代数结构 课程教学大纲

Course Outline

<table>
<tr><td colspan="6">课程基本信息（Course Information）</td></tr>
<tr><td>课程代码
（Course Code）</td><td>MA150</td><td>*学时
（Credit Hours）</td><td>48</td><td>*学分
（Credits）</td><td>3</td></tr>
<tr><td rowspan="2">*课程名称
（Course Title）</td><td colspan="5">（中文）代数结构</td></tr>
<tr><td colspan="5">（英文）Algebraic Structures</td></tr>
<tr><td>*课程性质
（Course Type）</td><td colspan="5">选修课</td></tr>
<tr><td>授课对象
（Target Audience）</td><td colspan="5">致远学院 ACM 班</td></tr>
<tr><td>*授课语言
(Language of Instruction)</td><td colspan="5">中文</td></tr>
<tr><td>*开课院系
（School）</td><td colspan="5">电信学院计算机系</td></tr>
<tr><td>先修课程
（Prerequisite）</td><td colspan="5">离散数学，线性代数</td></tr>
<tr><td>授课教师
（Instructor）</td><td colspan="2">刘胜利</td><td>课程网址
(Course Webpage)</td><td colspan="2"></td></tr>
<tr><td>*课程简介（Description）</td><td colspan="5">（中文 300-500 字，含课程性质、主要教学内容、课程教学目标等）
“代数结构”一课是抽象代数领域的最基本课程。在本课程中，我们将学习基本的代数结构，如群、环、域等，以及这些代数结构上的映射，包括群同态、环同态等。本课程中的理论和技术不仅在数学领域有直接的应用，还广泛的应用于物理、工程、计算机科学中。特别地，它是密码学和编码学这两大主题的数学基石。
通过本课程的学习，使学生初步掌握基本且系统的代数知识和抽象严谨的代数方法，进一步熟悉和掌握代数处理问题的方法；进一步提高抽象思维能力和严格的逻辑推理能力；进一步理解具体和抽象、特殊与一般、有限与无限的辩证关系。结合 2002、2012 两界图灵奖获得者所提出的 RSA 加密算法、Goldwasser-Micali 加密算法，详细介绍算法所基于的代数结构，将所学理论直接应用于具体的算法中，有效地理解算法正确性及安全性所基于的代数理论。培养学生独立提出问题、分析问题和解决问题的能力，培养学生的数学基本素质，同时为今后的专业学习奠定基础。</td></tr>
<tr><td>*课程简介（Description）</td><td colspan="5">（英文与中文内容对应） “Algebraic Structure” is a basic course in the area of abstract algebra. In this course, we study fundamental algebraic structures, namely groups, rings, fields etc, and maps between these structures. The theory and techniques introduced in this course are not only used in many areas of mathematics, but also applied in the areas of physics, engineering and computer science. Specifically, it serves as an essential mathematical foundation course for cryptography and coding theory.
Via this course, students will learn the fundamental concepts and theory of Abstract Algebra and</td></tr>
</table>

	know how to apply the algebraic method to problems in computer science. Combined with the algorithms proposed by the 2002 and 2012 Turing Winners, i.e, RSA algorithm and Goldwasser-Micali algorithms, we give a detailed analysis of the algebraic structures underling the algorithms and present the algebraic principles which serves as the correctness and security of the algorithms. This course promotes the ability of students to propose, analyze and solve problems based on the knowledge of abstract algebra. It is a basement course for the professional courses in computer science.
课程教学大纲（course syllabus）	
*学习目标(Learning Outcomes)	**课程学习目标：** 要求学生熟练掌握群、环、域的基本理论和方法。包括：群、循环群、正规子群、商群、群同态、群的同构定理、群的直和分解、群在集合上的作用及西罗定理；环、理想、商环、环同态、环的同构定理；域、域的扩张、分裂域、域的构造以及尺规作图不能问题的证明等。利用所学习的理论知识了解计算机学科的算法中涉及的代数结构，初步理解密码领域的 RSA，Goldwasser- Micali 加密算法，以及通信领域中的纠删编码译码算法。 Learning Outcomes 1. The basic concepts and theorems of group, ring and field, including group, cyclic group, normal group, quotient group, group homomorphism, direct group, groups on sets, the isomorphism theorems, Sylow Theorems; 2. Ring, ideal, quotient ring, ring homomorphism, the isomorphism theorems, Integral Domain, Unique Factorization Domain, Principal Domain, Euclidean Domain; 3. Field, Field extension, splitting field, construction of fields, and the impossibility of classical problem of constructions with ruler and compass, Trisecting the angle, Duplicating the cube, Squaring the circle. 4. The RSA (2002 Turing Winner) algorithm and Goldwasser-Micali (2012 Turing Winner) algorithm. 5. Understanding algebraic structure under algorithms in computer science. **课程主要内容（教学大纲）** **第一章 群** (1) 基本概念及实例 群、子群、循环群； 对称即群：平面上的运动群、数域的对称，多项式的对称； 置换群：置换群概念及实例。 (2) 群的同构定理 陪集、正规子群、商群； 群的同态及分解定理； 群的第一同构定理； (3) 群的第二同构定理； (4) 群的第三同构定理。

