**中山大学研究生课程教学大纲**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 中文名称 | 有限域基础 | | | 课程编号 | | DCS5230 | |
| 英文名称 | Foundations and Applications of Finite Fields | | | | | | |
| 总学时 | 36学时 其中实验课：0 学时 | | | | | 学分 | 2 |
| 开课院系 | 计算机学院 | 课程负责人 | 韦宝典 | 课程性质 | | □必修 ☑选修 | |
| 授课团队 |  | | | | | | |
| 课程类别 | □公共课 □专业基础课 □专业方向课  □专业技术实践课 ☑选修课 | | | | | | |
| 授课方式 | 面授课程 | | 授课语言 | | 中文 | | |
| 考核方式 | 考察（展示+大报告） | | | | | | |
| 先修课  程要求 | 线性代数、离散数学 | | | | | | |
| 教学目标（100字以内）  为计算机等相关专业研究生开设有限域课程，使学生能够掌握有限域理论的基本概念、基本内容和基本应用，为学习后继课程，如编码和密码学等，打下必备数学基础，培养学生的抽象思维能力、逻辑推理能力和自学能力。 | | | | | | | |
| 课程简介（教学内容及基本要求）  本课程授课内容分为四部分：相关的基础数学知识、群的概念和性质、环的概念和性质、有限域的性质和构造，具体描述如下。  一、基础数学：初等数论  1、线性同余方程 (1) 有解的充要条件；(2) (扩展)欧几里得算法。  2、线性同余方程组 (1) 有解的充要条件；(2) 中国剩余定理CRT。  思政：用中国古人在数学上的贡献激发学生的爱国主义  3、二次同余方程组 (1) 欧拉函数、欧拉定理、欧拉准则，以RSA、Rabin、快速RSA算法为应用例子 (2) Legendre符号与Jacobi符号 | | | | | | | |
| 二、群  1、基本概念 (1) 定义与例子 (2) Abel群 (3) 元素的逆 (4) 元素幂运算及性质 (5) 同态与同构 思政：年轻先驱事例激励学生勇于创新。  2、子群 (1)定义、例子及相互关系 (2)子群判定 (3)陪集的定义及性质  3、循环群  三、环与整环  1、环 (1) 环的定义和例子 (2) 子环与扩环及相应例子 (3) 环的整除性  2、环的性质 (1) 加法消去律 (2) 环的同态、同构  思政：借同构的思想引导学生在学习科研生活中力求去繁求简的原则  3、整环 (1) 零因子和乘法消去律、例子 (2) 整环的分解域  4、理想：定义、性质及例子 5、剩余类环  四、有限域  1、概念与性质 (1) 域、子域与扩域的概念与例子，剩余类域  (2)主要性质1)乘法群与域的大小2)存在性与唯一性3)域的特征与自同构  思政：借有限域的精确无误差特性培养学生科学严谨一丝不苟的精神  2、有限域的构造：不可约多项式  3、多项式的因式分解 (1) Mobius变换域反变换 (2) Berlekamp算法  4、Frobenius自同构  5、特殊多项式：特征多项式、极小多项式、本原多项式  6、迹和范及其在二次方程求解中的应用  7、基：多项式基、对偶基与自对偶基、正规基  思政：课程结束之际指导学生正确看待付出与收获的关系 | | | | | | | |
| 教材及主要参考书目、文献与资料 | 教材：1. Zhe-xian Wan, Lectures on Finite Fields and Galois Rings, World Scientific Publishing Co. Pte. Ltd, 2006  主要参考书：2. Robert J.McElice;Finite Fields for Computer Scientists and Engineers，Boston: Kluwer Academic Publishers, 1987 | | | | | | |

注：每门课程都应填写此表。