“十二五”国家重点图书出版规划项目

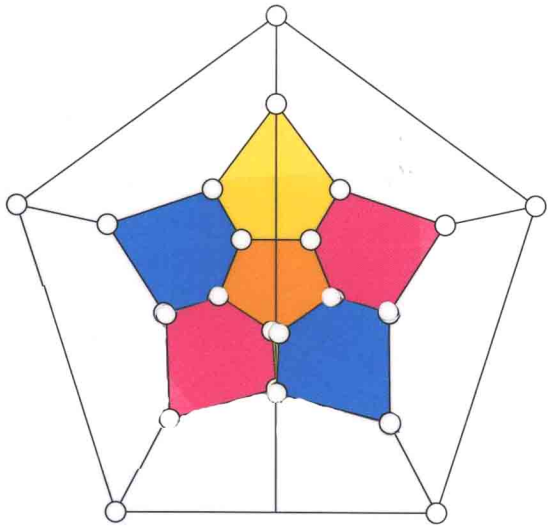
走向数学丛书

SCIENCE & HUMANITIES

有限域及其应用

FINITE FIELDS AND THEIR APPLICATIONS

著　冯克勤　廖群英



大连理工大学出版社
DALIAN UNIVERSITY OF TECHNOLOGY PRESS

“十二五”国家重点图书出版规划项目

走向数学丛书

SCIENCE
&
HUMANITIES

有限域及其应用

FINITE FIELDS AND THEIR APPLICATIONS

著　冯克勤　廖群英

大连理工大学出版社
DALIAN UNIVERSITY OF TECHNOLOGY PRESS

“走向数学”丛書

陳省身題

科技强国，数学当奉

吴文俊

2010.1.10

“十二五”国家重点图书出版规划项目

走向数学丛书

编写委员会

续编说明

自从1991年“走向数学”丛书出版以来，已经出版了三辑，颇受我国读者的欢迎，成为我国数学传播与普及著作的一个品牌。我想，取得这样可喜的成绩主要原因是：中国数学家的支持，大家在百忙中抽出宝贵时间来撰写此丛书；天元基金的支持；与湖南教育出版社出色的出版工作。

但由于我国毕竟还不是数学强国，很多重要的数学领域尚属空缺，所以暂停些年不出版亦属正常。另外，有一段时间来考验一下已经出版的书，也是必要的。看来考验后是及格了。

中国数学界屡屡发出继续出版这套丛书的呼声。大连理工大学出版社热心于继续出版；世界科学出版社（新加坡）愿意出某些书的英文版；湖南教育出版社也乐成其事，

尽量帮忙。总之，大家愿意为中国数学的普及工作尽心尽力。在这样的大好形势下，“走向数学”丛书组成了以冯克勤教授为主编的编委会，领导继续出版工作，这实在是一件大好事。

首先要挑选修订重印一批已出版的书；继续组稿新书；由于我国的数学水平距国际先进水平尚有距离，我们的作者应面向全世界，甚至翻译他们的优秀著作。

我相信在新的编委会的领导下，丛书必有一番新气象。

我预祝丛书取得更大成功。

王　元

2010 年 5 月于北京

编写说明

从力学、物理学、天文学，直到化学、生物学、经济学与工程技术，无不用到数学. 一个人从入小学到大学毕业的十六年中，有十三四年有数学课. 可见数学之重要与其应用之广泛.

但提起数学，不少人仍觉得头痛，难以入门，甚至望而生畏. 我以为要克服这个鸿沟还是有可能的. 近代数学难于接触，原因之一大概是由于其符号、语言与概念陌生，兼之近代数学的高度抽象与概括，难于了解与掌握. 我想，如果知道讨论对象的具体背景，则有可能掌握其实质. 显然，一个非数学专业出身的人，要把数学专业的教科书都自修一遍，这在时间与精力上都不易做到. 若停留在初等数学水平上，哪怕做了很多难题，似亦不会有助于对近代数学的了

解.这就促使我们设想出一套“走向数学”小丛书,其中每本小册子尽量用深入浅出的语言来讲述数学的某一问题或方面,使工程技术人员、非数学专业的大学生,甚至具有中学数学水平的人,亦能懂得书中全部或部分含义与内容.这对提高我国人民的数学修养与水平,可能会起些作用.显然,要将一门数学深入浅出地讲出来,决非易事.首先要对这门数学有深入的研究与透彻的了解.从整体上说,我国的数学水平还不高,能否较好地完成这一任务还难说.但我了解很多数学家的积极性很高,他们愿意为“走向数学”撰稿.这很值得高兴与欢迎.

