

蛙鸣

第 52 期

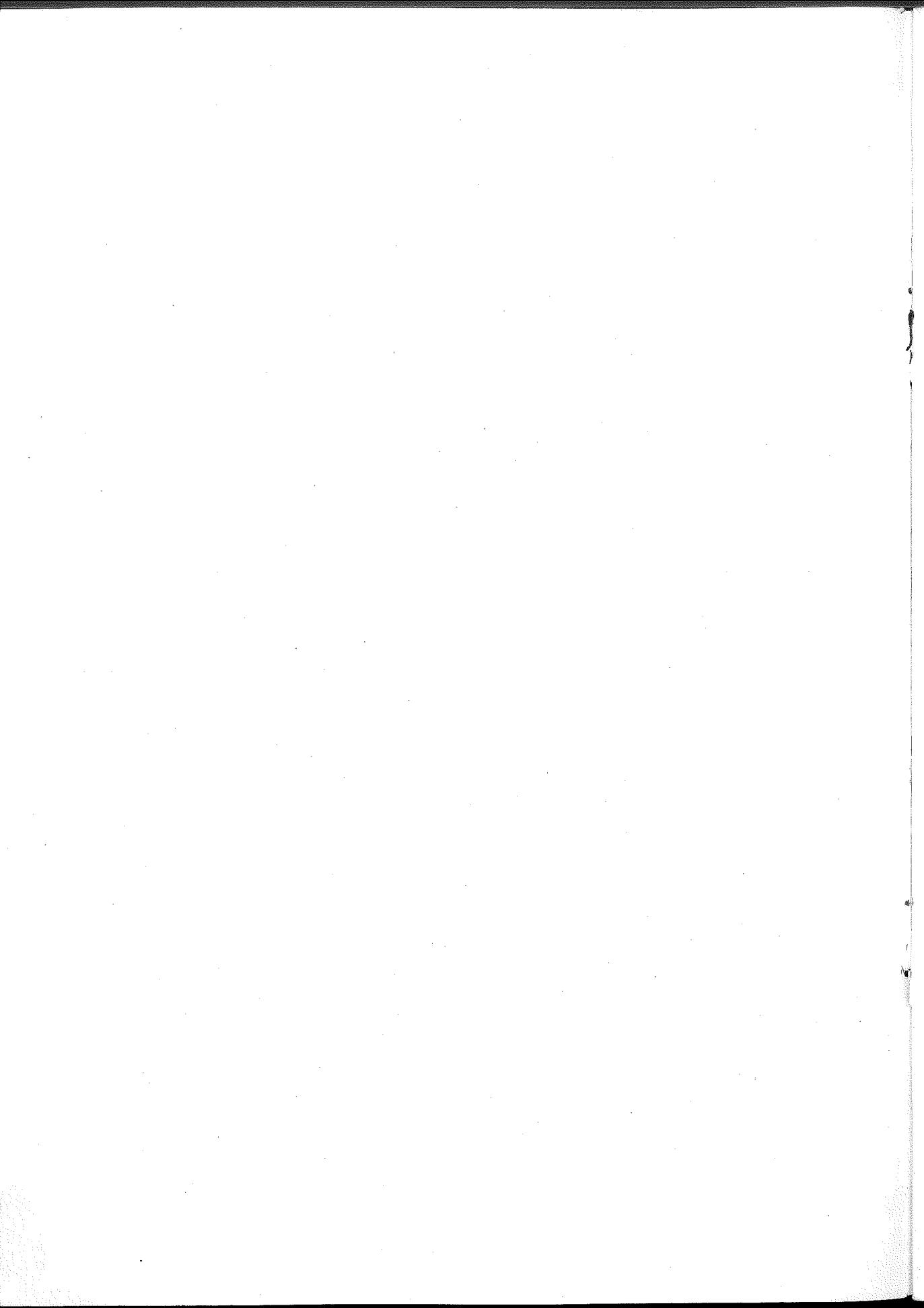
中国科学技术大学

《蛙鸣》编委会

数学系学生会学习部

主办

一九九五年十月



目 录

见闻篇

北京十日——夏令营散记 9201 喻甫祥 1

试题选登

第九届全国大学生数学夏令营 3

1995 年全国大学生数学模型竞赛试题 6

问题征解

117 — 119 13

研究与讨论

欧氏空间中两两成等角向量组 9301 许斌 11

Z_n^* 群的结构探索 9301 吴畏 14

Hall 定理与 $G[H]$ 的可迁性 9101 张林 21

周长最大的椭圆内接 n 边形 9301 马翔 24

关于魔方 9301 黄华君 29

数学小品

面面俱到的代表性 9301 马翔 17

小议 n 点集中特定距离的个数 9301 黄华君 19

日知录

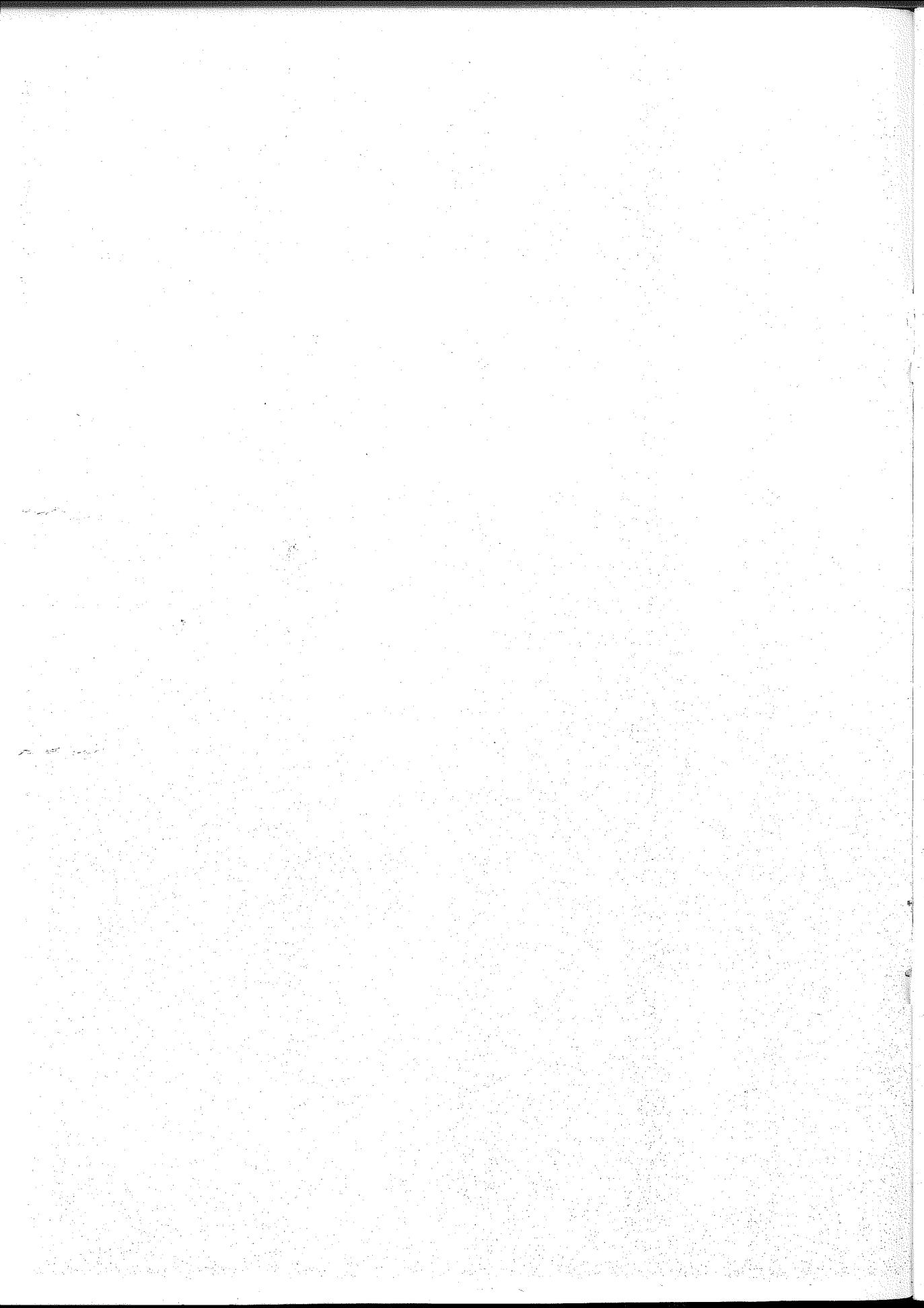
标准形的妙用 9301 黄华君 23

人物传记

数坛巾帼 9401 虞咏峰 8

主 编 马 翔

责任编辑 黄华君 王凌峰 马 翔



北京十日

——夏令营散记

见闻篇

喻甫祥

七月十八日中午，我和陈玉国一下火车，就让北京的雨给淋得浑身不舒服。挤了两个小时的公共汽车，才到了中关村。雨却停了。

次日上午，数学所举行了第九届数学夏令营的开幕式。新任的龙瑞麟所长致了开幕词。接着我们被告知，数学所给营员安排的活动有学术报告，数学测试和旅游等。我们高兴地见到了杨乐院士。

简短的开幕式结束后，杨乐做了题为《复分析漫谈》的报告。杨乐是青年三杰中保持活力的唯一一人（另外两杰是英年早逝的张广厚和长期住院的陈景润），被引为青年学生的楷模。今天他针对我们的课程学习情况，准备了一些浅显的材料，从它们讲到复分析的精深理论，真可谓深入浅出。其逻辑之严密，语言之流畅，及板书之漂亮，都给我留下了深刻印象。杨乐名不虚传。我愿承认这是我听到的最好的报告。

但隔一两天举行的学术报告会就不那么好懂了。这大概就是一个北大朋友告诉我的道理：抱着想听懂的目的去是会失败的，反之则会有所收获。北大陈维桓、潘承彪二教授分别介绍了微分几何和解析数论的发展史，潘的一句话很有意思：解析数论已到了山穷水尽的地步，正因如此她也充满了希望。数学所李树杰研究员介绍了变分法的兴衰史，和山路、山峰、山岭等相联系的两个定理非常美妙。王元院士做了题为《统计中的数论方法》的报告，令我耳目一新：原来数论也并非不实用啊。王元今年出人意料的推出了一部华罗庚传记，因其内容丰富翔实而受到广泛关注。我有幸搞到了有王元签名的这本《华罗庚》。

20 日和 22 日分别进行了三小时的数学测试。除第二试最后一题外，其余题目都不太难，少数可以一眼看穿。但是要在规定的时间内把所有题目想出来，工整的书写在考卷上，也并不容易。只有少走或不走弯路才成。第一试我没全对，而我以为所有水平高的都不会有错，所以第二试我必须多拿分才行。由于心理负担较重，我在考场上患得患失，实际上并没实现目标。

在报告、测试的间隙里，数学所组织大家到颐和园、天安门、长城、元

等名胜古迹游玩。北京倾倒了所有外省人。我重游故地，倍感亲切。

第二试结束后的 22 日下午，夏令营座谈会在数学所舒适的阅览室举行。数学所除院士外的在京精英都出席了。据介绍，拥有四位院士的数学所有一百多位科研人员，现有基础数学、计算数学和计算机软件三个方向，是国内外知名的开放研究所，和普林斯顿等国外研究院联系颇多，出国机会据言非常多。所领导还说，数学所每年光图书一项就花一百万元，资金充足，随着科技投入的增多，情况会更好；数学所的住宿等生活条件较好；入学考试题目不比科大、复旦的难，似乎非常容易考取。许以超研究员代表数学所表达了为振兴中国数学，要把夏令营坚持办下去的决心，其言真挚感人。鉴于没有自动发言的同学，科大、复旦被点名发言。我介绍了科大的“4-2-3 分流”人才培养模式，引起数学所的一定兴趣。复旦同学说复旦志愿基础的不多。一个家在厦门特区的同学向大家诉说了自己对数学有兴趣，但又不知怎样应对家人的“经济期待”的矛盾心情。会场一时寂静无声！

24 日上午举行了闭营式。此次活动的赞助单位华晨集团代表表示，华晨集团将一如既往的支持基础研究。随后宣布了获奖个人和团体。科大少年班蒋晓伟荣获一等奖，我获得了三等奖，南开、复旦分享了其余两个二等奖和两个三等奖；团体前三名则是南开大学、科大少年班和复旦大学。其实，前几名的差距并不大，这次没获奖的科大数学系陈玉国同学和少年班杨志青、方磊两位同学也都考得不错，我想北京大学、武汉大学等大学的同学也是如此。

