数学基础选讲

程艺 编著

中 国 科 学 技 术 大 学

二〇二二年一月

前　言

对于理工科专业大学新生, 数学是他们入学后面临的一大挑战. 即使那些在高中阶段成绩十分突出的学生, 也要经历较为艰难的适应过程. 他们不仅是要适应大学数学课程教学方法和目标要求 , 更重要的是要尽快提高抽象概念理解能力, 适应分析问题思维方式.

编写本《数学基础选讲》(简称《选讲》) , 正是希望为即将进入大学高中生或大学新生, 对大学数学课程中一些基本概念和思想, 对分析和处理问题思维方式等方面提供“先修”或辅助素材, 以期从思维方式上完善高中和大学数学教育的衔接. 所选择的专题, 虽然不是大学某门特定课程的“先修课程”, 但在兼顾与高中课程 (含选修模块) 衔接的同时, 聚焦分析、代数和几何等大学数学课程, 为学习这些课程做一些基础性铺垫和准备. 每个专题并不追求内容的完整性和深度, 试图以更加简洁方式, 从易于高中生或大学新生理解角度, 讲清楚一些大学数学课程中基本概念的形成和背景, 力争体现由浅入深, 由具体到抽象, 由形象直观到理性思维的认识规律. 帮助学生提高素养、拓宽视野, 更好地理解和体会如何从问题入手, 产生新的数学思想、方法和理论过程. 使学生在抽象思维养成和分析问题能力上“渐入佳境”.

第 1 讲主要从四个方面, 让学生进一步理解“无限”的概念. 从自然数归纳公理看自然数无限性以及数学归纳法在处理“无限”问题中重要性; 从集合之间的对应, 引出无限集合“基数”; 从有限求和到无限求和, 借用中学所学习的“任意”和“存在”两个量词, 准确刻画无限求和含义, 为微积分中极限理论做了基本介绍; 从两直线 (平面) 上点的“射影”、反演变换和球极投影, 介绍在几何上如何理解“无限远点”.

第 2 讲是关于整数的基本内容, 介绍了整数带余除法、辗转相除、素数、同余、同余类和同余方程,以及多项式等有关知识. 也为进一步学习代数学提供基本模型.

第 3 讲从有理数域、可公度和不可公度讲起, 从序到有界, 再到确界原理, 最后给出实数域的定义; 讨论了正实数的指数幂和对数; 解释了十进制无穷小数; 最后选择 Dedekind 分割作为实数构造的一种方法. 使学生对实数域有进一步理解.

第 4 讲是关于复数, 主要内容包括复数起源、复数域与实数域的区别、Euler 公式、代数学基本定理、单位根等有关问题. 最后通过一些例子简单介绍了复变数函数一些基本特点.

第 5 讲以空间解析几何作为基础, 从几何直观上介绍向量的代数运算、内积, 引进坐标系. 然后以三维空间作为具体例子, 抽象出一般向量空间的定义和内积, 完成从具体到抽象的过程. 并对向量空间, 线性方程组和解空间做了简单介绍. 为学生进一步学习线性代数做了铺垫.

第 6 讲是关于用直尺和圆规尺规作图问题. 让学生感受到如何将一个纯几何问题抽象成代数问题, 最终用代数方法, 解决著名的三个尺规作图不可解问题. 同时从尺规作图, 引进并简单介绍了数域的扩张.

第 7 讲是关于有限群的介绍. 虽然群论是一门比较深澳的数学理论, 但是通过回顾二次和三次方程代数求解方法, 逐步引进根的置换和置换的运算, 再抽象出“群”概念, 比较容易接受. 然后以对称群为模型, 介绍了有限群一些基本知识. 考虑到这个专题所涉内容的广泛性和深刻性, 这里只是从问题出发, 引入了群的概念和基本性质, 不再作更加深入的讨论.

《选讲》各专题之间虽有一定的连贯性, 但可作适当分类. 其中第 1、3、5 讲可作为《微积分》先修内容; 第 4、5 讲可作为《线性代数》先修内容; 第 1、5 讲提供了必要的几何基础知识; 而第 2、6、7 讲主要涉及部分代数学基本思想和内容.

《选讲》中的主要内容将会出现在本科数学专业的不同课程之中, 有些却超出其他理工科专业数学课程的基本要求. 因此对于选择数学专业的学生, 可将《选讲》作为“先修”和“热身”资料; 而对于选择非数学专业的理工科学生, 除了“先修”基本的数学思想和方法外, 还将会起到拓宽知识面, 提高数学素养的作用.

专题中一些带“$*$”内容可以根据情况进行取舍.每个专题都配有少量习题, 帮助学生理解专题内容.

编者在为中国科学技术大学少年班和创新班一年级《数学分析》教学中, 曾将《选讲》中部分内容穿插讲授, 或作为自学和教学补充材料提供给学生, 为他们打下“宽、厚、实”数学基础, 更好地学习数学课程, 起到了一定作用. 编者注意到, 目前一些大学正尝试在高中开展“先修计划”, 部分高中也开设了“强基班”. 也许《选讲》中的专题为“先修计划”或高中“强基班”提供数学方面的学习或参考材料.

本《选讲》在编写过程中参考借鉴了已经出版一些书籍 (见参考书目), 部分例题和习题也来自参考书目和一些网络资料. 在此向参考书籍和资料作者深表感谢. 编者的同事们对本书的编写给予了大力支持和鼓励, 提出了许多中肯意见和建议, 在此一并致谢. 鉴于编写水平有限, 选材恐有偏颇, 错误难以避免, 恳请读者不吝指正.

参考书目:

[1] R. Courant, H. Robbins 著, I Stewart 修订, 左平、张饴慈译:《什么是数学》, 复旦大学出版社, 2018.

[2] 谷超豪:《谈谈数学中的无限》, 上海教育出版社出版, 1988.

[3] 冯克勤、余红兵:《整数与多项式》, 高等教育出版社, 1999.

[4] W. Rudin 著, 赵慈庚、蒋铎译:《数学分析原理》, 机械工业出版社 2005.

[5] 程艺、陈卿、李平、许斌:《数学分析讲义》(第三册), 高等教育出版社, 2020.

[6] K. F. Riley, M. P. Hobson, S. J. Bence: Mathematical Methods for Physics and Engineering, Cambridge University Press, 2006.

[7] 楼红卫:《数学分析–要点·难点·拓展》, 高等教育出版社, 2020.

[8] 陈发来、陈效群、李思敏、王新茂:《线性代数与解析几何》, 高等教育出版社, 2011.

[9] 李尚志:《三等分角与数域扩充》, 湖南教育出版社, 2004.

[10] 李世雄:《代数方程与置换群》, 上海教育出版社, 1981.

[11] 欧阳毅、申伊垠:《代数学I: 代数学基础》, 高等教育出版社, 2016.

编者

2021 年 2 月于中国科学技术大学

目　录

前言 ····· **I**

第 1 讲　无限 ····· **1**
§1.1 自然数的无限性和数学归纳法 ····· 1
§1.2 无限集合 ····· 4
§1.3 无限求和 ····· 11
§1.4 无限远点* ····· 21
第 1 讲习题 ····· 33

第 2 讲　整数 ····· **36**
§2.1 正整数与整数 ····· 36
§2.2 数的整除性 ····· 38
§2.3 Euclid 辗转相除法 ····· 40
§2.4 素数和整数的素因子分解 ····· 42
§2.5 Euler 函数 ····· 45
§2.6 同余 ····· 47
§2.7 同余方程（组） ····· 55
§2.8 多项式 ····· 60
第 2 讲习题 ····· 66

第 3 讲　实数 ····· **69**
§3.1 有理数域 ····· 69
§3.2 可公度与不可公度 ····· 72
§3.3 实数域 ····· 73
§3.4 正实数的指数幂和对数 ····· 79
§3.5 十进制小数 ····· 83
§3.6 Dedekind分割* ····· 87
第 3 讲习题 ····· 95

第 4 讲　复数 ····· **97**
§4.1 复数起源和复数域 ····· 97
§4.2 复数的几何含义和 Euler 公式 ····· 99
§4.3 代数基本定理 ····· 102
§4.4 单位根 ····· 104
§4.5 复变数函数* ····· 108
第 4 讲习题 ····· 112

第 5 讲　解析几何与向量空间 · · · · · 116
§5.1 向量及其代数运算 · · · · · 117
§5.2 向量的坐标表示和坐标系 · · · · · 122
§5.3 坐标变换 · · · · · 126
§5.4 平面、直线与二次曲面 · · · · · 129
§5.5 其它常用坐标系* · · · · · 135
§5.6 一般向量空间 · · · · · 137
§5.7 线性方程组 · · · · · 147
第 5 讲习题 · · · · · 153

第 6 讲　尺规作图 · · · · · 155
§6.1 尺规在作图中的功能 · · · · · 155
§6.2 作图的代数表示 · · · · · 156
§6.3 数域的扩张 · · · · · 162
§6.4 尺规作图与三次代数方程的根 · · · · · 167
§6.5 尺规作图中三个不可解问题 · · · · · 169
§6.6 等分圆周的尺规作图问题* · · · · · 172
第 6 讲习题 · · · · · 178

第 7 讲　有限群 · · · · · 180
§7.1 代数方程的求解 · · · · · 180
§7.2 对称多项式 · · · · · 183
§7.3 代数方程根的置换 · · · · · 185
§7.4 置换及其性质 · · · · · 189
§7.5 有限群及其性质 · · · · · 193
第 7 讲习题 · · · · · 207

第 1 讲　无限

无限（或无穷）在数学中起着重要作用. 自然数序列的无限性是最简单例子, 直线或平面上所有点的集合等等, 也都是包含无穷多个对象（或称为元素）. 在数学中, 我们将面临大量如何处理具有无穷多个元素集合, 还将面临如何从有限过渡到无限等一系列问题.

§1.1　自然数的无限性和数学归纳法

自然数就是熟知的

$$\mathbb{N} = \{0,\ 1,\ 2,\ 3,\ \cdots\},$$

其中的 $\{1, 2, 3, \cdots\}$ 也称为**正整数**. 自然数公理化定义由 Peano（皮亚诺, 1858 -1932）给出, 在此不作详细介绍. 自然数基本性质包括自然数的算术：自然数之间加法和乘法, 以及加法和乘法所服从交换律、结合律和分配律; 自然数的有序性: 任何两个自然数之间一定存在大小关系; 自然数的无限性: 自然数是没有止境的, 任何自然数 n 后, 还可以写出下一个自然数 $n+1$. 自然数的无限性可总结为下列归纳公理:

归纳公理： 设 $S \subseteq \mathbb{N}$, 如果 S 满足

(i)　$0 \in S$,

(ii)　若 $n \in S$, 则 $n+1 \in S$,

那么 $S = \mathbb{N}$.

由归纳公理, 不难得到下列最小数原理.

定理 1.1 (最小数原理)　设 T 是 $\mathbb{N}$ 非空子集. 则 T 中必有最小自然数.

证明　设

$$S = \{s \mid s \in \mathbb{N},\ s \leqslant t,\ \text{对任意 } t \in T \text{ 成立}\}.$$

显然, $0 \in S$, 因此 S 非空. 又因为 T 非空, 对 $t \in T$, 有 $t+1 > t$, 所以 $t+1 \notin S$, 也就是 $S \neq \mathbb{N}$.

据此推出: 存在 $s_0 \in S$, 而 $s_0 + 1 \notin S$. 否则, 若这样的 s_0 不存在, 就意味着对任意 $s \in S$, 都有 $s+1 \in S$, 根据归纳原理推出 $S = \mathbb{N}$, 这与 $S \neq \mathbb{N}$ 相矛盾.

若 $s_0 \notin T$, 则对于任意 $t \in T$, 都有 $s_0 < t$, 也就是 $s_0 + 1 \leqslant t$, 推出 $s_0 + 1 \in S$, 这与 s_0 选取矛盾. 所以 $s_0 \in T$. 但 $s_0 \in S$, 因此对任意 $t \in T$, 有 $s_0 \leqslant t$, 即 s_0 是 T 的最小数.

注意, 这里的“最小数原理”仅是自然数集的最小数原理. 例如, 数集

$$\left\{1,\ \frac{1}{2},\ \frac{1}{3},\ \frac{1}{4},\ \cdots,\ \frac{1}{n},\ \cdots\right\}$$

中就没有最小数.

归纳公理是常用的数学归纳法基础. 所谓数学归纳法是数学推理中基本方式之一. 用来证明包含无限序列命题的数学定理.

例 1.1.1 任意 $n+2$ 条边凸多边形内角之和等于180° 的 n 倍.

这是一个对每一个正整数 n 都成立命题. 如果采用一个一个地验证, 不管验证到多少, 仍然不能说明命题为真. 必须采用严格数学推理方法加以证明.

显然, 当 $n=1$ 时, 凸多边形就是三角形, 因此用独立于该命题的其它结果, 得出三角形内角之和等于 180° .

对于 $n=2$ 凸四边形, 作一条对角线把四边形分成两个三角形,因此利用三角形内角之和等于 180° 的结论推出凸四边形内角之和等于 $2\cdot 180^\circ$.

接着对于 $n=3$ 凸五边形, 把它分解成三角形和凸四边形,再利用已经证明的关于三角形和凸四边形内角之和结论得到凸五边形内角之和等于 $180^\circ+2\cdot 180^\circ=3\cdot 180^\circ$.

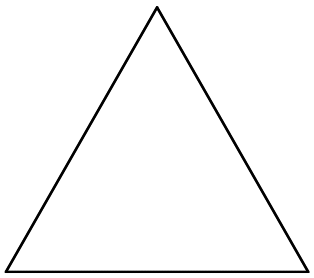


图 1.1： n=1

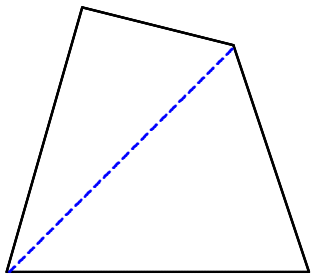


图 1.2： n=2

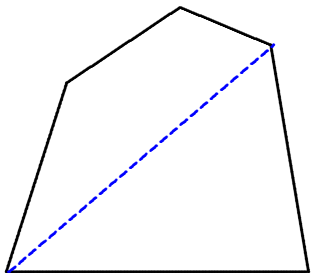


图 1.3： n=3

以此类推, 可以逐次证明 $n=4, n=5$ 等情形. 每一步都以同样方式由前面的结论推出.

上述推导思想基于以下两点：

一是对 $n=1$ 或前几个情形的正确性, 可通过验证得到. 在例1.1.1中, 借助熟知的三角形内角之和等于 180° , 可以直接验证前几种情形的正确性.

二是存在一种一般方法表明：如果命题对 n 成立, 那么对 $n+1$ 也成立. 在例1.1.1中, 这个一般方法就是把 $n+2$ 条边凸多边形分解成三角形和 $n+1$ 条边凸多边形.

因此, 为了证明命题对所有正整数 n 成立, 把上述分析提炼为如下定理.

定理 1.2 设 A_n $(n=1,2,\cdots)$ 为一系列命题, 如果

(i) 当 $n=1$ 时, A_1 成立;

(ii) 对任意正整数 n, 由 A_n 成立可推出 A_{n+1} 成立. 或由前 n 个 $A_1, A_2, \cdots, A_n$ 成立可推出 A_{n+1} 成立.

那么, A_n 对所有 $n \geqslant 1$ 成立.

证明 采取反证法: 假设有某个命题 A_r $(r>1)$ 不成立, 那么, 集合

$$S = \{k \geqslant 1 \mid A_k \text{ 不成立}\}$$

非空 ($r \in S$). 根据最小数原理, 存在最小数 $n \in S$. 由 (i) 可知 $1 \notin S$, 所以 $n > 1$. 又因为 n 是 S 中最小数, 所以$n-1 \notin S$, 即 A_{n-1} 成立, 由 (ii) 推出 A_n 也成立. 但是 $n \in S$ 表示 A_n 不成立, 因此推出矛盾. 说明假设是错误的, 所以 A_n $(n \geqslant 1)$ 都成立. □

例 1.1.2 对任意正整数 n, 求证 $f(n) = n^4 + 2n^3 + 2n^2 + n$ 能被 6 整除.

证明 当 $n=1$ 时, $f(1)=6$, 显然能被 6 整除.

假设 $f(n)$ 能够被 6 整除, 那么

$$\begin{aligned} f(n+1) =& (n+1)^4 + 2(n+1)^3 + 2(n+1)^2 + (n+1) \\ =& (n^4 + 4n^3 + 6n^2 + 4n + 1) \\ & + 2(n^3 + 3n^2 + 3n + 1) + 2(n^2 + 2n + 1) + (n+1) \\ =& (n^4 + 2n^3 + 2n^2 + n) + (4n^3 + 12n^2 + 14n + 6) \\ =& f(n) + (4n^3 + 12n^2 + 14n + 6) \end{aligned}$$

根据归纳假设, 上式右边第一项能够被 6 整除, 第二项中 $12n^2+6$ 也能够被 6 整除. 因此只要证明剩余的 $4n^3+14n$ 能够被 6 整除, 或要证明 $2n^3+7n$ 能够被 3 整除即可.

为此, 需要再次用归纳法去证明: 对任意正整数 n, $2n^3+7n$ 能够被 3 整除.

这个命题对 $n=1$ 显然成立. 假设对一般 n, $2n^3+7n$ 能够被 3 整除, 那么对 $n+1$, 有

$$2(n+1)^3 + 7(n+1) = (2n^3 + 7n) + 3(2n^2 + 2n + 3).$$

根据归纳假设, 右边第一项能被 3 整除, 而第二项是 3 的倍数, 当然也能被 3 整除. 这样就证明了对任意正整数 n, $2n^3+7n$ 能够被 3 整除. 因此也就证明了对任意正整数 n, $f(n) = n^4 + 2n^3 + 2n^2 + n$ 能被 6 整除.

这里再次强调使用数学归纳法必须确保定理1.2中条件 (i) 和 (ii) 真正被满足.

例 1.1.3 用 $\max\{a,b\}$ 表示 a 和 b 中较大的一个数. 考虑下列命题:

对任意正整数 n, 命题 A_n: 若 a, b 是使得 $\max\{a, b\} = n$ 成立的任意两个正整数, 则 $a = b$.

按照归纳法步骤, 不难验证A_1 显然成立, 这是因为对任意两个满足 $\max\{a, b\} = 1$ 正整数, 一定有 $a = b = 1$.

假设 A_n 成立, 那么对 A_{n+1}, 设 a, b 是使得 $\max\{a, b\} = n + 1$ 的任意两个正整数, 令

$$a' = a - 1,\ b' = b - 1$$

则 $\max\{a', b'\} = n$, 因为已经假设 A_n 成立, 因此推出 $a' = b'$, 即 $a = b$, 也就是命题对 $n + 1$ 也成立. 这样根据数学归纳法, 就有对任意 n, 命题都成立.

但是, 取 $a = 5, b = 2$, 则 $n = \max\{5, 2\} = 5$, 命题对 $n = 5$ 成立, 意味着 $5 = 2$. 这样的结论显然是错误的. 那么问题出在哪里呢?

在上述推导中, 由 $a' = a-1$, $b' = b-1$ 不难看出 , 对任意两个满足 $\max\{a, b\} = n+1$ 的正整数 a, b, 并不能保证 a', b' 仍然是正整数, 因此也就无法使用归纳假设.

§1.2 无限集合

有限个元素所组成的集合称为有限集合. 有限集合中元素个数是一个最基本量, 称为集合的**基数**. 有限集合基数可以通过计算集合中元素个数得到, 不管该集合的元素是什么. 例如集合$\{a, b, c, d\}$ 基数是 4, 集合$\{2, 4, 6, 8\}$ 基数也是 4. 空集 ϕ 的基数为 0. 计算一个有限集合基数, 其实是将集合的元素与自然数子集 $\{1, 2, \cdots, n\}$ 作 1-1 对应, 其中的 n 就是集合基数.

两个有限集合基数大小也可以直接进行比较, 例如一群小朋友分苹果. 每个小朋友仅拿一个苹果, 如果苹果分光了, 还有小朋友没有拿到, 说明小朋友集合基数大于苹果集合基数. 若每个小朋友都拿到一个, 还有剩余苹果, 说明小朋友集合基数小于苹果集合基数. 如果正好每人分得一个苹果, 没有剩余, 说明小朋友与苹果集合的基数相等.

1° 集合的 1-1 对应

现将通过 1-1 对应来考察有限集合基数是否相等的做法, 推广到一般集合中去, 为此先给出如下定义.

定义 1.3 设A, B为两个集合, f 是两个集合之间的映射

$$f : A \longrightarrow B$$

(i) 若对 A 中任意元素 a, a', 只要 $a \neq a'$, 就有 $f(a) \neq f(a')$, 则称映射为***单射***.

(ii) *若对 B 中任意元素 b, 至少存在A 中元素 a, 使得 $f(a)=b$, 则称映射为**满射**.*

(iii) *若映射既是单射又是满射, 则称映射为1-1 **映射(或称1-1对应)**.*

形象地说, 如果把 A 看成是子弹的集合, B 看成是靶子的集合, 那么

单射表示不同的子弹击中不同的靶子.

满射表示任何一个靶子至少被一颗子弹击中.

1-1 映射表示每颗子弹击中一个靶子, 每个靶子只被一颗子弹击中.

利用 1-1 对应, 可以比较两个集合之间的基数, 特别是当选择自然数的子集合 $\{1,2,\cdots,n\}$ 作为标准, 则通过考察与它是否 1-1 对应, 定义有限集合与无限集合.

定义 1.4 *设 A,B 为两个集合.*

(i) *若存在$A\to B$ 的 1-1 对应, 则称A 和 B 有**相同基数**, 或者称两者**等势**.*

(ii) *若存在$A\to B$ 的满射, 但不存在$A\to B$ 的单射 (因此也就不存在A 和 B之间 1-1 对应) , 则称集合A比集合B具有**更大基数**.*

(iii) *若存在正整数 n, 使得A与集合 $\{1,2,\cdots,n\}$ 之间有1-1 对应, 则称A为**有限集合**, n 为其基数; 若这样的n不存在, 则称A为**无限集合**.*

2° 可数集合

以下为了方便, 考虑正整数集合, 并仍然定义

$$\mathbb{N}=\{1,\ 2,\ 3,\ \cdots\},$$

我们将看到, 从基数角度看, 无限集合中去掉或增加有限个元素基数不变. 因此包含 0 的自然数集合与不包含 0 的正整数集合的基数是相等的.

定义 1.5 *正整数集合 $\mathbb{N}=\{1,\ 2,\ 3,\ \cdots\}$ 的基数称为**可数的**, $\mathbb{N}$ 称为**可数集合**. 任何与 $\mathbb{N}$ 1-1 对应集合的基数也是可数的, 这样的集合统称为**可数集合**.*

对于有限集合 A , 数一数 A 中元素个数, 就是把 A 中元素与自然数子集合 $\{1,2,\cdots,n\}$ 1-1 对应

$$\begin{array}{ccccc} 1 & 2 & 3 & \cdots & n \\ \updownarrow & \updownarrow & \updownarrow & \cdots & \updownarrow \\ a_1 & a_2 & a_3 & \cdots & a_n \end{array}$$

或者说就是给 A 中元素进行一种不重复排列 (或编号) , 当然, 排列方式不唯一. 显然, 对于有限集合, 去掉若干个元素, 或增加若干个元素, 都不可能与原集合 1-1 对应, 也就是基数不可能再相等.

对于可数集合 A, 也可以通过与 $\mathbb{N}=\{1,\ 2,\ 3,\ \cdots\}$ 的 1-1 对应进行不重复的排

列 (编号):

$$\begin{array}{cccccc} 1 & 2 & 3 & \cdots & n & \cdots \\ \updownarrow & \updownarrow & \updownarrow & \cdots & \updownarrow & \cdots \\ a_1 & a_2 & a_3 & \cdots & a_n & \cdots \end{array}$$

因此可数集合也称为**可列**集合, 集合的元素可以排列为:

$$A = \{a_1, a_2, \cdots, a_n, \cdots\}.$$

但是对于可数集合, 其中无限个元素组成的子集合也具有相同基数. 例如 $\mathbb{N}$ 中所有偶数组成子集合与 $\mathbb{N}$ 是 1-1 对应的:

$$\begin{array}{cccccc} 1 & 2 & 3 & \cdots & n & \cdots \\ \updownarrow & \updownarrow & \updownarrow & \cdots & \updownarrow & \cdots \\ 2 & 4 & 6 & \cdots & 2n & \cdots \end{array}$$

因此所有偶数集合也是可数集合, 虽然偶数只是正整数中的一部分. 同样, 正整数中所有完全平方数集合 $\{1, 4, 9, 16, 25, \cdots, \}$ 也是可数的:

$$\begin{array}{cccccc} 1 & 2 & 3 & \cdots & n & \cdots \\ \updownarrow & \updownarrow & \updownarrow & \cdots & \updownarrow & \cdots \\ 1^2 & 2^2 & 3^2 & \cdots & n^2 & \cdots \end{array}$$

可见, 无限集合具有一些独特的性质.

性质 1.6 设 U 是一个无限集合, 若存在从 $\mathbb{N} = \{1, 2, 3, \cdots\}$到 U的满射

$$f : \mathbb{N} \longrightarrow U,$$

则 U是可数集合. 特别, $\mathbb{N}$ 的任何无限真子集是可数集.

证明 证明关键是通过满射, 构造 U 中所有元素一个不重复排列, 也就是建立 U 与 $\mathbb{N}$ 1-1 对应. 记 $j_1 = 1$, 并令

$$a_1 = f(j_1) = f(1) \in U,$$

因为f为满射且U是无限集, 所以集合

$$E_1 = \{n > j_1 \mid f(n) \neq a_1\}$$

非空. 根据最小数原理, E_1 存在最小数 $j_2 > j_1$, 记

$$a_2 = f(j_2) \in U.$$

且 $a_2 \neq a_1$. 根据 j_2 的选取, 推出 $1, 2, \cdots, j_2$ 在 f 下的像只能是 a_1 或 a_2 :

$$f : \{1, 2, \cdots, j_2\} \longrightarrow \{a_1, a_2\}.$$

再令

$$E_2 = \{n > j_2 \mid f(n) \neq a_1, f(n) \neq a_2\},$$

并取 E_2 的最小数 $j_3 > j_2$.记

$$a_3 = f(j_3),$$

因此 a_1, a_2, a_3 两两不等, 且

$$f : \{1, 2, \cdots, j_2, \cdots, j_3\} \longrightarrow \{a_1, a_2, a_3\}.$$

假设已经取到 $j_k > j_{k-1} > \cdots > j_1$, 使得 $a_l = f(j_l),\ l = 1, 2, \cdots, k$ 两两互不相等, 并且 $1, 2, 3, \cdots, j_k$ 在 f 下的像为 $\{a_1, \cdots, a_k\}$:

$$f : \{1, 2, \cdots, j_k\} \longrightarrow \{a_1, a_2, \cdots, a_k\}.$$

那么记

$$E_{k+1} = \{n > j_k \mid f(n) \neq a_l,\ l = 1, 2, \cdots, k\},$$

取 E_{k+1} 的最小数 $j_{k+1} > j_k$ 并记

$$a_{k+1} = f(j_{k+1}),$$

则 $a_{k+1}, a_k, \cdots, a_1$ 互不相等, 且

$$f : \{1, 2, 3, \cdots, j_k, \cdots, j_{k+1}\} \longrightarrow \{a_1, \cdots, a_k, a_{k+1}\}.$$

由于 f 是满射, 这样得到一个严格递增的正整数数列 $j_1 < j_2 < j_3 < \cdots$和 U中元素的一个排列

$$U = f(\mathbb{N}) = \{a_1, a_2, a_3, \cdots\}.$$

因此 U 是可数的.

设 V 为 $\mathbb{N}$ 的无限真子集. 取定一个V中的元素m, 定义映射$f : \mathbb{N} \to V$如下:

$$\text{对任意 } n \in \mathbb{N},\ f : n \longmapsto f(n) = \begin{cases} n, & \text{当 } n \in V \\ m, & \text{当 } n \notin V. \end{cases}$$

显然$f : \mathbb{N} \to V$是满射. 由前面推导结果可知V为可数集. □

根据性质1.6, 在 $\mathbb{N}$ 中去掉有限个数, 或即使去掉无限个数, 只要剩余的数仍然是无限集合, 那么基数不变. 下面性质说明在可数集合中增加有限个元素, 甚至增加可数个元素, 基数仍然不变.

性质 1.7 *有限集合与可数集合的并集是可数集合; 有限个可数集合的并集仍然是可数集合; 可数个可数集合的并集还是可数集.*

证明 这里只讨论第三种情形. 设$A_1, A_2, \cdots$为可数个可数集. 记

$$A_k = \{a_{k1}, a_{k2}, \cdots, a_{kn}, \cdots\}, \quad k = 1, 2, 3, \cdots.$$

那么并集$\bigcup\limits_{k=1}^{\infty} A_k$里所有元素可以有如下排列:

$$\begin{array}{cccc} a_{11} & a_{12} & a_{13} & \cdots \\ a_{21} & a_{22} & a_{23} & \cdots \\ a_{31} & a_{32} & a_{33} & \cdots \\ \cdots & \cdots & \cdots & \cdots \end{array}$$

顺时针旋转45°, 可以把上述排列看成一个大三角形状的排列,沿着箭头就可得到所有元素一个排列

$$\begin{gathered} a_{11} \to \\ \to a_{21} \to a_{12} \to \\ \to a_{31} \to a_{22} \to a_{13} \to \\ \to \cdots \to \cdots \to \cdots \to \cdots \to \end{gathered}$$

因此给出了$\mathbb{N}$到并集一个满射, 但不一定是单射, 因为元素 a_{ij} 中可能出现重复. 根据性质1.6 可知结论成立. □

注意到性质1.7 证明中使用的排列方法并不唯一.

推论 1.8 整数集合

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \cdots, \pm n, \cdots\}$$

是可数集, 因此与正整数集 $\mathbb{N}$ 有相同基数.

证明 记

$$\begin{aligned} \mathbb{Z}_+ &= \mathbb{N} = \{1, 2, 3, \cdots, n, \cdots\}, \\ \mathbb{Z}_- &= \{-1, -2, -3, \cdots, -n, \cdots\}, \end{aligned}$$

那么 $\mathbb{Z}_-$ 与 $\mathbb{N}$ 1-1 对应, 因此是可数集. 所以,

$$\mathbb{Z} = \mathbb{Z}_- \cup \{0\} \cup \mathbb{Z}_+$$

是可数集. □

定义 1.9 集合A, B的直积$A \times B$(或者笛卡尔积)定义为

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

$A_1, A_2, \cdots, A_n$的直积定义为

$$\prod_{k=1}^{n} A_k = A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \cdots, a_n) \mid a_k \in A_k,\ k = 1, 2, \cdots, n\}.$$

类似于性质1.7 证明, 可得到如下命题

性质 1.10 有限个可数集合的直积是可数集.

证明 这里只考虑两个可数集合的直积. 设

$$A = \{a_1, a_2, \cdots, a_n, \cdots\},\ B = \{b_1, b_2, \cdots,\ b_n, \cdots\},$$

那么

$$A \times B = \{(a_i, b_j) \mid a_i \in A,\ b_j \in B\}$$

记 $a_{ij} = (a_i, b_j)$, 类似性质1.7 证明, 可以给出 $\mathbb{N} \longrightarrow A \times B$ 的一个满射, 因此$A \times B$ 是可数集. □

推论 1.11 有理数集合是可数集, 也就是说有理数集与正整数集基数相等.

证明 设有理数集为

$$\mathbb{Q} = \left\{ \frac{p}{q} \;\middle|\; p, q \in \mathbb{Z},\ q \neq 0 \right\}.$$

那么

$$f_1 : \mathbb{Z} \times \mathbb{Z}_+ \longrightarrow \mathbb{Q},\ f_1(p, q) = \frac{p}{q}$$

给出 $\mathbb{Z} \times \mathbb{Z}_+ \longrightarrow \mathbb{Q}$ 的满射. 因为 $\mathbb{Z} \times \mathbb{Z}_+$ 与自然数集合 $\mathbb{N}$ 1-1 对应:

$$f_2 : \mathbb{N} \longrightarrow \mathbb{Z} \times \mathbb{Z}_+,$$

所以复合映射

$$f = f_1 \circ f_2 : \mathbb{N} \longrightarrow \mathbb{Q}$$

是满射, 根据性质1.6, 有理数集 $\mathbb{Q}$ 是可数集合. □

通常把有理数集排序为

$$\mathbb{Q} = \{r_1, r_2, \cdots, r_n, \cdots\}.$$

注记 有理数是“可列”的, 但并不是说可按照随意要求把它排列起来. 即使是考虑 $[0, 1]$ 区间上的有理数, 也无法按照大小将它们排列起来.

3° 不可数集合

以上是与正整数集合有相同基数可数集合的主要性质. 自然要问: 是否存在基数小于或大于可数集合基数的无限集合?

定义 1.12 设 A 是无限集合, $A_0 \subset A$ 是 A 的子集, 定义

$$A\backslash A_0 = \{a \mid a \in A,\ a \notin A_0\},$$

即$A\backslash A_0$ 表示从 A 中去掉 A_0 剩余元素集合 , 称为 A_0 在 A 中的**余集**.

设 A 是一个无限集合, 从 A 中取一个元素a_1, 又从 $A\backslash\{a_1\}$ 中取一个元素a_2, 显然 $a_2 \neq a_1$. 若已经取到互不相等的 $a_1, a_2, \cdots, a_n$, 则由于 A 是无限集合, $A\backslash\{a_1, a_2, \cdots, a_n\}$ 非空, 所以从中还可以取 $a_{n+1},\ a_{n+1} \neq a_i,\ i = 1, 2, \cdots, n.$ 这样的操作可以一直继续下去. 因此得到 A 的一个可数的子集 $A_0 = \{a_1, a_2, \cdots, a_n, \cdots\}$.

定义映射$f : A \longrightarrow \mathbb{N}$ 如下:

$$f(a) = \begin{cases} n, & \text{当 } a = a_n \in A_0 \\ 1, & \text{当 } a \in A\backslash A_0 \end{cases}$$

它是从 A 到 $\mathbb{N}$ 的一个满射. 根据定义1.4, 如果 f 又是单射, 那么 A 的基数与 $\mathbb{N}$ 相同, 如果 f 不是单射, 那么 A 有比 $\mathbb{N}$ 更大的基数. 所以

定理 1.13 不存在基数比可数集合基数更小的无限集合.

但是, 却存在比可数集合基数更大的无限集合.

定义 1.14 无限集合称为**不可数**, 是指不存在它与$\mathbb{N}$之间的*1-1* 对应. 根据定理*1.13*, 不可数集合有比 $\mathbb{N}$更大的基数.

为了构造一个不可数集合, 需要引入一个新的概念:

定义 1.15 对于非空集合 A , 记 2^A 是它的所有子集构成的集合

$$2^A = \{X \mid X \subset A\},$$

并称为 A 的**幂集**.

例如 (以下 ϕ 表示空集) , 当$A = \{a, b\}$ 时

$$2^A = \{\phi, \{a\}, \{b\}, \{a, b\}\}.$$

当 $A = \{x, y, z\}$ 时

$$2^A = \{\phi, \{x\}, \{y\}, \{z\}, \{x, y\}, \{x, z\}, \{y, z\}, \{x, y, z\}\}.$$

不难看出, 当 A 中元素个数 (基数) 为 2 时, 2^A 中元素个数 (基数) 为 $2^2 = 4$, 当 A 中元素个数 (基数) 为 3 时, 2^A 中元素个数 (基数) 为 $2^3 = 8$.

设 A 是包含 n 个元素的有限集合, 那么 A 中元素的各种可能组合所构成的子集就是幂集 2^A 中元素, 因此 2^A 中元素的个数为

$$C_n^0 + C_n^1 + \cdots + C_n^n = 2^n.$$

翻译成“基数”, 即是

$$2^A \text{ 的基数} = 2^A \text{ 的基数}.$$

然而, 当 A 是无限集合时, 就没有那么简单了. 下面, 重点考虑自然数集$\mathbb{N}$ 的幂集

$$2^{\mathbb{N}} = \{X \mid X \subseteq \mathbb{N}\}.$$

即 $\mathbb{N}$ 所有子集组成的集合.

定理 1.16 （Cantor 康托, 1845-1918) $2^{\mathbb{N}}$ 是不可数集合.

证明 显然, $\mathbb{N}$ 中单个数构成的最简单子集 $\{1\}, \{2\}, \cdots, \{n\}, \cdots \in 2^{\mathbb{N}}$, 因此 $2^{\mathbb{N}}$ 是无限集合.

假设 $2^{\mathbb{N}}$ 是可数集, 则可将 $2^{\mathbb{N}}$ 中元素进行编号:

$$2^{\mathbb{N}} = \{U_1, U_2, \cdots\}.$$

注意到每个 $U_1, U_2, \cdots$ 都是 $\mathbb{N}$ 的子集, 因此令

$$V = \{k \in \mathbb{N} \mid k \notin U_k\} \subset \mathbb{N}.$$

若 $V \in 2^{\mathbb{N}}$, 即存在某一个 U_n 使得 $V = U_n$, 那么当 $n \in U_n$ 时, 就意味着 $n \in V$, 这与 V 的定义矛盾; 当 $n \notin U_n$ 时, 推出 $n \notin V$, 也与 V 的定义矛盾.

所以 V 不可能是 $2^{\mathbb{N}} = \{U_1, U_2, \cdots\}$ 中某一个, 也就是 $V \notin 2^{\mathbb{N}}$.

但是 V 是$\mathbb{N}$ 的子集合, 根据 $\mathbb{N}$ 的幂集定义有 $V \in 2^{\mathbb{N}}$, 所以矛盾. 这样就证明了$2^{\mathbb{N}}$ 不可能是可数集. □

定理 1.17 实数集和无理数集（参见第 *3* 讲）是不可数集合.

习题 9 实际上证明了实数的二进制小数是不可数的. 再由习题 8, 在实数中去掉可数的有理数, 剩余的无理数也是不可数的.

注记 根据上述讨论, 实数集具有比有理数集更大的基数.这引出另一个问题, 是否存在一个集合, 它的基数比有理数的基数大, 但比实数的基数小? 著名的 *Cantor* 连续统假设认为不存在这样的集合. 这些内容已经超出本专题范围, 不再讨论.

§1.3 无限求和

众所周知, 有限个数相加, 结果还是一个数. 但是, 当考虑由无限个数相加（简称**无限求和**）, 问题变得复杂了. 首先观察以下三种无限求和问题

(i) $1+\dfrac{1}{2}+\dfrac{1}{2^2}+\cdots+\dfrac{1}{2^n}+\cdots$;

(ii) $1+2+2^2+\cdots+2^n+\cdots$;

(iii) $1-1+1-1+\cdots+(-1)^{n-1}+\cdots$.

对于(i) , 假如相加的总和是一个数, 不妨将该数记为

$$S=1+\frac{1}{2}+\frac{1}{2^2}+\cdots+\frac{1}{2^n}+\cdots,$$

按照通常算术运算, 有

$$2S=2+S,$$

因此得到 $S=2$.

同样, 对于(ii) , 假如相加的总和是一个数, 记为

$$S=1+2+2^2+\cdots+2^n+\cdots,$$

按照计算应该有

$$2S=S-1,$$

因此 $S=-1$, 即无限个正数相加总和是 -1.

而对于(iii) , 假如相加的总和是一个数:

$$S=1-1+1-1+\cdots+(-1)^{n-1}+\cdots.$$

根据加法结合律, 下列两种不同的结合方式, 给出了两个不同的结果

$$S=\begin{cases}(1-1)+(1-1)+\cdots+(1-1)+\cdots=0;\\ 1-(1-1)-(1-1)-\cdots-(1-1)-\cdots=1.\end{cases}$$

可见, 无限个数相加是否还是一个数并不显然. 因此, 我们面临这样一个问题: 如何判断无限个数相加结果仍然是一个数? 或者说如何定义无限个数相加?

仍然以上述三种情形为例, 先把前 n 项 (有限项) 加起来, 对于 (i) 有

$$1+\frac{1}{2}+\frac{1}{2^2}+\cdots+\frac{1}{2^n}=\frac{1-\dfrac{1}{2^{n+1}}}{1-\dfrac{1}{2}}=2-\frac{1}{2^n},$$

随着求和项数越来越多, 也就是随着 n 越来越大, 结果也越来越接近 2.

而对于(ii) , 它的前 n 项和为

$$1+2+2^2+\cdots+2^n=\frac{1-2^{n+1}}{1-2}=2^{n+1}-1,$$

随着相加项越来越多, 结果也随着 n 增大而越来越大, 加到最后不可能等于某个数.

对于(iii) , 它的前 n 项和满足

$$1-1+1-1+\cdots+(-1)^{n-1}=\begin{cases}0 & \text{当 } n \text{ 是偶数}\\ 1 & \text{当 } n \text{ 是基数}\end{cases}$$

每增加一项, 结果会从 0 变到 1, 或从 1 变到 0, 总是在0 和 1 之间摇摆不定.

进一步观察 (i) . 记前 n 项和为

$$S_n=1+\frac{1}{2}+\frac{1}{2^2}+\cdots+\frac{1}{2^n},$$

不难发现 S_n 与 2 的误差满足

$$|S_n-2|=\frac{1}{2^n}.$$

随着求和项越来越多, 也就是 n 越来越大, S_n 与 2 的误差越来越小. 例如要想 S_n 与 2 误差小于 $\frac{1}{10}$, 只要求和项数超过 4 就足够了:

$$|S_n-2|=\frac{1}{2^n}<\frac{1}{10}\quad \text{当 } n>4.$$

要想 S_n 与 2 误差小于 $\frac{1}{100}$, 只要求和项数超过 7 就足够了:

$$|S_n-2|=\frac{1}{2^n}<\frac{1}{100}\quad \text{当 } n>7.$$

总之, 无论要求误差如何小, 只要求和的项数超过某个正整数, 其结果与 2 的误差达到要求. 比如要使误差小于任意一个正数 ε, 只要求和项数 n 是满足 $n>\left|\frac{\ln\varepsilon}{\ln 2}\right|$ 的正整数即可:

$$|S_n-2|=\frac{1}{2^n}<\varepsilon,\quad \text{当 } n>\left|\frac{\ln\varepsilon}{\ln 2}\right|.$$

因此, 有理由相信, 无限多个数 $1,\frac{1}{2},\frac{1}{2^2},\cdots,\frac{1}{2^n},\cdots$ 相加总和应该是2.

1° 量词的规则

为了将上述分析更加准确地表述, 这里回顾关于 **全称量词** (简称 “任意”) 与 **存在量词** (简称 “存在”) 的使用规则.

一个含有全称量词的命题称为**全称命题** , 通常表述为

$$\text{对任意 } x\in U,\ A(x) \text{ 成立.}$$

这里 $A(x)$是一个含变量 x 的命题. 意思是说 “对所有U中的 x, $A(x)$ 都成立” , U 是给定的集合 (范围) , 因此 “任意” 是在一定范围内的 “任意” . 例如: “三角形的三条高交于一点” . 这里 “任意” 的范围仅限于三角形.

类似地, **存在命题**表述为:

$$\text{存在 } x \in U \text{ , } A(x) \text{ 成立 .}$$

就是说“至少有一个 U中元素 x 使得 $A(x)$ 成立”. 因此“存在”也是在一定范围内的“存在”. 例如: “当 $a^2-4b>0$ 时, 抛物线 $y=x^2+ax+b$ 上至少有一点位于 x 轴下方”. 这里“存在”的范围是抛物线上的点.

当一个命题中出现两个以上量词, 有些情况比较简单. 例如: “对任意整数 x, 对任意整数 y, $x+y=y+x$”. 显然这里两个全称量词“任意–任意”的顺序无关大局, 因此可以把命题简写为: “对任意整数 x 和 y, $x+y=y+x$”. 同样, 两个以上存在量词相邻出现, 它们的顺序也不要紧. 例如:“存在整数 x,存在整数 y ,使得 $x+y=2$, $x+2y=3$”. 可以表述为“存在整数 x 和 y, 使得 $x+y=2$, $x+2y=3$”. 因此, 相同类型量词可以交换次序或者合并.

但是对于不同类型量词来说, 这条规则不成立.

例 1.3.1 对任意的整数 a, 存在整数 b, 满足$b=a+1$.

这是一个“任意-存在”命题, 如果改变任意和存在的顺序, 则原命题就会变成“存在整数 b, 对任意的整数 a, 满足 $b=a+1$”. 显然是一个错误命题.

否定一个全称命题只需要找到一个反例,即全称命题“对任意$x\in U$, $A(x)$ 成立”的否定, 等价于存在命题“存在 $x\in U$, $A(x)$ 不成立”.

否定一个存在命题则需要说明所有情形都不成立,即存在命题“存在 $x\in U$, $A(x)$ 成立”的否定为全称命题“对任意 $x\in U$, $A(x)$ 不成立”.

对一个含有不同类型量词的命题来说,它的否命题可以通过改变量词顺序 (或者说是改变量词类型) 实现.

例 1.3.2 数集 $E=\{a_1,a_2,\cdots,a_n,\cdots\}$ 有界.

用量词可以表述为: 存在一个实数 M, 使得对任意正整数 n, 有

$$|a_n|\leqslant M.$$

它的否命题为: 数集 $E=\{a_1,a_2,\cdots,a_n,\cdots\}$ 无界, 即对任意正数 M, 存在一个正整数 n 使得 $|a_n|>M$. 因此, 数集 E 有界的“存在–任意”以及最后陈述“ $|a_n|\leqslant M$”命题的否命题变成了“任意–存在”并且用“ $|a_n|>M$”否定命题最后的陈述.

以上关于全称量词和存在量词以及它们使用规则的简单回顾, 对用来表述无限求和已经足够了.

2° 无穷级数和无穷数列收敛和发散

设有无限多个(可数个)数 $a_1, a_2, \cdots, a_n, \cdots$, 把它们形式上相加称为**无穷级数**, 或简称为**级数**, 记为

$$\sum_{n=1}^{\infty} a_n = a_1 + a_2 + \cdots + a_n + \cdots$$

级数的前 n 项(有限项)相加是一个确切的数, 称为级数的**部分和**, 记为

$$S_n = \sum_{k=1}^{n} a_n = a_1 + a_2 + \cdots + a_n.$$

定义 1.18 对于级数 $\sum\limits_{n=1}^{\infty} a_n$ 和一个数 a, 如果

对任意正数 ε, 存在一个正整数 N, 使得对任意大于 N 正整数 n (有时表述为"当 $n > N$ 时"), 下列不等式成立

$$|S_n - a| = \Big|\sum_{k=1}^{n} a_k - a\Big| < \varepsilon.$$

那么称级数总和为 a, 记

$$a = \sum_{n=1}^{\infty} a_n = a_1 + a_2 + \cdots + a_n + \cdots,$$

或者说级数**收敛**于 a. 不收敛于任何数的级数称为是**发散**的.

根据上述定义, $1 + 2 + 2^2 + \cdots + 2^n + \cdots$ 是发散的, 当然也就不能用一个数来表示总和. 因为对任何数 a, 只要取 $\varepsilon = 1$, 那么对任意正整数 N, 都存在 $n > N$, 使得

$$|S_n - a| = |2^{n+1} - 1 - a| > 1.$$

例 1.3.3 讨论级数 $\sum\limits_{n=1}^{\infty} \dfrac{1}{n(n+1)} = \dfrac{1}{1\cdot 2} + \dfrac{1}{2\cdot 3} + \cdots + \dfrac{1}{n(n+1)} + \cdots$ 敛散性.

解 因为级数前 n 项部分和为

$$\begin{aligned} S_n =& \frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{n(n+1)} \\ =& 1 - \frac{1}{2} + \frac{1}{2} - \frac{1}{3} + \cdots + \frac{1}{n} - \frac{1}{n+1} \\ =& 1 - \frac{1}{n+1} \end{aligned}$$

因此, 对任意正数 ε, 只要取 N 是满足 $N > \dfrac{1}{\varepsilon} - 1$ 的正整数(表明 N 是存在的), 那么当 $n > N$ 时, 就有

$$|S_n - 1| = \frac{1}{n+1} < \frac{1}{N+1} < \varepsilon.$$

也就是级数收敛于 1.

例 1.3.4 设 $|q| < 1$, 讨论几何级数 $\sum\limits_{n=1}^{\infty} q^n = 1 + q + q^2 + \cdots$ 的敛散性.

解 因为级数前 n 项部分和为

$$S_n = 1 + q + q^2 + \cdots + q^{n-1} = \frac{1-q^n}{1-q},$$

所以对任意正数 ε, 只要取 N 是满足 $N > \left|\dfrac{\ln \varepsilon(1-q)}{\ln |q|}\right|$ 的一个正整数, 那么当 $n > N$ 时, 就有

$$\left|S_n - \frac{1}{1-q}\right| = \frac{|q|^n}{1-q} < \frac{|q|^N}{1-q} < \varepsilon,$$

所以对于公比 $|q| < 1$ 的几何级数收敛

$$1 + q + q^2 + \cdots + q^n + \cdots = \frac{1}{1-q}, \quad |q| < 1.$$

例如, 取公比 $q = \dfrac{1}{2}$, 就有

$$1 + \frac{1}{2} + \frac{1}{2^2} + \cdots + \frac{1}{2^n} + \cdots = 2.$$

取公比 $q = \dfrac{1}{3}$, 就有

$$1 + \frac{1}{3} + \frac{1}{3^2} + \cdots + \frac{1}{3^n} + \cdots = \frac{3}{2}.$$

从级数收敛定义中不难看出, 级数前 n 项部分和 ($n = 1, 2, \cdots$) 实际上形成了一个无穷数列

$$\{S_1, S_2, S_3, \cdots, S_n, \cdots\},$$

一般地, 称数集 $\{x_1, x_2, \cdots, x_n, \cdots\}$ 为**无穷数列**, 简称为**数列**, 记为 $\{x_n\}$, 其中 x_n 称为数列的通项. 因此关于无穷级数收敛性定义, 也可以独立地用来定义数列的收敛性.

定义 1.19 设 $\{x_n\}$ 是一个数列, 如果有一个数 x, 使得下列命题成立:

对任意 $\varepsilon > 0$ 的数, 存在一个正整数 N, 使得对任意 $n > N$, 下列不等式成立

$$|x_n - x| < \varepsilon,$$

那么称数列 $\{x_n\}$ 收敛于 x, 记为

$$\lim_{n \to +\infty} x_n = x.$$

或称数列为***收敛数列***, 不收敛于任何数的数列 $\{x_n\}$ 称为 ***发散数列***.

因此, 级数 $\sum\limits_{n=1}^{\infty} a_n$ 收敛于 a 当且仅当级数部分和构成的数列 $\{S_n\}$ 收敛于 a.

例 1.3.5 常数列 $\{x_n\}$, $x_n = x$, 是收敛的.

例 1.3.6 设 $|q| < 1$, 讨论数列 $\{q^n\} = \{1, q, q^2, \cdots, q^n, \cdots\}$ 的敛散性.

解 对任意小正数 ε, 不妨设 $0<\varepsilon<1$, 只要取 N 是满足 $N>\dfrac{\ln\varepsilon}{\ln|q|}$ 的正整数, 那么当 $n>N$ 时, 就有

$$|q^n|=|q|^n<|q|^N<\varepsilon,$$

因此

$$\lim_{n\to+\infty}q^n=0.$$

这里, 限制 ε 取值范围并不失一般性, 因为当 $\varepsilon\geqslant 1$ 时, 显然 $|q|^n<1\leqslant\varepsilon$ 对任意 n 成立.

例 1.3.7 $\lim\limits_{n\to+\infty}\sqrt[n]{n}=1.$

证明 令 $\sqrt[n]{n}=1+\lambda_n,\ n=1,2,\cdots$, 则 $\lambda_n>0\ (n>1)$, 并且

$$n=(1+\lambda_n)^n=1+n\lambda_n+\frac{n(n-1)}{2}\lambda_n^2+\cdots,$$

因此

$$n>1+\frac{n(n-1)}{2}\lambda_n^2,$$

由此解得

$$\lambda_n<\sqrt{\frac{2}{n}},$$

故有

$$0<\sqrt[n]{n}-1=\lambda_n<\sqrt{\frac{2}{n}},$$

所以, 对任意 $\varepsilon>0$, 取正整数 $N>\dfrac{2}{\varepsilon^2}$, 则当 $n>N$ 时, 就有

$$0<\sqrt[n]{n}-1<\sqrt{\frac{2}{n}}<\varepsilon,\ \text{或}\ |\sqrt[n]{n}-1|<\varepsilon.$$

因此数列 $\{\sqrt[n]{n}\}$ 收敛于 1.

