近世代数与初等数论

张卫明

Email：zhangwm@ustc.edu.cn
Homepage: http://staff.ustc.edu.cn/~zhangwm/mant
Tel: 63600683, 15209827756

- 何谓近世代数
- 何谓初等数论
- 数论、近世代数与密码学的关系
- 参考书及学习建议

何为近世代数

近世代数的诞生

1811～1832

法国数学家Evariste Galois(1811-1832) 入了群与扩域的工具,解决了高次方程的求根问题.

“把数学运算归类， 学会按照难易程度，而不是按照它们的外部特征加以分类，这就是我所理解的未来数学家的任务，这就是我所要走的道路。”

关于代数的观念

从人们的观念上来看,人们关于代数的观念大致有三种：

1 用字母的代数

2 解方程

3 各种代数结构的理论

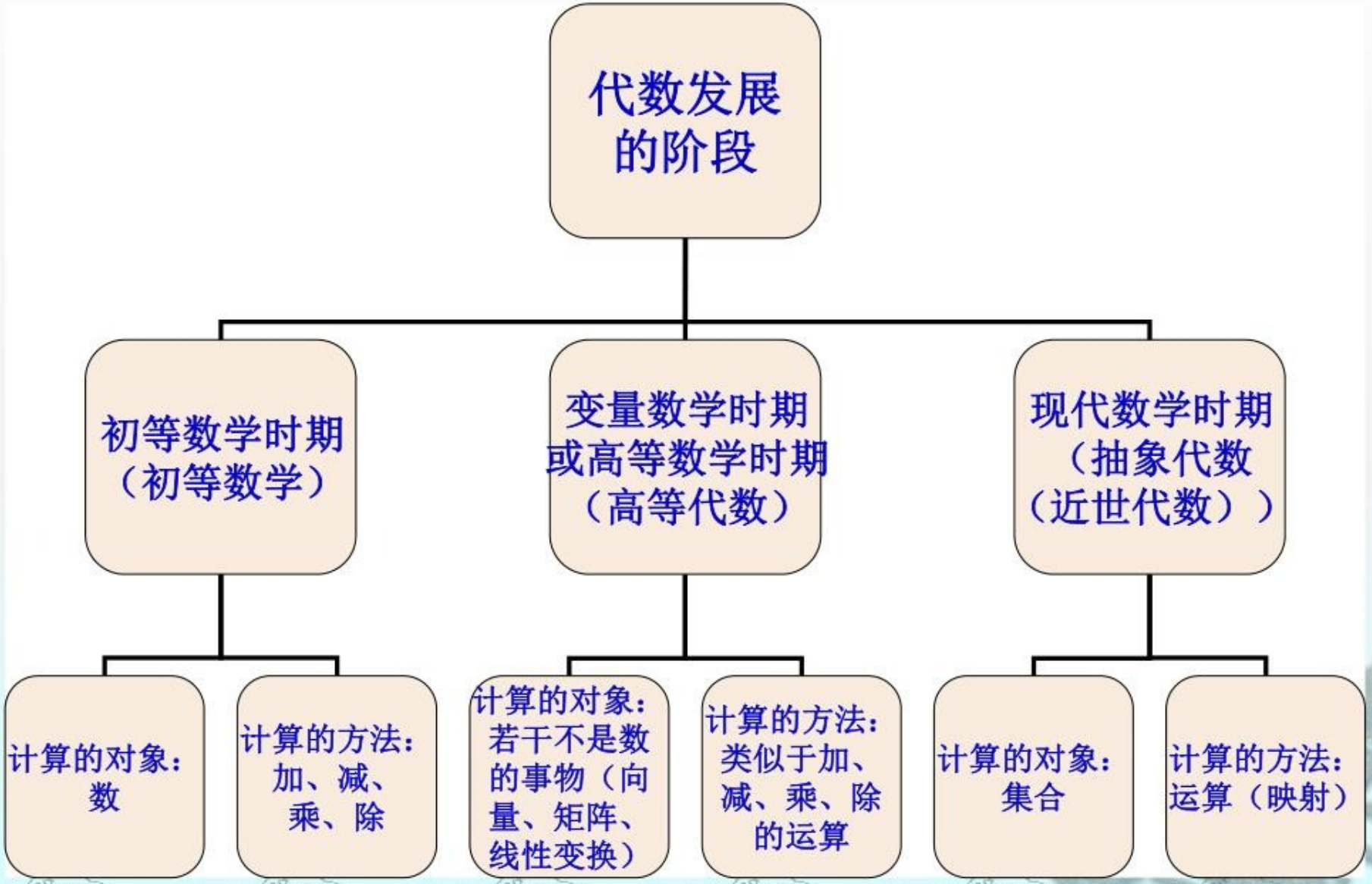
何为近世代数

- 初等代数、高等代数、线性代数都称为经典代数.它的研究对象主要是代数方程和线性方程组.

- 而现代代数学也即近世代数(又称为抽象代数),其主要内容是研究各种代数系统(代数结构),而对于代数结构,其基本成分则是集合和集合上的映射

- 当然,所谓代数结构实际上就是带有运算的集合.一般说来,这些运算还适合某些所希望的若干条件.

何为近世代数


代数发展的阶段
初等数学时期（初等数学）
变量数学时期或高等数学时期（高等代数）
现代数学时期（抽象代数（近世代数））
计算的对象：数
计算的方法：加、减、乘、除
计算的对象：若干不是数的事物（向量、矩阵、线性变换）
计算的方法：类似于加、减、乘、除的运算
计算的对象：集合
计算的方法：运算（映射）

代数学发展的四个阶段

代数学经历了漫长的发展过程,抽象代数(近世代数)是19世纪最后20年直到20世纪前30年才发展起来的现代数学分支.

1 最初的文字叙述阶段

2 代数的简化文字阶段

3 符号代数阶段

4 结构代数阶段

1 最初的文字叙述阶段

