华章数学译丛

HZ BOOKS
华章教育

55

PEARSON

Algebra

(Second Edition)

代数

（原书第2版）

（美）Michael Artin
麻省理工学院 著

姚海楼 平艳茹 译

机械工业出版社
China Machine Press

（原书第2版）

代 数

本书由著名代数学家与代数几何学家Michael Artin所著，是作者在代数领域数十年的智慧和经验的结晶。书中既介绍了矩阵运算、群、向量空间、线性算子、对称等较为基本的内容，又介绍了环、模型、域、伽罗瓦理论等较为高深的内容。本书对于提高数学理解能力，增强对代数的兴趣是非常有益处的。此外，本书的可阅读性强，书中的习题也很有针对性，能让读者很快地掌握分析和思考的方法。

作者结合多年来的教学经历及读者的反馈，对本版进行了全面更新，更强调对称、线性群、二次数域和格等具体主题。本版的具体更新情况如下：

- 新增球体、积环和因式分解的计算方法等内容，并补充给出一些结论的证明，如交错群是单群、柯西定理、分裂定理等。
- 修订了对SU_2表示、正交关系等内容的讨论，并把线性变换和因子分解都拆分为两章来介绍。
- 新增大量习题，并用星号标注出具有挑战性的习题。

本书在麻省理工学院、普林斯顿大学、哥伦比亚大学等著名学府得到了广泛采用，是代数学的经典教材之一。

作者简介

Michael Artin 当代领袖型代数学家与代数几何学家之一，美国麻省理工学院数学系荣誉退休教授。1990年至1992年，曾担任美国数学学会主席。2002年获得美国数学学会颁发的Leroy P. Steele终身成就奖，2005年被授予哈佛大学百年奖章，2013年获得Wolf数学奖。Artin的主要贡献包括他的逼近定理、在解决沙法列维奇–泰特猜测中的工作以及为推广“概形”而创建的“代数空间”概念。

Algebra
(Second Edition)

ISBN 978-7-111-36701-7
定价：79.00元

PEARSON
www.pearson.com

投稿热线：(010) 88379604
客服热线：(010) 88378991 88361066
购书热线：(010) 68326294 88379649 68995259
封面设计：杨宇扬

华章网站：www.hzbook.com
网上购书：www.china-pub.com
数字阅读：www.hzmedia.com.cn

上架指导：数学
ISBN 978-7-111-48212-3
9 787111 482123 >
定价：79.00元

华章数学

55

Algebra

(Second Edition)

代数

（原书第2版）

（美）Michael Artin 著

麻省理工学院

姚海楼 平艳茹 译

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

代数（原书第2版）/（美）阿廷（Artin，M.）著；姚海楼，平艳茹译．—北京：机械工业出版社，2014.12
（华章数学译丛）
书名原文：Algebra，Second Edition

ISBN 978-7-111-48212-3

I. 代… II. ①阿… ②姚… ③平… III. 代数 IV. O15

中国版本图书馆CIP数据核字（2014）第233028号

本书版权登记号：图字：01-2010-6654

本书是一本代数学的经典著作，既介绍了矩阵运算、群、向量空间、线性变换、对称等较为基本的内容，又介绍了环、模、域、伽罗瓦理论等较为高深的内容，对于提高数学理解能力、增强对代数的兴趣是非常有益处的．

本书是一本有深度、有特点的著作，适合数学工作者以及基础数学、应用数学等专业的学生阅读．

出版发行：机械工业出版社（北京市西城区百万庄大街22号　邮政编码：100037）
责任编辑：迟振春　　责任校对：殷　虹
印　　刷：三河市宏图印务有限公司　　版　　次：2015年1月第1版第1次印刷
开　　本：186mm×240mm　1/16　　印　　张：29
书　　号：ISBN 978-7-111-48212-3　　定　　价：79.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzjsj@hzbook.com

译 者 序

这本书的特色很浓. 它给人的感觉是完全背离了 Serge Lang 那本经典的《代数》，也完全背离了 Jacobson 的《抽象代数学》与《基本代数》或者 Hungerford 的《代数》. 书里讲的内容很广泛，不算太难，深度中等，大学阶段就可以看，其中一些内容也可作为研究生的代数教材. 该书对于提高数学理解能力、增强对代数的兴趣是非常有益处的. 此外，本书的可阅读性强，书中的习题也很有针对性，能让读者很快地掌握分析和思考的方法. 美国伊利诺伊大学教授杰拉尔德·雅努斯评论该书为："对于有一定线性代数和微积分基础而且学习动机很强的本科生而言，这是一本极好的教材. 其内容和编写方式值得称道. 作者在前言中列出了其编写所遵循的三个原则(简言之：例证应有助于理解定义、专业要点仅在需要时才在书中较后位置呈现、主题对大多数从事数学研究及教学的人而言都应是重要的)，且特别强调这些原则中并不包括'按照所教的方法做'这一项. 整本书的编写风格是：给出基本概念、列出许多重要的例证以及简单明了地讨论一些前沿课题."

该书作者 Michael Artin 教授在 2002 年被美国数学学会授予 Steele 终身成就奖，在 2005 年被授予哈佛大学百年奖章，在 2013 年获得了 Wolf 数学奖. Michael Artin 是当代领袖型代数学家与代数几何学家之一，美国麻省理工学院数学系荣誉退休教授. 1990 年至 1992 年，曾担任美国数学学会主席. Artin 的主要贡献包括他的逼近定理、在解决沙法列维奇-泰特猜想中的工作以及为推广"概形"而创建的"代数空间"概念. 正因为这样，作者在该书里着力强调代数同其他数学分支的联系，特别是同拓扑和代数几何的联系. 作者对本版进行了全面更新，更强调对称、线性群、二次数域和格等具体主题，让读者体会到代数在其他数学分支中的威力. 同时，同第 1 版相比，习题变化很大. 从习题中，读者对书中内容以及内容的延拓会有很深的体会.

我们一接到翻译该书第 2 版任务，就深为书中内容所吸引，怀着愉悦的心情将本书翻译完，以便让更多的数学爱好者分享这部精彩著作. 译者花了八个月的时间将其译完. 翻译的过程也是学习该书的过程，并得到了许多收获. 但由于译者学识以及翻译时间的限制，译稿一定有不当之处，欢迎读者指正.

姚海楼　平艳茹
于北京工业大学
2014 年 9 月

前　言

基本概念和命题在代数中或许很重要，
原因在于它们是人们为探索公理及概括性
而投入了孜孜不倦的热情所总结出来的，
它们在代数中的重要性甚至可能会超过在任何其他学科中．
但是，我坚信，
具有极端复杂性的特殊问题才构成了数学的主干和核心，
而掌握其难点往往需要更刻苦地钻研．

——Herman Weyl

本书源于多年前我的代数课程补充讲义．我那时想比课本上更详尽地讨论一些具体的课题，比如，对称、线性群、二次数域，再将群论的重点由置换群转到矩阵群．格，另一个常见的主题，就自然出现了．

我希望具体的东西能激发学生的兴趣并使抽象的东西更容易理解．简言之，同时学习具体和抽象两个方面，学生能考虑得更深远．这项工作进展得很顺利．我花了很长时间来确定什么内容要加进去，我逐渐写出了更多的讲义，最终上课就仅用讲义而不用教材了．虽然这样形成了一本与众不同的书，但当我把材料汇总起来时却遇到了很多难题．我不建议以这种方式写书．

与多数代数书不同，本书更突出特殊的主题．每次重写一些章节的时候内容就会扩充，因为多年来我注意到，与抽象的概念相比，学生更喜欢具体的数学题材．结果，上面提到的这些东西就成了本书的主体．

在写本书时，我尽量遵守下面的原则：

1. 基本的例子放在抽象的定义之前．

2. 技巧只要在本书的其他地方出现，它就应该被介绍．

3. 对一般的数学工作者而言，所有讨论的主题都应该是重要的．

虽然这些原则听起来有点像爱国主义的教义，但我发现把它们明确地讲出来是有益的．当然，我有时也会违背这些原则．

书中的章节按照我讲课的顺序编排，线性代数、群论和几何构成第一学期的内容．环的第一次引入是在第十一章，虽然在逻辑上这一章和前面的章节没有关系．我采用这样的编排是因为想从一开始就强调代数与几何的联系，而且因为前面几章的内容对其他领域的人来说也是最重要的．本书的前半部分没有侧重计算，但在后面的章节里弥补了这一不足．

关于第 2 版的说明

本书第 2 版做了广泛的修订，融入了我 20 年的教学经验和许多人的建议. 我已将修订部分在课堂上发给学生，初稿在过去的两年里一直用做讲义. 这样，我从学生那里得到了许多宝贵的建议. 本书的整体组织结构没变，但有两章太长把它们拆分了.

书中还添加了一些新的内容. 这些内容都不多，通过在别处做些改动就平衡了. 这些新内容包括：若尔当形的提早介绍(第四章)，一小节关于连续性的问题(第五章)，交错群是单群的证明(第七章)，球体的简短讨论(第九章)，积环(第十一章)，分解多项式的计算机方法和限定多项式的根的取值范围的柯西定理(第十二章)，基于对称函数的分裂定理的证明(第十六章). 此外还添加了一些好的练习题. 但这本书太厚了，因此我尽力遏制了添加内容的冲动.

给教师的话

使用本书的教师可以适当取材. 不要试图全讲整本书，但是一定要包括一些有意义的特定主题，例如平面图形的对称、SU_2 的几何、虚二次数域上的算术. 如果你不想讨论这些问题，那么这本书不适合你.

使用本书需要的预备知识相对较少. 学生应熟悉微积分、复数的基本性质和数学归纳法. 了解证明肯定是有用的. 第九章(线性群)中要用到的拓扑学概念不作为预备知识要求.

建议你关注具体的例子，特别是前几章中的. 这一点对学习这门课而对证明的构成没有明确概念的学生来讲是至关重要的.

教师可以花一个学期讲授前 5 章，但这样会使本书的目的大打折扣，真正有意义的内容从第六章(对称)才开始. 尽快学到第六章，这样就可以以轻松的节奏学完第六章. 尽管对称很快能吸引学生的注意力，但是对称不是一个轻松的主题，教师很容易为内容陶醉而学生却跟不上进度.

目前，我班上的大多数学生来上课前就熟悉了矩阵运算和模算术，在班上我根本没讲第一章(矩阵)而直接留了作业. 下面是关于第二章(群)的建议.

1. 对抽象的问题浅尝辄止，在第六、七章还会遇到它们.
2. 例如，重点放在矩阵群. 对称的例子最好推迟到第六章讲授.
3. 不要在计算上花费太多时间，在第十二章和第十三章自然会大量涉及.
4. 不强调商群的构造.

商群提出了一个在教学上如何讲授的问题. 虽然商群的结构在概念上很难，但在多数初等例子里商群是很容易作为同态的像给出的，因而不需要抽象定义. 模算术几乎是其仅有的反例. 由于模 n 的整数构成一个环，对于群的商，模算术不是一个具有启发性的好例子. 第一次真正使用商群是在第七章讨论生成元和关系时. 在本书的早期手稿里，我把商群推迟到那里讲授，但是，由于担心引起代数界的不满，我最后还是把商群放到了第二

章. 如果你不打算在课程中讲授生成元和关系，那么可将商的深入讨论推迟到第十一章(环)，在那里商起着重要的作用，而且模算术成了最好的富于启发性的例子.

在第三章(向量空间)中，我试图建立这样一种用基计算的方式，它使学生不会为保持下标一致而烦恼. 由于记号在整本书中都使用，建议采纳这些记号.

在第五章定义的矩阵指数在第十章用于描述单参数群，所以，如果你计划讲单参数群，迟早要讨论矩阵指数. 但不要陷入过多讲授微分方程的诱惑，因为你是在讲授代数，不讲授过多的微分方程是可以理解的.

除去前两节，第七章(群论的进一步讨论)包含了可选的内容. 关于托德-考克斯特算法一节是为讨论生成元和关系用的，否则没有什么用处. 这一节也很有趣.

第八章(双线性型)没有什么特别的. 我没能解决这个主题的主要教学问题，即同一主题有太多的变化，但通过集中于实的和复的情形，我尽量使讨论简短.

在第九章(线性群)，计划把时间花在 SU_2 的几何上. 在我扩充关于 SU_2 一节内容之前，我的学生每年都抱怨，之后他们开始索要补充读物，想学更多的东西. 许多学生在上这门课时不熟悉拓扑学概念，但我发现学生不熟悉拓扑学概念所带来的困难是可以克服的. 的确，这一章是学生了解流形的很好切入点.

若干年来我一直反对把群表示写入第十章，因为它太难了. 但是学生常常要求学习这个主题，我不断地问自己：化学家都能教的东西，为什么我们不能教？最终，依照本书的逻辑结构要求还是纳入了群表示这一主题. 作为回报，埃尔米特型有了一个应用.

你可能发现在第十三章中二次数域的讨论对于一般的代数课程来说太长了. 考虑到这一点，我将第十三章第五节(分解理想)作为一个自然的停顿点.

在入门级的代数课程里，似乎应该提及域的最重要的例子，因此第十五章讨论了函数域. 伽罗瓦理论是否应该放到本科生课程中一直是一个有争议的问题. 但是作为对称讨论的高潮，我把它安排在这里.

对一些较难的练习题标上了星号. 虽然我讲授代数课程多年，但这本书的许多方面仍是试验性的，我非常感谢使用本书的人提出批评和建议.

致谢

我主要想感谢我的学生，多年来是他们使我的课堂如此令人神往. 其中很多人在本书中会看到自己的贡献，我希望你们能原谅我没有一一列举你们的名字.

第 1 版致谢

许多人用了我的讲义并给出了宝贵的建议，其中包括：Jay Goldman，Steve Kleiman，Richard Schafer 和 Joe Silverman. Harold Stark 在数论方面、Gil Strang 在线性代数方面给予了帮助. 此外，下列人员阅读了手稿并给出了建议：Ellen Kirkman，Al Levine，Barbara Peskin 和 John Tate. 我要特别感谢 Barbara Peskin 在她生命的最后一年通读了整本书两遍.

需要数学精确性的插图是 George Fann 和 Bill Schelter 在计算机上制作的，我自己做不来. 感谢 Marge Zabierek，八年里他每年都重录手稿，直到手稿放到计算机里我能自己修订为止. 感谢 Mary Roybal 对手稿的细致而老练的编辑工作.

我在写本书时对其他书参考得不多，但 Birkhoff 和 MacLane 的经典著作以及师从 van der Waerden 的学习对我影响很大. Herstein 的书也一样对我影响深刻，我曾多年用之作为教材. 在 Noble 的书以及 Paley 和 Weichsel 的书中我发现了好的练习题.

第 2 版致谢

许多人对第 1 版做过评论，一些在文中提及了. 我恐怕忘记了提及许多人.

要特别感谢以下这些人：Annette A' Campo 和 Paolo Maroscia 对第 1 版做了仔细的转换和修正；Nathaniel Kuhn 和 James Lepowsky 提出了宝贵意见；Annette 和 Nat 最终教会了我怎样证明正交关系.

感谢那些审阅我的手稿并给出建议的人. 他们是：Alberto Corso，Thomas C. Craven，Sergi Elizade，Luis Finotti，Petter A. Linnell，Brad Shelton，Hema Srinivasan 和 Nik Weaver. Roger Lipsett 阅读了全部修订后的手稿并给出了建议. Brett Coonley 帮忙解决了把手稿变成 TeX 文档时遇到的技术问题.

也感谢在 Pearson 出版社工作的 Caroline Celano，她仔细而全面地对手稿进行了编辑；还有在 Laserwords 工作的 Patty Donovan，她总是优雅地回复我要求进一步校正的请求，尽管她的耐心曾经多次受到考验.

我同 Gil Strang 与 Harold Stark 几乎交谈过所有问题.

最后，感谢麻省理工学院的本科生，他们阅读且评论了修订的文本并修正了错误. 这些读者包括 Nerses Aramyan、Reuben Aronson、Mark Chen、Jeremiah Edwards、Giuliano Giacaglia、Li-Mei Lim、Ana Malagon、Maria Monks 和 Charmaine Sia. 我越来越依赖他们，特别是 Nerses、Li-Mei 和 Charmaine.

"1，2，3，5，4…"

"不！爸爸，是 1，2，3，4，5."

"哎，如果我想说 1，2，3，5，4，为什么不行呢?"

"不是那样数数的."

——Carolyn Artin

记　号

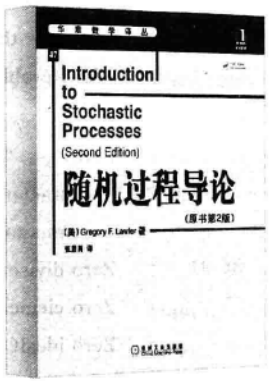
$\langle A\rangle$	理想 A 的类(13.7.2)
A^{t}	矩阵 A 的转置(1.3.1)
A_n	交错群(2.5.6)
$\mathbf{C}$	复数域(2.2.2)
C_n	n 阶循环群(6.4.1)
$C(x)$	元素 x 的共轭类(7.2.3)
$\mathrm{cof}(A)$	矩阵 A 的伴随矩阵(1.6.7)
D_n	二面体群(6.4.1)
$\mathrm{det}A$	矩阵 A 的行列式(1.4.1)
e_i，e_{ij}	标准基向量(1.1.24)，矩阵单位(1.1.21)
F^n	系数在域 F 上的 n 维列向量空间(3.3.6)
$F^{m\times n}$	系数在域 F 上的 $m\times n$ 矩阵空间(3.3.6)
$\mathbf{F}_p$	整数模 p 的域(3.2.4)
GL_n	一般线性群(2.2.4)
I	单位矩阵(1.1.11)，二十面体群(6.12.1)
$\mathrm{im}\varphi$	映射 φ 的像(2.5.4)
$\ker\varphi$	同态 φ 的核(2.5.5)，(4.1.5)
K^G	固定域(16.5.1)
l^∞	有界序列空间(3.7.2)
M，M_n	平面等距群，n 维空间的等距群(第六章第二节)
$\mathbf{N}$	正整数集合，又叫自然数(A.2.1)
$N(H)$	子群 H 的正规化子(7.6.1)
$n!$	n 的阶乘：整数 1，2，…，n 的乘积
$\binom{n}{k}$	二项式系数(A.1.1)
O_n	正交群(6.7.3)，(9.1.2)
$O_{3,1}$	洛仑兹群(9.1.5)
PSL_n	射影群(9.8.1)
$\mathbf{R}$	实数域(2.2.2)
R^+	环 R 的加群(2.1.1)
$R^\times$	环 R 的可逆元构成的乘法群(2.1.1)

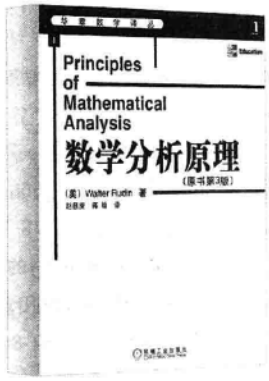
S_n	对称群(2.2.5)
$\mathbf{S}^n$	n 维球面(第九章第二节)
SL_n	特殊线性群(2.2.11)，(9.1.3)
SO_n	特殊正交群(5.1.11)，(9.1.3)
SP_{2n}	辛群(9.1.4)
SU_n	特殊酉群(9.1.3)
T	四面体群(6.12.1)
U_n	酉群(8.3.14)，(9.1.3)
$\langle x\rangle$	由元素 x 生成的子群(2.4.1)
Z	群的中心
$\mathbf{Z}$	整数环(2.2.2)
$Z(x)$	元素 x 的中心化子(7.2.2)
ζ_n	n 次单位根 $e^{2\pi i/n}$(12.4.7)
$\lfloor\mu\rfloor$	小于等于 μ 的最大整数：μ 的下取整(13.7.7)
ω	3 次单位根 $e^{2\pi i/3}$(10.4.14)
$\approx$	指两个结构是同构的，比如 $G\approx G'$(2.6.3)
$\equiv$	同余，如在 $a\equiv b(\mathrm{mod}\ n)$中所示(2.9.1)，参见(2.8.2)和(2.7.14)
$*$	如果 A 是复矩阵，则 A^* 是伴随矩阵$\overline{A}^t$(8.3.5)
	在矩阵表示中，$*$ 表示未定元素
	带星号的练习是较难的
$\oplus$	直和(3.6.5)，(14.7.2)

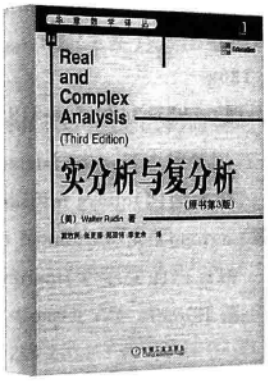
如果 S 和 T 为集合，我们使用如下记号：

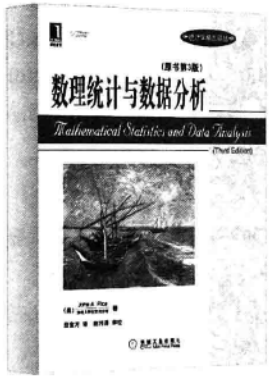
$\lvert S\rvert$	集合 S 中元素的个数，也称为集合 S 的阶
$[S]$	S 的子集，可看作 S 的子集的集合中的元素(2.7.8)
$s\in S$	s 是 S 的一个元素
$S\subset T$	S 是 T 的子集，或 S 包含在 T 中. 换言之，S 的每个元素也是 T 的元素
$T\supset S$	T 包含 S，这与 $S\subset T$ 是一回事
$S<T$	S 是 T 的真子集，意指它是子集，且 T 含有不是 S 的成员的元素
$T>S$	这与 $S<T$ 是一回事
$S\cap T$	集合的交，它是 S 和 T 所有公共元素的集合
$S\cup T$	集合的并，它是包含在集合 S 和 T 之一中的元素的集合
$S\times T$	集合的积. 其元素是有序对$(s,\ t)$： $S\times T=\{(s,\ t)\mid s\in S,\ t\in T\}$
$\varphi: S\to T$	从 S 到 T 的一个映射，是其定义域为 S 而值域为 T 的一个函数
$s\rightsquigarrow t$	这个弯弯的箭头指出所讨论的映射将把元素 s 映射为元素 t，即 $\varphi(s)=t$
■	文中话题的转移符号，如证明或例子结束了，回到文中的主线

推荐阅读









■ **时间序列分析及应用：R语言（原书第2版）**
作者：Jonathan D. Cryer Kung-Sik Chan
ISBN：978-7-111-32572-7
定价：48.00元

■ **随机过程导论（原书第2版）**
作者：Gregory F. Lawler
ISBN：978-7-111-31544-5
定价：36.00元

■ **数学分析原理（原书第3版）**
作者：Walter Rudin
ISBN：978-7-111-13417-6
定价：28.00元

■ **实分析与复分析（原书第3版）**
作者：Walter Rudin
ISBN：978-7-111-17103-9
定价：42.00元

■ **数理统计与数据分析（原书第3版）**
作者：John A. Rice
ISBN：978-7-111-33646-4
定价：85.00元

■ **统计模型：理论和实践（原书第2版）**
作者：David A. Freedman
ISBN：978-7-111-30989-5
定价：45.00元

目　录

第一章 矩 阵

有了一些增加或减少，
或在上面添加一点或拿走一点，
人们在第一眼还是会说大小没变.

——Leonhard Euler[⊖]

矩阵是本书的中心角色，它是理论的重要组成部分，并且许多具体例子都基于矩阵. 因而，发展处理矩阵的方法是非常重要的. 因为矩阵遍及数学的各个分支，所以这里用到的技巧在其他地方也一定会用到.

第一节 基 本 运 算

设 m 和 n 是正整数，一个 $m\times n$ 矩阵是按 m 行 n 列矩形排列的 mn 个数：

【1.1.1】
$$\begin{array}{c} \\ m\text{ 行} \end{array}\begin{array}{c} n\text{ 列} \\ \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \end{array}$$

例如，$\begin{bmatrix} 2 & 1 & 0 \\ 1 & 3 & 5 \end{bmatrix}$是 2×3 矩阵(两行三列). 我们通常用大写字母 A 表示矩阵.

矩阵中的数称为矩阵元素，用 a_{ij} 表示，其中 i，j 为指标(整数)，$1\leqslant i\leqslant m$，$1\leqslant j\leqslant n$. 指标 i 称为行指标，而 j 称为列指标. 因而 a_{ij} 是位于矩阵 i 行 j 列的元素：

$$\begin{array}{c} \\ i \end{array}\begin{array}{c} j \\ \begin{bmatrix} & \vdots & \\ \cdots & a_{ij} & \cdots \\ & \vdots & \end{bmatrix} \end{array}$$

在上面的例子中，$a_{11}=2$，$a_{13}=0$，而 $a_{23}=5$. 有时把元素为 a_{ij} 的矩阵记为(a_{ij}).

一个 $n\times n$ 的矩阵叫做方阵. 一个 1×1 的矩阵$[a]$只含有一个元素，我们不区分这样的矩阵和它的元素.

一个 $1\times n$ 的矩阵是一个 n 维行向量. 当矩阵只有一行时，我们省略行指标 i，而将其记成一个行向量：

$$[a_1 \quad a_2 \quad \cdots \quad a_n] \quad 或 \quad (a_1,\ a_2,\ \cdots,\ a_n)$$

⊖ 这是欧拉《代数》一书的第一句话，《代数》一书于 1770 年在圣彼得堡出版.

逗号在行向量中可以有，也可以没有. 同样，一个 $m\times 1$ 的矩阵是一个 m 维列向量：

$$\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}$$

在本书中，多数情况我们不区分一个 n 维列向量和一个 n 维空间的点坐标. 在少数几个需要区分的地方，我们会明确指出来.

矩阵的*加法*和向量的加法一样. 令 $A=(a_{ij})$ 和 $B=(b_{ij})$ 是两个 $m\times n$ 的矩阵，它们的和 $A+B$ 是一个 $m\times n$ 矩阵 $S=(s_{ij})$，其中 $s_{ij}=a_{ij}+b_{ij}$. 因此

$$\begin{bmatrix} 2 & 1 & 0 \\ 1 & 3 & 5 \end{bmatrix}+\begin{bmatrix} 1 & 0 & 3 \\ 4 & -3 & 1 \end{bmatrix}=\begin{bmatrix} 3 & 1 & 3 \\ 5 & 0 & 6 \end{bmatrix}$$

只有两个同样形状的矩阵(即它们都是 m 行 n 列的矩阵)才能相加.

矩阵和数的*标量乘法*与向量的标量乘法一样定义. 一个数 c 乘一个 $m\times n$ 矩阵 $A=(a_{ij})$ 得到一个 $m\times n$ 矩阵 $B=(b_{ij})$，其中 $b_{ij}=c\cdot a_{ij}$ 对于所有 i，j 都成立. 因此

$$2\begin{bmatrix} 2 & 1 & 0 \\ 1 & 3 & 5 \end{bmatrix}=\begin{bmatrix} 4 & 2 & 0 \\ 2 & 6 & 10 \end{bmatrix}$$

数也称为*标量*. 我们假设标量都是实数. 在后面的章节里，还会出现其他标量. 只要记住，除了偶尔提到实二维或实三维空间的几何外，本章的结果对于复数标量也是成立的.

*矩阵乘法*是一个复杂的运算. 我们先学习同样大小(比如说 m)的一个行向量 A 和一个
2 列向量 B 的乘积 AB. 如果 A 与 B 的元素分别记为 a_i 与 b_i，积 AB 是一个 1×1 的矩阵，即标量

【1.1.2】
$$a_1b_1+a_2b_2+\cdots+a_mb_m$$

因此，

$$\begin{bmatrix} 1 & 3 & 5 \end{bmatrix}\begin{bmatrix} 1 \\ -1 \\ 4 \end{bmatrix}=1-3+20=18$$

当我们把 A 和 B 看成带有下标的向量时，这个定义的作用是很明显的. 例如，考虑含有 m 种成分的糖果条，用 a_i 表示每一糖果条中(成分)$_i$ 的克数，b_i 表示每克(成分)$_i$ 的价格，则矩阵乘积 AB 算出每个糖果条的价格：

$$(\text{克}/\text{条})\cdot(\text{价格}/\text{克})=(\text{价格}/\text{条})$$

一般地，对于两个矩阵 $A=(a_{ij})$ 和 $B=(b_{ij})$，只有当 A 的列数等于 B 的行数时它们的积才有定义. 如果 A 是一个 $\ell\times m$ 矩阵，且 B 是一个 $m\times n$ 矩阵，这时它们的积是一个 $\ell\times n$ 矩阵. 用符号表示，即

$$(\ell\times m)\cdot(m\times n)=(\ell\times n)$$

积矩阵中的元素由矩阵 A 的所有行和矩阵 B 的所有列的乘积按照(1.1.2)的规则计算. 如果用 $P=(p_{ij})$ 表示积矩阵 AB，则

【1.1.3】
$$p_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{mj}$$

这就是矩阵 A 的第 i 行和 B 的第 j 列的乘积.

$$\begin{bmatrix} & & \\ a_{i1} & \cdots & a_{in} \\ & & \end{bmatrix} \begin{bmatrix} & b_{1j} & \\ & \vdots & \\ & b_{mj} & \end{bmatrix} = \begin{bmatrix} & \vdots & \\ \cdots & p_{ij} & \cdots \\ & \vdots & \end{bmatrix}$$

例如，

【1.1.4】
$$\begin{bmatrix} 2 & 1 & 0 \\ 1 & 3 & 5 \end{bmatrix} \begin{bmatrix} 1 \\ -1 \\ 4 \end{bmatrix} = \begin{bmatrix} 1 \\ 18 \end{bmatrix}$$

矩阵乘法的这种定义方法提供了非常方便的计算工具. 回到糖果条的例子，设有 ℓ 种糖果条，则可构造一个 $\ell \times m$ 矩阵 A，使其第 i 行给出(条)$_i$ 的各成分的克数. 如果要算 n 年中每一年的价格，则可以构造一个矩阵 B，使其第 j 列是(年)$_j$ 的各成分的价格. 矩阵乘积 $AB=P$ 算出每个糖果条的价格：$p_{ij}=$(条)$_i$ 在(年)$_j$ 的价格.

引入矩阵概念的理由之一是为了提供一个书写线性方程组的简明形式. 线性方程组

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m \end{aligned}$$

可利用矩阵记号写为

【1.1.5】
$$AX = B$$

其中 A 为系数矩阵，X 和 B 是列向量，AX 是矩阵乘积：

$$\begin{bmatrix} & & \\ & A & \\ & & \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}$$

我们简称这个形式的方程为“方程”或“方程组”.

矩阵方程

$$\begin{bmatrix} 2 & 1 & 0 \\ 1 & 3 & 5 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 1 \\ 18 \end{bmatrix}$$

表示如下三个未知量两个方程的方程组：

$$\begin{aligned} 2x_1 + x_2 &= 1 \\ x_1 + 3x_2 + 5x_3 &= 18 \end{aligned}$$

方程(1.1.4)给出了一个解 $x_1=1$，$x_2=-1$，$x_3=4$. 还有其他的解.

定义矩阵乘积的和式(1.1.3)也可以写成总和的形式或用求和号“Σ”表示为

4 【1.1.6】
$$p_{ij}=\sum_{\nu=1}^{m}a_{i\nu}b_{\nu j}=\sum_{\nu}a_{i\nu}b_{\nu j}$$

每一个这样的表达式都是和的简写形式. 大Σ表示将所有下标为 $\nu=1$，2，…，m 的项加起来. 最右边的记号表示应该把所有可能的下标为 ν 的项加起来. 我们认为读者应该明白，如果 A 是一个 $\ell\times m$ 矩阵，B 是一个 $m\times n$ 矩阵，则下标 ν 应该从 1 到 m. 我们用希腊字母 ν 这样一个不太常用的符号来明确区分求和时候的下标.

处理数集合的两个最重要的记号之一是如上所用到的求和记号，另一个是矩阵记号. 实际上，两者中记号Σ更为常用. 但是由于矩阵记号更为紧凑，我们将尽可能地使用矩阵记号. 在后面几章里，我们的任务之一就是把复杂的数学结构转换成矩阵记号，从而方便地处理它们.

矩阵运算满足一些等式，如分配律

【1.1.7】 $A(B+B')=AB+AB'$ 和 $(A+A')B=AB+A'B$

以及结合律

【1.1.8】 $(AB)C=A(BC)$

只要矩阵具有适当的行列数使得运算能够进行，这些运算律就成立. 例如，对于结合律，要有正整数 ℓ，m，n，p，使行列数为 $A=\ell\times m$，$B=m\times n$，$C=n\times p$. 因为(1.1.8)中的两个积相等，所以可以将括号省去而记为 ABC. 这样三个矩阵的积 ABC 是一个 $\ell\times p$ 矩阵. 例如，计算矩阵乘积

$$ABC=\begin{bmatrix}1\\2\end{bmatrix}\begin{bmatrix}1&0&1\end{bmatrix}\begin{bmatrix}2&0\\1&1\\0&1\end{bmatrix}$$

的两种方式为

$$(AB)C=\begin{bmatrix}1&0&1\\2&0&2\end{bmatrix}\begin{bmatrix}2&0\\1&1\\0&1\end{bmatrix}=\begin{bmatrix}2&1\\4&2\end{bmatrix}\quad\text{和}\quad A(BC)=\begin{bmatrix}1\\2\end{bmatrix}\begin{bmatrix}2&1\end{bmatrix}=\begin{bmatrix}2&1\\4&2\end{bmatrix}$$

标量乘法与矩阵乘法是相容的，即有

【1.1.9】 $c(AB)=(cA)B=A(cB)$

这些等式的证明是很简单的，没有多大意义.

然而，交换律对于矩阵乘法并不成立，即

5 【1.1.10】 通常 $AB\neq BA$

即使是两个方阵的乘积也会不同，例如：

$$\begin{bmatrix}1 & 1\\ 0 & 0\end{bmatrix}\begin{bmatrix}2 & 0\\ 1 & 1\end{bmatrix}=\begin{bmatrix}3 & 1\\ 0 & 0\end{bmatrix},\quad \text{而}\begin{bmatrix}2 & 0\\ 1 & 1\end{bmatrix}\begin{bmatrix}1 & 1\\ 0 & 0\end{bmatrix}=\begin{bmatrix}2 & 2\\ 1 & 1\end{bmatrix}$$

如果恰好 $AB=BA$ 成立，则称矩阵 A 和矩阵 B 是可换的.

由于矩阵乘法不满足交换律，因此在讨论矩阵方程时要多加注意. 当乘积有定义时，可以在方程 $B=C$ 的两边左乘矩阵 A 而得到 $AB=AC$. 同样，在乘积有定义时也可得到 $BA=CA$. 但我们不能由 $B=C$ 得到 $AB=CA$!

所有元素都是 0 的矩阵称为零矩阵，在不至于引起混淆的前提下，简记为 0.

矩阵 A 的元素 a_{ii} 称为对角元素，一个非零元素都是对角元素的矩阵称为对角矩阵. (非零这个词的意思是不同于零. 这个词很不美观，但是很方便，所以经常使用.)

若一个 $n\times n$ 对角矩阵的对角元素均是 1，就称为 $n\times n$ 恒等矩阵(或单位矩阵)，记作 I_n. 它在乘法中的作用就像数字 1 一样：如果 A 是一个 $m\times n$ 矩阵，则有

【1.1.11】
$$AI_n = A \quad \text{和} \quad I_mA = A$$

我们通常省去下标，用 I 表示 I_n.

下面是两种表示恒等矩阵 I 的简单方法：

$$I=\begin{bmatrix}1 & & 0\\ & \ddots & \\ 0 & & 1\end{bmatrix}=\begin{bmatrix}1 & & \\ & \ddots & \\ & & 1\end{bmatrix}$$

我们常用一块空白或单独一个 0 来表示矩阵中一整块为零的区域.

我们用 $*$ 表示矩阵中任意的未定元素. 这样

$$\begin{bmatrix}* & \cdots & *\\ & \ddots & \vdots\\ & & *\end{bmatrix}$$

表示一条对角线下面元素为 0，而其他元素未定的矩阵. 这样的矩阵称为上三角矩阵. 例如下面的(1.1.14)中的矩阵即为上三角矩阵.

设 A 是一个 $n\times n$ 方阵. 若有矩阵 B 使得

【1.1.12】
$$AB = I_n \quad \text{且} \quad BA = I_n$$

6

则称 B 为 A 的逆，记作 A^{-1}：

【1.1.13】
$$A^{-1}A = I = AA^{-1}$$

当 A 有逆时，称 A 为可逆矩阵. 例如，矩阵 $\begin{bmatrix}2 & 1\\ 5 & 3\end{bmatrix}$ 可逆，其逆为 $\begin{bmatrix}3 & -1\\ -5 & 2\end{bmatrix}$，直接计算 AA^{-1} 和 $A^{-1}A$ 就可以检验这一点. 另外两个例子是

【1.1.14】
$$\begin{bmatrix}1 & \\ & 2\end{bmatrix}^{-1}=\begin{bmatrix}1 & \\ & \frac{1}{2}\end{bmatrix} \quad \text{和} \quad \begin{bmatrix}1 & 1\\ & 1\end{bmatrix}^{-1}=\begin{bmatrix}1 & -1\\ & 1\end{bmatrix}$$

我们后面将看到，如果存在矩阵 B 使得 $AB=I_n$ 和 $BA=I_n$ 这两个关系之一成立，则

A 可逆，并且 B 就是 A 的逆(见(1.2.20))．由于矩阵乘法是不可交换的，所以这并不是显而易见的．另一方面，如果矩阵有逆，则逆是唯一的．下面的引理证明了如果矩阵 A 有逆，则其逆是唯一的．

【1.1.15】引理 *设矩阵 A 是方阵，且有右逆 R 满足 $AR=I$，并且 A 还有左逆 L 满足 $LA=I$，则 $R=L$．从而 A 是可逆的，且 R 为 A 的逆．*

证明 $R=IR=(LA)R=L(AR)=LI=L.$ ■

【1.1.16】命题 *令 A 和 B 是 $n\times n$ 可逆矩阵，则其乘积 AB 和逆 A^{-1} 也是可逆矩阵，且有 $(AB)^{-1}=B^{-1}A^{-1}$，$(A^{-1})^{-1}=A$．更一般地，若 A_1，A_2，…，A_m 都是可逆的 $n\times n$ 矩阵，则积 $A_1A_2\cdots A_m$ 是可逆矩阵，且有 $(A_1A_2\cdots A_m)^{-1}=A_m^{-1}\cdots A_2^{-1}A_1^{-1}$．*

证明 假设 A 和 B 是可逆矩阵，要证明乘积矩阵 $B^{-1}A^{-1}=Q$ 是 $AB=P$ 的逆矩阵，只要验证 $QP=I=PQ$ 即可．其他断言的证明类似． ■

这样，$\begin{bmatrix}1 & \\ & 2\end{bmatrix}\begin{bmatrix}1 & 1\\ & 1\end{bmatrix}=\begin{bmatrix}1 & 1\\ & 2\end{bmatrix}$ 的逆是 $\begin{bmatrix}1 & -1\\ & 1\end{bmatrix}\begin{bmatrix}1 & 0\\ & \frac{1}{2}\end{bmatrix}=\begin{bmatrix}1 & -\frac{1}{2}\\ & \frac{1}{2}\end{bmatrix}$.