夏令营结束后，我住进了北大老乡的宿舍里，准备逛一逛北京的书店，会一会北京的师友。九章数学书店在海淀图书城很不起眼，但好书非常多，好多书我都想读一读，但最后还是没买几本，“贪多嚼不烂”啊。我没去易地营业的王府井书店，只在汽车里看到了面目全非的书店旧址。北大数学系有很多同学，他们因军训比我少念了一年，但都考过了 TOFEL 或正在准备，其中一位将于八月份去美国；学习抓得很紧，暑假上自习到晚上十点才回来；北大数学系也注重应用，有些同学拥有私人电脑。由数学系领衔的方正集团闻名全国。我那些学文科或经济的老乡也都很忙碌。北大校园里随处可见拎着书包的学生。当然，林子大了，什么鸟都有：老乡隔壁的一位文科生和我聊了半天考经，介绍了一些通过考试的法门，听到“精妙处”我不禁瞠目结舌。

27 日中午，我登上了返肥的火车。夏令营考得不好，我有些惭愧，细想起

来还有些后怕：我是不敢再参加这种考试了。但不管怎么说，我得到了一次全面的锻炼。而且，夏令营活动让我长了知识，开了眼界。见到新老朋友也让我异常高兴。数学夏令营只是我大学生活的一个中间站，但它应当是一个特别的中间站。在北京度过的十个月日夜夜，将在我脑海里打下不浅的烙印。

第九届全国大学生数学夏令营

试题选登

第一试试题

(三小时完成，每题 20 分)

1. 设实值函数 $f \in C^2([0, \pi])$ ，且 $f(0) = f(\pi) = 0$ ，令 $f(x)$ 的 Fourier 展开式为

$$f(x) = \sum_{k=1}^{\infty} a_k \sin kx,$$

令

$$S_n(x) = \sum_{k=1}^n a_k \sin kx, \quad n = 1, 2, \dots$$

证明：

a) $a_k = -\frac{2}{\pi k^2} \int_0^\pi f''(x) \sin kx dx, \quad k = 1, 2, \dots$

b) $\int_0^\pi [f(x) - S_n(x)]^2 dx \leq \frac{1}{3n^3} \int_0^\pi [f''(x)]^2 dx, \quad n = 1, 2, \dots$

2. 试求所有适合条件 $0 < n < m, m^n = n^m$ 的正整数对 (m, n) 。

3. 设实值函数 $f \in C^1([0, +\infty))$ ，且满足条件 $\lim_{x \rightarrow +\infty} (f(x) + f'(x)) = 0$ 。

试证： $\lim_{x \rightarrow +\infty} f(x) = 0$ 。

4. 给定线性映射 $A : \mathbb{R}^n \rightarrow \mathbb{R}^n, B : \mathbb{R}^n \rightarrow \mathbb{R}^m$ 。记 $N(B) = \{x \in \mathbb{R}^n | Bx = 0\}$ ，令 $\pi : \mathbb{R}^n \rightarrow N(B)$ 为正交投影。如果 $\pi \circ A : \mathbb{R}^n \rightarrow N(B)$ 限制在 $N(B)$ 上

为线性同构, 且存在正数 a , 使得

$$\inf_{0 \neq y \in \mathbb{R}^m} \sup_{0 \neq x \in \mathbb{R}^n} \frac{(y, Bx)}{|x| \cdot |y|} \geq a,$$

试证: 对任意 $f \in \mathbb{R}^n, g \in \mathbb{R}^m$, 线性方程组

$$\begin{cases} Ax + B^T y = f \\ Bx = g \end{cases}$$

都存在唯一解, 其中 B^T 为由 $(y, Bx) = (B^T y, x), \forall y \in \mathbb{R}^m, \forall x \in \mathbb{R}^n$ 定义的 B 的共轭线性映射.

5. 设 $f(z)$ 在单位圆 $\{z \in \mathbb{C} \mid |z| < 1\}$ 内解析, 且 $|f(z)| < 1, \forall |z| < 1$. 设 $f(z)$ 在 $z = 1$ 处解析, 且 $f(0) = 0, f(1) = 1$. 试证: $f'(1) \geq 1$.

第二试试题

(三小时完成. 每题 25 分)

1. 设 $n \in \mathbb{N}$. 求值:

$$(1) \quad \operatorname{Re} \int_{|z|=n\pi} \tan z dz; \quad (2) \quad \int_{|z|=n\pi+\frac{\pi}{2}} \frac{1}{\sin^2 z} dz.$$

2. 设 $f(x)$ 为 \mathbb{R} 上的实 Lebesgue 可测函数. 试证:

- (a) 若对所有整数 n 及所有实数 x , 都有 $f(nx) = nf(x)$, 则存在实数 λ , 使得 $f(x) = \lambda x$ 在 \mathbb{R} 上几乎处处成立;
- (b) 若有 $f(x+y) = f(x) + f(y), \forall x, y \in \mathbb{R}$, 试证: 存在实数 λ , 使得 $f(x) = \lambda x, \forall x \in \mathbb{R}$.

3. 设实值函数 $f \in C^1(\mathbb{R}^2)$ 适合偏微分方程

$$\frac{\partial f}{\partial x} + f \frac{\partial f}{\partial y} = 0.$$

试证: f 为常数.

4. 设 x 为特征 2 的有限域 F 上的超越元. 给定 F 上 $n \times n$ 方阵 P, Q . 对 F 上 n 维列向量 $a = (a_1, \dots, a_n)^T$ (T 表示转置) 定义映射 $f: a \mapsto x^a = (x^{a_1}, \dots, x^{a_n})^T$, $f_Q: a \mapsto x^{Qa} = (x^{b_1}, \dots, x^{b_n})^T$, 其中 $Q_a = (b_1, \dots, b_n)^T$. 记

I 为单位方阵. 对 F 上 n 维向量 a, b , 定义形式乘法

$$\begin{pmatrix} I & Pf_Q \\ 0 & I \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a + Pf_Q(b) \\ b \end{pmatrix}.$$

给定 $2n \times 2n$ 非异方阵

$$A = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}, B = \begin{pmatrix} B_1 & B_2 \\ B_3 & B_4 \end{pmatrix}, C = \begin{pmatrix} C_1 & C_2 \\ C_3 & C_4 \end{pmatrix}$$

及 $n \times n$ 方阵 P_1, P_2, Q_1, Q_2 . 按上面定义可引进公式

$$\begin{pmatrix} l \\ r \end{pmatrix} = A \begin{pmatrix} I & P_1 f_{Q_1} \\ 0 & I \end{pmatrix} B \begin{pmatrix} I & P_2 f_{Q_2} \\ 0 & I \end{pmatrix} C \begin{pmatrix} L \\ R \end{pmatrix}, \quad (*)$$

其中 L, R 为 F 上 n 维列向量, 因此 l, r 也为 F 上 n 维列向量.

下面解释公式 (*) 的含义. 所谓“密码”是指将一个重要信件变成一组由 $2n$ 维列向量 $(L^T, R^T)^T$ 表达的数据. 每个列向量 $(L^T, R^T)^T$ 表示一个字, 称为原码字. 经过公式 (*), 原码字 $(L^T, R^T)^T$ 变为加密后的码字 $(l^T, r^T)^T$. 将这一组加密后的码字用无线电波发射出去, 我方接收到后, 再代入 (*) 之逆映射公式 (注意, 映射 $(L^T, R^T)^T \rightarrow (l^T, r^T)^T$ 必须为一一对应), 便解密为原码字, 从而获得重要信息. 然而敌方也可接收到这一组加密后的码字. 敌方若也能解密, 则称这种加密方案被破译.

另一方面, 公式 (*) 可改写为

$$\begin{pmatrix} l \\ r \end{pmatrix} = D \begin{pmatrix} L \\ R \end{pmatrix} + E \begin{pmatrix} s \\ t \end{pmatrix}, \quad (**)$$

其中 D 为 F 上 $2n \times 2n$ 非异方阵, E 为 F 上 $2n \times 2n$ 方阵, 又

$$s = f(F_1 L + F_2 R),$$

$$t = f(F_3 L + F_4 R + F_5 s),$$

其中 F_1, F_2, F_3, F_4, F_5 为 $n \times n$ 方阵.

所谓“公开钥密码”是指上面的加密方案 (**)(即 (*)) 中的常数方阵 F_1, F_2, F_3, F_4, D, E 都公开, 但是常数方阵 $A, B, C, P_1, P_2, Q_1, Q_2, F_5$ 都不公开.

试证: 此加密方案可以被破译.

* 试题选登 *

1995 年全国大学生 数学模型竞赛试题

A 题 一个飞行管理问题

在约 10,000 米高空的某边长 160 公里的正方形区域内, 经常有若干架飞机作水平飞行. 区域内每架飞机的位置和速度向量均由计算机记录其数据, 以便进行飞行管理. 当一架欲进入该区域的飞机到达区域边缘时, 记录其数据后, 要立即计算并判断是否会与区域内的飞机发生碰撞. 如果会碰撞, 则应计算如何调整各架(包括新进入的)飞机飞行的方向角, 以避免碰撞. 现假定条件如下:

- 1) 不碰撞的标准为任意两架飞机的距离大于 8 公里;
- 2) 飞机飞行方向角调整的幅度不应超过 30 度;
- 3) 所有飞机飞行速度均为每小时 800 公里;
- 4) 进入该区域的飞机在到达区域边缘时, 与区域内飞机的距离应在 60 公里以上;
- 5) 最多需考虑 6 架飞机;
- 6) 不必考虑飞机离开此区域后的状况.

请你对这个避免碰撞的飞行管理问题建立数学模型, 列出计算步骤, 对以下数据进行计算(方向角误差不超过 0.01 度), 要求飞机飞行方向角调整的幅度尽量小.

设该区域 4 个顶点的座标为 (0,0),(160,0),(160,160),(0,160). 记录数据为:

飞机编号 横坐标X 纵坐标Y 方向角度(度)

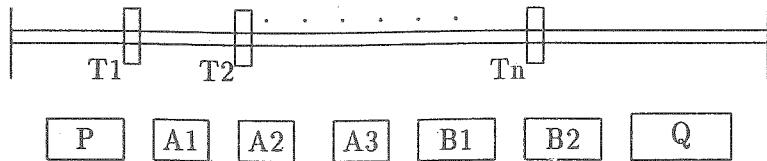
1	150	140	243
2	85	85	236
3	150	155	220.5
4	145	50	159
5	130	150	230
新进入	0	0	52

注: 方向角指飞行方向与 X 轴正向的夹角.

试根据实际应用背景对你的模型进行评价与推广.

B 题 天车与冶炼炉的作业调度

某钢铁厂冶炼车间的厂房布局是, 地面沿一直线依次安置着 7 个工作点: 辅料供应处 P; A 组 3 座转炉(冶炼成品钢) A1,A2,A3; B 组 2 座冶炼炉(冶炼半成品钢, 简称半钢) B1,B2; 原料供应处 Q. 这些设备的上方贯通着一条运送物料的天车轨道, 上面布置着若干天车 T1,T2,...,Tn 为炉子作业服务. 布局示意图如下.



天车与冶炼炉的作业过程与工序为: 天车从 Q 处吊起原料一罐(吊罐时间 t_y)运至 B1 或 B2 处放下(放罐时间 t_i), 并将上一炉的原料空罐吊起(吊空罐时间 t_o)返回 Q 处放下(放空罐时间 t_k), B 组炉在原料罐放下后即可在辅助作业下开始冶炼(冶炼时间 t_b), 冶炼后将半钢倒入空半钢罐(时间计人 t_b), 由天车吊起半钢罐(吊罐时间 t_d)运至 A1 或 A2、A3 处将半钢倒入转炉(倒入时间 t_e), 并将空罐返回 B1 或 B2 处放下(放空罐时间 t_c). 再由天车从 P 处吊起辅料一槽(吊槽时间 t_g)运至 A1 或 A2、A3 处加入转炉(加入时间 t_f), 并将空槽返回 P 处放下(放空槽时间 t_h). A 组炉在半钢和辅料加入后即可开始冶炼(冶炼时间 t_a), 冶炼后成品钢的输出不用天车(输出时间计人 t_a). 天车通过相邻两个工作点的运行时间都相同, 记为 t_x .

由于各台天车在同一条轨道上运行, 因此其顺序位置 T_1, T_2, \dots, T_n 不可交换. 在同一时间同一座炉子上只能允许一台天车作业; 但 P、Q 两处可以允许多台天车同时作业. 在 P,A1,...,Q 每两个相邻工作点之间最多能容纳 2 台天车同时停放.

天车与冶炼炉作业调度的要求为: (1) 成品钢产量尽量高; (2) 各台天车的作业率(天车作业时间所占比例)尽量均衡(考虑到设备及人员安全等因素, 一般天车作业率不超过 70 %); (3) 绝不允许出现天车相撞等事故; (4) 调度规则尽量简明, 以利于现场人员使用.

