由于三个元素共有 $3!=6$ 个排列，从而 K_4 共有 6 个自同构．因此，在同构意义下，K_4 的自同构群就是三次对称群 S_3，即 $\mathrm{Aut}K_4 = S_3$．这里的 S_3 是集合 $\{a, b, c\}$ 上的三次对称群．

（证毕）

定理 2　无限循环群的自同构群是一个 2 阶循环群；n 阶循环群的自同构群是一个 $\varphi(n)$ 阶群，其中 $\varphi(n)$ 为 Euler 函数．

证　由于在同构映射下，循环群的生成元与生成元相对应，而生成元的相互对应完全决定了群中所有元素的对应，因此，一个循环群有多少个生成元就有多少个自同构．

由于无限循环群有两个生成元，n 阶循环群有 $\varphi(n)$ 个生成元，从而其自同构群分别为 2 阶循环群和 $\varphi(n)$ 阶群．

（证毕）

推论 2　无限循环群的自同构群与三阶循环群的自同构群同构．

证　由定理 2 知，这两种群的自同构群都是 2 阶群．凡 2 阶群显然彼此同构．

下面进一步讨论群的一种特殊的自同构——内自同构．

定理 3　设 G 是一个群，$a\in G$．则

1）$\sigma_a: x \to axa^{-1}$　　$(x\in G)$

是 G 的一个自同构，称为 G 的一个内自同构；

2）G 的全体内自同构作成一个群，称为群 G 的　自同构

__，记为 Inn$G$;

3) Inn$G$ Aut$G$.

证 1) 易知 σ_a 是 G 的一个双射变换．又由于

$$a(xy)a^{-1} = (axa^{-1})(aya^{-1}),$$

即 $\sigma_a(xy) = \sigma_a(x)\cdot\sigma_a(y)$，故 σ_a 是 G 的一个自同构．

2) 设 σ_a 与 σ_b 为 G 的任二内自同构，则对 G 中任意元素 x 有

$$\begin{aligned}\sigma_a\sigma_b(x) &= \sigma_a(\sigma_b(x)) = \sigma_a(bxb^{-1})\\ &= a(bxb^{-1})a^{-1} = (ab)x(ab)^{-1}\\ &= \sigma_{ab}(x),\end{aligned}$$

即 $\sigma_a\sigma_b = \sigma_{ab}$ 仍为 G 的一个内自同构．

又易知 $\sigma_{a^{-1}}$ 是 σ_a 的逆元，即 $\sigma_a^{-1} = \sigma_{a^{-1}}$．

因此，Inn$G \leq$ Aut$G$，即 Inn$G$ 作成一个子群．

3) 设 τ 是 G 的任意一个自同构，σ_a 是 G 的任意一个内自同构．任取 $x\in G$，令 $\tau^{-1}(x) = y$，即 $\tau(y) = x$，则

$$\begin{aligned}\tau\sigma_a\tau^{-1}(x) &= \tau\sigma_a(y) = \tau(aya^{-1})\\ &= \tau(a)\tau(y)\tau(a^{-1}) = \tau(a)x\tau(a)^{-1}\\ &= \sigma_{\tau(a)}(x),\end{aligned}$$

即 $\tau\sigma_a\tau^{-1} = \sigma_{\tau(a)}$ 仍是 G 的一个内自同构．故

Inn$G$ Aut$G$.

(证毕)

设 N 为群 G 的一个正规子群，则对 G 中任意元素 a，有

$$aNa^{-1} \quad N \quad \text{或} \quad \sigma_a(N) \quad N,$$

即 N 对 G 的任意内自同构都不变．反之，若 G 的一个子群有此性质，则它显然是 G 的一个正规子群．这就是说，G 的正规子群就是对 G 的所有内自同构都不变的子群．因此，也常称正规子群为<u>不变子群</u>．

定义 1 对群 G 的所有自同构都不变的子群，亦即对 G 的任

何自同构 σ 都有

$$\sigma(N) \quad N$$

的子群 N，叫做 G 的一个特征子群．

显然，群 G 与 e 都是 G 的特征子群．

特征子群一定是正规子群，但反之不成立．例如，由于 Klein 四元群 K_4 是交换群，它的每个子群都是正规子群，因此由例 1 知，$N=\{e, a\}$ 是 K_4 的一个正规子群，但它不是 K_4 的特征子群，因为由例 1 知

$$\sigma=\begin{matrix} e & a & b & c \\ e & b & a & c \end{matrix}$$

是 K_4 的一个自同构，然而却有

$$\sigma(N)=\{e, b\}\check{n} \quad N .$$

再讨论一种比特征子群更特殊的子群——全特征子群．

定义 2 设 H 是群 G 的一个子群．如果 H 对 G 的每个自同态映射都不变，即对 G 的每个自同态映射 Ψ 都有

$$\Psi(H) \quad H,$$

则称 H 为群 G 的一个 特征子群．

同样，G 与 e 显然都是群 G 的全特征子群．又显然全特征子群一定是特征子群．但反之不成立．

例 2 群 G 的中心 C 是 G 的一个特征子群．

证 任取 $c\in C$, $x\in G$, $\sigma\in \mathrm{Aut}G$, 则

$$\begin{aligned}\sigma(c)\,x &= \sigma(c)\cdot\sigma[\sigma^{-1}(x)] = \sigma[c\cdot\sigma^{-1}(x)] \\ &= \sigma[\sigma^{-1}(x)\,c] = \sigma[\sigma^{-1}(x)]\cdot\sigma(c) \\ &= x\sigma(c),\end{aligned}$$

即 $\sigma(c)\in C$, $\sigma(C) \quad C$．即 C 是 G 的一个特征子群．

（证毕）

但应注意，群的中心不一定是全特征子群．

例 3 有理数域 Q 上的 2 阶线性群 $G=GL_2(Q)$ 的中心（Q 上

所有 2 阶纯量矩阵)不是全特征子群．

证　任取 $A\in G$，即 A 为有理数域 Q 上一个 2 阶满秩方阵，则行列式 $|A|$ 是个有理数．因此可令

$$|A| = \frac{b}{a}2^{n(A)},$$

其中 a，b 为奇数，$n(A)$ 是与 A 有关的整数．

由于 $|AB| = |A| \cdot |B|$，故有

$$n(AB) = n(A) + n(B).$$

于是易知

$$\phi: \quad A \to \begin{matrix} 1 & n(A) \\ 0 & 1 \end{matrix}$$

是 G 到自身的一个映射．又由于

$$\phi(AB) = \begin{matrix} 1 & n(AB) \\ 0 & 1 \end{matrix} = \begin{matrix} 1 & n(A)+n(B) \\ 0 & 1 \end{matrix}$$

$$= \begin{matrix} 1 & n(A) \\ 0 & 1 \end{matrix} \begin{matrix} 1 & n(B) \\ 0 & 1 \end{matrix} = \phi(A)\phi(B),$$

故 ϕ 是群 G 的一个自同态映射．但是，ϕ 把 G 的中心元素 $\begin{matrix} 2 & 0 \\ 0 & 2 \end{matrix}$ 却变成非中心元素 $\begin{matrix} 1 & 2 \\ 0 & 1 \end{matrix}$，因此，$G$ 的中心不是全特征子群．

(证毕)

例 4　证明：循环群 $G = \blacksquare a \blacksquare$ 的子群都是全特征子群．

证　设 $H = \blacksquare a^s \blacksquare \leq G$，$\phi$ 为 G 的任一自同态且 $\phi(a) = a^t$，则 $\phi(a^s) = a^{st} \in H$ 从而 $\phi(H) \quad H$，即 H 是 G 的全特征子群。

(证毕)

由以上讨论和例子可知，全特征子群、特征子群和正规子群(不变子群)间的关系是：

全特征子群　特征子群　正规子群．

定理 4　设 C 是群 G 的中心，则

$$\mathrm{Inn}G \cong G/C.$$

证　易知

$$\phi: \quad a \to \sigma_a \quad (a \in G)$$

是群 G 到 $\mathrm{Inn}G$ 的一个满射．又由定理 2 知 $\sigma_{ab} = \sigma_a\sigma_b$，即 $\phi(ab) = \phi(a)\phi(b)$，故 $G \sim \mathrm{Inn}G$．

又若 σ_a 是 G 的恒等自同构，即对 G 中任意元素 x 都有 $\sigma_a(x) = x$，即有 $axa^{-1} = x$，　　$ax = xa$，则 $a \in C$．

反之，任取 $c \in C$，则显然 σ_c 是 G 的恒等自同构，故

$$C = \mathrm{Ker}\,\phi.$$

于是由群同态基本定理知，

$$\mathrm{Inn}G \cong G/C.$$

（证毕）

此定理表明，欲求群 G 的内自同构群 $\mathrm{Inn}G$，只须求 G 的中心 C，再作 G/C，即得 $\mathrm{Inn}G$．但是要定出一个已知群的自同构群，一般是非常困难的．这是因为，在大多数情况下，一个群的本身的性质不能转移到它的自同构群上去．例如，由例 1 知，交换群的自同构群可能是不可换的；推论 2 说明，不同构的群其自同构群却可能是同构的．另外，无限群的自同构群可能无限也可能有限，等等．

尽管如此，然而对有些群，则可以定出它的自同构群的一些性质．例如，可以证明无中心群的自同构群也必为无中心群．从而可知，当 $n \geq 3$ 时 $\mathrm{Aut}S_n$ 是无中心群．对此留作习题，不再详述．

习题　3.5

1. 证明：阶数 ≤ 7 的循环群的自同构群都是循环群．

2. 证明：非交换群的自同构群不能是循环群．

提示：反证法并用定理 4．

3. 证明：若群 G 的自同构群是一个单位元群（即 G 只有恒等自同构），

则 G 必为交换群且每个元素都满足方程 $x^2 = e$.

提示：利用定理 4 并证 $a \to a^{-1}$ 是 G 的自同构.

4. 证明：任何非交换单群 G 必与其内自同构群 $\mathrm{Inn}G$ 同构.

5. 设 N 是群 G 的一个子群. 证明：N 是 G 的特征子群，当且仅当对 G 的每个自同构 σ 都有 $\sigma(N) = N$.

6. 证明：若 G 是一个无中心群，则其自同构群 $\mathrm{Aut}G$ 也是一个无中心群.

提示：取 $\tau(a) = b \neq a$，则 $\tau\sigma_a = \sigma_b\tau$.

§6 共轭关系与正规化子

在这一节里，我们来讨论共轭关系以及与其相关的正规化子. 为此先介绍群中共轭元素的概念.

定义 1 设 a，b 为群 G 的两个元素. 如果存在 $c \in G$ 使

$$a = cbc^{-1},$$

则称 a 与 b 共轭，也称 a 是 b 的共轭元素.

由此定义易知，群中元素的共轭关系是一个等价关系. 而且一个元素 a 只与自身共轭当且仅当 a 是 G 的中心元素，即 a 与 G 中每个元素可换.

这样，我们便可以对群 G 中全体元素按是否共轭来进行分类，即同一类中的元素相互共轭，不同类中的元素不共轭. 特别，当 G 为有限群时，如果用 c_0 表示 G 的中心 C 的元素个数，别的共轭类(如果存在的话，每类中元素的个数都大于 1)设为 C_1，C_2，…，C_m 且其元素的个数分别表示为 $c_1, c_2, \cdots, c_m$ (即 $|C_i| = c_i, i = 1, 2, \cdots, m$)，于是有以下等式：

$$|G| = c_0 + c_1 + \cdots + c_m. \tag{1}$$

这个等式叫做群 G 的类等式或类方程(也称群等式或群方程).

例 1 易知 S_3 的元素有三个共轭类，即

$$(1); \quad (12), (13), (23); \quad (123), (132).$$

故

$$S_3 = \{(1)\} \cup \{(12),(13),(23)\} \cup \{(123),(132)\}.$$

从而 S_3 的类等式为

$$|S_3| = 6 = 1 + 3 + 2.$$

下面讨论每个共轭类中元素个数同群的阶的进一步的关系. 为此需要以下概念.

定义 2 设 S 是群 G 的一个子集. 称

$$N(S) = \{x \mid x \in G, xS = Sx \text{ 即 } xSx^{-1} = S\}$$

为 S 在 G 中的正规化子.

元素 a 的正规化子简记为 $N(a)$.

定理 1 设 S 是群 G 的任一非空子集. 则

1) $N(S) \leq G$;

2) 当 $S = H \leq G$ 时, $H \quad N(H)$ 且 $H \quad N(H)$.

证 1) 因为 $e \in N(S)$, 故 $N(S)$ 非空. 又在 $N(S)$ 中任取 x, y, 则 $xS = Sx$, $yS = Sy$. 从而

$$x^{-1}S = Sx^{-1},$$

$$(xy)S = x(yS) = x(Sy)$$

$$= (xS)y = (Sx)y = S(xy).$$

即 x^{-1}, $xy \in N(S)$, 故 $N(S) \leq G$.

2) 任取 $a \in H$, 由于 H 是子群, 故 $aH = Ha$, 从而

$$H \quad N(H).$$

又任取 $b \in N(H)$, 则 $bH = Hb$, 从而 $H \quad N(H)$.

(证毕)

如果 $H \quad K \leq G$, 则对 K 中任意元素 k 便有 $kH = Hk$, 从而便有 $k \in N(H)$, 即

$$K \quad N(H).$$

这就是说, 子群 H 的正规化子 $N(H)$(也叫 H 的正规化群)是 G 中以 H 作为其正规子群的最大子群.

显然, 子群 H 的正规化子是整个群 G 当且仅当 H 是群 G 的

一个正规子群．另外，也可能出现另一个极端，即 $H = N(H)$．例如，三次对称群 S_3 的子群 $H = \{(1), (12)\}$就属于这种情况．

下面再将元素的共轭进一步推广到子集的共轭．

定义 3 设 S 是群 G 的一个非空子集，则称 xSx^{-1} $(x \in G)$ 为 S 的一个共轭子集．

当 S 为子群时，称 xSx^{-1} 为 S 的一个共轭子群．

易知，子集的共轭关系是群的所有非空子集间的一个等价关系．从而可依此分类，每个这样的类称为一个 轭子集类．

同样，群的子群的共轭关系则是一个群的所有子群间的一个等价关系，因此，也可将一个群的所有子群按是否共轭来进行分类，每个这样的类都称为一个 轭子群类．

又易知，群 G 的子群 H 只与自身共轭(即此共轭子群类只含一个子群)的充分与必要条件是，H 是 G 的一个正规子群．

下面给出一个共轭子集类中子集的个数．

定理 2 设 S 是群 G 的一个非空子集，$N(S)$为 S 在 G 中的正规化子．则 G中与 S 共轭的子集数等于$(G : N(S))$，即 S 的所有共轭子集与 G 关于 $N(S)$的所有陪集间可建立双射．

证 令 M 是 G 中含 S 的共轭子集类(即与 S 共轭的全体子集)，再令

$$\phi: \quad xSx^{-1} \quad \to \quad x \cdot N(S) . \qquad (\forall\, x \in G)$$

若 $xSx^{-1} = ySy^{-1}$，则便有$(y^{-1}x)S = S(y^{-1}x)$，从而

$$y^{-1}x \in N(S), \quad x \cdot N(S) = y \cdot N(S) .$$

即 ϕ是 M 到 $N(S)$的左陪集的一个映射．又易知 ϕ还是满射和单射，从而为双射．

(证毕)

当 S只包含一个元素或 S 为子群时，可分别得到以下两个推论．

推论 1 群 G中与元素 a 共轭的元素个数为$(G : N(a))$．

由此可知，当 G为有限群时，G的每个共轭类 C_i $(i = 1, 2,$

…, m)中的元素个数 $c_i=(G:N(a_i))$，其中 $a_i\in C$．因此它们都是$|G|$的因数，且 G 的类等式(1)也可以改写成

$$|G|=|C|+\sum_{i=1}^{m}(G:N(a_i)),\qquad (2)$$

其中 C 是群 G 的中心，$a_i\in C$，$i=1,2,\cdots,m$．

推论 2 群 G 中与子群 H 共轭的子群个数为$(G:N(H))$．

同样，当 G 为有限群时，G 中每个共轭子群类中的子群个数都是$|G|$的一个因数．

作为类等式的一个应用，下面证明有限群的一个重要性质，它在一定意义下是 Lagrange 定理的逆定理．

定理 3(A .L .Cauchy) 设 G 是一个有限群，且$|G|=pn$，其中 p 是一个素数．则 G 有 p 阶子群．

证 对 n 用归纳法．

当 $n=1$ 时，G 是 p 阶群，G 本身就是 G 的一个 p 阶子群，定理成立．

假定对一切阶为 $pk(1\leq k<n)$ 的群结论成立，下证对阶为 pn 的群 G 结论成立．

分两种情况讨论．

1) 若有 $H<G$ 使 $p\nmid(G:H)$，则由于

$$pn=|G|=|H|(G:H),$$

故 $p\mid|H|$．于是由归纳假设，H 有 p 阶子群，它也是 G 的 p 阶子群;

2) 若对任意 $H<G$ 都有 $p\mid(G:H)$，则由于类等式 (2) 中的$N(a_i)<G$,故

$$p\mid(G:N(a_i)),\quad i=1,2,\cdots,m.$$

但是$|G|=pn$，于是由类等式(2)知，$p\mid|C|$．但中心 C 是交换群，故由§2 定理 5 知，C 有 p 阶子群，它当然也是 G 的一个 p

阶子群.

(证毕)

推论 3 pq 阶群(p, q 为素数且 $p < q$)有惟一的 q 阶正规子群.

证 由定理 3 知，pq 阶群 G 有 q 阶子群 H. 由于对 G 中任意元素 x，xHx^{-1} 都是 G 的 q 阶子群，而由上一章§7 推论 3 知，G 只有一个 q 阶子群，从而

$$xHx^{-1} = H.$$

因此，H 是 G 的惟一的 q 阶正规子群.

(证毕)

为进一步讨论共轭元素类同共轭子群类间的关系，先证明以下

引理 1 设 S，T 是群 G 的两个共轭子集，且 $T = cSc^{-1}$，$c \in G$，则

$$N(T) = cN(S)c^{-1}, \text{即 } N(cSc^{-1}) = cN(S)c^{-1}.$$

证 任取 $x \in N(T)$，则 $xT = Tx$. 由于 $T = cSc^{-1}$，故有

$$x(cSc^{-1}) = (cSc^{-1})x \quad \text{或} \quad (c^{-1}xc)S = S(c^{-1}xc).$$

从而 $c^{-1}N(T)c \quad N(S)$，$N(T) \quad cN(S)c^{-1}$.

同理，由于 $S = c^{-1}Tc$，故由上知 $N(S) \quad c^{-1}N(T)c$，从而

$$cN(S)c^{-1} \quad N(T).$$

因此，$N(T) = cN(S)c^{-1}$，即 $N(cSc^{-1}) = cN(S)c^{-1}$.

(证毕)

群的一个共轭子群类与一个共轭元素类间有以下关系.

定理 4 设 G 是群 G 的一个共轭元素类. 则 G 中各元素的正规化子作成的集合恰好是 G 的一个共轭子群类.

证 任取 a，$b \in G$，且设 $b = cac^{-1}$. 则由引理 1 知，有

$$N(b) = cN(a)c^{-1}.$$

又设子群 H 与 $N(a)$ 共轭，其中 $a \in G$. 令

$$H = dN(a)d^{-1},$$

则由引理 1 知,

$$H = N(dad^{-1}).$$

但是 $dad^{-1} \in G$, 即与 $N(a)$共轭的子群必为 C_1 中某个元素的正规化子.

(证毕)

再来讨论共轭子群的指数.

引理 2 共轭子群在群中有相同的指数.

证 设 H, K 是群 G 的两个共轭子群, 且 $K = cHc^{-1}$, 则由引理 1 知,

$$N(K) = cN(H)c^{-1}.$$

于是易知

$$\phi: \quad x \to cxc^{-1} \quad (x \in N(H))$$

是 $N(H)$ 到 $N(K)$ 的同构映射, 且 $\phi(H) = K$. 又因 $H \subset N(H), K \subset N(K)$, 从而由第一同构定理知, $N(H)/H \cong N(K)/K$, 故

$$(N(H) : H) = (N(K) : K).$$

又因为

$$(G : H) = (G : N(H))(N(H) : H),$$

$$(G : K) = (G : N(K))(N(K) : K),$$

而 H 与 K 共轭, 故由推论 2 知, $(G : N(H)) = (G : N(K))$. 从而

$$(G : H) = (G : K).$$

(证毕)

现在来证明以下重要结果.

* **定理 5** 如果群 G 中有一个具有限指数(大于 1)的子群, 则在 G 中必有一个具有限指数(大于 1)的正规子群.

证 设 $H < G$ 且 $(G : H)$ 有限, 则由于

$$(G : H) = (G : N(H)) \cdot (N(H) : H),$$

故$(G:N(H))$有限，从而 G 中与 H 共轭的子群个数有限．令

$$H_1=H,\ H_2,\ \cdots,\ H_m$$

为与 H 共轭的共轭子群类．由于$(G:H)$有限，故由引理 2，每个$(G:H_i)$均有限．于是由 Poincare 定理，交

$$K=H_1\cap H_2\cap\cdots\cap H_m$$

的指数也有限；又由于 $H_1,\ H_2,\ \cdots,\ H_m$ 是 G 的一个共轭子群类，故对任意 $x\in G$，显然

$$xH_1x^{-1},\quad xH_2x^{-1},\ \cdots,\ xH_mx^{-1}$$

仍是这个共轭类，只不过可能其中的子群次序不同．于是

$$xKx^{-1}=\bigcap_{i=1}^{m}xH_ix^{-1}=K,$$

即 $K\quad G$．又因为 $K=H_1\cap H_2\cap\cdots\cap H_m\quad H<G$，故

$$K\quad G.$$

从而$(G:K)$有限且大于 1．

（证毕）

本节最后，我们介绍一个和正规化子极为相近的概念．

定义 4 设 S 是群 G 的一个非空子集．称

$$C(S)=\{x\mid x\in G,\ x\text{ 与 }S\text{ 中每个元素可换}\}$$

为 S 在 G 中的<u>中心化子</u>．

例 2 求 $S=\{(12),(13)\}$在三次对称群 S_3 中的正规化子和中心化子．

解 易知

$$N(S)=\{(1),(23)\},\ C(S)=\{(1)\}.$$

显然，对群 G 中任意一个元素 a 来说，其中心化子与正规化子则是一致的，即 $C(a)=N(a)$．

另外易知 $C(S)\leq G$，而且整个群 G 的中心化子 $C(G)$就是 G 的中心．但是应注意，与正规化子不同，即使 S 是一个子群，也不一定有

$$S\quad C(S).$$

这种情况的一个极端例子是，当 G 是一个非交换群时，显然

$$G \supsetneq C(G) .$$

又显然 $C(S) \subseteq N(S)$．更进一步地有

定理 6 设 H 是群 G 的一个子群，则

$$C(H) \subseteq N(H) .$$

证 任取 $c \in C(H)$，$x \in N(H)$，则有 $Hx = xH$．于是对 H 中任意元素 h，有 $h' \in H$ 使

$$hx = xh' \quad \text{或} \quad x^{-1}hx = h' .$$

由此，再根据 c 同 H 中每个元素可换，故可得

$$\begin{aligned}(xcx^{-1})h &= xc(x^{-1}h) = xch'x^{-1} \\ &= xh'cx^{-1} = h(xcx^{-1}) .\end{aligned}$$

于是 $xcx^{-1} \in C(H)$，从而 $C(H) \subseteq N(H)$．

(证毕)

其实，从这个定理的证明可知，当 H 是群 G 的任意非空子集时，定理结论仍然成立．

习题 3.6

1. 试分别写出四次单位根乘群 U_4 和四次对称群 S_4 的类等式．

2. 证明：群中子集的共轭关系是一个等价关系．

3. 证明：

1) 若 C_1，C_2 是群 G 的两个共轭元素类，则 C_1C_2 是 G 的一些共轭元素类的并集；

2) 若 C_1 是群 G 的一个共轭元素类，则 $C_1^{-1} = \{x^{-1} \mid x \in C_1\}$，更一般地 C_1^m (m 为任意整数) 也是 G 的一个共轭元素类．

4. 设 a 是群 G 的一个元素，证明：

$$\langle a \rangle \subseteq N(a) \subseteq N(\langle a \rangle) .$$

5. 证明：S_n 的所有对换构成一个共轭类．

6. 设 G 是有限群，且 $H < G$．证明：

$$G \neq \bigcup_{x \in G} xHx^{-1} .$$

提示：反证法并利用推论 2．

* §7 群■的■直■积

在群的研究中，往往要从已知的群出发，来研究与其相关联的一些群，如子群、正规子群和商群，等等．其中商群就是从已知的群与其正规子群出发所构造出来的一种新的群，它与原来的群有着密切的联系．本节要介绍另外一种非常重要而且基本的方法，利用这种方法也可以从已知的群构造出新的群来，这就是群的直积．

首先介绍加氏积的概念．

设 A_1，A_2，…，A_n 为任意 n 个集合，则称集合

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

为这 n 个集合的加氏积．并且规定

$$(a_1, a_2, \cdots, a_n) = (b_1, b_2, \cdots, b_n)$$

当且仅当 $a_1 = b_1$，$a_2 = b_2$，…，$a_n = b_n$．

在加氏积的基础上，我们来介绍群的直积的概念．

定理 1 设 A_1，A_2，…，A_n 为任意 n 个群．则加氏积 $A_1 \times A_2 \times \cdots \times A_n$ 对运算

$$(a_1, a_2, \cdots, a_n)(b_1, b_2, \cdots, b_n) = (a_1 b_1, a_2 b_2, \cdots, a_n b_n)$$

作成一个群，称为群 A_1，A_2，…，A_n 的__积__，而称每个 A_i 为这个直积的一个直积因子．

证 群定义中各条件的验算是显然的．特别，若 e_i 是 A_i 的单位元时，则

$$(e_1, e_2, \cdots, e_n)$$

是直积的单位元，而 $(a_1^{-1}, a_2^{-1}, \cdots, a_n^{-1})$ 是 $(a_1, a_2, \cdots, a_n)$ 的逆元．

(证毕)

易知，直积是交换群(有限群)当且仅当每个直积因子都是交换群(有限群)．而且当每个 A_i 都是有限群时，有

$$|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdot \cdots \cdot |A_n| .$$

在直积中，若令

$$G_i = \{(e_1, \cdots, e_{i-1}, a_i, e_{i+1}, \cdots, e_n) \mid a_i \in A_i\},$$

则易知

$$\phi: \quad a_i \to (e, \cdots, e_{i-1}, a_i, e_{i+1}, \cdots, e_n)$$

是 A_i 到 G_i 的一个同构映射．因此，G_i 是直积的一个子群，且

$$A_i \cong G_i, \quad i = 1, 2, \cdots, n .$$

定理 2 设 A_1，A_2，$\cdots$，A_n 是 n 个群，又

$$G = A_1 \times A_2 \times \cdots \times A_n,$$

则 G 的上述子群 G_1，G_2，$\cdots$，G_n 与 G 有以下关系：

1) G_1，G_2，$\cdots$，G_n 都是 G 的正规子群；

2) $G = G_1 G_2 \cdots G_n$，即 G 中每个元素都可表为 G_1，G_2，$\cdots$，G_n 中元素的积；

3) $G_1 G_2 \cdots G_{i-1} \cap G_i = e, \quad i = 2, \cdots, n$.

证 1) 例如，任取

$$(a_1, e_2, \cdots, e_n) \in G_1, \quad (x_1, x_2, \cdots, x_n) \in G,$$

其中 e_i 为群 A_i 的单位元，则

$$(x_1, x_2, \cdots, x_n)(a_1, e_2, \cdots, e_n)(x_1, x_2, \cdots, x_n)^{-1}$$
$$= (x_1 a x_1^{-1}, e_2, \cdots, e_n) \in G_1,$$

故 $G_1 \quad G$.

同理有 $G_i \quad G$，$i = 2, \cdots, n$.

2) 与 3) 显然 .

(证毕)

定义 1 设 G_1，G_2，$\cdots$，G_n 为群 G 的 n 个子群．如果这 n 个子群满足定理 2 中的条件 1), 2), 3)，则称群 G 是子群 G_1，G_2，$\cdots$，G_n 的内直积．而把定理 1 中所说的直积称为外直积 .

定理 3 设 G_1，G_2，$\cdots$，G_n 为群 G 的 n 个子群，则 G 是这 n 个子群的内直积的充分与必要条件是：

1° $G = G_1 G_2 \cdots G_n$，且 G 中每个元素的表示法是惟一的；

2° G_i 中任意元素同 $G_j\ (i\neq j)$中任意元素可换．

证 必要性．设 G是子群 G_1，G_2，…，G_n 的内直积，但 G 中有元素表为 G_1，G_2，…，G_n 中元素相乘时不惟一．令

$$g=a_1\cdots a_{i-1}a_i\cdots a_n=b_1\cdots b_{i-1}b_i\cdots b_n\quad(a_j,b_j\in G_j),$$

$$a_i\neq b_i,\qquad a_{i+1}=b_{i+1},\qquad\cdots,\qquad a_n=b_n,$$

则有

$$(b_1\cdots b_{i-1})^{-1}(a_1\cdots a_{i-1})=b_ia_i^{-1}\in G_1\cdots G_{i-1}\cap G_i,$$

这与 $G_1\cdots G_{i-1}\cap G_i=e$矛盾．故条件 1°成立．

又设 $i\neq j$，任取 $a_i\in G_i$，$a_j\in G_j$，则由定理 2 知，G_i，G_j 都是 G的正规子群，故

$$a_ia_ja_i^{-1}a_j^{-1}\in G_i\cap G_j\ .$$

但由定理 2 易知 $G_i\cap G_j=e$，故

$$a_ia_ja_i^{-1}a_j^{-1}=e,\qquad a_ia_j=a_ja_i,$$

即条件 2°也成立．

充分性 设 G的子群 G_1，G_2，…，G_n 满足条件 1°，2°，下证必满足定理 2 中的条件 1)，2)，3)．

满足条件 2)显然，故只用证明满足条件 1)，3)．

任取 $g_i\in G_i$，$a\in G$，且令

$$a=a_1a_2\cdots a_i\cdots a_n\quad(a_j\in G_j,\ j=1,\cdots,n),$$

则由 2°易知

$$ag_ia^{-1}=a_ig_ia_i^{-1}\in G_i,$$

故 $G_i\quad G$，即定理 2 中的条件 1)成立．

又若 $G_1G_2\cdots G_{i-1}\cap G_i\neq e$，则必有

$$e\neq a_i=a_1a_2\cdots a_{i-1}\in G_1G_2\cdots G_{i-1}\cap G_i,$$

其中 $a_j\in G_j$，$j=1$，…，$i-1$．这与 1°矛盾．故定理 2 中的条件 3) 也成立．因此，群 G是子群 G_1，G_2，…，G_n 的内直积．

(证毕)

这个定理说明，对于子群的内直积来说，定理 2 中的条件 1)，2)，3)同条件 1°，2°是等价的．从而也可以利用条件 1°，2°来作

为内直积的定义.

另外易知,定理 2 中的条件 3)也可以换成条件 3′)

$$G_1 G_2 \cdots G_{i-1} G_{i+1} \cdots G_n \cap G_i = e,$$

$$i = 1, 2, \cdots, n.$$

由定理 2 知,由群的外直积可以引出一个内直积.同样,由内直积也将引出一个外直积.

事实上,设群 G 是其子群 G_1, G_2, …, G_n 的内直积,则令

$$\text{群} = G_1 \times G_2 \times \cdots \times G_n,$$

易知

$$\varphi: \quad a_1 a_2 \cdots a_n \to (a_1, a_2, \cdots, a_n) \quad (a_i \in G_i)$$

是群 G 与群群的一个同构映射.因此

$$G \cong \text{群}.$$

这样一来,如果把同构的群不加区分的话,外直积与内直积就是一致的了.因此,当群 G 是子群 G_1, G_2, …, G_n 的内直积时,也往往表示成

$$G = G_1 \times G_2 \times \cdots \times G_n.$$

而且在一般情况下,把内或外直积均简称为积.

由直积定义可知,对一个直积,可以在其直积因子间添加括号或去掉括号,而且直积因子也可以任意交换次序.

例 1 设 $G = \blacksquare a \blacksquare$ 为 n 阶循环群, $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$ 为 n 的标准分解式,则易知 G 是子群

$$G_i = \blacksquare a^{p_1^{k_1} \cdots p_{i-1}^{k_{i-1}} p_{i+1}^{k_{i+1}} \cdots p_s^{k_s}} \blacksquare \qquad (i = 1, 2, \cdots, s)$$

的直积: $G = G_1 \times G_2 \times \cdots \times G_s$. 其中 $|G_i| = p_i^{k_i}$.

证 显然 G_i G. 又令 $n_i = p_1^{k_1} \cdots p_{i-1}^{k_{i-1}} p_{i+1}^{k_{i+1}} \cdots p_s^{k_s}$, 则

$$(n_1, n_2, \cdots, n_s) = 1.$$

故存在整数 u_1, u_2, …, u_s 使

$$n_1 u_1 + n_2 u_2 + \cdots + n_s u_s = 1.$$

从而,任取 $a^m \in G$, 有

$$a^m = (a^{n_1})^{mu_1}(a^{n_2})^{mu_2}\cdots(a^{n_s})^{mu_s} \in G_1 G_2 \cdots G_s .$$

因此，$G = G_1 G_2 \cdots G_s$．再因 $|G_i| = p_i^{k_i}$，而 $G_1 G_2 \cdots G_{i-1} \cap G_i = e$，因此

$$G = G_1 \times G_2 \times \cdots \times G_s .$$

例 2 设 $G = \blacksquare a \blacksquare$ 为 2 阶循环群．则易知外直积

$$G \times G = \{(e, e), (e, a), (a, e), (a, a)\}$$

与 Klein 四元群 K_4 同构．

下面利用直积来定义两类重要的群．

定义 2 一个群如果能够分解成它的真子群的直积，则称这个群为可分解群；否则称为 不可分解群．

一个群若能够分解成其真子群且为单群的直积，则称为 全可分解群．

例 3 S_n 是不可分解群．

证 由本章 §2 知，当 $n \neq 4$ 时 S_n 的非平凡正规子群只有 A_n．又易知 S_4 的非平凡正规子群只有 A_4 与 Klein 四元群 K_4，而且 $K_4 \quad A_4$．因此，S_n 是不可分解群．

例 4 有理数加群 Q_+ 是不可分解群．

证 设 H，K 是 Q_+ 的任二真子群，则有

$$0 \neq \frac{b}{a} \in H, \qquad 0 \neq \frac{d}{c} \in K .$$

于是易知

$$0 \neq bd = ad \cdot \frac{b}{a} = bc \cdot \frac{d}{c} \in H \cap K,$$

即 Q_+ 的任二真子群的交都不是 0．因此，Q_+ 是不可分解群．

(证毕)

定理 4 无限循环群是不可分解群；n 阶循环群是不可分解群当且仅当 n 为素数的方幂．

证 1) 设 H，K 是无限循环群 $G = \blacksquare a \blacksquare$ 的任二真子群，且

$$H = \blacksquare a^{s} \blacksquare, \qquad K = \blacksquare a^{t} \blacksquare .$$

则由习题 2. 7 知，

$$H \cap K = \blacksquare a^{[s,\ t]} \blacksquare \neq e,$$

即 $G = \blacksquare a \blacksquare$ 中任二真子群的交都不是 e. 因此，G 是不可分解群 .

2) 设 $G = \blacksquare a \blacksquare$，且 $|a| = p^{k}$，p 为素数；又设 H，K 为 G 的任二真子群，且

$$H = \blacksquare a^{p^{s}} \blacksquare, \qquad K = \blacksquare a^{p^{t}} \blacksquare, \qquad 0 < s < t < k,$$

则 $H \cap K = \blacksquare a^{p^{t}} \blacksquare = K \neq e$. 因此，$G$ 是不可分解群 .

反之，设 n 阶循环群 $G = \blacksquare a \blacksquare$ 不可分解，则由例 1 知 n 必为素数的方幂 .

(证毕)

定理 5 设 G 是一个完全可分解群，且 N G. 则有 H G 使

$$G = N \times H,$$

即完全可分解群的任何正规子群都是其直积因子 .

证 设 $G = G_1 \times G_2 \times \cdots \times G_n$，其中 G_i 为 G 的真子群且为单群，则显然有

$$G = N \cdot G_1 G_2 \cdots G_n . \qquad (1)$$

但是 $N \cap G_1$ G_1，G_1 是单群，故

$$N \cap G_1 = G_1, \quad \text{或} \quad N \cap G_1 = e .$$

当 $N \cap G_1 = G_1$ 时，有 $NG_1 = N$，这时可在(1)式中把 G_1 删去；当 $N \cap G_1 = e$ 时，有 $NG_1 = N \times G_1$，这时可在(1)式中把 NG_1 改写成 $N \times G_1$.

如此继续下去，一般由于

$$(N \cdot G_1 G_2 \cdots G_{k-1}) \cap G_k \quad G_k,$$

但 G_k 为单群，从而

$$NG_1 G_2 \cdots G_{k-1} \cap G_k = G_k,$$

或

$$NG_1 G_2 \cdots G_{k-1} \cap G_k = e .$$

同上面道理，可以在(1)中把 G_k 删去或把

$$(NG_1G_2\cdots G_{k-1})G_k$$

改写成

$$(NG_1G_2\cdots G_{k-1})\times G_k,$$

按此法把多余的 G_i 一一删去，而把剩下的乘积改为直积，即得

$$G=N\times G_{i_1}\times\cdots\times G_{i_r}.$$

令 $H=G_{i_1}\times\cdots\times G_{i_r}$，即得

$$G=N\times H.$$

(证毕)

推论　完全可分解群的正规子群及商群均为完全可分解群.

证　在定理 5 的证明中，把

$$G=G_1\times G_2\times\cdots\times G_n$$

中不同于 G_{i_1}，…，G_{i_r} 的直积因子的乘积记为 N'，则有

$$G=N'\times G_{i_1}\times\cdots\times G_{i_r}.$$

但由定理 5 知，

$$G=N\times G_{i_1}\times\cdots\times G_{i_r},$$

从而可知 $N'\supseteq N$. 由于 N'是完全可分解群，故 G 的正规子群 N 也是完全可分解群.

又由定理 5，$G=N\times H$，从而 $G/N\cong H$. 但正规子群 H 是完全可分解群，从而商群 G/N 为完全可分解群.

(证毕)

习题　3.7

1. 设 $G=G_1\times\cdots\times G_n$. 证明：当 $i\neq j$ 时，

$$G_i\cap G_j=e.$$

2. 证明：定理 3 中的“每个元素表示法惟一”可改为“单位元表示法惟一”.

3. 设 $G=G_1\times G_2$，$G=G_1'\times G_2$. 证明：

$$G_1\cong G_1'.$$

4. 设 $G = G_1 \times G_2 \times \cdots \times G_n$. 证明:

$$\varphi_i: \quad a_1 a_2 \cdots a_n \to a_i \quad (a_j \in G_j)$$

是群 G 到 G_i 的满同态 .

5. 设 G_1 , G_2 是两个群 . 证明:

$$G_1 \times G_2 \cong G_2 \times G_1 .$$

6. 设群 $G = G_1 \times G_2$. 证明: $G' \cong G_1$, G_2 , $G' \cong G_2$, G_1 .

7. 设群 $G = G_1 \times G_2$, $N \trianglelefteq G_1$. 证明: $N \trianglelefteq G$.

8. 设 G_1 , G_2 , … , G_n 是群 G 的正规子群且 $G = G_1 G_2 \cdots G_n$. 证明:

$G_1 G_2 \cdots G_{i-1} \cap G_i = e$ G 中每个元素表示法惟一 .

* §8 Sylow 定理

有限群是代数学的一个重要分支, 它在群的理论中占着非常重要的地位 . 有限群之所以重要, 不仅因为这种理论对数学本身特别是群论产生重要影响, 而且在实际应用中, 例如在理论物理、量子力学、量子化学以及结晶学等方面都有广泛应用 . 前述关于有限单群分类问题解决后, 对整个有限群理论研究带来深远影响, 一些长期得不到解决的猜想迎刃而解 . 尽管如此, 有限群理论中仍存在大量问题等待进一步研究解决 .

在本书此前的所有讨论中, 除置换群外, 虽然也不断地涉及到有限群并得到有限群的一些结论, 但那仍然是关于有限群的一些零星结果 . 本章最后两节, 将集中介绍关于有限群理论中两个最基本最重要的内容, 即 Sylow 定理和有限交换群基本定理 . 本节先讨论关于有限群的 Sylow 定理 .

根据 Lagrange 定理, 如果 H 是有限群 G 的一个子群, 则 $|H|$ 是 $|G|$ 的一个因数 . 但是, 这个定理的逆定理不成立, 即若 m 是 $|G|$ 的一个因数, 则 G 并不一定有 m 阶子群 . 例如, 四次交代群 A_4 , $|A_4| = 12$, 尽管易知它有 2, 3, 4 阶子群, 但它却没有 6 阶子群 .

虽然不是对$|G|$的每个因数 m 群 G 都有 m 阶子群，但是对 $|G|$的某些特殊因数 m，G却有 m 阶子群．例如§6 定理3 指出，对$|G|$的每个素因数 p，G必有 p 阶子群．本节要证明的 Sylow 定理，将进一步推广这一结果，并包含着与其相关联的一系列非常深刻的结论．

定义1 设 G是一个有限群，且$|G| = p^s m$，其中 p 是素数，s是非负整数，$p \nmid m$．则称 G的 p^s 阶子群为 G 的一个 Sylow p - 子群．

Sylow p - 子群有时也简称为Sylow 子群．

对于任意有限群 G与任意的素数 p 来说，G的 Sylow p - 子群是否存在？如果存在，有多少个以及它们之间有些什么样的关系？以下所证明的三个 Sylow 定理，将对这些问题作出全面而彻底的回答．

为了证明 Sylow 定理，我们下面先介绍重陪集概念及其简单性质．

定义2 设 H，K 为群 G(不一定有限)的两个子群，又令 $x \in G$．则称 G的子集

$$HxK = \{hxk \mid h \in H, k \in K\}$$

为群 G关于子群 H，K 的一个重陪集．

简称 HxH 为关于 H 的一个重陪集．

引理1 对群 G的任二重陪集 HxK 与 HyK，若

$$HxK \cap HyK \neq \varnothing,$$

则必 $HxK = HyK$．

证 由于 $HxK \cap HyK \neq \varnothing$，故有元素 $a \in HxK \cap HyK$．令

$$a = h_1 x k_1 = h_2 y k_2 \quad (h_i \in H, k_i \in K),$$

则 $x = h_1^{-1} h_2 y k_2 k_1^{-1} \in HyK$．从而对任意 $h \in H$，$k \in K$，有

$$hxk = (hh_1^{-1} h_2) y (k_2 k_1^{-1} k) \in HyK,$$

因此，$HxK \subseteq HyK$.

同理有 $HyK \subseteq HxK$. 故 $HxK = HyK$.

(证毕)

由于对群 G 中任何元素 x 总有 $x \in HxK$，因此，这个引理表明，类似于群的左或右陪集分解，可将 G 分解成互不相交的若干个重陪集的并. 而称这种分解为群 G 关于子群 H，K 的重陪集分解.

另外，显然

$$HxK = \bigcup_{k \in K} Hxk = \bigcup_{h \in H} hxK,$$

即重陪集 HxK 是一切形如 $Hxk(k \in K)$ 的右陪集的并；同时也是一切形如 $hxK(h \in H)$ 的左陪集的并. 因此，群 G 的重陪集分解，实际上就是 G 的普通左或右陪集分解按某种方式的重组与合并.

现在进一步问：包含在重陪集 HxK 内的 H 的右陪集有多少个？

下面引理回答这个问题.

引理 2 在群 G 的重陪集 HxK 中，含子群 H 的右陪集的个数等于 $(K : K \cap x^{-1}Hx)$；含子群 K 的左陪集的个数等于

$$(H : H \cap xKx^{-1}).$$

证 设

$$S = \{Hxk \mid k \in K\}, \quad T = \{(K \cap x^{-1}Hx)k \mid k \in K\};$$

并令 $\varphi: Hxk \to (K \cap x^{-1}Hx)k \quad (\forall k \in K)$.

如果 $Hxk_1 = Hxk_2 (k_1, k_2 \in K)$，则

$$xk_1 \cdot k_2^{-1}x^{-1} \in H, \quad k_1k_2^{-1} \in x^{-1}Hx,$$

从而 $k_1k_2^{-1} \in K \cap x^{-1}Hx$. 因此

$$(K \cap x^{-1}Hx)k_1 = (K \cap x^{-1}Hx)k_2,$$

这说明 φ 是 S 到 T 的一个映射.

类似证明，可知 φ 是单射. 又显然 φ 是满射.