注 值得记住 2×2 矩阵的逆：

【1.1.17】
$$\begin{bmatrix}a & b\\ c & d\end{bmatrix}^{-1}=\frac{1}{ad-bc}\begin{bmatrix}d & -b\\ -c & a\end{bmatrix}$$

分母 $ad-bc$ 是矩阵的行列式．如果行列式为 0，则矩阵不可逆．我们在本章第四节讨论行列式．

7

我们将看到大多数方阵是可逆的，尽管由矩阵乘法的定义这个事实并不明显．但当矩阵很大时，具体找出其逆并不是简单问题．所有可逆 $n\times n$ 矩阵的集合称为 n 维一般线性群．当我们在下一章引入群的概念时，一般线性群是最重要的例子之一．

为了供以后参考，我们注意到有下面的引理：

【1.1.18】引理 *一个方阵如果有一行或者一列元素全是 0，则这个方阵是不可逆的．*

证明 如果 $n\times n$ 矩阵 A 有一行元素全是 0，且 B 是任意一个 $n\times n$ 矩阵，则乘积矩阵 AB 的相应行也全是 0．因此，乘积矩阵 AB 不是单位矩阵．因此 A 没有右逆．类似地，如果 $n\times n$ 矩阵 A 有一列元素全是 0，则 A 没有左逆． ■

矩阵的分块乘法

在我们感兴趣的情形里有各种简化矩阵乘法的技巧．分块乘法是其中之一．设 M，M' 分别为 $m\times n$ 和 $n\times p$ 矩阵，r 是小于 n 的整数．可将两个矩阵如下分块：

$$M=[A\,|\,B]\quad,\quad M'=\begin{bmatrix}A'\\ B'\end{bmatrix}$$

其中 A 有 r 列，而 A' 有 r 行．矩阵乘积可如下计算：

【1.1.19】　$$MM' = AA' + BB'$$

注意这个公式和一个行向量与一个列向量的乘法规则是一样的.

我们也可以将矩阵分成四块. 假设把一个 $m\times n$ 矩阵 M 和一个 $n\times p$ 矩阵 M' 分成矩形的子矩阵

$$M=\left[\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right],\quad M'=\left[\begin{array}{c|c} A' & B' \\ \hline C' & D' \end{array}\right]$$

其中 A，C 的列数与 A'，B' 的行数相同. 在此情形，分块矩阵乘法与 2×2 矩阵的乘法相同：

【1.1.20】　$$\left[\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right]\left[\begin{array}{c|c} A' & B' \\ \hline C' & D' \end{array}\right]=\left[\begin{array}{c|c} AA'+BC' & AB'+BD' \\ \hline CA'+DC' & CB'+DD' \end{array}\right]$$

这一规则也可以由矩阵乘法的定义直接验证.

请用分块矩阵乘法矩阵来验证下面的等式

$$\left[\begin{array}{cc|c} 1 & 0 & 5 \\ 0 & 1 & 3 \end{array}\right]\left[\begin{array}{cc|cc} 2 & 3 & 1 & 1 \\ 4 & 8 & 0 & 0 \\ \hline 1 & 0 & 1 & 0 \end{array}\right]=\left[\begin{array}{cc|cc} 7 & 3 & 6 & 1 \\ 7 & 8 & 3 & 0 \end{array}\right]$$

除了可以简化计算之外，分块乘法也是数学归纳法证明矩阵的有用工具.

矩阵单位

矩阵单位是最简单的非零矩阵. $m\times n$ 矩阵单位 e_{ij} 在 i，j 位置有 1 作为它的唯一非零元素：

【1.1.21】　$$e_{ij}=\begin{array}{c} \\ i \\ \\ \end{array}\begin{array}{c} \begin{array}{c} \\ j \\ \\ \end{array} \\ \begin{bmatrix} \vdots & & \\ \cdots & 1 & \cdots \\ \vdots & & \end{bmatrix} \end{array}$$

我们通常用大写字母表示矩阵，但是传统上用小写字母表示矩阵单位.

注　矩阵单位的全体所构成的集合是所有 $m\times n$ 矩阵的空间的一组基，这是因为每一个 $m\times n$ 矩阵 $A=(a_{ij})$ 是矩阵单位 e_{ij} 的线性组合：

【1.1.22】　$$A=a_{11}e_{11}+a_{12}e_{12}+\cdots+a_{mn}e_{mn}=\sum_{i,j}a_{ij}e_{ij}$$

求和符号下面的 i，j 表示对所有 $i=1,\cdots,m$ 和所有 $j=1,\cdots,n$ 求和. 例如

$$\begin{bmatrix} 3 & 2 \\ 1 & 4 \end{bmatrix}=3\begin{bmatrix} 1 & \\ & \end{bmatrix}+2\begin{bmatrix} & 1 \\ & \end{bmatrix}+1\begin{bmatrix} & \\ 1 & \end{bmatrix}+4\begin{bmatrix} & \\ & 1 \end{bmatrix}=3e_{11}+2e_{12}+1e_{21}+4e_{22}$$

一个 $m\times n$ 矩阵单位 e_{ij} 和一个 $n\times p$ 矩阵单位 e_{jl} 的乘积由下面的公式给出：

【1.1.23】　$$e_{ij}e_{jl}=e_{il}\quad,\quad e_{ij}e_{kl}=0\quad \text{如果 } j\neq k$$

注　只在第 i 个位置是 1 而其余位置为 0 的列向量 e_i 类似于矩阵单位，集合 $\{e_1,e_2,\cdots,e_n\}$ 构成 n 维向量空间 $\mathbf{R}^n$ 的标准基（参见第三章(3.4.15)）. 如果 $X=(x_1,$

x_2，…，x_n)是列向量，则

9 【1.1.24】 $$X = x_1e_1 + x_2e_2 + \cdots + x_ne_n = \sum_i x_ie_i$$

矩阵单位与标准基向量的乘法由下面的公式给出：

【1.1.25】 $$e_{ij}e_j = e_i \quad , \quad e_{ij}e_k = 0 \quad \text{如果} \quad j \neq k$$

第二节 行 约 简

用一个 $n\times n$ 矩阵去左乘一个 $n\times p$ 矩阵，例如

【1.2.1】 $$AX = Y$$

可以通过对 X 的行作用计算出来. 如果令 X_i 和 Y_i 分别表示 X 和 Y 的第 i 行，则用向量形式表示为：

【1.2.2】 $$Y_i = a_{i1}X_1 + a_{i2}X_2 + \cdots + a_{in}X_n,$$

$$\boxed{A}\begin{bmatrix}-X_1-\\-X_2-\\\vdots\\-X_n-\end{bmatrix} = \begin{bmatrix}-Y_1-\\-Y_2-\\\vdots\\-Y_n-\end{bmatrix}$$

例如，矩阵乘积

$$\begin{bmatrix}0 & 1\\-2 & 3\end{bmatrix}\begin{bmatrix}1 & 2 & 1\\1 & 3 & 0\end{bmatrix} = \begin{bmatrix}1 & 3 & 0\\1 & 5 & -2\end{bmatrix}$$

最下面一行可计算为：$-2[1\quad 2\quad 1]+3[1\quad 3\quad 0]=[1\quad 5\quad -2]$.

左乘一个可逆矩阵称为*行变换*. 下面讨论的这些行变换将会用到一些称为*初等矩阵*的方阵. 有三种类型的 2×2 初等矩阵：

【1.2.3】 (i) $\begin{bmatrix}1 & a\\0 & 1\end{bmatrix}$ 或 $\begin{bmatrix}1 & 0\\a & 1\end{bmatrix}$, (ii) $\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$, (iii) $\begin{bmatrix}c & \\ & 1\end{bmatrix}$ 或 $\begin{bmatrix}1 & \\ & c\end{bmatrix}$

此处 a 可以是任意标量，c 可以是任意非零标量.

也有三种类型的 $n\times n$ 初等矩阵. 通过对称地拼接 2×2 初等矩阵到恒等矩阵可得到这
10 些类型的初等矩阵. 为节省空间，下面展示了 5×5 矩阵，但矩阵规模假设是任意的.

【1.2.4】

类型(i)

$$\begin{array}{c} \\ i \\ \\ j \\ \\ \end{array}\!\!\begin{array}{c} \begin{array}{ccccc} i & & & j & \end{array} \\ \begin{bmatrix}1 & & & & \\ & 1 & & a & \\ & & 1 & & \\ & & & 1 & \\ & & & & 1\end{bmatrix} \end{array} \quad \text{或} \quad \begin{array}{c} \\ j \\ \\ i \\ \\ \end{array}\!\!\begin{array}{c} \begin{array}{ccccc} i & & & j & \end{array} \\ \begin{bmatrix}1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & a & & 1 & \\ & & & & 1\end{bmatrix} \end{array} \quad (i \neq j)$$

一个非零非对角元加在了恒等矩阵上.

类型(ii)

$$\begin{array}{c} \\ i \\ \\ j \\ \\ \end{array}\begin{array}{c} \begin{array}{cccccc} & & i & & j & \end{array} \\ \begin{bmatrix} 1 & & & & & \\ & 0 & & 1 & & \\ & & 1 & & & \\ & 1 & & 0 & & \\ & & & & & 1 \end{bmatrix} \end{array}$$

恒等矩阵的第 i 个和第 j 个对角元素用 0 代替，且在$(i,\ j)$和$(j.\ i)$位置各加上一个 1.

类型(iii)

$$\begin{array}{c} \\ i \\ \\ \\ \\ \end{array}\begin{array}{c} \begin{array}{c} i \end{array} \\ \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & c & & \\ & & & 1 & \\ & & & & 1 \end{bmatrix} \end{array} \quad (c \neq 0)$$

恒等矩阵的一个对角元素被非零标量 c 代替.

注　初等矩阵 E 在矩阵 X 上的作用：要得到矩阵 EX，必须

【1.2.5】

类型(i)：i，j 位置具有 a：用 a 乘以 X 的第 j 行再加到第 i 行上去.

类型(ii)：互换 X 的第 i 行和第 j 行.

类型(iii)：X 的第 i 行乘以非零标量 c.

这些是初等行变换，请自行检验这些法则.

【1.2.6】**引理**　初等矩阵是可逆矩阵，它们的逆矩阵也是初等矩阵.

证明　初等矩阵的逆矩阵对应着相应行变换的逆变换："第 i 行减去第 j 行的 a 倍"，再"互换第 i 行与第 j 行"，或"第 i 行乘以 c^{-1} 倍". ■ 11

我们现在对矩阵 M 施行初等行变换(1.2.5)，目的是将其化成更简单的矩阵M'：

$$M \xrightarrow{\text{变换序列}} \cdots \rightarrow M'$$

由于每一次初等变换都可以用初等矩阵左乘来实现，因此可以把这一系列的变换用初等矩阵的乘法来表示：

【1.2.7】
$$M' = E_k E_{k-1} \cdots E_2 E_1 M$$

这个过程称为行约简.

作为一个例子，我们用初等变换从左向右化简下面的矩阵，消去尽可能多的非零元素.

【1.2.8】
$$M = \begin{bmatrix} 1 & 1 & 2 & 1 & 5 \\ 1 & 1 & 2 & 6 & 10 \\ 1 & 2 & 5 & 2 & 7 \end{bmatrix} \rightarrow\rightarrow \begin{bmatrix} 1 & 1 & 2 & 1 & 5 \\ 0 & 0 & 0 & 5 & 5 \\ 0 & 1 & 3 & 1 & 2 \end{bmatrix} \rightarrow$$

$$\begin{bmatrix}1&1&2&1&5\\0&1&3&1&2\\0&0&0&5&5\end{bmatrix}\to\to\begin{bmatrix}1&0&-1&0&3\\0&1&3&1&2\\0&0&0&1&1\end{bmatrix}\to\begin{bmatrix}\mathbf{1}&0&-1&0&3\\0&\mathbf{1}&3&0&1\\0&0&0&\mathbf{1}&1\end{bmatrix}=M'$$

矩阵M'不能再用行变换化简了.

这里是用行约简解线性方程组的方法. 假设给定由 n 个未知量的 m 个方程组成的线性方程组，比如说 $AX=B$，其中 A 是一个 $m\times n$ 矩阵，X 是未知列向量，而 B 是给定的列向量. 为解这个方程组，我们构造 $m\times(n+1)$矩阵，该矩阵也称为增广矩阵：

【1.2.9】
$$M=[A|B]=\left[\begin{array}{ccc|c}a_{11}&\cdots&a_{1n}&b_1\\ \vdots&&\vdots&\vdots\\ a_{m1}&\cdots&a_{mn}&b_n\end{array}\right]$$

用行变换化简 M. 注意到 $EM=[EA|EB]$. 令

$$M'=[A'|B']$$

为一系列行变换的结果. 关键的事实是：

12 【1.2.10】**命题** *方程组 $A'X=B'$ 与 $AX=B$ 同解.*

证明 由于M'可由一系列初等行变换得到，故存在初等矩阵 E_1，…，E_k 使得

$$M'=E_k\cdots E_1M=PM$$

其中 $P=E_k\cdots E_1$ 是可逆矩阵，且 $M'=[A'|B']=[PA|PB]$. 若 X 是原方程组 $AX=B$ 的解，则两边左乘 P：$PAX=PB$，即 $A'X=B'$. 从而 X 也是新方程组的解. 反之，若 $A'X=B'$，则 $P^{-1}A'X=P^{-1}B'$，亦即 $AX=B$. ■

例如，考虑方程组

【1.2.11】
$$\begin{aligned}x_1+x_2+2x_3+x_4&=5\\ x_1+x_2+2x_3+6x_4&=10\\ x_1+2x_2+5x_3+2x_4&=7\end{aligned}$$

其增广矩阵行约简如上所示(1.2.8). 行约简表明这个方程组等价于约简最后结果M'定义的方程组：

$$\begin{aligned}x_1-x_3&=3\\ x_2+3x_3&=1\\ x_4&=1\end{aligned}$$

我们可立即得到该方程组的解：取 $x_3=c$ 是任意常数，然后解出 x_1，x_2 和 x_4. (1.2.11)的一般解可以写为

$$x_3=c,\quad x_1=3+c,\quad x_2=1-3c,\quad x_4=1$$

的形式，其中 c 是任意常数.

回到任意矩阵的行约简. 不难看出，任意矩阵 M 都可以经过一系列行变换化为行阶梯矩阵. (1.2.8)的最终约简结果就是行阶梯矩阵的一个例子. 下面是定义. 一个行阶梯矩

阵是具有下面这些性质的矩阵：

【1.2.12】

(a) 如果第 i 行是零，则所有 $j>i$ 的行也是零.

(b) 如果第 i 行不是零，则它的第一个非零元为 1，称之为主元.

(c) 如果第 $i+1$ 行不是零，则第 $i+1$ 行的主元在第 i 行的主元的右边.

(d) 主元上面的元素皆为零.（由(c)，主元下面的元也是零.）

(1.2.8) 的矩阵 M' 与下面例子中矩阵的主元已经用黑体标出.

作行约简时，先找到有非零元(比如说 m)的第一列(如果没有，则 $M=0$ 且它本身已经是行阶梯矩阵). 用(ii)型初等行变换互换行，将非零元 m 移到顶行. 用(iii)型变换将元 m 正规化为 1. 这个元就变成了主元. 然后用一系列(i)型变换将该列其他元清零，得到如下 13
形式的块矩阵：

$$\left[\begin{array}{c|c|ccc} 0\cdots0 & 1 & * & \cdots & * \\ \hline 0\cdots0 & 0 & * & \cdots & * \\ \vdots & \vdots & \vdots & & \vdots \\ 0\cdots0 & 0 & * & \cdots & * \end{array}\right], \quad \text{将它写为} \left[\begin{array}{c|c|c} & 1 & B_1 \\ \hline & & D_1 \end{array}\right] = M_1$$

继续对较小的矩阵 D_1 进行行变换. 因为 D_1 的左边各块都是零，这些变换对于矩阵 M_1 的其他部分没有影响. 对矩阵的行数应用数学归纳法，可以假设 D_1 可约简为行阶梯矩阵，比如说 D_2，于是 M_1 可以约简为矩阵：

$$\left[\begin{array}{c|c|c} & 1 & B_1 \\ \hline & & D_2 \end{array}\right] = M_2$$

这个矩阵满足行阶梯矩阵要求的前三个条件. 这时，可将 D_2 主元上方的 B_1 中的元清零，从而最终约简得到一个行阶梯矩阵. ■

可以证明，由给定矩阵 M 经过行约简得到的阶梯矩阵是唯一的，它与所用的行变换的先后顺序无关. 因为这不太重要，故省去其证明.

正如前面所说的，使用行约简的原因是，当 A' 是一个行阶梯矩阵时，可以立即解出方程组 $A'X=B'$. 另一个例子：设

$$[A'\,|\,B'] = \left[\begin{array}{cccc|c} \mathbf{1} & 6 & 0 & 1 & 1 \\ 0 & 0 & \mathbf{1} & 2 & 3 \\ 0 & 0 & 0 & 0 & \mathbf{1} \end{array}\right]$$

由于第三个方程是 $0=1$，因而方程组 $A'X=B'$ 无解. 另一方面，

$$[A'\,|\,B'] = \left[\begin{array}{cccc|c} \mathbf{1} & 6 & 0 & 1 & 1 \\ 0 & 0 & \mathbf{1} & 2 & 3 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

有解. 任取 $x_2=c$，$x_4=c'$，由第一个方程解出 x_1，由第二个方程解出 x_3. 一般的法则如下：

【1.2.13】命题 令 $M'=[A'\,|\,B']$ 为一个行阶梯矩阵，此处 B' 为列向量，则方程组 $A'X=B'$ 有解的充分必要条件是最后一列 B' 没有主元. 这时，如果第 i 列没有主元，则未知量 x_i 可 14

取任意值. 当指定这些任意值后，就唯一确定了其他未知量.

齐次线性方程组 $AX=0$ 有平凡解 $X=0$. 从行阶梯形又可看出，当未知量个数大于方程个数时，齐次线性方程组 $AX=0$ 必有非平凡解.

【1.2.14】推论 当 $m<n$ 时，每个具有 n 个未知量的由 m 个方程组成的齐次线性方程组 $AX=0$ 有一个使某个 x_i 非零的解 X.

证明 对分块矩阵$[A|0]$进行行约简得到$[A'|0]$，其中A'是行阶梯形. 方程 $A'X=0$ 与 $AX=0$ 同解. A'的主元数(比如 r)至多等于矩阵的行数 m，所以小于 n. 命题 1.2.13 告诉我们可以任意指定 $n-r$ 个 x_i 的值. ■

现在我们用行约简刻画可逆方阵.

【1.2.15】引理 一个行阶梯方阵 M 要么是恒等矩阵 I，要么它的底行为零.

证明 比如说 M 是 $n\times n$ 行阶梯矩阵. 因为有 n 个列，故至多有 n 个主元. 如果有 n 个主元，则每个列必须有一个. 这种情形下，$M=I$. 如果主元个数少于 n，则某一行为零，从而底行也为零. ■

【1.2.16】定理 令 A 是一个方阵，则下列条件等价：

(a) A 可以由一系列行变换约简为恒等矩阵.

(b) A 是初等矩阵的乘积.

(c) A 可逆.

证明 我们通过证明(a)⇒(b)⇒(c)⇒(a)来证明命题. 设 A 可以经过行变换约简为单位矩阵：$E_k\cdots E_1A=I$. 在这个式子两边左乘 $E_1^{-1}\cdots E_k^{-1}$，得 $A=E_1^{-1}\cdots E_k^{-1}$. 因为初等矩阵的逆是初等矩阵，故(b)成立，所以(a)蕴含着(b). 由于可逆矩阵的乘积是可逆的，故(b)蕴含着(c). 如果 A 是可逆的，则对其进行行约简得到的行阶梯矩阵A'也可逆. 由于可逆矩阵没有零行，因此引理 1.2.15 说明A'是恒等矩阵. ■

行约简给出了一种计算可逆矩阵 A 的逆的方法：像前面一样，用行变换把 A 约简为恒等矩阵：$E_k\cdots E_1A=I$. 在其两边右乘 A^{-1}，

$$E_k\cdots E_1I=E_k\cdots E_1AA^{-1}=IA^{-1}=A^{-1}$$

【1.2.17】推论 令 A 是可逆矩阵. 要计算其逆 A^{-1}，先对 A 用初等行变换 E_1，E_2，...，
15 E_k 把它约简为恒等矩阵. 当同一系列初等行变换用于 I 时，得到 A^{-1}.

【1.2.18】例 求矩阵

$$A=\begin{bmatrix}1 & 5\\ 2 & 6\end{bmatrix}$$

的逆. 为此，先构造 2×4 的块矩阵

$$[A\mid I]=\left[\begin{array}{cc|cc}1 & 5 & 1 & 0\\ 2 & 6 & 0 & 1\end{array}\right]$$

对矩阵 A 作行变换将其化为恒等矩阵，右边也同时作行变换，则最终右边化为 A^{-1}.

$$[A \mid I]=\left[\begin{array}{cc|cc}1 & 5 & 1 & 0\\ 2 & 6 & 0 & 1\end{array}\right]\to\left[\begin{array}{cc|cc}1 & 5 & 1 & 0\\ 0 & -4 & -2 & 1\end{array}\right]\to$$

【1.2.19】
$$\left[\begin{array}{cc|cc}1 & 5 & 1 & 0\\ 0 & 1 & \frac{1}{2} & -\frac{1}{4}\end{array}\right]\to\left[\begin{array}{cc|cc}1 & 0 & -\frac{3}{2} & \frac{5}{4}\\ 0 & 1 & \frac{1}{2} & -\frac{1}{4}\end{array}\right]=[I/A^{-1}]$$ ■

【1.2.20】命题　令 A 是一个方阵，且它有左逆 B:$BA=I$ 或右逆 B:$AB=I$，则 A 可逆，且 B 为其逆.

证明　设 $AB=I$. 我们对 A 作行约简. 比如说 $A'=PA$，此处 $P=E_k\cdots E_1$ 是相应的初等矩阵的乘积，且A'是行阶梯矩阵. 则 $A'B=PAB=P$. 因为 P 是可逆的，所以它的最后一行非零. 于是，A'的最后一行也非零. 所以，A'是恒等矩阵(1.2.15)，从而 P 是 A 的左逆. 这样，A 既有左逆又有右逆，从而它是可逆的，且 B 是 A 的逆.

如果 $BA=I$，在上面的推理中我们互换 A 与 B 的角色. 我们发现 B 是可逆的，且它的逆是 A. 这样，A 是可逆的，且它的逆是 B. ■

我们现在回到方程的个数与未知量的个数相等的线性方程组的主要定理上.

【1.2.21】定理(方阵方程组)　下列条件对于方阵 A 是等价的：

(a) A 是可逆的.

(b) 对于任意列向量 B，方程组 $AX=B$ 有唯一解.

(c) 齐次线性方程组 $AX=0$ 只有平凡解 $X=0$.

证明　已知方程组 $AX=B$，我们将增广矩阵$[A|B]$行约简为行阶梯矩阵$[A'|B']$. 方程组 $A'X=B'$同解. 如果 A 可逆，则A'是恒等矩阵，所以唯一解是 $X=B'$. 这就证明了(a)⇒(b).

如果一个 $n\times n$ 矩阵 A 不是可逆的，则A'有一个零行. 方程组 $A'X=0$ 中有一个平凡的方程. 所以主元个数小于 n. 齐次线性方程组 $A'X=0$ 有一个非平凡解(1.2.13). 所以 16
方程组 $AX=0$(1.2.14)也有一个非平凡解. 这就表明，如果(a)不成立，则(c)也不成立，因此(c)⇒(a).

最后，显然(b)⇒(c). ■

我们特别注意定理中的(c)⇒(b)：

如果齐次线性方程组 $AX=0$ 只有平凡解，则对于任意列向量 B，一般方程组 $AX=B$ 有唯一解.

这非常有用，因为齐次方程组比一般方程组更容易处理.

【1.2.22】例　存在一个 n 次多项式 $p(t)$满足对于实直线上 $n+1$ 个不同[⊖]的实数 $t=a_0$，a_1，…，a_n有 $p(a_i)=b_i$. 要确定这个多项式，得解一个以 $p(t)$的待定系数所构成的线性方

⊖ 集合的诸元素中如果没有两个是相等的，则称集合的诸元素是不同的.

程组. 为了不用过多的记号，我们就次数是 2 的多项式举例说明. 令 $p(t)=x_0+x_1t+x_2t^2$. 令 a_0，a_1，a_2 和 b_0，b_1，b_2 已知，要解的方程由将 a_i 代替多项式中的 t 得到. 将多项式的系数 x_i 移到右边，得到方程组：

$$x_0+a_ix_1+a_i^2x_2=b_i,\quad i=0,1,2$$

这是一个由三个未知量 x_0，x_1，x_2 的三个线性方程组成的方程组 $AX=B$，其中

$$A=\begin{bmatrix}1 & a_0 & a_0^2\\ 1 & a_1 & a_1^2\\ 1 & a_2 & a_2^2\end{bmatrix}$$

齐次方程(其中 $B=0$)要求多项式有三个根 a_0，a_1，a_2. 而一个非零的二次多项式至多有两个根，所以齐次方程组只有平凡解. 因此，方程组对于任意指定的一组值 b_0，b_1，b_2 有唯一解.

顺便说一句，有一个公式叫拉格朗日插值公式，它明确地给出了多项式 $p(t)$ 的表达式. ■

第三节 矩阵的转置

在上一节中，为了求解线性方程组我们对矩阵进行了行变换. 我们也可以对矩阵施行
17 列变换来简化矩阵，显然会得到类似的结果.

矩阵的转置就是把行列互换. 一个 $m\times n$ 矩阵 A 的转置是一个 $n\times m$ 矩阵 A^t，由矩阵 A 按照对角线反射得到，即 $A^t=(b_{ij})$，其中 $b_{ij}=a_{ji}$. 例如，

$$\begin{bmatrix}1 & 2\\ 3 & 4\end{bmatrix}^t=\begin{bmatrix}1 & 3\\ 2 & 4\end{bmatrix}\quad 和\quad \begin{bmatrix}1 & 2 & 3\end{bmatrix}^t=\begin{bmatrix}1\\ 2\\ 3\end{bmatrix}$$

下面是转置矩阵的运算法则.

【1.3.1】 $(AB)^t=B^tA^t$，$(A+B)^t=A^t+B^t$，$(cA)^t=c\cdot A^t$，$(A^t)^t=A$

利用上面的第一个公式，可由关于左乘的相应事实得到关于右乘的事实. 用初等矩阵 E(1.2.4)右乘矩阵 A 的作用是下列的初等列变换：

【1.3.2】若初等矩阵第 i 行第 j 列元素是 a，就将第 i 列乘以 a 加到第 j 列上去，互换第 i 列与第 j 列，用非零标量 c 乘第 i 列.

注意在上述第一个运算中，下标 i，j 是(1.2.5a)中下标次序的颠倒.

第四节 行 列 式

每一个方阵 A 都有一个数与之对应，这个数称为行列式，记作 $\det A$. 本节定义行列式并推导它的性质.

1×1 矩阵的行列式就是其唯一的元素

【1.4.1】 $$\det[a]=a$$

2×2 矩阵的行列式为

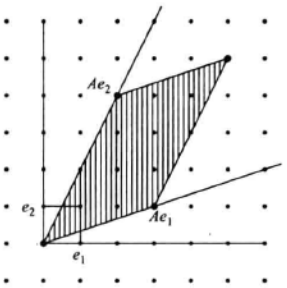
【1.4.2】
$$\det\begin{bmatrix} a & b \\ c & d \end{bmatrix} = ad - bc$$

2×2 矩阵 A 的行列式有一个几何解释. 左乘矩阵 A 将二维实向量空间的列向量映射到自身，在这个映射下单位方形的像所构成的平行四边形的面积是矩阵 A 的行列式的绝对值. 行列式值的正负取决于映射正方形的方向在作用后是保持还是相反. 而且，$\det A = 0$ 当且仅当平行四边形退化成一个线段或一个点，当矩阵的两列成比例时才会发生这种情形.

当矩阵为 $\begin{bmatrix} 3 & 2 \\ 1 & 4 \end{bmatrix}$ 时，下面给出了矩阵行列式的图示. 阴影部分是单位方形在映射下的像. 它的面积为 10.

这个几何解释延伸到高维空间. 用一个 3×3 矩阵 A 的左乘映射三维列向量空间 $\mathbf{R}^3$ 到自身，且它的行列式 $\det A$ 的绝对值是单位立方体映像的体积. 18

【1.4.3】图



全体 $n \times n$ 实矩阵构成一个 n^2 维向量空间，记作 $\mathbf{R}^{n\times n}$. 我们将 $n \times n$ 矩阵的行列式视为此空间到实数的一个函数：

$$\det : \mathbf{R}^{n\times n} \to \mathbf{R}$$

这意味着 $n \times n$ 矩阵的行列式是 n^2 个矩阵元素的函数. 对每一个正整数 n 有一个这样的函数. 有许多计算行列式的公式，可是，当 n 较大时它们全部都很复杂. 这些公式不仅复杂，而且也不容易直接证明两个公式定义的是同一个函数.

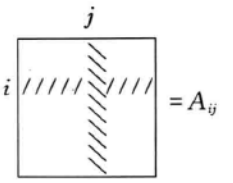
我们采用下面的策略：选择一个公式作为行列式的定义，这样，所讨论的是一个特定的函数. 我们证明所选择的函数是仅有的具有某些特殊性质的函数. 于是，要验证某个其他公式定义的是同一个行列式函数，只需证明它所定义的函数具有同样的性质. 这常常不是太难的.

一个 $n \times n$ 矩阵的行列式可根据某些 $(n-1)\times(n-1)$ 行列式用关于子式展开的过程计算. 一个矩阵的子矩阵的行列式叫做子式. 利用这种展开可给出行列式函数的一个递归定义.

递归这个词意味着一个 $n \times n$ 矩阵的行列式可以利用 $(n-1)\times(n-1)$ 矩阵的行列式来定义. 既然我们已经定义了 1×1 矩阵的行列式，就能够利用递归定义来计算 2×2 行列式，进而计算 3×3 行列式，等等.

设 A 是一个 $n \times n$ 矩阵，用 A_{ij} 表示在 A 中删去第 i 行与第 j 列得到的 $(n-1)\times(n-1)$ 子矩阵：

【1.4.4】



19

例如，若

$$A=\begin{bmatrix}1&0&3\\2&1&2\\0&5&1\end{bmatrix},\quad \text{则 } A_{21}=\begin{bmatrix}0&3\\5&1\end{bmatrix}$$

注 按第一列对子式展开为下述公式：

【1.4.5】 $$\det A=a_{11}\det A_{11}-a_{21}\det A_{21}+a_{31}\det A_{31}-\cdots\pm a_{n1}\det A_{n1}$$

符号是交错的，以正号开始.

这个展开式用求和记号表示为：

【1.4.6】 $$\det A=\sum_{\nu}\pm a_{\nu 1}\det A_{\nu 1}$$

交错符号可表示为$(-1)^{\nu+1}$，后面还会出现. 我们把这个公式和(1.4.1)都作为行列式的递归定义.

对于1×1和2×2矩阵，其行列式公式与(1.4.1)和(1.4.2)一致. 上面给出的3×3矩阵的行列式为

$$\det A=1\cdot\det\begin{bmatrix}1&2\\5&1\end{bmatrix}-2\cdot\det\begin{bmatrix}0&3\\5&1\end{bmatrix}+0\cdot\det\begin{bmatrix}0&3\\1&2\end{bmatrix}=1\cdot(-9)-2\cdot(-15)=21$$

后面将推出行列式的一些其他公式，包括按行和按列关于子式展开(参见本章第六节的定义).

知道行列式所满足的一些性质是重要的. 我们再次列出行列式的一些性质，其证明推迟到本节的最后. 为了能对除了行列式之外的其他函数应用这些性质，我们将这些性质按一般函数δ的性质给出.

【1.4.7】定理(行列式的唯一性) 在$n\times n$矩阵空间中存在唯一的函数δ且具有下面的性质，即矩阵的行列式(1.4.5)具有下面的性质.

(i) 用I表示恒等矩阵，则$\delta(I)=1$.

(ii) 函数δ对于矩阵A的各行是线性的.

(iii) 若矩阵A的两个相邻行相等，则$\delta(A)=0$.

函数δ对于矩阵A的各行是线性的是指：令A_i表示矩阵A的第i行，令A，B，D为三个矩阵，除去第k行外其他矩阵元素相同. 进一步假设矩阵D的第k行满足$D_k=cA_k+c'B_k$，其中c，c'是标量. 则$\delta(D)=c\delta(A)+c'\delta(B)$：

【1.4.8】 $$\delta\begin{bmatrix}\vdots\\cA_i+c'B_i\\\vdots\end{bmatrix}=c\delta\begin{bmatrix}\vdots\\-A_i-\\\vdots\end{bmatrix}+c'\delta\begin{bmatrix}\vdots\\-B_i-\\\vdots\end{bmatrix}$$

20

线性性质使我们能每次对一行进行处理而保持其他行不变. 例如，由于[0　2　3]=2[0　1　0]+3[0　0　1]，故

$$\delta\begin{bmatrix}1&&\\&2&3\\&&1\end{bmatrix}=2\delta\begin{bmatrix}1&&\\&1&\\&&1\end{bmatrix}+3\delta\begin{bmatrix}1&&\\&&1\\&&1\end{bmatrix}=2\cdot1+3\cdot0=2$$

也许行列式最重要的性质就是它与矩阵乘法的相容性.

【1.4.9】定理(行列式的乘法性质)　对于 $n\times n$ 矩阵 A，B，有 $\det(AB)=(\det A)\cdot(\det B)$.

下面的定理给出了行列式的加法性质，这些性质在(1.4.7)中已经列出.

【1.4.10】定理　令 δ 是满足性质(1.4.7)(i)、(ii)、(iii)的 $n\times n$ 矩阵 A 的行列式函数，则

(a) 如果矩阵 A' 是将矩阵 A 的第 j 行的倍数加到第 i 行上得到的矩阵，且 $i\neq j$，则 $\delta(A')=\delta(A)$.

(b) 如果矩阵 A' 是互换矩阵 A 的第 j 行与第 i 行得到的矩阵，且 $i\neq j$，则 $\delta(A')=-\delta(A)$.

(c) 如果矩阵 A' 是把矩阵 A 的第 i 行乘以标量 c 得到的矩阵，则 $\delta(A')=c\delta(A)$. 如果矩阵 A 的某一行全是零，则 $\delta(A)=0$.

(d) 如果矩阵 A 的第 i 行等于第 j 行的倍数，且 $i\neq j$，则 $\delta(A)=0$.

现在按相反的次序依次证明上述定理. 相当多的要点需要检验使得证明冗长，而这是不可避免的.

定理 1.4.10 的证明　结论(c)的第一部分是行的线性性质(1.4.7)(ii)的一部分. 结论(c)的第二部分是第一部分的直接结果，因为为零的行可用 0 乘而不改变矩阵，即当标量 c 取零时乘 $\delta(A)$ 的情形.

其次，我们证明性质(a)，(b)，(d)当 i 和 j 相邻的情形，比如令 $j=i+1$. 为使得证明简洁，我们将矩阵简略表示，记第 i 行为 R，记第 j 行为 S，且省略其他行，矩阵 A 记为 $\begin{bmatrix}R\\S\end{bmatrix}$，则由第 i 行的线性性质，得

【1.4.11】
$$\delta\begin{bmatrix}R+cS\\S\end{bmatrix}=\delta\begin{bmatrix}R\\S\end{bmatrix}+c\delta\begin{bmatrix}S\\S\end{bmatrix}$$

右边第一项是 $\delta(A)$，第二项是零(1.4.7). 这就证明了(a)对于相邻行的情形. 为了证明(b)，重复使用(a). R，S 如前所述：

【1.4.12】
$$\delta\begin{bmatrix}R\\S\end{bmatrix}=\delta\begin{bmatrix}R-S\\S\end{bmatrix}=\delta\begin{bmatrix}R-S\\S+(R-S)\end{bmatrix}=\delta\begin{bmatrix}R-S\\R\end{bmatrix}=\delta\begin{bmatrix}-S\\R\end{bmatrix}=-\delta\begin{bmatrix}S\\R\end{bmatrix}$$

最后，(d)对于相邻行成立由(c)和(1.4.7)(iii)得到.

要完成证明，我们要证明对于任意不同的行(a)，(b)，(d)成立. 设第 i 行是第 j 行的倍数. 我们反复交换相邻两行可以得到两个相邻行成比例的情形，记这个矩阵为 A'，则(d)对于相邻行的结论告诉我们 $\delta(A')=0$，且(b)关于相邻行的结论告诉我们

21

$\delta(A')=\pm\delta(A)$，所以 $\delta(A)=0$，这就证明了(d). 至此，(a)和(b)对于相邻行的结论的证明推广到了任意行的情形. ■

定理 1.4.10 中的规则(a)，(b)，(c)表明了用一个初等矩阵去乘一个矩阵如何影响行列式函数 δ，从而得到下面的推论.

【1.4.13】推论 *令 δ 是 $n\times n$ 矩阵的行列式函数且具有性质(1.4.7)，令 E 是初等矩阵. 对于任意矩阵 A，$\delta(EA)=\delta(E)\delta(A)$，而且，*

(i) 如果 E 是第一类初等矩阵(将一行的倍数加到另一行上去)，则 $\delta(E)=1$.

(ii) 如果 E 是第二类初等矩阵(互换两行)，则 $\delta(E)=-1$.

(iii) 如果 E 是第三类初等矩阵(某一行乘上 c)，则 $\delta(E)=c$.

证明 定理 1.4.10 中的规则(a)，(b)，(c)描述了初等行变换对矩阵行列式 $\delta(A)$ 的影响，它们告诉了如何从 $\delta(A)$ 计算 $\delta(EA)$. 于是，$\delta(EA)=\delta(E)\delta(A)=\varepsilon\delta(A)$，此处根据初等矩阵的类型，$\varepsilon=1$，$-1$ 或 c. 令 $A=I$，则 $\delta(E)=\delta(EI)=\delta(E)\delta(I)=\varepsilon\cdot\delta(I)=\varepsilon$. ■

乘法性质的证明(定理 1.4.9) 我们把第一步想象为矩阵 A 的行约简，例如 $EA=A'$. 假设已经证明了 $\delta(A'B)=\delta(A')\delta(B)$. 应用推论 1.4.13：$\delta(E)\delta(A)=\delta(A')$. 由 $A'B=E(AB)$，由推论得 $\delta(A'B)=\delta(E)\delta(AB)$，因此

$$\delta(E)\delta(AB)=\delta(A'B)=\delta(A')\delta(B)=\delta(E)\delta(A)\delta(B)$$

消去 $\delta(E)$，我们看到乘法性质对于矩阵 A，B 也成立. 情况既然如此，由归纳法只要证明对于行约简的矩阵 A 乘法性质成立即可. 设 A 是行约简的矩阵，则 A 或者是恒等矩阵或者最下面一行为零. 显然当 A 是恒等矩阵时，乘法性质成立. 而当 A 的最下面一行为零时，AB 的最下面一行也是零. 定理 1.4.10 表明 $\delta(A)=\delta(AB)=0$. 乘法性质在此情形也成立. ■

行列式的唯一性的证明(定理 1.4.7) 证明分两部分. 为证明唯一性，对矩阵 A 施行行约简，得 $A'=E_kE_{k-1}\cdots E_1A$. 推论 1.4.13 给出了从 $\delta(A')$ 计算 $\delta(A)$ 的方法. 若 A' 是恒等矩阵，则 $\delta(A')=1$. 否则 A' 的最后一行为零，对于这种情形，定理 1.4.10 证明了
22 $\delta(A')=0$. 两种情形下的 $\delta(A)$ 计算就解决了.