现设定: $t_a = 48$, $t_b = 27$, $t_i = 3$, $t_o = 2$, $t_c = 2$, $t_d = 3$, $t_e = 5$, $t_f = 2$, $t_g = 2$, $t_h = 1$, $t_y = 3$, $t_k = 2$ (单位: 分钟), $t_x = 15$ 秒; A 组炉平均每炉产量 $W_a = 120$ 吨. 在不超过 5 台天车的条件下, 设计一种满足上述要求的天车与冶炼炉的作业

调度方案:

- (1) 各台天车负责哪些作业(列出《工序清单》);
- (2) 在所给方案的一个运行周期内,每一时刻天车和冶炼炉处于什么状态(画出《天车—炉子作业运行图》);
- (3) 一份供现场人员使用的《调度规则说明书》;
- (4) 在所给方案下计算各台天车的作业率.

并按每天冶炼炉数估计该车间成品钢的年产量(扣除设备维修日,每台转炉作业日每年按300天计算).

实际生产过程中, t_a, t_b, \dots, t_k 都是随机的(上面设定的数值可视为平均值),讨论你的调度方案如何适用于实际生产过程.试提出该车间提高钢产量到年产300万吨以上的建议.

* 人物传记 *

数 坛 巾 帜

虞咏峰

近日,联合国第四届世界妇女大会在北京召开,这又一次唤起了全社会对妇女问题的关注.历史上,妇女为争得与男子平等的权利和社会地位,经历了长期的斗争,推动了社会的进步,并且涌现出大批女性的骄傲代表.下面要为大家介绍的,就是数学界的三位巾帼奇才.

古希腊女数学家希帕提娅是数学史上第一位杰出的女性.她生活在埃及的亚历山大,距今约一千六百多年.古希腊人活泼开朗,热爱科学、艺术,她的父亲就是一名出色的数学教师,因此,希帕提娅从小受到良好的教育.17岁时,在一场辩论会上,她用简单的推理解释了芝诺悖论而出名.后来,她协助父亲校订了欧几里得的《几何原本》和托勒密的《数学汇编》,以后这些书便成为了经典著作的范本流传至今.她还给丢番图的《算术》和阿波罗尼斯的《圆锥曲线论》作评注,书中也有她自己的创见.

希帕提娅被人誉为“女神”，无论走到哪里，人们象接待贵族那样迎接她，从欧、亚、非三洲各地来的学生都来听她讲的数学课，她得到了极高的荣誉。

下一位是近代俄国伟大的女数学家索菲·柯瓦列夫斯卡娅。1850 年出生在莫斯科的一个贵族家庭，自幼聪明好学，尤其在数学上表现出天才，但是沙皇政府禁止妇女接受高等教育，索菲为了去西欧上大学不得不采取一种“假婚”的做法：选一位也想出国的青年朋友，形式上结为夫妇，“妻子”可以不受家庭约束到国外去，所以她同莫斯科大学古生物系毕业生弗拉季米尔一起前往德国海德堡大学。在那里，除了自己专心学习外，她帮助过其他许多女青年，其中一位叫尤莉亚，她想申请听著名化学家本生的课，但被本生训斥一顿后轰了出来。索菲十分气愤，立即去找这位盛气凌人的怪教授，当面义正辞严地驳斥本生的大男子主义，同时机智地说服他收下尤莉亚，本生哑口无言，只好答应。

1870 年索菲到了柏林大学，大胆地求教于魏尔斯特拉斯。这位数学分析之父被她的热情、诚恳感动了，因为柏林大学拒绝招收女生，所以他为索菲单独授课达四年之久。后来她完成了关于微分方程、阿贝尔积分和土星光环的三篇论文，获哥廷根大学博士学位。回国后，沙皇政府仍然不准妇女进大学，而且对她进行迫害，她的丈夫无辜受到刑事指控，有口难辩，含冤自尽。索菲悲痛欲绝，但她决不是一个软弱的女性，公开地和恶势力作斗争，经过亲自调查，以充分的事实为丈夫恢复了名誉。同时她又以顽强的毅力继续数学研究，但仍被环境所迫逃往男女比较平等的瑞典，被聘为斯德哥尔摩大学讲师，后成为终身教授。1888 年她因解决了刚体绕定点转动的一般情形问题而获法国科学院最高奖博尔丹奖，后又成为俄国彼得堡科学院通讯院士。

她一生兴趣广泛，对文学有很深的造诣。少年时期她就喜欢写诗，成年后她写过不少小说和剧本，大多反映妇女解放运动。就象她自己说的那样：“如果心灵上不是一个诗人，那就不可能成为数学家。”

第三位则堪称数学界的泰山北斗，她就是本世纪德国犹太女数学家爱米·诺特。她 1882 年生于德国的埃尔兰根。青少年时期她并不象前两位那样才气焕发，而且没有任何出众之处，但对数学兴趣浓厚。本世纪初世界数学

中心是德国哥廷根大学。1916年，从埃尔兰根大学博士毕业的爱米来到这里，受到希尔伯特的赏识。在哥廷根大学就职论文中，她把对称不变性和物理守恒定律联系在一起，给出诺特定理。但顽固的旧势力反对爱米当讲师；他们说：“当我们的战士从战场回到课堂，发现自己将拜倒在女人脚下读书，会有何感想呢？”希尔伯特批驳道：“候选人的性别不应该成为反对她当讲师的理由，大学评议会毕竟不是洗澡堂。”在希尔伯特的据理力争下，爱米终于走上了讲台。

第一次世界大战结束后，妇女身上的枷锁多少有所解脱。坎坷的生活，永远不能挫伤爱米的研究热情，她开始自己独特的研究方向，1921年写出了《整环的理想理论》，崭新的数学分支——抽象代数，经爱米之手破土而出，后来成为二十世纪数学园地中最耀眼夺目的鲜花。她领导一个学派，手下有丢林、韦特、费廷，两个苏联人乌利逊和亚历山大洛夫，还有荷兰人范德瓦尔登，他们后来都成为了世界著名的数学家。但是好景不长，1933年希特勒上台后，疯狂驱赶和屠杀犹太人。诺特刚战胜了对于女性的偏见，却又痛苦地看到了政治谎言和种族歧视，看到了文明人的愚昧怎样摧毁了德国数学的优秀传统。她被迫迁往美国普林斯顿，在那里度过余生。

爱米·诺特的数学思想直接影响了30年代以后的代数学，乃至代数拓扑学、代数数论、代数几何的发展，而这些均属现代数学的主流。爱因斯坦这样评价她：“诺特女士是自从妇女开始受到高等教育以来最有创造性的数学天才，她使纯粹数学成了一首逻辑概念的诗篇。”

纵观这三位女数学家，因为她们分别属于不同时代，不好比较她们在数学上的贡献大小，但我认为索菲·柯瓦列夫斯卡娅尤为可贵和崇高。她在妇女受到严重歧视的时代，冲破传统的偏见和社会的压制，刻苦勤奋，勇于探索，在数学领域攀登上举世瞩目的高峰，宣告妇女也能和男人一样在科学上有所发明创造。

回顾索菲逝世以来一个世纪，妇女不能进大学的时代已经一去不复返了，女教授、女科学家、女工程师也不再是凤毛麟角。但是，妇女的地位并没有完全改善。全社会都应该来关心这个问题，反思自己的傲慢与偏见。而妇女更需要依靠自己的力量，全力投入世界的创造，以恢复倾斜的社会平衡。

欧氏空间中两两成等角的向量组

研究与讨论

许斌

在欧氏空间中, 向量 α, β 之间的夹角 θ 定义为

$$\theta = \arccos \frac{(\alpha, \beta)}{\sqrt{(\alpha, \alpha)(\beta, \beta)}},$$

这里 (\cdot, \cdot) 为欧氏空间中向量的内积. 若 $0 < \theta < \frac{\pi}{2}$, 称 α 与 β 成锐角; 若 $\frac{\pi}{2} < \theta < \pi$, 则称 α 与 β 成钝角. 记 n 维欧氏空间为 E_n . 本文中约定 $n \geq 2$.

1. 几个结论

引理 1: E_n 中单位向量组 $\{\alpha_1, \alpha_2, \dots, \alpha_k\}$ ($k \leq n$) 两两成相等的锐角 $\theta = \arccos \sigma$, 则 $\{\alpha_1, \alpha_2, \dots, \alpha_k\}$ 线性无关.

定理 1: $\forall k \leq n$, E_n 中存在单位向量组 $\{\alpha_1, \alpha_2, \dots, \alpha_k\}$, 两两成相等的锐角 $\theta = \arccos \sigma$.

引理 2: E_n 中至多有 $n+1$ 个两两成钝角的向量.

定理 2: 1) E_n 中存在 $n+1$ 个单位向量 $\{\alpha_1, \alpha_2, \dots, \alpha_{n+1}\}$, 它们两两成相等的钝角 $\theta_n = \arccos(-\frac{1}{n})$;

2) 如果 E_n 中单位向量组 $\{\beta_1, \beta_2, \dots, \beta_{n+1}\}$ 两两成相等的钝角 θ'_n , 则 $\theta'_n = \theta_n$.

2. 引理与定理的证明

引理 1 的证明: 设 $\sum_{i=1}^k \lambda_i \alpha_i = 0, \lambda_i \in \mathbb{R}$. 由于

$$\left(\sum_{i=1}^k \lambda_i \alpha_i, \alpha_j \right) = \sigma \lambda_1 + \dots + \sigma \lambda_{j-1} + \lambda_j + \sigma \lambda_{j+1} + \dots + \sigma \lambda_k = 0,$$

得

$$\begin{pmatrix} 1 & \sigma & & \cdots & \sigma \\ \sigma & 1 & & \cdots & \sigma \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ \sigma & \sigma & \cdots & 1 \end{pmatrix}_{k \times k} \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_k \end{pmatrix} = 0.$$

记

$$\Sigma_k(\sigma) = \begin{pmatrix} 1 & \sigma & \cdots & \sigma \\ \sigma & 1 & \cdots & \sigma \\ \vdots & \vdots & \ddots & \vdots \\ \sigma & \sigma & \cdots & 1 \end{pmatrix}$$

有 $\det(\Sigma_k(\sigma)) = (1 - \sigma)^{k-1}[1 + (k-1)\sigma] > 0$. 因此 $\lambda_1 = \cdots = \lambda_k = 0$, 即 $\{\alpha_1, \alpha_2, \dots, \alpha_k\}$ 线性无关.

定理 1 的证明: 由于 $\Sigma_k(\sigma)$ 是正定对称阵, 故存在 k 阶实方阵 $P_k(\sigma)$, 使 $\Sigma_k(\sigma) = P_k(\sigma)P_k'(\sigma)$. 取 E_n 的一组 ON 基 $\{\varepsilon_1, \dots, \varepsilon_k, \dots, \varepsilon_n\}$, 令

$$\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_k \end{pmatrix} = P_k(\sigma) \begin{pmatrix} \varepsilon_1 \\ \varepsilon_2 \\ \vdots \\ \varepsilon_k \end{pmatrix}$$

即可. 同时由 $\dim V(\alpha_1, \dots, \alpha_k) \leq n$, 及 $\{\alpha_1, \dots, \alpha_k\}$ 线性无关, 得 $k \leq n$.

引理 2 的证明: 对欧氏空间的维数 n 进行归纳.

当 $n = 2$ 时, 命题显然成立.

假设维数为 $n-1$ ($n \geq 3$) 时命题成立, 对 n 维欧氏空间 V 用反证法. 设 V 中有单位向量组 $\{\alpha_1, \dots, \alpha_{n+1}, \alpha_{n+2}\}$, $(\alpha_i, \alpha_j) < 0$, $1 \leq i \neq j \leq n+2$. 记 α_{n+2} 生成的空间为 U , $\alpha_t = \xi_t + \lambda_t \alpha_{n+2}$, $\xi_t \in U^\perp$, $\lambda_t \in \mathbb{R}$, $1 \leq t \leq n+1$. 于是

$$0 > (\alpha_t, \alpha_{n+2}) = (\xi_t + \lambda_t \alpha_{n+2}, \alpha_{n+2}) = \lambda_t,$$

$0 > (\alpha_t, \alpha_s) = (\xi_t + \lambda_t \alpha_{n+2}, \xi_s + \lambda_s \alpha_{n+2}) = (\xi_t, \xi_s) + \lambda_t \lambda_s$, $1 \leq t \neq s \leq n+1$, 则得 $(\xi_t, \xi_s) < -\lambda_t \lambda_s < 0$. 这样在 $n-1$ 维空间 U^\perp 中存在 $n+1$ 个向量 $\xi_1, \xi_2, \dots, \xi_{n+1}$ 两两成钝角, 与归纳假设矛盾.

定理 2 的证明: 1) 取 E^n 中的 ON 基 $\{\varepsilon_1, \dots, \varepsilon_n\}$, 令

$$\alpha_i = [\varepsilon_i - \frac{1}{n}(1 + \sqrt{\frac{1}{n+1}})(\varepsilon_1 + \cdots + \varepsilon_n)] \cdot \sqrt{\frac{n+1}{n}}, \quad (i = 1, \dots, n),$$

$$\alpha_{n+1} = \frac{1}{\sqrt{n}}(\varepsilon_1 + \cdots + \varepsilon_n),$$

不难验证 $(\alpha_i, \alpha_j) = -\frac{1}{n}$, $1 \leq i \neq j \leq n$, $(\alpha_i, \alpha_i) = 1$.

