面向21世纪课程教材
Textbook Series for 21st Century

近世代数基础

刘绍学

高等教育出版社
HIGHER EDUCATION PRESS

面向21世纪课程教材
Textbook Series for 21st Century

近世代数基础

刘绍学

高等教育出版社
HIGHER EDUCATION PRESS

(京)112 号

内容提要

本书是教育部“高等教育面向 21 世纪教学内容和课程体系改革计划”的研究成果，是面向 21 世纪课程教材和普通高等教育“九五”国家级重点教材。本书作者在介绍近世代数课程的传统内容时，在以下各方面进行了有益的探索：强调代数系统的出现是刻画物理量和几何量的需要；较深入地介绍一些具体的群、环、域以及介绍代数的应用；注意讲授近世代数中的数学思想等。全书共四章及一个附录。第一章由刻画“对称”而引入群的概念；第二章介绍群论基础；第三章介绍环、域和模；第四章介绍有限域和 Galois 理论；附录介绍了计算代数几何的基石——Gröbner 基和 Buchberger 算法。

本书可作为高等学校数学专业的教科书，也可供相关专业师生和有关科研人员参考。

图书在版编目(CIP)数据

近世代数基础/刘绍学. －北京：高等教育出版社，
1999

面向 21 世纪教材　普通高等教育“九五”国家级重点教材

ISBN 7－04－007450－8

Ⅰ.近…　Ⅱ.刘…　Ⅲ.抽象代数－高等教育－教材　Ⅳ.O153

中国版本图书馆 CIP 数据核字(1999)第 64453 号

近世代数基础
刘绍学

出版发行	高等教育出版社		
社　　址	北京市东城区沙滩后街 55 号	**邮政编码**	100009
电　　话	010－64054588	**传　　真**	010－64014048
网　　址	http://www.hep.edu.cn		
经　　销	新华书店北京发行所		
印　　刷	国防工业出版社印刷厂		
纸张供应	山东高唐纸业集团总公司		
开　　本	787×960　1/16	**版　　次**	1999 年 10 月第 1 版
印　　张	13.5	**印　　次**	1999 年 10 月第 1 次印刷
字　　数	200 000	**定　　价**	14.60 元

凡购买高等教育出版社图书，如有缺页、倒页、脱页等质量问题，请在所购图书销售部门联系调换。

序 言

代数学是以数、多项式、矩阵、变换和它们的运算，以及群、环、域和模等为研究对象的学科.简单地说，代数学是研究代数系统(带有一些运算的集合)的.我们知道，数、多项式和矩阵的出现是由于刻画现实世界中几何量和物理量的需要.同样，群等也是由于直接或间接刻画新的几何量和物理量的需要而出现的.这样，研究这些对象就有两种途径：第一种是紧密结合它们出现的背景去研究，例如用群论方法去研究晶体的分类等；第二种是把数、多项式、矩阵、群等作为数学对象去研究，这时常和它们出现的背景相去甚远，或者几乎完全脱离这些背景.然而这两种研究应该是相辅相成浑然一体的.

在编写本书时，我们有以下的一些考虑.

一、在本课程中我们试图进行一些探索，在内容上除了第二、三、四章给出本课程的传统内容外，我们安排了第一章的“对称与群”和附录的“多元多项式环”.“对称与群”强调抽象代数系统的出现是由于刻画物理量和几何量的需要.“多元多项式环”中主要介绍 Gröbner 基，Buchberger 算法，它们是计算代数几何的基石，同时又是“初等”的，其难度和深度适中，是能够放在基础课中的.这使我们有一个恰当的方式来介绍多元多项式环这个重要的具体环，并能突出算法这个有用的数学概念以及代数与计算机的联系.虽然讲此内容可能有时间上的困难，但为了保留这一点探索意图，并把希望寄托于未来，因此把它作为附录放在原来第五章的位置.

二、讲抽象群、环、域理论的同时，较深入地介绍一些具体群、具体环和具体域.在本教程中我们选择了变换群(包括运动群、置换群)，这里没有足够的篇幅谈论矩阵群是一个遗憾.对域论，我们选择了多项式的分裂域——Galois 理论，对环论，选择了复数域上多元多项式环——Gröbner 基理论.这些具体的群、环、域不但有助于我们学习抽象理论，同时也使我们看到代数的一些应用：平面有限对称图形的分类，几何作图不能问题，根式解五次方程不能问题，编码问题，初等几何的机器证明等.