例 1.3.8 设 $x_n=(-1)^{n-1}\ (n=1,2,\cdots)$, 则数列 $\{x_n\}$ 发散.

证明 对任何数 x, $|x-1|\geqslant 1$ 或 $|x+1|\geqslant 1$, 因此只要取 $\varepsilon_0=\dfrac{1}{2}$, 那么对任意正整数 N, 必有奇数 $2n+1>N$ 和偶数 $2n>N$, $x_{2n+1}=1,\ x_{2n}=-1$. 因此

$$|x_{2n+1}-x|>\varepsilon_0,\ \text{或}\ |x_{2n}-x|>\varepsilon_0,$$

所以数列 $\{(-1)^{n-1}$ 发散.

3° 无穷级数的收敛性

从新回到无穷级数.

定理 1.20 如果级数 $\sum\limits_{n=1}^{\infty} a_n$ 收敛, 那么通项构成的数列$\{a_n\}$ 收敛于 0:

$$\lim_{n\to+\infty} a_n = 0.$$

证明 不妨设级数收敛于 a. 对任意正数 ε, $\dfrac{\varepsilon}{2}$ 也是正数, 因此存在正整数 N, 使得当 $n > N$ (当然也有 $n+1 > N$) 时,有

$$|S_n - a| < \frac{\varepsilon}{2},\ |S_{n+1} - a| < \frac{\varepsilon}{2},$$

由此推出

$$|a_{n+1}| = |S_{n+1} - S_n| \leqslant |S_{n+1} - a| + |S_n - a| < \varepsilon$$

对 $n > N$ 成立, 根据数列极限定义, 即 $\lim\limits_{n\to+\infty} a_n = 0$. □

根据上述定理, 不难得到级数 $\sum\limits_{n=1}^{\infty}(-1)^{n-1}$ 发散, 因为 $a_n = (-1)^{n-1}$ 发散.

读者不难发现, 利用定义说明级数收敛, 必须事先知道收敛的值. 自然要问, 是否存在一些方法, 直接判断级数是否收敛, 而无需事先知道收敛值. 这个问题在大学《数学分析》中将会有明确和丰富的答案, 这里作如下分析.

假设级数 $\sum\limits_{n=1}^{\infty} a_n$ 收敛于 a, 那么对任意正数 ε, 当然 $\dfrac{\varepsilon}{2}$ 也是正数, 因此存在正整数 N, 使得当 $n > N$ 时, 有

$$|S_n - a| < \frac{\varepsilon}{2}.$$

另取任意正整数 $p > 0$, $n + p > N$, 因此也有

$$|S_{n+p} - a| < \frac{\varepsilon}{2}.$$

这样就推得

$$|S_{n+p} - S_n| \leqslant |S_{n+p} - a| + |S_n - a| < \varepsilon,$$

上式就是

$$|a_{n+1} + a_{n+2} + \cdots + a_{n+p}| = |S_{n+p} - S_n| < \varepsilon.$$

其中 $|a_{n+1} + a_{n+2} + \cdots + a_{n+p}|$ 表示级数求和中从第 $n+1$ ($n > N$) 项开始任意有限段 (从第 $n+1$ 项, 到 $n+p$ 项) 和式的绝对值. 因此, 级数 $\sum\limits_{n=1}^{\infty} a_n$ 收敛的必要条件是对级数中充分靠后的、任意有限长度的一段和式必须小于 ε. 下面的定理说明, 上述分析反过来也是对的.

定理 1.21 (Cauchy (柯西, 1789-1857) 收敛准则) 级数 $\sum\limits_{n=1}^{\infty} a_n$ 收敛的充分必要条件是: 于任意正数 ε, 存在一个正整数 N, 使得不等式

$$|a_{n+1} + a_{n+2} + \cdots + a_{n+p}| = |S_{n+p} - S_n| < \varepsilon,$$

对任意满足 $n > N$ 的正整数 n 和任意正整数 p 成立.

上述分析实际上已经给出定理的必要性的证明, 而充分性的证明需要用到实数的完备性, 在此不做进一步讨论.

该定理的基本性体现在给出一个与定义等价命题, 重要性体现在只要看对于充分靠后 (由$n > N$ 刻画)、并且任意有限长度 (由 p 的任意性刻画) 一段和式充分小, 就能断定级数是收敛的, 而无需事先知道级数的收敛值.

例 1.3.9 用 Cauchy 收敛准则证明级数 $\sum\limits_{n=1}^{\infty}\dfrac{1}{n}$ 发散.

证明 取 $\varepsilon_0=\dfrac{1}{2}$ (表示存在正数 ε_0), 使得对任意正整数 N, 只要取 $n=p>N$ (表示存在大于 N 的 n以及 p), 就有

$$\Big|\frac{1}{n+1}+\cdots+\frac{1}{n+p}\Big|=\frac{1}{n+1}+\cdots+\frac{1}{n+n}>\frac{n}{2n}=\varepsilon_0,$$

也就是存在这样的正数 ε_0, 使得级数 $\sum\limits_{n=1}^{\infty}\dfrac{1}{n}$ 不满足 Cauchy 收敛准则, 因此发散. □

上述例子说明, 虽然 $\sum\limits_{n=1}^{\infty}\dfrac{1}{n}$ 中通项 $a_n=\dfrac{1}{n}$ 满足

$$\lim_{n\to\infty}a_n=\lim_{n\to\infty}\frac{1}{n}=0,$$

但也不能保证级数收敛, 也就是定理1.20的逆命题不成立.

例 1.3.10 判断下列级数的收敛性.

$$\sum_{n=0}^{\infty}\frac{1}{n!}=1+\frac{1}{1!}+\frac{1}{2!}+\frac{1}{3!}+\cdots+\frac{1}{n!}+\cdots.$$

解 我们无法猜测该级数具体收敛值, 因此也就无法验证它是否满足收敛定义, 但是有了Cauchy 收敛准则, 对于任意正数 ε, 取 N 是满足 $N>\dfrac{2}{\varepsilon}$ 的正整数, 对于满足 $n>N$ 的正整数 n 和任意正整数 p, 有

$$\begin{aligned}
&\Big|\frac{1}{(n+1)!}+\frac{1}{(n+2)!}+\cdots+\frac{1}{(n+p)!}\Big|\\
&\quad<\Big|\frac{1}{n(n+1)}+\frac{1}{(n+1)(n+2)}+\cdots+\frac{1}{(n+p-1)(n+p)}\Big|\\
&\quad=\Big|\frac{1}{n}-\frac{1}{n+1}+\frac{1}{n+1}-\frac{1}{n+2}+\cdots+\frac{1}{n+p-1}-\frac{1}{n+p}\Big|\\
&\quad=\Big|\frac{1}{n}-\frac{1}{n+p}\Big|<\frac{2}{n}<\frac{2}{N}<\varepsilon,
\end{aligned}$$

因此, 并不需要事先知道级数收敛值, 根据Cauchy 收敛准则就能判断出该级数一定收敛于一个数. 记这个数为 e:

$$\mathrm{e}=\sum_{n=0}^{\infty}\frac{1}{n!}=1+\frac{1}{1!}+\frac{1}{2!}+\frac{1}{3!}+\cdots+\frac{1}{n!}+\cdots.$$

并称为**自然常数**. 对于数 e, 不难发现 $\mathrm{e}>2$, 同时有

$$\mathrm{e}=1+\frac{1}{1!}+\frac{1}{2!}+\cdots+\frac{1}{n!}+\cdots<1+1+\frac{1}{2}+\cdots\frac{1}{2^{n-1}}+\cdots=3,$$

也就是说, 数 e 满足 $2<\mathrm{e}<3$. 不仅如此, 还可以证明

定理 1.22 *自然常数 e 是一个无理数.*

证明 因为 $2<\mathrm{e}<3$, 所以 e 不是整数, 假设 $\mathrm{e}=\dfrac{p}{q}$ 是有理数, 其中 p,q 是正整数, 那么 q 必然满足 $q\geqslant 2$. 这样就有

$$\begin{aligned}q!\mathrm{e}=(q-1)!p=&\left[q!+q!+\frac{q!}{2!}+\cdots\frac{q!}{(q-1)!}+1\right]\\&+\frac{1}{q+1}+\frac{1}{(q+2)(q+1)}+\frac{1}{(q+3)(q+2)(q+1)}+\cdots.\end{aligned}$$

注意到上式左边和右边方括号内都是整数, 而右边剩余的部分满足

$$\begin{aligned}0&<\frac{1}{q+1}+\frac{1}{(q+2)(q+1)}+\frac{1}{(q+3)(q+2)(q+1)}+\cdots\\&<\frac{1}{3}\left(1+\frac{1}{3}+\frac{1}{3^2}+\frac{1}{3^3}+\cdots\right)=\frac{1}{2}.\end{aligned}$$

因此矛盾. 说明 e 只能是无理数. □

大家知道, 有限个有理数相加, 其总和还是有理数. 但是上述例子却表明, 无限个有理数相加, 即使是收敛的, 其总和可能不再是有理数. 这种现象在十进制小数中也有所体现. 设

$$a=a_0.a_1a_2a_3\cdots,$$

是一个无穷小数, 也可以将它表示为一个无穷级数

$$a=a_0+\frac{a_1}{10}+\frac{a_2}{10^2}+\frac{a_3}{10^3}+\cdots$$

其中 a_0 是整数, $a_1,a_2,a_3,\cdots$ 是取值于$\{0,1,2,\cdots,9\}$ 的整数.

根据Cauchy收敛准则, 对任意 $\varepsilon>0$ (不妨设 $\varepsilon<1$), 只要取 $N>\lg\dfrac{1}{\varepsilon}$, 当 $n>N$ 时, 对任意正整数 p, 有

$$\begin{aligned}\left|\frac{a_{n+1}}{10^{n+1}}+\cdots+\frac{a_{n+p}}{10^{n+p}}\right|&\leqslant\frac{9}{10^{n+1}}\left(1+\frac{1}{10}+\cdots+\frac{1}{10^{n+p-1}}\right)\\&=\frac{9}{10^{n+1}}\left(\frac{1-\dfrac{1}{10^{n+p}}}{1-\dfrac{1}{10}}\right)<\frac{1}{10^n}<\varepsilon\end{aligned}$$

因此, 任何这样的级数一定收敛.

当小数部分有限时, 即从某项开始 $a_k=0,\ k>k_0$, a 显然是有理数. 当小数部分出现无限循环时, 仍然是一个有理数. 例如当

$$a_{3k+1}=a_1,\ a_{3k+2}=a_2,\ a_{3k+3}=a_3,\ k=1,2,\cdots$$

时, 该数表示为

$$a = a_0 + 0.\dot{a_1}\dot{a_2}\dot{a_3}$$

其中小数部分满足

$$10^3(0.\dot{a_1}\dot{a_2}\dot{a_3}) = a_1a_2a_3 + 0.\dot{a_1}\dot{a_2}\dot{a_3},$$

因此

$$a = a_0 + 0.\dot{a_1}\dot{a_2}\dot{a_3} = a_0 + \frac{a_1a_2a_3}{999}.$$

反之, 任何有理数均可表示为有限或无限循环小数 (见第 3 讲§3.5) .

当小数部分出现无限不循环时, 级数仍然收敛于一个数, 这个数不再是有理数, 称为无理数.

注记 实数理论和极限理论是数学基础性内容. 这里, 虽然用到了有关极限知识, 仅仅是用来讨论无限求和收敛性中一些简单问题. 关于极限内容, 在大学任何一门《数学分析》或《微积分》课程中还会详细介绍.

关于实数, 尤其是无理数, 可通过十进制小数构造, 也可借助*Cauchy*收敛准则思想, 通过定义一种“有理数 *Cauchy*数列”来构造, 还可以通过所谓*Dedekind* (戴德金, *1831-1916*) 分割来构造. 有关*Dedekind* 的方法将在第 *3* 讲中介绍.

§1.4 无限远点*

本节将从几何角度讨论“无限”问题

1° 射影变换下的无限远点

两直线之间的射影 设 l 和 l' 是平面上两条相交直线, 任取两直线外一点 Q, 那么连接 Q 与 l 上任意点 P 的直线 QP, 交直线 l' 于 P' 点. 设想一下从Q 发出的光, 把 l 上点 P 投射到 l' 上, 因此 P' 就是 P 在 l' 上影子, 当 P 在 l 上移动时, 影子P' 在l' 上也随之移动 (图1.4) . 这种对应称为**透视** 或者称为**射影**, Q 称为**射影中心**.

注意到在 l 上有一个点比较特殊. 设 R 是 l 上的点, 使得直线 QR 与 l' 平行. 当 P 沿着 l 从左边越来越接近 R 时, 它的影子 P' 在 l' 上向右移动越来越远. 当 P 到达 R 时, 它的影子消失在 l' 右边尽头. 当 P 越过 R 处在 R 右边时, 它的影子 (也就是直线 QP 与 l' 的交点) 却出现在 l' 的左边, 而且 P 从右边越来越接近 R 时, 影子 P' 就在 l' 的左边越来越远之处, 直至消失在左边尽头 (图1.1) .

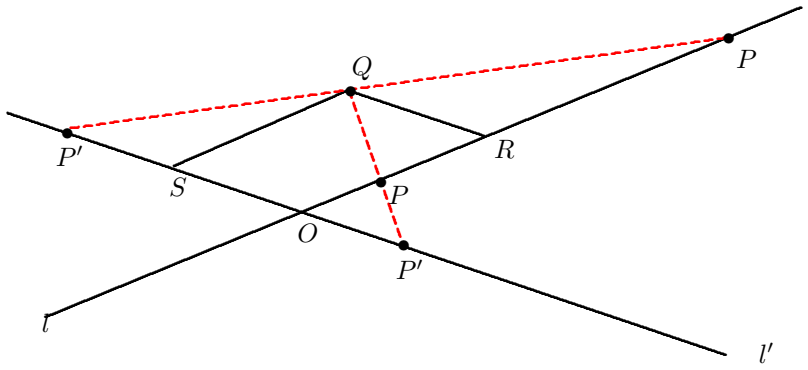


图 1.4

因此, 可以设想两条平行线 QR 与 l' 在一个假想的点: **无限远点**（或称为**理想点**）相交, 那么 R 的影子就是那个无限远点, 而且l' 上右去的无限远点和左去的无限远点应该是同一个点, 因为它们是同一个点 R 的影子, 也就是通过射影对应同一个点 R.

不但如此, 任何与 l' 平行直线, 它们的无限远点也是 R 的影子. 因此, 任何两条平行线有相同的无限远点, 或者说平行线在无限远点相交.

同样, 在 l' 上也有一个特殊点. 设 S 是 l' 上一点, 使得直线 QS 与 l 平行. 当 P 沿l 向左越走越远时, P' 就从 S 的右边越来越接近 S, 当 P 沿l 向右越走越远时, P' 就从 S 的左边越来越接近 S. 类似地, 在 l 上引进无限远点, 使它的影子对应 l' 上的点 S .

这样, 只有引进直线的无限远点之后, 从 Q 点作直线 l 和 l' 的射影对应, 才能使 l 上每一点都能与 l' 上每一点对应. 特别 l 上的点 R 对应 l' 上无限远点, 而 l 上无限远点对应 l' 上点 S.

现规定: 在每一条直线上除了普通点之外, 再加上一个“理想点”, 也就是“无限远点”. 相互平行的直线具有相同的“无限远点”, 相互不平行的直线有不同的无限远点. 再把无限远点的全体看做一条**无限远直线**, 这样构成的平面称为 **射影平面**.

性质 1.23 *在射影平面上, 任何两条直线都有唯一的交点.*

(i) *如果两条直线都不是无限远直线, 又不平行, 那么交点就是有限处一点.*

(ii) *如果两条直线都不是无限远直线, 但相互平行, 那么交点就是所共有的无限远点.*

(iii) *如果其中一条直线是无限远直线, 另一条直线是非无限远直线, 那么交点就是那条非无限远直线的无限远点.*

两平面之间的射影 在平面上引进无限远点以及无限远直线后, 再来看一看一个平

面到另一个平面透视问题.

设有两相交平面 Π 和 Π' 以及两平面外一点 Q. 对于平面 Π 上任意一点 P, 直线 QP 交Π' 于 P', 也就是说 P' 是 P 在Π' 上的影子. 当 P 在Π 上一条直线上移动时, 它的影子 P' 也在 Π' 的一条直线上移动. Π 上点和直线被投射到 Π' 上点和直线.

但是也有例外: 当直线 QP 平行于 Π' 时, P 在Π' 上没有普通点与之对应. Π 上这些特殊点构成一条平行于 Π' 的直线 l. 这条直线在 Π' 上没有普通直线与之对应. 如果规定这样的点 P 对应 QP 上无限远点, 那么直线 l 就对应 Π' 上无限远直线 (图1.5) .

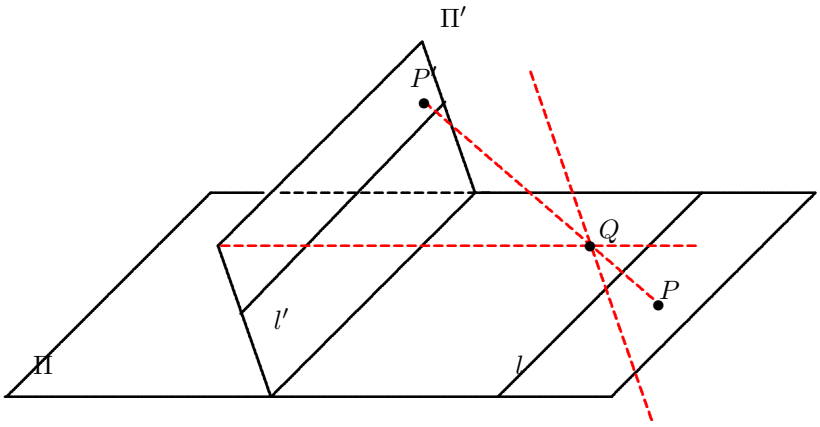


图 1.5

同样, Π' 上也有一条直线 l', 该直线平行于 Π, 且直线上任何一点 P' 是 QP' 上无限远点的影子, 因此整个直线是 Π 无限远直线的对应.

射影变换 通过引进无限远点 (或无限直线), 两个射影平面上的点在一个中心射影下确立了一个1-1 对应, 而且没有例外. 平面上的几何图形, 也会投射到另一张平面, 例如平面上的圆, 可投射成一个椭圆. 把一个几何图形经过投射变成另一个几何图形称为**射影变换**. 由此产生一门学科称为**射影几何**, 其主要内容就是要研究在有限次射影变换下, 哪些几何性质是不变的.

需要注意的是, 本节讨论射影是以一点 Q 为中心的**中心射影**, 除了中心射影, 还可建立所谓的**平行射影**, 如同从太阳上照射到地球平面上的阳光一样. 当然, 引进了无限远以后, 也可以把平行射影看成是中心在无限远点的中心射影.

以下所说 “点” 或 “直线” , 都包括无限远点或无限远直线. 特别, 用 “普通点” 或 “普通直线” 表示那些不是无限远点或无限远直线的点或直线.

性质 1.24 *在射影变换下保持不变一些简单性质如下:*

(i) 直线上任意一点都可以通过某个射影, 对应到无限远点; 平面上任意一条直线都可以通过某个射影对应到无限远直线, 因此该直线上所有点都对应到无限远点.

(ii) 如果平面上三个点, 或者更多点在一条直线上, 那么通过射影后对应点仍然在一条直线上.

(iii) 平面上三个或更多直线交于一点, 那么通过射影后对应直线仍然交于一点.

根据上述性质, 三角形在射影变换下仍然是三角形. 但是诸如直线段的长度, 两直线夹角等等, 在射影变换下一般是会改变的, 正如人的影子长度不等于身高一样. 等腰三角形或等边三角形可以射影成一个各边不等的三角形.

本节目的不是全面介绍射影几何, 也不展开讨论射影变换下不变的几何性质. 仅通过下列例子来感受引进无限远点后对证明下列定理带来的便利.

2° Desargues 定理

Desargues（笛沙格, 1591-1661）定理是射影几何中最早发现结果之一, 该定理具体描述如下:

定理 1.25 (Desargues） 设 $\triangle ABC$ 和 $\triangle A'B'C'$ 是平面上两个三角形. 如果连接它们对应顶点直线 AA', BB', CC' 交于一点, 那么对应边延长线的三个交点在一条直线上.

证明 因为引进了无限远点和无限远直线, 根据性质1.23, 对应边延长线 BC 和 $B'C'$, AB 和 $A'B'$, AC 和 $A'C'$ 分别都有交点 , 设交点分别为 P, Q, R.

为证明 P, Q, R 在一条直线上, 连接 Q, R, 并做一射影变换, 使 Q, R 所在直线投影到无限远直线（也就是将 Q, R 投影到无限远点）. 投影后三角形还是三角形, 只是投影后两个三角形的两组对应边 AB 和 $A'B'$, 以及 BC 和 $B'C'$ 分别交于无限远点, 因此有

$$AB \parallel A'B'; \quad AC \parallel A'C'.$$

这样, 只要证明投影后第三组对应边 BC 和 $B'C'$ 延长线交点也在无限远点, 或者说只要 $BC \parallel B'C'$, 那么投影后三个交点都在无限远直线上. 根据性质1.24, 就可知道原来的三个交点一定也在一条直线上.

根据上述分析, 现在只需证明当三角形 $\triangle ABC$ 和 $\triangle A'B'C'$ 两条对应边 $AB \parallel A'B'$, $AC \parallel A'C'$ 时, 由定理中连接对应顶点直线交于一点的条件, 推出 $BC \parallel B'C'$ 即可.

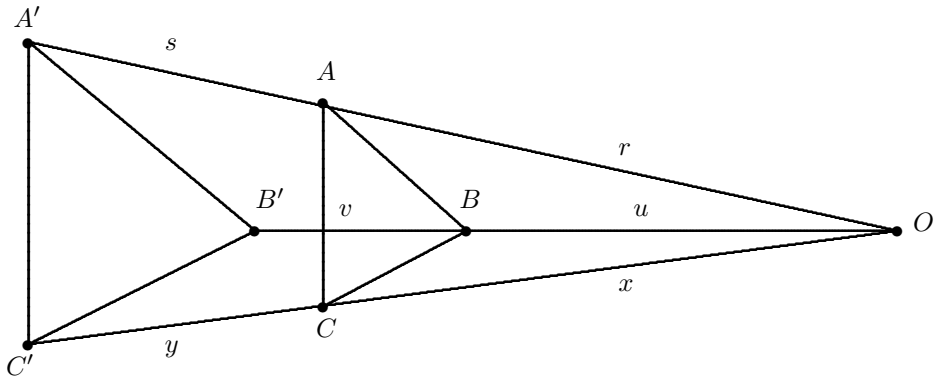


图 1.6

设对应顶点连线交于 O, 如 (图1.6) 所示

$$AB \parallel A'B' \text{ 推出 } \frac{u}{v}=\frac{r}{s},$$
$$AC \parallel A'C' \text{ 推出 } \frac{x}{y}=\frac{r}{s},$$

因此

$$\frac{u}{v}=\frac{x}{y},$$

即 $BC \parallel B'C'$. 这样就完成了定理证明. □

3° 齐次坐标

大家知道, 引进坐标系后, 平面上点 P 就与一个数组1-1 对应, 在直角坐标系下, 这个数组记为 (x,y), 称为 P 坐标. 有了坐标系, 平面上一条直线 l 上点的坐标 (x,y) 满足一个线性方程

$$l:\ ax+by+c=0,$$

这里, a,b,c 是常数, 它确定了直线的位置和方向. 例如

当 $c=0$, 表示直线过原点 $O(0,0)$;

当 $a=0,b=1,c=0$, 对应直线方程是 $y=0$, 即是平面上的 x 轴;

当 $a=1,b=-1,c=0$, 确定的直线为 $x=y$, 它表示过O 点并平分x 轴和 y 轴正向之间夹角.

同样, 一个坐标满足的二次方程就确定了一个二次曲线, 例如圆、椭圆、抛物线和双曲线等等. .

反之, 一组数组 (x,y)又可“几何化”, 并称为一个“点”, (x,y) 所满足的方程称为一条“曲线”, 特别当该方程是线性方程时, 就称为“直线”.

平面如此, 空间也是如此, 两个数的数组如此, 三个数, 乃至多个数的数组也是如此 (详情见第 5 讲) .

问题是, 在添加了无限远点的直线和添加了无限直线的平面上, 无限远点的坐标是什么? 无限远直线的方程是什么? 如果仍然把解析几何方法应用到射影几何中去, 就需要建立一个既能包括普通点又能包括无限远点的坐标系. 以下以平面为例 (图1.7) .

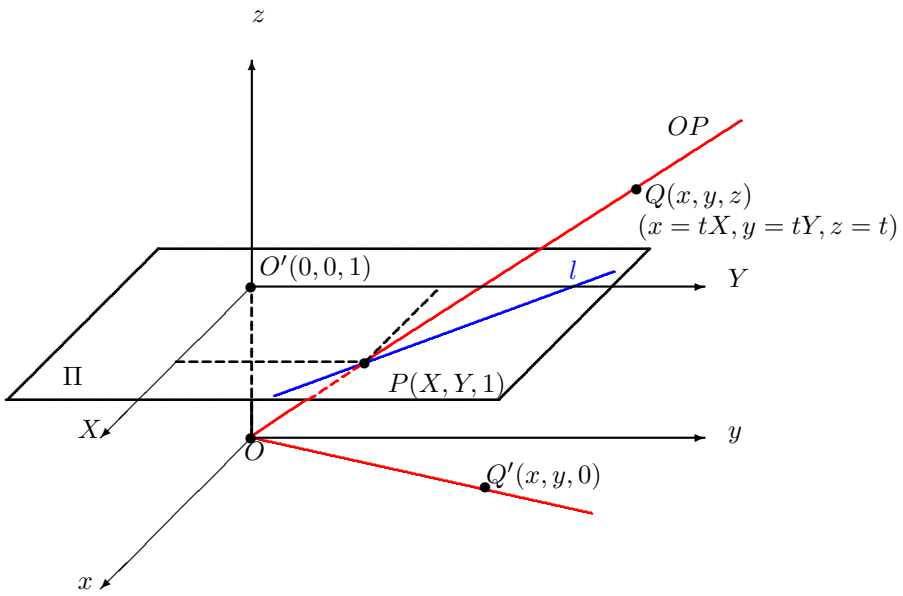


图 1.7

设平面 Π 上的直角坐标系为 $O'XY$, 把 Π 放到一个具有三维直角坐标系的空间 $Oxyz$ 中, 使得 Π 的原点位于 $Oxyz$ 中的 $(0,0,1)$ 点, 并且使得 Π 平行于 $Oxyz$ 中的 Oxy 平面. 这样 Π 上任何一点 $P(X,Y)$ 在 $Oxyz$ 空间就有了一个三维的坐标 $P(X,Y,1)$.

取 O 为射影中心点, 那么 Π 上每一点 P 与过该点和 O 的直线 OP 1-1 对应. 该直线上任意一个异于 O 的点 Q 都是P 点的影子, 而 Π 上无限远点则与过 O 点并与 Π 平行的直线1-1 对应.

首先考虑 P 是Π 上的普通点, 那么 OP上任何异于 O 的点 Q 的坐标 $Q(x,y,z)$ 称为 P 的**齐次坐标**, 特别, P 本身的坐标 $(X,Y,1)$ 也是 P 的一个齐次坐标. 其它齐次坐标 (即直线 OP 上其它点的坐标) (x,y,z) 满足

$$x = tX,\ y = tY,\ z = t,\quad t \neq 0.$$

因此 P 的齐次坐标表示为 (tX,tY,t).

对平面 Π 上一个普通点 P 引进的齐次坐标, 需要用三个数的数组而不是我们熟悉的两个数的数组, 并且不是唯一的, 它带有一个任意非零因子 t.

但是对 Π 上的无限远点而言, 它对应的是过 O 与 Π 平行的直线 (也就是空间

中Oxy 平面上的直线), 这条直线上任意异于 O 的一点的坐标为 $Q'(x,y,0)$, 所以定义 $(x,y,0)$ 为 Π 上无限远点的齐次坐标.

这样就把包含Π 和 Π 的无限远点在内的射影平面上任何一点的齐次坐标用三个数的数组 (x,y,z) 表示, 其中当 $z\neq 0$ 时, 表示普通点 $(X,Y,1)=\left(\frac{x}{z},\frac{y}{z},1\right)$ 的齐次坐标, $z=0$ 时表示无限远点的齐次坐标.

现在考虑平面Π 上直线 l 的方程

$$l:\ aX+bY+c=0.$$

其中 a,b,c 为不全为零的常数. 因此 l 上点的齐次坐标满足的方程(简称**直线的齐次坐标方程**)为

$$l:\ ax+by+cz=0,$$

特别, Π 上无限远直线 l_∞ 的齐次坐标方程如下

$$l_\infty:\ z=0.$$

不难看出, 写出直线的齐次坐标方程时, 无限远直线的方程不过是一个特例而已.

从三维空间 $Oxyz$ 上看, 平面 Π 上直线 l 的齐次坐标方程 $ax+by+cz=0$ 就是 $Oxyz$ 空间中过直线 l 和直线外一点 O (原点)的平面方程, 这个平面是从 O 点发出的光将 l 投射到空间的影子, 影子平面上任意点的坐标, 都是直线 l 上某一点的齐次坐标. 而无限远直线的影子平面正是空间中的 Oxy 平面, 它的方程是 $z=0$, 任何点的坐标正是无限远直线上点的齐次坐标(关于空间平面方程, 参见第 5 讲).

称三元数组 (a,b,c) 为**直线(包括无限远直线) l 的齐次坐标**. 对任意的 $t\neq 0$, (ta,tb,tc) 也是同一直线的齐次坐标.

不难发现, 刻画平面上直线(含无限远直线)方程中, 点和直线是完全对称的, 即在

$$ax+by+cz=0$$

中, 三个齐次坐标 (x,y,z) 表示点, 而三个齐次坐标 (a,b,c) 表示直线.

4° 反演变换下的无限远点

反演变换 给定平面上一点 O, 称为**反演中心**, 以及常数 k, 称为**反演幂**(这里始终设 $k>0$). 对于平面上任何异于 O 的点 P, 作射线 OP, 在射线上取一点 P' 使得 OP 的长度和 OP' 的长度满足 (图1.8)

$$|OP|\cdot|OP'|=k^2,$$

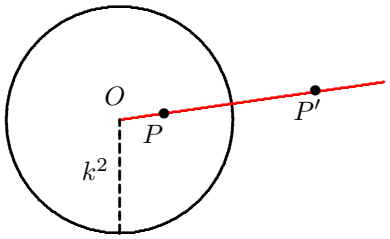


图 1.8

这样就定义了平面上除 O 点之外任意一点 P 到 P' 的一个变换, 称为以 O 为反演中心、以 k 为反演幂的**反演变换**. 或简称为**反演**. P' 称为 P 的**反演点**.

性质 1.26 对给定的反演中心和反演幂, 有

(i) 如果 P' 是 P 的反演点, 那么 P 是 P' 的反演点.

(ii) 设 C 是以反演中心 O 为圆心, k 为半径的圆, 并称为***反演基圆***. 那么当 P 是圆内一点时, P' 是圆外一点, 反之如果 P 在圆外, 那么 P' 就在圆内. 当 P 在圆上时, $P'=P$.

(iii) 当 P 沿着固定射线越来越接近 O 时, 反演点沿着同一射线向相反方向越走越远. 只要 P 和 O 充分接近, P' 与 O 距离就任意远.

无限远点和扩充平面 按照定义, 在平面上只有一点例外, 即反演中心 O 没有对应的反演点, 也没有任何一点以 O 作为反演点.

为此, 类似于在射影变换时做法, 引进一个 “理想点” , 称为**无限远点**, 记为 ∞, 使它与 O 互为反演点. 但是, 与射影变换情形区别在于, 因为 O 只有一个点, 因此在不同的射线上得到的无限远点只能认为是一个点. 这样, 我们在考虑反演变换时, 在平面上添加无限远点 ∞, 而且只能添加一个无限远点, 使得平面上任何一点 (包括 O 和 ∞) 都有反演点与之对应.

如果把平面看成是复平面 $\mathbb{C}$, 并设反演中心为为 z_0, 那么反演变换就转化为复数 $z\to z'$ 的变换

$$z\longmapsto z'=z_0+\frac{k^2}{\overline{z}-\overline{z}_0}=z_0+\frac{k^2}{|z-z_0|^2}(z-z_0),$$

特别, 当 $z_0=0$, 有

$$z\longmapsto z'=\frac{k^2}{\overline{z}}=\frac{k^2}{|z|^2}z,$$

这里$\overline{z}=x-\mathrm{i}y$ 为 $z=x+\mathrm{i}y$ 的复共轭. 添加无限远点后, 记

$$\mathbb{C}_\infty=\mathbb{C}\cup\{\infty\},$$

并称为**扩充复平面**.

对于反演变换的如下结论.

定理 1.27 设 O 是反演中心, $k>0$ 是反演幂. C 是以O 为圆心, 以 k 为半径的基圆, 则在反演变换下

(i) 过 O 的直线变成过 O 的直线;

(ii) 过 O 的圆变成一条不过 O 的直线;

(iii) 不过 O 的直线变成过 O 点的圆;

(iv) 不过 O 的圆变成不过 O 点的圆.

当引进无限远点以后, 任何直线可以看成是广义的圆. 因此上述结论概括起来就是: ***反演变换把圆变成圆***.

证明 (i) 是显然的, 因为过 O 的任何直线上点的反演点仍然在这条直线上.

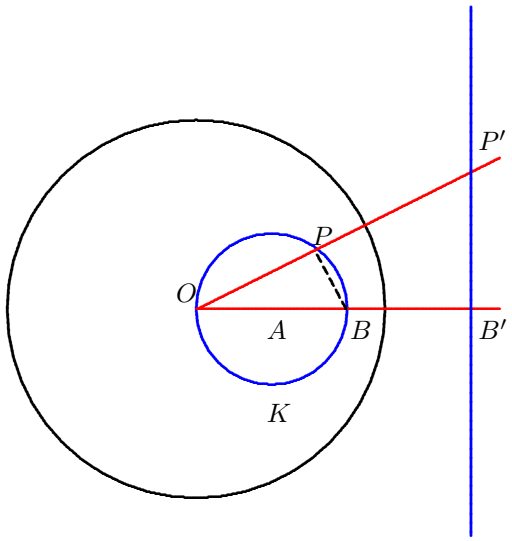


图 1.9

关于 (ii) 可采取初等办法, 如图1.9, 设 K 是过 O 的任意一个圆, 圆心在 A 点, OAB 为圆 K 的一条直径. P 为 K 上任意一个动点. 并记 $\angle POA=\theta$ $(-\frac{\pi}{2}<\theta<\frac{\pi}{2})$.

设 B 的反演点为 B', 那么 $|OB|\cdot|OB'|=k^2$,

设 P' 是 P 的反演点, 那么 $|OP|\cdot|OP'|=k^2$.

在直角三角形 $\triangle OPB$ 中,

$$|OP|=|OB|\cos\theta.$$

因此

$$|OB'|=\frac{k^2}{|OB|}=|OP'|\cos\theta,$$

这样就推出 $\angle OB'P'$ 为直角. 也就是圆 K 上任何一点 P 关于圆 C 的反演点都在垂直 OB', 垂足在 B' 的直线上, 于是 (ii) 得证.

(iii) 是性质1.26和 (ii) 的直接推论.

为了证明 (iv) , 把反演变换转化成复数变换. 取复平面原点为反演中心 O, $k>0$ 为反演幂, 因此反演变换为

$$z \longmapsto z' = \frac{k^2}{\overline{z}}.$$

设 K 是一个不过 O、以 z_1 为圆心、以 a 为半径的圆, 因此圆方程为

$$|z-z_1|^2 = (z-z_1)(\overline{z}-\overline{z}_1) = a^2.$$

因为 K 不过 O 点 (即 $z=0$ 不满足圆的方程), 所以

$$|z_1|^2 \neq a^2,$$

把 $z = \dfrac{k^2}{\overline{z'}}$ 代入得

$$\left(\frac{k^2}{\overline{z'}} - z_1\right)\left(\frac{k^2}{z'} - \overline{z}_1\right) = a^2,$$

整理得

$$k^4 + |z_1|^2|z'|^2 - k^2(z_1\overline{z'} + \overline{z}_1 z') = a^2|z'|^2,$$

或

$$|z'|^2 - \frac{k^2}{|z_1|^2-a^2}(z_1\overline{z'} + \overline{z_1}z') + \frac{k^4}{|z_1|^2-a^2} = 0$$

令

$$z_2 = \frac{k^2 z_1}{|z_1|^2-a^2},\ b = \frac{k^2 a}{||z_1|^2-a^2|},$$

那么 z' 满足

$$K':\ (z'-z_2)(\overline{z'}-\overline{z}_2) = b^2$$

这是以 z_2 为圆心、以b 为半径, 且不过 O （ $|z_2|^2 \neq b^2$ ）的圆, 所以 (iv) 成立. □

5° 球极投影

为了进一步理解扩充复平面, 引进如下**球极投影** (图1.10): 在三维坐标空间 $Ouvw$ 中, 作一个以 $(0,0,r)$ 为圆心, r 为半径的球

$$u^2 + v^2 + (w-r)^2 = r^2,$$

球上的点 $N(0,0,2r)$ 称为“北极点”, $S(0,0,0)$ 称为“南极点”. 把平面 Ouv 看成是复平面, 因此复平面的原点与球的南极点重合.

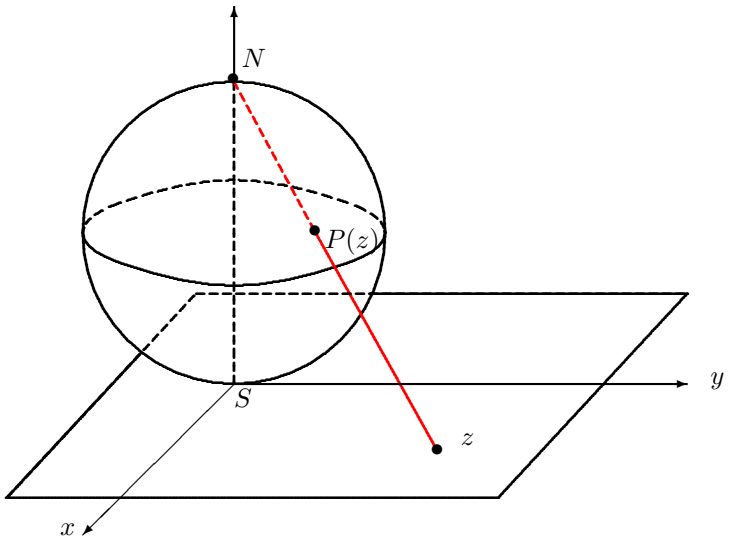


图 1.10

用直线段将球面的北极点 N 与复平面上任意点z 相连, 此线段交球面于$P(z)$ 点, 就建立复平面上点与球面上点 1-1 对应, $z \longmapsto P(z)$ 只有北极点例外 . 称这种对应为**球极投影**.当我们在复平面上引进无限远点 ∞ 后, 规定 ∞ 对应球面上的北极点, 因此, 添加了无限远点的扩张复平面 $\mathbb{C}_\infty = \mathbb{C} \cup \{\infty\}$ 通过球极投影就与球面是1-1 对应的. 称这样的球面为 **复球面**.

为了进一步讨论球极投影解析表达式, 不妨设球的半径为 $\dfrac{1}{2}$, 因此球心空间坐标为 $\left(0, 0, \dfrac{1}{2}\right)$, 北极点坐标为 $(0, 0, 1)$.

设球面上与 $z = x + \mathrm{i}y$ 对应点 $P(z)$ 的空间坐标为 (u, v, w), 因此

$$u^2 + v^2 + \left(w - \frac{1}{2}\right)^2 = \frac{1}{4}, \quad \text{或} \quad u^2 + v^2 = w(1 - w).$$

因为 z 的空间坐标为 $(x, y, 0)$, 根据球极投影, $(0, 0, 1)$, (u, v, w) 和 $(x, y, 0)$ 在一条直线上,

$$\frac{u - 0}{x - 0} = \frac{v - 0}{y - 0} = \frac{w - 1}{0 - 1},$$

由此得

$$x = \frac{u}{1 - w}, \ y = \frac{v}{1 - w}, \quad \text{即} \quad z = \frac{u + \mathrm{i}v}{1 - w}.$$

从上式以及$u^2 + v^2 = w(1 - w)$ 不难得到

$$x^2 + y^2 = |z|^2 = \frac{u^2 + v^2}{(1 - w)^2} = \frac{w}{1 - w},$$

解出 w 并得到

$$u=\frac{x}{x^2+y^2+1}=\frac{z+\overline{z}}{2(|z|^2+1)},$$
$$v=\frac{y}{x^2+y^2+1}=\frac{z-\overline{z}}{2\mathrm{i}(|z|^2+1)},$$
$$w=\frac{x^2+y^2}{x^2+y^2+1}=\frac{|z|^2}{|z|^2+1}.$$

这样就得到了 $z=x+\mathrm{i}y$ 和对应点 $P(z)=(u,v,w)$ 之间的变换关系.

有了球极投影中复数 z 与球面上点 $P(z)$ 对应关系, 不难看出

性质 1.28 设球心坐标为 $\left(0,0,\frac{1}{2}\right)$, 半径为 $\frac{1}{2}$. 那么在球极投影下

(i) 球面上纬线投影到复平面上以 O 为圆心的圆, 特别, 球面上赤道投影到复平面上以 O 为圆心的单位圆.

(ii) 球面上经线投影到复平面上过 O 的直线.

所谓球面上纬线即是球面上满足

$$w=c\ (0\leqslant c<1\text{ 是常数}),\quad u^2+v^2=c(1-c)$$

的点构成的圆, 纬线上点对应的 z 满足

$$|z|^2=\frac{c}{1-c},$$

它表示复平面上以 O 为圆心、以$\sqrt{\frac{c}{1-c}}$ 为半径的圆. 球面上赤道对应 $c=\frac{1}{2}$, 因此它在复平面上投影是单位圆 $|z|^2=1$. 而球面上经线是由满足

$$\frac{v}{u}=c\ (\text{常数})$$

的点 (u,v,w) 构成, 对应复平面上是过O 所有满足幅角为常数 $\frac{y}{x}=\tan\theta=c$ 的复数, 因此是过 O 直线.

如果考虑复平面上以 O 为反演中心, 1 为反演幂反演变换, 那么 z 和反演点 z' 在同一条射线上, 并分别在单位圆的两侧. 对应到球面上, $P(z)$ 和 $P(z')$ 都在同一条经线上, 并且分别在南北两个半球. 而 O 和其反演点 ∞ 对应球面上的南极点和北极点. 这样扩充复平面 $\mathbb{C}_\infty$ 上的反演变换, 对应到复球面上, 即是南北半球上处在同一经线上的点之间的变换, 其中 $\mathbb{C}_\infty$ 上原点 O 和无限远点 ∞ 之间的反演变换, 在球面上无非是南极点和北极点之间的变换而已.

第 1 讲习题

1. 证明: 对任意正整数 n, 有

$$1^3+2^3+3^3+\cdots+n^3=\left[\frac{n(n+1)}{2}\right]^2.$$

2. 证明: 对任意正整数 n, 有

$$1+\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{3}}+\cdots+\frac{1}{\sqrt{n}}<2\sqrt{n}.$$

3. 证明: 对任意非负整数 n, $3^{2n}+7$ 能被 8 整除.

4. 证明: 对任意正整数 n 和 $p>-1$, 有

$$(1+p)^n\geqslant 1+np.$$

5. （平均不等式） 设 $a_1,a_2,\cdots,a_n$ 是 n 个正实数, 则有

$$\frac{n}{\frac{1}{a_1}+\frac{1}{a_2}+\cdots+\frac{1}{a_n}}\leqslant\sqrt[n]{a_1a_2\cdots a_n}\leqslant\frac{a_1+a_2+\cdots+a_n}{n}.$$

6. 试用归纳法证明

$$\sum_{r=1}^{n}\frac{1}{2^r}\tan\left(\frac{\theta}{2^r}\right)=\frac{1}{2^n}\cot\left(\frac{\theta}{2^n}\right)-\cot\theta.$$

提示: 利用正切和余切的半角公式

$$\tan\phi=\cot^{-1}\phi=\frac{2\tan\frac{\phi}{2}}{1-\tan^2\frac{\phi}{2}}.$$

7. 设 $f_1:E_1\longrightarrow E_2,\ f_1:E_2\longrightarrow E_3$ 分别是满射, 证明 $f_2\circ f_1:E_1\longrightarrow E_3$ 也是满射.

8. 不可数集合中去掉一个可数集合的余集 (定义1.12) 仍然是不可数的.

9. 设 $A_i=\{0,1\}\ i=1,2,\cdots$ (每个 A_i 只含两个元素0 和 1). 证明: 可数个 $A_1,A_2,\cdots$ 的直积

$$E=A_1\times A_2\times\cdots=\{x=(a_1,a_2,\cdots)\mid a_i=0\text{ 或 }1\}$$

是不可数集合.

提示: 采取反证法, 假设 E 可数, 则 E 中元素可排列如下:

$$E=\{x_1,x_2,\cdots\}$$

令

$$x=(a_1,a_2,\cdots),\ a_i=\begin{cases}1, & x_i\text{ 中第}i\text{ 个分量}=0\\ 0, & x_i\text{ 中第}i\text{ 个分量}=1,\end{cases}\quad i=1,2,\cdots,$$

若 $x = x_n$, 推出矛盾, 所以 E 不可数.

E 中的元素x 实际上对应一个二进制小数 (参见§3.5 的注记) :

$$x = (a_1, a_2, \cdots) \longrightarrow 0.a_1a_2\cdots = \frac{a_1}{2} + \frac{a_2}{2^2} + \cdots,\ a_i = 0 \text{ 或 } 1.$$

因此本题利用二进制, 实际上证明了实数集合是不可数集合.

10. 设 a 是一个数, 试用量词表述数列 $\{x_n\}$ 收敛于 a 的否命题.

11. 用定义证明:
$$\sum_{n=1}^{\infty} \frac{1}{(2n-1)(2n+1)} = \frac{1}{2}.$$

12. 设有两个级数 $\sum\limits_{n=1}^{\infty} a_n$ 和 $\sum\limits_{n=1}^{\infty} b_n$, 试证明: 如果 $|a_n| \leqslant b_n,\ n = 1, 2, \cdots$, 那么级数 $\sum\limits_{n=1}^{\infty} b_n$ 收敛就推出级数 $\sum\limits_{n=1}^{\infty} a_n$ 收敛.
提示: 利用 *Cauchy* 收敛准则.

13. 证明: 收敛数列一定是有界数列.

14. 证明: 若数列 $\{x_n\}$ 收敛于 x, $\{y_n\}$ 收敛于 y, 则数列 $\{x_n + y_n\}$ 收敛于 $x + y$. 因此得出两个收敛级数也可以相加, 且
$$\sum_{n=1}^{\infty} a_n + \sum_{n=1}^{\infty} b_n = \sum_{n=1}^{\infty} (a_n + b_n).$$

15. 证明: 若数列 $\{x_n\}$ 收敛于 x, $\{y_n\}$ 收敛于 y, 则数列 $\{x_n y_n\}$ 收敛于 xy.
提示: 利用收敛数列必有界的结果.

16. 证明: 若数列 $\{x_n\}$ 和 $\{x'_n\}$ 同收敛于 x, 且
$$x_n < y_n < x'_n,\ n = 1, 2, \cdots,$$
则数列 $\{y_n\}$ 也收敛于 x.

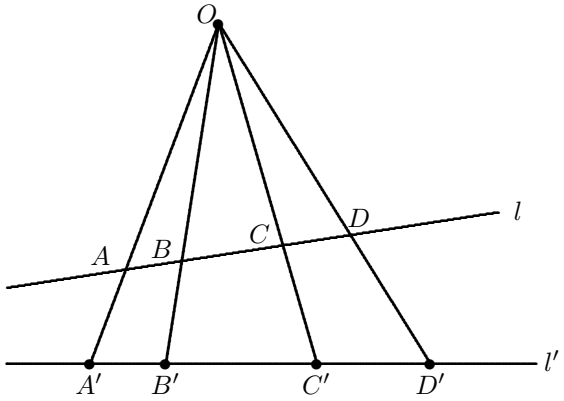
17. 设 $a > 0$, 求证 $\lim\limits_{n\to+\infty} \sqrt[n]{a} = 1$.
提示: 对 $a > 1$, $a = 1$, $0 < a < 1$ 分别考虑. 其中对 $a > 1$ 情形, 可采取类似例 *1.3.7* 的方法.

18. 在平面直角坐标系中, 设 $Q(0, 1)$ 为射影中心点, 求直线 $y = x - 1$ 上任何一点 P 在 x 轴上的投影 P' 的坐标.
提示: 将直线 $y = x - 1$ 上的 P 的坐标用参数表示: $(\lambda, \lambda - 1)$, 写出过 $Q(0, 1)$ 和 $P(\lambda, \lambda - 1)$ 点的直线方程, 并求其与直线 $y = 0$ (x 轴) 的交点.

19. 设 A,B,C,D 是直线 l 上四个有序点, 定义它们的**交比** 为

$$(ABCD)=\frac{CA}{CB}\Big/\frac{DA}{DB}.$$

证明: 在中心射影下, 交比不变. 即 (如图) 直线 l 上四个有序点 A,B,C,D 的交比等于直线 l' 上与之投影对应的四个有序点 A',B',C',D' 的交比相等.



注记 在四个有序点 A,B,C,D 的交比中, 如果点 D 趋向无限远点 (记为 ∞), 那么 $\dfrac{DA}{DB}$ 趋于1, 因此定义包含无限远点 ∞ 的交比为

$$(ABC\infty)=\frac{CA}{CB}.$$

第 2 讲　整数

数是数学的基础, 为了更好地理解数系, 首先考虑自然数. 自然数在数系中, 乃至在整个数学中扮演的基础性角色, 使得 Kronecker（克罗内克 1823-1891）发出这样感慨:“上帝创造了自然数, 其余的都是人的工作”.

§2.1　正整数与整数

记自然数集合如下,

$$\mathbb{N} = \{0, 1,\ 2,\ 3,\ \cdots\},$$

在这个集合中有最基本的算术, 算术的基础在于正整数加法和乘法服从某些规则. 现将加法和乘法运算等规则罗列如下.

加法运算: 对任意 $a, b \in \mathbb{N}$, 有唯一确定正整数, 称为 a 与 b 的和, 记为 $a + b$. 加法运算满足下列规则

(*1*) 交换律　$a + b = b + a$.

(*2*) 结合律　$(a + b) + c = a + (b + c)$.

(*3*) *0* 元　$a + 0 = 0 + a = a$.

乘法运算: 对任意 $a, b \in \mathbb{N}$, 有唯一确定正整数, 称为 a 与 b 的积, 记为 $a \cdot b$ 或 ab. 乘法运算满足下列规则

(*4*) 交换律　$ab = ba$.

(*5*) 结合律　$(ab)c = a(bc)$.

(*6*) 分配律　$a(b + c) = ab + ac$.

(*7*) 单位元　$1 \cdot a = a \cdot 1 = a$.

(*8*) *0*元　$0 \cdot a = a \cdot 0 = 0$.

顺序关系: 对任意 $a, b \in \mathbb{N}$, 如果存在 $c \in \mathbb{N}$ 使得 $a = b + c$, 则记为 $a > b$ 或 $b < a$. 可以证明, 下列三个关系

(*9*) $a < b,\ a = b,\ a > b$ 有且仅有一个成立.

顺序关系满足

(*10*) 由 $a<b$, $b<c$ 推出 $a<c$.

(*11*) 由 $a<b$ 推出 $a+c<b+c$ 对任何 $c\in\mathbb{N}$ 成立.

(*12*) 由$a<b$ 推出 $ac<bc$ 对任何 $c\in\mathbb{N}$ $c\neq 0$ 成立.