(5) 群在集合上的作用，正规作用，共轭作用，左乘等。Faithful 作用，传递作用。Orbit-Stablizer 定理、Orbit-Counting 定理(Burside 引理)，及串珠染色问题的解决。Sylow-p 群的定义和性质。西罗定理：西罗第一定理(sylow p 群的存在性)、西罗第二定理(sylow p 群的个数)、西罗第三定理(sylow p 群的关系)。

(6) 群的直积：群的内直积、群的外直积、及其两者之间的关系

(7) 有限交换群的结构

(8) 结构最简单的群：循环群的阶及其元素的级；

(9) 有限 p 群的分解；

(10) 有限交换群的直和分解。

第二章 环

(1) 基本概念及实例

环、子环、整环、除环及域；

环的特征及其性质；

环上的广义分配律。

(2) 环的同构定理

环同态、环同态的核、及其性质；

理想，集合生成的理想、理想的性质；

商环的定义、与环同态及其核间的关系；

环的分解定理；

环的第一同构定理；

环的第二同构定理；

环的第三同构定理。

环的一一对应定理

(3) 素理想与极大理想

素元、不可约元及其关系；

素理想与极大理想的定义；

多项式环、多项式除算法及剩余定理；

惟一分解环、主理想环、Euclid 环及其性质

分式环与分式域。

不可约多项式、本原多项式

第三章 域

1. 域的基本概念；
2. 域的扩张；

代数元及代数扩张；

3. 极小多项式
4. 分裂域及其同构扩张定理；

分裂域的应用：尺规做图不能问题（三等分角、立方倍积、化圆为方）

第四章 应用

2002 年度图灵奖获得者 Rivest, Shamir, Adleman 所提出的 RSA 算法；
2012 年度图灵奖获得者 Goldwasser 和 Micali 所提出的 GM 概率加密算法。

Course Teaching Outline

Part I : Group

1） Basic concept and examples

Group, subgroup and cyclic group.

Group is symmetry: Dihedral Group, symmetry of numerical field, and polynomials.

Permutation groups

2) Isomorphism Theorem of group

Coset, Normal group and quotient group.

Group homomorphism and Factorization Theorem.

The 1st Isomorphism Theorem

The 2nd Isomorphism Theorem

The 3rd Isomorphism Theorem

3) Groups Acting on Sets

Groups acting on sets: regular acting, conjugate acting, left multiplication, faithful acting, transitive acting , etc.

Orbit-Stablizer Theorem.

Orbit-Counting (Burside Lemma) theorem and applications.

Sylow Theorem: the 1st, 2nd, 3rd Theorems.

4) External and Internal Direct Products

External and Internal Direct Products and the connections between them.

5) Structure of finite abelian groups.

The simplest group: cyclic groups and their orders, the order of an element.

Factorization of finite p-group.

Direct Products of finite abelian group

Part II: Ring

1) Basic concept and examples

Ring, subring, integral ring, division ring, and field.

Character of Ring and its property.

General distribution law of Ring.

2) Isomorphism Theorem of Ring

Ring homomorphism, kennel of ring homomorphism and its properties.

Ideals, ideals generated by subset, and the properties of ideals.

Quotient Ring and relations between kennel of ring homomorphism and ideals.
Factorization Theorem of Rings.
The 1st Isomorphism Theorem
The 2nd Isomorphism Theorem
The 3rd Isomorphism Theorem
The one-one corresponding Theorem.

3) Prime ideals and maximal ideals.
Prime, irreducible and their relations.
Definition of Prime ideals and maximal ideals.
Polynomial ring, division between polynomials and remaiders.
Unique Factorization Ring, Principal Ring, Euclid Ring and their properties.
Fraction Ring and field.
Irreducible polynomials and primitive polynomials.

Part III: Field

Basic concept and examples
Field extension
Algebraic and Algebraic extension.
Minimal polynomials
Split field and the isomorphic extension theorem.
Application and split filed: the impossible question with ruler and compasse

Part IV: Applications

1) RSA algorithm which was proposed by Turing Winners of 2002, Rivest, Shamir, Adleman;
2) GM probabilistic encryption algorithm which was proposed by Turing Winners of 2012, Goldwasser and Micali.