因此，φ是 S 到 T 的一个双射．

同理可证引理中的另一结论．

(证毕)

有了以上引理，下面就可以来证明三个 Sylow 定理了．

定理 1(第一 Sylow 定理——存在性和包含性) 设 G 是有限群，且 $|G| = p^s m$，其中 p 是素数，s 是正整数，$p \nmid m$．则对 G 的每个 $p^i\ (i = 0, 1, \cdots, s-1)$ 阶子群 H，总存在 G 的 p^{i+1} 阶子群 K 使 $H \subset K$．

证 设 G 关于 $p^i\ (0 \leq i < s)$ 阶子群 H 的重陪集分解为

$$G = Hx_1H \cup Hx_2H \cup \cdots \cup Hx_rH, \tag{1}$$

且 Hx_jH 是由 t_j 个 H 的右陪集所组成．于是由引理 2 知

$$t_j = (H : H \cap x_j^{-1}Hx_j), \quad j = 1, 2, \cdots, r. \tag{2}$$

由于 $|H| = p^i$，故 $t_j \mid p^i$，且由(1)可得

$$(G : H) = t_1 + t_2 + \cdots + t_r. \tag{3}$$

由(2)知，若某个 $t_j = 1$，则

$$H = H \cap x_j^{-1}Hx_j \subset x_j^{-1}Hx_j.$$

但是 $|H| = |x_j^{-1}Hx_j| = p^i$，故 $H = x_j^{-1}Hx_j$．从而

$$x_jH = Hx_j, \quad x_j \in N(H).$$

反之，对任意 $Ha \subset N(H)$，则令 $Ha \subset Hx_jH\ (1 \leq j \leq r)$．但由于 $a \in Ha$，从而

$$a \in N(H) \cap Hx_jH, \quad Ha = aH.$$

令 $a = h_1x_jh_2\ (h_1, h_2 \in H)$，则 $x_j = h_1^{-1}ah_2^{-1}$．于是由此易知

$$Ha = Hx_j = x_jH, \quad x_j^{-1}Hx_j = H,$$

因此又有 $t_j = (H : H \cap x_j^{-1}Hx_j) = 1$．

以上表明，在 $t_1, t_2, \cdots, t_r$ 中 $t_j = 1$ 的个数就是 $x_1, x_2, \cdots, x_r$ 在 $N(H)$ 中的个数 $(N(H) : H)$．

由于 $|G| = p^s m = |H|(G : H) = p^i(G : H)\ (i = 0, 1, \cdots, s-1)$，故

$$p \mid (G : H),$$

从而由(3)知,

$$p \mid (N(H) : H), \quad p \mid | N(H)/H |,$$

于是由§6 定理3 知, $N(H)/H$ 有 p 阶子群 K/H, 其中 $H \subset K$ 且

$$| K | = | K/H | \cdot | H | = p \cdot p^i = p^{i+1}.$$

由于当 $i = 0$ 时 $p^0 = 1$ 阶子群(即单位元群)总存在, 从而以上论证表明 p, p^2, …, p^s 阶子群总存在, 且其中的 p^i 阶子群还是 p^{i+1} 阶子群的正规子群. 特别其中的 p^s 阶子群就是 G 的 Sylow p - 子群.

(证毕)

定理 2(第二 Sylow 定理 - 共轭性) 设 G 是有限群, p 是素数. 则 G 的所有 Sylow p - 子群恰好是群 G 的一个共轭子群类.

证 设 $| G | = p^s m$, $p \nmid m$. 显然, 与 Sylow p - 子群共轭的子群都是 Sylow p - 子群.

下面进一步证明: G 的任二 Sylow p - 子群必共轭.

设 H, K 是群 G 的任二 Sylow p - 子群, 从而

$$| H | = | K | = p^s.$$

根据引理 1, 设 G 关于 H, K 的重陪集分解为

$$G = Hx_1K \cup Hx_2K \cup \cdots \cup Hx_rK,$$

且重陪集 Hx_iK 中含 H 的右陪集的个数为

$$t_i = (K : K \cap x_i^{-1} H x_i), \quad i = 1, 2, \cdots, r.$$

由此得

$$(G : H) = t_1 + t_2 + \cdots + t_r. \tag{4}$$

由于 $| G | = | H | \cdot (G : H)$ 和 $| H | = p^s$, 故 $p \nmid (G : H)$; 又因为每个 t_i 都是 p 的非负整数次方幂, 故由(4)知, 至少有一个 $t_i = 1$. 例如不妨设 $t_1 = 1$, 即

$$(K:\ K\cap x_1^{-1}Hx_1)=1,$$

从而 $K=K\cap x_1^{-1}Hx_1$ $x_1^{-1}Hx_1$. 但是 $|K|=|x_1^{-1}Hx_1|=p^s$, 故

$$K=x_1^{-1}Hx_1,$$

即 H 与 K 共轭 .

因此, G 的全体 Sylow p - 子群恰好是一个共轭子群类 .

(证毕)

例 1 求出三次对称群 S_3 的所有 Sylow p - 子群 .

解 由于 $|S_3|=6=2\cdot 3$, 故当素数 $p\neq 2$, 3 时, S_3 的 Sylow p - 子群就是 S_3 的 $p^0=1$ 阶子群, 即 $\{(1)\}$. S_3 的 Sylow 2 - 子群 $(p=2)$ 有 3 个, 即

$$H_1=\{(1),(12)\},\quad H_2=\{(1),(13)\},$$

$$H_3=\{(1),(23)\}.$$

它们是 S_3 的一个共轭子群类 . 最后, S_3 的 Sylow 3 - 子群 $(p=3)$ 只有一个, 即 $H_4=\{(1),(123),(132)\}$, 它当然是 S_3 的一个正规子群 .

再来证明最后一个 Sylow 定理 .

定理 3(第三 Sylow 定理——计数定理) 设 G 是有限群, 且 $|G|=p^sm$, 其中 p 是素数, $p\nmid m$. 若 G 的 Sylow p - 子群共有 k 个, 则 $k\mid |G|$ 且

$$k\equiv 1(\mathrm{mod}\ p).$$

证 首先, 设 H 是群 G 的一个 Sylow p - 子群, 则由定理 2 及 §6 推论 2 知,

$$k=(G:\ N(H)).$$

从而 $k\mid |G|$.

其次, 根据引理 1, 设

$$G=Hx_1H\cup Hx_2H\cup\cdots\cup Hx_rH$$

是 G 关于 H 的重陪集分解, 并设

$$t_i = (H : H \cap x_i^{-1} H x_i) \quad (i = 1, 2, \cdots, r)$$

是 HxH 中含 H 的右陪集的个数，则

$$(G : H) = t_1 + t_2 + \cdots + t_r . \tag{5}$$

同定理 1 一样，t_1，t_2，…，t_r 中共有 $(N(H) : H)$ 个是 1，而其余的 t_i 都是 p 的正整数次幂．于是由(5)知

$$p \mid (G : H) - (N(H) : H) .$$

但是

$$(G : H) = (G : N(H)) \cdot (N(H) : H) = k(N(H) : H), \tag{6}$$

故

$$p \mid (N(H) : H) \cdot (k - 1) . \tag{7}$$

又因为现在的 H 是 G 的 Sylow p - 子群，故 $p \nmid (G : H)$．从而由(6)知，$p \nmid (N(H) : H)$．再由(7)得 $p \mid k - 1$，即

$$k \equiv 1 \pmod{p} .$$

(证毕)

作为第三 Sylow 定理的一个应用，我们来证明

定理 4 设 G 是有限群，$|G| = pq$，其中 p，q 是互异的素数，且 $p \nmid q - 1$，$q \nmid p - 1$．则 G 是一个循环群．

证 由第三 Sylow 定理，G 的 Sylow p - 子群的个数 k 整除 $|G| = pq$，且 $p \mid k - 1$，从而 $p \nmid k$，$(k, p) = 1$，故 $k \mid q$．但 q 是素数，故

$$k = 1 \text{ 或 } q .$$

又由假设 $p \nmid q - 1$，故 $k \neq q$，只有 $k = 1$．即 G 只有一个 Sylow p - 子群 P，从而是 G 的一个正规子群．

同理，G 只有一个 Sylow q - 子群 Q，它也是 G 的一个正规子群．

由于 $p \neq q$，故 $|P| = p$，$|Q| = q$，从而 P，Q 都是素阶循环群．设

$$P = \blacksquare a \blacksquare , \qquad Q = \blacksquare b \blacksquare ,$$

由 Lagrange 定理知，$|P\cap Q|=1$．但是 $P \quad G$，$Q \quad G$，故

$$aba^{-1}b^{-1}\in P\cap Q, \qquad ab=ba,$$

于是 $|ab|=pq=|G|$．因此，G 是循环群且

$$G=\blacksquare ab\blacksquare .$$

(证毕)

例 2 凡 15 阶群都是循环群．

证 设 G 是任意一个 15 阶群．由于 $|G|=3\cdot 5$，$3\nmid 5-1$，$5\nmid 3-1$，故由定理 4 知，G 是一个循环群．

例 3 凡 33 阶群及 35 阶群都是循环群．

证 同例 1 一样，由定理 4 直接可得．

例 4 凡 200 阶群都不是单群．

证 设 G 是任意一个 200 阶群．则由于

$$|G|=200=2^3\cdot 5^2,$$

故 G 有 5^2 阶子群，即 G 的 Sylow 5-子群．设 G 共有 k 个 Sylow 5-子群，则由第三 Sylow 定理知，

$$k\mid 2^3\cdot 5^2 \quad 且 \quad k\equiv 1 \pmod 5.$$

由此又易知只能 $k=1$．即 G 的 Sylow 5-子群只有一个．于是仍由第三 Sylow 定理知，它是 G 的正规子群．故 G 不是单群．

(证毕)

一般来说，一个群不能是其 Sylow 子群的直积．例如，由例 1 可知，三次对称群 S_3 就属于这种情况．

下面给出有限群是其 Sylow 子群直积的充要条件．

定理 5 设 G 是有限群，且 $|G|=p_1^{k_1}p_2^{k_2}\cdots p_m^{k_m}$ 为标准分解式．则 G 是其 Sylow p_i-子群 $P_i(i=1,2,\cdots,m)$ 的直积的充要条件是，每个 P_i 都是 G 的正规子群．

证 必要性显然，下证充分性．

设每个 $P_i(i=1,2,\cdots,m)$ 都是 G 的正规子群．则由于

$$|P_i|=p_i^{k_i}, \quad i=1,2,\cdots,m,$$

从而有 $|P_1P_2\cdots P_m|=p_1^{k_1}p_2^{k_2}\cdots p_m^{k_m}=|G|$．因此

$$G = P_1 P_2 \cdots P_m .$$

又易知 $P_1 P_2 \cdots P_{i-1} \cap P_i = e$, $i = 2, \cdots, m$, 故

$$G = P_1 \times P_2 \times \cdots \times P_m .$$

(证毕)

顺便指出，这个定理中的 Sylow p_i - 子群 P_i 就是由 G 中所有阶为 p_i 的方幂的元素作成的集合 .

由定理 5 立即可得

推论 1 任何有限交换群都是其所有 Sylow 子群的直积 .

对于有限交换群来说，Lagrange 定理的逆定理也成立 . 即以下的

推论 2 设 G 是有限交换群 . 如果 $d \mid |G|$, 则 G 有 d 阶子群 .

证 设 $|G| = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ 为 $|G|$ 的标准分解式 .由于 $d \mid |G|$, 故可设

$$d = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m},$$

其中 $0 \leq r_i \leq k_i$, $i = 1, 2, \cdots, m$. 但由第一 Sylow 定理知，G 有 $p_i^{r_i}$ 阶子群 $H_i (i = 1, 2, \cdots, m)$, 从而 G 有 d 阶子群

$$H = H_1 \times H_2 \times \cdots \times H_m .$$

(证毕)

下一节我们还将进一步专门讨论有限交换群的基本理论 .

本节最后介绍一种与 Sylow p - 子群密切相关的群— p - 群 .

定义 3 若群 G 中每个元素的阶都有限，并且都是素数 p 的方幂，则称 G 是一个 p - 群 .

习题 2. 4 第 5 题中的群 G_p 是一个无限 p - 群 .

显然，由第一 Sylow 定理知，有限群 G 的每个 p - 子群都包含在 G 的某个 Sylow p - 子群中 .

当然，群 G 的两个不同的 p - 子群可能会包含在 G 的两个不同的 Sylow p - 子群中 .

关于有限 p - 群，有以下

定理 6 有限群 G 是 p - 群的充要条件是，$|G|$ 是 p 的方幂 .

证 充分性显然，下证必要性 .

设有限群 G 是 p - 群，但 $|G|$ 有素因数 $q \neq p$.则由 Sylow 定理知，G 有 q 阶元素 这与 G 是 p - 群矛盾 .因此，$|G|$ 必是素数 p 的方幂 .

(证毕)

由于 Sylow p - 子群都是 p - 群，因此由推论 1 可知，任何有限交换群都可表为 p - 群的直积 . 这表明在群论中研究 p - 群的重要性 .

p - 群有很多基本和重要的性质，不再赘述 .

习题 3.8

1. 试求出 4 次交代群 A_4 的所有 Sylow 子群 .

2. 设 G 是 np 阶群 $(p$ 是素数 $)$. 证明：若 $n < p$，则 G 有 p 阶正规子群 .

提示：利用第三 Sylow 定理 .

3. 设 G 是一个有限群，P 是 G 的一个 Sylow p - 子群，H 是 G 的一个 p 子群 . 证明：若 $H \quad N(P)$，则 $H \quad P$.

4. 设 K 是群 G 的一个有限正规子群，P 是 K 的一个 Sylow p - 子群 . 证明：$G = N(P)K$.

5. 设 P 是有限群 G 的一个 Sylow p - 子群 . 证明：若 G 有子群 H 包含 $N(P)$，则 $N(H) = H$.

6. 证明：有限群 G 必有一个最大的正规 p - 子群 H .即 H 是 G 的正规 p - 子群，又若 K 也是 G 的正规 p - 子群，则必 $K \quad H$.

7. 证明：196 阶群 G 必有一个阶大于 1 的 Sylow 子群，它是 G 的一个正规子群 .

8. 设 H, K 是群 G(不一定有限)的两个 p - 子群，且 $K \quad G$. 证明：HK 也是 G 的一个 p - 子群 .

提示：利用群同构定理：$HK/K \cong H/H \cap K$.

*§9 有限交换群

上一节利用 Sylow 定理证明了有限交换群可以分解成它的 Sylow 子群的直积．但 Sylow 子群不一定是循环群，也不一定是不可分解群．本节将进一步加细这种分解，从而得到有限交换群的基本定理和结构定理．

为证明有限交换群的基本定理，先证明以下

引理 设 a 是群 G 的一个有限阶元素，且 $H \leq G$．又设 k 是使 $a^k \in H$ 的最小正整数．则

1) 当 $a^s \in H$ 时，$k \mid s$;

2) 当 $\blacksquare a \blacksquare \cap H \neq e$ 时，$k < |a|$．

证 1) $\blacksquare$ 令

$$s = kq + r, \quad 0 \leq r < k.$$

则由于 $H \leq G$, 故

$$a^s = a^{kq} \cdot a^r, \quad a^r = a^s \cdot (a^k)^{-q} \in H.$$

再由 k 的最小性知，$r = 0$．因此，$k \mid s$．

2) 因为 $\blacksquare a \blacksquare \cap H \neq e$, 故有 $b \in \blacksquare a \blacksquare \cap H$，$b \neq e$．令

$$b = a^s \in H.$$

因为 $a^{|a|} = e \in H$，故由 k 的最小性知，$k \leq |a|$．

如果 $k = |a|$, 则由 1) 知，$|a| \mid s$．于是

$$b = a^s = e,$$

这与 $b \neq e$ 矛盾．因此，$k < |a|$．

(证毕)

定理 1(有限交换群基本定理) 任何阶大于 1 的有限交换群 G 都可以惟一地分解为素幂阶循环群(从而为不可分解群)的直

积:

$$G = \blacksquare a_1 \blacksquare \times \blacksquare a_2 \blacksquare \times \cdots \times \blacksquare a_n \blacksquare ,$$

其中$\blacksquare a_i \blacksquare$是 $p_i^{\alpha_i}$ (p_i 为素数, $i = 1, 2, \cdots, n$)阶循环群 .

我们称每个 $p_i^{\alpha_i}$ ($i = 1, 2, \cdots, n$)为群 G的初等因子, 而称其全体 $p_{11}^{\alpha_1}$, $p_{22}^{\alpha_2}$, $\cdots$, $p_{nn}^{\alpha_n}$ 为群 G的 等因子组 .

证 由于阶大于 1 的有限交换群都可以惟一地分解为其 Sylow 子群的直积, 故只需假设 G 是素幂阶有限交换群即可 . 因此, 设

$$| G | = p^{\alpha}, \quad p \text{是素数}, \quad \alpha \text{是正整数} .$$

1) 存在性 设 $G = \blacksquare a_1, a_2, \cdots, a_n \blacksquare$, 且 a_1 , a_2 , $\cdots$, a_n 是 G 的使

$$| a_1 | + | a_2 | + \cdots + | a_n |$$

最小的一组 n 元生成系 . 即对 G 的任何一组 n 元生成系 x_1 , x_2 , $\cdots$, x_n 均有

$$| a_1 | + | a_2 | + \cdots + | a_n | \leq | x_1 | + | x_2 | + \cdots + | x_n | .$$

下证:

$$G = \blacksquare a_1 \blacksquare \times \blacksquare a_2 \blacksquare \times \cdots \times \blacksquare a_n \blacksquare . \tag{1}$$

为此, 令

$$H_i = \prod_{j \neq i} \blacksquare a_j \blacksquare , \quad i = 1, 2, \cdots, n,$$

于是, 要证 1) 成立显然只需证明

$$\blacksquare a_i \blacksquare \cap H_i = e, \quad i = 1, 2, \cdots, n .$$

设若不然, 例如不妨设

$$\blacksquare a_i \blacksquare \cap H_i \neq e, \quad i = 1, 2, \cdots, r,$$

$$\blacksquare a_j \blacksquare \cap H_j = e, \quad j = r+1, \cdots, n,$$

其中 $r \geq 1$. 现在令 k_i 是使 $a_i^{k_i} \in H_i$ ($i = 1, 2, \cdots, r$)的最小正整数且不妨设

$$k_1 = \min(k_1, k_2, \cdots, k_r),$$

则由于 $a_i^{| a_i |} = e \in H_i$, 故由引理, $k_i \mid | a_i |$. 但是, $| G | =$

p^{α}，故每个 $|a_i|$ (从而每个 k_i)都是 p 的方幂．于是

$$k_1 \mid k_i, \quad i=2,3,\cdots,r, \tag{2}$$

特别，由引理还可知

$$k_1 < |a_1| . \tag{3}$$

再由于 $a_1^{k_1} \in H_1 = \langle a_2 \rangle \langle a_3 \rangle \cdots \langle a_n \rangle$，故可令

$$a_1^{k_1} = a_2^{s_2} a_3^{s_3} \cdots a_r^{s_r} a_{r+1}^{s_{r+1}} \cdots a_n^{s_n}, \tag{4}$$

从而由此可知

$$a_j^{s_j} \in \langle a_j \rangle \cap H_j = e, \quad j=r+1,\cdots,n,$$

故 $a_j^{s_j} = e$，$j=r+1,\cdots,n$．于是由(4)知

$$a_1^{k_1} = a_2^{s_2} a_3^{s_3} \cdots a_r^{s_r}, \tag{5}$$

由此等式又可知 $a_i^{s_i} \in H_i$，从而由引理，$k_i \mid s_i$．再由(2)知，$k_1 \mid s_i (i=2,3,\cdots,r)$．令

$$s_i = k_1 q_i, \quad i=2,3,\cdots,r, \tag{6}$$

并且令

$$b_1 = a_1 a_2^{-q_2} \cdots a_r^{-q_r}, \tag{7}$$

则由此可知 $a_1 = b_1 a_2^{q_2} \cdots a_r^{q_r}$．从而

$$G = \langle b_1, a_2, \cdots, a_n \rangle,$$

即 b_1，a_2，$\cdots$，a_n 也是群 G 的一组 n 元生成系．

然而由(7)以及(5)、(6)可知

$$b_1^{k_1} = a_1^{k_1} a_2^{-k_1 q_2} \cdots a_r^{-k_1 q_r} = e,$$

于是由(3)知，$|b_1| \leq k_1 < |a_1|$．从而

$$|b_1| + |a_2| + \cdots + |a_n| < |a_1| + |a_2| + \cdots + |a_n|,$$

这与 $|a_1| + |a_2| + \cdots + |a_n|$ 的最小性矛盾．

因此，(1)式成立．

2) 惟一性 设

$$G = \langle a \rangle \times \langle a \rangle \times \cdots \times \langle a \rangle = \langle b \rangle \times \langle b \rangle \times \cdots \times \langle b \rangle \tag{8}$$

是 G 的两种这样的分解，且其初等因子组分别为

$$m_1,\ m_2,\ \cdots,\ m_r\ ,\qquad n_1,\ n_2,\ \cdots,\ n_s\ .$$

由于 $|G| = p^{\alpha}$，故每个 m_i 和每个 n_j $(i = 1, 2, \cdots, r;\ j = 1, 2, \cdots, s)$都是 p 的方幂．不妨假定

$$m_1 \geq m_2 \geq \cdots \geq m_r,\qquad n_1 \geq n_2 \geq \cdots \geq n_s\ .$$

①■若 $r \neq s$ 且不妨设 $r < s$，又 $m_1 = n_1,\ \cdots,\ m_r = n_r$．则由(7)知，$G$ 的阶按第一种分解为

$$m_1 m_2 \cdots m_r = n_1 n_2 \cdots n_r,$$

而按第二种分解又为

$$n_1 n_2 \cdots n_r \cdot n_{r+1} \cdots n_s,$$

这显然是不可能的．

②■若 $m_1 = n_1,\ \cdots,\ m_{t-1} = n_{t-1}$，但 $m_t > n_t$．则令

$$H = \{x^{n_t} \mid x \in G\},$$

并由此易知 $H \leq G$ 且由(8)有

$$H = \blacksquare a_1^{n_t} \blacksquare \times \cdots \times \blacksquare a_r^{n_t} \blacksquare = \blacksquare b_1^{n_t} \blacksquare \times \cdots \times \blacksquare b_s^{n_t} \blacksquare\ .$$

因为 $|a_i| = m_i$，故

$$|a_i^{n_t}| = \frac{m_i}{(n_t, m_i)},\qquad i = 1,\ 2,\ \cdots,\ r\ .$$

但因 m_i，n_j 都是 p 的方幂，故 $n_t \mid m_i$ $(i = 1, 2, \cdots, t)$．从而 H 的阶按第一种分解为正整数

$$\frac{m_1}{n_t},\ \frac{m_2}{n_t},\ \cdots,\ \frac{m_{t-1}}{n_t},\ \frac{m_t}{n_t},\ \frac{m_{t+1}}{(n_t, m_{t+1})},\ \cdots,\ \frac{m_r}{(n_t, m_r)}$$

之积．同理，H 的阶按其第二种分解又为正整数

$$\frac{n_1}{n_t},\ \frac{n_2}{n_t},\ \cdots,\ \frac{n_{t-1}}{n_t},\ \blacksquare 1,\ \ 1,\ \ \cdots,\ \ 1$$

之积．这显然也是不可能的．

因此，由①与②可知：$r = s$ 且 $m_i = n_i$ $(i = 1, 2, \cdots, r)$．从而 ■a_i■ ■b_i■．亦即 G 的两种分解的初等因子组相同．

(证毕)

应注意，如果有限交换群 G 的初等因子组为

$p_1^{k_1}$，$p_2^{k_2}$，…，$p_n^{k_n}$，则其中的素数 p_1，p_2，…，p_n 不一定是互不相同的，甚至也可以是完全相同的．另外，在 G 的两种这种分解中，如果 $|a_i| = |b_i|$，则只能肯定 $\blacksquare a_i \blacksquare \cong \blacksquare b_i \blacksquare$，但却不一定有

$$\blacksquare a_i \blacksquare = \blacksquare b_i \blacksquare .$$

由定理 1 可知，一个有限交换群完全由其初等因子组所决定．

定理 2　两个阶大于 1 的有限交换群同构的充要条件是，二者有相同的初等因子组．

证　1) 充分性．设阶大于 1 的有限交换群 G 与 $\blacksquare$ 有相同的初等因子组：

$$p_1^{k_1},\ p_2^{k_2},\ \cdots,\ p_n^{k_n} .$$

则由定理 1 知，G 与 $\blacksquare$ 有相应的分解：

$$G = \blacksquare a_1 \blacksquare \times \blacksquare a_2 \blacksquare \times \cdots \times \blacksquare a_n \blacksquare ,$$

$$\blacksquare = \blacksquare b_1 \blacksquare \times \blacksquare b_2 \blacksquare \times \cdots \times \blacksquare b_n \blacksquare ,$$

其中 $|a_i| = |b_i| = p_i^{k_i}$，$i = 1, 2, \cdots, n$．于是据此易知

$$\varphi: \quad a_1^{x_1} a_2^{x_2} \cdots a_n^{x_n} \qquad b_1^{x_1} b_2^{x_2} \cdots b_n^{x_n}$$

(其中 $x_1, x_2, \cdots, x_n$ 为任意整数)是群 G 到 $\blacksquare$ 的一个同构映射，因此

$$G \cong \blacksquare .$$

2) 必要性．设 $G \cong \blacksquare$，且仍用 φ 表示群 G 到 $\blacksquare$ 的一个同构映射．如果 G 的初等因子组为

$$p_1^{k_1},\ p_2^{k_2},\ \cdots,\ p_n^{k_n} ,$$

则由定理 1 知，G 有分解

$$G = \blacksquare a_1 \blacksquare \times \blacksquare a_2 \blacksquare \times \cdots \times \blacksquare a_n \blacksquare ,$$

其中 $|a_i| = p_i^{k_i}$，$i = 1, 2, \cdots, n$．在 φ 之下仍设

$$\varphi: \quad a_i \qquad b_i , \qquad i = 1, 2, \cdots, n,$$

由于 φ 是同构映射，故

$$|b_i| = |a_i| = p_i^{k_i} , \qquad i = 1, 2, \cdots, n,$$

从而由此以及 $|\overline{G}| = |G| = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$ 可知

$$\overline{G} = \overline{\langle b_1 \rangle} \times \overline{\langle b_2 \rangle} \times \cdots \times \overline{\langle b_n \rangle},$$

即 $\overline{G}$ 与 G 有相同的初等因子组 $p_1^{k_1}$, $p_2^{k_2}$, …, $p_n^{k_n}$.

(证毕)

我们知道，循环群是完全研究清楚了的一个群类．现在由定理 1 与定理 2 可知，有限交换群也是研究清楚了的另一个重要群类．这两类群在群论的整个研究中占着重要地位并起着基本的作用．

下面介绍一种特殊的有限交换群．

定义 初等因子组为 $p, p, \cdots, p$ (p 为素数)的有限交换群，称为<u>等交换群</u>．

例 1 给出 Klein 四元群的分解和其初等因子组．

解 令 $e=(1)$, $a=(12)$, $b=(34)$, $c=(12)(34)$, 则 Klein 四元群为

$$K_4 = \{e, a, b, c\},$$

且易知

$$K_4 = \langle a \rangle \times \langle b \rangle = \langle a \rangle \times \langle c \rangle = \langle b \rangle \times \langle c \rangle,$$

从而其初等因子组为 2，2．因此，Klein 四元群是一个初等交换群．

例 2 在同构意义下，给出所有 8 阶交换群．

解 因为 $8 = 2^3$，故相应 8 阶交换群的初等因子组共有三种：

$$2^3, \quad 2, 2^2, \quad 2, 2, 2.$$

因此，在同构意义下 8 阶交换群共有三个，即

$$C_8, \quad C_2 \times C_4, \quad C_2 \times C_2 \times C_2,$$

其中 C_i 为 i 阶循环群，$i=2, 4, 8$．

例 3 在同构意义下，给出所有 45 阶交换群．

解 因为 $45 = 3^2 \cdot 5$，故相应 45 阶交换群的初等因子组共有二种：

3^2，5 ， 3，3，5 .

因此，在同构意义下45阶交换群共有二个，即

$$C_9 \times C_5, \quad C_3 \times C_3 \times C_5,$$

其中 C_i 为 i 阶循环群，$i=3,5,9$.

而且由此可知，45阶交换群都不是初等交换群 . 实际上，更一般的，凡阶有两个或两个以上互异素因子的交换群都不是初等交换群 .

有限交换群基本定理，是有限交换群的最重要的结构定理 . 但是，有限交换群还有另一形式的结构定理，即以下的

定理3(不变因子定理) 任何阶大于1的有限交换群 G 都可以惟一地分解为

$$G = \blacksquare b_1 \blacksquare \times \blacksquare b_2 \blacksquare \times \cdots \times \blacksquare b_m \blacksquare,$$

其中 $|b_i| > 1 (i=1,2,\cdots,m)$，且 $|b_i| \mid |b_{i+1}|$，$i=1,2,\cdots,m-1$.

我们称每个 $|b_i|$ 为群 G 的不变因子，而称其全体 $|b_1|, |b_2|, \cdots, |b_m|$ 为 G 的不变因子组 .

证 1) 存在性 . 根据定理1，设 G 的全体初等因子不妨是

$$p_1^{k_{11}} \le p_1^{k_{12}} \le \cdots \le p_1^{k_{1s_1}}, \quad \cdots, \quad p_r^{k_{r1}} \le p_r^{k_{r2}} \le \cdots \le p_r^{k_{rs_r}}, \tag{9}$$

其中 $p_1, p_2, \cdots, p_r$ 为互异的素数 . 并设在 G 的直积分解中，相应于初等因子 $p_i^{k_{ij}}$ 的循环群为 $\blacksquare a_{ij} \blacksquare$ (即 $|a_{ij}| = p_i^{k_{ij}}$) . 现在令 $m = \max(s_1, s_2, \cdots, s_r)$，且

$$b_m = a_{1s_1} a_{2s_2} \cdots a_{rs_r} .$$

则易知

$$\begin{aligned} |b_m| &= |a_{1s_1}| \cdot |a_{2s_2}| \cdots |a_{rs_r}| \\ &= p_1^{k_{1s_1}} p_2^{k_{2s_2}} \cdots p_r^{k_{rs_r}} . \end{aligned}$$

再令 $b_{m-1} = a_{1,s_1-1} \cdot a_{2,s_2-1} \cdots a_{r,s_r-1}$，同样有

$$|b_{m-1}| = p_1^{k_{1,s_1-1}} p_2^{k_{2,s_2-1}} \cdots p_r^{k_{r,s_r-1}} .$$

如此下去(当某个 $p_i^{k_{ij}}$ 在(8)中取完时就不再取)，可得 b_1，b_2，$\cdots$，b_{m-1}，b_m，且显然有

$$G = \blacksquare b_1 \blacksquare \times \blacksquare b_2 \blacksquare \times \cdots \times \blacksquare b_m \blacksquare$$

和 $|b_i| > 1$，$|b_i| \mid |b_{i+1}|$.

2) 惟一性．设 G 除上面的分解外另有

$$G = \blacksquare c_1 \blacksquare \times \blacksquare c_2 \blacksquare \times \cdots \times \blacksquare c_s \blacksquare,$$

其中 $|c_i| > 1$，$|c_i| \mid |c_{i+1}|$．则将每个循环群 $\blacksquare c_i \blacksquare$ 按定理 1 分解为阶是素数幂的循环群的直积，所有这些素数幂 $(i = 1, 2, \cdots, s)$ 就是 G 的初等因子组，即 (8)．

但由于 $|c_i| \mid |c_{i+1}|$，故必

$$|c_s| = p_1^{k_{1s_1}} p_2^{k_{2s_2}} \cdots p_r^{k_{rs_r}} = |b_m|,$$

如此下去，必 $s = m$ 且 $|c_i| = |b_i|$，从而 $\blacksquare c_i \blacksquare$ 与 $\blacksquare b_i \blacksquare$ 同构，$i = 1, 2, \cdots, m$.

(证毕)

由定理 2 和定理 3 直接可得以下

推论　两个阶大于 1 的有限交换群同构的充要条件是，二者有相同的不变因子组．

例 4　设 C_i 是 i 阶循环群．求有限交换群

$$G = (C_2 \times C_8) \times (C_3 \times C_9 \times C_9) \times (C_5 \times C_{25})$$

的初等因子组、不变因子组和关于不变因子的直积分解．

解　G 的初等因子组为

$$2, 2^3;\quad 3, 3^2, 3^2;\quad 5, 5^2;$$

再根据定理 3 可知，G 的不变因子组为 $2^3 \cdot 3^2 \cdot 5^2$，$2 \cdot 3^2 \cdot 5$，3，即

$$3, 90, 1800.$$

最后，关于 G 的不变因子的直积分解为

$$G = C_3 \times (C_2 \times C_9 \times C_5) \times (C_8 \times C_9 \times C_{25})$$
$$= C_3 \times C_{90} \times C_{1800}.$$

例 5　在同构意义下，利用不变因子给出所有 72 阶交换群．

解　因为 $72 = 2^3 \cdot 3^2$，故相应于 72 阶交换群的初等因子组共有以下六种：

$2,2,2,3,3$ ， $2,2^2,3,3$ ， $2^3,3,3$ ，

$2,2,2,3^2$ ， $2,2^2,3^2$ ， $2^3,3^2$ ．

故相应的不变因子组也共有六种，即

2，6，6 ， 6，12 ， 3，24 ，

2，2，18 ， 2，36 ， 72 ．

从而互不同构的 72 阶交换群共有六个，它们是

$C_2\times C_6\times C_6$， $C_6\times C_{12}$， $C_3\times C_{24}$，

$C_2\times C_2\times C_{18}$， $C_2\times C_{36}$， C_{72} ．

由本节讨论明显可知，有限交换群的初等因子和不变因子的概念和理论，完全类似于高等代数中 λ- 矩阵的初等因子和不变因子的概念和理论 ．

习题 3.9

1．证明：对任意素数 p_1， p_2，…， p_m 和任意正整数 k_1， k_2，…， k_m，总存在有限交换群 G，其初等因子组为

$$p_1^{k_1}\ ,\ p_2^{k_2}\ ,\ \cdots,\ p_m^{k_m}\quad .$$

2．设 p 是素数．试给出同构意义下的所有 p^4 阶交换群．

3．给出同构意义下的所有 108 阶交换群 ．

4．设 G 是阶大于 1 的有限群．证明：若除 e 外其余元素的阶均相同，则 G 为素幂阶群 ．

5．设 G 是有限交换群．证明：G 是循环群的充要条件是，$|G|$ 是 G 中所有元素的最小公倍 ．

提示：利用习题 2.7 第 12 题 ．

6．用 C_k 表示 k 阶循环群．证明：

$$C_{m_1}\times C_{m_2}\times\cdots\times C_{m_n}\cong C_{m_1m_2\cdots m_n}$$

当且仅当正整数 m_1， m_2，…， m_n 两两互素 ．

7．设 G 是群，$H\leqslant G$．证明：如果关于 H 的任意两个左陪集的乘积仍是一个左陪集，则 $H\lhd G$ ．

8．举例指出，存在群 G，C 为其中心，而商群 G/C 的中心的阶大于 1 ．

9．设 $N\lhd G$，$|N|=m$，$(m,n)=1$．证明：若 $|a|=n$，则 aN 的

阶也是 n；反之，若 aN 的阶是 n，则在 G 中有 n 阶元 b 使 $aN = bN$．

提示：令 $ms + nt = 1$，$b = a^{ns}$．

10. 称群 G 中元素 $a^{-1}b^{-1}ab$ 为元素 a 与 b 的换位元．证明：

1) 由 G 中所有换位元生成的子群 K 是 G 的一个正规子群；

2) G/K 是交换群；

3) 若 $N \trianglelefteq G$，且 G/N 可换，则 $N \geqslant K$．

11. 设 H，K 是群 G 的两个有限正规子群，并且 $(|H|, |K|) = 1$．证明：如果商群 G/H 与 G/K 都是交换群，则 G 也是交换群．

12. 设 k 是一个奇数．证明：$2k$ 阶群 G 必有 k 阶子群．

提示：在 G 中取一个 2 阶元 a，可先证

$$G = x_1, \cdots, x_k, ax_1, \cdots, ax_k;$$

再由 Cayley 定理，$G \cong$ 一个置换群且

$$(x_1, ax_1)(x_2, ax_2)\cdots(x_k, ax_k) \in$$ 这个置换群

再利用第二章 §6 例 3 即得．

13. 设 G 是一个有限 p-群．证明：G 的中心 C 的阶大于 1．

14. 证明：p^2 阶群必是交换群，其中 p 是一个素数．

提示：利用上题和习题 3.2 第 6 题．

15. 证明：群 G 的子集 S 的中心化子等于 S 中各元素的正规化子的交．

16. 证明：如果有限 p-群 G 只有一个指数为 p 的子群，则 G 是一个循环群．

提示：令 $|G| = p^n$，并对 n 用归纳法．

17. 证明：n 阶群的自同构群是有限群，且其阶是 $(n-1)!$ 的一个因数．

18. 设 G_1，G_2 是两个群．证明：若 $G_1 \cong G_2$，则 $AutG_1 \cong AutG_2$．再举例指出反之不成立．

19. 设 P 是有限群 G 的一个 Sylow p-子群，$N \trianglelefteq G$．证明：

1) $P \cap N$ 是 N 的一个 Sylow p-子群；

2) PN/N 是 G/N 的一个 Sylow p-子群．

20. 设 S_3 是 $M = 1, 2, 3$ 上的三次对称群．证明：

$$\mathrm{Aut}S_3 \cong S_3.$$

提示：$\mathrm{Aut}S_3 \ni \tau \mapsto$ 由 τ 导出 H_1，H_2，H_3 上（H_i 是 S_3 的 2 阶子群）

的一个置换．

21. 设 G 是一个有限群，且 $|G| = p^2q$，其中 p，q 是两个互异素数．证明：G 不是单群．

提示：利用 Sylow 定理．

22. 设 G 是一个有限群，且 $|G| = pqr$，其中 p，q，r 是互异素数．证明：G 不是单群．

提示：利用 Sylow 定理．

23. 证明：不存在 56 阶单群．

24. 证明：凡 455 阶群必为循环群．

提示：利用 Sylow 定理指出，455 阶群的 5、7、13 阶子群都只各有一个．

25. 设 G 是一个有限非可换单群，p 是一个素数，且 $p \mid |G|$．证明：G 的 Sylow p - 子群的个数 $k > 1$．

26. 设 G 是一个有限群，$H \quad G$，$K \quad G$，又 P 是 G 的一个 Sylow p - 子群．证明：

1) $|P \cap HK| = \dfrac{|P \cap H| \cdot |P \cap K|}{|P \cap H \cap K|}$；

2) $P(H \cap K) = PH \cap PK$．

提示：1) $P \cap H$ 是 H 的 Sylow p - 子群，其余同理；

2) $|PHK| = |P^2HK| = |PH \cdot PK|$．

27. 证明：当 $n \geq 3$ 时，全体 3 - 循环是交代群 A_n 的一个生成系．

28. 证明：当 $n \geq 5$ 时，n 次交代群 A_n 是单群．

提示：设 $e \neq H \quad A_n$．先证 H 必含 3 - 循环，再证 H 包含全体 3 - 循环．

29. 证明：当 $n \geq 5$ 时，n 次对称群 S_n 不是可解群．

30. 若一个 n 次置换是 a_1 个 1 - 循环，a_2 个 2 - 循环，…，a_n 个 n - 循环(不相连循环且每个数码都出现)之积，则称此置换有循环结构

$$1^{a_1}, 2^{a_2}, \cdots, n^{a_n} \quad .$$

证明：二 n 次置换 σ，τ 共轭 σ 与 τ 有相同循环结构．

31. 设 a 是群 G 中阶为 $m_1 m_2 \cdots m_n$ 的一个元素．证明：若正整数 m_1，m_2，…，m_n 两两互素，则 a 可惟一表示为

$$a = a_1 a_2 \cdots a_n,$$

其中 a_i 都是 a 的方幂，且 $|a_i| = m_i\ (i = 1, 2, \cdots, n)$.

提示：对 n 用数学归纳法.

第四章　环　与　域

群是有一个代数运算的代数系统．但是，我们在数学特别是在高等代数中，遇到过很重要的讨论对象，例如，数、多项式、函数以及矩阵和线性变换等，都有两个代数运算．这一事实说明，在近世代数中研究有两个代数运算的代数系统，也具有非常重要的现实意义．在有两个代数运算的代数系统中，最基本最重要的就是环与域．

环论起源于19世纪关于实数域的扩张和分类的研究．后在1908年魏得邦(J .H .M .Wedderburn) 发表了有限次代数结构定理的著名论文，给出了环结构研究的模式；又在1921年前后，诺特(E .Noether)建立了环的理想理论并提出了满足升链条件的环，即所谓的诺特环；1927年阿丁(E .Artin)又提出了用降链条件来区分环，从而得到所谓的阿丁环，并推广了魏得邦定理；1945年雅可布逊(N .Jacobson)更创造了环的根的理论，得到了环的基本而重要的构造定理．他们都为环论的研究和发展做出了非常关键和巨大的贡献．此外还有众多的数学家在环论的研究中也有不可磨灭的成就，不再一一叙述．

这一章主要介绍环与域的定义和初步性质，以及理想、环同态基本定理和一些常见的重要的环与域．

§1　环的定义

在介绍环的定义之前，我们需要先回顾一下加群的概念，并

稍作进一步地介绍 .

我们知道，一个交换群的代数运算叫做加法并用加号表示时，称为一个加群 . 为了符合通常习惯，加群中的单位元用 0 表示，并称为零元；元素 a 的逆元用 $-a$ 表示，并称为 a 的负元 . 于是有

$$0+a=a+0=a,$$

$$a+(-a)=-a+a=0 .$$

如果我们把 $a+(-b)$ 简记为 $a-b$，那么在加群中就有了一个减法，它是加法的逆运算 .