自然数最重要, 最本质的性质是**归纳公理**, 在第 1 讲已经做了介绍, 并由归纳公理出发, 讨论了最小数原理和数学归纳法. 需要补充的是, 除了最小数原理外, 还可以得到所谓**最大数原理**. 为了保持完整性, 现将它们罗列如下:

归纳公理: 设 $S\subseteq\mathbb{N}$, 如果 S 满足 *(a)* $0\in S$, *(b)* 若 $n\in S$ 推得 $n+1\in S$, 那么 $S=\mathbb{N}$.

定理 2.1 (最小数原理) 设 S 是 $\mathbb{N}$ 非空子集. 则 S 中必有最小数.

定义 2.2 设 S 是 $\mathbb{N}$ 的非空子集. 称 S 有上界, 是指存在 $m\in\mathbb{N}$, 使得对任意的 $s\in S$, 有$s\leqslant m$.

定理 2.3 (最大数原理) 设 S 是 $\mathbb{N}$ 非空子集, 并有上界, 则 S 中必有最大数.

通过引进负数: $-a$, $a\in\mathbb{N}$, 现将自然数扩展为整数

$$\mathbb{Z}=\{0,\pm1,\pm2,\pm3,\cdots\}.$$

它包含 0, 正整数 $\mathbb{Z}_+=\{1,2,3,\cdots\}$ 和负整数 $\mathbb{Z}_-=\{-1,-2,-3,\cdots\}$. 整数 $\mathbb{Z}$ 中可定义加法, 它适用加法运算 (1)、(2) 和 (3), 并且对每个 $a\in\mathbb{Z}$ 有唯一的 $x\in\mathbb{Z}$, 使得

$$a+x=0.$$

将 x记作 $-a$, 于是对任意 $a,b\in\mathbb{Z}$, 方程

$$a+x=b$$

在 $\mathbb{Z}$ 中有唯一解 $x=b-a$. 这样 $\mathbb{Z}$ 中可以作加法逆运算, 称为减法. 在代数学中, 将可作加、减法运算并适合上述运算规则的集合称为**加法群**, 因此 $\mathbb{Z}$ 是一个加法群.

整数 $\mathbb{Z}$ 中乘法适合运算规律 (4), (5), (6), (7), (8). 对既能作加法、减运算, 又能作乘法运算的集合, 称为**(交换)环**. 注意, 对乘法, 有

$$ab=0 \quad \text{当且仅当} \quad a=0 \ \text{或}\ b=0.$$

具有这种性质的环称为**无零因子环**. 因此, $\mathbb{Z}$ 是无零因子环, 从而乘法消去率成立, 即对任何 $b\neq 0$,

$$ab=cb \text{ 推出 } a=c.$$

整数 $\mathbb{Z}$ 中也有顺序概念, 它适合规律 (9), (10), (11), (12) 只是在规律 (12) 应增加条件 $c>0$, 即修改成

(12') 由 $a<b$ 推得 $ac<bc$, 其中 $c>0$.

其他类似 $\mathbb{N}$ 的性质还有

例 2.1.1 对整数集 $\mathbb{Z}$ 中非空子集 E, 若 E 有下 (或上) 界, 即若存在 $m\in\mathbb{Z}$, 使得对任意的 $n\in E$, 有 $n\geqslant m$ (或 $n\leqslant m$), 则 E 中必有最小 (或大) 整数.

证明 设 E 的下界为 $l\in\mathbb{Z}$, 则对任意 $n\in E$, $n-l\geqslant 0$, 并且 $E'=\{n-l\mid n\in E\}\subset\mathbb{N}$ 是非空子集, 因此 E' 有最小数 $m\geqslant 0$, 这样 $n=m+l$ 就是 E 的最小整数. □

整数 $\mathbb{Z}$ 中还可以定义**绝对值**:

$$|a|=\begin{cases}a, & a\in\mathbb{Z}_+\\ 0, & a=0\\ -a, & -a\in\mathbb{Z}_-\end{cases}$$

因此 $|a|$ 是非负整数. 绝对值由如下性质:

(13) $|ab|=|a||b|$.

(14) (三角不等式) $|a+b|\leqslant|a|+|b|$.

以上就是自然数集合 $\mathbb{N}$ 与整数集合 $\mathbb{Z}$ 的一些基本常识.

§2.2 数的整除性

整数集合 $\mathbb{Z}$ 除了加法和乘法外, 还可以做减法, 即加法逆运算. 但是一般不能作除法, 也就是说对两个整数 a,b, $b\neq 0$, $\dfrac{a}{b}$ 不一定是整数, 或者说不一定存在整数 c, 使得 $a=bc$, 由此引出整数第一个基本概念: **数的整除性**.

定义 2.4 *设 a,b 是两个整数, $b\neq 0$. 如果存在一个整数 c 使得 $a=bc$, 则称 b **整除** a, 用 $b\mid a$ 表示, 并称 b 是 a 的一个**约数** (或**因子**), 而 a 为 b 的**倍数**. 如果不存在上述整数 c, 则称 b **不整除** a, 用 $b\nmid a$ 表示.*

上述定义直接导出下列基本性质.

定理 2.5 *设 a,b,c 是整数.*

(i) *若 $b\mid a$, 且 $c\neq 0$, 则 $bc\mid ac$, 反之亦然, 特别地 $b\mid a$ 等价于 $(\pm b)\mid(\pm a)$.*

(ii) *若 $b\mid c$, 且 $c\mid a$, 则 $b\mid a$.*

(iii) *若 $b\mid a$, 且$b\mid c$, 则 $b\mid(xa+yc)$, 其中 $x,y\in\mathbb{Z}$.*

(iv) *若 $b\mid a$, 且 $a\neq 0$, 则 $|b|\leqslant|a|$; 于是若 $b\mid a$, 且 $a\mid b$, 则 $|a|=|b|$.*

从该定理出发, 可得到下列定理

定理 2.6 (带余除法) 设 a,b 为整数 $b\neq 0$, 则存在唯一的一对整数 $q,\ r$, 使得

$$a=bq+r,\ 0\leqslant r<|b|,$$

整数 q 称为 a 被 b 除的**商**, r 称为 a 被 b 除的**余数**. .

证明 当 $b\mid a$ 时, 取 $r=0$ 和整数 $q=\dfrac{a}{b}$. 当 $b\nmid a$ 时, 设

$$E=\{a-bk\mid k\in\mathbb{Z}\}$$

易知 $E\cap\mathbb{Z}_+$ 非空 (例如取 $k=-nb$, 所以$a-bk=a+nb^2$, 当 n 是足够大正整数时, 能保证 $a-bk>0$, 也就是 E 中有正整数), 根据最小数原理, $E\cap\mathbb{Z}_+$ 有最小正整数, 设为

$$r=a-bq>0,\ q\in\mathbb{Z}.$$

若 $r=|b|$, 则 $a=b(q\pm 1)$, 这与 $b\nmid a$ 矛盾.

若 $r>|b|$, 记 $r'=r-|b|>0$, 则 $r'=r-(\pm b)=a-b(q\pm 1)\in E$, 而且$r>r'>0$, 这与 r 是 $E\cap\mathbb{Z}_+$ 中的最小正整数相矛盾. 所以 $r<|b|$.

要证明唯一性, 可假设若另有一对整数 q_1,r_1 满足

$$a=bq_1+r_1,\ 0\leqslant r_1<|b|,$$

则

$$b(q-q_1)+(r-r_1)=0,$$

推出 $b\mid(r-r_1)$. 但是 $0\leqslant|r-r_1|<|b|$, 所以只有 $r-r_1=0$, 从而 $q-q_1=0$. □

带余除法最简单例子是 $b=2$ 的情形, 此时, 整数被 2 除的余数只有两种可能, 0 或 1, 其中余数为 0 (即能被2 整除)的整数为偶数, 余数为 1 的整数为奇数, 偶数和奇数的一般表达式为

$$2k,\ 2k+1,\ k\in\mathbb{Z}.$$

类似地考虑被 3 除的整数, 其余数只能有$0,1,2$ 三种可能. 因此被 3 除的整数分为三类, 分别是

$$3k;\ 3k+1;\ 3k+2,\ k\in\mathbb{Z}.$$

数的整除性引出另一个重要概念, 即

定义 2.7 设 $a,\ b$ 是不全为零整数. 如果整数 d 满足:

(i) d 是 a 和 b 的公共约数 (简称公约数或公因子), 即 $d\mid a,\ d\mid b$.

(ii) d 是 a 和 b 的公约数中最大的, 即如果另有一个公约数 d', 则 $d'\leqslant d$.

那么称 d 是a,b 的**最大公约数** (或最大公因子) .记 a 和 b 的最大公约数为

$$d=(a,b).$$

如果两个整数 a 和 b 的最大公约数 $(a,b)=1$, 那么称 a 和 b ***互素***.

注意, 如果 d 是 a 和 b 的公约数, 那么 $-d$ 也是公约数, 因此**最大公约数一定是正整数**. 例如 $(4,6)=2,\ (6,9)=3,\ (10,9)=1$.

这里只考虑两个数的最大公约数, 对包含两个以上数组的最大公约数记为

$$d=(a_1,a_2,\cdots,a_n)$$

特别当 $(a_1,a_2,\cdots,a_n)=1$ 时, 称数组 $a_1,a_2,\cdots,a_n$ 互素.

如果数组 $a_1,a_2,\cdots,a_n$ 中任意两个数互素: $(a_i,a_j)=1,\ i\neq j$, 那么称数组 $a_1,a_2,\cdots,a_n$ **两两互素**. 很明显, 两两互素数组一定是互素的. 但一组互素数组未必两两互素, 例如 $(2,3,4)=1$, 但其中的 2 和 4 不是互素的.

§2.3 Euclid 辗转相除法

现在的问题是如何求两个数的最大公约数. 为了解决这个问题, 首先根据带余除法, 给出下面引理.

引理 2.8 对任意两个整数 a 和 b , 由带余除法可知

$$a=bq+r.$$

那么

$$(a,b)=(b,r)$$

也就是说 a 和 b 的最大公约数是 a 被 b 除的余数 r 与 b 的最大公约数.

证明 设 u 是 a 和 b 的公约数, 则存在整数 s,t 使得

$$a=su,\ b=tu,$$

推出

$$r=a-bq=su-tuq=(s-tq)u,$$

所以 u 也能整除 r , 因此 a 和 b 的任何公约数也是 b 和 r 的公约数. 反之, 如果一个整数能够整除 b 和 r , 当然也能整除 $a=bq+r$ 和 b.

总之, a,b 和 b,r 的公约数是一样的, 当然就有 $(a,b)=(b,r)$. 特别当 $r=0$ 时 (即 a 能被 b 整除), 显然有 $(a,b)=(b,0)=b$. □

下面给出著名的Euclid（欧几里得, 约公元前330 - 公元前275 ）**辗转相除法**.

对任意两个整数 a 和 b, 不妨设 $b>0$, 反复利用带余除法,

$$\begin{array}{lll}
\text{用 } b \text{ 除 } a: & a=bq_0+r_0, & 0<r_0<b,\\
\text{用 } r_0 \text{ 除 } b: & b=r_0q_1+r_1, & 0<r_1<r_0,\\
\text{用 } r_1 \text{ 除 } r_0: & r_0=r_1q_2+r_2, & 0<r_2<r_1,\\
\text{用 } r_2 \text{ 除 } r_1: & r_1=r_2q_3+r_3, & 0<r_3<r_2,\\
\vdots & \vdots & \vdots\\
\text{用 } r_{n-1} \text{ 除 } r_{n-2}: & r_{n-2}=r_{n-1}q_n+r_n, & 0<r_n<r_{n-1},\\
\text{用 } r_n \text{ 除 } r_{n-1}: & r_{n-1}=r_nq_{n+1}+0. &
\end{array}$$

只要余数 $r_1,r_2,\cdots$ 不出现 0, 就一直做下去. 因为

$$b>r_1>r_2>r_3>\cdots>0$$

所以辗转相除的过程不会无限制继续下去, 最多有限步（ $n\leqslant b$）就结束了, 也就有 $r_{n-1}=r_nq_{n+1}+0$.

利用引理2.8, 有

$$(a,b)=(b,r_0)=(r_0,r_1)=\cdots(r_{n-1},r_n)=(r_n,0)=r_n$$

因此, 通过“辗转相除”, 直到最后一个不为零的余数就是 a 和 b 的最大公约数.

例如取 $a=325,b=208$, 则 208 除 325 余117; 117 除 208 余91; 91 除 117 余 26; 26 除 91 余 13; 13 除 26 余 0. 所以 $(325,208)=13$.

辗转相除法还直接导致一个有意思结果.

从辗转相除第一个方程得到 $r_0=a-bq_0$, 因此 r_0 表示为 a 和 b 整系数线性组合:

$$r_0=k_0a+l_0b,$$

这里 $k_0=1,l_0=-q_0$ 都是整数. 代入下一个方程有

$$r_1=b-r_0q_1=b-(k_0a+l_0b)q_1=k_1a+l_1b$$

其中 k_1,l_1 也是整数. 重复上述过程, 最后有

$$r_n=(a,b)=ka+lb.$$

其中 k,l 为整数. 这样辗转相除法不但求出任意两个整数 a 和 b 的最大公约数 (a,b), 还得到方程 $ka+lb=(a,b)$ 一对整数解k,l , 也就是得到下列结论：

定理 2.9 (Bezout 裴蜀, 1730 -1783) *对任意两个整数 a 和 b, 存在一对整数 k,l 使得 a 和 b 的最大公约数表示为 a 和 b 的整系数线性组合*

$$ka+lb=(a,b)$$

上式称为 *Bezout* 公式 . 特别 a 和 b 互素当且仅当下列方程有整数解

$$ka + lb = 1.$$

顺便指出, Bezout 公式可以独立于辗转相除法加以证明, 以便向多个数的数组推广. 这里为了简化, 把对包含两个数的数组的 Bezout 公式看作是辗转相除法的推论.

利用Bezout 公式, 可以得到下列结果.

推论 2.10 设 a 和 b 是任意两个整数,

(i) 若整数 d 满足 $d \mid a,\ d \mid b$, 则 $d \mid (a, b)$.

(ii) 对任意正整数 m, 有 $(ma, mb) = m(a, b)$.

证明 设 d 是 a 和 b 公约数, 即 $d \mid a,\ d \mid b$, 因此 d 也能整除 $ka + lb$, 根据Bezout 公式知, d 能够整除 (a, b).

为了证明 (ii) , 设 $d = (a, b),\ e = (ma, mb)$. 因为 $md \mid ma,\ md \mid mb$, 所以由 (i) 可知 $md \mid (ma, mb)$, 即 $md \mid e$.

另一方面, 由 Bezout 公式, 存在整数 k, l, 使得 $d = ka + lb$. 由此推得

$$md = mka + mlb = k(ma) + l(mb)$$

所以$e \mid md$, 综上得 $e = md$. □

§2.4 素数和整数的素因子分解

定义 2.11 对于任何大于 *1* 的正整数 p, 如果 p 没有真因子, 即 p 的正约数只有 *1* 和 p 自身, 则称 p 为***素数 (或质数)***, 否则称为***合数***.

于是, 整个正整数被分为三类: 数 1 作为单独一类, 两外还有素数类和合数类.

素数有很多, 例如

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \cdots$$

关于素数最经典的一个结果是

定理 2.12 素数有无穷多个.

定理的证明早在公元前 3 世纪, 就由Euclid 给出, 证明的方法至今仍是数学推理的一个典范, 即 “反证法” . 该方法在此之前已经反复使用过.

证明 假设素数的个数只有有限个, 因此用 $p_1, p_2, \cdots, p_n$ 来表示全部有限个素数.

考虑整数

$$N = p_1 p_2 \cdots p_n + 1$$

由于 $N > 1$ 且 $N \neq p_j, j = 1, \cdots, n$, 因此 N 是合数, 故有素因子（素约数）p, 由于已经假设所有素数都在这里, p 必然等于 $p_1, \cdots, p_n$ 中某一个, 因而 p 能整除 $N - p_1 p_2 \cdots p_n = 1$, 也就是 p 能整除 1. 这显然是一个荒谬结论. 导致出现荒谬结论的原因说明假设是错误的, 因而它的反面必然是正确的. □

素数的重要性在于这样一个事实: **任何大于1 的正整数都能表示为素数的乘积**. 这是因为对于大于1 的整数 a, 如果它是合数就一定有非平凡约数$a = p_1 p_2$, 如果 p_1 和 p_2 两者至少有一个是合数, 则可继续分解. 这样的分解只有有限步, 直至分解到不能分解为止.

当一个整数被分解成素数乘积后, 根据整数乘法交换性, 这些素因子乘积次序无关紧要. 那么在不计次序时, 一个整数的素因子分解是唯一的.

定理 2.13 (算术基本定理) *每个大于 1 的正整数均可分解成有限个素数乘积, 如果不计素因子在乘积中次序, 那么分解是唯一的.*

仍然采取 Euclid 的证明方法, 为此做一些准备.

引理 2.14 *设 p 是素数, a 和 b 是两个整数. 如果 p 能整除 ab, 那么p 至少能够整除 a 和 b 中某一个.*

推而广之, 设 p 是素数, $a_1, a_2, \cdots, a_n$ 是 n 个整数. 如果 p 能整除这些数的乘积 $a_1 a_2 \cdots a_n$, 那么p 至少能够整除 $a_1, a_2, \cdots, a_n$ 中某一个.

引理的证明 因为素数 p 只有1 和自身 p 是它的约数. 如果 p 不能整除 a, 那么两者一定互素$(a, p) = 1$, 根据 Bezout 公式, 存在整数 k, l 使得

$$1 = ka + lp.$$

两边乘以 b, 得到

$$b = kab + lpb.$$

因为 p 整除 ab, 所以有$ab = pr$, 这样

$$b = kpr + lpb = p(kr + lb)$$

也就是 p 能整除 b. 这样就证明了如果 p 不能整除 a, 那么一定能够整除 b, 也就是 p 至少能够整除 a 和 b 中某一个.

关于第二个断言的证明, 采用归纳的方法.

当 $n = 2$ 时, 即两个数的情形下, 证明已经给出.

假设 p 能整除 $a_1 \cdots a_{n-1}$, 推出 p 能整除 $a_1, \cdots, a_{n-1}$ 中至少某一个.

那么当 p 能整除 $a_1\cdots a_{n-1}a_n=(a_1\cdots a_{n-1})a_n$ 时. 根据 $n=2$ 情形可知 p 能整除 $a_1\cdots a_{n-1}$ 和 a_n 中某一个. 如果 p 能整除 a_n, 则结论得证, 如果 p 能整除 $a_1\cdots a_{n-1}$, 根据归纳假设, p 能整除 $a_1,\cdots,a_{n-1}$ 中某一个. 无论哪种情形, p 一定能整除 $a_1,\cdots,a_{n-1},a_n$ 中某一个. □

算术基本定理的证明 假设正整数 a 有两种素因子分解

$$a=p_1\cdots p_r=q_1\cdots q_s,$$

这里 $p_1,\cdots,p_r$ 和 $q_1,\cdots,q_s$ 都是素数. 显然 p_1 能整除上式左边, 当然也能整除上式右边, 即 p_1 能整除 $q_1\cdots q_s$. 根据引理 p_1 一定能整除 $q_1,\cdots,q_s$ 至少某一个, 不妨设 p_1 能整除 q_k, 由于 q_k 是素数, 所以 $q_k=p_1$, 利用消去法两边消去这个共同素因子, 在剩余的部分继续上述过程, 最后得到 $p_1,\cdots,p_r$ 一定是 $q_1,\cdots,q_s$ 中的一部分.

上述做法完全可对称地对 $q_1,\cdots,q_s$ 实施, 因此得到 $q_1,\cdots,q_s$ 是 $p_1,\cdots,p_r$ 的一部分. 综上分析 $\{p_1,\cdots,p_r\}$ 与 $\{q_1,\cdots,q_s\}$ 完全重合. □

算术基本定理虽然针对正整数, 但不难推广到所有整数, 如果再把素因子中相等的因子合并, 最后有

定理 2.15 (标准分解) *设 n 是任意整数, 则 n 可唯一分解为*

$$n=\varepsilon p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$$

这里 $\varepsilon=\pm1$, $p_1,\cdots,p_k$ 是两两不同的素数, $\alpha_1,\cdots,\alpha_k$ 是正整数. 也称 α_j 是分解中素因子 p_j 的重数, $j=1,\cdots,k$.

以上讨论说明, 素数是构成整数最基本单元, 如同构成物质的基本粒子, 或像人类 “基因”. 自然要问, 如何在众多正整数中筛选出所有素数? 或能否通过一个表达式产生素数? 在整个正整数中有没有素数分布的 “图谱”?

首先看看如何在正整数中筛选出素数. 一种古老和简单的方法, 是对于给定正整数 n, 按照 $1,2,3,\cdots,n$ 排列, 然后逐一划掉所有 2 的倍数那些数 (不含 2 本身), 再逐一划掉 3 的倍数 (不含3 本身), 如此下去留下的就是 n 以内素数. 这个过程称为 “Eratosthems (爱拉陀塞姆, 约公元前274-194) 筛法”.

另一种考虑是研究产生素数的公式. Fermat (费马, 1601-1665) 曾给出下列公式

$$F(n)=2^{2^n}+1$$

通常称由上式给出的数为Fermat**数**. 可以验证对 $n=1,2,3,4$, Fermat 数是素数, 但是对 $n=5$, Fermat 数是合数

$$2^{2^5}+1=641\cdot6700417$$

对那些是素数的Fermat数, 就称为Fermat**素数**.

还有其它一些能够产生素数的简洁公式, 例如

$$f(n) = n^2 - n + 41,$$

当 $n = 1, 2, \cdots, 40$, $f(n)$ 都是素数, 但是 $f(41) = 41^2$ 不再是素数. 公式

$$f(n) = n^2 - 79n + 1601$$

从 $n = 1$ 直到 $n = 79$, 都是素数, 但是当 $n = 80$ 时就不再是素数了.

虽然人们没有寻找到求出素数规律性公式, 但发现在 n 以内素数的 "密度" (或者说 "分布") 却有一定的规律.

设 A_n 表示 n 以内素数的个数, 则 A_n/n 近似于 $1/\ln n$, 而且随着 n 增大, 这种近似越来越精确. 细节就不再讨论了.

§2.5 Euler 函数

Euler (欧拉, 1707-1783) 研究了另外一个问题, 即任意正整数 n 以内与 n 互素的正整数个数问题. 为此 Euler 定义了如下函数:

定义 2.16 *对任意正整数 n, 用 $\varphi(n)$ 表示 n 以内 (即从 1 到 n) 且与 n 互素正整数的个数. 称为Euler **函数**.*

例如 $\varphi(1) = 1$, 而 $\varphi(14) = 6$, 因为在不超过 14 的正整数中, 共有 1, 3, 5, 9, 11, 13 等 6 个数与 14 互素. 为了进一步研究 Euler 函数, 首先有

引理 2.17 *对任意一个素数 p 以及 p^α (α 是正整数), 有*

$$\varphi(p) = p - 1,$$
$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right).$$

证明 $\varphi(p) = p - 1$ 是显然的, 因为在1 到 p 的数中, 除了 p 自身, 其它 $p - 1$ 个数都与 p 互素.

设正整数 $\alpha > 1$, 则在 1 到 p^α 中是 p 倍数的数为

$$p,\ 2p,\ 3p,\ \cdots,\ p^{\alpha-1}p,$$

共有 $p^{\alpha-1}$ 个, 在 1 到 p^α 中除掉这些数, 剩余的都与 p^α 互素,因此与 p^α 互素的数共有 $p^\alpha - p^{\alpha-1}$ 个, 这样就证明了第二个等式. □

下列定理表明, 对一般正整数 n, $\varphi(n)$ 也可以严格计算.

定理 2.18 (Euler 定理) 对任意的正整数 n, 设 n 素因子分解为

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

其中, $p_1,\ p_2,\ \cdots,\ p_k$ 是n 的互不相等素因子, α_j 是素因子 p_j 的重数, $j = 1, \cdots, k$, 那么 *Euler* 函数在 n 的取值为

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

证明 证明分以下步骤.

第一步: 在 1 到 n 中是 p_1 倍数的数分别是

$$p_1,\ 2p_1,\ 3p_1,\ \cdots,\ \frac{n}{p_1}p_1,$$

共有 $\dfrac{n}{p_1} = p_1^{\alpha_1 - 1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ 个, 排除这些p_1 倍数的数, 就得到在 1 到 n 中与 p_1 互素整数的个数

$$n - \frac{n}{p_1} = n\left(1 - \frac{1}{p_1}\right).$$

第二步: 同理, 在 1 到 n 中是 p_2 倍数的数为

$$p_2,\ 2p_2,\ 3p_2,\ \cdots,\ \frac{n}{p_2}p_2,$$

共有$\dfrac{n}{p_2}$ 个. 但是, 其中有些数也是 p_1 的倍数, 因为 p_1 与 p_2 互素, 这些是 p_1 倍数的数出现在

$$1,\ 2,\ 3,\ \cdots,\ \frac{n}{p_2}$$

之中.在这 $\dfrac{n}{p_2}$ 个数中, 除去这些重复的数, 剩余的就是那些是 p_2 倍数但是与 p_1 互素的数, 根据第一步的结果, 它们的个数为 $\dfrac{n}{p_2}\left(1 - \dfrac{1}{p_1}\right)$.

因此, 在 1 到 n 与 p_1 互素的数中, 再排除那些是 p_2 倍数的数, 就得到与 p_1 和 p_2 都互素的数, 它们的个数为

$$n - \frac{n}{p_1} - \frac{n}{p_2}\left(1 - \frac{1}{p_1}\right) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right).$$

第三步: 1到 n 中, 是 p_3 的倍数的数共有 $\dfrac{n}{p_3}$ 个:

$$p_3,\ 2p_3,\ 3p_3,\ \cdots,\ \frac{n}{p_3}p_3,$$

其中有些数也是 p_1 或 p_2 的倍数, 并在第一步和第二步中已经排除过. 同样因为 $p_1,\ p_2$ 与 p_3 互素, 所以这些数出现在

$$1,\ 2,\ 3,\ \cdots,\ \frac{n}{p_3}$$

中, 因此除去这些重复排除的数, 剩余的数正是1 到 $\frac{n}{p_3}$ 中与 p_1 和 p_2 互素的那些数, 它们的个数由第二步可知是 $\frac{n}{p_3}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)$. 因此在1 到 n 中与 $p_1,\ p_2,\ p_3$ 都互素的数的个数为

$$\begin{aligned} &n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)-\frac{n}{p_3}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\\ &=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_3}\right). \end{aligned}$$

按同样的程序递推下去, 就得到定理中的结果. □

由Euler 定理, 直接得出被称为 Euler 函数的**积性**的性质:

推论 2.19 *对任意两个正整数 m,n, 若 $(m,n)=1$, 则*

$$\varphi(mn)=\varphi(m)\varphi(n).$$

证明是显然的, 设 $m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k},\ n=q_1^{\beta_1}q_2^{\beta_2}\cdots q_l^{\beta_l}$. 因为 $(m,n)=1$, 所以两个正整数的素数因子不重复, 利用 Euler 定理就得 $\varphi(mn)=\varphi(m)\varphi(n)$.

§2.6 同余

对于一个固定的正整数 m, 根据带余除法, 任何被 m 除的整数, 余数只可能是 $0,1,\cdots,m-1$ 中某一个. 因此, 可以根据除 m 的余数是否相等, 将整数进行分类.

1° 同余式

定义 2.20 *如果两个整数 a 和 b 同被 m 除有相同的余数(“同余”), 也就是 $m\mid(a-b)$. 则称 a 和 b **模** m **同余**, 或 a **模** m **同余于** b, m 称为**模**. 记为*

$$a\equiv b\ (\mathrm{mod}\ m)$$

*并称为(模 m 的)**同余式**. 如果 $m\nmid(a-b)$, 则称a 和 b **模** m **不同余**.*

两个数同余与通常两个数相等有许多类似性质, 将这些性质罗列如下

性质 2.21

(i) (自反性) $a\equiv a\ (\mathrm{mod}\ m)$;

(ii) (对称性) $a\equiv b\ (\mathrm{mod}\ m)$, 则 $b\equiv a\ (\mathrm{mod}\ m)$;

(iii) (传递性) $a\equiv b\ (\mathrm{mod}\ m),\ b\equiv c\ (\mathrm{mod}\ m)$, 则 $a\equiv c\ (\mathrm{mod}\ m)$.

如果 $a \equiv a' \pmod{m}$, $b \equiv b' \pmod{m}$, 那么

(iv) $a \pm b \equiv a' \pm b' \pmod{m}$;

(v) $ab \equiv a'b' \pmod{m}$.

(vi) 当 m 为素数时, 有

$$a \equiv 0 \pmod{m} \text{ 或 } b \equiv 0 \pmod{m}, \text{ 当且仅当 } ab \equiv 0 \pmod{m}.$$

证明 对 (i), (ii), (iii) 直接根据定义可证,

对于(iv) 和 (v), 因为 $m \mid (a - a')$ 等价于存在整数 r 使得 $a = a' + rm$. 同理 $m \mid (b - b')$ 等价于存在整数 s 使得 $b = b' + sm$, 由此推出

$$a \pm b = a' \pm b' + (r \pm s)m$$
$$ab = a'b' + (srm \pm a's \pm b'r)m$$

所以 $a \pm b$ 与 $a' \pm b'$ 模 m 同余, ab 与 $a'b'$ 模 m 同余.

对于(vi) : 若 $m \mid a$ 或 $m \mid b$, 则 $m \mid ab$, 反之, 若 $m \mid ab$, 则 m 至少能整除 a, b 中某一个 (引理 2.14) . □

下面是若干关于同余的简单实用的定理.

定理 2.22

(i) 若 $ac \equiv bc \pmod{m}$, 则

$$ac \equiv bc \left(\mod \frac{m}{(c,m)}\right).$$

特别当 $(c, m) = 1$ 时, 有 $a \equiv b \pmod{m}$.

(ii) 若 $a \equiv b \pmod{m}$, $d \mid m$, 则 $a \equiv b \pmod{d}$.

证明 记

$$m_1 = (c, m),\ m_2 = \frac{m}{(c,m)},$$

因此 $m = m_1 m_2,\ c = km_1$, 由已知条件知

$$m \mid (a - b)c, \text{ 或 } m_1 m_2 \mid (a - b)km_1,$$

所以$m_2 \mid (a - b)k$, 因此

$$m_2 \mid (a - b)c.$$

特别当 $m_1 = (c, m) = 1$ 时, $m = m_2$ 不能整除 c, 只能整除 $a - b$.

若 $d \mid m$, 记 $m = dm_1$. 如果 $m \mid (a - b)$, 即存在整数 k, 使得 $a - b = mk = dm_1 k$, 推得 $d \mid (a - b)$. □

2° 同余类

定义 2.23 设集合 E 中的元素之间存在一种关系记为 $a \sim b,\ a,b \in E$. 如果这种关系满足

自反性: $a \sim a,\ a \in E$;

对称性: 若 $a \sim b$, 则 $b \sim a$;

传递性: 若 $a \sim b,\ b \sim c$, 则 $a \sim c$.

那么称为**等价关系**. 两个元素具有等价关系 $a \sim b$ 也称为 a 和 b 彼此**等价**.

例如, 平面上三角形之间相似是一种等价关系, 两个数相等当然是等价关系. 而性质2.21 中的 (i)、(ii) 和 (iii) 表明整数之间模 m 的同余关系也是一种等价关系.

一般来说, 任何等价关系 $\sim$ 将集合 E 中元素按彼此等价归为一类, 称为关系 $\sim$ 的**等价类**. 不同的类中元素彼此不等价.

同样, 同余关系也可将整数按模 m 是否同余分为若干个两两不相交的类, 使得同一个类中任意两个整数模 m 同余, 不同类中任意两个整数模 m 不同余. 每一个这样的类称为 **模 m 同余类**.

具体来讲对一个整数 a, 将 a 所属的同余类记为$[a](\mathrm{mod}\ m)$ 或简记为 $[a]$, 这个类包含所有模 m 与 a 同余的整数

$$[a] = \{x \mid x \in \mathbb{Z},\ x \equiv a\ (\mathrm{mod}\ m)\}$$

a 是这个类的**代表元**.

如果 $a \equiv b\ (\mathrm{mod}\ m)$, 说明 a 和 b 属于同一类, 所以 $[a] = [b]$, 否则 $[a]$ 和 $[b]$ 作为 a 和 b 为代表的两个类是不相交的.

根据带余除法, 任何整数必与 $0, 1, 2, \cdots, m-1$ 中某一个模 m 同余, 而数组 $0, 1, 2, \cdots, m-1$ 内任何两个数彼此模 m 不同余, 因此模 m 恰好有 m 个同余类, 它们分别以余数 $0, 1, 2, \cdots, m-1$ 为代表元. 记这些同余类形成的集合为

$$\mathbb{Z}_m = \{[0],\ [1],\ [2],\ \cdots,\ [m-1]\}.$$

这是一个以 “类” 为元素的集合, 集合的元素的个数为 m 个.

例如, 取 $m = 2$, 则模 2 同余类只有两个, 一个是模 2 余 0 同余类 $[0]$, 也就是所有偶数全体. 另一个是模 2 余 1 同余类 $[1]$, 即所有奇数全体, 集合

$$\mathbb{Z}_2 = \{[0],\ [1]\}$$

共有两个元素, 一个是偶数集合, 另一个是奇数集合.

几何上看, 整数 $\mathbb{Z}$ 对应实数轴上所有整数点, 也就是以长度为 1 的等分点 (图2.1) .

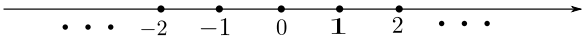


图 2.1

而 $\mathbb{Z}_m$ 对应的是圆上 m 个等分点, 例如钟表上的 12 个刻度, 就是 $\mathbb{Z}_{12}$ 中元素对应的点. 每过 12个小时, 指针指向同一个位置. 例如 3 小时, 15 小时, 27 小时等等, 都指向 [3] 的位置, 因为 $3, 15, 27, \cdots$, 模 12 同余, 属于模12 的同余类 [3] (图2.2) .

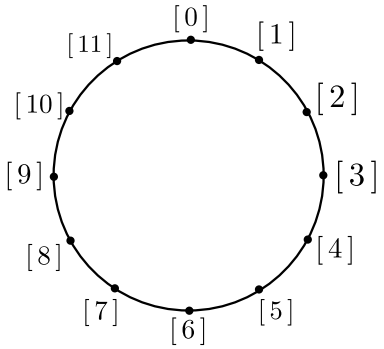


图 2.2

3° 同余类的运算

性质2.21 中的 (iv) 和 (v) 还说明, 对于模 m 的同余关系如同相等关系一样还有类似的 “加法”、“减法” 和 “乘法” . 对于相等关系, 有下列结果

$$ab = 0, \quad \text{当且仅当 } a = 0 \text{ 或 } b = 0.$$

但是对于同余关系, 必须对模 m 加以限制. 如果模 m 不是素数, 性质2.21 中的 (vi) 不成立. 例如

$$8 \equiv 2 \pmod 6,\ 9 \equiv 3 \pmod 6, \text{ 但是, } 72 \equiv 0 \pmod 6.$$

根据性质2.21 , 下面定义集合 $\mathbb{Z}_m$ 中元素的加法、减法和乘法运算.

同余类加减法 设 $[a],\ [b] \in \mathbb{Z}_m$, 则将模 m 同余类 $[a \pm b]$ 定义为 $[a]$ 与 $[b]$ 的和 (差)

$$[a] \pm [b] = [a \pm b].$$

首先要验证这样定义的合理性, 即不管选取什么样的代表元, 两个类之间的加减是唯一确定的: 假如在 $[a]$ 和 $[b]$ 中分别另取两个代表元 $a' \in [a],\ b' \in [b]$, 即 $a \equiv$

$a' \pmod m,\ b \equiv b' \pmod m$, 从而由同余性质2.21 中的 (iv) 得

$$a \pm b \equiv a' \pm b' \pmod m$$

也就是$a' \pm b'$ 与 $a \pm b$ 属于同一类, 所以$[a' \pm b'] = [a \pm b]$.

同余类乘法 同理, 可以定义 $[a]$ 和 $[b]$ 的乘积如下:

$$[a][b] = [ab],$$

根据性质2.21 中的 (v), 这样的定义的类之间的乘积与代表元的选取无关.

同余类中零元和单位元 称同余类 $[0]$ 和 $[1]$ 为 $\mathbb{Z}_m$ 中的零元和单位元 , 它们满足:

$$[a] + [0] = [0] + [a] = [a],\ [1][a] = [a][1] = [a].$$

容易验证上述定义的同余类之间的加法和乘法满足

(i) 交换律: $[a] + [b] = [b] + [a];\ [a][b] = [b][a]$,

(ii) 结合律: $([a] + [b]) + [c] = [a] + ([b] + [c]);\ ([a][b])[c] = [a]([b][c])$,

(iii) 分配律: $[a]([b] + [c]) = [a][b] + [a][b]$.

虽然 $\mathbb{Z}_m$ 只有有限个元素, 但是 $\mathbb{Z}_m$ 与整数集合 $\mathbb{Z}$ 有同样的运算规律, 所以也是加法群和交换环, 称为**模 m 的同余类环**.

下面以 $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$ 为例, 分别给出元素之间的加法和乘法.

加法	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

乘法	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

同余类的逆 关于 $\mathbb{Z}_m$ 中元素在乘法运算下是否可逆问题, 需要进一步讨论.

回顾一下在有理数 $\mathbb{Q}$ 中, 一个非零有理数 α 的所谓逆元, 是指方程 $\alpha x = 1$ 在 $\mathbb{Q}$ 中有唯一解. 这个解 x 就称为有理数 α 的逆, 记为 $x = \alpha^{-1} \in \mathbb{Q}$.

但是在 $\mathbb{Z}_m$ 中, 并非对所有非零元素 $[a]$, 方程 $[a][x] = [ax] = [1]$ 在 $\mathbb{Z}_m$ 中都有解, 也就是 $[a]$ 在 $\mathbb{Z}_m$ 中不一定都有逆. 例如对 $\mathbb{Z}_6$ 中的 $[2]$, 就不存在 $[x]$, 使得 $[2][x] = [2x] = 1$ 有解, 因为不会存在整数 x 使得 $2x \equiv 1 \pmod 6$.

另外, 对 $\mathbb{Z}_6$ 中两个非零元素 $[2]$ 和 $[3]$, 有 $[2][3] = [0]$, 这也说明 $\mathbb{Z}_6$ 中的 $[2]$ 和 $[3]$ 不可能有逆.

然而, 如果考虑 $\mathbb{Z}_m$ 的子集合

$$\mathbb{Z}_m^* = \{[a] \mid [a] \in \mathbb{Z}_m,\ (a, m) = 1\},$$

则 $\mathbb{Z}_m^*$ 中的元素却有逆, 也就是说, 只有当 $(a, m) = 1$ 时, $[a]$ 可逆且 $[a]^{-1} \in \mathbb{Z}_m^*$.

定理 2.24 集合 $\mathbb{Z}_m^*$ 中元素满足

(i) $[1] \in \mathbb{Z}_m^*$.

(ii) 若 $[a], [b] \in \mathbb{Z}_m^*$, 则 $[a][b] \in \mathbb{Z}_m^*$.

(iii) 若 $[a] \in \mathbb{Z}_m^*$, 则方程 $[a][x] = [1]$ 在 $\mathbb{Z}_m^*$ 中有唯一解, 记为 $[x] = [a]^{-1}$.

任何满足上述三条的集合称为***乘法群***, 因此 $\mathbb{Z}_m^*$ 是 (可交换的) 乘法群, 且元素的个数为 $1, 2, \cdots, m$ 中与 m 互素的整数个数, 即 $\varphi(m)$ (定义*2.16* 中的*Euler* 函数) .

证明 (i) 是显然的, 因为 $(1, m) = 1$.

对于 (ii), 只要用到若 $(a, m) = 1, (b, m) = 1$ 就有 $(ab, m) = 1$ 这个简单事实就有 $[a], [b] \in \mathbb{Z}_m^*$, 推出 $[a][b] \in \mathbb{Z}_m^*$.

对于(iii) 的证明如下:

对任意的 $[a] \in \mathbb{Z}_m^*$, 因为$(a, m) = 1$, 所以

$$0a - 1,\ a - 1, 2a - 1, \cdots, (m-1)a - 1$$

这 m 个数两两互不同余, 否则若 $j > i$, 使得 $ia - 1$ 与 $ja - 1$ 同余, 就导致 $m \mid (j - i)a$, 但 $(a, m) = 1$, 因此只能 $m \mid (j - i),\ 0 < j - i < m$, 这显然是不可能的.

因此, 这 m 个数所在的同余类共 m 个, 与 $\mathbb{Z}_m$ 一致:

$$\{[0a - 1], [a - 1], [2a - 1], \cdots, [(m-1)a - 1]\} = \mathbb{Z}_m,$$

这样就意味着, 必存在唯一的 k, 使得 $[ka - 1] = [0]$, 即存在唯一的 k, 使得 $ka \equiv 1 \pmod m$, 所以 $[x] = [k]$ 是方程 $[a][x] = [1]$ 的唯一解.

因 $m \mid ka-1$, 所以存在整数 b, 使得 $ka-1=mb$, 或 $ka+mb=1$. 根据Bezout 定理2.9, $(k,m)=1$, 这就推得解 $[x]=[k]\in\mathbb{Z}_m^*$. □

例 2.6.1 当 $m=5$, 有

$$\mathbb{Z}_5^*=\{[1],[2],[3],[4]\},$$

元素逆分别为

$$[1]^{-1}=[1],\ [2]^{-1}=[3],\ [3]^{-1}=[2],\ [4]^{-1}=[4].$$

当 $m=12$, 有

$$\mathbb{Z}_{12}^*=\{[1],[5],[7],[11]\},$$

元素逆分别为

$$[1]^{-1}=[1],\ [5]^{-1}=[5],\ [7]^{-1}=[7],\ [11]^{-1}=[11],.$$

当 $m=14$, 有

$$\mathbb{Z}_{14}^*=\{[1],[3],[5],[9],[11],[13]\},$$

元素逆分别为

$$[1]^{-1}=[1],\ [3]^{-1}=[5],\ [5]^{-1}=[3],\ [9]^{-1}=[11],\ [11]^{-1}=[9],\ [13]^{-1}=[13].$$

因此要使得$\mathbb{Z}_m$ 中除 $[0]$ 外每个元素都可逆, 只有当 $m=p$ 是素数. 因为此时除 0 以外, $1,2,\cdots,p-1$ 都与p 互素, 也就有$\mathbb{Z}_p=\{[0]\}\cup\mathbb{Z}_p^*$.

定理 2.25 *设 p 是任意素数, 则 $\mathbb{Z}_p$ 中元素满足*

(i) *对任意的 $[a],[b]\in\mathbb{Z}_p$, 有*

$$[a]\pm[b]=[a\pm b]\in\mathbb{Z}_p,\quad [a][b]\in\mathbb{Z}_p;$$

(ii) *$\mathbb{Z}_p$ 中有 0 元 $[0]$ 和单位元 $[1]$, 即对任意的 $[a]\in\mathbb{Z}_p$, 有*

$$[a]+[0]=[a],\quad [a][1]=[a];$$

(iii) *对 $\mathbb{Z}_p$ 中任何非零的 $[a]$, 存在逆元 $[x]=[a]^{-1}\in\mathbb{Z}_p$, 使得*

$$[a][a]^{-1}=[a]^{-1}[a]=[1].$$

*任何满足上述三条的集合称为**域**, 因此对素数 p, $\mathbb{Z}_p$ 是一个域. 因为 $\mathbb{Z}_p$ 中共有 p 个同余类, 因此称为**有限域**.*

总结一下, 通过对整数和同余类的讨论, 我们接触到这样几个数学概念:

环: 满足加法、乘法以及交换律、结合律、分配律, 并有 0 元和单位元集合称为(交换)环. 例如整数集合 $\mathbb{Z}$ 和同余类集合 $\mathbb{Z}_m$.

群： 满足乘法和除法（乘法的逆运算）及交换律、结合律并有单位元集合, 称为（乘法）群. 例如 $\mathbb{Z}_m^*$（定理2.24）.

域： 既是交换环又是乘法群（除法除 0 元素外）集合, 称为域. 例如理数集合 $\mathbb{Q}$ 以及 $\mathbb{Z}_p$（p 为素数）, 其中 $\mathbb{Z}_p$ 中的元素个数是有限的, 因此是有限域.

例 2.6.2 十进制表示的正整数 $n = a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_0$ 能被 3 整除的充分必要条件是 $a_n + a_{n-1} + \cdots + a_0$ 能被 3 整除.这里 $0 \leqslant a_n, a_{n-1}, \cdots a_0 \leqslant 9$.

证明 在$\mathbb{Z}_3$ 中, 不难验证 $[10^k] = [1]$, 所以

$$\begin{aligned}[n] &= [a_n][10^n] + [a_{n-1}][10^{n-1}] + \cdots + [a_0][1] \\ &= [a_n][1] + [a_{n-1}][1] + \cdots + [a_0][1] \\ &= ([a_n] + [a_{n-1}] + \cdots + [a_0])[1] \\ &= [a_n + a_{n-1} + \cdots + a_0][1] \\ &= [a_n + a_{n-1} + \cdots + a_0]\end{aligned}$$

因此 $[n] = [0]$ 等价于 $[a_n + a_{n-1} + \cdots + a_0] = [0]$, 也就是 n 能被 3 整除等价于$a_n + a_{n-1} + \cdots + a_0$ 能被 3 整除.

4° Fermat-Euler 定理

最后给出二个重要的定理.

定理 2.26 (Fermat 定理) *设 a 是整数, p 是素数.*

(i) *若$p \nmid a$,* 则 $a^{p-1} \equiv 1 \pmod{p}$.

(ii) *若$p \mid a$,* 则 $a^p \equiv a \pmod{p}$.

证明 当 $p \nmid a$ 时, 考虑以下 $p-1$ 个 a 的倍数:

$$m_1 = a,\ m_2 = 2a,\ \cdots,\ m_{p-1} = (p-1)a.$$

在$p \nmid a$ 前提下, 这些数有如下特点:

对 $m_r = ra$ $(1 < r < p)$: 因 $p \nmid r$, 推出 $p \nmid m_r$.

对 $m_s - m_r = (s-r)a$ $(1 \leqslant r < s \leqslant p-1)$: 因 $p \nmid (s-r)$, 推出 $p \nmid (m_r - m_s)$.

因此 $m_1, m_2, \cdots, m_{p-1}$ 被 p 整除的余数两两不等且不等于 0, 所有的 $p-1$ 个余数只能是 $1, 2, \cdots, p-1$. 虽然有可能不会按次序对应, 但根据同余性质2.21 中的 (v), 有

$$m_1 m_2 \cdots m_{p-1} \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}.$$

另一方面, 注意到

$$m_1 m_2 \cdots m_{p-1} = 1 \cdot 2 \cdots (p-1)a^{p-1} = (p-1)!a^{p-1},$$

由上述两式得

$$(p-1)!\left(a^{p-1}-1\right)\equiv 0 \pmod{p},$$

但是 p 不能整除 $(p-1)!$, 这样由性质2.21 中的 (vi) 得, p 只能整除 $a^{p-1}-1$.

当 $p \mid a$ 时, (ii) 的结论是显然的. □

定理 2.27 (Euler定理) *设 m 为正整数, a 为整数, 且 $(a,m)=1$, 则*

$$a^{\varphi(m)}\equiv 1 \pmod{m}.$$

该定理是Fermat 定理的推广, 此处不再证明.

§2.7 同余方程(组)

给定正整数 m, 以及 n 次整系数多项式

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0 \quad (a_n,a_{n-1},\cdots,a_0\in\mathbb{Z}),$$

下列方程

$$f(x)\equiv 0 \pmod{m}$$

称为**模 m 的 n 次同余方程**. 本专题只讨论一次同余方程(组)的求解问题.

给定正整数 m, 一次同余方程一般表示为

$$ax\equiv b \pmod{m} \quad (a,b\in\mathbb{Z}).$$

如果 $x=x_0\in\mathbb{Z}$ 是方程的一个解: $m \mid (ax_0-b)$, 那么对任意的 $x\in[x_0]$, 有 $x=x_0+km$, 其中 k 是整数,推出 $(ax-b)=(ax_0-b)+kam$, 所以 $m \mid (ax-b)$, 即 x 也是方程的解. 因此将属于同一同余类中的解视为相同的, 只有那些模 m 不同余的解才视为不同的解.

一次同余方程组就是若干个一次同余方程的联立方程组

$$a_1x\equiv b_1 \pmod{m_1},\cdots,a_sx\equiv b_s \pmod{m_s}.$$

1° 一次同余方程

定理 2.28 *设 $(a,m)=d$, 则一次同余方程*

$$ax\equiv b \pmod{m}.$$

有解的充分必要条件是 $d \mid b$. 当此条件成立时, 共有 d 个解. 若 $(a,m)=1$, 则解唯一.

证明 设方程有解 x, 因 $d \mid m$, 由 $m \mid (ax-b)$ 推出 $d \mid (ax-b)$. 但 $d \mid a$, 所以 $d \mid b$.

反之, 若 $d \mid b$, 由Bezout 定理2.9知, 存在整数 k, l 使得

$$ka + lm = (a, m) = d,$$

因 $\dfrac{b}{d}$ 是整数, 同乘以上式两边, 得

$$ak\frac{b}{d} + ml\frac{b}{d} = b,$$

由此得整数 $x_0 = k\dfrac{b}{d}$ 满足 $m \mid (ax_0 - b)$, 因此是方程的一个解. 令

$$x_r = x_0 + r\frac{m}{d}, \quad r = 0, 1, \cdots, d-1,$$

推出

$$ax_r - b = ax - b + rm\frac{a}{d},$$

其中 $\dfrac{a}{d}$ 是整数, 所以 $m \mid (ax_r - b)$, 即 $x_r,\ r = 0, 1, \cdots, d-1$ 满足方程. 另一方面

$$x_r - x_s = (r-s)\frac{m}{d},\ r \neq s,$$

因 $r - s < d$, 所以 $m \nmid (x_r - x_s)$. 即 $x_r,\ r = 0, 1, \cdots, d-1$ 互不同余, 因此是 d 个解. □

定理 2.29 设 $d = (a, m),\ d \mid b$, 则同余方程

$$ax \equiv b \pmod{m} \tag{1}$$

等价于下列形式

$$x \equiv b' \pmod{m'}. \tag{2}$$

其中 $b' = \dfrac{b}{d}c,\ m' = \dfrac{m}{d},\ c$ 是同余方程 $\dfrac{a}{d}x \equiv 1 \pmod{m'}$ 的解.

注意, 虽然 (1) 有 d 个解, 而 (2) 的解唯一, 但只要证明 (1) 和 (2) 有同解即可. 不妨设同解为 x_0. (2) 的其它解都属于同一个模 m' 的同余类: $[x_0] (\mathrm{mod}\ m')$, 其中的数 $x_0 + rm' = x_0 + r\dfrac{m}{d},\ r = 0, 1, 2, \cdots, d-1$ 满足 (1), 但两两模 m 互不同余, 因此是 (1) 的 d 个解. 反之, (1) 的 d 个解模 m' 是同余的, 因此给出 (2) 的唯一解.

证明 为了简化证明, 不妨设$d = 1$, 所以$b' = bc,\ m' = m,\ ac \equiv 1 \pmod{m}$, 或 $ac = 1 + km$. 由此推出 $m \nmid c$, 那么 $m \mid (ax - b)$ 等介于 $m \mid (acx - bc)$, 把 $ac = 1 + km$ 代入后, 就等价于 $m \mid (x - bc)$. □

定理 2.30 设 $(a, m) = 1$, 若 $m = m_1 m_2$, 且 $(m_1, m_2) = 1$, 则同余方程 $ax \equiv b \pmod{m}$ 等价于下列同余方程组

$$ax \equiv b \pmod{m_1},\ ax \equiv b \pmod{m_2}.$$

证明 $(a,m)=1$ 等价于 $(a,m_1)=(a,m_2)=1$, 且 $m \mid (ax-b)$ 当且仅当 $m_1 \mid (ax-b)$, $m_2 \mid (ax-b)$(习题6). □

2° 一次同余方程组

根据定理2.29, 以下只考虑下列形式的同余方程组.

$$x \equiv b_1 \pmod{m_1}, \cdots, x \equiv b_s \pmod{m_s}.$$

对于一次同余方程组, 不一定总有解, 即使其中的每一个同余方程都有解.