三、关于群、环、域、模都有彼此类似的基本概念：子系统(子群、子环、子域、子模)，商系统(商群、商环、商模)，同态和同构等等，以及作为它们的支柱

的一些具体例子,这些是代数的基础.当然还要对群、环、域、模中的每一个至少选择一个较深入的结构定理,否则内容将是散漫的而无重心和方向.对环论,我们选择了整除理论和 Gröbner 基理论.对域论,是分裂域理论——Galois 理论.对群论,是 Sylow 定理和有限交换群的结构定理,而且强调了后者,这不仅是因为它是一个典型结构定理(分解定理),而且也顺便为模论提供了一个好的结果.

四、一个好的数学思想是一定会在不同场合下重复出现的.使初学者能看到这些重复是有益的.在本教程中分解型结构思想重复出现在有限交换群的结构定理和代数簇的分解定理中,当然它们又都是整数和一元多项式的唯一分解一脉相承的.Galois 对应思想重复出现在 Galois 理论中和代数簇和理想的对应中.

五、本教材中我们对基本内容努力写得细致一些,这使得读者甚至可以自学.同时在某些适当的地方粗略(略去证明)介绍一些进一步的情况,好像在爬山到达一定高度时,停下来欣赏一下周围的景色,这对提高游兴是有益的.然而用这种方式去介绍五次方程不能用根式解问题是一种不得已!它太重要了,不能略去;另一方面无法(没有学时)把它作为基本内容放在本基础课中.

六、本教材的基本内容也就是我们认为抽象代数基础课应该提供给数学专业学生的必需内容.也许有的材料(如自由群或 Gröbner 基等)没有时间去讲,然而在教材中提供方便,使得读者有机会知道这些内容是应该的.但无论如何,内容和学时之间是有矛盾的.也许可由任课教师选讲其中部分章节,也许采用傅种孙教授提倡的讲法:讲重点,讲难点,讲思路,讲体会,利用本教材写得较细致的方便而把基本推导留给学生自学,这样"精讲"加"自学"的方式能完成主要内容的学习.

七、习题是重要的.我们认识到,学一门课的同时,作一个有代表性的较系统的大习题(学年作业)是非常有益的.在有限交换群的结构定理之后,我们布置了矩阵的 Jordan 标准型的模论证法以及主理想整环上有限生成周期模的结构定理的证明这样的大习题.我们相信,相对独立地完成这个大习题的读者定会对本基础课有较亲切的理解而受益匪浅.

我于 1996 年冬至 1997 年夏完成初稿,1997 年秋至 1998 年夏在山东大学等几所大学试用.1998 年秋,四川大学、厦门大学和北京师范大学参加试用的教师们在北京作了逐章逐节的讨论和修改,最后由彭联刚(四川大学)和林亚南(厦门大学)执笔完成并编写了习题.书中有关用计算机计算的例子都是罗运伦同志提供的.这样,这本书实际上是一个集体作品.

在本书中,作者常在一些地方和读者交流体会和理解,有时提到一些补充资料.这些不属于正文的"旁白"都用楷体字排出.

作者特别感谢两届系领导黄惟明、余玄冰以及张英伯、何青等同志,没有他们的推动与鼓励,这本书是不可能出现的.感谢审稿人石生明教授,他仔细地审阅全书,指出若干疏漏和该改进的地方,提出了建议,为本书增色许多.继过去在代数数论教材编审小组的长期共事,这次与责任编辑张小萍同志的再度合作,特别使我感到愉快。感谢石生明同志和张小萍同志,是在他俩的建议下,我在最后时刻写出了编码这一节.在近世代数教科书中介绍一点编码——代数学的一个最直接而重要的应用,是自然的和必要的.读者会喜欢它的.

本书荣幸地得到北京师范大学、四川大学、厦门大学三校教务处,天元基金委,教育部"面向21世纪教学内容和课程体系改革"项目以及普通高等教育"九五"国家重点教材项目的资助,在此作者表示衷心的感谢.

限于作者水平,书中定有许多不妥的地方,敬请读者指正.

刘绍学

1998年12月于北京师大

目　录

第一章　对称与群

抽象代数是以群、环、域、模为主要研究对象的学科. 本章将引进群(带有一个二元运算的集合)的概念,并特别强调群这一概念出现的背景. 学习完本章后,我们期望读者能对"对称即群"有一个初步但明确的理解.

§1　平面的运动群

我们来探讨平面上有限图形的对称问题. 人们都会说圆比正方形更对称些,正六边形比正三角形更显得对称一些. 如果问正三角形和正方形谁更对称一些,该怎么回答呢?

看来要把图形的对称这个直观概念说得确切一些,也就要给它一个定义,一个反映客观实际,能为大家接受的定义.

