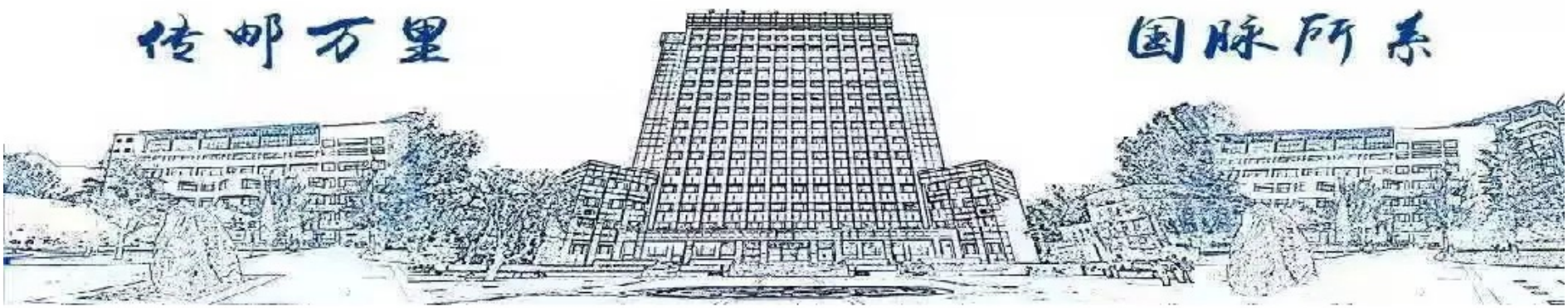
网络空间安全学院
School of Cyberspace Security, BUPT

信息安全数学基础

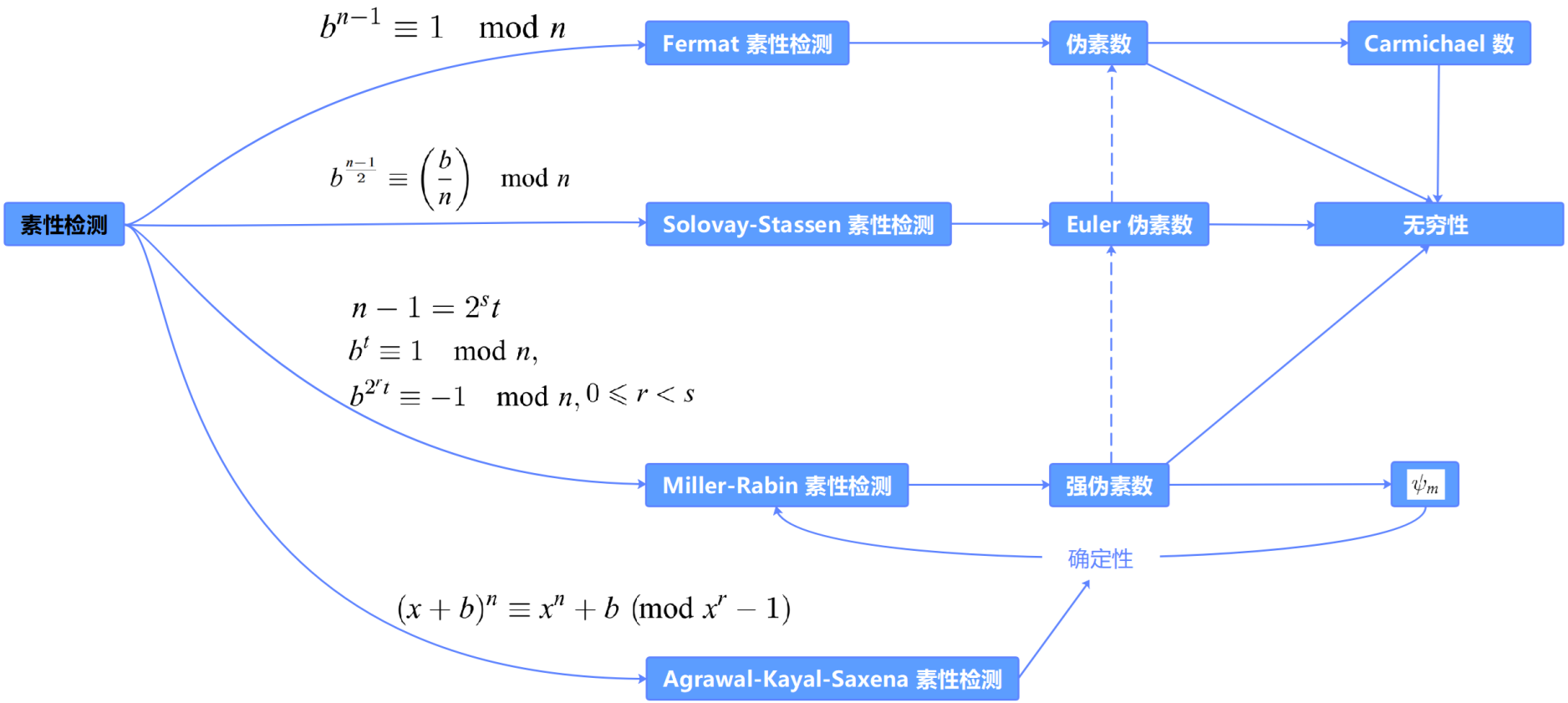
—— 群 (1)

信数课题组

北京邮电大学



上次课回顾


$b^{n-1} \equiv 1 \mod n$
Fermat 素性检测
伪素数
Carmichael 数
$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \mod n$
素性检测
Solovay-Stassen 素性检测
Euler 伪素数
无穷性
$n-1=2^s t$
$b^t \equiv 1 \mod n,$
$b^{2^r t} \equiv -1 \mod n, 0 \leqslant r < s$
Miller-Rabin 素性检测
强伪素数
ψ_m
确定性
$(x+b)^n \equiv x^n + b \pmod{x^r - 1}$
Agrawal-Kayal-Saxena 素性检测

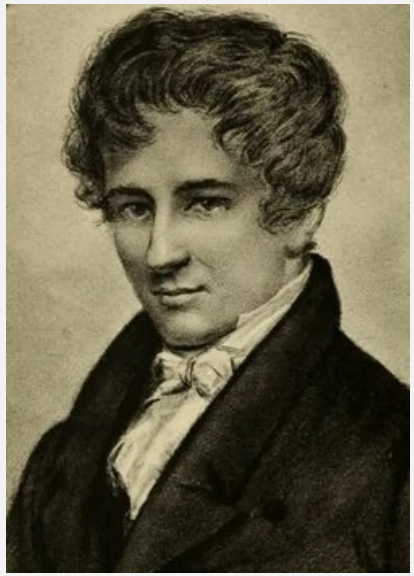
目录

目录

尼尔斯·亨利克·阿贝尔

(Niels Henrik Abel, 1802.8.5 — 1829.4.6)

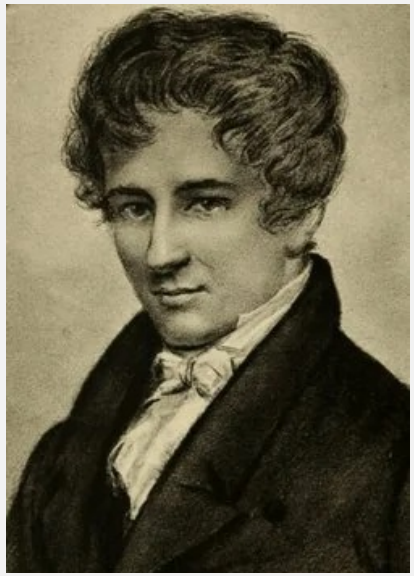
挪威数学家. 在很多数学领域做出了开创性的工作, 是十九世纪挪威最伟大的数学家. 最著名的一个成果是首次完整地给出了高于四次的一般代数方程没有一般形式的代数解的证明, 这个问题是那个时代最著名的未解决问题之一, 悬疑达 250 多年. 他也是椭圆函数领域的开拓者, 阿贝尔函数的发现者. 尽管阿贝尔的数学成就极高, 却在生前没有得到认可. 他的生活非常贫困, 因病去世, 享年 27 岁.



尼尔斯·亨利克·阿贝尔

(Niels Henrik Abel, 1802.8.5 — 1829.4.6)

挪威数学家. 在很多数学领域做出了开创性的工作, 是十九世纪挪威最伟大的数学家. 最著名的一个成果是首次完整地给出了高于四次的一般代数方程没有一般形式的代数解的证明, 这个问题是那个时代最著名的未解决问题之一, 悬疑达 250 多年. 他也是椭圆函数领域的开拓者, 阿贝尔函数的发现者. 尽管阿贝尔的数学成就极高, 却在生前没有得到认可. 他的生活非常贫困, 因病去世, 享年 27 岁.



