二次互反律
Law of quadratic reciprocity

背景与定理内容

二次方程 $x^2-7=0$ 没有整数解和有理数解, 但有实数解 $\pm\sqrt{7}$. 这启示我们, 如果将解的条件放宽 (这里是允许解存在于一个更大的环或域, 如整环 $\mathbb{Z}[\sqrt{7}]$ 或实数域 $\mathbb{R}$), 方程的可解性可能会发生变化. 换个角度, 我们在模 p (p 为素数) 的意义下考虑上述方程整数解的存在性, 即允许系数与解变动 p 的若干整数倍. 例如, 取 $p=3$, 有 $4^2=16\equiv 7 \pmod 3$, 从而在模 3 的意义下 $x=4$ 是上述方程的一个解. 现在考虑一般的情形:

定义 1 (二次剩余)**.** *设 p 为素数, n 为与 p 互素的整数. 称 n 为模 p 的*二次剩余*, 如果存在整数 m 使得 $m^2\equiv n \pmod p$ 成立, 否则称 n 为模 p 的*二次非剩余*.*

为表征二次剩余与否, 我们定义 **Legendre 符号**

$$\left(\frac{n}{p}\right):=\begin{cases}1, & \text{若 } n \text{ 是模 } p \text{ 的二次剩余},\\ -1, & \text{若 } n \text{ 是模 } p \text{ 的二次非剩余},\\ 0, & \text{若 } n=0.\end{cases}$$

两个 (奇) 素数之间的二次剩余满足如下关系, 称为*二次互反律*.

定理 1 (二次互反律)**.** *对于奇素数 $p\neq q$, 有*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

定理 2 (补充定理)**.** *对于奇素数 p, 有* $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$, $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$.

应用举例

二次互反律可以简化 Legendre 符号的计算, 尤其对于较大的素数. 在此之前, 我们需要列举 Legendre 符号的基本性质:

命题 1.

- *设 p 为素数, a 为与 p 互素的整数, k 为任意整数, 有* $\left(\frac{a}{p}\right)=\left(\frac{a+kp}{p}\right)$.
- 乘性: *设 p 为素数, m,n 为与 p 互素的整数, 有* $\left(\frac{m}{p}\right)\left(\frac{n}{p}\right)=\left(\frac{mn}{p}\right)$.
- Euler 准则: *设 p 为奇素数, a 为与 p 互素的整数, 有* $\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \pmod p$.

第一条性质从 Legendre 符号的定义即可看出; 第二条性质说明为判断二次方程 $x^2\equiv n \pmod p$ 的可解性, 只需分别考虑 n 的素因子; 第三条性质为 Legendre 符号的计算提供了一般方法.

例 1 (开始的例子)**.** *由 Euler 准则,* $\left(\frac{7}{3}\right)\equiv 7^{\frac{3-1}{2}}\equiv 1 \pmod 3$, *从而 7 是模 3 的二次剩余.*

例 2 (大素数)**.** *31 是模 103 的二次非剩余, 因为* $\left(\frac{31}{103}\right)\overset{*}{=}-\left(\frac{103}{31}\right)=-\left(\frac{-21}{31}\right)=-\left(\frac{-1}{31}\right)\left(\frac{21}{31}\right)=\left(\frac{21}{31}\right)=\left(\frac{3}{31}\right)\left(\frac{7}{31}\right)\overset{*}{=}-\left(\frac{31}{3}\right)\cdot[-\left(\frac{31}{7}\right)]=\left(\frac{1}{3}\right)\left(\frac{3}{7}\right)\overset{*}{=}\left(\frac{1}{3}\right)\cdot[-\left(\frac{7}{3}\right)]=-1$. *其中带 $*$ 的等号用到了二次互反律.*

Euler 的多面体公式 $V-E+F=2$

背景介绍

对于一个简单多面体 (表面能同胚于一个球面的多面体), 记它的**顶点 (vertex)** 数为 V, **棱 (edge)** 数为 E, **面 (face)** 数为 F, 则这三个量满足公式 $V-E+F=2$, 即 Euler 多面体公式 (Euler's Polyhedron Formula). 这一公式早在 1639 年被 Descartes 注意到并证明; 通过 Descartes 的手稿, Leibniz 1675 年也知道这个公式; 1750 年, Euler 独立证明并发表了这个公式.

后来, Poincaré 认识到 Euler 多面体公式的推广是典型的拓扑性质的定理, 即 $V-E+F=\chi$, 其中 χ 为 **Euler 示性数 (Euler characteristic)**, 是一个拓扑不变量; 例如上述球面 (sphere) 有 $\chi=2$, 而环面 (torus) 有 $\chi=0$. 这确立了 Euler 公式在拓扑学中的重要地位.

证明概述

定理 3. *(Euler 的多面体公式) 对于简单多面体, 有公式 $V-E+F=2$.*

在这里, 我们给出 Cauchy 在 1811 年提出的一种证明方法. 勒让德利用球面三角学给出了证明; Descartes 在他的手稿中也给出了证明, 用到了球面上多边形的立体角和它的平面角之间的关系. 后两种证明请阅读**王敬赓《直观拓扑》**p18&p21

证明. 任取球面上一点, 去掉该点任意一个闭邻域, 得到的图形同胚于一个平面; 由于简单多面体同胚于球面, 故去掉任意一个面的简单多面体可以在给定平面上展开成**平面图 (各边互不交叠)**. 以正方体为例, 如图 1 所示, 这里正方体 1a去掉了面 EFGH, 展开成为平面图 1b.

