# 代数结构与组合数学

# Algebraic Structure and Combinatorial Mathematics

北京大学信息科学技术学院

曹永知

2020年2月

# 数学课程？！

音乐能激发或抚慰情怀，
绘画使人赏心悦目，
诗歌能动人心弦，
哲学使人获得智慧，
科学可改善物质生活，
但数学能给予以上的一切。

—克莱因（1849-1925，德国数学家）

# 引 言

- 课程简介
  - 代数结构
  - 组合数学
- 学习安排
  - 教学要求
  - 教学安排
  - 教学资源

# 代数的历史 http://en.wikipedia.org/wiki/Timeline_of_algebra

| Year | Event |
|---|---|
| Circa 1800 BC | The Old Babylonian Strassburg tablet seeks the solution of a quadratic elliptic equation.[citation needed] |
| Circa 1800 BC | The *Plimpton 322* tablet gives a table of Pythagorean triples in Babylonian Cuneiform script.[1] |
| 1800 BC | Berlin Papyrus 6619 (19th dynasty) contains a quadratic equation and its solution.[2][3] |
| 800 BC | Baudhayana, author of the Baudhayana Sulba Sutra, a Vedic Sanskrit geometric text, contains quadratic equations, and calculates the square root of 2 correct to five decimal places |
| Circa 300 BC | Euclid's *Elements* gives a geometric construction with Euclidean tools for the solution of the quadratic equation for positive real roots.[4] The construction is due to the Pythagorean School of geometry.[citation needed] |
| Circa 300 BC | A geometric construction for the solution of the cubic is sought (doubling the cube problem). It is now well known that the general cubic has no such solution using Euclidean tools.[citation needed] |
| 150 BC | Jain mathematicians in India write the “Sthananga Sutra”, which contains work on the theory of numbers, arithmetical operations, geometry, operations with fractions, simple equations, cubic equations, quartic equations, and permutations and combinations |
| Circa 100 BC | Algebraic equations are treated in the Chinese mathematics book *Jiuzhang suanshu* (*The Nine Chapters on the Mathematical Art*), which contains solutions of linear equations solved using the rule of double false position, geometric solutions of quadratic equations, and the solutions of matrices equivalent to the modern method, to solve systems of simultaneous linear equations.[5] |
| 1st century | Heron of Alexandria, the earliest fleeting reference to square roots of negative numbers. |
| Circa 150 | Greek mathematician Hero of Alexandria, treats algebraic equations in three volumes of mathematics.[citation needed] |
| Circa 200 | Hellenistic mathematician Diophantus lived in Alexandria and is often considered to be the "father of algebra", writes his famous *Arithmetica*, a work featuring solutions of algebraic equations and on the theory of numbers.[citation needed] |
| 499 | Indian mathematician Aryabhata, in his treatise *Aryabhatiya*, obtains whole-number solutions to linear equations by a method equivalent to the modern one, describes the general integral solution of the indeterminate linear equation, gives integral solutions of simultaneous indeterminate linear equations, and describes a differential equation.[citation needed] |
| Circa 625 | Chinese mathematician Wang Xiaotong finds numerical solutions to certain cubic equations.[6] |
| Circa 7th century Dates vary from the 3rd to the 12th centuries.[7] | The *Bakhshali Manuscript* written in ancient India uses a form of algebraic notation using letters of the alphabet and other signs, and contains cubic and quartic equations, algebraic solutions of linear equations with up to five unknowns, the general algebraic formula for the quadratic equation, and solutions of indeterminate quadratic equations and simultaneous equations. [citation needed] |
| 7th century | Brahmagupta invents the method of solving indeterminate equations of the second degree and is the first to use algebra to solve astronomical problems. He also develops methods for calculations of the motions and places of various planets, their rising and setting, conjunctions, and the calculation of eclipses of the sun and the moon |
| 628 | Brahmagupta writes the *Brahmasphuta-siddhanta*, where zero is clearly explained, and where the modern place-value Indian numeral system is fully developed. It also gives rules for manipulating both negative and positive numbers, methods for computing square roots, methods of solving linear and quadratic equations, and rules for summing series, Brahmagupta's identity, and the Brahmagupta theorem |
| 700s | Virasena gives explicit rules for the Fibonacci sequence, gives the derivation of the volume of a frustum using an infinite procedure, and also deals with the logarithm to base 2 and knows its laws |
| Circa 800 | The Abbasid patrons of learning, al-Mansur, Haroun al-Raschid, and al-Mamun, had Greek, Babylonian, and Indian mathematical and scientific works translated into Arabic and began a cultural, scientific and mathematical awakening after a century devoid of mathematical achievements.[8] |