- 古希腊之前直到丢番图(Diophantine,公元250年)时代,
- 此时算术或代数尚未形成任何简化的符号表达法,代数运算则都采用通常的语言叙述方式表达,因而代数推理也都采用直观的方法.
- 在中国古代则有著名的筹算法,
- 古希腊则借助于几何图形的变换方法.

如毕达哥拉斯(Pythagoras,公元前585-497)几何数论方法.例如通过图形的组合可以得到

$$1+3+5+7+\cdots+(2n-1)=n^2$$

2 简化文字阶段

➢直到古希腊数学后期,数学家丢番图才开始把通常的语言叙述作简化,利用简化的文字符号代替一些相对固定的代数表达式. 这一时期大致延续到欧洲文艺复兴时代.

➢丢番图对代数学的发展做出了突出的贡献,《算术》一书研究了一系列不定方程的求解问题.

例如把一个平方数表为两个平方数之和的问题.

➢ 正是在丢番图关于整数诸如此类表法研究的基础上,17世纪伟大的法国数学家费马(Pierre de Fermat,1601-1665)提出了不定方程$x^n+y^n=z^n$在$n\geq 3$时不可解问题.19世纪费马问题的研究也是导致近世代数理想论产生的重要契机.

3 符号代数阶段

- 经过欧洲文艺复兴之后的好几位数学家的努力而大致在17世纪完成。它的标志是用字母表示数.
- 较早的代表著作是德国数学家M.Stiefel(1486-1567)1553年的《综合算术》.其利用10进制小数表示实数.
- 法国数学家韦达(F.Viete,1540-1603).韦达是第一个系统使用字母表示数的人,在代数、三角学等许多方面都做出了杰出的贡献.

4 结构代数阶段

这一阶段代数学的研究对象不再是个别的数字运算，而是抽象的运算系统(如群、环、域等)的代数结构.它起因于年轻的法国数学家Evariste Galois(1811-1832)对代数方程式解的研究.

- 二次方程求根式解
- 16世纪中叶，两位意大利数学家G.Cardano(1506)与L.Ferrari(1545)发现了三、四次方程的求根公式

- 1824年，挪威数学家阿贝尔解决了用根式求解五次方程的不可能性问题.