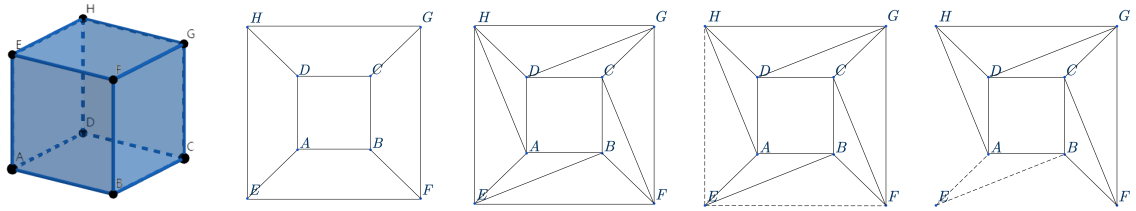


图 1. 以正方体为例的操作流程

由于只去掉了一个面, 证多面体的 Euler 公式等价于证平面图的 Euler 公式$V-E+F=1$. 我们接着对平面图做以下操作: 对于平面图里顶点数不是 3 的面, 在保持图是平面图的前提下, 向这个面添加**边 (edge)**(比如从给定顶点出发, 向在同个面内的所有其他顶点连线); 我们对所有的面做这样的操作, 最后得到了一个每个面只有 3 个顶点的平面图, 如图 1c.

接着从最外围的面开始 (至少有 1 条边不与其他面相邻), 如果这个面只有 1 条边不与其它面相邻, 去掉这条边, 如图 1d; 如果这个面有 2 条边不与其他面相邻, 同时去掉这 2 条边, 如图 1e.

我们重复上述操作, 最终得到一个三角形平面图, 这个图 $V=3$, $E=3$, $F=1$, 满足 $V-E+F=1$. 由于所有关于平面图的操作均保持 $V-E+F$ 不变, 故原来的关于平面图的等式也成立, 至此 Euler 的多面体公式得证. □

应用

1. 得到不可平面图的必要条件　2. 证明正多面体只有五种　参考: 王敬赓《直观拓扑》

高次方程一般没有根式解

背景介绍

解代数方程一直是数学中的重要问题. 对于二次方程$ax^2+bx+c=0, a\neq 0$ 而言, 我们很容易能解出其两个根为$x=\dfrac{-b\pm\sqrt{b^2-4ac}}{2a}$. 事实上, 古巴比伦留下的陶片显示, 在大约公元前 2000 年 (2000 BC) 古巴比伦的数学家就能解一元二次方程了. 对于三次方程$ax^3+bx^2+cx+d=0, a\neq 0$ 而言, 由于涉及到复数开根, 所以其一般解被发现的较晚. 一般而言我们认为是尼科洛 · 塔尔塔利亚最早在 1553 年发现了三次方程的一般解. 三次方程的根式解复杂程度比二次方程提高了很多, 其中包括了开三次根、复数等运算. 四次方程的根式解在三次方程根式解出现不久后就被人们发现, 但是其解的复杂程度非常巨大, 已经几乎失去了实用价值, 只有理论研究的作用.

当二次、三次、四次方程的根式解被得到后, 数学家当然不会满足, 他们开始向五次方程挑战. 人们相信五次方程根式解的出现只是时间问题, 不管它有多复杂, 总会被人们发现. 然而无论数学家如何改进解方程的方法, 都无法在与五次方程斗争的路上前进哪怕一小步. 终于, 在 1824 年, 阿贝尔证明了一般的五次方程没有根式解. 之后, 伽罗瓦创造性地引入了群这一数学概念, 对方程是否存在根式解给出了一个具体的刻画. 至此, 解代数方程的这一挑战才画上 (不那么完美的) 句号.

定理叙述

要想证明高次方程无根式解, 我们首先需要定义什么叫根式解. 所谓根式解就是用加、减、乘、除、开n 次根号进行有限次迭代的解. 具体而言, 我们有

定义 2. *设$f(x)\in K[x]$ 是一个多项式, 其中K 是一个域. 若存在域扩张链*

$$K=K_0\subset K_1\subset K_2\subset\cdots\subset K_m$$

满足K_m 包含f 的所有根, 且对于$t=0,\cdots,m-1$, 有$K_{t+1}=K_t[a]$, 其中a 满足$\exists n\in\mathbb{N}, a^n\in K_t$. 则称$f$ 有根式解, 或者f 根式可解.

阿贝尔发现五次方程一般没有根式解, 即

定理 4. *存在一个五次多项式f 使得f 根式不可解.*

伽罗瓦在描述可解性的时候引入了伽罗瓦群的概念.

定义 3. *设$f(x)\in K[x]$ 为一个多项式, 设F 为f 的分裂域. 定义f 的伽罗瓦群为$\mathrm{Gal}_K(f)=\{\sigma:\sigma$是$F$的自同构, 且$\sigma|_K=\mathrm{id}\}$.*

同时与可解多项式对应地定义了可解群.

定义 4. *若一个有限群G 满足存在正规子群链$G=G_m\trianglerighteq G_{m-1}\trianglerighteq\cdots\trianglerighteq G_0$, 且$G_{t+1}/G_t$ 都是循环群, 则称G 是可解群.*

伽罗瓦神奇地洞察了可解多项式与可解群的关系, 即

定理 5. *如果f 可根式解, 那么$\mathrm{Gal}_K(f)$ 是可解群; 如果$\mathrm{Gal}_K(f)$ 是可解群, 且域K 的特征满足$\mathrm{char}\,K\nmid\deg f$, 则$f$ 可根式解.*

在大部分情况下五次以上的多项式的伽罗瓦群并不可解, 因此不能根式解.

四平方和定理

背景介绍

四平方和定理说明每个正整数均可表示为 4 个整数的平方和. 它是费马多边形数定理和华林问题的特例. 1743 年, 瑞士数学家欧拉发现了一个著名的恒等式: $(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+w^2)=(ax+by+cz+dw)^2+(ay-bx+cw-dz)^2+(az-bw-cx+dy)^2+(aw+bz-cy-dx)^2$ 根据上述欧拉恒等式可知如果正整数m 和n 能表示为 4 个整数的平方和, 则其乘积mn 也能表示为 4 个整数的平方和. 1751 年, 欧拉又得到了另一个一般的结果. 即对任意奇素数 p, 同余方程 $x^2+y^2+1\equiv 0 \pmod p$ 必有一组整数解x,y 满足$0\le x<\frac{p}{2}$,$0\le y<\frac{p}{2}$

至此, 证明四平方和定理所需的全部引理已经全部证明完毕. 此后, 拉格朗日和欧拉分别在 1770 年和 1773 年作出最后的证明.