# 代数的历史

⋮

| | |
|---|---|
| 1806 | Jean-Robert Argand publishes proof of the Fundamental theorem of algebra and the Argand diagram, |
| 1824 | Niels Henrik Abel proved that the general quintic equation is insoluble by radicals.[23] |
| 1832 | Galois theory is developed by Évariste Galois in his work on abstract algebra.[23] |
| 1847 | George Boole formalizes symbolic logic in *The Mathematical Analysis of Logic*, defining what now is called Boolean algebra, |
| 1873 | Charles Hermite proves that e is transcendental, |
| 1878 | Charles Hermite solves the general quintic equation by means of elliptic and modular functions |
| 1981 | Mikhail Gromov develops the theory of hyperbolic groups, revolutionizing both infinite group theory and global differential geometry, |
| 2007 | a team of researches throughout North America and Europe used networks of computers to map E8 (mathematics).[29] |

**4000 Years of Algebra** by Robin Wilson:

http://www.gresham.ac.uk/lectures-and-events/4000-years-of-algebra

# 代数的分类

- 初等代数(elementary algebra)
  - 在实数或复数范围内，加减乘除运算，未知数，低次方程求解等
- 线性代数(linear algebra)
  - 矩阵、线性方程组、向量空间
- 抽象/近世代数(abstract/modern algebra)
  - 群、环、域等公理化定义的代数结构
- 泛代数(universal algebra)
  - 研究所有代数结构的共同性质

# 代数

- 代数是研究数、数量、关系与结构的数学分支。
- 代数的研究对象不仅是数字，还包括各种抽象化的结构。
  - 例如，整数集作为一个带有加法、乘法和序关系的集合就是一个代数结构，其中我们只关心各种关系及其性质，而并不关心“数本身是什么”这样的问题。

# 代数（续）

- 代数学是慷慨大方的，它给予人的往往比人们对她所要求的还要多。

—达朗贝尔

- 代数是搞清楚世界上数量关系的智力工具。

—怀特海

# 代数应用举例

- 计算机科学
  - 半群理论在自动机理论和形式语言中发挥了重要作用
  - 有限域理论是编码理论的数学基础，在通信中起着重要作用
  - 格和布尔代数是电子线路设计、电子计算机硬件设计和通信系统设计的重要工具

  ...

# 代数应用举例（续）

## Algebraic Structures for Capturing the Provenance of SPARQL Queries

FLORIS GEERTS, University of Antwerp
THOMAS UNGER, University College Dublin
GRIGORIS KARVOUNARAKIS, LogicBlox
IRINI FUNDULAKI, ICS-FORTH
VASSILIS CHRISTOPHIDES, Inria Paris-Rocquencourt

The evaluation of SPARQL algebra queries on various kinds of annotated RDF graphs can be seen as a particular case of the evaluation of these queries on RDF graphs annotated with elements of so-called *spm-semirings*. Spm-semirings extend semirings, used for representing the provenance of positive relational algebra queries on annotated relational data, with a new operator to capture the semantics of the non-monotone SPARQL operators. Furthermore, spm-semiring-based annotations ensure that desired SPARQL query equivalences hold when querying annotated RDF. In this work, in addition to introducing spm-semirings, we study their properties and provide an alternative characterization of these structures in terms of semirings with an embedded boolean algebra (or seba-structure for short). This characterization allows us to construct spm-semirings and identify a universal object in the class of spm-semirings. Finally, we show that this universal object provides a provenance representation of poly-sized overhead and can be used to evaluate SPARQL queries on arbitrary spm-semiring-annotated RDF graphs.

