上海交通大学　致远学院　2015 年秋季学期

《代数结构》课程教学说明

一. 课程基本信息

1. 开课学院（系）：致远学院
2. 课程名称:《代数结构》 (Algebraic Structures 英文名)
3. 学时/学分：48 学时/ 3 学分
4. 先修课程：离散数学，线性代数
5. 上课时间：每周周一 10:00-12:30
6. 上课地点：东下院 204
7. 任课教师：刘胜利 slliu@sjtu.edu.cn
8. 办公室及电话：34204405
9. 助教：吕林，lvlin3896@qq.com
10. Office hour：每周三上午 10:00-12:00，电院群楼 3-429 或者 3-414

二. 课程主要内容（如何可以，请提供中英文）

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;
群的第二同构定理;
群的第三同构定理。

(3) 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)。

(4) 群的直积：群的内直积、群的外直积、及其两者之间的关系

(5) 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；
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。

三. 课程教学进度安排（如何可以，请提供中英文）

	教学内容	教学形式	作业
第 1 周	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。 教学重点：有限群的实例，如 Zp*, Z_N*, U_N；平方剩余群 QR_p, QR_N，为以后引入 RSA 算法和 GM 概论加密算法打下基础。	课堂教学	P5，习题1-1题目：4，8 P16，习题1-2题目：5，12， 13，16
第 2 周	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。	课堂教学	P25，习题 1-3 题目：5，6，7，8，18，19
第 3 周	对称即群：平面上的运动群、数域的对称，多项式的对称；	课堂教学	证明：如果 $N=n_1\cdot n_2$，且 $\gcd(n_1, n_2)=1$，那么 $\Zz_N^*\cong \Zz_{n_1}^*\times \Zz_{n_2}^*$。 P32，习题 1-4 题目：3, 4,6 P40，习题 1-5 题目：1, 5, 12
第 4 周	国庆放假		
第 5 周	置换群，n 阶对称群定义及性质	课堂教学	P54. 习题 1-6 题目：5.(1)(4), 12, 24, 25
第 6 周	陪集、正规子群、商群；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；	课堂教学	P.71 习题 2-1：1，8，11，12，20，22
第 7 周	群的同态及分解定理；群的第一同	课堂教学	P.79 习题 2-2：2, 5,

	构定理；群的第二，三同构定理；		6，9，10，11
第 8 周	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。	课堂教学	习题 2-3：1，6，7，16，18， 19
第 9 周	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。	课堂教学	P.104 习题 2-5：1, 3, 4， 6。 补充题： Group G acts on set X. Let $G(x)$ denote the stabilizer of $x\in X$. Prove: If $y=ax$ for $a\in G, x,y\in X$, then $G(y)=aG(x)a^{-1}$.
第 10 周	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)。	课堂教学	P.111 习题 2-6：1, 2, 3, 4， 6
第 11 周	群的直积：群的内直积、群的外直积及其关系 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。	课堂教学	待定
第 12 周	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；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； 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；	课堂教学	待定

	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 13 周	域的基本概念； 域的扩张； 代数元及代数扩张； 极小多项式	课堂教学	待定
第 14 周	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）	课堂教学	待定
第 15 周	2002 年度图灵奖获得者 Rivest, Shamir, Adleman 所提出的 RSA 算法；	课堂教学	待定
第 16 周	2012 年度图灵奖获得者 Goldwasser 和 Micali 所提出的 GM 概率加密算法。	课堂教学	待定
17-18 周	答疑及考试		

四. 课程考核方式及说明

30%为平时成绩（作业，课堂表现等）
70%为考试成绩

五. 教材与参考书

《近世代数》，韩士安 林磊著 科学出版社

Abstract Algebra: The Basic Graduate Year， Robert B. Ash，**电子版，可下载**