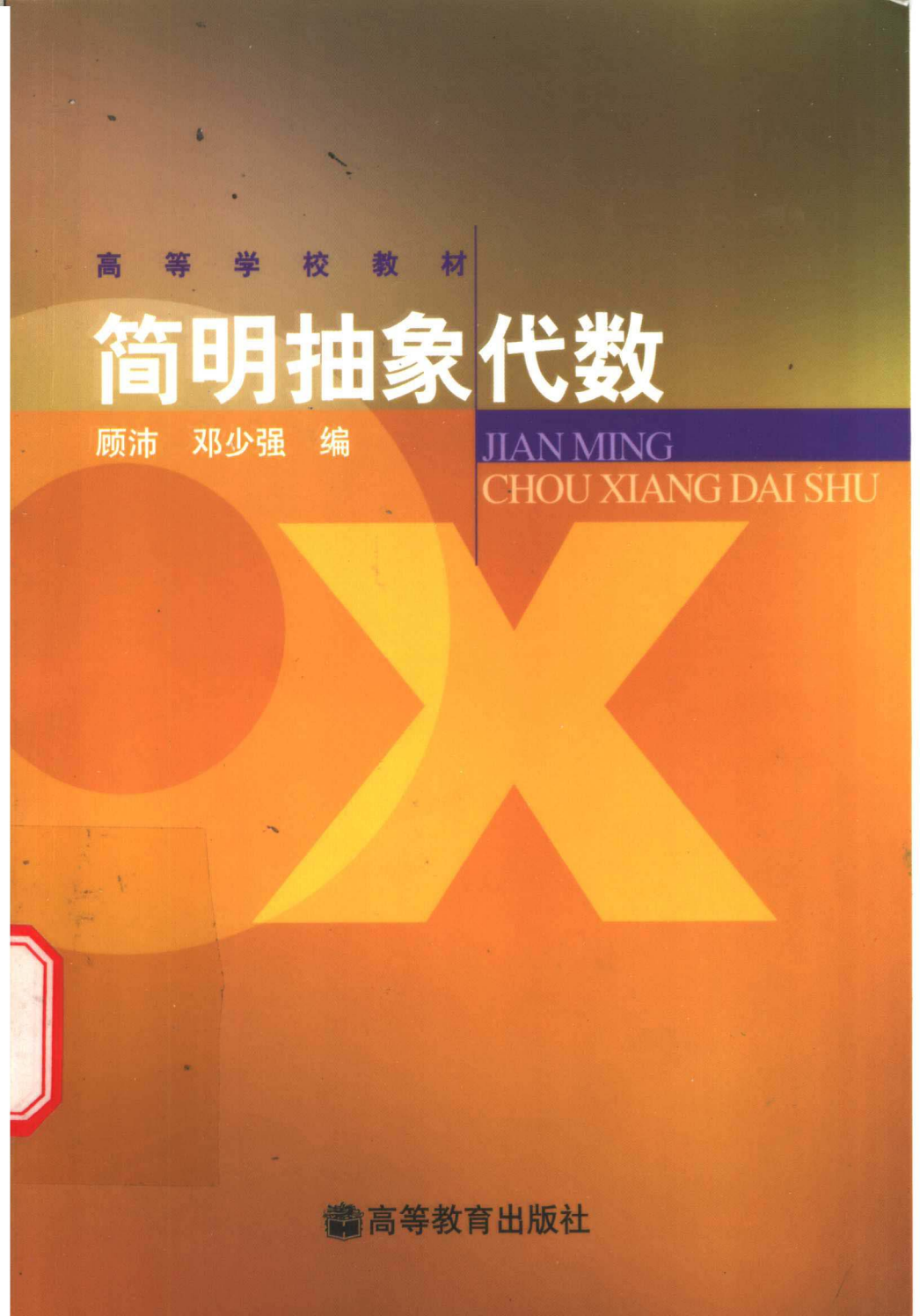
高等学校教材

简明抽象代数

顾沛　邓少强　编

JIAN MING
CHOU XIANG DAI SHU



高等教育出版社

高等学校教材

简明抽象代数

顾　沛　邓少强　编

高等教育出版社

内容提要

本书是大学本科一学期周3学时的“抽象代数”课的教材，主要内容是群、环、域的基础知识.本书的特点是简明实用，注重讲清抽象代数的思想和精神.本书还配备了适当数量的习题，并分基本题与补充题两个层次设置，便于学生自学和教师选题.

本书可作为综合性大学、一般院校或师范院校的“抽象代数”课教材，特别适合周3学时的教学使用.

图书在版编目(CIP)数据

简明抽象代数/顾沛，邓少强编.—北京：高等教育出版社，2003.4
ISBN 7-04-011916-1

Ⅰ.简… Ⅱ.①顾…②邓… Ⅲ.抽象代数-高等学校-教材 Ⅳ.O153

中国版本图书馆CIP数据核字(2003)第043834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		
排　　版	高等教育出版社照排中心		
印　　刷	廊坊市科通印业有限公司		
开　　本	850×1168　1/32	版　　次	2003年4月第1版
印　　张	4.375	印　　次	2003年4月第1次印刷
字　　数	100 000	定　　价	7.60元

前　言

现在，代数学在数学中的地位越来越重要，代数学在各个学科中的应用越来越广泛．但是，过去非数学专业本科生的代数知识往往只限于“线性代数”或“高等代数”．不接触抽象代数，这对于许多专业是一种缺陷．南开大学数学科学学院，从2001级本科生起，“抽象代数”不仅仍规定为数学专业的必修课，也列为“计算数学”，“信息科学”，“统计学”，“应用数学”等专业方向的必修课，周3学时，共上19周．本书最初是为此而写的．但我们的想法是，本书要以相当广泛一个层面的学生为对象．物理、化学、生物、电子、计算机、控制论、软件、通信工程、信息安全、经济、金融、管理、保险等学科的学生，逐渐也都需要学习抽象代数．为他们开设“抽象代数”课程，多半也是周3学时．现在的“抽象代数”教材，大多内容求全求多，不适合他们用．而本书则以少而精为特色，力求简明实用．

这里说的简明实用，有以下几层意思．一是内容较少，都经过挑选，但已经包含了抽象代数的最基本的知识和方法；二是以知识为载体，注重讲清抽象代数的思想和精神；三是概念和定理的引入力求简单自然；四是设置了“*”节，习题也分两个层次设置，便于教学实用；五是针对性强，适用于周3学时“抽象代数”课的教学；六是通俗易懂，便于自学．

本书主要内容是群，环，域的基础知识，主要目的是讲清这门课程的“抽象”特点，及研究代数体系的基本方法，以给学生继续学习的知识和能力．本书注重讲清数学思想，而不追求一切推理都十

分严格；但凡不严格的地方，书中都明确指出，或说“略去证明”，或说“请读者自己证明”，等等．为了让读者了解抽象代数的创始者伽罗瓦和他的思想，本书还给出了附录“伽罗瓦理论简介”．

抽象代数中考察的元素，集合，运算，关系，都是抽象的；代数体系是带有运算的集合，也是抽象的．抽象的定义要结合具体的例子去掌握，去记忆．抽象的定理要结合具体的应用去理解，去消化．如果能自己举出例子，自己找到应用，就更好．学完一章后，脑子里不能只有大批概念和命题，而一定要有几个有血有肉，有条有理的原型．要能借助于原型把理论展开．读者要特别体会研究抽象代数体系的基本思路，基本理论和基本方法．

建议读者重视以下四个方面的理论：一是结构方面的理论，要确切理解各种代数体系的结构中出现的概念；二是同构方面的理论，要明白两个代数体系同构的充分必要条件；三是分类方面的理论，要体会把代数体系在同构意义下分成若干类的研究思路；四是分解方面的理论，要弄懂把一个复杂事物分解成简单成分的研究方法．

做适当数量，适当难易的习题，是学好一门课程的有机组成部分．本书每节后配有适量的习题和补充题，“习题”属于基本要求，“补充题”则属于进一步的要求．教师可根据不同的教学对象灵活掌握，自学者也可根据自己的基础和要求灵活掌握．习题和补充题中的许多内容，也是正文的必要补充．

本书的第一章“群”和附录“伽罗瓦理论简介”由顾沛执笔，第二章“环”和第三章“域”由邓少强执笔；顾沛还负责总体构思和统稿．

本书写作过程中参考了很多有关书籍，就不一一列出了．

作者十分感谢本书的责任编辑薛春玲同志的辛勤劳动，她的工作为本书增色不少．

作者有多年“高等代数”和“抽象代数”的教学经验，本书胶印本也经过南开大学数学科学学院周3学时的“抽象代数”课的教学

实践.但本书中一定还存在一些疏漏和错误,希望广大读者提出批评和指正,我们将不胜感谢!

作者

2003 年 2 月

策划编辑　徐　刚
责任编辑　薛春玲
封面设计　刘晓翔
责任绘图　朱　静
版式设计　王艳红
责任校对　尤　静
责任印制　韩　刚

郑重声明

目　录

第一章　群

抽象代数的研究对象是代数体系，即带有运算的集合，例如群、环、域．本书假定读者已经了解集合与映射的基本知识，下边仅介绍一下映射的嵌入与开拓、映射的交换图以及直积的概念．

§1.1　运算及关系

定义 1.1.1　设 A_0 是集合 A 的非空子集，定义 A_0 到 A 的映射 i 如下

$$i(x)=x,\ \forall x\in A_0,$$

则 i 称为 A_0 到 A 的**嵌入映射**．

定义 1.1.2　设 A_0 是集合 A 的非空子集，f 是 A_0 到集合 B 的映射，若有 A 到 B 的映射 g，使

$$g(x)=f(x),\forall x\in A_0,$$

则称 g 为 f 的**开拓映射**，称 f 为 g 在 A_0 上的**限制映射**，并记

$$f=g|_{A_0}.$$

直观上，开拓映射是把一个映射的定义域扩大；限制映射是把一个映射的定义域缩小．从这个意义上说，嵌入映射是把一个恒等映射值域所在的集合扩大．嵌入映射一定是单射，不一定是满射．开拓映射既不一定是单射，也不一定是满射．

定义 1.1.3 一个映射如果既能表成某几个映射的连续作用(也称映射的乘积)的结果,又能表成另几个映射的连续作用的结果,例如有 $f_3f_2f_1=g_2g_1$,就可有图 1.1,则称下图为**映射的交换图**.

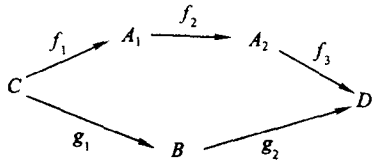


图 1.1

例 1 设 f 是 A_0 到 B 的映射,A_0 是 A 的子集,i 是 A_0 到 A 的嵌入映射,g 是 A 到 B 的映射,且 g 是 f 的开拓映射,则下面的图 1.2 是交换图:

即有 $gi=f$.

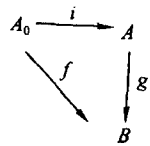


图 1.2

定义 1.1.4 设 A,B 是两个集合,则称

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

为 A 与 B 的**直积**.

类似地,可以定义有限多个(k 个)集合的直积:

$$A_1\times\cdots\times A_k=\{(a_1,\cdots,a_k)\mid a_i\in A_i,i=1,\cdots,k\}.$$

我们要研究的是带有运算的集合.对于数集中的运算,例如加法和乘法运算,我们是熟悉的.它们的本质都在于,由数集中的任两个元素,可以按照某种法则惟一地确定数集中的一个元素.在线性代数中我们又学习到线性空间中的"数乘"运算,其本质在于,由数集中的一个元素和向量集中的一个元素,按照某种法则,可以惟一地确定向量集中的一个元素.

现在我们把上述本质抽象出来,利用集合、直积和映射的概念,来定义"代数运算"这一概念.

定义 1.1.5 设 A,B,D 均是非空集合，则 $A\times B$ 到 D 的任一映射 f，称为 A 与 B 到 D 的一个**代数运算**.

这就是说，若有 $a\in A,b\in B$，则 $(a,b)\in A\times B$，$f((a,b))=d\in D$，即 a 与 b 惟一地确定 d，我们就说 a 与 b 运算的结果是 d. 为简单，常记 $f((a,b))$ 为 $a\circ b$，于是上面的运算就写成了 $a\circ b=d$. 为了区别不同的运算法则，我们有时也把代数运算的符号“$\circ$”改记为“$+$”或“$\times$”，于是就有了

$$3+5=8 \quad 和 \quad 3\times 5=15$$

的写法，也有了“加法”、“乘法”以及“数乘”等关于运算的叫法. 在乘法或数乘等运算中，我们常常把符号“$\circ$”省去，记 $a\circ b$ 为 ab.

例 2 设 V 是 n 维欧氏空间，$\mathbb{R}$ 是实数集，则求 V 中两向量 α,β 的内积，就是 V 与 V 到 $\mathbb{R}$ 的一个代数运算.

例 3 设 $A=\{1,2\}$，$B=\{1,2\}$，$D=\{$奇，偶$\}$，f 是一个 $A\times B$ 到 D 的映射，如下所示：

$$(1,1)\to 奇,\quad (2,2)\to 奇$$

$$(1,2)\to 奇,\quad (2,1)\to 偶$$

它也是一个 A 与 B 到 D 的代数运算.

当 A、B 都是有限集合的时候，A 与 B 到 D 的代数运算，我们常用一个表来说明，叫做“运算表”. 例 3 的运算表为

$\circ$	1	2
1	奇	奇
2	偶	奇

这里，竖行中的“1,2”，指 A 中的元素；横行中的“1,2”，指 B 中的元素.

通常较多用到的代数运算，是 $A=B=D$ 时的情形，即 A 与 A 到 A 的代数运算，也称为 A 中的“**二元运算**”或“**运算**”. 此时也说“集合 A 对于该运算是封闭的”. 一个集合中，可以有一种运算，也可以有多种运算. 我们感兴趣的运算，常常是满足某种规律的运

算,例如针对一种运算而言的结合律和交换律,针对两种运算而言的分配律.它们都是数集中相应运算规律的推广.

定义 1.1.6 设集合 A 中有一种二元运算"$\circ$",如果

$$(a\circ b)\circ c=a\circ(b\circ c),\quad \forall a,b,c\in A,$$

则称该运算满足**结合律**.

定义 1.1.7 设集合 A 中有一种二元运算"$\circ$",如果

$$a\circ b=b\circ a,\quad \forall a,b\in A,$$

则称该运算满足**交换律**.

定义 1.1.8 设集合 A 中有两种代数运算"$\circ$"和"$+$",如果

$$a\circ(b+c)=a\circ b+a\circ c,\quad \forall a,b,c\in A,$$

则称该运算满足"$\circ$对$+$的分配律",简称满足**分配律**.

例 4 设Z是全体整数的集合,Z中的二元运算是数的减法,则该运算既不满足结合律,也不满足交换律.

例 5 设$\mathbb{C}^{n\times n}$是复数域上全体 $n(n\geqslant 2)$阶方阵的集合,$\mathbb{C}^{n\times n}$中有两种运算,一种是矩阵的加法,一种是矩阵的乘法.加法运算既满足结合律,又满足交换律;乘法运算满足结合律,不满足交换律;乘法对加法满足分配律,加法对乘法不满足分配律.

结合律的一个重要作用是使表达式 $a_1\circ a_2\circ\cdots\circ a_n$ 有意义,因为这时无论怎样加括号,运算的结果都是一样的,这给我们带来了方便.抽象代数中研究的运算都满足结合律.

交换律的一个重要作用是使等式$(ab)^n=a^nb^n$ 成立.抽象代数中研究的运算有的满足交换律,有的不满足交换律.

分配律的一个重要作用是使一个集合中的两种运算之间产生一种联系.

抽象代数在研究集合时,有时要把集合分成一些子集来讨论.这时就要用到集合的分类,而集合的分类又和"等价关系"密切相关.为了讲清"等价关系",我们先来介绍"关系"的概念.

我们知道实数集合中"大于"、"小于"、"等于"这些关系,也知道 n 阶复方阵集合中"相合"、"相似"这些关系.现在我们把它们

的本质抽象出来.

如果有一种性质 R,使集合 A 中任意两元素 a,b,或者有性质 R,或者没有性质 R,二者必居其一,我们就说"R 给定了 A 中的一个关系".当 a,b 有性质 R 时,称 a 与 b 有关系,记为 aRb;当 a,b 没有性质 R 时,称 a 与 b 没有关系,记为 $a\not Rb$.

有性质 R 的 a,b 如果记为 (a,b),就是直积 $A\times A$ 中的一个元素,全体这样的 (a,b),就构成了 $A\times A$ 的一个子集,不妨把这个子集仍记为 R,于是

$$aRb \Longleftrightarrow (a,b)\in R.$$

这样,我们就可以用 $A\times A$ 的一个子集,来刻画 A 中的一个关系.

定义 1.1.9 设 A 是一个非空集合,R 是 $A\times A$ 的一个子集,$a,b\in A$,若 $(a,b)\in R$,则称 a 与 b 有关系 R,记为 aRb,且称 R 为 A 的一个**关系(二元关系)**.在不致引起混淆时,aRb 也可记为 $a\sim b$.

例 6 实数集 $\mathbb{R}$ 中的"$\leqslant$"关系,可以用 $\mathbb{R}\times\mathbb{R}$ 中的子集 R_1(见图 1.3)来刻画;实数集 $\mathbb{R}$ 中的"$=$"关系,可以用 $\mathbb{R}\times\mathbb{R}$ 中的子集 R_2(见图 1.4)来刻画.

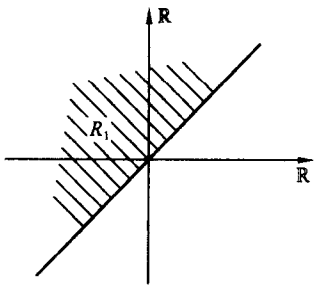


图 1.3

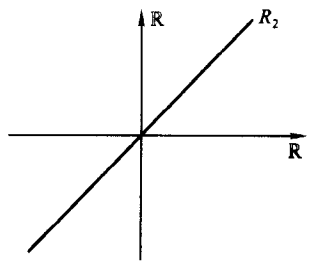


图 1.4

实数集中的"$=$"关系,可以总结推广为一般集合中的等价关系.

定义 1.1.10 若集合 A 的一个关系 R 满足

① 反身性：aRa，　$\forall a \in A$；

② 对称性：$aRb \Longrightarrow bRa$，　$\forall a, b \in A$；

③ 传递性：$aRb, bRc \Longrightarrow aRc$，　$\forall a, b, c \in A$.

则称关系 R 为 A 的一个**等价关系**.

例 7 实数集中的“$\leqslant$”关系不是等价关系，因其不满足对称性.

例 8 n 阶复方阵集合中的“相合”是等价关系，“相似”也是等价关系. 可见，同一集合中可以有多种不同的等价关系.

定义 1.1.11 若将集合 A 分成一些非空子集，每个子集称为 A 的一个类，使得 A 的每一元素属于且仅属于一个类，则称这些类的全体为集合 A 的一个**分类**，也称为 A 的一个**分划**.

A 的等价关系与 A 的分类之间有密切的联系，这由以下两个定理可以看出.

定理 1.1.1 集合 A 的一个分类决定 A 的一个等价关系.

证 我们利用 A 的分类来定义 A 的一个关系 R，然后证明 R 是等价关系. 定义：当且仅当 a 与 b 同在一类时，aRb. 据定义知这样规定的 R 是 A 的一个关系. 又因为 $a \in A$，a 与 a 同在一类，所以 R 满足反身性；$a, b \in A$，若 aRb，表明 a 与 b 同在一类，则 b 与 a 也同在一类，所以 bRa，即 R 满足对称性；$a, b, c \in A$，若 aRb, bRc，表明 a 与 b 同在一类，b 与 c 同在一类，则 a 与 c 也同在一类，所以 aRc，即 R 满足传递性. 据定义 1.1.10，R 是 A 的一个等价关系. □

在给出下一个定理之前，我们先给出由等价关系派生出来的三个概念：等价类，商集合和自然映射.

定义 1.1.12 设集合 A 中有等价关系 R，$a \in A$，则 A 中与 a 有关系（也称与 a 等价）的所有元素的集合 $\{b \in A \mid bRa\}$，称为 a 所在的**等价类**，记为 $\bar{a}$，a 称为这个等价类的**代表元**.

从以上定义及等价关系的传递性易知，若 aRb，则 $\bar{a} = \bar{b}$，即等

价的两个元素所在的等价类是同一个，因此，同一个等价类可以有不同的代表元.这使我们在讨论有关等价类的问题时，经常要注意说明，所讨论的内容虽然形式上与等价类的代表元有关，实质上却与之无关.

定义 1.1.13 设集合 A 中有等价关系 R，则以 R 为前提的所有等价类(重复的只取一个)的集合 $\{\bar{a}\}$，称为 A 对 R 的**商集合**，记为 A/R.

我们注意到，等价类 $\bar{a}$ 是 A 的子集合，却是 A/R 的元素.

一个集合通过等价关系，在新的层次上产生出与原集合有联系的新的集合——商集合，这也反映出等价关系不同于一般二元关系的重要性.

定义 1.1.14 设集合 A 中有等价关系 R，则映射 $\pi: A \to A/R$，

$$\pi(a)=\bar{a}, \quad \forall a \in A$$

称为 A 到 A/R 的**自然映射**.

自然映射一定是满射，但却不一定是单射.

定理 1.1.2 集合 A 的一个等价关系决定 A 的一个分类.

证 记 A 中的等价关系为 R，容易证明，R 决定的商集合 A/R，就是 A 的一个分类.事实上，商集合是全体等价类(重复的只取一个)的集合，每个等价类是 A 的一个子集，也是 A 的一个"类"，A 中的每一个元素 a 属于一个类 $\bar{a}$，以下证明 a 仅属于 $\bar{a}$，便完成证明.

若还有 $a \in \bar{b}$，则据定义 1.1.12，aRb，即 a 与 b 等价，而等价的两个元素所在的等价类是同一个，所以 $\bar{b}=\bar{a}$. □

定理 1.1.1 与定理 1.1.2 表明，对一个集合 A，给定等价关系与给定分类，是同一件事的两种不同的表现形式.

比等价关系更进一步的二元关系是同余关系.

定义 1.1.15 设集合 A 中有二元运算"$\circ$"，如果 A 的一个等价关系 R 在该运算下仍然保持，即

$$aRb, cRd \Longrightarrow (a\circ c)R(b\circ d), \forall a,b,c,d\in A,$$

则称 R 为 A 关于运算"$\circ$"的一个**同余关系**.此时,a 所在的等价类 $\bar{a}$,也叫作 a 的**同余类**.

例 9 设$\mathbb{Z}$为整数集,$0\neq m\in\mathbb{Z}$,在$\mathbb{Z}$中定义关系 R 为 $aRb \Longleftrightarrow m\mid(a-b)$,则 R关于$\mathbb{Z}$中的加法和乘法都是同余关系.

此例中的关系 R,也称为"以 m 为模的**模等关系**",aRb 在初等整数论中记为 $a\equiv b,(\mathrm{mod}\ m)$,称为"对模 m,a 与 b 模等"或"对模 m,a 与 b 同余".

例 10 设 $P^{n\times n}$是数域P上所有 $n(n\geqslant 2)$阶方阵的集合,在 $P^{n\times n}$中定义关系 R 为:

$$ARB \Longleftrightarrow |A| = |B|(|A|,|B|\text{为 } A、B \text{ 的行列式}),$$

则 R 关于 $P^{n\times n}$中的加法运算不是同余关系,R 关于 $P^{n\times n}$中的乘法运算是同余关系.

设 R 是集合 A 中关于运算"$\circ$"的同余关系,则因同余关系是等价关系,所以可以产生新的集合 A/R,又因同余关系在运算"$\circ$"下仍然保持,所以可以在 A/R 中产生一种与 A 中运算"$\circ$"有联系的运算"$\bar{\circ}$":

$$\bar{a}\,\bar{\circ}\,\bar{b} = \overline{(a\circ b)},\quad \forall a,b\in A.$$

要说明上面的规定确实是 A/R 中的一个二元运算,就要说明等号右边的元素,确实是被等号左边有次序的两个元素 $\bar{a}$,$\bar{b}$ 惟一确定的.即等价类的运算不仅归结为代表元的运算,而且不依赖于代表元的选择.这当且仅当该等价关系是同余关系时是正确的.我们把它的证明留作练习.作为提示,请读者重温定义 1.1.13 之前的那句话.

习 题

1. 设 $A=\{1,2,\cdots,10\}$,请构造 $A\times A$ 到 A 的映射使

(1) 该映射 f_1 是满射;

(2) 该映射 f_2 不是满射;

(3) 能否构造映射 f_3 是单射？为什么？

2. 设 $A=\{1,2,3\}$，试定义 A 中的两个不同的二元运算.

3. 设 $A=\{2n \mid n\in \mathbf{N}\}$（$\mathbf{N}$[①]是自然数集），作集合 $C\neq D$，使数的除法既是 A 与 A 到 C 的代数运算，又是 A 与 A 到 D 的代数运算.

4. 下列各关系是否为等价关系？说明理由.

(1) 在 $\mathbf{R}$ 中，$xRy \Longleftrightarrow |x-y|\leqslant 3$；

(2) 在 $\mathbf{R}$ 中，$xRy \Longleftrightarrow |x|=|y|$；

(3) 在 $\mathbf{Z}$ 中，$xRy \Longleftrightarrow x-y$ 为奇数；

(4) 在 $\mathbf{C}^{n\times n}$（n 阶复方阵集）中，$ARB \Longleftrightarrow$ 有 $P,Q\in \mathbf{C}^{n\times n}$ 使 $A=PBQ$.

5. 下列各二元运算 $*$，是否满足交换律，结合律？

(1) 在 $\mathbf{Q}$（$\mathbf{Q}$ 是有理数集）中，$a*b=ab+1$；

(2) 在 $\mathbf{Q}$ 中，$a*b=\frac{1}{2}ab$；

(3) 在 $\mathbf{N}$ 中，$a*b=2^{ab}$；

(4) 在 $\mathbf{N}$ 中，$a*b=a^b$.

6. 在 $\mathbf{Z}$ 中定义关系 R 为：$aRb \Longleftrightarrow 3|(a-b)$.

(1) 证明 R 是 $\mathbf{Z}$ 中的等价关系，写出 $\mathbf{Z}/R$ 中所有元素 $\bar{0},\bar{1},\bar{2}$ 的含义；

(2) 证明 R 关于 $\mathbf{Z}$ 中的加法是同余关系，写出在 $\mathbf{Z}/R$ 中相应产生的“加法运算”的加法表：

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$			
$\bar{1}$			
$\bar{2}$			

(3) 证明 R 关于 $\mathbf{Z}$ 中的乘法是同余关系，写出在 $\mathbf{Z}/R$ 中相应产生的“乘法运算”的乘法表：

---

① 本书中自然数集 $\mathbf{N}=\{1,2,\cdots\}$，不包括零，特此声明.

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$			
$\bar{1}$			
$\bar{2}$			

补充题

1. 设 f 是 A 到 C 的映射，g 是 B 到 D 的映射，定义 $f\times g$ 如下：

$$(f\times g)(a,b)=(f(a),g(b)),\quad \forall (a,b)\in A\times B.$$

证明：$f\times g$ 是 $A\times B$ 到 $C\times D$ 的映射，且若 f,g 均为满射(单射)时，$f\times g$ 也为满射(单射).

2. 有人说："等价关系定义中的第①条"反身性"可以取消"，因为假设 R 是非空集合 A 中的一个关系，且该关系满足对称性和传递性，则该关系一定满足反身性，证明如下："$\forall a,b\in R$，从 aRb 得 bRa，又从传递性得 aRa，这表明 R 满足反身性".他的说法对吗？为什么？

3. 设 R 是非空集合 A 中任一关系，再定义 A 中两个关系 R_1,R_2 分别为：

$$xR_1y\Longleftrightarrow \text{当 } x=y,xRy,yRx \text{ 之一成立；}$$

$$xR_2y\Longleftrightarrow \text{若有 } x_0,x_1,\cdots,x_n,\text{其中 } x=x_0,x_n=y,$$

$$\text{使 } x_0Rx_1,x_1Rx_2,\cdots,x_{n-1}Rx_n.$$

(1) R_1 是否满足对称性？是否为等价关系？说明理由；

(2) 证明：R_2 是一个等价关系；

(3) 证明：若 R 是等价关系，则 $R_2=R$，即 $xR_2y\Longleftrightarrow xRy,\forall x,y\in A$；

(4) 取 $A=\mathbf{Z}$，m 为一固定整数.取 R 为：$xRy\Longleftrightarrow x-y=m$，求关系 R_1 及 R_2.

4. 设 R 是集合 A 中的等价关系，A 中有运算"$\circ$"，在商集合 A/R 中定义"$\bar{\circ}$"如下：

$$\bar{a}\,\bar{\circ}\,\bar{b}=\overline{(a\circ b)},\quad \forall a,b\in A.$$

证明："$\bar{a}=\bar{c},\bar{b}=\bar{d}\Longrightarrow \overline{(a\circ b)}=\overline{(c\circ d)}$"的充分必要条件是：$R$ 是 A 中关于

运算"$\circ$"的同余关系.(这也就表明,当且仅当 R 是同余关系时,等价类的运算"$\bar{\circ}$"才不依赖于代表元的选择.)

§1.2 半群与群

抽象代数是从抽象的观点研究代数体系的,本节介绍一种重要的代数体系——群.先介绍比群简单的一种代数体系——半群.

一个代数体系首先是一个集合,其次,这个集合中定义有运算(一种或多种运算),再其次,运算满足某些规律.代数体系可以是千差万别的,我们有必要把具有某些共同特点的代数体系集中起来,统一研究,寻找它们的共同规律.半群和群的概念就是这样产生的.

定义 1.2.1 设非空集合 S 中有一个二元运算"$\circ$",且该运算满足结合律,则称代数体系 $\{S;\circ\}$ 是一个**半群**,也简称 S 是一个半群.

若半群 $\{S;\circ\}$ 中存在一个元素 $e_1(e_2)$,使

$$e_1\circ a=a(a\circ e_2=a),\quad \forall a\in S.$$

则称 $e_1(e_2)$ 为 S 的**左(右)幺元**.若 $e\in S$,既是 S 的左幺元,又是 S 的右幺元,则称 e 为 S 的**幺元**,也称为**单位元**.有幺元的半群称为**幺半群**.

例 1 设N是自然数集,则 $\{\mathbb{N};\cdot\}$ 是幺半群,幺元是数 1.$\{\mathbb{N};+\}$ 是半群,但不是幺半群,因为 $0\notin\mathbb{N}$.也可说成,自然数集对于数的乘法构成幺半群;自然数集对于数的加法构成半群,但不构成幺半群.

例 2 记 $M(A)$ 为非空集合 A 的所有变换(到自身的映射称为变换)的集合,则 $\{M(A);\cdot\}$ 是幺半群,恒等变换 id_A 是幺元,这里"$\cdot$"表示映射的乘法运算.

例 3 记非空集合 A 的所有子集的集合为 $P(A)$,称为 A 的幂集,则 $\{P(A);\cup\}$ 是幺半群,幺元是空集 $\varnothing$;$\{P(A);\cap\}$ 也是幺

半群，幺元是 A. 这里“$\cup$”，“$\cap$”分别表示集合求并与求交的运算. 这是两个不同的幺半群，虽然集合是同一个集合 $P(A)$.

命题 1.2.1 幺半群中的幺元是惟一的.

证 若 e 与 e' 均是幺元，则 $e'=e'e=e$. □

定义 1.2.2 设 $\{S;\circ\}$ 是幺半群，e 是幺元，$a\in S$，若 $a_1(a_2)\in S$，使 $a_1a=e(aa_2=e)$，则称 $a_1(a_2)$ 为 a 的**左(右)逆元**. 若 b 既是 a 的左逆元，又是 a 的右逆元，即有 $ba=ab=e$，则称 b 为 a 的**逆元**，记为 $b=a^{-1}$，称 a 为**可逆元**.

定义 1.2.3 一个幺半群 $\{G;\circ\}$ 中如果每一个元都是可逆元，则 G 就称为**群**. 若运算“$\circ$”还满足交换律，则 G 就称为**交换群，或阿贝尔(Abel)群**.

通常为应用上的方便，不借助于“幺半群”的概念直接定义“群”，则可以说，群是一个集合 G，且关于 G 中运算“$\circ$”满足以下四个条件：

① $\forall a,b\in G$，有 $a\circ b\in G$，即运算“$\circ$”对 G 是封闭的；

② $\forall a,b,c\in G$，有 $(a\circ b)\circ c=a\circ(b\circ c)$，即运算“$\circ$”满足结合律；

③ 存在 $e\in G$，使 $\forall a\in G$，有 $e\circ a=a\circ e=a$，即 G 中存在幺元；

④ $\forall a\in G$，$\exists b\in G$，使 $b\circ a=a\circ b=e$，即 G 中任意元为可逆元.

事实上，后两个条件③，④还可以简化为

③′ 存在 $e\in G$，使 $\forall a\in G$，有 $e\circ a=a$，即 G 中存在左幺元；

④′ $\forall a\in G$，$\exists b\in G$，使 $b\circ a=e$，即 G 中任意元都存在左逆元.

简化条件后群的定义与原来定义的等价性的证明给读者留作练习. 而这表明，群 G 中的左幺元就是右幺元，G 中任一元 a 的左逆元就是 a 的右逆元.

从上面看出，“群”是一个“有结构的集合”，请认真体会这一重

要的“代数体系”.“群”的概念,也可以由朴素的“对称”概念产生.例如,说正方形有“对称性”,可以看成是在平面的某些“旋转”和某些“反射”下,正方形整体保持“不变”;而所有使正方形保持“不变”的平面变换,对于变换的乘法就构成一个群.请读者自己验证这一命题.搞清群与对称的联系,对于群的学习会有很大帮助.

例 4 整数集$\mathbb{Z}$,有理数集$\mathbb{Q}$,实数集$\mathbb{R}$,复数集$\mathbb{C}$,对于数的加法运算都构成群.

例 5 非零实数集$\mathbb{R}^*$,对于数的乘法构成群.

例 6 记S_A为非空集合A的所有可逆变换的集合,则$\{S_A;\cdot\}$是群,这里“$\cdot$”表示映射的乘法运算.这个群称为A的**全变换群**.恒等变换是它的幺元.

例 7 $\{1,-1\}$对于数的乘法构成群.

至此,我们对群的认识是:群不仅是一个集合,更重要的是,它是带有某种运算的集合,这种运算还满足某些条件.下边我们来推导群的一些基本性质.我们不妨把群中的运算称作乘法,并把运算符号省去,记$a\circ b$为ab.

命题 1.2.2 群G的运算满足**左(右)消去律**.即

$$\forall a,b,c\in G,ab=ac(ba=ca)\Longrightarrow b=c.$$

证 我们只证左消去律成立.因G是群,故$a^{-1}\in G$,用a^{-1}左乘式$ab=ac$的两边得

$$a^{-1}(ab)=a^{-1}(ac),$$

再根据结合律有$(a^{-1}a)b=(a^{-1}a)c$,即$eb=ec$,再由幺元的定义得$b=c$. □

命题 1.2.3 群G中任一元a的逆元是惟一的.

证 若b与b'均为a的逆元,便有$ba=e=b'a$,据右消去律得$b=b'$. □

命题 1.2.4 在群G中,$\forall a,b\in G$,方程$ax=b$及$xa=b$的解均存在且惟一.

证 只对$ax=b$证明.因G是群,故$a^{-1}\in G$,又因群中运算

封闭，$a^{-1}b \in G$，代入验证即知 $a^{-1}b$ 是 $ax = b$ 的一个解，又若 x_1, x_2 均是 $ax = b$ 的解，即有 $ax_1 = b$ 和 $ax_2 = b$，故 $ax_1 = ax_2$，由群中消去律成立知 $x_1 = x_2$. □

命题 1.2.5 若半群 G 满足：$\forall a, b \in G$，方程 $ax = b$，$xa = b$ 均有解，则 G 是群.

证 我们利用定义 1.2.3 中关于群的定义的四个条件①，②，③′，④′来完成证明. 由于 G 是半群，所以①，②已成立. 因 $xa = a$ 在 G 中有解，记一个解为 e_a，即有 $e_a a = a$. 下证 e_a 是 G 的左幺元. $\forall c \in G$，因 $ax = c$ 在 G 中有解，记为 d，即有 $ad = c$，所以 $e_a c = e_a ad = (e_a a)d = ad = c$，故 e_a 是 G 的左幺元. ③′已成立. 又 $\forall a \in G$，$xa = e_a$ 在 G 中有解，解就是 a 的左逆元，故④′成立. □

定理 1.2.6 有限半群 G 若满足左、右消去律，则 G 是群.

证 因 G 有限，可设 $G = \{a_1, \cdots, a_n\}$，$\forall a, b \in G$，我们证明方程 $ax = b$，$xa = b$ 均有解，从而据上一命题完成证明.

因半群对运算封闭，故 $aa_1, \cdots, aa_n \in G$. 我们断言，$aa_1, \cdots, aa_n$ 必两两不等，从而就是 $a_1, \cdots, a_n$ 的一个排列. 因若不然，不妨设 $aa_1 = aa_2$，则据左消去律有 $a_1 = a_2$，矛盾.

既然 $aa_1, \cdots, aa_n$ 是 $a_1, \cdots, a_n$ 的一个排列，而 $b \in G$，故必有一个 $aa_i = b$，$1 \leqslant i \leqslant n$，于是 a_i 就是方程 $ax = b$ 的解. 同理可证方程 $xa = b$ 有解. □

由于群 G 中任一元 a 有逆元 a^{-1}，所以我们不仅可以规定 a 的正整数次幂，也可以规定 a 的负整数次幂和 a 的零次幂.

定义 1.2.4 设 G 为群，n 为正整数，$\forall a \in G$，规定

$$a^n = \overbrace{aa\cdots a}^{n\text{个}};$$

$$a^{-n} = (a^{-1})^n;$$

$$a^0 = e.$$

由此可得对任意整数 m, n，有 $a^m a^n = a^{m+n}$，$(a^m)^n = a^{mn}$.

若 G 是交换群，还有 $(ab)^m = a^m b^m$.

当 G 是交换群时，我们有时把运算记为加法，这时的幺元常称为零元，记为 0，$a \in G$ 的逆元常称为 a 的负元，记为 $-a$，对于加法群 G，乘法群中 a 的 n 次幂相当于 a 的 n 倍，与定义 1.2.4 相应地，有

定义 1.2.5 设 G 为加法群，n 为正整数，$\forall a \in G$，规定

$$na = \overbrace{a + a + \cdots + a}^{n\text{个}};$$

$$(-n)a = n(-a);$$

$$0a = 0.$$

注意最后一式等号左边的 0 是整数 0，等号右边的 0 是 G 中的零元.