有某种对称的图形,就是经过某些运动后仍能回到自身的图形. 例如,圆经过绕圆心的旋转以及绕过圆心的直线的翻摺都是回到自身,而正方形只能绕其中心旋转 $\frac{\pi}{2}, \pi, \frac{3}{2}\pi$ 或绕其对角线或对边中点连线所作的翻摺才能回到自身,也许这就是圆比正方形更对称一些的解释. 用使图形回到自身的所有运动来刻画这一图形的对称应该是自然的,也符合我们对对称的直观感觉.

在这里我们回忆一下平面及其运动的概念.

用朴素平面几何的说法,可把平面想象为可向各方无限延伸的黑板面,我们还有平面上的点及两点距离的概念. 用解析几何的说法,平面就是集合 $\mathbb{R}^2 = \{(x,y) \mid x,y \in \mathbb{R}\}$,其中 $\mathbb{R}$ 是实数域,以及点 $A = (a_1,a_2)$, $B = (b_1,b_2)$ 之间的距离 $|AB| = \sqrt{(a_1 - b_1)^2 + (a_2 - b_2)^2}$. (用线性代数的语言,平面也就是二维欧氏空间.)今后我们把关于平面 P 的这两种刻画——几何直观的刻画和代数语言的刻画——等同起来.

定义 1.1　M 是任意一个非空集合, M 的变换是指 M 到自身的一个对应. M 的一一变换是指 M 到自身上的一一对应.

定义 1.2　(几何的定义)　平面 P 的一个运动是指平面 P 的一个保距变换. 亦即若 ϕ 是平面 P (点集)的一个变换,且对 P 上任意点 A 和点 B, $\phi(A)$ 和 $\phi(B)$ 的距离等于 A 和 B 的距离,则称 ϕ 为平面 P 的一个运动. 易见平面 P 的运动是 P 的一一对应.

由线性代数中欧氏空间的理论,我们有下面

定理 1.3a (代数的形式) 平面 $\mathbb{R}^2$ 的一个运动,是且仅是 $\mathbb{R}^2$ 中具有下面形式的变换

$$\begin{aligned} \phi: \quad \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ (x,y) &\longmapsto (x',y'), \end{aligned}$$

且

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = O\begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} a_1 \\ a_2 \end{pmatrix},$$

其中 O 是 2×2 正交矩阵, $A=(a_1,a_2)^T$ 是一个取定的向量.

利用平面几何的方法,或把平面几何和上述定理结合起来,可以证明下面著名的结果.

定理 1.3b (几何的形式,M. Chasles (1793—1880)) 平面的运动有且只有下列三种:

a) 沿任一给定向量的平移;

b) 以任意点为中心的旋转;

c) 绕某一直线作翻摺后再沿该直线上的一个向量作一平移(包括作纯翻摺的情况).

我们还知道,在定理 1.3a 中当 $A=(0,0)^T$ 而 $\det|O|=1$ 时,运动 ϕ 就是绕原点的旋转;而当 $A=(0,0)^T$ 且 $\det|O|=-1$ 时, ϕ 就是以某一过原点的直线为轴的翻摺;而 $O=E$ (单位矩阵)时, ϕ 就是沿向量 $A=(a_1,a_2)^T$ 的平移.

对我们来说非常重要的是,两个变换是可以相乘的,这就是

定义 1.4 M 是一个非空集合, ϕ 和 ψ 是 M 的两个变换.规定 M 到自身的映射 $\rho(x)=\phi(\psi(x))$ (对任意 $x\in M$),则易知 ρ 是 M 的变换.我们定义 ρ 是变换 ϕ 和变换 ψ 的乘积,记作 $\rho=\phi\circ\psi$.注意到 M 的两个一一变换的乘积仍是一个一一变换,我们特把 M 的一一变换全体记作 $T(M)$,并把映射

$$\begin{aligned} \circ: \quad T(M)\times T(M) &\longrightarrow T(M) \\ (\phi,\psi) &\longmapsto \phi\circ\psi \end{aligned}$$

称为 $T(M)$ 的一个乘法.

我们知道,变换的乘法适合结合律,即 $(\phi\circ\psi)\circ\theta=\phi\circ(\psi\circ\theta)$.

我们还知道恒等变换 I (即把 M 的每一元素 x 对应到 x 本身的变换)是 M 的一一变换, M 的一一变换 ϕ 的逆变换 ϕ^{-1} 是 M 的一一变换,以及 $\phi\circ\phi^{-1}=\phi^{-1}\circ\phi$ 是恒等变换 I.

定义 1.5 M 是一个非空集合, $T(M)$ 是 M 的所有一一变换的全体.我

们把 $T(M)$ 以及变换的乘法放在一起来考察，记作 $(T(M),\circ)$（这里 $\circ$ 表示变换的乘法），并称之为 M 的变换群.

