<<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

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。

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。

书籍目录

版权说明