由此可得，对于任意整数 m，n，及任意 a，$b \in G$ 有 $ma + na = (m+n)a$，$m(na) = (mn)a$，$m(a+b) = ma + mb$.

下边我们给出群的阶和群中元素的阶的概念，以及相关的一些基本性质.

定义 1.2.6 群 G 中所含元素的个数 $|G|$，称为**群 G 的阶**. 若 $|G|$ 有限，则称 G 为**有限群**，若 $|G|$ 无限，则称 G 为**无限群**.

例 4，例 5 中的群是无限群，例 7 中的群是有限群.

对于有限群，我们可以用所谓"**群表**"来给出. 给出一个群，就是给出这个群中的所有元素以及所有元素的运算结果. 对于有限群来说，这两个任务，群表都能完成.

例 7 中的群，群表如右：

	1	−1
1	1	−1
−1	−1	1

当群表关于自左上至右下的对角线对称时，该群是交换群. 例

7 中的群就是交换群.

定义 1.2.7 设 G 是群,运算记为乘法(加法),a 是 G 中一个元素.如果 $\forall k\in\mathbf{N}$,有 $a^k\neq e(ka\neq 0)$,则称**元素 a 的阶为无穷**.如果 $\exists k\in\mathbf{N}$,使 $a^k=e(ka=0)$,则称 $\min\{k\in\mathbf{N}\mid a^k=e(ka=0)\}$ 为 a 的**阶**.

由此定义易知,任一个乘法群 G 中,幺元的阶为 1,且只有幺元的阶为 1;G 中任一元 a 与其逆元 a^{-1} 有相同的阶.下边的命题给出了群中元素的阶的其他一些性质.

命题 1.2.7 设 a 是群 G 中一元,则

a 的阶是无穷$\Longleftrightarrow\forall m\neq n,m,n\in\mathbf{Z}$,有 $a^m\neq a^n$.

证 "$\Longrightarrow$"若不然,有 $m_0\neq n_0,m_0,n_0\in\mathbf{Z}$,使 $a^{m_0}=a^{n_0}$,不妨设 $m_0>n_0$.用 a^{-n_0} 右乘等号两边,得 $a^{m_0-n_0}=e,m_0-n_0\in\mathbf{N}$,这与"$a$ 的阶是无穷"矛盾.

"$\Longleftarrow$"$\forall m\in\mathbf{N}$,取 $n=0$,则 $m\neq n$,于是 $a^m\neq a^n=e$,由定义 1.2.7 知,a 的阶是无穷. □

命题 1.2.8 设 a 是群 G 中一元,a 的阶为 d,则

① $\forall h\in\mathbf{Z}$,有 $a^h=e\Longleftrightarrow d\mid h$,

② $\forall m,n\in\mathbf{Z}$,有 $a^m=a^n\Longleftrightarrow d\mid(m-n)\Longleftrightarrow m\equiv n\pmod d$.

证 ① "$\Longleftarrow$":设 $h=qd$,则 $a^h=a^{qd}=(a^d)^q=e^q=e$.

"$\Longrightarrow$":反设 $d\nmid h$,则由带余除法得 $h=qd+r,0<r<d$ 及 $a^{qd+r}=e$,故 $(a^d)^qa^r=e$,故 $a^r=e$,而 $0<r<d$.这与"a 的阶为 d"矛盾.

② $a^m=a^n$ 就是 $a^{m-n}=e$,由①立即得证. □

命题 1.2.9 设 a 是群 G 中一元,a 的阶为 $d,k\in\mathbf{N}$,则

① a^k 的阶为 $d/(d,k)$,这里 (d,k) 是 d,k 的最大公因数;

② a^k 的阶为 $d\Longleftrightarrow(d,k)=1$.

证 ① 记 a^k 的阶为 q,证 $q=d/(d,k)$.

设 $d=(d,k)d_1,k=(d,k)k_1$,则 $(d_1,k_1)=1$.我们依据"两

个自然数若互相整除则相等”去证 $q=d_1$，从而完成证明.

因 a^k 的阶为 q，$(a^k)^q=e$，即 $a^{kq}=e$，据命题 1.2.8①知 $d\mid kq$，即 $(d,k)d_1\mid(d,k)k_1q$，亦即 $d_1\mid k_1q$，又因 $(d_1,k_1)=1$，故 $d_1\mid q$.

另一方面，$(a^k)^{d_1}=a^{(d,k)k_1d_1}=(a^d)^{k_1}=e^{k_1}=e$，而 a^k 的阶为 q，据命题 1.2.8①，$q\mid d_1$，所以 $q=d_1$.

② 这是①的直接推论. □

命题 1.2.10 设 a,b 是群 G 中的元素，a 的阶为 m，b 的阶为 n，$ab=ba$，$(m,n)=1$，则 ab 的阶为 mn.

证 记 ab 的阶为 q，去证 $q=mn$.

因 $ab=ba$，故 $(ab)^{mn}=a^{mn}b^{mn}=(a^m)^n(b^n)^m=e^ne^m=e$，据命题 1.2.8①知 $q\mid mn$.

又 $(ab)^{qm}=a^{qm}b^{qm}=(a^m)^q(b^{qm})=b^{qm}$，而 $(ab)^{qm}=((ab)^q)^m=e^m=e$，于是 $b^{qm}=e$，再据命题 1.2.8①知 $n\mid qm$. 又因 $(m,n)=1$，故 $n\mid q$.

同理可得 $m\mid q$. 再由 $(m,n)=1$，知 $mn\mid q$. 所以 $q=mn$.

□

习 题

1. 下列各集合中所给的 $*$ 是否是二元运算？若是，问该集合关于该运算，是否是半群，幺半群，群？

(1) $\mathbf{Z}$ 中，$a*b=a-b$；

(2) $\mathbf{Z}$ 中，$a*b=a+b-ab$；

(3) $\mathbf{Q}-\{0,1\}$ 中，$a*b=ab$；

(4) $\mathbf{C}_{n\times n}$ 中，$\boldsymbol{A}*\boldsymbol{B}=\boldsymbol{A}+\boldsymbol{B}$；

(5) $\mathbf{C}_{n\times n}$ 中，$\boldsymbol{A}*\boldsymbol{B}=\boldsymbol{AB}$；

(6) $M=\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}1&0\\0&-1\end{pmatrix},\begin{pmatrix}-1&0\\0&1\end{pmatrix},\begin{pmatrix}-1&0\\0&-1\end{pmatrix}\right\}$ 中，$\boldsymbol{A}*\boldsymbol{B}=\boldsymbol{AB}$.

2. 任给你一个有两个元素的集合 $G=\{a,b\}$，请你在 G 中定义一种二

元运算 $*$，使 $|G;*|$ 是群.

3. 设群 G 中每个非幺元的阶都是 2，证明 G 为 Abel 群.

4. 定理 1.2.6 对无限半群是否成立？说明理由.

5. 设 G 是有限群，k 是大于 2 的整数，证明：G 中阶为 k 的元的个数一定是偶数.

6. 设 m 是自然数，$\mathbf{Z}_m$ 表示集合 $|0,1,2,\cdots,m-1|$，在 $\mathbf{Z}_m$ 中定义 $*$ 如下：

$$a * b = ab/m \text{ 所得的余数}.$$

(1) 证明：$*$ 是 $\mathbf{Z}_m$ 中的二元运算；

(2) 证明 $|\mathbf{Z}_m;*|$ 是交换幺半群；

(3) 构造 $|\mathbf{Z}_4;*|$ 的半群表.

7. 设 F 是平面上的一个图形. 令 G_F 为全体保持 F 不变的(从整体上不变)平面正交变换所成的集合. 证明：

(1) G_F 关于变换的乘法构成一个群，它称为图形 F 的对称群；

(2) 设 F 是如图 1.5 所示的正方形 $ABCD$，请列出 G_F 中的所有元素.

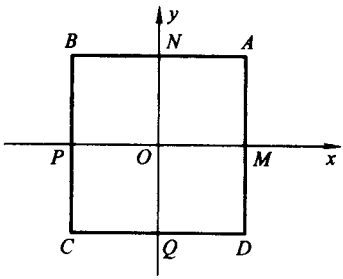


图 1.5

8. 设 G 是乘法群，$a,b \in G$，证明：

(1) a 与 a^{-1} 有相同的阶；

(2) a 与 bab^{-1} 有相同的阶；

(3) ab 与 ba 有相同的阶.

补充题

1. 证明下边关于“群”的定义，与定义 1.2.3 是等价的.

定义：设 G 是一个非空集合，且关于其中的运算“$\circ$”满足以下四个条件，则称 $|G;\circ|$ 是一个群：

(1) “$\circ$”对 G 是封闭的；

(2) “$\circ$”满足结合律；

(3) G 中对“$\circ$”存在左幺元；

(4) G 中任一元对“$\circ$”存在左逆元.

2. 如果在半群 G 中再定义一种“一元运算”(即 G 到 G 的一个映射 $a \mapsto a'$),且满足:

$$a'(ab) = b = (ba)a', \forall a, b \in G,$$

证明:此半群 G 必为群.

3. 如果半群 $\{G;\cdot\}$ 有左幺元 e,又 $\forall a \in G$,a 有右逆元(即有 $a' \in G$,使 $aa' = e$),问 $\{G;\cdot\}$ 一定是群吗? 为什么?

4. 判断以下两命题是否正确,并详细说明理由.

(1) 有限群 G 中任一元的阶都是有限的;

(2) 一个群 G 中,如果任一元的阶都是有限的,则 G 是有限群.

5. 设 a, b 是群 G 中的 m 阶元和 n 阶元,且 $ab = ba$,证明:G 中存在 $[m, n]$ 阶元.($[m, n]$ 表示 m, n 的最小公倍数)

§1.3 子群与商群

抽象代数研究代数体系,常常通过子体系与商体系去研究,它们是子集合与商集合的推广,对群来说,就是子群与商群.

定义 1.3.1 设 H 是群 G 的一个非空子集,如果 H 对于 G 的运算也构成群,则称 H 为 G 的一个**子群**,记作 $H < G$.

子群的运算与原群的运算一致,这一点是重要的.因此,子群 H 的幺元就是原群 G 的幺元 e,子群 H 中任一元 a 的逆元就是在 G 中 a 的逆元 a^{-1}.

对任一群 G,$H = \{e\}$ 与 $H = G$ 都是 G 的子群,它们称为 G 的**平凡子群**,G 的其他子群称为**非平凡子群**.

例 1 $\{\mathbb{R}_+;\cdot\} < \{\mathbb{R}^*;\cdot\}$,这里 $\mathbb{R}_+$ 表示全体正实数.

$\{\{1, -1\};\cdot\} < \{\mathbb{R}^*;\cdot\}$.

$\{\mathbb{R}_+;\cdot\}$ 不是 $\{\mathbb{R};+\}$ 的子群,虽然 $\mathbb{R}_+$ 是 $\mathbb{R}$ 的子集合.

例 2 设 V 是数域 $\mathbb{P}$ 上的 n 维线性空间,S_V 为 V 上的全体可逆变换,由 §1.2 例 6 知 $\{S_V;\cdot\}$ 是群.现再以 $GL(V)$ 表示 V 上全体可逆线性变换的集合,以 $SL(V)$ 表示 V 上全体行列式为 1 的线性变换的集合,则 $GL(V) < S_V$,$SL(V) < S_V$,$SL(V) < GL(V)$.

我们称$GL(V)$为 V 的**一般线性群**，称 $SL(V)$为 V 的**特殊线性群**.

由于在 n 维线性空间中取定一组基后，V 上的线性变换与 P 上的 n 阶方阵之间就建立了一一对应的关系，所以，也常用 $GL_n(\mathbb{R})$表示 n 阶实可逆方阵的集合关于矩阵乘法构成的群，称为一般实线性群，用 $SL_n(\mathbb{R})$表示行列式为 1 的 n 阶实方阵关于矩阵乘法构成的群，称为特殊实线性群. 于是也有 $SL_n(\mathbb{R}) < GL_n(\mathbb{R})$.

例 3 设 $m \in \mathbb{Z}$，则 $m\mathbb{Z} = \{mn \mid n \in \mathbb{Z}\}$是整数加群$\mathbb{Z}$的子群.

上边各例都是用定义 1.3.1 去判断一个群的子集是否是子群，下边的定理提供了判断子群的稍为简便一些的方法.

定理 1.3.1 设 H 是群 G 的非空子集，则下面的条件是等价的：

① $H < G$；

② $a, b \in H \Longrightarrow ab \in H, a^{-1} \in H$；

③ $a, b \in H \Longrightarrow ab^{-1} \in H$.

证 ①$\Longrightarrow$②：因 H 是群，对运算封闭，故 $ab \in H$，H 中任一元 a 的逆元也在 H 中. 又因 H 是 G 的子群，两者的运算是一致的，故 a 在 H 中的逆元就是 a 在 G 中的逆元 a^{-1}，所以 $a^{-1} \in H$.

②$\Longrightarrow$③：据②有 $b \in H \Longrightarrow b^{-1} \in H$，又有 $a, b^{-1} \in H \Longrightarrow ab^{-1} \in H$. 故③成立.

③$\Longrightarrow$①：已知 H 是群 G 的一个非空子集，下边我们从③按定义 1.3.1 去证明 $H < G$. 即验证 H 对于 G 的运算也构成群. 因 H 非空，故 H 中至少有元素 a，而由③，$a, a \in H \Longrightarrow aa^{-1} \in H$，即 $e \in H$，从而 H 中有幺元. 又 $\forall b \in H$，由③，$e, b \in H \Longrightarrow eb^{-1} \in H$，即 $b^{-1} \in H$，即 H 中任一元有逆元. 又 $\forall a, b \in H$，由③，$a, b^{-1} \in H \Longrightarrow a(b^{-1})^{-1} \in H$，即 $ab \in H$，故 H 对运算封闭. 又 $H \subseteq G$，而 G 是群，运算满足结合律，所以其子集 H 中元素的运算

也满足结合律.由以上四点据定义 1.2.3 知,H 对于 G 的运算构成群. □

今后,常常用定理中的③去验证非空子集 H 是群 G 的子群.要注意的是,如果运算记作加法,则③中的 $ab^{-1}\in H$,应改为 $a+(-b)\in H$ 或 $a-b\in H$.

若子集 H 是有限的,则可有更简单的方法验证 H 是群 G 的子群.

命题 1.3.2 设 H 为群 G 的非空有限子集,则

$H<G\Longleftrightarrow H$ 对 G 中的运算封闭.

证 "$\Longrightarrow$":据定义 1.3.1 立得.

"$\Longleftarrow$":因 G 是群,故 G 中的运算满足结合律和左、右消去律.从而其子集 H 中的元素对于 G 中的运算也满足结合律和左、右消去律.现 H 对 G 中的运算封闭,于是 H 对 G 中的运算构成有限半群,又满足左、右消去律.据定理 1.2.6,H 对 G 中的运算是群,即 $H<G$. □

命题 1.3.3 若 H_1,H_2 均是群 G 的子群,则 $H_1\cap H_2<G$.

证 因 $e\in H_1\cap H_2$,故 $H_1\cap H_2$ 是 G 的非空子集.$\forall\, a,b\in H_1\cap H_2$,则有 $a,b\in H_1$ 和 $a,b\in H_2$,因 $H_1<G$ 和 $H_2<G$,据定理 1.3.1 有 $ab^{-1}\in H_1$ 和 $ab^{-1}\in H_2$,从而有 $ab^{-1}\in H_1\cap H_2$,再据定理 1.3.1 知 $H_1\cap H_2<G$. □

用同样的方法可以证明,群 G 的任意多个(可以是无穷多个)子群的交仍是子群.

为了给讨论商群作准备,我们先介绍群中子群的左陪集和右陪集的概念.

定义 1.3.2 设 H 是群 G 的一个子群,$a\in G$,则

$$aH=\{ah\mid h\in H\},\ Ha=\{ha\mid h\in H\}$$

分别称为以 a 为代表的 H 的**左陪集**,**右陪集**.

关于右陪集的讨论与关于左陪集的讨论是类似的,下边我们

主要讨论左陪集.

定理 1.3.4 设 H 是群 G 的子群,则由

$$aRb \Longleftrightarrow a^{-1}b \in H$$

所确定的 G 中的关系 R 是一个等价关系,且 a 所在的等价类 $\bar{a}$ 恰为以 a 为代表的 H 的左陪集 aH. 故 H 的全体左陪集(重复的只取一个)的集合 $\{aH\}$ 是 G 的一个分类.

证 首先证明 R 是等价关系. 给定 G 中的 a 和 b 后,我们可以惟一地确定 $a^{-1}b$ 属于 H,所以 R 是 G 中的一个关系.

$\forall a \in G, a^{-1}a = e \in H$,故 aRa. 即 R 满足反身性. 又若 aRb,即 $a^{-1}b \in H$,因 H 是群,故 $(a^{-1}b)^{-1} \in H$,即 $b^{-1}a \in H$,故 bRa,即 R 满足对称性. 又若 aRb, bRc,则 $a^{-1}b \in H, b^{-1}c \in H$,因 H 是群,$(a^{-1}b)(b^{-1}c) \in H$,即 $a^{-1}c \in H$,所以 aRc,故 R 满足传递性. 据定义 1.1.10,R 是 G 中的一个等价关系.

再证明 $\forall a \in G, \bar{a} = aH$. $\forall b \in \bar{a}$,有 aRb,故 $a^{-1}b \in H$,即有 $h \in H$,使 $a^{-1}b = h$,即 $b = ah \in aH$,故 $\bar{a} \subseteq aH$,又 $\forall b \in aH$,即有 $h \in H$,使 $b = ah$,故 $a^{-1}b = h \in H$,即 $b \in \bar{a}$,故 $aH \subseteq \bar{a}$. 于是 $\bar{a} = aH$.

据定理 1.1.2 知,上述等价关系决定集合 G 的一个分类,每一个类就是该等价关系下的一个等价类 a,现 $\bar{a} = aH$,故 $\{aH\}$ 是 G 的一个分类. □

推论 1.3.5 设 H 是群 G 的子群,$a, b \in G$,则 $aH = bH \Longleftrightarrow a^{-1}b \in H$.

定义 1.3.3 设 H 为群 G 的子群,G 关于等价关系"$aRb \Longleftrightarrow a^{-1}b \in H$"的商集合 G/R 称为 G 对 H 的**左商集**,也称为 G 对 H 的**左陪集空间**,也记为 G/H.

G/H 的基数 $|G/H|$ 称为 H **在** G **中的指数**,记为 $[G:H]$.

应该注意的是,以上叙述中都把群 G 中的运算记作乘法,并且省去了运算符. 如果群 G 中的运算记作加法,则以 a 为代表的 H 的左陪集应该记作 $a + H = \{a + h \mid h \in H\}$,导出 G 对 H 的左陪集空

间的关系应记作“$aRb \Longleftrightarrow b-a\in H$”.

例 4 $[\mathbf{Z}:m\mathbf{Z}]=m$,这里 $m\in\mathbf{N}$.

由例 3 知,$m\mathbf{Z}<\mathbf{Z}$.于是可以考虑$\mathbf{Z}$对 $m\mathbf{Z}$ 的左陪集空间.我们有

$$\begin{aligned}\mathbf{Z}&=(0+m\mathbf{Z})\cup(1+m\mathbf{Z})\cup\cdots\cup((m-1)+m\mathbf{Z})\\&=\bar{0}\cup\bar{1}\cup\cdots\cup\overline{(m-1)}.\end{aligned}$$

上述第一个等式把整数加群$\mathbf{Z}$表成了 m 个左陪集的并,第二个等式则把$\mathbf{Z}$表成了 m 个等价类的并.故$[\mathbf{Z}:m\mathbf{Z}]=m$.

定理 1.3.6(Lagrange 定理) 设 G 是有限群,$H<G$,则有

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

从而子群 H 的阶是群G 的阶的因子.

证 首先,H 的任一左陪集 aH 中的元素个数,都等于 H 中的元素个数$|H|$.事实上,

$$\phi:h\to ah,\ \forall\, h\in H$$

是 H 到aH 的双射.

其次,根据定理 1.3.4,G 可以表为H 的全体不相交的左陪集的并,再据定义 1.3.3,这些左陪集的个数是$[G:H]$,从而 G 中有$[G:H]\cdot|H|$个元素,即$|G|=[G:H]\cdot|H|$. □

推论 1.3.7 设 G 是有限群,$K<G$,$H<K$,则有

$$[G:H]=[G:K]\cdot[K:H].$$

证 据定理 1.3.6 有

$$|G|=[G:K]\cdot|K|=[G:K]\cdot[K:H]\cdot|H|,$$
$$|G|=[G:H]\cdot|H|.$$

于是

$$[G:H]\cdot|H|=[G:K]\cdot[K:H]\cdot|H|.$$

约去等号两边的$|H|$,便完成证明. □

过去我们从“群是有结构的集合”自然想到,群 G 的子群个数比子集个数会少得多;现在我们知道,群 G 的子群的阶是$|G|$的因子,而子集则没有这一要求,所以又一次看出,子群的数目比子

集少得多.

从左、右陪集的定义知道,一般地,没有

$$aH = Ha, \forall a \in G.$$

如果群 G 的某个子群 H 有上述性质,则将连带产生许多很好的性质,并可由此导出商群的概念.具有这种性质的子群 H,我们将称为 G 的正规子群.但是,我们更愿意用另一种形式来定义"正规子群",因为它比较容易用来检验 G 的一个子群 H 是不是正规子群.

定义 1.3.4 设 G 是群,$H < G$,如果有

$$ghg^{-1} \in H, \forall g \in G, \forall h \in H,$$

则称 H 为 G 的一个**正规子群**,记为 $H \lhd G$.

例 5 平凡子群均是正规子群.

例 6 可换群的任何子群都是正规子群.

例 7 $SL(V) \lhd GL(V)$.

下边的定理给出正规子群的几个充要条件,也说明了正规子群的形式上不同的定义的等价性.

定理 1.3.8 设 G 是群,$H < G$,则下边的条件是等价的:

① $H \lhd G$;

② $gH = Hg, \forall g \in G$;

③ $g_1 H \cdot g_2 H = g_1 g_2 H, \forall g_1, g_2 \in G$.

这里 $g_1 H \cdot g_2 H = \{g_1 h_1 g_2 h_2 \mid h_1, h_2 \in H\}$.

证 ①$\Longrightarrow$②:因 $H \lhd G$,故 $\forall g \in G, \forall h \in H$,有

$$gh = ghg^{-1}g \in Hg; \quad hg = gg^{-1}hg \in gH.$$

故 $gH = Hg$.

②$\Longrightarrow$③:$\forall g_1, g_2 \in G$,考虑 $g_1 H \cdot g_2 H$ 中的任一元素 $g_1 h_1 g_2 h_2, h_1, h_2 \in H$,由②有 $h_1 g_2 \in Hg_2 = g_2 H$,故有 $h_3 \in H$,使 $h_1 g_2 = g_2 h_3$.故 $g_1 h_1 g_2 h_2 = g_1 g_2 h_3 h_2 \in g_1 g_2 H$,从而 $g_1 H \cdot g_2 H \subseteq g_1 g_2 H$.

又 g_1g_2H 的任一元 $g_1g_2h = g_1eg_2h \in g_1H \cdot g_2H$，从而 $g_1g_2H \subseteq g_1H \cdot g_2H$. 故 $g_1H \cdot g_2H = g_1g_2H$, $\forall g_1, g_2 \in G$.

③$\Longrightarrow$①：已知 $H < G$，现 $\forall g \in G$, $\forall h \in H$，由③有

$$ghg^{-1} = ghg^{-1}e \in gH \cdot g^{-1}H = gg^{-1}H = eH = H,$$

据定义 1.3.4 知 $H \lhd G$. □

一般地，子群 H 的两个左陪集的乘积不一定仍是左陪集，但由定理 1.3.8 知，当 H 是 G 的正规子群时，两个左陪集的乘积一定是左陪集，并且乘积的代表元就是原来两个左陪集代表元的乘积.

定理 1.3.9 设 G 是群，$H < G$，R 是 G 中由"$aRb \Longleftrightarrow a^{-1}b \in H$"定义的关系，则

$$R \text{ 是 } G \text{ 中的同余关系} \Longleftrightarrow H \lhd G.$$

此时，商集合 G/R 对同余关系 R 导出的运算也构成一个群，称为 G 对 H 的**商群**，记为 G/H.

证 "$\Longleftarrow$"：定理 1.3.4 已经告诉我们，上述 R 是 G 中的一个等价关系. 现设 a_1Rb_1, a_2Rb_2，去证 $a_1a_2Rb_1b_2$. 即要证 $(a_1a_2)^{-1}(b_1b_2) \in H$，因

$$(a_1a_2)^{-1}(b_1b_2) = a_2^{-1}(a_1^{-1}b_1)a_2a_2^{-1}b_2,$$

而 $a_1^{-1}b_1 \in H$, $a_2^{-1}b_2 \in H$ 及由 $H \lhd G$ 知 $a_2^{-1}(a_1^{-1}b_1)a_2 \in H$，故 $(a_1a_2)^{-1}(b_1b_2) \in H$. 据定义 1.1.15 知，$R$ 关于群 G 中的运算是同余关系.

"$\Longrightarrow$"：现设 R 是 G 中的同余关系，去证 $H \lhd G$. 已知 $H < G$，下面 $\forall g \in G$, $\forall h \in H$，证明 $ghg^{-1} \in H$. 因为 $g^{-1}(gh) = h \in H$. 故 $gR(gh)$. 又有 $g^{-1}Rg^{-1}$. 再据 R 是 G 中的同余关系知，$gg^{-1}R(gh)g^{-1}$，即 $eRghg^{-1}$，按 R 的定义，$e^{-1}ghg^{-1} \in H$，这就是 $ghg^{-1} \in H$. □

事实上，这充要条件也可从 §1.1 最后两个自然段关于同余关系导出商集合中的一个运算，以及定理 1.3.8 中①$\Longleftrightarrow$③，很简

单地得出来.

此时,§1.1 中的

$$\bar{a} \circ \bar{b} = \overline{(a \circ b)}, \forall a, b \in A.$$

就是

$$aH \cdot bH = (a \cdot b)H, \forall a, b \in G,$$

即 $\forall aH, bH \in G/R, aH \cdot bH = (a \cdot b)H$. 从而这就是在左陪集空间(左商集)中定义的二元运算.

这一运算满足结合律,因为 $\forall aH, bH, cH \in G/R$,有

$$(aH \cdot bH) \cdot cH = abH \cdot cH = (abc)H = aH \cdot (bc)H = aH \cdot (bH \cdot cH).$$

这一运算有左幺元 eH,因为 $\forall aH \in G/R$,有

$$eH \cdot aH = (ea)H = aH.$$

G/R 中任一元 aH 有左逆元 $a^{-1}H$,因为

$$a^{-1}H \cdot aH = (a^{-1}a)H = eH.$$

所以商集合 G/R 对于同余关系 R 导出的运算也构成一个群,我们称之为 G 对 H 的商群,记为 G/H. 商群中的幺元 eH 常常简记为 H.

要注意的是,只有对 G 中的正规子群 H,才能谈论商群,对一般的子群是不能谈商群而只能谈左陪集空间(左商集).

例 8 由于平凡子群都是正规子群,故有商群 $G/\{e\}$ 和 G/G,事实上,$G/\{e\}$ 的结构与 G 是一样的,而 G/G 中只有一个元素 e.

例 9 由于整数加群 $\{\mathbf{Z}; +\}$ 是可换群,故其任一子群 $m\mathbf{Z}$ 是 $\mathbf{Z}$ 的正规子群,所以有商群 $\mathbf{Z}/m\mathbf{Z}$. 据例 4 知

$$\mathbf{Z}/m\mathbf{Z} = \{\bar{0}, \bar{1}, \cdots, \overline{(m-1)}\}.$$

注意到 $\mathbf{Z}$ 中的运算是加法,所以商群中的运算通常仍记为加法,于是 $\bar{r}_1 + \bar{r}_2 = \overline{(r_1 + r_2)} = \bar{r}$,其中 r 是这样得到的:$r_1 + r_2 = qm + r, 0 \leqslant r < m$. 这个群通常简记为 $\mathbf{Z}_m$,称为模 m 的**剩余类加群**.

习 题

1. 举出乘法群 $GL_2(\mathbb{R})=\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\mid a,b,c,d\in\mathbb{R},\begin{vmatrix}a & b\\ c & d\end{vmatrix}\neq 0\right\}$ 的两个非平凡子群.

2. 设 G 是群，p 是素数，$|G|=p$，证明：G 只有平凡子群.

3. 设 G 为 Abel 群，$n\in\mathbb{N}$，证明：$\{a\in G\mid a^n=e\}$ 是 G 的子群.

4. 证明：指数为 2 的子群是正规子群，即设 $H<G$，且 $[G:H]=2$，则必有 $H\lhd G$.

5. 设 G 是群，$H\lhd G$，$K\lhd G$，且 $H\cap K=\{e\}$，证明：

$$hk=kh,\ \forall\, h\in H,k\in K.$$

6. 证明：任一群都不能写成两个真子群的并.

7. 设 G 是群，R 是 G 的一个等价关系，且有

$$(ax)R(ay)\Longrightarrow xRy,\ \forall\, a,x,y\in G.$$

证明：幺元 e 为代表的等价类 H 是 G 的一个子群.

8. 若群 G 中只有一个阶为 m 的子群 H，证明：$H\lhd G$.

9. 设 H 是群 G 的一个子群，记

$N_G(H)=\{g\in G\mid gHg^{-1}=H\}$，(称 $N_G(H)$ 为 H 在 G 中的**正规化子**)

(1) 证明：$N_G(H)<G$；

(2) 证明：$H\lhd N_G(H)$.

补充题

1. 设 H 是整数加群 $\mathbb{Z}$ 的任一个子群，证明必有 $m\in\mathbb{Z}$ 使得 $H=m\mathbb{Z}$.

2. 设 H_1,H_2 为群 G 的两个有限子群.记

$$H_1H_2=\{h_1h_2\mid h_1\in H_1,h_2\in H_2\},$$

证明：$|H_1H_2|=|H_1||H_2|/|H_1\cap H_2|$.

3. 幺半群 $|M;\cdot|$ 中的元素 a，如果有 $b\in M$，使 $ba=ab=e$，则称 a 为可逆元，称 b 为 a 的逆元，记 $b=a^{-1}$.证明：$|M;\cdot|$ 中所有可逆元关于 M 的运算构成一群.

4. 设 A,B 是两个乘法群，e 与 e' 分别为 A 与 B 的幺元，在 $A\times B$ 中定义乘法为 $(a_1,b_1)(a_2,b_2)=(a_1a_2,b_1b_2)$.证明：

(1) $A\times B$ 关于所定义的乘法构成群(称为 A 与 B 的**外直积**);

(2) $A_1=\{(a,e')\mid a\in A\}$ 和 $B_1=\{(e,b)\mid b\in B\}$ 均为 $A\times B$ 的正规子群;

(3) $A_1\cap B_1=\{(e,e')\}$, $A\times B=A_1B_1$(称为 A_1 与 B_1 的**内直积**).

5. 设 H,K 是乘法群 G 的两个子群,定义 $HK=\{hk\mid h\in H,k\in K\}$.

(1) 证明:HK 是 G 的子群$\Longleftrightarrow HK=KH$;

(2) 证明:若 H,K 中有一个是 G 的正规子群,则 HK 是 G 的子群;

(3) 证明:若 H,K 均是 G 的正规子群,则 $HK\lhd G$.

§1.4 群的同态与同构

同态与同构是抽象代数研究代数体系的重要工具.一旦证明了一个代数体系与已知的某代数体系同构,我们就可以在抽象的意义下把它看成是已知的那个代数体系.抽象代数最基本最重要的课题,就是搞清各种代数体系在同构意义下的分类.群的同态与同构,则是研究群与群之间关系的重要工具和手段.

定义 1.4.1 设 $\{G_1;\cdot\}$ 与 $\{G_2;*\}$ 是两个群,f 是 G_1 到 G_2 的一个映射,如果

$$f(a\cdot b)=f(a)*f(b),\quad \forall a,b\in G_1.$$

则称 f 是 G_1 到 G_2 的一个**同态映射**,简称**同态**.若 G_1 与 G_2 是同一个群,则称 f 是**自同态**.若同态 f 还是单射,则称 f 是**单同态**;若同态 f 还是满射,则称 f 是**满同态**.当 f 是满同态时,称 G_1 与 G_2 是同态的,记为 $G_1\sim G_2$.若同态 f 还是双射(双射即可逆映射,也即既是单射又是满射),则称 f 是 G_1 到 G_2 的一个**同构映射**,简称**同构**,此时称群 G_1 与 G_2 是同构的,记为 $G_1\simeq G_2$.

例 1 设 V 是数域 P 上的 n 维线性空间,f 是 V 的一般线性群 $GL(V)$ 到 P 中非零元的乘法群 $\{P^*;\cdot\}$ 的映射,

$$f(A)=\det(A),\ \forall A\in GL(V).$$

则 f 是满同态.这是因为两个线性变换乘积的行列式等于线性变

换行列式的乘积.

例 2 设 V 是 n 维实线性空间,则 $GL(V)\simeq GL_n(\mathbb{R})$.

证 在 V 中取一组基 $\{\alpha_1,\cdots,\alpha_n\}$, $\forall A\in GL(V)$,记 A 在这组基下的方阵为 $f(A)$,则根据线性代数中的结论知

$$f:GL(V)\to GL_n(\mathbb{R})$$

是双射,且

$$f(A\cdot B)=f(A)\cdot f(B),\quad \forall A,B\in GL(V).$$

据定义 1.4.1, f 是群 $GL(V)$ 到 $GL_n(\mathbb{R})$ 的一个同构映射,故 $GL(V)\simeq GL_n(\mathbb{R})$.

例 3 设 G 是一个群, $H\lhd G$,记 π 是 G 到 G/H 的映射,

$$\pi(g)=gH,\quad \forall g\in G.$$

则 π 是满同态,称 π 为群 G 到商群 G/H 的**自然同态**.

群的同态与同构有以下一些简单的性质.

命题 1.4.1 若 f 是群 G_1 到群 G_2 的同态, g 是群 G_2 到群 G_3 的同态,则 gf 是 G_1 到 G_3 的同态.若 f,g 都是满(单)同态,则 gf 也是满(单)同态.若 f,g 都是同构,则 gf 也是同构.若 f 是同构,则 f^{-1} 也是同构.

命题 1.4.2 设 f 是群 G_1 到群 G_2 的同态, e_1,e_2 分别为 G_1,G_2 的幺元,则有 $f(e_1)=e_2$ 及 $\forall a\in G, f(a^{-1})=f(a)^{-1}$.

证 由 $f(e_1)=f(e_1e_1)=f(e_1)f(e_1)$,两边左乘 $f(e_1)^{-1}$,得 $f(e_1)=e_2$. $\forall a\in G, f(a^{-1})f(a)=f(a^{-1}a)=f(e_1)=e_2$,故 $f(a^{-1})=f(a)^{-1}$. □

命题 1.4.3 设 f 是群 G_1 到群 G_2 的同态, $H<G_1$,则 H 的象集合 $f(H)$ 也是 G_2 的子群,特别, $f(G_1)<G_2$.

证 $e_2=f(e_1)\in f(H)$,知 $f(H)$ 非空. $\forall a_2,b_2\in f(H)$,有 $a_1,b_1\in H$ 使 $f(a_1)=a_2, f(b_1)=b_2$,于是

$$a_2b_2^{-1}=f(a_1)f(b_1)^{-1}=f(a_1)f(b_1^{-1})=f(a_1b_1^{-1})\in f(H).$$

据定理 1.3.1, $f(H)<G_2$. □

定义 1.4.2 设 f 是群 G_1 到群 G_2 的同态，则 G_2 的幺元 e_2 的完全原象 $\{a \in G_1 \mid f(a) = e_2\}$ 称为**同态映射 f 的核**，记为 $\ker f$.

例 4 设 G 是群，$H \lhd G$，π 是 G 到 G/H 的自然同态，则 $\ker \pi = H$.

命题 1.4.4 设 f 是群 G_1 到群 G_2 的同态，则 $\ker f \lhd G_1$.

证 记 e_1, e_2 分别为 G_1, G_2 的幺元，因 $e_1 \in \ker f$，故 $\ker f$ 非空. $\forall a, b \in \ker f$，有

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = e_2 e_2^{-1} = e_2,$$

故 $ab^{-1} \in \ker f$. 据定理 1.3.1，$\ker f < G_1$. 又 $\forall g \in G_1, a \in \ker f$，有

$$f(gag^{-1}) = f(g)f(a)f(g^{-1}) = f(g)e_2 f(g)^{-1} = e_2,$$

故 $gag^{-1} \in \ker f$. 据定义 1.3.4，$\ker f \lhd G_1$.

命题 1.4.5 设 f 是群 G_1 到群 G_2 的同态，则 f 是单同态 $\Longleftrightarrow \ker f = \{e_1\}$，这里 e_1 是 G_1 的幺元.

证 "$\Longrightarrow$"：据命题 1.4.2 知，$f(e_1) = e_2$，故 $\{e_1\} \subseteq \ker f$，又 $\forall a \in \ker f$，$f(a) = e_2 = f(e_1)$，因 f 是单射，$a = e_1$，故 $\ker f \subseteq \{e_1\}$.

"$\Longleftarrow$"：若 $f(a) = f(b)$，$a, b \in G_1$，则 $f(ab^{-1}) = f(a) \cdot f(b)^{-1} = e_2$，故 $ab^{-1} \in \ker f$，现 $\ker f = \{e_1\}$，故 $ab^{-1} = e_1$，即 $a = b$，故 f 是单同态. □

定理 1.4.6(群的同态基本定理) 设 f 是群 G_1 到群 G_2 的满同态映射，则 $G_1/\ker f \simeq G_2$.

证 记 $N = \ker f$，据命题 1.4.4 知，$N \lhd G_1$.

令

$$\phi: G_1/N \to G_2,$$
$$gN \mapsto f(g),$$

则 ϕ 是 G_1/N 到 G_2 的映射，因若 $g_1 N = g_2 N$，$g_1, g_2 \in G_1$，据推

论 1.3.5 知 $g_1^{-1}g_2 \in N$，故 $f(g_1^{-1}g_2)=e_2$，即 $f(g_1)^{-1}f(g_2)=e_2$，故 $f(g_1)=f(g_2)$. 这表明 G_1/N 中任一元素在 ϕ 下只有惟一的象，所以 ϕ 是映射.