这里再强调一下，我们并不是把集 $T(M)$ 叫作变换群，而是把带有乘法运算的 $(T(M),\circ)$ 叫作变换群. 代数学的特点是研究带有运算的集合. 对于一个集合，只有在其中引入运算后，才是代数学研究的对象.

把上面提到的已知事实总结一下便有下面的

命题 1.6 变换群 $(T(M),\circ)$ 具有下列性质：

G1) 对任意 $\phi,\psi\in T(M)$，有 $\phi\circ\psi\in T(M)$；

G2) 对任意 $\phi,\psi,\theta\in T(M)$，有 $(\phi\circ\psi)\circ\theta=\phi\circ(\psi\circ\theta)$；

G3) 存在 $I\in T(M)$ 使得对任意 $\phi\in T(M)$，有 $I\circ\phi=\phi\circ I=\phi$；

G4) 对任意 $\phi\in T(M)$，存在 $\phi^{-1}\in T(M)$，使得 $\phi\circ\phi^{-1}=\phi^{-1}\circ\phi=I$. □

现在我们从一般集 M 及其一一变换回到平面 $\mathbb{R}^2$ 及其运动上来.

用 $M(\mathbb{R}^2)$ 表示平面 $\mathbb{R}^2$ 的所有运动，运动只不过是特殊（保距）的一一变换，即有 $M(\mathbb{R}^2)\subseteq T(\mathbb{R}^2)$，后者是 $\mathbb{R}^2$ 的所有一一变换的全体. 很容易证明：平面的两个运动（保距变换）的乘积仍是一个运动，一个运动 ϕ 的逆变换 ϕ^{-1} 仍是一个运动. 当然恒等变换是一个保距变换. 这样我们就得到

命题 1.7 $M(\mathbb{R}^2)$ 对于变换的乘法具有下列性质：

G1) 对任意 $\phi,\psi\in M(\mathbb{R}^2)$，有 $\phi\circ\psi\in M(\mathbb{R}^2)$；

G2) 此时当然对任意 $\phi,\psi,\theta\in M(\mathbb{R}^2)$，有 $(\phi\circ\psi)\circ\theta=\phi\circ(\psi\circ\theta)$；

G3) 恒等变换 $I\in M(\mathbb{R}^2)$. 此时当然对任意 $\phi\in T(M)$，有 $I\circ\phi=\phi\circ I=\phi$；

G4) 对任意 $\phi\in M(\mathbb{R}^2)$，也有 $\phi^{-1}\in M(\mathbb{R}^2)$，此时当然也有 $\phi\circ\phi^{-1}=\phi^{-1}\circ\phi=I$. □

很自然地，我们该有下面的

定义 1.8 称 $(M(\mathbb{R}^2),\circ)$ 为平面 $\mathbb{R}^2$ 的运动群，这里 $\circ$ 表示运动的乘法（也就是变换的乘法）.

现在来考察使平面图形 K 仍回到自身的平面运动的全体，把它记作 $S(K)$. 我们知道，平面图形 K 也就是平面 $\mathbb{R}^2$ 上一些点的集合，即 $K\subseteq\mathbb{R}^2$，且 K 中任意两点间有距离；而使 K 保持不变的运动也就是使 $\phi(K)=K$ 的运动 ϕ（这里 $\phi(K)=\{\phi(x),x\in K\}$）.

定义 1.9 我们把 $S(K)$ 称作平面图形 K 的对称.

这样，我们就把图形 K 的直观对称的概念用精确的数学语言——集合 $S(K)$ 来刻画：K 的对称就是集合 $S(K)$. 我们当然无法“证明”，这个 $S(K)$ 就是你心目中的对称，$S(K)$ 只是我们心目中直观对称概念的一个数学模

型.然而从实践上来看,这个数学模型是可接受的,是好的.读者容易证明下面

命题 1.10 $(S(K),\circ)$ 满足上面命题中的 G1) - G4)这四个条件.□

定义 1.11 我们称 $(S(K),\circ)$ 为平面图形 K 的对称群.

例 1 正方形的对称群是由下列平面运动组成:恒等运动,绕其中心转 $90°,180°,270°$ 的旋转,以及关于它的两条对角线,两条对边中点连线所作的翻摺.一共 8 个运动.

很容易验证这 8 个运动,使正方形仍回到自身上去.另一方面利用 Chasles 定理可得其它的平面运动都不使该正方形回到自身,故得上述结果.