承蒙国家自然科学基金委员会、中国数学会数学传播委员会与湖南教育出版社的支持,得以出版这套“走向数学”丛书,谨致以感谢.

王　元

1990 年于北京

引 言

我们在学习数学的过程中，从小学到中学，数的范围不断扩大. 开始我们知道自然数(即正整数和零)，并且在自然数集合中可以进行加法和乘法运算. 后来学习了负整数之后，所有整数组成的集合$\{0,\pm1,\pm2,\cdots\}$之中又可进行减法运算. 随后又学习了分数，于是在有理数集合中可以进行加减乘除四则运算(其中0不能作为除数). 到了中学，数的概念又扩大为实数和复数，在实数集合与复数集合中均可进行四则运算. 能够进行四则运算并且满足一些运算法则(结合律，交换律，分配律)的任意集合，在数学上都叫做是一个域。所以，我们在中学已经学过三个域：有理数域、实数域和复数域. 而自然数集合和整数集合都不是域，因为两个整数相除不一定为整数.

有理数域、实数域和复数域都是无限域，这些域中都有无限多个数. 这本小册子要向读者介绍的主要对象是有限域，即由有限个“数”构成的域.

首先遇到的问题是：有限域是否存在？如果你学过一点初等数论，那么你已经接触过许多有限域了. 设p是一个素数(也

叫质数)，如 $p=2,3,5,7,\cdots$，对于每个整数 a，我们用$[a]$表示模 p 同余于 a 的所有整数组成的集合. 由于每个整数被 p 除的余数恰好是 $0,1,2,\cdots,p-1$ 当中的一个，所以恰好有 p 个集合：$[0],[1],[2],\cdots,[p-1]$. 以 $\boldsymbol{F}_p$ 表示这 p 个元素组成的集合，并且自然地定义如下运算

$$[a]+[b]=[a+b],\quad [a]-[b]=[a-b],\quad [a]\cdot[b]=[a\cdot b].$$

利用同余式的性质，可以证明 $\boldsymbol{F}_p$ 是 p 元有限域，例如对于$p=3$，$\boldsymbol{F}_3=\{[0],[1],[2]\}$，我们有

$$[2]+[2]=[2+2]=[4]=[1],$$
$$[1]-[2]=[1-2]=[-1]=[2],$$
$$[2]\cdot[2]=[2\cdot 2]=[4]=[1].$$

注意 4 被 3 除余 1，从而$[4]=[1]$，同样地$[-1]=[2]$. 进而由于$[2]\cdot[2]=[1]$，可知$[2]^{-1}=[2]$. 同样有$[1]^{-1}=[1]$. 因此我们可以做除法$[a]/[b]$(其中$[b]\neq[0]$)，比如

$$[1]/[2]=[1]\cdot[2]^{-1}=[1]\cdot[2]=[2].$$

对于没有学过初等数论的读者，我们将在第 1 章讲述这批有限域，同时介绍本书中所用到的一些初等数论知识.

以上对每个素数 p，我们都给出了一个 p 元有限域. 由于素数有无穷多个，所以我们已经有了无穷多个有限域. 其中最简单的有限域是 $p=2$ 时的二元域 $\boldsymbol{F}_2$，它只有两个元素$[0]$和$[1]$，其中$[0]$是被 2 除尽的全部整数，也就是偶数；而$[1]$是全部奇数，$\boldsymbol{F}_2$ 中的加法和乘法为：

$$[0]+[0]=[0],$$
$$[0]+[1]=[1]+[0]=[1],$$
$$[1]+[1]=[2]=[0],$$
$$[0]\cdot[0]=[0]\cdot[1]=[1]\cdot[0]=[0],$$

$$[1]\cdot[1]=[1].$$

这里只有$[1]+[1]=[0]$是比较特别的，但是也不奇怪，因为这不过是表示一个熟知的事实：奇数加奇数等于偶数. 二元域在数学上虽然简单，但却是通信中使用最广泛的数学工具，因为$[0]$和$[1]$可以分别表示开关逻辑电路中“开”和“关”两个状态，或者脉冲电路中两个不同方向的脉冲.