其次，上边一段可以逆推回去：$f(g_1)=f(g_2) \Longrightarrow g_1N=g_2N$，$\forall\, g_1, g_2 \in G_1$，因此 ϕ 是单射.

再由 f 是满射，知 ϕ 也是满射，从而 ϕ 是双射.

$\forall\, aN, bN \in G/N$，由 f 是同态，有

$$\phi(aN\cdot bN)=\phi(abN)=f(ab)=f(a)f(b)=\phi(aN)\cdot\phi(bN),$$

所以 ϕ 还是同态映射，于是 ϕ 是同构映射，故 $G_1/N \simeq G_2$. □

这个定理的结论，是两个群同构，而在抽象的意义下，两个同构的群，是相同的群. 所以，这一定理是很重要的，称为群的同态基本定理.

推论 1.4.7 设 G 为一群，f 是 G 到另一群的同态映射，则 G 的**同态象** $f(G)$ 必同构于 G 的商群 $G/\ker f$；反之，G 的任一商群都可看作 G 的同态象.

证 设 f 是 G 到 G' 的同态，则 f 也可看作 G 到 $f(G)$ 的满同态，故据定理 1.4.6，有 $G/\ker f \simeq f(G)$.

反之，设 G/N 是 G 的任一商群，即有 $N \lhd G$，则 G 到 G/N 的自然同态 π 是满同态，故 G/N 可看作 G 的同态象 $\pi(G)$. □

由此我们也看到，两个群间的任一个满同态映射，都可以看作一个群到某一个商群上的自然同态；要找出一个群 G 的所有同态象，就相当于找出 G 的所有的商群，也就相当于找出 G 的所有的正规子群.

定理 1.4.8 设 f 是群 G_1 到群 G_2 的满同态，$N=\ker f$，则

① f 建立了 G_1 中包含 N 的子群与 G_2 中子群间的双射；

② 上述双射把正规子群对应到正规子群；

③ 若 $H \lhd G_1$，$N \subseteq H$，则 $G_1/H \simeq G_2/f(H)$.

这一定理的证明，我们留给读者作为练习.

推论 1.4.9 设 G 是群，$N \lhd G$，π 是 G 到 G/N 的自然同态，则 π 建立了 G 中包含 N 的子群与 G/N 的子群间的双射，而且把正规子群对应到正规子群. 又若 $H \lhd G$，$N \subseteq H$，则 $G/H \simeq (G/N)/(H/N)$.

从推论 1.4.7 我们知道，一个群的同态象总与该群的某一商群同构，故在讨论满同态时，我们可以只考虑群到它的商群上的自然同态，而不失一般性. 所以，下边的定理我们就用这样的语言来叙述，请读者自己把它改写为更一般的语言.

下边定理中谈到的群 G 的子群 H，不再有“包含同态核 N”的限制.

定理 1.4.10 设 G 是群，$N \lhd G$，π 是 G 到 G/N 的自然同态，$H < G$，则

① HN 是 G 中包含 N 的子群，且

$$HN = \pi^{-1}(\pi(H)).$$

即 HN 是 H 在 π 映射下的象集合 $\pi(H)$ 的完全原象 $\pi^{-1}(\pi(H))$.

② $(H \cap N) \lhd H$，且 $\ker(\pi|_H) = H \cap N$.

③ $HN/N \simeq H/(H \cap N)$.

证 ① $\forall h_1, h_2 \in H$，$\forall n_1, n_2 \in N$，即 $\forall h_1 n_1, h_2 n_2 \in HN$，

$$h_1 n_1 (h_2 n_2)^{-1} = h_1 n_1 n_2^{-1} h_2^{-1} = h_1 h_2^{-1} h_2 n_1 n_2^{-1} h_2^{-1}.$$

因 $N \lhd G$，$h_2 n_1 n_2^{-1} h_2^{-1} \in N$，因 $H < G$，$h_1 h_2^{-1} \in H$，于是 $h_1 n_1 (h_2 n_2)^{-1} \in HN$，据定理 1.3.1 知 $HN < G$，且 $N \subseteq HN$，又

$$\begin{aligned} \pi(HN) &= \{hnN \mid h \in H, n \in N\} \\ &= \{hN \mid h \in H\} = \pi(H). \end{aligned}$$

即 G 中包含同态核 N 的子群 HN 在 π 映射下的象集是 G/N 中的子群 $\pi(H)$. 据定理 1.4.8①，π 建立的双射就把 HN 对应到 $\pi(H)$，从而 $HN = \pi^{-1}(\pi(H))$.

② 因两个子群的交仍是子群，知 $(H \cap N) < G$，又 $(H \cap N) \subseteq H$，故 $(H \cap N) < H$. 再由 $N \lhd G$，用定义 1.3.4 可验证 $(H \cap N) \lhd$

H. 再注意到 $\forall\, h \in H, \pi|_H(h) = \pi(h)$, 便可证明 $\ker(\pi|_H) = H \cap N$.

③ 由①知 $\pi(H) = \pi(HN) = HN/N$, 所以 π 是 H 到 HN/N 的满同态映射, 故据同态基本定理有

$$H/(\ker(\pi|_H)) \simeq HN/N.$$

而由②$\ker(\pi|_H) = H \cap N$, 故上式就是我们要证的结果. □

习 题

1. 设 exp 为 $|\mathbb{R}; +|$ 到 $|\mathbb{R}^+; \cdot|$ 的映射, $\exp(x) = e^x$, $\forall\, x \in \mathbb{R}$, 等号右端的 e 为自然对数的底. 证明: exp 是群的同构映射.

2. 设 $\phi: |\mathbb{R}^+; \cdot| \to |\mathbb{R}^+; \cdot|$, $\phi(x) = |x|$, $\forall\, x \in \mathbb{R}$, 问 ϕ 是否为群的满同态映射, 若是, 求出 $\ker\phi$, 并判断 ϕ 是否为同构映射, 又, 能否说: "$|\mathbb{R}^+; \cdot|$ 与 $|\mathbb{R}^+; \cdot|$ 是同态的"?

3. 设 $f: |\mathbb{R}; +| \to |\mathbb{C}^*; \cdot|$,

$$f(x) = \cos x + \sqrt{-1}\sin x, \forall\, x \in \mathbb{R}.$$

证明 f 是一个群同态, 并求出 $\ker f$.

4. 设 $O_n(\mathbb{R})$ 是 n 阶实正交方阵的集合, $G = |1, -1|$ 是两个元素构成的乘法群. 证明:

(1) $O_n(\mathbb{R})$ 关于矩阵乘法构成群;

(2) 映射 $\phi: \mathbf{A} \to |\mathbf{A}|$ 是 $O_n(\mathbb{R})$ 到 G 的群同态;

(3) $\ker\phi = SO_n(\mathbb{R})$ (右端表示行列式为 1 的 n 阶实正交方阵的集合);

(4) $O_n(\mathbb{R})/SO_n(\mathbb{R}) \simeq G$.

5. 设 f 和 g 都是群 $|G; \cdot|$ 到群 $|H; *|$ 的同态, $D = |x \in G | f(x) g(x)|$, 证明: $D < G$.

6. 设 f 是群 G_1 到 G_2 的映射, $a \in G_1$.

(1) 若 f 是同态, 问 a 的阶是否一定等于 $f(a)$ 的阶? 为什么?

(2) 若 f 是同构, 问 a 的阶是否一定等于 $f(a)$ 的阶? 为什么?

7. 请把定理 1.4.10 改写为用更一般的语言来叙述, 第一句是: "设 f 是群 G_1 到 G_2 的满同态, $H < G$, 记 $N = \ker f$, 则…."

8. 设 $a, b \in \mathbb{R}$, 定义 $\mathbb{R}$ 到自身的映射(称为 $\mathbb{R}$ 的变换) $T_{(a,b)}$ 为

$$T_{(a,b)}(x) = ax + b, \forall\, x \in \mathbb{R}.$$

证明：

(1) $a \neq 0$ 时 $T_{(a,b)}$ 是双射；

(2) $G = \{T_{(a,b)} \mid a \neq 0\}$ 关于映射的乘法构成群；

(3) 记 $H = \{T_{(1,b)} \mid b \in \mathbb{R}\}$（$T_{(1,b)}$ 称为由 b 决定的平移），则 $H \lhd G$；

(4) $G/H \simeq \{\mathbb{R}^*; \cdot\}$.

9. 举例说明下边的命题不正确：

设 G_1, G_2 是群，$N_1 \lhd G_1, N_2 \lhd G_2$，且有 $G_1 \simeq G_2, N_1 \simeq N_2$，则必有 $G_1/N_1 \simeq G_2/N_2$.

补充题

1. 证明定理 1.4.8.

2. 设 σ 是群 G 到 G 的同构（称为 G 的自同构），且满足

$$\sigma(g) = g \Longrightarrow g = e.$$

证明：(1) $f: g \to \sigma(g)g^{-1}$ 是单射；

(2) 若 G 是有限群，则 G 的每个元素均可以写成 $\sigma(g)g^{-1}$ 的形式；

(3) 若 G 是有限群，且 σ^2 是 G 上的恒等变换 id_G，则 G 为奇数阶 Abel 群.

3. 完全类似于“群的同构”，可以定义“幺半群的同构”，只要把原来“群”的字样换成“幺半群”. 现 $\{\mathbb{Z}; *\}$ 中的“$*$”规定为：

$$a * b = a + b - ab, \forall\, a, b \in \mathbb{Z}.$$

证明：(1) $\{\mathbb{Z}; *\}$ 是一个幺半群；

(2) $\{\mathbb{Z}; *\}$ 与幺半群 $\{\mathbb{Z}; \cdot\}$ 同构.

4. 证明群 $\{\mathbb{Q}^*; \cdot\}$ 与 $\{\mathbb{Q}; +\}$ 不同构.

5. 求 $\{\mathbb{C}^*; \cdot\}$ 的子群 N，使 $\{\mathbb{C}^*; \cdot\}/N \simeq \{\mathbb{R}^+; \cdot\}$.

6. 设 H 是群 G 的正规子群，且 $|H| = n, [G:H] = m$，且 $(m, n) = 1$. 证明：H 是 G 的惟一的 n 阶子群.

§1.5 循 环 群

本节对循环群的讨论虽然不长，但却是完整的、彻底的. 它浓缩了抽象代数研究一般代数体系的思想、方法. 请读者由此用心体

会抽象代数这门学科的精神实质.

定义 1.5.1 由一个元素 a 反复运算生成的群

$$G=\{a^n \mid n\in \mathbf{Z}\}$$

称为**循环群**,记为$\langle a\rangle$,a 称为这个循环群的**生成元**.

由于循环群中的任一元都可表为生成元的方幂,所以有

命题 1.5.1 循环群都是交换群.

例 1 n 次单位根的全体 $U_n=\{z\in\mathbf{C}\mid z^n=1\}$ 对于复数的乘法运算构成一个循环群,n 次本原单位根是这个循环群的生成元.

特别地,$U_2=\{1,-1\}$,-1 是生成元;$U_3=\{1,\omega,\omega^2\}$,$\omega=\frac{-1+\sqrt{-3}}{2}$是生成元;$U_4=\{1,\sqrt{-1},-1,-\sqrt{-1}\}$,$-\sqrt{-1}$是生成元.

定理 1.5.2 循环群的任一子群也是循环群.

证 设 G_1 是 $G=\langle a\rangle$的一个子群,下边设法找出 G_1 的生成元.

取 $k=\min\{m\in\mathbf{N}\mid a^m\in G_1\}$.去证 $G_1=\langle a^k\rangle$.由 $a^k\in G_1$ 及 G_1 对运算封闭知$\langle a^k\rangle\subseteq G_1$.

反之,$\forall a^m\in G_1$,要证 $a^m\in\langle a^k\rangle$,即存在 q,使 $a^m=a^{qk}$,也即 $m=kq$,也即 $k\mid m$.做带余除法

$$m=qk+r,0\leqslant r<k.$$

则 $a^r=a^{m-qk}=a^m\cdot(a^k)^{-q}\in G_1$.若 $r\neq 0$,便与 k 的取法矛盾,所以 $r=0$,即 $m=kq$.这证明了 $G_1\subseteq\langle a^k\rangle$. □

推论 1.5.3 整数加群$\mathbf{Z}$的子群必形如 $m\mathbf{Z}$,$m\in\mathbf{N}\cup\{0\}$.

证 注意到这里的运算是加法.$\{\mathbf{Z};+\}$的生成元是 1.

$$\{\mathbf{Z};+\}=\{n\cdot 1\mid n\in\mathbf{Z}\}.$$

设 G_1 是$\{\mathbf{Z};+\}$的子群.据定理 1.5.2 的证明过程知,如果 $G_1\neq\{0\}$,则有 $k\in\mathbf{N}$,使 $G_1=\langle k\cdot 1\rangle=\{n\cdot k\mid n\in\mathbf{Z}\}=k\mathbf{Z}$.

$G_1=\{0\}$可以写成 $G_1=0\,\mathbf{Z}$,而 $G=k\mathbf{Z}$通常写成 $m\mathbf{Z}$. □

把循环群作为代数体系来研究，重要的问题是，在同构意义下，循环群有多少种？每一种的结构如何？下面的定理回答了这一问题，该定理的结论和证明方法都是典型的，请读者重视.

定理 1.5.4 设群 $G=\langle a\rangle$. 若 G 是无限阶的，则 G 与 $\{\mathbb{Z};+\}$ 同构；若 G 是有限阶 m 阶的，则 G 与 $\{\mathbb{Z}_m;+\}$ 同构.

所以，两个循环群同构$\Longleftrightarrow$它们有相同的阶.

证 我们借助于群的同态基本定理去完成证明.

令

$$\phi:\{\mathbb{Z};+\}\to G$$
$$n\mapsto a^n$$

$\forall n_1,n_2\in\{\mathbb{Z};+\}$，有

$$\phi(n_1+n_2)=a^{n_1+n_2}=a^{n_1}\cdot a^{n_2}=\phi(n_1)\cdot\phi(n_2).$$

又因 G 中任一元都可表为 a^n，所以 ϕ 是一个满同态映射.

据同态基本定理有

$$\{\mathbb{Z};+\}/\ker\phi\simeq G.$$

再据推论 1.5.3 知，$\ker\phi$ 必形如 $m\mathbb{Z}$，$m\in\mathbb{N}\cup\{0\}$.

若 $m=0$，则 $\ker\phi=\{0\}$，于是 $G\simeq\{\mathbb{Z};+\}$，此时 G 的阶为无限.

若 $m\neq0$，则 $\ker\phi=m\mathbb{Z}$，$m\in\mathbb{N}$. 于是 $G\simeq\{\mathbb{Z};+\}/m\mathbb{Z}=\{\mathbb{Z}_m;+\}$，此时 G 的阶为有限，即 m. □

这样，就证明了循环群可分为两大类：无限阶的与有限阶的. 而无限阶循环群都与 $\{\mathbb{Z};+\}$ 同构，有限阶循环群又依其阶 m 分别与 $\{\mathbb{Z}_m;+\}$ 同构. $\{\mathbb{Z};+\}$ 及 $\{\mathbb{Z}_m;+\}$ 的结构我们是清楚的，从而所有循环群的结构我们都搞清楚了.

定理还表明，$\forall m\in\mathbb{N}$，m 阶循环群都是存在的，并且在同构意义下只有一个 m 阶循环群. 这样，我们对于循环群的存在问题、分类问题、数量问题都已给出回答. 这是抽象代数研究方式的一个缩影. 抽象代数研究一种代数体系，就是要解决这种体系的存在问题、分类问题、数量问题.

下面讨论循环群的子群的特点. Lagrange 定理(定理 1.3.6)告诉我们,对有限群 G 而言,子群的阶一定是原来群的阶 $|G|$ 的因子.那么自然会问,对于 $|G|$ 的任一个因子 m_1,是否一定存在 G 的子群 G_1,使 $|G_1| = m_1$? 答案是否定的.读者可以随着学习的深入自己举例说明.

但是对于循环群,相应的命题是正确的,这就是下面的定理.

定理 1.5.5 设 G 是 m 阶循环群,m_1 是 m 的一个正整数因子,则存在 G 的惟一的 m_1 阶子群.

证 因 m 阶循环群在同构下只有一种结构,即 $\{\mathbb{Z}_m; +\}$,故不妨设

$$G = \{\mathbb{Z}_m; +\} = \{\bar{0}, \bar{1}, \cdots, \overline{(m-1)}\} = \langle \bar{1} \rangle.$$

因 $m_1 | m$,故 $\frac{m}{m_1}$ 是正整数,且 $0 < \frac{m}{m_1} \leqslant m$. 容易验证,

$$\langle \overline{(\frac{m}{m_1})} \rangle = \{\bar{0}, \overline{(\frac{m}{m_1})}, \overline{(2\frac{m}{m_1})}, \cdots, \overline{(m-1)\frac{m}{m_1}}\}$$

是 G 的 m_1 阶子群.惟一性的证明留给读者作练习. □

事实上,还有进一步描述循环群特点的

定理 1.5.6 设 G 是 m 阶群,则 G 是循环群的充要条件是,对 m 的每个正整数因子 m_1,都存在 G 的惟一的 m_1 阶子群.

这一定理的证明是 1956 年才给出的,有一定难度,在此略去.

从 $\{\mathbb{Z}_m; +\}$ 的结构中我们看出,m 阶循环群的生成元的阶也是 m(注意到这两个"阶"字含义是不同的).即如果 $G = \langle a \rangle$ 是 m 阶的,当运算记为乘法时,必

$$a^m = e, a^k \neq e, 0 < k < m,$$
$$\langle a \rangle = \{a^0, a^1, \cdots, a^{m-1}\}.$$

当运算记为加法时,必

$$ma = 0, ka \neq 0, 0 < k < m,$$
$$\langle a \rangle = \{0 \cdot a, 1 \cdot a, \cdots, (m-1) \cdot a\}.$$

利用循环群的性质，我们还可以证明下面的

命题 1.5.7 有限群 G 的任一元素 a 的阶是有限的，且是 G 的阶的因子.

证 设 a 的阶为 d，群运算不妨记为乘法，则有

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

所以 G 的子群 $\langle a\rangle$ 的阶也为 d. 据定理 1.3.6 立得结论. □

循环群 $G=\langle a\rangle$，可以看作 G 中一个元素 a 生成的子群，其中元素形为 $\{a^n\mid n\in\mathbb{Z}\}$. 由于 a^n 中的 n 可以是正整数、负整数和零，所以 G 中的元素也可以看作 $\{a,a^{-1}\}$ 中任意有限多个元素的乘积，即

$$x_1x_2\cdots x_m,\text{其中 } x_1,\cdots,x_m\in\{a,a^{-1}\}.$$

由类似的思路，我们可以定义群 G 中一个非空子集 S 生成的子群.

定义 1.5.2 设 S 是群 G 中一个非空子集，记 $S^{-1}=\{a^{-1}\mid a\in S\}$，则

$$\{x_1\cdots x_m\mid x_1,\cdots,x_m\in S\cup S^{-1}\}.$$

是 G 的一个子群，称为 S **生成的子群**，记为 $\langle S\rangle$.

其中“$\langle S\rangle$ 是 G 的子群”一点，用定理 1.3.1 容易验证，请读者自行完成.

我们还可以从另外的角度来看群 G 中非空子集 S 生成的子群 $\langle S\rangle$.

若 $\langle a\rangle\subseteq G$，则 $\langle a\rangle$ 可以看作 G 中所有包含 $\{a\}$ 的子群的交，它是 G 中包含 $\{a\}$ 的最小的子群. 类似地，若 S 是 G 中非空子集，则 $\langle S\rangle$ 可以看作 G 中所有包含 S 的子群的交，它是 G 中包含 S 的最小的子群.

如果 $\langle S\rangle=G$，则称 S 为群 G 的一个**生成组**. 如果群 G 有一个有限子集 S 作为 G 的生成组，则称 G 为**有限生成群**. 有限群自身就可以看作一个生成组，所以，有限群一定是有限生成群，但有

限生成群不一定是有限群，例如$\{\mathbf{Z};+\}=\langle 1\rangle$就是无限群.

习 题

1. 设循环群 G 的生成元为 a，f 是 G 到群 K 的同态映射，证明 $f(G)$ 也是循环群，且 $f(a)$ 是 $f(G)$ 的生成元.

2. 设 $G_1=\langle a\rangle$ 是无限阶循环群，$G_2=\langle b\rangle$ 是 m 阶循环群，讨论：G_1，G_2 各有哪些生成元？

3. 设 S 是群 G 中一个非空子集，记 $S^{-1}=\{a^{-1}\mid a\in S\}$，记

$$\langle S\rangle=\{x_1x_2\cdots x_m\mid m\in\mathbf{N},x_1,x_2,\cdots,x_m\in S\cup S^{-1}\}.$$

证明：$\langle S\rangle<G$.

4. 一个群的两个不同的子集会不会生成相同的子群？

5. 设 G 是循环群，$N<G$，证明：G/N 也是循环群.

6. 设 a，b 是群 G 中的元素，a 的阶为 m，b 的阶为 n，$ab=ba$，$\langle a\rangle\cap\langle b\rangle=\{e\}$，证明：$ab$ 的阶是 $[m,n]$（$[m,n]$ 为 m，n 的最小公倍数）.

7. 设 G_1，G_2 各是 m 阶和 n 阶循环群，证明：G_1 与 G_2 同态 $\Longleftrightarrow n\mid m$.

8. 证明 4 阶群只有两种结构，一种是 4 阶循环群，一种是 Klein 四元群. 后者的群表如下：

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

补充题

1. 证明：任何循环群都可以看作循环群$\{\mathbf{Z};+\}$的同态象.

2. 设 G 是 n 阶交换群. 记 $K=\{k\in\mathbf{N}\mid a^k=e,,\forall a\in G\}$. 证明：$G$ 为循环群 $\Longleftrightarrow n=\min K$.

3. 设群 G 只有有限个子群，证明：G 必为有限群.

4. 证明：$\{\mathbb{Q};+\}$ 的任一有限生成子群必是循环群.

5. 设 $G=\langle a,b\rangle$ 为由 a 和 b 生成的群，其中 $a\neq b$，a 为 n 阶元，b 为 2 阶元，且 $aba=b$，证明：$|G|=2n$.

6. 证明定理 1.5.5 中的“惟一性”：G 是 m 阶循环群，m_1 是 m 的一个正整数因子，则 G 中有惟一的 m_1 阶子群.

§1.6 变换群与置换群

变换群在历史上和理论上都有重要的意义. 人们研究群，最早是从研究变换群中的置换群开始的. 本节将证明，任一个群都与某一个变换群同构. §1.2 例 6 中曾提到全变换群的概念，现在把相关的概念叙述为

定义 1.6.1 设 A 是非空集合，A 的所有可逆变换关于映射的乘法构成的群，称为 A 的**全变换群**，记为 $\{S_A;\cdot\}$，简记为 S_A. S_A 的一个子群称为 A 的一个**变换群**. 当 A 为含有 n 个元素的有限集时，S_A 也叫作 n **元对称群**，也记作 S_n. S_n 中的一个元素称为一个 n **元置换**. S_A 的一个子群称为一个 n **元置换群**.

例 1 设 A 是整个平面上所有点的集合，在平面上建立直角坐标系. 记 R_θ 是平面绕原点按逆时针方向旋转 θ 角的变换，$H=\{R_\theta\mid 0\leqslant\theta<2\pi\}$，则 H 是 A 的一个变换群.

定理 1.6.1(凯莱(Cayley)定理) 任何一个群都与一个变换群同构.

证 设 G 是一个群. $\forall a\in G$，令 $\phi_a:G\to G$.

$$\phi_a(g)=ag,\forall\ g\in G.$$

则因 $\forall g\in G$，有 $a^{-1}g\in G$，而 $\phi_a(a^{-1}g)=g$，故 ϕ_a 是 G 到自身的满映射. 又若 $\phi_a(g_1)=\phi_a(g_2)$，即 $ag_1=ag_2$，由群中消去律知 $g_1=g_2$，所以 ϕ_a 还是单射，从而 ϕ_a 是双射，即是 G 到自身的可逆映

射，故 $\phi_a \in S_G$.

令 $T=\{\phi_a \mid a \in G\} \subseteq S_G$. 注意到 $(\phi_b)^{-1}=\phi_b^{-1}$，$\phi_a \cdot \phi_b^{-1}=\phi_{ab^{-1}} \in T$，据定理 1.3.1 便知 $T<S_G$，即 T 是 G 的一个变换群. 再令 $f: G \to T$，

$$f(a)=\phi_a, \forall\, a \in G.$$

则 f 是 G 到 T 的满映射，又若 $\phi_a=\phi_b$，$a, b \in G$，则 $\phi_a(e)=\phi_b(e)$，即 $ae=be$，所以 $a=b$，故 f 还是单射，从而 f 是双射. 又

$$f(ab)=\phi_{ab}=\phi_a \cdot \phi_b=f(a) \cdot f(b), \forall\, a, b \in G.$$

所以 f 还是群同态. 于是 f 是群 G 到群 T 的同构，便有 $G \simeq T$.

□

证明中的 ϕ_a 称为群 G 中由 a 决定的**左平移变换**. 类似地，还有由 a 决定的**右平移变换**：

$$\psi_a(g)=ga, \forall\, g \in G.$$

推论 1.6.2 任一有限群都与一个置换群同构.

凯莱定理使我们可以将对群的研究归结为对变换群的研究，对有限群的研究归结为对置换群的研究. 下边介绍一下置换群.

若 $\sigma \in S_n$，则 σ 称为一个 n 元置换，通常表示为

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

它的含义是 $\sigma(1)=i_1, \sigma(2)=i_2, \cdots, \sigma(n)=i_n$. 由于 σ 是双射，所以 $i_1, i_2, \cdots, i_n$ 是 $1, 2, \cdots, n$ 的一个排列. 并且不同的排列得到的置换 σ 也不同. 因此，n 元置换的个数，就是 $1, 2, \cdots, n$ 的所有排列的个数. 于是有

命题 1.6.3 n 元对称群 S_n 的阶为 $n!$.

当 $j_1, j_2, \cdots, j_n$ 是 $1, 2, \cdots, n$ 的一个排列时，也可记

$$\sigma=\begin{pmatrix} j_1 & j_2 & \cdots & j_n \\ \sigma(j_1) & \sigma(j_2) & \cdots & \sigma(j_n) \end{pmatrix}.$$

从而，一个 n 元置换可以有 $n!$ 种记法.

置换是一种映射，所以，置换的乘法、置换的逆与映射的乘法、映射的逆有类似的表示法.但读者应注意，有些书中还有其他的表示法.

例 2 S_3 中有 $3!=6$ 个元素：

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

容易看出，S_3 不是交换群，例如，取

$$f=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\varphi=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}.$$

则

$$\varphi\cdot f=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},$$
$$f\cdot\varphi=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}.$$

所以，$\varphi\cdot f\neq f\cdot\varphi$.还可以看出

$$f^{-1}=\begin{pmatrix}3&2&1\\1&2&3\end{pmatrix}=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\varphi^{-1}=\begin{pmatrix}2&1&3\\1&2&3\end{pmatrix}=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}.$$

上述表示置换 σ 的记号，在括号中写成两行，略嫌烦琐，又看不出 σ 的特点，下面引入轮换的概念和记号，并给出置换的另一种表示法.

定义 1.6.2 设集合 $\{i_1,i_2,\cdots,i_r\}$ 为集合 $\{1,2,\cdots,n\}$ 的一个子集.若 $\sigma\in S_n$，满足

$$\sigma(i_1)=i_2,\sigma(i_2)=i_3,\cdots,\sigma(i_{r-1})=i_r,\sigma(i_r)=i_1,$$

及

$$\sigma(k)=k,\forall\, k\in\{1,2,\cdots,n\}\setminus\{i_1,i_2,\cdots,i_r\},$$

则称 σ 为 S_n 中的一个 r **－轮换**，或称 r **－循环置换**，记为 $\sigma=(i_1i_2$

$\cdots i_r)$. $i_1, i_2, \cdots, i_r$ 均称为轮换 σ 中的文字，r 称为**轮换 σ 的长**.

特别，2－轮换(ij)称为**对换**，恒等置换可记为 1－轮换.

用轮换的定义和群中元素的阶的定义可以证明

命题 1.6.4 在 S_n 中，r－轮换的阶为 r.

任一个 r－轮换都可以有 r 种表示法：

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

定义 1.6.3 在 S_n 中，如果若干个轮换间没有共同文字，则称它们是**不相交的轮换**.

用定义不难证明

命题 1.6.5 在 S_n 中，两个不相交的轮换的乘积是可交换的.

定理 1.6.6 $\forall \sigma \in S_n$，σ 都可表为 S_n 中一些不相交轮换之积.

证 取 $a \in \{1,2,\cdots,n\}$，作序列

$$a=\sigma^0(a), \sigma(a), \sigma^2(a), \cdots\cdots$$

(σ^0 就是恒等置换 id)其中一定包含重复的文字，记 $\sigma^m(a)$是第一个与前面相重复的文字，并设它与 $\sigma^k(a)(0 \leqslant k < m)$重复. 可证 $k=0$，因若不然，由 $\sigma^{k-1}(a) \neq \sigma^{m-1}(a)$，及 $\sigma(\sigma^{k-1}(a))=\sigma(\sigma^{m-1}(a))$，推出 σ 把两个不同的文字映到相同的文字，这与“σ 是单射”矛盾. 因此 $k=0$，即 $\sigma^m(a)=a$. 作轮换

$$\sigma_1=(a, \sigma(a), \cdots, \sigma^{m-1}(a)).$$

则 σ 与 σ_1 在文字 $a, \sigma(a), \cdots, \sigma^{m-1}(a)$上的作用相同.

若 $m=n$，则 $\sigma=\sigma_1$，本身就已表为一个轮换. 若 $m<n$，则取 $b \in \{1,2,\cdots,n\} \setminus \{a, \sigma(a), \cdots, \sigma^{m-1}(a)\}$，仿照上面的方法再作一个轮换

$$\sigma_2=(b, \sigma(b), \cdots, \sigma^{l-1}(b)).$$

则 σ 与 σ_2 在文字 $b, \sigma(b), \cdots, \sigma^{l-1}(b)$上的作用相同. 而且因 σ 是单射，知 σ_1 与 σ_2 不相交.

这样继续下去，直到 $1,2,\cdots,n$ 用完为止．这就得到有限个不相交的轮换 $\sigma_1,\sigma_2,\cdots,\sigma_s$ 使

$$\sigma=\sigma_1\sigma_2\cdots\sigma_s. \qquad \square$$

注意到，由于对 a,b 等选择可以不同，选择的先后也可以不同，所以上述各轮换 $\sigma_1,\sigma_2,\cdots,\sigma_s$ 的次序可以不同．但任一文字 c 所在的轮换是惟一的，即 $(c,\sigma(c),\sigma^2(c),\cdots)$，虽然形式上未必是以 c 起头．因此，有

命题 1.6.7 任一 n 元置换表为不相交轮换的乘积时，如果不计次序，表法是惟一的．

例 3 $\begin{pmatrix}1&2&3&4&5&6&7\\1&7&5&2&3&6&4\end{pmatrix}=(1)(274)(35)(6)=(274)(35)=(35)(274)$．

后两个等号中，删去了 1－轮换 $(1),(6)$，效果是一样的，这是因为在轮换的定义 1.6.2 中，轮换对不出现的文字的作用效果，是保持该文字不变．

直接验证可得

例 4 $(i_1i_2\cdots i_r)=(i_1i_r)(i_1i_{r-1})\cdots(i_1i_3)(i_1i_2)$．

即，任一个 r－轮换都可写成 $r-1$ 个对换（不一定是不相交的对换）的乘积．再利用定理 1.6.6，便有

命题 1.6.8 任一 n 元置换都可以表为一些对换的乘积．

一个置换表为对换之乘积的表示法是不惟一的，但其中对换个数的奇偶性不变．对它的证明我们略去了．

定义 1.6.4 当一个置换能表为奇（偶）数个对换的乘积时，称为**奇置换（偶置换）**．

命题 1.6.9 两个偶置换之积是偶置换，两个奇置换之积是偶置换，偶置换与奇置换之积是奇置换，奇置换与偶置换之积是奇置换．偶置换的逆置换是偶置换，奇置换的逆置换是奇置换．

定义 1.6.5 n 元偶置换的全体对置换的乘法构成一个群，称为 n 元**交错群**，记为 A_n．用正规子群的定义及命题 1.6.9 容易

证明

命题 1.6.10 $A_n \lhd S_n, |A_n| = \frac{n!}{2}$.

命题 1.6.11 设置换 σ 表为不相交轮换的乘积是

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

这里 σ_i 是 r_i - 轮换($i = 1, 2, \cdots, s$),则作为群 S_n 中的元素,σ 的阶是 $r_1, r_2, \cdots, r_s$ 的最小公倍式$[r_1, r_2, \cdots, r_s]$.

这一命题的证明留给读者.

例 5 例 3 中置换的阶为$[3,2] = 6$.

下边介绍群的自同构群和内自同构群.

定义 1.6.6 群 G 到自身的同构映射,称为 G 的一个**自同构**,群 G 的全体自同构的集合记为 $\mathrm{Aut}G$.

命题 1.6.12 设 G 是群,则 $\mathrm{Aut}G < S_G$,称 $\mathrm{Aut}G$ 为**群 G 的自同构群**.

证 $\forall \theta_1, \theta_2 \in \mathrm{Aut}G$,据同构映射的性质知 $\theta_2^{-1} \in \mathrm{Aut}G$,$\theta_1 \theta_2^{-1} \in \mathrm{Aut}G$,再据定理 1.3.1 知,$\mathrm{Aut}G < S_G$. □

命题 1.6.13 设 G 为群,$a \in G$,定义映射 $\sigma_a : G \to G$ 为

$$\sigma_a(g) = aga^{-1}, \forall g \in G,$$

则 $\sigma_a \in \mathrm{Aut}G$,**称为由 a 决定的内自同构**.记

$$\mathrm{Inn}G = \{\sigma_a \mid a \in G\},$$

则 $\mathrm{Inn}G \lhd \mathrm{Aut}G$,称 $\mathrm{Inn}G$ 为 G 的**内自同构群**.

证 由 $\sigma_{a^{-1}} \cdot \sigma_a(g) = a^{-1}(aga^{-1})a = g$ 知 σ_a 的逆映射是 $\sigma_{a^{-1}}$,从而 σ_a 是双射,又

$$\begin{aligned}\sigma_a(g_1 g_2) &= ag_1 g_2 a^{-1} = ag_1 a^{-1} ag_2 a^{-1} \\ &= \sigma_a(g_1)\sigma_a(g_2), \forall g_1, g_2 \in G,\end{aligned}$$

所以 $\sigma_a \in \mathrm{Aut}G$.

$\forall \sigma_{a_1}, \sigma_{a_2} \in \mathrm{Inn}G$,考察 $\sigma_{a_1} \cdot (\sigma_{a_2})^{-1}$ 在 G 中任一元 g 上的作用,有

$$\sigma_{a_1}\cdot(\sigma_{a_2})^{-1}(g)=\sigma_{a_1}\sigma_{a_2^{-1}}(g)=\sigma_{a_1}(a_2^{-1}ga_2)=a_1(a_2^{-1}ga_2)a_1^{-1}$$
$$=a_1a_2^{-1}g(a_1a_2^{-1})^{-1}=\sigma_{a_1a_2^{-1}}(g),$$

所以 $\sigma_{a_1}\cdot(\sigma_{a_2})^{-1}=\sigma_{a_1a_2^{-1}}\in \mathrm{Inn}G$，因此据定理 1.3.1，$\mathrm{Inn}G<\mathrm{Aut}G$.

又 $\forall\,\theta\in\mathrm{Aut}G$，$\forall\,\sigma_a\in\mathrm{Inn}G$，我们去证 $\theta\sigma_a\theta^{-1}\in\mathrm{Inn}G$，再据正规子群的定义便证出 $\mathrm{Inn}G\lhd\mathrm{Aut}G$.

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

所以 $\theta\sigma_a\theta^{-1}=\sigma_{\theta(a)}\in\mathrm{Inn}G$. □

如果我们定义映射 $f:G\to\mathrm{Inn}G$ 为

$$f(a)=\sigma_a,\ \forall\,a\in G,$$

则容易验证 $f(ab)=\sigma_{ab}=\sigma_a\sigma_b=f(a)f(b)$，从而 f 是满同态映射，且

$$\ker f\lhd G,\ G/\ker f\simeq\mathrm{Inn}G.$$

$\forall\,a\in\ker f$，因 $f(a)=id$，即 $\sigma_a=id$，也即 $\sigma_a(g)=g$，$\forall\,g\in G$，也即 $aga^{-1}=g$，$\forall\,g\in G$，也即 $ag=ga$，$\forall\,g\in G$. 所以

$$\ker f=\{a\in G\mid ag=ga,\ \forall\,g\in G\}.$$

定义 1.6.7 群 G 中，与 G 中所有元素可交换的元素的集合称为**群 G 的中心**，记为 $C(G)$.

以上讨论说明，$C(G)=\ker f$，$G/C(G)\simeq\mathrm{Inn}G$.

习 题

1. 计算 S_5 中 σT，$\sigma^{-1}T\sigma$，σ^2，其中

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

2. 列出 S_3 的群表.

3. 把(12)(123)(14)写成不相交轮换的乘积.

4. 证明：置换群 G 中若有奇置换，则 G 中一定有指数为 2 的子群.

5. 设 G_1, G_2 是群，$N_1 \lhd G_1$，$N_2 \lhd G_2$，且有 $N_1 \simeq N_2$ 及 $G_1/N_1 \simeq G_2/N_2$，问是否一定有 $G_1 \simeq G_2$？

6. 设 G 是有限群，且 G 的任何真子群都是循环群，问 G 是否一定是循环群？

7. 举例说明定理 1.5.5 对非循环的有限群不成立.

8. 证明：$S_3 = \langle (12), (13) \rangle$.

9. 证明命题 1.6.11.

10. 证明：$\forall \sigma \in S_n$，有

$$\sigma(i_1 i_2 \cdots i_r)\sigma^{-1} = (\sigma(i_1)\sigma(i_2)\cdots\sigma(i_r)).$$

11. 设 G 是 n 阶交换群，m 是与 n 互素的自然数，定义 f 为：$f(a) = a^m$，$\forall a \in G$. 证明：$f \in \mathrm{Aut}G$.

