# <<代数学基础与有限域>>

#### 图书基本信息

书名: <<代数学基础与有限域>>

13位ISBN编号: 9787040192308

10位ISBN编号:7040192306

出版时间:2006-7

出版时间:高等教育出版社

作者:林东岱

页数:187

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

# <<代数学基础与有限域>>

#### 前言

有理数域、实数域和复数域都是我们比较熟悉的数域,这些域有个共同的特点,就是它们的元素 个数都是无限的。

我们这本书要向大家介绍的有限域,则只含有限多个元素。

有限域是现代代数学的重要分支之一。

有限域的理论最早可追溯到费尔马(FERMAT 1601—1665)、欧拉(EULER 1707—1783)和高斯 (GAUSS 1777—1855),他们实质研究了一种称之为有限素域的有限域。

有限域的一般理论则主要是从伽罗华(GALOIS 1811—1832)的工作开始。

1830年,他在p元有限域的基础上,采用域扩张方法构造出全部可能的有限域,证明了每个有限域的元素个数一定是某个素数的幂,而且对每个素数幂,本质上也只有一个相应的有限域。

## <<代数学基础与有限域>>

#### 内容概要

本书系统介绍了有限域的基本内容和基本知识。

全书共分为七章,第一章介绍代数学的基础知识,第二章介绍有限域的结构,第三章介绍有限域上的 多项式,第四章介绍有限域上的离散对数问题,第五章介绍有限域上的椭圆由线,第六章介绍伪随机 序列,第七章介绍有限域在编码学和密码学等方面的应用。

每章的后面均附有习题,有些习题是对正文内容的补充,以供学生复习巩固书中所学内容。

本书可作为数学、信息科学或其他相关专业的研究生教材,也可作为相关领域中的教学、科研人员以及工程技术人员的参考书。

## <<代数学基础与有限域>>

#### 书籍目录

第一章代数学基础 1.1 群 1.2 环与理想 1.3 多项式环 1.4 域和扩域 习题第二章 有限域的结构 2.1 有限域的特征性质 2.2 不可约多项式的根 2.3 迹 , 范数和基 2.4 单位根和割圆多项式 2.5 有限域元素的表示 习题第三章 有限域上的多项式 3.1 多项式的阶和本原多项式 3.2 不可约多项式 3.3 不可约多项式的构造 3.4 有限域上多项式因式分解 习题第四章 有限域上的离散对数问题 4.1 有限域上的离散对数问题 4.2 Shanks算法 4.3 Pohlig-Heliman算法 4.4 Pollardp方法 4.5 指数演算方法 习题第五章 有限域上的椭圆曲线 5.1 椭圆曲线上的群结构 5.2 椭圆曲线的射影坐标表示 5.3 椭圆曲线上的有理点 5.4 椭圆曲线密码学 习题第六章 伪随机序列 6.1 二元序列的伪随机性 6.2 线性移位寄存器序列 6.3 Berlekamp Massey算法 6.4 线性递归-阵列 习题第七章 有限域的应用 7.1 纠错码简介 7.1.1 线性码 7.1.2 循环码 7.2 有限域与分组密码 7.2.1 分组密码概述 7.2.2 AES分组密码算法 习题参考文献索引

# <<代数学基础与有限域>>

#### 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