埃瓦里斯特·伽罗瓦

(Évariste Galois, 1811.10.25 — 1832.5.31)

法国数学家. 与阿贝尔并称为现代群论的创始人. 用群论彻底解决了根式求解代数方程的问题, 而且由此发展了一整套关于群和域的理论, 人们称之为伽罗瓦理论, 并把其创造的“群”叫作伽罗瓦群（Galois Group）. 在世时在数学上研究成果的重要意义没被人们所认识, 曾呈送科学院 3 篇学术论文, 均被退回或遗失. 21 岁时死于一次决斗.

数学天才阿贝尔的生前身后名

出生在挪威芬岛的一个小乡村, 父亲是当地的牧师. 12 岁时, 父亲当选国会议员, 被送往首都奥斯陆的天主教学校学习. 起初成绩平平, 直到 16 岁时遇到新来的数学老师 Bernt Michael Holmboe, 由此改变了他的一生.

Holmboe 是挪威一位著名天文学家的助教, 只比阿贝尔大九岁. 他使阿贝尔第一次感受到数学的意义和乐趣, 并发现了其无与伦比的数学天分, 两人亦师亦友. 在 Holmboe 的指导下, 阿贝尔系统学习了牛顿、欧拉、拉格朗日及高斯等当时著名数学家的著作. 不久, 阿贝尔证明了二项式定理对所有实数成立, 扩展了欧拉关于该定理只对有理数成立的结果.

18 岁时, 阿贝尔的父亲去世. 次年在 Holmboe 等老师的资助下阿贝尔进入奥斯陆大学读书, 不久就成为挪威小有名气的数学家. 1823 年夏, 阿贝尔又在老师们的资助下前往丹麦首都哥本哈根. 在数学家 Carl Ferdinand Degen 的启发下, 研究五次方程的根式解的存在性问题. 次年 22 岁时, 天才地证明了, 除特殊情况外五次或以上代数方程的根式解并不存在, 解决了困扰数学界 250 年之久的世界性难题（证明中已经出现了“群论”这一近世代数的基本思想, 但没有来得及发展和完成这一划时代的工作）. 由于经济条件不佳, 无法支付高昂的印刷费用, 因此最初的论文只有短短的六页. 阿贝尔将论文寄给高斯, 大概高斯不相信能用这么短的篇幅证明这个世界著名的——包括他自己也还无法解决的问题, 因此将其弃置一旁.

1825 年在老师们有力推荐下, 阿贝尔申请到为期两年的研究基金, 游学欧陆. 期间,

数学天才阿贝尔的生前身后名 (续)

阿贝尔在柏林结识著名工程师、业余数学家克雷勒 (August Leopold Crelle). 后来, 在 Crelle 创办的世界第一份纯粹和应用数学期刊第一期上发表了关于一般五次方程不存在根式解的完整证明.

此外, 阿贝尔在欧洲游学期间开始研究椭圆函数、超椭圆函数以及一类后来以他名字命名的阿贝尔函数, 并于 1826 年 10 月完成了他一生中最重要的工作——代数微分的可加性定理, 提出了椭圆函数的双周期特性, 对椭圆积分理论基础作出了卓越贡献. 阿贝尔将题为《论一类非常广泛的超越函数的一般性质》的长达 65 页的论文呈交法国科学院, 科学院秘书傅立叶读了引言, 委托勒让德 (法国数学家、椭圆积分理论的奠基人之一) 负责审查. 论文引起了勒让得的重视, 并推荐给大数学家柯西. 勒让得引用古罗马诗人弗拉库斯的话, 称该论文是一个“比青铜还不朽的里程碑”, 但柯西却将之视为天方夜谭而不予理会, 把稿件放在什么地方, 竟记不起来了. 直到阿贝尔死后两年才有人去科学院将论文找出来, 1841 年才得以发表.

阿贝尔在数学方面的成就是多方面的. 除了五次方程之外, 还研究了更广的一类代数方程, 后人发现这是具有交换的伽罗瓦群的方程, 并称交换群为阿贝尔群. 阿贝尔还研究过无穷级数, 得到了一些判别准则以及关于幂级数求和的定理, 这些工作使他成为分析学严格化的推动者. 另外, 还完成了有关超越函数的研究报告, 展示代数函数理论, 被称为阿贝尔定理, 是后期阿贝尔积分及阿贝尔函数的理论基础. 阿贝尔的名字还与近代数学中许多概念和定理联系在一起，例如阿贝尔级数、阿贝尔可和性等等.

数学天才阿贝尔的生前身后名 (续)

尽管阿贝尔的成就极高, 生前却郁郁不得志, 特别是在他的祖国一直得不到应有的重视, 因此无法获得固定教席以专心于研究. 1827 年阿贝尔从欧洲回到挪威, 只能靠为学生补习功课糊口, 而且常常入不敷出, 还必须偿还从前欠下的债务. 不久, 阿贝尔染上肺结核病, 之后病情日益加重, 4 月 6 日凌晨在贫病与孤寂中死去.

在阿贝尔生前, 克雷勒十分关心和同情他的处境, 多方奔走呼吁, 希望通过自己对普鲁士政府的影响, 全力帮助这位纯良的天才在柏林谋得一个永久职位. 直到阿贝尔去世前不久, 人们才认识到他的价值. 1828 年, 四名法国科学院院士上书给挪威国王, 请他为阿贝尔提供合适的科学研究平台, 勒让德也在科学院会议上对阿贝尔大加赞赏. 可惜已经太迟了, 在阿贝尔去世两天后, 来自柏林大学的教学教授职位聘书才寄到他的家中. 此后荣誉和褒奖接踵而来, 阿贝尔去世一年后, 他和同时代的德国数学家卡尔 • 雅可比共同获得法国科学院著名的 Grand Prix 奖, 以褒奖两位当时世界上最有成就的数学家. 双方在完全不知道对方的情况下, 各自对椭圆函数进行独立研究, 是举世公认的椭圆函数论的两位独立奠基人, 被称为“椭圆双雄”. 椭圆函数的出现, 拉开了 19 世纪数学的核心研究领域之一——单复变函数的大幕.

阿贝尔死后从未离开过公众视线, 他的朋友、同行和民众均在媒体猛烈抨击奥斯陆大学校方、挪威当局和法国科学院里陈腐的官僚作风, 相关的反思和讨论在挪威的各种公开出版物上持续了 70 多年. 对阿贝尔的追念在 1902 年他诞辰 100 周年之际达到了顶点, 举办盛大庆典、建立阿贝尔纪念碑以及设立阿贝尔奖.

理工男的人文情怀 ——伽罗瓦作为史上最传奇的数学家, 一生都在作死.

小时候与数学老师互相看不起, 惨遭留级.

中学时写出了关于五次方程代数解（史上首次引入“群”概念）的论文, 寄给大数学家柯西, 要求他转交法兰西科学院审查. 结果柯西不屑一顾, 直接扔了.

次年写出三篇论文, 寄给科学院秘书傅立叶. 结果傅立叶暴毙, 文稿遗失.

第三年又写了论文, 寄给科学院院士泊松. 结果泊松批示：不知所云.

两次投考巴黎综合工科学校落榜, 只因在面试时无法容忍人类的愚蠢, 用黑板刷击中了主考官的面部. （打人不打脸啊!!!）

好不容易被巴黎高等师范学院录取, 却在校报上抨击校长, 惨遭退学.

他爹因不堪天主教而自杀, 伽罗瓦只身复仇, 以“企图暗杀国王罪”被捕. 获释之后上街示威, 再次被捕……在圣佩拉吉监狱度过了人生最后一年.

狱中爱上一个烟花女子, 出来以后找情敌决一死战. 情敌是军官（传说是位居全国前列的枪手）, 但他偏偏要跟人比枪. 决战前夜, 伽罗瓦已知不免, 通宵记下了自己研究数学五年的所得. 据说遗稿空白处还写着：我没有时间了, 没有时间了……享年 21 岁.

在被情敌击毙之后, 他的朋友 Chevalier 根据遗嘱, 将伽罗瓦的遗稿寄给了大数学家高斯, 高斯依然未予理睬.

伽罗瓦在天亮之前最后几个小时记下的内容, 解决了困扰数学家们长达几个世纪的难题, 开创了一门新的学科——近世 (抽象) 代数. 数十年后, 他的研究成果才被世界认可, 并成为现代计算机的理论基础.

目录

求代数方程 $f(x) = \sum_{i=0}^{i=n} c_i x_i = 0$ 的**根式解**一直是古典代数的中心课题.

对于一元二次方程 $ax^2 + bx + c = 0, a \neq 0$, 有一般求根公式

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

尽管其起源说法不一 (如公元前 2000 年左右的古巴比伦人、3 世纪三国时期的赵爽、7 世纪印度的婆罗摩笈多、8 世纪阿拉伯的花拉子密 (Al-Khwārizmi) 在其著作《代数学》中, 给出了上述实根的一般解法等), 但人们很早就掌握了这一结果.