注意 *试图用乘法的相容性和推论 1.4.13 来定义行列式是个很自然的想法. 由于我们可以把一个可逆矩阵写成初等矩阵的乘积，因此这些性质定义了每个可逆矩阵的行列式. 但有多种方式把一个给定的矩阵表示成初等矩阵的乘积. 如果不通过上面证明中的步骤，我们并不清楚两个不同的乘积是否给出相同的行列式. 实际上要使这种想法得以实现并不容易.*

要完成定理 1.4.7 的证明，我们必须证明所定义的行列式函数(1.4.5)具有性质(1.4.7). 对矩阵的阶数 n 应用数学归纳法来证明. 首先，性质(1.4.7)对 $n=1$ 成立，此时，$\det[a]=a$. 假设对于 $(n-1)\times(n-1)$ 矩阵我们已经证明了其行列式具有此性质. 这样，所有性质(1.4.7)，(1.4.10)，(1.4.13)和(1.4.9)对于 $(n-1)\times(n-1)$ 矩阵成立. 对于 $n\times n$ 矩阵的行列式，由行列式的定义(1.4.5)来验证(1.4.7)对于行列式函数 $\delta=\det$ 成

立．作为参考，它们是

(i) 用 I 表示恒等矩阵，$\det(I)=1$.

(ii) det 关于矩阵的行是线性的.

(iii) 若矩阵 A 的相邻两行相同，则行列式 $\det(A)=0$.

(i) 如果 $A=I$，则 $a_{11}=1$，$a_{\nu 1}=0$，$\nu>1$. 展开式(1.4.5)可简化为 $\det=1\cdot\det(A_{11})$，而且 $A_{11}=I_{n-1}$. 由归纳法，$\det(A_{11})=1$ 且 $\det(I_n)=1$.

(ii) 为证明行的线性性质，我们回到(1.4.8)引入的记号. 我们证明展开式(1.4.5)中每一项的线性性质，亦即

【1.4.14】
$$d_{\nu 1}\det(D_{\nu 1}) = ca_{\nu 1}\det(A_{\nu 1}) + c'b_{\nu 1}\det(B_{\nu 1})$$

对每一个下标 ν 成立. 令 k 如(1.4.8)中所示.

情形 1：$\nu=k$. 我们变换的行已经从子式 A_{k1}，B_{k1}，D_{k1} 中去掉，所以它们相等，且它们的行列式的值也相等. 另一方面，a_{k1}，b_{k1}，d_{k1} 分别是行 A_k，B_k，D_k 的第一个元素. 于是，

$$d_{k1} = ca_{k1} + c'b_{k1}$$

且(1.4.14)成立.

情形 2：$\nu\neq k$. 如果用 A'_k，B'_k，D'_k 表示分别从行 A_k，B_k，D_k 通过去掉第一个元素得到的向量，则 A'_k 是子式 $A_{\nu 1}$ 的行，等等. 这里 $D'_k=cA'_k+c'B'_k$，对 n 用归纳法，

$$\det(D'_{\nu 1}) = c\det(A'_{\nu 1}) + c'\det(B'_{\nu 1})$$

另一方面，因为 $\nu\neq k$，所以系数 $a_{\nu 1}$，$b_{\nu 1}$，$d_{\nu 1}$ 是相等的. 所以，(1.4.14)在这种情形也成立.

(iii) 假设矩阵 A 的 k 行和 $k+1$ 行是相等的. 除非 ν 等于 k 或 $k+1$，否则子式 $A_{\nu 1}$ 有两行相等，且由归纳法，它的行列式为零. 所以，(1.4.5)里至多两项不同于零. 另一方面，去掉相等行的任一行给出同一个矩阵. 所以，$a_{k1}=a_{k+11}$，$A_{k1}=A_{k+11}$. 这样，

$$\det(A) = \pm a_{k1}\det(A_{k1}) \mp a_{k+11}\det(A_{k+11}) = 0$$

这就完成了定理 1.4.7 的证明. ■ 23

【1.4.15】**推论**

(a) 一个方阵 A 是可逆的当且仅当它的行列式不同于零. 如果 A 是可逆的，则

$$\det(A^{-1}) = (\det A)^{-1}$$

(b) 矩阵 A 的行列式与其转置矩阵 A^t 的行列式相等.

(c) 如果把行换成列，性质(1.4.7)和(1.4.10)仍成立.

证明

(a) 如果 A 是可逆的，则它是初等矩阵的乘积，比如说，$A=E_1E_2\cdots E_r$(1.2.16). 这样，$\det A=(\det E_1)\cdots(\det E_r)$. 初等矩阵的行列式是非零的(1.4.13)，故 $\det A$ 是非零的. 若 A 是不可逆的，则存在初等矩阵 E_1，E_2，$\cdots E_r$ 使得矩阵 $A'=E_1E_2\cdots E_rA$ 的最下面一行为零(1.2.15). 这样，$\det A'=0$，从而 $\det A=0$. 如果 A 是可逆的，则 $\det(A^{-1})\det A=\det(A^{-1}A)=\det I=1$，所以，$\det(A^{-1})=(\det A)^{-1}$.

(b) 容易验证如果 E 是初等矩阵，则 $\det E=\det E^t$，若 A 是可逆的，记作 $A=E_1\cdots E_k$

如上. 则 $A^t=E_k^t\cdots E_1^t$，由乘法性质，$\det A=\det A^t$. 若 A 是不可逆的，则 A^t 也是不可逆的. 这样，$\det A$ 与 $\det A^t$ 均为零.

(c) 由(b)可得证. ■

第五节 置 换

一个集合 S 的置换是一个 S 到 S 的双射 p：

【1.5.1】 $$p:S\to S$$

【1.5.2】表

i	1	2	3	4	5
$p(i)$	3	5	4	1	2

展示了五个指标的集合{**1**，**2**，**3**，**4**，**5**}的置换：$p(1)=3$，等等. 这是一个双射，因为每一个指标在底行里恰好出现一次.

指标集{**1**，**2**，…，n}上所有置换的全体所构成的集合称为对称群，记作 S_n，将在第二章中讨论.

置换的这种定义的益处在于可以把置换的复合看成是函数的复合. 如果 q 是另一个置换，则先施行 p 置换再施行 q 置换意味着函数的复合 $q\circ p$. 复合称为积置换，记作 qp.

注意 人们有时候喜欢将指标 **1**，**2**，…，n 的一个置换看成是同一个指标集的元素按不同顺序排列，如同表(1.5.2)的底行所示. 这对我们并无益处. 在数学上，人们试图追踪一个元素连续施行两个或多个置换后的结果. 例如，我们想通过反复地对换指标得到一个置换. 除非全部列出来，否则追踪已经做的所有置换就变成了一场梦魇.

上面的表格太笨拙了. 循环记号更常用. 为了把上面的置换 p 用循环记号表示，我们
24 从任意一个指标开始，比如 **3**，继续下去：$p(3)=4$，$p(4)=1$ 且 $p(1)=3$. 这是三个指标串形成的置换的一个循环，记为

【1.5.3】 $$(3\ 4\ 1)$$

这个记号意义如下：指标 **3** 被映射为 **4**，指标 **4** 被映射为 **1**，括号的末端表示指标 **1** 被映回最前面的 **3**：

由于有三个指标，因此这是一个 3-循环.

同样，$p(2)=5$ 和 $p(5)=2$，用类似的记号，有两个指标形成 2-循环(**2 5**). 2-循环叫做对换.

置换 p 的循环表示就是把这些循环一个接一个写在一起：

【1.5.4】 $$p=(3\ 4\ 1)(2\ 5)$$

这个置换很容易从这个记号得到.

由于循环记号不是唯一的，因此循环记号稍显冗繁. 有两个理由. 首先，从异于 **3** 的

指标开始. 因此,

$$(3\ 4\ 1),(1\ 3\ 4)\quad 和\quad (4\ 1\ 3)$$

是同一个 3-循环的不同记号. 其次,在循环中指标的次序没有影响. 循环由指标集的互斥集合构成,可以任意顺序表示. 例如,可以有

$$p=(5\ 2)(1\ 3\ 4)$$

指标集(此处为 **1**, **2**, **3**, **4**, **5**)可以任意分组为循环,其结果是某个置换的循环记号. 例如,(**3 4**)(**2**)(**1 5**)表示这样的置换:交换两对指标,而 **2** 保持不变. 而 1-循环(即该指标保持不变)在循环记号中经常省略. 我们可以把这个置换记作(**3 4**)(**1 5**). 4-循环

【1.5.5】　　$$q=(1\ 4\ 5\ 2)$$

理解为没有出现的指标 **3** 是不变的. 因此,在一个置换的循环记号表示中,每个指标至多出现 1 次. (当然,这个约定是在指标集已知的情况下.)这个约定的唯一例外是恒等置换. 我们不愿采用空的符号来表示置换,因此恒等置换用 1 表示.

为了计算置换的乘积 qp,其中 p 和 q 如上,我们跟随这两个置换下的指标变化,但务必注意 qp 就是 $q\circ p$,"先施行 p,再施行 q". 故由于 p 将 **3**→**4** 且 q 将 **4**→**5**,qp 将 **3**→**5**. 不巧的是,我们在读循环的时候是从左向右,但施行置换时是从右向左以之字形方式. 这 25
需要花些时间去适应,但最终我们会习惯的. 这个乘积的结果是一个 3-循环:

$$qp=[\overset{后做这个}{(1\ 4\ 5\ 2)}]\circ[\overset{先做这个}{(3\ 4\ 1)(2\ 5)}]=(1\ 3\ 5)$$

缺失的指标 **2** 与 **4** 是固定不变的. 另一方面,

$$pq=(2\ 3\ 4)$$

置换的复合不满足交换律.

任何一个置换 p 都有一个伴随的置换矩阵 P. 用置换 p 的矩阵左乘一个向量 X 置换向量的元素.

例如,如果有三个指标,则和循环置换 $p=(1\ 2\ 3)$相应的矩阵 P 左乘列向量 X 的运算如下:

【1.5.6】　　$$PX=\begin{bmatrix}0&0&1\\1&0&0\\0&1&0\end{bmatrix}\begin{bmatrix}x_1\\x_2\\x_3\end{bmatrix}=\begin{bmatrix}x_3\\x_1\\x_2\end{bmatrix}$$

用矩阵 P 左乘就把向量 X 的第一个分量变成第二个分量,第二个分量变成第三个分量,以此类推.

详细写出任意置换的矩阵很重要,并验证相应于置换的乘积 pq 的矩阵是积矩阵 PQ. 和对换(**2 5**)相应的矩阵是一个第二类型的初等矩阵,即恒等矩阵交换两行得到的矩阵. 这一点容易看出. 但是对于一般的置换,确定其相应的矩阵就变得扑朔迷离.

注　为了具体地写出置换矩阵,最好使用 $n\times n$ 矩阵单位 e_{ij},第 i 行第 j 列元素为 1 而其他位置为 0,见以前(1.1.21)的定义. 和对称群 S_n 中的置换 p 相应的矩阵是

【1.5.7】 $$P = \sum_i e_{pi,i}$$

(为了使下标尽量紧凑，将 $p(i)$写成 pi.)

这个矩阵对向量 $X=\sum e_j x_j$ 的作用如下：

【1.5.8】 $$PX = \left(\sum_i e_{pi,i}\right)\left(\sum_j e_j x_j\right) = \sum_{i,j} e_{pi,i} e_j x_j = \sum_i e_{pi,i} e_i x_i = \sum_i e_{pi} x_i$$

运算由公式(1.1.25)得到. 当 $i\neq j$ 时，在双下标求和中的项 $e_{pi,i}e_j$ 为零.

26 为了把(1.5.8)右边表示为列向量，必须重新编号使得右边的标准基向量是正确的顺序，即 e_1，…，e_n 而不是置换后的顺序 e_{p1}，…，e_{pn}. 令 $pi=k$ 且 $i=p^{-1}k$. 则

【1.5.9】 $$\sum_i e_{pi} x_i = \sum_k e_k x_{p^{-1}k}$$

这是个令人费解的地方：置换 p 置换向量的第 i 个分量 x_i 对应于 p^{-1}置换指标.

例如，(1.5.6)中的 3×3 矩阵 P 是 $e_{21}+e_{32}+e_{13}$，且

$$PX = (e_{21}+e_{32}+e_{13})(e_1x_1+e_2x_2+e_3x_3) = e_1x_3+e_2x_1+e_3x_2$$

【1.5.10】命题

(a) 一个置换矩阵 P 的每一行和每一列只有一个 1，其余元素全是 0. 反过来，这样的矩阵是一个置换矩阵.

(b) 置换矩阵的行列式为 ± 1.

(c) 令 p 和 q 是两个置换，相应的置换矩阵为 P 和 Q. 则置换 pq 的相应的矩阵为矩阵 P 和 Q 的积矩阵.

证明 我略去(a)和(b)的证明. (c)用下面的计算证明：

$$PQ = \left(\sum_i e_{pi,i}\right)\left(\sum_j e_{qj,j}\right) = \sum_{i,j} e_{pi,i}e_{qj,j}\sum_j e_{pqj,qj}e_{qj,j} = \sum_j e_{pqj,j}$$

计算由公式(1.1.23)可得. 在双下标求和中的项 $e_{pi,i}e_{qj,j}$ 为零除非 $i=qj$. 故 PQ 是相应于置换的乘积 pq 的矩阵. ■

注 相应于置换 p 的矩阵的行列式称为置换 p 的符号：

【1.5.11】 $$\operatorname{sign} p = \det P = \pm 1$$

一个置换是偶置换如果其符号是 +1，是奇置换如果符号是 −1. 置换(**1 2 3**)带符号 +1，为偶置换. 而任何对换，例如(**1 2**)，带符号 −1，是奇置换.

每个置换可有多种方式写成对换的乘积. 如果一个置换 p 等于 k 个对换 $\tau_1\cdots\tau_k$ 的乘积，其中 τ_i 是对换，则数 k 永远是偶数，如果 p 是偶置换；数 k 永远是奇数，如果 p 是奇置换.

至此便完成了对置换和置换矩阵的讨论. 在第七章和第十章还会回来讨论置换问题.

第六节 行列式的其他公式

有类似行列式定义(1.4.5)的公式，既有按列用子式展开行列式的公式，也有用子式

27 按行展开来计算行列式的公式.

仍用记号 A_{ij} 代表从矩阵 A 中删除第 i 行第 j 列后得到的矩阵.

用子式按照第 j 列展开的展开式：

$$\det A = (-1)^{1+j}a_{1j}\det A_{1j} + (-1)^{2+j}a_{2j}\det A_{2j} + \cdots + (-1)^{n+j}a_{nj}\det A_{nj}$$

或以求和记号表示：

【1.6.1】
$$\det A = \sum_{\nu=1}^{n}(-1)^{\nu+j}a_{\nu j}\det A_{\nu j}$$

用子式按照第 i 行展开的展开式：

$$\det A = (-1)^{i+1}a_{i1}\det A_{i1} + (-1)^{i+2}a_{i2}\det A_{i2} + \cdots + (-1)^{i+n}a_{in}\det A_{in}$$

【1.6.2】
$$\det A = \sum_{\nu=1}^{n}(-1)^{i+\nu}a_{i\nu}\det A_{i\nu}$$

例如，按照第二行展开得：

$$\det\begin{bmatrix}1 & 1 & 2\\ 0 & 2 & 1\\ 1 & 0 & 2\end{bmatrix} = -0\det\begin{bmatrix}1 & 2\\ 0 & 2\end{bmatrix} + 2\det\begin{bmatrix}1 & 2\\ 1 & 2\end{bmatrix} - 1\det\begin{bmatrix}1 & 1\\ 1 & 0\end{bmatrix} = 1$$

为了验证这些公式得到行列式，可以验证性质(1.4.7).

出现在公式中的交错的正负号可从下图中读出：

【1.6.3】
$$\begin{bmatrix}+ & - & + & \cdots\\ - & + & - & \\ + & - & + & \\ \vdots & & & \ddots\end{bmatrix}$$

表示交错符号的记号 $(-1)^{i+j}$ 看上去似乎是学究式的，不如上面的图容易记忆. 然而，这个记号是有用的，因为它是以代数规则确定的.

我们给出行列式的另一个表达式，即完全展开式. 完全展开式是利用线性性质按行展开的，先按第一行展开，然后按第二行展开，以此类推. 对于一个 2×2 矩阵，展开式如下：

$$\begin{aligned}\det\begin{bmatrix}a & b\\ c & d\end{bmatrix} &= a\det\begin{bmatrix}1 & 0\\ c & d\end{bmatrix} + b\det\begin{bmatrix}0 & 1\\ c & d\end{bmatrix}\\ &= ac\det\begin{bmatrix}1 & 0\\ 1 & 0\end{bmatrix} + ad\det\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} + bc\det\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} + bd\det\begin{bmatrix}0 & 1\\ 0 & 1\end{bmatrix}\end{aligned}$$

28

展开式中的第一项和第四项为零，且

$$\det\begin{bmatrix}a & b\\ c & d\end{bmatrix} = ad\det\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} + bc\det\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} = ad - bc$$

对于 $n\times n$ 矩阵作完全展开得到行列式的完全展开式，即公式

【1.6.4】
$$\det A = \sum_{\mathrm{perm}\,p}(\mathrm{sign}\,p)a_{1,p1}\cdots a_{n,pn}$$

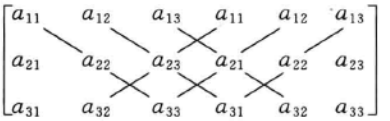
其中和是关于 n 个下标的所有置换的全体进行的，符号 $(\mathrm{sign}\,p)$ 是置换的符号.

对于 2×2 矩阵，完全展开式给出了公式(1.4.2)．对于一个 3×3 矩阵，完全展开式有 6 项，因为三个下标的置换共有 6 个：

【1.6.5】 $$\det A = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31}$$

为了帮助记忆这个展开式，下面给出一个矩阵块$[A\,|\,A]$：

【1.6.6】



三个带正号的项是从左上向右下的三条对角元素的乘积，而三个带负号的项是从右下到左上的对角元素的乘积．

注意 *类似的方法对于 4×4 行列式不成立．*

完全展开式较实际应用更具理论价值．除非 n 很小或者矩阵很特殊我们才用完全展开式来计算行列式，否则会因为项数太多而不便计算．完全展开式的理论意义在于行列式表示为一个以矩阵中的元素 a_{ij} 为变量的 n^2 个变量的多项式，其系数为 ± 1．例如，若矩阵中的每一个元素 a_{ij} 是关于变量 t 的可导函数，则可导函数的和与积仍然是可导函数，$\det A$ 也是 t 的可导函数．

余子式矩阵

一个 $n\times n$ 矩阵 A 的余子式矩阵仍然是一个 $n\times n$ 矩阵 $\mathrm{cof}(A)$，它的第 i 行第 j 列元素是

29 【1.6.7】 $$\mathrm{cof}(A)_{ij} = (-1)^{i+j}\det A_{ji}$$

其中 A_{ji} 是去掉第 j 行第 i 列后得到的矩阵．故余子式矩阵是矩阵 A 的$(n-1)\times(n-1)$子式带上(1.6.3)中的正负号构成的矩阵的转置．这个矩阵提供了求逆矩阵的公式．

要计算余子式矩阵，最安全的办法是将计算分为三个步骤：首先计算矩阵 A_{ij} 的行列式 $\det A_{ij}$，再加上正负号，最后转置．下面是计算一个特定的 3×3 矩阵的余子式矩阵：

【1.6.8】 $$A = \begin{bmatrix}1&1&2\\0&2&1\\1&0&2\end{bmatrix}:\ \begin{bmatrix}4&-1&-2\\2&0&-1\\-3&1&2\end{bmatrix},\ \begin{bmatrix}4&1&-2\\-2&0&1\\-3&-1&2\end{bmatrix},\ \begin{bmatrix}4&-2&-3\\1&0&-1\\-2&1&2\end{bmatrix} = \mathrm{cof}(A)$$

【1.6.9】定理 *令 A 是一个 $n\times n$ 矩阵，$C=\mathrm{cof}(A)$ 是其余子式矩阵，且令 $\alpha=\det A$．如果 $\alpha\neq 0$，则 A 是可逆矩阵，且 $A^{-1}=\alpha^{-1}C$．无论 A 是否可逆，总有 $CA=AC=\alpha I$．*

此处 αI 是对角线元素均为 α 的对角矩阵．对于一个 2×2 矩阵的逆，定理给出了前面得到的公式(1.1.17)．上面(1.6.8)中计算了一个 3×3 矩阵 A 的余子式矩阵，矩阵 A 的行列式恰好为 1，故其余子式矩阵与其逆矩阵相同，即 $A^{-1}=\mathrm{cof}(A)$．

定理 1.6.9 的证明 我们证明矩阵乘积 CA 中第 i 行第 j 列元素在 $i=j$ 时为 α，在 $i\neq j$ 时为 0．令 A_i 表示矩阵 A 的第 i 列．记 C 和 A 的元素为 c_{ij} 和 a_{ij}，则乘积 CA 的第 i 行第 j 列的元素为

【1.6.10】
$$\sum_{\nu} c_{i\nu} a_{\nu j} = \sum_{\nu} (-1)^{\nu+i} \det A_{\nu i} a_{\nu j}$$

当 $i=j$ 时，这是公式(1.6.1)对于行列式按照第 j 列的子式展开. 故如所断言的那样，CA 的对角线元素均为 α.

假设 $i\neq j$，我们以下面的方式构造一个新矩阵 M：M 的元素和 A 的元素除去第 i 列外是相同的. M 的第 i 列 M_i 等于 A 的第 j 列 A_j. 因此，M 的第 i 列与第 j 列都是 A_j，故 $\det M=0$.

令 D 是 M 的余子式矩阵，其元素记为 d_{ij}. DM 的第 i 行第 j 列的元素是

$$\sum_{\nu} d_{i\nu} m_{\nu i} = \sum_{\nu} (-1)^{\nu+i} \det M_{\nu i} m_{\nu i}$$

这个和等于 $\det M$，为零.

另一方面，由于在形成 $M_{\nu i}$ 时 M 的第 i 列被删掉了，因此子式等于 $A_{\nu i}$. 又由于 M 的第 i 列等于 A 的第 j 列，所以，DM 的第 i 行第 j 列的元素也等于

$$\sum_{\nu} (-1)^{\nu+i} \det A_{\nu i} a_{\nu j}$$

30

这就是我们要确定的 CA 的第 i 行第 j 列的元素. 因此，CA 的第 i 行第 j 列的元素为零，且 $CA=\alpha I$. 故如果 $\alpha\neq 0$，则 $A^{-1}=\alpha^{-1}\mathrm{cof}(A)$. 类似地，积 AC 用子式按行展开来计算. ■

一个表为展开形式的一般代数行列式
也许就像看似均匀的多种液体的混合物一样，由于沸点不同，
可以用分部蒸馏法加以分离.

——James Joseph Sylvester

练　习

第一节　基本运算

1.1　矩阵 $A=\begin{bmatrix}1 & 2 & 5\\ 2 & 7 & 8\\ 0 & 9 & 4\end{bmatrix}$ 的元素 a_{21} 和 a_{23} 是什么？

1.2　对于下列矩阵 A，B，计算积 AB 和 BA.

$$A=\begin{bmatrix}1 & 2 & 3\\ 3 & 3 & 1\end{bmatrix},\quad B=\begin{bmatrix}-8 & -4\\ 9 & 5\\ -3 & -2\end{bmatrix};\quad A=\begin{bmatrix}1 & 4\\ 1 & 2\end{bmatrix},\quad B=\begin{bmatrix}6 & -4\\ 3 & 2\end{bmatrix}$$

1.3　令 $A=[a_1\cdots a_n]$ 是一个行向量，令 $B=\begin{bmatrix}b_1\\ \vdots\\ b_n\end{bmatrix}$ 是一个列向量. 计算积 AB 和 BA.

1.4　验证矩阵乘法的结合律 $\begin{bmatrix}1 & 2\\ 0 & 1\end{bmatrix}\begin{bmatrix}0 & 1 & 2\\ 1 & 1 & 3\end{bmatrix}\begin{bmatrix}1\\ 4\\ 3\end{bmatrix}$.

注意：这是一个自验证问题．你必须乘对了，否则结果出不来．若你需要练习更多矩阵乘法，可以以本题为模型．

⊖1.5 令矩阵 A，B，C 的大小分别为 $\ell\times m$，$m\times n$ 和 $n\times p$．要计算乘积 AB 需要计算多少次乘法？乘积 ABC 以怎样的顺序运算才能使所做乘法的数量最小？

1.6 计算 $\begin{bmatrix}1 & a\\ & 1\end{bmatrix}\begin{bmatrix}1 & b\\ & 1\end{bmatrix}$ 和 $\begin{bmatrix}1 & a\\ & 1\end{bmatrix}^n$．

1.7 求计算 $\begin{bmatrix}1 & 1 & 1\\ & 1 & 1\\ & & 1\end{bmatrix}^n$ 的公式，并用归纳法证明该公式．

31

1.8 计算下面的分块矩阵的乘积：

$$\left[\begin{array}{cc|cc}1&1&1&5\\0&1&0&1\\\hline1&0&0&1\\0&1&1&0\end{array}\right]\left[\begin{array}{cc|cc}1&2&1&0\\0&1&0&1\\\hline1&0&0&1\\0&1&1&3\end{array}\right],\quad \left[\begin{array}{c|cc}0&1&2\\\hline0&1&0\\3&0&1\end{array}\right]\left[\begin{array}{c|cc}1&2&3\\\hline4&2&3\\5&0&4\end{array}\right]$$

1.9 令 A，B 是方阵．

(a) 何时有 $(A+B)(A-B)=A^2-B^2$？(b) 展开 $(A+B)^3$．

1.10 令 D 是对角线元素为 d_1，…，d_n 的对角矩阵，且 $A=(a_{ij})$ 是任意 $n\times n$ 矩阵．计算乘积矩阵 DA 和 AD.

1.11 证明上三角矩阵的乘积仍然是上三角矩阵．

1.12 在下面每一种情形，求与给定矩阵可交换的所有 2×2 矩阵．

(a) $\begin{bmatrix}1&0\\0&0\end{bmatrix}$ (b) $\begin{bmatrix}0&1\\0&0\end{bmatrix}$ (c) $\begin{bmatrix}2&0\\0&6\end{bmatrix}$ (d) $\begin{bmatrix}1&3\\0&1\end{bmatrix}$ (e) $\begin{bmatrix}2&3\\0&6\end{bmatrix}$

1.13 一个方阵 A 是幂零的，如果 $A^k=0$ 对于某个正整数 k 成立．证明：如果 A 是幂零的，则 $I+A$ 是可逆矩阵．用找出其逆矩阵的方法证明．

1.14 求出无限多个矩阵 B 使得 $BA=I_2$，其中

$$A=\begin{bmatrix}2&3\\1&2\\1&1\end{bmatrix}$$

并证明不存在矩阵 C 使得 $AC=I_3$．

1.15 A 为任意矩阵，确定乘积 $e_{ij}A$，Ae_{ij}，e_jAe_k，$e_{ii}Ae_{jj}$ 和 $e_{ij}Ae_{kl}$．

第二节 行约简

2.1 对(1.2.8)中给出的矩阵 M 的约简矩阵，确定每一个运算相应的初等矩阵．计算这些初等矩阵的乘积 P，并验证 PM 就是最终行约简的结果．

2.2 求方程组 $AX=B$ 的所有解，其中

$$A=\begin{bmatrix}1&2&1&1\\3&0&0&4\\1&-4&-2&2\end{bmatrix},\quad B=\text{(a)}\begin{bmatrix}0\\0\\0\end{bmatrix},\text{(b)}\begin{bmatrix}1\\1\\0\end{bmatrix},\text{(c)}\begin{bmatrix}0\\2\\2\end{bmatrix}$$

⊖ 由 Gilbert Strang 建议．

2.3　求出方程 $x_1+x_2+2x_3-x_4=3$ 的全部解.

2.4　确定在例(1.2.18)中矩阵行约简中所用到的初等矩阵，并验证这些初等矩阵的乘积是 A^{-1}.

32

2.5　求下列矩阵的逆矩阵：

$$\begin{bmatrix} & 1 \\ 1 & \end{bmatrix},\ \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix},\ \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix},\ \begin{bmatrix} & 1 \\ 1 & \end{bmatrix},\ \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix}$$

2.6　下面的矩阵是基于帕斯卡三角形. 求其逆矩阵.

$$\begin{bmatrix} 1 & & & & \\ 1 & 1 & & & \\ 1 & 2 & 1 & & \\ 1 & 3 & 3 & 1 & \\ 1 & 4 & 6 & 4 & 1 \end{bmatrix}$$

2.7　画出矩阵 $A=\begin{bmatrix} 2 & -1 \\ 2 & 3 \end{bmatrix}$ 在平面 $\mathbf{R}^2$ 上的乘积的作用效果的草图.

2.8　证明：如果两个 $n\times n$ 矩阵的乘积 AB 是可逆的，则因子 A，B 都是可逆的.

2.9　考虑任意的线性方程组 $AX=B$，其中 A，B 是实矩阵，

(a) 证明：如果方程组有多于一个的解，则方程组有无穷多组解.

(b) 证明：若在复数域有解，则也有实数解.

2.10　令 A 是方阵. 证明：若方程组 $AX=B$ 对某个指定的列向量 B 有唯一解，则对任意列向量 B，方程组 $AX=B$ 有唯一解.

第三节　矩阵的转置

3.1　一个矩阵 B 称为对称的，如果 $B=B^t$. 证明：对于任意方阵 B，BB^t 和 $B+B^t$ 是对称的，且如果 A 是可逆矩阵，则 $(A^{-1})^t=(A^t)^{-1}$.

3.2　令 A，B 是 $n\times n$ 对称矩阵. 证明其乘积 AB 是对称矩阵当且仅当 $AB=BA$.

3.3　假设对于矩阵 A 先做一次行变换，再做一次列变换. 解释如果把变换的次序倒过来，先做一次列变换，再做一次行变换会怎样.

3.4　如果行变换和列变换都可以使用，那么矩阵能简化到什么程度？

第四节　行列式

4.1　计算下列行列式：

(a) $\begin{bmatrix} 1 & i \\ 2-i & 3 \end{bmatrix}$　(b) $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$　(c) $\begin{bmatrix} 2 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 2 \end{bmatrix}$　(d) $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 5 & 2 & 0 & 0 \\ 8 & 6 & 3 & 0 \\ 0 & 9 & 7 & 4 \end{bmatrix}$

33

4.2　(自己验证)对于下列矩阵，验证行列式的乘法法则 $\det AB=(\det A)\cdot(\det B)$.

$$A=\begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix},\quad B=\begin{bmatrix} 1 & 1 \\ 5 & -2 \end{bmatrix}$$

4.3　对 n 用归纳法计算 $n\times n$ 矩阵的行列式：

$$\begin{bmatrix} 2 & -1 & & & & & \\ -1 & 2 & -1 & & & & \\ & -1 & 2 & -1 & & & \\ & & -1 & . & & & \\ & & & & . & & \\ & & & & & 2 & -1 \\ & & & & & -1 & 2 \end{bmatrix}$$

4.4 令 A 是一个 $n\times n$ 矩阵. 用 $\det A$ 表示 $\det(-A)$.

4.5 用行约简证明 $\det A^t=\det A$.

4.6 证明 $\det\begin{bmatrix} A & B \\ 0 & D \end{bmatrix}=(\det A)(\det D)$，如果 A 和 D 都是方块阵.

第五节 置换

5.1 将下列置换表示为互斥循环的乘积：

(1 2)(1 3)(1 4)(1 5)，**(1 2 3)(2 3 4)(3 4 5)**，**(1 2 3 4)(2 3 4 5)**，**(1 2)(2 3)(3 4)(4 5)(5 1)**.

5.2 令 p 是一个四元置换**(1 3 4 2)**.

(a) 求其相应的置换矩阵 P.

(b) 将 p 写成对换的乘积并计算相应的矩阵之积.

(c) 确定 p 的符号.

5.3 证明一个置换矩阵 p 的逆是其转置.

5.4 由 $p(i)=n-i+1$ 定义的 n 元置换的相应的置换矩阵是什么？p 的循环分解是什么？置换 p 的符号是什么？

5.5 在文中，置换(1.5.2)与(1.5.5)的积 qp 和 pq 看作是不同的. 然而，这两个乘积都是 3-循环的. 这是偶然的吗？

第六节 行列式的其他公式

6.1 (a) 利用按最后一行展开求下列行列式：

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix},\quad \begin{bmatrix} 1 & 1 & 2 \\ 2 & 4 & 2 \\ 0 & 2 & 1 \end{bmatrix},\quad \begin{bmatrix} 4 & -1 & 1 \\ 1 & 1 & -2 \\ 1 & -1 & 1 \end{bmatrix},\quad \begin{bmatrix} a & b & c \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

(b) 用完全展开式求这些矩阵的行列式.

(c) 计算这些矩阵的伴随矩阵，并由此验证定理 1.6.9.

6.2 令 A 是一个具有整数元素 a_{ij} 的 $n\times n$ 矩阵. 证明 A 是可逆的，且 A^{-1} 中的元素是整数当且仅当 $\det A=\pm 1$.

34

杂题

*M.1 令一个 $2n\times 2n$ 的矩阵由 $M=\begin{bmatrix} A & B \\ C & D \end{bmatrix}$ 形式给出，其中每个块都是 $n\times n$ 矩阵. 设 A 是可逆的且 $AC=CA$. 用块乘证明 $\det M=\det(AD-CB)$. 给出一个例子表明当 $AC\neq CA$ 时，这个公式未必成立.

M.2 令 A 是一个 $m\times n$ 矩阵且 $m<n$. 通过比较 A 和一个在 A 的底行添加 $n-m$ 行零所得到的 $n\times n$ 方阵

证明 A 没有左逆.

M. 3　一个方阵的迹(trace)是其对角线元素之和：

$$\text{trace}A = a_{11} + a_{22} + \cdots + a_{nn}$$

证明 $\text{trace}(A+B) = \text{trace}A + \text{trace}B$，且 $\text{trace}(AB) = \text{trace}(BA)$，若 B 是可逆的，则 $\text{trace}A = \text{trace}BAB^{-1}$.

M. 4　证明方程 $AB-BA=I$ 对于实 $n\times n$ 矩阵 A，B 没有解.

M. 5　将矩阵 $\begin{bmatrix}1 & 2\\ 3 & 4\end{bmatrix}$ 表示为尽量少的初等矩阵的乘积，并证明你的表示是最短的.

M. 6　求最小整数 n 使得每个可逆的 2×2 矩阵可写成不超过 n 个的初等矩阵的乘积.

M. 7　(*范德蒙德行列式*)

(a) 证明 $\det\begin{bmatrix}1 & 1 & 1\\ a & b & c\\ a^2 & b^2 & c^2\end{bmatrix} = (a-b)(a-c)(b-c)$.

(b) 对 $n\times n$ 矩阵证明类似的结论，用行变换把第一列除去第一个元素外清零的办法求行列式的值.

(c) 用范德蒙德行列式证明在任意 $n+1$ 个点 t_0，…，t_n 取任意指定的值的 n 次多项式 $p(t)$ 是唯一确定的.

*M. 8　(*一个关于逻辑的练习*)考虑 m 个线性方程 n 个未知量的方程组 $AX=B$，此处 m 和 n 未必相等. 系数矩阵 A 有左逆 L，使得 $LA=I_n$. 如果是这样，我们可以如在学校里学到的那样解方程组：

$$AX = B,\quad LAX = LB,\quad X = LB$$

但是当我们试图将解代回检验时，却遇到了麻烦：如果 $X=LB$，则 $AX=ALB$. 我们似乎希望 L 是一个右逆，而右逆并没有给出.

(a) 找出例子说明上面的验证有问题.

(b) 上面的证明步骤恰恰说明了什么？右逆的存在性说明什么？解释清楚.

M. 9　令 A 是一个 2×2 矩阵，且 A_1，A_2 是 A 的列. 令 P 是以原点 0 和 A_1，A_2，A_1+A_2 为顶点的平行四边形，确定初等行变换对 P 的面积的影响，并以此证明 A 的行列式的值 $|\det A|$ 等于 P 的面积. 35

*M. 10　令 A，B 是 $m\times n$ 和 $n\times m$ 矩阵. 证明 I_m-AB 是可逆的当且仅当 I_n-BA 是可逆的.

提示：也许目前你能寻求的证明途径就是用其他矩阵找出逆矩阵的具体表示式. 作为一个启发式的工具，你可以试一试代入 $(1-x)^{-1}$ 的幂级数展开式. 这个代换没有意义，除非某个级数收敛，且不需要这种情形. 但任何方法也是允许的，倘若以后你能验证你的猜测话.

㊀M. 11　(*离散狄利克雷问题*)函数 $f(u, v)$ 是调和函数，若它满足拉普拉斯方程 $\frac{\partial^2 f}{\partial u^2}+\frac{\partial^2 f}{\partial v^2}=0$. 狄利克雷问题要求平面区域 R 上的调和函数满足指定边界条件. 这个练习解决离散狄利克雷问题.

令 f 是一个实值函数，它的定义域是整数集合 $\mathbf{Z}$. 为了避开非对称性，离散导数定义为整数平移 $\mathbf{Z}+\frac{1}{2}$，作为一阶差分 $f'\left(n+\frac{1}{2}\right)=f(n+1)-f(n)$. 离散的二阶导数回到整数：$f''(n)=f'\left(n+\frac{1}{2}\right)-f'\left(n-\frac{1}{2}\right)=f(n+1)-2f(n)+f(n-1)$.

㊀ 我从 Peter Lax 那里学到了这个问题，他告诉我他是跟我父亲 Emil Artin 学的.

令函数 $f(u, v)$的定义域为平面上坐标为整数的格子点的全体. 离散二阶导数公式表明离散版的拉普拉斯公式是:

$$f(u+1,v)+f(u-1,v)+f(u,v+1)+f(u,v-1)-4f(u,v)=0$$

故 f 是调和函数, 如果它在点(u, v)处的函数值是它上下左右邻近四个点的函数值的平均值.

平面上一个**离散区域** R 是整数格子点的有限集合. 它的**边界** ∂R 是不属于 R 的格子点的集合, 但 ∂R 和 R 的某些点之间的距离是 1. 我们称 R 是区域 $\overline{R}=R\cup\partial R$ 的**内部**. 设函数 β 在边界 ∂R 的定义已知. 离散狄利克雷问题要求一个定义在 $\overline{R}$ 上的函数 f 使其在边界上等于 β, 在内部的所有点处满足离散拉普拉斯方程. 这个问题导致了一个线性方程组, 简记为 $LX=B$. 为建立这个方程组, 记 β_{uv} 为函数 β 在边界上的值. 故对于边界点(u, v), $f(u, v)=\beta_{uv}$. 令 x_{uv} 表示函数 $f(u, v)$ 在 R 上点(u, v)处的未知值. 我们将 R 上的点任意排序, 并将未知值 x_{uv} 排成列向量 X. 系数矩阵 L 表示离散拉普拉斯方程, 除去这个点是某个边界点的邻近点的情形, 相应的项是给定的边界点的值. 这些项移到方程的右边形成向量 B.

(a) 当 R 是五个点$(0, 0)$, $(0, \pm1)$, $(\pm1, 0)$的集合时, 有八个边界点. 写出此情形下的线性方程组, 并求解狄利克雷问题, 其中 β 是定义在边界 ∂R 上的函数且如果 $v\leqslant 0$, $\beta_{uv}=0$; 如果 $v>0$, $\beta_{uv}=1$.

(b) **最大值原理**指出调和函数的最大值在边界上取得. 对离散调和函数证明最大值原理.

36 (c) 证明离散狄利克雷问题对每一个区域 R 和每一个边界函数 β 有唯一解.

第二章　群

在数学中没有几个概念比合成法则更加本质.