*教学内容、进度安排及要求
(Class Schedule &Requirements)

教学内容	学时	教学方式	作业及要求	基本要求	考查方式
群的定义、性质、实例，群的等价定义；子群的定义，性质、实例。构造新子群的方法：子群的交，集合生成子群。	3	课堂教学	P5，习题1-1题目：4,8 P16，习题1-2题目：5, 12， 13，16	群的基本概念，群及子群的判定	作业

	教学重点：有限群的实例，如 Zp*, Z_N*, U_N；为以后引入 RSA 算法和 GM 概论加密算法打下基础。					
	循环群定义，性质、实例。引入元素的级和群的阶的概念，以及如何求元素级。 群的同构，循环群的两种同构形式：有限循环群和无限循环群。	3	课堂教学	P25，习题 1-3 题目：5, 6, 7, 8, 18, 19	群的同构，循环群的同构形式	作业
	对称即群：平面上的运动群、数域的对称，多项式的对称；	3	课堂教学	P32，习题 1-4 题目：3, 4,6 P40，习题 1-5 题目：1, 5, 12	群所反馈的对称性	作业
	置换群，n 阶对称群定义及性质	3	课堂教学	自拟同构题目证明：如果$N=n_1\cdot n_2$，且$\gcd(n_1, n_2)=1$，那么 $\Zz_N^*\cong \Zz_{n_1}^*\times \Zz_{n_2}^*$。	置换群	作业
	陪集、Lagrange 定理及应用：Euler 定理，Fermat 定理。2002 年度图灵奖获得者 Rivest, Shamir, Adleman 所提出的 RSA 算法；	3	课堂教学	P54. 习题 1-6 题目：5.(1)(4), 12, 24, 25	陪集, Lagrange 定理	作业
	正规子群、商群；群的同态	3	课堂教学	P.71 习题 2-1：1，8，11，12，20，22	正规子群，商	作业

	及分解定理；群的第一同构定理；群的第二，三同构定理；				群，群的三个同构定理	
	子群和商群间的一一对应，以及结构的相似性。有限交换群的性质：素阶循环群的存在性；对于群阶的任一因子，都存在阶为该因子的子群。	3	课堂教学	P.79 习题 2-2：2，5，6，9，10，11	有限交换群中的子群	作业
	群在集合上的作用：正规作用，共轭作用，左乘等。Faithful 作用，传递作用。Orbit-Stablizer 定理、Orbit-Counting 定理 (Burside 引理)，及串珠染色问题的解决。			习题 2-3：1，6，7，16，18， 19	群在集合上的作用	作业
	西罗定理：西罗第一定理 (sylow p 群的存在性)、西罗第二定理 (sylow p 群的个数)、西罗第三定理 (sylow p 群的关系)。	3	课堂教学	P.104 习题 2-5：1, 3, 4, 6。	西罗的三个定理	作业
	群的直积：群的内直积、群的外直积及其	3	课堂教学	P.111 习题 2-6：1, 2, 3, 4， 6	群的直积及有限交换	作业

	关系 有限交换群的结构 结构最简单的群：循环群的阶及其元素的级；有限 p 群的分解； 有限交换群的直和分解。				群的直积分解	
	环、子环、整环、除环及域； 环的特征及其性质； 环上的广义分配律。 环同态、环同态的核、及其性质；理想，集合生成的理想、理想的性质；商环的定义、与环同态及其核间的关系；	3	课堂教学	p.119: 习题3-1: 1, 4, 17, 18. P. 129: 习题3-2: 2, 9.	环的基本概念，理想，环同态	作业
	环的分解定理； 环的第一同构定理； 环的第二同构定理； 环的第三同构定理。 环的一一对应定理　素元、不可约元及其关系；	3	课堂教学	page 138: 习题 3-3: 9,13,17. page 147: 习题 3-4: 5,7(2)(3).	环同态的三个同构定理	作业
	素理想与极大理想的定义； 多项式环、多项式除算法及剩余定理；	3	课堂教学	Page. 164，习题 4-1：5 Page. 181，习题 4-3：1(4)(6)，19 Page. 190，习题 4-4：	具有不同性质的环	作业

	惟一分解环、主理想环、Euclid 环及其性质； 分式环与分式域；			1，7		
	域的基本概念； 域的扩张； 代数元及代数扩张；	3	课堂教学	Find a splitting field for $f(x)=x^{2}+1$ over Z_{3} and the corresponding extension degree.	域的基本概念	作业
	极小多项式分裂域及其同构扩张定理； 分裂域的应用：尺规做图不能问题（三等分角、立方倍积、化圆为方）	3	课堂教学	Construct a finite field with 64 elements.(hint: find a splitting field over Z_{p}.)	域的知识的应用	作业
	2002 年度图灵奖获得者 Rivest, Shamir, Adleman 所提出的 RSA 算法；通信中的纠删码的编码和译码 2012 年度图灵奖获得者 Goldwasser 和 Micali 所提出的 GM 概率加密算法	3	课堂教学	复习	代数结构在算法中的应用	作业

	……					
*考核方式 (Grading)	综合成绩=30%作业成绩+70%期末考试成绩					
*教材或参考资料 (Textbooks & Other Materials)	1. 韩士安，林磊，``近世代数''，科学出版社 2. Robert B. Ash：Abstract Algebra: The Basic Graduate Year 3. Slides available at ftp://ftp.cs.sjtu.edu.cn/liu-sl/代数结构					
其它 （More）						
备注 （Notes）						

备注说明：

1．带*内容为必填项。

2．课程简介字数为 300-500 字；课程大纲以表述清楚教学安排为宜，字数不限。