求代数方程 $f(x) = \sum_{i=0}^{i=n} c_i x_i = 0$ 的**根式解**一直是古典代数的中心课题.

对于一元二次方程 $ax^2 + bx + c = 0, a \neq 0$, 有一般求根公式

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

尽管其起源说法不一 (如公元前 2000 年左右的古巴比伦人、3 世纪三国时期的赵爽、7 世纪印度的婆罗摩笈多、8 世纪阿拉伯的花拉子密 (Al-Khwārizmi) 在其著作《代数学》中, 给出了上述实根的一般解法等), 但人们很早就掌握了这一结果.

而一元三次、四次方程的解法一直到 16 世纪才出现. 当时, 意大利数学家帕乔利 (Luca Pacioli) 在一部百科全书式数学巨著最后以悲观的语调写道, “对于三次和四次方程, 直到现在 (16 世纪初) 还不可能形成一般规则”. 可能正是这语调的刺激, 他的同胞们纷纷对此发起挑战.

首先是费罗 (Scipione del Ferro) 发现了一元三次方程的解法, 但没有公开 (只传授了学生菲奥尔一部分——$x^3 + mx = n, m, n > 0$ 的解法).

首先是费罗 (Scipione del Ferro) 发现了一元三次方程的解法, 但没有公开 (只传授了学生菲奥尔一部分——$x^3 + mx = n, m, n > 0$ 的解法).

1535 年自学成才的塔塔利亚 (原名方塔纳, Nicolo Fontana) 在与菲奥尔“竞赛”时重复发现了一元三次方程的一般解法并战胜菲奥尔, 但对此解法也密而未宣, 后以诗歌密语的方式告诉了卡尔达诺 (Girolamo Cardano) 其中的一部分解法并让其保守秘密.

首先是费罗 (Scipione del Ferro) 发现了一元三次方程的解法, 但没有公开 (只传授了学生菲奥尔一部分——$x^3 + mx = n, m, n > 0$ 的解法).

1535 年自学成才的塔塔利亚 (原名方塔纳, Nicolo Fontana) 在与菲奥尔“竞赛”时重复发现了一元三次方程的一般解法并战胜菲奥尔, 但对此解法也密而未宣, 后以诗歌密语的方式告诉了卡尔达诺 (Girolamo Cardano) 其中的一部分解法并让其保守秘密.

后来卡尔达诺经过钻研把其他形式的一元三次方程也找出来, 从而得到了一元三次方程的一般解法. 紧接着, 卡尔达诺的学生兼助理费拉里 (Ludovico Ferrari) 把一元四次方程的解也求出来了, 即对一般的四次方程, 通过转化变为三次方程, 给出根式的一般解.

首先是费罗 (Scipione del Ferro) 发现了一元三次方程的解法, 但没有公开 (只传授了学生菲奥尔一部分——$x^3 + mx = n, m, n > 0$ 的解法).

1535 年自学成才的塔塔利亚 (原名方塔纳, Nicolo Fontana) 在与菲奥尔“竞赛”时重复发现了一元三次方程的一般解法并战胜菲奥尔, 但对此解法也密而未宣, 后以诗歌密语的方式告诉了卡尔达诺 (Girolamo Cardano) 其中的一部分解法并让其保守秘密.

后来卡尔达诺经过钻研把其他形式的一元三次方程也找出来, 从而得到了一元三次方程的一般解法. 紧接着, 卡尔达诺的学生兼助理费拉里 (Ludovico Ferrari) 把一元四次方程的解也求出来了, 即对一般的四次方程, 通过转化变为三次方程, 给出根式的一般解.

1543 年, 卡尔达诺和费拉里拜访费罗的学生兼女婿纳夫, 得知费罗早于塔塔利亚发现一元三次方程的解法, 便摒弃对塔塔利亚的承诺, 将其拓展的三次方程解法和费拉里的四次方程解法在 1545 年的著作《数学大典》(Ars Magns) 中公开发表.

首先是费罗 (Scipione del Ferro) 发现了一元三次方程的解法, 但没有公开 (只传授了学生菲奥尔一部分——$x^3 + mx = n, m, n > 0$ 的解法).

1535 年自学成才的塔塔利亚 (原名方塔纳, Nicolo Fontana) 在与菲奥尔“竞赛”时重复发现了一元三次方程的一般解法并战胜菲奥尔, 但对此解法也密而未宣, 后以诗歌密语的方式告诉了卡尔达诺 (Girolamo Cardano) 其中的一部分解法并让其保守秘密.

后来卡尔达诺经过钻研把其他形式的一元三次方程也找出来, 从而得到了一元三次方程的一般解法. 紧接着, 卡尔达诺的学生兼助理费拉里 (Ludovico Ferrari) 把一元四次方程的解也求出来了, 即对一般的四次方程, 通过转化变为三次方程, 给出根式的一般解.

1543 年, 卡尔达诺和费拉里拜访费罗的学生兼女婿纳夫, 得知费罗早于塔塔利亚发现一元三次方程的解法, 便摒弃对塔塔利亚的承诺, 将其拓展的三次方程解法和费拉里的四次方程解法在 1545 年的著作《数学大典》(Ars Magns) 中公开发表.

一元三次方程 $ax^3+bx^2+cx+d=0, a\neq 0$ 的求根公式：

$$x_1=-\frac{b}{3a}+\mu+\nu,$$
$$x_2=-\frac{b}{3a}+\omega_3\mu+\omega_3^2\nu,$$
$$x_3=-\frac{b}{3a}+\omega_3^2\mu+\omega_3\nu,$$

其中,

$$\omega_3=\frac{-1+i\sqrt{3}}{2},$$
$$\mu=\left(\frac{bc}{6a^2}-\frac{b^3}{27a^3}-\frac{d}{2a}+\sqrt{\Delta}\right)^{\frac{1}{3}},$$
$$\nu=\left(\frac{bc}{6a^2}-\frac{b^3}{27a^3}-\frac{d}{2a}-\sqrt{\Delta}\right)^{\frac{1}{3}},$$

而 $\Delta=\left(\frac{bc}{6a^2}-\frac{b^3}{27a^3}-\frac{d}{2a}\right)^2+\left(\frac{c}{3a}-\frac{b^2}{9a^2}\right)^3.$

该公式被称为卡尔达诺公式, 亦称为卡丹公式. 但在实际求根时有一定的局限性, 会出现用无理数表示有理数的情况. 譬如 $x^3-x-6=0$ 有解 $x=2$, 但用卡尔达诺公式却为 $\sqrt[3]{3+\frac{11\sqrt{6}}{9}}+\sqrt[3]{3-\frac{11\sqrt{6}}{9}}$.

一元四次方程 $ax^4+bx^3+cx^2+dx+e=0, a\neq 0$ 的求根公式：

$$x_1=-\frac{b}{4a}-\frac{1}{2}\sqrt{\delta_1+\Delta_3}-\frac{1}{2}\sqrt{2\delta_1-\Delta_3+\frac{\delta_2}{4\sqrt{\delta_1+\Delta_3}}},$$

$$x_2=-\frac{b}{4a}-\frac{1}{2}\sqrt{\delta_1+\Delta_3}+\frac{1}{2}\sqrt{2\delta_1-\Delta_3+\frac{\delta_2}{4\sqrt{\delta_1+\Delta_3}}},$$

$$x_3=-\frac{b}{4a}+\frac{1}{2}\sqrt{\delta_1+\Delta_3}-\frac{1}{2}\sqrt{2\delta_1-\Delta_3-\frac{\delta_2}{4\sqrt{\delta_1+\Delta_3}}},$$

$$x_4=-\frac{b}{4a}+\frac{1}{2}\sqrt{\delta_1+\Delta_3}-\frac{1}{2}\sqrt{2\delta_1-\Delta_3-\frac{\delta_2}{4\sqrt{\delta_1+\Delta_3}}},$$

其中，

$$\delta_1=\frac{b^2}{4a^2}-\frac{2c}{3a},$$

$$\delta_2=\frac{b^3}{a^3}-\frac{4bc}{a^2}+\frac{8d}{a},$$

$$\Delta_3=\frac{\sqrt[3]{\omega_3+\sqrt{\Delta}}+\sqrt[3]{\omega_3-\sqrt{\Delta}}}{3\sqrt[3]{2}a},$$

而 $\omega_3=2c^3-9bcd+27ad^2+27b^2e-72ace,$

$$\Delta=\omega_3^2-4(c^2-3bd+12ae)^3.$$

从 16 世纪后半叶直到 19 世纪初, 人们一直在致力于寻找一元五次方程的根式解, 但无一不以失败告终.

1770 年拉格朗日整理了各种求根技巧并最早研究了根之间的置换理论, 同时研究通过先解一个 $n-1$ 次方程然后去求 n 次方程的根, 但没有成功.

从 16 世纪后半叶直到 19 世纪初, 人们一直在致力于寻找一元五次方程的根式解, 但无一不以失败告终.