CCS Concepts: • **Information systems → Data provenance; Query languages for non-relational engines**

Additional Key Words and Phrases: Algebraic structures, annotations, provenance models, query languages, RDF, SPARQL

**ACM Reference Format:**
Floris Geerts, Thomas Unger, Grigoris Karvounarakis, Irini Fundulaki, and Vassilis Christophides. 2016. Algebraic structures for capturing the provenance of SPARQL queries. J. ACM 63, 1, Article 7 (February 2016), 63 pages.

# 代数应用举例（续）

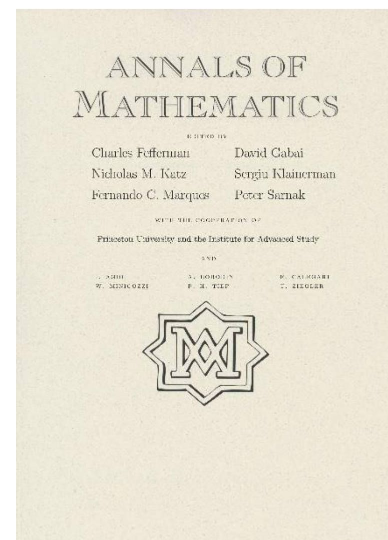
Annals of Mathematics, **160** (2004), 781–793

## PRIMES is in P

By Manindra Agrawal, Neeraj Kayal, and Nitin Saxena*

**Abstract**

We present an unconditional deterministic polynomial-time algorithm that determines whether an input number is prime or composite.




Received: 24 January 2002
Accepted: 21 March 2003
Published online: September 2004

# 代数应用举例（续）

cs.stackexchange.com/questions/9648/what-use-are-groups-monoids-and-rings-in-database-computations

导入 https://www.easyc... AUE: The alt.usag... 从 Firefox 导入

**Computer Science** beta

Questions Tags Users Badges

Computer Science Stack Exchange is a question and answer site for students, researchers and practitioners of computer science. It's 100% free, no registration required.

## What use are groups, monoids, and rings in database computations?

23

25

Why would a company like Twitter be interest in algebraic concepts like groups, monoids and rings. https://github.com/twitter/algebird

All I could find is:

> Implementations of Monoids for interesting approximation algorithms, such as Bloom filter, HyperLogLog and CountMinSketch. These allow you to think of these sophisticated operations like you might numbers, and add them up in hadoop or online to produce powerful statistics and analytics.

and in another part of the GitHub page:

> It was originally developed as part of Scalding's Matrix API, where Matrices had values which are elements of Monoids, Groups, or Rings. Subsequently, it was clear that the code had broader application within Scalding and on other projects within Twitter.

What could this broader application be? within Twitter and for general interest?

It seems like composition aggregations of databases have a monoid-like structure.

# Should I take abstract algebra to prepare for computer science graduate school?

http://www.quora.com/Should-I-take-abstract-algebra-to-prepare-for-computer-science-graduate-school

Quora

Search for questions, people, and topics

3 ANSWERS

**Daniel McLaury**, Ph.D. Student in Mathematics
4 upvotes by Nick Weinandt, Marc Bodnick, Nihal Balani, (more)

Most people don't, unless they're working in cryptography (in which case it's absolutely mandatory). There are also some applications of category theory to programming language theory.

Written 22 Jul, 2013. 847 views.