定理叙述

定理 6. *设$n\in\mathbb{N}^+$, 则存在$a,b,c,d\in\mathbb{N}$ 使得$n=a^2+b^2+c^2+d^2$.*

证明概述

只需证明所有素数可以写为四平方和. $2=1^2+1^2+0^2+0^2$, 因此只需证明奇质数可以表示成四个整数的平方和.

证明. 根据欧拉 1973 年的结果, 存在$0<x,y<\frac{p}{2}$ 使得$x^2+y^2+1^2+0^2=kp$. 令$m_0:=\min\{k\in\mathbb{N}^+:\exists x_i,i=1,2,3,4,kp=\sum_{i=1}^4 x_i^2\}$. 从$0<x,y<\frac{p}{2}$ 可知$m_0<p$.

若m_0 是偶数, 且$m_0p=x_1^2+x_2^2+x_3^2+x_4^2$. 不失一般性设$x_1,x_2$ 的奇偶性相同, 奇偶分析知x_3,x_4 的奇偶性也相同, 则$x_1+x_2,x_1-x_2,x_3+x_4,x_3-x_4$ 均为偶数. 从而$\frac{m_0}{2}p=\left(\frac{x_1+x_2}{2}\right)^2+\left(\frac{x_1-x_2}{2}\right)^2+\left(\frac{x_3+x_4}{2}\right)^2+\left(\frac{x_3-x_4}{2}\right)^2$ 但$\frac{m_0}{2}<m_0$, 与m_0 的定义矛盾.

现在用反证法证明$m_0=1$. 设$m_0>1$. 易知m_0 不可整除x_1,x_2,x_3,x_4 的最大公因数, 否则m_0^2 可整除m_0p, 则得m_0 是p 的因数, 但$1<m_0<p$ 且 p 为质数, 矛盾. 故存在不全为零、绝对值小于$\frac{1}{2}m_0$(注意m_0 是奇数在此的重要性) 的整数y_1,y_2,y_3,y_4 使得

$$y_i\equiv x_i \pmod{m_0}, 0<\sum_{i=1}^4 y_i^2<4(\frac{1}{2}m_0)^2=m_0^2, \sum_{i=1}^4 y_i^2\equiv\sum_{i=1}^4 x_i^2\equiv 0 \pmod{m_0}$$

从而 $\sum_{i=1}^4 y_i^2=m_0m_1$, 其中$m_1\in\mathbb{N}^+, m_1<m_0$. 下证$m_1p$ 可以表示成四平方和. 令:

$$\begin{cases} z_1=x_1y_1+x_2y_2+x_3y_3+x_4y_4, z_2=x_1y_2-x_2y_1+x_3y_4-x_4y_3 \\ z_3=x_1y_3-x_2y_4-x_3y_1+x_4y_2, z_4=x_1y_4+x_2y_3-x_3y_2-x_4y_1 \end{cases}$$

则有$\sum_{i=1}^4 z_i^2=\sum_{i=1}^4 y_i^2\times\sum_{i=1}^4 x_i^2$. 且易知$z_1\equiv\sum_{i=1}^4 x_i^2\equiv 0 \pmod{m_0}$. 又有$z_2\equiv x_1x_2-x_2x_1+x_3x_4-x_4x_3\equiv 0 \pmod{m_0}$, 同理$z_3,z_4\equiv 0 \pmod{m_0}$. 故$z_1,z_2,z_3,z_4$ 是m_0 的倍数, 令$z_i=m_0t_i, i=1,2,3,4$, 则有 $m_0^2\sum_{i=1}^4 t_i^2=m_0m_1m_0p$, 从而 $\sum_{i=1}^4 t_i^2=m_1p<m_0p$, 与$m_0$ 的定义矛盾. □

四色定理

背景介绍

每个无外飞地的地图都可以用不多于四种颜色来染色, 且不会有两个邻接的区域颜色相同, 即四色定理. 这最早是 Guthrie 在 1852 年提出的猜想, 之后 De Morgan 致力于推动这个问题的研究工作. 1879 年, Kempe 发表了一个四色定理的 “证明”, 当时数学界认为四色问题的猜想就此得到解决. 但在 1890 年, Heawood 发表了一篇文章, 指出了 Kempe 证明中的一个错误. 虽然 Heawood 没能修正这个错误, 但 Heawood 将 Kempe 的证明加以修改, 证明了较弱的五色定理.

证明的主要思想是, 将一个含有 n 片区域的地图, 约化为不超过 $n-1$ 片区域的地图, 从而可以证明定理成立. 之后的证明工作便成了寻找 “不可避免的可约构形集”, 是由 Birkhoff 提出的, 即假设四色定理不成立, 则存在最小的不能约化的五色地图, 且最少用五种颜色染色的地图必出现某些构形, 只要再证明这些构形可以约化为区域更少的问题, 就可以推出矛盾, 最后证明四色定理. 1969 年, 德国数学家 Heesch 提出了 “放电法”, 为寻找不可避免的构形提供了系统的方法. 由于人工寻找构形并验证不可约过于缓慢, Heesch 试图利用计算机辅助证明. 后来, Heesch 的工作被介绍到了美国. 1975 年, Haken, Appel 在 Koch 提供计算机算法的帮助下, 最终得到了一个有 1936 个构形的不可避免构形集, 经伊利诺伊大学的主电脑 “IBM 360” 1200 小时的计算, 最终证明了这些构形都是可约构形, 至此四色定理得到了成功证明. 这是首个主要借助计算机证明的定理.