由于图形的对称性可由对称群这一代数对象来刻画,下一步我们就可用代数方法去研究图形的对称,这有点儿像笛卡尔坐标系把几何图形和方程式联系起来后,我们在解析几何中可用代数方法研究几何一样.不同的是在解析几何中我们用的是多项式,而这一次是用"群"了.

关于图形,以至晶体的对称群的研究请看相应的参考书.

练习

1.设 ϕ 是平面 $\mathbb{R}^2$ 的一个运动,其代数形式为

$$\begin{aligned}\phi:\quad & \mathbb{R}^2 \longrightarrow \mathbb{R}^2\\ & (x,y) \longmapsto (x',y'),\end{aligned}$$

满足 $\begin{pmatrix}x'\\y'\end{pmatrix}=O\begin{pmatrix}x\\y\end{pmatrix}$,其中 O 是 $\mathbb{R}$ 上一个 2×2 正交矩阵.证明:如果 $\det|O|=-1$,那么存在一条直线 l,使得运动 ϕ 是关于直线 l 的对称变换,即对任意 $A=(x,y)\in\mathbb{R}^2$,有 $\phi(A)=(x',y')\in\mathbb{R}^2$ 是 A 的关于直线 l 的对称点,从而 ϕ 是绕 l 的翻摺.

2.设 M 是一个非空集合.证明:变换群 $(T(M),\circ)$ 满足结合律,即命题 1.6 中的 G2).

3.设 K 是正六边形.写出 K 的对称群 $S(K)$.

§2 数域的对称

先回忆一下在高等代数中学过的数域的概念.

我们假定复数以及其加法、减法、乘法是大家都熟悉的.令 $\mathbb{C}$ 表示复数全体.

定义 2.1 称 $\mathbb{C}$ 的一个含有 0 和 1 的子集 F 为一个数环,如果 F 满足下列条件

F1) F 关于数的加法、减法和乘法是封闭的,即若 $a,b\in F$,则 $a+b$, $a-b$, $a\cdot b$ 都在 F 中;

如果除 F1)外 F 还满足

F2) 若 $0 \neq a \in F$ 则 a 的逆元 a^{-1} 也在 F 中,

则称 F 为一个数域.

显然,全体非负整数不是数环,而全体整数是数环但不是数域,全体有理数、全体实数都是数域.

例 1 $F = \{a + b\sqrt{2} \mid a, b$ 是有理数$\}$ 是数域.

平面图形是一个几何结构,即是把一个点集 M 连同此点集 M 中任意两点间有距离作为一个整体来考虑,而其对称群就是 M 的保持其任两点间距离的变换的全体,这些保持 M 的几何结构(即距离)的变换的全体,就刻画了几何结构的对称.

完全类似地,数域 F 是一个代数结构,即是把一个数集 F 连同此数集 F 中加、减、乘的运算作为一个整体一起来考虑.数域 F 的对称也同样地可用 F 的保持代数结构(即运算)的变换的全体来刻画,虽然它不像图形对称那样直观,但它是客观存在的.这样我们有下面的

定义 2.2 数域 F 的自同构 ϕ 是指

a) ϕ 是集合 F 到 F 上的一个一一对应(即 F 的一一变换);

b) 对所有 $x, y \in F$ 有: $\phi(x + y) = \phi(x) + \phi(y), \phi(xy) = \phi(x)\phi(y)$.

在定义中我们没有要求自同构保持 F 中的减法运算和取逆,这是因为它们是保持加法和乘法的推论:

命题 2.3 设 ϕ 是数域 F 的自同构,则有

1) $\phi(0) = 0, \phi(1) = 1$;

2) 对任意 $x, y \in F$, 有 $\phi(-x) = -\phi(x), \phi(x - y) = \phi(x) - \phi(y)$;

3) 对任意 $0 \neq x \in F$, 有 $x^{-1} \in F$, 使 $\phi(x^{-1}) = \phi(x)^{-1}$.

证明 1) 依定义 2.2 中 b),有 $\phi(0) = \phi(0 + 0) = \phi(0) + \phi(0)$, 从两侧消去 $\phi(0)$ 便得 $\phi(0) = 0$. 同样方法可证 $\phi(1) = 1$.

2) 依 1)及定义 2.2 中 b),有 $0 = \phi(0) = \phi(x + (-x)) = \phi(x) + \phi(-x)$, 故 $\phi(-x) = -\phi(x)$. 随之也有

$$\begin{aligned}\phi(x - y) &= \phi(x + (-y)) = \phi(x) + \phi(-y) \\ &= \phi(x) + (-\phi(y)) = \phi(x) - \phi(y).\end{aligned}$$

3) 用同样方法可证. □

和 §1 中两个保持几何结构的运动的乘积仍是保持该几何结构的运动完全类似的,我们有

命题 2.4 设 ϕ,ψ 是数域 F 的两个自同构,则 $\phi^{-1},\phi\psi$ 也都是数域 F 的自同构.