易知，在加群中以下运算规则总是成立的：

$$-a+a=a-a=0,$$

$$-(-a)=a,$$

$$a+c=b \qquad c=b-a,$$

$$-(a+b)=-a-b, \qquad -(a-b)=b-a .$$

另外，乘群中通常的指数运算规则在加群中则自然改为倍数规则，即

$$0a=0, \qquad (\text{左边的 } 0 \text{ 是数零，右边的 } 0 \text{ 是零元})$$

$$na=\overbrace{a+\cdots+a}^{n}, \qquad (-n)a=-(na), \quad n \text{ 为正整数},$$

且对任意整数 m，n 又有

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

$$m(na)=(mn)a,$$

$$n(a+b)=na+nb .$$

同样，加群的非空子集 H 能作成子群的充分与必要条件则改写成：

$$a,\ b\in H \qquad a+b\in H,$$

$$a\in H \qquad -a\in H;$$

或

$$a,\ b\in H \qquad a-b\in H .$$

有了这雪说明，下面来介绍环的定义．

定义 1 设非空集合 R 有两个代数运算，一个叫做加法并用加号 + 表示，另一个叫做乘法并用乘号表示．如果

1° R 对加法作成一个加群；

2° R 对乘法满足结合律：

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

3° 乘法对加法满足左右分配律：

$$a(b+c) = ab+ac, \quad (b+c)a = ba+ca,$$

其中 a，b，c 为 R 中任意元素，则称 R 对这两个代数运算作成一个环．

根据这个定义，凡数环都是环；另外，数域 F 上全体多项式的集合 $F[x]$，数域 F 上全体 n 阶方阵的集合以及 F 上一个向量空间的全体线性变换的集合，对各自通常的加法和乘法都作成环．我们分别称其为数域 F 上的多项式环、n 阶全阵环　性换环．

定义 2 如果环 R 的乘法满足交换律，即对 R 中任意元素 a，b 都有

$$ab = ba,$$

则称 R 为　换环(可换环)　否则称 R 为　交换环(非可换环)

如果环 R 只含有限个元素，则称 R 为有限环．否则称 R 为无限环．

有限环 R 的元素个数称为 R 的阶，无限环的阶称为无限．环 R 的阶用 $|R|$ 表示．

数环和数域上的多项式环都是交换环．当 $n>1$ 时，数域上的 n 阶全阵环和线性变换环都是非交换环．

除去数环 0 外，上面所举出的环都是无限环．在下面 §4，我们将介绍一种重要的有限环．

例 1 设 R 是一个加群，再对 R 中任意元素 a，b 规定

$$ab = 0,$$

则 R 显然作成一个环．这种环称为零乘环．

例 2 设 R 为整数集．则 R 对以下二运算作成环：

$$a \oplus b = a + b - 1, \quad a \otimes b = a + b - ab.$$

证 容易验算 R 对 $\oplus$ 作成一个加群，1 是零元，$2 - a$ 是元素 a 的负元．

此外，R 对乘法显然满足交换律，且易验证也满足结合律．下面仅证乘法对加法也满足分配律：因为

$$\begin{aligned} a \otimes (b \oplus c) &= a \otimes (b + c - 1) \\ &= a + (b + c - 1) - a(b + c - 1) \\ &= 2a + b + c - ab - ac - 1, \end{aligned}$$

$$\begin{aligned} (a \otimes b) \oplus (a \otimes c) &= (a + b - ab) \oplus (a + c - ac) \\ &= (a + b - ab) + (a + c - ac) - 1 \\ &= 2a + b + c - ab - ac - 1, \end{aligned}$$

故 $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$．

因此，R 对 $\oplus$，$\otimes$ 作成环，且是一个交换环．

（证毕）

定义 3 如果环 R 中有元素 e，它对 R 中每个元素 a 都有

$$ea = a,$$

则称 e 为环 R 的一个左单位元；如果环 R 中有元素 e'，它对 R 中每个元素 a 都有

$$ae' = a,$$

则称 e' 为环 R 的一个右单位元．

环 R 中既是左单位元又是右单位元的元素，叫做 R 的单位元．

实际上，由于环 R 对其乘法显然作成一个半群，故 R 的左、右单位元或单位元也就是该半群的左、右单位元或单位元．

如果环 R 有单位元，则显然是惟一的，一般用 1 表示．

一个环可能既无左单位元，也无右单位元，例如偶数环；也可能只有左单位元，而无右单位元，例如数域 F 上一切形如

$$\begin{matrix} a & b \\ 0 & 0 \end{matrix}$$

的方阵作成的环，$\begin{matrix} 1 & x \\ 0 & 0 \end{matrix}$ $(x\in F)$ 都是左单位元，但无右单位元．反之，也可能只有右单位元，而无左单位元，例如数域 F 上一切形如

$$\begin{matrix} a & 0 \\ b & 0 \end{matrix}$$

的方阵作成的环，$\begin{matrix} 1 & 0 \\ x & 0 \end{matrix}$ $(x\in F)$ 都是右单位元，但无左单位元．

但是，如果一个环 R 既有左单位元 e 也有右单位元 e 时，则由定义可知 $ee'=e'=e$，即它们相等，就是 R 的单位元．

例 3 证明：集合 M 的幂集 $P(M)$ 对运算

$$A+B=A\cup B-A\cap B,\qquad AB=A\cap B\quad (\forall A,B\in M)$$

作成一个有单位元的交换环．这个环称为 M 的幂集环．

证 显然，上述加法是 $P(M)$ 的代数运算且满足交换律；又显然空集 $\varnothing$ 是 $P(M)$ 的零元，而 A 的负元为 A 自身．因此，欲证 $P(M)$ 作成加群只剩下证该代数运算满足结合律．

先证：$(A+B)+C=A+(B+C)$．

任取 $x\in(A+B)+C=(A+B)\cup C-(A+B)\cap C$，则

$$x\in A+B,\ x\notin C;\qquad 或\qquad x\notin A+B,\ x\in C.$$

1° 若 $x\in A+B=A\cup B-A\cap B,\ x\notin C$，则

$$x\in A,\ x\notin B;\qquad 或\qquad x\notin A,\ x\in B.$$

若为前者，即 $x\in A,\ x\notin B,\ x\notin C$，则得 $x\notin B+C$，从而

$$x\in A\cup(B+C)-A\cap(B+C)=A+(B+C);\qquad (1)$$

若为后者，即 $x\notin A,\ x\in B,\ x\notin C$，则必 $x\in B+C$，从而也可

得(1)式．因此

$$(A+B)+C \quad A+(B+C)\ . \tag{2}$$

2° 若 $x\notin A+B$, $x\in C$, 则类似推理也可得(2)．因此，(2)式总成立．

同理可得 $A+(B+C) \quad (A+B)+C$,故

$$(A+B)+C=A+(B+C)\ .$$

因此，$P(M)$对上述加法作成一个加群．

又显然乘法满足结合律和交换律．至于乘法对加法的分配律，可类似于加法满足结合律的证法知，也成立．

又 $M\in P(M)$,且显然 M 是 $P(M)$的单位元．因此，$P(M)$对以上二运算作成一个有单位元的交换环．

(证毕)

下面进一步给出环中元素的一些运算规则．

1) $0a=a0=0$ (0 是环 R 的零元)．

因为 $0a+0a=(0+0)a=0a$,所以 $0a=0$．

又 $a0+a0=a(0+0)=a0$，所以 $a0=0$．因此

$$0a=a0=0\ .$$

2) $(-a)b=a(-b)=-ab$．

因为 $(-a)b+ab=(-a+a)b=0b=0$,故

$$(-a)b=-ab;$$

同理 $a(-b)=-ab$,得证．

3) $(-a)(-b)=ab$．

因为 $(-a)(-b)=a[-(-b)]=ab$, 故

$$(-a)(-b)=ab\ .$$

4) $c(a-b)=ca-cb$, $(a-b)c=ac-bc$．

因为 $c(a-b)=c[a+(-b)]=ca+c(-b)=ca-cb$,

$(a-b)c=[a+(-b)]c=ac+(-b)c=ac-bc$,

故得证．

5) $\sum_{i=1}^{m} a_i \sum_{j=1}^{n} b_j = \sum_{i=1}^{m}\sum_{j=1}^{n} a_i b_j$.

此等式由第一章§4 定理 3 直接可得 .

6) $(ma)(nb) = (na)(mb) = (mn)(ab)$，其中 m, n 为任意整数 .

事实上，当 m 与 n 为正整数时上式就是式 5)的特殊情况；当 m 与 n 中有一个为零时等式显然成立；当 m 与 n 中有负整数，例如 $m = -m'$ 为负整数时利用 $ma = -m'a = m'(-a)$，类似可得 .

在一般环中还可以引入正整数指数幂的概念，即令

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

当环有单位元时，还可对环中任意元素 a 规定

$$a^0 = 1 .$$

当环中有单位元，并且元素 a 有逆元(对乘法而言)，即在环中存在元素 b 使 $ab = ba = 1$ (b 由 a 惟一确定，记为 a^{-1}，且称 a 可__)时，还可对 a 引入负整数指数幂的概念，即规定

$$a^{-n} = (a^{-1})^n .$$

同样可验算通常的指数运算规则成立 .

以上诸性质说明，数的普通运算规则在环中基本都成立 . 但是应注意，并不是数的所有运算规则在环中都成立 . 例如，由于环的乘法不一定可换，因此，在一般环中以下运算规则不成立：

$$(ab)^n = a^n b^n , \qquad (a+b)^2 = a^2 + 2ab + b^2 .$$

定义 4 设 S 是环 R 的一个非空子集 . 如果 S 对 R 的加法与乘法也作成一个环，则称 S 是 R 的一个__环，记为 $S \leq R$ 或 $R \geq S$.

例 4 设 M 为任意集合 . 则 M 的全体有限子集(包括空集)作成幂集环 $P(M)$ 的一个子环 .

定理 1 环 R 的非空子集 S 作成子环的充要条件是：

$$a, b \in S \Rightarrow a - b \in S,$$

$$a, b \in S \Rightarrow ab \in S .$$

这个定理的证明是显然的，故从略 .

设 S 是环 R 的一个子环，应注意，当 R 有单位元时，S 不一定有；当 S 有单位元时，R 不一定有；即使二者都有单位元，此二单位元也未必相同．对此，可利用下面的全阵环举出各种不同的例子来．

例 5 环 R 上的 n 阶全阵环．

设 R 为任意环，称

$$A=\begin{matrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & & & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{matrix} \qquad (a_{ij}\in R)$$

为环 R 上的一个$m\times n$ 矩阵．当 $m=n$ 时，称 A 为环 R 上的一个 n 阶方阵．

环上矩阵的相等、R 中元素与矩阵的乘法以及矩阵的加法与乘法，同数域上的矩阵完全类似，不再赘述．同样可以证明，环 R 上的全体 n 阶方阵关于方阵的加法与乘法作成一个环．这个环用 $R_{n\times n}$ 表示，并称为 R 上的 n 阶全阵环．

这样，在环 R 的基础上，由于 n 为任意正整数，从而据此又可作出无数个新的环来．

当环 R 有单位元时，$R_{n\times n}$ 也有单位元，即

$$E=\begin{matrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{matrix}.$$

下面进一步设 R 为任意一个有单位元的交换环．

这样，我们也可以像高等代数中那样，来讨论 R 上方阵的行列式以及子式、代数余子式和伴随矩阵等概念．特别有

定理 2 设 R 是一个有单位元的交换环．则 R 上 n 阶全阵环 $R_{n\times n}$ 的方阵 A 在 $R_{n\times n}$ 中可逆的充要条件是，A 的行列式 $|A|$ 在 R 中可逆．

这个定理的证明同高等代数类似定理一致，故从略．

本节最后，介绍另一种环．

我们知道，一个环 R 关于其加法作成一个加群，用 $(R, +)$ 表示，并称其为 R 的加群．如果加群 $(R, +)$ 是一个循环群，则称环 R 是一个循环环．这样，如果 $(R, +) = \blacksquare a \blacksquare$，则循环环 R 可表为

$$R = \cdots, -2a, -a, 0, a, 2a, \cdots, a^2 = ka, k \text{ 为整数}.$$

特别，如果 a 在加群 $(R, +)$ 中的阶为 n，则 R 又进一步可表为

$$R = 0, a, 2a, \cdots, (n-1)a, a^2 = ka, 0 \leq k \leq n-1.$$

例如，整数环是一个无限循环环．又易知循环环必是交换环，而且循环环的子环也是循环环．但循环环不一定有单位元，例如，偶数环就是一个没有单位元的循环环．

定理 3 pq 阶环必为循环环（p, q 是两个互异素数）．

由上一章§2 推论知，这个定理的证明是显然的．

以后我们将知道，pq 阶环是一类完全清楚的环，在一定意义下这种环有而且只有 4 个．

在我们的环定义中，要求乘法必须满足结合律（从而也往往称为结合环）．受量子力学影响而发展起来的非结合环（即乘法不要求满足结合律），其研究也日趋完整．还有比结合环更广泛的环类（要求条件更弱）是 1936 年查森豪斯（H .Zassenhaus）所提出的 环（加法不要求可换）和 20 世纪 40 年代由范迪维尔（H .S . Vandiver）所提出的 环（加法只要求作成半群）．这些环受自然科学和数学中非线性同调代数、泛函分析、组合数学和计算机科学等的推动而迅速发展，现已成为环论中各个独立的分支．

但应注意，我们今后提到环时均仍指满足定义 1 的（结合）环．

习题 4.1

1. 设 R 为实数集．问：R 对数的普通加法以及新规定的乘法

$$a \quad b = |a| b$$

是否作成环？

2. 数域 F 上一切形如

$$\begin{matrix} a & b \\ 0 & 0 \end{matrix}$$

的方阵对普通加法和乘法是否作成环？是否可换和有单位元？哪些元素有逆元？

3. 设 R 为所有有理数对 (x_1, x_2) 作成的集合，加法与乘法分别为

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2),$$

$$(a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2).$$

问：R 是否作成环？是否可换和有单位元？哪些元素有逆元？

4. 如果环 R 中的元素 a 满足 $a^2 = a$，则称 a 为 R 的幂等元．如果环 R 中每个元素都是幂等元，则称 R 为 布尔(G.Boole, 1815～1864)环．证明：布尔环是交换环，而且其中任何元素 a 都有

$$a + a = 0.$$

5. 证明：加群 G 的全体自同态映射对以下运算

$$(\sigma + \tau)a = \sigma a + \tau a,$$

$$(\sigma\tau)a = \sigma(\tau a) \quad (\forall\, a \in G)$$

(σ, τ 为 G 的自同态映射)作成一个有单位元的环．

称这个环为加群 G 的自同态环．

6. 证明：对有单位元的环来说，其加法满足交换律可以由环定义中其它条件推出．

7. 设环 R 有单位元，又 $a, b \in R$．证明：如果 $a + b = ab$ 且 $1 - a$ 在 R 中有逆元，则 $ab = ba$．

提示：考虑 $(1 - a)(1 - b)$．

8. 证明：循环环必是交换环，并且其子环也是循环环．

§2 环的零因子和特征

大家知道，在数的普通乘法中，如果 $a \neq 0$，$b \neq 0$，则必 $ab \neq 0$．但这一性质在一般环中不再成立．

定义 1 设 $a \neq 0$ 是环 R 的一个元素．如果在 R 中存在元素

$b\neq 0$ 使 $ab=0$，则称 a 为环 R 的一个左零因子．

同样可定义右零因子．

左或右零因子统称为零因子，只在有必要区分时才加左或右．

不是左零因子也不是右零因子的元素，叫做正则元．

例 1　设 R 为由一切形如

$$\begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} \quad (x, y \text{ 为有理数})$$

的方阵作成的环，则 $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ 是 R 的一个左零因子，因为有

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix};$$

但 $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ 不是 R 的右零因子，因为，若

$$\begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

则只有 $x=y=0$．

例 2　数域 F 上二阶全阵环中，$\begin{pmatrix} 1 & 0 \\ 2 & 0 \end{pmatrix}$ 既是左零因子又是右零因子，因为有

$$\begin{pmatrix} 1 & 0 \\ 2 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 3 \end{pmatrix}=\begin{pmatrix} 2 & -1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 2 & 0 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

数环以及数域上的多项式环，都无零因子．

在无零因子的环中，关于乘法的消去律成立．

定理 1　在环 R 中，当 a 不是左零因子时，则

$$ab=ac,\quad a\neq 0 \qquad b=c; \tag{1}$$

当 a 不是右零因子时，则

$$ba=ca,\quad a\neq 0 \qquad b=c. \tag{2}$$

证　由 $ab=ac$，得

$$a(b-c)=0.$$

由于 $a\neq 0$ 且 a 不是左零因子，故 $b-c=0$，$b=c$.

同理可证另一结论.

(证毕)

如果对环 R 中任意元素 $a\neq 0$，b，c，(1)成立，则称环 R 满足左消去律；若(2)成立，则称 R 满足右消去律.

推论 当环 R 无左(或右)零因子时，则消去律成立；反之，若 R 中有一个消去律成立，则 R 中无左及右零因子，且另一个消去律也成立.

证 由于当 R 无左零因子时，R 也无右零因子，故由定理 1 即得消去律成立.

反之，设在 R 中左消去律成立，且

$$a\neq 0,\quad ab=0,\qquad \text{即 } ab=a0,$$

则 $b=0$，即 R 无左零因子，从而 R 也无右零因子，于是右消去律也成立.

(证毕)

定义 2 无零因子的交换环称为__环__.

例如，数环和数域上的多项式环都是整环. 而例 1 和例 2 中的方阵环都不是整环.

整环，其定义在不同的书中总稍有差异，请予留意.

下面讨论把环看作加群时，其元素的阶的情况.

定义 3 若(任意)环 R 的元素(对加法)有最大阶 n，则称 n 为环 R 的__征__(或__特征数__).

若环 R 的元素(对加法)无最大阶，则称 R 的__征是无限(或__)

用 char R 表示环 R 的特征.

由于有限群中每个元素的阶都有限，故有限环的元素对加法有最大阶，从而__限环的特征必有限__. 但是，以后将知道，无限环的特征也可能有限.

显然，一阶环即仅包含零元素的环，其特征是 1. 而在数环

中，除去 0 外，其特征均无限．

又例如，非空集合 M 的幂集环 $P(M)$ 是一个特征为 2 且除 $\varnothing$，M 外每个元素都是零因子的环．

定理 2　设 R 是一个环．令

$$M=\{n \mid n \text{ 是正整数且对 } R \text{ 中任意 } a,\ na=0\},$$

则当 M 是空集时 R 的特征无限；当 M 非空时，M 中最小的正整数就是环 R 的特征．

证　若 M 为空集，则说明 R 中元素的阶没有最大的．因若不然，设 a 是 R 中一个最大阶元，且阶为 n．由于 R 对加法是交换群，则由第二章 §2 定理 5 知，R 中任何元素的阶都是 n 的因数，从而对 R 中任何元素 x 都有

$$nx=0,$$

于是 $n\in M$．这与 M 是空集矛盾．

若 M 非空，且 n 是 M 中的最小正整数，则 R 中每个元素的阶都有限且是 n 的因数，故 R 有最大阶元．由上知，这个最大阶就是 n，因此 $\operatorname{char} R=n$．

(证毕)

一般来说，环中各元素对加法来说的阶是不相等的．但对无零因子的环来说，这种情况不会发生．

定理 3　设 R 是一个无零因子环，且 $|R|>1$．则

1)　R 中所有非零元素(对加法)的阶均相同；

2)　若 R 的特征有限，则必为素数．

证　1)　若 R 中每个非零元素的阶都无限，定理已对；若 R 中有某个元素 $a\neq 0$ 的阶为 n，则在 R 中任取 $b\neq 0$，有

$$a(nb)=(na)b=0b=0.$$

但 $a\neq 0$，R 又无零因子，故 $nb=0$，$|b|\leq n$．

设 $|b|=m$，则 $(ma)b=a(mb)=0$，$ma=0$，故 $n \mid m$．从而 $n\leq m=|b|$．

因此 $|b|=n$，即 R 中每个非零元素的阶都是 n．

2) 设 char $R=n>1$，且

$$n=n_1 n_2,\quad 1<n_i<n.$$

则在 R 中任取 $a\neq 0$，由于 R 中每个非零元素的阶都是 n，故

$$n_1 a\neq 0,\quad n_2 a\neq 0.$$

但是

$$\begin{aligned}(n_1 a)(n_2 a)&=(n_1 n_2)a^2\\&=na^2=0,\end{aligned}$$

这与 R 是无零因子环矛盾，故 n 必是素数.

(证毕)

由此定理知，特别，任何阶大于 1 的有限环若无零因子，则其特征都是素数.

定理 4 若环 R 有单位元，则单位元在加群 $(R,+)$ 中的阶就是 R 的特征.

证 若单位元 1 在 $(R,+)$ 中的阶无限，则 R 的特征当然无限；若 1 的阶是正整数 n，则在 R 中任取 $a\neq 0$，有

$$na=(n\cdot 1)a=0a=0.$$

即 n 是 R 中非零元素的最大阶，亦即

$$\text{char } R=n.$$

(证毕)

定理 5 若环 R 是交换环，特征是素数 p，则对 R 中任意元素 a_1，a_2，…，a_m 有

$$(a_1+a_2+\cdots+a_m)^p=a_1^p+a_2^p+\cdots+a_m^p.$$

证 因为将

$$(a_1+a_2+\cdots+a_m)^p$$

展开后除去项 a_1^p，a_2^p，…，a_m^p 外，其余各项的系数都是 p 的倍数，而 p 是 R 的特征，这些项都是零，随得证.

(证毕)

设 a 是环 R 的一个元素. 如果存在正整数 n，使 $a^n=0$，则称 a 是环 R 的一个幂零元.

在上节还定义过，如果 $a^2=a$，则称 a 是 R 的一个幂等元.

0 是环 R 的幂等元，也是幂零元．当 R 有单位元时，则单位元是幂等元．一般来说，一个环可能还有别的幂等元和幂零元．例如，从方阵环中很容易找到这样的元素．

显然，环中任何非零幂零元也是这个环中的零因子．

*　　*　　*　　*　　*

定义 4　设 R 是一个阶大于 1 且特征是素数 p 的环．如果对 R 中任意元素 a 都有

$$a^p = a,$$

则称 R 是一个 p - 环．

* **定理 6**　p - 环是交换环．

证　设 R 是任意一个 p - 环，并在 R 中任取元素 a，b．则

$$(a+b)^p = a^p + k_1 + k_2 + \cdots + k_{p-1} + b^p, \tag{3}$$

其中

$$k_1 = a^{p-1}b + a^{p-2}ba + a^{p-3}ba^2 + \cdots + ab a^{p-2} + ba^{p-1}, \tag{4}$$

k_2 为(3)式左端展开后 b 出现 2 次的所有项之和，…，k_{p-1} 是 b 出现 $p-1$ 次的所有项之和．

但由于 R 是 p - 环，故 $(a+b)^p = a+b$，$a^p = a$，$b^p = b$，从而由(3)知

$$k_1 + k_2 + \cdots + k_{p-1} = 0. \tag{5}$$

如果现在用 $2b$，$3b$，…，$(p-1)b$ 去代替(3)式中的 b，则根据(4)式及(5)式可知，分别有

$$jk_1 + j^2 k_2 + \cdots + j^{p-1} k_{p-1} = 0, \quad j = 2, \cdots, p-1.$$

这 $p-2$ 个等式再添上(5)式，即得以下 $p-1$ 个等式：

$$\begin{aligned} &k_1 + k_2 + \cdots + k_{p-1} = 0, \\ &2k_1 + 2^2 k_2 + \cdots + 2^{p-1} k_{p-1} = 0, \\ &\cdots\cdots \\ &(p-1)k_1 + (p-1)^2 k_2 + \cdots + (p-1)^{p-1} k_{p-1} = 0. \end{aligned} \tag{6}$$

由这 $p-1$ 个等式中诸 k_i 的系数构成一个 $p-1$ 阶行列式

$$D=\begin{vmatrix} 1 & 1 & \cdots & 1 \\ 2 & 2^2 & \cdots & 2^{p-1} \\ \cdots & \cdots & & \cdots \\ p-1 & (p-1)^2 & \cdots & (p-1)^{p-1} \end{vmatrix}$$

但由范德蒙(Vandermonde)行列式可知，有

$$D=1!\cdot 2!\cdot 3!\cdot\cdots\cdot(p-1)!\neq 0,$$

而且由于 p 是素数，故 $(p,D)=1$．从而存在整数 s，t 使

$$ps+Dt=1. \tag{7}$$

现在用行列式 D 中第 1 列各元素的代数余子式 A_{11}，A_{21}，…，$A_{(p-1)1}$ 依次分别乘(6)中的 $p-1$ 个等式后，再相加，于是由行列式性质可知

$$Dk_1=0.$$

由此，再根据(7)以及 R 的特征是 p 可得

$$k_1=1\cdot k_1=(ps+Dt)k_1=0.$$

这样，再根据(4)式以及 $a^p=a$，$b^p=b$ 便得

$$0=ak_1-k_1a=ab-ba.$$

从而有 $ab=ba$．因此，R 是交换环．

(证毕)

在后面§5，我们将看到 p-环的一个重要例子．

环的交换性的讨论，也是环的研究内容之一，其中不乏一些重要结果．一个比定理 6 更加普遍的结论是有名的 Jacobson 定理：如果环 R 中每个元素 a 都有一个与 a 有关的整数 $n(a)>1$ 存在使

$$a^{n(a)}=a,$$

则 R 必是交换环．对此不再作进一步详述．

下面介绍一个与零因子有密切联系的概念．

定义 5 设 S 是环 R 的一个非空子集．如果 R 中元素 a 使

$$aS=\{ax\mid x\in S\}=0,$$

即对 S 中任何元素 x 都有 $ax=0$，则称 a 是 S 的一个左零化子，

并简记为 $aS=0$.

右零化子可类似定义.

左或右零化子统称为零化子. 非零的零化子称为真零化子.

设 R 是一个阶大于 1 且有单位元的交换环. 下面讨论全阵环 $R_{n\times n}$ 中 n 阶方阵是零因子的条件.

为此，先定义环 R 上矩阵的秩的概念.

定义 6　设环 R 如上，A 是环 R 上一个 $m\times n$ 矩阵，并且 $t=\min(m,n)$. 又令 S_i 为由 A 中所有 $i(i=1,2,\cdots,t)$ 阶子式作成的 R 的子集. 如果 S_1 有真零化子，则称矩阵 A 的秩是 0；如果 S_1，…，S_r 都无真零化子，但 S_{r+1} 有真零化子，则称矩阵 A 的秩是 r.

矩阵 A 的秩记为 $r(A)$. 显然 $0\leq r(A)\leq t$.

和普通矩阵类似，如果 S_{r+1} 有真零化子，则显然 S_{r+2}，…，S_t 都有真零化子.

引理　设 R 是有单位元的交换环，$|R|>1$，又

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & & & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix},\quad X=\begin{pmatrix} x_1 \\ x_2 \\ \cdots \\ x_n \end{pmatrix},\quad a_{ij}\in R.$$

则 R 上齐次线性方程组 $AX=0$ 在 R 中有非零解的充要条件是

$$r(A)<n.$$

本引理证明从略，留作习题.

为表述方便起见，在以下定理中把环的零元素也算作零因子.

* **定理 7**　设环 R 如引理，$A\in R_{n\times n}$. 则 A 是全阵环 $R_{n\times n}$ 的零因子的充要条件是，$|A|$ 是环 R 的零因子.

证　1) 设 A 是全阵环 $R_{n\times n}$ 的零因子，则在 $R_{n\times n}$ 中存在 $B\neq 0$ 或 $C\neq 0$ 使

$$AB=0\quad 或\quad CA=0.$$

设若 $AB=0$，并不妨设

$$B=\begin{matrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \cdots & & & \cdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{matrix}$$

中的某个 $b_{ij}\neq 0(1\leq i,j\leq n)$，则根据 $AB=0$ 可得

$$AB_j=0,$$

其中 $B_j\neq 0$ 是 B 的第 j 列构成的列矩阵．这就是说，齐次线性方程组 $AX=0$ 有非零解 $X=B_j$．因此由引理知，$r(A)<n$．从而 $S_n=|A|$ 有真零化子，即 $|A|$ 是环 R 的零因子．

设若 $CA=0$，则 $(CA)^{\mathrm{T}}=0^{\mathrm{T}}$，从而有

$$A^{\mathrm{T}}C^{\mathrm{T}}=0.$$

于是由上知，$r(A^{\mathrm{T}})<n$．但是 $r(A)=r(A^{\mathrm{T}})$，从而亦有 $r(A)<n$ 和 $|A|$ 是环 R 的零因子．

2) 设 $|A|$ 是环 R 的零因子，则在 R 中存在元素 $k\neq 0$ 使 $k|A|=0$．亦即 $S_n=|A|$ 有真零化子．从而由定义 4 知，$r(A)<n$．再由引理知，齐次线性方程组 $AX=0$ 在 R 中有非零解：

$$x_1=k_1,\quad x_2=k_2,\quad \cdots,\quad x_n=k_n.$$

于是 R 上 n 阶方阵

$$K=\begin{matrix} k_1 & 0 & \cdots & 0 \\ k_2 & 0 & \cdots & 0 \\ \cdots & & & \cdots \\ k_n & 0 & \cdots & 0 \end{matrix}\neq 0,$$

但是 $AK=0$．即 A 是全阵环 $R_{n\times n}$ 的零因子．

(证毕)

习题 4.2

1. 证明：

1) 若环 R 有正则元，则其全体正则元对乘法作成一个半群．

2) 环 R 的元素 $a\neq 0$ 是正则元，当且仅当由 $axa=0$ 可得 $x=0$．

2. 设环 R 有左单位元 e. 证明: 如果 R 没有右零因子, 则 e 是环 R 的单位元.

3. 证明: 数域上 n 阶全阵环的元素 $A\neq 0$ 若不是零因子, 就是可逆元(即可逆方阵).

4. 证明: 交换环的全体幂零元作成一个子环.

5. 设 a 是环 R 的一个幂零元. 证明: 若有正整数 $n>1$ 使 $a^n=a$, 则 $a=0$.

6. 设 $Z_{n\times n}$ 为整数环 Z 上的 $n(n>1)$ 阶全阵环. 举例给出其子环 S_1, S_2 除共同满足 $S_1\quad S_2\quad Z_{n\times n}$ 外, 并分别满足:

1) S_1 与 S_2 都有单位元, 但不相等;

2) S_1 与 S_2 有相同的单位元;

3) S_1 有单位元, S_2 无单位元;

4) S_1 无单位元, S_2 有单位元;

5) S_1 与 S_2 都无单位元.

7. 设 R 是一个无零因子的环. 证明: 若 $|R|$ 为偶数, 则 R 的特征必为 2.

8. 证明: p - 环无非零幂零元.

§3 除 环 和 域

我们知道, 一个环不一定有单位元, 即使有单位元, 也不一定每个非零元都有逆元. 但是, 有些环却具有这种性质. 例如, 数域不仅有单位元, 而且每个非零元都有逆元.

定义 1 设 R 是一个环. 如果 $|R|>1$, 又 R 有单位元且每个非零元素都有逆元, 则称 R 是一个 环(或体)

可换除环称为域.

按照这个定义, 数域都是域; 整数环是有单位元的交换环, 但不是域.

除环和域有以下重要性质.

定理 1 除环和域没有零因子.

证 设 R 是一个除环, $a\in R$. 如果

$$a\neq 0,\qquad ab=0,$$

则 $b=a^{-1}(ab)=0$，即 R 无零因子．

（证毕）

由此定理可知，除环和域的特征只能是素数或无限．

下面介绍一种重要的除环——四元数除环．

例 1 令

$$D=\{a\cdot 1+bi+cj+dk \mid a,\ b,\ c,\ d \text{ 为实数}\},$$

并称 D 中的元素为四元数．另规定系数为零的项可以略去不写，且

$$a1=a,\quad 1i=i,\quad 1j=j,\quad 1k=k.$$

于是

$$G=\{1,\ i,\ j,\ k,\ -1,\ -i,\ -j,\ -k\}\subset D.$$

由第二章§1 例 4 知，G 对所规定的乘法作成一个群，即四元数群．根据 G 的乘法现在再规定：

1° $a_1+a_2i+a_3j+a_4k=b_1+b_2i+b_3j+b_4k$ 当且仅当对应系数相等；

2° $(a_1+a_2i+a_3j+a_4k)+(b_1+b_2i+b_3j+b_4k)$

$=(a_1+b_1)+(a_2+b_2)i+(a_3+b_3)j+(a_4+b_4)k$；

3° 两个四元数相乘可按通常分配律先展开，再合并各项中的实系数，最后根据四元数群的乘法表代入相应元素，即

$$(a_1+a_2i+a_3j+a_4k)(b_1+b_2i+b_3j+b_4k)$$

$$=(a_1b_1-a_2b_2-a_3b_3-a_4b_4)+(a_1b_2+a_2b_1+a_3b_4-a_4b_3)i+$$

$$(a_1b_3+a_3b_1+a_4b_2-a_2b_4)j+(a_1b_4+a_4b_1+a_2b_3-a_3b_2)k.$$

因此，任意两个四元数的和与积仍是一个四元数．

对以上规定的加法和乘法，可以验算 D 作成一个环，1 是它的单位元．又因为

$$(a-bi-cj-dk)(a+bi+cj+dk)=a^2+b^2+c^2+d^2,$$

故当 $a+bi+cj+dk\neq 0$ 时有逆元，且

$$(a+bi+cj+dk)^{-1}=\frac{a-bi-cj-dk}{a^2+b^2+c^2+d^2}.$$

因此，D作成一个除环，通常称其为 元数除环．

由于例如 $ij \neq ji$，故四元数除环是一个非可换除环．

这是历史上第一个非可换除环的例子．它是 1843 年由哈密顿所首先提出来的．

这里顺便指出，有限除环必为域．即有限除环一定可换．这是著名的魏得邦 (J.H.M.Wedderburn, 1882～1948) 定理，是 1905 年由魏得邦所首先证明的，以后又有一些初等证法．对此，我们就不再详述了．

定理 2 有限环若有非零元素不是零因子，则必有单位元，且每个非零又非零因子的元素都是可逆元．

证 设 $a \neq 0$ 是有限环 R 的任意非零因子元素，则 a，a^2，a^3，…中必有相等的．不妨设

$$a^m = a^n, \quad 1 \leq m < n,$$

于是有 $a^{m-1}(a - a^{n-m+1}) = 0$．但 $a \neq 0$ 且 a 不是零因子，故

$$a - a^{n-m+1} = 0, \quad a = a^{n-m+1}.$$

从而对任意 $x \in R$，有 $ax = a^{n-m+1}x$，$a(x - a^{n-m}x) = 0$．于是

$$x - a^{n-m}x = 0, \quad a^{n-m}x = x;$$

同理有 $xa^{n-m} = x$．即 a^{n-m} 是环 R 的单位元．

再由 $a \cdot a^{n-m-1} = a^{n-m-1} \cdot a = a^{n-m}$ 可知，a 是 R 的可逆元．

(证毕)

推论 阶大于 1 的有限环 R 若无零因子，则必为除环．

实际上，根据魏得邦定理，这样的环 R 还是一个域．

定理 3 设 R 是环且 $|R| > 1$．则 R 是除环当且仅当对 R 中任意元素 $a \neq 0$，b，方程

$$ax = b \quad (\text{或 } ya = b)$$

在 R 中有解．

证 必要性显然，下证充分性．

在 R 中任取 $a \neq 0$，$b \neq 0$，由条件可设

$$ac = b, \quad bd = c.$$

于是

$$abd = ac = b \neq 0,$$

从而 $ab \neq 0$，即 R 无零因子．

又因为方程 $ax = a$ 在 R 中有解，设为 e．则有

$$ae = a, \quad a(e^2 - e) = 0.$$

但 $a \neq 0$，R 又无零因子，故 $e^2 - e = 0$，$e^2 = e \neq 0$．从而进一步易知 e 是环 R 的全体非零元素的右单位元．再由于方程 $ax = e$ 在 R 中有解且此解显然不是零元素，即每个非零元素都有右逆元．因此，R 的全体非零元素对 R 的乘法作成一个群，而这个群的单位元就是 R 的单位元，从而 R 是除环．

(证毕)

我们知道，粗略地说，在环中可以施行“加、减、乘”运算．定理 3 表明，在除环(或域)中又可以施行“加、减、乘、除”运算．但是应注意，由于除环(对乘法)不一定可换，故在除环中虽然 $a^{-1}b(a \neq 0)$ 及 ba^{-1} 都有意义，是除环中确定的元素，但二者并不一定相等．

当然，如果是在域中，便有 $a^{-1}b = ba^{-1}$．这时我们就把这个共同的元素记为 $\frac{b}{a}$，亦即

$$\frac{b}{a} = a^{-1}b = ba^{-1} \quad (a \neq 0).$$

由此我们可以进一步得到通常熟知的以下分式运算规则在域中都成立：

1) $\frac{b}{a} = \frac{d}{c} \quad ad = bc;$

2) $\frac{b}{a} + \frac{d}{c} = \frac{bc + ad}{ac};$

3) $\frac{b}{a} \cdot \frac{d}{c} = \frac{bd}{ac};$

4) $\dfrac{\frac{b}{a}}{\frac{d}{c}} = \dfrac{bc}{ad}$.

定义 2 设 F_1 是域(除环) F 的一个子集，且 $|F_1| > 1$. 如果 F_1 对 F 的两个运算也作成一个域(除环)，则称 F_1 是 F 的一个域(子除).

定理 4 设 F_1 是域 F 的一个子集，且 $|F_1| > 1$. 则 F_1 作成 F 的一个子域当且仅当

$$a,\ b \in F_1 \qquad a - b \in F_1,$$

$$a \neq 0,\ b \in F_1 \qquad \frac{b}{a} \in F_1.$$

简言之，即 F_1 对“减法与除法”封闭.

这个定理的证明是显然的.

我们知道，除环或域(更一般的对任何环)对加法作成一个交换群(即加群)，但对乘法只能作成一个半群而不能作成群，因为其零元没有逆元素. 但是，除环的全体非零元素对乘法显然作成一个群，而且域的全体非零元素对乘法还作成一个交换群. 更一般的，一个有单位元的环的全体可逆元对乘法显然也作成群.

定义 3 设 R 是一个有单位元的环，则 R 的可逆元也称为 R 的单位；R 的全体可逆元(单位)作成的群，称为 R 的单位群，并用 R^* 或 $U(R)$ 表示.

例如，整数环 Z 和 12 阶循环环 $R_{12} = \{0, e, 2e, \cdots, 11e\}$ $(e^2 = e)$ 的单位群分别为

$$Z^* = 1,\ -1, \qquad R_{12}^* = e,\ 5e,\ 7e,\ 11e,$$

其中 R_{12}^* 的单位元是 e 且每个元素的逆元为自身. 又数域 F 上 n 阶全阵环的单位群是全体 n 阶满秩方阵对乘法作成的群，即 F 上的 n 阶线性群 $GL_n(F)$.

例 2 证明:

$$Z[i] = \{a + bi \mid a,\ b \in Z\}$$

作成一个有单位元的整环(这个环称为Gauss 整环)，并且其单位群是 $\pm 1, \pm i$.

证 $Z[i]$ 作成有单位元的整环显然．又显然 $\pm 1, \pm i$ 均为其单位．下证：$Z[i]$ 没有别的单位．

设 $\varepsilon = a + bi$ 是 $Z[i]$ 的任一单位，则有 $\eta \in Z[i]$ 使

$$\varepsilon\eta = 1, \quad |\varepsilon|^2 |\eta|^2 = 1 .$$

这只有 $|\varepsilon|^2 = a^2 + b^2 = 1$，从而只有

$$a = \pm 1,\ b = 0; \quad \text{或} \quad a = 0,\ b = \pm 1 .$$

即 ε 只能是 ± 1 及 $\pm i$.

因此，± 1 和 $\pm i$ 是环 $Z[i]$ 的全部单位．故

$$U(Z[i]) = \pm 1, \pm i .$$

(证毕)

利用单位群来研究环，这是研究环的重要方法之一．例如，S Z .Ditor, K .E .Eldridge 和 R .W .Gilmer 等人于 1970 年前后便利用这种方法研究环，后者还完全确定了单位群是循环群的有限交换环．

习题 4.3

1. 证明域中元素满足分式运算规则 1) —4)．

2. 证明本节定理 4．

3. 证明：域和其子域有相同的单位元．

4. 设 α, β, γ 是三个四元数．证明：

$$(\alpha\beta - \beta\alpha)^2 \gamma = \gamma(\alpha\beta - \beta\alpha)^2 .$$

提示：若 $\Delta = ai + bj + dk$，则 $\Delta^2 = -a^2 - b^2 - c^2$，再计算 $\alpha\beta - \beta\alpha$.

5. 证明：1) 集合

$$R = \left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \middle| \ a, b \in \text{数域 } F \right\}$$

关于方阵的普通加法与乘法作成一个有单位元的交换环．又问：单位群 $R^* = ?$

2) 当 F 为有理数域时 R 还作成域，但当 F 为实数域时 R 不作成域．

6. 设 F 是一个域，且 $|F|=4$．证明：

1) $\mathrm{char}\ F=2$；

2) F 中非 0 及 1 的两个元素都满足方程 $x^2=x+1$．

§4　环的同态与同构

与群的同态与同构概念相对应，这一节来讨论环的同态与同构．

定义　设 R 与 $\bar{R}$ 是两个环．如果有一个 R 到 $\bar{R}$ 的映射 ϕ 满足

$$\phi(a+b)=\phi(a)+\phi(b),$$

$$\phi(ab)=\phi(a)\phi(b),\qquad (\forall\ a,b\in R)$$

则称 ϕ 为环 R 到 $\bar{R}$ 的一个<u>同态映射</u>．

如果有一个 R 到 $\bar{R}$ 的同态满射时，简称 R 与 $\bar{R}$ <u>同态</u>，记为

$$R\sim\bar{R}.$$

如果 ϕ 是环 R 到 $\bar{R}$ 的一个同态映射，而且 ϕ 又是双射时，则称 ϕ 为环 R 到 $\bar{R}$ 的一个<u>同构映射</u>．当 R 与 $\bar{R}$ 间存在同构映射时，称环 R 与 $\bar{R}$ <u>同构</u>，记为

$$R\cong\bar{R}.$$

特别，当 $R=\bar{R}$ 时，称 ϕ 为环 R 的一个<u>自同构</u>．

当 R 与 $\bar{R}$ 为除环或域时，则以上的同态映射、同构映射或自同构就称为除环或域的同态映射同构映射或自同构．

与群的同态相平行，环的同态也有类似的定理．

定理 1　设 R 与 $\bar{R}$ 是各有两个代数运算的集合，且 $R\sim\bar{R}$．则当 R 是环时，$\bar{R}$ 也是一个环．

定理 2　设 R 与 $\bar{R}$ 是两个环，且 $R\sim\bar{R}$．则 R 的零元的象是 $\bar{R}$ 的零元，R 的元素 a 的负元的象是 a 的象的负元；当 R 是交换环时，$\bar{R}$ 也是交换环；当 R 有单位元时，R 也有，并且单位元的象是单位元．

以上两个定理的证明，同群论中相应定理的证明类似，故从略．

但应注意，环有没有零因子，在同态映射下不一定能够保持．

例 1 设 Z 是整数环，R 为 4 阶循环环，即

$$R=\{0,a,2a,3a\},$$

其中 a 在加群 $(R,+)$ 中的阶为 4(从而 R 的特征为 4)，且 $a^2=a$．则易知映射

$$\varphi:\quad n\quad na$$

是环 Z 到环 R 的一个同态满射．在这里，整数环 Z 没有零因子，但是循环环 R 却有零因子，因为在 R 中

$$2a\cdot 2a=4a^2=0,$$

即 $2a$ 是环 R 的零因子．

例 2 设 Z 是整数环，又

$$R=\{(a,b)\mid a,b\in Z\}.$$

则可以验算 R 对运算

$$(a_1,b_1)+(a_2,b_2)=(a_1+a_2,b_1+b_2)$$

$$(a_1,b_1)(a_2,b_2)=(a_1a_2,b_1b_2)$$

作成一个环，且易知

$$\varphi:\quad (a,b)\quad a$$

是环 R 到 Z 的一个同态满射．又因为

$$(1,0)(0,1)=(0,0),$$

即环 R 有零因子，但它的同态像 Z 却没有零因子．

以上两例说明，若环 $R\sim$ 环，则当 R 无零因子时，环可以有；反之，当 R 有零因子时，环可以没有．

但是，当两个环同构时，则这种情况当然不会发生．

定理 3 设 R 与环是两个环，且 $R\cong$ 环．则 R 是整环(除环、域)当且仅当环是整环(除环、域)．

这个定理的证明是明显的．

例 3 设 $F_{n\times n}$ 是域 F 上的 n 阶全阵环．任取 $N\in F_{n\times n}$，如果矩阵的加法不变，但乘法改为

$$A \oplus B = A \cup B,$$

证明：1) F 上全体 n 阶方阵对此二运算作成环，此环记为 F_N；

2) $F_N \cong F_{n\times n}$ 当且仅当 N 为满秩方阵．

证　易验算 F_N 作成环；又当 N 为满秩方阵时，易知

$$\varphi: \quad A \quad AN$$

是环 F_N 到 $F_{n\times n}$ 的一个同构映射，故 $F_N \cong F_{n\times n}$．

反之，设 $F_N \cong F_{n\times n}$，而 N 为降秩方阵且设

$$r(N) = r, \quad 0 \leq r < n.$$

则由高等代数知，存在秩为 $n-r$ 的 n 阶方阵 B，C 使

$$NB = CN = 0.$$

于是对任意 $A \in F_N$ 都有

$$A \oplus B = ANB = 0, \quad C \oplus A = CNA = 0.$$

从而环 F_N 没有单位元．这与环 F_N 和 $F_{n\times n}$ 同构相矛盾．因此，N 必为满秩方阵．

（证毕）

本节最后，我们介绍在环论中常用到的一个定理——挖补定理．

* **定理 4**　（挖补定理）　设 S 是环 R 的一个子环，且 S 与环 $\square$ 同构，即

$$R \geq S \cong \square.$$

又若 $\square \cap (R-S) = \quad$，即 $\square$ 同 S 在 R 里的余集 $R-S$ 无公共元素，则存在环 $\square$ 使

$$R \cong \square, \quad \square \leq \square.$$

证　令

$$S = \{a, b, \cdots\},$$

$$\square = \{\square, \square, \cdots\},$$

且在同构 $S \cong \square$ 之下，x 的象是 $\square$；又 S 在 R 中余集 $R-S$ 的元素用 u，v，…表示．于是

$$R = S \cup (R - S) = \{a, b, \cdots\} \cup \{u, v, \cdots\} .$$

现在作一个新的集合

$$\text{环} = \text{环} \cup (R - S) = \{\text{环}, \text{环}, \cdots\} \cup \{u, v, \cdots\},$$

并规定 R 到环 的一个映射:

$$\varphi: \quad x \quad \text{环}, \quad y \quad y, \quad (\forall\, y \in R - S) .$$

则显然这是 R 到环 的一个双射 .

再在集合 环 中规定二运算:

$$a' + b' = c', \quad \text{若 } a + b = c;$$
$$a'b' = d', \quad \text{若 } ab = d,$$

其中 a', b' 为环 中任意元素, 且 a, b, c, d 为 a', b', c', d' 在 φ 之下的逆象 . 易知此二运算是 环 的两个代数运算, 并且 φ 是 R 与环 的一个同构映射 . 因此, 环 也是环且 $R \cong$ 环 . 特别, φ 保持原同构 $S \cong$ 环 以及环 环 的原来的运算, 因此 环 $\leq$ 环 . 从而

$$S \leq R \cong \text{环} \geq \text{环} .$$

(证毕)

例 4 设 R 是例 2 中所给出的环, 又令

$$S = \{(a, 0) \mid a \in Z\} .$$

则显然在 $(a, 0) \quad a (\forall\, a \in Z)$ 之下 $S \cong Z$. 又 $Z \cap (R - S) = \quad$, 因此由定理 4 知

$$R \cong \text{环} = Z \cup \{(a, b) \mid 0 \neq b \in Z\},$$

且 $Z \leq$ 环 .