证明概述

这里我们简述五色定理的证明, 其中的细节可参考**王敬赓《直观拓扑》**p77. Kempe 证明四色定理的过程虽有误, 但提供了 “分构形研究” 的重要思想, 这在五色定理的证明中有所体现.

引理 1. *地图染色问题中, 必存在一个区域, 与它边界相邻的区域数小于等于 5.*

这个引理可以利用平面图的 Euler 公式 $V-E+F=1$ 证明.

定理 7 (五色定理)**.** *每个无外飞地的地图都可以用不多于五种颜色来染色, 且不会有两个邻接的区域颜色相同.*

证明. 对于一个区域数为 n 的地图, 由引理, 我们只需要讨论如图 1 所示的四种构形. 其中 a, b, c 三种构形显然可以用五种颜色染色. 以 c 为例, 若 C_1 和 C_3, C_2 和 C_4 是不同的区域, 则此构形的染色问题可以约化为将 C 和 C_1 合并后的染色问题. 若 C_1 和 C_3 是同一片区域, 则可以合并 C 和 C_2. 对于构形 d, D_1 至 D_5 中一定有两个所代表的区域是不相邻的, 不妨设为 D_1 和 D_3, 则 D_1 和 D_3 可以染成同色, 这样构形 d 也可以用五种颜色染色, 此构形的染色问题可以约化为将 D, D_1, D_3 合并后的染色问题. 至此我们把原问题约化为了 $n-1$ 或 $n-2$ 个区域的染色问题. □

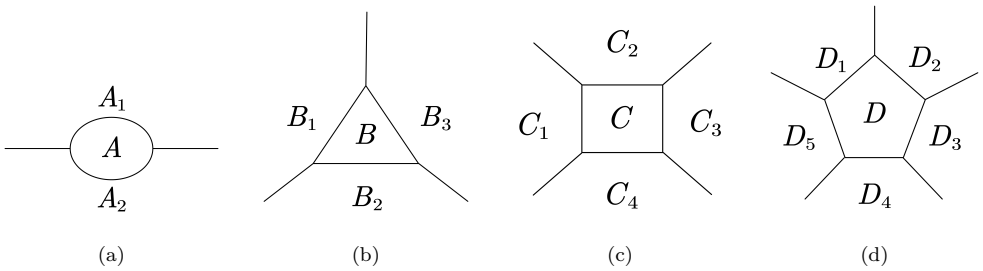


图 2. Kempe 使用的不可避免构形集

Brouwer 不动点定理

背景介绍

数学中有许多不动点定理——泛函分析中的 Banach 不动点定理、拓扑学中的 Brouwer 不动点定理、它的推广与延伸——Schauder 不动点定理和 Kakutani 不动点定理, 以及 Lefschetz 不动点定理等等. 在数十个不动点定理中, 本文的主角 Brouwer 不动点定理尤为出名, 它不仅在拓扑学上有着极为重要的地位, 更是在微分方程、微分几何乃至博弈论等方面有着各式各样的应用. 定理以荷兰数学家、哲学家 L. E. J. Brouwer(1881-1966) 命名, 他在拓扑学、集合论、复分析和数学基础和哲学等领域作出了重要贡献.

Brouwer 不动点定理是代数拓扑的早期成果之一, $n = 3$ 的情形由 Piers Bohl 在 1904 年证明, 但他的工作并未被人注意. 1909 年, Brouwer 也证明了此情形; 一年后, J. Hadamard 证明了一般情形, 同年, Brouwer 系统性地使用同调论等工具也完成了对任意维数的证明.

定理叙述

定理的常见形式有以下两种, 后者更为一般化, 可以直接推广到 Banach 空间上成为 Schauder 不动点定理. 记 n 维球面 $D^n := \{x \in \mathbb{R}^n : \|x\| \leqslant 1\}$.

定理 8. *若 $f : D^n \to D^n$ 连续, 则存在 $x \in D^n$, 使得 $f(x) = x$.*

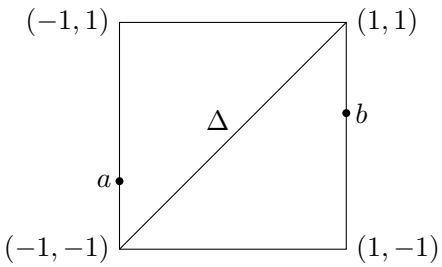
定理 9. *设 K 是欧氏空间的非空紧凸子集, 则连续映射 $f : K \to K$ 必有不动点.*

证明概述

我们为大家叙述 $n = 1$ 时的一种 (分析的) 证明, 注意 $D^1 = [-1, 1]$.

定理 10. *连续函数 $f : D^1 \to D^1$ 有不动点.*

证明. 定义 $g : [-1, 1] \to [-2, 2], g(x) = f(x) - x$, 它显然是连续的. 若 $g(1)$ 或 $g(-1)$ 为 0, 则命题得证. 若不然, 则有 $g(-1) = f(-1) + 1 > 0, g(1) = f(1) - 1 < 0$. 故由零点定理, 存在 $c \in (-1, 1), g(c) = 0$, 此即 $f(c) = c$. □



遗憾的是, 上述证明没有高维的推广 (特别地, $n = 2$ 的情形可以用代数拓扑中基本群的工具解决). M.W.Hirsch 利用单纯逼近定理给出了一个证明 (*A proof of the nonretractibility of a cell onto its boundary*, 1963); 另有分析学的证明, 主要思想是利用适当的光滑函数来逼近 f(N. Dunford and J. Schwartz, *Linear Operators I*, 1958, pp467-470); 最常见的 (也是最初的) 还是代数拓扑的证明. 在证明中, 我们构造 "同调函子" H_n 将问题进行转化, 具体过程这里略去了.

简而言之, 代数拓扑的强大工具将本问题转移到了代数领域, 并在那里得以解决. 在拓扑学中, 这一结果与 Jordan 曲线定理、毛球定理、维数不变性定理 (这一重要结果的论证在 1911 年也由 Brouwer 给出) 和 Borsuk–Ulam 定理一样, 是表征 Euclid 空间拓扑的关键定理之一.

