

<<置换多项式及其应用>>

图书基本信息

书名：<<置换多项式及其应用>>

13位ISBN编号：9787560338118

10位ISBN编号：7560338119

出版时间：2012-10

出版时间：哈尔滨工业大学出版社

作者：孙琦，万大庆 编著

页数：86

字数：70000

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>

<<置换多项式及其应用>>

内容概要

本书系统地介绍了置换多项式的产生、发展和理论，并且着重介绍了它在现代科学中的广泛应用。论述深入浅出，简明生动，读后有益于提高数学修养，开阔知识视野。

本书可供从事这一数学分支相关学科的数学工作者、大学生以及数学爱好者研读。

<<置换多项式及其应用>>

书籍目录

第1章 剩余类环的置换多项式

1. 从完全剩余系谈起
2. 置换多项式的判别与构造
3. 迪克森多项式
4. 置换谱

第2章 置换多项式的应用举例

1. 密码系统简介
2. 迪克森多项式与RSA系统
3. 置换有理函数与RSA系统
4. 置换多项式与一致分布

第3章 有限域上的置换多项式

1. 置换多项式的判别
2. 置换多项式的构造
3. 置换多项式的群
4. 例外多项式
5. 完备映射

附录 代数基础

1. 初等数论
2. 群, 环, 域
3. 有限域
4. 多项式

参考文献

外国人名索引

编辑手记

<<置换多项式及其应用>>

章节摘录

版权页：插图：即 f 保持 G 的运算，则称 f 是群 G 到群 H 的一个同态。

如果 f 是满射，即 H 中每一元都是 G 中某一元的象，则称 f 是满同态；如果 f 是单射，即当 $a \neq b$ 时， $f(a) \neq f(b)$ ，则称 f 是单同态，既满又单的同态称为同构，此时 G 和 H 称为同构的群，当 $G=H$ 时， f 称为 G 的自同态。

如果对所有 $a \in G, h \in H$ (H 为 G 的子群)，都有 $aha^{-1} \in H$ ，则称 H 为 G 的正规子群。

子群 H 在 G 中是正规的当且仅当任一左陪集 aH 和右陪集 Ha 相等。

这样，对正规子群，陪集之间可以定义运算 $(aH)(bH) = (ab)H$ 在这种运算下，所有 H 的陪集作成一群，记为 G/H ，称为 G 关于 H 的商群。

$|G/H| = [G:H]$ 。

定义同态 $f: G \rightarrow G/H, f(a) = aH (a \in G)$ ， f 称为 G 到商群 H 的标准同态。

(2) 置换群。

设 n 是一个正整数，如果 a_1, \dots, a_n 是 $1, 2, \dots, n$ 的一个排列，则称为一个 n 元置换。

置换可以理解为把 i 变换成 a_i ，因此是 $\{1, 2, \dots, n\}$ 到自身的一个一一映射，两个置换的复合也是一个置换，所有 n 元置换在复合运算下作成一群，称为 n 元置换群，常用 S_n 表示。

S_n 的元素个数是 $n!$

。

<<置换多项式及其应用>>

编辑推荐

《丛书(第3辑):置换多项式及其应用》由哈尔滨工业大学出版社出版。

<<置换多项式及其应用>>

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>