1770 年拉格朗日整理了各种求根技巧并最早研究了根之间的置换理论, 同时研究通过先解一个 $n-1$ 次方程然后去求 n 次方程的根, 但没有成功.

也许是看到拉格朗日这么有创意的想法都不能找到五次方程的求根公式, 人们开始朝着相反的方向努力.

1799 年鲁菲尼 (Paolo Ruffini) 率先表示五次以上的一般代数方程不可能有求根公式, 到 1813 年的 14 年间发表了六个不同版本的五次方程不存在通解的证明, 但鲁菲尼的理论中存在一个重要的假设一直没有完全证明.

从 16 世纪后半叶直到 19 世纪初, 人们一直在致力于寻找一元五次方程的根式解, 但无一不以失败告终.

1770 年拉格朗日整理了各种求根技巧并最早研究了根之间的置换理论, 同时研究通过先解一个 $n-1$ 次方程然后去求 n 次方程的根, 但没有成功.

也许是看到拉格朗日这么有创意的想法都不能找到五次方程的求根公式, 人们开始朝着相反的方向努力.

1799 年鲁菲尼 (Paolo Ruffini) 率先表示五次以上的一般代数方程不可能有求根公式, 到 1813 年的 14 年间发表了六个不同版本的五次方程不存在通解的证明, 但鲁菲尼的理论中存在一个重要的假设一直没有完全证明.

1824 年, 阿贝尔独立于鲁菲尼证明了五次及以上方程不存在根式通解 (其中包括鲁菲尼没能证明的部分, 现称为阿贝尔定理), 这一结论被称为阿贝尔 -鲁菲尼定理.

另一方面, 1799 年 22 岁的高斯在博士论文中证明了每个实系数多项式至少有一个实根或复根, 这个结论被称为” 代数学基本定理”, 开创了探讨数学研究中关于根存在性问题的新途径.

三年后高斯证明了分圆方程可用根式求解, 因此何种高次方程能用根式求解又成为摆在数学家面前的一道难题. 于是, 就有了后来伽罗瓦开创性的工作.

受拉格朗日想法的启发, 伽罗瓦 (独立于阿贝尔的证明) 创造性地引入改变数学历史进程的一个概念：群. 对于任意一个有理多项式 $f(x)$, 伽罗瓦的办法是：从 $f(x)$ 出发找到一个特别的群 (现在称为 $f(x)$ 的 Galois 群), 证明了 $f(x) = 0$ 可以根式解当且仅当 Galois 群是一个交换群 (后人也称之为 Abel 群).

另一方面, 1799 年 22 岁的高斯在博士论文中证明了每个实系数多项式至少有一个实根或复根, 这个结论被称为" 代数学基本定理", 开创了探讨数学研究中关于根存在性问题的新途径.

三年后高斯证明了分圆方程可用根式求解, 因此何种高次方程能用根式求解又成为摆在数学家面前的一道难题. 于是, 就有了后来伽罗瓦开创性的工作.

受拉格朗日想法的启发, 伽罗瓦 (独立于阿贝尔的证明) 创造性地引入改变数学历史进程的一个概念：群. 对于任意一个有理多项式 $f(x)$, 伽罗瓦的办法是：从 $f(x)$ 出发找到一个特别的群 (现在称为 $f(x)$ 的 Galois 群), 证明了 $f(x) = 0$ 可以根式解当且仅当 Galois 群是一个交换群 (后人也称之为 Abel 群).

要证明上面这个结论, 需要用到接下来的几乎所有知识, 譬如群、置换、交换群、正规子群、单群、交错群、同构、环与域、域的扩张、Galois 群、Galois 基本定理等，甚至课程之外的换位子群、可解群等.

定义 6.1.1

设 S 是一个非空集合. 称 $S \times S$ 到 S 的映射为 S 的**结合法或运算**, 记作

$$S \times S \to S$$

$$(a, b) \mapsto ab$$

定义 6.1.1

设 S 是一个非空集合. 称 $S \times S$ 到 S 的映射为 S 的**结合法**或**运算**, 记作

$$S \times S \to S$$

$$(a, b) \mapsto ab$$

注：此时, 我们称映射满足封闭性.

对于这个映射, 元素对 (a, b) 的像叫做 a 与 b 的**乘积**, 记作 $a \otimes b$ 或 $a \cdot b$ 或 $a * b$ 等, 简记为 ab. 这个运算叫做**乘法**.

人们也常把该运算叫做**加法**, 此时元素对 (a, b) 的像叫做 a 与 b 的**和**, 记作 $a \oplus b$ 或 $a + b$.

这时, S 叫做**代数系统**.

例 6.1.1　自然数集 $\mathbb{N} = \{0,\ 1,\ 2, \cdots,\ n, \cdots\}$.

① 定义“$+$”：普通加法,

$\forall\ a, b \in \mathbb{N}, a + b \in \mathbb{N}$.

所以,“$+$”是 $\mathbb{N} \times \mathbb{N}$ 到 $\mathbb{N}$ 的运算, 或称 $\mathbb{N}$ 对映射“$+$”满足封闭性.

② 定义“$\cdot$”：普通乘法,

$\forall\ a, b \in \mathbb{N}, a \cdot b \in \mathbb{N}$.

称 $\mathbb{N}$ 对映射“$\cdot$”满足封闭性.

③ 定义“$-$”：普通减法,

$a = 2, b = 5, a - b = -3 \notin \mathbb{N}$, 所以, $\mathbb{N}$ 对映射“$-$”不满足封闭性.

定义 6.1.2

设 S 是一个具有运算的非空集合. 如果 $a, b, c,$ 都是 S 中的元素, 则我们有两种方式得到它们的乘积 $(ab)c$ 和 $a(bc)$. 如果对 S 中的任意元素 $a, b, c,$ 都有 $(ab)c = a(bc)$, 则称该运算满足**结合律**.

定义 6.1.2

设 S 是一个具有运算的非空集合. 如果 $a, b, c,$ 都是 S 中的元素, 则我们有两种方式得到它们的乘积 $(ab)c$ 和 $a(bc)$. 如果对 S 中的任意元素 $a, b, c,$ 都有 $(ab)c = a(bc)$, 则称该运算满足**结合律**.

例 6.1.2 对于 $A = \{$ 所有整数 $\}$,

运算 $+$: 普通加法, 则 $(a + b) + c = a + (b + c)$, 满足结合律;

运算 $-$: 普通减法, 则 $(a - b) - c \neq a - (b - c)$, 不满足结合律, 除非 $c = 0$.

例 6.1.3 对于集合 $\{a, b, c\}$, 定义运算 $\circ$ 如下：

$\circ$	a	b	c
a	a	b	c
b	c	b	a
c	b	a	c

验证是否满足结合律？

解：$(xy)z = x(yz)$ 共需验证 $3 \times 3 \times 3 = 27$ 个.

(i) $(a \circ b) \circ c = b \circ c = a,\ a \circ (b \circ c) = a \circ a = a.$

(ii) $(b \circ a) \circ c = c \circ c = c,\ b \circ (a \circ c) = b \circ c = a.$

所以, 不满足结合律.

定义 6.1.3

设 S 是一个具有运算的非空集合. 如果 S 满足结合律, 那么 S 叫做一个**半群**.

定义 6.1.3

设 S 是一个具有运算的非空集合. 如果 S 满足结合律, 那么 S 叫做一个**半群**.

定义 6.1.4

设 S 是一个具有运算的非空集合. 如果 S 中有一个元素 e, 使得对 S 中所有元素 a, 都有 $ea = ae = a$ 成立, 则称该元素 e 为 S 中的**单位元**.

定义 6.1.3

设 S 是一个具有运算的非空集合. 如果 S 满足结合律, 那么 S 叫做一个**半群**.

定义 6.1.4

设 S 是一个具有运算的非空集合. 如果 S 中有一个元素 e, 使得对 S 中所有元素 a, 都有 $ea = ae = a$ 成立, 则称该元素 e 为 S 中的**单位元**.

注：当 S 的运算写作加法时, 这个 e 叫做 S 中的零元, 通常记作 0.

定义 6.1.3

设 S 是一个具有运算的非空集合. 如果 S 满足结合律, 那么 S 叫做一个**半群**.

定义 6.1.4

设 S 是一个具有运算的非空集合. 如果 S 中有一个元素 e, 使得对 S 中所有元素 a, 都有 $ea = ae = a$ 成立, 则称该元素 e 为 S 中的**单位元**.

注：当 S 的运算写作加法时, 这个 e 叫做 S 中的零元, 通常记作 0.

性质 6.1.1

设 S 是一个具有运算的非空集合, 则 S 中的单位元 e 是唯一的.

定义 6.1.3

设 S 是一个具有运算的非空集合. 如果 S 满足结合律, 那么 S 叫做一个**半群**.