例 2.7.1 在一次同余方程组

$$x \equiv 0 \pmod 2,\ x \equiv 1 \pmod 4$$

中, 每个同余方程都有解, 但没有联立解.

自然要问, 什么条件能保证一组同余方程有解? 下列著名的中国剩余定理给出了同余方程组有联立解的完美回答, 也就是只要每个同余方程的模两两互素, 则方程组一定有解. 该定理还给出了求解的具体方法. 这里仅以三个一次同余方程联立的方程组来解释该定理, 但结论不难推广到包含 n 个一次同余方程组情形.

定理 2.31 (中国剩余定理) *设 m_1, m_2, m_3 是两两互素的正整数, 则对任意整数 b_1, b_2, b_3, 下列关于 x 的同余方程组必有解.*

$$x \equiv b_1 \pmod{m_1},\ x \equiv b_2 \pmod{m_2},\ x \equiv b_3 \pmod{m_3}. \tag{3}$$

而且全部解属于模 $m_1m_2m_3$ 的同一个同余类.

证明 把同余方程组(3)分解为三组同余方程组

$$x_1 \equiv 1 \pmod{m_1},\ x_1 \equiv 0 \pmod{m_2},\ x_1 \equiv 0 \pmod{m_3}; \tag{4}$$

$$x_2 \equiv 0 \pmod{m_1},\ x_2 \equiv 1 \pmod{m_2},\ x_2 \equiv 0 \pmod{m_3}; \tag{5}$$

$$x_3 \equiv 0 \pmod{m_1},\ x_3 \equiv 0 \pmod{m_2},\ x_3 \equiv 1 \pmod{m_3}; \tag{6}$$

如果这三组同余方程组(4)-(6)分别有解 x_1, x_2, x_3, 那么(3)的解就为

$$x = b_1x_1 + b_2x_2 + b_3x_3.$$

因此, 证明归结为分别求解(4)-(6).

关于(4), 由条件可知 $(m_2m_3,\ m_1)=1$, 根据 Bezout 公式, 存在整数 k_1, l_1, 使得

$$k_1(m_2m_3) + l_1m_1 = 1 \tag{7}$$

推出 $k_1(m_2m_3) \equiv 1 \pmod{m_1}$, 取 $x_1 = k_1m_2m_3$, 则 x_1 满足 (4) 中第一个方程, 并自然满足 (4) 中第二个、第三个方程. 所以 $x_1 = k_1m_2m_3$ 是 (4) 的一个解.

同理, 因 $(m_1m_3, m_2) = 1$ 和 $(m_1m_2, m_3) = 1$, 分别存在整数 k_2, l_2 和 k_3, l_3 使得

$$k_2(m_1m_3) + l_2m_2 = 1, \tag{8}$$

$$k_3(m_1m_3) + l_3m_3 = 1. \tag{9}$$

也就得到 (5) 和 (6) 的解:

$$x_2 = k_2(m_1m_3),\ x_3 = k_3(m_1m_2),$$

这样方程组 (3) 的一个解为

$$x = k_1b_1m_2m_3 + k_2b_2m_1m_3 + k_3b_3m_1m_2.$$

其中 k_1, k_2, k_3 是从三个 Bezout 公式中解出的整数. 因此解同余方程组 (3) 最终转化为利用 Euclid 辗转相除法求出 Bezout 公式 (7) - (9) 中的整数 .

若 x' 是 (3) 的另一个解, 则 $m_i \mid (x - x')$, $i = 1, 2, 3$, 因 m_1, m_2, m_3 两两互素, 推得 $m_1m_2m_3 \mid (x - x')$ (习题 6), 也就是 $x \equiv x' \pmod{m_1m_2m_3}$, 属于同一个同余类. □

例 2.7.2 (孙子问题) 今有物不知其数, 三三数之余二, 五五数之余三, 七七数之数余二, 问该物几何?

解 设该物共有 N 个, 那么上述问题实际上是要解下列同余方程组

$$N \equiv 2 \pmod 3,\ N \equiv 3 \pmod 5,\ N \equiv 2 \pmod 7.$$

根据中国剩余定理, 分别取 $m_1 = 3, m_2 = 5, m_3 = 7$ 以及$b_1 = 2, b_2 = 3, b_3 = 2$, 因此

欲求 x_1, 先解 $35k_1 + 3l_1 = 1$ 得 $k_1 = 2, l_1 = -23$, 所以$x_1 = 70$.

欲求 x_2, 先解 $21k_2 + 5l_2 = 1$ 得 $k_2 = 1, l_2 = -4$, 所以 $x_2 = 21$.

欲求 x_3, 先解 $15k_3 + 7l_3 = 1$ 得 $k_3 = 1, l_2 = -2$, 所以 $x_3 = 15$.

最终孙子问题的解为

$$x = 2 \cdot 70 + 3 \cdot 21 + 2 \cdot 15 = 233.$$

减去 $3 \cdot 5 \cdot 7 = 105$ 的倍数就得到同一同余类中最小的正整数解 $x = 23$.

注记 例*2.7.2* 中的孙子问题源于约公元*400*年的数学著作《孙子算经》(作者不详). 这是历史上首次提到了一次同余方程组问题以及具体解法.

南宋时期的数学家秦九昭 (*1202-1261*) 在他的著作《数书九章》(成书于*1247*年) 中对此类问题的解法作了完整系统的论述, 并把求解一次同余方程组的一般步骤称为“大衍求一术”. 可以说秦九昭是研究一次同余方程组集大成者.

明代数学家程大位(*1533-1606*)将孙子问题的解答编成了《孙子歌诀》:

"三人同行七十稀,五树梅花廿一枝, 七子团员半个月,除百零五便得知."

歌诀中前三句中的"三人"、"五树"和"七子"分别指三个模 *3, 5, 7*. 而"七十稀"、"廿一枝"和"半个月"是求出的三个解 $x_1 = 70,\ x_2 = 21,\ x_3 = 15$. 最后一句中"百零五"是指三个模的乘积 $3 \cdot 5 \cdot 7 = 105$. 并说明了如何得到最小正整数解.

正是中国古代科学家对同余方程组系统研究, 产生了举世公认的"中国剩余定理".

推论 2.32 设正整数 m_1, m_2, m_3 两两互素, 若同余方程组

$$a_1x \equiv b_1 \pmod{m_1},\ a_2x \equiv b_2 \pmod{m_2},\ a_3x \equiv b_3 \pmod{m_3} \tag{10}$$

中每个方程都有解, 则一定有联立解.

这里仍然只取三个方程为例, 其结论不难推广到包含 n 个方程情形..

证明 根据定理2.28, 每个方程有解意味着 $d_i \mid b_i,\ d_i = (a_i, m_i)\ (i = 1, 2, 3)$. 再根据定理2.29, 方程等价于

$$x \equiv b_1' \pmod{m_1'},\ x \equiv b_2' \pmod{m_2'},\ x \equiv b_3' \pmod{m_3'}, \tag{11}$$

其中 $m_i' = \dfrac{m_i}{d_i},\ i = 1, 2, 3$. 显然 m_1, m_2, m_3 两两互素推出 m_1', m_2', m_3' 两两互素, 根据中国剩余定理, 方程(11)有解, 推出方程(10)有解. □

例 2.7.3 求解同余方程组

$$5x \equiv 7 \pmod{12},\ 7x \equiv 1 \pmod{10}.$$

解 显然, 12 和 10 不互素, 所以不能直接应用定理. 根据定理2.30, 在第一个方程中, $12 = 3 \cdot 4$, 因此等价于

$$5x \equiv 7 \pmod{3},\ 5x \equiv 7 \pmod{4},$$

并继续简化为

$$x \equiv 2 \pmod{3},\ x \equiv 3 \pmod{4},$$

同理, 在第二个方程中, $10 = 2 \cdot 5$, 利用定理2.30并继续简化得下列等价形式

$$x \equiv 1 \pmod{2},\ x \equiv 3 \pmod{5}.$$

注意到 $x \equiv 3 \pmod{4}$ 和 $x \equiv 1 \pmod{2}$ 等介于 $x \equiv 3 \pmod{4}$. 所以本题同余方程组等介于下列可用中国剩余定理求解的同余方程组

$$x \equiv 2 \pmod{3},\ x \equiv 3 \pmod{4},\ x \equiv 3 \pmod{5}.$$

§2.8 多项式

在本专题的最后, 简要介绍有关多项式的基本内容, 这是因为多项式与整数有很多相似之处. 所谓多项式是指

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0\ (a_n\neq 0),$$

这里, n 是非负整数, 称为多项式 **次数**, 记为 $\deg f(x)=n$. 次数为 0 多项式称为**平凡多项式**, 次数大于 0 多项式称为**非平凡多项式**.首项 (最高次数项) 系数为 1 多项式, 称为**首一多项式**.

多项式系数 $a_n,a_{n-1},\cdots,a_0$ 可以属于整数 $\mathbb{Z}$, 也可以属于有理数域 $\mathbb{Q}$、实数域 $\mathbb{R}$、复数域 $\mathbb{C}$ 或其他域 (例如定理2.25中定义的有限域 $\mathbb{Z}_p$, p 是素数). 称系数属于整数 $\mathbb{Z}$, 或某个域 $\mathbb{F}$ 的多项式为 "$\mathbb{Z}$ 上多项式" , 或 "域 $\mathbb{F}$ 上多项式" , 记整数 $\mathbb{Z}$, 或域 $\mathbb{F}$ 上多项式的全体为 $\mathbb{Z}[x]$, 或 $\mathbb{F}[x]$. $\mathbb{Z}$ 或 $\mathbb{F}$ 上两个多项式

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0\ \ (a_n\neq 0),$$
$$g(x)=b_mx^m+b_{m-1}x^{m-1}+\cdots+b_0\ \ (b_m\neq 0)$$

之间可以进行加法和乘法运算, 其结果还是 $\mathbb{Z}$ 或 $\mathbb{F}$ 上多项式, 并且有

$$\deg(f+g)\leqslant\max\{\deg f,\deg g\},$$
$$\deg(fg)=\deg f+\deg g.$$

1° 多项式带余除法和最大公因式

设 $\mathbb{F}$ 是给定域, $f(x),g(x)\in\mathbb{F}[x],\ g(x)\neq 0$, 如果存在 $h(x)\in\mathbb{F}[x]$, 使得

$$f(x)=g(x)h(x),$$

那么称 $g(x)$ 在 $\mathbb{F}[x]$ 中整除 $f(x)$, 记为 $g(x)\mid f(x)$, 并称 $g(x)$ 是$f(x)$ 的一个**因式**, $f(x)$ 是 $g(x)$ 的一个**倍式**. 对于两个多项式 $f(x),\ g(x)$, 如果 $h(x)\mid f(x),\ h(x)\mid g(x)$, 那么称 $h(x)$ 是 $f(x),\ g(x)$ 的**公因式**.

定理 2.33 (带余除法) 设 $\mathbb{F}$ 是给定域, $f(x),g(x)\in\mathbb{F}[x],g(x)\neq 0$, 那么存在唯一的一组多项式 $q(x),\ r(x)\in\mathbb{F}[x]$, 使得

$$f(x)=q(x)g(x)+r(x),$$

其中$r(x)$ 或者为 0, 或者 $\deg r(x)<\deg g(x)$.

定理中 $q(x)$ 与 $r(x)$ 分别称为 $f(x)$ 被 $g(x)$ 整除的**商式**和**余式**.

证明 如果 $\deg f(x) < \deg g(x)$, 那么取 $q(x) = 0,\ r(x) = f(x)$, 如果 $g(x) = c \neq 0$ (常数) , 那么取 $q(x) = \dfrac{1}{c}f(x),\ r(x) = 0$, 所以不妨设

$$\deg f(x) \geqslant \deg g(x) > 0,$$

记 $n = \deg f(x),\ m = \deg g(x)$, $f(x)$ 和 $g(x)$ 的首项系数分别为 $a_n,\ b_m$. 令

$$q_1(x) = \frac{a_n}{b_m}x^{n-m},$$

那么

$$f_1(x) = f(x) - q_1(x)g(x)$$

的次数满足 $\deg f_1(x) < \deg f(x)$. 如果 $\deg f_1(x) \geqslant \deg g(x)$, 那么对 $f_1(x)$ 重复上述过程, 就得到一列多项式 $f_0(x) = f(x), f_1(x), f_2(x), \cdots$, 和 $q_1(x), q_2(x), \cdots$, 使得

$$f_{i+1}(x) = f_i(x) - q_{i+1}(x)g(x),\ i = 0, 1, 2, \cdots .$$

而且

$$\deg f(x) > \deg f_1(x) > \deg f_2(x) > \cdots ,$$

这样的过程有限步后必然会停止, 即存在 l, 使得 $f_l(x) = 0$ 或 $\deg f_l(x) < \deg g(x)$. 于是

$$q(x) = q_1(x) + \cdots + q_l(x),\quad r(x) = f_l(x)$$

便给出定理中的表示. 假如有两组表示

$$f(x) = q_1(x)g(x) + r_1(x),\ f(x) = q_2(x)g(x) + r_2(x),$$

那么推出 $(q_1(x) - q_2(x))g(x) = r_1(x) - r_2(x)$, 比较两边次数就可得到

$$q_1(x) = q_2(x),\ r_1(x) = r_2(x),$$

因此唯一性得证. □

注记 由于整数不可以做除法, 所以带余除法对整系数多项式不适用. 但是对 $f(x), g(x) \in \mathbb{Z}[x], g(x) \neq 0$, 如果限制 $g(x)$ 的首项系数为 *1*, 那么上述证明过程和结论都适用于整系数多项式.

定义 2.34 设 $f(x),\ g(x) \in \mathbb{F}[x]$, $f(x)$ 与 $g(x)$ 的**最大公因式**是指满足如下条件首一多项式$d(x) \in \mathbb{F}[x]$:

(i) $d(x)$ 是 $f(x)$ 与 $g(x)$ 公因式, 即 $d(x) \mid f(x),\ d(x) \mid g(x)$;.

(ii) 若 $d_1(x)$ 是 $f(x)$ 与 $g(x)$ 公因式, 则 $\deg d_1(x) \leqslant \deg d(x)$.

记 $d(x) = (f(x),\ g(x))$. 若 $d(x) = 1$, 则称 $f(x)$ 和 $g(x)$**互素**.

根据带余除法, 对 $f(x)=q(x)g(x)+r(x)$, 类似整数情形, 有

$$(f(x),g(x))=(g(x),r(x)).$$

同样类似整数情形, $f(x)$ 和 $g(x)$ 最大公因式可通过多项式的 Euclid 辗转相除法给出, 具体做法如下:

给定不全为零的 $f(x),\ g(x)\in\mathbb{F}[x]$, 如果 $g(x)=0$, 那么

$$(f(x),\ g(x))=\alpha f(x),$$

其中 $\alpha\in\mathbb{F}$ 是常数使得 $\alpha f(x)$ 为首一多项式. 如果 $f(x)$ 和 $g(x)$ 都不为零, 不妨设 $\deg f(x)\geqslant\deg g(x)$. 相继计算如下带余除法

$$\begin{aligned}
&f(x)=q_0(x)g(x)+r_0(x), && (\deg r_0(x)<\deg g(x))\\
&g(x)=q_1(x)r_0(x)+r_1(x), && (\deg r_1(x)<\deg r_0(x))\\
&r_0(x)=q_2(x)r_1(x)+r_2(x), && (\deg r_2(x)<\deg r_1(x))\\
&\cdots\cdots\\
&r_{n-2}(x)=q_n(x)r_{n-1}(x)+r_n(x), && (\deg r_n(x)<\deg r_{n-1}(x))\\
&r_{n-1}(x)=q_{n+1}r_n(x)+0
\end{aligned}$$

直至出现余式为零. 因为 $r_0(x),r_1(x),\cdots$, 的次数依次降低, 这样的步骤一定有限. 所以

$$(f(x),g(x))=(g(x),r_0(x))=(r_0(x),r_1(x))\cdots=(r_n(x),0)=\alpha r_n(x),$$

其中$\alpha\in\mathbb{F}$ 使得 $\alpha r_n(x)$ 为首一多项式.

从多项式辗转相除的第一个方程得到 $r_0(x)=f(x)-q_0(x)g(x)$, 因此 $r_0(x)$ 能表示为 $f(x)$ 和 $g(x)$ 的线性组合

$$r_0(x)=\alpha_0(x)f(x)+\beta_0(x)g(x),$$

这里 $\alpha_0(x)=1,\beta_0(x)=-q_0(x)$ 都是$\mathbb{F}[x]$ 中多项式. 代入下一个方程有

$$\begin{aligned}
r_1(x)&=g(x)-r_0(x)q_1(x)=g(x)-(\alpha_0(x)f(x)+\beta_0(x)g(x))q_1(x)\\
&=\alpha_1(x)f(x)+\beta_1(x)g(x),
\end{aligned}$$

其中 $\alpha_0(x),\beta_0(x)\in\mathbb{F}[x]$. 重复上述过程, 最后有

$$r_n=\alpha_n(x)f(x)+\beta_n(x)g(x).$$

其中 $\alpha_n(x),\beta_n(x)\in\mathbb{F}[x]$. 乘以一个常数 α, 使得 $\alpha r_n(x)$ 为首一多项式. 综上所述, 有

定理 2.35 (多项式的Bezout 公式) 设 $f(x), g(x) \in \mathbb{F}[x]$ 且不全为零.

(i) 存在 $\alpha(x), \beta(x) \in \mathbb{F}[x]$, 使得

$$\alpha(x)f(x) + \beta(x)g(x) = (f(x),\ g(x)),$$

(ii) $f(x),\ g(x)$ 互素当且仅当存在 $\alpha(x), \beta(x) \in \mathbb{F}[x]$, 使得

$$\alpha(x)f(x) + \beta(x)g(x) = 1.$$

由多项式的 Bezout 公式, 可直接得到下列结果:

定理 2.36 设 $f(x), g(x), h(x) \in \mathbb{F}[x]$.

(i) 若 $\tilde{d}(x) \mid f(x),\ \tilde{d}(x) \mid g(x)$, 则 $\tilde{d}(x) \mid (f(x), g(x))$;

(ii) 若 $(f(x), g(x)) = 1,\ (f(x), h(x)) = 1$, 则 $(f(x), g(x)h(x)) = 1$.

证明 因 $(f(x),\ g(x)) = \alpha(x)f(x) + \beta(x)g(x)$, 所以(i) 成立. 对于 (ii), 由条件存在 $\alpha_1(x), \beta_1(x), \alpha_2(x), \beta_2(x) \in \mathbb{F}[x]$, 使得

$$\alpha_1(x)f(x) + \beta_1(x)g(x) = 1,$$
$$\alpha_2(x)f(x) + \beta_2(x)h(x) = 1,$$

则

$$(\alpha_1\alpha_2 f + \alpha_1\beta_2 h + \alpha_2\beta_1 g)f(x) + \beta_1\beta_2 gh = 1,$$

所以(ii) 成立. □

2° 多项式的可约性和因式分解

定义 2.37 一个系数属于域 $\mathbb{F}$ 的多项式 $p(x) \in \mathbb{F}[x]$, 如果能够分解成两个系数属于同一域 $\mathbb{F}$ 非平凡多项式$p_1(x), p_2(x)$ 的乘积 (因式分解):

$$p(x) = p_1(x)p_2(x),$$

那么就称 $p(x)$ 是***域*** $\mathbb{F}$ ***上可约多项式***, 否则称为***域*** $\mathbb{F}$ ***上不可约多项式***.

例 2.8.1 注意到, 可约或不可约与多项式系数所在域密切相关. 例如:

$x^2 - 4$ 在 $\mathbb{Q}$ 上是可约的:$x^2 - 4 = (x - 2)(x + 2)$.

$x^2 - 2$ 在 $\mathbb{Q}$ 上不可约, 但在 $\mathbb{R}$ 上可约: $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$.

$x^2 + 1$ 在 $\mathbb{R}$ 上不可约, 但在 $\mathbb{C}$ 上可约: $x^2 + 1 = (x - \mathrm{i})(x + \mathrm{i})$

随着系数所在范围的扩大

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C},$$

可约性也在发生变化. $\mathbb{F}$ 上不可约多项式在 $\mathbb{F}[x]$ 中的作用与素数在 $\mathbb{Z}$ 的作用相似.

引理 2.38 (Euclid 引理) 设 $f(x), g(x) \in \mathbb{F}[x]$, $p(x)$ 是 $\mathbb{F}$ 上不可约多项式, $p(x) \mid f(x)g(x)$, 则 $p(x) \mid f(x)$ 或 $p(x) \mid g(x)$.

证明 若 $p(x) \nmid f(x)$, $p(x) \nmid g(x)$, 则 $(p(x), f(x)) = 1$, $(p(x), g(x)) = 1$. 根据定理2.36, 有 $(p(x), f(x)g(x)) = 1$, 矛盾. □

如同整数可以分解为素数的乘积一样, $\mathbb{F}[x]$ 中任何一个多项式可以分解为 $\mathbb{F}$ 上不可约多项式的乘积.

定理 2.39 设 $\mathbb{F}$ 是一个域, 则

(i) $\mathbb{F}[x]$ 中有无穷多个首项系数为 *1* 的不可约多项式.

(ii) $\mathbb{F}[x]$ 中任何多项式 $f(x)$ 可唯一分解为不可约多项式的乘积:

$$f(x) = \alpha p_1^{m_1}(x) \cdots p_r^{m_r}(x),$$

这里 $\alpha \in \mathbb{F}$, $p_1(x), \cdots, p_r(x)$ 是 $\mathbb{F}[x]$ 中首项系数为 *1* 的不可约多项式, $m_1, \cdots, m_r$ 表示重数.

关于(i), 对包含无穷多个数的域 $\mathbb{F}$ 情形, 如 $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ 等, 是非常简单地, 因为对任意的 $a \in \mathbb{F}$, 一次式 $x - a \in \mathbb{F}[x]$ 都是不可约的, 因此有无穷多个. 但是对只有有限个元素的域, 如 $\mathbb{Z}_p$ (p 是素数), 情况就比较复杂, 在此就不讨论了.

关于(ii), 可仿照整数的素因子分解唯一性的证明, 从多项式的 Bezout 公式, 导出多项式最大公因式的基本性质即可证得.

3° 多项式的根

本节只需用到加减和乘法运算, 不需要作除法, 因此用 $\mathbb{D}$ 表示$\mathbb{Z}$ 或域 $\mathbb{Q}, \mathbb{R}$ 及 $\mathbb{C}$.

定义 2.40 设 $f(x) \in \mathbb{D}[x]$, 若元素$a \in \mathbb{D}$ 满足 $f(a) = 0$, 则称 a 是 $f(x)$ (在 $\mathbb{D}$ 上) 的**根**或**零点**. 有时也称 a 为方程 $f(x) = 0$ 在在 $\mathbb{D}$ 上的根.

定理 2.41 设 $f(x) \in \mathbb{D}[x]$, 则

(i) $a \in \mathbb{D}$ 是 $f(x)$ 的根当且仅当 $(x - a) \mid f(x)$.

(ii) $a_1, a_2, \cdots, a_m$ 是 $f(x)$ 不同的根当且仅当 $(x - a_1) \cdots (x - a_m) \mid f(x)$.

证明 (i): 根据多项式带余除法, 以 $x - a$ 除 $f(x)$, 得

$$f(x) = q(x)(x - a) + r(x),$$

这里 $q(x), r(x) \in \mathbb{D}[x]$, 而 $\deg r(x) < \deg(x - a) = 1$, 因此 $r(x) = r$. 将 $x = a$ 代入上式得 $r = f(a)$ 以及

$$f(x) = q(x)(x - a) + f(a).$$

这样定理中两个方面都得到证明.

(ii): 设 $a_1, a_2, \cdots, a_m$ 是 $f(x)$ 不同的根, 当 $m = 1$ 即是(i) 的情形; 假设结论对 $m-1$ 已经成立, 则有

$$f(x) = (x - a_1) \cdots (x - a_{m-1})q(x),$$

其中 $q(x) \in \mathbb{D}[x]$, 在上式中代入 $x = a_m$, 得

$$(a_m - a_1) \cdots (a_m - a_{m-1})q(a_m) = 0,$$

因为 $a_m - a_i \neq 0,\ i = 1, \cdots, m-1$, 所以 $q(a_m) = 0$, 也就是 a_m 是多项式 $q(x)$ 的根, 根据(i), 有 $q(x) = (x - a_m)h(x)$, 其中 $h(x) \in \mathbb{D}[x]$, 于是就有

$$f(x) = (x - a_1) \cdots (x - a_{m-1})(x - a_m)h(x).$$

反之显然. □

推论 2.42 设 $\mathbb{F}$ 是域, $f(x) \in \mathbb{F}[x]$ 是不可约多项式当且仅当 $f(x)$在 $\mathbb{F}$ 上没有根.

推论 2.43 $\mathbb{D}[x]$ 中 n 次多项式至多只有 n 个不同的根; 若至少有 $n+1$ 个不同根, 则该多项式一定是零多项式.

下面讨论重根问题.

定义 2.44 设 $f(x) \in \mathbb{D}[x]$, $a \in \mathbb{D}$ 是 $f(x)$ 的一个根, 如果 $f(x)$ 能被 $(x-a)^r$ 整除, 但不能被 $(x-a)^{r+1}$ 整除, 则称正整数 r 为根 a 的***重数***, 当 $r = 1$ 时, 称 a 为 $f(x)$ 的***单根***; 当 $r > 1$ 时, 称 a 为 $f(x)$ 的 r 重***重根***.

定理 2.45 设 $f(x) \in \mathbb{D}[x], \deg f(x) = n$,

(i) 若 a 是$f(x)$ 的 r 重根, 则存在 $q(x) \in \mathbb{D}[x]$, 使得

$$f(x) = (x - a)^r q(x),\ q(a) \neq 0.$$

(ii) 若 $f(x)$ 有 s 个不同的根 $a_1, a_2, \cdots, a_s$, 重数分别是 $r_1, r_2, \cdots, r_s$, 且 $r_1 + r_2 + \cdots + r_s = n$,则

$$f(x) = \alpha(x - a_1)^{r_1}(x - a_2)^{r_2} \cdots (x - a_s)^{r_s}.$$

其中 $\alpha \in \mathbb{D}$.

证明 (i) 中 $f(x) = (x-a)^r q(x)$ 是显然的. 若 $q(a) = 0$, 则 $q(x) = (x-a)q_1(x)$, 因此 $f(x) = (x-a)^{r+1}q_1(x)$, 这与 a 是 $f(x)$ 的 r 重根矛盾.

关于(ii) 的证明如下. 首先由(i) 得

$$f(x) = (x - a_1)^{r_1} q(x),\ q(a_1) \neq 0.$$

同时注意到 $f(x)$ 的其它根也是 $q(x)$ 的根, 因此归纳即可征得结论. □

第 2 讲习题

1. 设 $n>1$ 为整数, 如果对于任何整数 m, 或者 $n|m$, 或者 $(n,m)=1$, 那么 n 必定是素数.

2. 设 n 为正整数, 且 $n\geqslant 2$. 如果对任何不超过 $\sqrt{n}$ 的素数都不能整除 n, 那么 n 一定是素数.

3. (1) 若整数 a 被 6 整除的余数是$r, 0\leqslant r<6$. 则 a^3 被 6 整除的余数也是 r.
(2) 设 $a_1,a_2,\cdots,a_n$ 是整数. 若 $a_1+a_2+\cdots+a_n$ 能被 6 整除, 则 $a_1^3+a_2^3+\cdots+a_n^3$ 也能被 6 整除.

4. 设正整数 $n>2$, 证明: 在 n 和 $n!$ 之间一定存在素数.

5. 求正整数 n, 使得 2^n+16 为完全平方数.

6. 设 $m=m_1m_2,\ (m_1,m_2)=1$, 其中m_1,m_2 是正整数. 证明

$$m\mid n \ \text{ 当且仅当 } \ m_1\mid n,\ m_2\mid n.$$

若 $(m_1,m_2)>1$, 试举例说明结论不成立.

7. 考虑正整数的素因子标准分解

$$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$$

这里 $p_1,\cdots,p_k$ 是两两不同的素数, $\alpha_1,\cdots,\alpha_k$ 是对应素因子的重数.
证明: n 的所有因子 (即能整除 n 的数, 包括 n 和 1) 是这样的数

$$m=p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k}$$

其中 $0\leqslant\beta_i\leqslant\alpha_i,\ i=1,2,\cdots,k$. 而且$n$ 所有不同因子 (包括 n 和 1) 的个数为

$$(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_k+1).$$

例如

$$144=2^43^2,$$

的所有因子共 $5\cdot 3$ 个, 具体为

$$1,2,4,8,16,3,6,12,24,48,9,18,36,72,144$$

8. 如果把自然数看成是一个等差的 (无穷) 数列, 那么定理2.12表明, 该数列中有无穷多个素数. 试证明下列等差数列

$$4n+3,\ n=1,2,3,\cdots,$$

中也有无穷多个素数.

提示: 任何大于 2 的素数一定是奇数, 因而一定是 $4n+1$ 或 $4n+3$ 这种形式. 假设只有有限个 $4n+3$ 形式的素数 $p_1, p_2, \cdots, p_r$, 考虑

$$N = 4(p_1 p_2 \cdots p_r) - 1 = 4(p_1 p_2 \cdots p_r - 1) + 3.$$

类似定理2.12的证明, 以及利用两个 $4n+1$ 形式的数相乘还是 $4n+1$ 形式的数的结论推出假设是错误的.

9. 对互素的两个数 $15, 7$, 求出整数 k, l 使得 $15k + 7l = 1$.

10. 求 $a = \underbrace{11\cdots1}_{50}$ 被 7整除的余数.

提示: 利用 $b = 111111$ 能被 7 整除的结果.

11. 求 2014^{2015} 被 13 整除的余数.

12. 证明: $30 \mid (n^{19} - n^7)$, 其中 n 是任意正整数.

13. 设正整数 $n = a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_0$ $(0 \leqslant a_n, a_{n-1}, \cdots, a_0 \leqslant 9)$, 证明: $11 \mid n$ 当且仅当 $11 \mid ((-1)^n a_n + (-1)^{n-1} a_{n-1} + \cdots + (-1)a_1 + a_0)$

提示: 不难发现: 模 11 有

$$[10^{2k}] = [(99+1)^k] = [1],\ [10^{2k+1}] = [10^{2k}][10] = [1][10] = [10],$$

另一方面, 利用同余类加法有

$$[10] + [1] = [0].$$

14. 设 p, q 是两个不同的素数, a 是一个整数, 且

$$a^{p-1} \equiv 1 \pmod{q},\ a^{q-1} \equiv 1 \pmod{p},$$

证明: $a^{pq} \equiv a \pmod{pq}$

15. 求解同余方程组

$$x \equiv 1 \pmod{4},\ x \equiv 2 \pmod{5},\ x \equiv 4 \pmod{7}.$$

16. 求有理系数多项式 $\alpha(x),\ \beta(x)$, 使得

$$x^3\alpha(x) + (1-x)^2\beta(x) = 1.$$

17. (1) 试证明: 首一的整系数代数方程

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \quad (a_{n-1}, \cdots, a_1, a_0 \in \mathbb{N})$$

的根如果是有理数, 则只能是整数.

(2) 试求 $x^4+5x^3+2x^2-10x+6=0$ 的整数根.

提示: 反证法, 若有理根为 $x=\dfrac{p}{q}$, $q\neq 1$, 推出 $-\dfrac{p^n}{q}$ 为整数, 矛盾. 其次证明方程的整数根一定能够整除 a_0, 因此对具体方程, 只要将零次项系数 a_0 进行素因子分解, 给出可能的整数根, 并逐一验证即可得到 *(2)* 中方程的整数根.

18. 设 m,n 是正整数, 证明 $\mathbb{F}[x]$ 上多项式 x^m-1 与 x^n-1 的最大公因式为 $x^{(m,n)}-1$. 即

$$(x^m-1,\ x^n-1)=x^{(m,n)}-1.$$

提示: 不妨设 $m>n$, 利用整数 m 和 n 的带余除法 $m=qn+r$, $0\leqslant r<n$, 有

$$x^m-1=x^{qn+r}-x^r+x^r-1=x^r(x^{nq}-1)+(x^r-1).$$

因为 $x^n-1|x^{nq}-1$, 所以得到多项式 x^m-1 和 x^n-1 对应的带余除法

$$x^m-1=q(x)(x^n-1)+(x^r-1).$$

再利用 m 和 n 的 *Euclid* 辗转相除法以及对应 x^m-1 和 x^n-1 的多项式的辗转相除法即可证得.

第 3 讲　实数

对实数的认识, 甚至包括无理数, 可追述到古希腊时代, 但真正把实数系构建起来还是十九世纪的事情. 随着微积分学的严格化, 极限理论逐步建立, 也使得实数理论日臻完善. 主要以 Weierstrass（魏尔斯特拉斯, 1815 - 1897）,Cantor（康拓, 1845 -1918）和 Dedekind（戴德金, 1831-1916）的工作最具代表性. 本专题只介绍 Dedekind 的方法, 其它方法构造出的实数系与 Dedekind 方法构造的实数系本质上是等价的.

§3.1　有理数域

自然数是从计算集合（如一群羊,一篮苹果）元素个数过程中抽象出来的. 在实际生活中, 不仅要计数还需要进行如长度、面积、时间、重量等度量.为了把度量问题变为计数问题, 首先要选择一个度量单位, 也就是度量标准, 如公尺、亩、小时、斤等等, 然后看被度量的量包含多少个单位.比如一段距离正好是15个公尺, 那么这个距离就是15公尺.

但是, 往往出现这样的情况,计算一段距离的单位个数未必恰到好处,可能会出现15个公尺还多一点,16个公尺又不够情况. 那么只有把原有单位分成 n 等分,引进新的更小单位继续度量,例如 1 公尺分为 100厘米,1 亩分为10分,1小时分为60分钟, 还有我国古代把1 斤分为 16 两等等. 继续丈量的结果就是1公尺39厘米,1小时18分钟,1亩半（5分）或古制的 1 斤 12 两等等.

如果把原单位确定为 1, 那么再等分就是 $\frac{1}{n}$, 如果一个量正好等于小单位 $\frac{1}{n}$ 的 m 倍,那么它的度量用 $\frac{m}{n}$ 表示. 显然 n 个 $\frac{1}{n}$ 就是 1.

这些量之间也可以做加法, 仍以长度为例,把长度单位分成 3 分,一段距离的长度正好等于2个 $\frac{1}{3}$, 即 $\frac{2}{3}$. 若把长度单位分成 4 分, 另一个距离正好为 3个 $\frac{1}{4}$, 为了把两个距离相加,我们把长度单位分成 12 分（3 和4 的倍数,相当于把 $\frac{1}{3}$ 分成 4分,把 $\frac{1}{4}$ 分成3分）,那么第一段距离就是8个 $\frac{1}{12}$,而第二段距离就是9 个 $\frac{1}{12}$,两者相加就是 17个 $\frac{1}{12}$,因为12个 $\frac{1}{12}$ 等于一个单位,所以总距离为 1 个单位又 5 个 $\frac{1}{12}$.用数学式子表示就是

$$\frac{2}{3}+\frac{3}{4}=\frac{8+9}{12}=\frac{17}{12}=1+\frac{5}{12}.$$

把这些量抽象出来（也就是抛开公尺、亩、小时、斤等具体度量,如同在计数时抛开是羊还是苹果一样）,就产生了两个正整数之比,也就是分数 $\frac{m}{n}$, 其中 m,n 是正整数（m 可以是 0, 但 $n\neq 0$, 因为把一个单位分成 0 等分是没有意义的）.

把上述从实际度量中抽象出来的正整数之比扩大到所有整数之比也就产生了由分数表示的**有理数**, 记为

$$\mathbb{Q}=\left\{\frac{m}{n}\;\middle|\; m,n\in\mathbb{Z},\ n\neq 0\right\}.$$

这里 $\mathbb{Z}$ 表示所有整数集合 (见第2讲) 显然,它包含了所有整数 (即$n=1$ 的分数) .

1° 有理数的算术

定义有理数之间的加法和减法:

$$\frac{m}{n}\pm\frac{m'}{n'}=\frac{mn'\pm nm'}{nn'},$$

以及乘法:

$$\frac{m}{n}\cdot\frac{m'}{n'}=\frac{mm'}{nn'},$$

不难验证这些运算如同整数一样满足交换律、结合律以及乘法对加法的分配律. 与整数不同的是,有理数之间可以做除法,或者说任何一个非零的有理数$\dfrac{m}{n}\in\mathbb{Q},\ m\neq 0$, 一定有逆元

$$\left(\frac{m}{n}\right)^{-1}=\frac{n}{m}\in\mathbb{Q},\ \text{满足}\ \frac{m}{n}\cdot\frac{n}{m}=1,$$

这样两个有理数的除法为

$$\frac{m}{n}\div\frac{m'}{n'}=\frac{m}{n}\cdot\left(\frac{m'}{n'}\right)^{-1}=\frac{mn'}{nm'}\in\mathbb{Q}.$$

2° 有理数的序

根据整数的序, 可按如下方式定义有理数之间序 (或大小)

$$\frac{m}{n}-\frac{m'}{n'}=\frac{mn'-nm'}{nn'}\begin{cases}>0, & \text{当 } mn'-nm' \text{ 与 } nn' \text{ 同号},\\ =0, & \text{当 } mn'-nm'=0,\\ <0, & \text{当 } mn'-nm' \text{ 与 } nn' \text{ 异号}.\end{cases}$$

这样, 对任意两个有理数 $a,b\in\mathbb{Q}$, 三种情况: $a<b,\ a=b, a>b$ 有且仅有一种成立, 而且若 $a<b,\ b<c$, 则 $a<c$.

有理数的序与有理数的加法和乘法是相容的, 也就是若 $a<b$, 那么 $a+c<b+c$ 对任何 $c\in\mathbb{Q}$ 成立, 若 $a>0, b>0$, 则 $ab>0$.

3° 有理数的几何解释

在直线 L 上任取一点为原点 O, 再将任意一点取作 1 (习惯上取在 O 的右边), 以两点之间距离为度量的尺度或单位 (这样就有了数轴),如果从原点开始, 依单位长度往

正向逐次丈量, 就得到自然数在数轴上对应点 ,同理往原点左侧的丈量得到负整数对应点.

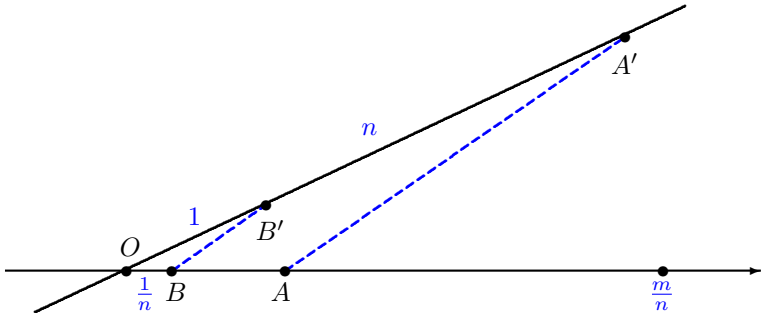


图 3.1

为描述有理数对应的点, 就要把单位进行等份, 几何上可以这么做: 设数轴上 1 对应的点为 A, 过原点作一条异于数轴直线 L', 对任意自然数 $n>1$,在 L' 上取点 A', B' 满足 $OA'=n$, $OB'=1$,过点 B' 作线段 AA' 平行线, 交数轴于 B 点,则 $OB=\dfrac{1}{n}$. 利用 OB 作为新的尺度逐次丈量 m 次, 就得到 $\dfrac{m}{n}$. 因此可以在数轴上表出所有有理数(图3.1) . 把有理数对应数轴上的点称为有理点,并不再区分有理数还是有理点.

4° 有理数的稠密性

有理数是“处处稠密”的, 即任何两个有理数 a 和 b 之间必然存在无穷多个有理数.

不妨设 $a<b$, 显然有理数 $c=\dfrac{a+b}{2}$ 满足 $a<c<b$, 对 a, c 和 c, b 不断重复这个过程就会发现 a 和 b 之间有无穷多个有理数.

总之,引进有理数以后,在实际问题中使得度量长度、面积、时间、重量等等变得更加精细.

从数学上看, 有理数不但保持了整数所有算术性质,对加法和乘法满足的交换律、结合律和分配律, 同时还具有乘法的逆运算(或者说任何非零的有理数都有逆元), 满足这些规律的集合称为**域**.

远在古希腊时代,人们就已经掌握了有理数的这些性质. 以Pythagoras (毕达哥拉斯, 约公元前580 -约前500) 为代表的学派认为, 数(就是整数和整数之比,也就是有理数) 不但用来计数、丈量,甚至所有的音阶都可以用数来表示.他们甚至把数上升到哲学层面, 提出“数是万物之源”, “数是万物的本质”,并赋予了诸如 $1, 2, 3, \cdots$ 等数以“灵性”.

§3.2 可公度与不可公度

设有两个线段 a 和 b, 如果 b 的长度是 a 长度的正整数 m 倍,那么可以用 a 作为 b 的度量, 即 $b = ma$. 当 b 不等于 a 的整数倍时, 如果存在正整数 n, 使得 a 分为 n 等分后, b 恰好是等分长度 $\frac{a}{n}$ 的 m 倍, 那么

$$b = \frac{m}{n}a.$$

因此 a 和 b 长度之比是一个有理数. 或者说 a 和 b 有一个公共度量 $\frac{a}{n}$, 它的 n 倍等于 a, 而它的 m 倍等于 b, 称 a 和 b 是**可公度的**,**或可通约的**, 否则称为**不可公度的或不可通约的**.

显然, 可公度性具有传递性: 若 a 和 b 可公度, b 和 c 可公度, 则 a 和 c 可公度.

如果选 a 为单位线段 ($a = 1$), 则与之可公度的线段对应数轴上的有理点.

随后, 人们就发现了与单位线段不可公度的线段 (图3.2), 这就是边长为一的正方形 (称为 “单位正方形”) 的对角线. 设单位正方形对角线长度为 x, 则根据勾股定理

$$x^2 = 1^2 + 1^2 = 2.$$

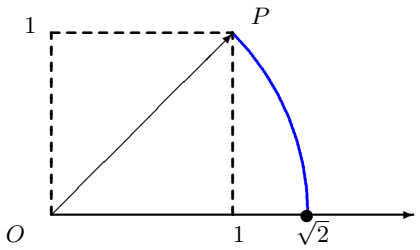


图 3.2

定理 3.1 *单位正方形对角线线段与单位线段不可公度, 也就是不存在有理数满足* $x^2 = 2$.

证明 采用反证法. 假如存在两个正整数 m, n, 使得

$$x = \frac{m}{n},\ (m, n) = 1.$$

因此

$$2 = x^2 = \frac{m^2}{n^2},$$

由此推出 $m^2 = 2n^2$, 即 m^2 是偶数, 所以m 自身也是偶数 $m = 2k$, 代入得 $4k^2 = 2n^2$, 又得 n^2 是偶数, 继而 n 是偶数. 这与 $(m, n) = 1$ 相矛盾. □

所以单位正方形对角线长度与 1 之比不再是两个整数之比, 即不再是有理数. 这样使得本来看似完美无瑕、代表万物、具有灵性的有理数家族中突然闯进了一个 “魔鬼” . 人们把那些与 1 不可公度 (当然与所有有理数也不可公度) 的数称为**无理数**.

顺便说一句, “有理数” 的英文的词根是 “ratio” , 即是 “比例” 意思, 与古希腊人定义是相同的, 后来出现了 “rational number” 这个词, 中文翻译为 “有理数” , 把不是有理

数(不能表示为整数之比)的数“irrational number”干脆翻译成了“无理数”, 其实本意与“有理”还是“无理”毫无关系.

定理3.1还表明, 虽然有理数是稠密的, 但有理数之间不“连续”, 也就是有理数之间存在“空隙”. 例如, 把有理数 $\mathbb{Q}$ 分成两组

$$X = \{x \mid x \in \mathbb{Q}, x < 0; \text{ 或 } x^2 < 2, x > 0\},$$
$$Y = \{y \mid y \in \mathbb{Q}, y^2 > 2, y > 0\},$$

则, 在两组有理数之间, 不存在有理数. 进一步发现, 虽然 X “上面封顶”, Y “下面有底”, 但是

定理 3.2 *对于上述两组有理数, X 在 $\mathbb{Q}$ 中无最大数, Y 在 $\mathbb{Q}$ 中无最小数. 也就是说 X 中没有最大的有理数, Y 中没有最小的有理数.*

证明 设 $a \in \mathbb{Q}$, 且 $a > 0$, 令

$$a' = a - \frac{a^2 - 2}{a + 2} = \frac{2a + 2}{a + 2},$$

则 a' 是有理数, 而且

$$a'^2 - 2 = \frac{2(a^2 - 2)}{(a + 2)^2}.$$

若 $a \in X$, 则 $a^2 - 2 < 0$, 推出 $a' > a$, 且 $a'^2 - 2 < 0$, 即 $a' \in X$. 因此对任何 X 中的有理数 $a > 0$, 在 X 中一定还存在比 a 大的有理数 $a' \in X$, 也就是说 X 中不存在最大有理数.

若 $a \in Y$, 则 $a^2 - 2 > 0$, 推出 $a' < a$, 且 $a'^2 - 2 > 0$, 即 $a' \in Y$, 所以任何 Y 中的有理数 a, 必存在比 a 小的有理数 $a' \in Y$, 也就是说 Y 中不存在最小有理数. □

有理数的不连续性或者说有理数之间存在空隙这一缺憾, 正是需要弥补的, 而填满这些空隙的就是无理数.只有这样才能使微积分建立在坚实的数的基础上. 同时还将看到, 有理数空隙的“数量”远远多于有理数.

§3.3 实数域

如果说从整数扩充至有理数是从测量等直观思想出发, 那么要将有理数系扩展到连续的、没有空隙的数系, 这种直观思想就不够了. 另一种想法是从有理数系算术运算等规则出发, 通过补充一些要求, 达到扩展目的.

1° 实数域的定义

首先, 抽象地给出下列一系列定义.

(1) 域

定义 3.3 设 F 是一个集合, 它具有加法和乘法运算, 若这些运算满足下列公理, 则称 F 为域

加法: 对任意 $x, y \in F$, 可定义 $x + y \in F$. 加法运算满足

(i) 有零元 0: 且 $x + 0 = 0 + x = x$.

(ii) 有负元: 对每个 $x \in F$, 有 $-x \in F$, 且 $x + (-x) = -x + x = 0$.

(iii) 交换律: $x + y = y + x$.

(iv) 结合律: $x + (y + z) = (x + y) + z$.

乘法: 对任意 $x, y \in F$, 可定义 $x \cdot y \in F$ 且满足

(i) 有单位元 1: 且 $1 \cdot x = x \cdot 1 = x$.

(ii) 有逆元: 对任意的 $x \in F$, $x \neq 0$, 有 $x^{-1} \in F$, 使得 $x \cdot x^{-1} = x^{-1} \cdot x = 1$.

(iii) 交换律: $x \cdot y = y \cdot x$.

(iv) 结合律: $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

(v) 分配律: $(x + y) \cdot z = x \cdot z + y \cdot z$.

(2) 序

定义 3.4 设 S 是一个集合 , 若 S 上可定义一种关系, 记为 $<$, 满足

(i) 对任意的 $x, y \in S$, 有 $x < y$, $x = y$, $y < x$ 有且仅有一种成立

(ii) 对任意的 $x, y, z \in S$, 若 $x < y$, $y < z$, 那么 $x < z$, 即满足传递性.

定义了“序”的集合称为有序集.

有时也用 $y > x$ 代替 $x < y$, 用 $x \leqslant y$ 表示 $x < y$ 或 $x = y$, 也就是对 $y < x$ 的否定.

(3) 有序域

定义 3.5 若集合 F 既是一个域, 又是有序集, 还满足如下条件:

(i) 当 $x, y, z \in F$, 且 $y < z$ 时, 有 $x + y < x + z$;

(ii) 当 $x, y \in F$, 且 $x > 0$, $y > 0$, 则 $xy > 0$.

则称 F 是有序域.

从有序域的定义, 可直接推出一些简单性质, 下面列出其中主要的两条:

性质 3.6 设 F 是一个有序域, $x \in \mathbb{F}$,

(i) 若 $x > 0$, 则 $x + (-x) > 0 + (-x)$, 得 $-x < 0$. 反之亦然;

(ii) 若 $x \neq 0$, 则 $x^2 > 0$ *(即任意非零元的平方一定大于 0).*

不难验证有理数集 $\mathbb{Q}$ 满足以上三个定义, 因此有理数集是有序域. 正如定理3.2所揭示的那样, 有理数是不连续的, 也就是有理数之间存在空隙. 为了定义一个集合, 使之既能继承有理数的性质, 又能是一个连续的、没有空隙的数集, 特给出如下的确界原理.

(4)确界原理

首先对有序集, 引进所谓“界”的概念.

定义 3.7 设 S 是有序集, $E \subset S$,

(i) 若存在 $\alpha \in S$, 使得对任意 $x \in E$, 有 $x \leqslant \alpha$, 则称 E 有上界, α 为 E 的一个上界. 同理定义下界.

(ii) 若 $\alpha \in S$ 是 E 的最小上界, 则称 α 为 E 的上确界, 记为 $\alpha = \sup E$. 同理定义下确界$\beta \in S$, 并记为 $\beta = \inf E$.

下面给出在定义实数域中最关键、最本质的确界原理:

定义 3.8 (确界原理) 对有序集 S , 如果对 S 的任意非空子集 E:

(i) 只要 E 有上界, 就在 S 中有上确界, 那么称 S 满足上确界原理.

(ii) 只要 E 有下界, 就在 S 中有下确界, 那么称 S 满足下确界原理.

如果 S 同时满足上、下确界原理, 那么称 S 满足确界原理.

注意, 这里着重强调“在 S 中”就是强调上确界 $\sup E \in S$ 或下确界 $\inf E \in S$.

例 3.3.1 仍然考虑 $\mathbb{Q}$ 的两个子集合

$$X = \{x \mid x \in \mathbb{Q}, x < 0; \text{ 或 } x^2 < 2, x > 0\},$$
$$Y = \{y \mid y \in \mathbb{Q}, y^2 > 2, y > 0\},$$

显然 Y 也是X 在 $\mathbb{Q}$ 中所有上界的集合, X 是 Y 在 $\mathbb{Q}$ 中所有下界的集合. 根据定理3.2, Y 中没有最小数, 所以 X 在 $\mathbb{Q}$ 中没有最小的上界, 即在 $\mathbb{Q}$ 中不存在上确界. 同理 Y 在 $\mathbb{Q}$ 中没有下确界. 因此有理数集 $\mathbb{Q}$ 不满足确界原理.

下列定理说明定义3.8中有序集 S 满足上确界原理和下确界原理彼此是等价的.

定理 3.9 设 S 是有序集, 则 S 满足上确界原理当且仅当 S 满足下确界原理.

证明 不妨设 S 中有上界的子集一定有上确界, 要证明 S 中任意有下界的子集 E, 在S 中有下确界.

设 E 是S 中任意有下界的子集, 记 E 所有下界的集合为

$$E' = \{x \mid x \in S, x \text{ 是 } E \text{ 的下界}\}$$

则 E 中的元素都是 E' 的上界, 因此 E' 有上确界: $\alpha = \sup E' \in S$, 也就是最小上界. 所

以对任意的 $x \in E$, 有 $\alpha \leqslant x$, 这样就推出 α 是E 的一个下界.

设 $\beta \in S$ 是 E 的任意一个下界, 则 $\beta \in E'$, 推出 $\beta \leqslant \alpha$, 所以 α 是E 的最大下界, 即: $\alpha = \inf E \in S$. 类似可证明 S 满足下确界原理一定也满足上确界原理. □

(5)实数域的定义

通常, 将域、序、有序域和确界原理的定义称为**实数公理**, 同时注意到如果一个集合是有序域, 它自然有域和序的结构. 因此

定义 3.10 满足实数公理的集合, 或满足确界原理的有序域称为实数域, 记为 $\mathbb{R}$, 其中元素称为实数.

