国家出版基金资助项目

现代数学中的著名定理纵横谈丛书

丛书主编　王梓坤

JACOBI THEOREM

Jacobi定理

刘培杰数学工作室　编著

哈尔滨工业大学出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

国家出版基金项目
NATIONAL PUBLICATION FOUNDATION

现代数学中的著名定理纵横谈丛书
丛书主编　王梓坤

JACOBI THEOREM

Jacobi 定理

刘培杰数学工作室　编著

哈尔滨工业大学出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

内容简介

本书通过一道日本数学奥林匹克试题研究讨论雅可比定理及其相关知识.

本书可供从事这一数学分支或相关学科的数学工作者、大学生以及数学爱好者研读.

图书在版编目(CIP)数据

Jacobi 定理/刘培杰数学工作室编著. —哈尔滨:哈尔滨工业大学出版社,2017.6

(现代数学中的著名定理纵横谈丛书)

ISBN 978-7-5603-6511-4

Ⅰ.①J… Ⅱ.①刘… Ⅲ.①雅可比方法 Ⅳ.①O241.6

中国版本图书馆 CIP 数据核字(2017)第 048319 号

策划编辑 刘培杰 张永芹
责任编辑 张永芹 聂兆慈
封面设计 孙茵艾
出版发行 哈尔滨工业大学出版社
社 址 哈尔滨市南岗区复华四道街 10 号 邮编 150006
传 真 0451-86414749
网 址 http://hitpress.hit.edu.cn
印 刷 黑龙江艺德印刷有限责任公司
开 本 787mm×960mm 1/16 印张 23.25 字数 240 千字
版 次 2017 年 6 月第 1 版 2017 年 6 月第 1 次印刷
书 号 ISBN 978-7-5603-6511-4
定 价 98.00 元

⊙代序

读书的乐趣

你最喜爱什么——书籍.

你经常去哪里——书店.

你最大的乐趣是什么——读书.

这是友人提出的问题和我的回答.真的,我这一辈子算是和书籍,特别是好书结下了不解之缘.有人说,读书要费那么大的劲,又发不了财,读它做什么?我却至今不悔,不仅不悔,反而情趣越来越浓.想当年,我也曾爱打球,也曾爱下棋,对操琴也有兴趣,还登台伴奏过.但后来却都一一断交,"终身不复鼓琴".那原因便是怕花费时间,玩物丧志,误了我的大事——求学.这当然过激了一些.剩下来唯有读书一事,自幼至今,无日少废,谓之书痴也可,谓之书橱也可,管它呢,人各有志,不可相强.我的一生大志,便是教书,而当教师,不多读书是不行的.

读好书是一种乐趣,一种情操;一种向全世界古往今来的伟人和名人求

教的方法，一种和他们展开讨论的方式；一封出席各种活动、体验各种生活、结识各种人物的邀请信；一张迈进科学宫殿和未知世界的入场券；一股改造自己、丰富自己的强大力量. 书籍是全人类有史以来共同创造的财富，是永不枯竭的智慧的源泉. 失意时读书，可以使人重整旗鼓；得意时读书，可以使人头脑清醒；疑难时读书，可以得到解答或启示；年轻人读书，可明奋进之道；年老人读书，能知健神之理. 浩浩乎！洋洋乎！如临大海，或波涛汹涌，或清风微拂，取之不尽，用之不竭. 吾于读书，无疑义矣，三日不读，则头脑麻木，心摇摇无主.

潜能需要激发

我和书籍结缘，开始于一次非常偶然的机会. 大概是八九岁吧，家里穷得揭不开锅，我每天从早到晚都要去田园里帮工. 一天，偶然从旧木柜阴湿的角落里，找到一本蜡光纸的小书，自然很破了. 屋内光线暗淡，又是黄昏时分，只好拿到大门外去看. 封面已经脱落，扉页上写的是《薛仁贵征东》. 管它呢，且往下看. 第一回的标题已忘记，只是那首开卷诗不知为什么至今仍记忆犹新：

日出遥遥一点红，飘飘四海影无踪.