Cayley–Hamilton 定理

定理内容

在线性代数中，Cayley–Hamilton 定理表明对于任意交换环上的方阵 (例如实方阵或复方阵) 而言, 其特征多项式就是该矩阵的零化多项式.

对于交换环 R 上的 $n\times n$ 的矩阵 $\boldsymbol{A}$, 设 $\boldsymbol{I}_n$ 是 R 上 $n\times n$ 的单位矩阵, 那么 $\boldsymbol{A}$ 的特征多项式是 $p_{\boldsymbol{A}}(\lambda)=\det(\lambda\boldsymbol{I}_n-\boldsymbol{A})$, 其中 det 表示取行列式, $\lambda\in R$ 是该多项式的变量. Cayley–Hamilton 定理断言: $p_{\boldsymbol{A}}(\boldsymbol{A})=\boldsymbol{O}$, 其中 $\boldsymbol{O}$ 表示零矩阵.

举一简单的例子以助理解: 假设 $\boldsymbol{A}=\begin{pmatrix}1&2\\3&4\end{pmatrix}$, 那么 $\boldsymbol{A}$ 的特征多项式为

$$\begin{aligned}p_{\boldsymbol{A}}(\lambda)=\det(\lambda\boldsymbol{I}_2-\boldsymbol{A})&=\begin{vmatrix}\lambda-1&-2\\-3&\lambda-4\end{vmatrix}\\&=(\lambda-1)(\lambda-4)-(-2)(-3)=\lambda^2-5\lambda-2\end{aligned}$$

Cayley–Hamilton 定理声称: 将上式中的 λ 换成 $\boldsymbol{A}$, 常数项用单位矩阵替换, 则一定有

$$p_{\boldsymbol{A}}(\boldsymbol{A})=\boldsymbol{A}^2-5\boldsymbol{A}-2\boldsymbol{I}_2=\boldsymbol{O}$$

真有这么巧吗? 让我们验算一下:

$$\boldsymbol{A}^2-5\boldsymbol{A}-2\boldsymbol{I}_2=\begin{pmatrix}7&10\\15&22\end{pmatrix}-\begin{pmatrix}5&10\\15&20\end{pmatrix}-\begin{pmatrix}2&0\\0&2\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$$

定理意义

Cayley–Hamilton 定理极大地**降低了寻找矩阵的零化多项式的难度**. 如果多项式 $f(x)=a_kx^k+a_{k-1}x^{k-1}+\cdots+a_1x+a_0$ 使得 $f(\boldsymbol{A})=a_k\boldsymbol{A}^k+a_{k-1}\boldsymbol{A}^{k-1}+\cdots+a_1\boldsymbol{A}+a_0\boldsymbol{I}_n=\boldsymbol{O}$, 就称多项式 $f(x)$ 是矩阵 $\boldsymbol{A}$ 的零化多项式. 零化多项式对于研究矩阵的代数性质有很大的帮助. 从前将 n 阶方阵全体看作一个 n^2 维的向量空间时, 我们只知道每个方阵都存在零化多项式, 并且次数最多是 n^2; 有了 Cayley–Hamilton 定理之后我们发现特征多项式就是一个零化多项式, 次数也从原来的 n^2 降成了 n. 对于阶数较高的方阵, 直接计算其特征多项式比较困难, 可结合牛顿恒等式 ($n=2$ 时就是初中时学过的韦达定理) 计算其各项系数.

既然零化多项式已经容易找到, 我们可以**减少一些矩阵运算的计算量**. 仍以 $\boldsymbol{A}=\begin{pmatrix}1&2\\3&4\end{pmatrix}$ 为例, 经过计算其特征多项式我们得到 $\boldsymbol{A}^2-5\boldsymbol{A}-2\boldsymbol{I}_2=\boldsymbol{O}$, 那么 $\boldsymbol{A}^2=5\boldsymbol{A}+2\boldsymbol{I}_2$, 也就是说计算 $\boldsymbol{A}^2$ 转化为计算 $\boldsymbol{A}$ 的线性组合了. 对于一般的 n 阶方阵 $\boldsymbol{A}$, 这意味着计算 $\boldsymbol{A}^k$ 可以化归为计算 $\boldsymbol{A}^{k-1}$, 起到了降幂的作用. 计算矩阵的逆也变得更简单了: 仍以 $\boldsymbol{A}=\begin{pmatrix}1&2\\3&4\end{pmatrix}$ 为例, 由 $\boldsymbol{A}^2-5\boldsymbol{A}-2\boldsymbol{I}_2=\boldsymbol{O}$ 得到 $\boldsymbol{A}\cdot\dfrac{1}{2}(\boldsymbol{A}-5\boldsymbol{I}_2)=\boldsymbol{I}_2$, 于是直接得到 $\boldsymbol{A}^{-1}=\dfrac{1}{2}(\boldsymbol{A}-5\boldsymbol{I}_2)$, 也就是说简化了逆矩阵的计算. 对于一般的 n 阶方阵也可以沿用相同的思路去计算矩阵的逆. 结合 Cayley–Hamilton 定理与多项式余式、Sylvester 公式等知识还可以进行更多矩阵相关的巧妙计算.

Cayley–Hamilton 定理的证明有诸多版本, 最简单的版本利用了伴随矩阵: 设 $\boldsymbol{A}$ 的特征多项式是 $p(t)$, 又设 $\boldsymbol{B}:=\operatorname{adj}(t\boldsymbol{I}_n-\boldsymbol{A})$, 则根据伴随矩阵的定义有 $(t\boldsymbol{I}_n-\boldsymbol{A})\boldsymbol{B}=\det(t\boldsymbol{I}_n-\boldsymbol{A})\boldsymbol{I}_n=p(t)\boldsymbol{I}_n$, 按 t 的幂次展开并比较该等式左右两侧系数, 再经过简单的计算即可得证. 从抽象代数的视角来看, 这实际上是建立了从矩阵环到矩阵多项式环的一个自然的环同构. 从 Zariski 拓扑的观点去看, Cayley–Hamilton 定理还说明可对角化矩阵在全体方阵中是稠密的.