——Nicolas Bourbaki

第一节　合成法则

集合 S 上的合成法则就是将 S 中的元素 a，b 结合成另外一个元素，比如说 p. 这个概念的模型是实数的加法和乘法. $n\times n$ 矩阵集合上的乘法是另一个例子.

规范地，合成法则是一个有两个变量的函数或映射：

$$S\times S\to S$$

此处 $S\times S$ 表示集合的积集，它的元素是集合 S 中的元素对.

合成法则作用在元素对 a，b 上所得到的元素通常用类似乘法或加法的记号表示：

$$p=ab, a\times b, a\circ b, a+b$$

或者其他什么符号，具体使用什么符号依所讨论的问题而定. 元素 p 可以叫做 a，b 的积或和，这取决于所采用的记号是乘还是加.

多数情形我们采用乘法记号 ab. 任何采用乘法记号的结果都可以用其他符号(如加法等)改写，结果同样成立. 改写只是个记号变化.

现在就把 ab 看成集合 S 上的某个特定元素，即由 S 中的元素 a，b 应用合成法则得到的. 因此，如果合成法则是矩阵的乘法，且如果 $a=\begin{bmatrix}1&3\\0&2\end{bmatrix}$，$b=\begin{bmatrix}1&0\\2&1\end{bmatrix}$，则 ab 表示矩阵 $\begin{bmatrix}7&3\\4&2\end{bmatrix}$. 一旦计算出积 ab，那么 a，b 就不能从积中复原.

用乘法记号，合成法则的结合律是指：

【2.1.1】　　$(ab)c=a(bc)$　　(结合律)

对于 S 中的任意 a，b，c 成立. 此处 $(ab)c$ 是指先算 a 与 b 的乘积 ab，再计算 ab 与 c 的乘积. 合成法则的交换律是指：

【2.1.2】　　$ab=ba$　　(交换律)

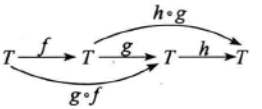
对于 S 中的任意 a，b 成立. 矩阵乘法满足结合律但不满足交换律.

通常用改变 a，b 在加法 $a+b$ 中的顺序来表示交换律，即 $a+b=b+a$ 对任意 a，b 成立. 乘法记号对于交换律没有特别的含义.

结合律比交换律更基础，一个原因是函数的复合满足结合律. 令 T 是一个集合，g 和 f 是 T 到 T 的映射(或者函数)，令 $g\circ f$ 表示复合映射 $t\rightsquigarrow g(f(t))$：先用 f 作用再用 g 作用. 规则

$$g, f \rightsquigarrow g \circ f$$

是映射 $T \to T$ 的集合上的复合运算. 该复合运算满足结合律. 若 f, g 和 h 是 T 到 T 的三个映射, 则 $(h \circ g) \circ f = h \circ (g \circ f)$:



两个复合映射都把元素 t 映射为 $(h(g(f(t))))$.

当 T 只包含两个元素时, 比如 $T=\{a, b\}$, 则存在 T 到 T 的四个映射:

i: 恒等映射, 定义为 $i(a)=a$, $i(b)=b$;

τ: 对换, 定义为 $\tau(a)=b$, $\tau(b)=a$;

α: 常函数, $\alpha(a)=\alpha(b)=a$;

β: 常函数, $\beta(a)=\beta(b)=b$.

映射 $T \to T$ 的集合 $\{i, \tau, \alpha, \beta\}$ 上的合成法则由下面的乘法表给出:

【2.1.3】

	i	τ	α	β
i	i	τ	α	β
τ	τ	i	β	α
α	α	α	α	α
β	β	β	β	β

合成的方式如下:

	f
	⋮
g	$\cdots$ $g \circ f$

38

因此 $\tau \circ \alpha = \beta$, 而 $\alpha \circ \tau = \alpha$. 函数的复合不满足交换律.

回到一般的合成法则, 假设我们要求一个集合中 n 个元素的乘积 $a_1 a_2 \cdots a_n =$? 有许多种不同的方式计算这个乘积. 例如, 可以先求积 $a_1 a_2$, 然后再和第三个元素 a_3 相乘, 以此类推:

$$((a_1 a_2) a_3) a_4 \cdots$$

也有其他的方法给出按照指定顺序的这些元素的乘积. 但如果乘法运算满足结合律, 则所有计算结果都是 S 中的同一个元素. 这使得我们可以探讨任意元素串的乘积.

【2.1.4】命题 令集合 S 上的合成法则满足结合律. 则有唯一一种方式来定义 S 中任意 n 个元素 a_1, a_2, $\cdots a_n$ 的乘积, 暂时记作 $[a_1 a_2 \cdots a_n]$, 这个乘积具有以下性质:

(i) 一个元素的积是其自身: $[a_1]=a_1$.

(ii) 两个元素的积 $[a_1 a_2]$ 由合成法则给出.

(iii) 对于任意整数 i: $1 \leqslant i < n$, 有 $[a_1 a_2 \cdots a_n] = [a_1 \cdots a_i][a_{i+1} \cdots a_n]$.

方程(iii)右边是先算两个积$[a_1\cdots a_i]$和$[a_{i+1}\cdots a_n]$，然后这两个积再按照合成法则计算其乘积.

证明 对 n 用数学归纳法. (i)和(ii)已经定义了 $n\leqslant 2$ 的乘积. 当 $n=2$ 时(iii)成立. 假设当 $r\leqslant n-1$ 已经定义了 r 个元素的乘积且乘积是唯一的并满足(iii)，然后按照下面的规则定义 n 个元素的乘积：

$$[a_1\cdots a_n]=[a_1\cdots a_{n-1}][a_n]$$

其中右边的项已经定义好了. 如果满足(iii)的乘积存在，那么这个公式给出了积，这正是(iii)中当 $i=n-1$ 的情形. 故若 n 个元素的乘积存在，积就是唯一的. 我们必须检验(iii)对于 $i<n-1$ 成立.

$$\begin{aligned}
[a_1\cdots a_n] &= [a_1\cdots a_{n-1}][a_n] && \text{(定义)}\\
&= ([a_1\cdots a_i][a_{i+1}\cdots a_{n-1}])[a_n] && \text{(归纳假设)}\\
&= [a_1\cdots a_i]([a_{i+1}\cdots a_{n-1}][a_n]) && \text{(结合律)}\\
&= [a_1\cdots a_i][a_{i+1}\cdots a_n] && \text{(归纳假设)}
\end{aligned}$$

至此完成了证明. 从现在起，在表示乘积时将省去括号而直接记为 $a_1\cdots a_n$. ■

集合 S 中的元素 e 称为合成法则的恒等元，如果 e 满足

【2.1.5】 $$ea=a \text{ 与 } ae=a, \text{对所有 } a\in S$$

至多有一个恒等元，因为若 e 和 e' 是两个恒等元，则由于 e 是恒等元，故 $ee'=e'$，又有 e' 也是恒等元，故 $e=ee'$. 因此 $e=ee'=e'$.

矩阵乘法和函数的复合都有恒等元，对于 $n\times n$ 矩阵，它是恒等矩阵 I，对于 $T\to T$ 的映射集合，它是恒等映射——将元素映射为自身的映射是恒等映射. 39

注 如果合成法则用乘法表示，则恒等元通常用 1 来表示；如果合成法则用加法表示，则恒等元用 0 来表示. 这些元素与数字 1 和 0 无关，但是在合成法则中起到恒等元的作用.

假设集合 S 上定义了一个满足结合律且有恒等元 1 的合成法则，并记作乘法. S 中的元素 a 是可逆的如果存在另一个元素 b 使得

$$ab=1 \quad 与 \quad ba=1$$

且如果上式成立，则 b 称为 a 的逆. 元素 a 的逆记作 a^{-1}，或当合成法则用加法记时，逆记作 $-a$.

下面不加证明地列出了逆的性质. 除去最后一条性质外，其他性质在矩阵中已经讨论过. 作为最后一个性质的示例，参看练习 1.3.

- 如果 a 有左逆 l 和右逆 r，即 $la=1$ 和 $ar=1$，则 $l=r$，a 是可逆的，且 r 是其逆.
- 如果 a 是可逆的，则其逆是唯一的.
- 乘积的逆按照相反次序：如果 a 和 b 均可逆，则乘积 ab 可逆，且

$$(ab)^{-1}=b^{-1}a^{-1}$$

- 一个元素 a 可以有左逆或右逆，尽管它是不可逆的.

幂记号可以用于满足结合律的运算：当 $n>0$ 时，$a^n=a\cdots a$(n 个因子)，$a^{-n}=a^{-1}\cdots$

a^{-1}，且 $a^0=1$. 通常的幂运算律成立：$a^r a^s=a^{r+s}$，且$(a^r)^s=a^{rs}$. 当合成法则用加法表示时，幂运算记号 a^n 改用记号 $na=a+\cdots+a$.

除非合成法则满足交换律，否则不建议采用分式记号$\frac{a}{b}$，因为不知道这个分式记号所指的是 ba^{-1}还是 $a^{-1}b$，而这二者可以是不同的.

第二节 群与子群

一个群是一个带有下列性质的合成法则的集合 G：

- 合成法则满足结合律：$(ab)c=a(bc)$对 G 中任意 a，b，c 成立.
- G 包含单位元 1，使得对于 G 中任意元素 a 有 $1a=a1=a$.
- G 中任意元素 a 均有逆，即存在元素 b 使得 $ab=ba=1$.

阿贝尔群是合成法则交换的群.

例如，非零实数的集合按照乘法构成的群和实数集合按照加法构成的群都是阿贝尔群. 所有 $n\times n$ 可逆矩阵集合按照矩阵乘法合成法则构成一般线性群，但不是交换群，除非 $n=1$.

当满足复合运算律时，通常把表示该集合的群和该集合用同一个符号表示.

群 G 的阶是其包含的元素个数，通常记作 $|G|$：

40 【2.2.1】 $|G|=G$ 的元素个数，G 的阶

如果 G 的阶是有限的，则 G 称为有限群；否则称为无限群. 同样的术语适用于集合. 一个集合 S 的阶 $|S|$ 是 S 中所含的元素个数.

下面列出我们熟悉的一些无限交换群的记号：

【2.2.2】 $\mathbf{Z}^+$：整数集合，加法作为它的复合法则 — 整数加群，

$\mathbf{R}^+$：实数集合，加法作为它的复合法则 — 实数加群，

$\mathbf{R}^\times$：非零实数集合，乘法作为它的复合法则 — 实数乘法群，

$\mathbf{C}^+$，$\mathbf{C}^\times$：类似的群，用复数集合 $\mathbf{C}$ 代替实数集合 $\mathbf{R}$.

注意 也有用 $\mathbf{R}^+$ 来表示正实数集合的. 为了避免混淆，最好用记号$(\mathbf{R},+)$来表示实数加群，即具体地把合成法则表示出来. 但是，我们的记号更紧凑. 此外，用符号 $\mathbf{R}^\times$ 表示非零实数乘法构成的群. 所有实数在乘法下不构成群，因为 0 没有逆.

【2.2.3】命题(消去律) 令 a，b，c 是群 G 中的元素，群 G 的合成法则用乘法表示. 若 $ab=ac$或 $ba=ca$，则 $b=c$. 若 $ab=a$ 或 $ba=a$，则 $b=1$.

证明 $ab=ac$ 两边左乘 a^{-1}得到 $b=c$. 其他证明类似. ■

这个证明中用 a^{-1}左乘很关键. 若元素 a 不可逆，则消去律不一定成立. 例如，

$$\begin{bmatrix}1 & 1\\ & \end{bmatrix}\begin{bmatrix}1 & 1\\ 2 & \end{bmatrix}=\begin{bmatrix}1 & 1\\ & \end{bmatrix}\begin{bmatrix}3 & \\ & 1\end{bmatrix}$$

两个基本的群的例子是由前面讨论过的合成法则——矩阵乘法和函数的合成——通过把不可逆的元素去掉而得到.

注 $n\times n$ 一般线性群是由所有 $n\times n$ 可逆矩阵构成的群. 将它记为

【2.2.4】 $$GL_n = \{n\times n \text{ 可逆矩阵 } A\}$$

如果我们希望指出考虑的是实数矩阵还是复数矩阵，则把它们相应地记为 $GL_n(\mathbf{R})$ 或 $GL_n(\mathbf{C})$.

令 M 表示集合 T 到自身的映射的集合. 映射 $f: T\to T$ 有逆函数当且仅当它是一一映射. 这样的映射也称为 T 的一个置换. 置换的集合在映射合成法则下构成一个群. 如在第一章第五节中一样，置换的合成用乘法表示，即用 qp 表示 $q\circ p$.

注 指标集合 $\{\mathbf{1},\mathbf{2},\cdots,\boldsymbol{n}\}$ 的置换群称为对称群，记作 S_n:

【2.2.5】 $$S_n \text{ 是指标 } \mathbf{1},\mathbf{2},\cdots,\boldsymbol{n} \text{ 的置换群}$$ 41

n 个元素的集合共有 $n!$ (n 的阶乘 $=1\cdot 2\cdot 3\cdot\cdots\cdot n$) 个置换，所以对称群 S_n 是阶为 $n!$ 的有限群.

集合 $\{a, b\}$ 的置换由恒等置换 i 和对换 τ 构成，形成一个二阶群. 如果用 **1** 代替 a，用 **2** 代替 b，就得到二阶对称群 S_2. 实际上只有一个二阶群 G. 为了说明这一点，注意到群中有一个恒等元 1 和另一个元素 g. 群的乘法表中有 4 个元素 11，1g，g1 和 gg. 除去 gg，其他元素都由恒等元性质得出. 而且由消去律有 $gg\neq g$. 仅有一种可能，就是 $gg=1$. 故乘法表完全确定. 只有一个群运算律.

下面我们描述对称群 S_3. 这个群是六阶群，可以作为按照合成法则构成的最小的非交换群的例子. 后面会经常用到这个群. 为了刻画这个群，选取两个特殊的置换来表示其他的置换. 取循环置换(**1 2 3**)和对换(**1 2**)，并分别用 x 和 y 表示. 容易验证

【2.2.6】 $$x^3 = 1, y^2 = 1, yx = x^2y$$

利用消去律，可以看到 6 个元素 1，x，x^2，y，xy，x^2y 是不同的. 所以群 S_3 有 6 个元素:

【2.2.7】 $$S_3 = \{1, x, x^2; y, xy, x^2y\}$$

在以后，我们会把(2.2.6)和(2.2.7)作为对称群 S_3 的“一般表示”. 注意 S_3 不满足交换律，因为 $yx\neq xy$.

法则(2.2.6)也可直接验证，对 S_3 的计算有它们就足够了. 不断应用上面的法则，x，y 以及其逆的任意积都等于(2.2.7)中某个元素. 为此，用最后一个法则把所有出现的 y 移到右边，而用前面两个法则使其幂变小. 例如:

【2.2.8】 $x^{-1}y^3x^2y = x^2yx^2y = x^2(yx)xy = x^2(x^2y)xy = xyxy = x(x^2y)y = 1$

用这些法则可以写出 S_3 的乘法表. 因此，这些法则称为群的定义关系，我们会在第七章正式学习这一概念.

我们到此为止. S_n 的结构随着 n 的增加变得非常复杂.

一般线性群和对称群如此重要的一个原因，是许多其他群都作为子群包含在它们之中. 群 G 的子集 H 称为一个子群，如果它具有下列性质:

【2.2.9】

- 封闭性：若 $a\in H$ 并且 $b\in H$，则 $ab\in H$.
- 恒等元：$1\in H$.
- 逆元：若 $a\in H$，则 $a^{-1}\in H$.

对这些条件解释如下：第一个条件告诉我们可以用 G 上的合成法则在 H 上定义一个合
42 成法则，称为诱导法则. 第二个和第三个条件指出 H 关于这个诱导法则构成一个群. 注意，(2.2.9)提到了群定义中除了结合律的所有要点. 因为结合律自动地由 G 转移到 H，我们不需要再提及它.

注意

(i) 在数学上，学习每一个术语的定义非常重要. 有直觉是不够的. 例如2×2可逆上三角矩阵的集合 T 是一般的线性群 GL_2 的子群. 只有一种方法证明，就是回到定义. 确实 T 是 GL_2 的子集. 验证任意两个可逆上三角矩阵的乘积还是可逆上三角矩阵，恒等矩阵是上三角的，可逆上三角矩阵的逆矩阵还是上三角的可逆矩阵. 当然这些都容易验证.

(ii) 封闭性作为群的一个公理指的是群 G 中任意两个元素的乘积 ab 仍是群中的元素. 我们把封闭性包含在合成法则中. 这样在群的定义中就不必单独指出运算的封闭性了.

【2.2.10】**例**

(a) 绝对值为 1 的复数的集合——复平面的单位圆上点的集合——是乘法群 $\mathbf{C}^\times$ 的子群，称为圆群.

(b) 所有行列式为 1 的 $n\times n$ 实矩阵构成一般线性群 GL_n 的子群，称为特殊线性群，记为 SL_n：

【2.2.11】 $SL_n(\mathbf{R})$ 是所有行列式为 1 的实 $n\times n$ 矩阵 A 的集合

对于这个特殊线性群，定义(2.2.9)中的性质很容易验证，这里省去验证过程. ■

注 每个群 G 都有两个明显的子群：群 G 自身和由单独一个恒等元构成的平凡子群 $\{1\}$. 一个子群如果不是这两个子群之一，则称为真子群.

第三节 整数加群的子群

这里我们用整数加群 $\mathbf{Z}^+$ 的子群回顾一些基本的数论理论. 首先，列出群运算用加法表示时子群用到的公理：一个用加法表示合成法则的群 G 的子集 S 是一个子群，如果满足下列性质：

【2.3.1】

- 封闭性：如果 a，$b\in S$，则 $a+b\in S$；
- 单位元：$0\in S$；
- 逆元：若 $a\in S$，则 $-a\in S$.

令 a 是异于 0 的整数. 记由所有 a 的倍数构成的 $\mathbf{Z}$ 的子集为 $\mathbf{Z}a$：

【2.3.2】 $$\mathbf{Z}a=\{n\in\mathbf{Z}\mid \text{存在 } k\in\mathbf{Z},\text{使 } n=ka\}$$

43 这是整数加群 $\mathbf{Z}^+$ 的子群. 它的元素也可以描述为被 a 整除的整数.

【2.3.3】定理 令 S 是整数加群 $\mathbf{Z}^+$ 的子群. 则 S 或为平凡子群$\{0\}$，或是有形式 $\mathbf{Z}a$，其中 a 为 S 中最小正整数.

证明 令 S 是 $\mathbf{Z}^+$ 的一个子群. 则 $0\in S$. 如果 0 是 S 中唯一的元素，则 S 为平凡子群. 因而对这一情形结论成立. 否则，S 包含异于 0 的整数 n，且要么 n 是正数，要么 $-n$ 是正数. 由子群的第三个性质知：$-n\in S$. 故 S 含有正整数. 我们必须证明 $S=\mathbf{Z}a$，其中 a 为 S 中最小正整数.

首先证明 $\mathbf{Z}a$ 是 S 的子集，换句话说，$ka\in S$ 对于任意整数 k 成立. 如果 k 是正整数，则 $ka=a+a+\cdots+a$(k 项). 由于 $a\in S$，由子群的封闭性和归纳法知 $ka\in S$. 子群中元素的逆元仍属于 S，因此 $-ka\in S$. 最后，$0a=0\in S$.

其次，证明 S 是 $\mathbf{Z}a$ 的子集，即 S 中任意元素 n 是 a 的整数倍. 用带余除法，记 $n=qa+r$，其中 q，r 都是整数且余数 r 的取值范围为 $0\leqslant r<a$. 由于 $\mathbf{Z}a\subseteq S$，故 $qa\in S$，当然 $n\in S$. 因为 S 是子群，故也有 $r=n-qa\in S$. 现在，根据我们的选取，a 为 S 中最小正整数，而余数 r 满足 $0\leqslant r<a$. 因此，属于 S 的唯一余数是 0. 所以，$r=0$ 且 n 是 a 的整数倍数 qa. ■

这一刻画导致定理 2.3.3 在两个整数 a，b 生成的子群上的一个惊人的应用. 设 a 和 b 都非零整数. 由 a 和 b 的所有整数组合 $ra+sb$ 构成的集合

【2.3.4】 $$S=\mathbf{Z}a+\mathbf{Z}b=\{n\in Z\mid n=ra+sb,\text{其中 } r,s \text{ 是任意整数}\}$$

是 $\mathbf{Z}^+$ 的子群，这时子群被称为由 a，b 生成的子群，因为它是同时包含这两个元素的最小子群. 设 a，b 是不全为零的整数，故 S 不是平凡子群$\{0\}$. 定理 2.3.3 告诉我们存在某个正整数 d，使这个子群具有 $\mathbf{Z}d$ 的形式，它是能被 d 整除的整数的集合. 生成元 d 叫做 a 与 b 的最大公因数，原因在下面命题的(a)和(b)中给出. a 与 b 的最大公约数记作 $\gcd(a,b)$.

【2.3.5】命题 设 a，b 是不全为零的整数，并设 d 是 a 与 b 的最大公约数，且是生成子群 $S=\mathbf{Z}a+\mathbf{Z}b$ 的正整数，则有 $\mathbf{Z}d=\mathbf{Z}a+\mathbf{Z}b$. 则

(a) d 整除 a 与 b.

(b) 若整数 e 整除 a 和 b，则 e 整除 d.

(c) 存在整数 r 和 s，使 d 可以写为 $d=ra+sb$ 的形式.

证明 (c)部分是 d 属于 $\mathbf{Z}a+\mathbf{Z}b$ 的另一种说法. 其次，注意到 a，b 都在子群 $S=\mathbf{Z}d$ 中，因而 d 整除 a 与 b. 最后，若 e 是整除 a 和 b 的整数，则 e 整除整数 a 和 b 的线性组合 $ra+sb$. 由假设，$d=ra+sb$，故 e 整除 d. ■

注意 e 整除 a 和 b，则 e 整除任何具有形式 $ma+nb$ 的整数. 故(c)蕴含(b). 但(b)不蕴含(c). 正如我们将看到的，性质(c)是个功能强大的工具.

反复使用带余除法容易求得最大公约数. 例如，若 $a=314$，$b=136$，则

$$314=2\cdot 136+42,\quad 136=3\cdot 42+10,\quad 42=4\cdot 10+2$$

44

利用这些方程中的第一个，可以证明 314 和 136 的线性组合可以由 136 与 42 的线性组合来表示，反之亦然. 故 $\mathbf{Z}(314)+\mathbf{Z}(136)=\mathbf{Z}(136)+\mathbf{Z}(42)$，因此 $\gcd(314,136)=\gcd(136,42)$. 类似地，$\gcd(136,42)=\gcd(42,10)=\gcd(10,2)=2$. 故 314 与 136 的最大

公约数为 2. 这种求两个整数的最大公约数的迭代法叫做欧几里得算法.

如果给出了整数 a，b，则第二种求这两个数的最大公约数的方法是求得每一个整数的素整数分解，然后将所有公共的素因子收集起来. 命题 2.3.5 中的性质(a)和(b)用这种方法很容易验证. 但是没有定理 2.3.3，性质(c)，即由这种方法确定的最大公约数 d 是 a 和 b 的线性组合这个性质并不是显然的. 这里我们并不做进一步讨论. 在第十二章我们再回来讨论它.

两个非零整数 a 和 b 称为是*互素的*，如果仅有唯一的正整数 1 同时整除这两个数. 这样，它们的最大公约数是 1：$\mathbf{Z}a+\mathbf{Z}b=\mathbf{Z}$.

【2.3.6】推论 *一对整数 a 和 b 互素当且仅当存在整数 r 和 s 使得 $ra+sb=1$.*

【2.3.7】推论 *令 p 是一个素整数. 若 p 整除 a 与 b 的乘积 ab，则 p 整除 a 或者 p 整除 b.*

证明 假设素数 p 整除 ab，但不整除 a. p 仅有的正因子是 1 和 p. 因 p 不整除 a，故 $\gcd(a,\ p)=1$. 因此有整数 r 和 s 使得 $ra+sp=1$. 两边同乘以 b：$rab+spb=b$，注意到 p 整除 rab 和 spb，故 p 整除 b. ■

有一个与整数对 a，b 有关的 $\mathbf{Z}^+$ 的子群，即交集 $\mathbf{Z}a\cap\mathbf{Z}b$，它是包含在 $\mathbf{Z}a$ 和 $\mathbf{Z}b$ 中的整数的集合. 现在假设 a，b 均非零，则 $\mathbf{Z}a\cap\mathbf{Z}b$ 是一个子群. 它不是平凡子群$\{0\}$，因为它包含乘积 ab，而 ab 不是零. 故 $\mathbf{Z}a\cap\mathbf{Z}b$ 对于某个正整数 m 具有形式 $\mathbf{Z}m$. 这个整数 m 称为 a，b 的*最小公倍数*，记作 $\mathrm{lcm}(a,\ b)$，原因由下面的命题给出.

【2.3.8】命题 *令 a 和 b 是非零整数，且 m 是它们的最小公倍数——正整数生成子群 $S=\mathbf{Z}a\cap\mathbf{Z}b$. 故 $\mathbf{Z}m=\mathbf{Z}a\cap\mathbf{Z}b$. 则*

(a) *m 被 a 和 b 整除.*

(b) *如果 n 被 a 和 b 整除，则 n 被 m 整除.*

证明 上述两个断言均得证于事实：一个整数被 a 与 b 整除当且仅当这个整数属于集合 $\mathbf{Z}m=\mathbf{Z}a\cap\mathbf{Z}b$. ■

【2.3.9】推论 *令 $d=\gcd(a,\ b)$ 和 $m=\mathrm{lcm}(a,\ b)$ 分别是正整数对 a 与 b 的最大公约数和最小公倍数. 则 $ab=dm$.*

证明 由于 b/d 是一个整数，故 a 整除 ab/d. 类似地，b 整除 ab/d. 故 m 整除 ab/d，
45 且 dm 整除 ab. 其次，记 $d=ra+sb$. 则 $dm=ram+sbm$. 右边两项均能被 ab 整除，所以 ab 整除 dm. 由于 ab 和 dm 都是正数且相互整除，故 $ab=dm$. ■

第四节 循 环 群

现在看一个重要的抽象子群的例子，即由 G 中任意一个元素 x 生成的*循环子群*. 我们用乘法的记号，由 x 生成的循环子群 H 是 x 的所有幂的元素的集合：

【2.4.1】
$$H=\{\cdots,x^{-2},x^{-1},x,x^2,\cdots\}$$

它是 G 的包含 x 的最小子群，经常记作$\langle x\rangle$. 但是想正确地解释(2.4.1)，必须记住 x^n 是 G 中某个元素的记号，它是以某种特定方式得到的. 不同的幂可以表示同一个元素. 例如，若群 G 是乘法群 $\mathbf{R}^\times$，且 $x=-1$，则列出的所有元素都等于 1 或 -1，且 H 就是集合$\{1,\ -1\}$.

有两种情形：x 的幂 x^n 都是互不相同的元素，或不是互不相同的元素．我们分析 x 的幂都是互不相同的情形．

【2.4.2】命题 令 $\langle x\rangle$ 是群 G 的由元素 x 生成的循环子群，且令 S 表示满足 $x^k=1$ 的整数 k 的集合．

(a) 集合 S 是整数加群 $\mathbf{Z}^+$ 的子群．

(b) 两个幂 $x^r=x^s$ 对于 $r\geqslant s$ 成立当且仅当 $x^{r-s}=1$，即当且仅当 $r-s\in S$．

(c) 假设 S 是非平凡子群，则 $S=\mathbf{Z}n$ 对某个正整数 n 成立．则幂 1，x，x^2，…，x^{n-1} 是子群 $\langle x\rangle$ 中不同的元素，且 $\langle x\rangle$ 的阶为 n．

证明

(a) 如果 $x^k=1$ 且 $x^l=1$，则有 $x^{k+l}=x^kx^l=1$．这表明若 k，$l\in S$，则 $k+l\in S$．于是子群的第一个性质(2.3.1)成立．因为 $x^0=1$，故 $0\in S$．最后，若 $k\in S$，即 $x^k=1$，则 $x^{-k}=(x^k)^{-1}=1$．从而，$-k\in S$．

(b) 由消去律 2.2.3 可得．

(c) 设 $S\neq\{0\}$．定理 2.3.3 表明 $S=\mathbf{Z}n$，其中 n 为 S 中最小正整数．如果 x^k 是任意幂，用 n 去除 k，记作 $k=qn+r$，$0\leqslant r<n$．则 $x^{qn}=1^q=1$ 且 $x^k=x^{qn}x^r=x^r$．因此 x^k 是 1，x，x^2，…，x^{n-1} 之一．从(b)知，这些幂是不同的，因为 x^n 是满足 $x^n=1$ 的最小正整数． ■

在这个命题的(c)中描述的群 $\langle x\rangle=\{1,x,x^2,\cdots,x^{n-1}\}$ 称为 n 阶循环群．之所以叫做循环群是因为群中的元素由 x 反复相乘重复得到其中的 n 个元素．

群中的一个元素 x 有阶 n，如果 n 是满足满足 $x^n=1$ 的最小正整数，这等价于说由 x 生成的循环子群 $\langle x\rangle$ 有阶 n．

使用对称群 S_3 通常的记号，元素 x 有阶 3，元素 y 有阶 2．在任何群中，恒等元是唯一阶为 1 的元素．

46

如果对于任意正整数 n 有 $x^n\neq1$，则称 x 是无限阶的．在 $GL_2(\mathbf{R})$ 中矩阵 $\begin{bmatrix}1&1\\0&1\end{bmatrix}$ 是无限阶的，而 $\begin{bmatrix}1&1\\-1&0\end{bmatrix}$ 是 6 阶的．

当 x 是无限阶时，群 $\langle x\rangle$ 称为无限循环群．对于无限循环群，没什么好讨论的．

【2.4.3】命题 令 x 是群中阶为 n 的元素，且 k 是一个整数，写成 $k=qn+r$，其中 q 和 r 均为整数，且 $0\leqslant r<n$．

- $x^k=x^r$．
- $x^k=1$ 当且仅当 $r=0$．
- 令 $d=\gcd(k,n)$，则 x^k 的阶等于 $\dfrac{n}{d}$．

我们也会讲到群 G 中由子集 U 生成的子群，这是指 G 中包含 U 的最小子群，它由 G

中所有可以表成 U 的元素和它们的逆的串的乘积的元素构成. G 的子集 U 称为生成 G，如果 G 中的元素都可表示成这样的积. 例如，在(2.2.7)中，我们看到子集 $U=\{x, y\}$ 生成对称群 S_3. 初等矩阵生成 GL_n(定理 1.2.16). 在这两个例子中，不需要逆. 但情况并非总如此. 一个由 x 生成的无限循环群$\langle x\rangle$就需要用负幂的元素填满.

克莱因四元群 V 是由四个矩阵

【2.4.4】
$$\begin{bmatrix}\pm 1 & \\ & \pm 1\end{bmatrix}$$

组成的最简单的非循环群. 任意两个不是恒等元的元素生成 V. *四元数群* H 是 $GL_2(C)$ 中非循环的小子群的例子. 它由八个矩阵

【2.4.5】
$$H=\{\pm\mathbf{1}, \pm\boldsymbol{i}, \pm\boldsymbol{j}, \pm\boldsymbol{k}\}$$

构成，其中

$$\mathbf{1}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix},\quad \boldsymbol{i}=\begin{bmatrix}\mathrm{i} & 0\\ 0 & -\mathrm{i}\end{bmatrix},\quad \boldsymbol{j}=\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix},\quad \boldsymbol{k}=\begin{bmatrix}0 & \mathrm{i}\\ \mathrm{i} & 0\end{bmatrix}$$

这些矩阵可由物理上的 Pauli 矩阵乘以 i 得到. 元素 $\boldsymbol{i}$, $\boldsymbol{j}$ 生成 H，通过计算可得下列公式：

【2.4.6】
$$\boldsymbol{i}^2=\boldsymbol{j}^2=\boldsymbol{k}^2=-\mathbf{1}, \boldsymbol{ij}=-\boldsymbol{ji}=\boldsymbol{k}, \boldsymbol{jk}=-\boldsymbol{kj}=\boldsymbol{i}, \boldsymbol{ki}=-\boldsymbol{ik}=\boldsymbol{j}$$

第五节 同 态

设 G 和 G' 为用乘法记号表示的两个群. 一个*同态* $\varphi: G\to G'$ 是 G 到 G' 的映射，使得对于 G 中任意元素 a，b 有

47 【2.5.1】
$$\varphi(ab)=\varphi(a)\varphi(b)$$

这个方程左边的意思是

先在 G 中做 a 与 b 的乘积，然后再用 φ 映射到 G' 中的元素，

而方程右边的意思是

先把 a 与 b 分别用 φ 映射到 G' 中的元素后，再对 G' 中的像做乘积.

直观上，一个同态就是两个群中与合成法则相容的映射，它提供了将两个不同的群联系起来的一种方法.

【2.5.2】**例** 下列映射是同态：

(a) 行列式函数 $\det: GL_n(\mathbf{R})\to\mathbf{R}^\times$ (1.4.10).

(b) 符号同态 $\sigma: S_n\to\{\pm 1\}$ 将置换映射为相应的正负号(1.5.11).

(c) 幂指数映射 $\exp: \mathbf{R}^+\to\mathbf{R}^\times$ 定义为 $x\rightsquigarrow \mathrm{e}^x$.

(d) 映射 $\varphi: \mathbf{Z}^+\to G$ 定义为 $\varphi(n)=a^n$，其中 a 为 G 中指定元素.

(e) 绝对值映射 $|\ |: \mathbf{C}^\times\to\mathbf{R}^\times$. ■

在例子(c)和(d)中，定义域中的合成法则用加法记号，值域中的用乘法记号. 同态的条件(2.5.1)必须考虑在内. 同态的条件变为

$$\varphi(a+b)=\varphi(a)\varphi(b)$$

这个公式表明指数映射是一个同态，即 $e^{a+b}=e^a e^b$.

需要提及下面的同态，虽然这些同态不太有趣. 平凡同态 $\varphi:G\to G'$ 将 G 中每一个元素映射为 G' 中的恒等元. 若 H 是 G 的子群，则包含映射 $i:H\to G$ 定义为对于任意的元素 $x\in H$，有 $i(x)=x$，这是一个同态.

【2.5.3】命题 令 $\varphi:G\to G'$ 是群同态.

(a) 如果 a_1，…，a_k 是 G 中的元素，则 $\varphi(a_1\cdots a_k)=\varphi(a_1)\cdots\varphi(a_k)$.

(b) φ 把恒等元映射为恒等元：$\varphi(1_G)=1_{G'}$.

(c) φ 把逆元映射为逆元：$\varphi(a^{-1})=\varphi(a)^{-1}$.

证明 第一个断言由定义和归纳法可得. 其次，由于 $1\cdot 1=1$ 及 φ 是同态，故 $\varphi(1)\cdot\varphi(1)=\varphi(1\cdot 1)=\varphi(1)$，由(2.2.3)两边消去 $\varphi(1)$ 得到 $\varphi(1)=1$. 最后，$\varphi(a^{-1})\cdot\varphi(a)=\varphi(a^{-1}\cdot a)=\varphi(1)=1$. 因此 $\varphi(a^{-1})=\varphi(a)^{-1}$. ■

群同态确定了两个重要的子群：像和核.

注 同态 $\varphi:G\to G'$ 的像常记作 $\mathrm{im}\varphi$，它是 φ 的像的集合：

【2.5.4】
$$\mathrm{im}\varphi=\{x\in G'\mid x=\varphi(a),a\in G\}$$

像的另外一个记号是 $\varphi(G)$.

48

映射 $\mathbf{Z}^+\to G$ 将 n 映射为 a^n，该映射的像是由 a 生成的循环子群.

同态的像是其值域的一个子群. 我们验证封闭性，省略其他性质的验证. 设 x 和 y 是像中的元素，这就是说存在两个元素 a，$b\in G$ 使得 $x=\varphi(a)$，$y=\varphi(b)$. 由于 φ 是同态，$xy=\varphi(a)\varphi(b)=\varphi(ab)$. 所以，$xy=\varphi($某元素$)$，它也是像中的元素.

注 同态的核更微妙也更重要. φ 的核记作 $\ker\varphi$，是 G 中所有映射到 G' 恒等元的那些元素的集合：

【2.5.5】
$$\ker\varphi=\{a\in G\mid\varphi(a)=1\}$$

核是 G 的子群，因为若 a 和 b 是核中的元素，则 $\varphi(ab)=\varphi(a)\varphi(b)=1\cdot 1=1$，故 ab 也是核中的元素，等等，其他可类似验证.

行列式同态 $GL_n(\mathbf{R})\to\mathbf{R}^\times$ 的核是一个特殊线性群 $SL_n(\mathbf{R})$(2.2.11). 符号同态 $S_n\to\{\pm 1\}$ 的核称为交错群. 它由所有偶置换组成，记作 A_n：

【2.5.6】 交错群 A_n 是偶置换群

核之所以重要是因为它控制了全部同态. 它不仅告诉我们 G 中哪些元素映射为 G' 中的恒等元，而且告诉我们哪些元素对在 G' 中的像是相同的.

注 如果 H 是 G 的子群，且 a 是 G 中元素，则记号 aH 表示所有乘积 ah，$h\in H$ 的全体：

【2.5.7】
$$aH=\{g\in G\mid g=ah,h\in H\}$$

这个集合称为 H 在 G 中的左陪集，“左”指的是元素 a 出现在左边.

【2.5.8】命题 令 $\varphi:G\to G'$ 是一个群同态，a 和 b 是 G 中元素. 令 K 是 φ 的核. 下列条件是等价的：

- $\varphi(a)=\varphi(b)$，

- $a^{-1}b\in K$,
- $b\in aK$,
- 陪集 bK 与陪集 aK 相等.

证明 若 $\varphi(a)=\varphi(b)$，则 $\varphi(a^{-1}b)=\varphi(a^{-1})\varphi(b)=\varphi(a)^{-1}\varphi(b)=1$. 因此 $a^{-1}b\in K$. 要证明反过来也成立，只需把论证倒过来. 若 $a^{-1}b\in K$，则 $1=\varphi(a^{-1}b)=\varphi(a)^{-1}\varphi(b)$，所以 $\varphi(a)=\varphi(b)$. 这就证明了前两个结论是等价的，从而得证它们与其余的等价. ■

49

【2.5.9】推论 同态 $\varphi:G\to G'$ 是内射的当且仅当它的核 K 是 G 的平凡子群 $\{1\}$.

证明 若 $K=\{1\}$，则命题 2.5.8 表明 $\varphi(a)=\varphi(b)$ 仅当 $a^{-1}b=1$，亦即 $a=b$ 时成立. 反之，若 φ 是内射，则恒等元是 G 中满足 $\varphi(a)=1$ 的唯一元素，故 $K=\{1\}$. ■

同态的核的另一个重要性质在下一个命题中阐述. 如果 a 和 g 是群 G 中的元素，则 gag^{-1} 称作由 g 引出的 a 的共轭.

【2.5.10】定义 群 G 的子群 N 是正规子群，如果对于 N 中任意元素 a 和 G 中任意元素 g，共轭 $gag^{-1}\in N$.

【2.5.11】命题 一个同态的核是一个正规子群.

证明 如果 a 是同态 $\varphi:G\to G'$ 的核且 g 是群 G 的任意元素，则 $\varphi(gag^{-1})=\varphi(g)\varphi(a)\varphi(g^{-1})=\varphi(g)1\varphi(g)^{-1}=1$. 因此 gag^{-1} 也属于核. ■

因此，特殊线性群 $SL_n(\mathbf{R})$ 是一般线性群 $GL_n(\mathbf{R})$ 的正规子群，交错群 A_n 是对称群 S_n 的正规子群. 交换群的任何子群都是正规的，因为如果 G 是交换群，则 $gag^{-1}=a$ 对于所有的 a 和 g 成立. 但是非交换群的子群未必是正规的. 例如，在对称群 S_3 中，利用 (2.2.7)中的表示，2 阶循环子群 $\langle y\rangle$ 不是正规子群，因为 $y\in G$，但是 $xyx^{-1}=x^2y\notin\langle y\rangle$.