定义 6.1.4

设 S 是一个具有运算的非空集合. 如果 S 中有一个元素 e, 使得对 S 中所有元素 a, 都有 $ea = ae = a$ 成立, 则称该元素 e 为 S 中的**单位元**.

注：当 S 的运算写作加法时, 这个 e 叫做 S 中的零元, 通常记作 0.

性质 6.1.1

设 S 是一个具有运算的非空集合, 则 S 中的单位元 e 是唯一的.

证：设 e 和 e' 都是 S 中的单位元. 由单位元的定义知, $e' = ee' = e$. 因此, 单位元是唯一的.

例 6.1.4 对 $N = \{a, b, c\}$, 运算为 $\circ$.

$\circ$	a	b	c
a	a	b	c
b	c	b	a
c	b	a	c

则元素 a 为 N 中的单位元. 因为

$$a \circ a = a, \quad a \circ b = b, \quad a \circ c = c, \quad b \circ a = b, \quad c \circ a = c.$$

定义 6.1.5

设 S 是一个具有运算且有单位元的非空集合, a 是 S 中的一个元素. 如果 S 中存在一个元素 a' 使得 $aa' = a'a = e$, 则称该元素 a 为**可逆元**, 称 a' 为 a 的**逆元**, 通常记作 a^{-1}.

定义 6.1.5

设 S 是一个具有运算且有单位元的非空集合, a 是 S 中的一个元素. 如果 S 中存在一个元素 a' 使得 $aa' = a'a = e$, 则称该元素 a 为**可逆元**, 称 a' 为 a 的**逆元**, 通常记作 a^{-1}.

注：当 S 的运算叫做加法时, 这个 a' 叫做元素 a 的**负元**, 通常记作 $-a$.

定义 6.1.5

设 S 是一个具有运算且有单位元的非空集合, a 是 S 中的一个元素. 如果 S 中存在一个元素 a' 使得 $aa' = a'a = e$, 则称该元素 a 为**可逆元**, 称 a' 为 a 的**逆元**, 通常记作 a^{-1}.

注：当 S 的运算叫做加法时, 这个 a' 叫做元素 a 的**负元**, 通常记作 $-a$.

性质 6.1.2

设 S 是一个有单位元的半群, 则对 S 中的任意可逆元 a, 其逆元 a' 是唯一的.

定义 6.1.5

设 S 是一个具有运算且有单位元的非空集合, a 是 S 中的一个元素. 如果 S 中存在一个元素 a' 使得 $aa' = a'a = e$, 则称该元素 a 为**可逆元**, 称 a' 为 a 的**逆元**, 通常记作 a^{-1}.

注：当 S 的运算叫做加法时, 这个 a' 叫做元素 a 的**负元**, 通常记作 $-a$.

性质 6.1.2

设 S 是一个有单位元的半群, 则对 S 中的任意可逆元 a, 其逆元 a' 是唯一的.

证：设 a' 和 a'' 都是 a 的逆元, 即 $aa' = a'a = e$, $aa'' = a''a = e$. 根据半群满足结合律得到, $a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a''$. 因此, a 的逆元 a' 是唯一的.

例 6.1.5 对 $N = \{a, b, c\}$, 运算为 $\circ$.

$\circ$	a	b	c
a	a	b	c
b	c	b	a
c	b	a	c

元素 a 为 N 中的单位元, 且有

$$b \circ c = a, \quad c \circ b = a, \quad \therefore b^{-1} = c.$$

定义 6.1.6

设 S 是一个具有运算的非空集合. 如果 a, b 都是 S 中的元素, 则我们有两种方式得到它们的乘积 ab 和 ba. 如果对 S 中的任意元素 a, b, 都有 $ba = ab$, 则称该运算满足**交换律**.

定义 6.1.6

设 S 是一个具有运算的非空集合. 如果 a, b 都是 S 中的元素, 则我们有两种方式得到它们的乘积 ab 和 ba. 如果对 S 中的任意元素 a, b, 都有 $ba = ab$, 则称该运算满足**交换律**.

例 6.1.6 设 S 是矩阵集合, 定义“$\times$”为矩阵乘法, 则对 $\forall\, A, B \in S$, 不总能有 $AB = BA$. 如

$$A = \begin{pmatrix} 1 & 2 \end{pmatrix}, B = \begin{pmatrix} 1 \\ 3 \end{pmatrix},$$

$$A \times B = \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 1 \\ 3 \end{pmatrix} = 1 \times 1 + 2 \times 3 = 7,$$

$$B \times A = \begin{pmatrix} 1 \\ 3 \end{pmatrix} \begin{pmatrix} 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 6 \end{pmatrix},$$

即运算“$\times$”不满足交换律.

定义 6.1.7

设 G 是一个具有运算的非空集合. 如果 G 中的运算满足以下条件:

(i) 结合律, 即对任意的 $a, b, c \in G$, 都有 $(ab)c = a(bc)$;

(ii) 单位元, 即存在元素 $e \in G$, 使得对任意的 $a \in G$, 都有 $ae = ea = a$;

(iii) 可逆性, 即对任意的 $a \in G$, 都存在 $a' \in G$ 使得 $aa' = a'a = e$.

则称 G 为一个**群**.

定义 6.1.7

设 G 是一个具有运算的非空集合. 如果 G 中的运算满足以下条件:

(i) 结合律, 即对任意的 $a, b, c \in G$, 都有 $(ab)c = a(bc)$;

(ii) 单位元, 即存在元素 $e \in G$, 使得对任意的 $a \in G$, 都有 $ae = ea = a$;

(iii) 可逆性, 即对任意的 $a \in G$, 都存在 $a' \in G$ 使得 $aa' = a'a = e$.

则称 G 为一个**群**.

注：群满足封闭性、结合律、单位元、逆元.

定义 6.1.7

设 G 是一个具有运算的非空集合. 如果 G 中的运算满足以下条件:

(i) 结合律, 即对任意的 $a, b, c \in G$, 都有 $(ab)c = a(bc)$;

(ii) 单位元, 即存在元素 $e \in G$, 使得对任意的 $a \in G$, 都有 $ae = ea = a$;

(iii) 可逆性, 即对任意的 $a \in G$, 都存在 $a' \in G$ 使得 $aa' = a'a = e$.

则称 G 为一个**群**.

注：群满足封闭性、结合律、单位元、逆元.

注：当 G 的运算写作乘法时, G 叫做**乘群**;

当 G 的运算写作加法时, G 叫做**加群**.

定义 6.1.7

设 G 是一个具有运算的非空集合. 如果 G 中的运算满足以下条件:

(i) 结合律, 即对任意的 $a, b, c \in G$, 都有 $(ab)c = a(bc)$;

(ii) 单位元, 即存在元素 $e \in G$, 使得对任意的 $a \in G$, 都有 $ae = ea = a$;

(iii) 可逆性, 即对任意的 $a \in G$, 都存在 $a' \in G$ 使得 $aa' = a'a = e$.

则称 G 为一个**群**.

注: 群满足封闭性、结合律、单位元、逆元.

注: 当 G 的运算写作乘法时, G 叫做**乘群**;

当 G 的运算写作加法时, G 叫做**加群**.

定义 6.1.8

群 G 的元素个数叫做群 G 的**阶**, 记作 $|G|$. 当 $|G|$ 为有限数时, G 叫做**有限群**; 否则, G 叫做**无限群**.

定义 6.1.9

如果群 G 中的运算满足交换律, 即对任意的 $a, b \in G$, 都有 $ba = ab$, 那么 G 叫做一个**交换群**, 或**阿贝尔** (Abel) **群**.

定义 6.1.9

如果群 G 中的运算满足交换律, 即对任意的 $a, b \in G$, 都有 $ba = ab$, 那么 G 叫做一个**交换群**, 或**阿贝尔** (Abel) **群**.

例 6.1.7 (1) 自然数集 $\mathbb{N} = \{0, 1, \cdots\}$, 映射 "$+$" 为普通加法运算, 则

(i) 满足封闭性.

(ii) 具有结合律.

(iii) 没有零元和负元.

所以, $\mathbb{N}$ 对 "$+$" 是半群.

(2) 自然数集 $\mathbb{N}$, 映射 "$\cdot$" 为普通乘法运算, 则

(i) 满足封闭性.

(ii) 满足结合律.

(iii) 有单位元 1.

(iv) 没有逆元, 因为对 $\forall\, a \neq 1 \in \mathbb{N}$, 没有 a', 使得 $a \cdot a' = 1$.

例 6.1.8 请回答：

(1) 整数集 $\mathbb{Z} = \{\cdots, -n, \cdots, -2, -1, 0, 1, 2, \cdots, n, \cdots\}$ 对于通常意义下的加法“$+$”, 构成交换群吗？

(2) 非零整数集 $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ 对于通常意义下的乘法”$\cdot$”, 构成群吗？

答：对于问题 (1):

(i) 满足封闭性: $\forall\ a, b \in \mathbb{Z},\ a + b \in \mathbb{Z}$.