Upvote | 4 Downvote Comment

**Justin Rising**, MSE in CS
2 upvotes by Edwin Khoo and Quora User.

I think that regardless of what subfield of CS you're interested in, it's good to be basically comfortable working with algebraic structures. Semirings show up all over the place, and you'll be slowed down if you stumble over them.

Written 29 Jun, 2014. 485 views.

Upvote | 2 Downvote Comment

**Anonymous**
6 upvotes by Anurag Bishnoi (Ph.D. student in Mathematics at Ghent University.), Jessica Su (CS PhD student at Stanford), Nick Weinandt, (more)

**Yes.**

It would be quite beneficial to know as much as possible about finite fields, and polynomials and vector spaces over finite fields. In order to reach this level, one has to go through group theory and basic ring theory at an undergraduate level. Finite fields are used all over theoretical computer science: error-correcting codes, cryptography, derandomization, and combinatorics in general. Group theory may also be helpful in the study of graphs, but that depends on your precise interests.

Written 22 Jul, 2013. 434 views.

Upvote | 6 Downvote Comment

# 组合数学

- 组合数学是一个既古老又年轻的数学分支。美国的组合数学大师赖瑟(H．J．Ryser)写了一本专著《组合数学》，已被广泛引用。书中一开头就讲公元前2200多年禹从神龟背上看到的幻方，以及公元前1100多年中国隐约产生的排列概念，用来说明组合数学是自古就有的数学分支。
- 1666年莱布尼兹所著《组合学论文》一书问世，这是组合数学的第一部专著。书中首次使用了组合论(Combinatorics)一词。

# 组合数学（续）

- 广义的组合数学就是离散数学，离散数学是狭义的组合数学和图论、代数结构、数理逻辑等的总称。
- 狭义的组合数学主要研究满足一定条件的组态（也称组合模型）的存在、计数以及构造等方面的问题。组合数学的主要内容有组合计数、组合设计、组合矩阵、组合优化等。
- 因为计算机科学的核心内容是使用算法处理离散数据，随着计算机科学的日益发展，组合数学的重要性也日渐凸显。

# 组合应用举例

- 化学：分子、晶体中原子的排列
- 生物：基因、蛋白质结构
- 物理：统计力学
- 通信：组合编码，纠错等
- 计算机科学：资源分配和调度，算法有效性分析

…

# 我们能收获什么？

- 技巧是数学知识中最有价值的部分，比仅仅获得信息还要有价值得多。但是，我们应该怎样教技巧呢?学生只有通过模仿与实践才能学到技巧。在数学中，技巧是解决问题的能力，是构想证明的能力，是敏锐地评判答案与证明的能力。因而，在数学中，技巧比仅仅掌握信息还重要得多。