注记 在实数公理中, 有时用下列连续(完备)性公理替代确界原理. 事实上两者是完全等价的. 本专题采用确界原理主要是为了后续的推导方便.

所谓连续(完备)性公理的定义如下:

定义 3.11 设 S 是有序集, 如果对 S 中任意两个非空子集 X 和 Y, 只要满足

$$x \leqslant y, \quad x \in X, \ y \in Y,$$

就一定存在 $c \in S$, 使得

$$x \leqslant c \leqslant y.$$

那么称 S 满足连续(或完备)性公理.

定理 3.12 有序集S 满足连续性公理, 当且仅当 S 满足确界原理.

证明 对 S, 若连续性公理成立, 对任何非空有上界集合 $X \subset S$, 令

$$Y = \{y \mid y \in S \text{ 是 } X \text{ 的上界}\},$$

因此对任意的 $x \in X$, $y \in Y$, 有 $x \leqslant y$. 根据连续性公理, 一定存在 $c \in S$, 使得对任意的 $x \in X$, $y \in Y$, 有 $x \leqslant c \leqslant y$. 第一个不等式说明 c 是X 的上界, 第二个不等式说明 c 是X 的最小上界, 因此 X 的上确界存在 $c = \sup X$, 由定理*3.9*, S 满足确界原理.

反之, 若 S 满足确界原理, 那么任取两个非空子集X 和 Y, 它们满足对于任何 $x \in X$, $y \in Y$, 有 $x \leqslant y$. 则 Y 中的任何元素都是 X 的上界. 根据确界原理, X 在 S 中有上确界, 记为 $c = \sup X$, $c \in S$. 作为 X 中最小上界, 有 $x \leqslant c \leqslant y$ 对任意的 $x \in X$, $y \in Y$ 成立, 因此 S 满足连续性公理. □

2° 实数域及其性质

在给出了实数一系列抽象定义后, 下面的定理是本专题的核心, 它说明满足实数公理的实数域是存在的.

定理 3.13 实数域 $\mathbb{R}$（即满足确界原理的有序域）是存在的. 并包含有理数域 $\mathbb{Q}$ 作为子域.

证明过程实际上是一个构造实数域过程. 在本专题最后一节, 将介绍 Dedekind 的构造方法.

例 3.3.2 在实数域 $\mathbb{R}$ 中, 存在唯一的正实数满足 $x^2 = 2$. 此数记为 $x = \sqrt{2}$.

证明 设 $E = \{x \mid x^2 < 2,\ x > 0\}$ 是 $\mathbb{R}$ 中非空有上界的子集合, 因为 $\mathbb{R}$ 满足确界原理, 因此 E 有上确界 $\alpha = \sup E \in \mathbb{R}$.

若 $\alpha^2 < 2$, 令

$$\alpha' = \alpha - \frac{\alpha^2 - 2}{\alpha + 2} = \frac{2\alpha + 2}{\alpha + 2},$$

于是

$$\alpha' > \alpha,\ \alpha'^2 - 2 = \frac{2(\alpha^2 - 2)}{(\alpha + 2)^2} < 0.$$

也就是 $\alpha' \in E$, 但 $\alpha' > \alpha$, 这与 $\alpha = \sup E$ 矛盾. 同理也可排除 $\alpha^2 > 2$, 因此只能有 $\alpha^2 = 2$. 唯一性则是显然的, 因为对任意的 $0 < x_1 < x_2$, 根据序公理的性质有 $x_1^2 < x_2^2$, 因此不可能同时等于 2. □

实数域 $\mathbb{R}$ 有两个特点：一是几何上看, 实数与数轴上的点 1-1 对应. 因此“实数”和“点”不再区分, 或称数是点的坐标. 整数、有理数、无理数对应的点分别称为“整数点”、“有理点”和“无理点”. 二是 $\mathbb{R}$ 以及无理数的集合都是不可数的（见第 1 讲定理1.17 ）.

除了上述特点, 实数域还有下列重要性质.

定理 3.14 实数域 $\mathbb{R}$ 满足

(i) *Archimedes*（阿基米德, 公元前*287*年-公元前*212*年）性：若 $x, y \in \mathbb{R}$ 且 $x > 0$, 则一定存在最小整数 n, 使得

$$(n-1)x \leqslant y < nx.$$

若 $y > 0$, 则 $n > 0$. 若 $x = 1$, 则对任意实数 y, 一定存在整数 n, 使得

$$n - 1 \leqslant y < n.$$

(ii) 有理数在实数中的稠密性：若 $x, y \in \mathbb{R}$ 且 $x < y$, 则一定存在 $c \in \mathbb{Q}$, 使得

$$x < c < y.$$

证明 对任意 $x > 0$, 设 $E = \{nx \mid n \in \mathbb{Z}\}$, 假如 y 是 E 上界, 那么 E 在 $\mathbb{R}$ 中一定有上确界 $\alpha = \sup E \in \mathbb{R}$. 因为 $x > 0$, 所以 $\alpha - x$ 不是 E 的上界, 也就是存在整数 m, 使得 $mx \in E$, $\alpha - x < mx$, 这样就有 $\alpha < (m+1)x \in E$, 这与 α 是上确界矛盾. 推得 y 不是 E 的上界, 推因此一定存在 $n_1 \in \mathbb{Z}$, 使得 $n_1 x > y$.

将上述结果应用到 $x>0$ 和 $-y\in\mathbb{R}$ 上, 则存在 $n_2\in\mathbb{Z}$, 使得 $n_2x>-y$. 两者结合起来, 就是存在 $n_1,n_2\in\mathbb{Z}$, 使得

$$-n_2x<y<n_1x.$$

记

$$S=\{k\mid k\in\mathbb{Z},\ kx>y\},$$

则 S 包含 n_1 因此非空, 同时对 $k\in S$, 有

$$k>\frac{y}{x}>-n_2,$$

即 $-n_2$ 是 S 的一个下界, 根据第 2 讲例2.1.1关于有下界整数集必有最小数的结论, S 中有最小整数 n, 使得

$$(n-1)x\leqslant y<nx.$$

关于(ii) 的证明如下, 由于 $x<y$, 得 $y-x>0$, 对 $y-x$ 和 1, 根据(i), 存在整数 n, 使得

$$n(y-x)>1,\ \text{ 或 }\ ny>nx+1.$$

因 $y-x>0$, 所以 $n>0$ 是正整数. 再对 1 和 nx 利用 (i), 存在整数 m 使得

$$m-1\leqslant nx<m.$$

综合上述不等式, 有

$$nx<m\leqslant nx+1<ny.$$

因 $n>0$, 从而

$$x<\frac{m}{n}<y.$$

□

3° 绝对值

实数的绝对值定义为, 对任意的 $a\in\mathbb{R}$,

$$|a|=\begin{cases}a & \text{当 } a\geqslant 0;\\ -a, & \text{当 } a<0.\end{cases}$$

绝对值满足

(i) 正定性: $|a|\geqslant 0$, 等号成立当且仅当 $a=0$;

(ii) 对称性: $|a-b|=|b-a|$;

(iii) 三角不等式: $|a+b|\leqslant|a|+|b|$.

因此两个数差的绝对值给出对应数轴上点的距离.

§3.4 正实数的指数幂和对数

在实数域 $\mathbb{R}$ 中, n 个相同实数 a 相乘还是一个实数, 记为 a^n, 正整数 n 称为指数. 本节的目的是将指数推广到一般实数 x, 给出 a^x $(a>0)$ 是一个实数的确切定义.

另一方面, 对给定实数 $a>0, a\neq 1$, 考虑方程 $a^x=y$, 若对任意实数 $y>0$, 方程有唯一的实数解 x, 则称 x 是 y 以 a 为底的对数. 这样就完成了幂函数、指数函数和对数函数的定义.

1° 正实数的指数幂

设 $a>0$, 下面将分别对指数 x 是整数、有理数和实数情形, 依次讨论数 a^x 的确切定义.

(1) 当 $x=n$ 为整数时, 定义 a 的整数次幂如下

$$a^n=\begin{cases}\overbrace{a\cdot a\cdots a}^{n}, & n>0;\\ 1, & n=0;\\ \left(\dfrac{1}{a}\right)^{-n}, & n<0.\end{cases}$$

因此 $a^n\in\mathbb{R}$. 可以验证, 对整数 n,m, 无论正负, 有

$$a^na^m=a^{n+m},\ a^nb^n=(ab)^n,\ a>0,\ b>0.$$

(2) 当 $x=\dfrac{1}{n}$ (n 为正整数) 时, 即要证明正实数 a 的 n 次方根的存在性.

定理 3.15 *对任意实数 $a>0$ 以及任意整数 $n>0$, 存在唯一实数 $y>0$ 满足 $y^n=a$. 称 y 为 a 的 n 次方根, 记为 $y=\sqrt[n]{a}$ 或 $y=a^{1/n}$.*

证明 若存在这样的 y, 显然是唯一的, 因为只要 $0<y_1<y_2$, 就有 $y_1^n<y_2^n$, 所以不可能同时等于 a. 下面证明存在性, 设

$$E=\{t\mid t\in\mathbb{R},\ t>0,\ t^n<a\},$$

首先, E 是非空集合: 取 $t_0=\dfrac{a}{1+a}$, 则 $t_0^n<a$, 因此 $t_0\in E$.

其次, E 有上界: 取 $1+a\in\mathbb{R}$, 对任意 $t\in E$, $t^n<a<(1+a)^n$, 推得 $t<1+a$, 所以 $1+a$ 是 E 的一个上界.

根据确界原理, E 在 $\mathbb{R}$ 中存在上确界 $y=\sup E\in\mathbb{R}$. 要证明 $y^n=a$, 只要证明无论是 $y^n<a$ 或是 $y^n>a$ 都会导致矛盾.

假设 $y^n<a$, 取

$$0<h<1,\ \text{且}\ \ h<\frac{a-y^n}{n(y+1)^{n-1}},$$

则

$$\begin{aligned}(y+h)^n-y^n&=h\left((y+h)^{n-1}+(y+h)^{n-2}y+\cdots+y^{n-1}\right)\\&<hn(y+h)^{n-1}<hn(y+1)^{n-1}<a-y^n,\end{aligned}$$

推得 $(y+h)^n<a$, 所以 $y+h\in E$. 但 $y+h>y$, 这与 y 是 E 的上确界矛盾.

假设 $y^n>a$, 取

$$k=\frac{y^n-a}{ny^{n-1}},$$

则 $0<k<y$. 对任意的 $t\geqslant y-k$, 有

$$\begin{aligned}y^n-t^n\leqslant y^n-(y-k)^n&=k\left(y^{n-1}+y^{n-2}(y-k)+\cdots+(y-k)^{n-1}\right)\\&<kny^{n-1}=y^n-a,\end{aligned}$$

所以 $t^n>a$, 即 $t\notin E$, 这就意味着 $y-k$ 是 E 的一个上界. 但 $y-k<y$, 因此与 y 是 E 的最小上界矛盾. □

推论 3.16 设实数 $a>0,\ b>0$ 或 $a_1>0,\cdots,a_m>0$, 以及整数 $n>0$, 有

$$(ab)^{\frac{1}{n}}=a^{\frac{1}{n}}b^{\frac{1}{n}},\quad (a_1\cdots a_m)^{\frac{1}{n}}=a_1^{\frac{1}{n}}\cdots a_m^{\frac{1}{n}}.$$

只要令 $\alpha=a^{1/n},\ \beta=b^{1/n}$, 就有

$$ab=\alpha^n\beta^n=(\alpha\beta)^n,$$

根据定理3.15 中的唯一性可得 $(ab)^{1/n}=\alpha\beta=a^{1/n}b^{1/n}$. 第二个等式可用归纳法证明.

(3) 当 $x=\dfrac{m}{n},\ (m,n)=1,\ n>0$ 为有理数时, 首先在推论3.16 中, 取 $a_1=\cdots=a_m=a$, 就有

$$(a^m)^{\frac{1}{n}}=\left(a^{\frac{1}{n}}\right)^m,$$

因此, 正实数 a 的有理数的指数幂如下:

$$a^x=(a^m)^{\frac{1}{n}}=\left(a^{\frac{1}{n}}\right)^m\in\mathbb{R},$$

并可证明对任意两个有理数 x,y, 有

$$a^xa^y=a^{x+y},\ (a^x)^y=a^{xy},\ a^xb^x=(ab)^x,\ a>0,b>0.$$

(4) 当 x 是任意实数时, 若 $a>1$, 考虑集合

$$E(x)=\{a^r \mid r\in\mathbb{Q},\ r<x\},$$

那么只要 $r_0>x$ 是有理数, a^{r_0} 就是 $E(x)$ 的上界. 根据确界原理, E 在 $\mathbb{R}$ 中存在上确界, 因此定义

$$a^x=\sup E(x)\in\mathbb{R}.$$

若 $a=1$, 则定义 $a^x=1$.

若 $0<a<1$, 则定义

$$a^x=\left(\frac{1}{a}\right)^{-x}.$$

定理 3.17 *设 a 是正实数, x,y 为任意实数, 则*

$$a^{x+y}=a^xa^y.$$

证明 不妨设 $a>1$. 对任意满足 $r_1<x,\ r_2<y$ 的有理数 r_1,r_2, 有$a^{r_1}\in E(x),\ a^{r_2}\in E(y)$. 因为有理数 $r=r_1+r_2<x+y$, 所以

$$a^{r_1}a^{r_2}=a^r\leqslant\sup E(x+y)=a^{x+y},$$

由$r_1<x,r_2<y$ 的任意性, 推出

$$\sup E(x)\sup E(y)\leqslant\sup E(x+y),\ \text{即}\ a^xa^y\leqslant a^{x+y}.$$

反之, 对任意的有理数 $r<x+y$, 根据有理数的稠密性, 取有理数 r_1 满足

$$x>r_1>x-\frac{x+y-r}{2},$$

令 $r_2=r-r_1$, 则有理数 r_2 满足

$$r_2=r-r_1<r-\left(x-\frac{x+y-r}{2}\right)=\frac{r-x+y}{2}<y.$$

因此

$$a^r=a^{r_1}a^{r_2}\leqslant\sup E(x)\sup E(y)=a^xa^y,$$

根据 $r<x+y$ 的任意性得 a^xa^y 是 $E(x+y)$ 的一个上界, 因此

$$x^{x+y}=\sup E(x+y)\leqslant a^xa^y.$$

因此, 定理中等式成立. □

2° 正实数的对数

在定义了实数 $a>0$ 的任意次幂 $a^x=y$ 后, 现在考虑逆问题.

定理 3.18 设 $a>0,\ a\neq 1$, 对任意的 $y>0$, 方程 $a^x=y$ 有唯一实数解 x, 记为 $x=\log_a y$. 称 x 是 y 以 a 为底的对数, 特别, 以自然常数 e 为底的对数记为 $\ln y$.

证明 方程 $a^x=y$ 若有解, 那么唯一性显然, 这是因为若 $a^{x_1}=a^{x_2}=y$, 根据实数的指数幂的性质, 有 $a^{x_1-x_2}=1$, 因此 $x_1=x_2$.

为了证明解的存在性, 分两种情况讨论.

(1) 当 $a>1$ 时, 因为对任意 $b\in\mathbb{R}$, a^b 是一个实数, 因此令

$$A(y)=\{b\mid b\in\mathbb{R},\ a^b<y\}\subset\mathbb{R}.$$

第一步要证明 $A(y)$ 非空.

若 $y>1$, 只要取正整数 $n>\dfrac{a-1}{y-1}$, 则由不等式 (见本讲习题 8)

$$a-1\geqslant n(a^{\frac{1}{n}}-1)$$

推得 $a^{1/n}<y$, 即 $\dfrac{1}{n}\in A(y)$.

若 $0<y\leqslant 1$, 令 $a=1+\alpha,\ \alpha>0$, 只要取正整数 $n>\dfrac{1-y}{y\alpha}$, 就有

$$a^n=(1+\alpha)^n>1+n\alpha>\frac{1}{y},$$

所以 $a^{-n}<y$, 也就是 $-n\in A(y)$. 无论 $y>1$ 或 $0<y\leqslant 1$, $A(y)$ 非空.

第二步要证明 $A(y)$ 有上界.

因 $a=1+\alpha,\ \alpha>0$, 取正整数 $n>\dfrac{y-1}{\alpha}$, 则 $a^n>1+n\alpha>y$, 所以对任意 $b\in A(y)$, 有

$$a^b<y<a^n,$$

推出 $b<n$, 即 n 为 $A(y)$ 的上界. 根据确界原理 $A(y)$ 在 $\mathbb{R}$ 中有上确界, 记为

$$x=\sup A(y)\in\mathbb{R}.$$

第三步要证明 x 满足方程 $a^x=y$.

为此只要排除 $a^x<y$ 和 $a^x>y$ 即可.

若 $a^x<y$, 令 $y'=ya^{-x}>1$, 根据第一步证明结果, 存在正整数 n, 使得 $\dfrac{1}{n}\in A(y')$, 也就是 $a^{1/n}<y'=ya^{-x}$, 推得 $a^{x+1/n}<y$, 从而 $x<x+\dfrac{1}{n}\in A(y)$, 这与 $x=\sup A(y)$ 相矛盾.

同理可排除 $a^x>y$.

这样当 $a>1$ 时, 就证明了方程 $a^x=y$ 有唯一的实数解 x. 也就是对实数 $y>0$, 定义了y 的对数 $x=\sup A(y)=\log_a y$.

(2) 当 $0<a<1$ 时, $\dfrac{1}{a}>1$, 对实数 $\dfrac{1}{y},\ y>0$, 根据 (1) 的证明, 方程

$$\left(\frac{1}{a}\right)^x=\frac{1}{y}$$

有解, 也就是 $a^x=y$ 有解. □

定理 3.19 设 $a>0$, 对 $y_1>0, y_2>0$, 有

$$\log_a(y_1y_2)=\log_a y_1+\log_a y_2.$$

证明 令 $x_1=\log_a y_1,\ x_2=\log_a y_2$, 则 $a^{x_1}=y_1,\ a^{x_2}=y_2$, 继而推得

$$a^{x_1+x_2}=y_1y_2.$$

根据定理3.18 中解的存在唯一性, 对 $y_1y_2>0$, 存在唯一的 x 使得 $a^x=y_1y_2$, 即可得到定理的结果. □

注记 *16、17 世纪, Napier(纳皮尔, 1550 - 1617)在研究天文学过程中为了简化计算而发明了对数. 对数的发明为天文、航海以及工程等方面处理复杂计算发挥了巨大作用, 被称为数学史上重大发现. Galileo(伽利略, 1564 - 1642)曾为此感叹道: "给我空间、时间及对数, 我就可以创造一个宇宙." 可见当时影响之大.*

Napier 在发明对数时, 并没有意识到指数和对数互逆关系, 原因是当时还没有指数明确概念. 因此对数的发明早于指数. 直到18 世纪, Euler 才发现了指数和对数互逆关系, 并首先使用指数 $a^x=y$ 来定义对数 $x=\log_a y$. 同时指出: "对数源于指数". 可以说 Napier 从实际问题中发明了对数, Euler 在数学中发现了对数的源头.

§3.5 十进制小数

设 $x>0$ 是实数, 根据Archimedes 性, 存在非负整数 $a_0\geqslant 0$, 使得

$$a_0\leqslant x<a_0+1.$$

对 $0\leqslant 10(x-a_0)<10$, 再利用Archimedes 性, 存在非负整数 a_1, 使得

$$a_1\leqslant 10(x-a_0)<a_1+1$$

或

$$a_0+\frac{a_1}{10}\leqslant x<a_0+\frac{a_1}{10}+\frac{1}{10}.$$

显然 $0 \leqslant a_1 < 10$ 或 $0 \leqslant a_1 \leqslant 9$.

若存在 0 和 9 之间的非负整数$a_1, a_2, \cdots, a_n$ 使得

$$a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \cdots + \frac{a_n}{10^n} \leqslant x < a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \cdots + \frac{a_n}{10^n} + \frac{1}{10^n}$$

则对

$$0 \leqslant 10^{n+1}\left(x - a_0 - \frac{a_1}{10} - \frac{a_2}{10^2} - \cdots - \frac{a_n}{10^n}\right) < 10$$

利用Archimedes 性, 存在非负整数 $0 \leqslant a_{n+1} \leqslant 9$, 使得上式对 $n+1$ 也成立.

令 E 是按上述步骤得到的数的集合

$$E = \left\{a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \cdots + \frac{a_n}{10^n}, \;\middle|\; n = 0, 1, 2. \cdots, \right\}$$

则 x 是 E 在 $\mathbb{R}$ 中的上界, 因此 E 在 $\mathbb{R}$ 中有上确界. 下面要说明 $x = \sup E$.

若不然, 令 $x' = \sup E < x$, 那么

$$0 < x - x' < \frac{1}{10^n},\ n = 1, 2, \cdots,$$

这是不可能的. 因此 $x = \sup E$, 它可表示为下列小数形式

$$x = a_0.a_1a_2\cdots a_n\cdots = a_0 + \frac{a_1}{10} + \cdots + \frac{a_n}{10^n} + \cdots$$

其中 $0 \leqslant a_1, a_2, \cdots, a_n, \cdots \leqslant 9$.

几何上看比较直观, 选定 $a_0 \leqslant x < a_0 + 1$ 后, 将数轴上以 a_0 和 $a_0 + 1$ 为端点的区间 $[a_0, a_0 + 1]$ 进行10 等分, 选择一个等分区间

$$\left[a_0 + \frac{a_1}{10},\ a_0 + \frac{a_1 + 1}{10}\right],\ 0 \leqslant a_1 \leqslant 9,$$

使得

$$a_0 + \frac{a_1}{10} \leqslant x < a_0 + \frac{a_1}{10} + \frac{1}{10},$$

如此下去就得到 x 的十进制表示. 当然这种几何描述仅是一个直观上的展示.

如果把 $x = a_0.a_1a_2.\cdots.a_n\cdots$ 中整数部分表示为

$$a_0 = b_s\cdots b_0 = b_s10^s + \cdots + b_0,$$

其中 $0 \leqslant b_i \leqslant 9,\ b_s \neq 0$, 那么

$$\begin{aligned} x &= b_s\cdots b_0.a_1\cdots a_n\cdots \\ &= b_s10^s + \cdots + b_0 + \frac{a_1}{10} + \cdots + \frac{a_n}{10^n} + \cdots, \end{aligned}$$

其中$0 \leqslant b_i \leqslant 9,\ b_s \neq 0, 0 \leqslant a_1, a_2, \cdots, a_n, \cdots \leqslant 9$.

对于小数部分, 有三种可能.

1° 有限小数

若 $a_1, a_2, \cdots, a_n, \cdots$ 中只有有限项非零, 不妨设 $a_j = 0, j > m$, 那么

$$x = a_0.a_1a_2\cdots a_m = a_0 + \frac{a_1}{10} + \cdots + \frac{a_m}{10^m}.$$

称为有限小数. 通分后可以表示成分数形式 $x = \dfrac{b}{10^m}$, 其中 b 是一个整数. 如果 b 和 10^m 有公因子, 可以简化成不可约分数. 但是并不是所有有理数都可以表示成有限小数. 例如 $\dfrac{5}{11}$ 就不能表示为有限小数. 这是因为假如

$$\frac{5}{11} = \frac{b}{10^n}$$

则 $5 \cdot 10^n = 11 \cdot b$, 推出 11 能整除 10^n. 这显然是不可能的.

2° 无限循环小数

若 $a_1, a_2, \cdots, a_n, \cdots$ 中出现无限循环情况, 即从某项 a_n 开始, 存在一个正整数 k, 使得 $a_{n+1}, a_{n+2}, \cdots, a_{n+k}$ 重复出现, 或者说当 $n+l$ 与 $n+j$ 模 k 相等时, 有

$$a_{n+l} = a_{n+j} \quad \text{当} \quad l \equiv j \pmod{k},\ j = 1, 2, \cdots, k$$

这样的小数称为无限循环小数, 记为

$$x = a_0.a_1a_2\cdots a_n\dot{a}_{n+1}\cdots\dot{a}_{n+k}$$

那么

$$10^n(x - a_0.a_1a_2\cdots a_n) = 0.\dot{a}_{n+1}\cdots\dot{a}_{n+k}$$

所以

$$\begin{aligned} 10^{n+k}(x - a_0.a_1a_2\cdots a_n) &= a_{n+1}\cdots a_{n+k} + 0.\dot{a}_{n+1}\cdots\dot{a}_{n+k} \\ &= a_{n+1}\cdots a_{n+k} + 10^n(x - a_0.a_1a_2\cdots a_n) \end{aligned}$$

解得

$$x = a_0.a_1a_2\cdots a_n + \frac{a_{n+1}\cdots a_{n+k}}{10^{n+k} - 10^n}$$

所以无限循环小数是有理数.

反之,任意有理数, 如果不是有限小数, 则一定是无限循环小数. 例如, $\dfrac{5}{11} = 0.\dot{4}\dot{5}$.

一般情况下, 设 $\dfrac{p}{q}$ 是有理数, 其中 $0 < p < q$, $(p, q) = 1$, 则存在正整数 r 使得

$$10^{r-1}p < q,\ 10^r p > q$$

为了简化,不妨设 $r=1$ 也就是

$$p<q,\ 10p>q$$

利用整数的带余除法, 有

$$10p=a_1q+p_1,\ 0\leqslant p_1<q$$

因此, 其中的 a_1 满足

$$a_1p<a_1q\leqslant 10p,$$

推得 $0\leqslant a_1<10$, 即 a_1 是 $0,1,\cdots,9$ 中某个整数. 所以

$$\frac{p}{q}=\frac{a_1}{10}+\frac{1}{10}\frac{p_1}{q}.$$

对 $\dfrac{p_1}{q}$ 重复上述过程

$$\frac{p_1}{q}=\frac{a_2}{10}+\frac{1}{10}\frac{p_2}{q}$$

所以

$$\frac{p}{q}=\frac{a_1}{10}+\frac{a_2}{10^2}+\frac{1}{10^2}\frac{p_2}{q}$$

如此下去 $0\leqslant a_n\leqslant 9$, $0\leqslant p_n<q$, 若某个余数 $p_n=0$, 则上述过程终止, $\dfrac{p}{q}$ 就是有限小数, 若所有余数 $p_n\neq 0$, 则在 0 到 q 的有限个整数中,必有两个余数相等, 因此带余除法重复进行, 这样就产生了无限循环小数. 总之有如下结论:

定理 3.20 *数 a 是有理数, 当且仅当 a 可表示为十进制有限小数或无限循环小数.*

3° **无限不循环小数**

在十进制小数

$$x=a_0.a_1a_2.\cdots.a_n\cdots\quad(0\leqslant a_1,a_2,\cdots,a_n,\cdots\leqslant 9)$$

中, 除了前两种情况之外, $a_1,a_2,\cdots,a_n,\cdots$ 中既不是有限个非零, 也不出现循环, 因此称为无限不循环小数, 这样的数不再是有理数, 它们正是 $\mathbb{R}$ 中的无理数.

注记 十进制是最常用的计数系统, 当然也可以采用其它进制来计数. 例如二进制, 即任何数都可表示为

$$\begin{aligned}x&=b_s\cdots b_0.a_1\cdots a_n\cdots\\&=b_s2^s+\cdots+b_0+\frac{a_1}{2}+\cdots+\frac{a_n}{2^n}+\cdots,\end{aligned}$$

此时 $0\leqslant b_i\leqslant 1, i=0,\cdots,s; b_s\neq 0$, 以及 $0\leqslant a_i\leqslant 1, i=1,2,\cdots$. 也就是 b_i 和 a_i 只能是 *0* 或 *1*. 例如 $0,1,10,11,100,101,110,111,1000,1001,1010$ 分别表示

$0,1,2,3,4,5,6,7,8,9,10$ 等等. 注意到上式小数部分 $\frac{a_1}{2}+\cdots+\frac{a_n}{2^n}+\cdots$ 可能出现无限求和, 但根据第 *1* 讲, 它是收敛的.

二进制是由*Leibniz*（莱布尼兹, *1646-1716*）于*300* 多年前给出的. 但在现代数字电子电路中, 逻辑门的实现直接应用了二进制, 因此现代计算机和依赖计算机设备中都用到二进制. 二进制数的每个位, 称为一个比特（*Binary digit,* 简写为 *Bit*）, 例如 *1010* 是 *4* 比特.

§3.6 Dedekind分割*

本节将介绍 Dedekind 的思想, 给出实数域存在性（定理3.13）的证明 .

Dedekind 用有理数域 $\mathbb{Q}$ 的分割来定义实数, 并证明这样定义的实数满足实数公理, 并包含 $\mathbb{Q}$ 作为子集合 , 因此给出了定理3.13 一种构造性证明.

1° 有理数的分割

定义 3.21 若将有理数域 $\mathbb{Q}$ 分割成两个非空且不相交子集A 和 A':

$$\mathbb{Q}=A\cup A',\ A\cap A'=\phi,$$

使得对任意 $a\in A$ 和 $a'\in A'$, 有$a<a'$. 则称为 $\mathbb{Q}$ 的一个分割, 记为 $A|A'$, 其中 A 称为分割的下组, A' 称为分割的上组.

从集合角度看, A 和 A' 在 $\mathbb{Q}$ 中互为余集（定义1.12）:

$$A=\mathbb{Q}\setminus A'=\{a\mid a\in\mathbb{Q},\ 但\ \ a\notin A'\};$$
$$A'=\mathbb{Q}\setminus A=\{a'\mid a'\in\mathbb{Q},\ 但\ \ a'\notin A\}.$$

因此知其一半, 就知其另一半. 但重要的是, 只有验证了对任意 $a\in A,\ a'\in A'$, 有$a<a'$, $A|A'$ 才是分割.

从几何角度看, 一个分割实际上是把数轴上所有有理点分成左边部分（即“下组”）和右边部分（即“上组”）.

分割有三种可能:

（1）在下组A内无最大数,而在上组 A' 内有最小数 r,

$$A=\{a\mid a\in\mathbb{Q},\ a<r\},\ A'=\{a'\mid a'\in\mathbb{Q},\ a'\geqslant r\};$$

（2）在下组A内有最大数 r, 而在上组 A' 内无最小数,

$$A=\{a\mid a\in\mathbb{Q},\ a\leqslant r\},\ A'=\{a'\mid a'\in\mathbb{Q},\ a'>r\};$$

(3)在下组A内无最大数, 上组 A' 内也无最小数, 例如

$$A=\{a \mid a\in\mathbb{Q},\ a<0;\ \text{或 } a>0 \text{ 但 } a^2<2\},$$
$$A'=\{a' \mid a'\in\mathbb{Q},\ a'>0 \text{ 且 } a'^2>2\}.$$

因为分割是对有理数域 $\mathbb{Q}$ 的分割, 这里所说的 "数" 当然是指有理数.

上述三种分割中, 前两种上组和下组以有理数作为明确分界线, 称为 **有理分割**. 为了确定起见,我们约定：**凡是说到有理分割时,常把作为分界线的有理数 r 放在上组内**, 这样只需考虑第一种和第三种分割 . 不管是第一种还是第三种分割, 分割的下组内都无最大数.

那么会不会有第四种可能的分割呢? 即分割 $A|A'$ 中, 下组有最大数, 上组有最小数. 事实上, 这样分割不可能存在. 可以采取反证法加以说明：

假如存在 $\mathbb{Q}$ 的一个分割 $A|A'$, 使得 A 有最大数 $a^*\in A$, 而 A' 有最小数 $b^*\in A'$. 根据分割的定义, 有 $a^*<b^*$. 但是, 有理数 $c=\dfrac{a^*+b^*}{2}$ 满足 $a^*<c<b^*$, 即 c 大于下组的最大数, 小于上组的最小数, 所以 c 既不属于下组 A, 又不属于上组 A', 这显然与 A 和 A' 是 $\mathbb{Q}$ 的一个分割矛盾.

Dedekind 的思想是一个分割对应一个 "数" , 当分割是有理分割时, 对应的数就是有理数, 例如 0 , 1 和一般的有理数 r 分别为

$$0=A_0|A_0',\quad A_0=\{a|\ a<0\},\ A_0'=\{a'|\ a'\geqslant 0\};$$
$$1=A_1|A_1',\quad A_1=\{a|\ a<1\},\ A_1'=\{a'|\ a'\geqslant 1\};$$
$$r=A_r|A_r',\quad A_r=\{a|\ a<r\},\ A_r'=\{a'|\ a'\geqslant r\}.$$

当分割不是有理分割, 即是(3)中形式的分割时, 就对应一个新的 "数" , 称为 "无理数" . 因此把所有分割构成的集合定义成实数集合.

定理 3.22 下列集合满足实数公理, 因此给出了一个实数模型.

$$\mathbb{R}=\{A|A' \ \big|\ \mathbb{Q} \text{ 的所有分割}\}$$

下面就要逐一验证上述集合是有序域, 同时满足确界原理, 因此它就是定理3.13 中所要求的实数域. 这里仅仅验证以下四点, 一是如何在两个分割之间定义 "大小" , 二是两个分割怎么做加法, 三是两个分割如何相乘, 四是这些由分割形成的集合 $\mathbb{R}$ 满足确界原理. 其它验证请读者自行完成.

2° 分割的序

设 $\alpha=A_\alpha|A_\alpha'$, $\beta=A_\beta|A_\beta'$ 是两个分割, 则根据分割定义, 要么 $A_\alpha\subset A_\beta$ (因此 $A_\beta'\subset A_\alpha'$), 要么 $A_\beta\subset A_\alpha$ (因此 $A_\alpha'\subset A_\beta'$). 据此, 定义 α 和 β 的序如下:

当 $A_\alpha \subsetneq A_\beta$ (因此也有 $A'_\beta \subsetneq A'_\alpha$) 时,就定义 $\alpha < \beta$.

当 $A_\beta \subsetneq A_\alpha$ (因此也有 $A'_\alpha \subsetneq A'_\beta$) 时, 就定义 $\alpha > \beta$.

当 $A_\alpha = A_\beta$ (因此也有$A'_\alpha = A'_\beta$) 时, 就定义 $\alpha = \beta$.

这样就定义了分割之间一种序 (也就是 “大小”) . 可以验证上述定义满足序公理有关性质.

特别, 对于一个分割 $\alpha = A_\alpha|A'_\alpha$, 如果 A_α 包含正有理数, 则 $A_0 \subset A_\alpha$, 所以 $\alpha > 0$, 反之 $\alpha \leqslant 0$.

3° 分割的加法

性质 3.23 设 $\alpha = A_\alpha|A'_\alpha,\ \beta = A_\beta|A'_\beta$ 是两个分割, 令

$$A_\gamma = \{a + b \mid a \in A_\alpha,\ b \in A_\beta\},\ A'_\gamma = \mathbb{Q} \setminus A_\gamma,$$

则它们给出 $\mathbb{Q}$ 的一个分割 $\gamma = A_\gamma|A'_\gamma$.

证明 显然 A_γ, A'_γ 都是有理数的子集合, 且

$$\mathbb{Q} = A_\gamma \cup A'_\gamma,\ A_\gamma \cap A'_\gamma = \phi.$$

因此要证明 $A_\gamma|A'_\gamma$ 是 $\mathbb{Q}$ 的一个分割, 就是要证明对任意的 $c = a + b \in A_\gamma,\ c' \in A'_\gamma$, 有 $c < c'$.

对任意的 $a \in A_\alpha,\ c' \in A'_\gamma$, 考察 $c' - a$ 在分割 $A_\beta|A'_\beta$ 的上组还是下组.

若$c' - a \in A_\beta$, 则存在 $d \in A_\beta$ 使得 $c' - a = d$, 推出 $c' = a + d \in A_\gamma$, 这与 A'_γ 的定义相矛盾. 因此 $c' - a$ 只能在 $A_\beta|A'_\beta$ 的上组: $c' - a \in A'_\beta$. 所以对任意的 $b \in A_\beta$, 有$c' - a > b$, 即 $c' > a + b = c$. □

定义 3.24 (加法) 任意两个分割 $\alpha = A_\alpha|A'_\alpha,\ \beta = A_\beta|A'_\beta$ 的加法定义为:

$$\gamma = \alpha + \beta.$$

其中分割 $\gamma = A_\gamma|A'_\gamma$ 由性质*3.23*给出.

不难验证这样定义的加法满足交换律和结合律. 但是, 关于加法的 0 元和负元还需要进一步明确, 为此有下列两个性质.

性质 3.25 对任意的 $\alpha = A_\alpha|A'_\alpha$, 以及 $0 = A_0|A'_0$, 有

$$\alpha + 0 = \alpha.$$

证明 根据性质3.23, $\alpha + 0 = \gamma = A_\gamma|A'_\gamma$ 是一个分割, 其中

$$A_\gamma = \{a + b \mid a \in A_\alpha,\ b \in A_0\},$$

下面要证明 $\gamma=\alpha$.

一方面由于 $b\in A_0$, 即 $b<0$, 对任意的 $a\in A_\alpha,\ a'\in A'_\alpha$, 推出 $a+b<a<a'$, 所以$a+b\in A_\alpha$. 这样就证明了 $A_\gamma\subset A_\alpha$.

另一方面, 由于 A_α 没有最大数, 任取 $a\in A_\alpha$, 一定存在有理数 $\tilde{a}\in A_\alpha$ 使得 $\tilde{a}>a$. 记 $b=a-\tilde{a}<0$, 所以 $b\in A_0$, 根据 A_γ 的定义, $a=\tilde{a}+b\in A_\gamma$, 推出 $A_\gamma\supset A_\alpha$.

综合两方面结论, 有 $A_\gamma=A_\alpha$, 也就是 $\alpha+0=\alpha$. □

性质 3.26 对于任意分割 $\alpha=A_\alpha|A'_\alpha$, 定义

$$A_\beta=\{b\mid \text{存在 } a'\in A'_\alpha,\ \text{使得 } b<-a'\},\ A'_\beta=\mathbb{Q}\setminus A_\beta,$$

则 $\beta=A_\beta|A'_\beta$ 是一个分割, 且 $\alpha+\beta=0$, 即 $\beta=-\alpha$ 是 α 的负元.

证明 任取 $b\in A_\beta$, 存在 $a'\in A'_\alpha$, 使得 $b<-a'$. 任取 $b'\in A'_\beta$, 即 $b'\notin A_\beta$, 所以对于任意 $a'\in A'_\alpha$, 有 $b'\geqslant -a'>b$. 这样就验证了 $A_\beta|A'_\beta$ 是一个分割.

其次要证明 $\alpha+\beta=0$, 也就是要证明

$$A_\gamma=\{a+b\mid a\in A_\alpha,\ b\in A_\beta\}=A_0.$$

任取 $a+b\in A_\gamma,\ a\in A_\alpha, b\in A_\beta$, 根据 A_β 的定义, 存在$a'\in A'_\alpha$ 使得 $b<-a'$, 或 $-b>a'$, 推出 $-b>a'>a$ 或 $a+b<0$, 也就是 $a+b\in A_0$, 即 $A_\gamma\subset A_0$.

反过来, 任取 $c\in A_0$, $c<0$, 或 $-d>0$. 所以在分割 $A_\alpha|A'_\alpha$ 是中, 分别存在 $a\in A_\alpha$ 和 $a'\in A'_\alpha$ 使得 $0<a'-a<-c$, 推出 $-a'>-a+c$.

记 $b=-a+c<-a'$, 根据 A_β 的定义得 $b\in A_\beta$. 因此 $c=a+b$, 其中 $a\in A_\alpha$, $b\in A_\beta$, 也就是 $c=a+b\in A_\gamma$. 这样就证明了 $A_0\subset A_\gamma$. 最终得 $A_\gamma=A_0$. □

4° 分割的乘法

设 $\alpha=A_\alpha|A'_\alpha,\ \beta=A_\beta|A'_\beta$ 是两个分割, 为了定义两者之间乘法, 分如下四种情况

（1）$\alpha\geqslant 0,\ \beta\geqslant 0$;

（2）$\alpha<0,\ \beta<0$;

（3）$\alpha\geqslant 0,\ \beta<0$;

（4）$\alpha<0,\ \beta\geqslant 0$.

对于（1）, 有下列性质:

性质 3.27 设 $\alpha\geqslant 0,\ \beta\geqslant 0$,, 令

$$A_\gamma=\{c\mid c<0,\ \text{或者存在 } a\in A_\alpha,\ b\in A_\beta,\ a>0,\ b>0 \text{ 使得 } c=ab\},$$

$$A'_\gamma=\mathbb{Q}\setminus A_\gamma,$$

则 $\gamma = A_\gamma|A'_\gamma$ 是 $\mathbb{Q}$ 的一个分割.

证明 若 $\beta = 0,\ A_\beta = A_0$. 根据定义, $A_\gamma = \{c \mid c < 0\} = A_0,\ A'_\gamma = A'_0$, 所以 $A_\gamma|A'_\gamma$ 是一个分割, 且 $0 = \alpha \cdot 0$.

若 $\beta > 0$, 任取 $c \in A_\gamma,\ c' \in A'_\gamma$, 显然 $c' \geqslant 0$.

如果 $c < 0$, 推出 $c < c'$;

如果 $c > 0$, 根据 A_γ 的定义, 存在 $a > 0, b > 0$, 使得 $c = ab$.

考察 $\dfrac{c'}{b} > 0$, 若 $\dfrac{c'}{b} \in A_\alpha$, 推得 $c' = \dfrac{c'}{b}b \in A_\gamma$, 矛盾. 因此 $\dfrac{c'}{b} \in A'_\alpha$, 也就是 $\dfrac{c'}{b} > a$, 最终也得到 $c' > ab = c$. 所以$A_\gamma|A'_\gamma$ 分割. □

性质3.27中定义的分割 $\gamma = A_\gamma|A'_\gamma$ 可定义为$\alpha = A_\alpha|A'_\alpha \geqslant 0,\ \beta = A_\beta|A'_\beta \geqslant 0$ 的乘积. 为了定义其他情形下分割之间的乘积, 首先要定义分割的 “绝对值” .

定义 3.28 分割 $\alpha = A_\alpha|A'_\alpha$ 的绝对值$|\alpha|$定义为

$$|\alpha| = \begin{cases} \alpha, & 若\alpha \geqslant 0; \\ -\alpha, & 若\alpha < 0. \end{cases}$$

或者说 $|\alpha|$ 对应的分割 $|\alpha| = A_{|\alpha|}|A'_{|\alpha|}$ 满足

$$A_{|\alpha|} = \begin{cases} A_\alpha, & 若\alpha \geqslant 0; \\ A_{-\alpha}, & 若\alpha < 0. \end{cases}$$

这里 $A_{-\alpha}$ 的定义由性质*3.26* 给出.

显然 $|\alpha| \geqslant 0$, 并且 $|\alpha| = 0$ 当且仅当 $\alpha = 0$.

定义 3.29 (乘法) 对于分割 $\alpha = A_\alpha|A'_\alpha,\ \beta = A_\beta|A'_\beta$,

若 $\alpha \geqslant 0, \beta \geqslant 0$, 则它们的乘积定义为*:*

$$\alpha\beta = \gamma,$$

其中分割 $\gamma = A_\gamma|A'_\gamma$ 由性质*3.27*给出.

利用以上定义和分割的绝对值, 其它情形分割的乘积定义如下*:*

$$\alpha\beta = \begin{cases} -|\alpha||\beta|, & 若\ \alpha > 0,\ \beta \leqslant 0, \\ -|\alpha||\beta|, & 若\ \alpha \leqslant 0,\ \beta > 0, \\ \ |\alpha||\beta|, & 若\ \alpha < 0,\ \beta < 0. \end{cases}$$

最后讨论非零分割的逆.

性质 3.30 如果分割 $\alpha > 0,\ \alpha = A_\alpha|A'_\alpha$, 定义

$$A_\beta = \left\{ b \mid b \leqslant 0 \text{ 或者存在 } a' \in A'_\alpha,\ 使得 b < \frac{1}{a'} \right\},\ A'_\beta = \mathbb{Q} \setminus A_\beta,$$

则 $\beta = A_\beta|A'_\beta$ 是一个分割, 且 $\alpha\beta = 1$. β 称为 α 的逆, 记为 $\beta = \alpha^{-1}$.

如果$\alpha < 0$, 那么它的逆定义为$-(-\alpha)^{-1}$.

证明 任取 $b \in A_\beta$, $b > 0$, 根据 A_β 的定义, 存在 $a' \in A'_\alpha$, 使得 $b < \dfrac{1}{a'}$.

任取 $b' \in A'_\beta$ (显然 $b' > 0$), 因为 $b' \notin A_\beta$, 所以对任意的$a' \in A'_\alpha$, 都有$b' \geqslant \dfrac{1}{a'}$, 由此推出 $b < b'$, 即 $\beta = A_\beta|A'_\beta$ 是一个分割.

根据乘法, 记 $\gamma = \alpha \cdot \beta$, $\gamma = A_\gamma|A'_\gamma$, 其中 A_γ 和 A'_γ 的定义由性质3.27 给出. 现在要证明 $\gamma = 1$, 即是要证明 $A_\gamma = A_1$.

任取 $c \in A_\gamma$, 若 $c < 0$, 显然有 $c \in A_1$. 若 $c > 0$, 则存在 $a \in A_\alpha$, $b \in A_\beta$, $a > 0$, $b > 0$, 使得 $c = ab$. 由于 $b > 0$, 所以存在 $a' \in A'_\alpha$ 使得 $b < \dfrac{1}{a'}$, 由此得 $c = ab < \dfrac{a}{a'} < 1$. 这样首先证明了 $A_\gamma \subset A_1$.

反之, 任取 $c \in A_1$, 若 $c < 0$, 显然有 $c \in A_\gamma$. 若 $c > 0$, 利用有理数的稠密性 (见 §3.1) , 分以下两种情况讨论:

当 A'_α 有最小数时, 记 $r \in A'_\alpha$ 是最小数, 因 $\alpha > 0$, 所以 $r > 0$.

取 $cr < a < r$, 则 $a \in A_\alpha$. 取 $b = \dfrac{c}{a}$, 则存在 $a' \in A'_\alpha$ 使得 $r < a' < \dfrac{a}{c}$, 或 $b < \dfrac{1}{a'}$, 推出 $b \in A_\beta$ 使得 $c = ab \in A_\gamma$.

当 A'_α 无最小数时, 取 $a \in A_\alpha$, $a > 0$, 存在非负整数 n, 使得

$$a_1 = \frac{a}{c^n} \in A_\alpha, \text{ 但是 } a'_1 = \frac{a}{c^{n+1}} \in A'_\alpha,$$

因 a'_1 不是 A'_α 的最小数, 所以存在 $a' \in A'_\alpha$, 使得 $a'_1 > a'$. 记 $b_1 = \dfrac{1}{a'_1}$, 则

$$b_1 = \frac{1}{a'_1} < \frac{1}{a'},$$

所以 $b_1 \in A_\beta$, 这样就得到

$$c = \frac{a}{c^n}\frac{c^{n+1}}{a} = \frac{a}{c^n}\frac{1}{a'_1} = a_1 b_1 \in A_\gamma,$$

也就证明了 $A_\gamma = A_1$, 也就是 $\alpha \cdot \beta = \gamma = 1$. □

关于序的传递性、加法和乘法的交换律、结合律以及乘法对加法的分配律比较简单, 读者可以自行完成验证.

5° 有序域

在验证了分割的序、加法、乘法后, 还要验证分割构成的集合满足有序域的定义.

性质 3.31 集合

$$\mathbb{R} = \{A|A' \;\Big|\; \mathbb{Q}\text{的所有分割}\}$$

是有序域.

证明 只要证明 $\mathbb{R}$ 满足有序域定义3.5中条件即可.

设 $\alpha = A_\alpha|A'_\alpha,\ \beta = A_\beta|A'_\beta,\ \gamma = A_\gamma|A'_\gamma$. 若 $\alpha < \beta$, 则根据分割的序, 有

$$A_\alpha \subsetneq A_\beta,$$

再由分割加法的性质3.23, 有

$$\alpha + \gamma = A_{\alpha+\gamma}|A'_{\alpha+\gamma},\ \beta + \gamma = A_{\beta+\gamma}|A'_{\beta+\gamma},$$

其中

$$A_{\alpha+\gamma} = \{a + c \mid a \in A_\alpha,\ c \in A_\gamma\},\ A'_{\alpha+\gamma} = \mathbb{Q}/A_{\alpha+\gamma},$$
$$A_{\beta+\gamma} = \{b + c \mid b \in A_\beta,\ c \in A_\gamma\},\ A'_{\beta+\gamma} = \mathbb{Q}/A_{\beta+\gamma},$$

由$A_\alpha \subsetneq A_\beta$, 推出 $A_{\alpha+\gamma} \subsetneq A_{\beta+\gamma}$, 这样就由 $\alpha < \beta$ 推出 $\alpha + \gamma < \beta + \gamma$.

下面证明由$\alpha > 0,\ \beta > 0$, 推出 $\alpha\beta > 0$.

根据分割的乘法 (性质3.27) , 有 $\alpha\beta = A_{\alpha\beta}|A'_{\alpha\beta}$, 其中

$A_{\alpha\beta} = \{c \mid c < 0,$ 或者存在 $a \in A_\alpha,\ b \in A_\beta,\ a > 0,\ b > 0$ 使得 $c = ab\}$,

$A'_{\alpha\beta} = \mathbb{Q}/A_{\alpha\beta}$.

因为 $\alpha > 0$, 所以在 $\alpha = A_\alpha|A'_\alpha$ 中,

$$A_0 \subsetneq A_\alpha,$$

也就是存在有理数 $a_0 \in A_\alpha$ 满足 $a_0 > 0$. 同理在 $\beta = A_\beta|A'_\beta$ 中, 存在有理数 $b_0 \in A_\beta$ 满足 $b_0 > 0$. 因此 $A_{\alpha\beta}$ 中包含正的有理数 a_0b_0, 也就是, $A_0 \subsetneq A_{\alpha\beta}$, 或 $\alpha\beta > 0$. □

6° **确界性 (完备性)**

最后验证分割的集合满足确界原理.

性质 3.32 集合

$$\mathbb{R} = \{A|A' \;\Big|\; \mathbb{Q}\text{的所有分割}\}$$

满足确界原理.

证明 设

$$X = \{\alpha = A_\alpha|A'_\alpha\} \subset \mathbb{R}$$

是 $\mathbb{R}$ 中有上界子集合, $\beta = B_\beta|B'_\beta \in \mathbb{R}$ 是 X 的一个上界, 即对于任意 $\alpha = A_\alpha|A'_\alpha \in X$, 有 $\alpha \leqslant \beta$, 也就是 $A_\alpha \subset B_\beta$. 那么首先验证

$$A_{\alpha_0} = \bigcup_{\alpha\in X} A_\alpha,\quad A'_{\alpha_0} = \mathbb{Q} \setminus A_0$$

是 $\mathbb{Q}$ 的一个分割.

对任意的 $a \in A_{\alpha_0}$, 存在某个 $\alpha \in X$, 使得 $a \in A_\alpha$; 对任意的 $b \in A'_{\alpha_0}$, 推出 $b \notin A_\alpha,\ \alpha \in X$, 所以 $a < b$.

其次验证 $\alpha_0 = A_{\alpha_0}|A'_{\alpha_0}$ 是 X 上确界. 对任意 $\alpha = A_\alpha|A'_\alpha \in X$,

$$A_\alpha \subset A_{\alpha_0},\ A'_{\alpha_0} \supset A'_\alpha,$$

所以 $\alpha_0 \geqslant \alpha$ 是 X 的上界. 若 $\beta = A_\beta|A'_\beta$ 是 X 的另一个上界: $\alpha \leqslant \beta,\ \alpha \in X$, 则 $A_\alpha \subset A_\beta$ 对任意 $\alpha = A_\alpha|A'_\alpha \in X$ 成立, 由此推出 $A_{\alpha_0} \subset A_\beta$, 即 $\alpha_0 \leqslant \beta$. 所以α_0 是最小上界. □

注记 虽然由 *Dedekind* 分割定义的 $\mathbb{R}$ 满足实数公理, 但要说明有理数域 $\mathbb{Q}$ 是它的子域, 需要做如下考虑. 首先记 $\mathbb{R}$ 中所有有理分割 (即第一种分割) 的集合为 $\mathbb{Q}^*$, 然后考虑 $\mathbb{Q}^*$ 与有理数域 $\mathbb{Q}$ 中的算术和序的一致性, 就可把 $\mathbb{Q}$ 看成 $\mathbb{R}$ 的子域.