注 群 G 的中心(用 Z 表示)是与 G 中每个元素都可以交换的元素的集合：

【2.5.12】
$$Z=\{z\in G\mid zx=xz,\text{对于任意 } x\in G\}$$

Z 是 G 的正规子群. 特殊线性群 $SL_2(\mathbf{R})$ 的中心由两个矩阵 I，$-I$ 组成. 如果 $n\geqslant 3$，则对称群 S_n 的中心是平凡子群.

【2.5.13】例 对称群间的同态 $\varphi:S_4\to S_3$.

存在三种方式把指标集为 $\{\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{4}\}$ 的集合划分为阶为 2 的子集对，即

【2.5.14】
$$\Pi_1:\{\mathbf{1},\mathbf{2}\}\cup\{\mathbf{3},\mathbf{4}\},\quad \Pi_2:\{\mathbf{1},\mathbf{3}\}\cup\{\mathbf{2},\mathbf{4}\},\quad \Pi_3:\{\mathbf{1},\mathbf{4}\}\cup\{\mathbf{2},\mathbf{3}\}$$

对称群 S_4 的一个元素置换这四个指标，在置换的过程中，也置换这三个划分. 这定义了从 S_4 到集合 $\{\Pi_1,\Pi_2,\Pi_3\}$ 的置换群(即对称群 S_3)的一个映射 φ. 例如，4-循环 $p=(\mathbf{1\ 2\ 3\ 4})$ 在 2 阶子集上的作用如下：

$$\{\mathbf{1},\mathbf{2}\}\rightsquigarrow\{\mathbf{2},\mathbf{3}\}\quad \{\mathbf{1},\mathbf{3}\}\rightsquigarrow\{\mathbf{2},\mathbf{4}\}\quad \{\mathbf{1},\mathbf{4}\}\rightsquigarrow\{\mathbf{1},\mathbf{2}\}$$
$$\{\mathbf{2},\mathbf{3}\}\rightsquigarrow\{\mathbf{3},\mathbf{4}\}\quad \{\mathbf{2},\mathbf{4}\}\rightsquigarrow\{\mathbf{1},\mathbf{3}\}\quad \{\mathbf{3},\mathbf{4}\}\rightsquigarrow\{\mathbf{1},\mathbf{4}\}$$

从上述作用来看，$p=(\mathbf{1\ 2\ 3\ 4})$ 作用在划分集合 $\{\Pi_1,\Pi_2,\Pi_3\}$ 是 $(\Pi_1\Pi_3)$ 对换，使 Π_2 保持不

50 变而将 Π_1 和 Π_3 互换.

如果 p 和 q 是 S_4 中的元素，则乘积 pq 是置换的复合 $p\circ q$，且 pq 对集合 $\{\Pi_1,\Pi_2,$

$\Pi_3\rangle$的作用是 q 和 p 作用的合成. 因此 $\varphi(pq)=\varphi(p)\varphi(q)$，且 φ 是同态.

这个映射是满射，故其像是整个群 S_3. 它的核能够被计算出来. 它是 S_4 中由恒等元和三个互斥对换的乘积所组成的子群：

【2.5.15】 $$K=\{1,(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}$$ ■

第六节 同 构

一个从群 G 到群 G' 的同构 $\varphi:G\to G'$ 是双射群同态——一个双射，使得 $\varphi(ab)=\varphi(a)\varphi(b)$ 对于所有 a，$b\in G$ 成立.

【2.6.1】例

- 当看成是实数加群 $\mathbf{R}^+$ 到它的像，即正实数乘法群的映射时，指数映射 e^x 是一个同构.
- 若 a 是群 G 中的一个无限阶的元素，则将 $n\rightsquigarrow a^n$ 的映射是整数加群 $\mathbf{Z}^+$ 到群 G 的无限阶循环子群$\langle a\rangle$的同构.
- $n\times n$ 置换矩阵的集合 $\mathcal{P}$ 是 GL_n 的子群，且将置换映射为相应的矩阵(1.5.7)的映射 $S_n\to\mathcal{P}$ 是一个同构. ■

推论 2.5.9 给出了验证一个群同态 $\varphi:G\to G'$ 是同构的方法. 为此，只需验证 $\ker\varphi=\{1\}$，这蕴含了 φ 是单射，且 $\mathrm{im}\varphi=G'$ 蕴含了 φ 是满射.

【2.6.2】**引理** *如果 $\varphi:G\to G'$ 是同构，则其逆映射 $\varphi^{-1}:G'\to G$ 也是同构.*

证明 一个双射的逆还是双射. 我们必须证明对于所有 G' 中的元素 x 和 y，有 $\varphi^{-1}(x)\varphi^{-1}(y)=\varphi^{-1}(xy)$. 令 $a=\varphi^{-1}(x)$，$b=\varphi^{-1}(y)$，且 $c=\varphi^{-1}(xy)$. 必须证明的是 $ab=c$. 因为 φ 是双射，故只需证明 $\varphi(ab)=\varphi(c)$ 就够了. 由于 φ 是同态，故

$$\varphi(ab)=\varphi(a)\varphi(b)=xy=\varphi(c)$$ ■

这个引理表明，当 $\varphi:G\to G'$ 是同构时，可以对这两个群的任何一个进行计算，然后用 φ 和 φ^{-1} 将一个群上的运算转化到另一个群上去. 所以，对群运算律，两个群上的性质是相同的. 为了直观地刻画这个结论，假设一个群的元素被放入没有标签的盒子里，且我们得到了神谕，当给我们两个盒子时，我们知道哪个盒子含有它们的乘积. 我们无法确定盒子里的元素来自 G 还是 G'.

两个群 G 和 G' 称为是*同构的*，如果存在从 G 到 G' 的同构 φ. 我们有时用符号“$\approx$”表示两个群同构：

【2.6.3】 $$G\approx G' \text{ 指的是 } G \text{ 同构于 } G'$$ 51

既然同构的群有相同的性质，因此当非正式地谈到同构的群时，把它们看成是相同的会很方便. 例如，我们经常忽略对称群 S_n 和与之同构的置换矩阵群 $\mathcal{P}$ 之间的差别.

注 *与给定的群 G 同构的群形成 G 的同构类.*

在同构类中的任何两个群是同构的. 当谈到给群分类时，就是指刻画这些同构类. 对所有群分类太难了，几乎是不可能做到的，但我们将看到每一个阶为素数 p 的群是循环

群. 所以，所有阶为素数 p 的群都是同构的. 阶为 4 的群有两个同构类(2.11.5)，阶为 12 的群有 5 个同构类(7.8.1).

关于同构，一个有趣但容易引起混乱的一点就是存在群 G 到其自身的同构 $\varphi: G \to G$. 这样的同构称为 G 的自同构. 当然，恒等映射是自同构，但几乎总存在其他的自同构. 最重要类型的自同构是共轭：令 g 是群 G 中一个固定的元素. 由 g 得到的共轭是一个群 G 到自身的映射 φ，定义为：

【2.6.4】 $$\varphi(x) = gxg^{-1}$$

这是一个自同构，因为首先它是一个同态：

$$\varphi(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \varphi(x)\varphi(y)$$

其次，这是一个双射. 因为它有逆函数——由 g^{-1} 得到的共轭.

如果群是交换群，则由 g 得到的共轭是恒等映射：$gxg^{-1} = x$. 但任何非交换群有非平凡的共轭，所以就有异于恒等映射的自同构. 例如，在对称群 S_3 中，如以往的表示，由 y 得到的共轭交换 x 和 x^2.

如前所述，元素 gxg^{-1} 称为元素 x 关于 g 的共轭. G 中的两个元素 x，x' 是共轭的，如果 $x' = gxg^{-1}$ 对某个 $g \in G$ 成立. 共轭 gxg^{-1} 的行为与元素 a 自身的行为非常相似，例如它在群中的阶是一样的. 这可由它是元素 x 在一个自同构下的像这一事实得到(参见下面引理 2.6.5 的讨论).

注 有时人们希望确定群 G 中的两个元素 x 和 y 是否共轭，即是否存在一个元素 $g \in G$ 的使得 $y = gxg^{-1}$. 解上面的方程不如解 $yg = gx$ 简单.

注 交换子 $aba^{-1}b^{-1}$ 是与群中元素对 a，b 相关联的另一个元素.

下面的引理通过把一些项从方程的一边移到另一边得到.

【2.6.5】引理 群的两个元素 a，b 可交换，即 $ab = ba$，当且仅当 $aba^{-1} = b$，且结论成立当且仅当 $aba^{-1}b^{-1} = 1$.

第七节 等价关系和划分

一个基本的数学构造是从一个集合 S 出发，根据给定的法则等同 S 的元素而得到新的
52 集合. 例如，可以将整数集合分为两类，即偶数和奇数. 所得到的新的集合由两个元素构成，一个元素叫做奇数，一个元素叫做偶数. 或者，可以将平面上的全等三角形视为等价的几何对象. 这个非常一般的过程来自不同的方面，我们现在就讨论这些方面.

注 集合 S 的一个划分 Π 是将 S 分为互不相交的非空的子集：

【2.7.1】 $$S = \text{不相交非空子集的并}$$

奇数集合和偶数集合这两个集合构成所有整数集合的一个划分. 采用通常的记号，集合

【2.7.2】 $$\{1\}, \{y, xy, x^2y\}, \{x, x^2\}$$

构成对称群 S_3 的一个划分.

注 集合 S 上的等价关系是 S 中某些元素对之间的关系. 我们通常将它们记为 $a \sim b$，

并称为 a 与 b 的一个等价. 一个等价关系需要满足下面的条件:

【2.7.3】

- 传递的: 若 $a\sim b$ 且 $b\sim c$, 则 $a\sim c$.
- 对称的: 若 $a\sim b$, 则 $b\sim a$.
- 自反的: 对所有 a, $a\sim a$.

三角形的全等是平面上三角形的集合 S 上的等价关系的例子. 如果 A, B 和 C 是三角形, 且如果 A 全等于 B, 且 B 全等于 C, 则 A 全等于 C, 等等.

共轭性是群上的一个等价关系. 群中两个元素共轭, $a\sim b$, 如果存在 $g\in G$ 使得 $b=gag^{-1}$. 我们验证传递性: 设 $a\sim b$ 且 $b\sim c$. 这意味着 $b=g_1ag_1^{-1}$ 和 $c=g_2bg_2^{-1}$ 对某个 g_1, $g_2\in G$ 成立. 则 $c=g_2(g_1ag_1^{-1})g_2^{-1}=(g_2g_1)a(g_2g_1)^{-1}$, 故 $a\sim c$.

集合 S 的划分和 S 上的等价关系这两个概念在逻辑上是等价的, 虽然实际上给出的通常只是二者之一.

【2.7.4】**命题** 集合 S 上的一个等价关系确定集合 S 的一个划分, 反之亦然.

证明 给定 S 上的划分 P, 可用下面的规则定义一个等价关系 R: 如果 a 和 b 属于划分的同一个子集, 则 $a\sim b$. 等价关系的三条件显然成立. 反之, 给定等价关系 R, 可以这样定义划分 P: 含 a 的子集是所有满足条件 $a\sim b$ 的元素 b 的集合. 这个子集称为 a 的等价类. 我们用 C_a 表示 a 的等价类:

【2.7.5】
$$C_a=\{b\in S\mid a\sim b\}$$

下一个引理完成此命题的证明. ■ 53

【2.7.6】**引理** 给定集合 S 上的等价关系, S 的等价类构成 S 的划分.

证明 这点很重要, 所以我们将仔细验证. 记住记号 C_a 代表以特定方式定义的子集. 划分由这些子集构成, 且一些记号可以描述同一个子集.

自反公理告诉我们 $a\in C_a$. 所以, 类 C_a 是非空的, 并且由于 a 可以是任意元素, 故这些类覆盖 S, 剩下需要证明的划分的性质是等价类间没有重叠部分. 为证明这一点, 先证明:

【2.7.7】
$$\text{如果 } C_a \text{ 和 } C_b \text{ 有一个共同的元素, 则 } C_a=C_b$$

因为 a 和 b 的作用可以互换, 只需证明若 C_a 和 C_b 有一个共同的元素, 比如 d, 则 $C_b\subset C_a$, 即任何属于 C_b 中的元素均属于 C_a. 如果 $x\in C_b$, 则 $b\sim x$. 由于 $d\in C_a$ 和 $d\in C_b$, 故 $a\sim d$, $b\sim d$, 对称性告诉我们 $d\sim b$. 故有 $a\sim d$, $d\sim b$ 和 $b\sim x$. 两次应用传递性得 $a\sim x$, 因此, $x\in C_a$. ■

例如, 群上由 $a\sim b$ 定义的关系(如果 a 和 b 具有相同的阶)是一个等价关系. 对于对称群 S_3 的一个相应划分在(2.7.2)中给出.

如果给定了集合 S 的划分, 我们可以构造一个新的集合 $\overline{S}$, 其元素是等价类或组成划分的子集. 我们想象把这些子集放在不同的堆中, 把这些堆看成是新的集合 $\overline{S}$ 的元素. 建议用一个记号将子集和集合 $\overline{S}$(堆)中的元素区分开来. 如果 U 是一个子集, 则常用 $[U]$ 表示 $\overline{S}$ 中相应的元素. 因此, 如果 S 是整数集合且奇和偶分别表示奇数和偶数子集, 则 $\overline{S}$ 包含两个元素[奇]和[偶].

我们将更广泛地应用这个记号. 当 S 的子集 U 作为 S 的子集的集合中的元素时，记作 $[U]$.

当给出集合 S 上一个等价关系，等价类形成一个划分，我们得到一个新的集合 $\overline{S}$，它的元素是等价类 $[C_a]$. 我们可以用另一种方式看待这个新的集合中的元素，因为这个集合是由元素间的等价关系变化得来的. 如果 a 和 b 属于 S，$a\sim b$ 意味着在 $\overline{S}$ 中 a 和 b 是相等的，因为 $C_a=C_b$. 用这种方式看待新集合的话，两个集合 S 和 $\overline{S}$ 的差别在于在 $\overline{S}$ 中更多的元素被宣布是“相等的”，即等价的. 对我来讲就像在学校里经常把全等三角形看成是一样的.

对于任何等价关系，存在一个自然的满射

【2.7.8】
$$\pi: S \to \overline{S}$$

把 S 中的元素 a 映射为它的等价类：$\pi(a)=[C_a]$. 当我们想把 $\overline{S}$ 看成是由集合 S 中的元素改变等价记号得到的时，$\overline{S}$ 中的元素 $[C_a]$ 用符号 $\overline{a}$ 表示更方便. 则映射 π 变成

54
$$\pi(a) = \overline{a}$$

我们可以在 $\overline{S}$ 中采用 S 中元素的符号，但在元素符号上面加上一横杠提醒我们在 $\overline{S}$ 中采用新规则：

【2.7.9】 如果 a 与 b 属于 S，则 $\overline{a}=\overline{b}$ 意味着 $a\sim b$

这一横杠符号的缺点是许多符号表示 $\overline{S}$ 中同一元素. 有时这个缺点可通过选取特殊元素（即每个等价类里的代表元）来克服. 例如，偶数与奇数常常用 $\overline{0}$ 与 $\overline{1}$ 表示：

【2.7.10】
$$\{[\text{偶}],[\text{奇}]\} = \{\overline{0},\overline{1}\}$$

虽然堆的图像较为直接，起初很容易掌握，但第二种看待 $\overline{S}$ 的方法更好，因为横杠记号在代数上更容易操作.

由映射定义的等价关系

集合之间的任意映射 $f: S\to T$ 在其定义域 S 上定义了一个等价关系，也就是由规则“如果 $f(a)=f(b)$ 则 $a\sim b$.”给出的等价关系.

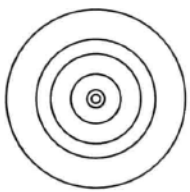
注 T 中元素 t 的原像是由满足 $f(s)=t$ 的所有元素 s 构成的 S 的子集. 用符号表示为

【2.7.11】
$$f^{-1}(t) = \{s \in S \mid f(s) = t\}$$

这是个象征性记号. 请记住只有当 f 是双射时 f^{-1} 才是映射. 原像也叫做映射 f 的纤维，且非空纤维是对于上面定义的等价关系的等价类.

作为映射的像，这里等价类集合 $\overline{S}$ 有另外的体现. 像的元素与非空纤维一一对应，而非空纤维是等价类.

【2.7.12】图



绝对值映射：$\mathbf{C}^\times \to \mathbf{R}^\times$ 的一些纤维

【2.7.13】**例** 如果 G 是有限群，定义映射 $f:G\to\mathbf{N}$ 到自然数{1，2，3，…}的集合，令 $f(a)$表示 G 中元素 a 的阶. 这个映射的纤维是同阶元素的集合(例如，见(2.7.2)). ■ 55

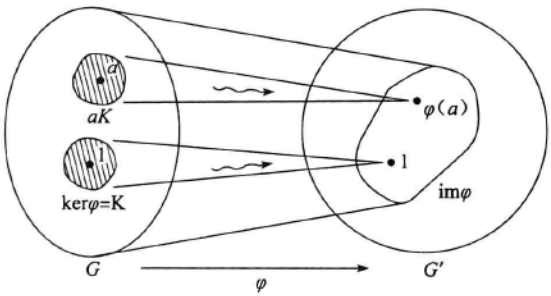
我们回到群同态 $\varphi:G\to G'$. 由 φ 定义的群 G 上的等价关系通常用≡表示，而不用～，～指的是同余.

【2.7.14】 $$\text{如果 } \varphi(a)=\varphi(b),\quad \text{则 } a\equiv b$$

我们看到 G 中元素 a 与 b 是同余的，即 $\varphi(a)=\varphi(b)$，当且仅当 b 属于核 K 的陪集 aK(2.5.8).

【2.7.15】**命题** 令 K 是同态 $\varphi:G\to G'$ 的核. φ 的包含 G 中元素 a 的纤维是核 K 的陪集 aK. 这些陪集构成了群 G 的划分，且这个划分对应着 φ 的像的元素.

【2.7.16】图



群同态的图解

第八节 陪 集

如前，如果 H 是群 G 的子群，且 $a\in G$，则子集

【2.8.1】 $$aH=\{ah\mid h\in H\}$$

称为左陪集. 子群 H 是一个特殊的左陪集，因为 $H=1H$.

G 中 H 的陪集是关于同余关系

【2.8.2】 $$a\equiv b,\text{如果 } b=ah \text{ 对某个 } h\in H \text{ 成立}$$

的等价类. 这很简单，但是让我们验证同余是等价关系.

传递性：假设 $a\equiv b$ 且 $b\equiv c$. 这表明对 h，$h'\in H$，有 $b=ah$ 和 $c=bh'$. 因此，$c=ahh'$. 由于 H 是子群，$hh'\in H$，这样 $a\equiv c$.

对称性：设 $a\equiv b$，则有 $b=ah$. 于是 $a=bh^{-1}$ 且 $h^{-1}\in H$，故 $b\equiv a$.

自反性：$a=a1$ 而 $1\in H$，故 $a\equiv a$.

注意，我们用到子群定义的所有性质：封闭性，逆元，恒等元. 56

【2.8.3】**推论** *群 G 的子群 H 的左陪集是群 G 的划分.*

证明 左陪集是同余关系(2.8.2)的等价类. ■

记住符号 aH 定义 G 的某个子集. 与任意等价关系一样，若干个记号可以表示同一集合. 例如，在对称群 S_3 中，用通常的表示(2.2.6)，元素 y 生成一个阶为 2 的循环子群 $H=\langle y\rangle$. 在 G 中有三个关于 H 的左陪集：

【2.8.4】 $H=\{1,y\}=yH$， $xH=\{x,xy\}=xyH$， $x^2H=\{x^2,x^2y\}=x^2yH$
这些集合的确是群的划分.

概括地讲，令 H 是群 G 的子群，a，$b\in G$. 下列结论是等价的：

【2.8.5】

- $b=ah$ 对于某个 $h\in H$，或 $a^{-1}b$ 是 H 的元素成立，
- b 是左陪集 aH 的元素，
- 左陪集 aH 与 bH 是相等的.

一个子群的左陪集的个数叫做这个子群 H 在群 G 中的指标. 指标表示为：

【2.8.6】 $$[G:H]$$

因此子群 $\langle y\rangle$ 在 S_3 中的指标为 3. 当 G 是无限群时，指标也是无限的.

【2.8.7】**引理** *群 G 的子群 H 的所有左陪集 aH 有相同的阶.*

证明 存在一个由子群 H 到陪集 aH 的映射：$h\to aH$ 将 h 映射为 ah，即 $h\rightsquigarrow ah$. 这个映射是双射，因为它的逆是由 a^{-1} 所诱导的乘法映射. ■

因为所有陪集有相同的阶，而这些陪集是群的一个划分，所以我们得到重要的计数公式：

【2.8.8】 $$|G|=|H|[G:H]$$

$$(G\text{ 的阶数})=(H\text{ 的阶数})(\text{陪集个数})$$

其中，如通常一样，$|G|$ 表示 G 的阶. 如果某项为无穷，等式的意义是显然的. 对于 S_3 的子群 $\langle y\rangle$，这个公式成为 $6=2\cdot 3$.

从计数公式得到(2.8.8)右边两项一定整除左边. 下面是这些结果中的一个，称为拉格朗日定理：

【2.8.9】**定理**(拉格朗日定理) *设 G 是有限群且 H 是 G 的子群. H 的阶整除 G 的阶.*

57 【2.8.10】**推论** *有限群的元素的阶数整除群的阶数.*

证明 一个群 G 的元素 a 的阶等于由 a 生成的循环子群 $\langle a\rangle$ 的阶(命题 2.4.2). ■

【2.8.11】**推论** *设群 G 的阶为 p 且 p 是素数. 设 $a\in G$ 是任意元，但不是恒等元. 则 G 是由 a 生成的循环群 $\langle a\rangle$.*

证明 元素 $a\neq 1$ 的阶大于 1 且它整除 $|G|=p$. 所以，a 的阶等于 p. 这也是由 a 生成的循环子群 $\langle a\rangle$ 的阶. 因为 G 的阶为 p，所以 $\langle a\rangle=G$. ■

这一推论对所有素数阶 p 的群作了分类. 它们构成一个同构类，即 p 阶循环群类.

当给定同态 $\varphi:G\to G'$ 时，计数公式也可以应用. 正如我们在(2.7.15)中所看到的，$\ker\varphi$ 的左陪集是映射 φ 的纤维，它们与像中的元素一一对应.

【2.8.12】 $$[G:\ker\varphi]=|\mathrm{im}\varphi|$$

【2.8.13】**推论** *设 $\varphi:G\to G'$ 是有限群的一个同态. 则*

- $|G|=|\ker\varphi|\cdot|\mathrm{im}\varphi|$，
- $|\ker\varphi|$ 整除 $|G|$，
- $|\mathrm{im}\varphi|$ 整除 $|G|$ 和 $|G'|$.

证明 第一个公式由(2.8.8)和(2.8.12)合起来得到，而且它蕴含着$|\ker\varphi|$和$|\mathrm{im}\varphi|$整除$|G|$. 因为$\mathrm{im}\varphi$是G'的子群，由拉格朗日定理可知，$|\mathrm{im}\varphi|$也整除$|G'|$. ■

例如，符号同态$\sigma:S_n\to\{\pm1\}$(2.5.2)(b)是满射，所以它的像的阶为2. 它的核即交错群A_n)有阶$\frac{1}{2}n!$. S_n的一半元素是偶置换，一半元素是奇置换.

当给出一串子群时，计数公式2.8.8有类似的结论.

【2.8.14】命题(指标的乘法性质) 令$G\supset H\supset K$是群G的子群，则$[G:K]=[G:H][H:K]$.

证明 我们假设右边两个指标都是有限的，比如，令$[G:H]=m$和$[H:K]=n$. 当其中一个指标无限时，推理是类似的. 我们列出H在G中的m个陪集，每个陪集选出代表元，比如g_1H，…，g_mH. 则$g_1H\cup\cdots\cup g_mH$是G的一个划分. 同样选出K在H中的所有陪集的代表元，得到H的一个划分$H=h_1H\cup\cdots\cup h_nK$. 由于用$g_i$乘的运算是可逆的，因此$g_iH=g_ih_1K\cup\cdots\cup g_ih_nK$是陪集$g_iH$的一个划分. 将这些划分组合起来，就构成了由$mn$个陪集$g_ih_jK$组成的$G$的一个划分. ■

右陪集

让我们回到陪集的定义. 这里使用的是左陪集aH，也可以定义子群H的右陪集并且重复上面的讨论. 群G的子群H的右陪集是集合 58

【2.8.15】
$$Ha=\{ha\,|\,h\in H\}$$

它们是关系(右同余)

$$a\equiv b,\text{如果存在 }h\in H,\text{使 }b=ha$$

的等价类. 右陪集和左陪集不一定相同，但它们也构成群的一个划分. 例如，S_3的子群$\langle y\rangle$的右陪集是

【2.8.16】
$$H=\{1,y\}=Hy,\quad Hx=\{x,x^2y\}=Hx^2y,\quad Hx^2=\{x^2,xy\}=Hxy$$

这和划分(2.8.4)中的左陪集不同. 然而，如果一个子群是正规子群，那么它的左陪集和右陪集就是相同的.

【2.8.17】命题 令H是群G的子群. 下列条件是等价的：

(i) H是正规子群：对于所有$h\in H$和$g\in G$有$ghg^{-1}\in H$.

(ii) 对于所有$g\in G$，$gHg^{-1}=H$.

(iii) 对于所有$g\in G$，左陪集gH等于右陪集Hg.

(iv) H在G中的每一个左陪集都是右陪集.

证明 记号gHg^{-1}代表所有元素ghg^{-1}所成的集合，其中$h\in H$.

假设H是正规子群. 故(i)成立，且蕴含$gHg^{-1}\subset H$对于所有$g\in G$成立. 用g^{-1}代替g也可证$g^{-1}Hg\subset H$. 在这个包含关系两边左乘g且右乘g^{-1}可得$H\subset gHg^{-1}$. 因此，$gHg^{-1}=H$. 这就证明了(i)蕴含(ii). 显然，(ii)蕴含(i). 其次，若$gHg^{-1}=H$，两边右乘g，得$gH=Hg$. 这证明了(ii)蕴含(iii). 类似可证明(iii)蕴含(ii). 由于(iii)蕴含(iv)是

显然的，因此只需验证(iv)蕴含(iii).

那么在什么情况下左陪集和右陪集相等？我们回忆一下右陪集全体是群 G 的一个划分，且注意到左陪集 gH 与右陪集 Hg 有一个共同的元素，即 $g=g\cdot 1=1\cdot g$. 所以，如果左陪集 gH 等于某个右陪集，那么这个右陪集一定是 Hg. ■

【2.8.18】命题

(a) *如果 H 是群 G 的子群且 g 是 G 中一个元素，则集合 gHg^{-1} 也是一个子群.*

(b) *如果群 G 只有一个 r 阶子群 H，则这个子群是正规的.*

证明 (a) 由 g 导出的共轭是群 G 的一个自同态(参见(2.6.4))，且 gHg^{-1} 是 H 的同态像. (b)参见(2.8.17)：gHg^{-1} 是阶为 r 的子群. ■

注意 *如果 H 是有限群 G 的子群，则用右陪集和左陪集的计数公式是一样的，所以左陪集的个数与右陪集的个数相等. 这对于 G 是无限群的情形也是成立的，虽然不能通过计数来证明(参见练习 M.8).*

59

第九节 模 算 术

这一节包含对数论里一个重要概念——整数的同余——的一个简短的讨论. 如果你以前没有遇到过这个概念，则需要了解关于同余的更多知识. 例如，参看[Stark]. 整个这一节都对一个固定的正整数 n 进行讨论.

注 *两个整数 a 和 b 说是模 n 同余的，即*

【2.9.1】
$$a\equiv b(\bmod n)$$

如果 n 整除 $b-a$，或如果对于某个整数 k，有 $b=a+nk$. 例如，$2\equiv 17(\bmod 5)$.

容易验证同余是等价关系，所以可以考虑等价类，称为同余类. 我们用画横杠的符号 $\bar{a}$ 来表示整数 a 模 n 的同余类. 这个同余类是整数集合：

【2.9.2】
$$\bar{a}=\{\cdots,a-n,a,a+n,a+2n,\cdots\}$$

如果 a 和 b 是整数，方程 $\bar{a}=\bar{b}$ 意味着 $a\equiv b(\bmod n)$，或 n 整除 $b-a$. 同余类 $\bar{0}$：

$$\bar{0}=\mathbf{Z}n=\{\cdots,-n,0,n,2n,\cdots\}=\{kn\,|\,k\in\mathbf{Z}\}$$

是整数加群 $\mathbf{Z}^+$ 的一个子群. 其他同余类是这个子群的陪集. 请注意 $\mathbf{Z}n$ 不是右陪集——它是 $\mathbf{Z}^+$ 的一个子群. 和子群 H 的陪集记号 aH 类似，但用加法记号表示合成法则，$a+H=\{a+h\,|\,h\in H\}$. 为简化符号，将子群 $\mathbf{Z}n$ 记为 H. 则 H 的陪集(同余类)是集合

【2.9.3】
$$a+H=\{a+kn\,|\,k\in\mathbf{Z}\}$$

n 个整数 0，1，…，$n-1$ 是这 n 个同余类的代表元.

【2.9.4】命题 *有 n 个模 n 的同余类，即 $\bar{0}$，$\bar{1}$，…，$\overline{n-1}$. $\mathbf{Z}n$ 在 $\mathbf{Z}$ 中的指标 $[\mathbf{Z}:\mathbf{Z}n]$ 是 n.*

令 $\bar{a}$ 和 $\bar{b}$ 表示整数 a，b 的同余类. 它们的和定义为 $a+b$ 的同余类，它们的积是 ab 的同余类. 换句话说，由定义，

【2.9.5】
$$\bar{a}+\bar{b}=\overline{a+b}\quad,\quad \bar{a}\bar{b}=\overline{ab}$$

这个定义需要证明其合理性，因为同一个同余类可以用多个不同的整数表示. 任何与 a 模

n 同余的整数 a' 代表同一个类. 故最好是当 $a'\equiv a$，$b'\equiv b$ 时，$a'+b'\equiv a+b$ 和 $a'b'\equiv ab$ 都成立. 幸运的是，情况的确如此.

【2.9.6】引理 如果 $a'\equiv a(\bmod n)$，$b'\equiv b(\bmod n)$，则 $a'+b'\equiv a+b(\bmod n)$，$a'b'\equiv ab(\bmod n)$.

60

证明 假设 $a'\equiv a(\bmod n)$，$b'\equiv b(\bmod n)$，所以 $a'=a+rn$，且 $b'=b+sn$，其中 r，s 为整数. 这样，$a'+b'=a+b+(r+s)n$. 这表明 $a'+b'\equiv(a+b)(\bmod n)$. 同理，$a'b'=(a+rn)(b+sn)=ab+(as+rb+rns)n$，故 $a'b'\equiv ab(\bmod n)$. ■

同余类对于加法和乘法的结合律、交换律和分配律成立因为这些运算律对于整数的加法和乘法成立. 例如，分配律证明如下：

$$\begin{aligned}\bar{a}(\bar{b}+\bar{c}) &= \bar{a}\overline{(b+c)} = \overline{a(b+c)} && \text{（同余类加法和乘法的定义）}\\ &= \overline{ab+ac} && \text{（整数的分配律）}\\ &= \overline{ab}+\overline{ac} = \bar{a}\bar{b}+\bar{a}\bar{c} && \text{（同余类加法和乘法的定义）}\end{aligned}$$

其他运算律的证明是类似的，在此省略.

模 n 同余类的集合通常记作 $\mathbf{Z}/\mathbf{Z}n$，$\mathbf{Z}/n\mathbf{Z}$ 或 $\mathbf{Z}/(n)$. 加、减和乘可以通过取用 n 去除整数所得的余数而直接得到. 这就是公式(2.9.5)的含义. 这里两个公式表明，将整数 a 变到其同余类 $\bar{a}$ 的映射

【2.9.7】
$$\mathbf{Z}\to\mathbf{Z}/\mathbf{Z}n$$

与加法和乘法相容. 因而计算可在整数中进行，而在最后搬回到 $\mathbf{Z}/\mathbf{Z}n$ 上. 然而，如果使用较小的数字，则运算比较简单. 可通过在做了部分运算后取余数，从而保持运算中的数字都很小.

于是，如果 $n=29$，从而 $\mathbf{Z}/\mathbf{Z}n=\{\bar{0},\bar{1},\cdots,\overline{28}\}$，则 $(\overline{35})(\overline{17}+\overline{7})$ 可以按 $(\overline{35})\cdot(\overline{24})=\bar{6}\cdot(-\bar{5})=-\overline{30}=-\bar{1}$ 的顺序计算.

从长远考虑，数字上面加横杠是很烦人的，因而常被省去，但要记住下面的规则：

【2.9.8】 在 $\mathbf{Z}/\mathbf{Z}n$ 中说 $a=b$ 是指 $a\equiv b(\bmod n)$

模一个素数的同余有特殊的性质，将在下一章的开头讨论.

第十节 对应定理

令 $\varphi:G\to G'$ 是群同态，而 H 是 G 的子群. 则可以限制 φ 到 H 得到一个同态

【2.10.1】
$$\varphi|_H:H\to G'$$

这是指取相同的映射 φ 但将其定义域限制到 H. 故由定义，对所有 $h\in H$ 有 $[\varphi|_H](h)=\varphi(h)$.（为清楚起见，我们给符号 $\varphi|_H$ 加了括号）因为 φ 是同态，所以它的限制也是同态，且 $\varphi|_H$ 的核是 $\ker\varphi$ 与 H 的交：

【2.10.2】
$$\ker(\varphi|H)=(\ker\varphi)\cap H$$

61

由核的定义这是明显的. $\varphi|_H$ 的像与 H 在映射 φ 下的像 $\varphi(H)$ 是一样的.

计数公式也可以帮助描述这个限制. 根据推论(2.8.13)，像的阶既整除 $|H|$，也整除

$|\mathcal{G}|$. 如果$|H|$|和$|\mathcal{G}|$没有公因子，则$\varphi(H)=\{1\}$，因而可得$H\subset\ker\varphi$.

【2.10.3】例 符号同态$\sigma:S_n\to\{\pm1\}$的像的阶为2. 如果对称群S_n的子群H为奇数阶，则它包含在σ的核——由偶置换构成的交错群A_n中. 当H是由一个在群中阶为奇数的置换q生成的循环子群时，也是这样的. 每一个奇数阶的置换(例如奇数阶循环群)为偶置换. 另一方面，我们不能对偶数阶的置换得出任何结论. 它们可以是奇的，也可以是偶的. ■

【2.10.4】命题 *令$\varphi:G\to\mathcal{G}$是一个群同态且其核为K，令$\mathcal{H}$是$\mathcal{G}$的子群. 记逆像$\varphi^{-1}(\mathcal{H})$为$H$. 则$H$是$G$的子群且$H\supset K$. 如果$\mathcal{H}$是$\mathcal{G}$的正规子群，则$H$是$G$的正规子群. 如果$\varphi$是满射，且$H$是$G$的正规子群，则$\mathcal{H}$是$\mathcal{G}$的正规子群.*

例如，令φ表示行列式同态$GL_n(\mathbf{R})\to\mathbf{R}^\times$. 正实数集合是$\mathbf{R}^\times$的子群. 它是正规子群因为$\mathbf{R}^\times$是交换的. 它的逆像——具有正的行列式值的可逆矩阵的集合——是$GL_n(\mathbf{R})$的正规子群.

证明 证明是简单的，但必须记住，φ^{-1}不是映射. 由定义，$\varphi^{-1}(\mathcal{H})=\{x\in G|\varphi(x)\in\mathcal{H}\}$. 首先，如果$x\in K$，则$\varphi(x)=1\in\mathcal{H}$，故$x\in H$. 因此$H\supset K$. 下面验证子群的条件.

封闭性：设$x,y\in H$. 则$\varphi(x),\varphi(y)\in\mathcal{H}$. 由于$\mathcal{H}$是子群，故$\varphi(x)\varphi(y)\in\mathcal{H}$. 由于$\varphi$是同态，故$\varphi(x)\varphi(y)=\varphi(xy)$. 因而$\varphi(xy)\in\mathcal{H}$，且$xy\in H$.

有恒等元：$1\in H$因为$\varphi(1)=1\in\mathcal{H}$.

逆元：令$x\in H$，则$\varphi(x)\in\mathcal{H}$. 由于$\mathcal{H}$是子群，故$\varphi(x)^{-1}\in\mathcal{H}$. 由于$\varphi$是同态，故$\varphi(x)^{-1}=\varphi(x^{-1})\in\mathcal{H}$，且$x^{-1}\in H$.

假设$\mathcal{H}$是正规子群. 令$x\in H$，$g\in G$. 则$\varphi(gxg^{-1})=\varphi(g)\varphi(x)\varphi(g)^{-1}$是$\varphi(x)$的共轭，而$\varphi(x)\in\mathcal{H}$. 因为$\mathcal{H}$是正规子群，故$\varphi(gxg^{-1})\in\mathcal{H}$，因此$gxg^{-1}\in H$.

假设φ是满射，且H是G的正规子群. 令$a\in\mathcal{H}$且$b\in\mathcal{G}$. 存在元素$x\in H$，$y\in G$使得$\varphi(x)=a$，$\varphi(y)=b$. 由于H是正规子群，$yxy^{-1}\in H$，因此$\varphi(yxy^{-1})=bab^{-1}\in\mathcal{H}$. ■

【2.10.5】定理(对应定理) *令$\varphi:G\to\mathcal{G}$是一个群满同态且其核为K. 存在$\mathcal{G}$的子群到G的包含K的子群之间的双射：*

62

$$\{G\text{的含有}K\text{的子群}\}\leftrightarrow\{\mathcal{G}\text{的子群}\}$$

这个对应定义如下：

$$G\text{的含有}K\text{的子群}H\rightsquigarrow\text{像}\varphi(H)\text{是}\mathcal{G}\text{的子群}$$

$$\mathcal{G}\text{的一个子群}\mathcal{H}\rightsquigarrow\text{其逆像}\varphi^{-1}(\mathcal{H})\text{是}G\text{的子群}$$

如果H和$\mathcal{H}$是对应的子群，则H是G的正规子群当且仅当$\mathcal{H}$是$\mathcal{G}$的正规子群.

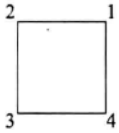
如果H和$\mathcal{H}$是对应的子群，则$|H|=|\mathcal{H}||K|$.

【2.10.6】例 回到在例2.5.13中定义的同态$\varphi:S_4\to S_3$和它的核K(2.5.15).

群S_3有6个子群，其中4个真子群. 用通常的表示，有一个3阶真子群，即循环群$\langle x\rangle$，有3个2阶子群，包括$\langle y\rangle$. 对应定理告诉我们存在4个S_4的包含K的真子群. 由于$|K|=4$，因此有一个12阶子群和3个8阶子群.

我们知道有一个12阶子群，即交错群A_4. 这是对应于S_3的循环群$\langle x\rangle$的子群.