证明 由于数域 F 的自同构首先是集 F 的变换,故 $\phi^{-1},\phi\psi$ 的意义是清楚的,它们都是集 F 的变换.

先证 $\phi\psi$ 是自同构.任取 $x,y\in F$,则依变换乘积的定义有

$$\begin{aligned}(\phi\psi)(xy)&=\phi(\psi(xy))=\phi(\psi(x)\psi(y))\\&=\phi(\psi(x))\cdot\phi(\psi(y))=(\phi\psi)(x)\cdot(\phi\psi)(y).\end{aligned}$$

类似地可证 $\phi\psi$ 保持加法.

再证 ϕ^{-1} 是自同构.任取 $x,y\in F$. 由于 ϕ 是 F 到 F 上的一一对应,故必有 $x',y'\in F$ 使得 $x=\phi(x'),y=\phi(y')$. 此时当然也有 $x'=\phi^{-1}(x),y'=\phi^{-1}(y)$. 这样就有

$$\phi^{-1}(xy)=\phi^{-1}(\phi(x')\phi(y'))=\phi^{-1}(\phi(x'y'))=x'y'=\phi^{-1}(x)\phi^{-1}(y).$$

类似地可证 ϕ^{-1} 保持加法.□

从以上命题,我们便有

定理 2.5 令 $\mathrm{Aut}(F)$ 表示数域 F 的所有自同构的全体,令 $\circ$ 表示变换的乘法,则 $(\mathrm{Aut}(F),\circ)$ 具有下列性质

G1) 对任意 $\phi,\psi\in\mathrm{Aut}(F)$,有 $\phi\circ\psi\in\mathrm{Aut}(F)$;

G2) 对任意 $\phi,\psi,\theta\in\mathrm{Aut}(F)$,有 $(\phi\circ\psi)\circ\theta=\phi\circ(\psi\circ\theta)$;

G3) 存在 $I\in\mathrm{Aut}(F)$ 使得对任意 $\phi\in\mathrm{Aut}(F)$,有 $I\circ\phi=\phi\circ I=\phi$;

G4) 对任意 $\phi\in\mathrm{Aut}(F)$,存在 $\phi^{-1}\in\mathrm{Aut}(F)$ 使得 $\phi\circ\phi^{-1}=\phi^{-1}\circ\phi=I$.

易见上面 G3)中的 I 就是 F 的恒等变换:对任意 $x\in F$,有 $I(x)=x$. 称之为恒等自同构.□

定义 2.6 我们称 $(\mathrm{Aut}(F),\circ)$ 为数域 F 的自同构群.

这里我们再作一次类比:数域 F 的自同构群相当于图形 K 的对称群,后者刻画了图形 K 的对称,前者则刻画了数域的"对称"——它是图形对称在数域上的一个类比概念.

例 2 有理数域 $\mathbb{Q}$ 的自同构群只有一个元素——恒等自同构 I.

这是因为,任取 $\mathbb{Q}$ 的一个自同构 ϕ,由 $\phi(1)=1$ 得 $\phi(2)=\phi(1+1)=\phi(1)+\phi(1)=2$,一般对任意正整数 n 有 $\phi(n)=n$,随之 $\phi(-n)=-\phi(n)=-n,\phi(1/n)=\phi(n^{-1})=\phi(n)^{-1}=n^{-1}$. 故对任意整数 n,m 我们有 $\phi(m/n)=\phi(m)\phi(1/n)=m\cdot 1/n=m/n$. 即 $\phi=I$.□

从上面证明中,可知对任意数域 F(它当然包含所有有理数)的自同构 ϕ 必有 $\forall x\in\mathbb{Q},\phi(x)=x$.

例 3 令 $F=\mathbb{Q}(\sqrt{2})=\{a+b\sqrt{2},|,a,b\in\mathbb{Q}\}$,易验证 F 是一个数域.