π 是超越数

背景介绍

超越一词最早在莱布尼兹 1962 年的一篇论文中出现, 用来描述函数. 他证明了 $\sin x$ 是 x 的超越函数. 现代超越数的概念最早由欧拉在 18 世纪提出. 1844 年, 刘维尔证明了超越数存在, 并在 1851 年给出了第一个例子: $L_b := \sum_{n=1}^{\infty} 10^{-n!}$. 1873 年, 埃尔米特证明了自然对数的底 e 是超越数. 1874 年, 康托证明了实数几乎是超越数, 并给出了一个构造超越数的系统方法. 1882 年, 林德曼证明了 π 是超越数. 后来, 又有许多数, 如 $\mathrm{e}^{\pi}, 2^{\sqrt{2}}, \sin 1, \ln a, e^b$ 等, 其中 a 是不为 1 的正有理数, b 是不为 0 的代数数.

定理叙述

定义 5. 若一个复数 $x \in \mathbb{C}$ 不是任何一个非零有理系数多项式的根, 则称其为超越数. 否则称其为代数数.

定理 11. π 是超越数, 即对于任何非零有理系数多项式 $f(x)$, 都有 $f(\pi) \neq 0$.

证明概述

证明π 是无理数很简单, 但是证明其是超越数却很难. 我们将使用林德曼-魏尔斯特拉斯定理证明π 是超越数, 在此之前我们需要先做一些基础的准备:

定义 6. 设 $\alpha_1, \cdots, \alpha_n \in \mathbb{C}$. 若对于不全为 0 的 $b_1, \cdots, b_n \in \mathbb{Q}$, 都有 $\sum_{i=1}^{n} b_i \alpha_i \neq 0$, 则称它们在 $\mathbb{Q}$ 上线性无关. 从定义可以得到, 一个不为 0 的复数自己本身一定是线性无关的.

设 $y_1, \cdots, y_n \in \mathbb{C}$. 若对于非 0 的有理系数 n 元多项式 $f(x_1, \cdots, x_n)$, 均有 $f(y_1, \cdots, y_n) \neq 0$, 则称它们在 $\mathbb{Q}$ 上代数无关. 从定义可以得到, 一个复数自己是代数无关的当且仅当这个复数是超越数.

定义 7. 对于复数$z \in \mathbb{C}$, 令$\mathrm{e}^z := \sum_{k=0}^{\infty} \frac{z^k}{k!}$. 这样我们就将$f(x) = \mathrm{e}^x$ 延拓到了$\mathbb{C}$ 上.

引理 2. 全体代数数构成一个数域, 即代数数的和、差、积、商仍为代数数.

至此基本的概念已经建立, 下面不加证明地叙述这个重要的定理:

引理 3 (林德曼-魏尔斯特拉斯定理)**.** 若 $\alpha_1, \alpha_2, \cdots, \alpha_n \in \mathbb{C}$ 都是代数数, 且他们在 $\mathbb{Q}$ 上线性无关, 则 $\mathrm{e}^{\alpha_1}, \mathrm{e}^{\alpha_2}, \cdots, \mathrm{e}^{\alpha_n}$ 在 $\mathbb{Q}$ 上代数无关.

准备工作完毕, 下面我们来证明π 是超越数.

证明. 由指数函数的定义知$\mathrm{e}^{\mathrm{i}\theta} := \sum_{k=0}^{\infty} \frac{(\mathrm{i}\theta)^k}{k!}$. 整理可得$\mathrm{e}^{\mathrm{i}\theta} = \sum_{k=0}^{\infty} (-1)^k \frac{\theta^{2k}}{(2k)!} + \mathrm{i} \sum_{k=0}^{\infty} (-1)^k \frac{\theta^{2k+1}}{(2k+1)!} = \cos\theta + \mathrm{i}\sin\theta$. 从而$\mathrm{e}^{\mathrm{i}\pi} = \cos\pi + \mathrm{i}\sin\pi = -1$. 故$\mathrm{e}^{\mathrm{i}\pi} + 1 = 0$, 从而$\mathrm{e}^{\mathrm{i}\pi}$ 在$\mathbb{Q}$ 上是代数相关的. 由引理 3可知$\mathrm{i}\pi$ 不是代数数. 又由引理 2可知, 若π 是代数数, 则由于$\mathrm{i}^2 + 1 = 0$ 知i 是代数数, 从而$\mathrm{i}\pi$ 是代数数, 矛盾! 故π 不是代数数, 从而是超越数. □

柯尼斯堡七桥问题

背景介绍

十八世纪初, 在东普鲁士的柯尼斯堡 (今俄罗斯加里宁格勒), 有两条河流经该地, 将其划分为四片陆地, 由 7 座桥梁连接. 当地的居民热衷于一个问题: 一个散步者能否设计出一条路线, 使得他走遍七座桥, 且每座桥只走一次?

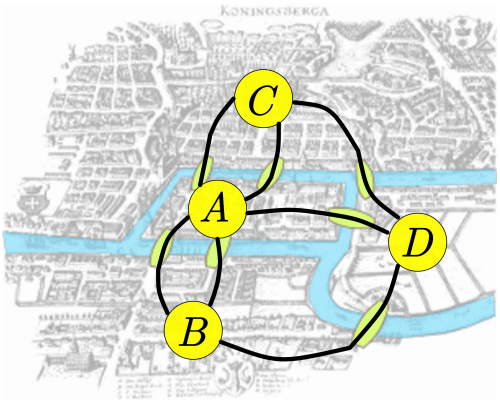


图 3. 柯尼斯堡的七座桥

这一问题在 Euler 1736 年发表的论文《柯尼斯堡的七座桥》中得到解决. Euler 将问题进行了合适的抽象, 将陆地抽象为**顶点 (vertex)**, 桥抽象为**边 (edge)**, 原始的问题就变成了**图 (graph)** 的一笔画问题: 能否遍历完所有的边而没有重复? 在数学史上, 柯尼斯堡七桥问题的解被认为是图论的第一个定理, 网络理论的第一个正确的证明, 以及拓扑学 (位置几何学) 的开端之一.