第 3 讲习题

1. 设 n 不是完全平方数的正整数, 证明 $\sqrt{n}$ 是无理数.

2. 证明: 不存在平方为 12 的有理数.

3. 证明: $\sqrt{3}$ 和 $\sqrt{\frac{3}{2}}$ 都不是有理数.

4. 证明: $\sqrt{2}+\sqrt{3}+\sqrt{5}$ 不是有理数.

5. 证明: 存在两个无理数 a, b, 使得 a^b 是有理数.
   提示: 可考虑
   $$x = \sqrt{2}^{\sqrt{2}} = 2^{\sqrt{2}/2},$$
   根据 §3.4 中关于正实数指数幂的讨论, x 是一个实数, 因此 x 要么是有理数, 要么是无理数, 无论哪种情况, 都推出本题结论成立. 注意, 本题不是证明 x 到底是有理数, 还是无理数, 而是要证明存在两个无理数 a, b, 使得 a^b 是有理数.

6. 试证明不等式 $b-1 \geqslant n(b^{1/n}-1)$, 这里 $b>1, n$ 是正整数.

7. 验证集合 $\mathbb{Q}(\sqrt{2}) = \{r+s\sqrt{2} \mid r, s \in \mathbb{Q}\}$ 是一个数域.

8. 由实数公理证明下列等式成立
   (1) 若 $x+y=x+z$, 则 $x=z$; (2) 若 $x \neq 0$, $xy=xz$, 则 $y=z$;

9. 设 A 是 $\mathbb{R}$ 中非空有下界的子集, 令 $-A = \{x \mid -x \in A\}$, 证明
   $$\inf A = -\sup(-A).$$

10. 设 A 和 B 是 $\mathbb{R}$ 中有下界的子集, $S = A \cup B$, 试证明 S 有有限的下确界, 并且
    $$\inf B = \min\{\inf A, \inf B\}.$$

11. 设 E 是 $\mathbb{R}$ 中有上界子集, $\sup E \notin E$, 则一定存在无穷数列 $\{x_n\} \subset E$, 使得
    $$\lim_{n\to+\infty} x_n = \sup E.$$
    提示: 说明存在 $x_n \in E$, 满足 $\sup E - \dfrac{1}{n} < x_n < \sup E$, 再用极限定义完成证明.

12. 证明 $\mathbb{R}$ 上任意无限个两两互不相交的开区间形成的集合是可数的.
    提示: 利用有理数的稠密性 (见定理*3.14*) 和有理数集的可数性.

13. 设 E 是区间 $[0,1]$ 中所有有理数集合. 试证可通过挖去以 E 中任意有理数为中心的开区间, 使得这些开区间总长度不超过 $\dfrac{1}{2}$.

提示: 虽然 E 在$[0,1]$ 中稠密, 但可数, 所以 $E=\{r_1,r_2,\cdots,\}$, 以 r_n 为中心挖去一个开区间, 通过控制开区间长度, 并利用无限求和方式给出开区间总长度的上界.事实上, 可以通过控制挖去开区间的长度, 使得挖去部分的总长度不超过任意小的数.

14. 设 ξ 是一个无理数, 证明集合 $S=\{m+n\xi \mid m,n\in\mathbb{Z}\}$ 在 $\mathbb{R}$中稠密.
提示: 对任意 $l\in\mathbb{Z}$, S 满足性质: $l(m+n\xi)\in S$, $(m+n\xi)\pm(m'+n'\xi)\in S$. 任取 $a<b$, 要证存在 S 中数介于两者之间. 不妨设 $0<a<b$. 对于任意正整数 i, 记 $n_i=-[i\xi]$ ($[x]$ 表示取整), 那么 $x_i=n_i+i\xi\in S$ 满足 $0<x_i<1$. 取正整数 k, 使得 $\dfrac{1}{k}<b-a$, 那么 S 中 $k+1$ 个数 $x_1,x_2,\cdots,x_{k+1}$, 至少有一对 x_i,x_j 满足 $0<x_j-x_i<\dfrac{1}{k}$. 再利用 *Archimedes* 性 (定理*3.14*), 存在满足 $n(x_j-x_i)>a$ 的最小正整数 n, 然后说明 $n(x_j-x_i)<b$, 最后利用 S 的性质及可完成证明.

第 4 讲　复数

复数虽然是中学必学内容, 但为了保持完整性, 这里还是简要回顾复数起源、复数基本运算以及几何含义.

§4.1　复数起源和复数域

复数历史可以追述到16世纪. 问题起源现在看来就是代数方程求根问题. 例如, 对于整数为系数一次代数方程

$$ax + b = 0, \quad a, b \in \mathbb{Z},\ a \neq 0,$$

如果 a 不能整除 b, 那么该方程在整数范围内没有解, 必须把整数扩充到有理数才有有理数解 $x = -\dfrac{a}{b}$. 对于二次方程

$$x^2 - 2 = 0,$$

在有理数域内不存在解, 因此有理数也不够用了, 只有在更广的实数范围内方程才有解 $x = \sqrt{2}$.

然而, 即使是实数范围内, 也无法解决所有二次代数方程求解问题. 例如方程

$$x^2 + 1 = 0$$

就没有实数解.

历史上还有一个十分著名问题, 即如何把 10 分成两部分, 使其积等于 40. 显然这个问题就是求二次代数方程的解

$$x(10 - x) = 40,$$

但是, 该方程也没有实数解.

正如从整数扩充到有理数, 从有理数扩充到实数一样, 能否继续扩充数域, 使得在原来范围内不可解方程, 在扩充的数域中可解. 仍然以上述两个方程为例, 如果按照通常求解方法, 则方程 $x^2 + 1 = 0$ 解为 $x_\pm = \pm\sqrt{-1}$, 而方程 $x(10 - x) = 40$ 解是 $x_\pm = 5 \pm \sqrt{-15}$. 这就碰到了一个新问题, 负数如何开平方根?

要使在实数域中没有意义的负数开方变得有意义, 我们引进一个新的 “数”

$$\mathrm{i} = \sqrt{-1},$$

它服从基本的运算规则：

$$\mathrm{i}^2 = -1.$$

引进的这个“数” i 就是一个符号, 它无法像其它数一样用来计数, 因此称为**虚数单位**. 如果 i 能够与其它实数一样进行加法和乘法运算, 并始终注意 $\mathrm{i}^2=-1$, 那么就产生了一类新符号

$$z=x+\mathrm{i}y,\ x,y\in\mathbb{R},$$

并称为**复数**, x 称为复数 z 的**实部**, y 称为复数 z 的**虚部**, 分别记为

$$x=\mathrm{Re}(z),\ y=\mathrm{Im}(z).$$

对于实部为零的复数, 称为**纯虚数**, 而虚部为零的复数就是实数. 两个复数相等, 当且仅当两者实部和虚部分别相等. 用记号 $\mathbb{C}$ 表示全部复数集合:

$$\mathbb{C}=\{x+iy\ \Big|\ x,y\in\mathbb{R}\}.$$

这样方程 $x^2+1=0$ 和 $x(10-x)=40$ 解就分别由新符号 $\pm\mathrm{i}$ 和 $5\pm\mathrm{i}\sqrt{5}$ 表示, 或者说它们在复数 $\mathbb{C}$ 范围内可解.

对任意两个复数

$$z_1=x_1+\mathrm{i}y_1,\ z_2=x_2+\mathrm{i}y_2,$$

它们之间的运算定义如下

$$\begin{aligned}z_1\pm z_2&=(x_1\pm x_2)+\mathrm{i}(y_1\pm y_2)\\ z_1z_2&=(x_1+\mathrm{i}y_1)(x_2+\mathrm{i}y_2)=x_1x_2+\mathrm{i}(x_1y_2+x_2y_1)+\mathrm{i}^2y_1y_2\\ &=(x_1x_2-y_1y_2)+\mathrm{i}(x_1y_2+x_2y_1)\end{aligned}$$

因此两个复数相加减还是复数, 两个复数相乘还是复数. 不难验证运算满足加法和乘法的交换律、结合律和分配律. 特别

$$(x+\mathrm{i}y)(x-\mathrm{i}y)=x^2+y^2$$

是一个实数. 称复数 $\overline{z}=x-\mathrm{i}y$ 为复数$z=x+\mathrm{i}y$ 的**共轭** 复数, 记

$$|z|^2=z\overline{z}=x^2+y^2.$$

并称 $|z|$ 为 z 的**模**. 同时可以定义零元 $0=0+\mathrm{i}0$ 和单位元 $1=1+\mathrm{i}0$, 显然 z 非零当且仅当 $|z|\neq0$.

对任何非零 $z=x+\mathrm{i}y$, 它的逆定义为

$$z^{-1}=\frac{x}{x^2+y^2}-\mathrm{i}\frac{y}{x^2+y^2}$$

满足 $zz^{-1}=z^{-1}z=1$. 因此两个复数 $z_1=x_1+\mathrm{i}y_1,\ z_2=x_2+\mathrm{i}y_2$ $(|z_2|\neq0)$ 的除法为

$$\begin{aligned}\frac{z_1}{z_2}&=\frac{x_1+\mathrm{i}y_1}{x_2+\mathrm{i}y_2}=\frac{(x_1+\mathrm{i}y_1)(x_2-\mathrm{i}y_2)}{(x_2+\mathrm{i}y_2)(x_2-\mathrm{i}y_2)}\\ &=\left(\frac{x_1x_2+y_1y_2}{x_2^2+y_2^2}\right)+\mathrm{i}\left(\frac{y_1x_2-x_1y_2}{x_2^2+y_2^2}\right)\end{aligned}$$

复数集合 $\mathbb{C}$ 在加法和乘法运算下封闭、具有零元和单位元, 并且非零元可逆, 因此满足域的定义3.3 , 称 $\mathbb{C}$ 为**复数域**, 它包含实数域 $\mathbb{R}$（虚部为零的复数的集合）, 因此是实数域的扩充. 然而, 下列定理体现了复数域与实数域之间区别.

定理 4.1 *复数域不可能成为有序域.*

证明 根据有序域定义3.5 和性质3.6, 有序域的特点之一是非零元素的平方为正. 假如存在一种序关系使得 $\mathbb{C}$ 满足有序域的定义3.5, 因为 $\mathrm{i} \neq 0$, 但 $\mathrm{i}^2 = -1 < 0$, 矛盾, 所以 $\mathbb{C}$ 不可能是有序域. □

注记 在复数域 $\mathbb{C}$ 中, 可以定义序关系, 使其成为有序集合（见习题 4）, 但定理 4.1 说明无论什么序关系, 都不可能使 $\mathbb{C}$ 成为有序域.

§4.2 复数的几何含义和 Euler 公式

一个复数 $z = x + \mathrm{i}y$ 1-1 对应一个数组 (x, y) ,把这数组看成是直角坐标系 Oxy 下平面上点 P 的坐标, 复数就对应平面上一个点, 就像把实数与数轴上的点 1-1 对应一样. 通常也用复数 $z = x + \mathrm{i}y$ 表示Oxy 平面上的点 $P(x, y)$. 特别, $0 = 0 + \mathrm{i}0$ 对应坐标平面上原点 O, 实数（即虚部为零复数）对应 x 轴上点, 而纯虚数（实部为零复数）对应 y 轴上点. 因此 $z = x + \mathrm{i}y$ 就成为复数的直角坐标表示. 称坐标平面为 **复平面**, x 轴称为**实轴**, 而 y 轴称为**虚轴**. 记 $\overrightarrow{OP}$ 为以原点 O 为起点, $P(x, y)$ 为终点的向量, 那么复数 $z = x + \mathrm{i}y$ 也与平面上向量 $\overrightarrow{OP}$ 1-1对应.

复数除了可以用直角坐标表示外, 还可以用极坐标表示. 取 x 轴正向半轴作为极轴, 坐标原点作为极点, 于是如果点 $z = x + \mathrm{i}y$ 极径记作 r, 极角记作 θ, 那么就有

$$z = x + \mathrm{i}y = r(\cos\theta + \mathrm{i}\sin\theta).$$

显然, 极径就是复数 z 的模, 是被唯一确定的:

$$r = |z| = \sqrt{x^2 + y^2}.$$

极角 θ 称为复数 z 的**幅角**, 用符号 $\mathrm{Arg}\ z$ 表示. 但是当 $z \neq 0$ 时, z 的幅角可以相差 2π 的任何一个整倍数:

$$\theta = \mathrm{Arg}\ z = \begin{cases} \arctan\dfrac{y}{x} + 2k\pi \ \text{(第一、第四象限)}, \\ \arctan\dfrac{y}{x} + (2k+1)\pi \ \text{(第二、第三象限)}. \end{cases}$$

这里, k 为任意整数. 函数 arctan 的值域为 $\left(-\dfrac{\pi}{2}, \dfrac{\pi}{2}\right)$. 用 arg 来表示Arg 中的一个值, 比如 arg$z$ 来表示Arg$z$ 中对应 $k = 0$ 的值, 并称arg$z$ 是Arg$z$ 的**主值**.

有了复数 $z=x+\mathrm{i}y$ 与平面上点 $P(x,y)$ 以及和向量 $\overrightarrow{OP}$ 的对应, 就可以把复数的代数运算赋予几何上的解释.

首先观察复数 $z=x+\mathrm{i}y$ 的模正是对应点 $P(x,y)$ 到原点的距离, 或者说是向量 $\overrightarrow{OP}$的长度

$$|z|=|\overrightarrow{OP}|.$$

z 的共轭复数 $\overline{z}=x-\mathrm{i}y$ 对应的点是 $P(x,y)$ 关于x 轴对称的点 $\overline{P}(x,-y)$.

两个复数 $z=x+\mathrm{i}y,\ z'=x'+\mathrm{i}y'$ 相加减, $z\pm z'$对应点的坐标为 $(x\pm x',y\pm y')$, 也是向量 $\overrightarrow{OP}\pm\overrightarrow{OP'}$ 的坐标, 或者说 $z+z'$ 表示以$O,\ z,\ z'$ 为三个顶点的平行四边形的第四个顶点, 其模 $|z+z'|$ 正是平行四边形从 O 到 $z+z'$ 的对角线长度, 因此有

$$|z+z'|\leqslant|z|+|z'|$$

而 $z-z'$的模

$$|z-z'|=\sqrt{(x-x')^2+(y-y')^2}$$

表示z 与 z' 之间距离.

用极坐标表示复数, 更容易看出两个复数乘积几何含义, 设

$$z=r(\cos\theta+\mathrm{i}\sin\theta),\ z'=r'(\cos\theta'+\mathrm{i}\sin\theta').$$

那么

$$\begin{aligned}zz'&=rr'[(\cos\theta\cos\theta'-\sin\theta\sin\theta')+\mathrm{i}(\cos\theta\sin\theta'+\sin\theta\cos\theta')]\\&=rr'[\cos(\theta+\theta')+\mathrm{i}\sin(\theta+\theta')],\\\frac{z}{z'}&=z\frac{\overline{z'}}{|z'|^2}=\frac{r}{r'}[(\cos\theta\cos\theta'+\sin\theta\sin\theta')+\mathrm{i}(-\cos\theta\sin\theta'+\sin\theta\cos\theta')]\\&=\frac{r}{r'}[\cos(\theta-\theta')+\mathrm{i}\sin(\theta-\theta')].\end{aligned}$$

因此 zz' 的模是 z 和 z' 模的乘积 $|zz'|=|z||z'|$, zz' 的幅角正是 z 和 z' 幅角之和. 换句话说复数 z' 乘以复数 z 就是把 z 逆时针旋转 θ', 长度乘以 r' 得到的复数. 两个复数相除也有类似解释. 对任意三个互不相等的复数 z_1,z_2,z_3, 有

$$z_3-z_1=(z_2-z_1)r(\cos\theta+\mathrm{i}\sin\theta),$$

这里 θ 是以 z_1,z_2,z_3 为顶点的三角形中z_1 的角,

$$r=\frac{|z_3-z_1|}{|z_2-z_1|}.$$

如果考虑复数 z 反复相乘

$$z^2=r^2(\cos2\theta+\mathrm{i}\sin2\theta),$$

以及

$$z^n = r^n(\cos n\theta + \mathrm{i}\sin n\theta),$$

这里 n 是任意正整数. 将$z = r(\cos\theta + \mathrm{i}\sin\theta)$ 代入上式左边, 并消去 r^n, 最终得到著名的De Moivre（**棣莫弗**, 1667-1754）**公式**:

$$(\cos\theta + \mathrm{i}\sin\theta)^n = \cos n\theta + \mathrm{i}\sin n\theta.$$

De Moivre 公式含义是对一个模长为 1 的复数 , 任何 n 倍复数的幅角是原复数幅角的 n 倍. 在此基础上, Euler 给出了下列著名的公式：

$$\mathrm{e}^{\mathrm{i}\theta} = \cos\theta + \mathrm{i}\sin\theta$$

这里 e 正是第 1 讲 §1.3 中给出的自然常数. 特别取 $\theta = \pi$, Euler 公式就给出了

$$\mathrm{e}^{\mathrm{i}\,\pi} + 1 = 0$$

这个公式把最常见的数 0, 1, π, e 以及虚数单位 i 联系在一起.

这里无法给出 Euler 公式严格证明, 只能从形式上给出解释. 在微积分中, 会给出 e^x 以及 $\sin x$, $\cos x$ 的 Taylor（泰勒, 1685-1731）展开式. 所谓 Taylor 展开式无非是将上述三个函数表示为无限求和形式:

$$\begin{aligned}
\mathrm{e}^x &= \sum_{n=0}^{\infty}\frac{x^n}{n!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots \\
\cos x &= \sum_{n=0}^{\infty}(-1)^n\frac{x^{2n}}{(2n!)} = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \cdots + (-1)^n\frac{x^{2n}}{2n!} + \cdots \\
\sin x &= \sum_{n=0}^{\infty}(-1)^n\frac{x^{2n+1}}{(2n+1)!} = x - \frac{x^3}{3} + \cdots + (-1)^n\frac{x^{2n+1}}{(2n+1)!} + \cdots .
\end{aligned}$$

虽然上述表示是对实数 x 而言, 但如果形式上把实数换成纯虚数 $x = \mathrm{i}\theta$, 代入 e^x 的表达式, 并借助 i 运算规则

$$\mathrm{i}^2 = -1,\ \mathrm{i}^3 = -\mathrm{i},\ \mathrm{i}^4 = 1,\ \cdots$$

不难发现

$$\begin{aligned}
\mathrm{e}^{\mathrm{i}\theta} = \sum_{n=0}^{\infty}\frac{(\mathrm{i}\theta)^n}{n!} &= \left(1 - \frac{\theta^2}{2!} + \frac{\theta^4}{4!} - \cdots + (-1)^m\frac{\theta^{2m}}{(2m)!} + \cdots\right) \\
&\quad + \mathrm{i}\left(\theta - \frac{\theta^3}{3!} + \frac{\theta^5}{5!} - \cdots + (-1)^m\frac{\theta^{2m+1}}{(2m+1)!} + \cdots\right) \\
&= \cos\theta + \mathrm{i}\sin\theta.
\end{aligned}$$

上述推导只是 Euler 公式一个形式上的 “证明” .

利用 Euler 公式, 复数 $x+\mathrm{i}y$ 可以表示成

$$z=x+\mathrm{i}y=r(\cos\theta+\mathrm{i}\sin\theta)=r\mathrm{e}^{\mathrm{i}\theta}$$

因此, 也可用 $\mathrm{e}^{\mathrm{i}\theta}$ 分别表示 $\cos\theta$ 和 $\sin\theta$:

$$\cos\theta=\frac{\mathrm{e}^{\mathrm{i}\theta}+\mathrm{e}^{-\mathrm{i}\theta}}{2},\quad \sin\theta=\frac{\mathrm{e}^{\mathrm{i}\theta}-\mathrm{e}^{-\mathrm{i}\theta}}{\mathrm{i}2}.$$

例 4.2.1 设 $z=\mathrm{e}^{\mathrm{i}\theta}=\cos\theta+\mathrm{i}\sin\theta$, 因此

$$z^k=\mathrm{e}^{\mathrm{i}k\theta}=\cos k\theta+\mathrm{i}\sin k\theta,\ k=1,2,\cdots,$$

当 $\theta\neq 2l\,\boldsymbol{\pi}$ 时, 对 k 求和得

$$\begin{aligned}\sum_{k=1}^{n}\mathrm{e}^{\mathrm{i}k\theta}&=\frac{\mathrm{e}^{\mathrm{i}\theta}-\mathrm{e}^{\mathrm{i}(n+1)\theta}}{1-\mathrm{e}^{\mathrm{i}\theta}}=\frac{\mathrm{e}^{\mathrm{i}\frac{\theta}{2}}-\mathrm{e}^{\mathrm{i}(n+\frac{1}{2})\theta}}{\mathrm{e}^{-\mathrm{i}\frac{\theta}{2}}-\mathrm{e}^{\mathrm{i}\frac{\theta}{2}}}\\&=\frac{\left[\cos\frac{\theta}{2}-\cos\left(n+\frac{1}{2}\right)\theta\right]+\mathrm{i}\left[\sin\frac{\theta}{2}-\sin\left(n+\frac{1}{2}\right)\theta\right]}{-2\mathrm{i}\sin\frac{\theta}{2}}\end{aligned}$$

因此,取实部,得

$$\sum_{k=1}^{n}\cos k\theta=\frac{\sin\left(n+\frac{1}{2}\right)\theta-\sin\frac{\theta}{2}}{2\sin\frac{\theta}{2}}$$

即

$$\frac{1}{2}+\sum_{k=1}^{n}\cos k\theta=\frac{\sin(n+\frac{1}{2})\theta}{2\sin\frac{\theta}{2}},\ \theta\neq 2l\,\boldsymbol{\pi}\,.$$

上述恒等式也可以直接证明. 因为利用三角函数的积化和差, 有

$$\begin{aligned}2\sin\frac{\theta}{2}\left(\frac{1}{2}+\sum_{k=1}^{n}\cos k\theta\right)&=\sin\frac{\theta}{2}+\sum_{k=1}^{n}\left[\sin\left(k+\frac{1}{2}\right)\theta-\sin\left(k-\frac{1}{2}\right)\theta\right]\\&=\sin\left(n+\frac{1}{2}\right)\theta.\end{aligned}$$

§4.3 代数基本定理

重新回到关于代数方程求解问题. 引进复数以后, 是不是仅仅解决如方程 $x^2+1=0$ 或 $x(10-x)=40$ 求解问题? 对其它二次, 乃至更高次数代数方程在复数范围内是否也可以求解?

首先考虑一般实系数 (a,b,c 均为实数, 且 $a\neq 0$) 二次代数方程

$$ax^2+bx+c=0,$$

根据求根公式, 方程的两个解 (有时也称为方程的两个根) 为

$$x_{\pm}=\frac{-b\pm\sqrt{b^2-4ac}}{2a},$$

当 $\Delta=b^2-4ac>0$ 时, 方程有两个实数根.

当 $\Delta=b^2-4ac=0$ 时, 方程有实的重根 $x=-\dfrac{b}{2a}$.

当 $\Delta=b^2-4ac<0$ 时, 方程没有实数根, 但在复数范围内方程有两个互为共轭复数根

$$x_{\pm}=\frac{-b}{2a}\pm \mathrm{i}\frac{\sqrt{|b^2-4ac|}}{2a}.$$

因此, 引进复数后, 对任何实系数二次方程在复数域范围内都可解.

自然希望像求解二次代数方程那样, 利用系数之间加、减、乘、除等四则运算和开平方根、开立方根、开四方根等得到更高次数的代数方程的根. 然而, 这种 “用根式” 求解代数方法到了五次及以上次数的代数方程就行不通了. 事实上, Ruffini (鲁菲尼, 1756-1822) 和 Abel (阿贝尔, 1802 $\sim$ 1829) 证明了不可能用根式的方法解一般 n 代数方程. 这一结果进一步促成了新的数学重大发展. 具体内容在第 7 讲中还将继续讨论. 需要指出的是, 五次及以上的代数方程求根问题, 虽然不能像二次代数方程那样用开方方法求根, 但并不表示高次代数方程的根不存在.

事实上, 下列定理解决了任意次代数方程根的存在性问题, 并被称为**代数基本定理**:

定理 4.2 *复系数的 n 次代数方程*

$$x^n+a_{n-1}x^{n-1}+\cdots a_1x+a_0=0.$$

在复数域中至少存在一个根. 这里不失一般性, 假设首项系数为 1.

推论 4.3 *复系数多项式*

$$f(x)=x^n+a_{n-1}x^{n-1}+\cdots a_1x+a_0$$

可以分解为 n 个因式的乘积

$$f(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n),$$

其中 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 是复数. 显然它们是 n 次代数方程 $f(x)=0$ 的根. 或者说任何一个 n 次代数方程一定有 n 个根 (重根的重数计作根的个数) .

关于代数基本定理证明, 已经超出了本专题范围, 在此不再介绍. 这里着重强调这样一件事情, 虽然 $n(n\geqslant 5)$ 次代数方程的根无法像二次代数方程那样通过系数之间的四则运算和开根号求出, 但代数基本定理告诉我们, n 次代数方程在复数范围内存在 n 个根. 并不需要随着 n 的不同去创造其它什么新的数.

推论 4.4 如果

$$f(x)=x^n+a_{n-1}x^{n-1}+\cdots a_1x+a_0$$

是实系数多项式, 那么

(i) 若 $z_0=x_0+iy_0$ 是方程 $f(x)=0$ 复数根, 则它的共轭 $\overline{z}_0=x_0-iy_0$ 也是方程的根, 也就是实系数代数方程的复根成对$(z_0,\overline{z}_0)$ 出现.

(ii) 实系数多项式一定能够分解为下列形式

$$f(x)=(x-\alpha_1)^{r_1}\cdots(x-\alpha_k)^{r_k}(x^2+\beta_1x+\gamma_1)^{s_1}\cdots(x^2+\beta_lx+\gamma_l)^{s_l},$$

这里$\alpha_i,\beta_j,\gamma_j$ 都是实数, 满足

$$\beta_j^2-4\gamma_j<0,\ j=1,2,\cdots,l.$$

$r_j,\ j=1,\cdots,k$ 是方程实根的重数, $s_j,\ j=1,\cdots,l$ 是成对出现的复根的重数, 因此有

$$r_1+\cdots+r_k+2s_1+\cdots+2s_l=n.$$

读者可作为习题自证.

注记 上述定理和推论表示在复数域上不可约多项式(见第 2 讲§2.8)只能是一次多项式, 而实数域上不可约多项式具有下列形式

$$x-\alpha\quad 或\quad x^2+\beta x+\gamma\ \ (\beta^2-4\gamma<0).$$

§4.4 单位根

定义 4.5 复数 ξ 称为(复)**单位根**, 如果存在某个正整数 n, 使 ξ 满足方程

$$z^n-1=0.$$

对固定的 n, 上述方程 n 个根记为 $\xi_1,\xi_2,\cdots,\xi_n$, 称为n **次单位根**.

例如当 $n=2$ 时, 方程 $z^2-1=0$ 有两个 2 次单位根: $\xi_1=-1,\ \xi_2=1$.

当 $n=3$ 时, 方程 $z^3-1=0$ 有三个 3 次单位根:

$$\xi_1=\cos\frac{2\pi}{3}+\mathrm{i}\sin\frac{2\pi}{3}=-\frac{1}{2}+\mathrm{i}\frac{\sqrt{3}}{2},$$
$$\xi_2=\cos\frac{4\pi}{3}+\mathrm{i}\sin\frac{4\pi}{3}=-\frac{1}{2}-\mathrm{i}\frac{\sqrt{3}}{2},$$
$$\xi_3=1.$$

当 $n=4$ 时, 方程 $z^4-1=0$ 有四个 4 次单位根:

$$\begin{aligned}\xi_1&=\cos\frac{2\pi}{4}+\mathrm{i}\sin\frac{2\pi}{4}=\mathrm{i}\\ \xi_2&=\cos\frac{4\pi}{4}+\mathrm{i}\sin\frac{4\pi}{4}=-1,\\ \xi_3&=\cos\frac{6\pi}{4}+\mathrm{i}\sin\frac{6\pi}{4}=-\mathrm{i},\\ \xi_4&=1.\end{aligned}$$

一般情况下, 根据De Moivre 公式, 方程 $z^n-1=0$ 有n 个互不相等的单位根:

$$\xi_k=\cos\frac{2k\pi}{n}+\mathrm{i}\sin\frac{2k\pi}{n}=\mathrm{e}^{2k\mathrm{i}\pi/n},\ k=1,2,\cdots,n.$$

在复平面上, 这些单位根对应的点恰好把单位圆 $|z|=1$ 分成 n 等分, 其中一个分点为 $\xi_n=1$. 我们把互不相等的 n 次单位根的集合记为

$$D_n=\{\xi_1,\xi_2,\cdots,\xi_n\}.$$

直接验证就可得到下列定理.

定理 4.6 集合 D_n 满足下列性质, 因此是一个乘法群.

(i) 在复数的乘法运算下是封闭的, 即对 $\xi_i,\ \xi_j\in D_n$, 有

$$\xi_i\xi_j=\xi_k\in D_n,\ \text{其中 } k \text{ 满足 } (i+j)\equiv k\ (\mathrm{mod}\ n),$$

(ii) 有单位元 $\xi_n=1\in D_n$, 并对任何 $\xi_i\in D_n$ 有逆元

$$\xi_i^{-1}=\xi_{n-i}\in D_n.$$

注意到在4次单位根中, $\xi_2=-1$ 实际上也是 2 次单位根: $\xi_2^2=1$, 但 ξ_1,ξ_3 不是. 自然要问, D_n 中哪些 n 次单位根也是更低次数的单位根?

定义 4.7 设 ξ 是单位根, 若 d 是使得 $\xi^d=1$ 成立最小正整数, 则称 d 为 ξ 的***阶***. 若 $\xi\in D_n$ 且 ξ 的阶恰好是 $d=n$, 则称 ξ 是***本原的*** n ***次单位根***.

根据定义, 在 4 次单位根的集合 D_4 中, ξ_2 的阶是2, ξ_4 的阶是 1, 只有 ξ_1,ξ_3 的阶是 4, 因此是本原的. 在 D_3 中, 除了 ξ_3 外, ξ_1,ξ_2 是本原的.

下面的任务是在单位根中如何区分哪些根是本原的, 本原单位根有哪些性质.

定理 4.8 设单位根 ξ 的阶是 d .

(i) ξ 是 n 次单位根当且仅当 $d\mid n$.

(ii) 对于整数 k, ξ^k 的阶仍为 d 当且仅当 k 与 d 互素: $(k,d)=1$.

证明 (i) 的证明: 若 $\xi^n=1$, 显然 $n\geqslant d$, 令 $n=qd+r,\ 0\leqslant r<d$. 由 $\xi^d=1$ 得

$$1=\xi^n=\xi^{qd}\xi^r=(\xi^d)^q\xi^r=\xi^r,$$

因为 d 是使得 $\xi^d=1$ 成立最小正整数, 所以 $r=0$, 即 $d\mid m$. 反之显然.

(ii) 的证明: 设 ξ^k 的阶为 d. 若 $(k,d)=c>1$, 则存在 $k'<k, d'<d$ 使得$k=k'c,\ d=d'c$. 所以

$$(\xi^k)^{d'}=\xi^{k'd'c}=(\xi^d)^{k'}=1,$$

但 $d'<d$, 这与 ξ^k 的阶是 d 矛盾, 因此 $(k,d)=1$.

设 ξ^k 的阶是 d', 因为 $(\xi^k)^d=(\xi^d)^k=1$, 所以ξ^k 的阶d' 满足 $d'\leqslant d$.

若 $d'<d$, 从 $\xi^{kd'}=1$ 推出 $d\mid kd'$, 而 $(k,d)=1$, 所以 $d\mid d'$, 这与 $d'<d$ 矛盾, 因此 $d'=d$. □

定理 4.9 *ξ 是一个本原的 n 次单位根, 当且仅当 D_n 中所有n 次单位根可由 ξ 的幂次生成, 也就是集合 D_n 可表示为*

$$D_n=\{\xi^0,\xi,\xi^2,\cdots,\xi^{n-1}\}.$$

证明 设 ξ 是一个本原的 n 次单位根, 显然 n 个数 $\xi^0,\xi,\xi^2,\cdots,\xi^{n-1}$ 都是 n 次单位根, 因此只要证明它们互不相同, 就表明它们构成所有的 n 次单位根的集合. 假如有

$$\xi^i=\xi^j\quad(0\leqslant i<j\leqslant n-1),$$

则 $\xi^{j-i}=1$, 但 $0<j-i<n$, 这与 ξ 是 n 次本原单位根矛盾.

反之, 设 D_n 中元素均由 n 次单位根 ξ 的幂次生成 $D_n=\{\xi^0,\xi,\xi^2,\cdots,\xi^{n-1}\}$, 记 ξ 的阶为 d. 若 $d<n$, 那么 ξ 的任何幂次 ξ^i 都满足 $(\xi^i)^d=1$, 也就是它们都是d 次单位根.即 $D_n\subset D_d$, 这是不可能的, 因为 D_d 中只有 d 个元素. □

对方程 $z^n-1=0$ 来说, 它的 n 次单位根中

$$\xi=\xi_1=\mathrm{e}^{2\pi\mathrm{i}/n}=\cos\frac{2\pi}{n}+\mathrm{i}\sin\frac{2\pi}{n}$$

是本原的, 因为 $(1,n)=1$. 因此 n 次单位根的集合 D_n 可以表示为

$$D_n=\{\xi^0,\xi,\xi^2,\cdots,\xi^{n-1}\}.$$

根据定理4.9, 只要 $(k,n)=1$, 则 D_n 中的 ξ^k 就是本原的, 因此, D_n 中本原的单位根的个数正是$1,2,\cdots,n$ 中与 n 互素的数的个数, 这个数就是Euler 函数 $\varphi(n)$ (见第 2 讲定义2.16) . 这样, 本原的 n 次单位根的集合为

$$B_n=\{\xi^k\mid\ 1\leqslant k\leqslant n,\ (k,n)=1\}$$

每个本原的 n 次单位根 $\xi^k \in B_n$, 都可通过幂次生成所有的 n 次单位根

$$D_n = \{1, \xi^k, \xi^{2k}, \cdots, \xi^{(n-1)k}\}, \quad \xi^k \in B_n.$$

因为 D_n 中的数对应复平面中单位圆上的 n 个等分点, 其中 $\xi_n = 1$ 在实轴上. 因此, 从几何上看, 即是从实轴出发, 沿单位圆旋转 $\dfrac{2\,\pi}{n}$, 则可跑遍所有等分点. 若对本原的 ξ^k, 因为 $(k, n) = 1$, 所以旋转 $\dfrac{2k\,\pi}{n}$, 也能跑遍所有等分点.

继续考虑方程 $z^n - 1 = 0$, 利用

$$z^n - 1 = (z-1)(z^{n-1} + z^{n-2} + \cdots + z + 1),$$

不难看出除 1 以外的 n 次单位根 ξ, ξ^2, $\cdots$, ξ^{n-1} 满足方程

$$z^{n-1} + z^{n-2} + \cdots + z + 1 = 0,$$

对应的多项式也有下列因式分解

$$z^{n-1} + z^{n-2} + \cdots + z + 1 = (z - \xi)(z - \xi^2)\cdots(z - \xi^{n-1}).$$

例如三次单位根

$$\xi = \cos\frac{2\,\pi}{3} + \mathrm{i}\sin\frac{2\,\pi}{3} = \frac{1}{2}(-1 + \mathrm{i}\sqrt{3}),$$
$$\xi^2 = \cos\frac{4\,\pi}{3} + \mathrm{i}\sin\frac{4\,\pi}{3} = \frac{1}{2}(-1 - \mathrm{i}\sqrt{3}).$$

是方程

$$x^2 + x + 1 = 0$$

的根. 同样地, 五次单位根除 1 以外都满足方程

$$x^4 + x^3 + x^2 + x + 1 = 0.$$

如果直接求解这个方程, 可作一些简单的代数变换, 先在方程两边除以 x^2 得

$$x^2 + x + 1 + \frac{1}{x} + \frac{1}{x^2} = 0$$

再作变换

$$z = x + \frac{1}{x},$$

方程就化为一个 2次方程

$$z^2 + z - 1 = 0.$$

求出它的两个根为

$$z_1 = \frac{-1 + \sqrt{5}}{2}, \ z_2 = \frac{-1 - \sqrt{5}}{2}.$$

再分别求解

$$x+\frac{1}{x}=\frac{-1\pm\sqrt{5}}{2}$$

就得到1 的五次复根. 上述方程能否用系数的代数运算和开方运算求解, 是判断能否用直尺和圆规作出正五边形的关键 (见第 6 讲) .

§4.5 复变数函数*

在第 2节中, 实际上已经把常见的实变数函数 $f(x)=\mathrm{e}^x$ 换成了复变数函数 $f(z)=\mathrm{e}^z$, 只不过限制z 为纯虚数 $z=\mathrm{i}\theta$. 那么是不是可以把定义在实数某个区域内初等函数的定义域都换成复数的某个区域. 下面, 通过一些具体的例子可以看到, 事情并不是那么简单, 即使可以定义类似的复变数函数, 函数的性质也发生了变化.

一般来说, 所谓复变数函数是指从复数的某个区域内 $D\subset\mathbb{C}$ 到复数的一个映射

$$f:\ D\subset\mathbb{C}\longrightarrow\mathbb{C},$$

或写成

$$f:\ z\in D\longmapsto w\in\mathbb{C}$$

记为 $w=f(z)$. 若对于每一个 $z\in D$, 有唯一复数 w 与之对应, 则称函数 (或映射) 在 D 内是**单值的**. 若有多个 w 与之对应, 则称函数是 **多值的**. 对于 D 内单值函数, 若对任意两个 $z_1,\ z_2\in D$, 对应两个不同的 $w_1,\ w_2$, 则称函数在 D 内是**单叶的**.

以下仅讨论几个具体例子.

1° 幂函数

考虑下列三种特殊情形:

(a) $w=z^n$, 这里 n 是正整数.

这是 n 个相同的复数 z 相乘, 其结果还是一个复数, 因此是单值的. 如果令

$$z=r(\cos\theta+\mathrm{i}\sin\theta),\ w=\rho(\cos\varphi+\mathrm{i}\sin\varphi),$$

那么

$$\rho=r^n,\ \varphi=n\theta.$$

从上式不难看出, 两个模相等复数 z_1,z_2 映射到同一个点 (即 $z_1^n=z_2^n$) , 当且仅当它们的幅角相差 $\dfrac{2\pi}{n}$ 整数倍. 因此要使映射 $w=z^n$ 是单叶的, 充分必要条件是定义域 D 内

任意两个点 z_1, z_2, 都不满足

$$|z_1| = |z_2|, \quad \text{或} \quad \arg z_1 - \arg z_2 = \frac{2k\,\pi}{n},\ k \neq 0 \text{ 是整数.}$$

例如, 扇形区域

$$D = \{z \;\Big|\; 0 < \arg z < \frac{2\,\pi}{n}\}$$

就是一个能保证映射 $w = z^n$ 单叶性的区域. 这个扇形区域被映射 $w = z^n$ 1-1 映射到

$$\widetilde{D} = \{w \;\Big|\; 0 < \arg w < 2\,\pi\,\}$$

即映到去掉正半轴的复平面.

(b) $w = \sqrt{z} = z^{\frac{1}{2}}$.

设 $z = r(\cos\theta + \mathrm{i}\sin\theta)$, 则

$$z \longrightarrow z^{\frac{1}{2}} = \begin{cases} r^{\frac{1}{2}}\left(\cos\frac{\theta}{2} + \mathrm{i}\sin\frac{\theta}{2}\right) = w \\ r^{\frac{1}{2}}\left(\cos\frac{\theta+2\,\pi}{2} + \mathrm{i}\sin\frac{\theta+2\,\pi}{2}\right) = -w. \end{cases}$$

因此, $w = z^{\frac{1}{2}}$ 是一个多值函数.

进一步分析发现, 当 z 绕一个不包含原点封闭曲线旋转一圈并回到原处, 那么z的幅角不会发生改变, 如果 z 绕包含原点封闭曲线旋转一圈并回到原处, 那么幅角 $\theta \to \theta + 2\,\pi$. 此时 $w = z^{\frac{1}{2}}$ 的函数值会产生如下变化

$$\begin{aligned} w &= r^{\frac{1}{2}}\left(\cos\frac{\theta}{2} + \mathrm{i}\sin\frac{\theta}{2}\right) \\ &\longrightarrow r^{\frac{1}{2}}\left(\cos\frac{\theta+2\,\pi}{2} + \mathrm{i}\sin\frac{\theta+2\,\pi}{2}\right) \\ &\longrightarrow -r^{\frac{1}{2}}\left(\cos\frac{\theta}{2} + \mathrm{i}\sin\frac{\theta}{2}\right) = -w. \end{aligned}$$

为了避免多值性, 我们把函数 $w = z^{\frac{1}{2}}$ 定义域所在复平面 $\mathbb{C}$ 从原点 0 到无穷 ∞ 剪开一个口子, 例如, 沿 x 轴正半轴剪开, 这样使得在剪开后定义域内无法形成任何包含原点封闭曲线, 也就避免了出现多值性. 或者说如果限制 z 的幅角取值在 $0 \leqslant \theta < 2\,\pi$ 范围内, 就可以保证函数的单值性.

一般函数 $w = \sqrt[n]{z} = z^{\frac{1}{n}}$ 与 $w = \sqrt{z} = z^{\frac{1}{2}}$ 性质类似.

(c) $w = z^{-1} = \dfrac{1}{z}$.

显然该映射的定义域为 $z \neq 0$. 设 $z = r\mathrm{e}^{\mathrm{i}\theta}$, 则

$$w = \frac{\overline{z}}{|z|^2} = \frac{1}{r}\mathrm{e}^{-\mathrm{i}\theta},$$

所以映射把 z 所在的复平面上单位圆盘内除 0 以外的点映射到 w 所在的平面单位圆盘外的点 .

2° **指数函数**

这里, 按下列方式引进指数函数

$$w = \mathrm{e}^z = \mathrm{e}^{x+\mathrm{i}y} = \mathrm{e}^x\mathrm{e}^{\mathrm{i}y} = \mathrm{e}^x(\cos y + \mathrm{i}\sin y),$$

它满足:

$$\mathrm{e}^{z_1}\mathrm{e}^{z_2} = \mathrm{e}^{z_1+z_2},$$

并且是以 $2\pi\mathrm{i}$ 为周期的周期函数

$$\mathrm{e}^{z+2\pi\mathrm{i}} = \mathrm{e}^z.$$

和通常一样, 对数函数定义为指数函数反函数. 把满足方程

$$\mathrm{e}^w = z \ (z \neq 0)$$

的函数 $w = f(z)$ 称为对数函数. 令 $w = u + iv,\ z = r\mathrm{e}^{\mathrm{i}\theta}$, 那么

$$\mathrm{e}^{u+\mathrm{i}v} = r\mathrm{e}^{\mathrm{i}\theta},$$

所以 $u = \ln r,\ v = \theta$, 因此

$$w = \ln|z| + \mathrm{i}\mathrm{Arg}z.$$

由于Arg$z$ 为多值函数, 所以对数函数 $w = f(z)$ 是多值函数, 并且每两个值相差 $2\pi\mathrm{i}$ 整数倍. 如果规定 Arg$z$ 取主值 arg$z$, 那么对数函数就是一个单值函数, 记为

$$\ln z = \ln|z| + \mathrm{i}\arg z.$$

3° **三角函数**

借助指数函数, 定义

$$\cos z = \frac{\mathrm{e}^{\mathrm{i}z} + \mathrm{e}^{-\mathrm{i}z}}{2},\ \sin z = \frac{\mathrm{e}^{\mathrm{i}z} - \mathrm{e}^{-\mathrm{i}z}}{2\mathrm{i}}$$

为复数 z 余弦函数和正弦函数. 由指数函数性质, 不难验证这样定义复变数三角函数满足与实变数三角函数类似性质. 其他三角函数也可类似定义.

4° **双曲函数**

类似复变数三角函数的定义, 还可以定义下列复变数双曲函数:

$$\cosh z = \frac{\mathrm{e}^z + \mathrm{e}^{-z}}{2},\ \sinh z = \frac{\mathrm{e}^z - \mathrm{e}^{-z}}{2}$$

它们也具有实变数双曲函数类似性质.

5° **Rokovsky 函数**

Rokovsky (茹科夫斯基, 1847-1921) 函数定义如下:

$$w = f(z) = \frac{1}{2}\left(z + \frac{1}{z}\right) \ (z \neq 0).$$

首先讨论该函数的单叶性. 若有两个 $z_1 \neq z_2$, 使得 $f(z_1) = f(z_2)$, 那么

$$(z_1 - z_2)\left(1 - \frac{1}{z_1 z_2}\right) = 0,$$

由此推出

$$z_1 z_2 = 1.$$

所以, $w = f(z)$ 是单叶的充分必要条件是定义域 D 内任何两个点 z_1, z_2 满足 $z_1 z_2 \neq 1$. 不难看出, 在单位圆内部 $D = \{z \mid |z| < 1, z \neq 0\}$, 或单位圆外部 $D' = \{z \mid |z| > 1\}$ 都可以保证函数单叶性. 以下不妨取 $D = \{z \mid |z| < 1, z \neq 0\}$ 作为函数定义域.

令 $z = r(\cos\theta + \mathrm{i}\sin\theta),\ w = u + \mathrm{i}v$, 则映射可以表示为

$$u = \frac{1}{2}\left(r + \frac{1}{r}\right)\cos\theta, \quad v = \frac{1}{2}\left(r - \frac{1}{r}\right)\sin\theta$$

如果取定 $r = r_0 < 1$, 那么 $|z| = r_0$ 给出单位圆内部一个同心圆. 令

$$a = \frac{1}{2}\left(r_0 + \frac{1}{r_0}\right),\ b = \frac{1}{2}\left(\frac{1}{r_0} - r_0\right)$$

则

$$u = a\cos\theta,\ v = -b\sin\theta,\ \text{或}\ \frac{u^2}{a^2} + \frac{v^2}{b^2} = 1$$

是 w 所在复平面上椭圆. 当 z 所在复平面上点沿圆 $|z| = r_0$ 从 $\theta = 0$ 逆时针转动, 则 w 所在复平面上对应点从 $w = a$ 出发顺时针转动.

当 $|z| = r_0$ 从单位圆内部逐渐接近单位圆时, w 所在平面上的椭圆压缩成 u 轴上一段线段 $[-1, 1]$. 当 $|z| = r_0$ 收缩到原点时, 对应的椭圆趋向无穷.

如果取定 $\theta = \theta_0$, 那么 $z = r(\cos\theta_0 + \mathrm{i}\sin\theta_0),\ 0 < r < 1$ 是z 所在单位圆内部一段射线段, 在茹科夫斯基函数映射下, 该线段对应 w 所在复平面上下列双曲线上的一段

$$\frac{u^2}{\cos^2\theta_0} - \frac{v^2}{\sin^2\theta_0} = 1.$$

第 4 讲习题

1. 计算 $\sqrt{5+\mathrm{i}12}$.

2. 设 z_1, z_2, z_3 均是模为一的复数, 且满足 $z_1+z_2+z_3=0$, 证明: $z_1^2+z_2^2+z_3^2=0$

3. 证明: 单位圆上任意一点 P 到单位元内接正 n 边形各顶点 $A_1, A_2, \cdots, A_n$ 距离的平方和是一个定值.
   提示: 在复平面上作圆心在原点 O 的单位圆, 使得射线 OA_n 是实轴的正半轴. 则正 n 边形顶点 $A_1, A_2, \cdots, A_n$ 对应的复数分别为 $\xi, \xi^2, \xi^3, \cdots, \xi^n$, 这里 $\xi = e^{2\pi i/n}$, $\xi^n = 1$. 再设单位圆上任意点 P 对应的复数为 z, $|z|=1$, 直接用复数计算 P 到各顶点距离的平方和即可.

4. 定义两个复数 $z=x+\mathrm{i}y$, $z'=x'+\mathrm{i}y'$ 之间的序关系如下:
   若 $x<x'$, 或者 $x=x'$ 但 $y<y'$, 就规定 $z<z'$.
   证明: 在上述定义下, 复数集合 $\mathbb{C}$ 是有序集 (参见定义3.4), 但不满足确界原理.
   提示: 设 $E=\{z=x+\mathrm{i} \mid 0 \leqslant x<1\}$, 那么任意 $1+\mathrm{i}y$ 都是实部最小的上界, 由于 y 的任意性, 因此没有最小上界.

5. 设四个任意复数 z_1, z_2, z_3, z_4, 证明: 这四个数同在一个圆上或一条直线上当且仅当 $\dfrac{z_4-z_1}{z_4-z_2}$ 和 $\dfrac{z_3-z_1}{z_3-z_2}$ 有相同的幅角, 或者说
   $$\frac{z_4-z_1}{z_4-z_2}\Big/\frac{z_3-z_1}{z_3-z_2}$$
   是实数.

6. 利用复数的极坐标表示, 证明余弦公式
   $$c^2=a^2+b^2-2ab\cos\theta.$$
   其中 a, b, c 分别是三角形的三条边的长度, θ 是边 c 的对应角.

7. 对任意的正整数 n, 证明下列等式
   $$\sum_{k=1}^{n}\cot^2\frac{k\pi}{2n+1}=\frac{2n(2n-1)}{6}$$
   提示: 由
   $$\cos(2n+1)x+\mathrm{i}\sin(2n+1)x=(\cos x+\mathrm{i}\sin x)^{2n+1}=\sin^{2n+1}x(\cot x+\mathrm{i})^{2n+1},$$
   将 $(\cot x+\mathrm{i})^{2n+1}$ 展开并比较等式两边的虚部得
   $$\sin(2n+1)x=\sin^{2n+1}x\sum_{j=0}^{n}(-1)^j\binom{2n+1}{2j+1}(\cot^{2(n-j)}x),$$

记n 次多项式

$$P(t)=\sum_{j=0}^{n}(-1)^j\binom{2n+1}{2j+1}t^{n-j}.$$

令 $x=\dfrac{k\,\pi}{2n+1}$, 推出

$$P\left(\cot^2\frac{k\,\pi}{2n+1}\right)=0, k=1,2,\cdots n.$$

即 $\cot^2\dfrac{k\,\pi}{2n+1}$ $(k=1,2,\cdots n)$ 是 $P(t)$ 的 n 个根, 由根与系数的关系即可证得.

8. 对任意的正整数 n, 证明下列等式

$$\sin\frac{\pi}{n}\sin\frac{2\,\pi}{n}\cdots\sin\frac{(n-1)\,\pi}{n}=\frac{n}{2^{n-1}}.$$

提示: 利用 n 次方程 $z^n-1=0$ 的 n 个单位根

$$\xi_k=e^{2\mathrm{i}k\,\pi/n}, k=1,2,\cdots n,$$

其中 $\xi_1,\xi_2,\cdots,\xi_{n-1}$ 满足方程 $z^{n-1}+z^{n-2}+\cdots+z+1=0$. 再利用因式分解

$$z^{n-1}+z^{n-2}+\cdots+z+1=(z-\xi_1)(z-\xi_2)\cdots(z-\xi_{n-1}),$$

将 $z=1$ 代入, 并求两边的模长即可.

9. 列出所有的 12 次本原单位根.

10. 设 z 是任意的复数, 试证: 对任意的正整数 n, $z^n+\dfrac{1}{z^n}$ 可以表示为 $w=z+\dfrac{1}{z}$ 的 n 次多项式.

11. 证明茹科夫斯基函数

$$f(z)=\frac{1}{2}\left(z+\frac{1}{z}\right),$$

当 $|z|=1$ 时, $f(z)\in[-1,1]$.

12. 求下列函数的最大值

$$f(x)=\sqrt{x^4-3x^2-6x+13}-\sqrt{x^4-x^2+1}$$

提示: 首先将两个根号内部表示成平方和的形式

$$f(x)=\sqrt{(x-3)^2+(x^2-2)^2}-\sqrt{x^2+(x^2-1)^2}$$

并令

$$z_1=(x-3)+\mathrm{i}(x^2-2),\ z_2=x+\mathrm{i}(x^2-1),$$

这样

$$f(x)=|z_1|-|z_2|\leqslant|z_1-z_2|=\sqrt{10}.$$

再利用不等式中等号成立的条件即可.