12. 设 G 是 n 阶群，G 的中心只有幺元. 证明：G 有且只有 n 个彼此不同的内自同构.

补充题

1. 证明：当 $n \geqslant 3$ 时，S_n 的中心 $C(S_n) = \{\mathrm{id}\}$.

2. 证明：在同构意义下 6 阶群只有两种，一种是 6 阶循环群，一种是 S_3.

3. 设 G 是阶数大于 2 的有限群且 G 中有阶数大于 2 的元素，证明：$|\mathrm{Aut}G| > 1$.

4. 证明：$S_3 \simeq \mathrm{Aut}S_3 = \mathrm{Inn}S_3$.

5. 证明：$S_n = \langle \{(12), (13), \cdots (1n)\} \rangle$.

6. 在 S_4 中完成下边两个例子，从而说明下边两个命题不真.

(1) $|A_4| = 12$，但 A_4 中不存在 6 阶子群.

这表明命题："若群 G 的阶是 n，m 是 n 的正整数因子，则 G 必有 m 阶子群"不真. 即定理 1.3.6(Lagrange 定理)的逆命题不真.

(2) 记 $K = \{(1), (12)(34), (13)(24), (14)(23)\}$，$N = \{(1), (12)(34)\}$. 则 $N \lhd K$，$K \lhd S_4$，但 N 不是 S_4 的正规子群.

这表明命题："正规子群的正规子群是正规子群"不真.

§1.7 单群与可解群*

本节的内容与多项式方程是否可用根式解的问题有关，可解

群的得名也与此有关.在附录“伽罗瓦理论简介”中将用到本节的一些概念和结果.

定义 1.7.1 如果群 G 只有平凡的正规子群,则称 G 为**单群**.

由此看出,单群是结构比较简单的群.因其简单,从而重要,单群在群论中的作用很像素数在整数论中的作用.把复杂的事物分成简单的事物,是科学研究中经常采用的方法,所以,对单群的研究特别是对有限单群的研究,长期以来是群论中一个主要内容.基本的问题是:在同构意义下有多少类有限单群?这个问题在20世纪八十年代已经解决,成为代数学在上个世纪的重大成就.问题的难点在非交换单群方面,而交换单群的情况则是容易的.

定理 1.7.1 设 G 为交换群,$G\neq\{e\}$,则 G 为单群的充分必要条件是 G 为素数阶循环群.

证 充分性的一面由定理 1.3.6 容易推出,因为素数阶群只有平凡子群.

下证必要性.取 $a\in G$,但 $a\neq e$,因 G 可换,则 $\langle a\rangle\lhd G$,又 G 是单群,故 $G=\langle a\rangle$,这表明 G 一定是循环群.其次,G 一定是有限阶循环群,因为否则 $\langle a^2\rangle$ 将是 $G=\langle a\rangle$ 的一个非平凡正规子群(请读者自己证明这一点),与 G 是单群产生矛盾.最后,G 一定是素数阶循环群,否则据定理 1.5.6 及 G 可换,G 将有非平凡正规子群. □

非交换单群的情况要复杂得多,我们也不会去全面讨论这样的问题.我们仅仅略去证明给出如下的结果.

定理 1.7.2 n 元交错群 A_n,当 $n\neq4$ 时都是单群,其中 $n=1,2,3$ 时,A_n 是交换单群;$n\geqslant5$ 时,A_n 是非交换单群.

这一定理证明的主要部分是:$n\geqslant5$ 时,A_n 是非交换单群.170年前法国青年数学家伽罗瓦(Galois)就已完成了这一证明,并由此推出一般5次和5次以上方程不可能有根式解的重要结论.

为讨论可解群,下面先引入一个群的导出群的概念.

定义 1.7.2 设 G 是群，$a,b\in G$，称 $a^{-1}b^{-1}ab$ 是 a 与 b 的**换位子**，记为 $[a,b]$. 称 G 中所有换位子生成的子群为 G 的**换位子群**，也称为 G 的 1 次**导出群**（简称为导出群），记为 $[G,G]$，也记为 $G^{(1)}$. $(G^{(1)})^{(1)}$ 称为 G 的 2 次导出群，也记为 $G^{(2)}$，这样下去，$G^{(k)}=(G^{(k-1)})^{(1)}$ 称为 G 的 k 次导出群. $G^{(0)}$ 定义为 G.

这里要注意的是，G 中所有换位子的集合关于 G 的运算并不一定构成群；导出群是这个集合“生成的子群”，所以是群.

定理 1.7.3 设 G 是群，则 $G^{(1)}\lhd G$.

证 注意到一个换位子的逆是另外一个换位子：$[a,b]^{-1}=[b,a]$，再由定义 1.5.2 知，$G^{(1)}$ 中任一元可表为 $[a_1,b_1]\cdots[a_n,b_n]$ 的形式. 而 $\forall g\in G$，

$$g([a_1,b_1]\cdots[a_n,b_n])g^{-1}=g[a_1,b_1]g^{-1}g\cdots g^{-1}g[a_n,b_n]g^{-1},$$

所以，为证 $G^{(1)}\lhd G$，只须证明 $g[a,b]g^{-1}\in G^{(1)}$.

事实上，

$$\begin{aligned}g[a,b]g^{-1}&=ga^{-1}b^{-1}abg^{-1}=ga^{-1}g^{-1}gb^{-1}g^{-1}gag^{-1}gbg^{-1}\\&=[gag^{-1},gbg^{-1}]\in G^{(1)}.\end{aligned}$$ □

定义 1.7.3 设 G 是群，如果有一非负整数 k，使 $G^{(k)}=\{e\}$，则称 G 为**可解群**.

命题 1.7.4 交换群都是可解群.

证 因交换群中所有换位子都是幺元 e，故 $G^{(1)}=\{e\}$. 事实上这也是 G 为交换群的充要条件. □

命题 1.7.5 可解群的子群都是可解群.

证 设 G 是可解群，则有 $k\in\mathbb{N}$ 使 $G^{(k)}=\{e\}$，又设 $H<G$，则据导出群的定义有 $H^{(1)}<G^{(1)}$，继续推下去，可得 $H^{(k)}<G^{(k)}=\{e\}$，故 H 是可解群. □

命题 1.7.6 可解群的商群或同态象是可解群.

证 因为所有的商群都可以看作自然同态下的同态象，故只须证明可解群的同态象是可解群. 设 G 是可解群，则有 $k\in\mathbb{N}$ 使 $G^{(k)}=\{e\}$. 又设 f 是 G 到 G' 的同态映射，下证 $f(G)$ 是可解群.

首先,据命题 1.4.3,$f(G)<G'$,从而 $f(G)$是群.其次,由于 $\forall a,b\in G, f([a,b])=f(a^{-1}b^{-1}ab)=f(a)^{-1}f(b)^{-1}f(a)f(b)=[f(a),f(b)]$是 $f(G)$中的换位子,于是可得 $f(G^{(1)})=(f(G))^{(1)}$,继续推下去可得 $f((G)^{(k)})=(f(G))^{(k)}$,这就是 $f(\{e\})=(f(G))^{(k)}$,也就是$(f(G))^{(k)}=\{e\}$,所以 $f(G)$是可解群. □

命题 1.7.7 设 G 是群,$H\lhd G$,若 H 和 G/H 都是可解群,则 G 也是可解群.

证 设 $k_1,k_2\in\mathbf{N}$,使 $H^{(k_1)}=\{e\}$,$(G/H)^{(k_2)}=\{e\}$.记 π 为 G 到 G/H 的自然同态,则与命题 1.7.6 类似可证 $\pi(G^{(k_2)})=(\pi(G))^{(k_2)}=(G/H)^{(k_2)}=\{\bar{e}\}$.所以

$$G^{(k_2)}\subseteq\ker\pi=H.$$

于是 $G^{(k_1+k_2)}=(G^{(k_2)})^{(k_1)}\subseteq H^{(k_1)}=\{e\}$.故 G 是可解群. □

命题 1.7.8 当 $n\leqslant 4$ 时,A_n 是可解群;当 $n\geqslant 5$ 时,A_n 不是可解群.

证 当 $n=1,2$ 时,A_n 都是幺群,当然是可解群.

当 $n=3$ 时,$|A_3|=\dfrac{3!}{2}=3$.即 A_3 是 3 阶循环群,是交换群,故是可解群.

当 $n=4$ 时,$|A_4|=\dfrac{4!}{2}=12$,又不难验证

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

是 A_4 的正规子群,且 K 是交换群,故 K 是可解群.又 $|A_4/K|=12/4=3$,即 A_4/K 是 3 阶循环群,故是可解群.再据命题 1.7.7 知,A_4 是可解群.

当 $n\geqslant 5$ 时,据定理 1.7.2,A_n 是非交换单群,再据定理 1.7.3,$A_n^{(1)}\lhd A_n$.A_n 非交换,由命题 1.7.4 的证明知 $A_n^{(1)}\neq\{e\}$,所以 $A_n^{(1)}=A_n$.从而 $A^{(2)}=(A_n^{(1)})^{(1)}=A_n^{(1)}=A_n$,继续下去,$\forall k\in\mathbf{N}$,都有 $A_n^{(k)}=A_n\neq\{e\}$,所以 A_n 不是可解群. □

习 题

1. 设 G 是非交换单群，证明：$G \simeq \mathrm{Inn}\ G$.

2. 设 $G=\langle a\rangle$ 是无限阶循环群，证明：$\langle a^2\rangle$ 是 G 的非平凡子群.

3. 设 G 为群，$H<G$ 且 $G^{(1)}\subseteq H$，证明：$H\lhd G$.

4. 设 G 为群，$H\lhd G$，证明：

(1) G 为 Abel 群$\Longleftrightarrow G^{(1)}=\{e\}$.

(2) G/H 为 Abel 群$\Longleftrightarrow G^{(1)}\subseteq H$.

5. 记 $K=\{(1),(12)(34),(13)(24),(14)(23)\}$. 证明：$A_4^{(1)}=K$，$A_4^{(2)}=\{e\}$，从而 A_4 是可解群.

6. 当 $n\geqslant 5$ 时，证明：

(1) $C(S_n)=\{(1)\}$；

(2) S_n 只有一个非平凡的正规子群 A_n；

(3) $S_n^{(1)}=A_n$；

(4) S_n 不是可解群.

7. 设 G 是群，$H<G$，$N\lhd G$，H 和 N 都是可解群，证明：HN 也是可解群.

8. 设 G 是 pq 阶群，其中 $p>q$ 并均是素数，则 G 中必有 p 阶正规子群. 证明 G 是可解群.

9. (1) 证明：非交换的有限单群 G 不是可解群；

(2) 用(1)证明：$n\geqslant 5$ 时，A_n 不是可解群.

补充题

1. 设 G 是群，$M\lhd G$，$N\lhd G$，且 G/N 是可解群，证明：G/MN 是可解群.

2. 设 G 是群，$M\lhd G$，$N\lhd G$，且 G/M 和 G/N 都是 Abel 群，证明：$M\cap N\lhd G$ 且 $G/(M\cap N)$ 是 Abel 群.

3. 设 G 是有限群，G 的子群序列

$$G=G_1\supset G_2\supset\cdots\supset G_t\supset G_{t+1}=\{e\}$$

满足 $G_{i+1}\lhd G_i$，$i=1,2,\cdots,t$，则称为**次正规群列**. G 的各阶导出群构成的子群序列

$$G \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \cdots \supseteq G^{(n)} \supseteq G^{(n+1)} \supseteq \cdots$$

称为 G 的**导出列**.

(1) 证明:G 的导出列中一旦出现等号,以后就一定全是等号,即若 $G^{(i)} = G^{(i+1)}$,必有 $G^{(i)} = G^{(i+1)} = G^{(i+2)} = \cdots$;

(2) 证明:G 是可解群$\Longleftrightarrow$ G 的导出列是次正规群列;

(3) 请由(1),(2)再编一个"G 是可解群"的充要条件,并证明它.

4. 设 G 是有限群.证明:

(1) G 中一定有次正规群列(定义见上题)

$$G = G_1 \supset G_2 \supset \cdots \supset G_t \supset G_{t+1} = \{e\}$$

使商群 G_i/G_{i+1} 均是单群,$i = 1,2,\cdots,t$(这样的次正规群列称为 G 的**合成群列**);

(2) 若 G 是交换群,则 G_i/G_{i+1} 的阶均为素数;

(3) 若 G_i/G_{i+1} 均是可解群(特别地,若均是交换群),$i = 1,2\cdots,t$,则 G 也必是可解群.

5. 证明以下命题:

(1) $n \geqslant 3$ 时,A_n 可由所有的 3-轮换生成:$A_n = \langle \{(ijk)\} \rangle$;

(2) $S_n^{(1)} = A_n$,从而 $A_n \lhd S_n$;

(3) $n \leqslant 4$ 时,S_n 是可解群;$n \geqslant 5$ 时,S_n 不是可解群.

6. 记 $K = \{(1),(12)(34),(13)(24),(14)(23)\}$,证明:$S_4$ 的非平凡正规子群只有 A_4 和 K.

第二章　环

前面我们介绍了群的概念及其主要性质.群是只有一种二元运算的代数体系,然而数学中出现的代数体系往往有两种或更多种运算.例如,数的集合中就有加法和乘法两种运算(减法和除法是它们的逆运算);多项式或矩阵的集合中都有加法和乘法两种运算.当然这两种代数运算之间经常是相互联系的,例如它们之间满足乘法对加法的分配律.这些代数体系有什么运算规律和普遍性质,是需要研究的问题.本章将研究具有两种二元运算的代数体系,即环的基本运算规律和基本性质.

§2.1　环、子环与商环

定义 2.1.1　设 R 是一个非空集合,如果在 R 中有两种二元运算,对于其中一种运算(用加法表示 R)成为一个交换群,对于另外一种运算(用乘法表示 R)成为半群,而且满足下列两条分配律:

$$a(b+c)=ab+ac,(a+b)c=ac+bc,\forall a,b,c\in R,$$

则称 R 为一个**环**.

在研究环的基本性质以前,先来看几个环的例子.

例 1　所有的数域在数的加法和乘法两种运算下都构成环.

例 2　设P是一个数域,则P上所有一元多项式组成的集合在多项式的加法和乘法这两种运算下构成一个环,称为数域P上的

一元多项式环，记为$P[x]$. 同样，P上所有n阶方阵在矩阵的加法和乘法下也构成一个环，记为$P^{n\times n}$.

例 3 前面我们已经知道整数的模m剩余类$\mathbb{Z}_m$在加法下成为一个交换群，现在我们在$\mathbb{Z}_m$中定义乘法运算：

$$\overline{a}\circ\overline{b}=\overline{ab},\ \forall\, a,b\in\mathbb{Z},$$

容易验证上述运算定义是合理的，事实上，若$\overline{a}=\overline{a_1}$，$\overline{b}=\overline{b_1}$，则$m\mid(a-a_1)$，$m\mid(b-b_1)$，又因为$ab-a_1b_1=(a-a_1)b+a_1(b-b_1)$，故$m\mid(ab-a_1b_1)$，即$\overline{ab}=\overline{a_1b_1}$. 从而上述定义与代表元的选取无关. 下面证明$\mathbb{Z}_m$在上述加法和乘法下成为一个环. 事实上，$\forall\, a,b,c\in\mathbb{Z}$.

$$\overline{a}\circ(\overline{b}\circ\overline{c})=\overline{a}\circ\overline{bc}=\overline{abc}.$$

同样，$(\overline{a}\circ\overline{b})\circ\overline{c}=\overline{abc}$. 故“$\circ$”满足结合律，从而$|\mathbb{Z}_m;\circ|$是半群. 此外，$\forall\, a,b,c\in\mathbb{Z}$，

$$\begin{aligned}\overline{a}\circ(\overline{b}+\overline{c})&=\overline{a}\circ\overline{(b+c)}\\&=\overline{a(b+c)}=\overline{ab+ac}\\&=\overline{ab+ac}=\overline{ab}+\overline{ac}\\&=\overline{a}\circ\overline{b}+\overline{a}\circ\overline{c}.\end{aligned}$$

同理，$(\overline{a}+\overline{b})\circ\overline{c}=\overline{a}\circ\overline{c}+\overline{b}\circ\overline{c}$，故$\mathbb{Z}_m$满足“$\circ$”对于“$+$”的两条分配律，因此是环.

由环的定义，在一个环R中有两种运算，即加法与乘法. 为方便计，我们将R对于加法做成的群的单位元记为0，称为R的零元. 设$a\in R$，我们将a在加法运算下的逆记为$-a$，称为a的负元. 将m个a连加得到的结果记为ma，并规定$0a=0$，$(-n)a=-(na)$. 同时将m个a连乘得到的结果记为a^m. 此外，将$a+(-b)$简写成$a-b$.

容易看出下列性质：

性质 2.1.1 (1) $(m+n)a=ma+na$，$m(-a)=-(ma)$，$(mn)a=m(na)$，

$m(a+b)=ma+mb$, $\forall a,b\in R$, $m,n\in\mathbb{Z}$.

(2) $a^m a^n=a^{m+n}$, $(a^m)^n=a^{mn}$, $\forall m,n\in\mathbb{N}$, $a\in R$.

性质 2.1.2 $\left(\sum_{i=1}^{n}a_i\right)\left(\sum_{j=1}^{m}b_j\right)=\sum_{i=1}^{n}\sum_{j=1}^{m}a_ib_j$.

性质 2.1.3 $\forall a,b\in R$,有 $a0=0a=0$,这里 0 为 R 的零元;此外,$(-a)b=a(-b)=-ab$,$(-a)(-b)=ab$.

这些性质的证明,可以用环的定义直接得出,我们将它留作习题.

我们知道,两个非零数的乘积一定非零,即数的乘法满足消去律.但是,在一般环中乘法消去律未必成立.例如,在前面的例 3 中,我们考虑$\mathbb{Z}_4$这个环,则$\bar{2}\neq\bar{0}$,但是$\bar{2}\ \bar{2}=\bar{4}=\bar{0}$,因此$\mathbb{Z}_4$不满足消去律.在线性代数中,我们知道$P^{n\times n}$也不满足消去律.为此,我们在环中定义零因子的概念.

定义 2.1.2 设 R 为一个环,$a,b\in R$,且 $a\neq0$,$b\neq0$,若 $ab=0$,则称 a 为 R 中的一个**左零因子**,b 为 R 中的一个**右零因子**,都简称为**零因子**.

下面我们定义几种特殊的环.

交换环:R 对于乘法交换的环.

幺环:R 对于乘法成为幺半群的环,一般将 R 对于乘法的单位元记为 1 或 e.

交换幺环:R 对于乘法成为交换幺半群的环.

整环:无零因子的交换幺环.

除环(体):R 中所有非零元对于乘法构成群的环.

域:交换的除环.即 R 中所有非零元对于乘法构成交换群的环.

由定义,所有域都是除环,在接下来的内容中,读者将看出这个包含关系是真包含.

容易看出任何数域都是域.下面给出一个非数域的域的例子.

例 4 在例 3 中我们取 $m = p$ 为一个素数，则 $\mathbb{Z}_p = \{\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{p-1}\}$.

容易看出 $\bar{1}$ 为幺元，又显然乘法是交换的，因而 $\mathbb{Z}_p$ 是交换幺环. 因 p 是素数，对任何 $a \in \mathbb{N}, a < p$，必存在 $l, n \in \mathbb{Z}$ 使得

$$la + np = 1,$$

于是 $\overline{la + np} = \overline{la} + \overline{np} = \overline{la} + \bar{0} = \bar{l}\,\bar{a} = \bar{1}$. 故对于乘法来说 $\bar{a}$ 的逆为 $\bar{l}$. 故 $\mathbb{Z}_p$ 为一个域. 由于它是有限集合，故不可能是数域.

关于零因子，我们有

命题 2.1.4 一个环 R 没有零因子，当且仅当 R 满足左右消去律.

证 若 R 没有零因子，设 $ax = ay$ 且 $a \neq 0$，则 $a(x - y) = 0$. 若 $x \neq y$，则 $x - y \neq 0$，与 R 没有零因子矛盾，故 $x = y$，即 R 满足左消去律. 同理可证 R 满足右消去律. 反之，若 R 满足左右消去律，且 $ax = 0$，若 $a \neq 0$，则 $ax = a0$，由左消去律，有 $x = 0$，故 R 没有右零因子. 同理 R 也没有左零因子. □

对于无零因子环，有一个重要的概念，即环的特征. 我们首先证明：

命题 2.1.5 设 $R \neq \{0\}$，且为无零因子环，则 R 中所有的非零元对于 R 的加法具有相同的阶，且当这一共同的阶有限时，必为素数.

证 记 $R^* = R - \{0\}$. 若 R^* 中所有元素对于加法的阶都是无穷，则命题正确. 若存在 $a \in R^*$ 的阶为有限 n 阶的，则 $\forall b \in R^*$，有

$$(na)b = a(nb) = 0,$$

因为 R 无零因子，故 $nb = 0$，这说明 b 的阶不超过 n. 设 b 的阶为 m，则 $mb = 0$，于是

$$a(mb) = (ma)b = 0,$$

故 $ma = 0$，因此 $n \leqslant m$，于是 $m = n$. 故 R^* 中所有元素对于加法的阶都等于 n. 下证 n 为素数，若 n 不是素数，则存在 $n_1, n_2 \in \mathbb{N}$,

$n_1 < n, n_2 < n$，使得 $n = n_1 n_2$，于是 $n_1 a \neq 0, n_2 a \neq 0$，但是

$$(n_1 a)(n_2 a) = na^2 = (na)a = 0.$$

这与 R 无零因子矛盾. □

现在我们可以引进环的特征的概念.

定义 2.1.3 设 R 为无零因子环，若 R 中所有的非零元都是无穷阶的，则称 R 的**特征**为 0；若 R 中所有的非零元都是有限 p 阶的（p 为素数），则称 R 的**特征**为 p. 环 R 的特征记为 Ch R.

对于特征为 p 的环，有两个重要的等式，我们将它的证明留作习题.

命题 2.1.6 设无零因子的交换环 R 的特征为 p，p 为素数，则

$$(a+b)^p = a^p + b^p, (a-b)^p = a^p - b^p, \forall a, b \in R.$$

最后我们介绍子环、理想和商环的概念.

定义 2.1.4 设 R 为环，若 R 的非空子集 R_1 对于 R 的加法与乘法也构成环，则称 R_1 为 R 的**子环**. 若子环 R_1 还满足 $ra \in R_1, \forall r \in R, a \in R_1$（$ar \in R_1, \forall a \in R_1, r \in R$），则称 R_1 为 R 的**左理想（右理想）**. 若 R 的子环 I 既是 R 的左理想，又是 R 的右理想，则称 I 为 R 的**双边理想**，简称**理想**.

在本书中，我们一般考虑的是双边理想. 因此，以后凡是出现“理想”这一名称，都是指双边理想.

命题 2.1.7 设 R 为一个环，则

(1) R 的非空子集 R_1 为 R 的子环的充要条件是：$\forall a, b \in R_1$ 有 $a - b \in R_1, ab \in R_1$；

(2) R 的非空子集 I 为 R 的理想的充分必要条件是，$\forall a, b \in I, \forall x, y \in R$，有 $a - b \in I, xa, ay \in I$.

证 (1) “$\Longrightarrow$”若 R_1 是 R 的子环，则 R_1 对于 R 的加法成为加法群，故 R_1 为加法群 R 的子群，因此 $a - b \in R_1, \forall a, b \in R_1$. 此外，$R_1$ 对于 R 的乘法成为半群，特别对于 R 的乘法封闭，故 ab

$\in R_1, \forall a, b \in R_1$.

"$\Longleftarrow$"因为 $a-b \in R_1, \forall a, b \in R_1$，故 R_1 是 R 作为加法群的子群，因而是加法群. 又 $ab \in R_1, \forall a, b \in R_1$，故 R_1 对于 R 的乘法封闭. 由于 R 对于乘法满足结合律，故 R_1 对于乘法也满足结合律，从而 R_1 对于乘法构成半群. 又 R 满足乘法对于加法的分配律，故 R_1 也满足乘法对于加法的分配律. 故 R_1 在 R 的加法和乘法下构成环，从而是 R 的子环.

(2) 由于理想必为子环，故由(1)及理想的定义直接可得.

□

推论 2.1.8 设 R 为幺环，则 R 的非空子集 I 为理想的充分必要条件是 $\forall a, b \in I, x, y \in R$，有 $a-b \in I, xay \in I$.

推论 2.1.9 设 R 为交换环，则 R 的非空子集 I 为理想的充分必要条件是 $\forall a, b \in I, x \in R$，有 $a-b \in I, xa \in I$.

任何环 R 至少有两个理想：R 本身和 $\{0\}$，它们都称为**平凡理想**. 如果 R 是交换环，则左理想、右理想和理想这三个概念是一致的. 人们通常利用 R 的非空子集来构造理想，为此需要下列结果.

命题 2.1.10 设 R 为环，$R_i, i \in X$ 为 R 的一簇理想，则 $\bigcap_{i \in X} R_i$ 也是 R 的理想.

证 由于 $0 \in \bigcap_{i \in X} R_i$，故 $\bigcap_{i \in X} R_i \neq \varnothing$. 设 $a, b \in \bigcap_{i \in X} R_i$，则 $\forall i \in X$，有 $a, b \in R_i$，由于 R_i 是理想，故 $a-b \in R_i$，且对任何 $x, y \in R$，有 $xa, ay \in R_i$. 故 $a-b \in \bigcap_{i \in X} R_i$，且 $\forall x, y \in R, xa, ay \in \bigcap_{i \in X} R_i$. 故 $\bigcap_{i \in X} R_i$ 是理想. □

值得注意的是命题 2.1.10 中的 X 可以是无限集. 现在设 A 为 R 的非空子集，则由上述命题，所有 R 中包含 A 的理想(这样的理想是存在的，例如 R 本身就是一个)之交仍为 R 的理想，称为由 A **生成的理想**，记为 $\langle A \rangle$. 它是 R 中包含集合 A 的最小理想.

若 R 为交换幺环，则 $\langle A \rangle$ 是由所有形如

$$\sum_{i=1}^{n} x_i a_i, n \in \mathbf{N}, x_i \in R, a_i \in A, i = 1,2,\cdots,n,$$

的元素组成的集合(记为 L).事实上,由于 $\forall a \in A, a = 1 \cdot a$(1 为 R 的幺元),故 $A \subseteq L$,此外,利用命题 2.1.7 给出的充分必要条件容易看出 L 是 R 的理想;另一方面,若 I 为 R 的理想且包含 A,则 $\forall x_i \in R, a_i \in A, 1 \leqslant i \leqslant n$,有 $x_i a_i \in I$,故 $\sum x_i a_i \in I$.故 $L \subseteq I$,这说明 L 是包含 A 的最小理想,故 $L = \langle A \rangle$.

特别,当 A 只包含一个元素 a 时,记 $\langle A \rangle$ 为 $\langle a \rangle$,称为由 a 生成的**主理想**.

例 5 若 R 为幺环,则

$$\langle a \rangle = \left\{ \sum_{i=1}^{m} x_i a y_i \mid x_i, y_i \in R, i = 1,2,\cdots,m, m \geqslant 1 \right\};$$

若 R 为交换环,则

$$\langle a \rangle = \{ ra + na \mid r \in R, n \in \mathbf{Z} \};$$

若 R 为交换幺环,则

$$\langle a \rangle = \{ ra \mid r \in R \}.$$

下面的定理给出了商环的定义.

定理 2.1.11 设 I 为环 R 的理想,在 R 中定义关系"$\sim$":

$$a \sim b \Longleftrightarrow a - b \in I.$$

则关系"$\sim$"是 R 中的等价关系,且对于 R 的加法和乘法都是同余关系.将 $a \in R$ 所在的等价类记为 $a + I$,在商集合 $R/\sim = R/I$ 上定义加法和乘法如下:

$$(a + I) + (b + I) = (a + b) + I,$$

$$(a + I)(b + I) = ab + I.$$

则 R/I 对于上述运算构成一个环,称为 R 对于理想 I 的**商环**.

证 先证明"$\sim$"为等价关系.设 $a \in R$,则 $a - a = 0 \in I$,故"$\sim$"满足反身性;又若 $a \sim b$,则 $b - a = -(a - b) \in I$,故"$\sim$"满足对称性;此外,设 $a \sim b, b \sim c$,则 $a - c = (a - b) + (b - c) \in I$,故"$\sim$"满足传递性.故"$\sim$"是等价关系.由于 R 对于加法来说是

交换群，因而 I 是加法群 R 的正规子群，从而关系“$\sim$”对于加法是同余关系. 对于乘法，设 $a\sim a_1, b\sim b_1$，则 $a-a_1\in I, b-b_1\in I$，由于 I 是理想，故

$$ab-a_1b_1=ab-ab_1+ab_1-a_1b_1=a(b-b_1)+(a-a_1)b_1\in I,$$

即 $ab\sim a_1b_1$，故关系“$\sim$”对于乘法也是同余关系. 显然 R/I 对于所定义的加法是交换群，又由于 R 满足结合律，由定义 R/I 的乘法也满足结合律. 最后，$\forall a,b,c\in R$ 有

$$\begin{aligned}((a+I)+(b+I))(c+I)&=((a+b)+I)(c+I)=(a+b)c+I\\&=(ac+bc)+I=(ac+I)+(bc+I)\\&=(a+I)(c+I)+(b+I)(c+I).\end{aligned}$$

类似可证

$$(a+I)((b+I)+(c+I))=(a+I)(b+I)+(a+I)(c+I).$$

即分配律成立. 因此 R/I 是环. □

推论 2.1.12 若 R 为交换环，则 R/I 也是交换环.

推论 2.1.13 若 R 为幺环，则 R/I 也是幺环，且 $1+I$ 为单位元.

习 题

1. 判断下列集合在指定的加法和乘法运算下是否构成环：

(1) $R=\{3n\mid n\in\mathbf{Z}\}$，运算为数的普通加法和乘法；

(2) $R=\{a+b\sqrt{5}\mid a,b\in\mathbf{Q}\}$，运算为数的普通加法与乘法；

(3) $R=\mathbf{Z}$，加法为 $a\oplus b=a+b-1, a,b\in R$，乘法为 $a\otimes b=a+b-ab, a,b\in R$；

(4) $R=\mathbf{Z}\times\mathbf{Z}$，加法与乘法定义为：

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

$$(a,b)(c,d)=(ac,bd),\forall(a,b),(c,d)\in\mathbf{Z}\times\mathbf{Z};$$

(5) $R=\{\boldsymbol{A}\in P^{n\times n}\mid \boldsymbol{A}=\boldsymbol{A}'\}$，运算为矩阵的普通加法与乘法；

(6) $R=\{\boldsymbol{A}\in\mathbf{R}^{n\times n}\mid \det\boldsymbol{A}\in\mathbf{Z}\}$，运算为矩阵的普通加法与乘法.

2. 设 R 是无零因子环，只有有限个元素但至少有两个元素. 证明：R 是除环(体).

3. 设 R 是环，若存在 $a_1, a_2, \cdots, a_n \in R, a_i \neq 0, i = 1, 2, \cdots, n$ 使得 $a_1 a_2 \cdots a_n = 0$，证明：R 有零因子.

4. 证明本节的性质 2.1.1—2.1.3.

5. 设 R 为环，$a \in R$，证明：

$$\langle a \rangle = \left\{ \sum_{i=1}^{m} x_i a y_i + ra + as + na \mid r, s \in R, x_i, y_i \in R, 1 \leqslant i \leqslant m, m \geqslant 1, n \in \mathbf{Z} \right\}.$$

6. 设 R 为无零因子环，I 为 R 的理想，问商环 R/I 是否一定是无零因子环？

7. 设 P 为数域. 证明：环 $P^{n \times n}$（普通加法与乘法）没有非平凡理想.

8. 设 R 为环，若 R 作为加法群是循环群，证明 R 是交换环.

补充题

1. 设集合 $R = \{a, b, c\}$，在 R 上定义加法和乘法，若加法“+”和乘法“·”的运算表分别为：

+	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

·	a	b	c
a	a	a	a
b	a	b	c
c	a	b	c

问 R 是否构成环？

2. 设 R 为幺环，称 $x \in R$ 为**可逆元**，若存在 $y \in R$ 使得 $xy = yx = 1$. 设 $a, b \in R$，证明：$1 - ab$ 可逆当且仅当 $1 - ba$ 可逆.

3. 设 R 为环，$a \in R$. 若 $\exists\, m \in \mathbf{N}$ 使得 $a^m = 0$，则称 a 为**幂零元**. 证明：若 R 为交换环，则 R 中所有幂零元组成的集合构成 R 的理想.

4. 设 R 为环，$a \in R$，若 $a \neq 0$ 且 $a^2 = a$，则称 a 为**幂等元**. 证明：

(1) 若环 R 的所有非零元素都是幂等元，则 R 必为交换环；

(2) 若 R 为无零因子环，且存在幂等元，则 R 只有惟一的幂等元，且 R 为幺环.

5. 设 $R = \mathbf{C} \times \mathbf{C}$，在 R 上定义加法与乘法如下：

$$(\alpha_1, \beta_1) + (\alpha_2, \beta_2) = (\alpha_1 + \alpha_2, \beta_1 + \beta_2),$$

$$(\alpha_1, \beta_1)(\alpha_2, \beta_2) = (\alpha_1 \alpha_2 - \beta_1 \overline{\beta}_2, \alpha_1 \beta_2 + \beta_1 \overline{\alpha}_2),$$

其中 $\bar{a}$ 为 a 的共轭复数. 证明: R 在上述运算下构成一个除环, 但不构成域. 称 R 为**四元数除环**.

6. 设 R 为无零因子环, e 是 R 的关于乘法的左(右)幺元, 证明: e 必是 R 的幺元.

§2.2 环的同态定理

在上一章中, 我们讲述了群的同态与同构. 在环论中, 同样需要研究同态与同构, 这样才能比较各种环之间的异同, 找出联系. 本节我们介绍这方面的主要内容. 我们先给出同态的定义.

定义 2.2.1 设 R_1、R_2 为两个环, f 为 R_1 到 R_2 的映射, 称 f 为一个**同态**, 如果下列条件成立:

(1) $f(a+b)=f(a)+f(b)$, $\forall a, b \in R_1$;

(2) $f(ab)=f(a)f(b)$, $\forall a, b \in R_1$.

若同态 f 是单射, 则称 f 为**单同态**; 若同态 f 是满射, 则称 f 为**满同态**. 若 f 为同态且是双射, 则称 f 为**同构**, 这时也称环 R_1 与 R_2 **同构**, 记为 $R_1 \simeq R_2$.

注意定义中环同态 f 事实上是两个环 R_1, R_2 分别作为加法群和乘法半群的同态. 因此下列性质是显然的: $f(0)=0$, $f(-a)=-f(a)$, $\forall a \in R_1$.

例 1 设 R_1、R_2 为两个环, 定义 R_1 到 R_2 的映射 f 为 $f(a)=0$, $\forall a \in R_1$, 则 f 是一个同态, 称为零同态.

例 2 设 P 为一个数域. V 为 P 上的 n 维线性空间. 设 End V 为 V 上所有线性变换的集合, 则 End V 对于线性变换的加法和乘法构成一个环. 取定 V 的一组基 $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$, 定义 End V 到 $P^{n\times n}$ 的映射:

$$\phi(A)=M(A;\alpha_1,\alpha_2,\cdots,\alpha_n), A \in \text{End } V.$$

其中 $M(A;\alpha_1,\alpha_2,\cdots,\alpha_n)$ 为 A 在 $\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$ 下的矩阵. 则由

高等代数中学过的知识知 ϕ 为一个环同构.

例 3 设 I 是环 R 的理想,则 R 到 R/I 的自然映射

$$\pi: R \to R/I, \pi(a) = a + I,$$

为一个满同态,称为自然同态.

下面命题的证明与群论中类似结果的证明非常相似,因此略去.

命题 2.2.1 设 f 为环 R_1 到 R_2 的同态,g 是环 R_2 到 R_3 的同态.则 gf 为 R_1 到 R_3 的同态.若 f, g 都是单同态,则 gf 是单同态;若 f, g 都是满同态,则 gf 是满同态.若 f, g 都是同构,则 gf 也是同构.当 f 为同构时,f^{-1} 为 R_2 到 R_1 的同构.

命题 2.2.2 设 f 为环 R_1 到 R_2 的满同态,则 $\ker f = f^{-1}(\{0\}) = \{a \in R_1 \mid f(a) = 0\}$ 为 R_1 的理想.

证 由于 $f(0) = 0$,故 $\ker f \neq \varnothing$. $\forall a, b \in \ker f$,有 $f(a - b) = f(a) - f(b) = 0 - 0 = 0$,故 $a - b \in \ker f$;又 $\forall x \in R_1, a \in \ker f$,有 $f(ax) = f(a)f(x) = 0, f(xa) = f(x)f(a) = 0$,故 $ax, xa \in \ker f$.据命题 2.1.7,$\ker f$ 是 R_1 的理想. □

下面的定理是非常重要的,称为**环的同态基本定理**.

定理 2.2.3 设 f 是环 R_1 到环 R_2 的满同态,则 $R_1/\ker f \simeq R_2$.

证明 f 是环同态,因而是加法群 R_1 到 R_2 的同态,设 π 为环 R_1 到 $R_1/\ker f$ 的自然同态,则 π 也是加法群 R_1 到 $R_1/\ker f$ 的自然同态,由群的同态基本定理及其证明,存在由加法群 $R_1/\ker f$ 到 R_2 的群同构 $\overline{f}$ 使得 $f = \overline{f} \circ \pi$.下证 $\overline{f}$ 为环同构,事实上,$\forall a, b \in R_1$,

$$\begin{aligned}\overline{f}(\pi(a)\pi(b)) &= \overline{f}(\pi(ab)) = \overline{f} \circ \pi(ab) = f(ab) \\ &= f(a)f(b) = \overline{f}(\pi(a))\overline{f}(\pi(b)).\end{aligned}$$

故 $\overline{f}$ 为 $R_1/\ker f$ 到 R_2 的环同构,因而 $R_1/\ker f \simeq R_2$. □

定理 2.2.4 设 f 是环 R_1 到 R_2 的满同态,$K = \ker f$,则有下

列结论：

(1) f 建立了 R_1 中包含 K 的子环与 R_2 的子环之间的一一对应；

(2) 上述映射将理想对应到理想；

(3) 如果 I 是 R_1 的理想，且包含 K，则有 $R_1/I \simeq R_2/f(I)$.