在这个例子中, 实际上就是把元素 $(a, 0)$ 与整数 a 完全等同起来, 从而

$$(x, y) + a = (x, y) + (a, 0)$$
$$= (x + a, y) .$$

习题 4.4

1. 如果环 R 中元素 a 同 R 中每个元素可换, 则称 a 为环 R 的一个 心

元素．R 的所有中心元素作成的集合叫做 R 的**中心**．证明：

1）环的中心是一个可换子环；

2）除环的中心是一个域．

2．证明：有理数域 Q 的自同构只有恒等自同构．

3．设 Q 是有理数域．证明：域

$$Q(i)=\{a+bi\mid a,b\in Q\}$$

有且只有两个自同构．

4．问：域 $Q(i)$ 与域

$$Q(\sqrt{2})=\{a+b\sqrt{2}\mid a,b\in Q\}$$

是否同构？同构时给出一个同构映射，不同构时证明之．

5．证明：每个无单位元的环 R 都可嵌入（即在同构意义下包含在）一个有单位元的环中．

提示：令 $K=\{(a,n)\mid a\in R,n\in Z\}$，且规定

$$(a,m)=(b,n)\quad a=b,\ m=n,$$

$$(a,m)+(b,n)=(a+b,m+n),$$

$$(a,m)(b,n)=(ab+na+mb,mn).$$

6．设 R 是一个环，$u\in R$．证明：R 对以下二运算作成一个环且与 R 同构：

$$a\ \ b=a+b-u,\quad a\ \ b=ab-au-ub+u^2+u.$$

7．证明：实数域的自同构只有恒等自同构．

§5　模 n 剩余类环

这一节，我们将讨论一种重要的有限环——模 n 剩余类环．

任意取定一个正整数 n，令 Z_n 为由 n 个同余类

$$\overline{0},\ \overline{1},\ \overline{2},\ \cdots,\ \overline{n-1}$$

作成的集合．下面规定同余类的加法与乘法，使 Z_n 作成一个环．

任取 $\overline{i},\overline{j}\in Z_n$，规定

$$\overline{i}+\overline{j}=\overline{i+j},\quad \overline{i}\cdot\overline{j}=\overline{ij}.$$

下面证明这是 Z_n 的两个代数运算．

设$\bar{i}=\bar{s}$，$\bar{j}=\bar{t}$，则

$$n \mid i-s, \quad n \mid j-t.$$

从而 $n \mid (i+j)-(s+t)$，即有

$$\overline{i+j}=\overline{s+t}.$$

这就是说，同余类的加法与每类中代表元素的选择无关，故加法是 Z_n 的一个代数运算．

此加法显然满足结合律与交换律；又 $\bar{0}$ 是零元，$\overline{-i}$ 是 $\bar{i}$ 的负元．因此，Z_n 对加法作成一个加群．

同法可证，同余类乘法$\bar{i}\cdot\bar{j}=\overline{ij}$也是 Z_n 的一个代数运算．

又易知乘法满足结合律和交换律，且乘法对加法满足分配律，故 Z_n 作成一个环，且是一个 n 阶有单位元的交换环．我们称其为**n 为模的剩余类环**，或简称**n 剩余类环**．

显然，环 $Z_n=\{\bar{0},\bar{1},\bar{2},\cdots,\overline{n-1}\}$ 关于加法作成一个 n 阶循环群，从而 Z_n 是一个 n 阶循环环．

下面进一步讨论这种环的一些性质．

首先，对任意整数 i，由于

$$(i,n)=(i+nq,n),$$

故类中若有一个整数同 n 互素，则这个类中的所有整数都同 n 互素．因此，我们就说**$\bar{i}$ 与 n 互素**．

这样，在类 $\bar{0}$，$\bar{1}$，$\bar{2}$，…，$\overline{n-1}$ 中，有且只有 $\varphi(n)$ 个类同 n 互素．

定理 1 Z_n 中非零元 $\bar{s}$ 如果与 n 互素，则为可逆元；如果不与 n 互素，则为零因子．

证 设 $\bar{s}\neq\bar{0}$，且 $(m,n)=1$，则存在整数 s，t 使

$$ms+nt=1,$$

于是

$$\bar{s}\cdot\bar{m}=\overline{ms+nt}=\bar{1},$$

即 $\bar{s}$ 是 $\bar{m}$ 的逆元．

又当$(m,n)=d>1$时，令

$$m=dm_1,\quad n=dn_1,\quad 1\leq n_1<n,$$

则$\overline{mn_1}\neq\overline{0}$且

$$\overline{m}\cdot\overline{n_1}=\overline{mn_1}=\overline{nm_1}=\overline{0},$$

即此时$\overline{m}$是Z_n的一个零因子．

(证毕)

此定理表明，模 n 剩余类环 Z_n 的单位群是一个$\varphi(n)$阶的交换群．

定理 2 如果 p 是素数，则环 Z_p 是一个域；如果 n 是合数，则环 Z_n 有零因子，从而不是域．

证 因为 Z_p 的所有非零元素都同 p 互素，于是由定理 1 知，每个非零元素都有逆元，故 Z_p 是一个域．

当 n 是合数时，设

$$n=n_1n_2,\quad 1<n_i<n.$$

则$\overline{n_1}\neq\overline{0}$，$\overline{n_2}\neq\overline{0}$，且

$$\overline{n_1}\cdot\overline{n_2}=\overline{n}=\overline{0},$$

故 Z_n 有零因子，从而不是域．

(证毕)

对于任意正整数 n，由于 Z_n 有单位元且

$$n\cdot\overline{1}=\overline{n}=\overline{0},\quad k\cdot\overline{1}=\overline{k}\neq\overline{0}\quad(1\leq k<n),$$

因此Z_n的特征是 n.

例 1 Z_5 是域．又由于

$$\overline{1}\cdot\overline{1}=\overline{1},\quad \overline{2}\cdot\overline{3}=\overline{1},\quad \overline{4}\cdot\overline{4}=\overline{1},$$

故$\overline{1}$，$\overline{4}$的逆元为自身，而$\overline{2}$与$\overline{3}$互为逆元．

例 2 Z_6 是环不是域．又由于

$$(1,6)=(5,6)=1,$$

$$(2,6)=(4,6)=2,\quad (3,6)=3,$$

故$\overline{1}$，$\overline{5}$是 Z_6 的可逆元，但$\overline{2}$，$\overline{3}$，$\overline{4}$是 Z_6 的零因子．

由§2可知，模 p(p是素数)剩余类环 Z_p 不仅是一个域，而且还是一个 p - 环．

定理3 设 m，n 是两个正整数，则

$$Z_m \sim Z_n \qquad n \mid m .$$

证 令

$$Z_m = \{\bar{0}, \bar{1}, \cdots, \overline{m-1}\}, \qquad Z_n = \{0, 1, \cdots, n-1\},$$

并设 $Z_m \sim Z_n$ 且φ为其一同态满射，则在φ之下单位元的象是单位元，即 $\bar{1}$ 1，从而对任意整数 x 有

φ: 瑚 珮，

特别有

$$\bar{0} = 瑗 \qquad 瑚 = 0 .$$

由于有 瑚 $= 0 \in Z_n$，故 $n \mid m$．

反之设 $n \mid m$．则易知上面的对应φ是剩余类环 Z_m 到 Z_n 的一个满射，而且是一个满同态，故 $Z_m \sim Z_n$．

(证毕)

本节最后，来讨论循环环的一个重要结论．

定理4 除去零乘环外，在同构意义下，循环环有而且只有整数环及其子环以及剩余类环及其子环．

证 整数环及其子环以及剩余类环及其子环都是循环环，这是显然的．下证在同构意义下只有这些循环环．

设

$$R = \{\cdots, -2a, -a, 0, a, 2a, \cdots\}, \quad a^2 = ka$$

为任一循环环且不是零乘环．则 $k \neq 0$．如果 a 在加群$(R, +)$中的阶无限，则易知

φ: ta tk (t 为任意整数)

是循环环 R 到整数环 Z 的子环

$$\blacksquare k\blacksquare = \{\cdots, -2k, -k, 0, k, 2k, \cdots\}$$

的一个同构映射，因此 $R\ddot{u}$ ■ k■ .

如果 a 在加群 $(R, +)$ 中的阶有限，而且是 n . 则此时

$$R=\{0, a, 2a, \cdots, (n-1)a\}, \qquad a^2 = ka, \ 1\leq k<n .$$

且易知以上的对应法则 φ 是 n 阶循环环 R 到模 nk 剩余类环 Z_{nk} 的子环

$$\text{珂}=\{0, \text{珵}, \overline{2k}, \cdots, \overline{(n-1)k}\}$$

的一个同构映射 . 因此，$R\ddot{u}$ 珂　Z_{nk} . 这就是说，n 阶循环环 R 可同构嵌入到模 nk 剩余类环 Z_{nk} 中 . 即在同构意义下 R 是 Z_{nk} 的子环 .

(证毕)

应该注意的是，整数环及其所有非零子环虽然作为加群它们彼此同构(因为都是无限循环群)，但作为环来说，它们彼此并不同构 .

例 3　Z_6 的子环 珂$=\{\bar{0}, \bar{2}, \bar{4}\}$ 与 Z_9 的子环 珮$=\{0, 3, 6\}$ 都是 3 阶循环环，但它们不同构 .

证　珂与珮的加群都是 3 阶循环群，当然同构 . 但作为环它们不同构：因若不然，设有同构 φ，则在 φ 之下必有

$$\bar{2} \quad 3, \ \bar{4} \quad 6 \quad \text{或} \quad \bar{2} \quad 6, \ \bar{4} \quad 3 .$$

从而均有 $\bar{2}=\bar{2}\cdot\bar{4}$　$3\cdot 6=0$，矛盾 .

实际上，在所有的 n 阶循环环中，有而且只有 $T(n)$ (n 的正因数个数)个是互不同构的 . 对此证明可参阅书末参考文献 [12] .

另外易知，循环环的任何子加群都是一个子环 . 就是说，循环环的子加群同子环是一回事 . 特别，整数环 Z 与模 n 剩余类环 Z_n，它们的子加群都是子环 . 由于 n 阶循环群有而且只有 $T(n)$ 个子群，从而 n 阶循环环有而且只有 $T(n)$ 个子环 . 特别，模 n 剩余类环 Z_n 有且只有 $T(n)$ 个子环 .

例 4　环 Z_6 有 $T(6)=4$ 个子环，它们是

$$\{\bar{0}\}, \quad \{\bar{0}, \bar{3}\}, \quad \{\bar{0}, \bar{2}, \bar{4}\}, \quad Z_6 .$$

而且它们的特征依次分别为 1，2，3，6．

例 5 $Z_n\ (n>1)$上 n 阶全阵环是一个 n^{n^2} 阶的有限非交换环．

例 6 $Z_2=\{0,1\}$(这里把 $\bar{0},\bar{1}$ 分别简记为 0,1)上的所有 2 阶上三角方阵，即

$$R_8=\left\{\begin{pmatrix}x & y\\ 0 & z\end{pmatrix}\middle|\ x,\ y,\ z\in Z_2\right\}$$

关于方阵的普通加法与乘法，作成一个有单位元的 8 阶非交换环．

这里顺便指出，有文献已经证明：在有单位元的环中，R_8 是阶数最小的非交换环．特别是，环 R_8 的单位群

$$R_8^*=\left\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\ \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\right\}$$

还是一个循环群，而且在有单位元的有限环中，单位群是循环群的非交换环(在同构意义下)只有 R_8．这当然是一个很重要的结论．

例 7 设 p，q 是互异素数．在同构意义下，pq 阶环不仅都是循环环，而且共有 4 个，它们是

$R_1=\{\bar{0},\bar{1},\bar{2},\cdots,\overline{pq-1}\}=Z_{pq}$，

$R_p=\{\bar{0},\bar{p},\overline{2p},\cdots,\overline{(pq-1)p}\}\quad Z_{p^2q}$，

$R_q=\{\bar{0},\bar{q},\overline{2q},\cdots,\overline{(pq-1)q}\}\quad Z_{pq^2}$，

$R_{pq}=\{\bar{0},\overline{pq},\overline{2pq},\cdots,\overline{(pq-1)pq}\}\quad Z_{p^2q^2}$．

这就是在同构意义下全部的 pq 阶环，而且每一个都可以同构嵌入到某个剩余类环中．其中 R_{pq} 还是一个零乘环．

习题 4.5

1．证明：同余类的乘法是 Z_n 的一个代数运算．

2．试指出环 Z_8 中的可逆元和零因子；再给出它的所有子环．

3．试给出 Z_{10} 的所有子环，并指出它们各自的特征．

4．证明 Euler 定理：设 n 是正整数，又 $(a,n)=1$，则

$$a^{\varphi(n)}\equiv 1\pmod{n}.$$

提示：利用定理 1 和元素的阶整除群的阶．

5. 设 $g(x)$是系数属于 Z_p 的一个多项式．证明：

$$[g(x)]^p = g(x^p)\ .$$

6. 设 $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ 是大于 1 的正整数 n 的标准分解式．证明：剩余类环 Z_n 有

$$p_1^{k_1-1} p_2^{k_2-1} \cdots p_m^{k_m-1}$$

个幂零元．

7. 证明：整数环的不同子环不同构．

8. 两个 n 阶循环环 R 与珮同构的充分与必要条件是，存在整数 $k(0 \leq k < n)$ 并在 R 与珮中分别有生成元 a 与琿满足

$$a^2 = ka,\quad 琿^2 = k琿.$$

提示：在同构映射下生成元相互对应．

§6 理 想

由前几节的讨论我们已经看到，群中有很多概念和定理都可以类推到环中．这一节所讨论的环的理想，就处于群中正规子群的地位．正规子群是群中极重要的概念，同样，理想也在环的讨论中占着非常重要的地位．

定义 1 设 N 是环 R 的一个子加群，即对 N 中任意元素 a，b，差 $a-b$ 仍属于 N．如果又有

$$r \in R,\ a \in N \qquad ra \in N,$$

则称 N 是环 R 的一个<u>左理想</u>；

如果

$$r \in R,\ a \in N \qquad ar \in N,$$

则称 N 是环 R 的一个<u>右理想</u>；

如果 N 既是环 R 的左理想又是右理想，则称 N 是环 R 的一个<u>双边理想</u>，或简称 想，并用符号 N R 表示．否则记为 N R．

由定义可知，一个理想一定是一个子环．但是应注意，一个子环不一定是一个理想．例如，整数环 Z 是数环

$$R=\{a+b\ \ 2\mid a,b\in Z\}$$

的一个子环，但它却不是数环 R 的理想．

显然，在交换环中，每个左或右理想都是双边理想．

例 1 令 $F_{2\times 2}$ 为域 F 上的 2 阶全阵环，并设

$$N_1=\left\{\begin{matrix}a & 0\\ b & 0\end{matrix}\ \middle|\ a,\ b\in F\right\},\qquad N_2=\left\{\begin{matrix}a & b\\ 0 & 0\end{matrix}\ \middle|\ a,\ b\in F\right\}.$$

则易知 N_1 是环 $F_{2\times 2}$ 的一个左理想(但不是双边理想)，而 N_2 是 $F_{2\times 2}$ 的一个右理想(也不是双边理想)．

另外易知

$$N=\left\{\begin{matrix}0 & 0\\ a & 0\end{matrix}\ \middle|\ a\in F\right\}$$

又是环 N_1 的一个双边理想，但它却不是全阵环 $F_{2\times 2}$ 的左理想也不是右理想．

下面举两个理想的例子．

例 2 令 F 是一个域，N 是多项式环 $F[x]$ 中常数项为零的全体多项式作成的集合，则易知 N 是 $F[x]$ 的一个理想．

例 3 令 F 为任一域，又令

$$I=\left\{\begin{matrix}0 & 0 & 0\\ 0 & 0 & a\\ 0 & 0 & 0\end{matrix}\ \middle|\ a\in F\right\},\qquad N=\left\{\begin{matrix}0 & 0 & x\\ 0 & 0 & y\\ 0 & 0 & 0\end{matrix}\ \middle|\ x,\ y\in F\right\},$$

$$R=\left\{\begin{matrix}a_1 & a_2 & a_3\\ 0 & a_4 & a_5\\ 0 & 0 & a_6\end{matrix}\ \middle|\ a_i\in F\right\}.$$

则易知 I N，N R，但是 $I\setminus R$．因此，同正规子群情况类似，理想的理想不一定是原环的理想，亦即理想也不具有传递性．

对任意的环 R，如果 $|R|>1$，则 R 至少有两个理想：一个是零理想$\{0\}$；另一个是 R 自身，称为环 R 的单位理想．这两个理想统称为环 R 的平凡理想．别的理想，如果有的话，称为

R 的 平凡理想　真理想 .

定义 2　只有平凡理想的非零环，称为 环 .

对于一个给定的环，要想弄清楚它的理想的情况，一般来说是非常困难的 . 但是，对于某些特定的环，它们理想的状况是很清楚的 .

我们知道，循环环的子环和子加群是一回事 . 进一步有

定理 1　N 是循环环 $R=\{\cdots,-2a,-a,0,a,2a,\cdots\}$ 的一个理想，当且仅当 N 是 R 的一个子加群(子环) .

证　理想当然是子加群 . 反之，设 N 是循环环 R 的一个子加群，则对任意 $c\in N$，$r\in R$，令

$$c=sa,\qquad r=ta,\qquad a^2=ka,$$

其中 s，t，k 为整数 . 则

$$\begin{aligned}rc&=(ta)(sa)=(ts)a^2\\&=(ts)(ka)=(tk)(sa)=(tk)c\in N .\end{aligned}$$

又因循环环是可换环，故 N　R .

(证毕)

由此定理可知，整数环及模 n 剩余类环 Z_n 的子加群、子环、理想三者都是一回事 . 由此特别可知，环 Z_n 有 $T(n)$ 个理想 .

定理 2　除环和域只有平凡理想 . 即它们都是单环 .

证　设 N 是除环 R 的任意一个理想 . 如果 $N\neq 0$，在 N 中任取 $a\neq 0$，则 $a^{-1}\in R$，于是

$$a^{-1}a=1\in N .$$

从而对 R 中任意元素 r，有

$$r\cdot 1=r\in N,$$

故 $N=R$. 即 R 只有平凡理想，因此 R 是单环 .

(证毕)

在一定意义下，这个定理的逆定理也成立 .

定理 3　设 R 是一个阶大于 1 的环，并且除平凡理想外无其他左或右理想 . 则当 R 有单位元时，R 为除环；当 R 无单位元

时，R 是素阶零乘环．

证 设 R 除$\{0\}$和 R 外无其他左理想．在 R 任取元素 $a\neq 0$，则显然

$$Ra=\{ra\mid r\in R\}$$

是 R 的一个左理想．

当 R 有单位元时，$a\in Ra$，从而 $Ra\neq 0$．于是 $Ra=R$．这表明方程 $ya=b(b\in R)$在 R 中有解，因此 R 是除环．

当 R 无单位元时，则由§3 定理 3 知：总存在元素 $a\neq 0$ 使 $Ra=0$．于是 $a^2=0$，而且

$$N=\{\cdots,-2a,-a,0,a,2a,\cdots\}$$

是环 R 的一个左理想，也是一个循环零乘环．故 $N=R$．再由假设可知，R 只能是一个素阶零乘环．

当 R 除$\{0\}$和 R 外无其他右理想时，同理可证．

(证毕)

推论 1 阶大于 1 的可换单环必为域或素阶零乘环．

下面将给出另一类重要单环．

定理 4 设 R 是一个有单位元的环，$K\subseteq R_{n\times n}$，则存在惟一的 $D\subseteq R$ 使 $K=D_{n\times n}$．

证 令 D 为由 K 中一切 n 阶方阵的所有元素作成的集合．下证：$D\subseteq R$．

用 $E_{ij}(i,j=1,2,\cdots,n)$表示(i,j)元素是 1 而其余元素全是 0 的 n 阶方阵．则易知

$$E_{ij}\cdot E_{st}=\begin{cases}E_{it}, & j=s;\\ 0, & j\neq s.\end{cases}\qquad(1)$$

而且 R 上每个 n 阶方阵都可由这 n^2 个方阵 E_{ij} 线性表示．

任取 $x,y\in D$，则在 K 中存在方阵 A，B 使

$$A=\cdots+xE_{ij}+\cdots,\qquad B=\cdots+yE_{st}+\cdots.\qquad(2)$$

从而根据(1)与(2)以及 $K\subseteq R_{n\times n}$ 可得

$$E_{1i}AE_{j1}-E_{1s}BE_{t1}=xE_{11}-yE_{11}=(x-y)E_{11}\in K.$$

因此，$x-y\in D$.

再任取 $r\in R$，则由于 K $R_{n\times n}$ 而 $A\in K$，故

$$(rE)A=rA=\cdots+rxE_{ij}+\cdots\in K,$$

$$A(rE)=Ar=\cdots+xrE_{ij}+\cdots\in K.$$

从而 rx，$xr\in D$. 因此，D R. 并且 K $D_{n\times n}$.

反之，任取 $A'\in D_{n\times n}$，并令

$$A'=\sum_{i=1}^{n}\sum_{j=1}^{n}a_{ij}E_{ij}\quad(a_{ij}\in D).\tag{3}$$

再任意取定 a_{ij}，则在 K 中有方阵

$$B'=\cdots+a_{ij}E_{st}+\cdots.$$

于是，由于 K $R_{n\times n}$，故

$$E_{is}B'E_{tj}=a_{ij}E_{ij}\in K.$$

从而由(3)可知 $A'\in K$，$D_{n\times n}$ K. 于是

$$K=D_{n\times n}.$$

设另有 D' R 使 $K=D'_{n\times n}$. 则对任意 $d\in D$ 有

$$dE\in D_{n\times n}=K=D'_{n\times n}.$$

于是 $d\in D'$，从而 D D'. 同理有 D' D. 因此

$$D'=D.$$

(证毕)

推论 2 设 R 是有单位元的环，且 $|R|>1$. 则

R 是单环 全阵环 $R_{n\times n}$ 是单环.

特别，域或除环上的 n 阶全阵环都是单环.

证 若 R 是单环，则由定理 4 直接可知，$R_{n\times n}$ 是单环.

反之，设 $R_{n\times n}$ 是单环且 D R，则由矩阵乘法易知：

$$D_{n\times n}\quad R_{n\times n}.$$

从而只有 $D_{n\times n}=\{0\}$ 或 $D_{n\times n}=R_{n\times n}$. 于是由定理 4 中的惟一性可知

$$D=\{0\}\quad\text{或}\quad D=R.$$

即 R 是单环.

(证毕)

定理5 设 R 是一个阶大于 1 的整环. 如果 R 只有有限个理想, 则 R 必为域.

证 在 R 中任取元素 $a\neq 0$, b, 由§3 定理 3 知, 只需证明方程 $ax=b$ 在 R 中有解即可.

易知

$$N_i=\{yd^i \mid y\in R\}\quad R,\qquad i=1,2,\cdots \tag{4}$$

但由于整环 R 只有有限个理想, 故必有正整数 s 与 t 满足

$$s<t,\qquad ba^s\in N_s=N_t.$$

从而由(4)知, 在 R 中有元素 c 使

$$ba^s=ca^t \quad 或 \quad a(a^{t-s-1}\cdot c)=b,$$

即方程 $ax=b$ 在 R 中解 $x=a^{t-s-1}\cdot c$.

(证毕)

下面我们要从环的元素出发, 来作出环的理想.

设 R 是一个环, 任取 $a\in R$, 则 R 中包含元素 a 的理想是存在的, 例如 R 本身就是一个. 易知, R 中包含 a 的全部理想的交也是 R 的一个理想, 且是 R 的包含元素 a 的最小理想. 这个理想记为

$$\blacksquare a\blacksquare,$$

并称其为 R 的 a 生成的主理想.

下面考察一下主理想$\blacksquare a\blacksquare$中的元素是些什么样子.

首先, 由于 $a\in\blacksquare a\blacksquare$, 从而对任意整数 n,

$$na\in\blacksquare a\blacksquare;$$

其次, 对 R 中任意元素 x, y 和 x_i, y_i $(i,j=1,2,\cdots,m)$来说, $\blacksquare a\blacksquare$必包含

$$xa,\qquad ay,\qquad x_iay_i,$$

从而包含所有这种元素的和, 即

$$xa+ay+na+(x_1ay_1+\cdots+x_may_m), \tag{5}$$

其中 n 是不固定的任意整数，而 m 是不固定的任意正整数．

另方面易知，R 的所有(5)中的元素已经作成一个包含 a 的理想，因此

$$\blacksquare a\blacksquare = xa + ay + na + \sum_{i=1}^{m} x_i a y_i$$

$$| \ x, \ y, \ x_i, \ y_i \in R, \ n \in Z, \ m \text{为正整数} \ .$$

这就是主理想 $\blacksquare a\blacksquare$ 中元素的一般表达形式．显然，这种表达形式是累赘的．但是

1) 当 R 是交换环时，由于

$$xa + ay + (x_1 a y_1 + \cdots + x_m a y_m)$$

$$= (x + y + x_1 y_1 + \cdots + x_m y_m) a = ra,$$

其中 $r = x + y + x_1 y_1 + \cdots + x_m y_m$，故此时 $\blacksquare a\blacksquare$ 中元素的表达形式可以简化为

$$\blacksquare a\blacksquare = \{ ra + na \mid r \in R, n \in Z \};$$

2) 当 R 有单位元时，由于

$$xa + ay + na = xa1 + 1ay + (n \cdot 1) a1,$$

故此时 $\blacksquare a\blacksquare$ 中元素的表达形式也可以简化，即有

$$\blacksquare a\blacksquare = \{ x_1 a y_1 + \cdots + x_m a y_m \mid x_i, y_i \in R, m \text{为正整数} \};$$

3) 当 R 既是交换环又有单位元时，更有

$$\blacksquare a\blacksquare = \{ ra \mid r \in R \} \ .$$

显然，循环环的每个理想都是主理想．因此，整数环与模 n 剩余类环的每个理想都是主理想．

下面进一步推广主理想的概念．

定义 3 设 S_1，S_2，…，S_m 为环 R 的 m 个子集，令

$$S_1 + S_2 + \cdots + S_m = \sum_{i=1}^{m} x_i \mid x_i \in S_i \ ,$$

并称其为子集 S_1，S_2，…，S_m 的和．

定理 6 若 N_1，N_2，…，N_m 是环 R 的 m 个(子环)理想，则

$$N_1 + N_2 + \cdots + N_m$$

也是环 R 的一个(子环)理想.

证 对 m 用数学归纳法.

当 $m = 1$ 时定理显然成立. 当 $m = 2$ 时, $N_1 + N_2$ 显然作成 R 的子加群. 又设 $r \in R$ 且

$$x = x_1 + x_2 \in N_1 + N_2, \quad x_i \in N_i,$$

则由于 N_1, N_2 是 R 的理想, 故

$$rx = r(x_1 + x_2) = rx_1 + rx_2,$$

$$xr = (x_1 + x_2)r = x_1 r + x_2 r$$

都属于 $N_1 + N_2$, 从而 $N_1 + N_2 \quad R$, 即 $m = 2$ 时定理成立.

假定对 $m - 1$ 定理成立, 则由于

$$N_1 + N_2 + \cdots + N_{m-1} + N_m$$

$$= (N_1 + N_2 + \cdots + N_{m-1}) + N_m,$$

故易知定理对 m 也成立.

(证毕)

在环 R 中任取 m 个元素 a_1, a_2, …, a_m, 则由定理 6 知

$$\blacksquare a_1 \blacksquare + \blacksquare a_2 \blacksquare + \cdots + \blacksquare a_m \blacksquare$$

是环 R 的理想. 这个理想简记为

$$\blacksquare a_1, a_2, \cdots, a_m \blacksquare,$$

并称其为 元素 a_1, a_2, …, a_m 生成的理想. 它显然是环 R 中包含元素 a_1, a_2, …, a_m 的最小理想.

应注意, 由多个元素生成的理想, 也可能是个主理想, 即也可能由一个元素生成.

例 4 设 Z 是整数环, 则

$$\blacksquare 4, 6 \blacksquare = \blacksquare 2 \blacksquare.$$

证 显然 $4, 6 \in \blacksquare 2 \blacksquare$, 因此, $\blacksquare 4, 6 \blacksquare \quad \blacksquare 2 \blacksquare$.

又由于 $2 = (-1) \cdot 4 + 1 \cdot 6 \in \blacksquare 4, 6 \blacksquare$, 故 $\blacksquare 2 \blacksquare \quad \blacksquare 4, 6 \blacksquare$. 因此, $\blacksquare 4, 6 \blacksquare = \blacksquare 2 \blacksquare$.

这个例子的更一般情况是, 若整数 a_1, a_2, …, a_m 的最大

公因数是 d，则

$$\blacksquare a_1, a_2, \cdots, a_m \blacksquare = \blacksquare d \blacksquare .$$

另外易证，若 N 是整数环 Z 的任一非零理想，a 是 N 中的最小正整数，则 $N = \blacksquare a \blacksquare$.

例 5 整数环上的多项式环 $Z[x]$的理想$\blacksquare 2, x \blacksquare$，不是主理想 .

证 因若不然，设

$$\blacksquare 2, x \blacksquare = \blacksquare g(x) \blacksquare ,$$

则 $2, x \in \blacksquare g(x) \blacksquare$. 由于 $Z[x]$是有单位元的交换环，故可令

$$2 = s(x)g(x), \qquad x = t(x)g(x),$$

这只有 $g(x) = \pm 1$. 但因为$\blacksquare 2, x \blacksquare$显然是由常数项为偶数的所有整系数多项式作成的理想，故$\pm 1 \notin \blacksquare 2, x \blacksquare$，矛盾 .

这就是说，由多个元素生成的理想也有不是主理想的 .

最后介绍理想的乘法 .

定义 4 设 R 是环，又 $A \quad R$，$B \quad R$. 则令

$$AB = \text{有限和} \sum a_i b_i \mid a_i \in A, b_i \in B .$$

并称其为理想 A 与 B 的<u>乘积</u> .

容易证明：$AB \quad R$.

习题 4.6

1. 证明：

1) 环中任意个理想的交仍是一个理想；

2) 环中包含子集 S 的所有理想的交是 R 中包含 S 的最小理想 .

2. 设 R 是环，$a, b \in R$. 证明：

1) $aR = \{ar \mid r \in R\}$，$Rb = \{rb \mid r \in R\}$分别为环 R 的右、左理想；

2) $aRb = \{arb \mid r \in R\} \leq R$.

3. 设 S 是环 R 的一个非空子集 . 证明：S 的全体左(右)零化子作成 R 的一个左(右)理想 . 称其为 S 的左(右)<u>零化理想</u> .

4. 设 R 为偶数环 . 证明：

$$N = \{4r \mid r \in R\} \quad R .$$

问：$N=\blacksquare 4\blacksquare$是否成立？$N$是由哪个偶数生成的主理想？

5. 证明：

1）若 $N \quad Z$，且 a 是 N 中最小的正整数，则 $N=\blacksquare a\blacksquare$；

2）若 a_1，a_2，…，a_m 是整数环 Z 中 m 个整数，且其最大公因数是 d，则

$$\blacksquare a_1, a_2, \cdots, a_m \blacksquare = \blacksquare d \blacksquare .$$

6. 证明：域 F 上多项式环 $F[x]$ 的每个理想都是主理想．

7. 举例指出，环 R 的中心不一定是 R 的理想．

8. 证明：§4 中例 3 中的环 F_N，当 N 为降秩方阵时，不是单环．

§7 商环与环同态基本定理

正规子群在群论中的重要意义是，由它可以产生商群，并能由此获得群论中很多重要结论．同样，利用理想也可以产生一些新的环，而且由此也可以得到环论中一系列相应的结果．

设 N 是环 R 的一个理想，则 N 当然是 R 的一个子加群．于是对于环 R 的加法来说，N 是 R 的一个正规子群，从而 R 关于 N 的一切陪集

$$a+N \quad (a\in R)$$

作成的集合 R/N，对陪集的加法

$$(a+N)+(b+N)=(a+b)+N$$

作成一个加群．现在的想法是，欲对 R/N 再规定另一个代数运算使其作成一个环．

设 $a+N$，$b+N$ 为 R/N 中任二陪集，再规定以下乘法：

$$(a+N)(b+N)=ab+N .$$

需证明这是 R/N 的一个代数运算，即其结果与陪集中代表元素的选择无关．

事实上，设

$$a+N=c+N,\quad b+N=d+N .$$

则 $a-c,\ b-d\in N$．由于 $N \quad R$，故

$$(a-c)b\in N, \qquad c(b-d)\in N,$$

从而$(a-c)b+c(b-d)=ab-cd\in N$. 因此

$$ab+N=cd+N,$$

亦即

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

这说明此运算与代表元素的选择无关.

我们把这个代数运算叫做陪集的乘法.

进一步有

定理 1　设 N 是环 R 的一个理想. 则 R/N 对陪集的加法与乘法作成一个环，称为 R 关于 N 的__环__(有时也称剩余类环)，且

$$R\sim R/N.$$

证　令

$$\varphi: a\mapsto a+N.$$

则易知这是 R 到 R/N 的一个关于加法与乘法的同态满射，故

$$R\sim R/N,$$

由于 R 是环，因此，R/N 也是环.

(证毕)

上面的同态映射 φ，称为环 R 到商环 R/N 的自然同态.

定理 2(环同态基本定理)　设 R 与 $\bar{R}$ 是两个环，且 $R\sim\bar{R}$. 则

1) 这个同态核 N，即零元的全体逆象，是 R 的一个理想；

2) $R/N\cong\bar{R}$.

证　设 φ 是环 R 到环 $\bar{R}$ 的一个同态满射.

1) 由第三章知，核 N 首先是环 R 的一个子加群；其次，设 $a\in N$，$r\in R$，则

$$a\varphi=\bar{0},\quad r\varphi\in\bar{R}.$$

于是在 φ 之下有

$$ra\varphi=(r\varphi)(a\varphi)=\bar{0},$$

$$ar\varphi=(a\varphi)(r\varphi)=\bar{0},$$

故 $ra,\ ar\in N$，即 N 是 R 的理想．

2) 令

$$\psi:\quad a+N\quad \varphi(a),$$

则由群同态基本定理知，作为加群，ψ 是 R/N 到 $\mathbb{Z}$ 的一个同构映射．又由于

$$(a+N)(b+N)=ab+N,$$

而 $\varphi(ab)=\varphi(a)\varphi(b)$，因此 ψ 是环 R/N 到环 $\mathbb{Z}$ 的一个同构映射，从而 $R/N\cong\mathbb{Z}$．

(证毕)

例 1 设 Z 是整数环，n 是任意正整数．证明：

$$Z/(n)\cong Z_n\ .$$

证 商环 $Z/(n)=\{0+(n),1+(n),\cdots,n-1+(n)\}$，而

$$Z_n=\{\bar{0},\bar{1},\cdots,\overline{n-1}\}\ .$$

由于商环中元素(即陪集)的加法与乘法同 Z_n 中元素(即同余类)的加法与乘法一致，故显然

$$\tau:\quad m+(n)\quad \bar{m}$$

是环 $\mathbb{Z}/(n)$ 与 Z_n 的同构映射，因此，$\mathbb{Z}/(n)\cong Z_n$．

顺便指出，由于显然 $\varphi:\ m\quad \bar{m}$ 是整数环 Z 到剩余类环 Z_n 的同态满射，且同态核为 (n)，因此由环同态基本定理知，亦有 $\mathbb{Z}/(n)\cong Z_n$．

例 2 设 $Z[i]$ 是 Gauss 整环，$Z[x]$ 是由全体整系数多项式作成的环．证明：

$$Z[x]/(x^2+1)\cong Z[i]\ .$$

证 这里 i 是虚单位，即 x^2+1 的一个根．易知

$$\varphi:\ f(x)\quad f(i)\qquad (\forall\ f(x)\in Z[x])$$

是环 $Z[x]$ 到 $Z[i]$ 的一个满同态，且 $\mathrm{Ker}\,\varphi=(x^2+1)$，故由环同态基本定理知，$Z[x]/(x^2+1)\cong Z[i]$．

(证毕)

定理 3　在环 R 到环 $\overline{R}$ 的同态映射下，则

1) R 的子环(理想)的象是 $\overline{R}$ 的一个子环(理想)；

2) $\overline{R}$ 的子环(理想)的逆象是 R 的一个子环(理想)．

这个定理的证明同群论中相应定理的证明完全类似，故从略．但应注意，在 1) 中把子环改成理想时，还应要求同态映射是一个满射．

定理 2 所证的同态基本定理也常称为环的<u>一同构定理</u>．进一步有

定理 4　(环第二同构定理)　设 R 是环且

$$H \leq R,\quad N \quad R,$$

则

1) N　$(H+N)$，$H \cap N$　H；

2) $H/(H \cap N) \cong (H+N)/N$．

证　1) 是显然的．以下证明 2)．

令 ϕ 是 R 到 R/N 的自然同态，则易知在 ϕ 之下有

$$H \sim (H+N)/N,$$

且这个同态的核为 $H \cap N$．于是由定理 2 知

$$H/(H \cap N) \cong (H+N)/N.$$

(证毕)

定理 5　(环第三同构定理)　设 R 是环，又

$$A \quad R,\quad B \quad R,\quad A \leq B.$$

则

$$B/A \quad R/A \quad \text{且} \quad R/A/B/A \cong R/B.$$

证　令 ϕ, σ 分别为 R 到 R/A 以及 R 到 R/B 的自然同态，则易知

$$\tau: \quad r+A \quad r+B$$

是 R/A 到 R/B 的一个满同态，且有

$$\sigma = \tau\varphi .$$

又易知 Ker $\tau = B/A$，故由定理 2 知

$$B/A \quad R/A \quad \text{且} \quad R/A \big/ B/A \cong R/B .$$

(证毕)

同群的情况一样，易知商环 R/N 中的子环或理想均呈 K/N 形，其中 K 是 R 中含 N 的子环或理想 .

习题 4.7

1. 设 N 是环 R 到环 $\overline{R}$ 的同态满射 φ 的核 . 证明：φ 是同构映射当且仅当 $N = \{0\}$.

2. 设 R 是有单位元的整环 . 证明：

1) 若 char $R = \infty$，则 R 有子环与 Z 同构；

2) 若 char $R = p$，则 R 有子环与 Z_p 同构 .

3. 设 φ 是环 R 到 $\overline{R}$ 的一个同态满射，K 为同态核，$N \quad R$. 证明：若 $K \quad N$，则 N 在 $\overline{R}$ 中的象的逆象就是 N .

4. 令 $R = \{a + bi \mid a, b \in Q\}$，$\overline{R}$ 为由一切形如

$$\begin{matrix} a & b \\ -b & a \end{matrix} \qquad (a, b \in Q)$$

的方阵作成的集合 . 证明：对普通加法与乘法来说，R 与 $\overline{R}$ 同构且 $\overline{R}$ 是一个域 .

5. 设 R 为环，$N \quad R$. 证明：

1) R/N 中的理想都具有形状 K/N，其中 K 是 R 的含 N 的理想；

2) 在自然同态 $R \sim R/N$ 之下，R 的理想 H 的象为 $H + N/N$.

§8 素理想和极大理想

本节介绍两种重要的理想 .

定义 1 设 R 是一个交换环，$P \quad R$. 如果

$$ab \in P \qquad a \in P \text{ 或 } b \in P,$$

其中 $a,\ b\in R$，则称 P 是 R 的一个素理想.

显然，环 R 本身是 R 的一个素理想；又零理想$\{0\}$是 R 的素理想当且仅当 R 无零因子，亦即 R 是一个整环.

例 1 整数环 Z 的全部素理想是：$\{0\}$，Z 以及由所有素数 p 生成的理想$\blacksquare p\blacksquare$.

证 这些理想显然都是 Z 的素理想. 又由于 Z 的理想都是主理想，因此，如果 n 是一个合数且

$$n=n_1n_2,\quad 1<n_1,\ n_2<n,$$

则 $n_1n_2=n\in\blacksquare n\blacksquare$，但是 $n\nmid n_1$，$n\nmid n_2$，即有

$$n_1\notin\blacksquare n\blacksquare,\quad n_2\notin\blacksquare n\blacksquare,$$

即$\blacksquare n\blacksquare$不是整数环 Z 的素理想.

(证毕)

例 2 设 R 是偶数环，p 是奇素数，又

$$\blacksquare 4\blacksquare=\{\cdots,-12,-8,-4,0,4,8,12,\cdots\},$$

$$\blacksquare 2p\blacksquare=\{\cdots,-6p,-4p,-2p,0,2p,4p,6p,\cdots\},$$

则$\blacksquare 4\blacksquare$不是 R 的素理想，而$\blacksquare 2p\blacksquare$是 R 的素理想.

证 因为 $2\cdot 2=4\in\blacksquare 4\blacksquare$，但 $2\notin\blacksquare 4\blacksquare$，故$\blacksquare 4\blacksquare$不是偶数环的素理想.

又设 $ab\in\blacksquare 2p\blacksquare$，其中 $a,\ b$ 是偶数. 设

$$a=2s,\quad b=2t,\quad ab=2pq,$$

其中 $s,\ t,\ q$ 为整数. 则由于 p 是奇素数，故可知 $p\mid st$. 从而

$$p\mid s\quad 或\quad p\mid t.$$

由此可知必有 $a\in\blacksquare 2p\blacksquare$或 $b\in\blacksquare 2p\blacksquare$，即$\blacksquare 2p\blacksquare$是偶数环的素理想.

(证毕)

定理 1 设 P 是交换环 R 的一个理想. 则 P 是 R 的素理想的充分与必要条件是，商环 R/P 无零因子，即为整环.

证 设 P 是 R 的素理想，则在商环 R/P 中任取二元素

$$\bar{a}=a+P,\quad \bar{b}=b+P,$$

且令 $\overline{ab}=\overline{0}$．于是有 $\overline{ab}=\overline{0}$，即 $ab\in P$．但因 P 是素理想，故有 $a\in P$ 或 $b\in P$．亦即有

$$\overline{a}=\overline{0} \quad 或 \quad \overline{b}=\overline{0}.$$

因此，商环 R/P 无零因子．又因为 R 可换，故 R/P 也可换，从而为整环．

反之，设 R/P 无零因子，且令 $ab\in P$．则

$$\overline{ab}=\overline{0}, \quad 即 \overline{a}\,\overline{b}=\overline{0}.$$

于是 $\overline{a}=\overline{0}$ 或 $\overline{b}=\overline{0}$，亦即 $a\in P$ 或 $b\in P$．因此，P 是 R 的一个素理想．

（证毕）

下面再介绍另一类与素理想有密切联系的重要理想．

定义 2 设 N 是环 R 的一个理想，且 $N\neq R$．如果除 R 和 N 外，R 中没有包含 N 的其它理想，则称 N 为环 R 的一个极大理想．

例 3 在模 8 剩余类环 Z_8 中，令

$$(\overline{4})=\{\overline{0},\overline{4}\},\quad (\overline{2})=\{\overline{0},\overline{2},\overline{4},\overline{6}\},$$

则 $(\overline{4})$ 不是 Z_8 的素理想（因为 $\overline{2}\cdot\overline{2}=\overline{4}\in(\overline{4})$，但是 $\overline{2}\notin(\overline{4})$），也不是 Z_8 的极大理想（因为 $(\overline{4})\subset(\overline{2})\subset Z_8$）．但是，易知 $(\overline{2})$ 既是 Z_8 的素理想也是 Z_8 的极大理想．

应该注意的是，素理想是在交换环内定义的，但极大理想并无这种限制．

定理 2 整数环 Z 的理想 N 是 Z 的极大理想，当且仅当 N 是由素数生成的理想．

证 设 $N=(p)$，p 是素数，又 K 是 Z 的一个理想，且

$$(p)\subseteq K\subseteq Z.$$

令 $K=(m)$，则 $p\in(m)$，$m\mid p$．只有

$$m=1 \text{ 或 } p,$$

即只有

$$K=(1)=Z \quad 或 \quad K=(p),$$

从而■p■是 Z 的极大理想．

反之，设 N 是 Z 的极大理想，由于 Z 的理想都是主理想，故可设 $N=$■n■，且不妨设 n 是正整数．如果 n 是合数，令

$$n=n_1n_2,\quad 1<n_i<n,$$

则 Z 的理想■n_1■$\neq Z$，■n_1■$\neq$■n■，但却有

$$N=\blacksquare n\blacksquare\quad\blacksquare n_1\blacksquare,$$

这与 N 是 Z 的极大理想矛盾．故 n 必为素数．

(证毕)

根据这个定理，并由例 1 可知，除平凡理想外，整数环的素理想和极大理想是一致的．但是，对有些环来说并不是这样．

例 4 ■x■、■y■与■x,y■都是整数环上二元多项式环 $Z[x,y]$的素理想．

证 1) ■x■与■y■是环 $Z[x,y]$的素理想．

在 $Z[x,y]$中任取二多项式：

$$f=f(x,y)=f_0(y)x^n+f_1(y)x^{n-1}+\cdots+f_{n-1}(y)x+f_n(y),$$

$$g=g(x,y)=g_0(y)x^m+g_1(y)x^{m-1}+\cdots+g_{m-1}(y)x+g_m(y).$$

设若

$$fg=f_0g_0x^{m+n}+\cdots+(f_{n-1}g_m+g_{m-1}f_n)x+f_ng_m\in\blacksquare x\blacksquare,$$

但 $f\notin$■x■，则必

$$f_ng_m=f_n(y)g_m(y)=0,\quad 但\ f_n(y)\neq 0.$$

从而 $g_m(y)=0$．因此，必有 $g\in$■x■．所以■x■是环 $Z[x,y]$的素理想．

同理，■y■也是环 $Z[x,y]$的素理想．

2) ■x,y■是环 $Z[x,y]$的素理想．

显然，■x,y■中的元素恰是 $Z[x,y]$中常数项为零的全体多项式，因此，若 $fg\in$■x,y■，即 fg 的常数项是 0，则必 f 或 g 至少有一个的常数项为 0，亦即必有

$$f\in\blacksquare x,y\blacksquare\quad 或\quad g\in\blacksquare x,y\blacksquare.$$

因此，■x,y■是环 $Z[x,y]$的素理想．

(证毕)

由于显然■x■ ■x, y■, ■y■ ■x, y■, 因此, 环 $Z[x, y]$ 的素理想■x■, ■y■都不是极大理想.