2) 设 E^n 中单位向量组 $\{\beta_1, \dots, \beta_{n+1}\}$ 两两成等钝角 θ'_n , $\cos \theta'_n = \lambda$. 取该空间的一组 ON 基 $\{\varepsilon_1, \dots, \varepsilon_n\}$, 设 $(\beta_1, \dots, \beta_{n+1}) = (\varepsilon_1, \dots, \varepsilon_n)P$, $P \in \mathbb{R}^{n \times (n+1)}$,

则

$$P'P = \begin{pmatrix} 1 & \lambda & \cdots & \lambda \\ \lambda & 1 & \cdots & \lambda \\ \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \cdots & 1 \end{pmatrix}_{(n+1) \times (n+1)}$$

因 $\text{rank } P'P = \text{rank } P < n+1$, 于是 $\det P'P = (1-\lambda)^n(1+n\lambda) = 0$, 由 $-1 < \lambda < 0$, 得 $\lambda = -\frac{1}{n}$, 即证得 $\theta'_n = \theta_n$.

3. 一个未解决的问题

E_n 中向量组 $\{\alpha_1, \alpha_2, \dots, \alpha_k\}$ 两两所成角都在区间 $[\alpha, \beta]$ 中, $0 < \alpha < \beta < \pi$, 求 k 的上确界.

最后, 向对本文给予帮助的周勇和马翔同学致谢.

117. (南开大学 陈天华提供)

已知 $\alpha_1 + \alpha_2 + \cdots + \alpha_n = 0$, 求证:

$$D = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \operatorname{tg}\alpha_1 & \operatorname{tg}\alpha_2 & \cdots & \operatorname{tg}\alpha_n \\ \operatorname{tg}^2\alpha_1 & \operatorname{tg}^2\alpha_2 & \cdots & \operatorname{tg}^2\alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \operatorname{tg}^{n-2}\alpha_1 & \operatorname{tg}^{n-2}\alpha_2 & \cdots & \operatorname{tg}^{n-2}\alpha_n \\ f(\alpha_1) & f(\alpha_2) & \cdots & f(\alpha_n) \end{vmatrix} = 0.$$

其中 $f(\alpha) = \begin{cases} \sin 2\alpha, & n \text{ 为奇数.} \\ \cos 2\alpha, & n \text{ 为偶数.} \end{cases}$

* * 问题征解 * *

118.* (9301 徐涛提供) 一辆吉普车欲穿越 100 公里的沙漠, 其总载油量为 50 升, 耗油量为 1 升/公里. 由于沿途无加油站, 必须利用吉普车自己运油至途中贮存起来备用. 问吉普车怎样才能以尽量少的油耗穿越沙漠?

119.* (陈计提供) 平面点集 M , 各点间的距离有 m 种值, 令 p_m 为点集 M 中点数的最大值. 证明或否定

$$m\sqrt{\ln m} < p_m \leqslant 3m^{\frac{5}{4}}.$$

* 研究与讨论 *

Z_n^* 群的结构探索

吴 畏

Z_n 作为 n 阶加法循环群, 已为我们熟知和常用. 同时, 通过定义 $\bar{ab} = \overline{ab}$, Z_n 对此乘法形成含么交换半群, Z_n^* 便是由 Z_n 中的全体乘法可逆元所形成的 Abel 群. 在探寻这种群的结构时, 我们发现需要用到一些初等数论中的知识, 特别是 Euler 函数 φ . 为此, 首先引入如下的

引理 1: 若 p 为素数, $n > 0$, 则 $\varphi(p^n) = p^{n-1}(p-1)$.

引理 2: 若 $(m, n) = 1$, 则 $\varphi(mn) = \varphi(m)\varphi(n)$.

证: 考查 mn 阶循环群 Z_{mn} , 因 $(m, n) = 1$, 故 $Z_{mn} \cong Z_m \oplus Z_n$. 设 $a, b \in Z_{mn}$ 分别为 m 阶元和 n 阶元, 则 $Z_{mn} = \{a^i b^j | 1 \leq i \leq m, 1 \leq j \leq n\}$. 又 $a^i b^j$ 为 mn 阶元 $\iff a^i$ 为 m 阶元且 b^j 为 n 阶元 $\iff (i, m) = 1$ 且 $(j, n) = 1$. 满足等价关系左边的有序对 (i, j) 有 $\varphi(mn)$ 对, 满足等价关系右边的有序对 (i, j) 有 $\varphi(m)\varphi(n)$ 对, 从而 $\varphi(mn) = \varphi(m)\varphi(n)$.

引理 3: 若 $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ (素数 p_i 两两不同, $\alpha_i > 0$), 则 $\varphi(n) = n(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_r})$.

另外, 对 $\bar{i}, \bar{j} \in Z_n^*$, $\bar{i} = \bar{j} \iff i \equiv j \pmod{n}$, 这一等价关系是以后进行语言转换的基础.

有了以上的准备工作, 现在可以进行对 Z_n^* 的探究了.

命题 1: Z_n^* 为 $\varphi(n)$ 阶群.

证: $\bar{i} \in Z_n^* \iff \exists \bar{j} \in Z_n^*, \text{使 } \bar{ij} = \bar{1} \iff ij \equiv 1 \pmod{n} \iff (i, n) = 1$. 从而 $|Z_n^*| = \varphi(n)$.

定理 1: (a) Z_2^*, Z_4^* 分别为 1 阶群和 2 阶群.

(b) 若 $n \geq 3$, 则 $Z_{2^n}^* \cong Z_2 \oplus Z_{2^{n-2}}$.

证: (b) $Z_8^* = \langle \bar{1}, \bar{3}, \bar{5}, \bar{7} \rangle$. 易知 Z_8^* 中无 4 阶元, 从而 $Z_8^* \cong Z_2 \oplus Z_2$.

下面为使叙述严谨, 将采用原根的语言.

易知, 没有模 16 的原根. 但存在 a , 使 $a^4 \equiv 1 \pmod{16}$. 但 $a^2 = 1 + 8k, 2 \nmid k$ (如 $a = 3$). 假设当 $n = 1$ 时, a 满足 $a^{2^{n-1}} = 1 + 2^{n+1}k_1, 2 \nmid k_1$, 则 $a^{2^n} = (a^{2^{n-1}})^2 = (1 + 2^{n+1}k_1)^2 = 1 + 2^{n+2}k_2, 2 \nmid k_2$, 从而在 $Z_{2^n}^*(n \geq 4)$ 中, 存在 \bar{a} , 其阶为 2^{n-2} . 又假设没有模 $2^{n-1}(n \geq 4)$ 的原根, 则对每个奇数 b ,

$$\begin{aligned} b^{2^{n-3}} &\equiv 1 \pmod{2^{n-1}}, \\ \Rightarrow 2^{n-1} &|(b^{2^{n-3}} - 1), \\ \Rightarrow 2^n &|(b^{2^{n-3}} - 1)(b^{2^{n-3}} + 1) = b^{2^{n-2}} - 1, \\ \Rightarrow b^{2^{n-2}} &\equiv 1 \pmod{2^n}. \end{aligned}$$

从而没有模 2^n 的原根. 上述论证说明在 2^{n-1} 阶群 $Z_{2^n}^*$ 中, 存在阶为 2^{n-2} 的元素, 但 Abel 群 $Z_{2^n}^*$ 不是循环群, 由有限生成 Abel 群的结构即知 $Z_{2^n}^* \cong Z_2 \oplus Z_{2^{n-2}}(n \geq 3)$.

命题 2: 对于每个素数 p , Z_p^* 为 $p-1$ 阶循环群.

证: $Z_p^* = Z_p - \{0\}$. 而我们熟知 Z_p 是 p 元有限域. 由有限域中的已知结果, 即知 Z_p^* 为 $p-1$ 阶循环群.

定理 2: 若 p 为奇素数而 $n > 0$, 则 $Z_{p^n}^*$ 为 $p^{n-1}(p-1)$ 阶循环群.

证: 由上, 取 a 为模 p 的一个原根. 则

$$(a+p)^{p-1} - a^{p-1} \equiv a^{p-1} + p(p-1)a^{p-2} - a^{p-1} \equiv p(p-1)a^{p-2} \not\equiv 0 \pmod{p^2}.$$

从而存在模 p 的一个原根 g , 使得 $g^{p-1} \not\equiv 1 \pmod{p^2}$. 与定理 1 类似, 我们可以证得 $g^{\varphi(p^r)} = 1 + p^r k, p \nmid k$. 设 g 模 p^r 的阶为 d , 则 $g^d \equiv 1 \pmod{p^r}, g^d \equiv 1 \pmod{p}$. 由 g 为模 p 的原根, $(p-1)|d$. 从而存在 $r_1 \leq r$, 使 $d = \varphi(p^{r_1})$. 但 $g^{\varphi(p^{r_1})} = 1 + p^{r_1} k_1, p \nmid k_1$, 于是只能有 $r_1 = r$. g 即为模 p^r 的原根, $Z_{p^r}^*$ 为 $\varphi(p^r)$ 阶循环群.

有了定理 1 和定理 2, 为了弄清楚 Z_n^* 的结构, 我们自然会想到下面的

定理 3: 若 $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ (素数 p_i 两两不同, $\alpha_i > 0$), 则

$$Z_n^* \cong Z_{p_1^{\alpha_1}}^* \oplus Z_{p_2^{\alpha_2}}^* \oplus \cdots \oplus Z_{p_r^{\alpha_r}}^*.$$

这一结论自然优美, 但并不显然, 以致笔者在未获证之前, 曾几度怀疑其正确性, 并力图举出反例, 结果反倒证明了几种定理 3 的特殊情形, 限于篇幅, 在本文中我们只能将其删掉了.

证: 记 Z_m^* 中元素为 $\bar{a}^{(m)}, a \in \mathbb{N}$. 定义映射

$$\varphi : Z_n^* \rightarrow Z_{p_1^{\alpha_1}}^* \oplus \cdots \oplus Z_{p_r^{\alpha_r}}^*, \bar{a}^{(m)} \mapsto (\bar{a}^{(p_1^{\alpha_1})}, \dots, \bar{a}^{(p_r^{\alpha_r})}),$$

由 $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, 映射 φ 可定义. 易验证 φ 是同态映射.

对每个 $(\bar{a}_1^{(p_1^{\alpha_1})}, \dots, \bar{a}_r^{(p_r^{\alpha_r})}) \in Z_{p_1^{\alpha_1}}^* \oplus \cdots \oplus Z_{p_r^{\alpha_r}}^*$, 由中国剩余定理, 存在 $a \in \mathbb{N}$, 使

$$(\bar{a}_1^{(p_1^{\alpha_1})}, \dots, \bar{a}_r^{(p_r^{\alpha_r})}) = (\bar{a}^{(p_1^{\alpha_1})}, \dots, \bar{a}^{(p_r^{\alpha_r})}),$$

从而 φ 是满同态. 若存在 $b \in \mathbb{N}$, 使

$$(\bar{b}^{(p_1^{\alpha_1})}, \dots, \bar{b}^{(p_r^{\alpha_r})}) = (\bar{1}^{(p_1^{\alpha_1})}, \dots, \bar{1}^{(p_r^{\alpha_r})}),$$

则 $b \equiv 1 \pmod{p_i^{\alpha_i}}, i = 1, \dots, r$. 所以 $b \equiv 1 \pmod{n}$, 即 $\bar{b}^{(n)} = \bar{1}^{(n)}$. 从而 φ 是单同态, $\varphi : Z_n^* \rightarrow Z_{p_1^{\alpha_1}}^* \oplus \cdots \oplus Z_{p_r^{\alpha_r}}^*$ 是同构.

综合三个定理, 我们终于得到

Z_n^* 结构定理: 若 $n = 2^{\alpha_0} p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ (奇素数 p_i 两两不同, $\alpha_i > 0$), 则

(a) $\alpha_0 = 0, 1$ 时, $Z_n^* \cong Z_{p_1^{\alpha_1-1}(p_1-1)}^* \oplus \cdots \oplus Z_{p_r^{\alpha_r-1}(p_r-1)}^*$.

(b) $\alpha_0 = 2$ 时, $Z_n^* \cong Z_2 \oplus Z_{p_1^{\alpha_1-1}(p_1-1)}^* \oplus \cdots \oplus Z_{p_r^{\alpha_r-1}(p_r-1)}^*$.