问题的解法

首先我们定义一个顶点上边的条数为它的**度数 (degree)**, 度数为奇数的我们称其为奇顶点, 度数为偶数的我们称其为偶顶点; 一笔画经过的第一个顶点称起点, 最后一个顶点称终点; 对于每一个顶点, 一笔画时由另一个顶点画向它的边称进入边, 由它画向另一个顶点的边称离开边.
我们可以论证以下能够一笔画的图的性质:

1. 一个图能被一笔画出, 则它一定是连通的 (任取两个顶点都存在一条路径将其连接);
2. 任取一个不是起点和终点的顶点, 由于进入边和离开边成对出现, 其必须是偶顶点;
3. 由起点出发的一条离开弧没有对应的进入弧, 画向终点的最后一条进入弧没有对应的离开弧; 若起点和终点不同, 则此图必有 2 个奇顶点; 若起点和终点相同, 则此图没有奇顶点;

对于柯尼斯堡七桥问题, 我们统计它每个顶点的度数: A 度数为 5, B,C,D 度数为 3. 则它的奇顶点数有四个, 与前面的性质 3 矛盾, 故我们断言七桥问题的图不能一笔画.

一笔画定理

最后, 我们介绍一笔画问题的一般判定法. 上面给出的一笔画问题的必要条件事实上也是充分条件. 具体的证明和更多的背景请阅读**王敬赓《直观拓扑》**p57

定理 12 (一笔画定理)**.** *一个图能被一笔画出当且仅当它是连通的, 且奇顶点个数为 0 或 2.*

拉格朗日定理

在群论中, 拉格朗日定理表明了对任何有限群 G, 每个 G 的子群的阶 (元素个数) 整除 G 的阶, 该定理以约瑟夫-路易-拉格朗日命名. 定理进一步表明, 对于有限群 G 的子群 H 而言,$|G|/|H|$ 不仅是个整数, 而且它的值等于指标 $[G:H]$, 其中 $[G:H]$ 是 H 在 G 中左陪集的个数.

定理 13 (拉格朗日定理)**.** *设 G 是有限群, 若 H 是 G 的子群, 那么 $|G| = [G:H] \cdot |H|$.*

如果将 $|G|, |H|$, 和 $[G:H]$ 看作基数, 那么这个定理对 G 是无限阶群的情况也是成立的.

证明. 规定 G 中的元素 x 与 y 等价如果存在 $h \in H$, 使得 $x = yh$, 这是一个等价关系. 于是 H 在 G 中的左陪集便是在此等价关系中的等价类. 因此, 左陪集构成了 G 的一个分划. 每个左陪集 aH 有与 H 相同的基数, 因为 $x \mapsto ax$ 定义了从 $H \to aH$ 的一个双射. 而左陪集的数量是指标 $[G:H]$, 综上所述,

$$|G| = [G:H] \cdot |H|.$$

□

应用

这个定理的一个推论是指群中元素的阶整除群的阶: 若群 G 有 n 个元素,$a \in G$, 那么 $a^n = e$.

这个定理可以用来证明费马小定理以及它的一般化：欧拉定理.

这个定理也表明任何素数阶群 G 是循环群, 也是单群, 因为由任何非单位元生成的子群必须是群 G 本身.

拉格朗日定理还可以用来证明有无限多个素数：假设存在一个最大的素数 p, 那么梅森素数 $2^p - 1$ 的任何素因子 q 满足：$2^p \equiv 1 \pmod{q}$, 意味着乘法群 $(\mathbb{Z}/q\mathbb{Z})^*$ 中 2 的阶是 p. 由拉格朗日定理,2 的阶必须整除 $(\mathbb{Z}/q\mathbb{Z})^*$ 的阶 $q-1$, 于是 p 整除 $q-1$, 所以 $p < q$, 这与 p 是最大的素数矛盾!

正弦定理和余弦定理

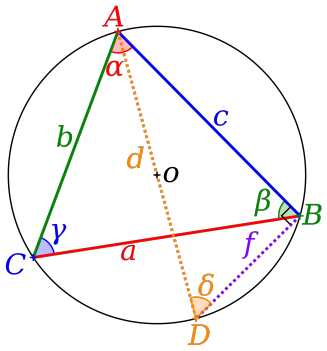
在三角学中, 正弦定理是一个把三角形的边与角联系起来的定理, 这定理表明:

$$\frac{a}{\sin\alpha} = \frac{b}{\sin\beta} = \frac{c}{\sin\gamma} = 2R,$$

这里 a, b 和 c 是三角形的边长, 而 α, β 和 γ 则分别是三条边所对应的角. R 是三角形外接圆半径. 当这式子的最后一部分不被使用时, 该定理也被陈述为以下形式:

$$\frac{\sin\alpha}{a} = \frac{\sin\beta}{b} = \frac{\sin\gamma}{c}.$$

当两个角度和一条边已知时, 正弦定理可用于计算三角形的剩余边, 这种技术称为三角测量.



在三角学中, 余弦定理涉及三角形的边长与其一个角的余弦值. 余弦定理指出:

$$\begin{aligned} c^2 &= a^2 + b^2 - 2ab\cos\gamma, \\ a^2 &= b^2 + c^2 - 2bc\cos\alpha, \\ b^2 &= a^2 + c^2 - 2ac\cos\beta. \end{aligned}$$

这里 a, b 和 c 是三角形的边长, 而 α, β 和 γ 则分别是三条边所对应的角.

