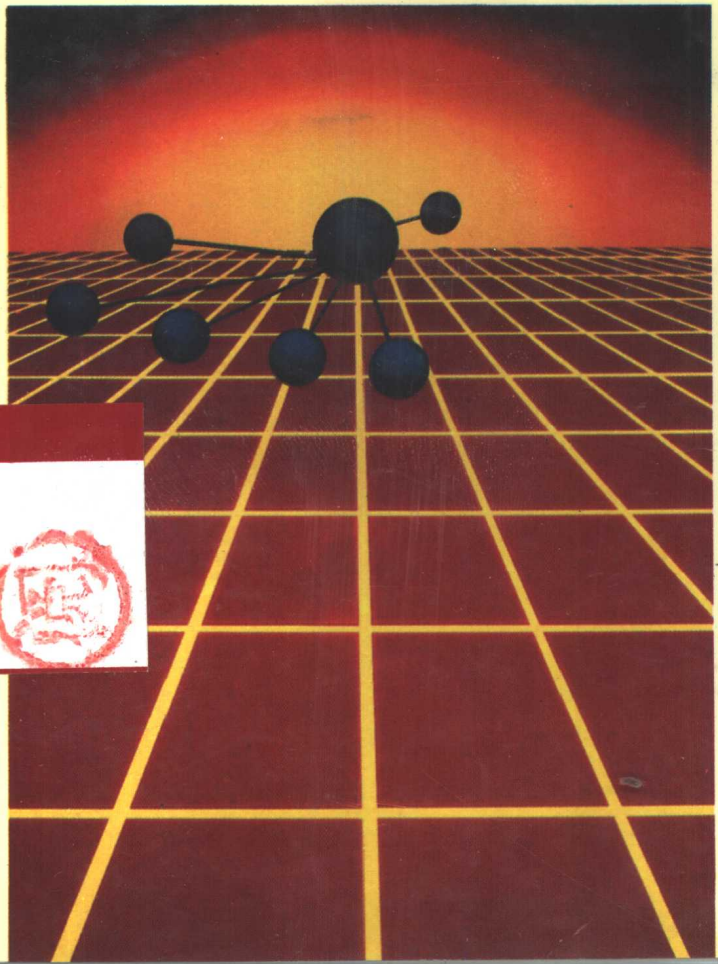
有限域 FINITE FIELDS

走向数学丛书

冯克勤 著



走向数学丛书

有限域

冯克勤 著

湖南教育出版社

有 限 域
Finite Fields

冯克勤
Feng Ke-qin 著

责任编辑：孟实华

湖南教育出版社出版发行
湖南省新华书店经销　湖南省新华印刷三厂印刷

787×1092 毫米　32 开　印张：6.25　字数：130,000
1991 年 12 月第 1 版　1998 年 4 月第 2 次印刷

ISBN7—5355—1377—8／G · 1372
定价：11.10元

"走向数学"丛書

陳省身題

作者简介

冯克勤，男，1941年生，天津宁河人。1968年中国科学技术大学研究生毕业，1973年在中国科学技术大学任教至今，教授。现任副校长和北京研究生院常务副院长，1979至1981年在美国作访问学者，后访问过德国、加拿大、前苏联、日本、瑞士、意大利、香港和台湾等地。

兼职有：中国数学会常务理事，《现代数学丛书》编委，《中国科学》、《科学通报》、《数学学报》、《代数集刊》和《数学年刊》编委，国务院学位委员会成员等。

科研方向为代数数论和代数编码理论，发表论文五十余篇，著作有：《分圆函数域》、《交换代数基础》、《代数数论入门》、《近世代数引论》、《初等数论讲义》、《射影几何趣谈》和《平方和》。译书多种。曾获中国科学院科技进步二等奖（1988），国家自然科学三等奖（1989）和第三届陈省身数学奖（1990）。

前　言

王　元

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，如果知道讨论的对象的具体背景，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支持，得以出版这套“走向数学”丛书，谨致以感谢.

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)，并且在自然数集合中可以作加法和乘法运算. 后来学习了负整数之后，在所有整数组成的集合{0，±1，±2，…}之中又可以作减法. 随后又学习了有理分数，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、分配律等)的任意集合，在数学上叫作域. 所以，在中学里我们已经学过三个域：有理数域、实数域和复数域. 而自然数集合与整数集合都不是域，因为除法在这些集合中不一定可行.

有理数域、实数域和复数域都是无限域，即每个域中都包含无限多个数. 这本小册子要向大家介绍的主要数学对象是有限域，即由有限个“数”组成的域.