(c) $\alpha_0 \geq 3$ 时, $Z_n^* \cong Z_2 \oplus Z_{2^{\alpha_0-2}} \oplus Z_{p_1^{\alpha_1-1}(p_1-1)}^* \oplus \cdots \oplus Z_{p_r^{\alpha_r-1}(p_r-1)}^*$.

值得一提的是, 如果直接引用初等数论中关于原根存在性的主要结论, 定理 1 和定理 2 的证明将大大简化, 但考虑到数论中对该结论的证明比较繁琐, 而文中利用抽象代数中的一些基本结论, 算是给出了比较简单的直接证明, 因此未嫌重复而一并写出, 敬请指正.

面面俱到的代表性

数学小品

马 翔

n 门学科的科学家参加大会, 他们来自于 n 个国家, 并且各国的人数相等, 各学科的人数也相等. 现在想从中选出 n 个代表作大会发言, 要求他们同时分属于不同的国家和学科. 请问能否保证做到这一点?

这个问题另一种等价表述是: 在 n^2 的棋盘上, 每一格中放有若干棋子(子数可以为 0, 即空格). 各行各列子数之和相等(不为 0). 问是否必能找到 n 个棋子分处不同的行和列?

下面我将给出肯定的回答——这粗看上去是很不显然的. 不但如此, 我还将证明更进一步的结论. 而有了这个结论的认识, 我们又会觉得原来的问题太显然了.

定义: 一个代表元组为一组 n 个分处不同行列的棋子. 第 i 行第 j 列的格子记为 (i, j) , 其中的棋子数记为 a_{ij} .

定理: 若 $n \times n$ 的棋盘上各行各列子数之和均相等, 则它可以完全分解为一些代表元组的叠加.

证明: $n = 2$ 时, 例如图 1 所示棋盘中放有 6 个棋子, 满足定理条件, 并且正可以分解为 3 个代表元组 $\{a, c\}, \{b, d\}, \{e, f\}$. 更一般的, 2×2 的棋盘必可分解为 m 个落于 $(1, 1)$ 和 $(2, 2)$ 的代表元组及 n 个落于 $(1, 2)$ 和 $(2, 1)$ 的代表元组.

a, b	e
f	c, d

图 1

下面用数学归纳法. 假设定理在 $n = k$ 时成立, $n = k + 1$ 时, 我们要证明如下命题: 对于棋盘上任意一颗棋子, 都存在至少一个代表元组包含它.

不妨设此棋子在 $(1, 1)$, 即有 $a_{11} > 0$. 又设各行各列子数之和为 m . 除 $(1, 1)$ 外, 考虑第一行和第一列当中棋子数最少但又非空的一格, 不妨设为 $(1, j)$, 于是 $a_{1j} > 0$, 从而可知第一列中除 $(1, 1)$ 外还有非空的一格(否则第一行与第一列子数和不等). 设此格为 $(i, 1)$, 则 $a_{i1} \geq a_{1j}$. 作如下变换: 从 $(i, 1)$ 格中取出 a_{1j} 个棋子放到 $(1, 1)$, 从 $(1, j)$ 中取出 a_{1j} 个棋子放到 (i, j) . 这样 $(1, j)$ 就成了空格, 而各行各列的子数和仍为 m . 反复利用这样的变换, 恰好可以把第一行第一列除 $(1, 1)$ 外所有的格子变为空格, 而 $a'_{11} = m$; 右下角的

k^2 的棋盘中 $a'_{ij} \geq 0$, 且各行各列之和为 m . 由归纳假设, 这个 k^2 的小棋盘可完全分解为 m 个 k 元代表组, 再各加上 $(1, 1)$ 中的一粒棋子, 就成为整个 $(k+1)^2$ 棋盘上的 m 个 $k+1$ 元代表组. 我们进一步注意到, 在变换后的 k^2 的小棋盘上增加了 $m - a_{11}$ 个棋子, 它们至多只能对应于 $m - a_{11}$ 个 $k+1$ 元代表组, 这说明还有 a_{11} 个代表元组是在原来的棋盘上就存在的, 并且均有棋子落于 $(1, 1)$ 格中, 这证明了前述命题.

由此, 对于一个 $(k+1)^2$ 棋盘, 只要其上还有棋子, 就可以从中取出一个代表元组, 且每次取完后仍保持了各行各列数之和相等, 不断进行下去直至取完为止, 也就完成了代表元组的分解, 且它们显然不交. 所以对于 $n = k+1$ 的情形, 定理也成立.

a_{11}	\cdots	a_{1j}	\cdots
\vdots	\ddots	\vdots	
a_{i1}	\cdots	a_{ij}	
\vdots			\ddots

 \rightarrow

$a_{11} + a_{1j}$	\cdots	0	\cdots
\vdots	\ddots	\vdots	
$a_{i1} - a_{1j}$	\cdots	$a_{ij} + a_{1j}$	
\vdots			\ddots

 \rightarrow

a'_{11}	0	\cdots	\cdots
0			
\vdots	k^2 小棋盘		
\vdots			

图 2

综上所述, 对于一切 $n \in \mathbb{N}$, 定理均成立.

附记:

- 提出这个问题, 是受到《近世代数引论》书中一习题的启发: “设 A 是群 G 的具有有限指数的子群. 试证: 存在 G 的一组元素 g_1, g_2, \dots , 它们既可以作为 A 在 G 中的右陪集代表元系, 又可以作为 A 在 G 中的左陪集代表元系.”
- 棋盘其实也可以看作方阵 $(a_{ij})_{n \times n}$. 那么能否利用方阵的积和式 Per 来做此题?
- 定理在三维的推广不成立, 具体点说, 如右图, 各“层”上的棋子数之和为 2, 但不存在一组两个不共“层”的代表元. 为何出现这种差异, 我也无法解释.

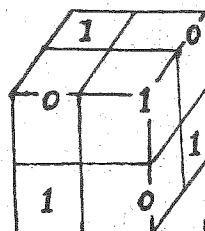


图 3

小议 n 点集中特定距离的个数

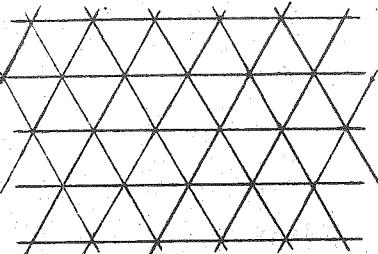
* 数学小品
*

黄华君

陈计提出过征解题：平面 n 个点，两两间距离有 m 种，问对给定的 m 值， n 的最大值 p_m 大致范围是多少？他猜测有 $m\sqrt{\ln m} < p_m < 3m^{\frac{5}{4}}$ 。现在，让我们从另一角度来考察：对给定的 n ，在 n 点集中，距离为 l 的点对至多有多少？

显然 n 越大时点对个数亦相应增大，所以我们不妨考察每一点“平均”应拥有多少这样的距离。简言之， A 为平面 n 阶简单图，任两点有线段连结当且仅当它们距离为 1。对 A 中任一点 a ， a 的度（即与 a 连结的线段个数）记为 $\tau(a)$ ，称 $\overline{\tau(A)} = \frac{1}{n} \sum_{a \in A} \tau(a)$ 为 A 的平均度。问对所有这样的 n 阶简单图 A ， $\overline{\tau(A)}$ 的最大值 $S(n)$ 是多少？

直观地看，似乎对 $\forall n \in N$ ，有 $S(n) \leq 6$ 。因为，我们通过观察右图那样的全平面上的正三角形网络，知每点的度都恰为 6。而且这个图似乎是离散点集中排列最“紧凑”，空间利用得“最好”的了。



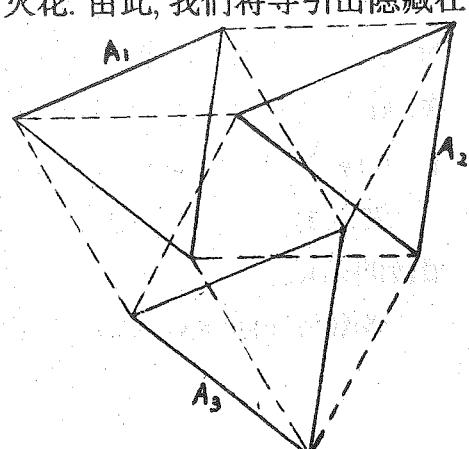
但是这一回，直觉却引导我们走进了误区。事实上，只要 n 充分大，则 $S(n)$ 可以大于任意指定的数。确切地说，我们将证明： $S(n)$ 的阶不比 $\ln n$ 低。

首先，我们构作一个平均度为 7 的图——把上述平面网络向某方向平移一个单位，并注意使平移前和平移后的点不重合。则这两个网络所组成的图每个点至少有 7 个度。

平移可增加平均度！这是个极为宝贵的火花。由此，我们将导引出隐藏在其背后的一系列奇妙结论。

考察右图，单位正三角形 A_1 ，向某方向平移一个单位得到 A_2 ，再向与第一次平移方向成 60° 的另一方向平移一个单位得到 A_3 ，则 A_1, A_2, A_3 9 点所组成系统中每点分属两个正三角形，每点均有 4 个度。

进一步思考，会得到这么个结果：



定理 $\overline{\tau(A \times B)} \geq \overline{\tau(A)} + \overline{\tau(B)}$.

这里的 $A \times B$, 是指一类新的图, 对其中任一个图来说, 它相当于一个图 “ B ”, 只不过这个图 “ B ” 中的“点”是图 A , 而“线段”则是图 A 平移 1 个单位的轨迹.

证明是显然的, 因为对 $A \times B$ 中任一点 a 来说, 它同时在一个图 A 中和一个图 B 中, 所以 $\tau_{A \times B}(a) \geq \tau_A(a) + \tau_B(a)$.

由此立即可得出结论: $S(mn) \geq S(m) + S(n)$, $S(n^t) \geq tS(n)$.

上式意味着什么呢? 注意到 $\frac{S(mn)}{\ln mn} \geq \frac{S(m) + S(n)}{\ln m + \ln n}$, 而 $\frac{S(m) + S(n)}{\ln m + \ln n}$ 介于 $\frac{S(m)}{\ln m}$ 和 $\frac{S(n)}{\ln n}$ 之间. 因此, 可认为函数 $G(n) = \frac{S(n)}{\ln n}$ 随 n 的增大不会有增加的趋势.

下面列出对一些小的 n , $\frac{S(n)}{\ln n}$ 大致可能值.

n	2	3	4	5	6	7	8	9
$S(n)$	1	2	2.5	2.8	3	3.43	3.5	4
$G(n)$	1.433	1.821	1.803	1.740	1.674	1.762	1.683	1.821

上述数据表明 $G(n)$ 并不是严格意义上的单调增, 即使对 $G(n^t)$ 也一样. 如虽然 $G(4)$ 和 $G(8)$ 都大于 $G(2)$, 但 $G(4) > G(8)$. 因此所谓之 $G(n)$ 的增加只是一种整体的趋势.

由于对给定的 A 和 B 而言, $A \times B$ 仍有很大的自由取法, 因此 $G(n)$ 的增加趋势应不会停止. 只要精心选择平移方向, 还是有希望实现点重合或是度增加这两种效果的, 这就能使 $G(n)$ 变得更大. 但 $G(n)$ 的增加量会很少, 估计其值是有上界的, 可能只比 $G(3)$ 大一些. 若果如其然, 则 $S(n) = O(\ln n)$, 陈计所提不等式 $m\sqrt{\ln n} < p_m < 3m^{\frac{5}{4}}$ 右端就几乎显然了——设 $S(n) \leq k \ln n$, k 为 $G(n)$ 上界. 则 p_m 个点所成完全图每点连了 $p_m - 1$ 条线段, 若只有 m 种距离, 则 $mS(p_m) \geq p_m - 1$, 故 $km \ln p_m \geq p_m - 1$, 注意 $\frac{p_m - 1}{\ln p_m}$ 当 $p_m \geq 3$ 时单调增, 可得 m 充分大时 $p_m < km \ln m = o(m^{\frac{5}{4}})$.

类似地, 我们也可把这套思想搬到球面或空间上的情形去讨论, 并得出相仿的结论.

感谢马翔同学对问题所提出的意见和建议.

研究与讨论

Hall 定理与 $G[H]$ 的可迁性

张 林

组合数学中有这样一个结论(详见 [1]):

Hall 定理: 有限集 X 的子集列 (X_1, \dots, X_n) 有相异代表列 (SDR) 的充要条件为: 对任意正整数 $r \leq n$, (X_1, \dots, X_n) 中任意 r 个子集之并至少含有 r 个元素.

我们要用到的是它的这样一个直接推论:

(*) 设矩阵 $A = (a_{ij})_{m \times n}$ 是 $\begin{pmatrix} 1 & \dots & n \\ \dots & \dots & \dots \\ 1 & \dots & n \end{pmatrix}_{m \times n}$ 的一个重新排列(为方便以

后记此事为 $A \in \text{Per}(m \times n)$), 则 $\exists \tau : [n] \rightarrow [m]$ 使 $\{a_{\tau(i)i} : 1 \leq i \leq n\} = [n]$ (这里 $[k] = \{1, \dots, k\}$), 即 A 有“相异代表序列”(简记为 SDRG).