  —波利亚

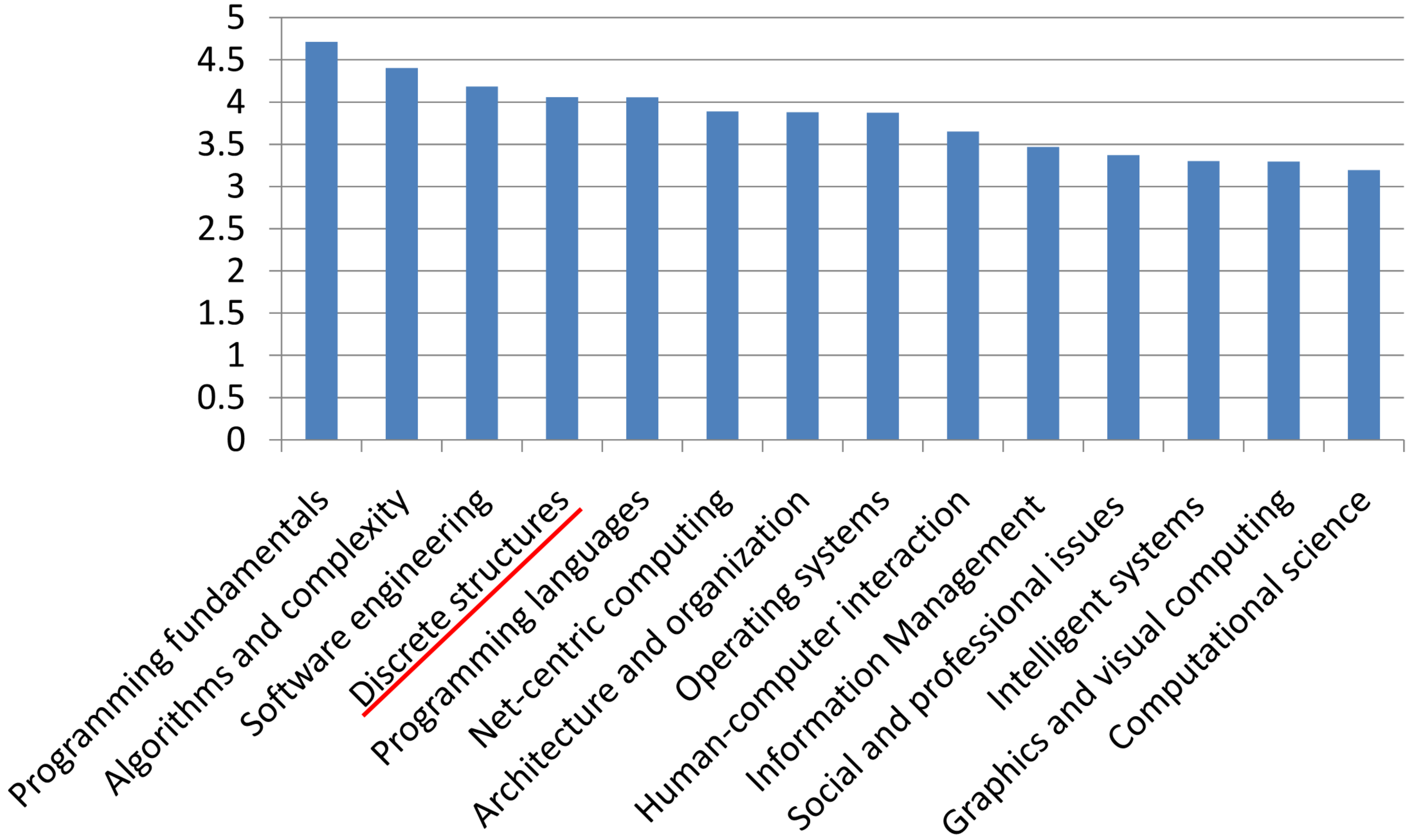
- 在数学的天地里，重要的不是我们知道什么，而是我们如何知道。

  —泰勒斯

ACM/IEEE-CS Computer Science Curricula 2013

# Importance of Knowledge Areas

http://www.sigart.org/CS2013-EAAI2011panel-RequestForFeedback.pdf



# 课程学习安排

- 学习要求
  - 知识体系：基本概念、基本计算、基本证明方法
  - 注意能力的培养：

    获取知识的能力----读书

    分析问题解决问题的能力----解题

    理论联系实际的能力----联系其它课程或研究课题
- 成绩评定
  - 平时成绩：40~50%（课堂、作业、期中测验）
  - 期末笔试：60~50%
- 期末考试时间：6月16日（周二）上午

# 预计课程进度（48学时）

- 代数系统的基本概念（8学时）

  二元运算的性质、代数系统构成、子代数与积代数、代数系统的同态与同构、代数系统上的同余关系与商代数

- 半群、独异点与群（12学时）

  半群与独异点的定义与性质、群的定义与分类、群的基本性质、子群、循环群、变换群与置换群、群的分解（陪集分解与Lagrange定理、共轭类分解与分类方程）、正规子群、商群及性质、群的同态与同构、群的直积