(ii) 满足结合律: $\forall\ a, b, c \in \mathbb{Z},\ (a + b) + c = a + (b + c)$.

(iii) 有零元 0: $\forall\ a \in \mathbb{Z},\ a + 0 = 0 + a = a$.

(iv) 有负元: $\forall\ a \in \mathbb{Z}, \exists -a \in \mathbb{Z},\ a + (-a) = (-a) + a = 0$.

(v) 满足交换律: $\forall\ a, b \in \mathbb{Z},\ a + b = b + a$.

因此, $\mathbb{Z}$ 是一个交换加群.

例 6.1.8 请回答：

(1) 整数集 $\mathbb{Z} = \{\cdots, -n, \cdots, -2, -1, 0, 1, 2, \cdots, n, \cdots\}$ 对于通常意义下的加法“$+$”, 构成交换群吗？

(2) 非零整数集 $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ 对于通常意义下的乘法”$\cdot$”, 构成群吗？

答：对于问题 (1):

(i) 满足封闭性: $\forall\ a, b \in \mathbb{Z},\ a + b \in \mathbb{Z}$.

(ii) 满足结合律: $\forall\ a, b, c \in \mathbb{Z},\ (a + b) + c = a + (b + c)$.

(iii) 有零元 0: $\forall\ a \in \mathbb{Z},\ a + 0 = 0 + a = a$.

(iv) 有负元: $\forall\ a \in \mathbb{Z}, \exists -a \in \mathbb{Z},\ a + (-a) = (-a) + a = 0$.

(v) 满足交换律: $\forall\ a, b \in \mathbb{Z},\ a + b = b + a$.

因此, $\mathbb{Z}$ 是一个交换加群.

对于问题 (2):

(i) 满足封闭性: $\forall\ a, b \in \mathbb{Z}^*,\ a \cdot b \in \mathbb{Z}^*$.

(ii) 满足结合律: $\forall\ a, b, c \in \mathbb{Z}^*,\ (a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(iii) 有单位元 1: $\forall\ a \in \mathbb{Z}^*,\ a \cdot 1 = 1 \cdot a = a.$

(iv) 没有逆元: $\forall\ a \neq 1 \in \mathbb{Z}^*$, 不存在 $a' \in \mathbb{Z}^*$, 使得 $a \cdot a' = a' \cdot a = 1.$

(iii) 有单位元 1: $\forall\, a \in \mathbb{Z}^*,\ a \cdot 1 = 1 \cdot a = a.$

(iv) 没有逆元: $\forall\, a \neq 1 \in \mathbb{Z}^*$, 不存在 $a' \in \mathbb{Z}^*$, 使得 $a \cdot a' = a' \cdot a = 1.$

例 6.1.9　有理数集 $\mathbb{Q}$、实数集 $\mathbb{R}$ 和复数集 $\mathbb{C}$,

(1) 对于通常意义下的加法, (封闭、结合律、单位元 0、逆元 $-a$ 和交换律), 是交换加群.

(2) 对于通常意义下的乘法, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$、$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ 和 $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ 满足封闭性、结合律、单位元 1、逆元 $a^{-1} = \frac{1}{a}$ 和交换律, 因此 $\mathbb{Q}^*$、$\mathbb{R}^*$ 和 $\mathbb{C}^*$ 都是交换乘群.

例 6.1.10 设 D 是一个非平方整数, 则集合

$$\mathbb{Z}(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}.$$

(1) 对于加法运算 $\oplus$:

$$(a + b\sqrt{D}) \oplus (c + d\sqrt{D}) = (a + c) + (b + d)\sqrt{D}$$

验证:

(i) 封闭性: $\forall\ A, B \in \mathbb{Z}(\sqrt{D}),\ A \oplus B \in \mathbb{Z}(\sqrt{D})$.

(ii) 结合律: $\forall\ A, B, C \in \mathbb{Z}(\sqrt{D}),\ (A \oplus B) \oplus C = A \oplus (B \oplus C)$.

(iii) 有单位元 0.

(iv) 负元: $\forall A = a + b\sqrt{D} \in \mathbb{Z}(\sqrt{D}), A^{-1} = -A = -a - b\sqrt{D}$.

此外满足交换律, 所以 $\mathbb{Z}(\sqrt{D})$ 构成一个交换加群 (Abel 加群).

(2) 对于乘法运算 $\otimes$:

$$(a+b\sqrt{D})\otimes(c+d\sqrt{D})=(ac+bdD)+(bc+ad)\sqrt{D}$$

验证:

(i) 封闭性.

(ii) 结合律.

(iii) 有单位元 1, 即 $c=1,d=0$, 有

$$\begin{cases} ac+bdD=a \\ bc+ad=b \end{cases},$$

即单位元为 1.

(iv) 至于逆元, 不是每个元素 $a+b\sqrt{D}$ 都有逆元, 譬如 2 无逆元.

所以, $\mathbb{Z}(\sqrt{D})$ 不构成一个乘群.

例 6.1.11 设 n 是一个正整数, 集合

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \cdots, n-1\},$$

证明: 集合 $\mathbb{Z}_n$ 对于加法运算 $\oplus$:

$$a \oplus b = a + b \mod n$$

构成一个交换加群, 其中 $a \mod n$ 是整数 a 模 n 的最小非负剩余.

证：满足：

(i) 封闭性.

(ii) 结合律.

(iii) 有单位元 (零元 0).

(iv) 可逆性 (有负元):

$$\forall\, a \in \mathbb{Z}_n,\ \exists\, n-a \in \mathbb{Z}_n \text{ 使得 } a \oplus (n-a) \equiv 0 \mod n.$$

(v) 交换律.

所以, $\mathbb{Z}_n$ 是交换加群.

例如, $n = 6$, 对于 $\mathbb{Z}_6 = \mathbb{Z}/6\mathbb{Z} = \{0, 1, 2, 3, 4, 5\}$:

$a \oplus b$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

例如, $n = 6$, 对于 $\mathbb{Z}_6 = \mathbb{Z}/6\mathbb{Z} = \{0, 1, 2, 3, 4, 5\}$:

$a \oplus b$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

注: $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \cdots, n-1\}$ 叫做**模 n 剩余类加群**, 其中 $n\mathbb{Z} = \{n, 2n, 3n, \cdots\}$, 如 $2\mathbb{Z} = \{\cdots, -2, 0, 2, 4, 6, \cdots\}$.

例 6.1.12 设 p 是一个素数, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$, 证明：集合 $\mathbb{F}_p^*$ 对于乘法运算 $\otimes$:

$$a \otimes b = a \cdot b \mod p$$

构成一个交换乘群.

证：满足：

(i) 封闭性. (ii) 结合律.

(iii) 有单位元 1. (iv) 交换律成立.

(v) 可逆性：任意元素有逆元.

事实上, 根据定理 2.2.9, 若 m 是一个正整数, a 满足 $(a, m) = 1$, 则存在整数 $a', 1 \leq a' \leq m$, 使得 $aa' \equiv 1 \mod m$, 所以有

$$\mathbb{F}_p^* = \{0, 1, \cdots, p-1\}, \forall\, a \in \mathbb{F}_p^*, (a, p) = 1,$$

$$\therefore\ a' \in \mathbb{F}_p^*, \text{使得 } aa' \equiv 1 \mod p.$$

所以是交换乘群.

例如, 对于 $p = 7$.

$a \otimes b$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

例 6.1.13 设 n 是一个合数. 证明：集合 $\mathbb{Z}_n \setminus \{0\} = \{1,\ 2, \cdots,\ n-1\}$ 对于乘法运算 $\otimes : a \otimes b = a \cdot b \mod n$ 不构成一个乘群.

例 6.1.13 设 n 是一个合数. 证明：集合 $\mathbb{Z}_n \setminus \{0\} = \{1,\ 2, \cdots,\ n-1\}$ 对于乘法运算 $\otimes : a \otimes b = a \cdot b \mod n$ 不构成一个乘群.

证：集合 $\mathbb{Z}_n \setminus \{0\}$ 对于乘法满足结合律且存在单位元 1.

但并不是所有元素都是可逆元, 如 n 的真因数 d 没有逆元,

因为对任意的 $d' \in \mathbb{Z}_n \setminus \{0\}$, 都有 $d \otimes d' = d \cdot d' \mod n \neq 1$.

例如, $n = 6$, 即 $\mathbb{Z}/6\mathbb{Z} \setminus \{0\} = \{1, 2, 3, 4, 5\}$.

则 $1^{-1} = 1, 5^{-1} = 5$, 而 $2^{-1}, 3^{-1}, 4^{-1}$ 不存在.

$a \otimes b$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

例 6.1.14 设 n 是一个合数, $\mathbb{Z}_n^* = \{a \mid a \in \mathbb{Z}_n, (a,n) = 1\}$, 则集合 $\mathbb{Z}_n^*$ 对于乘法运算 $\otimes : a \otimes b = a \cdot b \mod n$ 构成一个交换乘群.