8 阶子群可利用正方形的对称性来解释. 正方形四个顶点的标号如下图所示，通过$\frac{\pi}{2}$角度逆时针旋转对应 4-循环(**1 2 3 4**). 关于通过顶点 1 的对角线反射得到对换(**2 4**). 这两个置换生成一个 8 阶子群. 其他的 8 阶子群可以通过给正方形的顶点以另外的方式标号得到.



S_4 中也有不含 K 的一些子群. 对应定理对此没有给出讨论. ■

对应定理的证明 令 H 是 G 的含 K 的子群，$\mathcal{H}$是$\mathcal{G}$的子群. 我们必须验证下面几点：

- $\varphi(H)$是 G'的子群.
- $\varphi^{-1}(\mathcal{H})$是 G 的含 K 的子群.
- $\mathcal{H}$是$\mathcal{G}$的正规子群当且仅当 $\varphi^{-1}(\mathcal{H})$是 G 的正规子群.
- (对应的双射性)$\varphi(\varphi^{-1}(\mathcal{H}))=\mathcal{H}$且 $\varphi^{-1}(\varphi(H))=H$.
- $|\varphi^{-1}(\mathcal{H})|=|\mathcal{H}||K|$.

由于 $\varphi(H)$是同态 $\varphi|_H$ 的像，故它是$\mathcal{G}$的子群. 第二、第三条来自命题 2.10.4.

关于第四条，等式 $\varphi(\varphi^{-1}(\mathcal{H}))=\mathcal{H}$对应任意集合上的满射 $\varphi:S\to S'$和任意子集$\mathcal{H}\subset S'$成立. 而且 $H\subset\varphi^{-1}(\varphi(H))$对于任何映射和任何子集 $H\subset S$ 成立. 我们省略这些事实的验 63
证，只验证 $H\supset\varphi^{-1}(\varphi(H))$. 令 $x\in\varphi^{-1}(\varphi(H))$. 我们必须证明 $x\in H$. 由逆像的定义，$\varphi(x)\in\varphi(H)$，比如 $\varphi(x)=\varphi(a)$，$a\in H$. 则 $a^{-1}x\in K$(2.5.8)，且由于 $H\supset K$，故 $a^{-1}x\in H$. 由于 $a\in H$，$a^{-1}x\in H$，故 $x\in H$.

我们把最后一条的证明留作练习. ■

第十一节 积 群

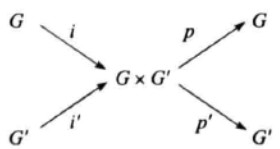
设 G，G'为两个群. 积集 $G\times G'=\{(a,a')\mid a\in G,\ a'\in G'\}$可按分量乘积构成一个群，即按如下规则

【2.11.1】
$$(a,a')\cdot(b,b')=(ab,a'b')$$

定义元素对的乘积. 元素对(1，1)是恒等元，而(a,a')的逆元是(a^{-1},a'^{-1}). $G\times G'$上的结合律由 G 和G'上的结合律得到.

这样得到的群称为 G 和G'的积，记为 $G\times G'$. 积群以简单的方式与其因子群 G 和G'相联系，我们可用由 $i(x)=(x,1)$，$i'(x')=(1,x')$，$p(x,x')=x$，$p'(x,x')=x'$定义的同态的语言加以总结：

【2.11.2】图



单同态 i，i'可用来将 G 和 G'等同于它们的像，$G\times G'$的子群 $G\times 1$，$1\times G'$. 映射 p，p'是满射，p 的核是 $1\times G'$，而 p'的核是 $G\times 1$. 这两个映射是投影.

显然，大家都期望把一个给定的群 G 分解成积，也就是说找到两个群 H 和 H'，使 G 同构于它们的积 $H\times H'$. 群 H 和 H'较简单，而且 $H\times H'$与其因子的关系也容易理解. 可是，给定的群是积的情形非常稀少，但的确偶有发生.

例如，令人惊叹的是 6 阶循环群可以被分解：一个 6 阶循环群 C_6 同构于 2 阶和 3 阶的循环群的积 $C_2\times C_3$. 要说明这点，令 $C_2=\langle y\rangle$，$C_3=\langle z\rangle$，且 $y^2=1$，$z^3=1$，令 x 表示积群$C_2\times C_3$中的元素$(y,\ z)$. 使得 $x^k=(y^k,\ z^k)$成为恒等元$(1,\ 1)$的最小正整数是 $k=6$. 故 x 的阶是 6. 由于 $C_2\times C_3$ 的阶也是 6，故 $C_2\times C_3=\langle x\rangle$. x 的方幂按照顺序为：

$$(1,1),(y,z),(1,z^2),(y,1)(1,z),(y,z^2)$$

只要两个整数 r 和 s 没有公因子，同样的论证就可用于 rs 阶循环群.

64 **【2.11.3】命题** *令整数 r 和 s 互素. rs 阶循环群同构于 r 阶循环群和 s 阶循环群的积.*

另一方面，4 阶循环群不同构于两个 2 阶循环群的积. $C_2\times C_2$ 中每个元素的阶或为 1 或为 2，而 4 阶循环群中有两个元素阶为 4.

下面的命题刻画了群的积.

【2.11.4】命题 *令 H 和 K 是群 G 的子群，令 $f:H\times K\to G$ 是乘法映射，定义为 $f(h,\ k)=hk$. 它的像是集合 $HK=\{hk\mid h\in H,\ k\in K\}$.*

(a) f 是单射的当且仅当 $H\cap K=\{1\}$.

(b) f 是积群 $H\times K$ 到群 G 的同态当且仅当 K 的元素与 H 的元素可交换：$hk=kh$.

(c) 如果 H 是 G 的正规子群，则 HK 是 G 的子群.

(d) f 是积群 $H\times K$ 到群 G 的同构当且仅当 $H\cap K=\{1\}$，$HK=G$，且 H 和 K 都是 G 的正规子群.

注意到乘法映射可以是双射尽管它可能不是群同态这点是重要的. 这种情况会发生，例如，当 $G=S_3$ 时，用通常的记号，$H=\langle x\rangle$，$K=\langle y\rangle$.

证明

(a) 如果 $H\cap K$ 包含一个元素 $x\neq 1$，则 $x^{-1}\in H$，且 $f(x^{-1},\ x)=1=f(1,\ 1)$，所以 f 不是单射. 假设 $H\cap K=\{1\}$. 令$(h_1,\ k_1)$和$(h_2,\ k_2)$是 $H\times K$ 中的元素使得 $h_1k_1=h_2k_2$. 在方程两边左乘 h_1^{-1}且右乘 k_2^{-1}，得到 $k_1k_2^{-1}=h_1^{-1}h_2$. 左边是 K 中元素，右边是 H 中元素. 由于 $H\cap K=\{1\}$，故 $k_1k_2^{-1}=h_1^{-1}h_2=1$，于是，$k_1=k_2$，$h_1=h_2$，且$(h_1,k_1)=(h_2,k_2)$.

(b) 令$(h_1,\ k_1)$和$(h_2,\ k_2)$是积群 $H\times K$ 中的元素. 这些元素在 $H\times K$ 中的积为$(h_1h_2,\ k_1k_2)$，且 $f(h_1h_2,\ k_1k_2)=h_1h_2k_1k_2$，而 $f(h_1,\ k_1)f(h_2,\ k_2)=h_1k_1h_2k_2$. 这些元素是相等的当且仅当 $h_2k_1=k_1h_2$.

(c) 假设 H 是正规子群. 我们注意 KH 是左陪集 kH 的并，其中 $k\in K$，而 HK 是所有右陪集 Hk 的并，其中 $k\in K$. 由于 H 是正规子群，$kH=Hk$，所以 $HK=KH$. HK 对

于乘法的封闭性得证，因为 $HKHK=HHKK=HK$. 还有，$(hk)^{-1}=k^{-1}h^{-1}$ 属于 $KH=HK$. 这证明了 HK 的逆元是封闭的.

(d) 假设 H 和 K 满足所给条件. 则 f 既是单射又是满射，所以是双射. 由(b)，f 是同构当且仅当对所有 $h\in H$，$k\in K$，有 $hk=kh$. 考虑交换子 $(hkh^{-1})k^{-1}=h(kh^{-1}k^{-1})$. 由于 K 是正规子群，故左边属于 K，又由于 H 是正规子群，故右边属于 H. 因为 $H\cap K=\{1\}$，故 $hkh^{-1}k^{-1}=1$，$hk=kh$. 反过来，如果 f 是同构，可以验证同构群 $H\times K$ 而不是 G 中列出的这些条件. ■

我们用这个命题对阶为 4 的群进行分类.

【2.11.5】命题 *存在两个 4 阶群的同构类. 一类是 4 阶循环群 C_4，一类是克莱因四元群，它同构于阶为 2 的两个群的积 $C_2\times C_2$.*

65

证明 令 G 是 4 阶群，故 G 的每个元素的阶都整除 4. 于是，考虑两种情形：

情形 1：G 有一个元素的阶为 4. 则 G 是 4 阶循环群.

情形 2：G 中每个除了单位元以外的元素的阶均为 2.

在此情形，对 G 中任意元素 x 有 $x=x^{-1}$. 令 x 和 y 是 G 中两个元素. 则 xy 的阶为 2，故 $xyx^{-1}y^{-1}=(xy)(xy)=1$. 这证明了 x 和 y 可交换(2.6.5)，且既然是群中任意元素，因此 G 是交换群. 故任意子群都是正规子群. 选取 G 中不同元素 x 和 y，令 H 和 K 是由 x 和 y 生成的 2 阶循环子群. 命题 2.11.4(d)表明 G 同构于积群 $H\times K$. ■

第十二节 商 群

在这一节我们将在群 G 的正规子群 N 的陪集的集合上定义合成法则. 这个运算法则使得正规子群的陪集成为一个群，称为商群.

整数模 n 的同余类的加法就是商结构的一个例子. 另一个熟悉的例子是角度的加法. 每个实数代表一个角，任意两个实数代表同一个角当且仅当它们相差 2π 的整数倍. 所有 2π 的整数倍的实数构成实数加群 $\mathbf{R}^+$ 的一个子群 N，角对应着 N 在 G 中的陪集 $\theta+N$. 角的群是元素是陪集的商群.

正规子群 N 在 G 中的陪集的集合通常用 G/N 表示.

【2.12.1】 G/N 是正规子群 N 在 G 中的陪集的集合

当把陪集 C 看成陪集集合中的元素时，用括号 $[C]$ 表示. 如果 $C=aN$，也可用加横杠的方式 $\bar{a}$ 表示元素 $[C]$，而陪集的集合记作 $\overline{G}$：

$$\overline{G}=G/N$$

【2.12.2】定理 *令 N 是 G 的正规子群，令 $\overline{G}$ 表示 N 在 G 中的陪集的集合. 存在 $\overline{G}$ 上的一个合成法则使其成为一个群，使得定义为 $\pi(a)=\bar{a}$ 的映射 $\pi:G\to\overline{G}$ 是一个核为 N 的满同态.*

注 映射 π 经常称为 G 到 $\overline{G}$ 的典范映射. “典范”是指这是仅有的一个有理由讨论的映射.

下一个推论非常简单，但很重要，值得单独列出来.

【2.12.3】推论 *令 N 是群 G 的正规子群，令 $\overline{G}$ 表示 N 在 G 中的陪集的集合. 令 $\pi:G\to\overline{G}$ 是*

典范同态. 令 a_1，…，a_k 是 G 中的元素使得积 $a_1\cdots a_k\in N$. 则 $\overline{a_1}\cdots\overline{a_k}=\overline{1}$.

66 **证明** 令 $p=a_1\cdots a_k$. 则 $p\in N$，故 $\pi(p)=\overline{p}=\overline{1}$. 由于 π 是同态，故 $\overline{a_1}\cdots\overline{a_k}=\overline{p}$. ■

定理 2.12.2 的证明 有下面几件事必须要做.

- 在 $\overline{G}$ 上定义合成法则.
- 证明 $\overline{G}$ 在此合成法则下成为一个群.
- 证明典范映射 π 是满同态.
- 证明 π 的核是 N.

我们采用下面的记号：如果 A 和 B 是群 G 的子集，则 AB 表示积 ab 的集合：

【2.12.4】 $$AB=\{x\in G\mid \text{存在 } a\in A, b\in B \text{ 使得 } x=ab\}$$

我们称此为集合的积，虽然在某些场合“集合的积”指的是元素对的集合 $A\times B$.

【2.12.5】**引理** 设 N 是群 G 的一个正规子群，则 N 的两个陪集 aN，bN 的积 $(aN)(bN)$ 仍是一个陪集，且 $(aN)(bN)=abN$.

我们注意集合 $(aN)(bN)$ 包含群 G 中所有形如 $anbn'$ 的元素，其中 n，$n'\in N$.

证明 因为 N 是子群，故 $NN=N$. 由于 N 是正规子群，故左右陪集相等：$Nb=bN$ (2.8.17). 于是由下面的形式推导证明了引理：

$$(aN)(bN)=a(Nb)N=a(bN)=abNN=abN$$ ■

这个引理使我们能够在 $\overline{G}=G/N$ 上定义乘法. 用(2.7.8)的括号记号，定义如下：如果 C_1 和 C_2 是两个陪集，则 $[C_1][C_2]=[C_1C_2]$，其中 C_1C_2 是积集. 这个引理表明积集是另一个陪集. 为计算积陪集 $[C_1][C_2]$，取任意元素 $a\in C_1$ 和 $b\in C_2$，使得 $C_1=aN$ 且 $C_2=bN$. 于是，$C_1C_2=abN$ 是含有元素 ab 的陪集. 故有非常自然的公式

【2.12.6】 $$[aN][bN]=[abN] \quad 或 \quad \overline{a}\,\overline{b}=\overline{ab}$$

这样，由映射 π 在(2.12.2)中的定义，

【2.12.7】 $$\pi(a)\pi(b)=\overline{a}\,\overline{b}=\overline{ab}=\pi(ab)$$

一旦我们证明了 $\overline{G}$ 是个群，则 π 是同态的事实就可从(2.12.7)得出. 由于典范映射 π 是满射(2.7.8)，因此下面的引理证明 $\overline{G}$ 是一个群.

【2.12.8】**引理** 令 G 是个群，且令 Y 是一个带有合成法则的集合，合成法则都用乘法记号表示. 令 $\varphi: G\to Y$ 是一个具有同态性质的满射，即对于所有 a，$b\in G$，均有 $\varphi(ab)=\varphi(a)\varphi(b)$. 则 Y 是一个群，且 φ 是同态.

67

证明 利用满射 φ 把群 G 所满足的公理推广到 Y 上. 下面是结合律的证明：令 y_1，y_2，$y_3\in Y$. 由于 φ 是满射，故 $y_i=\varphi(x_i)$，$x_i\in G$，$i=1$，2，3. 则

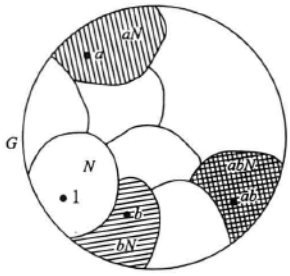
$$(y_1y_2)y_3=(\varphi(x_1)\varphi(x_2)\varphi(x_3))=\varphi(x_1x_2)\varphi(x_3)=\varphi((x_1x_2)x_3)$$

$$\overset{*}{=}\varphi(x_1(x_2x_3))=\varphi(x_1)\varphi(x_2x_3)=\varphi(x_1)(\varphi(x_2)\varphi(x_3))=y_1(y_2y_3)$$

等式中用 * 号标记的部分是群 G 的结合律. 其他部分可由 φ 的同态性质得到. 群的其他公理的验证类似可得. ■

剩下的唯一需要验证的是同态 π 的核为子群 N. $\pi(a)=\pi(1)$ 当且仅当 $\overline{a}=\overline{1}$，或 $[aN]=[1N]$，此式成立当且仅当 $a\in N$. ■

【2.12.9】图

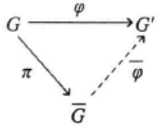


陪集乘法的简略图解

注意 在引理 2.12.5 中假设 N 是群 G 的正规子群是至关重要的. 如果 H 不是正规的，则存在 H 在 G 中的左陪集 C_1 和 C_2 使得积集 C_1C_2 不在一个左陪集内. 回到 S_3 的子群 $H=\langle y\rangle$，积集 $(1H)(xH)$ 包含 4 个元素：$\{1,\ y\}\{x,\ xy\}=\{x,\ xy,\ x^2y,\ x^2\}$. 这不是一个陪集. 子群 H 不是正规的.

下面的定理将商群的构造与一般的群同态联系起来，这个定理提供了确定(等同)商群的基本方法.

【2.12.10】**定理**(第一同构定理) 设 $\varphi:G\to G'$ 是一个满群同态，其核 $N=\ker\varphi$，则商群 $\overline{G}=G/N$ 与像 G' 同构. 准确地说，令 $\pi:G\to\overline{G}$ 是典范映射，则存在唯一一个同构映射 $\overline{\varphi}:\overline{G}\to G'$ 使得 $\varphi=\overline{\varphi}\circ\pi$.



68

证明 $\overline{G}$ 的元素是 N 的陪集，也是映射 φ 的纤维(2.7.15). 映射 $\overline{\varphi}$ 将非空纤维映射到纤维的像：$\overline{\varphi}(\overline{x})=\varphi(x)$. 对于任何集合间的满射 $\varphi:G\to G'$，可以形成纤维的集合 $\overline{G}$，然后可得到如上的图，其中 $\overline{\varphi}$ 是双射，它将一个纤维映射到它的像. 当 φ 是群同态时，$\overline{\varphi}$ 是同构，这是因为 $\overline{\varphi}(\overline{ab})=\varphi(ab)=\varphi(a)\varphi(b)=\overline{\varphi}(\overline{a})\overline{\varphi}(\overline{b})$. ■

【2.12.11】**推论** 令 $\varphi:G\to G'$ 是一个群同态，其核为 N，像为 H'. 商群 $\overline{G}=G/N$ 同构于 H'.

两个例子：绝对值映射 $\mathbf{C}^\times\to\mathbf{R}^\times$ 的像是正实数，其核是单位圆 U. 这个定理断言商群 $\mathbf{C}^\times/U$ 同构于正实数的乘法群. 另外，行列式是一个满同态 $GL_n(\mathbf{R})\to\mathbf{R}^\times$，其核为特殊线性群 $SL_n(\mathbf{R})$. 因而商群 $GL_n(\mathbf{R})/SL_n(\mathbf{R})$ 同构于 $\mathbf{R}^\times$.

还有第二、第三同构定理，虽然这些定理不如第一同构定理重要.

练　习

第一节　合成法则

1.1 令 S 是一个集合. 证明：对于任意 a，$b\in S$，由 $ab=a$ 定义的合成法则是结合的. 对怎样的集合这

个合成法则有恒等元？

1.2 证明在本节最后列出的逆的性质.

1.3 令 $\mathbf{N}$ 表示自然数集合$\{1, 2, 3, \cdots\}$，且令 $s:\mathbf{N}\to\mathbf{N}$ 是平移映射，定义为 $s(n)=n+1$. 证明 s 没有右逆，但有无穷多个左逆.

第二节 群与子群

2.1 作出对称群 S_3 的乘法表.

2.2 令 S 是具有恒等元和合成法则满足结合律的集合. 证明 S 的所有具有逆元的集合构成一个群.

2.3 令 x，y，z 和 w 是群 G 中的元素.

(a) 已知 $xyz^{-1}w=1$，求 y.

69 (b) 设 $xyz=1$，是否可据此得出 $yzx=1$ 或 $yxz=1$?

2.4 在下列何种情形下 H 是 G 的子群？

(a) $G=GL_n(\mathbf{C})$，$H=GL_n(\mathbf{R})$.

(b) $G=\mathbf{R}^\times$，$H=\{1, -1\}$.

(c) $G=\mathbf{R}^+$，H 是正整数集合.

(d) $G=\mathbf{R}^\times$，H 是正实数集合.

(e) $G=GL_2(\mathbf{R})$和 H 是所有形如$\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$的矩阵的集合，其中 $a\neq 0$.

2.5 在子群的定义中，子群 H 的恒等元要求是群 G 的恒等元. 可以只要求子群 H 有恒等元，不必要求此恒等元为群 G 的恒等元. 证明：如果 H 有恒等元，则这个恒等元是群 G 的恒等元. 类似地证明子群 H 中的逆元也是其在群 G 中的逆元.

2.6 令 G 是一个群. 定义一个*反群* G°有下面的合成法则 $a*b$：基础集合还是集合 G，但合成法则是 $a*b=ba$. 证明 G°是一个群.

第三节 整数加群的子群

3.1 令 $a=123$ 且 $b=321$. 求 $d=\gcd(a, b)$，并把 d 表示成 $ra+bs$ 的形式.

3.2 证明：如果正整数 a，b 的和是一个素数 p，则 $\gcd(a, b)=1$.

3.3 (a) 定义集合$\{a_1, a_2, \cdots, a_n\}$的最大公约数. 证明它是整数 a_1，a_2，$\cdots$，a_n 的组合.

(b) 如果$\{a_1, a_2, \cdots, a_n\}$的最大公约数是 d，则$\{a_1/d, a_2/d, \cdots, a_n/d\}$的最大公约数是 1.

第四节 循环群

4.1 令 a 和 b 是群 G 的元素. 设 a 的阶为 7 且 $a^3b=ba^3$. 证明 $ab=ba$.

4.2 一个 n 次单位根是一个复数 z 满足 $z^n=1$.

(a) 证明单位元的 n 次方根构成 $\mathbf{C}^\times$ 的 n 阶循环子群.

(b) 确定所有单位元的 n 次方根的积.

4.3 令 a 和 b 是群 G 的元素. 证明 ab 和 ba 有相同的阶.

4.4 刻画所有没有真子群的群.

4.5 证明循环群的任意子群还是循环群. 通过研究指数并应用对 $\mathbf{Z}^+$ 的子群的描述来加以证明.

4.6 (a) 令 G 是 6 阶循环群. G 有多少生成元？对 5 阶和 8 阶循环群讨论同样的问题.

(b) 讨论任意阶循环群的生成元的个数.

4.7 令 x 和 y 是群 G 的元素. 设 x，y 和 xy 的阶均为 2. 证明集合 $H=\{1, x, y, xy\}$是 G 的子群，且

70 阶为 4.

4.8 (a) 证明(1.2.4)中第一、第三型初等矩阵生成 $GL_n(\mathbf{R})$.

(b) 证明(1.2.4)中第一型初等矩阵生成 $SL_n(\mathbf{R})$. 先对 2×2 矩阵证明此结论.

4.9 对称群 S_4 有多少个 2 阶的元素?

4.10 举例说明群中有限阶元素的积未必是有限阶的. 如果是交换群呢?

4.11 (a) 采用行约简的方法证明对换生成对称群 S_n.

(b) 对于 $n\geqslant 3$, 证明 3-循环生成交错群 A_n.

第五节 同态

5.1 设 $\varphi: G\to G'$ 是群的满同态. 证明: 若 G 是循环群, 则 G' 也是循环群; 若 G 是阿贝尔群, 则 G' 也是阿贝尔群.

5.2 设 H 和 K 是群 G 的子群, 则 $H\cap K$ 是 H 的子群, 且如果 K 是 G 的正规子群, 则 $H\cap K$ 是 H 的正规子群.

5.3 令 U 是 2×2 可逆上三角矩阵 $A=\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ 的群, 且 $\varphi: U\to \mathbf{R}^\times$ 满足 $A\rightsquigarrow a^2$. 证明 φ 是同态, 并求此同态的核和像.

5.4 令 $f: \mathbf{R}^+\to \mathbf{C}^\times$ 满足 $f(x)=\mathrm{e}^{ix}$. 证明 f 是同态, 并求此同态的核和像.

5.5 证明: 形如 $M=\begin{bmatrix} A & B \\ 0 & D \end{bmatrix}$ 的 $n\times n$ 分块矩阵构成 $GL_n(\mathbf{R})$ 的一个子群 H, 其中 $A\in GL_r(\mathbf{R})$, $D\in GL_{n-r}(\mathbf{R})$; 且映射 $\varphi: H\to GL_r(\mathbf{R})$ 满足 $M\rightsquigarrow A$ 是一个同态. 同态的核是什么?

5.6 确定 $GL_n(\mathbf{R})$ 的中心.

提示: 要求可逆矩阵 A 使得其与任何可逆矩阵 B 可换. 不要用一般矩阵尝试, 要用初等矩阵尝试.

第六节 同构

6.1 令 G' 是形如 $\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$ 的实矩阵群. 映射 $\mathbf{R}^+\to G'$ 将 $x\to \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$ 是同构映射吗?

6.2 刻画所有同态 φ: $\mathbf{Z}^+\to\mathbf{Z}^+$. 确定哪些是单射, 哪些是满射, 哪些是同构.

6.3 证明: 函数 $f=\dfrac{1}{x}$, $g=\dfrac{x-1}{x}$ 生成一个函数群, 合成法则是函数的合成, 它同构于对称群 S_3.

6.4 证明: 在群中, 积 ab 和 ba 是共轭元.

6.5 确定两个矩阵 $A=\begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix}$ 与 $B=\begin{bmatrix} 1 & 1 \\ -2 & 4 \end{bmatrix}$ 在一般线性群 $GL_2(\mathbf{R})$ 中是否为共轭元. 71

6.6 矩阵 $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ 和 $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ 是否为 $GL_2(\mathbf{R})$ 中的共轭元? 是否为 $SL_2(\mathbf{R})$ 中的共轭元?

6.7 令 H 是 G 的子群, 并设 $g\in G$. 共轭子群 gHg^{-1} 定义为所有共轭 ghg^{-1} 的集合, 其中 $h\in H$. 证明 gHg^{-1} 是 G 的子群.

6.8 证明映射 $A\rightsquigarrow (A^t)^{-1}$ 是 $GL_2(\mathbf{R})$ 的自同构.

6.9 证明群 G 和它的反群 G^o(练习 2.6)同构.

6.10 确定下列群的自同构群.

(a) 10 阶循环群, (b)对称群 S_3.

6.11 令 a 是群 G 的元素. 证明: 如果集合 $\{1, a\}$ 是 G 的正规子群, 则 a 属于 G 的中心.

第七节 等价关系和划分

7.1 令 G 是一个群，证明：对于某个 $g\in G$ 使得 $b=gag^{-1}$ 的关系 $a\sim b$ 是一个等价关系.

7.2 集合 S 上等价关系由 $S\times S$ 的满足 $a\sim b$ 的对(a, b)所组成的集合 R 来确定. 将等价关系的公理用子集 R 来表示.

7.3 用练习 7.2 中的记号，两个等价关系 R 和 R' 的交 $R\cap R'$ 是否是等价关系？$R\cup R'$ 是否是等价关系？

7.4 设 R 是实数集合上的一个等价关系. R 可视为(x, y)平面的子集. 用练习 7.2 中的记号，解释自反性和对称性的几何意义.

7.5 用练习 7.2 中的记号，下面(x, y)平面的子集 R 定义了实数集合 $\mathbf{R}$ 上的一个关系. 确定哪个关系满足公理(2.7.3).

(a) $R=\{(s, s)\mid s\in\mathbf{R}\}$.

(b) $R=$空集.

(c) $R=$轨迹$\{xy+1=0\}$.

(d) $R=$轨迹$\{x^2y-xy^2-x+y=0\}$.

7.6 5 个元素的集合上可以定义多少种等价关系？

第八节 陪集

8.1 令 H 是交错群 A_4 的一个由置换**(1 2 3)**生成的循环子群. 具体写出 H 的所有左陪集和右陪集.

8.2 在实向量加群 $\mathbf{R}^m$ 中，令 W 是齐次线性方程组 $AX=0$ 的解集合. 证明非齐次线性方程组 $AX=B$ 的解集合或为空集或为 W 的一个(加法)陪集.

8.3 阶为某个素数 p 的方幂的群含有阶为 p 的元素吗？

8.4 阶为 35 的群是否含有阶为 5 的元素？是否含有阶为 7 的元素？

8.5 一个有限群包含阶为 10 的元素 x，也包含阶为 6 的元素 y，对该群 G 的阶有什么结论？

72 8.6 令 $\varphi:G\to G'$ 是群同态. 假设 $|G|=18$，$|G'|=15$，且 φ 不是平凡同态. 同态核的阶是多少？

8.7 22 阶群 G 包含元素 x 和 y，其中 $x\neq1$，y 不是 x 的幂. 证明由这些元素生成的子群是整个群 G.

8.8 令 G 是一个 25 阶群. 证明 G 至少有一个 5 阶子群，且如果它只有一个 5 阶子群，则此群是循环群.

8.9 令 G 是一个有限群. 在什么情况下由 $\varphi(x)=x^2$ 定义的映射 $\varphi:G\to G$ 是群 G 的自同构？

8.10 证明指标为 2 的任意子群为正规子群. 举例说明指标为 3 的子群未必是正规子群.

8.11 令 G 和 H 是 $GL_2(\mathbf{R})$的以下形式的子群：

$$G=\left\{\begin{bmatrix}x & y\\ 0 & 1\end{bmatrix}\right\},H=\left\{\begin{bmatrix}x & 0\\ 0 & 1\end{bmatrix}\right\}$$

其中 x 和 y 是实数，且 $x>0$. 群 G 中的元素可由右半平面的点来表示. 简要证明半平面可以分划为 H 的左陪集和右陪集.

8.12 令 S 是群 G 的包含恒等元 1 的子集，且使得左陪集 $aS(a\in G)$划分群 G. 证明 S 是 G 子群.

8.13 令 S 是一个带有合成法则的集合. S 的一个划分 $\Pi_1\cup\Pi_2\cup\cdots$ 是与合成法则相容的，对于所有 i 和 j，积集

$$\Pi_i\Pi_j=\{xy\mid x\in\Pi_i, y\in\Pi_j\}$$

包含在划分的某个单个子集 Π_k 中.

(a) 整数集合 $\mathbf{Z}$ 可以划分为三个子集[正整数]，[负整数]，[$\{0\}$]. 讨论合成法则 $+$，$\times$ 与这个划分的相容程度.

(b) 刻画与加法相容的所有整数集合的划分.

第九节 模算术

9.1 对于怎样的整数 n 使得 2 在 $\mathbf{Z}/\mathbf{Z}n$ 中有乘法逆元?

9.2 a^2 模 4 的可能值是什么? 模 8 呢?

9.3 证明每个整数 a 模 9 同余于其十进制各位数之和.

9.4 解同余方程 $2x\equiv 5$ 模 9 和模 6.

9.5 确定使同余方程 $2x-y\equiv 1$, $4x+3y\equiv 2(\mathrm{mod}\ n)$有解的整数 n.

9.6 证明中国剩余定理: 设 a, b, u, v 为整数, 且设 a, b 的最大公约数是 1, 则存在整数 x 使 $x\equiv u(\mathrm{mod}\ a)$且 $x\equiv b(\mathrm{mod}\ b)$.

提示: 先讨论 $u=0$, $v=1$ 的情形.

9.7 确定每一个矩阵 $A=\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$和 $B=\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}$的阶, 其中矩阵元素是模 3 同余的. 73

第十节 对应定理

10.1 描述如何从循环分解中区分一个置换是奇还是偶的.

10.2 令 H 和 K 是群 G 的子群.

(a) 证明 H 和 K 的两个陪集的交集 $xH\cap yK$ 或为空集或为子群 $H\cap K$ 的一个陪集;

(b) 如果 H 和 K 在 G 中的指标是有限的, 则 $H\cap K$ 在 G 中的指标也是有限的.

10.3 令 G 和 G' 是分别由 x 和 y 生成的 12 阶和 6 阶循环群, 令 $\varphi:G\to G'$ 是由 $\varphi(x^i)=y^i$ 定义的映射. 具体列出在对应定理中提到的对应.

10.4 用对应定理中的记号, 令 H 和 H' 是对应子群. 证明$[G:H]=[G':H']$.

10.5 参照在例 2.5.13 中的同态 $S_4\to S_3$, 确定 S_4 的包含核 K 的 6 个子群.

第十一节 积群

11.1 令 x 是群 G 中阶为 r 的元素, y 是群 G' 中阶为 s 的元素, 元(x, y)在积群 $G\times G'$ 中的阶是多少?

11.2 用对称群 S_3 的通常记号, 当 H 和 K 是子群$\langle y\rangle$和$\langle x\rangle$时, 命题 2.11.4 告诉我们什么?

11.3 证明两个无限循环群的积不是无限循环群.

11.4 在下面每一种情形中, 确定 G 是否同构于积群 $H\times K$.

(a) $G=\mathbf{R}^\times$, $H=\{\pm 1\}$, $K=\{$正实数$\}$.

(b) $G=\{2\times 2$ 可逆上三角矩阵$\}$, $H=\{$可逆对角矩阵$\}$, $K=\{$对角线元素为 1 的上三角矩阵$\}$.

(c) $G=\mathbf{C}^\times$, $H=\{$单位圆$\}$, $K=\{$正实数$\}$.

11.5 令 G_1 和 G_2 是群, 且 Z_i 是 G_i 的中心. 证明积群 $G_1\times G_2$ 的中心为 $Z_1\times Z_2$.

11.6 令 G 是一个分别包含阶为 3 和阶为 5 的正规子群的群. 证明 G 包含一个阶为 15 的元素.

11.7 令 H 是 G 的子群, 令 $\varphi:G\to H$ 是一个同态, 其在 H 上的限制为恒等映射, 令 N 是其核. 关于乘积映射 $H\times N\to G$ 有何结论?

11.8 令 G, G' 和 H 是群. 建立从 H 到积群的同态 $\Phi:H\to G\times G'$ 以及由同态 $\varphi:H\to G$ 和 $\varphi':H\to G'$ 构成的对(φ, φ').

11.9 令 H 和 K 是 G 的子群. 证明集合的积 HK 是 G 的子群当且仅当 $HK=KH$.

第十二节 商群

12.1 证明: 如果子群 H 不是群 G 的正规子群, 则存在左陪集 aH 与 bH, 它们的积不是陪集. 74

12.2 在一般线性群 $GL_3(\mathbf{R})$ 中，考虑形如

$$H=\begin{bmatrix}1 & * & *\\ & 1 & *\\ & & 1\end{bmatrix} \quad 和 \quad K=\begin{bmatrix}1 & 0 & *\\ & 1 & 0\\ & & 1\end{bmatrix}$$

的子集，其中 $*$ 代表任意实数. 证明 H 是 GL_3 的子群，K 是 H 的正规子群，确定商群 H/K. 确定 H 的中心.

12.3 令 P 是群 G 的划分且具有如下性质：对于划分中任意两个元素对 A，B，集合的积 AB 完全包含在划分的另一个元素 C 中. 令 N 是划分 P 的一个元素且包含 1. 证明 N 是 G 的正规子群且 P 是其陪集的集合.

12.4 令 $H=\{\pm 1, \pm i\}$ 是群 $G=\mathbf{C}^{\times}$ 中的四次单位根组成的子群. 明确写出 H 在 G 中的陪集. G/H 与 G 同构吗？

12.5 令 G 是上三角实矩阵 $\begin{bmatrix}a & b\\ 0 & d\end{bmatrix}$ 所组成的群，其中 $a\neq 0$，$d\neq 0$，对于下列子集 S，确定其是否为子群，是否为正规子群. 如果 S 是正规子群，确定商群 G/S.

(i) S 是定义中满足 $b=0$ 的子集.

(ii) S 是定义中满足 $d=1$ 的子集.

(iii) S 是定义中满足 $a=d$ 的子集.

杂题

M.1 描述一个整数矩阵 A 当其逆矩阵也是整数矩阵时其第一列列向量 $(a, c)^t$ 是什么.

M.2 (a) 每个偶数阶群都包含一个阶为 2 的元素.

(b) 每个 21 阶群都包含一个阶为 3 的元素.

M.3 分析下列三种情况，对 6 阶群进行分类：

(i) G 包含一个阶为 6 的元素.

(ii) G 包含一个阶为 3 的元素，但不包含一个阶为 6 的元素.

(iii) G 的所有元素的阶为 1 或 2.

M.4 一个*半群* S 是一个带有满足结合律的合成法则且有恒等元的集合. 元素不要求有逆元，且消去律不必成立. 一个半群 S 称为是由元素 s 生成的，如果 s 的非负幂的集合 $\{1, s, s^2, \cdots\}$ 等于 S. 对一个生成元的半群进行分类.

M.5 令 S 是一个满足削去律 2.2.3 的有限半群(见练习 M.4)，证明 S 是群.

*M.6 令 $a=(a_1, \cdots, a_k)$ 和 $b=(b_1, \cdots, b_k)$ 是 k 维空间 $\mathbf{R}^k$ 中的点. 从 a 到 b 的一条*路*是一个在 $\mathbf{R}^k$ 的区间 $[0, 1]$ 上取值的连续函数，即函数 $X:[0, 1]\to\mathbf{R}^k$，使 $t\rightsquigarrow X(t)=(x_1(t), \cdots, x_k(t))$，满足条件 $X(0)=a$ 和 $X(1)=b$. 若 S 是 $\mathbf{R}^k$ 的子集且 $a, b\in S$，定义 $a\sim b$，如果 a，b 可由一条完全在 S 中的路连起来.

75

(a) 证明 $\sim$ 是 S 上的一个等价关系. 注意你构造的路在集合 S 中.

(b) $\mathbf{R}^k$ 的子集 S 称为*路连通的*，如果对任意两点 a，$b\in S$，有 $a\sim b$ 成立. 证明 S 的任意子集可划分为路连通子集，而且不同子集中的两个点不能由 S 中的路连接.

(c) $\mathbf{R}^2$ 中的下列轨道中哪些是路连通的？$\{x^2+y^2=1\}$，$\{xy=0\}$，$\{xy=1\}$.

*M.7 $n\times n$ 矩阵集合可以等同于空间 $\mathbf{R}^{n\times n}$. 设 G 是 $GL_n(\mathbf{R})$ 的子群. 用练习 M.6 的记号，证明：

(a) 如果 A，B，C，$D \in G$，且如果 G 中有 A 到 B 的路和 C 到 D 的路，则 G 中有一条 AC 到 BD 的路.

(b) 可以连到恒等矩阵 I 的矩阵集合构成 G 的一个正规子群(称为 G 的连通分支).

*M. 8 (a) 群 $SL_n(\mathbf{R})$由第一型的初等矩阵生成(见练习 4.8). 用这一事实证明这个群是路连通的.

(b) 证明 $GL_n(\mathbf{R})$是两个路连通子集的并，并描述它们.

M. 9 (双陪集)令 H 和 K 是群 G 的子群，令 g 是 G 的元素. 集合

$$HgK = \{x \in G \mid x = hgk, \quad h \in H, k \in K\}$$

称为双陪集. 双陪集是群 G 的划分吗?

M. 10 令 H 是群 G 的子群. 证明双陪集(参见练习 M. 9)

$$HgH = \{h_1 g h_2 \mid h_1, h_2 \in H\}$$

是左陪集 gH 当且仅当 H 是正规的.

*M. 11 大多数可逆矩阵可以写成一个下三角矩阵 L 和一个上三角矩阵 U 且 U 的主对角线元素为 1 的矩阵乘积 $A=LU$.

(a) 当矩阵 A 已知，如何求 L 和 U.

(b) 证明分解的唯一性，即存在至多一种方式将矩阵 A 表示成这样的乘积.

(c) 证明每个可逆矩阵可以写成乘积 LPU 的形式，其中 L 和 U 同上，P 是置换矩阵.

(d) 刻画双陪集 LgU(参见练习 M. 9).

M. 12 (邮票问题)令 a 和 b 是互素的正整数.

(a) 证明每个充分大的正整数 n 可写成 $ra+sb$ 的形式，其中 r，s 为正整数.

(b) 确定不具有这种形式的最大整数.