进一步有

例 5 ■$x, y, 2$■是环 $Z[x, y]$ 的素理想也是极大理想.

证 设 $fg \in$ ■$x, y, 2$■, 即 fg 的常数项是偶数. 则必 f 与 g 中至少有一个的常数项是偶数, 亦即 f 或 g 至少有一个属于■$x, y, 2$■. 因此, ■$x, y, 2$■是环 $Z[x, y]$ 的素理想.

其次, 设若 D 是 $Z[x, y]$ 的理想, 且

$$■x, y, 2■ \quad D \quad Z[x, y].$$

则必存在常数项为 0 的 $f(x, y)$ 和奇数 c 使

$$f(x, y) + c \in D.$$

从而 $f(x, y) \in$ ■$x, y, 2$■ D, 因此 $c \in D$. 现在在环 $Z[x, y]$ 中任取一个多项式

$$g(x, y) + d \quad (g(x, y) \text{常数项为 } 0, \ d \text{ 是整数}).$$

若 d 是偶数, 则

$$g(x, y) + d \in ■x, y, 2■, \ \therefore g(x, y) + d \in D;$$

若 d 是奇数, 则由于 $c - d$ 是偶数且 $c \in D$, 从而

$$g(x, y) + d = g(x, y) + (c - d) + c \in D.$$

因此, $D = Z[x, y]$. 从而■$x, y, 2$■也是环 $Z[x, y]$ 的一个极大理想.

(证毕)

另外易知■$x^2 y, xy^2$■ ■x■, 且■$x^2 y, xy^2$■不是环 $Z[x, y]$ 的素理想. 于是由例 4 和例 5 可知, 有

$$■x^2 y, xy^2■ \quad ■x■ \quad ■x, y■ \quad ■x, y, 2■,$$

其中■$x^2 y, xy^2$■不是素理想, 后三个都是素理想, 而且最后一个还是一个极大理想.

为了利用极大理想来得到一个域, 我们先利用极大理想来求得一个单环, 即只有平凡理想的环.

定理 3 设 N 是环 R 的一个理想，则

$$N \text{ 是极大理想} \quad \Leftrightarrow \quad R/N \text{ 是单环}.$$

证 用 ϕ 表示 R 到 $\overline{R}=R/N$ 的自然同态．

设 N 是 R 的一个极大理想，而 $\overline{K}$ 为 $\overline{R}$ 的任一非零理想，则由上节知，在 ϕ 之下 $\overline{K}$ 的逆象 K 是 R 的一个理想．由于 $\overline{O}\in\overline{K}$，而 $\overline{O}$ 的逆象为 N，故 $N \quad K$．又因 $\overline{K}\neq\overline{O}$，故 $N\neq K$，即 $N \quad K$．但 N 是 R 的极大理想，故

$$K=R,\quad \overline{K}=\overline{R}.$$

即 $\overline{R}=R/N$ 只有平凡理想．

反之，设 $\overline{R}$ 是单环，K 是 R 的一个理想，且

$$N \quad K \quad R,$$

则 $\overline{K}=K/N \quad \overline{R}$．但由于 $N \quad K$，故 $\overline{K}\neq\overline{O}$，又因 $\overline{R}$ 是单环，故 $\overline{K}=\overline{R}$．

任取 $r\in R$，则 $r+N\in\overline{R}$，从而有 $k\in K$ 使

$$r+N=k+N,$$

于是 $r-k\in N \quad K$，$r\in K$，$K \quad R$．因此 $K=R$，即 N 是 R 的极大理想．

(证毕)

我们知道，域是单环．以下将指出，在一定条件下其逆也成立．

定理 4 设环 R 是一个单环，则当 R 有单位元且可换时，R 是一个域．

证 在 R 中任取 $a\neq0$，则■a■$\neq0$．但 R 是单环，只有平凡理想，故

$$■a■=R.$$

于是单位元 $1\in$■a■．但对有单位元可换环来说，■a■中元素都可表为

$$ra \quad (r\in R),$$

于是 $1 = a'a$，其中 $a' \in R$．即 R 中每个非零元都有逆元，从而 R 是一个域．

(证毕)

由以上两个定理立即可得

推论 1 设 R 是一个有单位元的交换环，N 是 R 的一个理想．则 R/N 是域的充分与必要条件是，N 是环 R 的一个极大理想．

证 设 R/N 是域，而域是单环，于是由定理 3 知，N 是 R 的一个极大理想．

反之，设 N 是 R 的一个极大理想，由定理 3，R/N 是单环．又因环 R 有单位元且可换，从而 R/N 也有单位元且可换，故由定理 4，R/N 是一个域．

(证毕)

根据这个推论，再结合定理 1 又可得

推论 2 有单位元交换环的极大理想必为素理想．

这样，在有单位元的交换环中，只要给出一个极大理想，便可立即得到一个与这个环有密切联系的域．于是，可以通过所得到的域进一步研究所给的环．

例 6 由素数 p 生成的理想是整数环 Z 的极大理想，而 Z 有单位元且可换，故由定理 2 知，$Z/(p)$ 即 Z_p 是一个域．

这样，我们从极大理想出发，又一次证明了 Z_p 是一个域．

习题 4.8

1. 问：(x) 是不是多项式环 $Z[x]$ 的极大理想？又 (x) 是不是 $Q[x]$ 的极大理想？

2. 证明：(4) 是偶数环 R 的极大理想，但 $R/(4)$ 不是域．

3. 问：偶数环 R 的极大理想是否均为 $(2p)$？其中 p 是素数．又其素理想是否只有 $\{0\}$，R 和 (4)？

4. 试给出模 6 与模 10 剩余类环 Z_6 与 Z_{10} 中的所有素理想和极大理想，并说明理由．

5. 设 R 是交换环，N　R．证明：R/N 是域的充分与必要条件是，N 是 R 的极大理想且由 $a^2 \in N$ 可得 $a \in N$．

提示：N　$\{b+ar \mid b \in N, r \in R\}$　R．

§9　环与域上的多项式环

这一节我们介绍另一种具体的环——多项式环．

在高等代数中所说的多项式，一般都是数域上的多项式．现在要进一步讨论环上的多项式．

本节均假设 R 是一个单位元的环．又设 x 是一个记号，称为 R 上的未定元．则形如

$$f(x) = a_0 x^0 + a_1 x + \cdots + a_n x^n \quad (a_i \in R)$$

的表达式称为 R 上未定元 x 的多项式．

尽管这里的 a_0，a_1，…，a_n 不一定是数，但我们仍然称它们为该多项式的数．另外，有关普通多项式的项、次数以及相等、相加、相乘等概念和运算，现在对于环上的多项式都可以基本照搬无误．特别，也约定系数为 0 的项可以略去不写，也可以任意添加．又约定

$$1x = x,\ (-a)x = -ax,$$

而 $x^0 = 1$，即 R 的单位元．这样，R 中每个元素都是 R 上一个特殊的多项式．

称系数全为零的多项式为零多项式，并仍用 0 表示．

根据以上规定，R 上未定元 x 的全体多项式，关于多项式的加法与乘法作成一个环，称为 R 上未定元 x 的多项式环．记为 $R[x]$．

R 是 $R[x]$ 的一个子环，且 $R[x]$ 的单位元就是 R 的单位元．显然，$R[x]$ 是交换环当且仅当 R 是交换环．

进一步有

定理 1　设 R 是一个有单位元的环．则多项式环 $R[x]$ 是整

环当且仅当 R 是整环.

证 显然只用证: 当 R 无零因子时, $R[x]$ 也无零因子.

在 $R[x]$ 中任取二非零多项式 $f(x)$ 与 $g(x)$, 且令

$$f(x)=a_0+a_1x+\cdots+a_mx^m,\quad a_m\neq 0,$$

$$g(x)=b_0+b_1x+\cdots+b_nx^n,\quad b_n\neq 0,$$

则由于 R 无零因子, $a_mb_n\neq 0$, 故

$$f(x)g(x)=a_0b_0+\cdots+a_mb_nx^{m+n}\neq 0,$$

即 $R[x]$ 无零因子.

(证毕)

普通带余除法在一般多项式环中可以得到推广.

定理 2 设 R 是有单位元的环, $R[x]$ 是 R 上未定元 x 的多项式环. 则对 $R[x]$ 中任意多项式 $f(x)$, $g(x)\neq 0$ ($g(x)$ 的最高系数是 R 的一个可逆元), 在 $R[x]$ 中存在惟一多项式 $q_1(x)$, $r_1(x)$ 及 $q_2(x)$, $r_2(x)$ 使

$$f(x)=g(x)q_1(x)+r_1(x),$$

$$r_1(x)=0 \text{ 或 } r_1(x)\text{次}<g(x)\text{次},$$

$$f(x)=q_2(x)g(x)+r_2(x),$$

$$r_2(x)=0 \text{ 或 } r_2(x)\text{次}<g(x)\text{次},$$

分别称 $q_1(x)$, $r_1(x)$ 与 $q_2(x)$, $r_2(x)$ 为 $f(x)$ 用 $g(x)$ 除所得的__商、右余式与__商、左余式.

这个定理的证明同高等代数中相应定理的证明完全一样, 故从略. 但应注意, 因为 R 不一定是可换环, 故商 $q_1(x)$ 与 $q_2(x)$ 以及余式 $r_1(x)$ 与 $r_2(x)$ 一般并不相等. 当然, 如果 R 是可换环, 它们则分别相等, 就不必再分左右了.

当 R 是一个有单位元的环时, R 上未定元 x_1 的多项式环 $R[x_1]$ 也是一个有单位元的环, 从而 $R[x_1]$ 上未定元 x_2 的多项式环 $R[x_1][x_2]$ 也是一个有单位元的环. 如此下去, 一般地可得环

$$R[x_1][x_2]\cdots[x_n].$$

我们称其为 R 上未定元 x_1, x_2, …, x_n 的 n 元多项式环, 或简

称为多元多项式环，并把它简记为

$$R[x_1, x_2, \cdots, x_n] .$$

由于 R 是 $R[x_1, x_2, \cdots, x_n]$ 的子环，且有相同的单位元，从而它们有相同的特征．

下面进一步讨论域 F 上的多项式环 $F[x]$．

有关高等代数中多项式整除、因式、最高公因式、不可约多项式、互素、因式分解以及根等概念和相应定理，对一般域上的多项式都成立．特别有

定理 3　设 F 是域 E 的一个子域．则 E 中元素 α 是 F 上多项式 $f(x)$ 的根，当且权当 $x-\alpha$ 整除 $f(x)$，其中 x 是 E 上未定元．

定理 4　设 F 是域 E 的一个子域，x 是 E 上未定元．则 F 上 $n(n>0)$ 次多项式 $f(x)$ 在 E 中根的个数（k 重根以 k 个计）不超过 $f(x)$ 的次数 n．

证　设 $\alpha, \alpha_1, \cdots, \alpha_n$ 是 $f(x)$ 在 E 中的全部根，则在 $E[x]$ 中，乘积

$$(x-\alpha)(x-\alpha_1)\cdots(x-\alpha_n)$$

整除 $f(x)$，从而有 $h(x)\in E[x]$ 使

$$f(x)=(x-\alpha)(x-\alpha_1)\cdots(x-\alpha_n)h(x),$$

于是

$$f(x)\text{次数}=m+h(x)\text{次数},$$

即 $n=m+h(x)$ 次数．因此 $m\leq n$．

（证毕）

应注意，对环上的多项式定理 5 不再成立．

例 1　求模 8 剩余类环 $Z_8=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5},\bar{6},\bar{7}\}$ 上 2 次多项式 $x^2-\bar{1}$ 在 Z_8 内的所有根．

解　用直接验算的方法可知，在 Z_8 内 $x^2-\bar{1}$ 有 4 个根：$\bar{1}$，$\bar{3}$，$\bar{5}$，$\bar{7}$（而且这 4 个根恰为 Z_8 的单位群中的全部元素）．

当然，在环内根的个数小于多项式的次数、甚至无根的情况

也是存在的.

例 2 模 4 剩余类环 $Z_4=\{\bar{0},\bar{1},\bar{2},\bar{3}\}$ 上的多项式

$$x^2+\bar{1}$$

在 Z_4 内只有一个根 $\bar{3}$; 而 $x^2+x+\bar{1}$ 在 Z_4 内无根.

不过, 对于例 2 出现的情况并无什么特别之处. 因为, 例如即使有理数域或实数域上的多项式在有理数域或实数域内也可能无根.

定理 5 设 F 是域 E 的一个子域, 又 F 上多项式■ $f(x)$ 在 $E[x]$ 中可分成一次因子的乘积. 则 $f(x)$ 在 E 中无重根的充分与必要条件是

$$(f(x),f'(x))=1.$$

这个定理的证明同高等代数中的证明一致, 也不在这里重复了.

最后讨论有理分式域.

设 F 是一个域, x 是 F 上未定元. 令

$$F(x)=\left\{\frac{f(x)}{g(x)}\,\middle|\, f(x),g(x)\in F[x],g(x)\neq 0\right\},$$

则易知 $F(x)$ 对有理分式的普通加法与乘法作成一个域, 称为 F 上未定元 x 的 理分式域.

$F[x]$ 是有理分式域 $F(x)$ 的一个子环.

例如, 以素数 p 为模的剩余类环 Z_p 是一个 p 阶有限域, 特征是 p. 而其上的多项式环 $Z_p[x]$ 是一个特征为 p 的无限环, $Z_p(x)$ 则是一个特征为 p 的无限域. 此例表明, 无限环或域的特征可能有限.

同样可讨论域 F 上多个未定元的有理分式域

$$F(x_1,x_2,\cdots,x_n).$$

习题 4. 9

1. 设 R 是环 K 的一个子环, 二者有相同的单位元, 又 x 是 K 上未定

元，$\alpha \in K$，并令

$$R[\alpha] = \{ f(\alpha) \mid f(x) \in R[x] \} .$$

证明：$R[x] \sim R[\alpha]$.

2. 试举例指出：环 $R[x]$ 中的 m 次与 n 次多项式的乘积可能不是一个 $m+n$ 次多项式 .

3. 试求出多项式

$$f(x) = \bar{3} + x - \bar{2}x^2 + \bar{4}x^3$$

在域 Z_5 中的所有根 .

4. 求出域 Z_3 上的所有 2 次不可约多项式 .

5. 设 F^* 是域 F 的非零元素作成的乘群 . 证明：F^* 的任何有限子群都是循环群 .

6. 设 R 是有理数域上的 2 阶方阵环，x 是 R 上未定元，又

$$f(x) = \begin{pmatrix} 2 & 1 \\ 0 & 0 \end{pmatrix} x^2 + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} x + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$g(x) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} x + \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} .$$

求 $f(x)$ 用 $g(x)$ 除所得的右商和右余式，并指出其右商 $\neq$ 左商，右余式 $\neq$ 左余式 .

* §10 分 式 域

对于整数环 Z 来说，利用极大理想 (p) 可以得到一个域 $Z/(p)$. 另一方面，利用任二整数的商(除数不为零)也可以得到一个域，即有理数域，它是包含整数环的最小数域 .

如果现在 R 是任意一个非零环，问：能否扩大 R 来得到一个包含 R 为子环的域？这要决定于 R 是一个什么样的环 .

首先，由于除环及域都没有零因子，因此，如果 R 能扩大为一个除环或域，R 首先不能有零因子 .

其次，当 R 是非交换环时，它当然不能扩大成一个域 . 但是能否一定扩大成一个除环呢？对此，1936 年马力茨夫曾给出

例子说明，一个无零因子的非交换环不一定能被一个除环包含．

因此，要把一个环扩大成一个域，就必须首先要求这个环是一个不含零因子的交换环，即整环．

本节主要讨论对整环怎样扩大成域的问题．

设 R 是一个阶大于 1 的整环．我们先看一下，如果 R 能被包含在一个域 K 中，那么域 K 中必须包含一些什么样的元素．

任取 $a,\ b\in R$，且 $a\neq 0$，则由于 $R\quad K$，而 K 是一个域，则 K 必须包含一切形如

$$\frac{b}{a}=a^{-1}b=ba^{-1}$$

的元素．我们称这个元素为 b 除以 a 所得的商．

下面证明，一切这样的商作成一个域，且 R 为其子环．

定理 1 设 K 是包含整环 $R(|R|>1)$ 的一个域，则 K 中一切形如

$$\frac{b}{a}=a^{-1}b=ba^{-1}\ (a,b\in R,\ a\neq 0)$$

的元素作成 K 的一个子域 F，它包含 R 为其子环．我们称 F 为环 R 的分式域或 域．

证 一切这样的商作成一个域是显然的．特别，$\frac{0}{a}$ 是 F 的零元，$\frac{-b}{a}$ 是 $\frac{b}{a}$ 的负元；又由于 $|R|>1$，在 R 中有 $a\neq 0$，而 $\frac{a}{a}$ 是单位元；最后，$\frac{a}{b}$ 是 $\frac{b}{a}$ 的逆元，其中 $a,\ b$ 是 R 中的非零元．

对 R 中任一元素 a 及 $b\neq 0$，由于

$$\frac{ab}{b}=a,$$

故 R 中每个元素都是 R 中某二元素的商，因此 $R\quad F$，R 是 F 的子环．

（证毕）

由这个定理可知，如果一个环 R 有分式域，则它的分式域完全由 R 所惟一确定．更一般地有

推论 同构的整环其分式域也同构．

这个推论的证明是显然的．

上面的讨论并未回答阶大于 1 的整环是不是有分式域．也就是说，没有回答阶大于 1 的整环是不是能包含在一个域中．但是，它却启发我们如何从这种环出发而得到它的分式域．

定理 2 整环的分式域存在．

证 设 R 是一个阶大于 1 的整环，且令

$$M=\{(a,b)\mid a,b\in R,\ a\neq 0\}.$$

对 M 的元素规定以下关系：

$$(a,b)\sim(c,d) \qquad ad=bc.$$

易知这是 M 的一个等价关系．由这个等价关系决定 M 的元素间的一个分类：每类中元素相互等价，不同类中的元素不等价．

M 中元素 (a,b) 所在的类用符号 $\frac{b}{a}$ 表示，并用 F 表示所有类作成的集合，即由所有

$$\frac{b}{a}\quad(a,b\in R,\ a\neq 0)$$

作成的集合．

根据 M 中所给的等价关系知，

$$\frac{b}{a}=\frac{d}{c} \qquad ad=bc.$$

再对 F 中元素规定加法与乘法如下：

$$\frac{b}{a}+\frac{d}{c}=\frac{bc+ad}{ac},\quad \frac{b}{a}\cdot\frac{d}{c}=\frac{bd}{ac}.$$

下证这是 F 的两个代数运算．

首先，当 $a\neq 0$，$c\neq 0$ 时，由于 R 无零因子，故 $ac\neq 0$．从而

$$\frac{bc+ad}{ac},\quad \frac{bd}{ac}$$

都有意义，是 F 中确定的元素

其次，设

$$\frac{b'}{a'}=\frac{b}{a},\quad \frac{d'}{c'}=\frac{d}{c},$$

则 $ab'=a'b,\ cd'=c'd$，且 $a'c'\neq 0,\ ac\neq 0$．从而

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

$$ac\cdot b'd'=bd\cdot a'c',$$

$$\frac{b'c'+a'd'}{a'c'}=\frac{bc+ad}{ac},\quad \frac{b'd'}{a'c'}=\frac{bd}{ac}.$$

即所规定的加法与乘法都是 F 的代数运算．

同样可验算加法与乘法都满足结合律和交换律，且乘法对加法满足分配律．

类$\frac{0}{a}$是零元，$\frac{-b}{a}$是$\frac{b}{a}$的负元；又类$\frac{a}{a}$是单位元，$\frac{a}{b}$是$\frac{b}{a}\neq 0$的逆元(此时 $ab\neq 0$)．

因此，F 作成一个域．

最后证明，在同构意义下，R 是 F 的子环．

在 R 中任意取定一个元素 $b\neq 0$，令

$$S=\left\{\frac{ab}{b}\,\middle|\, a\in R\right\},$$

则易知

$$\varphi:\quad a\quad \frac{ab}{b}$$

是 R 到 S 的一个同构映射，故 $R\cong S$．

于是由挖补定理知，在同构意义下，R 是 F 的子环，而 F 是 R 的分式域．

(证毕)

习题 4. 10

1. 证明：域 F 的分式域就是自身 .

2. 证明定理 2 中集合 M 的元素间的关系

$$(a, b)\sim(c, d) \qquad ad = bc$$

是一个等价关系 .

3. 证明定理 2 中的 φ 是 R 到 S 的一个同构映射 .

4. 问：Gauss 整环 $Z[i]$ 的分式域为何 ?

5. 设 p 是一个素数 . 证明：

$$R = \left\{ \frac{m}{n} \;\middle|\; m, n\in Z, (n, p) = 1 \right\}$$

是一个整环，并求其分式域 .

* §11 环■的■直■和

与群的直积相对应，本节来介绍环的直和 .

设 R_1'，R_2'，…，R_n' 是 n 个环，且令

$$R = \{(a_1, a_2, \cdots, a_n) \mid a_i \in R_i'\},$$

并规定：

$$(a_1, a_2, \cdots, a_n) = (b_1, b_2, \cdots, b_n) \qquad a_i = b_i,\ i = 1, 2, \cdots, n;$$

$$(a_1, a_2, \cdots, a_n) + (b_1, b_2, \cdots, b_n) = (a_1 + b_1, a_2 + b_2, \cdots, a_n + b_n),$$

$$(a_1, a_2, \cdots, a_n) \cdot (b_1, b_2, \cdots, b_n) = (a_1 b_1, a_2 b_2, \cdots, a_n b_n) .$$

则易知 R 对此二运算作成一个环 . 并且这个环的零元是

$$(0, 0, \cdots, 0),$$

又 $(a_1, a_2, \cdots, a_n)$ 的负元是 $(-a_1, -a_2, \cdots, -a_n)$.

我们称这个环 R 为环 R_1'，R_2'，…，R_n' 的<u>外直和</u> .

易知，环 R 可换当且仅当每个环 $R_i'(i = 1, 2, \cdots, n)$ 可换；环 R 有单位元 1 当且仅当每个环 R_i' 都有单位元，并且

$$1 = (1_1, 1_2, \cdots, 1_n),$$

其中 1_i 为环 R_i 的单位元，$i = 1$，2，…，n .

如果令

$$R_i = \{(0,\cdots,0,a_i,0,\cdots,0) \mid a_i \in R_i'\},$$

则易知 R_i 是环 R 的一个双边理想，并且 $R_i \cong R_i'$.

特别有

$$R = R_1 + R_2 + \cdots + R_n,$$

并且 R 中每个元素表为 R_1，R_2，…，R_n 中的元素之和时，只能有一种表示方法．据此，我们给出环的内直和的概念．

定义 1 设 R_1，R_2，…，R_n 是环 R 的 n 个理想．如果

1) $R = R_1 + R_2 + \cdots + R_n$;

2) R 中每个元素表为 R_1，R_2，…，R_n 中元素相加时，表示法惟一，

则称环 R 是子环 R_1，R_2，…，R_n 的内直和，简称__和__，并记为

$$R = R_1 \quad R_2 \quad \cdots \quad R_n$$

或

$$R = \sum_{i=1}^{n} R_i .$$

例 1 模 2 与模 3 剩余类环分别表为

$$Z_2 = \{\bar{0},\bar{1}\}, \quad Z_3 = \{\bar{0},\bar{1},\bar{2}\}.$$

则它们的外直和为

$$R = \{(\bar{0},\bar{0}),(\bar{0},\bar{1}),(\bar{0},\bar{2}),(\bar{1},\bar{0}),(\bar{1},\bar{1}),(\bar{1},\bar{2})\},$$

且易知 $R \cong Z_6$.

例 2 模 6 剩余类环 Z_6 是其子环 (也是理想)

$$R_1 = \{\bar{0},\bar{3}\} \quad 与 \quad R_2 = \{\bar{0},\bar{2},\bar{4}\}$$

的内直和，即 $Z_6 = R_1 \quad R_2$.

从外直和可以得到一个内直和．反过来，从内直和又可以得到一个外直和．因此，在同构意义下二者是一致的．

定理 1 设 $R_i\,(i = 1,2,\cdots,n)$是环 R 的理想，且 $R = \sum_{i=1}^{n} R_i$.

则此和是直和的充分与必要条件是，零元素只能表示成

$$0 = 0 + \cdots + 0 .$$

证 必要性显然,下证充分性.

设零元素只有一种表示法:$0 = 0 + \cdots + 0$,则任取 $a \in R$,并令

$$a = a_1 + a_2 + \cdots + a_n = b_1 + b_2 + \cdots + b_n ,$$

其中 $a_i , b_i \in R, i = 1, 2, \cdots, n$.于是有

$$0 = (a_1 - b_1) + (a_2 - b_2) + \cdots + (a_n - b_n) ,$$

从而 $a_i - b_i = 0, a_i = b_i , i = 1, 2, \cdots, n$.因此,和 $R = \sum_{i=1}^{n} R_i$ 是直和.

(证毕)

定理 2 如定理 1 所设,则和 $R = \sum_{i=1}^{n} R_i$ 是直和的充分与必要条件是:

$$R_i \cap (R_1 + \cdots + R_{i-1} + R_{i+1} + \cdots + R_n) = \{0\}, \quad i = 1, \cdots, n .$$

证 令 $N_i = R_i \cap (R_1 + \cdots + R_{i-1} + R_{i+1} + \cdots + R_n)$.设 $R = \sum_{i=1}^{n} R_i$ 是直和,且 $a \in N_i$.则 $a \in R_i$,且

$$a \in R_1 + \cdots + R_{i-1} + R_{i+1} + \cdots + R_n ,$$

于是可令 $a = a_1 + \cdots + a_{i-1} + a_{i+1} + \cdots + a_n (a_j \in R_j , j \neq i)$.

由此得

$$0 = a_1 + \cdots + a_{i-1} + (-a) + a_{i+1} + \cdots + a_n .$$

但由定理 1,0 的表示法惟一,故 $a = 0$.从而 $N_i = \{0\}$.

反之,设 $N_i = \{0\}$, $i = 1$, 2, $\cdots$, n.且令

$$0 = a_1 + \cdots + a_i + \cdots + a_n .$$

则 $a_i \in N_i = \{0\}$,从而 $a_i = 0, i = 1, 2, \cdots, n$.于是由定理 1 知,和 $R = \sum_{i=1}^{n} R_i$ 是直和.

(证毕)

如果 $R = \sum_{i=1}^{n} R_i$,则根据这个定理,特别可得

$$R_i \cap R_j = \{0\}, \quad i \neq j .$$

于是如果 $a_i \in R_i$，$b_j \in R_j$，则由于 R_i 与 R_j 都是 R 的理想，因此

$$a_i b_j \in R_i \cap R_j = \{0\},$$

从而 $a_i b_j = 0 (i \neq j)$．这样一来，对环 R 中的任意元素

$$a = a_1 + \cdots + a_n, \quad b = b_1 + \cdots + b_n \quad (a_i, b_i \in R_i)$$

便有

$$a + b = (a_1 + b_1) + \cdots + (a_n + b_n),$$

$$ab = a_1 b_1 + \cdots + a_n b_n .$$

这就是说，环 R 的运算完全取决于各被加项 R_i 的运算．从而 R 的结构也取决于各个 R_i 的结构．因此，研究环 R 可以转化为研究其各被加项 R_i．而且一般而言，R_i 的结构比环 R 的结构相对简单，讨论直和的重要性也正在于此．

定义 2 设 N 是环 R 的一个理想．如果存在 R 的理想 N' 使

$$R = N \quad N',$$

则称 N 是环 R 的一个直和项．

环的平凡理想当然都是环的直和项．另外由例 2 知，环 Z_6 的两个非平凡理想

$$R_1 = \{\overline{0}, \overline{3}\}, \qquad R_2 = \{\overline{0}, \overline{2}, \overline{4}\}$$

都是 Z_6 的直和项．

例 3 Z_8 的两个非平凡理想

$$N_1 = \{\overline{0}, \overline{4}\}, \qquad N_2 \{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$$

都不是 Z_8 的直和项．

证 因为 Z_8 只有理想 $\{0\}$，N_1，N_2，Z_8，然而 $N_1 \quad N_2$，$N_1 + N_2 = N_2 \neq Z_8$，故 N_1，N_2 都不是环 Z_8 的直和项．

(证毕)

由于在一个直和中可任意交换被加项次序，或任意加括后其结果仍为直和，因此，如果有直和 $R = \sum_{i=1}^{n} \quad R_i$，则其每个被加项 R_i 显然都是环 R 的直和项．

我们知道，理想的理想不一定是原环的理想，即理想不具有

传递性．但对于直和项来说，情况就不同了．

定理 3 如果环 R 的理想 N 是 R 的一个直和项，则 N 的理想也是环 R 的理想．

证 因为 N 是环 R 的直和项，故存在 N' R 使

$$R = N \quad N'.$$

设 N_1 N，任取 $a_1 \in N_1$，$r \in R$，并令

$$r = a + a' \quad (a \in N, a' \in N'),$$

则

$$ra_1 = (a + a')a_1$$
$$= aa_1 + a'a_1 . \tag{1}$$

但由于 $a_1 \in N_1$ N R，故 $a'a_1 \in N$；又由于

$$a' \in N' \quad R,$$

故 $a'a_1 \in N'$．从而 $a'a_1 \in N \cap N' = \{0\}$，即 $a'a_1 = 0$．于是由(1)知

$$ra_1 = aa_1 \in N_1 .$$

同理有 $a_1 r \in N_1$．因此，N_1 R．

(证毕)

下面定理给出直和的理想的状况．

定理 4 设环 $R = \sum_{i=1}^{m}$ R_i 若 N_i R_i，$i = 1,2,\cdots,m$，则

$$N_1 \quad N_2 \quad \cdots \quad N_m \quad R .$$

反之，设 N R，则当 R 有单位元时存在 N_i R_i 使

$$N = N_1 \quad N_2 \quad \cdots \quad N_m .$$

证 若 N_i R_i，则由定理 3 知 N_i R．从而

$$\sum_{i=1}^{m} \quad N_i \quad R .$$

反之，设 R 有单位元(从而每个 R_i 都有单位元)，且 N 是 R 的任意理想．则易知

$$\phi: \quad a = a_1 + \cdots + a_i + \cdots + a_m \quad a_i \in R_i$$

是环 R 到 R_i 的一个同态满射，于是

$$N_i = \phi(N) \quad R_i, \quad i = 1, 2, \cdots, m.$$

现任取 $b_i \in N_i$，则有 $b = b_1 + \cdots + b_i + \cdots + b_m \in N$. 但 R_i 有单位元，用 1_i 表示，于是有

$$N \ni 1_i b = 1_i b_1 + \cdots + 1_i b_i + \cdots + 1_i b_m$$
$$= 1_i b_i = b_i,$$

即有 $b_i \in N$. 从而 $N_i \quad N$. 因此 $\sum_{i=1}^{m} N_i \quad N$.

但是，$N \quad \sum_{i=1}^{m} N_i$ 是显然的. 因此

$$N = \sum_{i=1}^{m} N_i,$$

其中 $N_i \quad R_i$，$i = 1, 2, \cdots, m$.

(证毕)

这里指出，本定理后一部分要求 R 有单位元，即每个 R_i 都有单位元是必不可少的.

例 4 Z_4 的子环 $\{\bar{0}, \bar{2}\}$ 与自身的外直积

$$R = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{2}), (\bar{2}, \bar{0}), (\bar{2}, \bar{2})\}$$

是一个没有单位元的环，又

$$R_1 = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{2})\}, \quad R_2 = \{(\bar{0}, \bar{0}), (\bar{2}, \bar{0})\}$$

为其两个理想，且易知 $R = R_1 \quad R_2$ 和

$$N = \{(\bar{0}, \bar{0}), (\bar{2}, \bar{2})\} \quad R.$$

但在 R 中不存在理想 N_1，N_2 使 $N = N_1 \quad N_2$.

最后，我们将利用环的特征把环分解成一些相关理想的直和.

定理 5 设 R 是一个特征为 n 的环. 如果 $n = n_1 n_2$，且 $(n_1, n_2) = 1$，则存在 R 的理想 R_1 和 R_2 使

$$R = R_1 \quad R_2,$$

而且其中 $\mathrm{char} R_1 = n_1$，$\mathrm{char} R_2 = n_2$.

证 1) 因为 $(n_1, n_2) = 1$，故存在整数 s，t 使

$$n_1 s + n_2 t = 1 . \tag{2}$$

现在令

$$R_1 = \{ n_2 ta \mid a \in R \}, \qquad R_2 = \{ n_1 sa \mid a \in R \},$$

则易知 $R_i \quad R$, $i = 1, 2$.

又由于对 R 中任意元素 a, 根据(2)式可得

$$\begin{aligned} a &= 1 \cdot a = (n_1 s + n_2 t) a \\ &= n_2 ta + n_1 sa \in R_1 + R_2 , \end{aligned} \tag{3}$$

故 $R = R_1 + R_2$.

再设 $a \in R_1 \cap R_2$, 并令

$$a = n_2 ta, \qquad a = n_1 sa .$$

于是由此并根据 $n = n_1 n_2$ 是 R 的特征可知

$$n_1 a = n_2 a = 0,$$

从而由(3)式又得 $a = 0$. 故 $R_1 \cap R_2 = \{0\}$. 因此

$$R = R_1 \quad R_2 .$$

2) 令 $\operatorname{char} R_i = m_i$, $i = 1, 2$. 由于

$$n_1 (n_2 ta) = nta = 0, \qquad n_2 (n_1 sa) = nsa = 0,$$

故 $m_1 \le n_1$, $m_2 \le n_2$. 从而 $m_1 m_2 \le n_1 n_2 = n$. (4)

在 R 中任取元素 a, 并令

$$a = a_1 + a_2 \qquad (a_i \in R_i),$$

则有 $m_1 m_2 a = m_1 m_2 a_1 + m_1 m_2 a_2 = 0 + 0 = 0$. 于是

$$\operatorname{char} R \le m_1 m_2 , \quad \text{即 } n \le m_1 m_2 .$$

再由(4)式知, 必 $m_1 = n_1$, $m_2 = n_2$. 即

$$\operatorname{char} R_1 = n_1 , \qquad \operatorname{char} R_2 = n_2 .$$

(证毕)

引理 设环 $R = R_1 \quad R_2$, 又 $R_1 = N_1 \quad N_2$. 则

$$R = N_1 \quad N_2 \quad R_2 .$$

证 因为 $N_i \quad R_1$, 但 R_1 是环 R 的直和项, 故由定理 3 知, $N_i \quad R$, $i = 1, 2$.

又显然 $R = N_1 + N_2 + R_2$，且 R 中零元只能表示成 N_1，N_2，R_2 中的零元相加，故

$$R = N_1 \quad N_2 \quad R_2 .$$

(证毕)

这个引理表明，直和代入后仍为直和．

定理 6 设环 R 的特征是 n，且

$$n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m},$$

其中 p_i 是互异素数，$k_i \geq 1$，$i = 1, 2, \cdots, m$．则存在环 R 的理想 R_i，其特征为 $p_i^{k_i}$，并且

$$R = R_1 \quad R_2 \quad \cdots \quad R_m .$$

证 令 $n_1 = p_1^{k_1}$，$n_2 = p_2^{k_2} \cdots p_m^{k_m}$．则

$$n = n_1 n_2, \qquad (n_1, n_2) = 1 .$$

于是由定理 5，存在 R 的理想 R_1，R_1' 使

$$R = R_1 \quad R_1',$$

其中 $\operatorname{char} R_1 = p_1^{k_1}$，$\operatorname{char} R_1' = n_2 = p_2^{k_2} \cdots p_m^{k_m}$．

如果 $m > 2$，则对环 R_1' 可作同样讨论．如此下去，因此有 R 的理想 R_i 使

$$R = R_1 \quad R_2 \quad \cdots \quad R_m,$$

其中 $\operatorname{char} R_i = p_i^{k_i}$，$i = 1, 2, \cdots, m$．

(证毕)

这个定理的意义在于：讨论特征有限的环，可转化为讨论特征是素数幂的环．

习题 4.11

1. 设环 $R = \sum_{i=1}^{n} R_i$．证明：环 R 有单位元当且仅当每个理想 R_i 有单位元．并且

$$1 = 1_1 + 1_2 + \cdots + 1_n,$$

其中 1 是 R 的单位元，1_i 是 R_i 的单位元．

2. 设 $Z_2=\{0,1\}$，且

$$R=\{(a_1,a_2,\cdots,a_n)\mid a_i\in Z_2\},$$

即 R 是 n 个环 Z_2 的外直和．证明：R 是一个布尔环．又 R 的特征为何？

3. 设环 $R=\sum_{i=1}^{n} R_i$．证明：

ϕ_i：$a=a_1+\cdots+a_i+\cdots+a_n \longmapsto a_i$，$i=1,2,\cdots,n$．

（其中 $a_i\in R_i$）是环 R 到 R_i 的同态满射（称为正则投射），且

1）$\phi_i\phi_j=\begin{cases}\phi_i, & i=j;\\ 0, & i\neq j;\end{cases}$

2）$\phi_1+\phi_2+\cdots+\phi_n=\varepsilon$．

其中 0 是零同态（即把环的每个元素都变为零元素），ε 为环 R 的恒等变换．

4. 设 N 是环 R 的一个理想．证明：如果 N 有单位元，则 N 是环 R 的一个直和项．

提示：考虑一切元素 $a-ae$（$a\in R$，e 是 N 的单位元）．

5. 设 n_1，n_2，…，n_s 是 s 个两两互素的正整数．证明：剩余类环 $Z_{n_1n_2\cdots n_s}$ 与 Z_{n_1}，Z_{n_2}，…，Z_{n_s} 的外直和

$$Z_{n_1}\quad Z_{n_2}\quad\cdots\quad Z_{n_s}$$

同构．

6. 设 R 为环，e 是 R 的一个幂等元．又令

$$R(1-e)=\{r-re\mid r\in R\},\qquad (1-e)R=\{r-er\mid r\in R\},$$

$$(1-e)R(1-e)=\{r-re-er+ere\mid r\in R\}.$$

（R 不一定有单位元）证明：

1）$R(1-e)$、$(1-e)R$ 分别为环 R 的左、右理想；

2）eRe、$eR(1-e)$ 与 $(1-e)Re$ 都是 R 的子环，且后二者还是零乘环；

3）作为加群，R 有直和分解：

$$R=Re\quad R(1-e);\qquad R=eR\quad (1-e)R;$$

$$R=eRe\quad eR(1-e)\quad (1-e)Re\quad (1-e)R(1-e).$$

并分别称这三个直和分解为加群 $(R,+)$ 关于幂等元 e 的左、右和双边 Peirce 分解．

提示：用 e 乘某式一边或两边，并证 O 表示法惟一 .

* §12 非交换环

本章最后一节来简单讨论一下非交换环.

对任意正整数 n, n 阶交换环总是存在的, 因为, 模 n 剩余类环 Z_n 就是一个 n 阶交换环. 但是, n 阶非交换环是否存在? 回答显然是否定的. 因为, 显然凡 1 阶和素数阶环都是循环环, 从而都是交换环, 即素数阶的非交换环是不存在的. 本节将进一步讨论: 对什么样的正整数 n, 才存在 n 阶非交换环.

定理 1 对任意整数 $n>1$, 总存在 n^2 阶非交换环.

证 Z_n 作为加群, 作外直和 $Z_n \oplus Z_n$, 并令

$$R=(Z_n,+)\oplus(Z_n,+).$$

现在在加群 R 中再规定乘法如下:

$$(x_1,y_1)(x_2,y_2)=(x_2+y_2)(x_1,y_1). \tag{1}$$

由于当 $(a_1,b_1)=(c_1,d_1),(a_2,b_2)=(c_2,d_2)$ 时有

$$n\mid a_i-c_i,\quad n\mid b_i-d_i,\quad i=1,2,$$

故可知 n 整除 $(a_2+b_2)-(c_2+d_2)$. 于是 n 又整除

$$(a_2+b_2)(a_1-c_1) \quad 与 \quad c_1[(a_2+b_2)-(c_2+d_2)],$$

从而 n 整除它们的和 $a_1(a_2+b_2)-c_1(c_2+d_2)$.

同理, n 整除 $b_1(a_2+b_2)-d_1(c_2+d_2)$.

这就是说, (1) 确为 R 的代数运算.

进一步易证 R 对此代数运算满足结合律, 并且加法对乘法满足分配律. 从而 R 作成一个 n^2 阶的环.

另外, 这个环还是一个非交换环: 因为例如

$$(1,0) \quad 与 \quad (0,1)$$

都属于 R, 但是根据 (1), 有

$$(1,0)(0,1)=(1,0),\quad (0,1)(1,0)=(0,1),$$

即 $(1,0)(0,1)\neq(0,1)(1,0)$.

因此, R 便是一个 n^2 阶的非交换环.

(证毕)

下面再证明另一类非交换环的存在性.

定理 2 对任意素数 p 和任意整数 $n>1$, 总存在 p^s 阶非交换环, 其中 $s=\frac{n(n+1)}{2}$.

证 令 R 是由域 Z_p 上一切 n 阶上三角矩阵作成的集合. 则易知 R 对方阵的普通加法与乘法作成一个环, 而且是一个 p^s 阶的环.

令 E_{ij} 表示第(i,j)元素为 1 而其余元素全为 0 的 n 阶方阵. 则 E_{1n} 与 E_{mn} 都属于 R, 但易知

$$E_{1n}E_{mn}=E_{1n},\qquad E_{mn}E_{1n}=0,$$

即 $E_{1n}E_{nn}\neq E_{mn}E_{1n}$. 从而 R 不可换.

因此, R 是一个 p^s 阶的非交换环.

(证毕)

定理 3 设 n 为大于 1 的整数. 则存在 n 阶非交换环的充要条件是, n 有平方因子. 即存在整数 $d>1$ 使 $d^2\mid n$.

证 1) 必要性 设有 n 阶非交换环 R. 则 R 的加群$(R,+)$是一个 n 阶交换群. 从而由有限交换群的不变因子定理知, 存在阶大于 1 的循环子加群$\blacksquare b_i\blacksquare(i=1,2,\cdots,m)$使

$$(R,+)=\blacksquare b_1\blacksquare\quad\blacksquare b_2\blacksquare\quad\cdots\quad\blacksquare b_m\blacksquare,$$

其中$|b_i|>1(i=1,2,\cdots,m)$, 且 $|b_i|\mid|b_{i+1}|$, $i=1,2,\cdots,m-1$.

由此可知

$$n=|b_1|\cdot|b_2|\cdots|b_m|. \tag{2}$$

又必定 $m>1$: 因若 $m=1$, 则$(R,+)=\blacksquare b_1\blacksquare$为循环群, 即 R 为循环环, 从而 R 是交换环, 这与 R 是非交换环的假设矛盾.