- 环与域（3学时）

  环的定义及基本性质、特殊的环（整环、域）、子环、理想、商环及环同态

# 预计课程进度（续）

- 格与布尔代数（2学时）

  格的定义与性质、子格、格同态与格的直积、特殊的格（模格、分配格、有补格、布尔代数）

- 期中测验（2学时）
- 组合存在性定理（3学时）

  鸽巢原理及其应用，Ramsey定理及其应用

- 基本计数公式（3学时）

  加法法则与乘法法则，集合的排列与组合，多重集的排列与组合，二项式定理与组合恒等式，多项式定理

# 预计课程进度（续）

- **组合计数方法（7学时）**

  递推方程的公式求解，递推方程的其他解法（换元法、迭代归纳法、递归树法、尝试法等），生成函数的定义、性质及在计数中的应用，指数生成函数与组合计数，**Catalan**数，**Stirling**数

- **组合计数定理（7学时）**

  容斥原理（基本形式、对称筛公式、棋盘多项式及其应用），**Burnside**引理与**Polya**定理（一般形式与推广形式、在等价类计数中的应用）

- **课程总结（1学时）**

# 教材与参考书

- **教材：**
  - 耿素云、屈婉玲、王捍贫，离散数学教程，北京大学出版社，2004.
- **参考书：**
  - 屈婉玲、耿素云、王捍贫、刘田，离散数学习题解析，北京大学出版社，2008.
  - G. S. Rao, Discrete Mathematics Structures (2$^{nd}$ ed.), New Age International (P) Ltd., 2009.
  - D. P. Acharjya and Sreekumar, Fundamental Approach to Discrete Mathematics (2$^{nd}$ ed.), New Age International (P) Ltd., 2009.

# 网上教学平台

## http://course.pku.edu.cn/

请用北大统一账号登录

内容包括：

- 课件发布
- 作业布置
- 通知

# 2020年课程安排

- 本课程涉及教材第15-23章，其中15.5, 16.2, 17.8, 18.3, 20.2为选学内容
- 本学期顺序安排
  - 20.1, 21.1-21.4，22.1-22.6，23.1-23.2;
  - 15.1-15.4，16.1, 17.1-17.7，18.1-18.2，19.1-19.4;
  - 23.3-23.4


- 教学方式
  - 返校前：爱课程+Classin答疑 http://www.icourses.cn/sCourse/course_6447.html
  - 正常返校后，教室上课

# 教师与助教联系方式

- 曹永知
  - Office: 理科一号楼1623N
  - Email: caoyz@pku.edu.cn
  - Research: https://scholar.google.com/citations?user=VEhLdikAAAAJ&hl=zh-CN
    https://www.researchgate.net/profile/Yongzhi_Cao2
  - 答疑：平时上课前后；考试前单独安排
  - 助教：见后
- 收发作业时间：每周二课间（返校前，请以电子邮件“**x班+学号+姓名代组第x次作业**”发送至对应助教）

如果你能够尽到自己的本分，尽力完成自己应该做的事情，那么总有一天，你能够随心所欲地从事自己想要做的事情。

——齐格勒

# 作业分班（助教实验室在理科一号楼1708）

1班：学号<=1700012953；
助教：白宗磊，1601111273@pku.edu.cn

2班：1700012953<学号<=1800012797；
助教：金钊， jinzhao@pku.edu.cn

3班：1800012797<学号<=1800012951；
助教：郭晓熙，1801111344@pku.edu.cn

4班：1800012951<学号<= 1800013028；
助教：王梓丞，1801213708@pku.edu.cn

5班：1800013028<学号<= 1800013086；
助教：李喆琛，1901111292@pku.edu.cn

6班：学号>1800013086；
助教： 张博闻，zbinks@126.com

缓考：可只参加期末考试；也可参与过评，按最优取。

重修：要求同初次选修