证 (1) 由定理 1.4.8 知，f 建立了 R_1 中包含 K 的加法子群到 R_2 的加法子群之间的一一对应. 设 H 为 R_1 的子环，$H \supseteq K$，则 $\forall a', b' \in f(H)$，存在 $a, b \in H$，使 $f(a)=a'$，$f(b)=b'$，故 $a'-b'=f(a)-f(b)=f(a-b)\in f(H)$，$a'b'=f(a)f(b)=f(ab)\in f(H)$. 从而 $f(H)$ 是 R_2 的子环. 反之，设 $H' \subseteq R_2$ 是子环，则 $f^{-1}(H')=\{a\in R \mid f(a)\in H'\}$ 是 R_1 中包含 K 的加法子群. 又 $\forall a, b \in f^{-1}(H')$，有 $f(a-b)=f(a)-f(b)\in H'$，$f(ab)=f(a)f(b)\in H'$，故 $a-b\in f^{-1}(H')$，$ab\in f^{-1}(H')$. 从而 $f^{-1}(H')$ 是 R_1 的子环. 于是(1)成立.

(2) 设 $I \supseteq K$ 为 R_1 的理想，则由(1)，$f(I)$ 为 R_2 的子环. 又 $\forall a'=f(a)\in f(I)$，$x'\in R_2$，由于 f 为满射，可取 $x\in R$ 使 $f(x)=x'$，故由 I 为理想得 $a'x'=f(a)f(x)=f(ax)\in f(I)$，$x'a'=f(x)f(a)=f(xa)\in f(I)$. 从而 $f(I)$ 为 R_2 的理想. 另一方面，若 I' 为 R_2 的理想，则由(1)，$f^{-1}(I')$ 为包含 K 的子环. 又 $\forall a\in f^{-1}(I')$，$x\in R_1$，由于 I' 为理想，有 $f(ax)=f(a)f(x)\in I'$，$f(xa)=f(x)f(a)\in I'$，故 $ax, xa\in f^{-1}(I')$. 从而 $f^{-1}(I')$ 为 R_1 的理想.

(3) 设 I 是 R_1 的理想，且 $I \supseteq K$. 又设 π 是 R_1 到 R_1/I 的自然同态，π' 是 R_2 到 $R_2/f(I)$ 的自然同态，于是 $\pi'\circ f$ 是 R_1 到 $R_2/f(I)$ 的满同态，下面证明 $\ker(\pi'\circ f)=I$，事实上，若 $x\in I$，则 $f(x)\in f(I)$，从而 $\pi'(f(x))=0$，故 $x\in\ker(\pi'\circ f)$，反之，若 $x\in\ker(\pi'\circ f)$，则由 π' 的定义得 $f(x)\in f(I)$，故 $x\in f^{-1}(f(I))$，由(1)及(2)，f 建立了 R_1 中包含 K 的理想到 R_2 的理想的一一对应，而

作为理想 $f(f^{-1}(f(I)))=f(I)$，故 $f^{-1}(f(I))=I$，于是 $\ker(\pi' f)=I$. 再利用定理 2.2.3，结论成立. □

推论 2.2.5 设 I_1, I_2 均为环 R 的理想，且 $I_1 \subseteq I_2$，则有 $R/I_2 \simeq (R/I_1)/(I_2/I_1)$.

证 在定理 2.2.4，(3) 中取 $R_1=R$，$R_2=R_1/I_1$，f 为 R_1 到 R_2 的自然同态，即得证. □

习 题

1. 设 f 为环 R 到 R' 的满同态，且 $R' \neq \{0\}$. 证明：

(1) 若 R 为交换环，则 R' 也为交换环；

(2) 若 R 为幺环，则 R' 也为幺环；

(3) 若 R 为除环，则 R' 也为除环；

(4) 若 R 为域，则 R' 也为域；

(5) 若 R 为整环，是否 R' 必为整环？为什么？

2. 设 p 为一个素数，证明：环 $\mathbf{Z}_p$ 只有两个自同态，即零同态和恒等同态.

3. 证明：商环 $\mathbf{R}[x]/\langle x^2+1\rangle$ 与环 $\mathbf{C}$ 同构.

4. 证明：加法群 $\mathbf{Z}$ 与加法群 $\{2n \mid n \in \mathbf{Z}\}$ 同构，但是它们作为环（普通加法与乘法）不同构.

5. 设 R 为一个除环，R^* 为其非零元组成的乘法群，证明：R 作为加法群不与群 R^* 同构.

6. 证明：映射 $a+b\sqrt{-1} \to a-b\sqrt{-1}$ 是环 $\mathbf{C}$ 的同构.

7. 设 φ 为环 R 到 R' 的满同态，证明：φ 为同构 $\Longleftrightarrow \ker \varphi = \{0\}$.

8. 设 R 是一个环. 在 $\mathbf{Z}\times R$ 上定义加法与乘法如下：

$$(m,a)+(n,b)=(m+n,a+b),$$

$$(m,a)\cdot(n,b)=(mn,na+mb+ab),\ m,n\in\mathbf{Z},\ a,b\in R.$$

证明：$\mathbf{Z}\times R$ 是一个环，且 R 与 $\mathbf{Z}\times R$ 的一个理想同构.

补充题

1. 设 R 为无零因子环，含有 p 个元素，p 为素数. 证明：R 为域，且与 $\mathbf{Z}_p$ 同构.

2. 找出环Z_{12}中所有成为域的子环.

3. 证明:由所有形如

$$\begin{pmatrix} a+b\sqrt{-1} & c+d\sqrt{-1} \\ -c+d\sqrt{-1} & a-b\sqrt{-1} \end{pmatrix}, a,b,c,d\in\mathbb{R},$$

的矩阵组成的集合,在矩阵的加法与乘法运算下,构成一个与四元数除环同构的除环.

4. (挖补定理) 设R',S为两个环,$R'\cap S=\varnothing$.设S含有一个子环R使得R与R'同构.证明:存在一个环S',它与S同构,且包含R'作为一个子环.

5. 设R为无零因子幺环,证明:R中包含幺元e的最小子环必与Z_p(p为素数)或Z同构.

6. 设R为特征为p(p为素数)的交换幺环,证明:$(a+b)^p=a^p+b^p$,$(a-b)^p=a^p-b^p$,$\forall a,b\in R$.

§2.3 素理想与极大理想

本节介绍两种特殊的理想,这在讨论下面的内容时将是有用的,而且这两种理想在实际中也是非常重要的.我们还将讨论这两种理想与商环之间的关系.

定义 2.3.1 设I为环R的理想,如果由$ab\in I$可以推出$a\in I$或$b\in I$,则称I为R的一个**素理想**.

例 1 在整数环Z中,考虑由一个元素p生成的理想$\langle p\rangle$,则当p为素数时,$\langle p\rangle$为素理想.事实上,设$ab\in\langle p\rangle$,则$p\mid ab$,由于p为素数,故$p\mid a$或$p\mid b$,即$a\in\langle p\rangle$或$b\in\langle p\rangle$,所以$\langle p\rangle$为素理想.

定理 2.3.1 设R为交换幺环,I是R的一个理想,$I\neq R$,则I是素理想当且仅当R/I为整环.

证 设I为素理想,由于R是交换幺环,由定理 2.1.11 的推论,R/I也是交换幺环.设$(a+I)(b+I)=0+I$,则$ab+I=0+$

I,即 $ab\in I$.由于 I 是素理想,故 $a\in I$ 或 $b\in I$.这说明 $a+I=0+I$ 或 $b+I=0+I$,即 R/I 中没有零因子,从而是整环.

反之,设 R/I 为整环,且 $ab\in I$,于是 $ab+I=(a+I)(b+I)=0+I$,由于 R/I 没有零因子,故 $a+I=0+I$ 或 $b+I=0+I$,即 $a\in I$ 或 $b\in I$,故 I 为素理想. □

推论 2.3.2 交换幺环 R 是整环的充分必要条件是 $\{0\}$ 为 R 的素理想.

这是因为 $R\simeq R/\{0\}$. □

定理 2.3.3 设 f 为交换幺环 R 到 R' 的满同态,I 是 R 中包含 $K=\ker f$ 的一个素理想,则 $f(I)$ 是 R' 的素理想.

证 由定理 2.2.4,$f(I)$ 为 R' 的理想.设 $a',b'\in R'$,且 $a'b'\in f(I)$,则存在 $c\in I$ 使得 $a'b'=f(c)$.由于 f 为满同态,故存在 $a,b\in R$ 使得 $f(a)=a'$,$f(b)=b'$,于是 $f(a)f(b)=f(c)$.由于 f 为同态,故 $f(ab-c)=f(a)f(b)-f(c)=0$,即 $ab-c\in K\subseteq I$,故 $ab\in I$.注意到 I 为素理想,故有 $a\in I$ 或 $b\in I$,于是 $a'=f(a)\in f(I)$ 或 $b'=f(b)\in f(I)$.故 $f(I)$ 为素理想. □

定理 2.3.4 设 R 是交换幺环,I 是 R 的真理想,则 I 是 R 的素理想当且仅当对任何理想 M,N,由 $MN\subset I$ 可推出 $M\subset I$ 或 $N\subset I$.

证 必要性.若 I 是 R 的素理想,M,N 是 R 的理想且 $MN\subset I$,设 M 不包含于 I 且 N 不包含于 I,则存在 $a\in M,b\in N$ 且 $a\notin I,b\notin I$,但是 $ab\in MN\subset I$.这与 I 是素理想矛盾.

充分性.假设 I 满足定理的条件但不是素理想,则必存在 $a,b\in R$,$ab\in I$ 且 $a\notin I,b\notin I$.现在令 $M=\langle a\rangle,N=\langle b\rangle$.则由于 R 是交换环,故 $MN=\langle ab\rangle\subset I$.这与定理的条件矛盾,故 I 必是素理想. □

下面介绍极大理想的概念.

定义 2.3.2 设 R 是交换幺环,M 是 R 的理想,若 $M\neq R$,且不存在 R 的真理想 N 使得

$$M \subset N, M \neq N,$$

则称 M 为 R 的**极大理想**.

例 2 考虑例 1 中的整数环,设 p 是素数,则$\langle p\rangle$是Z的极大理想.事实上,设 N 是Z的理想,且$\langle p\rangle \subset N$,$\langle p\rangle \neq N$,则必存在 $l \in N$,使 $l \notin \langle p\rangle$,由于 p 是素数,故 p, l 互素,从而存在整数 a, b 使 $ap + bl = 1$,故 $1 \in N$,于是任何整数 $k = k \times 1 \in N$,从而 N 不是 R 的真理想.故$\langle p\rangle$是极大理想.

例 3 若 R 为域,则$\{0\}$为 R 的极大理想.事实上,设 N 为 R 的理想,且 $N \neq \{0\}$,则必存在 $a \in N$ 且 $a \neq 0$,由于域中每个非零元都存在逆元,从而 $1 = aa^{-1} \in N$,故 $\forall a \in R$,$a = a \cdot 1 \in N$,因此 $N = R$.故$\{0\}$为极大理想.

例 3 中的逆命题也成立,即若 R 是交换幺环,且$\{0\}$为 R 的极大理想,则 R 是域.证明留给读者.

定理 2.3.5 设 R 为交换幺环,M 为 R 的理想,则 M 是 R 的极大理想当且仅当 R/M 为域.

证 设 M 为 R 的极大理想,考虑自然同态:$\pi: R \to R/M$.由定理 2.2.4,对于 R/M 的任何理想 I,必有 R 的包含 M 的理想 A,使 $I = \pi(a) = A/M$.由于 M 为极大理想,故 $A = M$ 或 $A = R$,即 $I = \{0\}$或 $I = R/M$,故$\{0\}$为 R/M 的极大理想,即 R/M 是域.

反之,设 R/M 是域,则$\{0\}$是 R/M 的极大理想.设 A 为 R 的包含 M 的理想,则 A/M 是 R/M 的理想,故 $A/M = \{0\}$或 $A/M = R/M$,即 $A = M$ 或 $A = R$.故 M 为极大理想. □

推论 2.3.6 交换幺环的极大理想必为素理想.

这是因为域必为整环.

习 题

1. 设 R 为交换幺环,证明:R 为域当且仅当$\{0\}$为 R 的极大理想.
2. 证明:$\langle x\rangle$是$Z[x]$的素理想,但不是极大理想.
3. 找出Z_{12}的所有素理想和极大理想.

4. 设 p 为素数，试问$\langle p^2\rangle$是不是Z的素理想？$\langle 2p\rangle$是不是Z的素理想？

5. 设 $R=\{2n\mid n\in\mathbf{Z}\}$，证明：$\langle 4\rangle$是 R 的极大理想. $R/\langle 4\rangle$是域吗？

6. 设$\mathbf{Z}[\sqrt{-1}]=\{a+b\sqrt{-1}\mid a,b\in\mathbf{Z}\}$，运算为普通的加法和乘法. 证明：$\mathbf{Z}[\sqrt{-1}]$是整环，且$\mathbf{Z}[\sqrt{-1}]/\langle 1+\sqrt{-1}\rangle$是一个域.

7. 设 A 为环 R 的理想，P 为 A 的素理想，且 $P\neq A$. 证明：P 是 R 的理想.

8. 设 N 是环 R 的理想，且 R/N 是除环，证明：

(1) N 是 R 的极大理想；

(2) $\forall a\in R$，由 $a^2\in N$ 可推出 $a\in N$.

补充题

1. 设 $m\in\mathbf{N}, m>1$. 令

$$A=\{f(x)\mid f(x)\in\mathbf{Z}[x], m\mid f(0)\}.$$

证明：A 是$\mathbf{Z}[x]$的理想，且$\langle x\rangle\subset A$. 问何时 A 为素理想？

2. 设P为任何数域. 证明：$\langle x\rangle$为$P[x]$的极大理想.

3. 设 P 为环 R 的理想，$Q=R-P$. 证明：P 为素理想当且仅当 Q 对于 R 的乘法构成半群.

4. 试问$\mathbf{Z}_m$ $(m>1)$有多少理想？有多少素理想？有多少极大理想？

5. 在$\mathbf{Z}[x]$中，证明：$\langle x, n\rangle$是极大理想当且仅当 n 是素数.

§2.4 惟一析因环

本节考虑环中的因子分解问题. 从小学数学我们就知道，每个自然数都可以惟一地分解为一些素数的乘积. 此外，在高等代数中，我们学过数域上的一元多项式的因式分解定理. 自然我们希望考虑任何环上的因子分解问题. 由于一般环上因子分解问题比较复杂，本节只考虑整环，即没有零因子的交换幺环. 因子分解问题的实质，是将一个元素分解为一类特殊元素的乘积，最根本的问题是分解的存在性与惟一性.

要讨论因子分解，首先我们要将整数中整除(因子)和素数的

概念推广到一般环上.在本节中,除非特别说明,我们考虑的都是整环.

定义 2.4.1 设 R 为一个整环,$a,b\in R$,称 a 能被 b **整除**,若存在 $c\in R$ 使 $a=bc$,这时也称 b 为 a 的因子,记为 $b\mid a$.若 a 不能被 b 整除,则记为 $b\nmid a$.

要推广素数的概念比较复杂,我们首先定义环中一类特殊元.以下假设 R 为一个整环.

定义 2.4.2 设 R 为整环,用 U 表示幺半群 $R^*=R-\{0\}$ 中所有可逆元的集合,则 U 是一个交换群,称为 R 的单位群,U 中的元素称为**单位**.

注意单位不一定是单位元,任何整环中至少有 1 及 -1 两个单位(可能相等).

例 1 在集合 $\mathbb{Z}[\sqrt{-1}]=\{a+b\sqrt{-1}\mid a,b\in\mathbb{Z}\}$ 上定义普通的加法与乘法,则 $\mathbb{Z}[\sqrt{-1}]$ 成为一个整环,称为 Guass 整数环.在这个环中,除 ±1 外,$\pm\sqrt{-1}$ 也是单位,因为 $\sqrt{-1}(-\sqrt{-1})=1$.读者可以证明该环只有上述四个单位.

定义 2.4.3 设 $a,b\in R$,若存在 R 中单位 u 使得 $a=ub$,则称 a 与 b **相伴**,记为 $a\sim b$.

关于整除、单位和相伴有下列一些主要性质.其证明留作习题.

性质 1 $\forall a\in R, a\mid a$.若 $a\mid b, b\mid c$,则 $a\mid c$.

性质 2 若 u 是单位,则 $u\mid a,\forall a\in R$.

性质 3 若 a 与 b 相伴,则存在单位 u_1 使得 $b=au_1$;$u\in R^*$ 是单位当且仅当 $u\sim1$.

性质 4 相伴关系是 R 中的等价关系,且是幺半群 R^* 的同余关系.

定义 2.4.4 设 $a\in R^*$,则任何单位和 a 的相伴元都是 a 的因子,称为 a 的**平凡因子**.若 $b\mid a$,但 $a\nmid b$,则称 b 为 a 的**真**

因子.

从性质 2 看出,单位没有真因子.

定义 2.4.5 设 $a\in R^*-U$,若 a 没有非平凡的真因子,则称 a 为**不可约元素**.若 a 有非平凡的真因子,则称 a 为**可约元素**.

定义 2.4.6 若 $p\in R^*-U$,且由 $p\mid ab$ 可以推出 $p\mid a$ 或 $p\mid b$,则称 p 为**素元素**.

例 2 在整数环Z中,$U=\{1,-1\}$,于是 $a\sim b$ 当且仅当 $a=\pm b$,因而 a 为不可约元素当且仅当 $a=\pm p$,其中 p 为素数.而按定义,对于任何素数 p,$\pm p$ 显然是素元素,而且Z中只有这样的素元素.因此在Z中不可约元素与素元素是等价的.

一般地,我们有:

引理 2.4.1 素元素一定是不可约元素.

证 设 p 为素元素,a 是 p 的一个因子,则存在 $b\in R^*$ 使得 $p=ab$,即 $p\mid ab$,由素元素的定义必有 $p\mid a$ 或 $p\mid b$.若 $p\mid a$,则 a 不是 p 的真因子.若 $p\mid b$,则存在 $c\in R^*$ 使 $b=pc$,于是 $p=pac$,由于整环中消去律成立,故有 $ac=1$,从而 a 为单位,即 a 为平凡因子.这说明 p 没有非平凡的真因子.故 p 是不可约元素. □

引理 2.4.1 的逆不成立,我们将在习题中举例加以说明.

定义 2.4.7 如果整环 R 满足下列条件:

(1) 有限析因条件:$\forall a\in R^*-U$,a 可分解为有限个不可约元素的乘积.即存在不可约元素 $p_i(1\leqslant i\leqslant r)$ 使得

$$a=p_1p_2\cdots p_r;$$

(2) 若 $a\in R^*-U$ 有两种不可约元素乘积的分解:

$$a=p_1p_2\cdots p_r=q_1q_2\cdots q_s.$$

则有 $r=s$,而且适当交换顺序可以使得 $p_i\sim q_i$,$1\leqslant i\leqslant r$.

那么称 R **为惟一析因环**.

按照定义和我们以前学过的知识,整数环和任意数域 P 上的多项式环 $P[x]$ 都是惟一析因环.我们先看一看惟一析因环有些什么主要性质.

定理 2.4.2 一个惟一析因环 R 中不可约元素一定是素元素.

证 设 $p\in R^*$ 为不可约元素,且 $p\mid ab$,则存在 $c\in R$ 使得 $ab=pc$.下面证明必有 $p\mid a$ 或 $p\mid b$.若 a,b 中有一个等于 0,结论显然成立.若 a,b 中有一个是单位,无妨设 b 为单位.则有 $a=abb^{-1}=pcb^{-1}$,故 $p\mid a$,这时结论也成立.下设 $a,b\in R^*-U$,我们断言这时必有 $c\in R^*-U$.事实上,c 显然不为 0,若 $c\in U$,则 $pc\sim p$ 为不可约元素,而且它可以写成两个非单位 a,b 的乘积,因此有真因子,这是矛盾.故 $c\in R^*-U$.由于 R 是惟一析因环,存在 R^*-U 中不可约元素 $p_i(1\leqslant i\leqslant t)$ 使得

$$c=p_1p_2\cdots p_t.$$

此外,a,b 也可以写成不可约元素的乘积:

$$a=q_1q_2\cdots q_r;b=q'_1q'_2\cdots q'_s.$$

于是

$$q_1q_2\cdots q_rq'_1q'_2\cdots q'_s=pp_1p_2\cdots p_t$$

由分解的惟一性,p 必与某一个 q_i 或某一个 q'_i 相伴.若 $p\sim q_i$,则 $p=q_i\varepsilon,\varepsilon\in U$,故

$$a=q_1\cdots q_i\varepsilon\varepsilon^{-1}q_{i+1}\cdots q_r=p(\varepsilon^{-1}q_1\cdots q_{i-1}q_{i+1}\cdots q_r),$$

即 $p\mid a$.同样若 p 与某个 q'_i 相伴,则 $p\mid b$.即 p 必能整除 a,b 中的某一个.因而 p 是素元素. □

惟一析因环的另一个重要性质是最大公因子的存在性.我们先给出最大公因子的定义.

定义 2.4.8 设 $a_1,a_2,\cdots,a_n\in R$,若 c 同时能够整除 $a_1,a_2,\cdots,a_n$,则称 c 为 $a_1,a_2,\cdots,a_n$ 的**公因子**.若 $a_1,a_2,\cdots,a_n$ 的公因子 d 能被 $a_1,a_2,\cdots,a_n$ 的任何一个公因子整除,则称 d 为 $a_1,a_2,\cdots,a_n$ 的一个**最大公因子**.

定理 2.4.3 设 R 为惟一析因环,$a,b\in R$,则 a,b 的最大公因子存在.而且 a,b 的任何两个最大公因子都相伴.

证　先证明最大公因子的存在性.若 a,b 中有一个为零,例如 $a=0$,则 b 是 a,b 的最大公因子.若 a,b 中有一个是单位,例如 a 是单位,则 a 是 a,b 的最大公因子.下设 $a,b\in R^{*}-U$,则 a,b 都存在分解

$$a=q_1q_2\cdots q_r,\quad b=q'_1q'_2\cdots q'_s,$$

其中 $q_i,q'_j(i=1,2,\cdots,r;j=1,2,\cdots,s)$ 是不可约元素,即素元素(见定理 2.4.2).现在我们将出现在上述分解中的互相相伴的元写在一起,可以统一写成

$$a=\varepsilon_a p_1^{k_1}p_2^{k_2}\cdots p_n^{k_n},b=\varepsilon_b p_1^{l_1}p_2^{l_2}\cdots p_n^{l_n},$$

其中 $\varepsilon_a,\varepsilon_b$ 是单位,$k_i\geqslant 0,l_i\geqslant 0$,且 $p_1,p_2,\cdots,p_n$ 互不相伴.令 $m_i=\min(k_i,l_i),i=1,2,\cdots,n$,

$$d=p_1^{m_1}p_2^{m_2}\cdots p_n^{m_n}.$$

由定义显然 $d\mid a,d\mid b$,即 d 是 a,b 的公因子.假定 c 也是 a,b 的公因子,则显然 $c\neq 0$.若 c 是单位,则显然 $c\mid d$.若 c 不是单位,则存在分解

$$c=p'_1p'_2\cdots p'_t,$$

其中 p'_i 是素元素.由于 $c\mid a$,故 $p'_i\mid a$,于是 p'_i 必能整除某一个 p_j,由于它们都是不可约元素,故它们相伴,即 c 也可以写成

$$c=\varepsilon_c p_1^{h_1}p_2^{h_2}\cdots p_n^{h_n},$$

其中 ε_c 是单位.由于 $c\mid a$,而且 $p_1,p_2,\cdots,p_n$ 互不相伴,因此 $h_i\leqslant k_i$.同理由 $c\mid b$ 得 $h_i\leqslant l_i$.故 $h_i\leqslant m_i$,即 $c\mid d$.故 d 是 a,b 的最大公因子.至此证明了最大公因子的存在性.

假定 d,d' 都是 a,b 的最大公因子,则 $d\mid d',d'\mid d$,故存在 $u,v\in R$ 使得

$$d=ud',d'=vd.$$

若 d,d' 中一个为 0,则另一个必为 0,这时 $d=d'$.若 d,d' 都不为零,则 $d=uvd$,由消去律,得 $1=uv$,故 u,v 是单位.从而 d,d' 相伴.至此定理证毕.　□

利用归纳法,我们可以证明惟一析因环中任意有限个元素的最大公因子存在,而且任何两个最大公因子相伴.那么如何判断一个整环是惟一析因环呢?我们有下面的判定定理.

定理 2.4.4 假定一个整环 R 满足有限析因条件且每个不可约元素都是素元素,则 R 是惟一析因环.

证 设 $a\in R^*-U$,则 a 有分解 $a=p_1p_2\cdots p_r$(p_i是不可约元素).假定 a 还有另一个分解 $a=q_1q_2\cdots q_s$(q_i是不可约元素).我们证明 $r=s$ 且 p_i必与某个q_j相伴.为此对 r 用归纳法.当 $r=1$ 时

$$a=p_1=q_1q_2\cdots q_s.$$

若 $s>1$,则

$$p_1=q_1(q_2\cdots q_s).$$

这说明 p_1可以写成两个非单位的乘积,这是不可能的.故这时 $r=s=1$,$p_1=q_1$.

现在假定结论对 $r=k-1$ 成立.当 $r=k$ 时我们有

$$a=p_1p_2\cdots p_k=q_1q_2\cdots q_s.$$

于是 $p_1\mid q_1q_2\cdots q_s$,由于不可约元素是素元素,故 p_1必能整除 q_j,$j=1,2,\cdots,s$ 中的某一个,通过交换顺序,无妨设 $p_1\mid q_1$,由于 p_1,q_1都是不可约的,故 $p_1\sim q_1$.设 $p_1=\varepsilon q_1$,其中 ε 是单位.则

$$(\varepsilon p_2)\cdots p_k=q_2q_3\cdots q_s.$$

由归纳假设 $k-1=s-1=r-1$,且适当交换顺序可以使得 p_j与q_j相伴,$j=2,3,\cdots,r$.这说明结论对 $r=k$ 也成立.至此定理证毕. □

应该指出,定理 2.4.4 在实际中应用起来是十分不便的.在接下来的两节中,我们将利用定理 2.4.4 介绍两种特殊的惟一析因环.在本节的最后,我们给出一个非惟一析因环的例子.

例 3 设$Z[\sqrt{-3}]=\{a+b\sqrt{-3}\mid a,b\in Z\}$.在 R 中定义普通的加法和乘法,则$Z[\sqrt{-3}]$成为一个整环.我们首先可以确定,

$\mathbb{Z}[\sqrt{-3}]$中的单位只有 ± 1. 事实上，若 ε 是单位，则存在 $\varepsilon' \in \mathbb{Z}[\sqrt{-3}]$ 使得 $\varepsilon\varepsilon' = 1$，两边取模长平方得 $|\varepsilon|^2|\varepsilon'|^2 = 1$，由于 $|\varepsilon|^2$，$|\varepsilon'|^2$ 都是正整数，故 $|\varepsilon|^2 = 1$. 而在 $\mathbb{Z}[\sqrt{-3}]$ 中只有 ± 1 的模长平方为 1. 故 $\mathbb{Z}[\sqrt{-3}]$ 只有 ± 1 两个单位. 其次，我们可以证明 $\mathbb{Z}[\sqrt{-3}]$ 中模长为 2 的元素一定是不可约元素. 事实上，若 $|\alpha| = 2$ 且 $\alpha = \beta\gamma$. 则 $|\beta|^2|\gamma|^2 = 4$. 而对任何整数 a, b，$a^2 + 3b^2 \neq 2$. 故 $|\beta|^2, |\gamma|^2$ 中必有一个为 4，一个为 1. 由前面的讨论知道模长平方为 1 的元素是单位. 故 α 没有非平凡的真因子，从而是不可约元素. 最后，考虑 $\mathbb{Z}[\sqrt{-3}]$ 中的元素 4，我们有 $4 = 2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$. 而 $2, 1 \pm \sqrt{-3}$ 的模长都是 2，从而都是不可约元素. 但是 $1 \pm \sqrt{-3}$ 显然不与 2 相伴. 这说明 4 至少有两种分解. 故 $\mathbb{Z}[\sqrt{-3}]$ 不是惟一析因环.

习 题

1. 在交换环 R 中，若 $a \mid b$ 且 $a \mid c$，证明：$a \mid bx + cy, \forall x, y \in R$.

2. 证明本节关于整除，单位和相伴的性质 1—4.

3. 设 $R = \left\{ \frac{m}{2^n} \middle| m, n \in \mathbb{Z} \right\}$. 证明：$R$ 对于数的加法和乘法构成一个整环. 试找出 R 的不可约元素，素元素和单位.

4. 在 $\mathbb{Z}[\sqrt{-1}] = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Z}\}$ 中，证明：5 不是不可约元素.

5. 证明：$\sqrt{-3}$ 是 $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$ 的素元素.

6. 在环 $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ 中证明 $3 \nmid 1 + 2\sqrt{-5}$，并证明 3 是不可约元素但不是素元素，因此 $\mathbb{Z}[\sqrt{-5}]$ 不是惟一析因环.

7. 在一个环 R 中，若 $a \mid b$ 且 $b \mid a$，是否 a 与 b 一定相伴？为什么？

8. 设 π 为环 R 中的素元素，且 $\pi \mid a_1 a_2 \cdots a_n$，证明：必存在 i，$1 \leqslant i \leqslant n$ 使 $\pi \mid a_i$.

补充题

1. 设$\mathbf{Q}'[\sqrt{-3}]=\left\{\frac{a+b\sqrt{-3}}{2}\mid a,b\in\mathbf{Z},a+b\text{ 为偶数}\right\}$.

(1) 证明$\mathbf{Q}'[\sqrt{-3}]$在数的加法和乘法下构成一个环;

(2) 证明$\mathbf{Q}'[\sqrt{-3}]$的所有单位是$1,-1,\frac{1\pm\sqrt{-3}}{2},\frac{-1\pm\sqrt{-3}}{2}$;

(3) 证明在$\mathbf{Q}'[\sqrt{-3}]$中2与$1+\sqrt{-3}$相伴.

2. 设R,R'都是整环,R是惟一析因环,又φ是R到R'的满同态,试问R'是否为惟一析因环? 为什么?

3. 举例说明,一个惟一析因环的子环未必是惟一析因环.

4. 设R是惟一析因环,$a,b\in R^*$.若$m\in R$满足:

(1) m是a,b的公倍式,即$a\mid m,b\mid m$;

(2) 若n也是a,b的公倍式,则$m\mid n$.

m称为a,b的最小公倍式,试证明:

(1) 若m是a,b的最小公倍式,则当且仅当$m_1\sim m$时,m_1也是a,b的最小公倍式;

(2) R^*中任何两个元素都存在最小公倍式;

(3) 设$[a,b]$为a,b的一个最小公倍式,则有

$$[a,b](a,b)\sim ab,\quad [a,(b,c)]\sim([a,b],[a,c]).$$

5. 设R为惟一析因环,若a,b的最大公因子是单位,则称a,b互素.设$a_1=db_1,a_2=db_2$不全为零.证明:d是a_1,a_2的最大公因子当且仅当b_1,b_2互素.

6. 已知$\mathbf{Q}[x,y]$在多项式加法和乘法下构成环,证明:x与y互素.是否存在$r(x,y),s(x,y)\in\mathbf{Q}[x,y]$使得$r(x,y)x+s(x,y)y=1$?

§2.5 主理想整环

本节先介绍一种特殊的惟一析因环——主理想整环.一般说来,要证明一个具体的整环是惟一析因环是困难的.但是在某些特殊情形我们可以利用定理2.4.4直接判断,其中最典型的例子就

是本节介绍的主理想整环和下节将要介绍的欧几里得环.我们先给出主理想整环的定义

在§2.1中曾用$\langle A\rangle$表示环R中的子集A生成的理想,即所有包含A的理想之交.当A由一个元素a组成时,称$\langle A\rangle=\langle a\rangle$为由$a$生成的**主理想**.

若R是幺环,则$\langle a\rangle$由一切形如$\sum x_i a y_j, x_i, y_j \in R$的元素组成,其中和号表示有限项之和.特别,当$R$是交换幺环时,

$$\langle a\rangle = aR = Ra = \{xa \mid x \in R\}.$$

定义 2.5.1 若交换幺环的每个理想都是主理想,则称此环为**主理想环**.若一个主理想环是整环,则称此环为**主理想整环**.

例 1 $\mathbb{Z}$是主理想整环.事实上,设I为$\mathbb{Z}$的一个非零理想,则存在$m \in I$使得$m = \min\{|k| \mid k \in I, k \neq 0\}$.现在设$b \in I$,若$b = 0$,则$b = 0 \cdot m$;若$b \neq 0$,则存在$q, r \in \mathbb{Z}$使得$b = qm + r$,其中$0 \leqslant r < m$.于是$r = b - qm \in I$,由$m$的取法有$r = 0$,即$b = qm$.故$I = \langle m\rangle$.因而$\mathbb{Z}$是主理想整环.

例 2* $\mathbb{Z}[x]$不是主理想整环.显然$\mathbb{Z}[x]$是整环.若$\mathbb{Z}[x]$是主理想环.则存在$g(x) \in \mathbb{Z}[x]$使得$\langle 2, x^2+1\rangle = \langle g(x)\rangle$.故$2 \in \langle g(x)\rangle$,即$g(x) \mid 2$,从而$g(x) = \pm 1, \pm 2$.另一方面,由于$g(x) \in \langle 2, x^2+1\rangle$,故存在$u(x), v(x) \in \mathbb{Z}[x]$使得

$$g(x) = 2 \cdot u(x) + v(x)(x^2+1).$$

考虑两边在$x = 1$的值得$g(1) = 2(u(1) + v(1))$,于是只能$g(x) = \pm 2$.但是$\pm 2 \nmid x^2+1$,即$x^2+1 \notin \langle g(x)\rangle$.这是矛盾.故$\mathbb{Z}[x]$不是主理想整环.

本节主要目的是证明任何一个主理想整环必然为惟一析因环.我们先证明两个引理.

引理 2.5.1 设R为主理想整环.若R中一个序列

$$a_1, a_2, a_3, \cdots$$

里每一个元素都是前面一个元素的真因子,那么这个序列一定是

一个有限序列.

证 用这一序列元素作成一列主理想:

$$\langle a_1\rangle,\langle a_2\rangle,\langle a_3\rangle,\cdots$$

由于 a_{i+1} 是 a_i 的真因子,故

$$\langle a_i\rangle\subseteq\langle a_{i+1}\rangle,i=1,2,\cdots$$

令 I 为这些理想的并集.我们先证明 I 为 R 的理想.设 $a,b\in I$.则存在 i,j 使 $a\in\langle a_i\rangle,b\in\langle a_j\rangle$.无妨设 $i\leqslant j$,则 $a,b\in\langle a_j\rangle$.于是 $a-b\in\langle a_j\rangle\subseteq I$.另一方面对任何 $r\in R$,有 $ra\in\langle a_i\rangle\subseteq I$.这就证明 I 是 R 的理想.由于 I 是主理想环,故存在 $d\in R$ 使得 $I=\langle d\rangle$,由于 $d\in I$,故存在 a_n 使得 $d\in\langle a_n\rangle$.现在我们断定 a_n 是序列的最后一个元素.若不然则存在 a_{n+1},于是 $d\in\langle a_n\rangle,a_{n+1}\in\langle d\rangle$.故 $a_n\mid d,d\mid a_{n+1}$.故 $a_n\mid a_{n+1}$.这与假设 a_{n+1} 为 a_n 的真因子矛盾. □

引理 2.5.2 设 R 为一个主理想整环,$p\in R^*-U$ 为不可约元素,则$\langle p\rangle$为 R 的极大理想.

证 设 I 为 R 的理想且$\langle p\rangle\subseteq I$.由于 R 是主理想环,存在 $a\in R$ 使得 $I=\langle a\rangle$.故 $p\in\langle a\rangle$,从而存在 $r\in R$ 使得 $p=ra$.由于 p 是不可约元素,故 a 或是单位或是 p 的相伴元.若 a 是单位,则 $\langle a\rangle=R$,故 $I=R$;若 a 与 p 相伴,则 $I=\langle a\rangle=\langle p\rangle$.因此$\langle p\rangle$是极大理想. □

现在我们可以证明

定理 2.5.3 主理想整环是惟一析因环.

证 设 R 为主理想整环,为证 R 为惟一析因环,我们利用定理 2.4.4.先证明 R 满足有限析因条件.设 $a\in R^*-U$,若 a 不能写成有限个不可约元素的乘积,则 a 本身是可约元素,因此有真因子.设 $a=bc$,其中 b,c 都是 a 的真因子,则 b,c 中至少有一个不能写成有限个不可约元素的乘积.因为否则 a 也能写成有限个不可约元素的乘积,与假设矛盾.继续这样做下去,我们将得到一

个无穷序列

$$a, a_1, a_2, \cdots,$$

其中每个元素都是前面一个元素的真因子，这与引理 2.5.1 的结论矛盾．这说明 $R^* - U$ 中每个元素都一定能写成有限个不可约元素的乘积，即 R 满足有限析因条件．

接下来我们证明 R 中每个不可约元素为素元素．设 $p \in R$ 为不可约元素且 $p \mid ab$．考虑商环 $R/\langle p\rangle$，由于 $ab \in \langle p\rangle$，故 $\overline{a}\,\overline{b} = \overline{ab} = \overline{0}$．由引理 2.5.2，$\langle p\rangle$ 是极大理想，因此 $R/\langle p\rangle$ 是一个域，而域没有零因子，因此在 $R/\langle p\rangle$ 中必有 $\overline{a} = \overline{0}$ 或 $\overline{b} = \overline{0}$，即 $a \in \langle p\rangle$ 或 $b \in \langle p\rangle$．从而 $p \mid a$ 或 $p \mid b$．这说明 p 是素元素．因此 R 是惟一析因环． □

定理 2.5.3 的逆命题不真，如例 2 中的 $\mathbf{Z}[x]$ 不是主理想整环，但它是惟一析因环．其证明用到高等代数中的有关有理(整)系数多项式的知识．我们将它留作习题．

在本节的最后，我们给出一个主理想整环的特殊性质．读者可以自己举例说明，对于一般的惟一析因环，下面的定理是不成立的．

定理 2.5.4 设 R 为主理想整环，$a, b \in R$，d 为 a, b 的一个最大公因子，则存在 $u, v \in R$ 使 $d = ua + vb$．

证 由于 R 为主理想整环，故存在 d' 使得 $\langle d'\rangle = \langle a, b\rangle$．我们先证明 d' 也是 a, b 的最大公因子，事实上，因为 $a, b \in \langle d'\rangle$，故 $d' \mid a, d' \mid b$，这说明 d' 是 a, b 的公因子．此外，$d' \in \langle a, b\rangle$，故存在 $u', v' \in R$ 使得 $d' = u'a + v'b$，于是对于 a, b 的任何公因子 c，$c \mid (u'a + v'b) = d'$．故 d' 为 a, b 的最大公因子．又 R 是惟一析因环，故 d 与 d' 相伴，设 $d = \in d'$，$\in$ 为单位，则 $d = \in u'a + \in v'b$．定理证毕． □

习 题

1. 设 R 为整环，$\langle a\rangle, \langle b\rangle$ 是 R 的主理想．证明：$\langle a\rangle = \langle b\rangle$ 当且仅当 a 与

b 相伴.