证明: 只须令 $X = [n]$, $X_i = \{a_{1i}, \dots, a_{ni}\}$, 由 Hall 定理即得证.

对(无向)简单图 G , 记 $V(G)$ 为其顶点集, $E(G)$ 为其边集. 称 $\varphi \in \text{Sym } V(G)$ 为 G 的一个自同构, 若 $\forall x, y \in V(G)$, 有 $\{x, y\} \in E(G) \Leftrightarrow \{\varphi(x), \varphi(y)\} \in E(G)$. 记 $\text{Aut } G = \{\varphi : G \text{ 的自同构}\}$. 若 $\text{Aut } G$ 在 $V(G)$ 上可迁(传递), 称 G 点可迁. 对 $\{x, y\} \in E(G)$, 称有序组 (x, y) 为 G 的一个 1-链. 易见 $\text{Aut } G$ 可看为 $E(G)$ 上和 1-链全体上的置换群. 若 $\text{Aut } G$ 在 $E(G)$ 上或 1-链全体上可迁, 分别称 G 边可迁或 1-可迁.

回忆两个图 G, H 的字典序积(或称 composition) $G[H]$ (见 [2]): $V(G[H]) = V(G) \times V(H)$, $E(G[H]) = \{(x, y), (x', y')\} | \{x, x'\} \in E(G) \text{ 或者 } x = x' \text{ 且 } \{y, y'\} \in E(H)\}$. $\text{Aut } G[H]$ 中自然地有两类元素如下:

(1) $\sigma : \sigma$ 固定所有 (x, y) , $x \neq x_0$; 而 $\sigma|_{\{(x_0, y) : y \in V(H)\}} \in \text{Aut } H$.

(2) $g^* : g^*((x, y)) = (g(x), y)$. 其中 $g \in \text{Aut } G$.

记 $A(G)$ 为 G 的邻接阵, 即 $a_{ij} = 1 \Leftrightarrow \{x_i, x_j\} \in E(G)$. 其中 $V(G) = \{x_1, \dots, x_N\}$. 易证有:

性质 1 $A(G[H])$ 与 $I_n \times A(H) + A(G) \times J_m$ 置换相似. 其中 $n = |V(G)|$, $m = |V(H)|$, \times 为 Kronecker 乘积.

性质 2 对 $\forall \tau : V(G) \rightarrow V(H)$, $G[H]|_{\{(x, \tau(x)) : x \in V(G)\}} \cong G$.

性质 3 $(G_1[G_2])[G_3] = G_1[(G_2[G_3])]$, $\overline{G[H]} = \overline{G}[\overline{H}]$, $G[H]$ 连通 $\Leftrightarrow G$ 连通.
 $G[H]$ 正则 $\Leftrightarrow G, H$ 正则.

性质 4 G, H 点可迁 $\Rightarrow G[H]$ 点可迁.

命题: $G_1[H_1] \cong G_2[H_2]$, $|V(H_1)| = |V(H_2)|$, 则 $G_1 \cong G_2$.

证: 设 $V(H_1) = \{h_1, \dots, h_m\}$, $V(H_2) = \{h'_1, \dots, h'_m\}$, $V(G_1) = \{g_1, \dots, g_n\}$, $V(G_2) = \{g'_1, \dots, g'_n\}$. 设 $\alpha: G_1[H_1] \rightarrow G_2[H_2]$ 为同构. 以 α_{ij} 记 $\alpha((g_i, h_j))$ 第一分量的下标, 则 $(\alpha_{ij})^T \in \text{Per}(m \times n)$. 由 (*), 有 SDRC, 设为 $\{\alpha_{1\tau(1)}, \dots, \alpha_{n\tau(n)}\}$, 这表明 $\{(g_1, h_{\tau(1)}), \dots, (g_n, h_{\tau(n)})\}$ 在 α 下的象形如 $\{(g'_1, h'_{\alpha(1)}), \dots, (g'_n, h'_{\alpha(n)})\}$. 从而由性质 2 便得 $G_1 \cong G_2$.

定理: $G[H]$ 可迁 $\Rightarrow G$ 点可迁.

证: $\forall g_i \in V(G)$, 设 $\alpha \in \text{Aut}G[H]$ 使 $\alpha((g_1, h_1)) = (g_i, h_1)$, 类似前面命题的证明可知有 τ 使 $\{(g_1, h_1), (g_2, h_{\tau(2)}), \dots, (g_n, h_{\tau(n)})\}$ 在 α 下形如 $\{(g_1, h_{\alpha(1)}), \dots, (g_i, h_1), \dots, (g_n, h_{\alpha(n)})\}$. 由此得证.

问题: 前两个结论中是否能分别加上 $H_1 \cong H_2$ 和 H 点可迁?

定理: $G[H]$ 边可迁 $\Rightarrow G$ 边可迁, $G[H]$ 1-可迁 $\Rightarrow G$ 1-可迁. 为此

定义: 设 $A = (a_{ij}) \in \text{Per}(m \times n)$, 对 $S \subset [m] \times [n]$, 记 $a_s = \{a_{ij} : (i, j) \in S\}$, 定义 $S' = \{(i, j) : \exists k \text{ 使 } a_{kj} \in a_s\}$, $S'' = (S')'$, $S''' = (S'')'$, \dots . 则 $S \subset S' \subset \dots \subset [m] \times [n]$. 记 $\Delta(i, j) = \{(i, j)\}' \cup \{(i, j)\}'' \cup \dots$.

引理: 设 $A \in \text{Per}(m \times n)$, 若满足 $\Delta(1, 1) \cap \Delta(1, 2) = \emptyset$, 则存在一个同时包含 (1,1), (1,2) 的 SDRC.

由 (*) 不妨设 $m = 2$, 随后的证明几乎是穷竭法, 这里略去, 该引理的条件是不能完全去掉的, 反例如

$$\begin{pmatrix} 1 & 2 & 1 & 2 & 4 & 6 \\ 5 & 4 & 3 & 6 & 5 & 3 \end{pmatrix}.$$

定理的简证: 取定一边, 不妨设 $\{g_1, g_2\} \in E(G)$, 则 $\forall \{g_i, g_j\} \in E(G)$, 因 $G(m)$ 边可迁, $\exists \alpha \in \text{Aut}G(m)$ 使 $\{(g_1, h_1), (g_2, h_1)\}^\alpha = \{(g_i, h_1), (g_j, h_1)\}$. 以 α_{kl} 记 $\alpha((g_k, h_l))$ 第一分量的下标, 则 $(\alpha_{kl})^T \in \text{Per}(m \times n)$. 若 $(p, q) \in \Delta(1, 1) \cap \Delta(1, 2)$, 按 Δ 的定义可推出 $\{(g_q, h_p), (g_q, h_p)\} \in E(G(m))$ 而矛盾, 从而由引理, $\exists \tau$ 使 $\{(g_1, h_1), (g_2, h_1), (g_3, h_{\tau(3)}), \dots, (g_n, h_{\tau(n)})\}$ 在 α 下的象形如 $\{(g_1, h_{\alpha(1)}), \dots, (g_n, h_{\alpha(n)})\}$. 而 $\alpha(i) = \alpha(j) = 1$, 由此及前面的两类自同构便得 G 的边可迁性, 后一结论的证明完全类似.

特别对 $H = N_m$ 即 m 点无边图, 简记 $G(m) = G[N_m]$, 以上证明了 $G(m)$ 点/边/1-可迁 $\Leftrightarrow G$ 点/边/1-可迁, 由此可以对一些有关可迁性的图给出新的无穷列.

另外 $G(m)$ 换为 $G[H]$ 一般不成立, 如 P_3 (即 $\circ-\circ-\circ$) 边可迁, 但 $P_3[P_3]$ 非边可迁, 对 m -可迁也不成立, 如 P_3 2-可迁, 但 $P_3(2)$ 非 2-可迁.

参考文献:

- [1] 李乔, 《组合数学基础》.
- [2] Harary, *Graph Theory*.

标准形的妙用

黄华君

* 日 知 录 *

$\dot{x} = Ax(t) + f(x, t)$ 是一类典型的常微分方程. 我们已经知道, $x(t) = Ax(t)$ 的解为 $x(t) = e^{At}x(0)$, 这里

$$A \in F^{n \times n}, \quad x(t) \in F[t]^{n \times 1}, \quad e^{At} \triangleq \sum_{n=0}^{\infty} \frac{A^n}{n!} t^n.$$

一般方法是把 A 特征向量求出, 再把 $x(0)$ 用特征向量表示, 并利用

$$e^{(A-\lambda I)t} = \sum_{n=0}^{\infty} \frac{(A-\lambda I)^n}{n!} t^n$$

求出 $x(t)$, 怪麻烦的.

但如果注意到

$$e^{SJS^{-1}t} = \sum_{n=0}^{\infty} S\left(\frac{J^n}{n!} t^n\right) S^{-1} = Se^{Jt} S^{-1},$$

用 Jordan 标准形来做, 就会容易多了.

若考虑 A 的有理标准形, 还可知若 A 的不变因子组为 $\{\varphi_1(\lambda), \dots, \varphi_m(\lambda)\}$, $D = \frac{d}{dt}$, 则 $\dot{x} = Ax$ 和一组齐次线性方程组 $\{\varphi_i(D)y_i = 0\}_{i=1}^m$ 等价.

* 研究与讨论 *

周长最大的椭圆内接n边形

马 翔

我们熟知，在内接于一圆的 n 边形当中，周长和面积的最小值不存在，下确界为 0，而以正 n 边形同时达到两者最大值。如果推广到椭圆的内接 n 边形，又会有什么结果呢？

椭圆毕竟没有圆那么对称，因而尝试着用三角或微积分的方法去做是几乎行不通的。不过我们若注意到椭圆 $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$ 可由一个仿射变换 $(x', y') = (\frac{x}{a}, \frac{y}{b})$ 化为圆 $x'^2 + y'^2 = 1$ ，而图形中对应部分的面积只差一个比例常数 ab 。这样，只需要取一个单位圆内的正 n 边形，经过逆变换就得到了椭圆中面积最大的 n 边形。（容易看出，对于椭圆上一点 P ，只有一个面积取最大值的以 P 为顶点的内接 n 边形。）

然而这个办法对周长的最大值问题就无能为力了，因为线段长度在仿射变换下变化并不规则。我们可确认这里的周长最大值是存在的（利用高等数学中定理：定义在紧致空间上的连续函数达到最值）；但假使我们希望求出这些最大周长对于不同的 n 的某种统一表达式，自然会想到 $n \rightarrow \infty$ 时，这些最大周长将趋于给定椭圆的周长；而早有悲观的结论告诉过我们：椭圆周长不可用初等函数表示，从而给这思路的可行性打上大大的问号。有鉴于此，下面我们将转而考虑如下的问题：那些取到最大周长的椭圆内接 n 边形，应该具有怎样的特性？

取椭圆 \mathcal{E} 上一点 P ，考虑以它为顶点的全体内接 n 边形的周长，易知其中也有最大值。设 n 边形 $PP_1 \dots P_{n-1}$ 的周长达到最大（如图 1），在 $\widehat{PP_1P_2}$ 上任取一点 P'_1 ，则当 P'_1 与 P_1 重合时 $|P'_1P| + |P'_1P_2|$ 达到最大。联想起光学中的费马原理：光程取极值。取到极大值的 $\overline{PP_1P_2}$ 岂不正应是一条光路吗？由 $\overline{PP_1}$ 到 $\overline{P_1P_2}$ 岂不正应相当于在椭圆上作了一次反射？这样， PP_1 与 P_1P_2 与 \mathcal{E} 在 P_1 处的切线成相等的角，我们称此为 P_1 上的反射特性。同

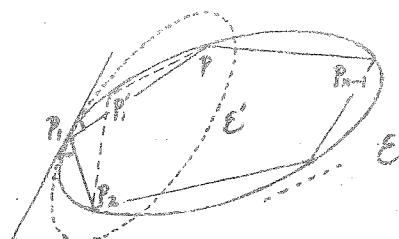


图 1

理可知 $P_2, P_3 \dots P_{n-1}$ 上均有反射特性, n 边形即可看作一条光路. 从直观上看, 光路一开始即被由 P 点出发的光线方向所决定; 当 P_1 逐渐远离 P 点时, $P_2, \dots P_{n-1}, P_n$ 均连续地沿 \mathcal{E} 上相同方向移动, 若要 P_n 与 P 正好重合, 这样的光路只有一条. 这样我们就得到了

定理 1: 给定椭圆 \mathcal{E} 和 \mathcal{E} 上一点 P , 存在唯一的以 P 为顶点的内接 n 边形(记为 $N(P)$), 其周长达到极大值(记为 $L(P)$). 确定此多边形的充要条件是它在(除 P 以外的) $n - 1$ 个顶点上均有反射特性.