4 结构代数阶段

- Galois摆脱了前人关于根的计算方法的研究途径,发现根的对称性群的结构能够决定根的可解性. Galois的研究不但确立了群论在数学中的地位,同时也开创了结构代数这个新型的代数学研究方向.
- Carl Gauss(1777-1855)为了解决Fermat问题,开始一般性的研究代数数域.他的学生E.Kummer(1810-1893)在Gauss方法的基础上引入理想数,使Fermat问题的研究推进了一步.直到19世纪末建立了群、环、域的系统理论.
- 1834年爱尔兰数学家William R.Hamiton(1805-1865)在Gauss把复数解释为二元数这一思想的启发下创建了一种奇特的不交换的数系,后来称之为Hamiton四元数.

4 结构代数阶段

- 上述三大进展奠定了近世代数学的重要基础.

- 1931年荷兰数学家B.L.van.der.Waerden出版了两卷本<近世代数学>,1955年该书第四版更名为<代数学>.这一著作标志着群、环、域等抽象结构理论已经成为现代代数学的主要研究对象,该著作同时也成为现代结构主义数学的起点.

- 1951年美国数学家N.Jacobson又出版了新的代数学著作,书名为<抽象代数学讲义>(共三卷).因此近世代数也被称为抽象代数.

抽象代数的应用

➢物理学家们认识到群论为描述物理学的对称性问题提供了所需的工具,这种对称性在基本粒子物理学的研究中是至关重要的。

➢1910 年,美国数学家维布伦（ O.Vebleh， 1880 — 1960 ）和物理学家詹斯（ J.Jeans ）一起讨论普林斯顿大学的数学课程改革时,詹斯提出：＂我们完全可以把群论去掉,因为它永远也不会在物理学中有任何作用。＂

➢群论后来成了物理学和的核心主题之一 。从三十年代起,外尔（ C.H.H.Weyl， 1885 — 1955 ）和韦格纳（ E.P.Wigner， 1902 —？）在物理学中开辟了群论的观点,而他们都是普林斯顿大学的教授。

•何谓初等数论

- •数论：数学分支，研究特殊数的性质和关系。
- •数论的重要研究对象是整数集合；特别重要的是素数！
- •素数是正整数乘法结构的基石：算术基本定理。
- •对素数的兴趣可以追溯的2500年前的古希腊
- •第一个问题可能是：素数是否有无穷多？《几何原本》中欧几里得给出了证明。简单而优美，是《Proofs from THE BOOK》收录的第一个证明，Paul Erdös称这本书是上帝掌管的。
- •17、18世纪费马（Fermat）和欧拉（Euler）证明了很多重要结果，并对素数的生成给出了许多猜想
- •19、20世纪 关于素数有很多重要进展，如素数的分布。