2. 设 R 为主理想整环,若 $a\in R, a\neq 0$ 且 $\langle a\rangle$ 为一个极大理想,证明:a 为不可约元素.

3. 设 R 是主理想整环,I 是 R 的非零理想.证明:

(1) R/I 的每个理想都是主理想,R/I 是主理想整环吗?

(2) R/I 中仅有有限多个理想.

4. 设 $A=\{16,24,36,60\}$,求整数 m 使得在整数环 $\mathbf{Z}$ 中 $\langle A\rangle=\langle m\rangle$.

5. 已知 $\mathbf{Q}[x]$ 是主理想整环,求 $f(x)\in\mathbf{Q}[x]$ 使得 $\langle x^2+1, x^5+x^3+1\rangle=\langle f(x)\rangle$.

补充题

1. 证明:$\mathbf{Q}[x,y]$ 不是主理想整环.

2. 设 R 为主理想整环,$a\in R$,令 $P=\{b\in R \mid b$ 与 a 互素$\}$.证明:集合 $\{x+\langle a\rangle \mid x\in P\}$ 在商环 $R/\langle a\rangle$ 的乘法下构成群.

3. 证明:$\mathbf{Z}[x]$ 为惟一析因环.

4. 若环 R 中严格递降理想序列 $N_1\supset N_2\supset\cdots$ 都是有限长,则称 R 满足**降链条件**.若 R 环中的任何一个理想的集合 S 中必存在一个理想不真包含 S 中任何其它理想,则称 S 满足**极小条件**.证明:一个环 R 满足降链条件当且仅当 R 满足极小条件.

§2.6 欧几里得环

本节介绍第二种特殊的惟一析因环——欧几里得环.

定义 2.6.1 设 R 为一个整环.若存在从 R^* 到 $\mathbf{N}\cup\{0\}$ 的映射 δ,使得 $\forall a,b\in R, b\neq 0$,存在 $q,r\in R$ 满足

$$a=qb+r,$$

其中 $r=0$ 或 $\delta(r)<\delta(b)$.则称 R 为**欧几里得(Euclid)环**.

形象地说,欧几里得环就是可以做辗转相除法的环.

例 1 $\mathbf{Z}$ 是欧几里得环.

事实上,只须作映射 $\delta:\mathbf{Z}^*\to\mathbf{N}\cup\{0\}$,使 $\delta(m)=|m|$ 即得.

例 2 设 P 为数域，则 $P[x]$ 是欧几里得环.

定义映射 δ 使得 $\delta(f(x))=\deg f(x)$，其中 $f(x)\neq 0$. 则容易验证 δ 满足定义 2.6.1 的条件. 因此 $P[x]$ 是欧几里得环.

定理 2.6.1 欧几里得环是主理想整环，因此是惟一析因环.

证 设 I 为欧几里得环 R 的理想，δ 为定义 2.6.1 中的映射. 若 I 只包含零元，则 $I=\langle 0\rangle$. 若 I 包含非零元，则集合 $\{\delta(x)\mid x\in I, x\neq 0\}\subseteq \mathbf{N}\cup\{0\}$ 中必存在最小者. 设 $a\in R^*\cap I$ 且 $\delta(a)$ 达到最小值，即 $\forall x\in I, x\neq 0$ 有 $\delta(x)\geqslant\delta(a)$. 由定义 $\forall b\in I$，存在 $q, r\in R$ 使得 $b=qa+r$，其中 $r=0$ 或 $\delta(r)<\delta(a)$. 由于 $a, b\in I$，故 $r=b-qa\in I$. 若 $r\neq 0$，则 $r\in I$ 且 $\delta(r)<\delta(a)$，与 a 的取法矛盾. 故 $r=0$，即 $b=qa$. 由 b 的任意性我们得 $I=\langle a\rangle$. 故 R 是主理想整环. □

在本节的最后我们简单介绍一下域上多项式环的主要性质. 设 F 为一个域，x 为一个文字(符号)，则由形如

$$\{a_n x^n+a_{n-1}x^{n-1}+\cdots+a_1 x+a_0 \mid n\in \mathbf{N}\cup\{0\},\ a_i\in F, i=1,2,\cdots,n\}$$

的所有元素组成的集合 $F[x]$ 称为 F 上的一元多项式环，简称为 F 上的多项式环. 与数域上的多项式环完全一样，可以在 $F[x]$ 上定义加法(合并同类项)和乘法(逐项展开相乘再合并同类项). 容易证明在上述加法和乘法下 $F[x]$ 成为一个环. 由于乘法是交换的，故 $F[x]$ 是交换环. 又显然 1 是 $F[x]$ 对于乘法的幺元，故 $F[x]$ 是交换幺环. 设

$$f(x)=a_n x^n+a_{n-1}x^{n-1}+\cdots+a_1 x+a_0, a_n\neq 0, n\geqslant 0.$$

则称 n 为非零多项式 $f(x)$ 的次数，记为 $\deg f(x)$(不定义零多项式的次数). 设 $f(x)\neq 0, g(x)\neq 0, f(x), g(x)\in F[x]$，则由于域上没有零因子，故有 $\deg(f(x)g(x))=\deg f(x)+\deg g(x)$. 因此 $f(x)g(x)\neq 0$. 故 $F[x]$ 没有零因子，因此 $F[x]$ 是整环. 容易将数域上多项式环上的带余除法推广到 $F[x]$ 上. 因此若 $g(x)\neq 0, g(x)\in F[x]$，则对任何 $f(x)\in F[x]$ 存在 $q(x), r(x)\in$

$F[x]$使得

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

其中 $r(x)=0$ 或 $\deg r(x)<\deg g(x)$，且这样的 $q(x),r(x)$惟一.现在我们作 $F[x]^*$到$\mathbf{N}\cup\{0\}$的映射 δ：

$$\delta(f(x))=\deg f(x),\forall f(x)\in F[x]^*.$$

则 δ 显然满足定义 2.6.1 的条件.因此 $F[x]$是一个欧几里得环，从而是主理想整环，也是惟一析因环.

让我们看一下 $F[x]$中的理想.设 I 为$F[x]$的理想，则存在 $f(x)\in F[x]$使得 $I=\langle f(x)\rangle$.若 $I\neq 0$，则 $f(x)\neq 0$，再设 $f(x)$可约，则存在 $f_1(x),f_2(x)\in F[x]$，$\deg f_1(x)>0$，$\deg f_2(x)>0$，使 $f(x)=f_1(x)f_2(x)$.于是$\langle f(x)\rangle\subset\langle f_1(x)\rangle$且$\langle f(x)\rangle\neq\langle f_1(x)\rangle$.这说明 $I=\langle f(x)\rangle$不是极大理想.反之，设 $f(x)$为不可约多项式，则我们有

定理 2.6.2 设 $f(x)\in F[x]$不可约，则$\langle f(x)\rangle$为 $F[x]$的极大理想，因此 $F[x]/\langle f(x)\rangle$是一个域.

证 由引理 2.5.2，$\langle f(x)\rangle$为极大理想.据定理 2.3.5，$F[x]/\langle f(x)\rangle$为域.

习 题

1. 证明下列环在指定的映射 δ 下成为 Euclid 环：

(1) Guass 整数环$\{\mathbf{Z}[\sqrt{-1}];+,\cdot\}$，$\delta(a+b\sqrt{-1})=a^2+b^2$；

(2) $\{\mathbf{Z}[\sqrt{-2}];+,\cdot\}$，$\delta(a+b\sqrt{-2})=a^2+2b^2$；

(3) $\{\mathbf{Z}[\sqrt{2}];+,\cdot\}$，$\delta(a+b\sqrt{2})=|a^2-2b^2|$；

(4) $\{\mathbf{Q}[\sqrt{-7}];+,\cdot\}$，其中$\mathbf{Q}[\sqrt{-7}]=\left\{a+b\left(\frac{1-\sqrt{-7}}{2}\right)\middle|a,b\in\mathbf{Z}\right\}$，$\delta\left(a+b\left(\frac{1-\sqrt{-7}}{2}\right)\right)=a^2+ab+2b^2$.

2. 证明任何一个域都是 Euclid 环.

3. 设 R 为 Euclid 环，且 $\delta(ab)=\delta(a)\delta(b)$，$\forall a,b\in R$.证明：$a$ 为 R 的

单位$\Longleftrightarrow \delta(a)=\delta(1)$.

4. 证明:$\mathbf{Z}[\sqrt{-6}]$不是 Euclid 环.

5. 证明:$\mathbf{Z}[\sqrt{10}]$不是 Euclid 环.

6. 设 R 为 Euclid 环,I 为 R 的理想,试问 I 是否一定是 Euclid 环?说明理由.

补充题

1. 设 R 为交换幺环,x 为一个文字.称

$$a_0+a_1x+a_2x^2+\cdots+a_nx^n, a_i\in R, i=1,2,\cdots,n$$

为 R 上的一个多项式,规定两个多项式相等当且仅当它们对应的各项系数都相等.将 R 上所有的多项式组成的集合记为 $R[x]$,在 $R[x]$ 上定义与域上多项式相类似的加法和乘法.

(1) 证明:$R[x]$在上述加法和乘法下构成一个环;

(2) 证明:$R[x]$是交换幺环;

(3) 若 R 是整环,则 $R[x]$也是整环.

2. 设 R 为惟一析因环,证明:$R[x]$也是惟一析因环.

3. 设 R 为整环,R 的一个元素 a 称为 $R[x]$的多项式 $f(x)$的一个根,若 $f(a)=0$.

(1) 证明:a 是 $f(x)$的一个根当且仅当 $f(x)$能被 $x-a$ 整除;

(2) R 的 k 个不同的元素 $a_1,a_2,\cdots,a_k$ 都是 $f(x)$的根当且仅当 $f(x)$能被 $(x-a_1)(x-a_2)\cdots(x-a_k)$整除;

(3) 设 $f(x)=a_0+a_1x+\cdots+a_nx^n$,其中 $a_n\neq 0$,则称 $f(x)$的次数为 n(不定义 0 多项式的次数).证明:若 $f(x)$的次数是 $n>0$,则 $f(x)$在 R 中至多有 n 个根.

第三章　域

本章研究域.和任何代数体系一样,我们研究域的最终目的是能将其分类.但是我们即将证明任何一个域都包含一个素域作为它的子域,而素域由它的特征惟一确定,而且结构很简单.因此分类的问题变为将素域进行扩张的问题.因为研究素域的扩张并不比研究一般域的扩张来得简单,因此本章将致力于一般域的扩张问题.域的扩张问题事实上我们早就接触过了,例如实数域是有理数域的扩张,复数域是实数域的扩张等.

§3.1　域的单扩张

为了后面的应用,我们介绍一下整环的分式域的概念.这是由整数环得到有理数域的过程的推广.

定义 3.1.1　设整环 R 为域 F 的子环,若对任何 $a\in F$,存在 $b,c\in R$ 使得 $a=bc^{-1}$,则称 F 为 R 的**分式域**.

定理 3.1.1　设 R 为整环,则 R 的分式域存在,而且 R 的分式域是包含 R 的最小域,因而惟一.

证　我们只给出这一定理的证明概要,证明的一些细节留作习题.在集合 $R\times R^*$ 上定义加法与乘法如下:

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

$$(a,b)(c,d)=(ac,bd),(a,b),(c,d)\in R\times R^*.$$

则 $R\times R^*$ 对于加法与乘法都成为交换幺半群,其单位元分别是

$(0,1),(1,1)$. 在 $R\times R^*$ 中定义关系"$\sim$":$(a,b)\sim(c,d)$当且仅当 $ad=bc$. 则"$\sim$"是一个等价关系. 且"$\sim$"对于上述乘法和加法都是同余关系.

现在令 $F=R\times R^*/\sim$ 为等价类的集合,将(a,b)所在的类记为$\frac{a}{b}$. 由于"$\sim$"是加法与乘法的同余关系,在 F 上可以定义加法与乘法:

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd},$$

$$\frac{a}{b}\frac{c}{d}=\frac{ac}{bd}.$$

容易证明 F 对于上述加法与乘法成为一个域. 且其单位元为$\frac{1}{1}$,而对于$\frac{a}{b}\in F\setminus\left\{\frac{0}{1}\right\},b\in R^*$,有$\left(\frac{a}{b}\right)^{-1}=\frac{b}{a}$. 将 R 中元素 a 对应到 F 中元素$\frac{a}{1}$,则 R 可以看作 F 的子环. 对任何 F 中元素$\frac{a}{b}$,有$\frac{a}{b}=\frac{a}{1}\left(\frac{b}{1}\right)^{-1}$,故 F 为 R 的分式域. 至此证明了分式域的存在性.

下证惟一性. 设 F_1 是任何一个包含 R 的域. 令 $F_2=\{ab^{-1}\mid a,b\in R,b\neq 0\}$. 我们证明 F_2 是 F_1 的子域. 事实上,$\forall\, a,b\in R$,$b\neq 0,ab^{-1}-cd^{-1}=(ad-bc)(bd)^{-1}$,因为 R 是 F 的子环,故 $ad-bc\in R,bd\in R$,因此 F_2 是 F_1 的加法子群. 又若 $ab^{-1},cd^{-1}\in F_2$,且 $ab^{-1}\neq 0,cd^{-1}\neq 0$,则 $ab^{-1}(cd^{-1})^{-1}=(ad)(bc)^{-1}\in F_2-\{0\}$,因此 $F_2-\{0\}$ 对 F_1 的乘法构成 F_1^* 的子群. 即 F_2 是 F_1 的子域. 作 R 的分式域 F 到 F_2 映射 ϕ 使得$\phi\left(\frac{a}{b}\right)=ab^{-1}$. 则 ϕ 是 F 到 F_2 的同构. 于是可以将 F 看作 F_1 的子域. 这说明分式域 F 是包含 R 的最小域. 因而分式域惟一. □

例 1 容易看出整数环的分式域就是有理数域.此外,设 P 为数域,$P[x]$为 P 上的多项式环.令 $P(x)$为 $P[x]$的分式域,则

$$P(x)=\left\{\frac{f(x)}{g(x)}\mid f(x),g(x)\in P[x],g(x)\neq 0\right\}.$$

而 $P(x)$上的加法与乘法即为有理分式的普通加法与乘法.

下面我们开始研究域的扩张.我们先介绍一类特殊的域.

定义 3.1.2 不包含任何非平凡子域的域称为**素域**.

例如高等代数中已经证明,任何数域都包含有理数域,因此有理数域不存在非平凡子域,故有理数域是素域.此外我们还可以证明域$Z_p=Z/\langle p\rangle$(p 是素数)也是素域.事实上,Z_p 对于加法是素数阶群,由定理 1.3.6,Z_p 作为加法群无非平凡子群,因此Z_p 没有非平凡的子域,故为素域.

设 K 为一个域.令 Π 为 K 中所有非零子域之交,则 Π 为 K 的子域且 $\Pi\neq\{0\}$(因为 K 的单位元 1 必然包含在 Π 中).显然 Π 不会再有非平凡子域,故为素域.这说明每个域必然包含惟一的一个素域作为其子域.关于素域我们有

定理 3.1.2 设 Π 为一个素域,则 $\Pi\simeq Q$ 或 $\Pi\simeq Z_p$(p 为素数).

证 设 e 为 Π 的单位元,则$Ze=\{ne\mid n\in Z\}$为 Π 的一个子环.作Z 到Ze 的同态 ϕ:$\phi(n)=ne$(请验证这确是环同态).ϕ 是满同态,因此$Ze\simeq Z/\ker\phi$.由于Z 为欧几里得环,故为主理想环,于是存在 $p\in Z$ 使 $\ker\phi=\langle p\rangle$.注意到 p 为整环Ze 的特征,故 p 为素数或 0.

若 p 为素数,则$Ze\simeq Z/\langle p\rangle=Z_p$ 为域,注意到$Ze\subseteq\Pi$,且 Π 是素域,故这时 $\Pi=Ze\simeq Z_p$.

若 $p=0$,则$Ze\simeq Z$,故Ze 的分式域 F,同构于Z 的分式域,即有理数域Q.但是 $F\subseteq\Pi$,且 Π 是素域,故 $\Pi=F\simeq Q$. □

由定理 3.1.2 及其证明我们看出,一个域包含的素域由该域的特征惟一确定.域的特征有以下的重要性质,有的书上将其作为

特征的定义.

定理 3.1.3 设 K 为域，p 为素数，则

(1) K 的特征为 p 当且仅当 $pa=0, \forall a\in K$；

(2) K 的特征为零当且仅当 $na\neq 0, \forall n\in \mathbf{N}, a\in K^*$.

证 设 e 为 K 的单位元，K 的素域为 Π.

(1) 若 K 的特征为 p，则 $\Pi\simeq \mathbf{Z}_p$，于是 $pe=0$，从而 $pa=(pe)a=0, \forall a\in K$.

反之，若 $pa=0, \forall a\in K$，则 $pe=0$，因此属于定理 3.1.2 的证明中的第一种情形，因此 $\Pi\simeq \mathbf{Z}_p$. 故 $\mathrm{Ch}\ K=p$.

(2) 若 K 的特征为 0，则 $\Pi\simeq \mathbf{Q}$，因此 $\mathbf{Z}e\simeq \mathbf{Z}$，故 $ne\neq 0, \forall n\in \mathbf{N}$. 由于域中没有零因子，故 $\forall a\in K^*$ 有 $na=(ne)a\neq 0$.

反之，若 $\forall n\in \mathbf{N}, a\in K^*$，有 $na\neq 0$，于是 $ne\neq 0$，即属于定理 3.1.1 证明中的第二种情形，因此 $\Pi\simeq \mathbf{Q}$. 故 $\mathrm{Ch}\ K=0$. □

由上面的讨论我们看出，每一个域都包含一个惟一的素域. 而素域由它的特征惟一确定. 这样要研究域我们只需从简单的素域出发，扩充即可得到任何一个域. 我们给出一个定义.

定义 3.1.3 若域 F 是域 K 的子域，则称 K 为 F 的**扩张**，或称 K 为 F 的**扩域**.

这样，要找出所有的域，我们只需找出素域的所有的扩域就可以了. 但是研究素域的扩张并不比研究一般域的扩张简单. 因此我们以下仍研究一般域的扩张.

设 K 为域 F 的一个扩张，S 为 K 的一个子集，K 中所有包含 $F\cup S$ 的子域之交仍然为一个域，它是 K 中包含 $F\cup S$ 的最小子域，称为由添加子集 S 于 F 所得的扩域，记为 $F(S)$. K 本身可以看成由 F 添加一个集合所得，只须令 $S=K$ 即可. 同样 K 的任何包含 F 的子域也可以看成由 F 添加某个集合而得.

让我们看一下 $F(S)$ 的结构. 用 $F[S]$ 表示由下列形式的一切有限和

$$\sum_{i_1,i_2,\cdots,i_n\geqslant 0} a_{i_1 i_2\cdots i_n}\alpha_1^{i_1}\alpha_2^{i_2}\cdots\alpha_n^{i_n},\alpha_j\in S,a_{i_1 i_2\cdots i_n}\in F,j=1,2,\cdots,n$$

构成的集合.则 $F[S]$是 K 的子环,$F[S]$作为整环的分式域即为 $F(S)$.事实上,$F[S]$的分式域显然包含 $F\cup S$,从而包含 $F(S)$.此外,包含 $F\cup S$ 的任何域必然包含 $F[S]$,因此 $F[S]\subset F(S)$.而一个整环的分式域是包含该整环的最小域,故 $F(S)$包含 $F[S]$的分式域.因此 $F(S)$就是 $F[S]$的分式域.

例 2 若 $S=\{\alpha\}$,则

$$F[\alpha]=\{f(\alpha)\mid f(x)\in F[x]\}.$$

当 $S=\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$是有限集合时,记 $F[S]$为 $F[\alpha_1,\alpha_2,\cdots,\alpha_n]$,$F(S)$为 $F(\alpha_1,\alpha_2,\cdots,\alpha_n)$.

定理 3.1.4 设 K 为域 F 的扩域,$S\subset K$.则

(1) $F(S)=\bigcup_{S'\subset S}F(S')$,其中 S'取遍 S 的所有有限子集;

(2) 若 $S=S_1\cup S_2$,则 $F(S)=F(S_1)(S_2)=F(S_2)(S_1)$.

证 (1) 显然对任何有限子集 $S'\subset S$,有 $F(S')\subseteq F(S)$.故 $\bigcup_{S'\subset S}F(S')\subseteq F(S)$.反之,$\forall a\in F(S)$,存在 $f,g\in F[S]$,$g\neq 0$,使得 $a=fg^{-1}$.由于 f,g 的表达式都是有限和的形式,因此存在 S 的有限子集 S'_0 使得 $f,g\in F[S'_0]$.于是 $a\in F(S'_0)$.故(1)成立.

(2) 只须证明 $F(S)=F(S_1)(S_2)$,另一等式的证明完全相同.由于 $F(S_1\cup S_2)$是 K 中包含 $F,S_1\cup S_2$ 的最小子域,而 $F(S_1)(S_2)$包含 F,S_1,S_2,且是一个域,故 $F(S)\subseteq F(S_1)(S_2)$.

另一方面,$F(S_1)(S_2)$是包含 $F(S_1),S_2$ 的最小子域,而 $F(S_1\cup S_2)$显然包含 $F(S_1),S_2$,且是域,故 $F(S_1)(S_2)\subseteq F(S_1\cup S_2)$.于是(2)成立. □

推论 3.1.5 $F(\alpha_1,\alpha_2,\cdots,\alpha_n)=F(\alpha_1)(\alpha_2)\cdots(\alpha_n)$.

由定理 3.1.4 及其推论,研究域的扩张归结为添加有限集合的扩张,而添加有限集合的扩张归结为添加一个元素的扩张.因此

添加一个元素的扩张是最重要的扩张.

定义 3.1.4 设 K 为域 F 的扩域，$\alpha\in K$，若存在域 F 上的非零多项式 $f(x)$ 使得 $f(\alpha)=0$，则称 α 为 F 上的**代数元**. 否则称 α 为 F 上的**超越元**.

定义 3.1.5 设 K 为 F 的扩域且存在 $\alpha\in K$ 使得 $K=F(\alpha)$，则称 K 为 F 的**单扩张**. 若 α 为 F 上的代数元，则称 K 为 F 的**单代数扩张**；若 α 为 F 上的超越元，则 K 称为 F 的**单超越扩张**.

定理 3.1.6 (1) 若 α 是域 F 上的超越元，则

$$F(\alpha)\simeq F(x),$$

其中 $F(x)$ 是 F 上的多项式环 $F[x]$ 的分式域.

(2) 若 α 是 F 上的代数元，那么

$$F(\alpha)\simeq F[x]/\langle p(x)\rangle,$$

其中 $p(x)$ 是 $F[x]$ 的一个由 α 惟一确定的首一不可约多项式，且 $p(\alpha)=0$.

证 我们已经知道 $F(\alpha)$ 是 $F[\alpha]$ 的分式域. 作 $F[x]$ 到 $F[\alpha]$ 的映射：

$$\phi\left(\sum a_k x^k\right)=\sum a_k\alpha^k.$$

容易看出 ϕ 是 $F[x]$ 到 $F[\alpha]$ 的满同态. 有以下两种情形.

情形 1. α 是 F 上的超越元，则 $\ker\phi=\{0\}$. 因此 ϕ 是 $F[x]$ 到 $F[\alpha]$ 的同构. 将 ϕ 开拓到 $F(x)$ 上，使 $\phi(ab^{-1})=\phi(a)\phi(b)^{-1}$. 则 ϕ 成为 $F(x)$ 到 $F(\alpha)$ 的同构. 故 $F(\alpha)\simeq F(x)$.

情形 2. α 是 F 上的代数元. 这时 $\ker\phi$ 是 $F[x]$ 的非零理想. 由于 $F[x]$ 是主理想整环，故存在 $F[x]$ 的非零多项式 $p(x)$ 使得 $\ker\phi=\langle p(x)\rangle$. 当然我们可以让 $p(x)$ 的首项系数为 1，这样的 $p(x)$ 是惟一的. 下面证明 $p(x)$ 是不可约多项式. 事实上，若不然，则存在两个次数 >0 的多项式 $f(x)$，$g(x)$ 使得

$$p(x)=f(x)g(x).$$

于是 $p(\alpha)=f(\alpha)g(\alpha)=0$. 由于 $F(\alpha)$ 没有零因子，故 $f(\alpha)=0$ 或 $g(\alpha)=0$. 因此 $f(x)\in\ker\phi$ 或 $g(x)\in\ker\phi$，即 $p(x)\mid f(x)$

或 $p(x)\mid g(x)$，故 $\deg f(x)\geqslant\deg\ p(x)$ 或 $\deg g(x)\geqslant\deg p(x)$. 这与 $p(x)=f(x)g(x)$ 矛盾.

这样，$p(x)$ 是一个不可约多项式. 从而 $\langle p(x)\rangle$ 是一个极大理想. 因此 $F[x]/\langle p(x)\rangle$ 是一个域，由环的同态基本定理，ϕ 可导出 $F[x]/\langle p(x)\rangle$ 到 $F[\alpha]$ 的同构，因此 $F[\alpha]$ 是域. 由于一个域的分式域就是其本身，故 $F[\alpha]=F(\alpha)$. 定理得证. □

定理 3.1.5 说明一个域的单超越扩张在同构意义下是惟一的，而单代数扩张与一个首一不可约多项式有关. 我们可以将单代数扩张描述得更清楚.

定义 3.1.6 设 K 为 F 的扩域，$\alpha\in K$ 是 F 上的代数元. $F[x]$ 中以 α 为根的不可约首一多项式称为 α 在 F 上的**不可约多项式**，记为 $\mathrm{Irr}(\alpha,F)$，它的次数称为 α 在 F 上的**次数**，记为 $\deg(\alpha,F)$.

由定理 3.1.5 及其证明可知，对于 F 上的代数元 α，$F(\alpha)\simeq F[x]/\langle\mathrm{Irr}(\alpha,F)\rangle$ 且

$$\begin{aligned}\langle\mathrm{Irr}(\alpha,F)\rangle&=\{f(x)\in F[x]\mid f(\alpha)=0\}\\&=\{f(x)\in F[x]\mid\mathrm{Irr}(\alpha,F)\mid f(x)\}.\end{aligned}$$

下面的讨论中我们将用到一般域上的线性空间的概念，其定义与线性代数中叙述的数域上的线性空间概念完全一致，基本性质也是一样的. 容易看出，若 K 是 F 的扩域，则 K 可以看成 F 上的线性空间.

定理 3.1.7 设 $F(\alpha)$ 是 F 的单代数扩张，$\deg(\alpha,F)=n$，则 $F(\alpha)$ 是 F 上的 n 维线性空间，且 $1,\alpha,\alpha^2,\cdots,\alpha^{n-1}$ 是 $F(\alpha)$ 的一组基.

证 注意到定理 3.1.5 的证明中的满同态 $\phi:F[x]\to F[\alpha]=F(\alpha)$，$\phi(f(x))=f(\alpha)$，$f(x)\in F[x]$. 由定义 $\ker\phi=\langle\mathrm{Irr}(\alpha,F)\rangle$. 由于 $\deg(\alpha,F)=n$，对任何 $g(x)\in F[x]$ 存在 $q(x)$，$r(x)$ 使得 $g(x)=q(x)\mathrm{Irr}(\alpha,F)+r(x)$，其中 $r(x)=0$ 或 $\deg r(x)<n$. 于是 $g(\alpha)=r(\alpha)$. 于是 $1,\alpha,\cdots,\alpha^{n-1}$ 是 F 上线性空间 $F(\alpha)$

的一组生成元.下面证明它们线性无关,事实上,若 $a_1, a_2, \cdots, a_n$ 使

$$a_1 + a_2\alpha + a_3\alpha^2 + \cdots + a_n\alpha^{n-1} = 0.$$

令 $h(x) = a_1 + a_2x + \cdots + a_nx^{n-1}$.则 $h(\alpha) = 0$,从而 $h(x) \in \ker \phi = \langle \mathrm{Irr}(\alpha, F) \rangle$,即 $\deg h(x) \geqslant n$,若 $h(x) \neq 0$,则 $\deg h(x) < n$,得到矛盾.故 $h(x) = 0$,即 $a_1 = a_2 = \cdots = a_n = 0$,故 $1, \alpha, \cdots, \alpha^{n-1}$ 线性无关.定理证毕. □

以下讨论域扩张的等价性问题.我们先给出一个定义.

定义 3.1.7 设 K_1, K_2 都是 F 的扩域,若存在 K_1 到 K_2 上的同构 ϕ 使得 $\phi|_F = \mathrm{id}_F$,则称 K_1, K_2 为 F 的**等价扩张**,ϕ 称为 F **- 同构**.当 $K_1 = K_2$ 时,称 ϕ 为 F **- 自同构**.例如,恒等映射就是一个 F - 自同构.

等价扩张显然是一个等价关系.关于单扩张的等价性我们有:

定理 3.1.8 (1) 若 $F(\alpha_1), F(\alpha_2)$ 都是 F 的单超越扩张,则 $F(\alpha_1), F(\alpha_2)$ 是 F 的等价扩张.

(2) 对任何 $F[x]$ 上的首一不可约多项式 $p(x)$,存在 F 的单代数扩张 $F(\beta)$ 使得 $\mathrm{Irr}(\beta, F) = p(x)$.且任何满足这个条件的两个单代数扩张一定是 F 的等价扩张.

证 (1) 注意定理 3.1.5 中的映射 ϕ.它说明任何单超越扩张都与 $F[x]$ 的分式域 $F(x)$ 同构.显然 $\phi|_F = \mathrm{id}_F$,故它导出从 $F(x)$ 到单超越扩张的 F - 同构.(1)得证.

(2) 由于 $p(x)$ 是不可约多项式,故 $\langle p(x) \rangle$ 是 $F[x]$ 的极大理想,因此 $F[x]/\langle p(x) \rangle$ 是域.$F[x]/\langle p(x) \rangle$ 中的元是等价类 $f(x) + \langle p(x) \rangle$,其中 $f(x) \in F[x]$,自然可以将 F 中的元素 a 等同于 $a + \langle p(x) \rangle$.于是 F 是 $F[x]/\langle p(x) \rangle$ 的子域.容易看出 $F(x + \langle p(x) \rangle) = F[x]/\langle p(x) \rangle$.事实上,令 $\alpha = x + \langle p(x) \rangle$,则对任何 $f(x) \in F[x]$ 有 $f(\alpha) = f(x) + \langle p(x) \rangle$.特别 $p(\alpha) = p(x) + \langle p(x) \rangle = 0 + \langle p(x) \rangle$,故 $\mathrm{Irr}(\alpha, F) = p(x)$.此外,定理

3.1.5 的证明说明任何两个这样的代数扩张都与 $F[x]/\langle p(x)\rangle$ F - 同构. □

值得注意的是,一个域的两个等价扩张不一定有相同的不可约多项式.例如,对于实数域$\mathbb{R}$,令 $\alpha=\sqrt{-1}$,$\beta=\sqrt{-2}$,则容易看出$\mathbb{R}(\alpha)$,$\mathbb{R}(\beta)$都是复数域$\mathbb{C}$,从而是$\mathbb{R}$ 的等价扩张.但是 $\mathrm{Irr}(\alpha,\mathbb{R})=x^2+1$,$\mathrm{Irr}(\beta,\mathbb{R})=x^2+2$.

习 题

1. 求 Guass 整数环$\mathbb{Z}[\sqrt{-1}]$的分式域.

2. 设 K 是有限域,$\mathbb{Z}_p$ 是 K 中的素域.证明:$\forall \alpha\in K$,α 是$\mathbb{Z}_p$ 上的代数元.

3. 设 θ 为$x^4+1\in\mathbb{Q}[x]$的一个根.在$\mathbb{Q}(\theta)$中将 x^4+1 分解为不可约因式之积.

4. 对下列的 $\alpha\in\mathbb{C}$,求 $\mathrm{Irr}(\alpha,\mathbb{Q})$:

(1) $1+\sqrt{2}$; (2) $\sqrt{2}+\sqrt{3}$;

(3) $\sqrt{1+\sqrt[3]{2}}$; (4) $\sqrt{\sqrt[3]{2}-\sqrt{-1}}$.

5. 试求$\mathbb{Q}(\sqrt[3]{2})$中元 $1+\sqrt[3]{2}+\sqrt[3]{4}$的逆元.

6. 证明:x^2+x+1 是$\mathbb{Z}_2[x]$中的不可约多项式.若 θ 是 x^2+x+1 的一个根.证明$\mathbb{Z}_2(\theta)$含有 4 个元素,并写出$\mathbb{Z}_2(\theta)$的加法表与乘法表,求出 x^2+x+1 的另一个根.

7. 设 F 是一个域,K 是 F 的扩域,$\alpha\in K$ 是 F 上的超越元.设 $E_1=F(\alpha)$,$E_2=F\left(\frac{\alpha^3}{1+\alpha}\right)$.证明:$E_1$ 是 E_2 的单代数扩张,并求 $\mathrm{Irr}(\alpha,E_2)$.

8. 设 α 是$\mathbb{Q}[x]$中不可约多项式 x^2-5x+7 的根,试将

$$\frac{1-7\alpha+2\alpha^2}{1+\alpha-\alpha^2}$$

写成 α 的多项式.

9. 设 α 为$\mathbb{Q}[x]$上的多项式 $x^8-8x^6+12x^4+2$ 的一个根,试求$\mathbb{Q}(\alpha^2)$作为$\mathbb{Q}$ 上线性空间的维数和一组基.

补充题

1. 试求复数 $\alpha=\sqrt{-1}$ 和 $\beta=\dfrac{2\sqrt{-1}+1}{\sqrt{-1}-1}$ 在 $\mathbb{Q}$ 上的不可约多项式，并判断 $\mathbb{Q}(\alpha)$ 与 $\mathbb{Q}(\beta)$ 是否同构.

2. 设 p 为奇素数，α 为 $\mathbb{Q}[x]$ 上多项式 $x^{p^2}+px^p+1$ 的一个根，试求 $\mathbb{Q}(\alpha^p)$ 作为 $\mathbb{Q}$ 上的线性空间的维数与一组基.

3. 设 K 为 F 的扩域，$\alpha\in K$，若 $F[\alpha]$ 是域，证明：α 为 F 上的代数元.

4. 证明：商环 $\mathbb{Z}[\sqrt{-1}]/\langle 2+\sqrt{-1}\rangle$ 是域，并求出其特征.

5. 设 K 是特征为 p 的域（$p>0$），且任何 $\alpha\in K$ 满足 $\alpha^p-\alpha=0$，试证明 $K\simeq\mathbb{Z}_p$.

6. 设 K 是 F 的扩域，$\alpha\in K^*$，α 是 F 上的代数元，且 $\mathrm{Irr}(\alpha,F)=x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$. 证明：$\alpha^{-1}$ 也是 F 上的代数元，且

$$\mathrm{Irr}(\alpha^{-1},F)=x^n+a_{n-1}a_n^{-1}x^{n-1}+\cdots+a_1a_n^{-1}x+a_n^{-1}.$$

§3.2 域的代数扩张

本节我们考虑一类特殊的扩张，即代数扩张.

定义 3.2.1 设 K 为域 F 的扩域. 若 K 中的每个元素都是 F 上的代数元，则称 K 为 F 的**代数扩张**.

一个自然的问题是，若 $K=F(S)$，且集合 S 中每个元素都是 F 上的代数元，那么 K 是否是 F 的代数扩张？本节将回答这个问题. 过程中我们将碰到一类更为特殊的扩张. 我们先给出其定义.

定义 3.2.2 设 K 为 F 的扩域，若 K 作为 F 上的线性空间是有限维的，则称 K 为 F 的**有限扩张**. K 的维数称为 K 在 F 上的**次数**，记为 $[K:F]$. 若 K 作为 F 上的线性空间是无限维的，则称 K 为 F 的**无限扩张**.

关于单扩张我们有

定理 3.2.1 设 $F(\alpha)$ 为 F 的单扩张，则下列三个条件等价.

(1) $F(\alpha)$是 F 的代数扩张；

(2) α 是F 上的代数元；

(3) $F(\alpha)$是 F 的有限扩张.

证 (1)$\Longrightarrow$(2)是显然的.若 α 是 F 上的代数元,则定理 3.1.5 说明 $F(\alpha)$是 F 上的有限维线性空间,故(2)$\Longrightarrow$(3)成立.若(3)成立,设$[F(\alpha):F]=n<\infty$,则$\forall \beta\in F(\alpha)$,$1,\beta,\beta^2,\cdots,\beta^n$一定线性相关,故存在不全为 0 的 $a_1,a_2,\cdots,a_n\in F$ 使得 $a_1+a_2\beta+\cdots+a_n\beta^n=0$,这说明 β 是 F 上代数元,故(1)成立.于是(1),(2),(3)等价. □

由定理 3.2.1 的证明容易看出,有限扩张一定是代数扩张.