13. 设在平面上四边形 $ABCD$ 内有一点 O, 使得 $\triangle OAB$ 和 $\triangle OCD$ 都是以 O 为直角顶点的等腰直角三角形, 求证: 必存在一点 P, 使得 $\triangle PBC$ 和 $\triangle PDA$ 都是以 P 为直角顶点的等腰直角三角形.

提示: 以 O 为原点作复平面, 并设 A,B,C,D 点对应的复数为 z_A, z_B, z_C, z_D. 根据题意有

$$z_B=\mathrm{i}z_A,\ z_D=\mathrm{i}z_C.$$

设 P 点对应复数为z_P,那么要使 $\triangle PBC$ 和 $\triangle PDA$ 都是以 P 为直角顶点的等腰直角三角形, 只要

$$z_p-z_C=\mathrm{i}(z_P-z_B)=\mathrm{i}(z_P-\mathrm{i}z_A),$$
$$z_P-z_A=\mathrm{i}(z_P-z_D)=\mathrm{i}(z_P-\mathrm{i}z_C)$$

同时成立. 显然, 这样的 z 有解.

14. 设 D 是锐角三角形 $\triangle ABC$ 内部一点, $\angle ADB=\angle ACB+90^\circ$, 并且

$$AC\cdot BD=AD\cdot BC.$$

求

$$\frac{AB\cdot CD}{AC\cdot BD}$$

的值.

提示: 如图4.1所示

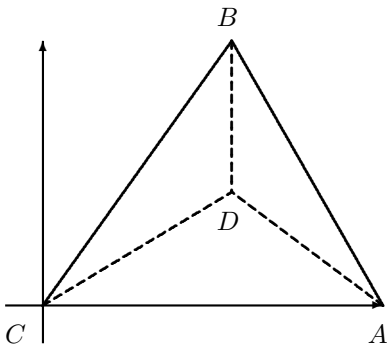


图 4.1

分别记点 A, B, D 对应的复数为 z_A, z_B, z_D, 那么题目的条件为

$$|z_A||z_B - z_D| = |z_B||z_A - z_D|,$$

要证

$$\frac{|z_A - z_B||z_D|}{|z_A||z_B - z_D|}.$$

利用

$$(z_B - z_D) = (z_A - z_D)r(\cos\theta + \mathrm{i}\sin\theta),$$

其中

$$r = \frac{|z_B - z_D|}{|z_A - z_D|},\ \theta = \angle ACB + 90^\circ.$$

并注意到

$$\cos\theta + \mathrm{i}\sin\theta = \mathrm{i}(\cos\angle ACB + \mathrm{i}\sin\angle ACB) = \frac{1}{|z_B|}z_B,$$

即可证得结果.

第 5 讲　解析几何与向量空间

在解析几何中, 通过引进坐标, 使得一些几何问题可以用代数方法来研究. 首先对平面解析几何做一个简要回顾.

在平面上取定一个点 O（称为原点）和交于该点的相互垂直的有向数轴, 就构成了平面坐标系. 平面上任何一点 P 都唯一对应一个数组 (x,y), 称为 P 点的坐标 (图5.1). 也可以说, 坐标系的建立, 使得平面上的点完全“数字化”了.

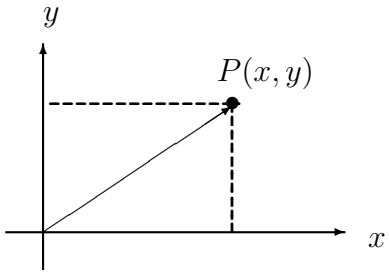


图 5.1

在坐标系中, 平面上任何两点 $P_1(x_1,y_1)$, $P_2(x_2,y_2)$ 距离可由点的坐标之间代数运算给出:

$$\rho(P_1,P_2)=\sqrt{(x_1-x_2)^2+(y_1-y_2)^2}$$

也可以把一些几何图形用代数方程表示.

例 5.0.1　已知椭圆是平面上到两定点 F_1 和 F_2 距离等于常数的动点轨迹, 试求椭圆的代数方程.

解　不妨取坐标系使得两定点坐标分别为 $F_1(p,0)$ 和 $F_2(-p,0)$. 那么, 任意动点 $P(x,y)$ 到 $F_1(p,0)$ 和 $F_2(-p,0)$ 的距离为

$$r_1=|PF_1|=\sqrt{(x-p)^2+y^2},\quad r_2=|PF_2|=\sqrt{(x+p)^2+y^2},$$

根据题意, 两者之和为常数 $r_1+r_2=2a$（显然 $a>p$, 否则无解）, 那么有

$$r_2^2-r_1^2=\begin{cases}(x+p)^2-(x-p)^2=4px,\\ (r_2+r_1)(r_2-r_1)=2a(r_2-r_1)\end{cases}$$

因此得到 $r_2-r_1=\dfrac{2px}{a}$, 与 $r_2+r_1=2a$ 联立解得

$$r_1=a-\frac{px}{a},\quad r_2=a+\frac{px}{a}.$$

把 r_1 代入 $r_1^2=(x-p)^2+y^2$:

$$\left(a-\frac{px}{a}\right)^2=(x-p)^2+y^2.$$

记 $b=\sqrt{a^2-p^2}$, 整理后即可得到椭圆上任意动点 $P(x,y)$ 的坐标所满足的代数方程

$$\frac{x^2}{a^2}+\frac{y^2}{b^2}=1,$$

其中 $a>b>0$ 分别称为椭圆的长半轴和短半轴, $F_1(p,0)$ 和 $F_2(-p,0)$称为椭圆焦点.

§5.1 向量及其代数运算

为了更好地用代数表示解决几何问题, 需要借助“向量”概念. 所谓向量来源于物理学, 一些物理量不仅有大小, 还有方向. 例如位移、力、速度、加速度等等, 抛开它们的物理意义, 只保留大小和方向两个要素, 就抽象为数学中向量概念. 因此, 向量就是**既有大小, 又有方向的量**.

一般用有向线段表示一个向量, 线段的长度表示向量的大小, 线段的方向表示向量的方向. 空间中以 A 为起点, B 为终点的有向线段表示的向量记为 $\overrightarrow{AB}$. 有时为了方便, 常用黑体小写字母 $\boldsymbol{a},\boldsymbol{b},\boldsymbol{e},\boldsymbol{n},\boldsymbol{v},\boldsymbol{x}$ 等表示向量.

若两个向量大小相等、方向相同, 则两者相等. 相等向量可以通过不改变大小和方向的平移使之重合. 通过平移, 使任何向量 $\boldsymbol{a}$ 等同于起点在原点的向量 $\boldsymbol{a}=\overrightarrow{OA}$.

有三种向量比较特别, 大小为 0 称为**零向量**; 大小等于 1 向量称为**单位向量**, 与向量 $\boldsymbol{a}$ 大小相等, 但方向相反向量, 称为 $\boldsymbol{a}$ 的**负向量**(或反向量),记为 $-\boldsymbol{a}$.

1° 向量的加法和数乘

设 $\boldsymbol{a},\boldsymbol{b}$ 是两个向量, 用起点为 O 的两个有向线段表示它们: $\boldsymbol{a}=\overrightarrow{OA},\boldsymbol{b}=\overrightarrow{OB}$, 则以 $\overrightarrow{OA},\overrightarrow{OB}$ 为邻边的平行四边形的对角线向量 $\boldsymbol{c}=\overrightarrow{OC}$ 就称为这两个向量的**加法**或**和**, 记作

$$\overrightarrow{OC}=\overrightarrow{OA}+\overrightarrow{OB} \quad \text{或简写成} \quad \boldsymbol{c}=\boldsymbol{a}+\boldsymbol{b}.$$

这种相加方法称为**平行四边形法则** (图 5.2). 也可以用**三角形法则** (图 5.3), 即以 $\boldsymbol{a}$ 的终点 A 为起点, 做一有向线段使其等于 $\boldsymbol{b}$: $\overrightarrow{AB}=\boldsymbol{b}$, 则以 O 为起点, B 为终点向量 $\overrightarrow{OB}$ 就是 $\boldsymbol{a}$ 与 $\boldsymbol{b}$ 的和

$$\boldsymbol{a}+\boldsymbol{b}=\overrightarrow{OA}+\overrightarrow{AB}=\overrightarrow{OB}.$$

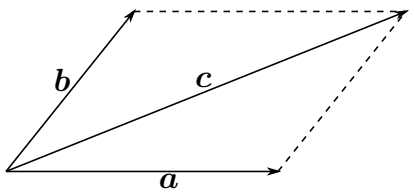


图 5.2

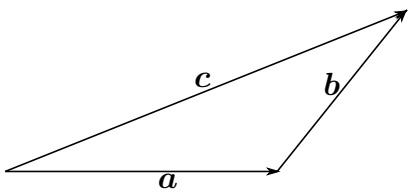


图 5.3

设 $\boldsymbol{a}=\overrightarrow{OA},\ \boldsymbol{b}=\overrightarrow{OB}$, 则 $-\boldsymbol{b}=\overrightarrow{BO}$, 因此

$$\boldsymbol{a}-\boldsymbol{b}=\boldsymbol{a}+(-\boldsymbol{b})=\overrightarrow{OA}+(-\overrightarrow{OB})=\overrightarrow{OA}+\overrightarrow{BO}=\overrightarrow{BA}$$

性质 5.1 向量加法满足如下性质:

(i) $\boldsymbol{a}+\boldsymbol{b}=\boldsymbol{b}+\boldsymbol{a}$, (交换律)

(ii) $(\boldsymbol{a}+\boldsymbol{b})+\boldsymbol{c}=\boldsymbol{a}+(\boldsymbol{b}+\boldsymbol{c})$, (结合律)

(iii) $\boldsymbol{a}+\boldsymbol{0}=\boldsymbol{a}$, $\boldsymbol{a}+(-\boldsymbol{a})=\boldsymbol{0}$.

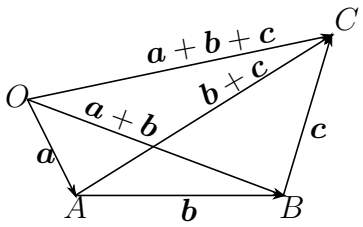


图 5.4

证明 从向量求和的平行四边形法则容易看出交换律成立. 而用三角形法则较易证明结合律 (图 5.4).

设 $\boldsymbol{a}=\overrightarrow{OA}$, $\boldsymbol{b}=\overrightarrow{AB}$, $\boldsymbol{c}=\overrightarrow{BC}$, 则 $\boldsymbol{a}+\boldsymbol{b}=\overrightarrow{OB}$, $\boldsymbol{b}+\boldsymbol{c}=\overrightarrow{AC}$, 所以

$$(\boldsymbol{a}+\boldsymbol{b})+\boldsymbol{c}=\overrightarrow{OB}+\overrightarrow{BC}=\overrightarrow{OC},\quad \boldsymbol{a}+(\boldsymbol{b}+\boldsymbol{c})=\overrightarrow{OA}+\overrightarrow{AC}=\overrightarrow{OC}.$$

□

向量另一个基本运算是数与向量的乘法.

设 λ 是一个实数, λ 与 $\boldsymbol{a}$ 相乘后是一个向量, 记为 $\lambda\boldsymbol{a}$, 其长度等于 $|\lambda||\boldsymbol{a}|$, 当 $\lambda>0$ 时 $\lambda\boldsymbol{a}$ 与 $\boldsymbol{a}$ 同向, 当 $\lambda<0$ 时 $\lambda\boldsymbol{a}$ 与 $\boldsymbol{a}$ 反向. 称 $\lambda\boldsymbol{a}$ 为数 λ 与向量 $\boldsymbol{a}$ 的**数乘**. 不难验证, 数乘满足下列性质

性质 5.2 设 λ,μ 是实数, $\boldsymbol{a},\boldsymbol{b}$ 是向量, 则

(i) $\lambda(\boldsymbol{a}+\boldsymbol{b})=\lambda\boldsymbol{a}+\lambda\boldsymbol{b}$,

(ii) $(\lambda+\mu)\boldsymbol{a}=\lambda\boldsymbol{a}+\mu\boldsymbol{a}$,

(iii) $(\lambda\mu)\boldsymbol{a}=\lambda(\mu\boldsymbol{a})$.

(iv) $0\boldsymbol{a}=0$, $1\boldsymbol{a}=\boldsymbol{a}$, $(-1)\boldsymbol{a}=-\boldsymbol{a}$.

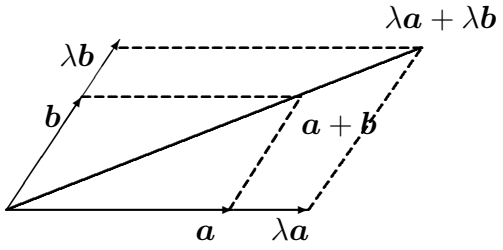


图 5.5

证明 这里只证明 (i) . 不妨设 $\lambda>0$, 则以 $\boldsymbol{a},\boldsymbol{b}$ 为边的平行四边形与以 $\lambda\boldsymbol{a},\lambda\boldsymbol{b}$ 为边的平行四边形对应边平行, 因此长度成比例, 即可得证. □

利用数乘, 可以把任意非零向量 $\boldsymbol{a}$ 分解为它的大小与一个同向的单位向量乘积. 记与 $\boldsymbol{a}$ 同向单位向量 $\boldsymbol{e}_a=\dfrac{\boldsymbol{a}}{|\boldsymbol{a}|}$, 它可以用来表示 $\boldsymbol{a}$ 的方向. 因此

$$\boldsymbol{a}=|\boldsymbol{a}|\boldsymbol{e}_a$$

2° 向量的共线和共面

定义 5.3 一组向量, 如果通过平移使它们同处一条直线上, 那么称它们**共线**. 共线的两个非零向量 $\boldsymbol{a}$ 和 $\boldsymbol{b}$ 也称为相互平行, 用 $\boldsymbol{a}\parallel\boldsymbol{b}$ 表示.

一组向量, 如果通过平移使它们同处一个平面上, 那么称它们**共面**. 不难看出, 两个

向量通过平移, 使得起点一致, 因此是一定共面.

向量共线和共面可以转化为等价的代数表示, 为此给出下列定义.

定义 5.4 对于两个向量 $\boldsymbol{a},\boldsymbol{b}$, 若存不全为零的实数 μ,ν 使得

$$\mu\boldsymbol{a}+\nu\boldsymbol{b}=0,$$

则称 $\boldsymbol{a},\boldsymbol{b}$ ***线性相关***; 若 $\mu\boldsymbol{a}+\nu\boldsymbol{b}=0$, 必推出 $\mu=\nu=0$, 则称 $\boldsymbol{a},\boldsymbol{b}$ ***线性无关***.

对于三个向量 $\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}$, 若存在不全为零的三个数 λ,μ,ν 使得

$$\lambda\boldsymbol{a}+\mu\boldsymbol{b}+\nu\boldsymbol{c}=0,$$

则称 $\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}$ ***线性相关***; 若 $\lambda\boldsymbol{a}+\mu\boldsymbol{b}+\nu\boldsymbol{c}=0$, 必推出 $\lambda=\mu=\nu=0$, 则称 $\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}$ ***线性无关***.

这样几何上共线共面问题就等介于代数上线性相关问题:

定理 5.5 两个向量$\boldsymbol{a},\boldsymbol{b}$ 共线, 当且仅当 $\boldsymbol{a},\boldsymbol{b}$ 线性相关, 三个向量 $\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}$ 共面, 当且仅当 $\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}$ 线性相关.

3° 向量的内积和夹角

设 $\boldsymbol{a}=\overrightarrow{OA},\boldsymbol{b}=\overrightarrow{OB}$ 是两个向量, $\theta(\boldsymbol{a},\boldsymbol{b})$ 为它们的夹角, 取值范围规定为 0 到 π.

定义 5.6 两个向量 $\boldsymbol{a},\boldsymbol{b}$ ***内积*** $\boldsymbol{a}\cdot\boldsymbol{b}$ 是一个实数, 定义为

$$\boldsymbol{a}\cdot\boldsymbol{b}=|\boldsymbol{a}|\ |\boldsymbol{b}|\ \cos\theta(\boldsymbol{a},\boldsymbol{b}).$$

若其中一个向量是零向量, 则内积规定为0. 内积也称作向量的数量积或点乘.

从定义直接看出 $\boldsymbol{a}\cdot\boldsymbol{b}>0$, 当且仅当 $\theta(\boldsymbol{a},\boldsymbol{b})<\frac{\pi}{2}$. $\boldsymbol{a}\cdot\boldsymbol{b}=0$, 当且仅当 $\theta(\boldsymbol{a},\boldsymbol{b})=\frac{\pi}{2}$, 此时称两个向量相互**正交**(或垂直), 记为 $\boldsymbol{a}\perp\boldsymbol{b}$.

从几何上看 (图 5.6), $|\boldsymbol{a}|\cos\theta$ 是向量 $\boldsymbol{a}$ 在向量 $\boldsymbol{b}$ 上投影向量的有向长度, 当夹角 θ 是锐角时, 投影向量的方向与 $\boldsymbol{b}$ 一致; 当夹角 θ 是钝角时, 投影向量的方向与 $\boldsymbol{b}$ 相反.

记 $\boldsymbol{a}$ 在 $\boldsymbol{b}$ 上的投影向量为 $\boldsymbol{a}_b$, 则

$$\boldsymbol{a}_b=|\boldsymbol{a}|\cos\theta\boldsymbol{e}_b=(\boldsymbol{a}\cdot\boldsymbol{e}_b)\boldsymbol{e}_b,$$

这里 $\boldsymbol{e}_b=\frac{1}{|\boldsymbol{b}|}\boldsymbol{b}$ 是 $\boldsymbol{b}$ 的单位向量.

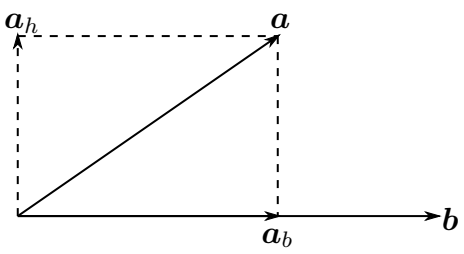


图 5.6

性质 5.7 内积满足下列代数性质.

(i) $\boldsymbol{a}\cdot\boldsymbol{b}=\boldsymbol{b}\cdot\boldsymbol{a}$. (交换律)

(ii) $(\lambda\boldsymbol{a})\cdot\boldsymbol{b}=\lambda\boldsymbol{a}\cdot\boldsymbol{b}$, 这里 λ 是任意实数. (结合律)

(iii) $(\boldsymbol{a}+\boldsymbol{b})\cdot\boldsymbol{c}=\boldsymbol{a}\cdot\boldsymbol{c}+\boldsymbol{b}\cdot\boldsymbol{c}$. (分配律)

(iv) $(\boldsymbol{a},\boldsymbol{a})=|\boldsymbol{a}|^2\geqslant 0$, 等号成立当且仅当 $\boldsymbol{a}=0$ (正定性)

证明 (i) 和 (iv) 是显然的. 在(ii) 证明中, 若 $\lambda>0$, 则 $|\lambda\boldsymbol{a}|=\lambda|\boldsymbol{a}|$, 且$\theta(\lambda\boldsymbol{a},\boldsymbol{b})=\theta(\boldsymbol{a},\boldsymbol{b})$, 所以等式成立. 若 $\lambda<0$, 则 $|\lambda\boldsymbol{a}|=-\lambda|\boldsymbol{a}|$, 且$\theta(\lambda\boldsymbol{a},\boldsymbol{b})=\pi-\theta(\boldsymbol{a},\boldsymbol{b})$, 所以$\cos\theta(\lambda\boldsymbol{a},\boldsymbol{b})=\theta(\boldsymbol{a},\boldsymbol{b})=-\cos\theta(\boldsymbol{a},\boldsymbol{b})$, 等式也成立.

(iii) 的证明如下: 如图5.7, 不妨设 $\boldsymbol{c}$ 是单位向量 $|\boldsymbol{c}|=1$. 因此 $\boldsymbol{a}+\boldsymbol{b}$ 以及$\boldsymbol{a}$, $\boldsymbol{b}$在 $\boldsymbol{c}$ 上的投影向量满足

$$(\boldsymbol{a}+\boldsymbol{b})_c=\boldsymbol{a}_c+\boldsymbol{b}_c,$$

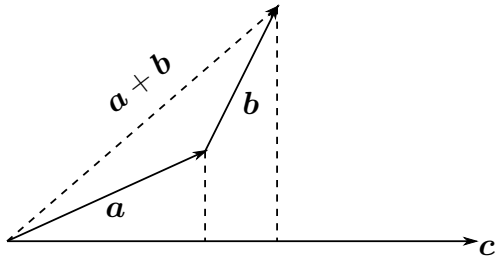


图 5.7

所以

$$\begin{aligned}(\boldsymbol{a}+\boldsymbol{b})\cdot\boldsymbol{c}&=(\boldsymbol{a}+\boldsymbol{b})_c\cdot\boldsymbol{c}=(\boldsymbol{a}_c+\boldsymbol{b}_c)\cdot\boldsymbol{c}\\&=\big((\boldsymbol{a}\cdot\boldsymbol{c})\boldsymbol{c}+(\boldsymbol{b}\cdot\boldsymbol{c})\boldsymbol{c}\big)\cdot\boldsymbol{c}=(\boldsymbol{a}\cdot\boldsymbol{c}+\boldsymbol{b}\cdot\boldsymbol{c})(\boldsymbol{c}\cdot\boldsymbol{c})\\&=\boldsymbol{a}\cdot\boldsymbol{c}+\boldsymbol{b}\cdot\boldsymbol{c}.\end{aligned}$$

这样就完成了该性质证明. □

4° 向量的外积和有向面积

向量另一个重要运算称为向量的外积. 为此先引进 “右手系” 的概念.

设 $\{\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}\}$ 是三个不共面向量构成的有序向量组, 并有同一个起点. 前两个向量 $\boldsymbol{a},\boldsymbol{b}$ 就决定了一个平面, 而 $\boldsymbol{c}$ 的方向指向平面的某一侧. 当右手四指顺着平面, 按照从 $\boldsymbol{a}$ 到 $\boldsymbol{b}$ 转动时, 如果拇指与 $\boldsymbol{c}$ 都指向平面的同一侧, 那么称 $\{\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}\}$ 为**右手系**, 否则称为左手系. 容易看出, 如果 $\{\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}\}$ 是右手系, 那么 $\{\boldsymbol{b},\boldsymbol{c},\boldsymbol{a}\}$ 和 $\{\boldsymbol{c},\boldsymbol{a},\boldsymbol{b}\}$ 仍是右手系. 但是 $\{\boldsymbol{b},\boldsymbol{a},\boldsymbol{c}\}$ 和 $\{\boldsymbol{a},\boldsymbol{b},-\boldsymbol{c}\}$ 都是左手系.

定义 5.8 向量 $\boldsymbol{a}$ 和 $\boldsymbol{b}$ 的**外积**是一个向量, 记为 $\boldsymbol{a}\times\boldsymbol{b}$, 其大小规定为以 $\boldsymbol{a},\boldsymbol{b}$ 为邻边平行四边形面积

$$|\boldsymbol{a}\times\boldsymbol{b}|=|\boldsymbol{a}||\boldsymbol{b}|\sin\theta(\boldsymbol{a},\boldsymbol{b}),$$

方向规定为: $\boldsymbol{a}\times\boldsymbol{b}$ 与 $\boldsymbol{a}$ 和 $\boldsymbol{b}$ 垂直, 且向量组 $\{\boldsymbol{a},\boldsymbol{b},\boldsymbol{a}\times\boldsymbol{b}\}$ 构成右手系 (图 5.8). 若 $\boldsymbol{a}$ 和 $\boldsymbol{b}$ 中有一个是零向量, 则两者的外积规定为零向量. 外积也称为向量积或叉乘.

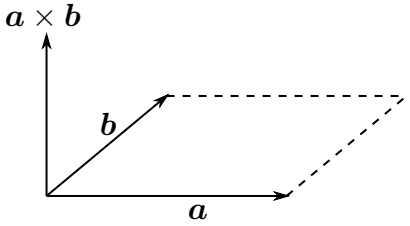


图 5.8

显然, 如果两个向量平行, 那么它们的外积等于零向量.

性质 5.9 向量的外积运算满足如下性质:

(i) $\boldsymbol{a}\times\boldsymbol{b}=0$, 当且仅当 $\boldsymbol{a}$ 和 $\boldsymbol{b}$ 平行.

(ii) $(\lambda\boldsymbol{a})\times\boldsymbol{b}=\boldsymbol{a}\times(\lambda\boldsymbol{b})=\lambda(\boldsymbol{a}\times\boldsymbol{b})$, 这里 λ 是一个实数.

(iii) $\boldsymbol{a}\times\boldsymbol{b}=-\boldsymbol{b}\times\boldsymbol{a}$, (反称性)

(iv) $(\boldsymbol{a}+\boldsymbol{b})\times\boldsymbol{c}=\boldsymbol{a}\times\boldsymbol{c}+\boldsymbol{b}\times\boldsymbol{c}$. (分配律)

证明 (i), (ii), (iii) 可以利用定义直接验证. 关于(iv) 的证明如下: 不妨设 $\boldsymbol{c}$ 是单位向量: $|\boldsymbol{c}|=1$. 注意到任意向量 $\boldsymbol{x}$ 与 $\boldsymbol{c}$ 的外积, 就是 $\boldsymbol{x}$ 在与 $\boldsymbol{c}$ 垂直的平面上的投影向量 $\boldsymbol{x}_1$ 顺时针旋转 90° 所得到的向量 (图5.9). 这是因为 $|\boldsymbol{x}_1|=|\boldsymbol{x}|\sin\theta(\boldsymbol{x},\boldsymbol{c})$, 而旋转后的方向与 $\boldsymbol{x},\boldsymbol{c}$ 垂直, 并形成右手系. 因此只要将$\boldsymbol{a},\boldsymbol{b},\boldsymbol{a}+\boldsymbol{b}$ 分别向与 $\boldsymbol{c}$ 垂直的平面投影得投影向量 $\boldsymbol{a}_1,\boldsymbol{b}_1$ 和 $\boldsymbol{a}_1+\boldsymbol{b}_1$. 整体顺时针旋转 90° 得到向量 $\boldsymbol{a}_2,\boldsymbol{b}_2$ 和 $\boldsymbol{a}_2+\boldsymbol{b}_2$ (图5.10). 这样 $\boldsymbol{a}_2=\boldsymbol{a}\times\boldsymbol{c},\boldsymbol{b}_2=\boldsymbol{b}\times\boldsymbol{c},\boldsymbol{a}_2+\boldsymbol{b}_2=(\boldsymbol{a}+\boldsymbol{b})\times\boldsymbol{c}$, 即是 (iv) . □

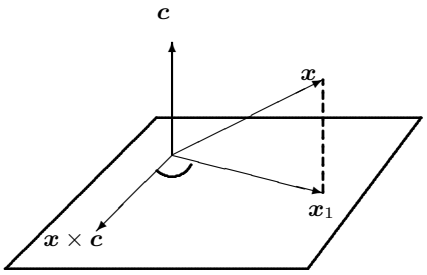


图 5.9

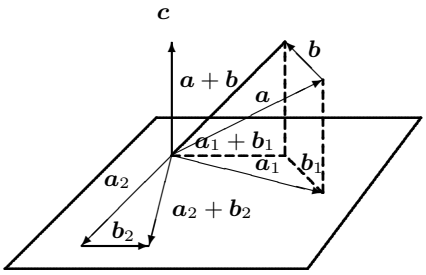


图 5.10

正如定义中所述, 向量 $\boldsymbol{a}\times\boldsymbol{b}$ 的大小是以 $\boldsymbol{a},\boldsymbol{b}$ 为邻边平行四边形面积, 但是由性质5.9 可知 $\boldsymbol{b}\times\boldsymbol{a}$ 的大小也是这个四边形面积, 只是方向与 $\boldsymbol{a}\times\boldsymbol{b}$ 相反. 因此我们实际上定义了**面积的有向性**, 即如果规定 $\boldsymbol{a}\times\boldsymbol{b}$ 为四边形面积的正向, 那么 $\boldsymbol{b}\times\boldsymbol{a}$ 就表示四边形面积的负向. 称 $\boldsymbol{a}\times\boldsymbol{b}$ 为以 $\boldsymbol{a},\boldsymbol{b}$ 为邻边的平行四边形的**有向面积**.

5° 向量的混合积和有向体积

定义 5.10 向量 $\boldsymbol{a}\times\boldsymbol{b}$ 与向量 $\boldsymbol{c}$ 内积 $(\boldsymbol{a}\times\boldsymbol{b})\cdot\boldsymbol{c}$ 称为三个向量 $\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}$ 的***混合积***.

性质 5.11 设 $\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}$ 为三个非零向量, 则

(i) $\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}$ 混合积的绝对值是以 $\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}$ 为棱平行六面体体积. 当 $\{\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}\}$ 为右手系时, $(\boldsymbol{a}\times\boldsymbol{b})\cdot\boldsymbol{c}>0$.

(ii) $(\boldsymbol{a}\times\boldsymbol{b})\cdot\boldsymbol{c}=0$ 当且仅当 $\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}$ 共面.

(iii) $(\boldsymbol{a}\times\boldsymbol{b})\cdot\boldsymbol{c}=(\boldsymbol{b}\times\boldsymbol{c})\cdot\boldsymbol{a}=(\boldsymbol{c}\times\boldsymbol{a})\cdot\boldsymbol{b}$.

证明 以 $\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}$ 为棱的平行六面体 (图 5.11) 是指: 将向量表示为同一起点的有向线段时, 以三个有向线段为棱的平行六面体. 它的底面积 S 等于 $|\boldsymbol{a}\times\boldsymbol{b}|$, 高 h 等于向量 $\boldsymbol{c}$ 在单位法向 $\dfrac{\boldsymbol{a}\times\boldsymbol{b}}{|\boldsymbol{a}\times\boldsymbol{b}|}$ 上投影向量的长度:

$$h=\frac{(\boldsymbol{a}\times\boldsymbol{b})|\cdot\boldsymbol{c}|}{|\boldsymbol{a}\times\boldsymbol{b}|},$$

所以体积

$$V=S\cdot h=|(\boldsymbol{a}\times\boldsymbol{b})\cdot\boldsymbol{c}|.$$

当 $\{\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}\}$ 为右手系时, 向量 $\boldsymbol{a}\times\boldsymbol{b}$ 与 $\boldsymbol{c}$ 的夹角为锐角, 所以 $(\boldsymbol{a}\times\boldsymbol{b})\cdot\boldsymbol{c}>0$.

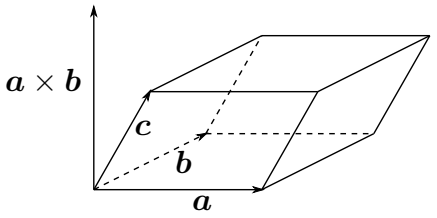


图 5.11

显然, 以$\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}$ 为棱的平行六面体体积为零, 当且仅当 $\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}$ 共面. 关于性质中第三条, 只要注意到 $(\boldsymbol{a}\times\boldsymbol{b})\cdot\boldsymbol{c},(\boldsymbol{b}\times\boldsymbol{c})\cdot\boldsymbol{a}$ 和 $(\boldsymbol{c}\times\boldsymbol{a})\cdot\boldsymbol{b}$ 表示同一个平行六面体的体积, 且对应的有序向量组 $\{\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}\},\{\boldsymbol{b},\boldsymbol{c},\boldsymbol{a}\}$ 和 $\{\boldsymbol{c},\boldsymbol{a},\boldsymbol{b}\}$ 要么同是右手系, 要么同是左手系, 因此表示的六面体体积要么同时为正, 要么同是为负, 因此相等. □

根据上述性质, 我们把混合积 $(\boldsymbol{a}\times\boldsymbol{b})\cdot\boldsymbol{c}$ 定义为以 $\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}$ 为棱的平行六面体的**有向体积**, 若 $\{\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}\}$ 为右手系,则体积为正, 若为左手系, 体积为负.

§5.2 向量的坐标表示和坐标系

1° 仿射坐标系

定理 5.12 *设向量组 $\{\boldsymbol{e}_1,\boldsymbol{e}_2,\boldsymbol{e}_3\}$ 由空间中三个不共面向量组成, 则对任意向量 $\boldsymbol{x}$, 都存在唯一数组 (x_1,x_2,x_3), 使得 $\boldsymbol{x}$ 表示为 $\boldsymbol{e}_1,\boldsymbol{e}_2,\boldsymbol{e}_3$ 的线性组合*

$$\boldsymbol{x}=x_1\boldsymbol{e}_1+x_2\boldsymbol{e}_2+x_3\boldsymbol{e}_3.$$

证明 设 $\boldsymbol{x}=\overrightarrow{OP},\boldsymbol{e}_1=\overrightarrow{OA},\boldsymbol{e}_2=\overrightarrow{OB},\boldsymbol{e}_3=\overrightarrow{OC}$. 过 P 点做平行直线 OC 的平行线, 交 AOB 所在平面于 Q 点. 再过 Q 作平行于 OB 的平行线, 交 OC 于 R. 则

$$\boldsymbol{x}=\overrightarrow{OP}=\overrightarrow{OR}+\overrightarrow{RQ}+\overrightarrow{QP}.$$

由于

$$\overrightarrow{OR}\parallel\overrightarrow{OA},\ \overrightarrow{RQ}\parallel\overrightarrow{OB},\ \overrightarrow{QP}\parallel\overrightarrow{OC},$$

因此分别共线, 即存在实数 x_1,x_2,x_3 使得

$$\overrightarrow{OR}=x_1\overrightarrow{OA}=x_1\boldsymbol{e}_1,\ \overrightarrow{RQ}=x_2\overrightarrow{OB}=x_2\boldsymbol{e}_2,\ \overrightarrow{QP}=x_3\overrightarrow{OA}=x_3\boldsymbol{e}_3,$$

即 $\boldsymbol{x}=x_1\boldsymbol{e}_1+x_2\boldsymbol{e}_2+x_3\boldsymbol{e}_3$. 若另有一组坐标 x_1',x_2',x_3', 使得 $\boldsymbol{x}=x_1'\boldsymbol{e}_1+x_2'\boldsymbol{e}_2+x_3'\boldsymbol{e}_3$, 则

$$(x_1-x_1')\boldsymbol{e}_1+(x_2-x_2')\boldsymbol{e}_2+(x_3-x_3')\boldsymbol{e}_3=0,$$

由于 $\boldsymbol{e}_1,\boldsymbol{e}_2,\boldsymbol{e}_3$ 不共面, 因此线性无关. 根据定理 5.5 , $x_1=x_1',x_2=x_2',x_3=x_3'$, 即坐标是唯一的. □

定义 5.13 空间中任意三个不共面向量组 $\{\boldsymbol{e}_1,\boldsymbol{e}_2,\boldsymbol{e}_3\}$ 称为空间中一组***基***, 对于任意向量 $\boldsymbol{x}$, 若

$$\boldsymbol{x}=x_1\boldsymbol{e}_1+x_2\boldsymbol{e}_2+x_3\boldsymbol{e}_3,$$

则称 (x_1,x_2,x_3) 为向量 $\boldsymbol{x}$ 在基 $\{\boldsymbol{e}_1,\boldsymbol{e}_2,\boldsymbol{e}_3\}$ 下的***仿射坐标***或简称***坐标*** .

空间中确定一点 O 和一组基 $\{\boldsymbol{e}_1,\boldsymbol{e}_2,\boldsymbol{e}_3\}$ (通常选择右手系), 合在一起记为 $[O;\boldsymbol{e}_1,\boldsymbol{e}_2,\boldsymbol{e}_3]$, 并称为空间的***仿射坐标系***. O 称为***原点***, 三个向量 $\boldsymbol{e}_1,\boldsymbol{e}_2,\boldsymbol{e}_3$ 也分别称为坐标系的***坐标向量***.

选定了仿射坐标系 $[O;\boldsymbol{e}_1,\boldsymbol{e}_2,\boldsymbol{e}_3]$, 下列三者之间存在一一对应关系:

$$\text{空间中点 } P \longleftrightarrow \text{ 向量 } \overrightarrow{OP} \longleftrightarrow \text{ 坐标 } (x_1,x_2,x_3).$$

因此也称 (x_1,x_2,x_3) 是点 P 的坐标.

一切关于向量从几何上定义的加法、数乘、内积、外积以及混合积都可以转化为坐标之间运算. 例如, 两个向量加法就是对应坐标加法, 数乘就是数与坐标相乘:

$$\lambda\boldsymbol{x}+\mu\boldsymbol{y}\longleftrightarrow(\lambda x_1+\mu x_1',\lambda x_2+\mu x_2',\lambda x_3+\mu x_3').$$

其中 $\boldsymbol{x}=x_1\boldsymbol{e}_1+x_2\boldsymbol{e}_2+x_3\boldsymbol{e}_3,\boldsymbol{y}=x_1'\boldsymbol{e}_1+x_2'\boldsymbol{e}_2+x_3'\boldsymbol{e}_3$.

2° 直角坐标系

为了进一步简化计算, 取空间中构成右手系, 并两两相互垂直的三个单位向量作为坐标向量, 记为 $\boldsymbol{i},\boldsymbol{j},\boldsymbol{k}$, 并称 $[O;\boldsymbol{i},\boldsymbol{j},\boldsymbol{k}]$ 为**直角坐标系**. 以 O 为原点, 沿三个坐标向量的数轴分别称为 x 轴、y 轴和 z 轴(图5.12),

在直角坐标系 $[O;\boldsymbol{i},\boldsymbol{j},\boldsymbol{k}]$ 中, 任何一个向量表示为(也称点 $P(x,y,z)$ 的**位置向量**)

$$\boldsymbol{x}=\overrightarrow{OP}=x\boldsymbol{i}+y\boldsymbol{j}+z\boldsymbol{k}.$$

有时也直接用向量坐标表示该向量

$$\boldsymbol{x}=\overrightarrow{OP}=(x,y,z),$$

这样, 三个坐标向量分别表示为

$$\boldsymbol{i}=(1,0,0),\quad \boldsymbol{j}=(0,1,0),\quad \boldsymbol{k}=(0,0,1).$$

有时, 也把直角坐标系记为 $Oxyz$, x 和 y 轴所在平面记为 Oxy 等等.

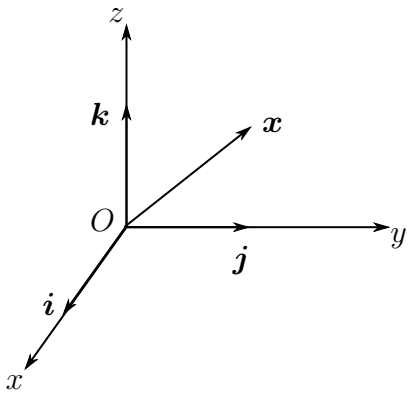


图 5.12

记 $\boldsymbol{x}=\overrightarrow{OP}$ 与三个坐标轴正向的夹角为 α,β,γ , 并称为向量 $\overrightarrow{OP}$ 的**方向角**. 这样

$$x=|\overrightarrow{OP}|\cos\alpha,\ y=|\overrightarrow{OP}|\cos\beta,\ z=|\overrightarrow{OP}|\cos\gamma.$$

或

$$\boldsymbol{x}=\overrightarrow{OP}=|\overrightarrow{OP}|(\cos\alpha\boldsymbol{i}+\cos\beta\boldsymbol{j}+\cos\gamma\boldsymbol{k}).$$

称方向角的余弦 $\cos\alpha,\cos\beta,\cos\gamma$ 为该向量 $\boldsymbol{x}=\overrightarrow{OP}$ **方向余弦**. 它们满足

$$\cos^2\alpha+\cos^2\beta+\cos^2\gamma=1.$$

3° 直角坐标系下向量的运算

直角坐标系的特殊性使得利用向量坐标进行计算变得更加简洁. 首先, 三个坐标向量 $\{\boldsymbol{i},\boldsymbol{j},\boldsymbol{k}\}$ 之间的内积和外积分别满足:

$$\boldsymbol{i}\cdot\boldsymbol{j}=\boldsymbol{j}\cdot\boldsymbol{k}=\boldsymbol{k}\cdot\boldsymbol{i}=0,\ \boldsymbol{i}\cdot\boldsymbol{i}=\boldsymbol{j}\cdot\boldsymbol{j}=\boldsymbol{k}\cdot\boldsymbol{k}=1.$$

$$\boldsymbol{i}\times\boldsymbol{j}=\boldsymbol{k};\ \boldsymbol{j}\times\boldsymbol{k}=\boldsymbol{i};\ \boldsymbol{k}\times\boldsymbol{i}=\boldsymbol{j},\ \boldsymbol{i}\times\boldsymbol{i}=\boldsymbol{j}\times\boldsymbol{j}=\boldsymbol{k}\times\boldsymbol{k}=0.$$

一般情况下, 设 $\boldsymbol{a}=a_1\boldsymbol{i}+a_2\boldsymbol{j}+a_3\boldsymbol{k},\ \boldsymbol{b}=b_1\boldsymbol{i}+b_2\boldsymbol{j}+b_3\boldsymbol{k},\ \boldsymbol{c}=c_1\boldsymbol{i}+c_2\boldsymbol{j}+c_3\boldsymbol{k}$, 则

(1) 向量的数乘与加法:

$$\mu\boldsymbol{a}+\nu\boldsymbol{b}=(\mu a_1+\nu b_1)\boldsymbol{i}+(\mu a_2+\nu b_2)\boldsymbol{j}+(\mu a_3+\nu b_3)\boldsymbol{k}.$$

(2) 向量的内积:

$$\boldsymbol{a}\cdot\boldsymbol{b}=(a_1\boldsymbol{i}+a_2\boldsymbol{j}+a_3\boldsymbol{k})\cdot(b_1\boldsymbol{i}+b_2\boldsymbol{j}+b_3\boldsymbol{k})=a_1b_1+a_2b_2+a_3b_3.$$

因此两向量的夹角、向量的模长(大小)以及两点之间的距离可分别表示为

$$\theta(\boldsymbol{a},\boldsymbol{b}) = \arccos\left(\frac{a_1b_1+a_2b_2+a_3b_3}{\sqrt{a_1^2+a_2^2+a_3^2}\sqrt{b_1^2+b_2^2+b_3^2}}\right),$$
$$|\boldsymbol{a}| = \sqrt{\boldsymbol{a}\cdot\boldsymbol{a}} = \sqrt{a_1^2+a_2^2+a_3^2},$$
$$d(P_1,P_2) = |\overrightarrow{P_1P_2}| = \sqrt{(a_1-b_1)^2+(a_2-b_2)^2+(a_3-b_3)^2}.$$

这里两点的坐标分别是 $P_1(a_1,a_2,a_3)$ 和 $P_2(b_1,b_2,b_3)$.

(3)向量的外积:

$$\begin{aligned}\boldsymbol{a}\times\boldsymbol{b} &= (a_1\boldsymbol{i}+a_2\boldsymbol{j}+a_3\boldsymbol{k})\times(b_1\boldsymbol{i}+b_2\boldsymbol{j}+b_3\boldsymbol{k})\\ &= (a_2b_3-a_3b_2)\boldsymbol{i}+(a_3b_1-a_1b_3)\boldsymbol{j}+(a_1b_2-a_2b_1)\boldsymbol{k}.\end{aligned}$$

对任意四个数 x_1,x_2,y_1,y_2, 引进二阶行列式的定义如下:

$$\begin{vmatrix}x_1 & x_2\\ y_1 & y_2\end{vmatrix} = x_1y_2-x_2y_1,$$

那么向量 $\boldsymbol{a}$ 和 $\boldsymbol{b}$ 的外积表示为

$$\boldsymbol{a}\times\boldsymbol{b} = \begin{vmatrix}a_2 & a_3\\ b_2 & b_3\end{vmatrix}\boldsymbol{i}+\begin{vmatrix}a_3 & a_1\\ b_3 & b_1\end{vmatrix}\boldsymbol{j}+\begin{vmatrix}a_1 & a_2\\ b_1 & b_2\end{vmatrix}\boldsymbol{k}.$$

其中三个系数行列式 $\begin{vmatrix}a_2 & a_3\\ b_2 & b_3\end{vmatrix}$, $\begin{vmatrix}a_3 & a_1\\ b_3 & b_1\end{vmatrix}$, $\begin{vmatrix}a_1 & a_2\\ b_1 & b_2\end{vmatrix}$ 分别是有向面积 $\boldsymbol{a}\times\boldsymbol{b}$ 在三个坐标平面 Oyz, Ozx, Oxy 上的有向投影.

(4)向量的混合积:

同样, 对任意三个数组 $x_1,x_2,x_3;y_1,y_2,y_3,z_1,z_2,z_3$ 共九个数, 定义三阶行列式如下:

$$\begin{vmatrix}x_1 & x_2 & x_3\\ y_1 & y_2 & y_3\\ z_1 & z_2 & z_3\end{vmatrix} = x_1y_2z_3+x_2y_3z_1+x_3y_1z_2-x_3y_2z_1-x_2y_1z_3-x_1y_3z_2$$

那么三个向量 $\boldsymbol{a}=a_1\boldsymbol{i}+a_2\boldsymbol{j}+a_3\boldsymbol{k}$, $\boldsymbol{b}=b_1\boldsymbol{i}+b_2\boldsymbol{j}+b_3\boldsymbol{k}$, $\boldsymbol{c}=c_1\boldsymbol{i}+c_2\boldsymbol{j}+c_3\boldsymbol{k}$ 的外积为:

$$\begin{aligned}\boldsymbol{a}\times\boldsymbol{b}\cdot\boldsymbol{c} &= (a_2b_3-a_3b_2)c_1+(a_3b_1-a_1b_3)c_2+(a_1b_2-a_2b_1)c_3\\ &= \begin{vmatrix}a_1 & a_2 & a_3\\ b_1 & b_2 & b_3\\ c_1 & c_2 & c_3\end{vmatrix}\end{aligned}$$

关于向量运算的其他性质的证明, 在坐标表示下也会变得更加简单.

例 5.2.1 证明 Cauchy 不等式

$$(a_1b_1+a_2b_2+a_3b_3)^2 \leqslant (a_1^2+a_2^2+a_3^2)(b_1^2+b_2^2+b_3^2),$$

等号成立当且仅当存在实数 λ 满足 $a_i=\lambda b_i,\ i=1,2,3.$

证明 设向量 $\boldsymbol{a}=a_1\boldsymbol{i}+a_2\boldsymbol{j}+a_3\boldsymbol{k},\ \boldsymbol{b}=b_1\boldsymbol{i}+b_2\boldsymbol{j}+b_3\boldsymbol{k}$, 则 Cauchy 不等式等价于

$$(\boldsymbol{a}\cdot\boldsymbol{b})^2=(|\boldsymbol{a}||\boldsymbol{b}|\cos\theta)^2 \leqslant |\boldsymbol{a}|^2|\boldsymbol{b}|^2$$

等号成立当且仅当 $\cos\theta=\pm1$, 即 $\boldsymbol{a}$ 与 $\boldsymbol{b}$ 共线, 因此线性相关.

4° **行列式与有向面 (体) 积**

对于任意实二阶行列式

$$\begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix},$$

把两行分别看成平面上两点的坐标 $P_1(a_1,a_2),\ P_2(b_1,b_2)$, 那么该行列式几何上就表示了以$O,P_1,P_2$ 为三个顶点或以 $\boldsymbol{a}=\overrightarrow{OP_1},\ \boldsymbol{b}=\overrightarrow{OP_2}$ 为棱平行四边形的面积. 因此, $\boldsymbol{a},\boldsymbol{b}$ 不共线, 当且仅当对应的行列式不为零. 行列式取正或负, 体现了面积的有向性.

对于任意实三阶行列式

$$\begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix}$$

只要把每一行作为空间中一点的坐标

$$P_1(a_1,a_2,a_3),\ P_2(b_1,b_2,b_3),\ P_3(c_1,c_2,c_3),$$

那么三阶行列式几何上就表示以O,P_1,P_2,P_3 为顶点或以

$$\boldsymbol{a}=\overrightarrow{OP_1},\ \boldsymbol{b}=\overrightarrow{OP_2},\ \boldsymbol{c}=\overrightarrow{OP_3}$$

为棱平行六面体的体积. 因此三个向量 $\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}$ 不共面, 当且仅当对应的行列式不为零. 行列式取正或负, 体现了体积的有向性.

§5.3 坐标变换

在确定的坐标系中, 空间中任意点及对应向量的坐标随之确定. 如果选择不同坐标系 (即选择不同原点和坐标向量), 那么空间中点或向量就对应不同的坐标. 因此, 有必

要考察点或向量在不同坐标系下坐标之间的关系. 这里将聚焦同是右手系的两个直角坐标系下点的坐标之间的变换关系.

几何上看, 同是右手系的两个直角坐标系 $[O;\ \boldsymbol{i},\boldsymbol{j},\boldsymbol{k}]$ 和 $[O';\boldsymbol{i}',\boldsymbol{j}',\boldsymbol{k}']$ 可以看成是将 $[O;\ \boldsymbol{i},\boldsymbol{j},\boldsymbol{k}]$ 平移, 使得坐标原点 O平移至 O', 再经过旋转使得 $\{\boldsymbol{i},\boldsymbol{j},\boldsymbol{k}\}$ 旋转为$\{\boldsymbol{i}',\boldsymbol{j}',\boldsymbol{k}'\}$, 从而得到坐标系 $[O';\boldsymbol{i}',\boldsymbol{j}',\boldsymbol{k}']$. 空间中的点在两个坐标系下坐标变换, 可以由坐标系的平移和旋转实现. 下面将平移和旋转两个动作分解讨论.