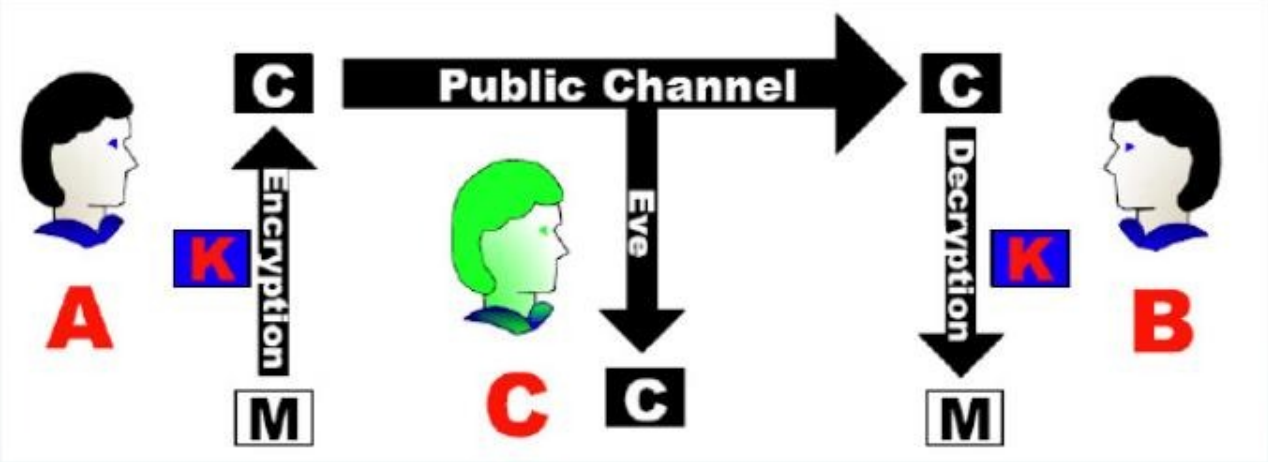
•何谓初等数论

- 现代数论始于高斯（Gauss），发明了同余语言。二次互反律的证明，开启了数论的新领域。
- 素性判定，
- 寻找大素数，梅森素数
- 大整数分解：ＲＳＡ
- 寻找方程的整数解：费马大定理

- 初等数论：即不依赖于复变函数、抽象代数和代数几何等高等数学。
- 相对地，可进一步学习解析数论（复变），代数数论（抽象代数）。

数论与近世代数在密码学中的应用

对称密码模型

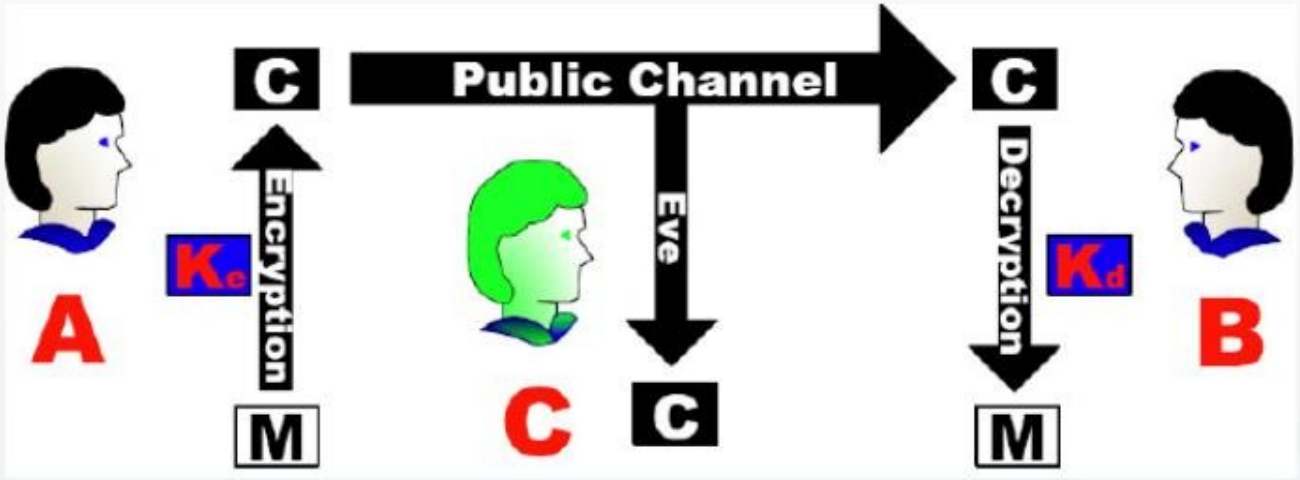


例如, 凯撒密码系统, 密码本, 3-DES, AES.

涉及数学问题, 模运算, 置换, 域的构造

数论与近世代数在密码学中的应用

非对称密码模型-公钥密码学



数论与近世代数在密码学中的应用

公钥密码学概述

1976年, Diffie 和Hellman在美国国家计算机会议上首次提出了公开密钥密码学的概念,并发表了开创性的论文“New Direction in Cryptography”(“密码学的新方向”). (现有的文献表明：早在20世纪60年代末, 英国机构GCHQ中的一部分人就认识到了Diffie-Hellman所提出的概念, 但这些消息并没有公开发表.)人们就积极寻求满足上述需求的公钥密码系统, 也就是说, 要寻找单向陷门函数, 其从一方是很容易计算的(知道加密密钥), 而从另一方却无法计算(不知道解密钥匙).