这样由(2)式知, $|b_1|\cdot|b_2|\mid n$. 如果令 $d=|b_1|$, 则 $d>1$, 且由于 $|b_1|\mid|b_2|$, 则可知

$$d^2\mid n.$$

即 n 有平方因子．

2) 充分性 设 n 有平方因子．例如，设

$$n = n_1^2 \cdot n_2, \quad n_1 > 1 .$$

由定理 1，总有 n_1^2 阶非交换环存在，令 R_1 是这样的一个环．再令 R_2 为任意一个 n_2 阶环(不管可换与否)．于是易知环的直和

$$R = R_1 \quad R_2$$

便是一个 $n_1^2 n_2 = n$ 阶的非交换环．

(证毕)

顺便指出，这个定理还是一个构造性定理．即它的证明过程也同时给出了具体构造 $n(n>1$ 且 n 有平方因子$)$ 阶非交换环的方法．

另外，定理 2 证明中所给出的环显然是一个有单位元的非交换环．

例 1 按定理 1 证明中所指出的方法，给出一个 4 阶非交换环．

解 由定理 1 的证明可知：

$$\begin{aligned} R_1 &= (Z_2, +) \quad (Z_2, +) \\ &= \{(0,0),(1,0),(0,1),(1,1)\} . \end{aligned}$$

另外易知，这个 4 阶非交换环的加群$(R_1, +)$是一个 Klein 四元群．如果依次用 0，a，b，c 表示 R_1 中的 4 个元素，则不难给出环 R_1 的乘法表．

另外还易知，Z_2 上的 4 个二阶方阵．

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

关于方阵的普通加法与乘法也作成一个 4 阶非交换环，这个环记为 R_2．容易证明，上面的 4 阶环 R_1 与 R_2 并不同构．

有文献已经证明，不同构的 4 阶非交换环只有这两个．而这两个非交换环又都是没有单位元的．据此，再根据定理 3 便知，

我们以前曾经提到过的一个事实：Z_2 上的所有 2 阶上三角方阵作成的环，是有单位元的阶数最小的非交换环．

例 2 按定理 3 证明中的方法，给出一个 12 阶非交换环．

解 例 1 中的环 R_1 是一个 4 阶非交换环，再取以 3 为模的剩余类环 Z_3，并作此二环的外直和：

$$R = R_1 \oplus Z_3,$$

则 R 是一个 12 阶环．但由于环 R_1 不可换，故 R 也不可换，因此 R 是一个 12 阶的非交换环．

习题 4.12

1. 验算 §12 定理 1 证明中给出的环 R 的结合律成立．

2. 问：§12 定理 1 证明中给出的环 R 是否有单位元？为什么？

3. 给出 §12 例 1 中 4 阶非交换环 R_1 的乘法表，并证明环 R_1 与环 R_2 不同构．

4. 令 R_1' 为由 Z_2 上 4 个二阶方阵

$$\begin{pmatrix}0&0\\0&0\end{pmatrix},\quad \begin{pmatrix}0&0\\0&1\end{pmatrix},\quad \begin{pmatrix}0&1\\0&1\end{pmatrix},\quad \begin{pmatrix}0&1\\0&0\end{pmatrix}$$

关于方阵的普通加法与乘法作成的环．证明：§12 例 1 中的环 R_1 与这个环 R_1' 同构．

5. 给出两个不同构的 12 阶非交换环．

6. 给出两个不同构的无限非交换环．

7. 证明：若 e 是环 R 的惟一的左单位元，则 e 必是 R 的单位元．

8. 设 R 是一个有单位元(用 1 表示)的环，$a, b \in R$．证明：如果 $1 + ab$ 在 R 中有逆元，则 $1 + ba$ 在 R 中也有逆元．

9. 设 R 是一个有单位元的环．如果 R 中元素 a，b 有 $ab = 1$，则称 b 是 a 的一个右逆元，而称 a 是 b 的一个左逆元．证明卡普兰斯基(I. Kaplansky)定理：若 R 中元素 a 有多于一个的右逆元，则 a 必有无限多个右逆元．

提示：令 $S = \{x \mid x \in R, ax = 1\}$，$T = \{xa - 1 + s \mid x \in S\}$，其中 s 是 S 中一个固定元素．再往证：$T \subset S$，$|S| = |T|$．

10. 设 R 是一个有单位元的环，a，b 是 R 中的单位(即可逆元)．证明：若有二互素整数 m，n 使

$$a^m = b^m, \quad a^n = b^n,$$

则必 $a = b$．

11. 设 R 为布尔环，即 R 中每个元素 x 都有 $x^2 = x$．证明：若 $|R| \geq 3$，则 R 不是整环．

12. 设 R 是一个 Jacobson 环，即对 R 中每个元素 a 都有与 a 有关的整数 $n > 1$ 使 $a^n = a$．证明：R 的幂等元都是中心元．

13. 设 R 是一个有单位元(用 1 表示)的有限环．证明：如果 $ab = 1$，则必 $ba = 1$．

14. 若对环 R 中每个元素 a 都有 $a' \in R$(a'与 a 相关)使 $a = aa'a$，则称 R 为<u>正则环</u>．证明：

1) p - 环是正则环．但反之不成立；

2) 再指出正则环的子环不一定是正则环；

3) 对正则环 R 中任二元素 a，b，都有 R 中幂等元 e_1，e_2 使

$$Ra = Re_1, \quad Ra + Rb = Re_2.$$

提示：若 $aa'a = a$，则令 $e_1 = a'a$．再令 $R(b - ba) = Re$，$e_2 = e_1 + e - e_1 e$．

15. 设 R 是一个正则环．证明：若 R 中元素 a 对 R 中任意元素 x 都有 $b \in R$ 使

$$ax + b + axb = 0,$$

则必 $a = 0$．

16. 设 $G = \langle a \rangle$ 为 n 阶循环群，$U(Z_n)$ 为模 n 剩余类环 Z_n 的单位群．证明：

$$\mathrm{Aut}G \cong U(Z_n);$$

再由此利用数论结论证明：

$\mathrm{Aut}G$ 是循环群 $\Leftrightarrow$ n 为 2，4，p^k，$2p^k$(p 为奇素数)．

提示：$\sigma_m \to$ 疑，其中 $\sigma_m(a) = a^m$．

17. 如果一个环的特征是素数，问：这个环是否一定无零因子？

18. 证明：若加群 G 为可分解群，则其自同态环不是域．

19. 证明：有理数域 Q 的加群$(Q, +)$的自同态环与 Q 同构．

20. 在所有 n 阶循环中，有而且只有 $T(n)$ 个是互不同构的，其中 $T(n)$ 表示 n 的正因数的个数．

21. 设 $Z[i]=\{a+bi \mid a,b\in Z\}$ 为Gauss 整环．问：环 Z[i]/ ■1 + i■ 有多少个元素？是否为域？

22. 设环 R 有一个分类，S 是所有类 $[a],[b],[c],\cdots$ 的集合．证明：如果

$$[x]+[y]=[x+y],$$

$$[x][y]=[xy]$$

是 S 的两个代数运算，则 $[0]$ 是 R 的理想，且给定的分类恰好是关于 $[0]$ 的陪集．

23. 令 R 是一个有单位元的可换环，N 是 R 的全体幂零元作成的集合．证明：N R 且 R/N 不含非零幂零元．

24. 设 N_1，N_2 是环 R 的两个理想，规定

$$N_1 N_2=\{\text{有限和}\sum a_i b_i \mid a_i\in N_1, b_i\in N_2\}.$$

证明：$N_1 N_2$ R，且 $N_1 N_2$ $N_1\cap N_2$．

25. 证明：n 阶循环环 R 是域的充分与必要条件是，n 为素数且 R 不是零乘环．

26. 如果环 R 是单环或者 R 的所有非平凡理想都是域，则称 R 为NF - 环．证明：若环 R 的阶为 pq（p,q 是互异素数），则

R 是 NF - 环 R 有单位元．

27. 设 R 为 p^2 阶环（p 为素数）．证明：

R 是 NF - 环 R 是域或 R ü Z_p Z_p．

提示：以上二题可参阅书末参考文献[14]．

28. 证明本章§2 引理．

提示：若 $AX=0$ 有解 $k_1\neq 0$，k_2，…，k_n，则 $k_1 M_n=0$（$m\geq n, M_n$ 为 A 的 n 阶子式）．反之，设 r(A) = $r<n$，则有 $kM_r\neq 0$，$kM_{r+1}=0$（M_{r+1} 包含 M_r）．可证 $kd_1,\cdots,kd_{r+1},0,\cdots,0$ 为非零解（$d_1,\cdots,d_{r+1}$ 是 M_{r+1} 末行元素的代数余子式）．

29. 设 $R[x]$ 是有单位元的交换环 R 上的多项式环．证明：

$0\neq f(x)$ 是 $R[x]$ 的零因子 有 $0\neq c\in R$ 使 $cf(x)=0$．

30. 设 Z_n^* 为模 n 剩余类环 Z_n 的单位群．证明：Z_n^* 中每个元素都满足 $x^2=1$ 的充要条件是，n 为以下整数：

2，3，4，6，8，12，24．

提示：分 n 为 $2^s \cdot 3^t$，p^k，$2^s p^t$（p 为素数且 > 3），$2^s \cdot p_1^{t_1} p_2^{t_2} \cdots p_n^{t_m}$（$p_i$ 为互异奇素数）．参书末参考文献[13]．

第五章　惟一分解整环

我们知道，整数环中的每一个合数都可以惟一地分解成素数的乘积；数域上每一个次数大于零的可约多项式，都可以惟一地分解成不可约多项式的乘积．这是整数环和数域上多项式环中元素的最基本最重要的性质之一．在这一章里，我们要把整数环和多项式环的这些讨论推广到更一般的环上去．

整数环和数域上的多项式环不是一般的环，它们都是有单位元的整环，我们的推广工作也只能在这种环中进行．因此，本章所说的环 K，均假定为单位元的整环且 $|K|>1$．

§1　相伴元和不可约元

要想推广整数环和多项式环中关于因子分解的理论，就必须首先对整除、因子、不可约多项式和素数等概念，在环 K 中作相应的推广．

定义 1　设 $a,\ b\in K$．如果存在元素 $c\in K$，使

$$a=bc,$$

则称 b 整除 a，也称 b 是 a 的一个子，记为 $b\mid a$．若 b 不能整除 a，则记为 $b\nmid a$．

通常整除的一些基本性质在这里均仍成立，不再赘述．

我们知道，环中有逆元的元素叫可逆元或单位．在环 K 中，1 和 -1 永远是单位．当然，K 可能还有别的单位．例如，虽然

整数环中的单位只有± 1，而域 F 上多项式环的单位则为全体零次多项式，即 F 中的全体非零元素．

在环 K 中，如果 $a=b\varepsilon$，其中 ε 是 K 的一个单位，则称 a 与 b 相伴，并称 a 是 b 的相伴元．

显然，环 K 中元素的相伴关系是一个等价关系．因此，若 a 与 b 相伴，则 a 与 b 互为相伴元．易知：

元素 a 与 b 相伴　　a 与 b 互相整除．

因此，整数环中两个整数相伴，当且仅当这两个整数相等或只差一个符号；域 F 上两个多项式相伴，当且仅当这两个多项式只差一个非零常数因子．

显然，环 K 中任何元素 a 永远能被单位及 a 的相伴元整除，即单位及 a 的相伴元永远是 a 的因子．我们称这种因子为 a 的当然因子(平凡因子)；别的因子，如果存在的话，称为 a 的当然因子(非平凡因子)或真因子．

例 1　求出 Gauss 整环 $Z[i]$ 中的所有单位以及整数 5 在 $Z[i]$ 中的所有真因子．

解　由上一章§3 例 2 知，$Z[i]$ 的所有单位是：

$$1,\quad -1,\quad i,\quad -i.$$

设 $\alpha=a+bi$ 是 5 在 $Z[i]$ 中的任一真因子，则存在 $\beta\in Z[i]$ 使

$$5=\alpha\beta,\qquad 25=|\alpha|^2|\beta|^2,$$

这只有 $|\alpha|^2=1$，5 或 25．

由于 α 是 5 的真因子，而环 $Z[i]$ 的单位只有 ± 1，$\pm i$，故 $|\alpha|^2\neq 1$；又 $|\alpha|^2\neq 25$：因若 $|\alpha|^2=25$，则由上知，$|\beta|^2=1$，即 β 是单位，α 与 5 相伴，这与 α 是 5 的真因子矛盾．故只有

$$|\alpha|^2=a^2+b^2=5.$$

解此方程可得

$$a=\pm 1,\qquad a=\pm 2,$$
$$b=\pm 2;\qquad b=\pm 1.$$

于是，5 的全部真因子共有 8 个，它们是

$$\pm 1 \pm 2i, \quad \pm 2 \pm i .$$

实际上，5 的不相伴的真因子只有两个：$1 \pm 2i$．而其余的真因子都与这两个中的某一个相伴．

（证毕）

定义 2 设 $a \in K$，$a \neq 0$，且 a 不是单位．如果 a 只有平凡因子，则称 a 为环 K 的一个不可约元；如果 a 有非平凡因子，则称 a 为环 K 的一个可约元．

显然，域 F 上多项式环 $F[x]$ 中的不可约元就是全体不可约多项式，而整数环 Z 中的不可约元就是全体正负素数．

定理 1 环 K 中不可约元 p 与任何单位 ε 的乘积 εp 仍是 K 的不可约元．

证 首先，由于 $\varepsilon \neq 0$，$p \neq 0$，而 K 无零因子，所以 $\varepsilon p \neq 0$；又 εp 也不是单位：因若不然，设

$$(\varepsilon p)\varepsilon' = 1 \quad \text{或} \quad p(\varepsilon\varepsilon') = 1,$$

这与 p 是不可约元矛盾．

其次，设 $b \mid \varepsilon p$，令 $\varepsilon p = bc$，且 b 不是单位，则有

$$p = b(\varepsilon^{-1} c),$$

即 $b \mid p$．但 p 是不可约元，故 b 只能是 p 的相伴元．设

$$b = \eta p = (\eta\varepsilon^{-1})(\varepsilon p) \quad (\eta \text{是单位}),$$

由于 $\eta\varepsilon^{-1}$ 也是单位，故 b 是 εp 的相伴元，即 εp 只有当然因子．因此，εp 是不可约元．

（证毕）

定理 2 设 a 是环 K 中的一个非零元．则 a 有真因子的充分与必要条件是，在 K 中存在非单位 b，c 使

$$a = bc .$$

证 设 a 有真因子 b，则存在 $c \in K$，使

$$a = bc .$$

由于 b 是 a 的真因子，故 b 不是单位．显然，c 也不是单位，

否则 b 与 a 相伴，这与 b 是 a 的真因子矛盾．因此，b 与 c 都不是单位．

反之，设 $a=bc$，其中 b 与 c 都不是单位，则由于整环 K 无零因子，消去律成立，故易知 b 也不是 a 的相伴元，从而 b 是 a 的真因子．

(证毕)

定义 3　设 $a\in K$．如果 K 中有不可约元 p_1，p_2，…，p_r 及不可约元 q_1，q_2，…，q_s 使

$$a=p_1p_2\cdots p_r=q_1q_2\cdots q_s$$

时便有 $r=s$，且适当交换不可约元的次序后，p_i 与 q_i 相伴 $(i=1,2,\cdots,r)$，则称元素 a 在 K 中惟一分解．

因为不可约元不能是零元，环 K 又无零因子，故零元不能表成不可约元相乘．同样易知，单位也不可能表成不可约元相乘．因此，在环 K 中，零元和单位当然都不能惟一分解．但是，别的元素如何？这个问题的一般回答是很困难的，有时甚至是不可解决的．即使我们要判断一个元素是不是不可约，有时也是不容易的．例如，要判断环 $F[x]$ 中的多项式是否不可约就属于这种情形．但是，对有些环中的有些元素来说，是完全可以作出判断的．

例 2　证明：9 在有单位元的整环

$$Z[\sqrt{5}i]=\{a+b\sqrt{5}i\mid a,b\in Z\}$$

中不能惟一分解．

证　首先易知，ε 是 $Z[\sqrt{5}i]$ 中的单位当且仅当 $|\varepsilon|=1$，从而可知 $Z[\sqrt{5}i]$ 中的单位只有 ±1．

其次，若 $|\alpha|^2=9$，则 α 必是环 $Z[\sqrt{5}i]$ 的不可约元．

事实上，若 $\beta=a+b\sqrt{5}i$ 是 α 的任一因子，则有 $\gamma\in Z[\sqrt{5}i]$，使

$$\alpha=\beta\gamma,\qquad |\beta|^2|\gamma|^2=|\alpha|^2=9,$$

这只有 $|\beta|^2 = 1, 3$ 或 9．但易知 $|\beta|^2 = a^2 + 5b^2 = 3$ 不可能，故只有

$$|\beta|^2 = 1 \text{ 或 } 9 .$$

当 $|\beta|^2 = 1$ 时，β 是可逆元；当 $|\beta|^2 = 9$ 时，$|\gamma|^2 = 1$，即 γ 是单位，于是 β 与 α 相伴．因此，α 只有平凡因子，即 α 是不可约元．

由此可知，环 $Z[\sqrt{5}i]$ 中的元素 3 及 $2 \pm \sqrt{5}i$ 都是不可约元．但是却有

$$9 = 3 \cdot 3 = (2 + \sqrt{5}i)(2 - \sqrt{5}i),$$

而且 3 又不与 $2 \pm \sqrt{5}i$ 中的任一个相伴，即 9 不能惟一分解．

（证毕）

定义 4 设 $p \in K$，$p \neq 0$，且 p 不是单位．如果 $p \mid ab$ 就必有 $p \mid a$ 或 $p \mid b$，则称 p 是 K 的一个**元**．

定理 3 整环 K 中的素元一定是不可约元．

证 设 p 是 K 中的任一素元，a 是 p 的任一因子，且

$$p = ab . \tag{1}$$

由于整环 K 有单位元，故 $p \mid p$，$p \mid ab$．但 p 是素元，故有

$$p \mid a \quad \text{或} \quad p \mid b .$$

若 $p \mid a$，令 $a = pc$，代入(1)得

$$p = pcb \quad \text{或} \quad cb = 1 .$$

即 b 是单位，从而 a 与 p 相伴．

若 $p \mid b$，则同上可得 a 是单位．

总之说明 p 只有平凡因子，从而 p 是不可约元．

（证毕）

应注意，这个定理的逆定理不成立，即不可约元不一定是素元．例如在例 2 中，$Z[\sqrt{5}i]$ 是有单位元的整环，3 是它的不可约元；又由于

$$3 \mid (2 + \sqrt{5}i)(2 - \sqrt{5}i),$$

但易知，3 不能整除 $2+\sqrt{5}i$ 与 $2-\sqrt{5}i$ 中任何一个，即 3 不是环 $Z[\sqrt{5}i]$ 的素元．

习题　5.1

1. 证明：在有单位元的整环 K 中，二元素相伴的充要条件是二者互相整除．

2. 设 p 是有单位元整环 K 的素元，ε 是 K 的单位．证明：εp 是 K 的素元．

3. 试指出环 $Z[x]$ 中的单位和不可约元．

4. 证明：在环 $Z[\sqrt{5}i]=\{a+b\sqrt{5}i \mid a,b\in Z\}$ 中，元素 $2+\sqrt{5}i$ 不能整除 3．

5. 令 $K=\left\{\frac{m}{2^n}\,\middle|\, m \text{ 为整数}, n \text{ 为非负整数}\right\}$．试指出环 K 中的单位和不可约元．

§2　惟一分解整环定义和性质

定义 1　设 K 是有单位元的整环．如果 K 中每个既不是零又不是单位的元素都能惟一分解，则称 K 为<u>一分解整环</u>．

由此定义可知，整数环 Z 及域 F 上多项式环 $F[x]$ 都是惟一分解整环．但上节例 2 中的环

$$Z[\sqrt{5}i]=\{a+b\sqrt{5}i \mid a,b\in Z\}$$

不是惟一分解整环，因为例如元素 9 在这个环中就不能惟一分解．

由上节知道，素元一定是不可约元，但不可约元不一定是素元．可是对整数环和域上多项式环来讲，素元和不可约元是一致的．更一般的，对任意惟一分解整环都是这样．

定理 1　设 K 是任意一个惟一分解整环．则 p 是 K 的素元当且仅当 p 是 K 的不可约元．

证 由上节知，K 中素元一定是不可约元．

反之，设 p 是 K 的一个不可约元，且 $p \mid ab$．令

$$ab = pc, \quad c \in K. \tag{1}$$

若 a, b 中有零元或单位，则显然 p 至少整除 a，b 中的一个．因此，下设 a 与 b 既不是零元也不是单位．

由于 K 无零因子，这时 $c \neq 0$．同时 c 也不是单位，否则，pc 将是不可约元且能表成两个非单位的乘积，由上节定理 2 知，pc 有真因子，矛盾．

因为 K 是惟一分解整环，而 $c \neq 0$ 且 c 又不是单位，因此，c 以及 a, b 都可惟一分解，设为

$$a = q_1 q_2 \cdots q_r, \quad b = q_1' q_2' \cdots q_s',$$
$$c = p_1 p_2 \cdots p_n, \quad q_i,\ q_j',\ p_t \text{ 为不可约元}.$$

则由(1)得

$$q_1 q_2 \cdots q_r q_1' q_2' \cdots q_s' = p p_1 p_2 \cdots p_n.$$

由惟一分解定义知，不可约元 p 一定与某个 q_i 或 q_j' 相伴．

若 p 与 q_i 相伴，则 $p \mid q_i$．但 $q_i \mid a$，从而 $p \mid a$;

若 p 与 q_j' 相伴，则类似可得 $p \mid b$.

总之，p 必整除 a，b 中的一个，即 p 是 K 的素元．

(证毕)

在一定意义下，这个定理的逆定理也成立．

定理 2 设 K 是有单位元的整环．如果

1) K 中每个既不是零又不是单位的元素都可分为不可约元的乘积;

2) K 中的不可约元都是素元;

则 K 是一个惟一分解整环．

证 任取 $a \in K$，且 $a \neq 0$，又不是单位．根据 1)，设

$$a = p_1 p_2 \cdots p_r, \quad p_i \text{ 为不可约元},$$

假定还有

$$a = q_1 q_2 \cdots q_s, \quad q_i \text{ 为不可约元},$$

下证 $r=s$，且适当交换不可约元的次序后使 p_i 与 q_i 相伴．

对 r 用归纳法证明这一事实．

当 $r=1$ 时，有

$$a=p_1=q_1 q_2\cdots q_s .$$

如果 $s>1$，则 q_1 将是 p_1 的一个真因子，但这是不可能的，故 $s=1$，且 $p_1=q_1$，结论成立．

假定 K 中能写成 $r-1$ 个素元的乘积的元素都有惟一分解，再证

$$a=p_1 p_2\cdots p_r=q_1 q_2\cdots q_s \tag{2}$$

也有惟一分解．

事实上，由于 $p_1 \mid q_1 q_2\cdots q_s$，则 p_1 必整除 q_1，q_2，…，q_s 中的一个．不妨设 $p_1 \mid q_1$，则 p_1 与 q_1 相伴．设

$$p_1=\varepsilon q_1,\quad \varepsilon \text{是单位},$$

代入(2)式，两端消去 q_1 后，所得元素设为 b，即

$$b=(\varepsilon p_2)p_3\cdots p_r=q_2\cdots q_s .$$

b 是 $r-1$ 个不可约元的乘积，故由归纳假设

$$r-1=s-1,$$

且适当交换不可约元次序，有

$$q_2=\varepsilon_2'(\varepsilon p_2),\quad q_3=\varepsilon_3' p_3,\quad \cdots,\quad q_r=\varepsilon_r' p_r,$$

其中 ε_i' 是单位．从而 $r=s$，且 p_i 与 q_i 相伴，即 a 可惟一分解．从而 K 是惟一分解整环．

(证毕)

这样，我们可以利用这个定理来判断一个有单位元的整环是不是惟一分解环．

整数环中的最大公因数和多项式环 $F[x]$ 中的最大公因式的概念和讨论，也可以在惟一分解整环中得到推广．

定义 2 设 K 是一个有单位元的整环．如果 c 是每个元素 a_1，a_2，…，a_n 的因子，则称 c 是这 n 个元素的一个公因子．

如果 d 是 a_1，a_2，…，a_n 的一个公因子，而且 a_1，a_2，…，a_n 的任何公因子都是 d 的一个因子，则称 d 是 a_1，a_2，…，a_n 的一个 大公因子．并记为

$$(a_1, a_2, \cdots, a_n) = d .$$

定理 3 设 K 为惟一分解整环，则 K 中任二元素都有最大公因子存在，且任二最大公因子间只差一个单位因子．

证 任取 $a \in K$．若 $a = 0$，则显然 b 是 a 与 b 的一个最大公因子；若 a 是单位，则显然 a 就是 a 与 b 的一个最大公因子．因此，下设 a，b 既不是零元也不是单位．

设

$$a = q_1 q_2 \cdots q_r, \qquad b = q_1' q_2' \cdots q_s',$$

其中 q_i，q_j' 是素元，且假定 p_1，p_2，…，p_n 是

$$q_1, \ q_2, \ \cdots, \ q_r, \ q_1', \ q_2', \ \cdots, \ q_s'$$

中互不相伴的素元，而其中别的素元都同某个 p_i 相伴．这样，a 与 b 可表为

$$a = \varepsilon_1 p_1^{t_1} p_2^{t_2} \cdots p_n^{t_n}, \qquad b = \varepsilon_2 p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n},$$

其中 ε_1，ε_2 是单位，而 t_i，k_i 是非负整数．

令 $l_i = \min(t_i, k_i)$，且

$$d = p_1^{l_1} p_2^{l_2} \cdots p_n^{l_n},$$

则显然 d 是 a，b 的一个公因子．

又假定 c 是 a，b 的任一公因子，若 c 是单位，则当然 $c \mid d$；若 c 不是单位，则令

$$c = p_1' p_2' \cdots p_t', \qquad p_i' \text{为素元}.$$

由于 $c \mid a$，故每个 $p_i' \mid a$，从而 p_i' 整除某个 p_j．但二者都是素元，故相伴．这样可设

$$c = \varepsilon_3 p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n},$$

其中 ε_3 是单位，m_i 是非负整数．由于 $c \mid a$，且 p_i 与 p_j $(i \neq j)$ 互不相伴，故 $m_i \leq t_i$．

同理可得 $m_i \leq k_i$．因此 $m_i \leq l_i$，从而 $c \mid d$，即 d 是 a 与 b

的一个最大公因子．

假定 d' 也是 a 与 b 的一个最大公因子，则易知 d 与 d' 互相整除，从而二者相伴．

（证毕）

利用数学归纳法可进一步推广这个定理．

推论　惟一分解整环 K 中的元素 a_1，a_2，…，a_n 在 K 中有最大公因子存在，而且其任二最大公因子均相伴．

我们知道，对于整数环或数域上的多项式环 R 来说，如果 $(a, b) = d$，则在 R 中存在元素 s，t 使

$$as + bt = d .$$

但这一事实对惟一分解整环一般不再成立．例如，由高等代数知，$Z[x]$ 是一个惟一分解整环，在这个环中 $(2, x) = 1$，但显然不存在整系数多项式 $s(x)$，$t(x)$ 使

$$2s(x) + xt(x) = 1 .$$

在惟一分解整环中还可以讨论互素的概念．

定义 3　如果惟一分解整环中的元素 a_1，a_2，…，a_n 的最大公因子是单位，则称这 n 个元素**互素**．并记为 $(a_1, a_2, \cdots, a_n) = 1$．

定理 4　在惟一分解整环 K 中，如果 $a \mid bc$，$(a, b) = 1$，则

$$a \mid c .$$

证　如果 a，b，c 中有零元或单位，则结论是明显的．因此下设 a，b，c 都不是零元和单位．

由于 K 是惟一分解整环，故可设

$$b = p_1 p_2 \cdots p_r , \qquad c = p_1' p_2' \cdots p_s' , \tag{3}$$

$$a = q_1 q_2 \cdots q_t , \tag{4}$$

其中 p_i，p_j'，q_k 都是素元．由于 $a \mid bc$，故存在 $d \in K$ 使

$$bc = ad . \tag{5}$$

把(3)，(4)代入(5)，得

$$p_1 p_2 \cdots p_r p_1' p_2' \cdots p_s' = q_1 q_2 \cdots q_t d .$$

由于 K 是惟一分解整环，而 $(a, b) = 1$，故 q_k 不能与任何 p_i 相

伴，只有 q_1，q_2，…，q_t 与 p_1'，p_2'，…，p_s' 中的元素相伴，从而 $a \mid c$.

(证毕)

习题 5.2

1. 证明：整数环上的多项式环 $Z[x]$ 是一个惟一分解整环.

2. 证明本节推论.

3. 设 K 是一个有单位元的整环，a，$b \in K$. 证明：主理想 (a) 与 (b) 相等当且仅当 a 与 b 相伴.

4. 设 K 是一个有单位元的整环. 证明：$K = (a)$ 当且仅当 a 是 K 的单位.

5. 设 a_1，a_2，…，a_n 是惟一分解整环 K 中 n 个不全为 0 的元素，且在 K 中有

$$a_1 = db_1, \quad a_2 = db_2, \quad \cdots, \quad a_n = db_n.$$

证明：$(a_1, a_2, \cdots, a_n) = d$ $\quad$ $(b_1, b_2, \cdots, b_n) = 1$.

提示：若 $(b_1, b_2, \cdots, b_n) = 1$，可设 $(a_1, a_2, \cdots, a_n) = d_0$.

§3 主理想整环

在这一节和下一节，主要介绍两种特殊的惟一分解整环，这就是主理想整环和欧氏环. 这两种环在环的讨论中也占有重要地位.

定义 设 K 是一个有单位元的整环. 如果 K 的每一个理想都是一个主理想，则称 K 是一个 **理想整环**.

由上一章知道，整数环和域 F 上的多项式环 $F[x]$ 都是主理想整环. 但是，整数环 Z 上的多项式环 $Z[x]$ 不是一个主理想整环，因为上一章 §7 曾指出，例如其理想 $(2, x)$ 就不是一个主理想.

应注意，尽管模 n 剩余类环 Z_n 的每个理想都是主理想，但是当 n 为合数时 Z_n 有零因子，从而此时 Z_n 并不是主理想整环.

定理 1 Gauss 整环 $Z[i]$ 是主理想整环.

证 令 $0 \neq N \in Z[i]$，而 α 是 N 中绝对值最小的一个非零元

素，下证 $N=(\alpha)$.

任取 $\beta\in N$，则

$$\frac{\beta}{\alpha}\in Q[i]=\{a+bi\mid a,b\in Q\}\ .$$

令

$$\frac{\beta}{\alpha}=r+si,\quad r,s\in Q\ .$$

设 m，n 是分别最接近 r，s 的两个整数，从而

$$0\leq|r-m|\leq\frac{1}{2},\quad 0\leq|s-n|\leq\frac{1}{2}\ .$$

于是 $\gamma=m+ni\in Z[i]$，并由上可得

$$\left|\frac{\beta}{\alpha}-\gamma\right|=\sqrt{(r-m)^2+(s-n)^2}$$

$$\leq\sqrt{\frac{1}{4}+\frac{1}{4}}=\frac{1}{2}<1\ .$$

但是 $\theta=\beta-\alpha\gamma\in N$，再由 $\left|\frac{\beta}{\alpha}-\gamma\right|<1$ 又得

$$|\theta|=|\beta-\alpha\gamma|<|\alpha|\ .$$

但 α 是 N 中绝对值最小的非零元素，故 $\theta=0$，即 $\beta-\alpha\gamma=0$，从而

$$\beta=\alpha\gamma\in(\alpha),$$

因此 $N=(\alpha)$.从而 $Z[i]$ 是主理想整环 .

（证毕）

本节要证明的一个主要结论是，主理想整环一定是惟一分解整环 . 为此，先证明以下两个引理 .

引理 1 设 K 是一个主理想整环 . 若在序列

$$a_1,\ a_2,\ \cdots,\ a_i,\ \cdots\quad (a_i\in K)\qquad (1)$$

里，每个元素都是前一个元素的真因子，则这个序列一定是个有限序列 .

证 由于 a_{i+1} 是 a_i 的真因子，对这些元素中的每一个作主理想，必得

$$(a_1) \subset (a_2) \subset (a_3) \subset \cdots,$$

令

$$N = (a_1) \cup (a_2) \cup (a_3) \cup \cdots,$$

则易知 $N \supset K$. 但由于 K 是主理想整环，故可设

$$N = (d).$$

由于 $d \in N$，故 d 属于某个 (a_n). 下证 a_n 是序列(1)中最后一个元素.

若不然，设在(1)中还有 a_{n+1}，则由于

$$d \in (a_n), \quad a_{n+1} \in N = (d),$$

因此 $a_n \mid d$, $d \mid a_{n+1}$，从而 $a_n \mid a_{n+1}$，这与 a_{n+1} 是 a_n 的真因子矛盾.

(证毕)

引理 2 主理想整环中不可约元生成的理想是极大理想.

证 设 p 是主理想整环 K 中的一个不可约元，而 $N = (a)$ 是 K 的一个理想，且

$$(p) \subset (a),$$

从而 $a \mid p$. 但 p 是不可约元，故 a 只能是单位或 p 的相伴元.

若 a 是单位，则 $(a) = K$; 若 a 是 p 的相伴元，则由上节习题知 $(p) = (a)$，这说明 (p) 是 K 的极大理想.

(证毕)

现在来证明本节的主要定理.

定理 2 主理想整环是惟一分解整环.

证 设 K 是一个主理想整环，任取 $a \in K$，且 $a \neq 0$，也不是单位.

1) 若 a 不能表成有限个不可约元的乘积，则 a 不是不可约元，从而 a 有真因子. 于是由 §1 定理 2 可得

$$a = a_1 b_1 \quad (a_1, b_1 \text{ 是 } a \text{ 的真因子}),$$

其中 a_1, b_1 至少有一个不能表成不可约元的乘积，否则 a 将表成不可约元的乘积. 不妨设 a_1 不能表成不可约元的乘积，从而 a_1 是不可约元. 同样，a_1 又有真因子 a_2，而 a_2 不能表成不可约

元的乘积，等等．这个过程显然可以无限延续下去，随得无穷序列

$$a,\ a_1,\ a_2,\ \cdots,$$

其中每个都是前一个的真因子，这同引理 1 矛盾．

因此，a 可表成不可约元的乘积．

2) 设 p 是 K 的一个不可约元，且 $p \mid ab$，则由于 K 是主理想整环，故由引理 2 知，$\blacksquare p\blacksquare$ 是 K 的极大理想，从而 $K/\blacksquare p\blacksquare$ 是一个域．又根据 $p \mid ab$ 知，$ab \in \blacksquare p\blacksquare$，从而

$$(a+\blacksquare p\blacksquare)(b+\blacksquare p\blacksquare) = ab+\blacksquare p\blacksquare = \blacksquare p\blacksquare\ .$$

但域无零因子，因此

$$a+\blacksquare p\blacksquare = \blacksquare p\blacksquare \quad \text{或} \quad b+\blacksquare p\blacksquare = \blacksquare p\blacksquare,$$

即 $a \in \blacksquare p\blacksquare$ 或 $b \in \blacksquare p\blacksquare$，亦即

$$p \mid a \quad \text{或} \quad p \mid b\ .$$

这说明 K 中的不可约元都是素元．

根据上节定理 2 知，K 是一个惟一分解整环．

(证毕)

应注意，这个定理的逆定理不成立，即一个惟一分解整环不一定是一个主理想整环．因为由上节知，$Z[x]$ 是一个惟一分解整环，但我们知道，$Z[x]$ 不是主理想整环．

习题　5.3

1. 证明：在主理想整环中，P 是素理想当且仅当 P 由素元生成．

2. 设 K 是主理想整环，又 $\blacksquare a, b\blacksquare = \blacksquare d\blacksquare$．证明：$d$ 是 a，b 的一个最大公因子．由此进一步指出，a 与 b 的任何最大公因子 d 均可表为

$$d' = as + bt, \qquad s,\ t \in K\ .$$

3. 问：主理想整环的子环是否是主理想整环？请证明或举出反例．

4. 设 K'，K 是两个主理想整环，且 $K' \leqq K$．又 a，$b \in K'$，d 是 a 与 b 在 K' 中的最大公因子．证明：d 也是 a 与 b 在 K 中的一个最大公因子．

5. 设 K 是一个主理想整环，又 $0 \neq a \in K$．证明：在 K 中仅有有限个

理想包含 a.

6. 证明：主理想整环 K 中的元素 a_1，a_2，…，a_n 互素的充要条件是，存在 b_1，b_2，…，$b_n \in K$，使

$$\sum_{i=1}^{n} a_i b_i = 1 .$$

§4 欧 氏 环

这一节我们介绍另一种惟一分解整环——欧氏环.

定义 设 K 是一个有单位元的整环. 如果

1) 有一个从 K 的非零元集 $K-\{0\}$ 到非负整数集的映射 ϕ 存在;

2) 这个 ϕ 对 K 中任意元素 a 及 $b\neq 0$，在 K 中有元素 q，r 使

$$a = bq + r, \quad r = 0 \text{ 或 } \phi(r) < \phi(b),$$

则称 R 关于 ϕ 作成一个欧氏环.

例 1 整数环 Z 是欧氏环.

证 1) 令

$$\phi: \quad a \quad |a|,$$

则 ϕ 显然是 $Z-\{0\}$ 到非负整数的一个映射.

2) 任给整数 a 及 $b\neq 0$，存在整数 q，r 满足

$$a = bq + r, \quad r = 0 \text{ 或 } 0 < r < |b|,$$

亦即 $r=0$ 或 $\phi(r) < \phi(b)$. 故 Z 关于 ϕ 作成一个欧氏环.

例 2 域 F 上多项式环 $F[x]$ 是一个欧氏环.

证 1) 令

$$\phi: \quad f(x) \quad f(x) \text{次数},$$

则 ϕ 是非零多项式集到非负整数集的一个映射.

2) 在 $F[x]$ 中任取 $f(x)$ 及 $g(x)\neq 0$，存在 F 上多项式 $q(x)$，$r(x)$ 满足

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

其中 $r(x)=0$ 或 $r(x)$ 的次数 $<$ $g(x)$ 的次数.

因此，$F[x]$也是一个欧氏环．

欧氏环同主理想整环有以下关系．

定理 欧氏环必是主理想整环，因而是惟一分解整环．

证 设 K 是任一欧氏环，$N \quad K$．

若 $N=0$，则 $N=\blacksquare 0\blacksquare$，当然是主理想；若 $N\neq 0$，设 K 是关于 ϕ 的一个欧氏环，则 N 的全体非零元素的象中一定有一个最小的，假定是 $\phi(a)$，其中 $a\in N$，$a\neq 0$．

任取 $b\in N$，则有 q，$r\in K$ 使

$$b=aq+r, \qquad r=0 \text{ 或 } \phi(r)<\phi(a),$$

因为 a，$b\in N$，N 是理想，故

$$r=b-aq\in N,$$

若 $r\neq 0$，则 $\phi(r)<\phi(a)$，这与 $\phi(a)$ 的最小性相矛盾．故必 $r=0$，从而

$$b=aq\in \blacksquare a\blacksquare,$$

故 $N \quad \blacksquare a\blacksquare$．但 $a\in N$，故又有 $\blacksquare a\blacksquare \quad N$．因此

$$N=\blacksquare a\blacksquare,$$

即 K 的每个理想都是主理想．因此，K 是主理想整环．

(证毕)

应注意，这个定理的逆定理不成立．就是说，一个主理想整环不一定是一个欧氏环．对此，1949 年 T．S．Matykin 曾举出过一个例子．

这样，根据以上各节的讨论，如果把全体欧氏环构成的类简记为“欧氏环”，则有以下关系：

欧氏环 主理想整环 惟一分解整环 有单位元整环．

习题 5.4

1．证明：凡域一定是欧氏环．

2．问：有理数域上多项式环 $Q[x]$ 的理想

$$\blacksquare x^2+1, x^5+x^3+1\blacksquare$$

等于哪个主理想？

3. 证明：Gauss 整环 $Z[i]$ 关于映射

$$\phi: \quad a+bi \qquad a^2+b^2$$

作成一个欧氏环．

提示：令 $\alpha\beta^{-1}=s+ti$，$q=a+bi$，其中 $s, t\in Q$，而 a, b 分别是最接近 s, t 的整数

4. 设 R 是一个整环．如果有一个 R^* 到非负整数集的映射 ϕ 满足

1°对 R 中任意元素 a 及 $b\neq 0$，有 $q, r\in R$ 使

$$a=bq+r, \qquad r=0 \text{ 或 } \phi(r)<\phi(b);$$

2°对 R 中任意非零元素 a, b 都有

$$\phi(ab)\geq\phi(a),$$

则称 R 是一个 V 欧氏环．证明：V 欧氏环有单位元，从而是欧氏环．

5. 证明：对欧氏环 R 可定义一个映射使其成为一个 V 欧氏环．

* §5 惟一分解整环的多项式扩张

我们知道，域是一个主理想整环，从而便是一个惟一分解整环(尽管其元素除去零元外全是可逆元即单位)．而数域或域上的多项式环也是惟一分解整环，它是高等代数的重要内容之一．本节要推广这些讨论，即假设 K 是任意一个惟一分解整环，我们将证明 K 上的多项式环 $K[x]$ 也是一个惟一分解整环．

定义 1 如果环 R 是环 S 的一个子环，则称 S 是环 R 的一个 环 张．

设 K 是一个惟一分解整环，则其上的多项式环 $K[x]$ 便是 K 的一个扩环，或称 K 的 项式扩张．

我们知道，K 的单位元就是 $K[x]$ 的单位元，而 K 的单位(可逆元)也就是 $K[x]$ 的全部单位．另外，由 §2 知，K 中任意有限个元素的最大公因子都存在，而且其任二最大公因子都相伴．

定义 2 设 $f(x)\in K[x]$ 如果 $f(x)$的所有系数的最大公因子是一个单位，即所有系数互素，则称 $f(x)$是一个 原多项式 .

设

$$f(x)=a_0+a_1x+\cdots+a_nx^n$$

为 $K[x]$中任一非零多项式，且

$$(a_0,a_1,\cdots,a_n)=d,$$

则令 $a_i=da_i'$， $i=1$， 2， …， n . 于是 a_1'， a_2'， …， a_n'互素，从而

$$f_1(x)=a_0'+a_1'x+\cdots+a_n'x^n$$

是一个本原多项式，而且

$$f(x)=df_1(x)\ .$$

这就是说， K 上任意非零多项式都可表示成 K 中一个非零元素与一个本原多项式相乘 . 而且易知，不同的表示法最多差一个单位因子 .

另外，根据定义，零多项式不是本原多项式；零次多项式是本原的当且仅当它是 K 的一个单位 .

引理 1 (Gauss 引理) 两个本原多项式的乘积仍是一个本原多项式 .

在高等代数中也有这样一个完全相同的引理 . 惟一的区别是，高等代数中所说的多项式是数域上的多项式，而现在的多项式是惟一分解整环上的多项式 . 但就这个引理的证明方法来说，二者是完全一致的，故不再赘述 .

在以下的讨论中，还要用到 K 的分式域 .

令 F 是惟一分解整环 K 的分式域 . 于是 $K[x]$中的每个多项式也是 $F[x]$中的多项式 .

引理 2 $K[x]$中两个本原多项式 $f_1(x)$与 $f_2(x)$在 $K[x]$中相伴的充要条件是，二者在 $F[x]$中相伴 .