今考察 F 的自同构群.任取 F 的自同构ϕ,注意到 $\forall a \in \mathbb{Q}$, $\phi(a) = a$,故有 $\phi(a + b\sqrt{2}) = \phi(a) + \phi(b)\phi(\sqrt{2}) = a + b \cdot \phi(\sqrt{2})$. 这样只要$\sqrt{2}$ 在 ϕ 下的象 $\phi(\sqrt{2})$ 定了,则 ϕ 也就完全确定了. ϕ 是自同构,是保持运算的,故$\sqrt{2}$ 所适合的有理系数代数关系式, $\phi(\sqrt{2})$ 也应该适合,特别$\sqrt{2}$ 是 $x^2 - 2 = 0$ 的根,即 $(\sqrt{2})^2 - 2 = 0$, 故由

$$0 = \phi(0) = \phi((\sqrt{2})^2 - 2) = \phi(\sqrt{2})^2 - 2$$

也知 $\phi(\sqrt{2})$ 是 $x^2 - 2 = 0$ 的根.因而 $\phi(\sqrt{2})$ 的可能值最多只有两个:$\sqrt{2}$ 和 $-\sqrt{2}$. 直接验证

$$I: \quad F \longrightarrow F \qquad \phi: \quad F \longrightarrow F$$
$$a + b\sqrt{2} \longmapsto a + b\sqrt{2}, \qquad a + b\sqrt{2} \longmapsto a - b\sqrt{2}$$

确是数域 F 的自同构.这样, F 的自同构群是 $\{I, \phi\}$, 其乘法是 $II = I$, $I\phi = \phi I = \phi$, $\phi\phi = I$, 或可写成如下的乘法表

$\circ$	I	ϕ
I	I	ϕ
ϕ	ϕ	I

例 4 令 $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} \mid a, b, c, d \in \mathbb{Q}\}$. 易验证 E 是一个数域.和例 3 完全类似,如果 ϕ 是 E 的自同构,则 ϕ 完全由 $\phi(\sqrt{2})$ 和 $\phi(\sqrt{3})$ 确定,而 $\phi(\sqrt{2})$ 的可能值只有 $\sqrt{2}$ 和 $-\sqrt{2}$, $\phi(\sqrt{3})$ 的可能值只有 $\sqrt{3}$ 和 $-\sqrt{3}$. 直接验证,可知下列变换都是数域 E 的自同构:

$$I: \quad a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} \longrightarrow a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3}$$
$$\phi_1: \quad a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} \longrightarrow a - b\sqrt{2} + c\sqrt{3} - d\sqrt{2}\sqrt{3}$$
$$\phi_2: \quad a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} \longrightarrow a + b\sqrt{2} - c\sqrt{3} - d\sqrt{2}\sqrt{3}$$
$$\phi_{12}: \quad a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} \longrightarrow a - b\sqrt{2} - c\sqrt{3} + d\sqrt{2}\sqrt{3}$$

这样, E 的自同构群是 $\{I, \phi_1, \phi_2, \phi_{12}\}$, 其乘法表为

$\circ$	I	ϕ_1	ϕ_2	ϕ_{12}
I	I	ϕ_1	ϕ_2	ϕ_{12}
ϕ_1	ϕ_1	I	ϕ_{12}	ϕ_2
ϕ_2	ϕ_2	ϕ_{12}	I	ϕ_1
ϕ_{12}	ϕ_{12}	ϕ_2	ϕ_1	I

表中 x -行 y -列交叉处的元素等于 $x \circ y$，例如 $\phi_1 \circ \phi_2 = \phi_{12}$ 等等. 常称这样的表为 Cayley 表，以示人们对为群论作出贡献的 A. Cayley(英国数学家，1821—1895)的敬意.

给两个数域 F 和 E，如果有 $F \subseteq E$，我们称 F 是 E 的子域，而称 E 为 F 的扩域.

对给定的两个数域 F 和 E，$F \subseteq E$. 令

$$\mathrm{Aut}(E:F) = \{\phi \in \mathrm{Aut}(E) \mid \forall x \in F, \phi(x) = x\},$$

即它的元素是那些使得 F 中元素不动的，数域 E 的自同构.

命题 2.7 $(\mathrm{Aut}(E:F), \circ)$ 满足定理 2.5 中的性质 G1)—G4). □

定义 2.8 我们称 $(\mathrm{Aut}(E:F), \circ)$ 为数域 E 在 F 上的对称群.

当然，一般说 $\mathrm{Aut}(E:F)$ 是 $\mathrm{Aut}(E)$ 的一个真子集，它不再刻画数域 E 的对称，它刻画的是数域 E 的保持 F 中元素不动的那种对称性. 我们将在下一节中看到这种对称性的意义.

取上面例 3 中的 $F = \mathbb{Q}(\sqrt{2})$，例 4 中的 $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$，则我们有 $\mathbb{Q} \subseteq F \subseteq E$. 关于这些数域，有下面结果.

例 5 $\mathrm{Aut}(E:\mathbb{Q}) = \mathrm{Aut}(E) = \{I, \phi_1, \phi_2, \phi_{12}\}$.