例1. 从门内出来容易, 但进入们内需要钥匙.
例2. 将信放进邮箱容易, 但取出邮件需要钥匙.

数学难题(安全性和有效性)

第一个公钥密码系统：基于背包问题的背包公钥密码系统.

目前大家所公认的高效安全的公钥密码体制, 按其所基于的数学难题可分为三类：

一. 基于大整数分解难题的公钥体制, 例如RSA和Rabin-William体制；

i) 给定两个素数p, q, 计算乘积$p \cdot q = n$ 很容易;

ii) 给定整数n, 求n 的素因数p, q 使得$n = p \cdot q$ 非常困难.

二. 基于有限域上离散对数难题的公钥体制, 例如美国政府的数字签名算法DSA, Diffie-Hellman的密钥交换体制, ElGamal加密和签名体制等；

已知有限循环群$G =< g >= \{g^k \mid k = 0, 1, 2, \ldots\}$ 及其生成元g 和阶$n = |G|$.

i) 给定整数a, 计算元素$g^a = h$ 很容易;

ii) 给定元素h, 计算整数$x, 0 \leq x \leq n$, 使得$g^x = h$ 非常困难.

三. 基于椭圆曲线离散对数难题的公钥体制, 即椭圆曲线密码体制（Elliptic Curves Cryptosystem, 简称ECC）, 它们绝大多数是基于有限域上离散对数难题的公钥密码体制在椭圆曲线群上的推广.

数论与近世代数在密码学中的应用

涉及数学问题

整除$b|a$, 因数
欧几里得算法
广义欧几里得算法
素数, 素数的产生, 整数分解
公因数 最大公因数(a, b)
模运算$a \equiv b \bmod n$
中国剩余定理
欧拉函数$\varphi(n)$
欧拉定理
费马小定理

二次剩余
指标
原根或素域的生成元
有限群
置换群
环
域
有限域的生成
安全椭圆曲线

初等数论的学习内容

第一章 整数的可除性：掌握整除、素数、最大公因数、欧几里得除法

第二章 同余：运用同余运算、欧拉定理、费马小定理以及模重复平方法，熟练运用中国剩余定理以及它们大模运算。

第三章 二次同余式与平方剩余：熟练运用勒让德符号和雅可比符号 以及求模 p 平方根。

第四章 原根与指标：掌握原根、指数、指标等的定义，熟练运用原根判别法则以及会具体求原根。

第五章 素性检验：掌握费马素性检验、欧拉素性检验和米勒．拉宾素性检验等，熟练运用素性检验判别法则求较大素数。

近世代数的学习内容

第八章 群

掌握群、子群、同态及同构等的定义，熟练运用群同构对群进行分类。 掌握有限群、循环群和置换群等的定义。

第十章 环

要求：掌握环、整环、理想等的定义，熟练运用多项式环方面的一些结构，特别是不可约多项式和本原多项式的产生。

第十一章 域和 Galois 理论

要求：掌握域、有限域、扩域、运用 域理论 构造素数和特征 2 的有限域， 以及会求多项式 基和正规基。

第十三章 椭圆曲线

要求：掌握有限域上椭圆曲线的构造，安全椭圆曲线的生成以及椭圆曲线密码的基本理论。

参考与学习建议

1. 《信息安全数学基础》，覃中平，张焕国等.
2. 《信息安全数学基础》，陈恭亮.

3. 《数论讲义》（上册），柯召，孙琦.
4. “Elementary Number Theory and Its Applications”《初等数论及其应用》，Kenneth H. Rosen

5 《应用近世代数》，胡冠章，王殿军.
6. 《近世代数引论》，冯克勤，李尚志，章璞.

参考与学习建议

1. **面向密**码学和信息安全的应用
2. **每**门课程都是探险之旅，沿着大师的足迹前行，学习证明的技巧，推广问题的思维方式。多做习题。
3. **利用**计算机，观察现象，探索规律，设置猜想