证 如果 $f_1(x)$与 $f_2(x)$在 $K[x]$中相伴，则由于 $K[x]$与 K 中的单位一致，而 K 中的单位也是 F 的单位，从而 $f_1(x)$与 f_2

(x)也在 $F[x]$中相伴．

反之，设 $f_1(x)$与 $f_2(x)$在 $F[x]$中相伴，则由于 $F[x]$中的单位就是 F中的全体非零元，故 F中有元素 $\frac{b}{a}\neq 0(a,b\in K)$，使

$$f_1(x)=\frac{b}{a}f_2(x),$$

从而有

$$f(x)=af_1(x)=bf_2(x)\ .$$

但由于 $f_1(x)$与 $f_2(x)$都是本原多项式，则 a与 b在 K中相伴：$b=a\varepsilon$，其中 ε是 K的单位．于是有

$$f_1(x)=\varepsilon f_2(x),$$

即 $f_1(x)$与 $f_2(x)$在 $K[x]$中相伴．

（证毕）

定理 1 $K[x]$中的本原多项式 $f(x)$在 $K[x]$中可约的充要条件是，$f(x)$在 $F[x]$中可约．

证 必要性显然，下证充分性．

设 $f(x)$在 $F[x]$中可约，则在 $F[x]$中有次数大于零的多项式 $f_1(x)$，$f_2(x)$使

$$f(x)=f_1(x)\cdot f_2(x)\ . \tag{1}$$

令

$$f_1(x)=\frac{b_0}{a_0}+\frac{b_1}{a_1}x+\cdots+\frac{b_n}{a_n}x^n\quad(a_i,b_i\in K),$$

两端各乘以 $a=a_0a_1\cdots a_n$，并将右端的结果记为 $g_1(x)$，于是得

$$af_1(x)=g_1(x)\in K[x]\ . \tag{2}$$

同理，有 $b\in K$使

$$bf_2(x)=g_2(x)\in K[x]\ . \tag{3}$$

再令

$$g_i(x)=d_ih_i(x),\quad i=1,2, \tag{4}$$

其中 $h_i(x)$是 $K[x]$中的本原多项式，$d_i\in K$．于是由(1)～(4)式

可得

$$ab f(x) = d_1 d_2 h_1(x) h_2(x) .$$

由于 $f(x)$ 是本原多项式，以及由 Gauss 引理，乘积 $h_1(x) h_2(x)$ 也是本原多项式，从而 $f(x)$ 与 $h_1(x) h_2(x)$ 在 $K[x]$ 中相伴．于是存在单位 $\varepsilon \in K$ 使

$$f(x) = \varepsilon h_1(x) h_2(x),$$

其中 $h_i(x)$ 的次数 $=$ $f_i(x)$ 的次数 > 0．即 $f(x)$ 在 $K[x]$ 中可约．

(证毕)

最后，来证明本节的主要结论．

定理 2 设 K 是惟一分解整环，则其多项式扩张 $K[x]$ 也是惟一分解整环．

证 在 $K[x]$ 中任取 $f(x) \neq 0$，且 $f(x)$ 也不是单位．令

$$f(x) = d f_1(x), \tag{5}$$

其中 $d \in K$，而 $f_1(x)$ 是本原多项式．

若 $f_1(x)$ 不是单位且可约，即有真因子，则令

$$f_1(x) = f_{11}(x) f_{12}(x),$$

其中 $f_{11}(x)$，$f_{12}(x)$ 是 $f_1(x)$ 的真因子．这样，由于 $f_1(x)$ 是本原多项式且不是单位，从而 $f_1(x)$ 必是次数大于零的多项式．于是由此可知，$f_{11}(x)$ 与 $f_{12}(x)$ 都不可能是 K 中的元素，亦即二者都是次数大于零且小于 $f_1(x)$ 的次数的多项式．

然后对 $f_{1i}(x)$ 像上面对待 $f_1(x)$ 那样继续分解，由于 $f(x)$ 次数有限，故总可得到 $K[x]$ 中次数大于零的不可约多项式 $q_1(x)$，$q_2(x)$，$\cdots$，$q_n(x)$ 使

$$f_1(x) = q_1(x) q_2(x) \cdots q_n(x) . \tag{6}$$

再由 $d \in K$，而 K 是惟一分解整环，故可令

$$d = p_1 p_2 \cdots p_m , \tag{7}$$

其中 p_i 是 K 的不可约元，即素元．于是由(5)，(6)，(7)得

$$f(x) = p_1 p_2 \cdots p_m q_1(x) q_2(x) \cdots q_n(x) .$$

若 $f(x)$ 另有分解

$$f(x) = p_1' p_2' \cdots p_s' g_1(x) g_2(x) \cdots g_t(x),$$

其中 p_i'都是 K 的素元，而 $g_j(x)$都是 $K[x]$的次数大于零的不可约多项式．

当然，所有 $q_i(x)$与所有 $g_j(x)$都是本原多项式．从而由 Gauss 引理知，乘积

$$q_1(x) q_2(x) \cdots q_n(x) \quad 与 \quad g_1(x) g_2(x) \cdots g_t(x)$$

也都是本原多项式，并且二者相伴．当然，乘积

$$p_1 p_2 \cdots p_m \quad 与 \quad p_1' p_2' \cdots p_s'$$

也相伴．故存在 K 的单位 ε 使

$$p_1 p_2 \cdots p_m = \varepsilon p_1' p_2' \cdots p_s'.$$

再由于 K 是惟一分解整环，故 $m = s$，且适当交换素元次序，有 p_i 与 p_i' 相伴，$i = 1, 2, \cdots, m$．

最后，由于 $\prod_{i=1}^{n} q_i(x)$ 与 $\prod_{j=1}^{t} g_j(x)$ 在 $K[x]$ 中相伴，故在 K 中存在单位 ε' 使

$$q_1(x) q_2(x) \cdots q_n(x) = \varepsilon' g_1(x) g_2(x) \cdots g_t(x). \qquad (8)$$

但由定理 1 知，$q_i(x)$与 $g_j(x)$也是分式域 F 上的多项式环 $F[x]$中的不可约多项式，而 $F[x]$是惟一分解整环，故由(8)知，$n = t$，且适当交换不可约多项式的次序，有 $q_j(x)$与 $g_j(x)$在 $F[x]$中相伴．从而由引理 2 知，$q_j(x)$与 $g_j(x)$ $(j = 1, 2, \cdots, n)$在 $K[x]$中也相伴．

因此，$f(x)$在 $K[x]$中有惟一分解．再由 $f(x)$的任意性，故知 $K[x]$是惟一分解整环．

(证毕)

由此定理可立即得到

推论 设 K 是惟一分解整环，又 x_1，x_2，$\cdots$，x_n 是 K 上 n 个不相关的未定元，则 $K[x_1, x_2, \cdots, x_n]$也是惟一分解整环．

这样，从一个惟一分解整环出发，我们又可以得到许许多多的惟一分解整环．

例如，由于整数环 Z 是惟一分解整环，从而其上的多项式环 $Z[x]$，更一般地，环 $Z[x_1, x_2, \cdots, x_n]$ 都是惟一分解整环．

习题 5.5

1. 设 K 是惟一分解整环，$0 \neq f(x) \in K[x]$，且

$$f(x) = d_1 f_1(x) = d_2 f_2(x),$$

其中 d_1，$d_2 \in K$，$f_1(x)$ 与 $f_2(x)$ 是本原多项式．证明：d_1 与 d_2 相伴，$f_1(x)$ 与 $f_2(x)$ 也相伴．

2. 设 K 是惟一分解整环．证明：

1) ε 是 K 的单位当且仅当 ε 是 $K[x]$ 的单位；

2) 可约的本原多项式必有次数大于零的多项式为其真因子．

3. 设 K 是一个惟一分解整环，又 $f(x)$，$g(x) \in K[x]$．证明：若乘积 $f(x)g(x)$ 是本原多项式，则 $f(x)$ 与 $g(x)$ 都是本原多项式．

4. 设 F 是惟一分解整环 K 的分式域．如果在 $F[x]$ 中有

$$f(x) = g(x)h(x),$$

但其中 $f(x), g(x) \in K[x]$，而且 $g(x)$ 是本原的，证明：

$$h(x) \in K[x].$$

5. 设 K 是惟一分解整环，又 u，$v \in K$，$u \neq 0$ 且

$$(u, v) = 1,\ f(x) \in K[x].$$

证明：在 K 的商域 F 中，若 $\frac{v}{u}$ 是 $f(x)$ 的根，则

$$u - v \mid f(1),\quad u + v \mid f(-1).$$

6. 设 α 是 Gauss 整环 $Z[i]$ 的一个元素．证明：若

$$|\alpha|^2 = \alpha\bar{\alpha} = p$$

是素数，则 α 是 $Z[i]$ 的不可约元．又问：反之如何？

7. 证明：$x^2 + 1$ 是多项式环 $Z[x]$ 中的不可约元，但商环 $Z[x]/\langle x^2 + 1\rangle$ 不是域．

8. 设 M 是主理想整环 K 的一个非零理想．证明：

$$M \text{ 是 } K \text{ 的极大理想} \qquad M \text{ 是 } K \text{ 的素理想}.$$

9. 设 K 是一个阶大于 1 且有单位元的整环．证明：K 中元素 $a \neq 0$ 是不可约元的充要条件是，$\langle a\rangle$ 在 K 的全体真主理想中是极大的．

10. 设 K 是一个阶大于 1 且有单位元的整环．证明：

K 是域 $\Leftrightarrow$ $K[x]$ 是主理想整环．

11. 证明：实数域 R 上的二元多项式环 $R[x, y]$ 不是主理想整环．

提示：考虑常数项为 0 的全体二元多项式．

12. 设 $Z[i]$ 是 Gauss 整环．证明：

1) 当 $mn \neq 0$ 时，$m+ni$ 是 $Z[i]$ 的素元 $\Leftrightarrow$ m^2+n^2 是素数；

2) 当 $mn=0$ 时，$m+ni$ 是 $Z[i]$ 的素元 $\Leftrightarrow$ $|m+ni|$ 是素数且

$$4 \mid |m+ni| - 3.$$

13. 证明：当 $m=-2, -1, 2, 3$ 时，整环

$$D=\{a+b\sqrt{m} \mid a, b\in Z\}$$

对于 $\varphi(\alpha)=|N(\alpha)|=|a^2-b^2m|$ 作成欧氏环．其中 $\alpha=a+b\sqrt{m}$．

提示：仿 §3 定理 1 证明：

第六章　域■的■扩■张

早在 19 世纪初，伽罗瓦在研究代数方程的著作里就出现了域的概念的萌芽．后来戴德金(J .W .R .Dedekind)和克罗内克(L .Kronecker)在不同背景下也提出了域的概念．系统研究域的理论始于韦伯(H .Weber)，而域的公理系统是迪克森(L .E .Dickson)和亨廷顿(E .V .Huntington)分别于 1903 和 1905 年独立创立的．在韦伯等人的影响下，施泰尼茨(E .Steinitz)对抽象域进行系统研究，于 1910 年发表论文“域的代数理论”，对域论本身以及相关科学的发展产生重大影响．

域是许多数学分支(如代数、代数数论、代数几何等)研究的基础．而有限域则在近代编码、正交试验设计和计算机理论中都有重要应用．

通过理想来研究环，这是研究环的基本方法．但是，由于域只有平凡理想，因此无法通过域的理想来研究域．要研究域，必须采取别的方法，其中最基本的方法就是对域进行扩张．域的扩张起源于数域的扩张．

本章要在上两章的基础上，采用扩张的方法对域作进一步的讨论．主要有单扩域、代数扩域、分裂域和有限域等．这些讨论虽然是初步的，但它也指出了研究域的最基本的方法．

§1　扩域和素域

定义 1　若域 F 是域 E 的一个子域，则称 E 为子域 F 的一

个__域__.

例如，复数域是实数域的扩域，而复数域和实数域又都是有理数域的扩域，等等.

我们知道，任何数域都包含有理数域，即有理数域是最小的数域，它不再含有任何真子域.

定义 2 若域 Δ 不含真子域，则称 Δ 是一个__域__.

这样，有理数域是一个素域. 另外，显然以素数 p 为模的剩余类域 Z_p 也是素域. 下面将证明，在同构意义下这就是全部的素域.

定理 1 设 Δ 是一个素域. 则

1) 当 $\mathrm{char}\Delta=\infty$ 时，$\Delta\cong Q$;

2) 当 $\mathrm{char}\Delta=p$ 时，$\Delta\cong Z_p$，其中 p 是素数.

证 令 e 是 Δ 的单位元，且令

$$Z'=\{ne\mid n\in Z\},$$

则

$$\phi:\quad n\quad ne$$

是整数环 Z 到 Z' 的一个同态满射.

1) 当 $\mathrm{char}\Delta=\infty$ 时，则 φ 是同构映射，从而

$$Z\cong Z'.$$

但同构的环的商域也同构，Z 的商域是有理数域 Q，而由于 Δ 是素域，故 Z' 在 Δ 中的商域就是 Δ 自身，从而 $Q\cong\Delta$，亦即

$$\Delta\cong Q.$$

2) 当 $\mathrm{char}\Delta=p$ 时，则易知，$\mathrm{Ker}\phi=\langle p\rangle$，故

$$Z/\langle p\rangle\cong Z_p\cong Z'.$$

由于 Z_p 是域，故 Z' 是域. 但 Δ 是素域，故 $Z'=\Delta$. 从而此时有

$$\Delta\cong Z_p.$$

(证毕)

这样，在同构意义下，素域只有 Q 以及模 p (素数) 剩余类域

Z_2，Z_3，…，Z_p，…．另外，由上面的证明可知，如果 Δ 是一个素域，e 是 Δ 的单位元，则

$$\Delta = \left\{ \frac{me}{ne} \,\middle|\, m, n \in Z, ne \neq 0 \right\}.$$

推论 1　每个域都包含一个素域且只包含一个素域．

证　设 E 是任意一个域，e 是 E 的单位元，则上面所说的 Δ 显然是包含在 E 中的一个素域．

如果 Δ′也是包含在 E 中的素域，则由于子域和域的单位元是一致的，故 $\Delta' = \Delta$．

*(*证毕*)*

推论 2　设 E 是一个域．则当 $\mathrm{char}E = \infty$ 时，E 包含一个与 Q 同构的素域；当 $\mathrm{char}E = p$ 时，E 包含一个与 Z_p 同构的素域．

证　由定理 1 直接可得．

研究域的基本方法是，从一个给定的域出发，来研究它的各种各样的扩域．

由于任何域都是它所包含的素域的扩域，因此，可以从素域出发来研究扩域．而且如果这样的扩域研究清楚了，也就是弄清楚了所有的域．但实践证明，从素域出发来研究扩域并没有什么特别的优越性．因此，往往的做法是从任意域出发来研究其扩域．

设 F 是任意一个给定的域，E 是 F 的一个扩域，S 是 E 的一个子集，用 $F(S)$ 表示 E 中包含 $F \cup S$ 的一切子域的交，因此它是 E 中包含 F 及 S 的最小子域．我们称其为 加子集 S 于 F 所得到的域．

$F(S)$ 是 E 的子域，但它是 F 的一个扩域．

下面粗略考察一下 $F(S)$ 中的元素是些什么样子．

在 S 中任取有限个元素 α_1，α_2，…，α_n，令

$$f(\alpha_1, \alpha_2, \cdots, \alpha_n)$$

为系数属于 F 的关于 α_1，α_2，…，α_n 的任意一个多项式，它是 F

(S)中一个确定的元素．由于 $F(S)$是一个域，因此，$F(S)$也包含这样两个多项式的商

$$\frac{f_1(\alpha_1,\alpha_2,\cdots,\alpha_n)}{f_2(\alpha_1,\alpha_2,\cdots,\alpha_n)},$$

其中 $f_2(\alpha_1,\alpha_2,\cdots,\alpha_n)\neq 0$．

另一方面，如果让 α_1，α_2，…，α_n 在 S 中任意变动，n 也不固定，那么一切这样的有理分式显然作成一个包含 $F\cup S$ 的子域．因此

$$F(S)=\left\{\frac{f_1(\alpha_1,\alpha_2,\cdots,\alpha_n)}{f_2(\alpha_1,\alpha_2,\cdots,\alpha_n)}\,\middle|\,\alpha_1,\alpha_2,\cdots,\alpha_n\in S,n=1,2,\cdots\right\}.$$

在 E 中适当选择 S 就能使 $E=F(S)$．例如，当取 $S=E$ 时总有 $F(S)=E$．但是，为了得到 E，实际上一般说 S 不必取这么大．

例如，$E=\{a+b\sqrt{2}\mid a,b\in Q\}$，则只需取

$$S=\{\sqrt{2}\}$$

就有 $Q(\sqrt{2})=E$ 了．

现在假定 $E=F(S)$．因为在 S 中任意取定有限个元素 α_1，α_2，…，α_n 后，一切形如

$$\frac{f_1(\alpha_1,\alpha_2,\cdots,\alpha_n)}{f_2(\alpha_1,\alpha_2,\cdots,\alpha_n)}\quad(f_2(\alpha_1,\alpha_2,\cdots,\alpha_n)\neq 0)$$

的元素也作成一个域(注意:这里的 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 是固定的)．如果令 $S_1=\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$，则这个域可简记为

$$F(S_1)=F(\alpha_1,\alpha_2,\cdots,\alpha_n).$$

它是添加有限个元素于 F 所得到的扩域，而 $E=F(S)$就是一切这种子域的并集．这一事实说明，研究 $F(S)$可归结为研究添加有限个元素于 F 所得到的域 $F(\alpha_1,\alpha_2,\cdots,\alpha_n)$．

定理2 令 E 是域 F 的一个扩域，而 S_1，S_2 是 E 的两个子集．则

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

证 $F(S_1)(S_2)$是包含 $F(S_1)$与 S_2 的域，于是也是包含 F，S_1，S_2 的域，从而是包含 F 与 $S_1 \cup S_2$的域．但是由于 $F(S_1 \cup S_2)$是包含 F 与 $S_1 \cup S_2$ 的最小域，故

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

另一方面，域 $F(S_1 \cup S_2)$包含 F 与 $S_1 \cup S_2$，从而包含 F，S_1，S_2，也包含 $F(S_1)$与 S_2．但 $F(S_1)(S_2)$是包含 $F(S_1)$与 S_2 的最小子域，故又有

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

因此，$F(S_1)(S_2) = F(S_1 \cup S_2)$．

同理有 $F(S_2)(S_1) = F(S_1 \cup S_2)$．故有

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

（证毕）

根据这个定理，对于域 $F(\alpha_1, \alpha_2, \cdots, \alpha_n)$有

$$F(\alpha_1, \alpha_2, \cdots, \alpha_n) = F(\alpha_1)(\alpha_2)\cdots(\alpha_n).$$

这就是说，讨论扩域 $F(\alpha_1, \alpha_2, \cdots, \alpha_n)$又可归结为讨论向 F 添加一个元素而得到的扩域．这种扩域很重要，将在下节作专门的讨论．

习题 6.1

1. 设 E 是域 F 的一个扩域，而 M 与 N 是扩域 E 的两个子集．证明：$F(M \cup N) = F(M)$当且仅当 $N \quad F(M)$．

2. 设 E 是特征为素数 p 的一个域．证明：

$$\Delta = \{0, e, 2e, \cdots, (p-1)e\}$$

作成 E 的一个子域，且为 E 中的素域．

3. 设 a 是一个正有理数，Q 是有理数域．证明：

$$Q(\sqrt{a}, i) = Q(\sqrt{a} + i).$$

4. 设 Q 是有理数域．证明：

$$Q\left(\frac{1}{5}, \sqrt{2} + \sqrt{3}, \sqrt{7} \quad \sqrt{3}\right) = Q(\sqrt{2}, \sqrt{3}).$$

5. 证明：$Q(\sqrt{2}+\sqrt{3})$是由一切形如

$$a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$$

的数作成的数域，其中 $a, b, c, d\in Q$.

§2 单 扩 域

定义 1 设 E 是域 F 的一个扩域，$\alpha\in E$. 如果存在 F 上非零多项式 $f(x)$ 使

$$f(\alpha)=0,$$

则称 α 为 F 上的一个代数元. 否则，称 α 为 F 上的一个超越元.

例如，$\sqrt{2}$ 是有理数域 Q 上的一个代数元，而圆周率 π 则是 Q 上的一个超越元. 但是应注意，π 是实数域上的一个代数元.

我们平常所说的代数数，就是指的复数范围内有理数域上的代数元.

定义 2 扩域 $F(\alpha)$ 叫做域 F 的单扩域(单扩张). 特别，当 α 为 F 上的代数元时，称 $F(\alpha)$ 为 F 的代数扩域(张)；当 α 为 F 上的超越元时，称 $F(\alpha)$ 为 F 的超越扩域(张)

例如，$Q(\sqrt{2})$ 是有理数域 Q 的一个单代数扩域，而 $Q(\pi)$ 则是 Q 的一个单超越扩域.

定义 3 设 α 是域 F 上的一个代数元，则 F 上首系数为 1 且有根 α、次数最低的多项式是存在的，称为 α 在 F 上的小多式.

若 α 的最小多项式的次数是 n，则称 α 是 F 上的一个 n 次代元.

例如，$\sqrt{3}$ 在 Q 上的最小多项式是 x^2-3，因此，$\sqrt{3}$ 是 Q 上的一个 2 次代数元.

一般的，易知 $\sqrt[n]{3}$ 在 Q 上的最小多项式是 x^n-3，而 $\sqrt[n]{3}$ 是 Q 上的一个 n 次代数元. 更一般的，对任意素数 p，$\sqrt[n]{p}$ 是 Q 上的

一个 n 次代数元．

下面进一步给出最小多项式的性质．

定理 1 域 F 上的代数元 α 在 F 上的最小多项式是惟一的．若 α 在 F 上的最小多项式是 $p(x)$，则 $p(x)$ 在 F 上不可约．又若 $f(x)$ 为 F 上的一个多项式且 $f(\alpha)=0$，则 $p(x) \mid f(x)$．

证 1) 设 $p_1(x)$ 与 $p_2(x)$ 都是 α 在 F 上的最小多项式，则若

$$g(x)=p_1(x)-p_2(x)\neq 0,$$

其次数将低于 $p_1(x)$ 的次数，且有 $g(\alpha)=0$，这是不可能的．故 $g(x)=0$，从而

$$p_1(x)=p_2(x),$$

即 α 的最小多项式是惟一的．

2) 若 α 在 F 上的最小多项式 $p(x)$ 在 F 上可约，且

$$p(x)=g_1(x)g_2(x),$$

其中 $g_i(x)\in F[x]$，且 $g_i(x)$ 次数 $<p(x)$ 次数．令 $x=\alpha$ 代入上式，得

$$p(\alpha)=g_1(\alpha)g_2(\alpha)=0.$$

但域无零因子，故 $g_1(\alpha)$ 与 $g_2(\alpha)$ 至少有一个等于零，这与 $p(x)$ 是 α 的最小多项式矛盾．因此，$p(x)$ 在 F 上不可约．

3) 令

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

其中 $r(x)=0$ 或 $r(x)$ 次数 $<p(x)$ 次数，则有

$$f(\alpha)=p(\alpha)q(\alpha)+r(\alpha).$$

但 $f(\alpha)=0$，$p(\alpha)=0$，从而 $r(\alpha)=0$．这只有 $r(x)=0$，否则将与 $p(x)$ 为 α 在 F 上的最小多项式矛盾．因此，$p(x) \mid f(x)$．

(证毕)

下面讨论单扩域的构造．

定理 2 设 $F[x]$ 为域 F 上未定元 x 的多项式环，$F(x)$ 为其

分式域．则

1) 当 α 为 F 上的超越元时，$F(\alpha)\cong F(x)$；

2) 当 α 为 F 上的代数元时，

$$F(\alpha)\cong F[x]/\blacksquare p(x)\blacksquare,$$

其中 $p(x)$ 为 α 在 F 上的最小多项式．

证 令

$$F[\alpha]=\{f(\alpha)\mid f(x)\in F[x]\},$$

则 $F[\alpha]$ 是域 $F(\alpha)$ 的一个子环．又易知

$$\phi:\quad f(x)\quad f(\alpha)$$

是 $F[x]$ 到 $F[\alpha]$ 的一个同态满射．

1) 当 α 为 F 上的超越元时，φ是同构映射，于是

$$F[x]\cong F[\alpha]\ .$$

但是，同构的环其分式域也同构，$F[x]$ 的分式域是 $F(x)$，又易知 $F[\alpha]$ 的分式域是 $F(\alpha)$，因此

$$F(\alpha)\cong F(x)\ .$$

2) 当 α 为 F 上的代数元时，设 $p(x)$ 为 α 在 F 上的最小多项式，则易知

$$\mathrm{Ker}\phi=\blacksquare p(x)\blacksquare,$$

于是由环同态基本定理，得

$$F[x]/\blacksquare p(x)\blacksquare\cong F[\alpha]\ .$$

由于 $p(x)$ 在域 F 上不可约，$\blacksquare p(x)\blacksquare$ 是 $F[x]$ 的极大理想，故 $F[x]/\blacksquare p(x)\blacksquare$ 为域，从而此时 $F[\alpha]$ 也是域．但 $F(\alpha)$ 是包含 F 及 α 的最小域，故 $F[\alpha]=F(\alpha)$．因此，有

$$F(\alpha)=F[\alpha]\cong F[x]/\blacksquare p(x)\blacksquare\ .$$

(证毕)

由此定理知，当 α 是域 F 上的代数元时，有 $F(\alpha)=F[\alpha]$，即每个关于 α 的有理分式都与 α 的一个多项式(系数属于 F)相等．

进一步更有以下的

定理 3 若 α 是域 F 上的 n 次代数元，则 $F(\alpha)$ 中的每个元素都可惟一地由 $1, \alpha, \cdots, \alpha^{n-1}$ 线性表出，即可惟一地表示成

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}, \quad a_i \in F.$$

这也就是说，F 的单代数扩域 $F(\alpha)$ 也是 F 上的一个 n 维空间，而且 $1, \alpha, \cdots, \alpha^{n-1}$ 是它的一个基.

证 设 $p(x)$ 是 α 在 F 上的最小多项式，次数为 n. 任取 $\beta \in F(\alpha)$，故可令

$$\beta = f(\alpha), \quad \text{其中 } f(x) \in F[x].$$

设

$$f(x) = p(x)q(x) + r(x), \quad q(x), r(x) \in F[x].$$

$$r(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1},$$

用 $x = \alpha$ 代入上式，由于 $p(\alpha) = 0$，故可得

$$f(\alpha) = r(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1},$$

即 $F(\alpha)$ 中每个元素都可用 $1, \alpha, \cdots, \alpha^{n-1}$ 线性表示.

其次，若有

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1},$$

其中 $a_i, b_i \in F$，则有

$$(a_0 - b_0) + (a_1 - b_1)\alpha + \cdots + (a_{n-1} - b_{n-1})\alpha^{n-1} = 0,$$

即 α 是 F 上多项式

$$g(x) = (a_0 - b_0) + (a_1 - b_1)x + \cdots + (a_{n-1} - b_{n-1})x^{n-1}$$

的根. 但由于 α 是 F 上的 n 次代数元，故只有 $g(x) = 0$，即

$$a_i = b_i, \quad i = 0, 1, 2, \cdots, n-1,$$

亦即 $F(\alpha)$ 中每个元素的表示法是惟一的.

(证毕)

给定域 F 后，F 上的单超越扩域的存在是显然的，因为当 x 为 F 上的未定元时，$F(x)$ 就是 F 的一个单超越扩域. 下面证明，单代数扩域也是存在的.

定理 4 设 F 是一个域，$p(x)$ 是 F 上任意一个给定的首系

数为 1 的不可约多项式，则存在 F 上单代数扩域 $F(\alpha)$，其中 α 在 F 上的最小多项式是 $p(x)$.

证 上面定理 3 的证明，可以启发我们如何来找出这样的代数元 α.

由于 $p(x)$ 在 F 上不可约，■ $p(x)$ ■是 $F[x]$ 的极大理想，故 $F[x]/$ ■ $p(x)$ ■是域 . 又易知

$$\varphi: \quad f(x) \quad \overline{f(x)} = f(x) + \blacksquare p(x) \blacksquare$$

是 $F[x]$ 到域 $F[x]/$ ■ $p(x)$ ■的一个同态满射，且

$$\mathrm{Ker}\varphi = \blacksquare p(x) \blacksquare .$$

由于 F $F[x]$，则 $\overline{F} = \varphi(F)$ $F[x]/$ ■ $p(x)$ ■ . 在 F 中任取 a, b . 当 $a \neq b$ 时，由于

$$p(x) \nmid a - b, \quad \overline{a - b} \neq \overline{0},$$

故 $\overline{a} \neq \overline{b}$. 即在 φ 之下

$$F \to \overline{F} = \{\overline{a} \mid a \in F\} .$$

这样，根据挖补定理，在域 $F[x]/$ ■ $p(x)$ ■中把 $\overline{F}$ 的元素 $\overline{a}$ 都换成 F 中对应的元素 a，设这样所得到的域为 K，并把 K 中元素 $\overline{x} = x +$ ■ $p(x)$ ■记为 α，于是由于在 φ 之下

$$p(x) \quad \overline{p(x)} = p(\overline{x}) = p(\alpha) = 0,$$

即 α 是 F 上不可约多项式 $p(x)$ 的根，故 $p(x)$ 是 α 在 F 上的最小多项式 . 而 K 为包含 F 与 α 的一个扩域，从而存在单代数扩域 $F(\alpha)$.

(证毕)

通过本节的讨论可知，对于单扩域的构造我们是了解得比较清楚的 .

习题 6.2

1. 设 α 是域 F 中的任一元素 . 证明：α 是域 F 上的代数元，且

$$F(\alpha) = F .$$

2. 设 $p(x)$ 为域 F 上首系数为 1 的多项式，且有根 α. 证明：若 $p(x)$

在 F 上不可约，则 $p(x)$是 α在 F 上的最小多项式．

3. 求 $\sqrt{2}+\sqrt{3}$在有理数域 Q 上的最小多项式，并证明：

$$Q(\sqrt{2},\sqrt{3})=Q(\sqrt{2}+\sqrt{3}).$$

4. 设 $F(\alpha)$与 $F(\beta)$是域 F 上两个单代数扩域，并且 α与 β在 F 上有相同的最小多项式，证明：$F(\alpha)\cong F(\beta)$．又问：反之如何？

5. 问：复数 i 及$\frac{2i+1}{i-1}$在 Q 上的最小多项式各为何？又单扩域 $F(i)$与 $F\left(\frac{2i+1}{i-1}\right)$是否同构？

6. 设 $p(x)$是域 F 上的 n 次不可约多项式．证明：域 $F[x]/(p(x))$中的每一个元素都可惟一地表示成

$$a_0+a_1x+\cdots+a_{n-1}x^{n-1}+(p(x)),\qquad a_i\in F.$$

§3 代■数■扩■域

由上一节看到，单代数扩域同单超越扩域的结构是很不相同的．一般来说，设 E 是域 F 的一个扩域，则 E 中的元素有些可能是 F 上的代数元，而另一些则可能是 F 上的超越元．

例如，实数域是有理数域 Q 的一个扩域，实的代数数都是 Q 上的代数元，其余的实数，例如 π以及 π与任何非零有理数的乘积，等等，则都是 Q 上的超越元．

定义 1 设 E 是域 F 的一个扩域．如果 E 中每个元素都是 F 上的代数元，则称 E 是 F 的一个代数扩域(张)．否则，称 E 是 F 的一个 越扩域(张)

F 中的元素当然都是 F 上的代数元．如果 E 是 F 的超越扩域，又 E 中除 F 的元素外，都是 F 上的超越元，则称 E 是 F 的一个 超越扩域(张)

例如，实数域是有理数域的超越扩域，但不是有理数域的纯超越扩域；又易知域 F 上关于未定元 x 的有理分式域 $F(x)$是 F 的一个纯超越扩域．

本节主要讨论代数扩域.

我们要问: 当集合 S 中的元素都是 F 上的代数元时, $F(S)$ 中的元素是否都是 F 上的代数元? 也就是说, $F(S)$ 是否为 F 的代数扩域?

这个看起来似乎正确的结论, 实际上并不明显. 这是因为, 域 $F(S)$ 除了包含 F 及 S 的全部元素外, 还要包含由 F 及 S 中的元素通过加、减、乘、除所得到的一切元素. 这就涉及到 F 上代数元的和、差、积、商是否仍为 F 上代数元的问题. 但是, 这个问题虽然是正确的, 然而却并不明显, 因而是需要证明的.

为了讨论这些问题, 我们先介绍扩域次数的概念.

设 E 是域 F 的一个扩域, 则对 E 中加法与乘法来讲, E 作成 F 上的一个向量空间. 于是 E 在 F 上的维数可能有限, 也可能无限.

定义 2 设 E 是域 F 的一个扩域, 则 E 作为 F 上向量空间的维数, 叫做 E 在 F 上的__数__, 记为 $(E:F)$.

当 $(E:F)$ 有限时, 称 E 为 F 的__限次扩域__; 否则称 E 为 F 的__限次扩域__.

例如, 当 α 是域 F 上的 n 次代数元时, 则由上节定理 3 知, $E=F(\alpha)$ 是 F 的 n 次扩域. 特别, 复数域是实数域上的 2 次扩域, $Q(\sqrt[3]{2})$ 是有理数域 Q 上的 3 次扩域, 而 $Q(\pi)$ 则是 Q 的一个无限次扩域. 从而实数域是有理数域的一个无限次扩域.

下面是关于扩域的次数定理.

定理 1 令 E 是域 K 的扩域, K 又是域 F 的扩域, 则

$$(E:F)=(E:K)(K:F).$$

证 先设 $(K:F)=m$, $(E:K)=n$, 而

$$\alpha_1,\alpha_2,\cdots,\alpha_m \text{ 与 } \beta_1,\beta_2,\cdots,\beta_n$$

分别为 K 在 F 上的一基和 E 在 K 上的一基. 下面证明, E 中的 mn 个元素

$$\alpha_i \blacksquare \beta_j,\quad i=1,\ \cdots,\ m;\quad j=1,\ \cdots,\ n \tag{1}$$

是 E 在 F 上的一基.

首先，在 E 中任取一个元素 α，令

$$\alpha = k_1\beta + k_2\beta + \cdots + k_n\beta_n, \tag{2}$$

其中 $k_j \in K$，$j=1,\ \cdots,\ n$. 再令

$$k_j = a_{1j}\alpha_1 + a_{2j}\alpha_2 + \cdots + a_{mj}\alpha_m, \tag{3}$$

其中 $a_{ij} \in F$. 将(3)代入(2)，即得

$$\alpha = \sum_{j=1}^{n}\sum_{i=1}^{m} a_{ij}\alpha_i\beta_j .$$

这就是说，α 在 F 上可由(1)中 mn 个元素线性表示.

其次，设有 $a_{ij} \in F$ 使

$$\sum_{j=1}^{n}\sum_{i=1}^{m} a_{ij}\alpha_i\beta_j = 0,$$

即

$$\sum_{j=1}^{n}\left(\sum_{i=1}^{m} a_{ij}\alpha_i\right)\beta_j = 0,$$

但是，$\sum_{i=1}^{m} a_{ij}\alpha_i \in K$，而 β_1，β_2，$\cdots$，β_n 在 K 上线性无关，故

$$\sum_{i=1}^{m} a_{ij}\alpha_i = 0,\quad j=1,\ \cdots,\ n.$$

又 α_1，α_2，$\cdots$，α_m 在 F 上线性无关，故

$$a_{ij} = 0,\quad i=1,\ \cdots,\ m;\quad j=1,\ \cdots,\ n.$$

从而(1)中 mn 个元素在 F 上线性无关. 因此，它是 E 在 F 上的一基，从而 $(E:F) = mn$，即

$$(E:F) = (E:K)(K:F).$$

由上面的证明同时易知，$(E:F)$ 无限当且仅当 $(E:K)$ 与 $(K:F)$ 中至少有一个无限，因此可认为上式仍成立.

(证毕)

用数学归纳法可进一步证明

推论 1 设 F_m，F_{m-1}，…，F_2，F_1 都是域，且每个都是前一个的子域，则

$$(F_m : F_1) = (F_m : F_{m-1})(F_{m-1} : F_{m-2})\cdots(F_2 : F_1).$$

例如，由于 $Q \subset Q(2) \subset Q(2,3)$，从而有

$$(Q(2,3) : Q) = (Q(2,3) : Q(2)) \cdot (Q(2) : Q),$$

但易知

$$(Q(2,3) : Q(2)) = (Q(2) : Q) = 2,$$

故 $(Q(2,3) : Q) = 4$.

关于有限次扩域，有下面非常重要的基本事实.

定理 2 有限次扩域必是代数扩域.

证 设 E 是 F 的一个 n 次扩域. 任取 $\alpha \in E$，由于 $(E : F) = n$，故 E 中 $n+1$ 个元素

$$1, \alpha, \alpha^2, \cdots, \alpha^n$$

在 F 上必线性相关. 从而在 F 中存在不全为零的元素 a_0，a_1，…，a_n 使

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0,$$

即 α 是 F 上非零多项式

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

的根，故 α 是 F 上的代数元，从而 E 是 F 的代数扩域.

（证毕）

根据这个定理，由于单代数扩域是有限次扩域，从而为代数扩域. 更一般地，还有

推论 2 若 α_1，α_2，…，α_n 都是域 F 上的代数元，则扩域 $F(\alpha_1, \alpha_2, \cdots, \alpha_n)$ 是 F 的有限次扩域，从而为代数扩域.

证 首先指出，若 α 是域 F 上的代数元，则 α 当然是 F 的任何扩域上的代数元.

现以 $n=2$ 为例来证明本推论.

因为

$$F \quad F(\alpha) \quad F(\alpha)(\alpha),$$

而 α，α 是 F 上的代数元，故 α 也是 $F(\alpha)$ 上的代数元．于是 $F(\alpha)$是 F 的有限次扩域，而

$$F(\alpha)(\alpha) = F(\alpha, \alpha)$$

又是 $F(\alpha)$上的有限次扩域．因此由次数定理知，$F(\alpha, \alpha)$是 F 的有限次扩域．再由定理 2 知，$F(\alpha, \alpha)$是域 F 的代数扩域．

对 n用数学归纳法可证明本推论．

(证毕)

当 α，α，…，α 为 F 上的代数元时，$F(\alpha, \alpha, \cdots, \alpha)$是 F 的有限次扩域．反之可以证明，F 的有限次扩域就是这种样子．就是说，如果 E 是 F 的有限次扩域，则 E 必是添加有限个代数元于 F 而得到的扩域．

事实上，设 $F \quad E$ 且 $(E : F) = n$．令 α，α，…，α 为 E 在 F 上的一基，则 α，α，…，α 当然都是 F 上的代数元，且易知有

$$E = F(\alpha, \alpha, \cdots, \alpha).$$

推论 3 域 F 上代数元的和、差、积、商均仍为 F 上的代数元．

证 设 α, β为 F 上的任二代数元，由推论 2 知，$F(\alpha, \beta)$为 F 的代数扩域，从而其中每个元素都是 F 上的代数元．但是，α 与 β的和、差、积、商都是 $F(\alpha, \beta)$中的元素，从而它们都是 F 上的代数元．

(证毕)

由这个推论所得到的一个特殊情况是，代数数的和、差、积、商仍为代数数．因此，在复数域内，所有代数数作成一个数域．这是一个重要的数域．数学的一个重要分支——代数数论就是在这个数域的范围内来讨论的．

推论 2 指出，添加有限个代数元于 F 所得到的扩域是有限次扩域，从而为代数扩域．现在进一步问：添加无限个代数元于

F 所得的扩域如何呢？

定理 3 设 E 是域 F 的一个扩域，S 是 E 的一个非空子集．如果 S 中的每个元素都是 F 上的代数元，则 $F(S)$ 是域 F 的代数扩域．

证 任取 $\alpha\in F(S)$，令

$$\alpha=\frac{f_1(\alpha_1,\alpha_2,\cdots,\alpha_n)}{f_2(\alpha_1,\alpha_2,\cdots,\alpha_n)},$$

其中 α_1，α_2，$\cdots$，$\alpha_n\in S$，f_1，f_2 的系数属于 F．则

$$\alpha\in F(\alpha_1,\alpha_2,\cdots,\alpha_n)\ .$$

由于 α_1，α_2，$\cdots$，α_n 都是域 F 上的代数元，故由推论 2 可知，$F(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 是 F 的代数扩域，从而 α 是 F 上的代数元．因此，$F(S)$ 是 F 的代数扩域．

(证毕)

这个定理中的 S 可以是有限集，也可以是无限集．当 S 是有限集时，即推论 2，此时 $F(S)$ 是 F 上的有限次扩域，当然也是代数扩域．但应注意，当 S 为无限集时，只能保证 $F(S)$ 是 F 的代数扩域，却不能保证是 F 的有限次扩域．

例如，令

$$S=\{\sqrt{2},\sqrt[3]{2},\sqrt[4]{2},\cdots\},$$

则由于 S 中每个元素都是有理数域 Q 上的代数元，故由定理 3 知，$Q(S)$ 是有理数域 Q 的代数扩域．但它却不是 Q 上的有限次扩域．

事实上，如果 $(Q(S)\ :\ Q)=n$，则由于 $\sqrt[n+1]{2}$ 在 Q 上的最小多项式是 $x^{n+1}-2$，故

$$(Q(\sqrt[n+1]{2})\ :\ Q)=n+1,$$

这显然与 $(Q(S)\ :\ Q)=n$ 矛盾．因此，$Q(S)$ 是 Q 的一个无限次扩域．

这就是说，代数扩域不一定是有限次扩域，即定理 2 的逆定

理不成立．

最后，再证明代数扩域的一个重要性质．

定理 4 设 F，K 是域 E 的两个子域且 $F \subset K$．若 E 是 K 的代数扩域，K 是 F 的代数扩域，则 E 是 F 的代数扩域．

证 任取 $\alpha \in E$，由于 E 是 K 的代数扩域，故有

$$0 \neq f(x) = k_0 + k_1 x + \cdots + k_m x^m \in K[x], \quad k_i \in K,$$

使 $f(\alpha) = 0$．但 K 又是 F 上的代数扩域，故 k_0，k_1，$\cdots$，k_m 是 F 上的代数元，于是

$$K' = F(k_0, k_1, \cdots, k_m)$$

是 F 上的有限次扩域，而 $K'(\alpha)$ 是 K' 上的有限次扩域，由于

$$F \subset K' \subset K'(\alpha),$$

故由次数定理知，$K'(\alpha)$ 是 F 的有限次扩域．从而为 F 的代数扩域，α 是 F 上的代数元，E 是 F 的代数扩域．

(证毕)

推论 4 设 E 是域 F 的超越扩域，则在 E 中存在子域 K 满足

$$F \subset K \subset E,$$

其中 K 是 F 的代数扩域，而 E 是 K 的纯超越扩域．

证 令 K 为 E 中 F 上的全体代数元作成的集合，由推论 3 知，K 是 E 的子域且为 F 的代数扩域．但由于 E 是 F 的超越扩域，故

$$F \subset K \subset E.$$

下面进一步证明 E 是 K 的纯超越扩域．

设 $\alpha \in E$，若 α 为 K 上代数元，则 $K(\alpha)$ 是 K 的代数扩域．但 K 又是 F 的代数扩域，故 $K(\alpha)$ 是 F 的代数扩域，α 是 F 上的代数元，从而 $\alpha \in K$．即 E 中只有 K 内的元素才是 K 上的代数元，因此 E 是 K 的纯超越扩域．

(证毕)

根据这个推论，对扩域的讨论可转化为对代数扩域和纯超越

扩域的讨论．

习题 6.3

1. 证明：1) 复数域是实数域的代数扩域；

2) 实数域是有理数域的超越扩域，但不是纯超越扩域．

2. 证明：域 F 上未定元 x 的有理分式域 $F(x)$ 是 F 的一个纯超越扩域．

3. 设 p 是一个素数．证明：

$$Q(\sqrt{p}, \sqrt[3]{p}, \sqrt[4]{p}, \cdots)$$

是有理数域 Q 上的一个无限次代数扩域．

提示：利用反证法．

4. 求有理数域 Q 的扩域 $Q(\sqrt[3]{2}+\sqrt[3]{4})$ 在 Q 上的次数．

提示：令 $\alpha=\sqrt[3]{2}$，则 $Q \quad Q(\alpha+\alpha^2) \quad Q(\alpha)$．

5. 不利用本节结论，直接证明代数数的和仍是代数数．

§4 多项式的分裂域

高等代数中的代数基本定理是说，任何复系数的 n 次多项式在复数域内都有 n 个根．亦即每个复系数的 n 次多项式在复数域内都可以分解成一次因子的乘积．

对一般域 E 来说，如果 E 上每个多项式都能分解成 E 上一次多项式的乘积，则称这样的 E 为<u>代数闭域</u>．

这样，复数域就是一个代数闭域．代数闭域不再有真正的代数扩域．

事实上，设 E 是一个代数闭域，而 α 是 E 上的任意一个代数元，则由于 α 在 E 上的最小多项式在 E 上不可约，又 E 上只有一次多项式不可约，故 α 在 E 上的最小多项式只能是 $x-a$，其中 $a\in E$．这样，便有

$$\alpha - a = 0, \qquad \alpha = a \in E .$$

我们不打算讨论代数闭域，但要讨论某一特定多项式在其中

可完全分解(即分解为一次因子相乘)的域.

定义1　设 E 是域 F 的一个扩域，$f(x)$ 是 F 上一个次数大于零的多项式. 如果 $f(x)$ 在 E 中可完全分解，而在任何包含 F 但比 E 小的子域上不能完全分解，则称 E 是 $f(x)$ 在 F 上的一个分裂域.

这就是说，E 是包含 F 且 $f(x)$ 能在其中完全分解的最小域.

例1　$Q(\sqrt{2})$ 是多项式 x^2-2 在有理数域 Q 上的一个分裂域.

但是，x^2-2 在实数域上的分裂域显然就是实数域本身.

定理1　令 E 是域 F 上多项式 $f(x)$ 的一个分裂域，且

$$f(x)=a_0(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n),$$

其中 $a_0\in F$，$\alpha_i\in E$. 则 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$，即 $f(x)$ 在 F 上的分裂域就是把 $f(x)$ 的全部根添加于 F 所得到的扩域. 因此，$f(x)$ 在 F 上的分裂域也称为 $f(x)$ 在 F 上的__域__.

证　因为 $F(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 是域，且

$$F\quad F(\alpha_1,\alpha_2,\cdots,\alpha_n)\quad E,$$

而 $f(x)$ 在 $F(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 中可完全分解，E 又是 $f(x)$ 在 F 上的分裂域，故只有

$$E=F(\alpha_1,\alpha_2,\cdots,\alpha_n).$$

(证毕)

由此定理可知，$f(x)$ 在 F 上的分裂域是 F 的一个有限次扩域，从而是 F 的一个代数扩域.

例2　求 $f(x)=x^3-1$ 在 Q 上的分裂域.

解　因为

$$f(x)=(x-1)\left(x-\frac{-1+\sqrt{3}i}{2}\right)\left(x-\frac{-1-\sqrt{3}i}{2}\right),$$

故由定理1知，$f(x)$ 在 Q 上的分裂域为

$$Q\left(1,\frac{-1+\sqrt{3}i}{2},\frac{-1-\sqrt{3}i}{2}\right)=Q(\sqrt{3}i),$$

这就是由一切复数 $a+b\sqrt{3}i(a,b\in Q)$作成的数域.

例 3 求 $f(x)=x^3-1$ 在实数域 R 上的分裂域.

解 因为

$$R\left(1,\frac{-1+\sqrt{3}i}{2},\frac{-1-\sqrt{3}i}{2}\right)=R(i)$$

是复数域，故 x^3-1 在实数域上的分裂域是复数域.

下面反转来讨论分裂域的存在问题.

定理 2 设 $f(x)$是域 F 上一个 $n(n>0)$次多项式，则 $f(x)$在 F 上的分裂域存在.

证 对 $f(x)$的次数 n 用归纳法.

当 $n=1$ 时，显然 F 本身就是 $f(x)$在 F 上的分裂域.

假定对 $n-1$ 次的多项式定理成立，下证 $f(x)$是 n 次时定理成立.

任取 $f(x)$的一个首系数为 1 且在 F 上不可约的因式 $p(x)$，由单扩域存在定理，有单扩域 $F(\alpha)$存在，其中 α 在 F 上的最小多项式是 $p(x)$.

在域 $F(\alpha)$上，$f(x)$至少可分解成

$$f(x)=(x-\alpha_1)f_1(x),$$

其中 $f_1(x)$是域 $F(\alpha)$上的 $n-1$ 次多项式. 于是由归纳假设，$f_1(x)$在 $F(\alpha)$上有分裂域存在，设为

$$F(\alpha)(\alpha_1,\cdots,\alpha_n),$$

其中 α_1，…，α_n 为 $f_1(x)$的根. 从而 α，α_1，…，α_n 就是 $f(x)$的所有根，而 $F(\alpha,\alpha_1,\cdots,\alpha_n)$就是 $f(x)$在 F 上的分裂域.