除了初等数论中为我们提供的 p 元域之外，是否还存在别的有限域呢？历史上，第一个明确地研究任意有限域的是法国年青而早逝的天才数学家伽罗华(Galois，1811—1832). 1830 年他在 p 元域的基础上，利用域扩张的方法构作出全部可能的有限域(见本书第 2.2 节). 后人把有限域也叫作伽罗华域.

有限域和读者所熟悉的有理数域、实数域和复数域一样，具有每个域的公共性质. 比如说在 $\boldsymbol{F}_p$ 中，每个非零元素$[a]$($\neq[0]$)都有逆元素$[b]$(即$[a]\cdot[b]=1$). 又比如说：若$[a][b]=[0]$，则$[a]=[0]$或者$[b]=[0]$. 另一方面，由于有限域中只有有限多个元素，使得它具有很多特别和奇妙的性质. 这些性质的研究近百年来一直成为数学的研究对象，发展成内容丰富的有限域理论. 与此同时，有限域的美妙性质在许多领域都有广泛的应用. 20 世纪中期开始，人们利用有限域构作各种试验设计方案，特别是数字通信的进步和数字计算机的发展，有限域在信息科学和计算机科学中有许多应用，成为不可缺少的数学工具. 这些应用领域提出许多数学问题，反过来也刺激和促进了有限域理论研究的发展.

在这本小册子里，我们在第一部分先给出全部有限域，并且介绍有限域的各种奇妙的性质. 在第二部分讲述有限域的一些应用. 这是一本通俗读物，爱好数学的中学生可以读懂本书的大

部分内容. 此外，本书还需要线性代数的初步知识，主要是向量空间概念，矩阵的运算和域上解线性方程组的知识. 除了“域”之外，我们还使用了抽象代数中另两个术语：“群”和“环”. 这些术语并不深奥，我们主要涉及很简单的交换群、多项式环和有限域. 问题的叙述和证明都尽量做得通俗，并举出例子加以说明，我们也常常加一些注记，为了使了解更多代数知识的人画龙点睛地指明事情的实质，或者描述一下有限域更深刻的理论进展，更广泛的应用，以及尚未解决的问题. 在数学发展的历史长河和广泛天地之中，有限域(finite field)只是数学田野(field)中一朵清新的小花，作者希望通过这朵小花使读者感受到数学之美，数学应用的广泛，以及数学和应用的相互促进.

本书于 1991 年在《走向数学》丛书中于湖南教育出版社出版. 18 年来，有限域的理论研究有很大的发展，特别是有限域的应用更为广泛. 这次大连理工大学出版社重新出版《走向数学》丛书时，本书作了很大的改动. 重新组织和扩展了有限域的理论部分，增加了有限域的许多应用. 与此同时，根据读者对原书的反应，我们也删去了原书的部分内容. 作者继续渴望听取读者的意见和建议，以便今后进一步改善.

本书得到国家自然科学基金〈信息处理中的关键数学问题〉(编号 10990011)的支持.

冯克勤　廖群英

2008 年 9 月于清华园

目 录

理 论 部 分

应 用 部 分

理 论 部 分

一

来自初等数论的有限域

初等数论是研究整数性质和方程整数解的一门学问. 17 世纪,法国数学家费马(Fermat,1601—1665)对于整数提出了一系列猜想,这些猜想引起大数学家欧拉(Euler,1707—1783)和高斯(Gauss,1777—1855)等人的浓厚兴趣. 他们在 18 和 19 世纪系统地研究了整数的性质,解决了费马的几乎全部猜想(只有一个猜想一直到 1994 年才由怀尔斯(Wiles)最终解决). 我们在本章第 1.1 节介绍由欧拉和高斯所研究的整数的两个基本性质:整除性和同余性. 利用这些性质,第 1.2 节给出有限域的第一批例子.

§ 1.1 整除性和同余性

在本书中,我们用 **Z** 表示全部整数组成的集合{0,±1,±2,