定理 3.2.2 设 E 为域F 的有限扩张,K 为 E 的有限扩张,则 K 是F 的有限扩张,且

$$[K:F]=[K:E][E:F].$$

证 设$[K:E]=n$,$[E:F]=m$.取定 K 作为E 上的线性空间的一组基$\alpha_1,\alpha_2,\cdots,\alpha_n$,$E$ 作为 F 上的线性空间的一组基$\beta_1,\beta_2,\cdots,\beta_m$.我们证明集合 $S=\{\alpha_i\beta_j\mid i=1,2,\cdots,n,j=1,2,\cdots,m\}$构成 K 作为F 上的线性空间的一组基.$\forall\gamma\in K$,由条件存在 $a_1,a_2,\cdots,a_n\in E$ 使得 $\gamma=a_1\alpha_1+\cdots+a_n\alpha_n$,又 $a_i\in E$,故存在 $b_{ij}\in F$,$i=1,2,\cdots,n$,$j=1,2,\cdots,m$ 使

$$a_i=b_{i1}\beta_1+b_{i2}\beta_2+\cdots+b_{im}\beta_m,\ i=1,2,\cdots,n.$$

将 a_i 的表达式代入γ 的表达式,我们看出 S 是K 作为F 上线性空间的生成元.此外,设 $c_{ij}\in F$,$i=1,2,\cdots,n$,$j=1,2,\cdots,m$,使

$$\sum_{i=1}^{n}\sum_{j=1}^{n}c_{ij}\alpha_i\beta_j=0,$$

则

$$\sum_{i=1}^{n}\Big(\sum_{j=1}^{n}c_{ij}\beta_j\Big)\alpha_i=0.$$

因为 $\alpha_1,\cdots,\alpha_n$ 是E－线性无关的,故

$$\sum_{j=1}^{n} c_{ij}\beta_j = 0, i = 1,2,\cdots,n.$$

又由于 $\beta_1,\cdots,\beta_m$ 是 F - 线性无关的，于是 $c_{ij} = 0, i = 1,2,\cdots,n, j = 1,2,\cdots,m$. 从而 S 是 F - 线性无关的. 定理证毕. □

推论 3.2.3 $F(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 是域 F 的代数扩张当且仅当 $F(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 是 F 的有限扩张当且仅当 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 是 F 上的代数元.

这是因为 $F(\alpha_1,\alpha_2,\cdots,\alpha_n) = F(\alpha_1)(\alpha_2)\cdots(\alpha_n)$.

推论 3.2.4 域 F 上的两个代数元的和、差、积、商(分母不为零)仍为 F 上的代数元.

推论 3.2.5 设 $E = F(S)$，其中 S 的元素都是 F 上的代数元，则 E 是 F 的代数扩张.

推论 3.2.5 回答了本节开始时提出的问题.

推论 3.2.6 若 E 是域 F 的代数扩张，K 是 E 的代数扩张，则 K 是 F 的代数扩张.

证 设 $\alpha \in K$，由于 α 是 E 上的代数元，存在不全为零的 $a_1, a_2,\cdots,a_n \in E$ 使得

$$a_1 + a_2\alpha + \cdots + a_n\alpha^{n-1} = 0.$$

这说明 α 是 $F(\alpha_1,\cdots,\alpha_n)$ 上的代数元，又 E 是 F 的代数扩张，故 $F(\alpha_1,\cdots,\alpha_n)$ 是 F 的有限扩张，从而 $F(\alpha_1,\cdots,\alpha_n,\alpha)$ 是 F 的有限扩张，故 α 为 F 上的代数元. □

最后我们看一下域扩张的一般过程

定义 3.2.3 设 K 为 F 的扩张，K 中在 F 上为代数元的元素的集合 K_0 称为 F 在 K 中的**代数闭包**.

定理 3.2.7 设 K 为 F 的扩张，K_0 为 F 在 K 中的代数闭包，则 K_0 是含于 K 的 F 的最大代数扩张，且 $\forall \delta \in K - K_0$，$\delta$ 是 K_0 上的超越元.

证明 由推论 3.2.4，K_0 是域，显然 $F \subseteq K_0$，由定义可知 K_0

是 F 在 K 中的最大代数扩张. $\forall \delta \in K - K_0$，若 δ 是 K_0 上代数元，则 $K_0(\delta) \supseteq K_0 \supseteq F$，由推论 3.2.6 知 δ 是 F 上代数元. 这是矛盾. □

由定理 3.2.7 可知任何域的扩张都可以分成两步进行，即先进行代数扩张，再进行超越扩张.

习 题

1. 求下列域扩张的次数：

(1) $[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}]$；　　(2) $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]$；

(3) $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2}+\sqrt{3})]$；　　(4) $\left[\mathrm{R}\left(\frac{2\sqrt{-1}+1}{\sqrt{-1}-1}\right):\mathrm{R}\right]$.

2. 设 K 为 F 的有限扩张，若 $[K:F]$ 是素数，证明：K 与 F 之间没有中间域，即不存在域 E 使得 $K \supset E \supset F$，且 $K \neq E$，$E \neq F$.

3. 设 K 是 F 的扩域，且 $[K:F]=p$ 为素数，证明

$$K = F(\alpha), \quad \forall \alpha \in K - F.$$

4. 设 R 为整环，且包含域 F 作为子环，若 $\forall \alpha \in R$ 为 F 上的代数元，证明：R 是 F 的代数扩张.

5. 设 K 为 F 的扩域，$\alpha \in K$ 是 F 上的代数元，且 $\deg(\alpha, F)$ 为奇数，证明：$F(\alpha^2) = F(\alpha)$.

6. 设 K 是 $\mathbb{Q}$ 的代数扩张，且 $[K:\mathbb{Q}]=2$. 证明：必存在 $\alpha = \pm p_1 p_2 \cdots p_n$，其中 $p_1, p_2, \cdots, p_n$ 为互不相同的素数，使得 $K = \mathbb{Q}(\sqrt{\alpha})$.

7. 证明：若 $a, b \in \mathbb{Q}$，$\sqrt{a}+\sqrt{b} \neq 0$，则 $\mathbb{Q}(\sqrt{a},\sqrt{b}) = \mathbb{Q}(\sqrt{a}+\sqrt{b})$.

8. 试证明对任何正整数 n，存在 $\mathbb{Q}$ 的代数扩张 K 使得 $[K:\mathbb{Q}]=n$.

补充题

1. 设 K 是有限域，K 的特征为 p，试证明 K 中的元素个数必为 p^n，其中 $n \in \mathrm{N}$.

2. 设 K 是 F 的有限扩张，证明：必存在中间域的升链

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_r = K,$$

其中 F_{i+1} 是 F_i 的单代数扩张，$i = 0, 1, \cdots, r-1$.

3. 设 K, E, F 是三个域，$F \subset E \subset K$，且 $[E:F]=m$. 设 $a \in K$ 在 F 上的次数为 n，且 $(m,n)=1$. 证明：a 在 E 上的次数也是 n.

4. 求 $[\mathbb{Q}(\sqrt[3]{2},\sqrt[3]{6},\sqrt[3]{24}):\mathbb{Q}]$，并求 $\mathbb{Q}(\sqrt[3]{2},\sqrt[3]{6},\sqrt[3]{24})$ 作为 $\mathbb{Q}$ 上的线性空间的一组基.

§3.3 多项式的分裂域

我们知道，在复数域上任何一个一元代数方程都有解，而在实数域上就不一定. 这说明求代数方程的根与数域的范围有关. 这个问题推广到一般域上就得到多项式的分裂域的概念.

设 F 是一个域，一般说来，并非每个 F 上多项式都能在 $F[x]$ 中分解成一次因式的乘积. 如果能做到这一点，则称 F 为一个代数闭域. 这时 F 不可能再有代数扩张. 例如，复数域是代数闭域，而实数域不是. 抽象代数中可以证明，每个域都可以扩张成一个代数闭域. 当然这一结果的证明已超出本书范围. 但是我们可以处理稍微简单一点的情形.

定义 3.3.1 设 F 为域，$f(x) \in F[x]$，F 的一个扩域 E 称为 $f(x)$ 在 F 上的一个**分裂域**，如果 $f(x)$ 在 $E[x]$ 上可以分解为一次因式的乘积：

$f(x)=a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$，$a \in F$，$\alpha_i \in E$，$i=1,2,\cdots,n$.

而且 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$.

由定义，分裂域是使该多项式分解成一次因式乘积的最小域. 本节将解决分裂域的存在性与惟一性问题.

定理 3.3.1 设 $f(x)$ 是域 F 上的多项式，且 $\deg f(x)>0$，则 $f(x)$ 在 F 上的分裂域存在.

证 对 $\deg f(x)$ 用数学归纳法证明. 当 $\deg f(x)=1$ 时，$f(x)=ax+b=a(x-a^{-1}b)$，$a,b \in F$，故 F 就是 $f(x)$ 的分裂域. 设结论对于 $\deg f(x)=k$ 时成立，当 $\deg f(x)=k+1$ 时，设 $p(x)$ 是 $f(x)$ 的一个不可约因式，令 $F_1=F[x]/\langle p(x)\rangle$，则 F_1 是 F 的单代

数扩张，且 $F_1 = F(\alpha_1)$，其中 $\alpha_1 = x + \langle p(x) \rangle$. 于是 $p(\alpha_1) = 0$，故在 F_1 上有 $f(\alpha_1) = 0$. 作为 $F_1[x]$ 内的多项式 $f(x)$ 有分解

$$f(x) = (x - \alpha_1) f_1(x), f_1(x) \in F_1[x], \deg f_1(x) = k.$$

由归纳假设，存在 $f_1(x)$ 在 F_1 上的分裂域 $E = F_1(\alpha_2, \cdots, \alpha_{k+1})$. 于是在 E 上 $f(x)$ 有分解 $f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_{k+1})$. 另一方面

$$E = F_1(\alpha_2, \cdots, \alpha_{k+1}) = F(\alpha_1)(\alpha_2, \cdots, \alpha_{k+1}) = F(\alpha_1, \alpha_2, \cdots, \alpha_{k+1}).$$

故 E 是 $f(x)$ 在 F 上的分裂域. 至此定理证毕. □

下面考虑域上一个多项式分裂域的个数问题. 我们先证明两个引理.

引理 3.3.2 设 F_1, F_2 为两个域，$\phi: F_1 \to F_2$ 为同构，则存在环 $F_1[x]$ 到 $F_2[x]$ 的同构 ϕ' 使得 $\phi'|_{F_1} = \phi$. 且 $p(x) \in F_1[x]$ 不可约当且仅当 $\phi'(p(x)) \in F_2[x]$ 不可约.

证 设 $f(x) = a_0 + a_1 x + \cdots a_n x^n \in F_1[x]$. 令 $\phi': F_1[x] \to F_2[x]$ 使得

$$\phi'(f(x)) = \phi(a_0) + \phi(a_1)x + \cdots \phi(a_n)x^n.$$

则 ϕ' 满足引理的要求. □

引理 3.3.3 设 F_1, F_2 为域，$\phi: F_1 \to F_2$ 为同构. K_1, K_2 分别为 F_1, F_2 的扩域. 将 ϕ 如同引理 3.3.2 那样扩充到 $F_1[x]$ 上，仍记为 ϕ. 设 $p(x) \in F_1[x]$ 为不可约多项式. 若 α_1, α_2 分别为 $p(x)$ 和 $p'(x) = \phi(p(x))$ 在 K_1 和 K_2 中的根，则 ϕ 可扩张为 $F_1(\alpha_1)$ 到 $F_2(\alpha_2)$ 上的同构 ϕ' 使得 $\phi'|_{F_1} = \phi, \phi'(\alpha_1) = \alpha_2$.

证 设 $\deg p(x) = \deg p'(x) = n$. 由定理 3.1.6，$1, \alpha_1, \cdots, \alpha_1^{n-1}$ 和 $1, \alpha_2, \cdots, \alpha_2^{n-1}$ 分别是 $F_1(\alpha_1)$ 作为 F_1 上线性空间和 $F_2(\alpha_2)$ 作为 F_2 上线性空间的基. 现在定义 $\phi': F_1(\alpha_1) \to F_2(\alpha_2)$ 使得

$$\phi'(a_0 + a_1\alpha_1 + \cdots + a_n\alpha_1^{n-1}) = \phi(a_0) + \phi(a_1)\alpha_2 + \cdots + \phi(a_n)\alpha_2^{n-1}.$$

由于 ϕ 为同构,故 ϕ' 为一一对应.显然 ϕ' 保持加法不变.下面证明 ϕ' 保持乘法不变.设

$$\sum_{i=0}^{n-1} a_i\alpha_1^i,\ \sum_{i=0}^{n-1} b_i\alpha_1^i \in F(\alpha_1),$$

令

$$f(x)=\Big(\sum_{i=0}^{n-1} a_ix^i\Big)\Big(\sum_{i=0}^{n-1} b_ix^i\Big).$$

设 $f(x)=p(x)q(x)+r(x)$,其中 $r(x)=0$ 或 $\deg r(x)<n$.则

$$\Big(\sum_{i=0}^{n-1} a_i\alpha_1^i\Big)\Big(\sum_{i=0}^{n-1} b_i\alpha_1^i\Big)=r(\alpha_1).$$

而由 ϕ 的定义有 $\phi(f(x))=p'(x)\phi'(q(x))+\phi'(r(x))$,$\phi'(r(x))=0$或$\deg\phi'(r(x))<n$.从而

$$\phi'\Big[\Big(\sum_{i=0}^{n-1} a_i\alpha_1^i\Big)\Big(\sum_{i=0}^{n-1} b_i\alpha_1^i\Big)\Big]=\phi'(r(\alpha_1))$$

$$=\phi(f(x))\big|_{x=\alpha_1}=\phi\Big[\Big(\sum_{i=0}^{n-1} a_ix^i\Big)\Big(\sum_{i=0}^{n-1} b_ix^i\Big)\Big]\Big|_{x=\alpha_1}$$

$$=\phi'\Big(\sum_{i=0}^{n-1} a_i\alpha_1^i\Big)\phi'\Big(\sum_{i=0}^{n-1} b_i\alpha_1^i\Big).$$

故 ϕ' 为同构.显然 $\phi'|_{F_1}=\phi$,$\phi'(\alpha_1)=\alpha_2$. □

定理 3.3.4 设 F_1,F_2 为域,$\phi:F_1\to F_2$ 为同构.将 ϕ 如同引理 3.3.2 开拓到 $F_1[x]$上,仍记为 ϕ.设 $f(x)\in F_1[x]$且 E_1,E_2 分别为 $f(x),\phi(f(x))$在 F_1,F_2 上的分裂域.则存在 E_1 到 E_2 的同构 ϕ'使得$\phi'|_{F_1}=\phi$.

证 对 $\deg f(x)$用归纳法证明.若 $\deg f(x)=1$,则 $\deg\phi(f(x))=1$.这时$E_1=F_1,E_2=F_2$,结论成立.若结论对 $\deg f(x)=k-1$ 成立,当 $\deg f(x)=k$ 时.取定 $f(x)$的一个不可约因式 $p(x)$.由引理 3.3.2,$p'(x)=\phi(p(x))$为 $F_2[x]$中不可约多项式.由定理 3.1.7 分别存在 F_1 和 F_2 的单代数扩张 $F_1(\alpha_1)$,$F_2(\alpha_2)$使得 α_1,α_2 的不可约多项式分别为 $p(x),p'(x)$.由引理

3.3.3，ϕ 可以扩充为 $F_1(\alpha_1)$ 到 $F_2(\alpha_2)$ 的同构 σ 使得

$$\sigma|_{F_1}=\phi,\sigma(\alpha_1)=\alpha_2.$$

又在 $F_1(\alpha_1)[x],F_2(\alpha_2)[x]$ 上有

$$f(x)=(x-\alpha_1)f_1(x),\phi(f(x))=(x-\alpha_2)f_2(x),$$

其中 $f_1(x)\in F_1(\alpha_1)[x],f_2(x)\in F_2(\alpha_2)[x]$. 由引理 3.3.2，$\sigma$ 可以扩充为 $F_1(\alpha_1)[x]$ 到 $F_2(\alpha_2)[x]$ 的同构映射 σ' 使得 $\sigma'|_{F_1(\alpha_1)}=\sigma$. 因此

$$\sigma'(f(x))=\phi(f(x)).$$

故 $\sigma'(f_1(x))=f_2(x)$. 由分裂域的定义，$f_1(x),f_2(x)$ 在 $F_1(\alpha_1),F_2(\alpha_2)$ 上的分裂域即为 $f(x),\phi(f(x))$ 在 F_1,F_2 上的分裂域 E_1,E_2. 由归纳假设 σ 可以扩充为 E_1 到 E_2 的同构 ϕ' 且 $\phi'|_{F_1}=\phi$. □

在定理 3.3.4 中，取 $F_1=F_2$，取 $\phi=\mathrm{id}_F$，便得到：$f(x)\in F_1[x]$ 的任何两个分裂域 E_1 与 E_2 是同构的. 至此我们已证明，对于任何域上的任何多项式，其分裂域存在且在同构意义下惟一. 下面我们举例说明如何求分裂域.

例 1 设 $f(x)\in\mathbb{R}[x]$，若 $f(x)$ 的根都是实根，自然 $f(x)$ 的分裂域是 $\mathbb{R}$. 若 $f(x)$ 至少有一个非实根，则 $f(x)$ 的分裂域为 $\mathbb{C}$. 事实上，任何多项式在 $\mathbb{C}[x]$ 上都可以分解成一次因式的乘积，因此 $f(x)$ 的分裂域是 $\mathbb{C}$ 的子域，包含 $\mathbb{R}$ 且不等于 $\mathbb{R}$. 但是 $[\mathbb{C}:\mathbb{R}]=2$，由定理 3.2.2 知 $\mathbb{C},\mathbb{R}$ 之间没有中间域. 故 $f(x)$ 的分裂域为 $\mathbb{C}$.

例 2 设 F 是一个域，求 $x^2+ax+b(a,b\in F)$ 在 F 上的分裂域 E.

解 若 x^2+ax+b 在 F 上可约，则 $E=F$. 若不可约，设 $\alpha_1=x+\langle x^2+ax+b\rangle$，则 α_1 是 x^2+ax+b 在域 $F[x]/\langle x^2+ax+b\rangle$ 上的一个根且

$$F(\alpha_1)\simeq F[x]/\langle x^2+ax+b\rangle.$$

在 $F(\alpha_1)$中$(x-\alpha_1)\mid(x^2+ax+b)$.故 x^2+ax+b 在 $F(\alpha_1)[x]$ 上有分解

$$x^2+ax+b=(x-\alpha_1)(x-\alpha_2),\alpha_2\in F(\alpha_1).$$

于是 $E=F(\alpha_1,\alpha_2)=F(\alpha_1)$.易见$[E:F]=2$.

例 3 求 $x^p-1\in\mathbb{Q}[x]$的分裂域 E,其中 p 为素数.

解 因为 $x^p-1=(x-1)(x^{p-1}+x^{p-2}+\cdots+x+1)$.故 x^p-1 的分裂域为 $x^{p-1}+x^{p-2}+\cdots+x+1$ 的分裂域.因为 p 为素数,故 $x^{p-1}+x^{p-2}+\cdots+x+1$ 在$\mathbb{Q}[x]$上不可约.设 α 是它的一个根,则$\mathbb{Q}(\alpha)=\mathbb{Q}(\alpha,\alpha^2,\cdots,\alpha^{p-1})$;且$(\alpha^k)^p=(\alpha^p)^k=1,1\leqslant k\leqslant p-1$.故 $\alpha,\alpha^2,\cdots,\alpha^{p-1}$都是 $x^{p-1}+x^{p-2}+\cdots+x+1$ 的根.注意它们两两不等,故在$\mathbb{Q}(\alpha)$上可以分解为

$$x^{p-1}+x^{p-2}+\cdots+x+1=(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{p-1}).$$

因此 $E=\mathbb{Q}(\alpha)$且$[E:\mathbb{Q}]=p-1$.

习 题

1. 求下列多项式在$\mathbb{Q}$上的分裂域:

(1) x^2+3; (2) x^5-1;

(3) $(x^2-2)(x^2-3)$; (4) x^4+1.

2. 求 $f(x)=x^3+x+1$ 在$\mathbb{Z}_2$上的分裂域.

3. 设 E 为 n 次多项式 $f(x)$在 F 域上的分裂域,证明:$[E:F]\leqslant n!$.

4. 证明:有理数域$\mathbb{Q}$上多项式 x^4+1 的分裂域是单扩域$\mathbb{Q}(\alpha)$,其中 α 是 x^4+1 的一个根.

5. 求有理数域上多项式 x^3-x^2-x-2 的分裂域 E,并求$[E:\mathbb{Q}]$.

6. 设 F 为特征为 p 的域,$F(\alpha)$是 F 的单扩域,其中 α 是 $F[x]$上多项式 x^p-a 的一个根,试问 $F(\alpha)$是不是 x^p-a 在 F 上的分裂域?为什么?

补充题

1. 设 x^3-a 是$\mathbb{Q}[x]$上的不可约多项式,α 为 x^3-a 的一个根.证明:$\mathbb{Q}(\alpha)$不可能是 x^3-a 在$\mathbb{Q}$上的分裂域.

2. 求$\mathbb{Q}[x]$上多项式 x^5-1 的分裂域.

3. 设 p 为素数，$\mathbf{Z}_p(a)$是$\mathbf{Z}_p$ 的单超越扩张，求 $x^p - a \in \mathbf{Z}_p(a)[x]$的分裂域.

4. 设 F 为域，F 的一个代数扩张 K 称为 F 的**正规扩张**，若 $F[x]$中的一个不可约多项式 $p(x)$在 K 中有一个根，则 $p(x)$的所有根都在 K 中，即在 K 中 $p(x)$可以分解为一次因式的乘积. 证明：

(1) F 的有限扩张 K 为正规扩张当且仅当 K 是 $F[x]$中一个多项式的分裂域；

(2) 设 E, K 都是 F 的扩域，且 $F \subseteq E \subseteq K$. 若 K 是 F 的正规扩张，则 K 也是 E 的正规扩张；

(3) F 的二次扩张是正规扩张.

5. 证明：$\mathbf{Q}(\sqrt[3]{5})$不是$\mathbf{Q}$ 的正规扩张.

6. 设$\mathbf{C}_0$是$\mathbf{Q}$ 在$\mathbf{C}$ 中的代数闭包($\mathbf{C}_0$称为代数数域). 证明：$\mathbf{C}_0$是$\mathbf{Q}$ 的正规扩张，且$[\mathbf{C}_0 : \mathbf{Q}] = +\infty$.

§3.4 域的可分扩张*

在高等代数中我们学过数域上多项式的重因式与重根的概念. 本节将介绍一般域上的有关性质.

设 F 是一个域，$f(x) \in F[x]$，$\deg f(x) > 0$，K 是 $f(x)$的一个分裂域. 则$f(x)$在 $K[x]$上有分解

$$f(x) = c(x - a_1)^{k_1}(x - a_2)^{k_2} \cdots (x - a_r)^{k_r},$$

其中 $k_i \geqslant 1, 1 \leqslant i \leqslant r$，且当 $i \neq j$ 时，$a_i \neq a_j$. 由于 $f(x)$的任何两个分裂域是同构的，因此在 $f(x)$的任何分裂域上都有类似的分解. 特别是 $f(x)$有无重根与分裂域无关，只与 $f(x)$有关. 下面我们先来看看如何根据 $f(x)$本身的性质来确定 $f(x)$是否有重根.

定义 3.4.1 设 F 是域，$f(x) \in F[x]$，若

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0.$$

则称 $F[x]$中多项式

$$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + a_1$$

为 $f(x)$的**形式微商**.

注意形式微商与分析中的导数的区别，因为在一般域上没有连续的概念，也没有极限的概念，所以这里的微商完全是从“形式”上定义的.

我们将形式微商的主要性质列出来，其证明留作习题.

性质 1 $a'=0, \forall a\in F$；当 F 的特征为 0 时，由 $f'(x)=0$ 可以推出 $f(x)\in F$.

性质 2 $x'=1$.

性质 3 $(af(x)+bg(x))'=af'(x)+bg'(x), \forall a,b\in F, f(x),g(x)\in F[x]$.

性质 4 $(f(x)g(x))'=f'(x)g(x)+f(x)g'(x), \forall f(x),g(x)\in F[x]$.

注意性质 1 中，当 Ch $F=p$ 不为 0 时，不能由 $f'(x)=0$ 推出 $f(x)\in F$，因为 $(x^p)'=px^{p-1}=(p\cdot 1)x^{p-1}=0$.

定理 3.4.1 设 F 为域，$f(x)\in F[x]$，K 为 $f(x)$ 的分裂域，α 是 $f(x)$ 在 K 中的一个 k 重根，则当 Ch $F\nmid k$ 时，α 是 $f'(x)$ 的 $k-1$ 重根，当 Ch $F\mid k$ 时，α 是 $f'(x)$ 的至少 k 重根.

证 由条件，存在 $g(x)\in K[x]$ 使 $f(x)=(x-\alpha)^k g(x)$，且 $g(\alpha)\neq 0$. 由性质 4 得

$$\begin{aligned} f'(x)&=k(x-\alpha)^{k-1}g(x)+(x-\alpha)^k g'(x)\\ &=(x-\alpha)^{k-1}(kg(x)+(x-\alpha)g'(x)). \end{aligned}$$

当 Ch $F\nmid k$ 时，$k\cdot 1\neq 0$，于是 $kg(\alpha)+(\alpha-\alpha)g'(\alpha)=k\cdot 1\cdot g(\alpha)\neq 0$，故 α 是 $f'(x)$ 的 $(k-1)$ 重根. 当 Ch $F\mid k$ 时，$kg(x)=k\cdot 1\cdot g(x)=0$，故 $f(x)=(x-\alpha)^k g'(x)$. 故 α 是 $f'(x)$ 的至少 k 重根. □

设 F 是域，$F[x]$ 为 F 上一元多项式环，$f(x),g(x)\in F[x]$，我们将 $f(x),g(x)$ 的首项系数为 1 的最大公因式记为 $(f(x),g(x))$. 最大公因式可以像高等代数中一样用辗转相除法得到. 与高等代数中一样，若 K 是 F 的扩域，$f(x),g(x)\in F[x]$，则 $f(x),g(x)$ 在 $K[x]$ 上的最大公因式与 $f(x),g(x)$ 作为

$F[x]$上的多项式的最大公因式是相同的.

定理 3.4.2 设 K 是 $f(x)$的分裂域,则 $f(x)$在 K 中无重根的充要条件是$(f(x),f'(x))=1$.

证 若 $f(x)$有 k 重根 α,其中 $k>1$. 由定理 3.4.1,α 是 $f(x)$的至少 $k-1$ 重根,于是在 $K[x]$中,$(x-\alpha)^{k-1}\mid f(x)$,$(x-\alpha)^{k-1}\mid f'(x)$. 因此$(x-\alpha)^{k-1}\mid(f(x),f'(x))$. 故 $\deg(f(x),f'(x))\geqslant 1$,从而$(f(x),f'(x))\neq 1$.

另一方面,若 $f(x)$在 K 中无重根,则

$$f(x)=c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n),$$

其中 $c\in K$,且当 $i\neq j$ 时,$\alpha_i\neq\alpha_j$. 由定理 3.4.1(注意,由于 $f(x)$无重根,这时不可能出现 Ch $F\mid k$ 的情况)知 α_i 不是 $f'(x)$的根,$i=1,2,\cdots,n$. 因此$(f(x),f'(x))=1$. □

下面我们将定理 3.4.2 用到不可约多项式上.

推论 3.4.3 设 $p(x)$是 $F[x]$中的不可约多项式,$\deg p(x)>0$. 则 $p(x)$在其分裂域中有重根的充要条件是 $p'(x)=0$.

证 若 $p'(x)=0$,则$(p(x),p'(x))=p(x)\neq 1$,故由定理 3.4.2,$p(x)$有重根. 反之,若 $p(x)$有重根,则$(p(x),p'(x))=d(x)\neq 1$,由于 $p(x)$不可约,故没有非平凡因子,故 $d(x)=cp(x)$,$c\in F$,$c\neq 0$. 另一方面 $d(x)\mid p'(x)$,若 $p'(x)\neq 0$,则 $\deg p'(x)<\deg p(x)$,得到矛盾. 于是只能 $p'(x)=0$. □

若 Ch $F=0$,则对 $F[x]$中任何不可约多项式 $p(x)$,若 $\deg p(x)>0$,则 $\deg p'(x)\geqslant 0$,因此 $p'(x)\neq 0$. 因此我们有:

推论 3.4.4 若 Ch $F=0$,$p(x)$为 $F[x]$中不可约多项式,且 $\deg p(x)>0$,则 $p(x)$在其分裂域中无重根.

定义 3.4.2 设 F 为域,$p(x)\in F[x]$为不可约多项式,若 $p(x)$在其分裂域中只有单根,则称 $p(x)$为 F 上**可分的不可约多项式**. 若 $f(x)\in F[x]$且$f(x)$的每个不可约因式都是可分的,则称 $f(x)$为 F 上的**可分多项式**.

定义 3.4.3 设 F 为域,若 $F[x]$中每个多项式都是可分多

项式，则称 F 为**完备域**.

由前面的讨论我们知道若 F 的特征为 0，则 $F[x]$ 上每个多项式都是可分的，因而是完备域.因此下面我们只讨论特征为 $p>0$ 的域.我们先看看特征为 p 的域上的不可分的不可约多项式的结构.

定理 3.4.5 设 F 的特征为 p，$f(x)$ 为 $F[x]$ 中不可分不可约多项式，则 $f(x)$ 在其分裂域 K 上有分解

$$f(x)=c(x-\alpha_1)^{p^e}(x-\alpha_2)^{p^e}\cdots(x-\alpha_r)^{p^e},$$

其中当 $i\neq j$ 时，$\alpha_i\neq\alpha_j$，$e\in\mathbf{N}$.且

$$h(x)=c(x-\alpha_1^{p^e})(x-\alpha_2^{p^e})\cdots(x-\alpha_r^{p^e}),$$

是 $F[x]$ 中可分的不可约多项式.

证 设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$，则 $f'(x)=na_nx^{n-1}+\cdots+a_1$.由于 $f(x)$ 不可分不可约，由推论 3.4.3 有 $f'(x)=0$.故 $ka_k=0$，$k=1,2,\cdots,n$.于是当 $k\nmid p$ 时 $a_k=0$.即

$$f(x)=a_{mp}x^{pm}+a_{(m-1)p}x^{p(m-1)}+\cdots+a_px^p+a_0.$$

令 $g(x)=a_mx^m+a_{(m-1)p}x^{m-1}+\cdots+a_px+a_0$，则 $f(x)=g(x^p)$.注意 $g(x)$ 也是不可约的，若 $g(x)$ 不可分，则进一步可将 $g(x)$ 写成 $g(x)=g_1(x^p)$.因为 $\deg f(x)>\deg g(x)>\deg g_1(x)$，故重复有限次后将得到 $F[x]$ 上一个可分的不可约多项式 $h(x)$ 且

$$f(x)=h(x^{p^e}).$$

由于 $h[x]$ 可分，故在其分裂域中有分解

$$h(x)=c(x-\beta_1)(x-\beta_2)\cdots(x-\beta_r),$$

其中当 $i\neq j$ 时，$\beta_i\neq\beta_j$.于是

$$f(x)=c(x^{p^e}-\beta_1)(x^{p^e}-\beta_2)\cdots(x^{p^e}-\beta_r).$$

设 α_i 是 $x^{p^e}-\beta_i$ 的一个根，即 $\beta_i=\alpha_i^{p^e}$.于是

$$f(x)=c(x-\alpha_1)^{p^e}(x-\alpha_2)^{p^e}\cdots(x-\alpha_r)^{p^e}.\qquad\square$$

定理 3.4.6 设域 F 的特征为 $p>0$，则 F 为完备域的充分必要条件为对任何 $a\in F$，存在 $b\in F$ 使 $a=b^p$.

证 若 F 为完备域，反设存在 $a\in F$ 使得 $a\neq b^p$，$\forall\, b\in F$. 作多项式 $f(x)=x^p-a$. 先证明 $f(x)$ 不可约. 若 $f(x)$ 可约，设 $f(x)=g(x)h(x)$，其中 $g(x)$，$h(x)$ 为 $F[x]$ 中首一多项式，$\deg g(x)>0$，$\deg h(x)>0$. 设 K 为 $f(x)$ 的分裂域，α 为 $f(x)$ 在 K 中的一个根，即 $a=\alpha^p$. 于是在 $K[x]$ 上

$$f(x)=(x-\alpha)^p,\ g(x)=(x-\alpha)^r,\ h(x)=(x-\alpha)^{p-r},$$

其中 $0<r<p$，于是 $\alpha^r\in F$. 由于 p 为素数，存在整数 u，v 使得 $up+vr=1$，于是

$$\alpha=\alpha^{(up+vr)}=(\alpha^p)^u(\alpha^r)^v=a^u(\alpha^r)^v\in F.$$

这是矛盾. 故 $f(x)$ 不可约，又 $f'(x)=p(x-\alpha)^{p-1}=0$. 由推论 3.4.3 知 $f(x)$ 是不可分的. 这与 F 完备矛盾.

反之，若 $\forall\, a\in F$，$\exists\, b\in F$ 使 $a=b^p$. 假设 $f(x)$ 为 $F[x]$ 中不可分的不可约多项式. 由定理 3.4.5，存在 $F[x]$ 中可分的不可约多项式 $h(x)$ 使 $f(x)=h(x^{p^e})$，其中 $e\in\mathbf{N}$. 设

$$h(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0.$$

由条件存在 $b_i\in F$，使 $a_i=(b_i)^{p^e}$，$i=0,1,2,\cdots,n$. 于是

$$f(x)=h(x^{p^e})=\sum_{i=0}^{n}b_i^{p^e}x^{p^e}=\Big(\sum_{i=0}^{n}b_ix\Big)^{p^e}$$

这与 $f(x)$ 不可约矛盾. 因此 F 是完备域. □

推论 3.4.7 有限域是完备域.

证 设有限域 F 的特征为 p，作 F 到自身的映射 $\sigma:\sigma(a)=a^p$. 由于 F 的特征为 p，故 $(a-b)^p=a^p-b^p$，故 $a=b$ 当且仅当 $a^p=b^p$，由于 F 有限，故 σ 是一一对应，特别 σ 是满射. 因此 F 完备. □

推论 3.4.8 完备域的代数扩张也是完备域.

证 设 F 为完备域，K 为 F 的代数扩张. 若 F 的特征为 0，自

然 Ch $K=0$,故 K 是完备域.设 Ch $F=$ Ch $K=p$,作映射 $\sigma: K \to K, \sigma(a)=a^p$,同推论 3.4.7 的证明知 σ 是 1-1 的.由 F 完备,$\sigma(F)=F$.设 $\alpha \in K, E=F(\alpha)$.则 $\sigma(E) \simeq E$ 且 $[\sigma(E):\sigma(F)]=[E:F]=\deg(\alpha, F)$.又 $\sigma(E)=\sigma(F(\alpha))=F(\sigma(\alpha)) \subset F(\alpha)$.此外 $[\sigma(E):F]=\deg(\sigma(\alpha), F)=\deg(\sigma(\alpha), \sigma(F))=[\sigma(E):\sigma(F)]=[E:F]$.即 $\sigma(E)$ 作为 F 上线性空间 E 的子空间与 E 的维数相同,因此 $\sigma(E)=E$.故存在 β 使 $\alpha=\beta^p$.故 K 是完备域.

□

从以上内容我们看出,绝大多数的域都是完备域.当然,不完备的域是存在的,例如特征为 $p>0$ 的素域上的单超越扩张就不是完备域,参见本节补充题 4.

下面讨论域的可分扩张,我们的主要目的是证明任何有限可分扩张都是单代数扩张.

上面已介绍过可分多项式的概念.由此得到可分扩张的概念.

定义 3.4.4 设 K 是域 F 的扩张,$\alpha \in K$ 是 F 上代数元,若 $\mathrm{Irr}(\alpha, F)$ 可分,则称 α 为 F 上的**可分元素**.如果 $\mathrm{Irr}(\alpha, F)$ 不可分,则称 α 为 F 上的**不可分元素**.F 的一个代数扩张 E 称为 F 的**可分扩张**,若 E 中任何元素都是 F 上的可分元素.

由于完备域上的多项式都是可分的,因此完备域的任何代数扩张都是可分扩张.特别地,有限域或特征为 0 的域的任何代数扩张都是可分扩张.

另外一个可分扩张的例子就是前面学过的多项式的分裂域,当多项式是可分时,也是可分扩张.由于其证明较难,在此略去.但由这一结果可推出.

定理 3.4.9 设 $E=F(\alpha_1, \alpha_2, \cdots, \alpha_n)$ 是域 F 上的有限扩张,且 $\alpha_i, i=1,2,\cdots,n$,都是 F 上的可分元素,则 E 是 F 的可分扩张.

证 因为 α_i 可分,故 $\mathrm{Irr}(\alpha_i, F), i=1,2,\cdots,n$,都是可分不

可约多项式. 于是 $f(x)=\prod_{i=1}^{n}\mathrm{Irr}(\alpha_i,F)$ 是可分多项式. 设 K 为 $f(x)$ 在 F 上的分裂域，则 K 是 F 的可分扩张. 由分裂域的定义有 $\alpha_i\in K$，故 $E=F(\alpha_1,\cdots,\alpha_n)\subset K$. 特别 E 上的每个元素都是 F 上的可分元素，故 E 为可分扩张.

推论 3.4.10 设 K 为 F 的代数扩张，$\alpha,\beta\in K$. 若 α,β 都是 F 上的可分元素，则 $\alpha\pm\beta,\alpha\beta,\alpha\beta^{-1}(\beta\neq0)$ 都是 F 上的可分元素.

现在我们可以证明本节的主要结果.

定理 3.4.11 设 K 为域 F 上的有限可分扩张，则 K 是 F 的单代数扩张.