(证毕)

给定 $f(x)$后，$f(x)$在 F 上的分裂域不仅是存在的，而且下面将证明，在同构意义下也是惟一的. 但应注意，却可能是不同的.

例如，复数域 $C=\{a+b\mathrm{i}\mid a,b\in F\}$是 x^2+1 在实数域 F 上的一个分裂域，而

珟珻 $= \{(a, b) \mid a, b \in F\}$

也是 $x^2 + 1$ 在实数域 F 上的一个分裂域，其中

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

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

这是由于在实数域的基础上建立复数的方法不同而产生了不同的分裂域．但是我们知道，C 与珟珻是同构的．

下面要一般地讨论这个问题．

定义 2 设 F 是域 E 的子域，$\bar{F}$ 是域珟珻的子域，且 σ 是 F 与 $\bar{F}$ 的一个同构映射．若 E 与珟珻的同构映射 φ 能保持 σ 不动，即对 F 中任何元素 a 都有

$$\varphi(a) = \sigma(a),$$

则称 φ 是 σ 的一个__张__．

如果 σ 是域 F 与 $\bar{F}$ 的同构映射，$a \in F$ 在 σ 之下的象记为珟珻 $= \sigma(a)$，则当

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$$

时，记

$$\bar{f}(x) = 珟珻_0 + 珟珻_1 x + \cdots + 珟珻_n x^n \in \bar{F}[x].$$

引理 1 设 σ 是域 F 与 $\bar{F}$ 的一个同构映射，则

1) $g(x) \mid f(x)$ 当且仅当珟珻$(x) \mid \bar{f}(x)$；

2) $p(x)$ 在 F 上不可约当且仅当珟珻(x) 在 $\bar{F}$ 上不可约．

证 由于 F 珟珻 $\bar{F}$，故易知

$$\varphi: \quad f(x) \quad \bar{f}(x)$$

是环 $F[x]$ 与环 $\bar{F}[x]$ 的一个同构映射．于是对 F 上多项式若有 $g(x) \mid f(x)$，令

$$f(x) = g(x)q(x), \quad q(x) \in F[x],$$

则有

$$\bar{f}(x) = 珟珻(x)珟珻(x), \quad 珟珻(x) \in \bar{F}[x],$$

反之亦成立．

由此随得，$p(x)$ 在 F 上不可约当且仅当珟珻(x) 在 $\bar{F}$ 上不可约．

(证毕)

引理 2 设 σ 是域 F 与域 $\overline{F}$ 的同构映射，$F(\alpha)$ 是 F 的单代数扩域，$p(x)$ 是 α 在 F 上的最小多项式，$\overline{F}(\overline{\alpha})$ 是 $\overline{F}$ 的单代数扩域，$\overline{p}(x)$ 是 $\overline{\alpha}$ 在 $\overline{F}$ 上的最小多项式．则

$$F(\alpha) \cong \overline{F}(\overline{\alpha}),$$

并且此同构是 σ 的扩张，它把 α 变为 $\overline{\alpha}$.

证 设 $p(x)$ 与 $\overline{p}(x)$ 的次数都是 n，则单扩域 $F(\alpha)$ 与 $\overline{F}(\overline{\alpha})$ 中的元素都可以惟一地表示成

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}, \qquad a_i \in F,$$

$$\overline{\alpha}_0 + \overline{\alpha}_1\overline{\alpha} + \cdots + \overline{\alpha}_{n-1}\overline{\alpha}^{n-1}, \qquad \overline{\alpha}_i \in \overline{F},$$

令

$$\varphi: \sum_{i=0}^{n-1} a_i\alpha^i \longrightarrow \sum_{i=0}^{n-1} \overline{\alpha}_i\overline{\alpha}^i,$$

则易知 φ 是 $\overline{F}(\alpha)$ 与 $\overline{F}(\overline{\alpha})$ 的一个同构映射，且在 φ 之下保持 σ，即 φ 是 σ 的扩张；又显然 $\varphi(\alpha) = \overline{\alpha}$.

(证毕)

定理 3 设 σ 是域 F 与域 $\overline{F}$ 的一个同构映射，$f(x)$ 与 $\overline{f}(x)$ 分别为 F 与 $\overline{F}$ 上的 $n > 0$ 次多项式．则 $f(x)$ 在 F 上的分裂域 $E = F(\alpha_1, \cdots, \alpha_n)$ 与 $\overline{f}(x)$ 在 $\overline{F}$ 上的分裂域 $\overline{E} = \overline{F}(\overline{\alpha}_1, \cdots, \overline{\alpha}_n)$ 同构，且此同构是 σ 的扩张．

证 对 $f(x)$ 与 $\overline{f}(x)$ 的次数 n 用数学归纳法．

当 $n = 1$ 时，$f(x)$ 与 $\overline{f}(x)$ 的分裂域就是 F 与 $\overline{F}$，结论当然成立．

假定定理对 $n - 1$ 成立，下证对 n 也成立．

任取 $f(x)$ 在 F 上的一个不可约因式 $p(x)$，由引理 1 知，$\overline{p}(x)$ 是 $\overline{f}(x)$ 在 $\overline{F}$ 上的一个不可约因式，不妨设 $p(\alpha) = 0$，$\overline{p}(\overline{\alpha}) = 0$，则由引理 2 知

$$F(\alpha) \cong \overline{F}(\overline{\alpha}),$$

且此同构是 σ 的扩张．现在在域 $F(\alpha)$ 与 $\overline{F}(\alpha)$ 上设

$$f(x)=(x-\alpha)f_1(x),\qquad \overline{f}(x)=(x-\overline{\alpha})\overline{f}_1(x),$$

则在 E 与 $\overline{E}$ 中，$f_1(x)$ 与 $\overline{f}_1(x)$ 都是 $n-1$ 次多项式，它们的根分别为 $\alpha_2,\cdots,\alpha_n$ 与 $\overline{\alpha}_2,\cdots,\overline{\alpha}_n$．由归纳假设，有

$$F(\alpha)(\alpha_2,\cdots,\alpha_n)\cong\overline{F}(\overline{\alpha})(\overline{\alpha}_2,\cdots,\overline{\alpha}_n),$$

且此同构保持原同构 $F(\alpha)\cong\overline{F}(\overline{\alpha})$，从而有

$$F(\alpha,\alpha_2,\cdots,\alpha_n)\cong\overline{F}(\overline{\alpha},\overline{\alpha}_2,\cdots,\overline{\alpha}_n),$$

且此同构是 σ 的扩张．

（证毕）

在此定理中，当 $F=\overline{F}$，且取 σ 为恒等自同构时，$\overline{f}(x)=f(x)$，于是得

推论　域 F 上多项式 $f(x)$ 的分裂域彼此同构．

习题　6.4

1．Q 上的单扩域 $Q(\sqrt[3]{2})$ 是不是 Q 上某个多项式在 Q 上的分裂域？

2．求 $f(x)=x^3-x^2-x-2$ 在 Q 上的分裂域．

3．证明：x^4+1 在 Q 上的分裂域是一个单扩域 $Q(\alpha)$，其中 α 是 x^4+1 的一个根．

4．设 x^3-a 是 Q 上一个不可约多项式，而 α 是 x^3-a 的一个根．证明：$Q(\alpha)$ 不是 x^3-a 在 Q 上的分裂域．

5．设 E 是域 F 上 $n>0$ 次多项式在 F 上的分裂域．证明：

$$(E:F)\leq n!.$$

■提示：对 n 用归纳法．

6．设 p 是一个素数，E 是 x^p-1 在 Q 上的分裂域．证明：

$$(E:Q)=p-1.$$

§5 有 限 域

在这一节里，我们要讨论一种特殊的域——有限域．它在实验设计和编码理论中有重要应用．

只包含有限个元素的域，叫做有限域．

例如，以素数 p 为模的剩余类环 Z_p 就是一个有限域．

定理 1 有限域 E 的元素个数是一个素数 p 的方幂 p^n，其中 $p=\mathrm{char}E$，而 n 是 E 在它所含素域上的次数．

证 设 Δ 是包含在 E 中的素域，由于 $\mathrm{char}E=p$，故 $|\Delta|=p$．又由于 $(E:\Delta)=n$，可取 E 的一基 α_1，α_2，$\cdots$，α_n，则 E 中每个元素都可惟一地表为

$$k_1\alpha_1+k_2\alpha_2+\cdots+k_n\alpha_n,\qquad k_i\in\Delta.$$

由于每个 k_i 在 Δ 中有 p 种取法，故系数共有 p^n 种取法；又由于每种取法决定 E 中惟一的一个元素，不同取法得到 E 中不同的元素，故 E 有 p^n 个元素．

（证毕）

由此定理可知，不存在诸如阶为 6，10，12 等等的有限域．

有限域也称为伽罗瓦域，一般记为 $GF(p^n)$，其中素数 p 为其特征，n 是它在素域上的次数．

定理 2 有限域 $E=GF(p^n)$ 是多项式

$$x^q-x\qquad(\text{其中 } q=p^n)$$

在其所含素域 Δ 上的分裂域．

证 因为 E 中全体非零元的集合 E^* 是一个 $q-1$ 阶乘群，故对 E^* 中任意 α 有

$$\alpha^{q-1}=1,\qquad \alpha^q=\alpha.$$

从而 E 的每个元素，包括 0 在内，都满足方程 $x^q=x$，即都是多项式

$$x^q-x$$

的根．现在若用 α_1，α_2，$\cdots$，α_q 表示有限域 E 的全体元素，于是在 $E[x]$ 中有

$$x^q-x=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_q),$$

且显然有

$$E=\Delta(\alpha_1,\alpha_2,\cdots,\alpha_q).$$

因此，E 是多项式 $x^q - x$ 在 Δ 上的分裂域．

(证毕)

由于特征为 p 的素域都同构，而多项式 $x^q - x$ 在同构的域上的分裂域也同构，因此，任何 p^n 阶有限域都同构．

下面讨论 p^n 阶有限域的存在问题．

定理 3 令 Δ 是特征为素数 p 的一个素域，$q = p^n$，其中 n 是正整数．则 $x^q - x$ 在 Δ 上的分裂域 E 是一个有 q 个元素的有限域．

证 $E = \Delta(\alpha_1, \alpha_2, \cdots, \alpha_q)$，其中 α_1，α_2，$\cdots$，α_q 是 $f(x) = x^q - x$ 在域 E 内的根．由于 E 的特征是 p，故

$$f'(x) = p^n x^{q-1} - 1 = -1.$$

于是 $(f(x), f'(x)) = 1$，从而 $f(x)$ 没有重根，即 α_1，α_2，$\cdots$，α_q 互异．现在令

$$F = \{\alpha_1, \alpha_2, \cdots, \alpha_q\},$$

则由于

$$(\alpha_i - \alpha_j)^{p^n} = \alpha_i^{p^n} - \alpha_j^{p^n} = \alpha_i - \alpha_j,$$

$$\left(\frac{\alpha_i}{\alpha_j}\right)^{p^n} = \frac{\alpha_i^{p^n}}{\alpha_j^{p^n}} = \frac{\alpha_i}{\alpha_j} \quad (\alpha_j \neq 0),$$

即 $\alpha_i - \alpha_j$ 与 $\dfrac{\alpha_i}{\alpha_j}$ 仍是 $f(x)$ 的根，从而仍属于 F，故 F 是 E 的一个子域．

但任何域同其子域都包含同一素域，故 F 包含 Δ，从而包含 $\Delta(\alpha_1, \alpha_2, \cdots, \alpha_q) = E$．因此

$$E = F = \{\alpha_1, \alpha_2, \cdots, \alpha_q\},$$

即 $x^q - x$ 在 Δ 上的分裂域就是一个 q 阶有限域．

(证毕)

这个定理说明，对任意给定的素数 p 和正整数 n，p^n 阶有限域是存在的．

定理 4 有限域 F 的非零元素作成的乘群是一个循环群．

证 设 F 是 q 阶有限域，F^* 是其非零元素乘群，阶为 $q-1$．令 m 是 F^* 中所有元素的最大阶，则由第二章§2 定理5 知，F^* 的 $q-1$ 个元素都是多项式

$$x^m - 1$$

的根，故 $m \geq q-1$．

另一方面，F^* 中每个元素的阶都整除 $q-1$，从而也有 $m \mid q-1$，$m \leq q-1$．因此，$m = q-1$．即 $q-1$ 阶群 F^* 有阶为 $q-1$ 的元素 α，从而 F^* 是循环群，且

$$F^* = ■\alpha■ = \{1, \alpha, \cdots, \alpha^{q-2}\}.$$

(证毕)

由此定理可知，任何有限域都可表示成

$$F = \{0, 1, \alpha, \cdots, \alpha^{q-2}\},$$

于是 $F = \Delta(\alpha)$，即 F 是其素域 Δ 的一个单扩域．这样的 α 称为 $q = p^n$ 阶有限域 F 的一个__根__，它是素域 Δ 上的 n 次代数元．

下面讨论有限域的子域．

定理5 设 E 是 p^n 阶有限域．则对 n 的每个正因子 m，存在且只存在一个 p^m 阶子域．

证 设 F 是 E 的一个子域，则 F 的特征也是 p，且 F 和 E 包含同一个素域 Δ，于是

$$|F| = p^m, \quad \text{其中 } m = (F : \Delta),$$

但由次数定理知，

$$n = (E : \Delta) = (E : F)(F : \Delta),$$

即 m 是 n 的正因数．

反之，设 $m \mid n$，则 $p^m - 1 \mid p^n - 1$．从而

$$x^{p^m-1} - 1 \mid x^{p^n-1} - 1 \quad \text{或} \quad x^{p^m} - x \mid x^{p^n} - x,$$

但在 E 上 $x^{p^n} - x$ 可完全分解，从而 $x^{p^m} - x$ 在 E 上也可完全分解．又由定理3 知，这个多项式在 E 中的全部根构成 E 的一个 p^m 阶子域，即 $x^{p^m} - x$ 在 E 的素域 Δ 上的分裂域．

由于 E 的 p^m 阶子域都是 $x^{p^m} - x$ 在素域 Δ 上的分裂域，故这样的子域也是惟一的．

(证毕)

最后我们指出如何具体构造出有限域的问题．

设 p 是任意给定的一个素数，n 是任一正整数．令 $p(x)$ 是域 Z_p 上一个 n 次不可约多项式，则 $\blacksquare p(x) \blacksquare$ 是环 $Z_p[x]$ 的极大理想．我们知道，域 $Z_p[x]/\blacksquare p(x)\blacksquare$ 中每个元素都可惟一地表示成

$$a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + \blacksquare p(x) \blacksquare, \qquad a_i \in Z_p,$$

但由于系数取自于 Z_p，每个 a_i 都有 p 种取法，故系数共有 p^n 种取法，亦即域 $Z_p[x]/\blacksquare p(x)\blacksquare$ 共包含 p^n 个元素．

例如，当 $p=2$ 时易知 $p(x) = x^2 + x + 1$ 是 Z_2 上一个不可约多项式，则

$$Z_2[x]/\blacksquare x^2 + x + 1\blacksquare$$

是一个 4 阶有限域．如果把

$$a_0 + a_1 x + \blacksquare x^2 + x + 1\blacksquare$$

简记为 $a_0 + a_1 x$，则这个有限域的 4 个元素就可以写成

$$0,\ 1,\ x,\ x+1.$$

但应注意，它们的系数都属于 Z_2，而且相乘时需用 $x^2 + x + 1$ 除后所得余式作为其乘积．例如，

$$x(x+1) = x^2 + x,$$

但是 $x^2 + x = (x^2 + x + 1) + 1$，故

$$x(x+1) = 1,$$

即 x 与 $x+1$ 互为逆元，等等．由此我们可以得到 4 元域

$$Z_2[x]/\blacksquare x^2 + x + 1\blacksquare = \{0, 1, x, x+1\}$$

的加法和乘法表如下：

+	0	1	x	$x+1$
0	0	1	x	$x+1$

1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

×	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

应该说明的是，为了简化起见，在这里我们把环 Z_2 的元素 $\bar{0}$，$\bar{1}$ 简记为 0，1．不仅如此，我们也可以把环 Z_n 中的元素聊简记为 i．例如

$$Z_9=\{0,1,2,3,4,5,6,7,8\},$$

当然，环 Z_9 中元素的运算仍遵从模 9 剩余类的加法与乘法规则．例如

$$2+7=0,\quad 2\cdot 7=5,$$

等等．只要稍加注意这是以 9 为模的运算，此外并不会造成混乱．

由于 $9=3^2$ 是素数 3 的方幂，因此 9 阶有限域是存在的．其构造方法如下．

首先取 3 阶有限域 $Z_3=\{0,1,2\}$；再取 Z_3 上的一个二次不可约多项式，例如易知 x^2+1 在 Z_3 上不可约．于是按照以上构造有限域的一般方法，可得 9 阶有限域为

$$Z_3[x]/■x^2+1■=\{0,1,2,x,x+1,x+2,$$
$$2x,2x+1,2x+2\}.$$

这里应再次强调的是，其加法和乘法既要遵从模 3 的加法和乘法(系数)又要遵从以 x^2+1 为模的加法和乘法(多项式)，也就是常说的“双模运算”．例如

$$2+(x+1)=x,\qquad (2x+1)+(2x+1)=x+2;$$

又
$$\begin{aligned}(2x+1)(2x+2)&=4x^2+6x+2\\&=x^2+2=(x^2+1)+1\\&=1.\end{aligned}$$

就是说，可以毫无顾忌地按多项式通常的运算规则进行加与乘，只是随时特别在最后时，系数要以模 3 取结果(即用 3 除取余数)，而整个多项式要以模 x^2+1 取结果(即用 x^2+1 除取余式)．由此我们不难得出以上 9 阶有限域的加法和乘法表．

习题 6.5

1. 证明：多项式 x^2+x+1 与 x^3+x+1 在 Z_2 上不可约．再求出 8 阶有限域 $Z_2[x]/(x^3+x+1)$ 的所有元素．

2. 试求出域 Z_2 上全部的三次不可约多项式．

3. 证明：包含域 Z_p 的每个有限域都是 Z_p 的单扩域．

4. 设 F 是一个域．证明：乘群 F^* 为循环群 $\Leftrightarrow$ F 为有限域．

5. 设 F 为 q 阶有限域，$f(x)$ 为 F 上一个 n 次不可约多项式．
证明：$f(x)$ 整除 $x^{q^n-1}-1$．

* §6 可■离■扩■域

我们知道，单扩域是一种很重要的扩域，而且还是一种构造非常简单的扩域．在代数扩域中，有不少的扩域都是单扩域．例如，易知有理数域 Q 的代数扩域

$$Q(3,\ \sqrt{2},\sqrt{5}\ \sqrt{2},\sqrt{4}\ \sqrt{3},\ \sqrt{6})=Q(\sqrt{2}+\sqrt{3})$$

就是一个单扩域；同样

$$Q(\sqrt{2},\ i)=Q(\sqrt{2}+i)$$

也是一个单扩域．

当然，普遍而言，要判断一个代数扩域是不是一个单代数扩域，并不是一件容易的事情．

本节要介绍一类重要的代数扩域，它们是单代数扩域．

定义 1 设 F 是一个域，E 是 F 的一个代数扩域．如果 E 的元素 α 在 F 上的最小多项式(在其分裂域中)没有重根，则称 α 为域 F 上的可离元；否则称为不可离元．

如果 E 中每个元素都是 F 上的可离元，则称 E 是 F 的 离域；否则称 E 是 F 的 可离扩域．

显然，域 F 中的每个元素都是 F 上的可离元．因此，如果 E 是 F 的不可离扩域，则当然是 E 中元素既有不可离元又有可离元．

由高等代数知，数域上的任何代数扩域都是可离扩域．更一般地，有

定理 1 设 $p(x)$ 是域 F 上的一个不可约多项式．则

1) 当 $\mathrm{char}\,F=\infty$ 时，$p(x)$ (在其分裂域中) 无重根；

2) 当 $\mathrm{char}\,F=p$ (素数) 时，$p(x)$ 有重根的充要条件是 $p(x)=g(x^p)$，其中 $g(x)\in F[x]$．

证 设

$$p(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}+a_nx^n,\qquad a_i\in F \tag{1}$$

则

$$p'(x)=a_1+2a_2x+\cdots+(n-1)a_{n-1}x^{n-2}+na_nx^{n-1}.$$

由第四章§9 知，$p(x)$ 有重根当且仅当

$$(p(x),p'(x))=d(x)\text{的次数}>0,$$

但由于 $p(x)$ 不可约，而且 $d(x)\mid p(x)$，$d(x)\mid p'(x)$，从而必 $p'(x)=0$，即

$$a_1=2a_2=\cdots=(n-1)a_{n-1}=na_n=0. \tag{2}$$

1) 当 $\mathrm{char}\,F=\infty$ 时，由上知 $a_i=0$，$i=1,2,\cdots,n$．于是

$$p(x)=a_0,$$

这与 $p(x)$ 是不可约多项式矛盾．故此时 $p(x)$ 无重根．

2) 当 $\mathrm{char}\,F=p$ 时，由(2)知，若 $p\nmid i(1\leq i\leq n)$ 则必 $a_i=0$．

于是由(1)得

$$\begin{aligned} p(x) &= a_0 + a_p x^p + \cdots + a_{(t-1)p} x^{(t-1)p} + a_{tp} x^{tp} \\ &= a_0 + a_p x^p + \cdots + a_{(t-1)p} (x^p)^{t-1} + a_{tp} (x^p)^t \\ &= g(x^p), \end{aligned}$$

其中 $g(x) = a_0 + a_p x + \cdots + a_{(t-1)p} x^{t-1} + a_{tp} x^t \in F[x]$.

(证毕)

由此定理得到一个重要推论.

推论 1 特征是∞的域的任何代数扩域，都是可离扩域.

特征在扩域的讨论中的重要性，其根本原因就在这里.

以下将看到，在特征为素数 p 的域中，既有可离扩域也有不可离扩域.

定义 2 如果域 F 的任何代数扩域都是可离扩域，则称 F 为<u>完全域</u>或<u>完备域</u>.

由推论 1 知，特征是∞的任何域都是完全域. 特别，凡数域都是完全域.

下面进一步讨论特征为素数 p 的域是完全域的条件.

定理 2 设 $\operatorname{char} F = p$，则域 F 是完全域的充分与必要条件是，F 中每个元素都是 F 中某个元素的 p 次幂.

证 1) 充分性. 设 F 中每个元素都是 F 中某个元素的 p 次幂. 下证 F 必是完全域，即 F 的任何代数扩域中的元素都是可离元.

因若不然，设 α 是 F 的一个不可离元，即 α 在 F 上的最小多项式 $p(x)$ 有重根. 于是由定理 1 知，可令

$$p(x) = a_0 + a_1 x^p + \cdots + a_{t-1} x^{p(t-1)} + a_t x^{pt}, \tag{3}$$

其中 $a_i \in F$. 于是由假设可令

$$a_i = b_i^p \quad (b_i \in F, i = 0, 1, \cdots, t),$$

并代入(3)，再由于 $\operatorname{char} F = p$，随得

$$\begin{aligned} p(x) &= b_0^p + b_1^p x^p + \cdots + b_{t-1}^p x^{p(t-1)} + b_t^p x^{pt} \\ &= (b_0 + b_1 x + \cdots + b_{t-1} x^{t-1} + b_t x^t)^p, \end{aligned}$$

即 $p(x)$ 在 F 上可约，矛盾．因此 F 是完全域．

2) 必要性．设 F 是完全域，但 F 中有元素 a 不是 F 中任何元素的 p 次幂．令 E 是 F 上多项式

$$f(x) = x^p - a$$

的分裂域．现任取其一根 $\beta \in E$，则 $\beta^p - a = 0$，从而

$$a = \beta^p,$$

由上面所设，$\beta \in F$．于是在 $E[x]$ 中有

$$x^p - a = x^p - \beta^p = (x - \beta)^p .$$

设 β 在 F 上的最小多项式为 $p(x)$，则 $p(x) \mid (x - \beta)^p$．从而必有

$$p(x) = (x - \beta)^k, \quad 1 \leq k \leq p .$$

若 $k = 1$，则 $p(x) = x - \beta$，$\beta \in F$，矛盾．于是只有 $k > 1$，这样，$p(x)$ 有重根，与假设 F 是完全域矛盾．因此，F 中每个元素都必须是 F 中某个元素的 p 次幂．

(证毕)

例 1 模 p(素数)剩余类域

$$Z_p = \{0, 1, \cdots, p - 1\} \quad (\text{这里 } i \text{ 即} \overline{i})$$

是一个完全域．

证 因为 Z_p 的单位群

$$Z_p^* = \{1, 2, \cdots, p - 1\}$$

是一个 $p - 1$ 阶群，故对其中任意元素 a 有

$$a^{p-1} = 1,$$

从而对域 Z_p 中任何元素 a(包括 0)有

$$a = a^p,$$

因此由定理 2 知，Z_p 是完全域．

更一般地，有

定理 3 凡有限域都是完全域．

证 设 F 是一个 q 阶有限域，且其特征为 p，则令

$$F=\{a_1, a_2, \cdots, a_q\},$$

于是

$$\{a_1^p, a_2^p, \cdots, a_q^p\} \quad F .$$

但是当 $i\neq j$ 时，有

$$a_i^p - a_j^p = (a_i - a_j)^p \neq 0, \quad \text{即 } a_i^p \neq a_j^p,$$

因此，a_1^p，a_2^p，$\cdots$，a_q^p 是 q 个互不相等的元素，故

$$F=\{a_1^p, a_2^p, \cdots, a_q^p\} .$$

从而 F 中每个元素都是 F 中某个元素的 p 次幂，故由定理 2 知，F 是完全域．

(证毕)

应该注意的是，在这个定理中虽然有

$$F=\{a_1, a_2, \cdots, a_q\}=\{a_1^p, a_2^p, \cdots, a_q^p\},$$

但却不一定像例 1 那样都有

$$a_i = a_i^p, \quad i=1, 2, \cdots, q .$$

例 2 易知 $Z_2=\{0,1\}$ 上 4 个方阵的集合

$$F=\begin{matrix}0&0\\0&0\end{matrix}, \begin{matrix}1&0\\0&1\end{matrix}, \begin{matrix}1&1\\1&0\end{matrix}, \begin{matrix}0&1\\1&1\end{matrix}$$

关于方阵的普通加法与乘法作成一个特征是 2 的域．如果这 4 个方阵依次用 0，1，a，b 表示，则易知

$$a=b^2, \quad b=a^2 .$$

从而 $a^2\neq a$，$b^2\neq b$．

在特征为 p 的无限域中可能有非完全域．

例 3 设 u 是模 p(素数)剩余类域 Z_p 上的一个未定元，则 $F=Z_p(u)$ 是特征为 p 的一个无限域．特别，F 不是一个完全域．

证 F 中的元素都是系数属于 Z_p 的关于 u 的有理分式．若 F 是完全域，则由定理 2，F 中每个元素都是 F 中某个元素的 p 次幂．特别，F 中元素 u 必是 F 中某个元素的 p 次幂．令

$$u=\left(\frac{f(u)}{g(u)}\right)^p, \quad f(u)\,g(u)\neq 0, \qquad (4)$$

并设其中

$$f(u) = a_0 + a_1 u + \cdots + a_m u^m, \quad a_i \in Z_p,$$

$$g(u) = b_0 + b_1 u + \cdots + b_n u^n, \quad b_j \in Z_p,$$

于是由(4)，并根据 $\mathrm{char}F = p$，可得

$$b_0^p u + b_1^p u^{p+1} + \cdots + b_n^p u^{pn+1} = a_0^p + a_1^p u^p + \cdots + a_m^p u^{pm}.$$

但由于 u 是域 Z_p 上的未定元，故

$$a_0 = a_1 = \cdots = a_m = b_0 = b_1 = \cdots = b_n = 0,$$

矛盾．因此，F 不是完全域．

下面给出一个元素是可离元的条件．

定理 4 设 $\mathrm{char}F = p$，α 是域 F 的某一扩域中的元素．则

$$\alpha \text{是 } F \text{ 上可离元} \quad F(\alpha) = F(\alpha^p).$$

证 1) 设 α 是 F 上的可离元，则 α 当然也是域 $F(\alpha^p)$ 上的可离元．令 α 在 $F(\alpha^p)$ 上的最小多项式是 $p(x)$，则由于 α 又是域 $F(\alpha^p)$ 上多项式 $x^p - \alpha^p$ 的根，从而

$$p(x) \mid x^p - \alpha^p = (x - \alpha)^p,$$

这只有

$$p(x) = (x - \alpha)^k, \quad 1 \leq k \leq p.$$

因 α 是 $F(\alpha^p)$ 上可离元，故必 $k = 1$，即

$$p(x) = x - \alpha \in F(\alpha^p).$$

于是 $\alpha \in F(\alpha^p)$，从而 $F(\alpha) \quad F(\alpha^p)$．

但是，显然 $F(\alpha^p) \quad F(\alpha)$，因此，$F(\alpha) = F(\alpha^p)$．

2) 反之，设 $F(\alpha) = F(\alpha^p)$，且 α 是 F 上的不可离元．则由定理 1 知，α 在 F 上的最小多项式

$$p(x) = g(x^p), \quad g(x) \in F[x],$$

于是 $g(\alpha^p) = p(\alpha) = 0$．又若 $g(x) = g_1(x)g_2(x)$，则必

$$p(x) = g(x^p) = g_1(x^p) \cdot g_2(x^p).$$

因此，由于 $p(x)$ 在 F 上不可约，故 $g(x)$ 在 F 上也不可约．从而 $g(x)$ 是 α^p 在 F 上的最小多项式．

如果 $g(x)$ 的次数为 $n(n>0)$，则 $p(x)=g(x^p)$ 的次数为 pn，且

$$(F(\alpha):F)=pn,\quad (F(\alpha^p):F)=n.$$

于是由次数定理知，$(F(\alpha):F(\alpha^p))=p$，从而 $F(\alpha)\neq F(\alpha^p)$，矛盾．故必 α 是 F 上可离元．

（证毕）

为了进一步证明可离元的性质，先证以下

引理　设 $E=F(\beta)$ 是域 F 的单扩域，且 β 是 F 上的可离元．则 E 上的可离元也是 F 上的可离元．

证　若 $\mathrm{char}F=\infty$，则由定理 1 知，结论显然．

若 $\mathrm{char}F=p$，α 是 E 上的任意可离元，则由定理 4 知

$$E(\alpha)=E(\alpha^p),\quad \text{即 } F(\alpha,\beta)=F(\alpha^p,\beta). \tag{5}$$

现在令 β 在域 $F(\alpha)=F[\alpha]$ 上的最小多项式是

$$g(x)=b_0+b_1x+\cdots+b_{n-1}x^{n-1}+x^n,\quad b_i\in F(\alpha),$$

且 $b_i=\sum_j a_{ij}\alpha^j$，则

$$(g(x))^p=b_0^p+b_1^px^p+\cdots+b_{n-1}^px^{p(n-1)}+x^{pn},$$

$$b_i^p=\Big(\sum_j a_{ij}\alpha^j\Big)^p=\sum_j a_{ij}^p(\alpha^p)^j\in F(\alpha^p),$$

从而 $(g(x))^p\in F(\alpha^p)[x]$，且有 $(g(\beta))^p=0$．

设 $\varphi(x)$ 是 β 在 $F(\alpha^p)$ 上的最小多项式，则由上知

$$\varphi(x)\mid (g(x))^p. \tag{6}$$

但 $g(x)$ 是 β 在 $F(\alpha)$ 上的最小多项式，又 $F(\alpha^p)\subseteq F(\alpha)$，且 $\varphi(\beta)=0$，故又有 $g(x)\mid\varphi(x)$．设

$$\varphi(x)=g(x)h(x)\quad (h(x)\in F(\alpha)[x]), \tag{7}$$

则由(6)知，有

$$g(x)h(x)\mid (g(x))^p\quad \text{或}\quad h(x)\mid (g(x))^{p-1}.$$

从而 $h(x)=(g(x))^k$，$0\le k\le p-1$．但 β 是 F 上可离元，而 $F\subseteq F(\alpha^p)$，从而 β 是 $F(\alpha^p)$ 上可离元，故 $\varphi(x)$ 不能有重根．于是

由(7)知 $h(x)$不能有重根．这只有 $k=0$．因此再由(6)知，$\varphi(x)=g(x)$．即 β在 $F(\alpha)$上与在 $F(\alpha^p)$上的最小多项式相同．从而

$$(F(\alpha,\beta):F(\alpha))=(F(\alpha^p,\beta):F(\alpha^p)),$$

于是由(5)知

$$(F(\alpha,\beta):F(\alpha))=(F(\alpha,\beta):F(\alpha^p)).$$

但因为 $F(\alpha^p)\quad F(\alpha)\quad F(\alpha,\beta)$，故$(F(\alpha):F(\alpha^p))=1$．从而

$$F(\alpha)=F(\alpha^p).$$

于是由定理 4 知，α是 F 上的可离元．

(证毕)

定理 5 若 α与 β是域 F 上的可离元，则 $F(\alpha,\beta)$是 F 的一个可离扩域．

证 任取 $\gamma\in F(\alpha,\beta)=F(\alpha)(\beta)$，则 γ 当然是 $F(\alpha)(\beta)$上的可离元．因为 β是 F 上可离元，当然也是 $F(\alpha)$上可离元，从而由引理知，γ是 $F(\alpha)$上可离元．

又因 α是 F 上可离元，再由引理知，γ是 F 上可离元．因此，$F(\alpha,\beta)$是 F的可离扩域．

(证毕)

推论 2 可离元的和、差、积、商(分母不为零)仍为可离元．

证 因若 α, β是域 F 上可离元，则 $\alpha\pm\beta$, $\alpha\beta$且当 $\beta\neq0$ 时 $\frac{\alpha}{\beta}$都属于 $F(\alpha,\beta)$，而 $F(\alpha,\beta)$是 F 的可离扩域，从而 $\alpha\pm\beta$, $\alpha\beta$, $\frac{\alpha}{\beta}(\beta\neq0)$都是可离元．

(证毕)

最后来证明本节关于可离扩域的主要结论．

定理 6 域 F 的有限次可离扩域必是 F 的单扩域．

证 设 E 是域 F 的任意一个有限次可离扩域．若 F 是有限域且 Δ 是包含在 F 中的素域，则 E 当然也是有限域．从而由上

节知

$$E = \Delta(\alpha) = F(\alpha),$$

即 E 是 F 上的单扩域．因此，下设 F 是无限域．

因为 E 是 F 的有限次可离扩域，故由§3 知，在 E 中存在 n 个元素 $\alpha, \beta, \cdots, \gamma$ 使

$$E = F(\alpha, \beta, \cdots, \gamma),$$

其中 $\alpha, \beta, \cdots, \gamma$ 都是 F 上可离元．由数学归纳法知，只需讨论 $n = 2$ 的情形就可以了．因此不妨设

$$E = F(\alpha, \beta), \quad \alpha 与 \beta 是 F 上可离元．$$

且令 $p(x)$ 与 $q(x)$ 分别为 α 与 β 在 F 上的最小多项式．

设 K 是乘积 $p(x)q(x)$ 在 E 上的分裂域，并令 $p(x)$ 与 $q(x)$ 在 K 中的全部根分别为

$$\alpha = \alpha_1, \alpha_2, \cdots, \alpha_s \quad 与 \quad \beta = \beta_1, \beta_2, \cdots, \beta_t.$$

现在考察 K 上的 $s(t-1)$ 个方程

$$(\beta_j - \beta_k)x = \alpha_i - \alpha_k, \qquad i = 1, 2, \cdots, s; \quad j = 2, \cdots, t.$$

由于 α, β 是 F 上可离元，$p(x)$ 与 $q(x)$ 都没有重根，故这 $s(t-1)$ 个方程的解只能是有限个．但 F 是无限域，故必存在 $a \in F$ 使

$$(\beta_j - \beta_k)a \neq \alpha_i - \alpha_k, \qquad i = 1, 2, \cdots, s; \quad j = 2, \cdots, t.$$

即 $(\alpha_i + a\beta_j) - a\beta_k \neq \alpha_i$，或

$$\theta - a\beta_k \neq \alpha_i, \quad 其中\ \theta = \alpha + a\beta. \tag{8}$$

这就是说，$\theta - a\beta_j\ (j = 2, \cdots, t)$ 都不是 $p(x)$ 的根．

下证：$F(\alpha, \beta) = F(\theta)$．

首先，因为 $\theta = \alpha + a\beta \in F(\alpha, \beta)$，故

$$F(\theta) \subseteq F(\alpha, \beta).$$

其次，令 $h(x) = p(\theta - ax) \in F(\theta)[x]$，则由(8)有

$$h(\beta) = p(\theta - a\beta) = p(\alpha) = 0.$$

因此，$h(x)$ 与 $q(x)$ 有公根 β．但由上知，$\theta - a\beta$ 都不是 $p(x)$ 的根．故

$$h(\beta) = p(\theta - a\beta) \neq 0, \quad j = 2, \cdots, t,$$

即 $q(x)$的根 $\beta, \cdots, \beta$ 都不是 $h(x)$的根．因此

$$(q(x), h(x)) = x - \beta.$$

但因为 $q(x), h(x) \in F(\theta)[x]$，故其最大公因式 $x - \beta$ 必为域 $F(\theta)$上的多项式，从而

$$\beta \in F(\theta).$$

由此根据(8)又得：$\alpha = \theta - a\beta \in F(\theta)$．从而又有

$$F(\alpha, \beta) \quad F(\theta).$$

因此，$F(\alpha, \beta) = F(\theta)$．

(证毕)

由于完全域的任何代数扩域都是可离扩域，因此，由这个定理可知，完全域的任何有限次扩域都是单扩域．特别，数域的任何有限次扩域都是单扩域．

例 4 令 Q 是有理数域，$\alpha = \sqrt{2}$，$\beta = \sqrt{5}$．按照定理 6 证明中所给出的方法，求 θ 使

$$Q(\sqrt{2}, \sqrt{5}) = Q(\theta).$$

解 $Q(\sqrt{2}, \sqrt{5})$显然是 Q 上 4 次代数扩域．

又 $\sqrt{2}$与 $\sqrt{5}$在 Q 上的最小多项式分别为

$$p(x) = x^2 - 2, \quad q(x) = x^2 - 5,$$

其根分别为：

$$\alpha = \alpha_1 = \sqrt{2}, \ \alpha_2 = -\sqrt{2}; \quad \beta = \beta_1 = \sqrt{5}, \ \beta_2 = -\sqrt{5}.$$

这时的 $s(t-1) = 2$ 个方程是

$$\sqrt{2} + \sqrt{5}x = 0, \quad \sqrt{2} + \sqrt{5}x = -\sqrt{2} - \sqrt{2}.$$

显然，Q 中除 0 外的任何有理数都不是其任何一个方程的解．例如，取 $a = 1$．于是由定理 6，有

$$\theta = \alpha + a\beta = \sqrt{2} + 1 \cdot \sqrt{5} = \sqrt{2} + \sqrt{5},$$

从而 $Q(\sqrt{2}, \sqrt{5}) = Q(\sqrt{2} + \sqrt{5})$．

实际上，任取任何非零有理数 a 均有

$$Q(\sqrt{2},\sqrt{5}) = Q(\sqrt{2}+a\sqrt{5}).$$

足见定理 6 中的 θ并不是惟一的．另外应注意，并非对任何的 α与 β都有 $Q(\alpha,\beta) = Q(\alpha+\beta)$．例如，显然，

$$Q(\sqrt{2},-\sqrt{2}) \neq Q(0),$$

因为实际上，$Q(\sqrt{2},-\sqrt{2}) = Q(\sqrt{2})$，但是 $Q(0) = Q$．

一般来说，要想求出定理 6 中的 θ并不容易．

习题 6.6

1. 设 Q 是有理数域，i 是虚数单位．证明：

$$Q(\sqrt{2},i) = Q(\sqrt{2}+i).$$

2. 设 p，q 都是素数．证明：

$$Q(\sqrt{p},\sqrt{q}) = Q(\sqrt{p}+\sqrt{q}).$$

3. 设 $\mathrm{char}F = p$，且域 F 不是完全域．证明：$p(x) = x^{p^n} - a$ 在域 F 上不可约的充要条件是，a 不是 F 中任何元素的 p 次幂．

4. 令 $F = Z_p(u)$ 是例 3 中的域．证明：F 上多项式 $f(x) = x^p - u$ 在 F 上不可约，但在其分裂域中有重根．

5. 设 $\mathrm{char}F = p$，α是域 F 上可离元．证明：α^p 也是 F 上可离元．

6. 设 $\mathrm{char}F = p$，α是域 F 上的不可离元．证明：若 $p\nmid r\ (r>0)$，则 α^r 也是 F 上不可离元．

7. 问：映射 $\varphi: a+b\sqrt{2} \to a+b\sqrt{3}$ 是否是有理数域 Q 上的单扩域 $Q(\sqrt{2})$ 与 $Q(\sqrt{3})$ 的同构映射？这两个单扩域是否同构？

8. 设有域 $F \subseteq K \subseteq E$，且 $(K:F) = m$，$\alpha\in E$ 是 F 上一个 n 次代数元，$(m,n) = 1$．证明：α也是 K 上的 n 次代数元．

提示：$F \subseteq K \subseteq K(\alpha)$，$F \subseteq F(\alpha) \subseteq K(\alpha)$，并利用次数定理．

9. 设 E 是域 F 的一个扩域．证明：若 $\alpha\in E$ 是 F 上的一个奇次代数元，则 α^2 也是 F 上的一个奇次代数元，并且

$$F(\alpha) = F(\alpha^2).$$

10. 设 E 是域 F 的 4 次扩域，且 $\mathrm{char}F\neq 2$．证明：存在一个满足 $F \subseteq K \subseteq E$ 的 F 的 2 次扩域 K 的充要条件是：$E = F(\alpha)$，而 α在 F 上的最小多项式是

$$x^4 + ax^2 + b, \quad a, b \in F .$$

11. 证明：$\varphi: a \to a^p$ 是伽罗瓦域 $GF(p^n)$ 的一个自同构，且这个自同构在 $GF(p^n)$ 的自同构群中的阶是 n.

12. 设 p 是一个素数. 证明：对任何正整数 n，都存在一个在域 Z_p 上不可约的 n 次多项式.

提示：参见书末文献[1]或[8].

13. 令 F 是一个有限域，Δ 是它所含的素域，且 $F = \Delta(\alpha)$. 问：α 是否一定是乘群 F^* 的生成元？

14. 证明：任何有限域都有比它大的代数扩域.

15. 设 α, β 分别是域 F 上的 m，n 次代数元. 证明：

1) $(F(\alpha,\beta) : F) \leq mn$;

2) 若 $(m, n) = 1$，则 $(F(\alpha,\beta) : F) = mn$.

本书所用符号

Z	整数集(环)
Q	有理数集(域)
$\|G\|$	群 G 的阶
$\|a\|$	群中元素 a 的阶
U_n	n 次单位根群
$GL_n(F)$	域 F 上一般线性群
$SL_n(F)$	域 F 上特殊线性群
$\leq$	子群或子环
$<$	真子群或真子环
	正规子群或理想
■M■	由 M 生成的子群或理想
■a■	由元素 a 生成的子群或理想
$\sim$	同态
$\cong$	同构
$T(M)$	M 的全体变换作成的半群
$S(M)$	集合 M 上的对称群
S_n	n 次对称群
A_n	n 次交代群
K_4	Klein 四元群
$C(G)$	群 G 的中心

$C(S)$	群中子集 S 的中心化子
$N(S)$	群中子集 S 的正规化子
Kerϕ	同态 ϕ 的核
Imϕ	同态 ϕ 的象
Aut$G$	群 G 的自同构群
Inn$G$	群 G 的内自同构群
$T(n)$	n 的正因数个数
$(G:H)$	子群 H 的指数
Z_n	模 n 剩余类环
$R_{n\times n}$	环 R 上的 n 阶全阵环
End$G$	加群 G 的自同态环
char$R$	环 R 的特征
$U(R)$, R^*	环 R 的单位群(乘群)
$P(M)$	M 的幂集环
r(A)	矩阵 A 的秩
GF(p^n)	伽罗瓦域
$(E:F)$	扩域 E 在子域 F 上的次数

名■词■索■引

五画

六画

七画

八画

十三画

十四画

十五画

其他

参■考■文■献

1　杨子胥，宋宝和．近世代数习题解．济南：山东科学技术出版社，2003

2　杨子胥．高等代数习题解(上、下册,修订版)．济南：山东科学技术出版社，2001

3　张禾瑞．近世代数基础．北京：人民教育出版社(修订本)，1978

4　吴品三．近世代数．北京：高等教育出版社，1979

5　熊全淹．近世代数．武汉：武汉大学出版社，1991

6　А．Г．库洛什．群论(翻译本)．北京：人民教育出版社，1964

7　王萼芳．有限群论基础．北京：北京大学出版社，1986

8　杨子胥．正交表的构造．济南：山东人民出版社，1978

9　J．S．Rose，A course on group theory，1978

10　N．H．McCOY，Rings and Ideals，1948

11　N．Jacobson，Structure of rings，1956

12　杨子胥．关于循环环及其幂等元，数学的实践与认识,1985,3

13　杨子胥，The structure of involutive rings which in the residue class rings，数学季刊，1994，3

14　杨子胥，郝秀梅，关于 NF—环的构造，数学研究与评论，1997，3