证：具有结合律, 单位元是 1, a 的逆元是 $a^{-1} \mod n$.

例如, $n = 15$.

$a \otimes b$	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

例 6.1.15 设有元素在数域 $\mathbb{K}$ 中的全体 n 级矩阵组成的集合

$$M_n(\mathbb{K}) = \{(a_{ij})_{1\leqslant i\leqslant n,\ 1\leqslant j\leqslant n} \mid a_{ij} \in \mathbb{K}, 1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n\}.$$

(1) 设 $A = (a_{ij})$, $B = (b_{ij}) \in M_n(\mathbb{K})$, 定义加法：$A + B = C = (c_{ij})$, 其中 $c_{ij} = a_{ij} + b_{ij}$, $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant n$, 则 $M_n(\mathbb{K})$ 对于加法有结合律、交换律和零元 0, 并且每个元素 $A = (a_{ij})$ 都有负元 $-A = (-a_{ij})$, 因此 $M_n(\mathbb{K})$ 构成一个交换加群.

例如, $n = 2$,

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} \\ a_{21}+b_{21} & a_{22}+b_{22} \end{pmatrix},$$

零元是 $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ 的负元为 $\begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix}$.

例 6.1.15 设有元素在数域 $\mathbb{K}$ 中的全体 n 级矩阵组成的集合

$$M_n(\mathbb{K}) = \{(a_{ij})_{1\leqslant i\leqslant n,\ 1\leqslant j\leqslant n} \mid a_{ij} \in \mathbb{K}, 1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n\}.$$

(1) 设 $A = (a_{ij})$, $B = (b_{ij}) \in M_n(\mathbb{K})$, 定义加法：$A + B = C = (c_{ij})$, 其中 $c_{ij} = a_{ij} + b_{ij}$, $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant n$, 则 $M_n(\mathbb{K})$ 对于加法有结合律、交换律和零元 0, 并且每个元素 $A = (a_{ij})$ 都有负元 $-A = (-a_{ij})$, 因此 $M_n(\mathbb{K})$ 构成一个交换加群.

例如, $n = 2$,

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} \\ a_{21}+b_{21} & a_{22}+b_{22} \end{pmatrix},$$

零元是 $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ 的负元为 $\begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix}$.

(2) 设 $A = (a_{ij})$, $B = (b_{ij}) \in M_n(\mathbb{K})$, 再定义乘法：$A \cdot B = C = (c_{ij})$, 其中

$c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj},\ 1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n$, 则 $M_n(\mathbb{K}) \setminus \{0\}$ 对于乘法不构成一个群. 为什么？

$c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj},\ 1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n$, 则 $M_n(\mathbb{K}) \setminus \{0\}$ 对于乘法不构成一个群. 为什么？ 因为此时乘法不满足运算的封闭性. 例如,

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

$c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$, $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant n$, 则 $M_n(\mathbb{K}) \setminus \{0\}$ 对于乘法不构成一个群. 为什么？ 因为此时乘法不满足运算的封闭性. 例如,

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

(3) 可逆矩阵 A (即存在 A' 使得 $AA' = A'A = I_n$) 所组成的集合, 记作 $\mathrm{GL}_n(\mathbb{K})$, 对于矩阵的乘法构成一个群, 通常称 $\mathrm{GL}_n(\mathbb{K})$ 为 n 级**一般线性群**; $\mathrm{GL}_n(\mathbb{K})$ 中全体行列式为 1 的矩阵对于矩阵乘法也构成一个群, 记作 $\mathrm{SL}_n(\mathbb{K})$, 称为**特殊线性群**.

例如, $n = 2, \mathrm{SL}_2(\mathbb{K})$ 中的乘法为

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix},$$

单位元是 $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ 的逆元为 $\begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}$.

下面讨论 n 个元素的乘积.

设 $a_1, a_2, \cdots, a_{n-1}, a_n$ 是群 G 中的 n 个元素.

通常归纳地定义这 n 个元素的乘积为

$$a_1 a_2 \cdots a_{n-1} a_n = (a_1 a_2 \cdots a_{n-1}) a_n.$$

即两两运算.

当 G 的元素叫做加法时, 通常归纳地定义这 n 个元素的和为

$$a_1 + a_2 + \cdots + a_{n-1} + a_n = (a_1 + a_2 + \cdots + a_{n-1}) + a_n.$$

性质 6.1.3

设 $a_1, a_2, \cdots, a_{n-1}, a_n$ 是群 G 中的 $n \geqslant 2$ 个元素, 则对任意的 $1 \leqslant i_1 < \cdots < i_k < n$, 有 $(a_1 \cdots a_{i_1}) \cdots (a_{i_k+1} \cdots a_n) = a_1 a_2 \cdots a_{n-1} a_n$.

性质 6.1.3

设 $a_1, a_2, \cdots, a_{n-1}, a_n$ 是群 G 中的 $n \geqslant 2$ 个元素, 则对任意的 $1 \leqslant i_1 < \cdots < i_k < n$, 有 $(a_1 \cdots a_{i_1}) \cdots (a_{i_k+1} \cdots a_n) = a_1 a_2 \cdots a_{n-1} a_n$.

证：对 n 作数学归纳法.

当 $n = 3$ 时, 由结合律得, $a_1(a_2 a_3) = (a_1 a_2) a_3 = a_1 a_2 a_3$. 结论成立.

假设 $n - 1$ 时结论成立.

对于 n, 如果 $i_k + 1 = n$, 则根据归纳假设,

$$(a_1 \cdots a_{i_1}) \cdots (a_{i_k+1} \cdots a_n) = (a_1 a_2 \cdots a_{n-1}) a_n = a_1 a_2 \cdots a_{n-1} a_n.$$

如果 $i_k + 1 < n$, 则根据归纳假设和结合律,

$$(a_1 \cdots a_{i_1}) \cdots (a_{i_{k-1}+1} \cdots a_{i_k})(a_{i_k+1} \cdots a_n)$$

$$= (a_1 \cdots a_{i_k})(a_{i_k+1} \cdots a_{n-1}) a_n = (a_1 a_2 \cdots a_{n-1}) a_n = a_1 a_2 \cdots a_{n-1} a_n.$$

结论成立.

根据数学归纳法原理, 结论对任意 n 成立.

性质 6.1.4

设 $a_1, a_2, \cdots, a_{n-1}, a_n$ 是群 G 中的任意 $n \geqslant 2$ 个元素，则

$$(a_1 a_2 \cdots a_{n-1} a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_2^{-1} a_1^{-1}.$$

性质 6.1.4

设 $a_1, a_2, \cdots, a_{n-1}, a_n$ 是群 G 中的任意 $n \geqslant 2$ 个元素, 则

$$(a_1 a_2 \cdots a_{n-1} a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_2^{-1} a_1^{-1}.$$

证：当 $n = 2$ 时, 根据性质 6.1.3, 有

$$(a_1 a_2)(a_2^{-1} a_1^{-1}) = a_1 (a_2 a_2^{-1}) a_1^{-1} = a_1 a_1^{-1} = e.$$

和

$$(a_2^{-1} a_1^{-1})(a_1 a_2) = a_2^{-1} (a_1^{-1} a_1) a_2 = a_2 a_2^{-1} = e.$$

所以, $(a_1 a_2)^{-1} = a_2^{-1} a_1^{-1}$.

假设 $n - 1$ 时结论成立. 对于 n, 由情形 $n = 2$ 及归纳假设, 有

$$\begin{aligned}(a_1 a_2 \cdots a_{n-1} a_n)^{-1} &= \big((a_1 a_2 \cdots a_{n-1}) a_n\big)^{-1} \\ &= a_n^{-1} (a_1 a_2 \cdots a_{n-1})^{-1} \\ &= a_n^{-1} a_{n-1}^{-1} \cdots a_2^{-1} a_1^{-1}.\end{aligned}$$

结论成立.

性质 6.1.5

设 $a_1, a_2, \cdots, a_n$ 是交换群 G 中的任意 $n \geqslant 2$ 个元素, 则对 $1, 2, \cdots, n$ 的任一排列 $i_1, i_2, \cdots, i_n$, 有

$$a_{i_1} a_{i_2} \cdots a_{i_n} = a_1 a_2 \cdots a_n.$$

性质 6.1.5

设 $a_1, a_2, \cdots, a_n$ 是交换群 G 中的任意 $n \geqslant 2$ 个元素, 则对 $1, 2, \cdots, n$ 的任一排列 $i_1, i_2, \cdots, i_n$, 有

$$a_{i_1} a_{i_2} \cdots a_{i_n} = a_1 a_2 \cdots a_n.$$

证：当 $n = 2$ 时, 根据交换得到 $a_2 a_1 = a_1 a_2$. 结论成立.

假设 $n - 1$ 时结论成立.