M. 13 (一个游戏)初始位置为点(1，1)，一个点(a, b)只允许移动到点$(a+b, b)$或$(a, a+b)$. 这样从始点移动一步后的位置是(2，1)或(1，2). 确定能到达的点.

M. 14 (生成 $SL_2(\mathbf{Z})$)证明两个矩阵

$$E = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, E' = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

76

生成所有行列式为 1 的整数矩阵的群 $SL_2(\mathbf{Z})$. 记住它们生成的子群由四个元素 E，E'，E^{-1}，E'^{-1}的积构成.

提示：不要直接将矩阵写成生成元的乘积. 用行约简.

M. 15 (初等矩阵生成的半群)确定矩阵 A 的半群 S(见练习 M. 4)，其中矩阵 A 是由下面两个矩阵作为项的任意长度的矩阵乘积：

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad 或 \quad \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

证明 S 中每个元素恰有一种方式可以表示为乘积的形式.

M. 16 (同音群：一个数学娱乐)由定义，英语单词是同音的，如果它们的音标在字典里是相同的. 同音群$\mathcal{H}$由字母表的字母生成，并服从下面的关系：发音相同的英文单词看做群中相同的元素，例如 $be=bee$，且由于$\mathcal{H}$是群，我们可以消去 be 得到 $e=1$. 试着确定群$\mathcal{H}$.

77

第三章　向量空间

总是从最简单的例子开始.

——David Hilbert

第一节　$\mathbf{R}^n$ 的子空间

向量空间的基本模型——这章的主题——是 n 维实向量空间 $\mathbf{R}^n$ 的子空间. 我们在本节里讨论它们. 向量空间的定义将在第三节给出.

尽管行向量写起来占的空间少，但矩阵乘法定义使列向量用起来更方便，所以，我们通常情况下使用列向量. 为节省空间，我们有时用矩阵的转置形式 $(a_1, \cdots, a_n)^t$ 写列向量. 如同第一章提到的，我们不区分列向量和 $\mathbf{R}^n$ 中有相同坐标的点. 列向量常记为小写字母 v 或 w，并且如果 v 等于 $(a_1, \cdots, a_n)^t$，则称 $(a_1, \cdots, a_n)^t$ 为 v 的坐标向量.

考虑向量的两个运算：

【3.1.1】

$$\text{向量加法：}\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} + \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} a_1 + b_1 \\ \vdots \\ a_n + b_n \end{bmatrix}$$

$$\text{标量乘法：} c\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} ca_1 \\ \vdots \\ ca_n \end{bmatrix}$$

这些运算使 $\mathbf{R}^n$ 成为一个向量空间.

(3.1.1)的 $\mathbf{R}^n$ 的一个子集 W 是子空间，如果它有下述性质：

【3.1.2】

78

(a) 如果 w 与 w' 是 W 里的向量，则 $w+w'$ 也是 W 里的向量.

(b) 如果 w 是 W 里的向量，c 是 $\mathbf{R}$ 的数，则 cw 也是 W 里的向量.

(c) 零向量在 W 里.

有另一种方式叙述子空间的条件：

【3.1.3】 W 是非空的，并且如果 $w_1, w_2, \cdots, w_n$ 是 W 里的元素，而 $c_1, c_2, \cdots, c_n$ 是标量，则线性组合 $c_1w_1 + c_2w_2 + \cdots + c_nw_n$ 也是 W 里的向量.

齐次线性方程组给出的例子：已知一个系数在 $\mathbf{R}$ 里的 $m \times n$ 矩阵 A，$\mathbf{R}^n$ 中所有坐标向量为齐次方程 $AX=0$ 的解的集合是一个子空间，称为 A 的**迷向子空间**. 虽然这是很简单的，但我们将检验子空间的条件.

- $AX=0$ 与 $AY=0$ 蕴含着 $A(X+Y)=0$：如果 X 与 Y 都是解，则 $X+Y$ 也是解.

- $AX=0$ 蕴含着 $AcX=0$：如果 X 是一个解，则 cX 也是解.
- $A0=0$：零向量是解.

零空间 $W=\{0\}$ 与整个空间 $W=\mathbf{R}^n$ 是子空间. 一个子空间是真子空间，如果它不是二者之一. 下一个命题描述了 $\mathbf{R}^2$ 的真子空间.

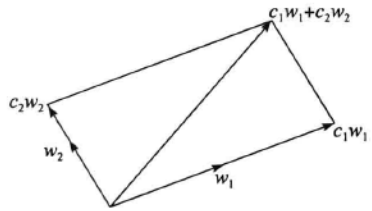
【3.1.4】命题 *令 W 是 $\mathbf{R}^2$ 的真子空间，且 w 是 W 的一个非零向量. 则 W 由 w 的标量倍数 cw 组成. 不同的真子空间有唯一的公共零向量.*

由已知非零向量 w 的标量倍数 cw 组成的子空间称为由 w 张成的子空间. 几何上，它是 $\mathbf{R}^2$ 中通过原点的直线.

命题的证明 首先注意由非零向量 w 张成的子空间 W 也是由 W 所包含的任意其他非零向量 w' 所张成的. 这是因为如果 $w'=cw$ 且 $c\neq 0$，则任一倍数 aw 也可写成 $ac^{-1}w'$ 的形式. 因此，分别由向量 w_1 和 w_2 张成的子空间 W_1 和 W_2 如果有非零的公共向量 v，则这两个子空间相等.

其次，$\mathbf{R}^2$ 的非零子空间 W 含非零元素 w_1. 因为 W 是子空间，所以它包含由 w_1 张成的子空间 W_1，并且如果 $W_1=W$，那么 W 由一个非零向量的标量倍数组成. 我们证明如果 W 不等于 W_1，那么它是整个空间 $\mathbf{R}^2$. 令 w_2 是在 W 里而不在 W_1 里的元素，并且令 W_2 是由 w_2 张成的子空间. 由于 $W_1\neq W_2$，这两个子空间的交仅含有 0 向量. 所以，向量 w_1 和 w_2 的任一个都不是另一个的倍数. 因此，w_i 的坐标向量(称为 A_i)是不成比例的，从而以这些向量作为列的 2×2 分块矩阵 $A=[A_1\mid A_2]$ 的行列式非零. 在此情形下，对任意向量 v 的坐标向量 B 解方程 $AX=B$，得线性组合 $v=w_1x_1+w_2x_2$. 这表明 W 是整个空间 $\mathbf{R}^2$. ■

几何上从向量加法的平行四边形法则也可看出每个向量是线性组合 $c_1w_1+c_2w_2$. 79



我们给出的 $\mathbf{R}^2$ 的子空间的描述在第四节通过维数概念进行阐明.

第二节 域

如同在第一章开始所提到的，本质上，关于矩阵运算的所有结论对于复数矩阵如同实数矩阵一样都是成立的，对于其他数系也是都成立的. 为描述这些数系，我们列出“标量”所需要的性质，这样就产生了域的概念. 在转到本章主要话题——向量空间——之前我们在此介绍域.

复数域 $\mathbf{C}$ 的子域是要描述的最简单的域. $\mathbf{C}$ 的子域是在四则运算加、减、乘、除下封闭且包含 1 的任意子集. 换言之，F 是 $\mathbf{C}$ 的一个子域，如果它具有下列性质：

【3.2.1】 $(+,-,\times,\div,1)$

- 若 a，$b\in F$，则 $a+b\in F$.
- 若 $a\in F$，则 $-a\in F$.
- 若 a，$b\in F$，则 $ab\in F$.
- 若 $a\in F$ 且 $a\neq 0$，则 $a^{-1}\in F$.
- $1\in F$.

这些蕴含着 $1-1=0$ 是 F 的一个元. 另一种叙述方式是说 F 是加群 $\mathbf{C}^+$ 的子群，而且 F 的非零元构成乘法群 $\mathbf{C}^\times$ 的子群.

一些 $\mathbf{C}$ 的子域的例子如下：

(a) 实数域 $\mathbf{R}$.

(b) 有理数(即整数的分数)域 $\mathbf{Q}$.

(c) 形如 $a+b\sqrt{2}$ 的所有复数的域 $\mathbf{Q}[\sqrt{2}]$，其中 a，$b\in\mathbf{Q}$.

抽象域的概念比起 $\mathbf{C}$ 的子域更难于掌握，但它包含了重要的新的域类，其中包括有限域.

【3.2.2】**定义** *域 F 是具有称为加法和乘法的两个合成法则*

$$F\times F\xrightarrow{+}F \qquad \text{和} \qquad F\times F\xrightarrow{\times}F$$
$$a,b \rightsquigarrow a+b \qquad\qquad a,b \rightsquigarrow ab$$

80 *并且满足下列公理的集合：*

(i) *加法使 F 成为阿贝尔群 F^+，其单位元记为 0.*

(ii) *乘法是交换的，并且使 F 的非零元集成为一个阿贝尔群 $F^\times$，其单位元记为 1.*

(iii) *分配律：对所有 a，b，$c\in F$，$a(b+c)=ab+ac$.*

前面两个公理分别描述加法和乘法的合成法则. 第三个公理(也就是分配律)是联系加法和乘法的.

实数满足这些公理，但它们就是通常代数运算所需要的全部公理，这一事实只有在使用它们后才能理解.

下一引理解释零元在乘法运算上的作用.

【3.2.3】**引理** *令 F 是域.*

(a) *F 的元素 0 与 1 是不同的.*

(b) *对 F 里的所有元素 a，有 $a0=0$ 与 $0a=0$.*

(c) *F 里的乘法满足结合律，并且 1 是恒等元.*

证明

(a) 公理(ii)蕴含着 1 不等于 0.

(b) 因 0 是加法恒等元，故 $0+0=0$. 于是 $a0+a0=a(0+0)=a0$. 由于 F^+ 是群，因此可消去 $a0$ 得 $a0=0$，从而得 $0a=0$.

(c) 因 $F-\{0\}$ 是阿贝尔群，故乘法运算限制到这个子集时是结合的. 我们需要证明当这

些元素至少有一个是0时，$a(bc)=(ab)c$. 在这种情形下，(b)表明所讨论的乘积为零. 最后，元素1是$F-\{0\}$上的恒等元. (b)中置$a=1$就证明了1在F的所有元素上是恒等的. ■

除复数的子域之外，最简单的域是称为素域的一些有限域，下面就来描述它们. 在第二章第九节中，我们看到，模n同余类的集合$\mathbf{Z}/n\mathbf{Z}$具有由整数的加法和乘法导出的加法和乘法法则. 对于整数，除了公理(ii)中乘法逆的存在性以外，域的所有公理都成立. 整数对除法不封闭. 正如我们面前所指出的，这些公理也延续到了同余类的加法和乘法. 但没有理由假定同余类存在乘法逆，事实上，逆也不一定存在. 例如，类2模6没有乘法逆. 因而，下面的事实是令人惊奇的：若p是素数，则所有模p非零的同余类皆有逆，这样集合$\mathbf{Z}/p\mathbf{Z}$是域. 这个域称为素域，通常记作$\mathbf{F}_p$.

用横杠记号并且选取模p同余类的通常代表元，

【3.2.4】 $$\mathbf{F}_p = \{\bar{0},\bar{1},\cdots,\overline{p-1}\} = \mathbf{Z}/p\mathbf{Z}$$

【3.2.5】**定理** *令p是一个素整数. 每一个非零同余类$\bar{a}(\mathrm{mod}\ p)$有乘法逆，因而$\mathbf{F}_p$是阶为p的域.*

在给出此定理证明之前先讨论下面定理. 81

如果a和b是整数，则$\bar{a}\neq 0$意思是p不能整除a，而$\overline{ab}=\bar{1}$意思是$ab\equiv 1(\mathrm{mod}\ p)$. 这个定理用同余的术语可以叙述如下：

【3.2.6】 设p是素数，并设a是不能被p整除的任意整数.

则有整数b使得$ab\equiv 1(\mathrm{mod}\ p)$.

一般来说，求同余类$\bar{a}(\mathrm{mod}\ p)$的逆并不容易，但当p不大时，可以通过反复试验找到. 一个系统的方法是计算$\bar{a}$的幂. 例如，设$p=13$而$\bar{a}=\bar{3}$，则$\bar{a}^2=\bar{9}$而$\bar{a}^3=\overline{27}=\bar{1}$. 我们幸运地得到：$\bar{a}$的阶为3且$\bar{3}^{-1}=\bar{3}^2=\bar{9}$. 另一方面，$\bar{6}$的幂遍历模13的每一个非零同余类. 计算幂也许不是求得$\bar{6}$的逆的最快的方法，但定理告诉我们非零同余类集$\mathbf{F}_p^\times$构成群. 所以，$\mathbf{F}_p^\times$的每一元素$\bar{a}$是有限阶的，并且如果$\bar{a}$有阶r，它的逆将是$\bar{a}^{(r-1)}$.

为了利用这种推理证明定理，我们需要消去律.

【3.2.7】**命题(消去律)** *令p是一个素整数，并且令$\bar{a}$，$\bar{b}$与$\bar{c}$是$\mathbf{F}_p$的元素.*

(a) 如果$\bar{a}\bar{b}=\bar{0}$，那么$\bar{a}=\bar{0}$或$\bar{b}=\bar{0}$.

(b) 如果$\bar{a}\neq\bar{0}$并且如果$\bar{a}\bar{b}=\bar{a}\bar{c}$，那么$\bar{b}=\bar{c}$.

证明

(a) 我们用整数a与b表示同余类$\bar{a}$与$\bar{b}$. 这时引理的断言变成：如果p整除ab，那么p整除a或p整除b. 这是推论2.3.7.

(b) 如果$\bar{a}\neq\bar{0}$并且$\bar{a}(\bar{b}-\bar{c})=\bar{0}$，那么由(a)知$\bar{b}-\bar{c}=\bar{0}$. ■

定理3.2.5的证明 设$\bar{a}\in F_p$是任意非零元. 考虑幂1，$\bar{a}$，$\bar{a}^2$，$\bar{a}^3$，…因为有无限多个幂而$\mathbf{F}_p$中仅有有限多个元素，所以必有两个幂是相等的，比如说$\bar{a}^m=\bar{a}^n$，其中$m<n$. 在等式两边消去$\bar{a}^m$得：$\bar{1}=\bar{a}^{(n-m)}$. 因此，$\bar{a}^{(n-m-1)}$是$\bar{a}$的逆. ■

为方便下面讨论，我们去掉字母上面的横杠，相信我们记得住何时用整数何时用同余类以及规则(2.9.8)：

如果 a 和 b 是整数，那么 $\mathbf{F}_p$ 中 $a=b$ 意味着 $a\equiv b(\mathrm{mod}\ p)$.

一般来说，与同余一样，域 $\mathbf{F}_p$ 中的计算也可以通过整数来进行，除了除法以外. 可以用 $\mathbf{F}_p$ 中的元素构成的矩阵 A 进行运算，不加变化地重复第一章的讨论.

假如要在素域 $\mathbf{F}_p$ 中求解 n 个具有 n 个未知量的线性方程的方程组. 以合适的方式选择同余类的代表，将方程组用一个整数方程组表示，比如说，$AX=B$，其中 A 是一个 $n\times n$ 整数矩阵，而 B 是一个整数列向量. 要在 $\mathbf{F}_p$ 中解方程组，我们模 p 求矩阵 A 的逆. 公式

82 $\mathrm{cof}(A)A=\delta I$ 对整数矩阵成立，其中 $\delta=\det A$(定理 1.6.9)，因而当矩阵元素由其同余类代替时，其在 $\mathbf{F}_p$ 中也成立. 若 δ 的同余类非零，则可以通过计算 $\delta^{-1}\mathrm{cof}(A)$ 在 $\mathbf{F}_p$ 中求 A 的逆.

【3.2.8】推论 *令 $AX=B$ 是 n 个具有 n 个未知量的线性方程组，其中 A，B 的元素属于 $\mathbf{F}_p$. 设 $\delta=\det A$. 如果 δ 不为零，则方程组在 $\mathbf{F}_p$ 中有唯一解.*

例如，考虑线性方程组 $AX=B$，其中

$$A=\begin{bmatrix}8 & 3\\ 2 & 6\end{bmatrix},\quad B=\begin{bmatrix}3\\ -1\end{bmatrix}$$

因为系数是整数，所以对任意素数 p，$AX=B$ 定义 $\mathbf{F}_p$ 上的一个方程组. A 的行列式是 42，故对所有不能整除 42 的 p，亦即对所有不同于 2，3 和 7 的 p，方程组在 $\mathbf{F}_p$ 中有唯一解. 例如，若 $p=13$ 当(mod 13)取值时，得到 $\det A=3$. 因为在 $\mathbf{F}_{13}$ 中 $3^{-1}=9$，故在 $\mathbf{F}_{13}$ 中模 13 有

$$A^{-1}=\begin{bmatrix}6 & -3\\ -2 & 8\end{bmatrix}=\begin{bmatrix}2 & -1\\ 8 & 7\end{bmatrix},\quad X=A^{-1}B=\begin{bmatrix}7\\ 4\end{bmatrix}$$

方程组在 $\mathbf{F}_2$ 或 $\mathbf{F}_3$ 中无解，但在 $\mathbf{F}_7$ 中碰巧有解，虽然在这个域中 $\det A\equiv 0$(模 7).

元素属于素域 $\mathbf{F}_p$ 的可逆矩阵为我们提供了有限群的新例子——有限域上的一般线性群：

$$GL_n(\mathbf{F}_p)=\{\text{元素属于 }\mathbf{F}_p\text{ 的 }n\times n\text{ 可逆矩阵}\}.$$

$$SL_n(\mathbf{F}_p)=\{\text{元素属于 }\mathbf{F}_p\text{ 的 }n\times n\text{ 可逆矩阵且行列式为 }1\}$$

例如，元素在 $\mathbf{F}_2$ 里的 2×2 可逆矩阵的群含有 6 个元素：

【3.2.9】
$$GL_2(\mathbf{F}_2)=\left\{\begin{bmatrix}1 & \\ & 1\end{bmatrix},\begin{bmatrix}1 & 1\\ 1 & \end{bmatrix},\begin{bmatrix} & 1\\ 1 & 1\end{bmatrix},\begin{bmatrix} & 1\\ 1 & \end{bmatrix},\begin{bmatrix}1 & 1\\ & 1\end{bmatrix},\begin{bmatrix}1 & \\ 1 & 1\end{bmatrix}\right\}$$

这个群同构于对称群 S_3. 按上面顺序所列的矩阵与对称群 S_3 的元素的通常列表$\{1,\ x,\ x^2,\ y,\ xy,\ x^2y\}$对应一致.

素域 $\mathbf{F}_p$ 有一个性质，即它使素域与 $\mathbf{C}$ 的子域区别开来，这个性质就是 1 自己相加若干次后得到 0，事实上是 p 的倍数. 域 F 的*特征* p 是作为加群 F^+ 的一个元素 1 的阶，倘若阶是有限的. 它是使得 m 个 1 的和 $1+\cdots+1$ 为零的最小正整数 m. 如果 1 的阶是无限的，即在 F 中 $1+\cdots+1$ 从不为 0，则我们说域 F *有特征零*，这似乎有点违背常规. 因此，$\mathbf{C}$ 的

子域有特征零，而素域 $\mathbf{F}_p$ 有特征 p.

【3.2.10】**引理** 任何域 F 的特征或者为零，或者为一个素数. 83

证明 为避免混淆，令$\bar{0}$和$\bar{1}$分别表示域 F 中的加法恒等元和乘法恒等元. 如果 k 是正整数，则用$\bar{k}$表示 k 个$\bar{1}$的和. 假设特征 m 不是零，那么 1 生成加群 F^+ 的阶为 m 的循环子群 H，且$\overline{m}=\bar{0}$. 由$\bar{1}$生成的循环子群 H 的不同元素是$\bar{k}$，这里 $k=0, 1, \cdots, m-1$(命题 2.4.2). 假设 m 不是素的，比如说 $m=rs$，并且 $1<r$，$s<m$，那么，$\bar{r}$和$\bar{s}$属于乘法群$F^\times = F-\{0\}$，但积 $\bar{r}\bar{s}$(其值为$\bar{0}$)却不在 $F^\times$ 里. 这与 $F^\times$ 是群矛盾. 所以，m 是素的. ■

素域 $\mathbf{F}_p$ 有一个著名的性质.

【3.2.11】**定理**(乘法群的结构) 令 p 是素数，素域的乘法群 $\mathbf{F}_p^\times$ 是阶为 $p-1$ 的循环群.

我们把这个定理的证明推迟到第十五章给出，在那里将证明每个有限域的乘法群都是循环群(定理 15.7.3).

注 循环群 $\mathbf{F}_p^\times$ 的生成元称为模 p 本原根.

有两个模 7 本原根，亦即 3 和 5，有四个模 11 本原根. 去掉数字上面的横杠，模 7 本原根 3 的幂 3^0，3^1，3^2，…以下面的顺序列出了 $\mathbf{F}_7$ 的非零元素：

【3.2.12】 $$\mathbf{F}_7^\times = \{1,3,2,6,4,5\} = \{1,3,2,-1,-3,-2\}$$

因此，有两种方式——加法的和乘法的——列出 $\mathbf{F}_p$ 的非零元素. 如果 α 是模 p 本原根，则

【3.2.13】 $$\mathbf{F}_p^\times = \{1,2,3,\cdots,p-1\} = \{1,\alpha,\alpha^2,\cdots,\alpha^{p-2}\}$$

第三节 向量空间

有了一些例子和域的概念后，我们给出向量空间的定义.

【3.3.1】**定义** 域 F 上的**向量空间** V 是满足下面合成法则的集合：

(a) 加法：$V\times V\to V$，记为 $v, w \rightsquigarrow v+w$，其中 $v, w\in V$，

(b) 标量乘法：$F\times V\to V$，记为 $c, v \rightsquigarrow cv$，其中 $c\in F$，$v\in V$.

这两个合成法则满足下列公理：

- 加法使 V 成为交换群 V^+，并带有恒等元，记为 0.
- $1v=v$，对所有 $v\in V$ 成立.
- 结合律：$(ab)v=a(bv)$，对所有 a，$b\in F$ 和 $v\in V$ 成立.
- 分配律：$(a+b)v=av+bv$ 和 $a(v+w)=av+aw$，对所有 a，$b\in F$ 和 v，$w\in V$ 成立. 84

元素在域 F 中的列向量的加法和标量乘法如(3.1.1)所定义，这样的列向量空间 F^n 构成域 F 上的向量空间.

一些实向量空间例子(**R** 上向量空间)如下：

【3.3.2】**例**

(a) 令 $V=\mathbf{C}$ 是复数集，忘掉两个复数的乘法，仅记住加法 $\alpha+\beta$ 和实数 r 与复数 α 的乘法 $r\alpha$. 这些运算使 V 成为一个实向量空间.

(b) 实多项式 $P(x)=a_nx^n+\cdots+a_0$ 的集合是一个实向量空间，多项式的加法和实数与多项式的乘法按合成法则进行.

(c) 实直线上的连续实值函数的集合是一个实向量空间，函数的加法 $f+g$ 和实数与函数的乘法按合成法则进行.

(d) 微分方程 $\frac{d^2y}{dt^2}=-y$ 的解集合是一个实向量空间. ■

当我们视其为向量空间时，每个例子都有比看上去更复杂的结构. 这是很典型的. 任一个特例肯定有区别于其他例子的额外特征，但这不是缺点. 相反地，抽象方法的好处在于公理的结果能够应用到许多不同的情形.

与群的子群和同构类似的两个重要概念是子空间和同构. 与 $\mathbf{R}^n$ 的子空间一样，域 F 上向量空间 V 的子空间 W 是在加法和标量乘法运算下封闭的非空子集. 子空间 W 称为 V 的一个真子空间，如果它既不是整个空间 V，也不是零空间 $\{0\}$. 例如，微分方程(3.3.2)(d)的解空间是实直线上所有连续函数空间的真子空间.

【3.3.3】命题 令 $V=F^2$ 是元素在域 F 中的列向量组成的向量空间. V 的每个真子空间 W 是由单个非零向量 w 的标量倍数 $\{cw\}$ 组成的. 不同的真子空间仅有零向量作为公共向量.

命题 3.1.4 的证明搬过来即可.

【3.3.4】例 令 F 是素域 $\mathbf{F}_p$. 空间 F^2 含有 p^2 个向量，其中有 p^2-1 个非零向量. 因为有 $p-1$ 个非零标量，由非零向量 w 张成的子空间 $W=\{cw\}$ 将含有 $p-1$ 个非零向量. 所以，F^2 含有 $(p^2-1)/(p-1)=p+1$ 个真子空间. ■

在同一个域 F 上，一个向量空间 V 到另一个向量空间 V' 的同构 φ 是一个与合成法则相容的一一映射 $\varphi:V\to V'$，即对所有 v，$w\in V$ 及所有 $c\in F$ 满足条件

【3.3.5】 $$\varphi(v+w)=\varphi(v)+\varphi(w) \quad 和 \quad \varphi(cv)=c\varphi(v)$$

85 的一一映射.

【3.3.6】例

(a) 令 $F^{n\times n}$ 表示域 F 上的 $n\times n$ 矩阵的集合，该集合是域 F 上的向量空间，它同构于长度为 n^2 的列向量的空间.

(b) 如果同(3.3.2)(a)一样，把复数集看作实向量空间，使得 $(a,\ b)^t\rightsquigarrow a+bi$ 的映射 $\varphi:\mathbf{R}^2\to\mathbf{C}$ 是一个同构. ■

第四节 基和维数

本节讨论在向量空间中使用加法和标量乘法时所用的术语. 新的概念有张成、线性无关和基.

这里使用向量的有序集会很方便. 我们已将无序集用花括号括起来表示，为了区别有序集和无序集，将有序集用圆括号括起来表示. 这样有序集 $(v,\ w)$ 和 $(w,\ v)$ 是不同的，而无序集 $\{v,\ w\}$ 和 $\{w,\ v\}$ 是相同的. 有序集允许重复. 这样 $(v,\ v,\ w)$ 是一个有序集，且

它与(v, w)不同，这与无序集的习惯不同，无序集$\{v, v, w\}$和$\{v, w\}$表示同一个集合.

注 令V是域F上的向量空间，并设$S=\{v_1, v_2, \cdots, v_n\}$是$V$中元素的一个有序集，$S$的一个线性组合是形如

【3.4.1】 $$w = c_1v_1 + c_2v_2 + \cdots + c_nv_n, \quad c_i \in F$$

的向量.

为方便起见，允许标量出现在向量的任一边. 我们简单地约定：如果v是一个向量，c是一个标量，则记号vc和cv代表由标量乘法得到的同一向量. 所以，

$$c_1v_1 + c_2v_2 + \cdots + c_nv_n = v_1c_1 + v_2c_2 + \cdots + v_nc_n$$

矩阵记号提供书写线性组合的紧凑方式，并且也是我们书写向量有序集的方式. 由于里面的元素是向量，所以称$S=(v_1, v_2, \cdots, v_n)$是超向量. 向量空间里两个元素的乘法没有定义，但有标量乘法. 这允许我们把超向量S和F^n里的列向量X的乘积理解为

【3.4.2】 $$SX = (v_1, \cdots, v_n)\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = v_1x_1 + \cdots + v_nx_n$$

由标量乘法和向量加法计算右边，我们得到另一个向量，即一个标量系数x_i写在了右边的线性组合.

我们拿线性方程

【3.4.3】 $$2x_1 - x_2 - 2x_3 = 0 \quad 或\ AX = 0, \quad 其中\ A = (2, -1, -2)$$

在$\mathbf{R}^3$的解子空间W作为例子. 两个特解w_1和w_2以及它们的线性组合$w_1y_1 + w_2y_2$如下所示.

【3.4.4】 $$w_1 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}, \quad w_2 = \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix}, \quad w_1y_1 + w_2y_2 = \begin{bmatrix} y_1 + y_2 \\ 2y_2 \\ y_1 \end{bmatrix}$$

如果我们写$S=(w_1, w_2)$，而w_i如(3.4.4)里所示，且$Y=(y_1, y_2)^t$，那么，组合$w_1y_1 + w_2y_2$可写成矩阵形式SY. 86

注 写成$S=(v_1, v_2, \cdots, v_n)$的线性组合的所有向量的集合构成$V$的子空间，称为由集合$S$张成的子空间.

同本章第一节中一样，这个张成(子空间)是V的包含S的最小子空间，常常记为SpanS. 单个向量(v_1)的张成是v_1的标量倍数cv_1的子空间.

可以定义无限多个向量集合的张成. 我们将在本章第七节讨论这样的张成. 现在假设集合都是有限的.

【3.4.5】引理 令S是V中向量的一个有序集，设W是V的子空间. 如果$S \subset W$，则$\mathrm{Span}S \subset W$.

元素在F中的$m \times n$矩阵的列空间是由该矩阵的列张成的F^m的子空间. 它有如下重

要解释：

【3.4.6】命题 令 A 是一个 $m\times n$ 矩阵，B 是一个列向量，A 与 B 的元素都在域 F 里. 方程组 $AX=B$ 在 F^n 里有解 X 当且仅当 B 在 A 的列空间里.

证明 令 A_1，A_2，…，A_n 表示 A 的列向量. 对任一个列向量 $X=(x_1, x_2, \cdots, x_n)^t$，矩阵之积 AX 是列向量 $A_1x_1+\cdots+A_nx_n$. 这是矩阵列向量的线性组合，是列空间的一个元素，并且，若 $AX=B$，那么 B 是这个线性组合. ■

向量 v_1，…，v_n 间的线性关系是等于零的任一线性组合——在 V 中成立的形如

【3.4.7】
$$v_1x_1+v_2x_2+\cdots+v_nx_n=0$$

的任一个方程，其中系数 $x_i\in F$. 线性关系是有用的，因为如果 x_n 不是零，则由方程(3.4.7)可解出 v_n.

【3.4.8】定义 向量的一个有序集 $S=(v_1, \cdots, v_n)$ 称为无关的，或线性无关的，如果除了系数 x_i 皆为零的平凡关系(即 $X=0$)外，这个集合的向量间没有线性关系 $SX=0$. 不是无关的集合是相关的.

无关集合 S 里不能有相同的向量. 若 S 里的两个向量 v_i 和 v_j 是相等的，则 $v_i-v_j=0$ 是其他系数都为零的形如(3.4.7)的一个线性关系. 还有，无关集合里没有零向量，因为若 v_i 是零，则 $v_i=0$ 就是一个线性关系.

【3.4.9】引理

(a) 一个向量的集合(v_1)是无关的当且仅当 $v_1\neq 0$.

(b) 两个向量的集合(v_1, v_2)是线性无关的当且仅当其中任一向量都不是另一向量的倍数.

87 (c) 线性无关集合在任意重新排序后仍是线性无关集合.

设 V 是空间 F^m，并且已知集合 $S=(v_1, v_2, \cdots, v_n)$ 里诸向量的坐标向量. 那么方程 $SX=0$ 给出了具有 n 个未知量 x_i 的 m 个齐次线性方程的方程组，我们可通过解这个方程组确定无关性.

【3.4.10】例 令 $S=(v_1, v_2, v_3, v_4)$ 为 $\mathbf{R}^3$ 里一个向量集合，其坐标向量为

【3.4.11】
$$A_1=\begin{bmatrix}1\\0\\1\end{bmatrix},\quad A_2=\begin{bmatrix}1\\2\\0\end{bmatrix},\quad A_3=\begin{bmatrix}2\\1\\2\end{bmatrix},\quad A_4=\begin{bmatrix}1\\1\\3\end{bmatrix}$$

用 A 表示列为这些向量的矩阵：

【3.4.12】
$$A=\begin{bmatrix}1&1&2&1\\0&2&1&1\\1&0&2&3\end{bmatrix}$$

这些向量的一般线性组合具有 $SX=v_1x_1+v_2x_2+v_3x_3+v_4x_4$ 的形式，它的坐标向量是 $AX=A_1x_1+A_2x_2+A_3x_3+A_4x_4$. 齐次方程 $AX=0$ 有非平凡解，因为这是一个具有四个未知量的三个齐次方程的方程组. 所以，集合 S 是相关的. 另一方面，由(3.4.12)的前三

列构成的 3×3 矩阵 A' 的行列式等于 1，于是方程 $A'X=0$ 只有平凡解. 所以，(v_1, v_2, v_3)是无关集合. ■

【3.4.13】定义 向量空间 V 的一个基是线性无关且张成 V 的一个向量集合$(v_1, \cdots, v_n)$.

我们常用如 $\boldsymbol{B}$ 的粗体符号表示基. 上面定义的集合(v_1, v_2, v_3)是 $\mathbf{R}^3$ 的一个基，因为方程 $A'X=B$ 对所有 B 都有唯一解(见 1.2.21). 在(3.4.4)中定义的集合(w_1, w_2)是方程 $2x_1-x_2-2x_3=0$ 的解空间的一个基，尽管我们还未证明这个结论.

【3.4.14】命题 集合 $\boldsymbol{B}=(v_1, \cdots, v_n)$是基当且仅当每个向量 $w\in V$ 可以以唯一方式写为组合 $w=v_1x_1+v_2x_2+\cdots+v_nx_n=\boldsymbol{B}X$.

证明 无关性的定义可以重新叙述为零向量仅有一个作为线性组合的表达式. 如果每个向量可唯一地写成组合，那么 $\boldsymbol{B}$ 是无关的，并且张成 V. 所以，它是一个基. 反过来，假设 $\boldsymbol{B}$ 是基，那么，V 中每个向量 w 都可写成线性组合. 设 w 有两种方式写成线性组合，比如说，$w=\boldsymbol{B}X=\boldsymbol{B}X'$. 令 $Y=X-X'$，则 $\boldsymbol{B}Y=0$. 这是线性无关向量 $v_1, v_2, \cdots, v_n$ 间的一个线性关系. 所以，$X-X'=0$. 这两个线性组合是相同的. ■

设 $V=F^n$ 是列向量空间. 同以前一样，e_i 表示在第 i 个位置为 1 而其他位置为 0 的列向量(见(1.1.24)). 集合 $\boldsymbol{E}=(e_1, e_2, \cdots, e_n)$是 F^n 的一个基，称为标准基. 如果 F^n 里的向量 v 的坐标向量是 $V=(x_1, x_2, \cdots, x_n)^t$，则 $v=\boldsymbol{E}X=e_1x_1+e_2x_2+\cdots+e_nx_n$ 是 v 写成 88
标准基的唯一表达式.

我们现在讨论把张成、无关性和基三个概念联系起来的主要事实. 最重要的结果是定理 3.4.18.

【3.4.15】命题 令 $S=(v_1, v_2, \cdots, v_n)$是向量的一个有序集，设 w 是 V 里的任一向量，并且 $S'=(S, w)$是把 w 添加到 S 里得到的集合.

(a) $\mathrm{Span}S=\mathrm{Span}S'$ 当且仅当 $w\in\mathrm{Span}S$.

(b) 假设 S 是无关的. 那么 S'是无关的当且仅当 $w\notin\mathrm{Span}S$.

证明 这是非常基本的结果，所以，我们略去大部分证明. 我们仅证明，如果 S 是无关的，但 S'不是无关的，则 w 属于 S 的张成. 若 S'是相关的，则有某个线性关系

$$v_1x_1+v_2x_2+\cdots+v_nx_n+wy=0$$

其中系数 $x_1, x_2, \cdots, x_n$ 和 y 不全为零. 如果系数 y 为零，则表达式变为 $SX=0$，因为假设 S 是无关的，故也得 $X=0$. 于是关系是平凡的，与假设矛盾. 所以，$y\neq0$，从而 w 可表示为 $v_1, v_2, \cdots, v_n$ 的线性组合. ■

注 向量空间 V 称为有限维的，如果存在有限集合 S，它张成 V. 否则，V 是无限维的.

本节后面余下部分所讨论的向量空间均是有限维的.

【3.4.16】命题 令 V 是有限维向量空间.

(a) 令 S 是张成 V 的有限子集，并设 L 是 V 的无关子集. 可通过把 S 的元素添加到 L 的办法得到 V 的一个基.

(b) 令 S 是张成 V 的有限子集，可通过去掉 S 的元素的办法得到 V 的一个基.

证明

(a) 如果 S 包含在 Span$L$ 里，则 L 张成 V，于是，它是一个基(3.4.5). 如果 S 不包含在 Span$L$ 里，则在 S 里选一个元素 v，使其不含在 Span$L$ 里. 由命题 3.4.15，$L'=(L, v)$是无关的. 我们用 L'替换 L. 因为 S 是有限的，故这种过程常常仅有限多步就结束了. 所以，我们最终得到 V 的一个基.

(b) 如果 S 是相关的，则存在线性关系 $v_1c_1+v_2c_2+\cdots+v_nc_n=0$，其中某个系数(比如说 c_n)是非零的. 从这个方程解出 v_n，这表明 v_n 在前 $n-1$ 个向量集合 S_1 的张成里. 命题 3.4.15(a)表明 Span$S$=SpanS_1. 所以，S_1 张成 V. 我们用 S_1 替换 S. 继续这个过程，最后必得到一个无关但仍张成 V 的集合：一个基.

注意 如果 V 是零向量空间$\{0\}$，那么这个证明会出问题. 因为从 V 中的任何向量(它们全部都等于零)集合开始，我们的过程会将它们一次一个地丢掉，直到只剩下一个向量
89 v_1. 因为 $v_1=0$，故集合(v_1)是相关的. 我们如何进行这个过程？零向量空间并不特别有意义，但它会潜伏在某个角落里，等待我们踏进它的陷阱. 我们必须允许在诸如解齐次线性方程组的某些运算过程中出现的向量空间可能是零空间. 为了避免今后需要把这种情形特别提出来，我们采用下面的定义：

【3.4.17】

- 空集是线性无关的.
- 空集的张成是零空间$\{0\}$.

这样，空集是零向量空间的基. 这些定义使我们能够扔掉最后一个向量 v_1，这样证明就不会出问题了. ■

现在我们来介绍关于无关的主要事实.

【3.4.18】定理 令 S 与 L 是向量空间 V 的有限子集. 假设 S 张成 V，并且 L 是无关的. 那么 S 至少含有同 L 一样多的元素：$|S|\geqslant|L|$.

同以前一样，$|S|$表示阶，即集合 S 的元素的个数.

证明 设 $S=(v_1, v_2, \cdots, v_m)$，$L=(w_1, w_2, \cdots, w_n)$，假设$|S|<|L|$，亦即 $m<n$，证明 L 是相关的. 为此，证明存在线性关系 $v_1x_1+v_2x_2+\cdots+v_nx_n=0$，其中系数 x_i 不全为零. 记这个未确定的关系为 $LX=0$.

因为 S 张成 V，故 L 的每个元素 w_j 是 S 的线性组合，比如说，$w_j=v_1a_{1j}+v_2a_{2j}+\cdots+v_ma_{mj}=SA_j$，其中 A_j 是系数列向量. 我们把这些列向量写成 $m\times n$ 矩阵

【3.4.19】

$$A=\begin{bmatrix} | & & | \\ A_1 & \cdots & A_n \\ | & & | \end{bmatrix}$$

于是

【3.4.20】

$$SA=(SA_1,\cdots,SA_n)=(w_1,\cdots,w_n)=L$$

在未定线性组合里用 SA 替换 L：

$$LX = (SA)X$$

标量乘法的结合律蕴含着 $(SA)X=S(AX)$. 对标量矩阵乘法的结合律的证明也是一样的(我们略去证明). 如果 $AX=0$，那么组合 LX 也是零. 现在，由于 A 是 $m\times n$ 矩阵，且 $m<n$，故齐次方程组 $AX=0$ 有非平凡解 X. 因此，$LX=0$ 就是我们要求的线性关系. ■

【3.4.21】命题 令 V 是有限维向量空间.

(a) V 的任两个基有相同的阶(元素个数相同).