证 设 F 为无限域，则存在 $\alpha_1,\alpha_2,\cdots,\alpha_n\in K$ 使得

$$K=F(\alpha_1,\alpha_2,\cdots,\alpha_n).$$

由于 $F(\alpha_1,\cdots,\alpha_n)=F(\alpha_1)(\alpha_2)\cdots(\alpha_n)$. 故只需证明 $E=F(\alpha_1,\alpha_2)$ 为 F 的单扩张. 设 $f(x)=\mathrm{Irr}(\alpha_1,F),g(x)=\mathrm{Irr}(\alpha_2,F)$，考虑 $f(x)g(x)$ 在 F 上的分裂域 L. 在 $L[x]$ 上有分解

$$f(x)=\prod_{i=1}^{s}(x-\beta_i),\quad g(x)=\prod_{j=1}^{t}(x-\gamma_j),$$

其中 $\alpha_1=\beta_1,\alpha_2=\gamma_1$. 因为 α_2 为 F 上可分元素，故 $g(x)$ 无重根，故 $\gamma_1,\cdots,\gamma_r$ 两两互异. 考虑集合

$$\left\{\frac{\alpha_1-\beta_i}{\gamma_j-\alpha_2}\,\middle|\,1\leqslant i\leqslant s,2\leqslant j\leqslant r\right\},$$

它是有限集，但是 F 是无限集，故必存在 $0\neq c\in F$ 使得

$$c\neq\frac{\alpha_1-\beta_i}{\gamma_j-\alpha_2},1\leqslant i\leqslant s,2\leqslant j\leqslant r,$$

现在令 $\alpha=\alpha_1+c\alpha_2$. 我们将证明 $F(\alpha_1,\alpha_2)=F(\alpha)$. 显然 $F(\alpha)\subseteq F(\alpha_1,\alpha_2)$. 另一方面，考虑 $F(\alpha)$ 上的多项式

$$h(x)=f(\alpha-cx).$$

则 $h(\alpha_2)=f(\alpha-c\alpha_2)=f(\alpha_1)=0$. 故 α_2 是 $h(x)$ 的根. 又由 c 的取法有

$$\alpha - c\gamma_j \neq \beta_i, 1 \leqslant i \leqslant s, 2 \leqslant j \leqslant r.$$

故 $\gamma_j, 2 \leqslant j \leqslant r$ 都不是 $h(x)$ 的根. 这样多项式 $g(x), h(x)$ 在 L 上只有惟一的公共根 α_2. 因为在 L 上 $g(x), h(x)$ 都能分解为一次因式之积, 且无重根. 故在 $L[x]$ 中 $(h(x), g(x)) = x - \alpha_2$. 但是 $g(x), h(x) \in F(\alpha)[x]$, 而最大公因式在扩域中求不会改变, 因此在 $F(\alpha)$ 上也有 $(h(x), g(x)) = x - \alpha_2$. 于是 $\alpha_2 \in F(\alpha)$, $\alpha_1 = \alpha - c\alpha_2 \in F(\alpha)$. 即 $F(\alpha_1, \alpha_2) \subseteq F(\alpha)$. 故 $F(\alpha_1, \alpha_2) = F(\alpha)$.

关于有限域的情形, 我们将证明留给读者作为习题. □

习 题

1. 设域 F 的特征为 p, $a \in F$, 且 $a \neq b^p$, $\forall b \in F$. 设 n 为非负整数. 证明: $x^{p^n} - a$ 是 $F[x]$ 中不可约多项式.

2. 设域 F 的特征为 p, $f(x)$ 是 F 上不可约多项式, 并且 $f(x)$ 可以写成 x^{p^e}, 但不能写成 $x^{p^{e+1}}$ 的多项式 $(e \geqslant 1)$. 证明: $f(x)$ 的每一个根的重数都是 p^e.

3. 证明: $\mathbb{Q}(\sqrt{-1}, \sqrt{2})$ 和 $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ 都是有理数域 $\mathbb{Q}$ 的单扩张.

4. 设域 F 不存在可分扩张. 证明: F 的任何代数扩域也不存在可分扩张.

5. 试举例说明, 一个域 F 的有限扩张 E 不一定是 F 的单扩张.

6. 设 E 是 $x^5 - 2 \in \mathbb{Q}[x]$ 的分裂域. 求 $\theta \in E$ 使得 $E = \mathbb{Q}(\theta)$.

补充题

1. 设域 F 的特征为 $p \neq 0$, $F(\alpha, \beta)$ 是 F 的代数扩张, α 可分, $\deg(\alpha, F) = n$, β 不可分, $\deg(\beta, F) = p$. 求 $[F(\alpha, \beta) : F]$.

2. 设 $Z_3(\alpha) = F$, 且 $\mathrm{Irr}(\alpha, Z_3) = x^2 + 1$. 又设 $F^* = F - \{0\}$, $\langle \alpha \rangle$ 为 α 生成的子群. 证明 $\langle \alpha \rangle$ 是 F^* 的真子群, 并求 $\theta \in F^*$ 使得 $F^* = \langle \theta \rangle$.

3. 设 K 是域 F 的有限扩张. 若存在 $\alpha \in K$ 使得 $K = F(\alpha)$, 则称 α 是 K 对于 F 的**本原元素**.

(1) 求 $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ 对于 $\mathbb{Q}$ 的本原元素;

(2) 设 E 是 F 的有限扩张.证明 E 中存在对于 F 的本原元素的充分必要条件是 E 与 F 之间只有有限个中间域.

4. 设 Π 为特征为 $p>0$ 的素域,F 为 Π 的单超越扩张,证明:F 不是完备域.

5. 证明定理 3.4.11 中的有限域的情形.

附录　伽罗瓦理论简介

求解多项式方程的问题，在19世纪上半世纪及其以前，曾长期是代数学研究的中心问题.求解一元二次方程 $ax^2 + bx + c = 0$ 的问题，在两三千年前的巴比伦时代就已经解决；现代把它的求根公式写作

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

这表明一元二次方程的根可以用方程系数的有限次加、减、乘、除和开方运算表出，我们称之为方程的“根式解”.求解一元三次方程和一元四次方程的问题，经过了漫长的时期，在公元16世纪被塔塔里亚(Tartaglia)、卡当(G. Cardan)、费拉里(L. Ferrari)等数学家解决，找到了求根公式，并且求根公式中也只含有方程系数的加、减、乘、除和开方运算(例如三次方程的求根公式中含有3次根式).此后的将近三百年间，许多数学家为寻找一元五次方程的求根公式付出了大量的劳动，但都没有成功.后来，拉格朗日(Lagrange)、高斯(Gauss)、鲁菲尼(P. Ruffini)、阿贝尔(N. H. Abel)等数学家从另外的角度对解高次方程的问题进行研究，得到了一些结果，并且证明了，文字系数的五次方程不存在根式解.在这些数学家工作的基础上，年轻的法国数学家伽罗瓦(Galois)创立了一整套理论，给出了“方程可用根式解”的充分必要条件，彻底地解决了这一问题.伽罗瓦不仅再次证明了文字系数的五次和五次以上的方程不存在根式解，而且给出了一种方法，可以判断任一数字系数的方程是否存在根式解.在伽罗瓦的方法中，不仅引入了群和域的概念(虽然没有术语)，而且引入了正规子群和正规扩域等许多

概念，还讨论了它们之间的联系，用来解决“方程是否可用根式解”的问题．这一整套理论后人称之为“伽罗瓦理论”．这一理论是如此超前，以致伽罗瓦投到巴黎科学院的论文，或被认为“难以理解”而退稿，或被不经意地遗失掉．伽罗瓦只活了 22 岁，他关于“方程可解性条件”的文章，是在他死后十多年才发表，死后三十多年才被人们理解的．伽罗瓦的思想如今已经发展为庞大的代数学科，伽罗瓦本人也成为近世代数（或称抽象代数）的奠基人．限于篇幅和本书的任务，我们只在下边介绍伽罗瓦理论的思路、主要结果和主要应用，不给出证明，希望读者能由此了解伽罗瓦理论的梗概．

一、伽罗瓦探寻“方程可用根式解”的思路

伽罗瓦不再像前人那样，千方百计去寻找根如何被方程的系数表出的方法（即求根公式），而是与拉格朗日一样，从根集的置换的角度出发，去思考问题．为了便于理解和简化叙述，我们采用群、域等现代的术语去说明伽罗瓦当年的思想，并且只在数域中讨论．

每一个多项式方程 $f(x)=0$，都可以看作某个系数域 F 上的多项式方程，F 是复数域$\mathbb{C}$的子域．n 次方程 $f(x)=0$ 在复数域$\mathbb{C}$中有 n 个根 $\{\alpha_1,\cdots,\alpha_n\}$，不妨设这里没有重根．这个根集到自身的置换最多有 $n!$ 个，它们构成一个群，同构于 S_n．但是这些根往往不是独立的，或者说根之间是有代数关系的．这 $n!$ 个置换中保持根之间在 F 中的全部关系（粗略地说，这里的“关系”，是指系数在 F 中的上述 n 个根的多项式等式关系）都不变的置换个数一般少于 $n!$ 个，它们又构成上述群的一个子群，同构于 S_n 的一个子群，称为**“方程 $f(x)=0$ 在 F 上的群”**，即为 $G(f,F)$．

$f(x)=0$ 既可以看作数域 F 上的多项式方程，又可以看作是 F 的某个扩域 F_1 上的多项式方程，F_1 仍是$\mathbb{C}$的子域．当 F 扩大成 F_1 时，根之间在方程系数域中的全部关系也就增加了，保持这全部关系都不变的置换就减少了，从而 $f(x)=0$ 在系数域上的群

就缩小了.当这种群缩成幺群时,即只有恒等置换才能保持根之间在 F 中的全部关系都不变,就表明方程的所有根都属于系数域了.

方程的系数域扩大的过程可以多次重复进行.如果每次扩大时添加的都是原系数域的根式,则扩域中的元素都能用原域中的元素的加、减、乘、除和根式表出.如果这种扩大系数域的方式能使方程 $f(x)$ 在扩域上的群成为幺群,那么方程 $f(x)=0$ 的根就一定可以用原来系数域中元素的加、减、乘、除和根式表出,方程 $f(x)=0$ 也就有了"根式解".这就是伽罗瓦探寻"方程可用根式解"的思路.

这里讲述的思想和所用的语言都比较抽象,让我们用一个具体例子来细加说明.

设方程为

$$x^4+bx^2+c=0$$

这里 b,c 是独立的(或称在 $\mathbb{Q}$ 上是代数无关的,即 b,c 不能作为 $\mathbb{Q}$ 上任意 2 元多项式的根).该方程的系数域可以看作是 $\mathbb{Q}(b,c)$,即有理数域添加 b,c 而成的域,记为 F.

我们知道,这个 4 次方程的 4 个根分别为

$$\alpha_1=\sqrt{\frac{-b+\sqrt{b^2-4c}}{2}},\quad \alpha_2=-\sqrt{\frac{-b+\sqrt{b^2-4c}}{2}},$$

$$\alpha_3=\sqrt{\frac{-b-\sqrt{b^2-4c}}{2}},\quad \alpha_4=-\sqrt{\frac{-b-\sqrt{b^2-4c}}{2}},$$

于是,

$$\alpha_1+\alpha_2=0,\quad \alpha_3+\alpha_4=0,$$

这是根在 F 中的两个关系.根集 $\{\alpha_1,\alpha_2,\alpha_3,\alpha_4\}$ 最多有 $4!=24$ 个可能的置换,而保持上述两个关系不变的置换只有下边 8 个:

$$\sigma_1=\begin{pmatrix}\alpha_1&\alpha_2&\alpha_3&\alpha_4\\ \alpha_1&\alpha_2&\alpha_3&\alpha_4\end{pmatrix},\quad \sigma_2=\begin{pmatrix}\alpha_1&\alpha_2&\alpha_3&\alpha_4\\ \alpha_2&\alpha_1&\alpha_3&\alpha_4\end{pmatrix},$$

$$\sigma_3=\begin{pmatrix}\alpha_1 & \alpha_2 & \alpha_3 & \alpha_4\\ \alpha_1 & \alpha_2 & \alpha_4 & \alpha_3\end{pmatrix},\quad \sigma_4=\begin{pmatrix}\alpha_1 & \alpha_2 & \alpha_3 & \alpha_4\\ \alpha_2 & \alpha_1 & \alpha_4 & \alpha_3\end{pmatrix},$$

$$\sigma_5=\begin{pmatrix}\alpha_1 & \alpha_2 & \alpha_3 & \alpha_4\\ \alpha_3 & \alpha_4 & \alpha_1 & \alpha_2\end{pmatrix},\quad \sigma_6=\begin{pmatrix}\alpha_1 & \alpha_2 & \alpha_3 & \alpha_4\\ \alpha_4 & \alpha_3 & \alpha_1 & \alpha_2\end{pmatrix},$$

$$\sigma_7=\begin{pmatrix}\alpha_1 & \alpha_2 & \alpha_3 & \alpha_4\\ \alpha_3 & \alpha_4 & \alpha_2 & \alpha_1\end{pmatrix},\quad \sigma_8=\begin{pmatrix}\alpha_1 & \alpha_2 & \alpha_3 & \alpha_4\\ \alpha_4 & \alpha_3 & \alpha_2 & \alpha_1\end{pmatrix}.$$

可以证明，这 8 个置换，也是 24 个置换中使根 $\alpha_1,\alpha_2,\alpha_3,\alpha_4$ 之间在 F 中全部关系都不变的仅有的置换. 这 8 个置换构成的集合是有结构的. 它们关于置换的乘法成群，称为该方程在 F 上的群，它同构于 S_4 的一个子群.

我们可以说，使根之间在 F 中全部关系都不变的置换的数目，是我们对根的无知程度的一个尺度，因为在这 8 个置换下我们不能把这些根区分开来.

我们再注意到 $\alpha_1^2-\alpha_3^2-\sqrt{b^2-4c}=0$. 它并不是根之间在 F 中的一个关系，因为 $\sqrt{b^2-4c}$ 不是 F 中的元素. 但如果把根式 $\sqrt{b^2-4c}$ 添加到 F 中去，形成扩域 $F_1=F(\sqrt{b^2-4c})$，则

$$\alpha_1^2-\alpha_3^2-\sqrt{b^2-4c}=0$$

就是根之间在 F_1 中的一个关系了. 由于 $\alpha_1+\alpha_2=0$ 和 $\alpha_3+\alpha_4=0$ 导致 $\alpha_1^2=\alpha_2^2$ 和 $\alpha_3^2=\alpha_4^2$，所以，上面 8 个置换中的前 4 个使根之间在 F_1 中的上述关系 $\alpha_1^2-\alpha_3^2-\sqrt{b^2-4c}=0$ 保持不变，但后 4 个置换则不能使之保持不变. 可以证明，这前 4 个置换能使根之间在 F_1 中的全部关系保持不变，从而构成方程在 F_1 上的群. 它是上述 8 个置换构成的群的子群.

我们再注意到 $\alpha_3-\alpha_4-2\sqrt{\dfrac{-b-\sqrt{b^2-4c}}{2}}=0$. 它并不是根之间在 F_1 中的一个关系，因为虽然 $\dfrac{-b-\sqrt{b^2-4c}}{2}\in F_1$，但它开

平方后一般不再是 F_1 中的元素. 可是,如果把 F_1 中元素的根式 $\sqrt{\frac{-b-\sqrt{b^2-4c}}{2}}$ 添加到 F_1 中去,形成扩域 $F_2=F_1\left(\sqrt{\frac{-b-\sqrt{b^2-4c}}{2}}\right)$,则

$$\alpha_3-\alpha_4-2\sqrt{\frac{-b-\sqrt{b^2-4c}}{2}}=0$$

就是根之间在 F_2 中的一个关系. 这个关系只在前两个置换 σ_1 和 σ_2 下保持不变,而在后 6 个置换下都不能保持不变. 可以证明,σ_1 和 σ_2 能使根之间在 F_2 中的全部关系保持不变,从而构成方程在 F_2 上的群,它是上述 4 个置换构成的群的子群.

我们再注意到 $\alpha_1-\alpha_2-2\sqrt{\frac{-b+\sqrt{b^2-4c}}{2}}=0$. 它并不是根之间在 F_2 中的一个关系,因为 $\sqrt{\frac{-b+\sqrt{b^2-4c}}{2}}$ 不是 F_2 中的元素. 但如果把 F_2 中元 $\frac{-b+\sqrt{b^2-4c}}{2}$ 的根式 $\sqrt{\frac{-b+\sqrt{b^2-4c}}{2}}$ 添加到 F_2 中去,形成扩域 $F_3=F_2\left(\sqrt{\frac{-b+\sqrt{b^2-4c}}{2}}\right)$,则

$$\alpha_1-\alpha_2-2\sqrt{\frac{-b+\sqrt{b^2-4c}}{2}}=0$$

就是根之间在 F_3 中的一个关系. 这个关系则只在置换 σ_1 和 σ_3 下保持不变. 但 σ_3 不能使根之间在 F_2 中的全部关系保持不变,从而也就不能使根之间在 $F_3(\supset F_2)$ 中的全部关系保持不变. 由于 σ_1 是恒等置换,做此置换的效果与不做是一样的,所以它当然使根之间在 F_3 中的全部关系保持不变. 于是方程在 F_3 上的群仅由恒等置换 σ_1 构成,它是幺群,是上述 $\{\sigma_1,\sigma_2\}$ 的子群. 此时,根

$\alpha_1,\alpha_2,\alpha_3,\alpha_4$ 已都在方程的扩大的系数域 F_3 中了，而由于扩大的过程中只添加了根式，所以 F_3 中的所有元素（包括 $\alpha_1,\alpha_2,\alpha_3,\alpha_4$），都可以用方程原来所在的域 F 中元素的加、减、乘、除和根式来表达．因此，该方程可用根式解．

从这个例子的讨论中我们看到，方程在系数域上的群，是方程在系数域中（根式解）可解性的关键，因为这个群的大小表示出方程的根在系数域上不可区分的程度．当这个方程在系数域上的群是最小的幺群时，表明根在系数域上可以完全区分开，或者说，根就在系数域中．

这个例子是为了帮助读者理解伽罗瓦的思路，而实际工作是在不知道方程的根的表达式的情形下进行的．伽罗瓦说明了，在不知道根的情况下，如何能找到方程在系数域上的群，以及通过预解式找到向系数域中添加的根式从而得到扩大的系数域．这样逐次进行，直到系数域扩大到方程在扩域上的群是幺群时，根就在扩大的系数域里了．这些步骤中包含了大量的理论，伽罗瓦是想由此说明他的理论，而不是想把这些步骤作为解方程的一个实际方法．

下边，我们用现代的语言来简要叙述伽罗瓦的理论及其在“方程根式解”和“规尺作图”两个方面的主要结果．

二、伽罗瓦基本定理

伽罗瓦理论的核心是伽罗瓦基本定理．为了介绍伽罗瓦基本定理，首先要介绍伽罗瓦群、不变子域和伽罗瓦扩张．它们的讨论不再限于数域的范围，也不再限于特征为 0 的域的范围．

1．伽罗瓦群、不变子域

设 K 是域 F 的有限扩张，则 K 的所有 F－自同构的集合关于映射的乘法构成一个群，称为 K 在 F 上的**伽罗瓦群**，记为 $\mathrm{Gal}(K/F)$．

设 G 为域 K 的自同构群 $\mathrm{Aut}\ K$ 的一个子群，则集合

$$\{a\in K \mid g(a)=a,\forall\, g\in G\}$$

是 K 的一个子域，称为 K 的 G - **不变子域**，记为 Inv G.

2. 伽罗瓦扩张

若域 F 的有限扩张 K 满足

$$\mathrm{Inv}(\mathrm{Gal}(K/F))=F,$$

则称 K 是 F 的**伽罗瓦扩张**.

按照伽罗瓦群和不变子域的定义，一般有

$$\mathrm{Inv}(\mathrm{Gal}(K/F))\supseteq F,$$

而等号成立的情况是特别值得注意的情况，这就是“K 是域 F 的伽罗瓦扩张”的情况.“K 是域 F 的伽罗瓦扩张”，将是伽罗瓦基本定理成立的条件.为了从不同角度去理解伽罗瓦扩张的特点，我们给出

定理 设 K 是域 F 的扩域，则下边三个条件是等价的：

① K 是 F 的伽罗瓦扩张；

② K 是 F 的有限可分正规扩张；

③ K 是可分多项式 $f(x)\in F[x]$ 的分裂域.

且此时有 $|\mathrm{Gal}(K/F)|=[K:F]$.（“正规扩张”请参见 §3.3 的补充题第 4 题）

最后这个等式的左边表达的是“群中元素的个数”，右边表达的是“域的扩张次数”，在伽罗瓦扩张这一条件下，群和域的性质居然可以统一在这样一个等式中.把这一点表达得更加淋漓尽致的是伽罗瓦基本定理.

3. 伽罗瓦基本定理

定理（伽罗瓦基本定理） 设 K 是域 F 的伽罗瓦扩张，记 $\mathrm{Gal}(K/F)$ 为 G，记 Γ 是 G 的所有子群的集合，记 Σ 是域 K 与 F 间的所有中间域的集合，则有

(1) 定义 Σ 到 Γ 的映射

$$\mathrm{Gal}: E\mapsto \mathrm{Gal}(K/E),\ \forall E\in\Sigma,$$

称之为伽罗瓦映射，则伽罗瓦映射是可逆映射，其逆映射为 Γ 到 Σ 的映射

$$\mathrm{Inv}: H \mapsto \mathrm{Inv}H, \forall H \in \Gamma.$$

(2) $\forall H_1, H_2 \in \Gamma$，有

$$H_2 \subset H_1 \Longleftrightarrow \mathrm{Inv}H_1 \subset \mathrm{Inv}H_2.$$

(3) $\forall H_1, H_2 \in \Gamma, H_2 \subset H_1$，则有

$$[H_1 : H_2] = [\mathrm{Inv}H_2 : \mathrm{Inv}H_1].$$

(4) $\forall H_1, H_2 \in \Gamma, H_2 \subset H_1$，则有

$$H_2 \lhd H_1 \Longleftrightarrow \mathrm{Inv}H_2 \text{ 是 } \mathrm{Inv}H_1 \text{ 的正规扩张},$$

且此时 $\mathrm{Gal}(\mathrm{Inv}H_2/\mathrm{Inv}H_1) \simeq H_1/H_2$.

为了帮助读者理解伽罗瓦基本定理，我们做如下解释：

“(1)”中叙述的伽罗瓦映射及其逆映射，是本定理的核心内容.群与域本来是不同的代数系统，现在在“K 是 F 的伽罗瓦扩张”的条件下，子群集合 Γ 与中间域集合 $\sum$ 之间建立了一一对应，这个一一对应也常称为“伽罗瓦对应”或“伽罗瓦组对”.下面的图表也许有助于理解这个一一对应.

$$\begin{array}{lccccc}
 & & \mathrm{Inv}H_2 & & \mathrm{Inv}H_1 & \\
 & & \| & & \| & \\
\sum: & K & E_2 & & E_1 & F \\
\mathrm{Gal}\downarrow & \uparrow \mathrm{Inv} & & & & \\
\Gamma: & \{e\} & H_2 & & H_1 & G \\
 & & \| & & \| & \\
 & & \mathrm{Gal}(K/E_2) & & \mathrm{Gal}(K/E_1) &
\end{array}$$

“(2)”给出了 $\sum$ 中顺序关系与 Γ 中顺序关系之间的联系：即上述一一对应在包含关系上是相反的.用图表来表示，为

$$\begin{array}{lccccccccc}
\sum: & K & \supset & \cdots & \supset & \mathrm{Inv}H_2 & \supset & \mathrm{Inv}H_1 & \cdots \supset & F \\
\downarrow & \uparrow & & & & & & & & \\
\Gamma: & \{e\} & \subset & \cdots & \subset & H_2 & \subset & H_1 & \cdots \subset & G
\end{array}$$

应注意的是，$\sum$ 和 Γ 对于包含关系一般不是全序集，而是偏序集，上图是对能排出顺序的一部分子集和中间域而言的.

“(3)”进一步给出了上述两个反向序列间的定量关系：子群 H_2 在 H_1 中的指数等于扩域 $\mathrm{Inv}H_2$ 对 $\mathrm{Inv}H_1$ 的扩张次数.

本来，“子群在大群中的指数”与“扩域对基域的扩张次数”，是完全不同的两个概念(请回忆这两个定义)，现在，在“伽罗瓦扩张”的条件下，却产生了相等的关系.上一定理最后的那个等式，是这里的特例，可以写作

$$[G:\{e\}]=[\mathrm{Inv}\{e\}:\mathrm{Inv}G],$$

这是因为 $G=\mathrm{Gal}(K/F)$，$\mathrm{Inv}\{e\}=K$，$\mathrm{Inv}G=F$.

“(4)”进一步给出上述两个反向序列的正规关系：正规子群对应着正规扩张.本来，从定义上看，“正规子群”与“正规扩张”，是毫无联系的两个概念(请回忆这两个定义).现在，在“伽罗瓦扩张”的条件下，这两者却产生了如此紧密的联系.

由于在群和域这两种代数体系间找到了诸多的联系，群中的问题就可以转化为域中的问题去考察，域中的问题也可以转化为群中的问题去考察，这将显示出伽罗瓦基本定理的强大威力.下边介绍伽罗瓦基本定理在“方程根式解”和“规尺作图”两个方面的重要应用，便可见一斑.

三、“方程可用根式解”的充要条件

用伽罗瓦基本定理，可以给出“多项式方程可用根式解”的充要条件.为此，先给出“多项式方程的伽罗瓦群”的概念.

1. 方程的伽罗瓦群

设 $f(x)$ 是域 F 上的多项式，即 $f(x)\in F[x]$.为简单，我们设 F 是特征为 0 的域，$f(x)$ 是无重根的多项式，记 K 是 $f(x)$ 的分裂域，则 $\mathrm{Gal}(K/F)$ 称为**方程 $f(x)=0$ 对基域 F 的伽罗瓦群**，记为 $G(f(x),F)$.

由于 K 是可分多项式 $f(x)\in F[x]$ 的分裂域，所以 K 是 F 的伽罗瓦扩张，从而可以用伽罗瓦基本定理.

事实上，方程的伽罗瓦群 $G(f(x),F)$ 与 $f(x)=0$ 的根集上

的一个置换群(S_n 的子群)是同构的,后者就是我们在"一、伽罗瓦探寻'方程可用根式解'的思路"中反复提到的,伽罗瓦当年定义的"方程 $f(x)=0$ 在系数域 F 上的群".现在我们具体计算时,常常仍把方程的伽罗瓦群写成置换群,这样比较简单、方便.

2. 方程可用根式解

设 K 是域 F 的扩张,如果有中间域序列

$$F=F_0\subset F_1\subset\cdots\subset F_i\subset F_{i+1}\subset\cdots\subset F_m=K$$

使得每一 F_{i+1} 是 $x^{n_{i+1}}-a_{i+1}\in F_i[x]$ 的分裂域,则称 K 是 F 的根式扩张.设多项式 $f(x)\in F[x]$,若有 F 的根式扩张 K 包含 $f(x)$ 的分裂域,则称**方程 $f(x)=0$ 对 F 可用根式解**.

由于 F_{i+1} 是 $x^{n_{i+1}}-a_{i+1}$ 的分裂域,所以,F_{i+1} 可以通过在 F_i 中添加 F_i 中元素 a_{i+1} 的 n_{i+1} 次根式 $\sqrt[n_{i+1}]{a_{i+1}}$ 及 n_{i+1} 次本原单位根得到.如果不计较单位根的添加,那么每一层只要在前一个中间域上添加一个根式,所以,每一层扩张也称"**单根式扩张**".相应地,上述根式扩张的中间域序列也称"**单根式扩张列**",或形象地称为"**根塔**".

由于上述根塔是有限层的,所以 K 中任一元素可以从 F 中的元素出发,经过有限步的加、减、乘、除及开各种次方而得到.现在 K 是 $f(x)$ 的分裂域,$f(x)=0$ 的根都在 K 中,因此 $f(x)=0$ 的根都可以从 F 中的元素出发,经有限步的加、减、乘、除及开各种次方得到.这就是"方程可用根式解"的朴素的含义,只不过现在用严格的数学语言叙述出来罢了.

3. "方程可用根式解"的充要条件

定理 设 F 是特征为 0 的域,$f(x)\in F[x]$ 是无重根的多项式,则方程 $f(x)=0$ 对 F 可用根式解的充要条件是,$f(x)=0$ 对基域 F 的伽罗瓦群 $G(f(x),F)$ 为可解群.

这个定理的证明,主要是运用伽罗瓦基本定理.这个定理的结论,给"方程是否可用根式解"的问题以一个彻底的回答,即看方程

的伽罗瓦群是否为可解群.这个定理也称为"**方程可用根式解的伽罗瓦准则**".关于"可解群"的概念,请参见§1.7"单群与可解群"."可解群"名称的来由,就与本定理叙述的内容有关.

4. 文字系数的5次和5次以上的方程不能用根式解

定理 次数≥5的文字系数的多项式方程不能用根式解.

所谓文字系数,就是方程所有系数是独立的(或称代数无关的),从而 n 次方程的 n 个根也是独立的,于是根之间在方程系数域中没有任何代数关系,前面谈到的"保持根之间在方程系数域中的全部关系"的条件现在相当于没有条件,因此,n 个根的所有 $n!$ 个置换就构成了方程在系数域上的群,它同构于 S_n.或者用现在的语言叙述为,文字系数的 n 次方程对基域的伽罗瓦群同构于 S_n.下边只需说明 $n\geqslant 5$ 时 S_n 不是可解群,再由"方程可用根式解的伽罗瓦准则",便知道定理是正确的.

据命题1.7.8,$n\geqslant 5$ 时 A_n 不是可解群;而 A_n 是 S_n 的子群,如果 S_n 是可解群,再据命题1.7.5,可解群的子群都是可解群,就推出 A_n 是可解群,这是矛盾.这样就说明了 $n\geqslant 5$ 时 S_n 不是可解群.

这个定理也表明,5次和5次以上的方程,没有通常意义下的"求根公式".

用"方程可用根式解的伽罗瓦准则",还可以说明,确有数字系数的5次及5次以上的方程不可用根式解.例如,有理数域上的5次方程

$$x^5+20x+16=0$$

就不可用根式解,因为它的伽罗瓦群是 S_5,不是可解群(读者若想了解求一个方程的伽罗瓦群的方法,可参看有关书籍).

四、"可用规尺作图"的充要条件

1. 概述

自古以来,就有一些用圆规直尺作图的问题长期悬而未决,消

耗了许多数学家的精力.比较著名的有三大规尺作图难题:三等分任意角的问题,立方倍积问题(对任意已知正立方体,作一正立方体,使其体积是前者体积的2倍),化圆为方问题(对任意已知圆,作一正方形,使其面积等于已知圆的面积).在伽罗瓦理论建立以后,人们用伽罗瓦理论证明了这些问题是不可能用圆规直尺作出的,才彻底解决了这些问题.那么,这样一些几何的问题,是如何用代数的方法去解决的呢?

2.“规尺作图”的严格化

规尺作图不能简单地说成“用圆规、直尺去作图”,应给出严格的定义作为讨论的基础.作图,是从已知图形去求作指定图形.而已知图形的条件都可以转化为点的条件(例如一个已知圆可转化为圆心及圆上一点这两个已知点),求作指定图形也可以转化为求作某些特殊点.

在平面上给定点集 $S=\{P_1,\cdots,P_n\}(n\geqslant 2)$,我们规定,除了在某些范围下选点以外,用圆规直尺可做且只可以做以下两件事:① 过 S 中任两点作直线;② 以 S 中任一点为圆心,以 S 中任两点的距离为半径作圆.

如果平面上一点 P 是①中两直线的交点,或是①中一直线与②中一圆的交点,或是②中两圆的交点,则称“**点 P 可用规尺直接从 S 作出**”.

如果有一串点 $P_1,\cdots,P_r=P$,使得 P_1 可用规尺直接从 S 作出,而且 P_{i+1} 可用规尺直接从 $S\cup\{P_1,\cdots,P_i\}$ 作出($i=1,\cdots,r-1$),则称“**点 P 可用规尺从 S 作出**”.

这里的前提“$n\geqslant 2$”,意味着至少应有两个已知点,这是因为否则①、②两件事均不能做.

3.几何问题代数化

在平面上建立坐标系以后,点转化为坐标——两个实数组成的有序数组(a,b),还可进一步转化为复数 $a+b\sqrt{-1}$.

$n=2$ 的情形即已知两个点的情形，可把已知点作为(0,0)和(0,1)来建立坐标系，这样，用规尺作图①、②就可作出平面上的全部有理点，即坐标为有理数的点. 这个意思还可以进一步用代数语言叙述为：已知两个点就是已知复平面上的两个复数0,1，由此用规尺作图①、②就可以作出复数域$\mathbb{C}$的子域$\mathbb{Q}(\sqrt{-1})$. 在这个基域$\mathbb{Q}(\sqrt{-1})$的基础上用规尺在复平面上作指定点 P 就相当于作指定复数 z，这也称为在欧几里得意义下作图. 古代三大作图难题，都可以归为这类问题.

$n>2$ 的情形，就是已知$\mathbb{Q}(\sqrt{-1})$的一个扩域 F. 把 F 作为基域用规尺在复平面上作指定点 P，就相当于作指定复数 z，这也称为在非欧几里得意义下作图.

4. “可用规尺作图”的充要条件

用伽罗瓦理论可以证明下边的定理，它也称为“**可用规尺作图的伽罗瓦准则**”.

定理 任给复数 $z_i=a_i+b_i\sqrt{-1}$，$i=1,\cdots,n$，并记 $\bar{z}_i$ 是 z_i 的共轭复数，记

$$F=\mathbb{Q}(\sqrt{-1},z_1,\cdots,z_n,\bar{z}_1,\cdots,\bar{z}_n),$$

则复数 z 可用规尺从数集 $S=\{0,1,z_1,\cdots,z_n\}$ 作出的充要条件是，存在**二次根式扩张列**

$$F=F_1\subset F_2\subset\cdots\subset F_t=K,$$

使 $z\in K$.

这里的“二次根式扩张列”，是指每一 F_{i+1}，是 $x^2-c_{i+1}\in F_i[x]$ 的分裂域，即每一层都是在前一层上添加一个二次根式得到的扩域，不妨设$\sqrt{c_{i+1}}\notin F_i$，从而每一层的扩张次数也都是2：$[F_{i+1}:F_i]=2$.

二次根式也即平方根，故上述二次根式扩张列也称为平方根塔. 定理也可以简述为：P 点可用规尺作图的充要条件是，与 P 点

相应的复数在基域的一个平方根塔中.

我们从规尺作图的定义来说明这一定理的内容.作平面上的 P 点,如果它是两已知直线的交点,从代数角度看,就是要解两个一次方程联立的方程组,解就在基域中;如果 P 点是一已知直线与一已知圆的交点,就是要解一个一次方程与二次方程联立的方程组,需要开平方,所以解在一个二次根式扩张中;如果 P 点是两个已知圆的交点,就是要解两个二次方程联立的方程组,需要开平方,所以解在一个二次根式扩张中.总之,P 点"用规尺直接作出",最多只需要一个二次根式扩张;P 点"用规尺逐步作出",最多只需要一个二次根式扩张列,或者说,平方根塔.

从这个定理出发,可以得到有关规尺作图的一些推论.为了解决古代三大规尺作图难题,要用到下边的推论.

推论 若在欧几里得意义下 z 可用规尺作图,则 z 是有理数域$\mathbb{Q}$ 上的代数元,且 z 在$\mathbb{Q}$ 上的不可约多项式 $\mathrm{Irr}(z,\mathbb{Q})$ 是 2^l(l 是非负整数)次多项式.

这个推论成立的原因是,在欧几里得意义下作图,基域 $F=\mathbb{Q}(\sqrt{-1})$,而 $\sqrt{-1}$也是$\mathbb{Q}$ 中元素 -1 的平方根,所以如果在二次根式扩张列中不在乎增加一层添加 $\sqrt{-1}$的二次根式扩张,就可以把基域看作是$\mathbb{Q}$.

又因为定理中的

$$F=F_1\subset F_2\subset\cdots\subset F_t=K$$

是二次根式扩张列,每一层都是 2 次扩张:$[F_{i+1}:F_i]=2$,所以,

$$[K:F]=[F_t:F_1]=[F_t:F_{t-1}]\cdots[F_2:F_1]=2^{t-1}.$$

现在,$F=\mathbb{Q}$,$z\in K$,于是$\mathbb{Q}\subset\mathbb{Q}(z)\subseteq K$,所以

$$[\mathbb{Q}(z):\mathbb{Q}]\mid[K:\mathbb{Q}]=2^m,$$

因此$[\mathbb{Q}(z):\mathbb{Q}]$可以写成 2 的方幂 2^l.注意到有限扩张一定是代数扩张,所以 z 是$\mathbb{Q}$ 上的代数元,且 $\mathrm{Irr}(z,\mathbb{Q})$的次数就是$[\mathbb{Q}(z):\mathbb{Q}]=2^l$.

5. 古代三大规尺作图难题的解决

用上述推论可以给出古代三大规尺作图难题以否定的回答：三者均不可用规尺作出.

(1) 三等分任意角问题

由于"角 θ 可作等价于 $\cos\theta$ 可作"(在单位圆上作出线段 $\cos\theta$ 便知),因此,已知 3θ 求作 θ,就是已知 $\cos 3\theta$ 求作 $\cos\theta$. 由 3 倍角公式

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta,$$

再记已知条件 $\cos 3\theta$ 为 a,则求作的 $\cos\theta$ 是方程

$$4x^3 - 3x - a = 0$$

的根. 这个方程的系数域可以看作是 $\mathbb{Q}(a)$. 这个方程的根中一般要出现系数的三次根式,因此一般不存在系数域的二次根式扩张列,使 $\cos\theta$ 含在这个二次根式扩张列中,所以,不可用规尺作图三等分任意角. 例如,不可用规尺作图三等分 60°角,因为此时 $3\theta = 60°$, $a = \cos 3\theta = 0.5$, $\mathbb{Q}(a) = \mathbb{Q}$, $\mathrm{Irr}(\cos\theta, \mathbb{Q}) = 4x^3 - 3x - 0.5$,而 $\cos\theta$ 含在 $\mathbb{Q}$ 的一个三次根式扩张中. 当然,这并不排除用规尺作图三等分某些特殊角,例如三等分 90°角,三等分 45°角.

(2) 立方倍积问题

为简单,我们不妨设已知的正立方体边长为 1,现求作一个正立方体,使其体积是已知立方体体积的 2 倍. 就是要求作一个边长为 $\sqrt[3]{2}$ 的正立方体. 这里要求作的 z 就是 $\sqrt[3]{2}$,而

$$\mathrm{Irr}(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2,$$

这是一个次数不为 2^l 的多项式,故据上述推论,$\sqrt[3]{2}$ 不能用规尺作出. 所以,用规尺作图解决立方倍积问题是不可能的.

(3) 化圆为方问题

为简单,我们不妨设已知圆的半径为 1,现求作一个正方形,使其面积等于已知圆的面积 π,就是要求作一个边长为 $\sqrt{\pi}$ 的正方形. 这里要求作的 z 就是 $\sqrt{\pi}$,而 $\sqrt{\pi}$ 是 $\mathbb{Q}$ 上的超越元,不是 $\mathbb{Q}$ 上的代

数元.故据上述推论,$\sqrt{\pi}$不能用规尺作出.所以,用规尺作图解决化圆为方问题是不可能的.

由此我们看到,长期困扰数学家的古代三大规尺作图难题,在伽罗瓦理论的强大威力下,都以否定的方式迎刃而解了.

名词索引

F

G

H

J

K

L

JIAN MING
CHOU XIANG DAI SHU

ISBN 7-04-011916-1
9 787040 119169 >
定价 7.60 元