对于 n, 如果 $i_n = n$, 则根据结合律和归纳假设,

$$a_{i_1} a_{i_2} \cdots a_{i_n} = (a_{i_1} a_{i_2} \cdots a_{i_{n-1}}) a_n = (a_1 a_2 \cdots a_{n-1}) a_n = a_1 a_2 \cdots a_{n-1} a_n.$$

如果 $i_n < n, i_k = n$, 则根据结合律、交换律及前面的结果,

$$\begin{aligned} a_{i_1} \cdots a_{i_{k-1}} a_{i_k} a_{i_{k+1}} \cdots a_{i_n} &= (a_{i_1} \cdots a_{i_{k-1}}) a_n (a_{i_{k+1}} \cdots a_{i_n}) \\ &= (a_{i_1} \cdots a_{i_{k-1}}) (a_{i_{k+1}} \cdots a_{i_n}) a_n \\ &= a_1 a_2 \cdots a_{n-1} a_n. \end{aligned}$$

结论成立.

根据数学归纳法原理, 结论对任意 n 成立.

定义 6.1.10

设 n 是正整数. 如果 $a_1 = a_2 = \cdots = a_n = a$, 则记 $a_1 a_2 \cdots a_n = a^n$, 称为 a 的 n 次幂.

特别地, 定义 $a^0 = e$ 为单位元, $a^{-n} = (a^{-1})^n$ 为逆元 a^{-1} 的 n 次幂.

定义 6.1.10

设 n 是正整数. 如果 $a_1 = a_2 = \cdots = a_n = a$, 则记 $a_1 a_2 \cdots a_n = a^n$, 称为 a 的 n **次幂**.

特别地, 定义 $a^0 = e$ 为单位元, $a^{-n} = (a^{-1})^n$ 为逆元 a^{-1} 的 n 次幂.

性质 6.1.6

设 a 是群 G 中的任意元, 则对任意的整数 m, n, 有

$$a^m a^n = a^{m+n}, \ (a^m)^n = a^{mn}.$$

定义 6.1.10

设 n 是正整数. 如果 $a_1 = a_2 = \cdots = a_n = a$, 则记 $a_1 a_2 \cdots a_n = a^n$, 称为 a 的 n **次幂**.

特别地, 定义 $a^0 = e$ 为单位元, $a^{-n} = (a^{-1})^n$ 为逆元 a^{-1} 的 n 次幂.

性质 6.1.6

设 a 是群 G 中的任意元, 则对任意的整数 m, n, 有

$$a^m a^n = a^{m+n}, \ (a^m)^n = a^{mn}.$$

证：分以下几种情况证明.

(i) $m > 0, n > 0$. 根据性质 6.1.5, 有 $a^m a^n = a^{m+n}$, $(a^m)^n = a^{mn}$.

(ii) $m = 0, n > 0$. 有 $a^m a^n = e a^n = a^{m+n}$, $(a^m)^n = (a^0)^n = e = a^{mn}$.

(iii) $m < 0, n > 0$. 有

$$a^m a^n = (a^{-1})^{-m} a^n = \begin{cases} a^{n-(-m)} = a^{m+n}, & \text{如果 } -m < n \\ e = a^{m+n}, & \text{如果 } -m = n \\ (a^{-1})^{-m-n} = a^{m+n}, & \text{如果 } -m > n \end{cases},$$

$$(a^m)^n = \left((a^{-1})^{-m}\right)^n = (a^{-1})^{-mn} = a^{mn}.$$

(iv) $n = 0$. 有 $a^m a^n = a^m e = a^m = a^{m+n}$, $(a^m)^n = e = a^{mn}$.

(v) $m > 0, n < 0$. 有

$$a^m a^n = a^m (a^{-1})^{-n} = \begin{cases} a^{m-(-n)} = a^{m+n}, & \text{如果 } m > -n \\ e = a^{m+n}, & \text{如果 } m = -n \\ (a^{-1})^{-n-m} = a^{m+n}, & \text{如果 } m < -n \end{cases},$$

$$(a^m)^n = \left((a^m)^{-1}\right)^{-n} = \left((a^{-1})^m\right) - n = (a^{-1})^{-mn} = a^{mn}.$$

(vi) $m < 0, n < 0$. 有

$$a^m a^n = (a^{-1})^m (a^{-1})^{-n} = (a^{-1})^{-m-n} = a^{m+n},$$

$$(a^m)^n = \left((a^m)^{-1}\right)^{-n} = (a^{-m})^{-n} = a^{mn}.$$

综上, 对任意的整数 m, n, 有

$$a^m a^n = a^{m+n}, \ (a^m)^n = a^{mn}.$$

定理 6.1.1

设 G 是一个具有运算的非空集合. 如果 G 是一个群, 则方程

$$ax = b,\ ya = b$$

在 G 中有解. 反过来, 如果上述方程在 G 中有解, 并且运算满足结合律, 则 G 是一个群.

定理 6.1.1

设 G 是一个具有运算的非空集合. 如果 G 是一个群, 则方程

$$ax = b,\ ya = b$$

在 G 中有解. 反过来, 如果上述方程在 G 中有解, 并且运算满足结合律, 则 G 是一个群.

证：设 G 是一个群. 在方程 $ax = b$ 两端左乘 a^{-1} 得, $a^{-1}(ax) = a^{-1}b$, 即 $x = a^{-1}b$ 是方程 $ax = b$ 的解. 同理, $y = ba^{-1}$ 是方程 $ya = b$ 的解.

定理 6.1.1

设 G 是一个具有运算的非空集合. 如果 G 是一个群, 则方程

$$ax = b,\ ya = b$$

在 G 中有解. 反过来, 如果上述方程在 G 中有解, 并且运算满足结合律, 则 G 是一个群.

证：设 G 是一个群. 在方程 $ax = b$ 两端左乘 a^{-1} 得, $a^{-1}(ax) = a^{-1}b$, 即 $x = a^{-1}b$ 是方程 $ax = b$ 的解. 同理, $y = ba^{-1}$ 是方程 $ya = b$ 的解.

反过来, 设方程 $ax = b,\ ya = b$ 在 G 中有解. 因为 G 非空, 所以 G 中有元素 c, 且 $cx = c$ 有解 $x = e_r$. 则对任意的 $g \in G$, $yc = g$ 有解, 故 $ge_r = (yc)e_r = y(ce_r) = yc = g$. 同理, $yc = c$ 的解 $y = e_l$ 对任意的 $g \in G$, 有 $e_l g = g$. 因此, $e_r = e_l e_r = e_l = e$ 是 G 中的单位元.

定理 6.1.1

设 G 是一个具有运算的非空集合. 如果 G 是一个群, 则方程

$$ax = b,\ ya = b$$

在 G 中有解. 反过来, 如果上述方程在 G 中有解, 并且运算满足结合律, 则 G 是一个群.

证：设 G 是一个群. 在方程 $ax = b$ 两端左乘 a^{-1} 得, $a^{-1}(ax) = a^{-1}b$, 即 $x = a^{-1}b$ 是方程 $ax = b$ 的解. 同理, $y = ba^{-1}$ 是方程 $ya = b$ 的解.

反过来, 设方程 $ax = b,\ ya = b$ 在 G 中有解. 因为 G 非空, 所以 G 中有元素 c, 且 $cx = c$ 有解 $x = e_r$. 则对任意的 $g \in G$, $yc = g$ 有解, 故 $ge_r = (yc)e_r = y(ce_r) = yc = g$. 同理, $yc = c$ 的解 $y = e_l$ 对任意的 $g \in G$, 有 $e_l g = g$. 因此, $e_r = e_l e_r = e_l = e$ 是 G 中的单位元.

对 G 中任意元素 g, 设方程 $gx = e,\ yg = e$ 在 G 中的解分别为 $x = g', y = g''$, 则 $g' = eg' = (g''g)g' = g''(gg') = g''e = g''$. 因此, g' 是 g 在 G 中的逆元. 故 G 是一个群.

本课作业

1. 证明：$G=\left\{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a,b\in\mathbb{Q}, a\neq 0\right\}$

   关于矩阵的乘法构成一个群, 其中 $\mathbb{Q}$ 表示有理数集合.

2. 设 $G=\left\{\begin{pmatrix} a & a \\ a & a \end{pmatrix} \mid a\in\mathbb{R}, a\neq 0\right\}$,

   证明：G 关于矩阵的乘法构成群.

3. 设 G 是群, $a_1,a_2,\cdots,a_r\in G$. 证明：

$$(a_1a_2\cdots a_r)^{-1}=a_r^{-1}a_{r-1}^{-1}\cdots a_1^{-1}.$$

4. 设 G 是群, $a,b\in G$, e 是单位元. 证明: 如果 $ab=e$, 则 $ba=e$.

交流与讨论

电子邮箱：

陈秀波：xb_chen@bupt.edu.cn

徐国胜：guoshengxu@bupt.edu.cn

金正平：zhpjin@bupt.edu.cn