

有限域及其应用



[有限域及其应用_下载链接1](#)

著者:冯克勤

出版者:大连理工大学出版社

出版时间:2011-7

装帧:

isbn:9787561157879

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，《有限域及其应用》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．

作者介绍:

冯克勤，清华大学教授。1941年出生，1968年中国科学技术大学数学系研究生毕业。1973至2000年在中国科学技术大学数学系和研究生院(北京)任教，2000年后到清华大学数学系工作。从事代数数论和代数编码理论研究。出版专著《分圆函数域》、《代数数论简史》等，出版大学生和研究生教材《整数与多项式》、《近世代数引论》、《交换代数基础》、《代数数论》和《代数与通信》等，主编丛书《走向数学》。..

目录:《有限域及其应用》

续编说明1

编写说明3

引言5

理论部分

一 来自初等数论的有限域1

1.1 整除性和同余性1

习题14

1.2 p 元有限域15

习题30

二 一般有限域31

2.1 域上的多项式环31

习题43

2.2 构造一般有限域43

习题55

三 有限域上的函数57

3.1 广义布尔函数57

习题61

3.2 幂级数61

习题78

3.3 加法特征和乘法特征79

习题92

3.4 高斯和与雅可比和92

习题104

四 有限域上的几何106

4.1 有限仿射几何107

习题117

4.2 有限射影几何118

习题128

4.3 平面仿射曲线和平面射影曲线128

习题135

五 有限域中解方程136

5.1 谢瓦莱-瓦宁定理:解的存在性136

习题150

5.2 多元二次方程150

习题167

5.3 费马曲线和阿廷-施莱尔曲线168

习题179

5.4 韦依定理179

习题189

应用部分

六 组合设计191

6.1 正交拉丁方191

习题205

6.2 区组设计205

习题212

6.3 阿达玛方阵212

习题218
七 纠错码219
7.1 纠错码220
习题229
7.2 线性码230
习题238
7.3 汉明码、多项式码和里德-马勒二元线性码240
习题255
7.4 循环码256
习题274
八 密码和信息安全275
8.1 凯撒大帝的密码277
8.2 m序列与图论——周游世界和一笔画282
习题293
8.3 构造m序列(并圈方法)293
习题303
8.4 公钥体制303
8.5 密钥的分配、更换和共享315
8.6 椭圆曲线算法329
结束语339
• • • • • (收起)

[有限域及其应用 下载链接1](#)

标签

数学

代数

走向数学丛书

科普

Math

评论

数学出身的人写的书一般都思路清晰～

同余类是有限域的建筑模块；从费马小定理到欧拉定理之间的推广；二元一次不定方程的完备求解。

这本书选题非常棒，填补了一般代数书的空白

有限域是伽罗华贡献给人类的永恒的礼物

[有限域及其应用_下载链接1](#)

书评

[有限域及其应用_下载链接1](#)