

<<有限域及其应用>>

图书基本信息

书名：<<有限域及其应用>>

13位ISBN编号：9787561157879

10位ISBN编号：7561157878

出版时间：2011-7

出版时间：大连理工大学出版社

作者：冯克勤

页数：343

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<有限域及其应用>>

### 内容概要

在这本《有限域及其应用》里，编者冯克勤、廖群英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，冯克勤、廖群英所著的《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。

## <<有限域及其应用>>

### 作者简介

1941年10月生于天津市宁河县，1964年中国科技大学数学系毕业，1968年中国科技大学数论代数方向研究生毕业，1973—2000年在中国科技大学任教，1985年任教授和博士生导师。

2000年至今任清华大学数学科学系教授。

研究方向为代数数论和在编码及信息安全中的应用。

获1991年陈省身数学奖等奖项。

现为International

Journal of Number

Theory, 《中国科学(数学卷)》等刊物编委：中科院信息安全国家重点实验室、北京大学国际数学研究和人才培养基地、复旦大学应用数学实验室、南开大学陈省身数学研究所等单位学术委员会委员。

1974年7月生于四川宜宾，1996年四川师范大学数学系毕业，1999年四川师范大学硕士研究生毕业，1999年至今在四川师范大学数学学院任教。

期间2002—2005年于四川大学师从孙琦教授攻读博士研究生，2007—2009年于清华大学与冯克勤教授合作从事博士后研究工作，2006年任副教授和硕士生导师。

研究方向为代数数论和在编码及信息安全中的应用。

## <<有限域及其应用>>

### 书籍目录

续编说明

编写说明

引言

理论部分

一 来自初等数论的有限域

1.1 整除性和同余性

习题

1.2  $P$ 元有限域

习题

二 一般有限域

2.1 域上的多项式环

习题

2.2 构造一般有限域

习题

三 有限域上的函数

3.1 广义布尔函数

习题

3.2 幂级数

习题

3.3 加法特征和乘法特征

习题

3.4 高斯和与雅可比和

习题

四 有限域上的几何

4.1 有限仿射几何

习题

4.2 有限射影几何

习题

4.3 平面仿射曲线和平面射影曲线

习题

五 有限域中解方程

5.1 谢瓦莱-瓦宁定理:解的存在性

习题

5.2 多元二次方程

习题

5.3 费马曲线和阿廷-施莱尔曲线

习题

5.4 韦依定理

习题

应用部分

六 组合设计

6.1 正交拉丁方

习题

6.2 区组设计

习题

<<有限域及其应用>>

6.3 阿达玛方阵

习题

七 纠错码

7.1 纠错码

习题

7.2 线性码

习题

7.3 汉明码、多项式码和里德-马勒二元线性码

习题

7.4 循环码

习题

八 密码和信息安全

8.1 凯撒大帝的密码

8.2 M序列与图论——周游世界和一笔画

习题

8.3 构造M序列(并圈方法)

习题

8.4 公钥体制

8.5 密钥的分配、更换和共享

8.6 椭圆曲线算法

结束语

<<有限域及其应用>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>