三岁孩童千两价，保主跨海去征东.

第一句指山东，二、三两句分别点出薛仁贵（雪、人贵）. 那时识字很少，半看半猜，居然引起了我极大的兴趣，同时也教我认识了许多生字. 这是我有生以来独立看的第一本书. 尝到甜头以后，我便千方百计去找书，向小朋友借，到亲友家找，居然断断续续看了《薛丁山征西》《彭公案》《二度梅》等，樊梨花便成了我心

中的女英雄.我真入迷了.从此,放牛也罢,车水也罢,我总要带一本书,还练出了边走田间小路边读书的本领,读得津津有味,不知人间别有他事.

当我们安静下来回想往事时,往往会发现一些偶然的小事却影响了自己的一生.如果不是找到那本《薛仁贵征东》,我的好学心也许激发不起来.我这一生,也许会走另一条路.人的潜能,好比一座汽油库,星星之火,可以使它雷声隆隆、光照天地;但若少了这粒火星,它便会成为一潭死水,永归沉寂.

抄,总抄得起

好不容易上了中学,做完功课还有点时间,便常光顾图书馆.好书借了实在舍不得还,但买不到也买不起,便下决心动手抄书.抄,总抄得起.我抄过林语堂写的《高级英文法》,抄过英文的《英文典大全》,还抄过《孙子兵法》,这本书实在爱得狠了,竟一口气抄了两份.人们虽知抄书之苦,未知抄书之益,抄完毫末俱见,一览无余,胜读十遍.

始于精于一,返于精于博

关于康有为的教学法,他的弟子梁启超说:"康先生之教,专标专精、涉猎二条,无专精则不能成,无涉猎则不能通也."可见康有为强烈要求学生把专精和广博(即"涉猎")相结合.

在先后次序上,我认为要从精于一开始.首先应集中精力学好专业,并在专业的科研中做出成绩,然后逐步扩大领域,力求多方面的精.年轻时,我曾精读杜布(J. L. Doob)的《随机过程论》,哈尔莫斯(P. R. Halmos)的《测度论》等世界数学名著,使我终身受益.简言之,即"始于精于一,返于精于博".正如中国革命一

样，必须先有一块根据地，站稳后再开创几块，最后连成一片.

丰富我文采，澡雪我精神

辛苦了一周，人相当疲劳了，每到星期六，我便到旧书店走走，这已成为生活中的一部分，多年如此. 一次，偶然看到一套《纲鉴易知录》，编者之一便是选编《古文观止》的吴楚材. 这部书提纲挈领地讲中国历史，上自盘古氏，直到明末，记事简明，文字古雅，又富于故事性，便把这部书从头到尾读了一遍. 从此启发了我读史书的兴趣.

我爱读中国的古典小说，例如《三国演义》和《东周列国志》. 我常对人说，这两部书简直是世界上政治阴谋诡计大全. 即以近年来极时髦的人质问题（伊朗人质、劫机人质等），这些书中早就有了，秦始皇的父亲便是受害者，堪称“人质之父”.

《庄子》超尘绝俗，不屑于名利. 其中“秋水”“解牛”诸篇，诚绝唱也.《论语》束身严谨，勇于面世，“己所不欲，勿施于人”，有长者之风. 司马迁的《报任少卿书》，读之我心两伤，既伤少卿，又伤司马；我不知道少卿是否收到这封信，希望有人做点研究. 我也爱读鲁迅的杂文，果戈理、梅里美的小说. 我非常敬重文天祥、秋瑾的人品，常记他们的诗句：“人生自古谁无死，留取丹心照汗青”“休言女子非英物，夜夜龙泉壁上鸣”. 唐诗、宋词、《西厢记》《牡丹亭》，丰富我文采，澡雪我精神，其中精粹，实是人间神品.

读了邓拓的《燕山夜话》，既叹服其广博，也使我动了写《科学发现纵横谈》的心. 不料这本小册子竟给我招来了上千封鼓励信. 以后人们便写出了许许多多

的“纵横谈”.