例 6 $\mathrm{Aut}(E:F) = \{I, \phi_2\}$. 这是因为自同构 ϕ_1, ϕ_{12} 使 F 中的有些数不对应本身.

练习

1. 证明：$F = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ 是数域.

2. 设 F 是数域. 证明：$\mathrm{Aut}(F:\mathbb{Q}) = \mathrm{Aut}(F)$.

3. 设 a, b, c, d 为有理数. 证明：如果 $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} = 0$，那么 $a = b = c = d = 0$.

4. 设 $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$ 和 $\mathbb{Q}(i, \sqrt{5}) = \{a + bi + c\sqrt{5} + di\sqrt{5} \mid a, b, c, d \in \mathbb{Q}\}$.

1) 证明：$\mathbb{Q}(i)$ 和 $\mathbb{Q}(i, \sqrt{5})$ 是域.

2) 若记 $F = \mathbb{Q}(i)$，$E = \mathbb{Q}(i, \sqrt{5})$，求 $\mathrm{Aut}(F)$，$\mathrm{Aut}(E)$ 和 $\mathrm{Aut}(E:F)$. 并写出 $\mathrm{Aut}(E)$ 的乘法表.

§3 多项式的对称

我们都熟悉 n 个变元 $x_1, x_2, \cdots, x_n$ 的 n 元多项式. 今把以数域 F 中的数作系数的 n 元多项式的全体记作 $F[x_1, x_2, \cdots, x_n]$(或简记作 $F[X]$)，每一 n 元多项式可以唯一地表示为不同类单项式的有限线性和：

$$f(x_1,x_2,\cdots,x_n)=\sum_{\alpha}a_{\alpha}x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n},$$

其中 $\alpha=(\alpha_1,\alpha_2,\cdots,\alpha_n)$，$\alpha_i\in\mathbb{Z}^+\cup\{0\}$，而 $a_\alpha\in F$.

令 $M=\{x_1,x_2,\cdots,x_n\}$. 用 S_n 表示集合 M 的变换群(见§1). S_n 常称作 n 元对称群. S_n 中的元素就是 $\{x_1,x_2,\cdots,x_n\}$ 的一个置换，略去字母 x 而只记下标，这时的置换可记作

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

其中 $(i_1,i_2,\cdots,i_n)$ 是 $1,2,\cdots,n$ 的一个排列，而 $\Sigma(j)=i_j$.

现在我们利用变换群 S_n 中的元素 Σ 去定义集合 $F[X]$ 到 $F[X]$ 的一个映射

$$\begin{array}{ccc}\phi_\Sigma: & F[X] & \longrightarrow & F[X]\\ & f(x_1,x_2,\cdots,x_n) & \longmapsto & f(x_{i_1},x_{i_2},\cdots,x_{i_n}),\end{array}$$

其中 $f(x_{i_1},x_{i_2},\cdots,x_{i_n})$ 是在多项式 $f(x_1,x_2,\cdots,x_n)$ 中将 x_1 换成 x_{i_1}，x_2 换成 x_{i_2}，… 后所得到的多项式.

不难证明这是集 $F[X]$ 的一个变换. 这实际上就是把其子集 $\{x_1,x_2,\cdots,x_n\}$ 的一个变换 Σ 用一种“自然方式”扩大成为整个集合 $F[X]$ 的一个变换 ϕ_Σ.

令 $T_n=\{\phi_\Sigma\mid\Sigma\in S_n\}$. T_n 是 $F[X]$ 的一些($n!$ 个)变换组成的集合. 注意到(请读者证明一下)

$$\phi_\Sigma\circ\phi_\theta=\phi_{\Sigma\cdot\theta},\quad(\phi_\Sigma)^{-1}=\phi_{\Sigma^{-1}}.$$

我们有

命题 3.1 $(T_n,\circ)$ 满足性质 G1)—G4)，称之为 $F[X]$ 的置换群.

如果把 n 元多项式和平面图形类比，把 $F[X]$ 和平面类比，则 $F[X]$ 的置换群相当于平面的运动群.

定义 3.2 令 $f(x_1,x_2,\cdots,x_n)$ 是一个 n 元多项式，令

$$S_f=\{\phi_\Sigma\in T_n\mid\phi_\Sigma(f)=f\}.$$

命题 3.3 $(S_f,\circ)$ 满足性质 G1)—G4). 称之为 n 元多项式 $f(x_1,x_2,\cdots,x_n)$ 的对称群.

例 1 $F[x_1,x_2,x_3,x_4]$ 中的多项式 $f=x_1x_2+x_3x_4$ 的对称群

$$S_f=\left\{\phi_\Sigma\middle|\Sigma=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix},\right.$$
$$\left.\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix},\right.$$