首先遇到的问题是：有限域是否存在？事实上，由0和1组成的集合就可以作成一个域. 其中乘法与通常一样：$0\times0=1\times0=0\times1=0$，$1\times1=1$. 由于这个集合的非零元素只有1，除法自

然定义为$\frac{0}{1}=0,\frac{1}{1}=1$. 至于加法，我们象通常那样：0+0=0，1+0=0+1=1，但是规定 1+1=0(即 2=0). 而减法为 0−0=1−1=0，1−0=1，但是规定 0−1=1(即−1=1). 可以直接验证，集合{0,1}对于如此规定的四则运算满足通常的运算法则. 于是我们构作了一个二元域，即由两个元素组成的域. 这显然是最简单的有限域.

如果你学过一点初等数论的知识，那么你实际上已经接触过许多有限域了，也许你没有意识到这一点. 设 p 是一个素数，对于每个整数 a，我们用$[a]$表示模 p 同余于 a 的所有整数构成的集合，叫作 a 所在的一个模 p 同余类. 由于每个整数模 p 均同余于 $0,1,2,\cdots,p-1$ 当中的一个数，所以共有 p 个模 p 同余类：$[0],[1],\cdots,[p-1]$. 以 $\boldsymbol{F}_p$ 表示这 p 个同余类组成的集合(每个同余类$[a]$是集合 $\boldsymbol{F}_p$ 中的一个元素)，并且在 $\boldsymbol{F}_p$ 中如下自然地定义加减乘运算：

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

再根据同余式的性质，可知若$[a]$和$[b]$是模 p 两个同余类，并且$[b]\neq[0]$，则存在唯一的同余类$[c]$，使得$[a]=[b]\cdot[c]$，于是$\frac{[a]}{[b]}=[c]$. 这表明 $\boldsymbol{F}_p$ 中可以作除法. 因此 $\boldsymbol{F}_p$ 是由 p 个元素构成的有限域. 这样，对每个素数 p，我们均可作成一个 p 元有限域 $\boldsymbol{F}_p$. 当 $p=2$ 时，如此作成的 $\boldsymbol{F}_2$ 就是前面所述的二元域.

从 17 世纪起，费尔马(Fermat，1601—1665)，欧拉(Euler，1707—1783)，勒让得(Legendre，1752—1833)和高斯(Gauss，1777—1855)等许多大数学家研究数论. 他们得到同余式的许多性质，实质上也研究了 p 元有限域的许多性质. 第一个明确地讨论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). 读者或许知道他是群论的创始人，他在

1828 年写了论文“关于五次方程的代数解法问题”，利用方程根之间的置换特性，证明了五次和五次以上一般代数方程是根式不可解的，由此产生出群的概念. 1830 年，他还写了“关于数论”一篇论文. 在 p 元域的基础上，采用域扩张方法构作出全部可能的有限域. 结果表明：每个有限域的元素个数必为某个素数 p 的方幂 $p^n(n\geqslant 1)$. 而且对每个素数幂 p^n，本质上只有一个 p^n 元有限域. 所以后来，人们把有限域也叫作伽罗华域. 狄柯逊(Dickson)于 1901 年写了一本书“线性群和伽罗华域理论”，在此书中把有限域理论系统地叙述成现在的形式.

有限域当然具有每个域的公共性质. 但是，因为它们只具有有限多个元素，使得它们与我们所熟悉的无限域有很大的不同. 有限域有许多奇妙的性质，人们利用有限域的优美特性构作出具有各种对称性质的组合结构，如正交拉丁方、平衡区组设计、差集合、有限射影平面、相关性能和随机性能良好的序列等等，这些组合结构有效地应用于试验设计、通信系统等许多实际领域中. 特别是计算机技术蓬勃发展，离散数学和离散代数结构的地位愈加重要，有限域已成为许多工程技术人员不可缺少的数学工具.

另一方面，有限域理论本身也吸引了人们的广泛兴趣，成为世界许多优秀数学家施展自己才华的场所. 数学本身和实际应用领域不断提出关于有限域的大量数学问题，这些问题的解决或者有益于应用，或者推动数学的发展. 例如在本世纪 40 年代，法国数学家韦依(A. Weil)关于有限域上代数方程组的解数，提出一个著名的猜想. 为了解决这个猜想，人们创造了许多新的数学思想和工具，使代数几何与代数数论这两门古老的数学学科得到极大的发展. 在这个基础上，韦依猜想终于由比利时年轻数学家德林(Deligne)于 1974 年证明. 由于这项工作，德林得到了

国际数学界的最高奖赏——菲尔兹奖.还值得一提的是,近年来苏美等国的数学家把代数几何与代数数论的这些深刻理论用于编码通信领域,构作出性能优于前人的纠错码,提出了保密通信的新体制.这是世人交口称赞的数学理论与实际应用高水平结合的一个精彩的例子.