从学生时代起,我就喜读方法论方面的论著.我想,做什么事情都要讲究方法,追求效率、效果和效益,方法好能事半而功倍.我很留心一些著名科学家、文学家写的心得体会和经验.我曾惊讶为什么巴尔扎克在51年短短的一生中能写出上百本书,并从他的传记中去寻找答案.文史哲和科学的海洋无边无际,先哲们的明智之光沐浴着人们的心灵,我衷心感谢他们的恩惠.

读书的另一面

以上我谈了读书的好处,现在要回过头来说说事情的另一面.

读书要选择.世上有各种各样的书:有的不值一看,有的只值看20分钟,有的可看5年,有的可保存一辈子,有的将永远不朽.即使是不朽的超级名著,由于我们的精力与时间有限,也必须加以选择.决不要看坏书,对一般书,要学会速读.

读书要多思考.应该想想,作者说得对吗?完全吗?适合今天的情况吗?从书本中迅速获得效果的好办法是有的放矢地读书,带着问题去读,或偏重某一方面去读.这时我们的思维处于主动寻找的地位,就像猎人追找猎物一样主动,很快就能找到答案,或者发现书中的问题.

有的书浏览即止,有的要读出声来,有的要心头记住,有的要笔头记录.对重要的专业书或名著,要勤做笔记,“不动笔墨不读书”.动脑加动手,手脑并用,既可加深理解,又可避忘备查,特别是自己的灵感,更要及时抓住.清代章学诚在《文史通义》中说:“札记之功必不可少,如不札记,则无穷妙绪如雨珠落大海矣.”

许多大事业、大作品，都是长期积累和短期突击相结合的产物. 涓涓不息，将成江河；无此涓涓，何来江河？

爱好读书是许多伟人的共同特性，不仅学者专家如此，一些大政治家、大军事家也如此. 曹操、康熙、拿破仑、毛泽东都是手不释卷，嗜书如命的人. 他们的巨大成就与毕生刻苦自学密切相关.

王梓坤

目录

椭圆曲线及其在密码学中的应用

绪论

1. 引　　言

日本数学奥林匹克与日本制造一样缺乏原创性,但善于模仿且能推陈出新. 与我国的 CMO 相比虽技巧性稍逊一筹,但能紧跟世界数学主流,且命题者颇具数学鉴赏力,知道哪些是“好数学”,哪些是包装精美的学术垃圾. 随着时间的推移,我们越来越能体会到其眼光的独到以及将尖端理论通俗化的非凡能力. 例如1992 年日本数学奥林匹克预赛题第 3 题为:

试题　坐标平面上,设方程

$$y^2 = x^3 + 2\,691x - 8\,019$$

所确定的曲线为 E,联结该曲线上的两点(3,9)和(4,53)的直线交曲线 E 于另一点,求该点的坐标.

解　由两点式易得所给直线的方程为 $y = 44x - 123$. 将它代入曲线方程并整理得

$$x^3 - 1\,936x^2 + (2 \times 44 \times 123 + 2\,691)x -$$
$$(123^2 + 8\,019) = 0$$

由韦达定理得

$$x + 3 + 4 = 1\,936$$

所以所求点 x 的横坐标为

$$x = 1\,936 - (3 + 4) = 1\,929$$

这道貌似简单的试题实际上是一道具有深刻背景的椭圆曲线特例.

2. 牛顿对曲线的分类

笛卡儿(Descartes)早就讨论过一些高次方程及其代表的曲线. 次数高于 2 的曲线的研究变成众所周知的高次平面曲线理论,尽管它是坐标几何的组成部分. 18 世纪所研究的曲线都是代数曲线,即它们的方程由 $f(x, y) = 0$ 给出,其中 f 是 x 和 y 的多项式. 曲线的次数或阶数就是项的最高次数.

