中国科学院研究生院

数学学科 硕转博资格考试综合笔试

考试大纲

二级学科：应用数学

考试科目：计算机数学　　考试时间：180 分钟

考试形式： 应用数学专业密码学和数学机械化方向的硕转博资格考试综合笔试试卷涵盖了研究生课程《代数学基础》、《纠错码》、《密码学》、《符号计算》、《计算代数几何》及其相关内容。《代数学基础》必做，另外至多选答三门，合计 150 分的试题解答。试卷满分为 150 分。

一、考试内容

（一）代数学基础（60 分）

1. 群（置换群，子群，群同态，群作用，Sylow 定理，有限生成阿贝尔群的结构）
2. 环（理想，主理想整环，欧几里德整环，局部化）
3. 商环，素理想，极大理想
4. 域（代数数，代数扩域，Galois 理论）
5. 代数簇，不可约代数簇，希尔伯特零点定理
6. 希尔伯特多项式

（二）纠错码（30 分）

1. 有限域，线性码
2. 循环码，BCH 码
3. Reed-Solomon 码
4. Reed-Muller 码
5. 码的参数界

（三）密码学（30 分）

1. 古典密码
2. 熵，熵的基本性质
3. 分组密码，DES，AES
4. RSA，大数分解，二次剩余
5. ElGamal，离散对数，ECC（椭圆曲线）

（四）符号计算（30 分）

1. 长整数计算与带余除法
2. 模运算，中国剩余定理和算法，多项式的赋值和插值
3. 一元多项式的结式与子结式
4. 多项式的最大公因子
5. 多项式的因式分解

（五）计算代数几何（30 分）

1. Groebner 基的基本性质和计算
2. 计算多项式理想的交和饱和理想
3. 代数簇的维数和仿射维数定理
4. 多元多项式的特征列
5. 几何定理证明

二、参考书目

[1] 陈玉福，计算机代数讲义(中国科学院研究生院教材)，高等教育出版社，2009.

[2] D. Cox, J. Little and D. O'Shea. *Ideals. Varieties, and Algorithms.* Springer, 2015.

[3] Serge Lang. *Algebra.* Springer-Verlag, 2002.

[4] F..J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes,* North-Holland Publishing Company, 1977.

[5] R.M. Roth. *Introduction to Coding Theory.* Cambridge University Press, 2006.

[6] D.R. Stinson. *Cryptography-Theory and Practice.* 3rd edition, CRC Press, 2006.

[7] 万哲先，代数和编码，第三版，高等教育出版社，2007.

[8] 王东明，夏壁灿，李子明，计算机代数（第二版），清华大学出版社，2007.

[9] 吴文俊，数学机械化，科学出版社，2003.