在这本小册子里,我们要向读者介绍有限域和它的某些应用.首先讲述有限域和它的优美特性.然后用有限域构作各种组合结构.我们也介绍有限域及其应用方面一些有趣的数学问题,有些问题至今还未解决.书中有一些习题供大家练习.限于篇幅和本丛书的宗旨,对于较高深的理论我们只能作一个粗略的描述.

本书只假定读者学过中学数学,并且懂得一点初等数论.所以问题的叙述和定理的证明都尽量作得通俗.我们也常常加一些注记,是为了使掌握更多代数知识(线性代数,近世代数)的人画龙点睛地明确事情的实质.在数学发展的历史长河和广阔天地里,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本身之美,数学应用的广泛,以及数学理论与实际应用的相互促进.

在本书即将定稿之时,美国宾州州立大学李文卿教授来华访问,介绍了近年来通信网络(Network theory)方面的发展,特别是现代数论在构作性能优良的通信网络方面的应用(包括李文卿本人的工作),引起作者极大的兴趣,并且促使作者在本书中增写了第三章,介绍用有限域构作通信网络的若干结果.因是仓促而就,文中论述的利用组合结构(差集合,m 序列)和有限域构作拉氏图的一些结果(即定理 3.4.2,3.4.5 和 3.5.1)只是记录下我们讨论的一些原始想法.我们希望在今后将用论文写成更完整的形式.

1988 年底，加拿大的林永康教授利用电脑证明了 10 阶有限射影平面的不存在性. 香港大学萧文强先生对此写了一篇介绍文章，刊登在台湾杂志《数学传播》(1990 年)离散数学专辑上. 现经作者和负责《数学传播》的台湾交通大学张镇华教授的慨然应允，作为附录转载于书末，我对他们的热情协助表示衷心谢意.

冯克勤

1990 年底于合肥

目　录

第一章　有限域

§1.1　来自初等数论的例子

我们在引言中说过，利用初等数论，对每个素数 p，可以构作出一个 p 元域 F_p. 在这节中我们利用初等数论更详细地讲述这些 p 元域和它们的性质，为今后讲述更一般的有限域增加些感性知识. 让我们先从初等数论的一些基本事实讲起.

初等数论的基本研究对象是自然数集合

$$N = \{0,1,2,3,\cdots\}$$

和整数集合

$$Z = \{0, \pm 1, \pm 2, \pm 3,\cdots\}.$$

整数集合 Z 中可以作加减乘三种运算，其中加法和乘法均有结合律和交换律，加法与乘法之间还有分配律. 但是 Z 中作除法并不总是可行的. 换句话说，设 a 和 b 为两个整数，其中 $b\neq 0$. 则 $\frac{a}{b}$ 不一定是整数. 如果 $\frac{a}{b}$ 是整数，我们称 b 整除 a，表示成 $b|a$.

否则，即若$\frac{a}{b}$不是整数，便称 b 不能整除 a，表示成 $b\nmid a$. 例如 $(-2)\mid 6, 2\nmid 3$，而 ± 1 可以整除任何整数，每个非零整数均可以整除 0，等等.

如果 $a,b\in\mathbf{Z}, b\neq 0, b\mid a$，我们称 b 是 a 的一个**因子**，a 叫作 b 的一个**倍数**. 每个非零整数 n 都有因子 ± 1 和 $\pm n$. 设 p 是一个大于 1 的正整数. 如果 p 的正因子只有 1 和 p，换句话说，p 不能写成两个正整数之积，而这两个正整数因子均小于 p，便称 p 为**素数**.

每一门学问都有几个最基本的结果作为这门学科的基石. 初等数论的基石是下面的算术基本定理，我们假定大家熟悉它，证明从略.

1.1.1 算术基本定理 每个大于 1 的正整数 n 均可写成有限个素数的乘积：

$$n = p_1 p_2 \cdots p_s.$$

并且若不计素因子 $p_1, \cdots, p_s$ 的次序，这个分解式是唯一的.

如果我们把相同的素因子收集在一起，则上式可以写成

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r},$$

其中 $p_1, \cdots, p_r$ 是彼此不同的素数，而 $a_i \geqslant 1 (1 \leqslant i \leqslant r)$. 这叫作正整数 n 的**标准分解式**.

初等数论的另一块基石，便是(欧几里德)除法算式.

1.1.2 除法算式 设 $a,b\in\mathbf{Z}, b>0$，则存在唯一的整数 q 和 r，使得 $a = qb + r$，并且 $0 \leqslant r < b$.

我们也假定读者熟悉这个除法算式而不加证明(虽然证明是很容易的). 只想再指出，如果 a 也是正整数，那么除法算式中