牛顿(Newton)第一个对高次平面曲线进行了广泛的研究. 笛卡儿按照曲线方程的次数来对曲线进行分类的计划深深地打动了牛顿,于是牛顿用适合于各次曲线的方法系统地研究了各次曲线,他从研究三次曲线着手. 这个工作出现在他的《三次曲线枚举》(*Enumeratio Linearum Tertii Ordinis*)中,这是作为他的《光学》(*Opticks*)英文版的附录在 1704 年出版的. 但实际上大约在 1676 年就做出来了,虽然在 La Hire 和

Wallis的著作中使用了负 x 值,但牛顿不仅用了两个坐标轴和负 x 负 y 值,而且还在所有四个象限中作图.

牛顿证明了怎样能够把一般的三次方程

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

所代表的一切曲线通过坐标轴的变换化为下列四种形式之一:

(1) $xy^2 + ey = ax^3 + bx^2 + cx + d.$

(2) $xy = ax^3 + bx^2 + cx + d.$

(3) $y^2 = ax^3 + bx^2 + cx + d.$

(4) $y = ax^3 + bx^2 + cx + d.$

牛顿把第三类曲线叫作发散抛物线(diverging parabolas),它包括如图 1 所示的五种曲线. 这五种曲线是根据右边三次式的根的性质来区分的:全部是相异实根;两个根是复根;都是实根但有两个相等,而且复根大于或小于单根;三个根都相等. 牛顿断言,光从一点出发对这五种曲线之一作射影,然后取射影的交线就能分别得到每一个三次曲线.

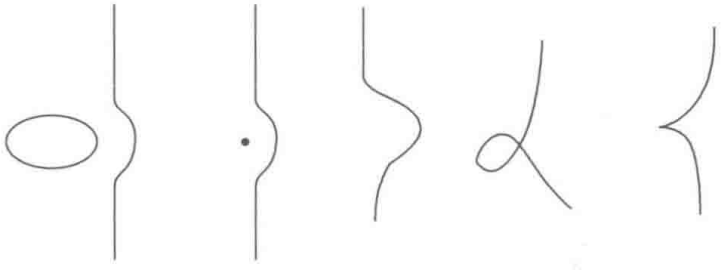

图 1

牛顿对他在《三次曲线枚举》中的许多断言都没有给出证明. 斯特林(Stirling)在《三次曲线》中证明了

或用别的方法重新证明了牛顿的大多数断言,但是没有证明射影定理,射影定理是由法国数学家克莱罗(Clairaut Alexis-Claude,1715—1763)和弗朗塞兄弟(Francois Nicole,1683—1758)证明的. 其实牛顿识别了 72 种三次曲线. 英国数学家斯特林加上了四种,修道院院长 Jean-Paul de Gua de Malves 在他 1740 年题为《利用笛卡儿的分析而不借助于微积分去进行发现……》(*Usage de Vanalyse de Descartes pourdécouvrir sans le Secours du calcul differential…*)的书里又加了两种.

牛顿关于三次曲线的工作激发了关于高次平面曲线的许多其他研究工作. 按照这个或那个原则对三次和四次曲线进行分类的课题继续使 18 和 19 世纪的数学家们感兴趣. 随着分类方法的不同,所找到的分类数目也不同.

椭圆曲线是三次的曲线,不过它们是在一个适当的坐标系内的三次曲线. 任一形如

$$y^2=(x-\alpha)(x-\beta)(x-\gamma)(x-\delta)$$

的四次曲线可以写成

$$\left(\frac{y}{x-\alpha}\right)^2=\left(1-\frac{\beta-\alpha}{x-\alpha}\right)\left(1-\frac{\gamma-\alpha}{x-\alpha}\right)\left(1-\frac{\delta-\alpha}{x-\alpha}\right)$$

因此它在坐标

$$X=\frac{1}{x-\alpha},Y=\frac{y}{(x-\alpha)^2}$$

之下是三次的,特别地,$y^2=1-x^4$ 在坐标 $X=\frac{1}{x-\alpha}$,$Y=\frac{y}{(x-\alpha)^2}$之下化为三次的:$Y^2=4X^3-6X^2+4X-1$.