(b) 令 $\boldsymbol{B}$ 是一个基. 如果有限向量集 S 张成 V，那么 $|S|\geqslant|\boldsymbol{B}|$，并且 $|S|=|\boldsymbol{B}|$ 当且仅当 S 是基.

(c) 令 $\boldsymbol{B}$ 是一个基. 如果向量集 L 是无关的，那么 $|L|\leqslant|\boldsymbol{B}|$，并且 $|L|=|\boldsymbol{B}|$ 当且仅当 L 是基.

90

证明

(a) 这里我们注意到，两个有限基 $\boldsymbol{B}_1$ 与 $\boldsymbol{B}_2$ 有相同阶，我们将在推论 3.7.7 里证明有限维向量空间的每个基都是有限的. 在定理 3.4.18 里取 $S=\boldsymbol{B}_1$ 和 $L=\boldsymbol{B}_2$ 表明 $|\boldsymbol{B}_1|\geqslant|\boldsymbol{B}_2|$，类似地，$|\boldsymbol{B}_2|\geqslant|\boldsymbol{B}_1|$.

(b)和(c)由(a)与命题 3.4.16 可得. ■

【3.4.22】定义 有限维向量空间 V 的维数是基中的向量个数. 维数记为 $\dim V$.

列向量空间 F^n 的维数是 n，因为标准基

$$\boldsymbol{E} = (e_1, e_2, \cdots, e_n)$$

含有 n 个元素.

【3.4.23】命题 如果 W 是有限维向量空间 V 的子空间，则 W 是有限维的，并且 $\dim W\leqslant\dim V$. 进一步，$\dim W=\dim V$ 当且仅当 $W=V$.

证明 我们从 W 的任意无关向量集 L 开始，该集合可能为空集. 如果 L 不张成 W，则在 W 中选取一向量 w 使之不含于 L 的张成里. 因此，$L'=(L, w)$是无关的(3.4.15). 用 L'替换 L.

显然，如果 L 是 W 的无关子集，那么将其视作 V 的子集时也是无关的. 因而，由定理 3.4.18 知 $|L|\leqslant\dim V$. 所以，添加元素到 L 的过程经过有限多步就能结束，我们就得到 W 的一个基. 因为 L 至多含有 $\dim V$ 个元素，故 $\dim W\leqslant\dim V$. 如果 $|L|=\dim V$，那么命题 3.4.21(c)表明 L 是 V 的一个基，所以，$W=V$. ■

第五节 用基计算

引入基的目的是提供一种计算的方法，本节我们将学习如何使用它. 考虑两个主题：如何用一组基表出一个向量，以及如何将同一个向量空间的两个不同的基联系起来.

设给定向量空间 V 的一个基 $\boldsymbol{B}=(v_1, \cdots, v_n)$. 记住：这意味着每一个向量 $v\in V$ 可以用恰好一种形式表示为线性组合：

【3.5.1】

$$v = v_1x_1 + \cdots v_nx_n, \quad x_i \in F$$

标量 x_i 称为 v 的坐标，而列向量

【3.5.2】
$$X=\begin{bmatrix}x_1\\ \vdots\\ x_n\end{bmatrix}$$

称为 v 关于这个基的坐标向量.

例如，$(\cos t,\ \sin t)$是微分方程 $y''=-y$ 的解空间的一个基. 该微分方程的每个解都是这组基的线性组合. 若已知另一解 $f(t)$，则 f 的坐标向量$(x_1,\ x_2)^t$ 是使 $f(t)=(\cos t)x_1+$
91 $(\sin t)x_2$ 的一个向量. 显然，为求 X 我们需要知道关于 f 的某些信息. 不需要很多：仅仅确定两个系数即可. f 的大多数性质隐含在解微分方程的事实里.

我们永远能做的是，已知 n 维向量空间的一个基 $\boldsymbol{B}$，从向量空间 F^n 到 V 定义一个向量空间同构(见 3.3.5)：

【3.5.3】
$$\psi:F^n\to V \quad 映 \quad X\rightsquigarrow \boldsymbol{B}X$$

我们常用 $\boldsymbol{B}$ 表示这个同构，因为它映向量 X 到 $\boldsymbol{B}X$.

【3.5.4】命题 令 $S=(v_1,\ v_2,\ \cdots,\ v_n)$是向量空间 V 的子集，设 $\psi:F^n\to V$ 为其定义是 $\psi(X)=SX$的映射. 那么

(a) ψ 是单射当且仅当 S 是无关的.

(b) ψ 是满射当且仅当 S 张成 V.

(c) ψ 是双射当且仅当 S 是 V 的基.

这个命题可由无关、张成和基的定义得到.

已知一组基，V 中向量 v 的坐标向量可由映射 ψ(3.5.3)的逆得到. 除非进一步明确地给出基，否则不会有逆函数的精确公式，但同构的存在本身就很有意义.

【3.5.5】推论 每个 n 维向量空间 V 同构于列向量空间 F^n.

注意，当 $m\neq n$ 时 F^n 与 F^m 不同构，因为 F^n 有具有 n 个元素的基，而基中元素的个数仅依赖于向量空间. 因此，域 F 上的有限维向量空间被完全分类. 列向量空间 F^n 是同构类的代表元.

n 维向量空间同构于列向量空间 F^n 的事实允许我们只要选定一个基，就能把向量空间的任何问题化简为熟悉的列向量的代数. 不幸的是，同一个向量空间 V 有许多组基. 当给出一个自然的基时，将 V 与同构的向量空间 F^n 等同起来是有用的，而当给出的基对问题不太合适时，那就不行了. 这种情形下，我们需要变换坐标，亦即基变换.

例如，齐次线性方程组 $AX=0$ 的解空间几乎没有自然基. 方程 $2x_1-x_2-2x_3=0$ 的解空间 W 的维数是 2，前面我们展示过它的一组基：$\boldsymbol{B}=(w_1,\ w_2)$，其中 $w_1=(1,\ 0,\ 1)^t$ 与 $w_2=(1,\ 2,\ 0)^t$(见(3.4.4))．利用这个基，我们得到向量空间的同构 $\boldsymbol{R}^2\to W$，记为 $\boldsymbol{B}$. 由于方程中的未知量标记为 x_i，因此这里需要选取另一符号来表示 $\boldsymbol{R}^2$ 的变量元素. 我们将使用 $Y=(y_1,\ y_2)^t$ 表示. 同构 $\boldsymbol{B}$ 映 Y 到(3.4.4)显示的 $\boldsymbol{B}Y=w_1y_1+w_2y_2$ 的坐标向量.

然而，关于两个特解 w_1 与 w_2 没有非常特别之处，其他大部分解对用起来也一样. 解

$w_1'=(0,\ 2,\ -1)^t$ 与 $w_2'=(1,\ 4,\ -1)^t$ 为我们提供 W 的另一组基 $\boldsymbol{B}'=(w_1',\ w_2')$. 任一组基都能唯一表出解. 解可表示为如下任一形式： 92

【3.5.6】
$$\begin{bmatrix} y_1+y_2 \\ 2y_2 \\ y_1 \end{bmatrix} \quad \text{或} \quad \begin{bmatrix} y_2' \\ 2y_1'+4y_2' \\ -y_1'-y_2' \end{bmatrix}$$

基的变换

假设给定同一个向量空间 V 的两个基，比如 $\boldsymbol{B}=(v_1,\ \cdots,\ v_n)$ 和 $\boldsymbol{B}'=(v_1',\ \cdots,\ v_n')$. 我们希望做两个计算. 首先问：两个基是如何联系起来的？其次，一个向量 $v\in V$ 关于每一个基都有坐标，但它们却是不同的. 因而我们问：两个坐标向量是如何联系起来的？这些就是称为基变换的计算，在后面几章中它们将是非常重要的. 如果你不谨慎地组织记号，它们会让你头疼.

我们将 $\boldsymbol{B}$ 看作旧基，把 $\boldsymbol{B}'$ 看作新基. 注意新基 $\boldsymbol{B}'$ 中的每个向量是旧基 $\boldsymbol{B}$ 的一个线性组合. 把这个线性组合写为

【3.5.7】
$$v_j' = v_1 p_{1j} + v_2 p_{2j} + \cdots + v_n p_{nj}$$

当用旧基计算时，列向量 $P_j=(p_{1j},\ p_{2j},\ \cdots,\ p_{nj})^t$ 是新基向量 v_j' 的坐标向量. 把这些列向量组成方阵 P，从而得到矩阵方程 $\boldsymbol{B}'=\boldsymbol{B}P$：

【3.5.8】
$$\boldsymbol{B}' = (v_1', \cdots, v_n') = (v_1, \cdots, v_n)\begin{bmatrix} \\ P \\ \\ \end{bmatrix} = \boldsymbol{B}P$$

P 的第 j 列是新基向量 v_j' 关于旧基的坐标向量. 矩阵 P 称为基变换矩阵. ⊖

【3.5.9】**命题**

(a) 令 $\boldsymbol{B}$ 和 $\boldsymbol{B}'$ 是向量空间 V 的两个基. 基变换矩阵 P 是可逆矩阵，由基 $\boldsymbol{B}$ 和 $\boldsymbol{B}'$ 唯一确定.

(b) 令 $\boldsymbol{B}=(v_1,\ \cdots,\ v_n)$ 是向量空间 V 的基. 其他基是形如 $\boldsymbol{B}'=\boldsymbol{B}P$ 的集合，其中 P 是任意可逆 $n\times n$ 矩阵.

证明

(a) 方程 $\boldsymbol{B}'=\boldsymbol{B}P$ 把基向量 v_i' 表示为基 $\boldsymbol{B}$ 的线性组合. 写出的线性组合仅有一种方式 (3.4.14)，因此，P 是唯一的. 为证 P 是可逆矩阵，我们互换 $\boldsymbol{B}$ 和 $\boldsymbol{B}'$ 的作用. 存在矩阵 Q 使得 $\boldsymbol{B}=\boldsymbol{B}'Q$. 因此

$$\boldsymbol{B} = \boldsymbol{B}'Q = \boldsymbol{B}PQ \quad \text{或} \quad (v_1, \cdots, v_n) = (v_1, \cdots, v_n)\begin{bmatrix} \\ PQ \\ \\ \end{bmatrix}$$

⊖ 这个基变换矩阵是第 1 版里用过的矩阵的逆矩阵.

这个方程把每个 v_i 表示为$(v_1, \cdots, v_n)$的组合. 乘积矩阵 PQ 中的元素是系数. 但因 $\boldsymbol{B}$ 是
93 基，故只有一种方式将 v_i 表示为$(v_1, \cdots, v_n)$的组合，也就是 $v_i = v_i$，或用矩阵记号，$\boldsymbol{B} = \boldsymbol{B}I$. 所以，$PQ = I$.

(b) 我们必须证明如果 $\boldsymbol{B}$ 是基，并且如果 P 是可逆矩阵，则 $\boldsymbol{B}' = \boldsymbol{B}P$ 也是基. 因为 P 是可逆的，故 $\boldsymbol{B} = \boldsymbol{B}'P^{-1}$. 这就告诉我们 v_i 在 $\boldsymbol{B}'$的张成里. 所以，$\boldsymbol{B}'$张成 V. 又由于它与 $\boldsymbol{B}$ 中元素个数相同，故它是基. ■

令 X 和 X'是任一向量 v 关于两个基 $\boldsymbol{B}$ 和 $\boldsymbol{B}'$的坐标向量，也就是，$v = \boldsymbol{B}X$，$v = \boldsymbol{B}'X'$. 替换 $\boldsymbol{B} = \boldsymbol{B}'P^{-1}$，得矩阵方程

【3.5.10】
$$v = \boldsymbol{B}X = \boldsymbol{B}'P^{-1}X$$

这表明 v 关于新基 $\boldsymbol{B}'$的坐标向量(称为 X')是 $P^{-1}X$. 也可以将其写为 $X = PX'$

回顾一下，我们有单个矩阵 P——基变换矩阵，它具有对偶的性质：

【3.5.11】
$$\boldsymbol{B}' = \boldsymbol{B}P \quad 和 \quad PX' = X$$

其中 X，X'表示任意向量 v 关于两个基的坐标向量. 每一个性质都刻画了 P. 仔细注意两个关系里斜撇符号的位置.

再次回到方程 $2x_1 - x_2 - 2x_3 = 0$，令 $\boldsymbol{B}$ 和 $\boldsymbol{B}'$是上面(3.5.6)里描述的解空间 W 的基. 基变换矩阵解方程

$$\begin{bmatrix} 0 & 1 \\ 2 & 4 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 2 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{bmatrix}. \text{ 它是 } P = \begin{bmatrix} -1 & -1 \\ 1 & 2 \end{bmatrix}$$

已知向量 v 关于两个基的坐标向量 Y 与 Y'(在(3.5.6)里出现)由方程

$$PY' = \begin{bmatrix} -1 & -1 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} y_1' \\ y_2' \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = Y$$

联系.

另一个例子：令 $\boldsymbol{B}$ 是微分方程 $\frac{\mathrm{d}^2y}{\mathrm{d}t^2} = -y$ 的解空间的基$(\cos t, \sin t)$. 如果允许复值函数，那么指数函数 $\mathrm{e}^{\pm it} = \cos t \pm i \sin t$ 也是解，$\boldsymbol{B}' = (\mathrm{e}^{it}, \mathrm{e}^{-it})$是解空间的新基. 基变换计算是

【3.5.12】
$$(\mathrm{e}^{it}, \mathrm{e}^{-it}) = (\cos t, \sin t) \begin{bmatrix} 1 & 1 \\ i & -i \end{bmatrix}$$

94 基变换矩阵容易确定的一种情形是 V 是列向量空间 F^n，旧基是标准基 $\boldsymbol{E} = (e_1, \cdots, e_n)$，而新基在这里记为 $\boldsymbol{B} = (v_1, \cdots, v_n)$，它是任意的. 令 v_i 关于标准基的坐标向量是列向量 B_i. 所以，$v_i = \boldsymbol{E}B_i$. 把这些列向量组成 $n \times n$ 矩阵，记之为$[\boldsymbol{B}]$：

【3.5.13】
$$[\boldsymbol{B}] = \begin{bmatrix} | & & | \\ B_1 & \cdots & B_n \\ | & & | \end{bmatrix}, \text{则} (v_1, \cdots, v_n) = (e_1, \cdots, e_n) \begin{bmatrix} | & & | \\ B_1 & \cdots & B_n \\ | & & | \end{bmatrix}$$

即 $\boldsymbol{B} = \boldsymbol{E}[\boldsymbol{B}]$. 所以，$[\boldsymbol{B}]$是从标准基 $\boldsymbol{E}$ 到 $\boldsymbol{B}$ 的基变换矩阵.

第六节 直 和

向量集的无关和张成的概念对于子空间是相似的. 如果 W_1, …, W_k 是向量空间 V 的子空间, 那么向量 v 的集合可以写为和

【3.6.1】 $$v = w_1 + \cdots + w_k$$

其中 w_i 是 W_i 的向量, 所有这样向量 $v \in V$ 的集合称为子空间的和或它们的张成, 记为

【3.6.2】 $$W_1 + \cdots, + W_k = \{v \in V \mid v = w_1 + \cdots + w_k, \text{其中 } w_i \in W_i\}$$

子空间的和是含有所有子空间 W_1, …, W_k 的最小子空间, 类似于向量集合的张成.

子空间 W_1, …, W_k 称为无关的, 如果除了对所有 i 有 $w_i = 0$ 的平凡和外, 其余的和 $w_1 + \cdots + w_k$(其中 $w_i \in W_i$)皆不为零. 换言之, 空间是无关的, 如果

【3.6.3】 $$w_1 + \cdots + w_k = 0(\text{其中 } w_i \in W_i) \text{ 蕴含着对所有 } i \text{ 有 } w_i = 0$$

注意 假设 v_1, …, v_k 是 V 的元素, 令 W_i 是向量 v_i 的张成. 那么, 子空间 W_1, …, W_k 是无关的当且仅当集合(v_1, …, v_k)是无关的. 如果比较(3.4.8)与(3.6.3), 这是显然的. 用子空间叙述更为整洁, 因为标量系数不需要放在(3.6.3)里 w_i 的前面. 由于每个子空间 W_i 在标量乘法下封闭, 因此标量倍数 cw_i 是 W_i 的另一元素.

我们略去下一命题的证明.

【3.6.4】**命题** 令 W_1, …, W_k 是有限维向量空间 V 的子空间, 设 $\boldsymbol{B}_i$ 是 W_i 的一个基.

(a) 下列条件是等价的:

- 诸子空间 W_i 是无关的, 而且和 $W_1 + \cdots + W_k$ 等于 V.
- 把诸基附和在一起所得集合 $\boldsymbol{B} = (\boldsymbol{B}_1, \cdots, \boldsymbol{B}_k)$ 是 V 的一个基.

(b) $\dim(W_1 + \cdots + W_k) \leqslant \dim W_1 + \cdots + \dim W_k$, 等号成立当前仅当诸子空间无关. 95

(c) 如果对 $I = 1, 2, \cdots, k$, W_i' 是 W_i 的子空间, 并且 W_1, …, W_k 是无关的, 那么 W_1', …, W_k' 也是无关的.

如果命题 3.6.4(a)的条件得到满足, 就说 V 是子空间 W_1, …, W_k 的直和, 记为 $V = W_1 \oplus \cdots \oplus W_k$:

【3.6.5】 $$V = W_1 \oplus \cdots \oplus W_k, \text{如果 } V = W_1 + \cdots + W_k \text{ 并且 } W_1, \cdots, W_k \text{ 是无关的}$$

如果 V 是直和, 则每个向量 $v \in V$ 恰好可以以一种方式写为(3.6.1)的形式.

【3.6.6】**命题** 令 W_1 与 W_2 是有限维向量空间 V 的子空间.

(a) $\dim W_1 + \dim W_2 = \dim(W_1 \cap W_2) + \dim(W_1 + W_2)$.

(b) W_1 与 W_2 是无关的当且仅当 $W_1 \cap W_2 = \{0\}$.

(c) V 是 W_1 与 W_2 的直和当且仅当 $W_1 \cap W_2 = \{0\}$ 且 $W_1 + W_2 = V$.

(d) 如果 $W_1 + W_2 = V$, 则存在 W_2 的子空间 W_2', 满足 $W_1 \oplus W_2' = V$.

证明 证明关键部分(a): 选择 $W_1 \cap W_2$ 的一个基 $\boldsymbol{U} = (u_1, \cdots, u_k)$, 把它扩张为 W_1 的一

个基$(\boldsymbol{U}, \boldsymbol{V})=(u_1, \cdots, u_k; v_1, \cdots, v_m)$. 也把$\boldsymbol{U}$扩张为$W_2$的一个基$(\boldsymbol{U}, \boldsymbol{W})=(u_1, \cdots, u_k; w_1, \cdots, w_n)$. 于是，$\dim(W_1 \cap W_2)=k$，$\dim W_1=k+m$与$\dim W_2=k+n$. 如果证明$k+m+n$个元素的集合$(\boldsymbol{U}, \boldsymbol{V}, \boldsymbol{W})=(u_1, \cdots, u_k; v_1, \cdots, v_m, w_1, \cdots, w_n)$是$W_1+W_2$的基，命题就成立.

必须证明$(\boldsymbol{U}, \boldsymbol{V}, \boldsymbol{W})$是无关的，且张成$W_1+W_2$. W_1+W_2的元素v有形式$w'+w''$，其中$w' \in W_1$，$w'' \in W_2$. 用W_1的基$(\boldsymbol{U}, \boldsymbol{V})$来写$w'$，比如说，$w'=\boldsymbol{U}X+\boldsymbol{V}Y=u_1x_1+\cdots+u_kx_k+v_1y_1+\cdots+v_my_m$. 也把$w''$写成$W_2$的基$(\boldsymbol{U}, \boldsymbol{W})$的组合$\boldsymbol{U}X'+\boldsymbol{W}Z$. 因此，$V=w'+w''=\boldsymbol{U}(X+X')+\boldsymbol{V}Y+\boldsymbol{W}Z$.

其次，假设已知元素$(\boldsymbol{U}, \boldsymbol{V}, \boldsymbol{W})$之间的线性关系$\boldsymbol{U}X+\boldsymbol{V}Y+\boldsymbol{W}Z=0$. 记这个关系为$\boldsymbol{U}X+\boldsymbol{V}Y=-\boldsymbol{W}Z$. 这个方程的左边属于$W_1$，而右边属于$W_2$. 所以，$-\boldsymbol{W}Z$属于$W_1 \cap W_2$，从而它是基$\boldsymbol{U}$的线性组合$\boldsymbol{U}X'$. 这就给出方程$\boldsymbol{U}X'+\boldsymbol{W}Z=0$. 由于$(\boldsymbol{U}, \boldsymbol{W})$是$W_2$的基，它是无关的，所以，$X'$和$Z$是零. 这样，已知关系简化为$\boldsymbol{U}X+\boldsymbol{V}Y=0$. 但$(\boldsymbol{U}, \boldsymbol{V})$也是无关集合. 于是，$X$与$Y$是零. 关系是平凡的. ■

第七节 无限维空间

有的向量空间太大了，无法由任意有限的向量集合张成，这样的向量空间称作是*无限维的*. 我们不常用到它们，但因为它们在分析中很重要，所以本节将对它们稍作讨论.

无限维向量空间最简明的例子是无限实行向量

【3.7.1】 $$(a)=(a_1, a_2, a_3, \cdots)$$

96 的空间$\mathbf{R}^\infty$. 也可以把一个无限维向量看作是一个实数序列$\{a_n\}$.

空间$\mathbf{R}^\infty$有许多重要的子空间，下面是一些例子.

【3.7.2】**例**

(a) 收敛序列：$C=\{(a) \in \mathbf{R}^\infty \mid \text{极限} \lim_{n\to\infty} a_n \text{ 存在}\}$.

(b) 绝对收敛级数：$\ell^1=\{(a) \in \mathbf{R}^\infty \mid \sum_1^\infty |a_n| < \infty\}$.

(c) 有限个非零项的序列：

$$Z=\{(a) \in \mathbf{R}^\infty \mid a_n=0 \text{ 对有限多个以外的 } n \text{ 成立}\}$$

所有上面的空间都是无限维的，还可以找出更多的无限维空间. ■

现在设V是向量空间，是否无限维都行. 向量的无限维集合S的张成应该是什么呢？困难在于：不可能为无限多个向量的组合$c_1v_1+c_2v_2+\cdots$指定一个取值. 如果讨论的是实数的向量空间，即$v_i \in \mathbf{R}^n$，假如级数$c_1v_1+c_2v_2+\cdots$收敛，则可以为它指定一个值. 但许多级数不收敛，我们就不知道该指定什么值了. 在代数中，习惯上只谈论有限多个向量的组合. 因此，无限集S的张成定义为由那些是S中有限多个元素的组合的向量v组成的集合：

【3.7.3】 $$v=c_1v_1+\cdots+c_rv_r, \quad \text{其中 } v_1, \cdots, v_r \in S$$

S中的v_i可是任意的，数r可以任意大，与向量v有关：

【3.7.4】 $$\mathrm{Span}S=\{S \text{ 中元素的有限组合}\}$$

例如，设 $e_i=(0,\cdots,0,1,0,\cdots)$是 $\mathbf{R}^\infty$ 中第 i 个位置值为 1 且是它仅有的非零坐标的行向量. 设 $\boldsymbol{E}=(e_1,e_2,e_3,\cdots)$是这些向量 e_i 的无限集合. 集合 $\boldsymbol{E}$ 不能张成 $\mathbf{R}^\infty$，因为向量

$$w=(1,1,1,\cdots)$$

不是一个(有限)组合，而 $\boldsymbol{E}$ 的张成是子空间 Z(3.7.2)(c).

一个集合 S(不论是否无限)称为无关的，如果除了在下式中使 $c_1=\cdots=c_r=0$ 的平凡关系外，没有其他的有限线性关系：

【3.7.5】 $$c_1v_1+\cdots+c_rv_r=0,\quad v_1,\cdots,v_r\in S$$

这里数 r 也允许是任意的，即条件对任意大的 r 及任意向量 $v_1,\cdots,v_r\in S$ 都成立. 例如，假如 w，e_i 是前面定义的向量，则集合 $S'=(w;e_1,e_2,e_3,\cdots)$是无关的. 在这个无关的定义下，命题 3.4.15 仍然成立.

与有限集一样，V 的基 S 是张成 V 的一个无关集合. 这样 $S=(e_1,e_2,e_3,\cdots)$是空间 Z 的基. 单项式 x^i 构成多项式空间的一组基. 应用佐恩引理或选择公理可以证明每个向量空间 V 都有一个基(参见附录，命题 A.3.3). 然而 $\mathbf{R}^\infty$ 的一个基中将有多达不可数的元素，因而它无法被明确地写出来. 97

暂时回到向量空间是有限维的情形(3.4.16)，问是否会存在一个无限基，在(3.4.21)中，我们看到任意两个有限基都有同样多的元素. 我们现在证明每个基都是有限的，从而完成讨论. 这由下面的引理来给出.

【3.7.6】**引理** 设 V 是有限维向量空间，并设 S 是张成 V 的任意集合. 则 S 中含有一个张成 V 的有限子集.

证明 由假设，有一个有限集，比如$(u_1,\cdots,u_m)$，它张成空间 V. 因为 $\mathrm{Span}S=V$，所以每一个 u_i 是 S 中有限多个元素的线性组合. 因而当将向量 $u_1,\cdots,u_m$ 用集合 S 表出时，仅需要其中的有限多个元素. 我们用到的元素组成一个有限子集 $S'\subset S$. 于是 $(u_1,\cdots,u_m)\subset\mathrm{Span}S'$. 因为$(u_1,\cdots,u_m)$张成 V，所以 S'亦张成 V. ■

【3.7.7】**推论** 设 V 是有限维向量空间.

(a) 每个基都是有限的.

(b) 每个张成 V 的集合 S 含有一个基.

(c) 每个无关集 L 是有限的，因而扩张为一个基.

我不必学 8+7：我将记住 8+8 然后减去 1.

T. Cuyler Young, Jr.

练　习

第二节　域[⊖]

2.1 证明：形如 $a+b\sqrt{2}$的数构成复数域的一个子域，其中 a，b 是有理数.

⊖ 原文的第一节未给出练习题. ——译者注

2.2 求 5 模 p 的逆，其中 $p=7$，11，13 和 17.

2.3 当系数视为域 $\mathbf{F}_7$ 中的元素时，计算多项式的乘积$(x^3+3x^2+3x+1)(x^4+4x^3+6x^2+4x+1)$. 说明你的答案.

2.4 考虑线性方程组$\begin{bmatrix}6 & -3\\ 2 & 6\end{bmatrix}\begin{bmatrix}x_1\\ x_2\end{bmatrix}=\begin{bmatrix}3\\ 1\end{bmatrix}$.

(a) 当 $p=5$，11，17 时，在 $\mathbf{F}_p$ 中求解.

(b) 当 $p=7$ 时，求解的个数.

2.5 求素数 p 使矩阵

$$A=\begin{bmatrix}1 & 2 & 0\\ 0 & 3 & -1\\ -2 & 0 & 2\end{bmatrix}$$

98 当其元在 $\mathbf{F}_p$ 中时可逆.

2.6 完全地解线性方程组 $AX=0$ 与 $AX=B$，其中

$$A=\begin{bmatrix}1 & 1 & 0\\ 1 & 0 & 1\\ 1 & -1 & -1\end{bmatrix} \quad 和 \quad B=\begin{bmatrix}1\\ -1\\ 1\end{bmatrix}$$

(a) 在 $\mathbf{Q}$ 中 (b) 在 $\mathbf{F}_2$ 中 (c)在 $\mathbf{F}_3$ 中 (d)在 $\mathbf{F}_7$ 中

2.7 通过找本原元，对所有 $p<20$ 的素数证明乘法群 $\mathbf{F}_p^{\times}$ 是循环群.

2.8 令 p 是素数.

(a) 证明费马定理：对每个整数 a，$a^p\equiv a(\mathrm{mod}\ p)$.

(b) 证明威尔逊定理：$(p-1)!\equiv -1(\mathrm{mod}\ p)$.

2.9 在群 $GL_2(\mathbf{F}_7)$中确定矩阵$\begin{bmatrix}1 & 1\\ & 1\end{bmatrix}$和$\begin{bmatrix}2 & \\ & 1\end{bmatrix}$的阶.

2.10 在域 $\mathbf{F}_2$ 中解释矩阵元素，证明四个矩阵$\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$，$\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$，$\begin{bmatrix}1 & 1\\ 1 & 0\end{bmatrix}$，$\begin{bmatrix}0 & 1\\ 1 & 1\end{bmatrix}$构成一个域.

提示：可利用矩阵加法和乘法各种运算律缩短证明过程.

2.11 证明符号集合$\{a+bi\mid a,\ b\in \mathbf{F}_3\}$构成有九个元素的域，如果合成法则模仿复数的加法和乘法. 同样的方法对 $\mathbf{F}_5$ 行得通吗？对 $\mathbf{F}_7$ 呢？给出解释.

第三节 向量空间

3.1 (a) 证明向量与域 F 的零元素的标量乘积是零向量.

(b) 证明：若 w 是子空间 W 的元素，则 $-w$ 也在 W 中.

3.2 下列子集中哪些是系数在 F 里的 $n\times n$ 矩阵的向量空间 $F^{n\times n}$的子空间？

(a) 对称矩阵$(A=A^t)$ (b) 可逆矩阵 (c) 上三角矩阵

第四节 基和维数

4.1 求 $n\times n$ 对称矩阵$(A=A^t)$空间的一个基.

4.2 设 $W\subset\mathbf{R}^4$ 是线性方程组 $AX=0$ 的解空间，其中 $A=\begin{bmatrix}2 & 1 & 2 & 3\\ 1 & 1 & 3 & 0\end{bmatrix}$. 求 W 的基.

4.3 证明三个函数 x^2，$\cos x$ 和 e^x 是线性无关的.

4.4 设 A 是一个 $m\times n$ 矩阵，并设 A'为由 A 上作一系列初等行变换得到的矩阵. 证明 A 的行与 A'的行张成同样的子空间.

4.5 令 $V=F^n$ 是列向量空间. 证明 V 的每个子空间都是某个其次线性方程组 $AX=0$ 的解空间. 99

4.6 求方程 $x_1+2x_2+3x_3+\cdots+nx_n=0$ 在 $\mathbf{R}^n$ 里解空间的一个基.

4.7 令$(X_1,\cdots,X_m)$与$(Y_1,\cdots,Y_n)$分别是 $\mathbf{R}^m$ 与 $\mathbf{R}^n$ 的基. mn 个矩阵 $X_iY_j^t$ 构成所有 $m\times n$ 矩阵的向量空间 $\mathbf{R}^{m\times n}$的一个基吗?

4.8 证明 F^n 中向量集$(v_1,\cdots,v_n)$是一个基当且仅当由诸 v_i 的坐标向量构成的矩阵是可逆的.

第五节 用基计算

5.1 (a) 证明集合 $\boldsymbol{B}=((1,2,0)^t,(2,1,2)^t,(3,1,1)^t)$是 $\mathbf{R}^3$ 的基.

(b) 求向量 $v=(1,2,3)^t$ 关于这个基的坐标向量.

(c) 设 $\boldsymbol{B}'=((0,1,0)^t,(1,0,1)^t,(2,1,0)^t)$求从 $\boldsymbol{B}$ 到 $\boldsymbol{B}'$的基变换矩阵 P.

5.2 (a) 当旧基是标准基 $\boldsymbol{E}=(e_1,e_2)$且新基是 $\boldsymbol{B}=(e_1+e_2,e_1-e_2)$时，在 $\mathbf{R}^2$ 中确定基变换的矩阵.

(b) 当旧基是标准基 $\boldsymbol{E}$ 且新基是 $\boldsymbol{B}=(e_n,e_{n-1}\cdots,e_1)$时，在 $\mathbf{R}^n$ 中确定基变换的矩阵.

(c) 令 $\boldsymbol{B}$ 是 $\mathbf{R}^2$ 的基，其中 $v_1=e_1$，而 v_2 是与 v_1 夹角为 120°的单位向量. 确定将标准基 $\boldsymbol{E}$ 联系到基 $\boldsymbol{B}$ 的基变换的矩阵.

5.3 令 $\boldsymbol{B}=(v_1,\cdots,v_n)$是向量空间 V 的基. 证明可以由 $\boldsymbol{B}$ 经过有限步下列类型的作用得到任意一个其他基 $\boldsymbol{B}'$.

(i) 对某个 $a\in F$，用 v_i+av_j 代替 v_i，其中 $i\neq j$.

(ii) 对某个 $c\neq 0$ 用，cv_i 代替 v_i.

(iii) 交换 v_i 和 v_j.

5.4 令是 $\mathbf{F}_p$ 素域，且设 $V=\mathbf{F}_p^2$. 证明：

(a) V 的基的个数等于一般线性群 $GL_2(\mathbf{F}_p)$的阶.

(b) 一般线性群 $GL_2(\mathbf{F}_p)$的阶是 $p(p+1)(p-1)^2$，而且特殊线性群 $SL_2(\mathbf{F}_p)$的阶是 $p(p+1)(p-1)$.

5.5 在下列空间里每个维数的子空间有多少个?

(a) $\mathbf{F}_p^3$ (b) $\mathbf{F}_p^4$.

第六节 直和

6.1 证明实 $n\times n$ 矩阵空间 $\mathbf{R}^{n\times n}$是对称矩阵$(A^t=A)$空间和反对称矩阵$(A^t=-A)$空间的直和.

6.2 方阵的迹是它的对角线上元素的和. 令 W_1 是迹为零的 $n\times n$ 矩阵空间. 求子空间 W_2 使得 $\mathbf{R}^{n\times n}=W_1\oplus W_2$.

6.3 令 $W_1,\cdots,W_k$ 是向量空间 V 的子空间，使得 $V=\sum W_i$. 假设 $W_1\cap W_2=0$，$(W_1+W_2)\cap W_3=0$，$\cdots$，$(W_1+\cdots+W_{k-1})\cap W_k=0$. 证明 V 是子空间 $W_1,\cdots,W_k$ 的直和. 100

第七节 无限维空间

7.1 令 $\boldsymbol{E}$ 是 $\mathbf{R}^\infty$ 中的向量集$(e_1,e_2\cdots)$，设 $w=(1,1,1,\cdots)$. 描述集合$(w,e_1,e_2\cdots)$的张成.

7.2 双边无穷行向量$(a)=(\cdots,a_{-1},a_0,a_1,\cdots)$构成一个空间，其中 $a_i\in\mathbf{R}$. 证明该空间同构于 $\mathbf{R}^\infty$.

*7.3 对每个正整数 p，可定义空间 ℓ^p 为使得$\sum|a_i|^p<\infty$的序列的空间. 证明 ℓ^p 是 ℓ^{p+1}的真子空间.

*7.4 令 V 是由可数无限集合张成的向量空间. 证明 V 的每个无关子集是有限的或是可数无限的.

杂题

M. 1 考虑行列式函数 $\det: F^{2\times 2}\to F$，其中 $F=F_p$ 是 p 个元素的素域而 $F^{2\times 2}$ 是 2×2 矩阵的空间. 证明这个映射是满射，并且所有非零行列式的值取同样多的次数，但行列式为 0 的矩阵比行列式为 1 的矩阵多.

M. 2 设 A 是 $n\times n$ 实矩阵. 证明存在整数 N 使 A 满足非平凡多项式关系 $A^N+c_{N-1}A^{N-1}+\cdots+c_1A+c_0=0$.

M. 3 (多项式路)

(a) 令 $x(t)$和 $y(t)$是实系数二次多项式. 证明路$(x(t),\ y(t))$的像包含在圆锥曲面上，亦即，存在实二次多项式 $f(x,\ y)$使得 $f(x(t),\ y(t))$恒为零.

(b) 令 $x(t)=t^2-1$ 与 $y(t)=t^3-t$. 求非零实多项式 $f(x,\ y)$使得 $f(x(t),\ y(t))$恒为零. 在 $\mathbf{R}^2$ 里画出$\{f(x,\ y)=0\}$的轨迹和路$(x(t),\ y(t))$.

(c) 证明每对实多项式 $x(t)$，$y(t)$满足某个实多项式关系 $f(x,\ y)=0$.

*M. 4 设 V 是无限域 F 上的向量空间. 证明 V 不是有限多个真子空间的并.

*M. 5 令 α 是 2 的实立方根.

(a) 证明$(1,\ \alpha,\ \alpha^2)$在 Q 上是无关的集合，亦即，没有形如 $a+b\alpha+c\alpha^2$ 的关系，其中 a，b，c 是整数.

提示：用 cx^2+bx+a 除 x^3-2.

(b) 证明实数 $a+b\alpha+c\alpha^2$ 构成域，其中 a，b，$c\in\mathbf{Q}$.

M. 6 (辣酱：数学游戏)我的堂兄 Phil 收集辣汁. 他有大约一百个不同的瓶子在书架上，它们当中许多(例如 Tabasco 牌子辣酱油)除水外仅有三种成分：辣椒，醋和食盐. Phil 手头最少需要有多少辣汁瓶子以便他混合已有的辣汁能够获得任意一个仅有这三种成分的辣汁配方？

101

第四章　线性算子

思维混乱和推理错误仍笼罩着代数的开端，
这是冷静深思的人们的诚挚而公正的抱怨.

——William Rowan Hamilton 爵士

第一节　维数公式

从域 F 上的一个向量空间到另一个向量空间的线性变换 $T:V\to W$ 是一个映射，它与加法和标量乘法相容：

【4.1.1】　　$T(v_1+v_2)=T(v_1)+T(v_2),\quad T(cv_1)=cT(v_1)$

对所有 V 中的 v_1，v_2 及所有 $c\in F$ 成立. 这个概念与群的同态相似，称之为同态也是合适的. 线性变换与任意线性组合相容：

【4.1.2】　　$$T\Big(\sum_i v_i c_i\Big)=\sum_i T(v_i)c_i$$

由元素属于 F 的 $m\times n$ 矩阵 A 的左乘，映射

【4.1.3】　　$$F^n \xrightarrow{A\text{左乘}} F^m \text{ 映 } X\rightsquigarrow AX$$

是一个线性变换. 的确，$A(X_1+X_2)=AX_1+AX_2$，且 $A(cX)=cAX$.

如果 $\boldsymbol{B}=(v_1,\cdots,v_n)$是域 F 上向量空间 V 的子集，映 $X\rightsquigarrow \boldsymbol{B}X$ 的映射 $F^n\to V$ 是一个线性变换.

另一个例子：设 P_n 为次数$\leqslant n$ 的形如

【4.1.4】　　$$a_n t^n+a_{n-1}t^{n-1}+\cdots+a_1 t+a_0$$

的实多项式函数的向量空间. 导数$\dfrac{\mathrm{d}}{\mathrm{d}t}$定义了从 P_n 到 P_{n-1}的一个线性变换.

有两个与线性变换相伴随的重要子空间：

【4.1.5】　　$$\ker T=T\text{ 的核 }=\{v\in V\mid T(v)=0\},$$
$$\mathrm{im}T=T\text{ 的像 }=\{w\in W\mid \text{对某个 } v\in V, w=T(v)\}$$

102

核常常称为线性变换的零空间. 与群同态类似，读者可能猜到，$\ker T$ 是 V 的子空间，而 $\mathrm{im}T$ 是 W 的子空间.

本节的主要结果是下面定理.

【4.1.6】**定理**(维数公式)　设 $T:V\to W$ 是一个线性变换. 则

$$\dim(\ker T)+\dim(\mathrm{im}T)=\dim V$$

线性变换 T 的零化度和秩分别是 $\ker T$ 和 $\mathrm{im}T$ 的维数，矩阵 A 的零化度和秩可类似地