不过, 我们以上的论述并不严格. 下面, 我们要指出 $N(P)$ 的另一个性质, 这需要

引理 1: YM, YN 与椭圆相切于 M, N, S, S' 是椭圆 \mathcal{E}' 的焦点, 则 $\angle SYM = \angle S'YN$. (图 2)

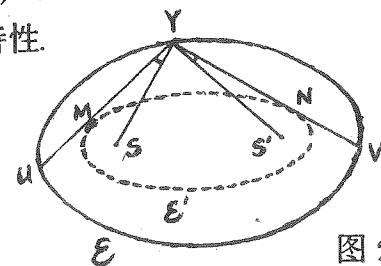


图 2

引理 2: YU, YV 是椭圆 \mathcal{E} 的两条弦, 位于 \mathcal{E} 的两焦点 S, S' 的两侧, 则路径 UYV 在 Y 上有反射特性的充要条件是 YU, YV 同与某个与 \mathcal{E} 同焦点的椭圆 \mathcal{E}' 相切. (引理证明均略)

定理 2: 椭圆 \mathcal{E} 内过 P 点的内接 n 边形达到周长最大值的充要条件是它外切于某个与 \mathcal{E} 同焦的椭圆 $\mathcal{E}(P)$.

证: 考虑内接 n 边形的各对邻边 PP_1 与 P_1P_2, P_1P_2 与 $P_2P_3 \dots P_{n-2}P_{n-1}$ 与 $P_{n-1}P$, 它们分别与某个同焦于 \mathcal{E} 的椭圆 \mathcal{E}_i 相切 ($i = 1, 2, \dots, n - 1$). 但每条边不能与多于一个同焦椭圆相切, 从而它们同切于一个公共椭圆 $\mathcal{E}(P)$.

由于 $N(P)$ 必须外切于 $\mathcal{E}(P)$, 它的唯一性也就很显然了. 此外, 由定理 2 可知 P 点上也应具有反射特性, 于是即使不固定 P , $L(P)$ 也是整个问题的极大值. 照一般的想法, 对于不同的 P , 这些极大值应是各不相等的, 那么哪一个又是最大值呢? 看是看不出来的, 不如先试算一下.

取 $n = 4$, 考虑两种情形, 如图 3 中的 $N(P)$ 和 $N(P')$, 设椭圆方程为 $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$, 则 $L(P) = 4\sqrt{a^2 + b^2}$, 由 P' 上的反射特性, 求得 P' 坐标 $(x', y') = (\frac{a^2}{\sqrt{a^2 + b^2}}, \frac{b^2}{\sqrt{a^2 + b^2}})$, 于是 $L(P') = 4\sqrt{a^2 + b^2} = L(P)$. 奇怪, 怎么会是一样的呢? 换六边形试试, P 和 P' 分别取

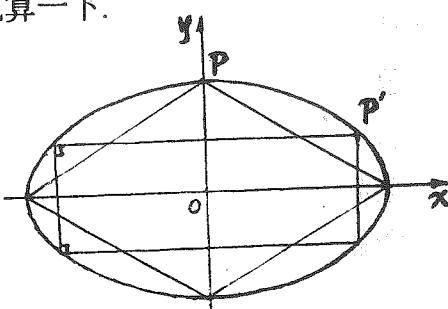


图 3

在长轴和短轴端点, 计算出来竟又是相等的周长 $4(a^2 + ab + b^2)/(a + b)$! 难道这些极值竟都会相等, 而与 P 点位置无关吗? 这太不可思议了. 这点证据似乎不

足以肯定它,那么就看看一般的取到周长极大值的内接四边形吧. 设椭圆方程为 $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$, 内接四边形相邻两顶点为 $P(a \cos \theta, b \sin \theta), Q(a \cos \varphi, b \sin \varphi)$; 由对称性, 另两点应为 $(-a \cos \theta, -b \sin \theta), (-a \cos \varphi, -b \sin \varphi)$, 周长为

$$\begin{aligned} L &= 2(\sqrt{a^2(\cos \theta - \cos \varphi)^2 + b^2(\sin \theta - \sin \varphi)^2} \\ &\quad + \sqrt{a^2(\cos \theta + \cos \varphi)^2 + b^2(\sin \theta + \sin \varphi)^2}) \\ &= 4\left(\sin \frac{\theta - \varphi}{2} \sqrt{a^2 \sin^2 \frac{\theta + \varphi}{2} + b^2 \cos^2 \frac{\theta + \varphi}{2}}\right. \\ &\quad \left.+ \cos \frac{\theta - \varphi}{2} \sqrt{a^2 \cos^2 \frac{\theta + \varphi}{2} + b^2 \sin^2 \frac{\theta + \varphi}{2}}\right) \end{aligned}$$

由 Cauchy 不等式: $x_1x_2 + y_1y_2 \leq \sqrt{(x_1^2 + y_1^2)(x_2^2 + y_2^2)}$, 于是

$$L \leq 4\sqrt{\left(\sin^2 \frac{\theta - \varphi}{2} + \cos^2 \frac{\theta - \varphi}{2}\right)(a^2 + b^2)} = 4\sqrt{a^2 + b^2}$$

这个最大值正是前面验算得到的值! 并且可以验证, 对于任意的 θ , 总可找到 φ 使得上式等号成立, 我们便证明了

命题 1: 过椭圆 $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$ 上任一点 P , 存在唯一的内接四边形, 其周长达到最大值 $4\sqrt{a^2 + b^2}$.

命题 1 的证明是难以推广到其它 n 的情形的, 我们必须另想办法. 思路二是: 在椭圆 \mathcal{E} 上取充分靠近的两点 $P, Q, N(P) = PP_1 \dots P_{n-1}$ 和 $N(Q) = QQ_1 \dots Q_{n-1}$ 分别是过 P 和过 Q 的周长达到极大的内接多边形,

设其周长分别为 $L(P), L(Q)$. 直观上图形必如图 4 所示, P_iP_{i+1} 与 Q_iQ_{i+1} 相交于 X_{i+1} . 由于 P, Q 非常接近, 且均有反射特性, 所以我们希望成立这样的命题 2: P, Q 在同一个以 X_1X_n 为焦点的椭圆上. 这样 $PX_1 + X_nP = QX_1 + X_nQ$, 以下同理有 $P_1X_1 + P_2X_2 = Q_1X_1 + Q_2X_2 \dots \dots$ 各式相加即证得 $L(P) = L(Q)$. 但命题 2 真的成立吗? 仔细想想其中有不少可疑之处, 最后我们会发现这是个假命题, 理由我就不多说了.

下面只好引用两个定理, 这样才能证明本文的中心结果定理 4.

引理 3 (Poncelet 闭包定理)

C 和 D 是圆锥曲线, 若有一 n 边形既内接于 C 又外切于 D , 则对 C 上任一点 P , 必有一 n 边形既内接于 C 又外切于 D .

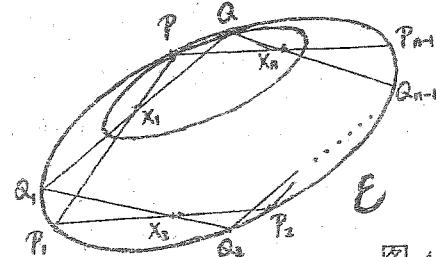


图 4

这个定理很有意思, 初看又难以下手. 不过可以尝试寻找一个射影变换, 把这两个圆锥曲线变为同心圆, 在此情形定理显然成立, 而“内接”和“外切”等性质在射影变换下不变, 从而定理对一般情形也成立.

引理 4 (Graves)

\mathcal{E} 和 \mathcal{E}' 是两个同焦椭圆, Y 是 \mathcal{E} 上任一点, YH 和 YK 分别与 \mathcal{E}' 相切于 H 和 K , 则 YH, YK 长度之和减去椭圆弧 HK 之长后为一常数.

证明参见 Salmon 的《圆锥曲线专论》, 其中用上了微积分的思想.

定理 3: 定理 2 中的 $\mathcal{E}(P)$ 和定理 1 中的 $L(P)$ 均与 P 的位置无关, 而由椭圆 \mathcal{E} 和边数 n 唯一确定.

证: i) 由引理 3, 过椭圆 \mathcal{E} 上另一点 Q , 也有 n 边形内接于 \mathcal{E} 而外切于 $\mathcal{E}(P)$; 由定理 2, 它周长达到极大. 而 $N(Q)$ 是唯一的, 从而 $\mathcal{E}(Q)$ 也唯一, $\therefore \mathcal{E}(Q)$ 即 $\mathcal{E}(P)$.

ii) 设 $P_n = P = P_0, P_{i-1}P_i$ 与 \mathcal{E}' 切于 X_i , 则

$$\begin{aligned} L(P) &= PP_1 + P_1P_2 + \cdots + P_{n-1}P \\ &= (PX_n + PX_1) + (P_1X_1 + P_1X_2) + \cdots + (P_{n-1}X_{n-1} + P_{n-1}X_n) \\ &= (\widehat{X_nX_1} + K) + (\widehat{X_1X_2} + K) + \cdots + (\widehat{X_{n-1}X_n} + K) \\ &= L(\mathcal{E}') + nK \end{aligned}$$

这里 K 是引理 4 中的常数, 最后结果显然与 P 无关, 证毕.

定理 3 无疑是非常漂亮的结果, 但细心的同学不禁要问, 作为不那么对称的椭圆, 却具有这样“对称”的结果, 这是必然还是偶然的呢? 在它背后隐藏着什么样的本质? 最终我们发现此性质在本质上与椭圆无关. 设想在 $N(P)$ 的各顶点附近对椭圆弧用切线来代替, 会有什么结果呢? 可以想到, 也许定理本身成立与否只和各顶点处的局部性质有关, 而无关乎椭圆的整体性质. 索性换一个矩形试试(图 5), 我们马上看出, 一束光线由其中 P 点出发, 最后又回到 P 点, 其光路存在, 唯一, 且其长也为定值. (与椭圆情形的差别只在于不同的光路在各段上还是平行的)

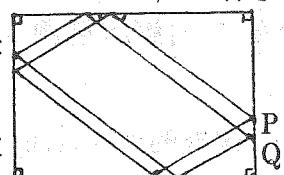


图 5

把矩形推广为圆内接四边形, 此性质仍然成立. 若是任给的不规则四边形呢? 这时没有类似定理. 不是定理不成立, 而是定理的条件本身得不到满足, 过其上一点一般不存在这样一个在

各顶点上都有反射特性的内接四边形。(注意: 最大值还是有的, 但它不是局部极大值, 在其上周长变化的“导数”不为 0.)

这一讨论给我们以启发, 在本问题当中, “椭圆”这一条件不过是保证了光路的某些特殊运动模式的存在, 除此之外椭圆的整体性质就可能并没什么作用。光程的相等, 不过是被这些模式本身的某种特性决定的, 从而是一种更为普遍的规律的表现。

但光是认识到这点还不够。例如考虑椭圆 ε 的内接“二边形”——实质上就是一束光线在两点间不断反射的模式。显然问题只有沿长轴或沿短轴来回一次这两解, 它们的“周长”并不相等, 这是怎么回事呢?

这时, 证明定理 4 前失败的思路二却启发了我们。那一思路的核心在于发现那些周长极大的 n 边形——那些光路之间是可以连续变动的, 这种连续性恰恰是定理成立的关键! 由此我们可以想象到真正的定理大致如下: 某问题的解为满足一定条件的一系列光路, 假若它们之间可以连续变化, 则它们的光程相等。有理由相信它的正确性, 设想每条路径均由有限维空间中的一“点”来代表, 沿此路径的光程有定义在此点的函数值, 则光路不过是空间中的一些极值点, 假若这些点在某种意义下连续, 由于极值点上“导数”(事实上是“变分”)为 0, 所以在这些极值点构成的集合上函数为常数, 这才是问题的本质!

不知大家还注意到与原问题对偶的问题没有? 也就是对椭圆 ε 求其周长最小的外切 n 边形。表面上看来它比“内接”情形更棘手, 不过确实它也有与前述定理完全对偶的结论, 即

定理 4: 给定椭圆 ε , 切于其上一点 Q 的外切 n 边形中, 有唯一的一个达到周长的极小值 $L(Q)$ 。确定此外切 n 边形的充要条件是它的各顶点在某个与 ε 同焦的椭圆 $\varepsilon(Q)$ 上。再者, $L(Q)$ 和 $\varepsilon(Q)$ 事实上均与 Q 点的选取无关。

这里的“对偶性”如何解释呢?