余弦定理涵盖了勾股定理. 如果 γ 是直角, 则 $\cos\gamma = 0$, 余弦定律变化为 $c^2 = a^2 + b^2$, 这就是勾股定理.

如果我们设边 c 所对应的角为 θ, 把三角形放在笛卡尔坐标系中, 将 BC 边放在 x 轴上, 顶点 C 与坐标原点重合, 那么点 A, B, C 的坐标即为

$$A = (b\cos\theta, b\sin\theta), B = (a, 0), \text{ and } C = (0, 0).$$

由距离公式:

$$c = \sqrt{(a - b\cos\theta)^2 + (0 - b\sin\theta)^2}.$$

将式子两边平方并化简:

$$\begin{aligned} c^2 &= (a - b\cos\theta)^2 + (-b\sin\theta)^2 \\ &= a^2 - 2ab\cos\theta + b^2\cos^2\theta + b^2\sin^2\theta \\ &= a^2 + b^2(\sin^2\theta + \cos^2\theta) - 2ab\cos\theta \\ &= a^2 + b^2 - 2ab\cos\theta. \end{aligned}$$

这个证明的一个优点在于它不需要分情况考虑三角形是否是锐角、直角或钝角.

Gauss-Bonnet-Chern 定理

一切的起点：三角形内角和

古希腊的 Pythagoras 学派在数学上有很多重要的发现, 其中有两个定理, 其一是 Pythagoras 定理, 是指欧式空间内的直角三角形的两条直角边的平方和等于斜边的平方, 另一个定理是欧式空间中的三角形的内角和等于 180° , 即对平面上的任何一个三角形, 若令 α, β, γ 为三角形的三个内角, 则有 $\alpha+\beta+\gamma=\pi$, 然后就可以发现三角形中的内角和是一个几何不变量, 尽管三个内角 α, β, γ 会因为三角形形状的不同而取值不同.

那么对于一般的多边形, 是否还有这样的规律呢? 接下来可以看到的事实是凸 n 边形的内角和是随 n 的变化而变化, 但外角和是一个常数 2π, 是一个几何不变量. 并发现了如下定理:

定理 14. *设 P 是平面上的一个最一般的多边形, 分为 m 块且含有 g 个洞,P 的转角和 $A(P)$ 满足 $A(P)=2\pi(m-g)$.*

Euler 数

定理 1 公式的右端其实就是 Euler 数. 在 1751 年大数学家 Euler 指出, 对于三维空间中的任意闭的凸多面体, 它的顶点数 V , 棱数 E 和面数 F 满足恒等式 $V-E+F=2$. 这就是多面体的 Euler 公式. 对于一般的流形 M, 根据它的一个单纯剖分, 则可以计算它的各个维数单形的个数, 如 n-单形共有 C_n 个, 则 M 的 Euler 数为 $\sum(-1)^n C_n$, 记作 $\chi(M)$, 且 $\chi(M)$ 是一个拓扑不变量, 与 M 的单纯剖分的选取无关.

Gauss-Bonnet-Chern 定理

对于球面, 即 $\mathbb{S}^2$ 上的三角形内角和, 我们有 $\alpha+\beta+\gamma=\pi+\dfrac{S_{\triangle ABC}}{R^2}$.

当 M 是一般的曲面 (流形) 时, 定义在 M 上的每一个点 u 的 Gauss 曲率为 $K(u)$, 其中 Gauss 曲率刻画流形 M 在点 u 处的弯曲程度, 如在半径为 R 的球面上 $K(u)=\frac{1}{R^2}$ 等, 故对于流形 M 上的曲边 $\triangle ABC$ 且假设三边都是测地线, 则有 $\alpha+\beta+\gamma=\pi+\displaystyle\int_D K(u)\mathrm{d}S$, 其中 D 为流形 M 上的单连通区域 [Q] $\triangle ABC$, 如果用转角和来表示, 则上式写为 $A(D)+\displaystyle\int_D K(u)\mathrm{d}S=2\pi$, 其中 $A(D)$ 表示曲边 $\triangle ABC$ 在各顶点处的转角和.

但对于三边不是测地线的曲边 $\triangle ABC$, 则对于 $A(D)+\displaystyle\int_D K(u)\mathrm{d}S=2\pi$ 的左边需加一个连通区域 D 边界上的测地总曲率项为 $\displaystyle\int_{\partial D} k_g\mathrm{d}s$, 因此就得到了流形上的 Gauss-Bonnet 公式: $A(D)+\displaystyle\int_D K(u)\mathrm{d}S+\int_{\partial D} k_g\mathrm{d}s=2\pi$. 若令 $\varphi(D)=\dfrac{1}{2\pi}\left(A(D)+\displaystyle\int_D K(u)\mathrm{d}S+\int_{\partial D} k_g\mathrm{d}s=2\pi.\right)$, 并将 φ 推广到流形 M 上的一般曲边多边形 P, 我们最终得到以下定理 (Gauss-Bonnet-Chern):

定理 15. $\varphi(P)\equiv\dfrac{1}{2\pi}\left(A(P)+\displaystyle\int_P K(u)\mathrm{d}S+\int_{\partial P} k_g\mathrm{d}s\right)=\chi(P).$

最后说明一下 Gauss-Bonnet 公式的发展历史, 1827 年, Gauss 证明了当 P 是流形 M 上的一个测地三角形时上述公式成立, 后来 Bonnet 将 Gauss 的结果推广到 M 上的一般三角形的情形, 在 1942 年又被 Weil 推广到了高维情形, 1943 年陈省身 (Chern) 给出了高维情形下的 Gauss-Bonnet 公式的一个新的证明, 为后来关于示性类的 Chern-Weil 理论打下扎实的基础, 本文到此为止就是将三角形的内角和公式推广到了高维无边流形的 Gauss-Bonnet 公式, 也称作 Gauss-Bonnet-Chern 定理 (公式). 该公式将几何量曲率和拓扑量 Euler 数联系在一起, 是数学中最为优雅和深刻的结论之一.