**Course Introduction:**

 “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.

**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

1. 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

1. 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.

1. External and Internal Direct Products

 External and Internal Direct Products and the connections between them.

1. 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.

1. 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.

1. 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 *com-passes*

**Part IV: Applications**

RSA algorithm which was proposed by Turing Winners of 2002, Rivest, Shamir, Adleman；

GM probabilistic encryption algorithm which was proposed by Turing Winners of 2012, Goldwasser and Micali.

**课程简介**

“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，以及这些代数结构中的映射，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。

**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。

* + 1. 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；

群的第二同构定理；

群的第三同构定理。

* + 1. 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)。
		2. 群的直积：群的内直积、群的外直积、及其两者之间的关系
		3. 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。

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；

1. 极小多项式
2. 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。