原题的大部分我都已在大一时解决, 但一直觉得并没理解透而没发表。不料去年暑假买了本《数学证明》, 第十章竟然就是作者本人(香港中文大学, 萧文强)和同事对同一问题的讨论。这才知道, 此问题最早大概是由 19 世纪瑞士著名几何学家 Steiner 解决的, 此后又多次被人重新提出并解答, 我乘坐的已经不知是历史上的第几班车了。不过, 旧话重提未始就没有新意啊。

关于魔方

研究与讨论

黄华君

一 问题的数学化

上期中, 马翔同学提出了有关魔方的等价类, 标准形和全系不变量等一系列问题, 本文意在对此给出个说法.

先介绍魔方的一些知识.

拆开一个魔方, 会发现它由 6 个面块和中心块联结在一起构成框架, 另有可拆卸的 12 个边块和 8 个角块. 面块, 边块, 角块分别粘有 1, 2, 3 片颜色片. 转动的实质是变动边块与角块.

转魔方时其实只有 6 个基本操作, 即把某面顺时针转 $\frac{\pi}{2}$. 若设 6 个面块颜色为 1, 2, …, 6, 则这 6 个基本操作可相应记为 r_1, r_2, \dots, r_6 . 所有与每面一种颜色的魔方 I 等价的魔方成一置换群 G . $G = \langle r_1, r_2, \dots, r_6 \rangle$.

再定义边块的“翻身”与角块的“自转”. 把一个边块“翻身”是指(通过转魔方)使这边块两个片对调位置, 至于角块的“自转”则是指使角块三个片轮换一下位置.

现在, 可以提出问题了.

[Question:] 把魔方拆下再装上, 共能得多少等价类? 各自标准形是什么? 有什么全系不变量?

二 问题的证明

容易验证, 下面几种操作可以通过基本操作实现.

- a) 3 个边块轮换位置; b) 2 个边块同时翻身; c) 一个角块顺时针自转一格, 另一角块逆时针自转一格; d) 对调两角块和两边块位置.

通过 c), d), 我们可把 8 个角块位置和其中 7 个角块的状态调好. 再用 a), b), 便可把 12 个边块中的 10 块位置和状态调好. 于是对任一魔方, 我们可转至只剩 3 块与 I 相异(如图 1), 这 3 块就决定了魔方所在的等价类. 易见它们有 24 种摆法, 但 b) 仍可作用

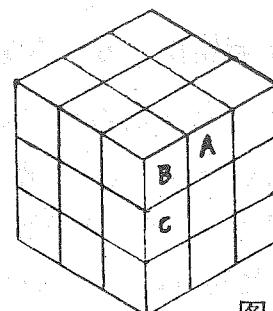


图 1

于这 3 块上, 故魔方至多有 12 个等价类.

下证恰为 12 个等价类, 只须证以下 3 个魔方与 I 不等价.

1° 把 I 中 A, C 两块对调所得魔方 J_1 .

2° 把 I 中 A 块翻身所得魔方 J_2 .

3° 把 I 中 B 块顺时针或逆时针自转一格所得魔方 J_3 .

现在我们分别来证明之.

1° 考虑基本操作 $r_1 \sim r_6$, 它们把某面顺时针转 $\frac{\pi}{2}$. 这相当于把一个面中除面块外的 8 个块位置进行置换 (如图 2). 若用对调的观点来看这个置换, 会发现它相当于偶数次块对调. 即 $1 \longleftrightarrow 3; 3 \longleftrightarrow 5; 5 \longleftrightarrow 7; 2 \longleftrightarrow 4; 4 \longleftrightarrow 6; 6 \longleftrightarrow 8$. 而 J_1 相当于把 I 的块对调一次. 显然, 无论转多少次, 作为置换来说每次转动都是块的偶置换, 不可能达到奇置换的效果. 故 1° 得证.

1	2	3
8	↗	4
7	6	5

 $\xrightarrow{r_i}$

7	8	1
6		2
5	4	3

图 2

定义块函数

$$T(K) = \begin{cases} 1, & \text{若 } K \text{ 由 } I \text{ 经偶数次块对调而得,} \\ -1, & \text{若 } K \text{ 由 } I \text{ 经奇数次块对调而得.} \end{cases}$$

则 T 为操作下的不变量.

2° 对此上期马翔已给了一个证明, 但如用片置换的观点看就会更清楚. J_2 相当于把 I 作 1 次片对调, 而转一下魔方却是片的偶置换, 故 J_2 与 I 不等价.

定义片函数

$$S(K) = \begin{cases} 1, & \text{若 } K \text{ 由 } I \text{ 经偶数次片对调而得,} \\ -1, & \text{若 } K \text{ 由 } I \text{ 经奇数次片对调而得.} \end{cases}$$

则 S 为操作下另一不变量.

3° J_3 与 I 的差别只在于角块, 因此关键要先找出记录角块在转动下变化情况的方法. 我们用颜色 1, 2, 3 涂在魔方上, 使相对面的颜色相同. 如果这情况下 J'_3 与 I' 不等价, 则 J_3 与 I 显然不等价.

此时, 每个角块的片恰含 1, 2, 3 三种颜色, 这 3 种颜色按 1-2-3 排列有 4 块为顺时针, 4 块为逆时针. 又每块 3 片恰对应 3 种方向: 上下向, 左右向, 前后向. 于是我们可用一个数字来代表角块的状态——设一角块上下向的片颜

色为 a_i , 3 种颜色排列情况为 b_i ($1 \rightarrow 2 \rightarrow 3$ 顺时针时 $b_i = -1$, 反之 $b_i = 1$), 则 $a_i b_i$ 的值就代表了这个角块的状态. (图 3 即是对 I 的角状态的描述.)

定义角函数

$$C(K) \in \{0, 1, 2\}, C(K) \triangleq \sum_{\substack{i=1 \\ K}}^8 a_i b_i \pmod{3}$$

(譬如 $C(I) = 0$.) 我们来看看转动时 C 值会如何变.

显见 r_1 不改变 C 的值. 现考虑 r_2 . 图 4 即 K 经操作 r_2 后角状态的变化情况 (这里设第 $3n+t$ 种颜

色即第 t 种颜色). 则 $C(r_2(K)) = C(K) + b_5^2 - b_1^2 + b_2^2 - b_6^2 = C(K)$. 即 r_2 不改变 C 的值, 同理 $r_3 \dots r_6$ 也不改变 C 值. 故 C 函数为操作下又一不变量. J_3 中因 B 块自转了 1 格, C 值只可能是 1 或 2, 而 $C(I) = 0$, 故 J_3 与 I 不等价, 证毕.

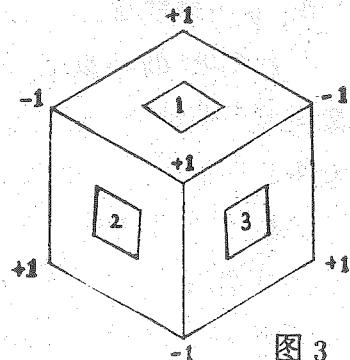


图 3

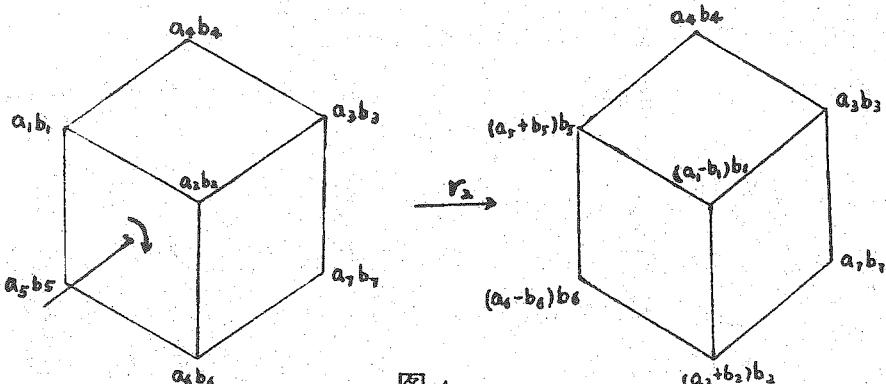


图 4

由以上三点, 我们就用 (T, S, C) 刻划出了魔方的 12 个等价类. 至于标准形, 就由 A, B, C 三块的位置与状态来决定.

三 回味篇

魔方, 也许是世界上最不可思议的玩具了. 初次接触它的人, 都会惊叹于它精巧的结构, 无常的变化. 它的每一种转动, 亦给人以种种美妙的想象. 在证明中, 我们也能找到很多和谐的美. 比如 $r_1 \sim r_6$ 的对称性, 比如点块(角块), 线块(边块), 面块, 体块(中心块) 恰好分别粘有 3, 2, 1, 0 片, 又比如它的 3 个不变量——块函数, 片函数, 角函数 … 都很对称!

证明就此告一段落, 但仍有余味待发挥.

(1) 容易算得: 魔方共有 $8! \cdot 3^8 \cdot 12! \cdot 2^{12}$ 种装法, 分属 12 个等价类. 故我们可从 I 出发, 转出约 4.3×10^{19} 种花样. 要是全世界都投身于浏览这些样式的工作, 每人每秒看一种花样, 也得没日没夜地花上 200 多年, 确为恒河之沙.

(2) 对 2^3 的小魔方, 又有怎样的结论呢? 易知角函数为它的全系不变量, 故有 3 个等价类, 与 I 等价的魔方有 $7! \cdot 3^7 / 3 = 3,674,160$ 个. (这才象人玩的玩具.)

(3) 时下有些魔方上面还标有数字和字母什么的. 若颜色转齐了中间那个字母却倒了, 未免有些扫兴. 因此我们也有必要对面块的自转进行一番讨论. 易见若 a, b 面相邻, 则 $(r_a r_b)^{105}$ 恰使 a 面与 b 面的中心块逆时针各转 $\frac{\pi}{2}$. 由这操作知可端正 5 个面块, 并使第 6 个面块任意转 π . 另一方面, 一个 r_i 相当于面块转 $\frac{\pi}{2}$, 对边块进行一次奇置换, 对角块进行一次奇置换. 记 I 为 6 个面块都端正的每面 1 种颜色的魔方, I' 为把 I 中某面块转了 $\frac{\pi}{2}$ 的魔方, 则这两个魔方必然不等价. 故若顾及面块方向, 魔方就会有 24 个等价类. 当然, 如果追求对称的话, 也是可以设法定义个面函数的.

最后, 提出几个尚待解决的问题, 有兴趣的同学不妨沿着这条路继续走下去.

(1) 作为置换群, 魔方有几个生成元? 表面看来, $r_1 \sim r_6$ 都很基本了. 但令人惊讶的是王凌峰同学指出若不论及面块的自转, 用其中 5 个就能把第 6 个表示出来, (不信可以亲自试试) 为什么会有这种结果? 还可更少吗? 注意: 生成元不一定用 r_i . (当然, 如果把面块运动群看作某种意义上的“6 维线性空间”(准确地说, 是环 Z_4 上秩为 6 的自由模), 就很容易证明: 若涉及面块的自转, 则生成元恰为 6 个.)

(2) 能否找到这样一个规则, 使得存在一多项式 $P(x)$, 对任一与 I_n 等价的 n^3 魔方, 按这规则必可在 $P(n)$ 步以内把它转全? 也就是说, 转魔方是否是 NPC 问题? 有理由相信, 存在多项式 $Q(x)$, 对任一与 I_n 等价的魔方, 它的最快转法的步数必小于 $Q(n)$. 因为 n^3 魔方有 $3(n-1)$ 个基本操作, 若把它看成有限生成自由群, 转 k 次时出现的魔方样式大致为 $[3(n-1)]^k$ 的数量级. 另一方面, n^3 魔方中一个块至多可转 24 个位置, 魔方表面不多于 $6n^2$ 块, 故与 I_n 等价的魔方不多于 $3^8 \cdot 2^{6n^2} \cdot (24!)^{\frac{6n^2}{24}} = p \cdot q^{n^2}$ 个(p, q 为常数). 因此转魔方大致所需步数为 $\frac{\log p \cdot q^{n^2}}{\log(3n-1)} = o(n^2)$. 但这并不表明必可找到一种统一的

方法, 对任意 n^3 魔方, 都能在多项式步数内转全. 更进一步的讨论就只能以待来者了.

注: NPC 是计算复杂性中一个重要的概念. 某问题的一个算法其计算量如果在 n^k 数量级, 那么计算机速度的提高足可应付 n 的增大 (这类问题称为 P -问题, P 是 *polynomial* 的简写). 但若计算量大于 n^k 级, 比如是 a^n 级, 则 n 增大时计算量即使使用高速计算机也应付不了. 所谓 NPC 是指这样一类典型的问题, 只要证明其中一个在 P 内, 就可推出一大批形形色色的问题都在 P 内. 它的重要性是不言而喻的. 想对此有所了解的同学可去看“走向数学丛书”中的《数学与电脑》一书. 另外科大王树禾老师编的《图论及其算法》中对 NPC 和图论中的 NPC 也作了详尽的论述, 颇值一读.