1° 坐标系的平移

设$O'\neq O$, 但 $\boldsymbol{i}=\boldsymbol{i}',\boldsymbol{j}=\boldsymbol{j}',\boldsymbol{k}=\boldsymbol{k}'$. 在两个坐标系 $[O;\ \boldsymbol{i},\boldsymbol{j},\boldsymbol{k}]$ 和 $[O';\ \boldsymbol{i},\boldsymbol{j},\boldsymbol{k}]$ 中, 记空间中任意点 P 的坐标分别为 (x,y,z) 和 (x',y',z'), 或

$$\overrightarrow{OP}=x\boldsymbol{i}+y\boldsymbol{j}+z\boldsymbol{k},\quad \overrightarrow{O'P}=x'\boldsymbol{i}+y'\boldsymbol{j}+z'\boldsymbol{k}.$$

若 O' 在 $[O;\ \boldsymbol{i},\boldsymbol{j},\boldsymbol{k}]$ 中的坐标为 (a,b,c), 或

$$\overrightarrow{OO'}=a\boldsymbol{i}+b\boldsymbol{j}+c\boldsymbol{k},$$

那么利用 $\overrightarrow{O'P}=\overrightarrow{OP}-\overrightarrow{OO'}$ 可得

$$x'\boldsymbol{i}+y'\boldsymbol{j}+z'\boldsymbol{k}=(x-a)\boldsymbol{i}+(y-b)\boldsymbol{j}+(z-c)\boldsymbol{k},$$

于是得到空间中点 P（或向量）在两个坐标系下坐标 (x,y,z) 和 (x',y',z') 的平移变换:

$$x'=x-a,\quad y'=y-b,\quad z'=z-c.$$

以及逆变换

$$x=x'+a,\quad y=y'+b,\quad z=z'+c.$$

2° 坐标系的旋转

考察原点相同两个坐标系 $[O;\ \boldsymbol{i},\boldsymbol{j},\boldsymbol{k}]$ 和 $[O;\boldsymbol{i}',\boldsymbol{j}',\boldsymbol{k}']$. 设两个坐标系的坐标向量 $\{\boldsymbol{i},\boldsymbol{j},\boldsymbol{k}\}$ 和 $\{\boldsymbol{i}',\boldsymbol{j}',\boldsymbol{k}'\}$ 之间之间夹角由下表给出:

	$\boldsymbol{i}$	$\boldsymbol{j}$	$\boldsymbol{k}$
$\boldsymbol{i}'$	α_1	β_1	γ_1
$\boldsymbol{j}'$	α_2	β_2	γ_2
$\boldsymbol{k}'$	α_3	β_3	γ_3

表中每一行分别表示向量 $\boldsymbol{i}',\boldsymbol{j}',\boldsymbol{k}'$ 在坐标系 $[O;\ \boldsymbol{i},\boldsymbol{j},\boldsymbol{k}]$ 中与三个坐标向量 $\boldsymbol{i},\boldsymbol{j},\boldsymbol{k}$ 的方向角（见 §5.2 中的 2°）. 由于 $\boldsymbol{i}',\boldsymbol{j}',\boldsymbol{k}'$ 是两两正交的单位向量, 因此向量 $\boldsymbol{i}',\boldsymbol{j}',\boldsymbol{k}'$ 在

$[O;\ \boldsymbol{i},\boldsymbol{j},\boldsymbol{k}]$ 中的坐标可由方向余弦来表示,

$$\begin{aligned}\boldsymbol{i}' &= \cos\alpha_1\boldsymbol{i} + \cos\beta_1\boldsymbol{j} + \cos\gamma_1\boldsymbol{k},\\ \boldsymbol{j}' &= \cos\alpha_2\boldsymbol{i} + \cos\beta_2\boldsymbol{j} + \cos\gamma_2\boldsymbol{k},\\ \boldsymbol{k}' &= \cos\alpha_3\boldsymbol{i} + \cos\beta_3\boldsymbol{j} + \cos\gamma_3\boldsymbol{k}.\end{aligned}$$

由于两组坐标向量是单位正交向量, 因此

$$\cos\alpha_i\cos\alpha_j + \cos\beta_i\cos\beta_j + \cos\gamma_i\cos\gamma_j = \delta_{ij} = \begin{cases}1, & i = j\\ 0, & i \neq j\end{cases}$$

注意到, 表中每一列分别表示向量 $\boldsymbol{i},\boldsymbol{j},\boldsymbol{k}$ 在坐标系 $[O;\boldsymbol{i}',\boldsymbol{j}',\boldsymbol{k}']$ 中的方向角. 例如向量 $\boldsymbol{i}$ 与$[O;\boldsymbol{i}',\boldsymbol{j}',\boldsymbol{k}']$ 三个坐标向量方向角为 $\alpha_1,\alpha_2,\alpha_3$. 因此也可以得到向量 $\boldsymbol{i},\boldsymbol{j},\boldsymbol{k}$ 的坐标在 $[O;\boldsymbol{i}',\boldsymbol{j}',\boldsymbol{k}']$ 中余弦表示. 设空间中任意点 P 在两个坐标系 $[O;\ \boldsymbol{i},\boldsymbol{j},\boldsymbol{k}]$ 和 $[O;\boldsymbol{i}',\boldsymbol{j}',\boldsymbol{k}']$中坐标分别为 (x,y,z), (x',y',z'), 则

$$\begin{aligned}\overrightarrow{OP} &= x\boldsymbol{i} + y\boldsymbol{j} + z\boldsymbol{k} = x'\boldsymbol{i}' + y'\boldsymbol{j}' + z'\boldsymbol{k}'\\ &= x'(\cos\alpha_1\boldsymbol{i} + \cos\beta_1\boldsymbol{j} + \cos\gamma_1\boldsymbol{k})\\ &\quad + y'(\cos\alpha_2\boldsymbol{i} + \cos\beta_2\boldsymbol{j} + \cos\gamma_2\boldsymbol{k})\\ &\quad + z'(\cos\alpha_3\boldsymbol{i} + \cos\beta_3\boldsymbol{j} + \cos\gamma_3\boldsymbol{k})\\ &= (x'\cos\alpha_1 + y'\cos\alpha_2 + z'\cos\alpha_3)\boldsymbol{i}\\ &\quad + (x'\cos\beta_1 + y'\cos\beta_2 + z'\cos\beta_3)\boldsymbol{j}\\ &\quad + (x'\cos\gamma_1 + y'\cos\gamma_2 + z'\cos\gamma_3)\boldsymbol{k},\end{aligned}$$

于是得到空间中点 P (或向量) 在两个坐标系下坐标 (x,y,z) 和 (x',y',z') 的旋转变换:

$$\begin{aligned}x &= x'\cos\alpha_1 + y'\cos\alpha_2 + z'\cos\alpha_3,\\ y &= x'\cos\beta_1 + y'\cos\beta_2 + z'\cos\beta_3,\\ z &= x'\cos\gamma_1 + y'\cos\gamma_2 + z'\cos\gamma_3.\end{aligned}$$

同样也可以导出上述变换的逆变换

$$\begin{aligned}x' &= x\cos\alpha_1 + y\cos\beta_1 + z\cos\gamma_1,\\ y' &= x\cos\alpha_2 + y\cos\beta_2 + z\cos\gamma_2,\\ z' &= x\cos\alpha_3 + y\cos\beta_3 + z\cos\gamma_3.\end{aligned}$$

例 5.3.1 保持 z 轴不变, 逆时针旋转 α 对应的坐标变换如下

	$\boldsymbol{i}$	$\boldsymbol{j}$	$\boldsymbol{k}$
$\boldsymbol{i}'$	α	$\frac{\pi}{2}-\alpha$	$\frac{\pi}{2}$
$\boldsymbol{j}'$	$\frac{\pi}{2}+\alpha$	α	$\frac{\pi}{2}$
$\boldsymbol{k}'$	$\frac{\pi}{2}$	$\frac{\pi}{2}$	0

$$x' = x\cos\alpha + y\sin\alpha,$$
$$y' = -x\sin\alpha + y\cos\alpha,$$
$$z' = z.$$

3° 变换的复合

将坐标系的平移和旋转合成, 就给出了空间中点的一般坐标变换. 任意两个坐标变换复合, 仍然是一个坐标变换. 不难验证, 无论是点 (或向量) 坐标的平移变换, 还是旋转变换, 都不会改变两点之间的距离以及点对应向量之间的夹角, 因此称这些变换为**刚体变换**. 简单地说, 一个几何图形在刚体变换下不改变图形形状, 只是改变了图形的位置.

§5.4 平面、直线与二次曲面

利用向量和坐标系, 空间中一些曲面和曲线可以表示为代数方程.

1° 平面

几何上看, 过一定点并垂直一个确定方向就可确定一个平面. 因此, 在坐标系 $Oxyz$ 中, 设平面 Π 过定点 $P_0(x_0, y_0, z_0)$, 并与给定向量 $\boldsymbol{n} = a\boldsymbol{i} + b\boldsymbol{j} + c\boldsymbol{k}$ 垂直, $\boldsymbol{n}$ 称为平面Π 的 **法向量**.

对Π 上任意一点 $P(x, y, z)$, 则 $\overrightarrow{P_0P} \perp \boldsymbol{n}$, 也就是

$$\boldsymbol{n} \cdot \overrightarrow{P_0P} = 0 \ \text{ 或者 } \boldsymbol{n} \cdot (\boldsymbol{r} - \boldsymbol{r}_0) = 0,$$

其中 $\boldsymbol{r} = \overrightarrow{OP}, \boldsymbol{r}_0 = \overrightarrow{OP_0}$ 分别是 P 和 P_0 位置向量. 注意到

$$\boldsymbol{r} - \boldsymbol{r}_0 = \overrightarrow{P_0P} = (x - x_0)\boldsymbol{i} + (y - y_0)\boldsymbol{j} + (z - z_0)\boldsymbol{k},$$

因此平面上任意点 $P(x, y, z)$ 的坐标满足下列三元一次方程

$$a(x - x_0) + b(y - y_0) + c(z - z_0) = 0,$$

或

$$ax + by + cz + d = 0,$$

其中 $d = -(ax_0 + by_0 + cz_0)$ 是一个已知数. 上述方程称为**平面一般方程**. 反之, 任意满足方程的点 (x, y, z) 都在平面上.这样就把平面的几何描述, 转化为一个代数方程.

空间中平面把空间分成三个部分: 法向量所指一侧称为“上”半部分, 另一侧称为“下”半部分, 以及平面本身. 判断空间中一点 $P'(x',y',z')$ 落在哪部分, 只要看平面上任何一点 P 到 P' 的向量 $\overrightarrow{PP'}$ 与平面法向量夹角是锐角、钝角或是直角, 也就是看 $\boldsymbol{n}\cdot\overrightarrow{PP'}$ 是正的、负的或是零. 因为 P 满足方程, 所以

$$\boldsymbol{n}\cdot\overrightarrow{PP'}=a(x'-x)+b(y'-y)+c(z'-z)=ax'+by'+cz'+d,$$

根据上式就有

P' 位于上半部分, 当且仅当 $\boldsymbol{n}\cdot\overrightarrow{PP'}=ax'+by'+cz'+d>0$,

P' 位于下半部分, 当且仅当 $\boldsymbol{n}\cdot\overrightarrow{PP'}=ax'+by'+cz'+d<0$,

P' 位于平面上, 当且仅当 $\boldsymbol{n}\cdot\overrightarrow{PP'}=ax'+by'+cz'+d=0$.

平面方程一些特殊情形是值得关注的.

（1） $d=0$, 方程退化为 $ax+by+cz=0$, 因此 $(0,0,0)$ 满足方程, 即平面过原点.

（2） $c=0$, 此时法向量 $\boldsymbol{n}=(a,b,0)$ 垂直于 z 轴, 所以方程 $ax+by+d=0$ 表示平行于 z 轴的平面. 对于 $a=0$ 或 $b=0$ 的情形类似.

（3） $a=b=0$, 此时法向量 $\boldsymbol{n}=(0,0,c)$ 平行于 z 轴, 所以方程 $cz+d=0$ 或者 $z=-\frac{d}{c}$ 表示过点 $(0,0,-\frac{d}{c})$ 且平行于 Oxy 平面的平面. 其他情形类似.

例 5.4.1 求过不共线的三点 $P_1(x_1,y_1,z_1),P_2(x_2,y_2,z_2),P_3(x_3,y_3,z_3)$ 的平面.

解 取P_1 为定点, 向量 $\overrightarrow{P_1P_2},\overrightarrow{P_1P_3}$ 在平面上, 因此平面法向量为 $\overrightarrow{P_1P_2}\times\overrightarrow{P_1P_3}$, 该平面的方程如下:

$$\overrightarrow{P_1P}\cdot(\overrightarrow{P_1P_2}\times\overrightarrow{P_1P_3})=\begin{vmatrix}x-x_1 & y-y_1 & z-z_1\\ x_2-x_1 & y_2-y_1 & z_2-z_1\\ x_3-x_1 & y_3-y_1 & z_3-z_1\end{vmatrix}=0,$$

若三点分别位于三个坐标轴上(图5.13) $P_1(\alpha,0,0),P_2(0,\beta,0),P_2(0,0,\gamma)$, 则方程为

$$\begin{vmatrix}x-\alpha & y & z\\ -\alpha & \beta & 0\\ -\alpha & 0 & \gamma\end{vmatrix}=0,$$

或简化为

$$\frac{x}{\alpha}+\frac{y}{\beta}+\frac{z}{\gamma}=1.$$

该平面分别与三个坐标轴在给定三点相截并称 α,β,γ 为平面与数轴的截距.

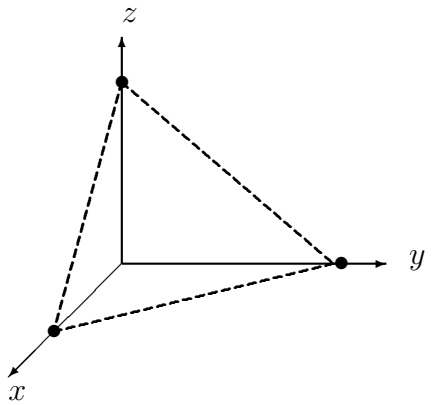


图 5.13

例 5.4.2 讨论两个平面的夹角.

设两个平面方程为

$$a_1x+b_1y+c_1z+d_1=0,\quad \boldsymbol{n}_1=a_1\boldsymbol{i}+b_1\boldsymbol{j}+c_1\boldsymbol{k};$$
$$a_2x+b_2y+c_2z+d_2=0,\quad \boldsymbol{n}_2=a_2\boldsymbol{i}+b_2\boldsymbol{j}+c_2\boldsymbol{k}.$$

它们的夹角 ϕ 定义为两个平面法向量 $\boldsymbol{n}_1$ 与 $\boldsymbol{n}_2$ 的夹角(图 5.14). 因此

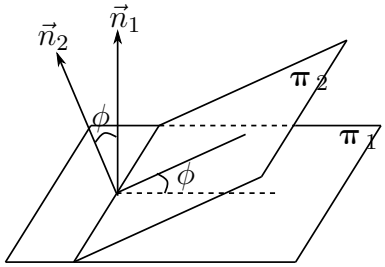


图 5.14

$$\cos\phi=\frac{\boldsymbol{n}_1\cdot\boldsymbol{n}_2}{|\boldsymbol{n}_1||\boldsymbol{n}_2|}=\frac{a_1a_2+b_1b_2+c_1c_2}{\sqrt{a_1^2+b_1^2+c_1^2}\sqrt{a_2^2+b_2^2+c_2^2}},$$

当 $\phi=0$ 时, 两平面平行: 即 $\boldsymbol{n}_1\parallel\boldsymbol{n}_2$, 当 $\phi=\boldsymbol{\pi}$ 时, 两平面垂直, 也就是 $\boldsymbol{n}_1\perp\boldsymbol{n}_2$, 即 $\boldsymbol{n}_1\cdot\boldsymbol{n}_2=a_1a_2+b_1b_2+c_1c_2=0$.

2° 直线

空间中过一定点 $P_0(x_0,y_0,z_0)$ 并沿着给定方向 $\boldsymbol{v}=l\boldsymbol{i}+m\boldsymbol{j}+n\boldsymbol{k}$, 就可确定一条直线, 向量 $\boldsymbol{v}$ 称为直线的**方向向量**. 对该直线上任意一点 $P(x,y,z)$, $\overrightarrow{P_0P}=\boldsymbol{r}-\boldsymbol{r}_0$ 与 $\boldsymbol{v}$ 共线, 因此有

$$\boldsymbol{r}=\boldsymbol{r}_0+t\boldsymbol{v},\quad \text{或}\quad \begin{cases}x=x_0+lt\\ y=y_0+mt\\ z=z_0+nt\end{cases}$$

也就是直线上任意一点 P 的坐标 (x,y,z) 表示为参数 t 的线性方程, 称为直线**参数方程**, 如果消去参数 t 就得到

$$\frac{x-x_0}{l}=\frac{y-y_0}{m}=\frac{z-z_0}{n}.$$

称为直线**点向式方程**, 上述方程实际上是含有两个三元一次方程的方程组. 如果方向向量的坐标之一为零, 例如 $l=0$, 此时直线方向与 x 轴垂直, 点向式方程应理解为下述方程组

$$x=x_0,\quad \frac{y-y_0}{m}=\frac{z-z_0}{n},$$

如果有两个为零, 例如 $l=0,m=0$, 则直线与 z 轴平行, 点向式方程理解为

$$x=x_0,\ y=y_0.$$

设直线 L 为两平面交线, 因此点 $P(x,y,z)$ 在交线 L 上当且仅当它在两个平面上, 也就是(x,y,z) 满足三元一次方程组

$$\begin{cases}a_1x+b_1y+c_1z+d_1=0\\ a_2x+b_2y+c_2z+d_2=0\end{cases}$$

称为直线的**一般方程**. 因为直线 L 垂直于两个平面法向量 $\boldsymbol{n}_1$ 和 $\boldsymbol{n}_2$, 因此可取 $\boldsymbol{v}=\boldsymbol{n}_1\times\boldsymbol{n}_2$ 为直线方向向量. 再从方程组求出一个特解$P_0(x_0,y_0,z_0)$, 则直线一般方程就化为点向式方程. 反之, 点向式方程也可表示为一般方程

$$\frac{x-x_0}{l}=\frac{y-y_0}{m},\quad \frac{x-x_0}{l}=\frac{z-z_0}{n}.$$

例 5.4.3 求过两个给定点 $P_1(x_1,y_1,z_1),P_2(x_2,y_2,z_2)$ 的直线方程.

只要取方向向量为 $\boldsymbol{v}=\overrightarrow{P_2P_1}=(x_2-x_1)\boldsymbol{i}+(y_2-y_1)\boldsymbol{j}+(z_2-z_1)\boldsymbol{k}$, 就有

$$\boldsymbol{r}=\boldsymbol{r}_1+t\boldsymbol{v}=\boldsymbol{r}_1+t(\boldsymbol{r}_2-\boldsymbol{r}_1)$$

$$\frac{x-x_1}{x_2-x_1}=\frac{y-y_1}{y_2-y_1}=\frac{z-z_1}{z_2-z_1}.$$

例 5.4.4 讨论两直线之间的关系.

给定两条直线

$$L_1:\boldsymbol{r}=\boldsymbol{r}_1+t\boldsymbol{v}_1,\ \ \text{其中 } \boldsymbol{r}_1=(x_1,y_1,z_1),\boldsymbol{v}_1=(l_1,m_1,n_1),$$

$$L_2:\boldsymbol{r}=\boldsymbol{r}_2+t\boldsymbol{v}_2,\ \ \text{其中 } \boldsymbol{r}_2=(x_2,y_2,z_2),\boldsymbol{v}_2=(l_2,m_2,n_2).$$

它们的关系可分 “共面” 和 “异面” 两种情形.

共面 直线 L_1 与 L_2 共面等价于 $\boldsymbol{v}_1,\boldsymbol{v}_2$ 与 $\boldsymbol{r}_1-\boldsymbol{r}_2$ 共面, 等价于

$$(\boldsymbol{r}_1-\boldsymbol{r}_2)\cdot\boldsymbol{v}_1\times\boldsymbol{v}_2=\begin{vmatrix}x_2-x_1 & y_2-y_1 & z_2-z_1\\ l_1 & m_1 & n_1\\ l_2 & m_2 & n_2\end{vmatrix}=0.$$

在共面情况下, 两直线方向向量 $\boldsymbol{v}_1$ 与 $\boldsymbol{v}_2$ 夹角 θ 就是两直线夹角.

$$\cos\theta=\frac{\boldsymbol{v}_1\cdot\boldsymbol{v}_2}{|\boldsymbol{v}_1||\boldsymbol{v}_2|}=\frac{l_1l_2+m_1m_2+n_1n_2}{\sqrt{l_1^2+m_1^2+n_1^2}\sqrt{l_2^2+m_2^2+n_2^2}}$$

当 $\cos\theta=\pm1$ 时, $\boldsymbol{v}_1\parallel\boldsymbol{v}_2$, 因此$\boldsymbol{v}_1,\boldsymbol{v}_2$ 线性相关, 即存在常数 λ , 使 $\boldsymbol{v}_1=\lambda\boldsymbol{v}_2$, 所以两直线平行当且仅当

$$\frac{l_1}{l_2}=\frac{m_1}{m_2}=\frac{n_1}{n_2};$$

当 $|\cos\theta|<1$时两直线相交, 特别, 两直线互相垂直当且仅当

$$l_1l_2+m_1m_2+n_1n_2=0.$$

异面 直线 L_1 与 L_2 异面的充分必要条件是 $(\boldsymbol{r}_1-\boldsymbol{r}_2)\cdot\boldsymbol{v}_1\times\boldsymbol{v}_2\neq0$, 此时两直线既不平行, 也不相交, 称为**异面直线**. 例如道路与横跨上空输电线就是异面的两条直线.

3° 二次曲面

由 1° 和 2° 可知, 空间中平面和直线由一次代数方程(组)表示, 一般来说空间中由方程

$$F(x,y,z)=0$$

确定的图形, 即满足方程的点 (x,y,z) 的集合

$$S=\{(x,y,z)\mid F(x,y,z)=0\}$$

称为**一般曲面**. 而两个一般曲面的交线, 称为**一般曲线**, 即是方程

$$F(x,y,z)=0,\ G(x,y,z)=0$$

给出的图形

$$L=\{(x,y,z)\mid F(x,y,z)=0,\ G(x,y,z)=0\}.$$

特别, 当 $F(x,y,z)=0$ 是二次代数方程时, 称曲面为**二次曲面**. 例如二次方程

$$(x-x_0)^2+(y-y_0)^2+(z-z_0)^2=R^2$$

表示以$P_0(x_0,y_0,z_0)$ 为球心, R 为半径的球面, 因此球面是二次曲面.

下面给出一些典型二次曲面.

椭球面 (图 5.15) 设 $a>0,b>0,c>0$,

$$\frac{x^2}{a^2}+\frac{y^2}{b^2}+\frac{z^2}{c^2}=1.$$

椭球面与Oxy 平面相交的交线是椭圆, 一般情况下若与平行Oxy 平面 $z=h$ ($|h|<c$) 相交, 交线也是一个椭圆, 只是椭圆长半轴和短半轴分别为

$$a'=a\sqrt{1-\frac{h^2}{c^2}},\ b'=b\sqrt{1-\frac{h^2}{c^2}}.$$

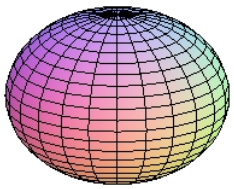


图 5.15

单叶和双叶双曲面 设 $a>0,b>0,c>0$,

$$\frac{x^2}{a^2}+\frac{y^2}{b^2}-\frac{z^2}{c^2}=\pm1.$$

上式取正号为单叶双曲面 (图 5.16), 取负号为双叶双曲面 (图 5.17).

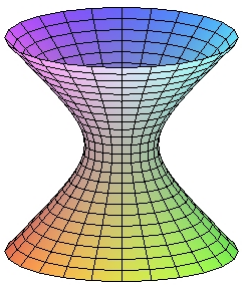


图 5.16

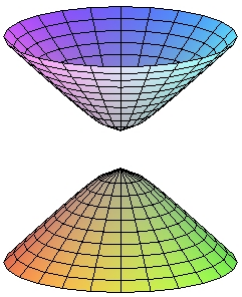


图 5.17

椭圆抛物面和双曲抛物面 设 $a>0, b>0$,

$$z=\frac{x^2}{a^2}\pm\frac{y^2}{b^2},$$

其中取正号为椭圆抛物面 (图 5.18) , 取负号为双曲抛物面 (图 5.19) . 双曲抛物面也称为**马鞍面**.

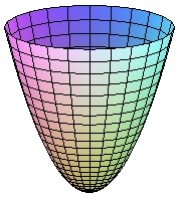


图 5.18

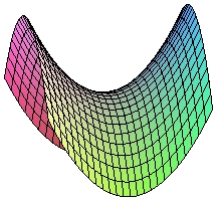


图 5.19

二次锥面 (图 5.20)

$$\frac{x^2}{a^2}+\frac{y^2}{b^2}-\frac{z^2}{c^2}=0,\quad a>0,\ b>0,\ c>0.$$

椭圆柱面、双曲柱面和抛物柱面 (图 5.21) , (图 5.22) , (图 5.23)

$$\frac{x^2}{a^2}+\frac{y^2}{b^2}=1\ (a>0,b>0);$$
$$\frac{x^2}{a^2}-\frac{y^2}{b^2}=1\ (a>0,b>0);$$
$$y^2=2px\ (p>0)$$

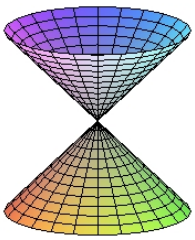


图 5.20

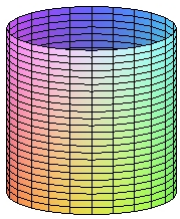


图 5.21

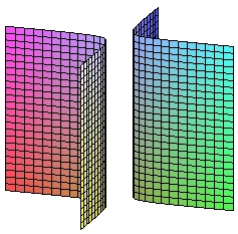


图 5.22

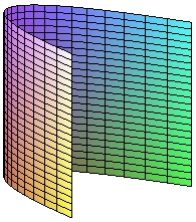


图 5.23

4° 坐标变换下二次曲面

以上罗列了一种椭球面、两种双曲面、两种抛物面、一种锥面以及三种柱面共九种二次曲面. 读者自然会问: 三元二次代数方程的一般形式为

$$a_1x^2+a_2y^2+a_3z^2+b_1xy+b_2yz+b_3xz+c_1x+c_2y+c_3z+d=0,$$

除了已经给出例子外, 其它二次代数方程表示什么样曲面? 同一个二次曲面在不同坐标系中代数方程有什么关系?

借助坐标变换, 可以证明, 尽管三元二次方程种类繁多, 但除一些退化情形 (如 $x^2+y^2=0, x^2-y^2=0$ 等等) 外, 通过坐标变换, 都可以变换到上述九种类型的**标准方程**, 因此三元二次代数方程所表示的曲面也仅仅有 (非平凡的) 九种. 正如在平面解析几何中, 通过 **配方法** (平面坐标变换), 可以把二元二次方程变换成标准椭圆、抛物或双曲方程一样.

例 5.4.5 二次方程 $z=xy$ 通过绕z 轴旋转 $-\dfrac{\pi}{4}$ (见例5.3.1), 则

$$x'=\frac{\sqrt{2}}{2}(x+y),\ y'=\frac{\sqrt{2}}{2}(x-y),\ z'=z,$$

方程变换为

$$z'=\frac{x'^2}{2}-\frac{y'^2}{2}.$$

因此 $z=xy$ 表示的也是马鞍面, 只是图5.17 中的马鞍面绕 z 轴旋转了$-\dfrac{\pi}{4}$ 而已.

§5.5 其它常用坐标系*

直角坐标系是通过确定原点和空间三个两两正交 (通常采用右手系) 的单位向量构成的, 它 (以及一般仿射坐标系) 的特征是: 任何一个坐标分量等于常数的点都构成一个平面. 例如 $z=c$ 表示空间中平行于坐标平面 Oxy 的平面, 因此称为**线性坐标系**. 下面介绍常用极坐标系、柱坐标系和球坐标系, 但这些坐标系已经不再是线性坐标系.

1° 平面的极坐标系

为了保持完整性, 首先回顾平面极坐标系. 在平面上取定一点 O (称为极点), 从极点引一条射线 Ox (称为极轴), 再选定一个长度单位和角度的正向 (通常取极轴正向的逆时针方向), 这样就构成了平面上的**极坐标系**. 对于平面上任意一点 P, 用 r 表示 P 到极点 O 距离 (向量 $\overrightarrow{OP}$ 的大小), θ 表示从极轴到向量 $\overrightarrow{OP}$ 正向夹角 (幅角), 则数

组 (r,θ) 可以用来确定点 P 在空间的位置, 并称为 P 点的极坐标. 这里, r 的取值范围为 $[0,+\infty)$, θ 的取值范围为 $[0,2\pi)$.

在平面直角坐标系 Oxy 中, 取原点为极坐标系极点, x 轴正向为极轴, 那么平面上任意点 P 的直角坐标和极坐标之间关系 (图 5.24) 如下:

$$\begin{cases} x = r\cos\theta \\ y = r\sin\theta \end{cases} \quad \text{或者} \quad \begin{cases} r = \sqrt{x^2+y^2} \\ \theta = \arctan\dfrac{y}{x} \end{cases}.$$

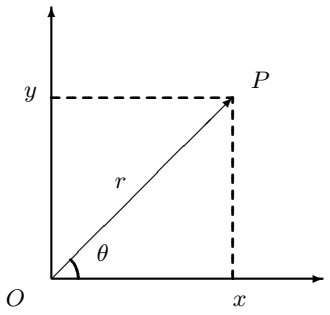


图 5.24

P 的位置向量可以表示为

$$\boldsymbol{r} = x\boldsymbol{i} + y\boldsymbol{j} = r\cos\theta\boldsymbol{i} + r\sin\theta\boldsymbol{j}.$$

不难发现, $r=$ 常数是平面上以原点为圆心的圆, $\theta=$ 常数是从原点出发的射线.

2° 柱面坐标系

取定直角坐标系 $Oxyz$, 对任意点 $P(x,y,z)$ 位置向量 $\overrightarrow{OP}$ 在 Oxy 平面上投影向量为 (图 5.25)

$$\overrightarrow{OP'} = x\boldsymbol{i} + y\boldsymbol{j},$$

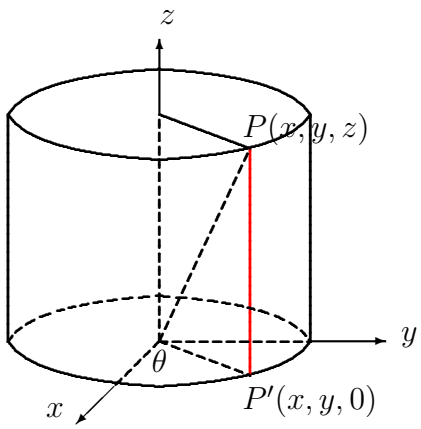


图 5.25

将该向量在 Oxy 中用极坐标表示

$$\overrightarrow{OP'} = r\cos\theta\boldsymbol{i} + r\sin\theta\boldsymbol{j},$$

因此, $P(x,y,z)$ 的位置向量可表示为

$$\overrightarrow{OP} = \overrightarrow{OP'} + z\boldsymbol{k} = r\cos\theta\boldsymbol{i} + r\sin\theta\boldsymbol{j} + z\boldsymbol{k}.$$

或者

$$x = r\cos\theta, \quad y = r\sin\theta, \quad z = z,$$

其中

$$0 \leqslant r < +\infty,\ 0 \leqslant \theta < 2\pi,\ -\infty < z < +\infty.$$

这样就给出了空间**柱面坐标系**. 数组$(r,\ \theta,\ z)$称为点 P 的柱面坐标. 在柱面坐标系中, $r=c>0$表示以 c 为半径圆柱面 $x^2+y^2=c^2$; $\theta=\theta_0$ 表示以 z 轴为边的半平面.

3° 球面坐标系

设 $P(x,y,z)$ 点位置向量 $\overrightarrow{OP}$ 与 z 轴方向角为 θ, $\overrightarrow{OP}$ 在 Oxy 平面投影向量为 $\overrightarrow{OP'}$ (图 5.26), 则

$$z=|OP|\cos\theta,\quad \boldsymbol{r}=\overrightarrow{OP}=\overrightarrow{OP'}+|OP|\cos\theta\boldsymbol{k}.$$

将点 P' 用 Oxy 平面的极坐标表示, 设 φ 是 $\overrightarrow{OP'}$ 在 Oxy 平面上的幅角, 则

$$\overrightarrow{OP'}=|OP'|\cos\varphi\boldsymbol{i}+|OP'|\sin\varphi\boldsymbol{j}.$$

令 $r=|OP|=|\boldsymbol{r}|$, 则 $|OP'|=|OP|\sin\theta$, 因此

$$\boldsymbol{r}=\overrightarrow{OP}=r\sin\theta\cos\varphi\boldsymbol{i}+r\sin\theta\sin\varphi\boldsymbol{j}+r\cos\theta\boldsymbol{k},$$

或

$$x=r\sin\theta\cos\varphi,\quad y=r\sin\theta\sin\varphi,\quad z=r\cos\theta.$$

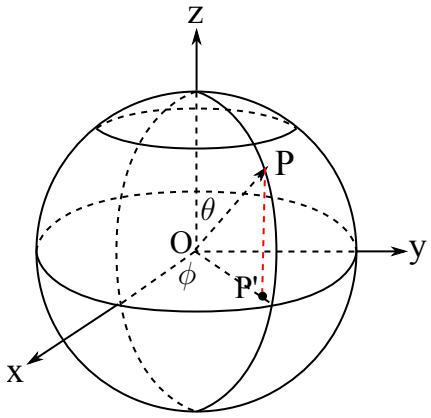


图 5.26

其中

$$0\leqslant r<+\infty,\ 0\leqslant\theta\leqslant\pi,\ 0\leqslant\varphi<2\pi.$$

数组 $(r,\ \theta,\ \varphi)$ 称为点 P 的球面座标, 所形成的坐标系称为 **球面座标系**. 显然 $r=$ 常数表示球面; $\theta=$ 常数表示锥面, $\varphi=$ 常数表示以 z 轴为边的半平面.

§5.6 一般向量空间

读者或已注意到, 在解析几何中, 无论是 “有大小, 有方向” 向量, 向量的加法和数乘, 还是向量共线或共面, 以及向量之间的夹角和内积, 几何上看十分直观. 当把几何对象或问题用代数表示, 空间中点或向量就由一组数 (x,y,z) 表示; 空间就成了数组的集合, 直观上的维数也就对应数组中数的个数; 共线或共面等价于线性相关.

把那些代数含义抽象出来, 可形成线性代数中向量空间的概念. 虽然以线性方程组解的结构为基础, 建立线性代数整体框架更加全面和深刻, 但解析几何却为理解向量空间提供了一个直观例子. 因此, 本节直接从这个直观例子出发, 抽象出一般向量空间的定义. 而从研究线性方程组入手, 导出向量空间、线性映射或线性变换的一整套理论, 将会在大学《线性代数》课程中详细讲授.

1° n 维向量空间

首先, 把空间中向量加法和数乘、所满足的性质5.1和性质5.2, 以及 “0 向量”、“负

向量”等概念悉数抽象出来, 作为一般向量空间的定义.

定义 5.14 设 V 是一个集合, V 中元素仍然称为“向量”, $\mathbb{F}$ 是一个给定数域(例如 $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ 等等), 又设 V 中定义两种运算(仍称为“加法”和“数乘”):

(1) 加法: 对任意 $\boldsymbol{a},\boldsymbol{b}\in V$, 对应 V 中唯一确定的向量, 记为 $\boldsymbol{a}+\boldsymbol{b}\in V$;

(2) 数乘: 对任意 $\boldsymbol{a}\in V$ 和任意 $\lambda\in\mathbb{F}$, 对应 V 中唯一确定的向量, 记为 $\lambda\boldsymbol{a}\in V$.

如果加法和数乘满足下列运算规则:

(i) $\boldsymbol{a}+\boldsymbol{b}=\boldsymbol{b}+\boldsymbol{a},\ \boldsymbol{a},\boldsymbol{b}\in V$;

(ii) $(\boldsymbol{a}+\boldsymbol{b})+\boldsymbol{c}=\boldsymbol{a}+(\boldsymbol{b}+\boldsymbol{c}),\ \boldsymbol{a},\boldsymbol{b},\boldsymbol{c}\in V$;

(iii) 存在一个元素$0\in V$, 称为“ *0* 向量”, 满足 $\boldsymbol{a}+0=0+\boldsymbol{a}=\boldsymbol{a},\ \boldsymbol{a}\in V$;

(iv) 对任意 $\boldsymbol{a}\in V$, 存在 $\boldsymbol{b}\in V$, 使得 $\boldsymbol{a}+\boldsymbol{b}=\boldsymbol{b}+\boldsymbol{a}=0$, 记$\boldsymbol{b}=-\boldsymbol{a}$, 称为 $\boldsymbol{a}$ 的“负向量”, 因此 $\boldsymbol{b}-\boldsymbol{a}=\boldsymbol{b}+(-\boldsymbol{a})$;

(v) 对$1\in\mathbb{F}$, 有 $1\cdot\boldsymbol{a}=\boldsymbol{a},\ \boldsymbol{a}\in V$;

(vi) $\lambda(\boldsymbol{a}+\boldsymbol{b})=\lambda\boldsymbol{a}+\lambda\boldsymbol{b},\ \boldsymbol{a},\boldsymbol{b}\in V,\ \lambda\in\mathbb{F}$;

(vii) $(\lambda+\mu)\boldsymbol{a}=\lambda\boldsymbol{a}+\mu\boldsymbol{a},\ \boldsymbol{a}\in V,\ \lambda,\mu\in\mathbb{F}$;

(viii) $(\lambda\mu)\boldsymbol{a}=\lambda(\mu\boldsymbol{a}),\ \boldsymbol{a}\in V,\ \lambda,\mu\in\mathbb{F}$;

那么称 V 是数域 $\mathbb{F}$ 上一个***向量空间***或***线性空间***.

今后为了方便, 将取 $\mathbb{F}$ 为实数域 $\mathbb{R}$, 除非特别说明.

在三维空间中, 通过选取三个不共面向量作为基向量, 进而得到坐标系. 向量共面(线)或不共面(线)等几何概念, 等价于“线性相关”和“线性无关”等代数概念(定理5.5). 将三维空间线性相关、线性无关的定义5.4推广到一般向量空间 V 上, 有

定义 5.15 设 V 是 $\mathbb{R}$ 上向量空间, $\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_k$ 是 V 中一组向量. 若存在不全为零实数 $\lambda_1,\lambda_2,\cdots,\lambda_k$, 使得

$$\lambda_1\boldsymbol{a}_1+\lambda_2\boldsymbol{a}_2+\cdots+\lambda_k\boldsymbol{a}_k=0,$$

则称向量组 $\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_k$ ***线性相关***. 若

$$\lambda_1\boldsymbol{a}_1+\lambda_2\boldsymbol{a}_2+\cdots+\lambda_k\boldsymbol{a}_k=0,$$

必推出 $\lambda_1=\lambda_2=\cdots=\lambda_k=0$, 则称 $\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_k$ ***线性无关***.

显然, V 中向量 $\boldsymbol{a}$ 和 $-\boldsymbol{a}$ 线性相关, 任意一个非零向量 $\boldsymbol{a}$ 线性无关; 线性无关的向量中不可能有 0 向量; 一组线性相关向量, 增加若干个向量仍然线性相关, 而一组线性无关向量, 去掉若干个, 剩余的非零个向量仍然线性无关(习题7).

定义 5.16 设 V 是 $\mathbb{R}$ 上向量空间, 如果 V 中存在 n 个向量 $\boldsymbol{e}_1,\boldsymbol{e}_2,\cdots,\boldsymbol{e}_n$, 满足

(i) $\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_n$ 线性无关.

(ii) 对任意 $\boldsymbol{x} \in V$, $\boldsymbol{x}$ 可由 $\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_n$ 线性表示, 即

$$\boldsymbol{x} = x_1\boldsymbol{e}_1 + x_2\boldsymbol{e}_2 + \cdots + x_n\boldsymbol{e}_n = \sum_{i=1}^{n} x_i\boldsymbol{e}_i,$$

那么称 $\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_n$ 称为 V 的一组**基**, 每个向量称为**基向量**; V 称为n **维向量空间**, n 称为 V 的**维数**, 并记 $n = \dim V$; 线性表示中的系数 $(x_1, x_2, \cdots, x_n)$ 称为向量 $\boldsymbol{x}$ 在基 $\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_n$ 下的**坐标**.

向量 $\boldsymbol{x}$ 在一组基 $\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_n$ 下的坐标是唯一的, 这是因为若存在两组坐标

$$\boldsymbol{x} = \sum_{i=1}^{n} x_i\boldsymbol{e}_i = \sum_{i=1}^{n} x_i'\boldsymbol{e}_i,$$

则 $\sum\limits_{i=1}^{n}(x_i - x_i')\boldsymbol{e}_i = 0$, 因基向量线性无关, 所以 $x_i = x_i'$, $i = 1, \cdots, n$, 即线性表示唯一.

必须说明: 在定义中, 若 $\boldsymbol{e}_1', \cdots, \boldsymbol{e}_m'$ 也是V 的一组基, 要证明 $n = m$ 才能使维数定义具有合理性. 这一结果包含在下列定理中.

定理 5.17 设 $\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_n$ 是向量空间 V 的一组基.

(i) 若 $\boldsymbol{a}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_r$ 是 V 中一组线性无关向量, 则 $r \leqslant n$.

(ii) 若 $\boldsymbol{e}_1', \cdots, \boldsymbol{e}_m'$ 是 V 的另一组基, 则 $m = n$.

证明 对于(i), 首先通过一个具体例子说明证明思路. 取$n = 2$, 并设 V 的基为 $\boldsymbol{e}_1, \boldsymbol{e}_2$. 只需证明不存在三个线性无关的向量即可. 采用反证法, 假设有三个向量 $\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3$ 线性无关, 根据定义5.16, $\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3$ 可由 $\boldsymbol{e}_1, \boldsymbol{e}_2$ 线性表示:

$$\boldsymbol{a}_1 = a_1\boldsymbol{e}_1 + a_2\boldsymbol{e}_2,\ \boldsymbol{a}_2 = b_1\boldsymbol{e}_1 + b_2\boldsymbol{e}_2,\ \boldsymbol{a}_3 = c_1\boldsymbol{e}_1 + c_2\boldsymbol{e}_2.$$

显然, a_1, a_2, 以及 b_1, b_2 和 c_1, c_2 分别不全为零. 若 $\lambda_1\boldsymbol{a}_1 + \lambda_2\boldsymbol{a}_2 + \lambda_3\boldsymbol{a}_3 = 0$, 则

$$(a_1\lambda_1 + b_1\lambda_2 + c_1\lambda_3)\boldsymbol{e}_1 + (a_2\lambda_1 + b_2\lambda_2 + c_2\lambda_3)\boldsymbol{e}_2 = 0,$$

因为 $\boldsymbol{e}_1, \boldsymbol{e}_2$ 线性无关, 所以

$$\begin{cases} a_1\lambda_1 + b_1\lambda_2 + c_1\lambda_3 = 0, \\ a_2\lambda_1 + b_2\lambda_2 + c_2\lambda_3 = 0. \end{cases}$$

这是两个方程的三元一次方程组. 不妨设 $a_1 \neq 0$, 将方程组中第一个方程两边乘以 $-\dfrac{a_2}{a_1}$ 并与第二个方程相加, 得

$$b'\lambda_2 + c'\lambda_3 = 0,$$

这里 b', c' 是常数. 从中求出不全为零的 λ_2, λ_3; 代入第一个方程求出 λ_1, 这样就得到不全为零的 $\lambda_1, \lambda_2, \lambda_3$ 满足方程组, 也就是满足 $\lambda_1\boldsymbol{a}_1 + \lambda_2\boldsymbol{a}_2 + \lambda_3\boldsymbol{a}_3 = 0$. 但是 $\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3$ 线性无关, 因此矛盾. 矛盾说明不可能有三个以上的向量线性无关.

对一般 n 和 r, 假如 $r > n$, 令

$$\boldsymbol{a}_i = \sum_{j=1}^{n} a_{ij}\boldsymbol{e}_j, \quad i = 1, 2, \cdots, r.$$

若有 $\lambda_1, \lambda_2, \cdots, \lambda_r$, 使得 $\lambda_1\boldsymbol{a}_1 + \lambda_2\boldsymbol{a}_2 + \cdots + \lambda_r\boldsymbol{a}_r = 0$, 那么 $\lambda_1, \lambda_2, \cdots, \lambda_r$ 满足 n 个 r 元一次方程的方程组

$$\begin{cases} a_{11}\lambda_1 + a_{12}\lambda_2 + \cdots + a_{1r}\lambda_r = 0, \\ a_{21}\lambda_1 + a_{22}\lambda_2 + \cdots + a_{2r}\lambda_r = 0, \\ \cdots\cdots \\ a_{n1}\lambda_1 + a_{n2}\lambda_2 + \cdots + a_{nr}\lambda_r = 0, \end{cases}$$

因 $n < r$, 对 n 采用归纳法, 并用类似上述具体例子, 可得到不全为零的解$\lambda_1, \lambda_2, \cdots, \lambda_r$, 因此推出矛盾, 这样就完成了证明.

对于 (ii), 因 $\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_n$ 是一组基, $\boldsymbol{e}'_1, \cdots, \boldsymbol{e}'_m$ 线性无关, 所以 $m \leqslant n$; 若 $\boldsymbol{e}'_1, \cdots, \boldsymbol{e}'_m$ 也是一组基, 但 $\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_n$ 线性无关, 所以 $n \leqslant m$, 即 $m = n$. □

上述定理说明: 向量空间 V 的基未必唯一, 但是不同基中向量个数一定相同.

如果 n 维向量空间 V 有两组基 $\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_n$ 和 $\boldsymbol{e}'_1, \boldsymbol{e}'_2, \cdots, \boldsymbol{e}'_n$, 那么两组基的基向量可以互相线性表示, 不妨设 $\boldsymbol{e}'_i$ 由 $\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_n$ 线性表示:

$$\boldsymbol{e}'_i = \sum_{j=1}^{n} \lambda_{ij}\boldsymbol{e}_j, \quad i = 1, 2, \cdots, n,$$

因此 V 中向量 $\boldsymbol{x}$ 分别在两组基的线性表示满足

$$\boldsymbol{x} = \sum_{i=1}^{n} x'_i\boldsymbol{e}'_i = \sum_{i=1}^{n} x'_i \sum_{j=1}^{n} \lambda_{ij}\boldsymbol{e}_j = \sum_{j=1}^{n} \left(\sum_{i=1}^{n} \lambda_{ij}x'_i \right) \boldsymbol{e}_j = \sum_{j=1}^{n} x_j\boldsymbol{e}_j$$

由此推出同一个向量 $\boldsymbol{x}$ 在两组基下坐标之间的坐标变换:

$$x_j = \sum_{i=1}^{n} \lambda_{ij}x'_i \quad j = 1, 2, \cdots, n.$$

例 5.6.1 设实数域 $\mathbb{R}$ 上由下列数组组成的集合

$$E_n = \{\boldsymbol{a} = (a_1, a_2, \cdots, a_n) \mid a_1, a_2, \cdots, a_n \in \mathbb{R}\},$$

对 E_n 中任意两个元素 $\boldsymbol{a}=(a_1,a_2,\cdots,a_n)$, $\boldsymbol{b}=(b_1,b_2,\cdots,b_n)$, 以及实数 $\lambda\in\mathbb{R}$, 定义加法和数乘如下:

$$\boldsymbol{a}+\boldsymbol{b}=(a_1+b_1,a_2+b_2,\cdots,a_n+b_n)$$
$$\lambda\boldsymbol{a}=(\lambda a_1,\lambda a_2,\cdots,\lambda a_n)$$

不难验证 E_n 满足向量空间的定义, 并且以 $(0,0,\cdots,0)$ 为 0 向量. 向量

$$\boldsymbol{e}_1=(1,0,\cdots,0),$$
$$\boldsymbol{e}_2=(0,1,\cdots,0),$$
$$\cdots\cdots$$
$$\boldsymbol{e}_n=(0,0,\cdots,1)$$

线性无关, 且对任意向量 $\boldsymbol{a}\in E_n$ 都可唯一表示为

$$\boldsymbol{a}=(a_1,a_2,\cdots,a_n)=a_1\boldsymbol{e}_1+a_2\boldsymbol{e}_2+\cdots+a_n\boldsymbol{e}_n.$$

因此 E_n 是 n 维向量空间, 称为n **维数组向量空间**或简称为**数组空间**.

例 5.6.2 集合 $\mathbb{Q}(\sqrt{2})=\{r+s\sqrt{2}\mid r,s\in\mathbb{Q}\}$ 是有理数域$\mathbb{Q}$ 上的 2 维向量空间.

证明 不难验证 $\mathbb{Q}(\sqrt{2})$ 满足向量空间定义5.14. 取 $\mathbb{Q}(\sqrt{2})$ 中两个向量 $\boldsymbol{e}_1=1,\boldsymbol{e}_2=\sqrt{2}$, 若存在有理数 λ_1,λ_2, 使得 $\lambda_1\boldsymbol{e}_1+\lambda_2\boldsymbol{e}_2=\lambda_1+\lambda_2\sqrt{2}=0$, 则当 $\lambda_2\neq0$ 时, 推出 $\sqrt{2}=-\dfrac{\lambda_1}{\lambda_2}$ 是有理数, 矛盾, 因此 $\lambda_2=0$, 进而推出 $\lambda_1=0$, 即 $\boldsymbol{e}_1,\boldsymbol{e}_2$ 线性无关.

对任意的 $\boldsymbol{x}=r+s\sqrt{2}\in\mathbb{Q}(\sqrt{2})$, 有 $\boldsymbol{x}=r+s\sqrt{2}=r\boldsymbol{e}_1+s\boldsymbol{e}_2$, 所以$\mathbb{Q}(\sqrt{2})$ 是 2 维向量空间, $\boldsymbol{e}_1=1,\boldsymbol{e}_2=\sqrt{2}$ 是 $\mathbb{Q}(\sqrt{2})$ 的一组基.

例 5.6.3 设 $F_n[x]$ 表示实数域 $\mathbb{R}$ 上次数不超过 n 的多项式全体

$$F_n[x]=\{f(x)=a_0+a_1x+\cdots+a_nx^n\mid a_0,a_1,\cdots,a_n\in\mathbb{R}\},$$

那么在多项式加法和数乘定义下, $F_n[x]$ 是 $\mathbb{R}$ 上 $n+1$ 维向量空间, 它的基为

$$1,x,x^2,\cdots,x^n\in F_n[x].$$

2° 向量空间的同构

定义 5.18 *设 V_1, V_2 是 $\mathbb{R}$ 上两个向量空间, 若存在 1-1 映射 $\sigma:V_1\longrightarrow V_2$ 满足*

(i) $\sigma(\boldsymbol{a}+\boldsymbol{b})=\sigma(\boldsymbol{a})+\sigma(\boldsymbol{b}),\ \boldsymbol{a},\boldsymbol{b}\in V_1$;

(ii) $\sigma(\lambda\boldsymbol{a})=\lambda\sigma(\boldsymbol{a}),\ \lambda\in\mathbb{R},\ \boldsymbol{a}\in V_1$,

*则称向量空间 V_1 与 V_2 **同构**, σ 称为**同构映射**. 当 $V_1=V_2$ 时, σ 称为**自同构**.*

根据定义, 显然有

$$\sigma(0)=0,$$
$$\sigma(-\boldsymbol{a})=-\sigma(\boldsymbol{a}),$$
$$\sigma(\lambda_1\boldsymbol{a}_1+\cdots+\lambda_m\boldsymbol{a}_m)=\lambda_1\sigma(\boldsymbol{a}_1)+\cdots+\lambda_m\sigma(\boldsymbol{a}_m),$$

这里 0 分别表示 V_1 和 V_2 中零向量, $\lambda_1,\cdots,\lambda_m$ 是任意实数, $\boldsymbol{a}_1,\cdots,\boldsymbol{a}_m\in V_1$.

定理 5.19 设 V_1,V_2,V_3 是$\mathbb{R}$ 上三个向量空间, 那么

(i) V_1 与自身同构, 同构映射即是 V_1 到 V_1 的恒同映射.

(ii) 若 $\sigma:V_1\longrightarrow V_2$ 是同构映射, 那么 $\sigma^{-1}:V_2\longrightarrow V_1$ 也是同构映射. 也就是若 V_1 与 V_2 同构, 则 V_2 与 V_1 同构.

(iii) 若 V_1 与 V_2 同构, V_2 与 V_3 同构, 则 V_1 与 V_3 同构.

(iv) 若 V_1 与 V_2 同构, 则同构映射把 V_1 中的任意线性无关组 $a_1,\cdots,\boldsymbol{a}_m$ 映射到 V_2 中的线性无关组 $\sigma(\boldsymbol{a}_1),\cdots,\sigma(\boldsymbol{a}_m)$.

(v) V_1 与 V_2 同构, 当且仅当 $\dim V_1=\dim V_2$.

定理中 (i), (ii), (iii) 表明向量空间同构关系是等价关系 (见定义2.23). 两个向量空间同构表明空间代数结构一样, 并不在意两个空间中向量的具体含义 .

证明 (i) 是显然的. 对于(ii) , 设 $\sigma:V_1\longrightarrow V_2$ 是同构映射, 因为是 1-1 映射, 所以逆映射 $\sigma^{-1}:V_2\longrightarrow V_1$ 存在而且也是 1-1 映射. 对任意 $\boldsymbol{a}',\boldsymbol{b}'\in V_2$,记

$$\boldsymbol{a}=\sigma^{-1}(\boldsymbol{a}'),\ \boldsymbol{b}=\sigma^{-1}(\boldsymbol{b}'),$$

那么 $\boldsymbol{a}'=\sigma(\boldsymbol{a}),\boldsymbol{b}'=\sigma(\boldsymbol{b})$, 推得 $\boldsymbol{a}'+\boldsymbol{b}'=\sigma(\boldsymbol{a}+\boldsymbol{b})$, 所以

$$\sigma^{-1}(\boldsymbol{a}'+\boldsymbol{b}')=\boldsymbol{a}+\boldsymbol{b}=\sigma^{-1}(\boldsymbol{a}')+\sigma^{-1}(\boldsymbol{b}').$$

对任意 $\lambda\in\mathbb{R}$,

$$\sigma^{-1}(\lambda\boldsymbol{a}')=\sigma^{-1}(\lambda\sigma(\boldsymbol{a}))=\sigma^{-1}(\sigma(\lambda\boldsymbol{a}))=\lambda\boldsymbol{a}=\lambda\sigma^{-1}(\boldsymbol{a}').$$

对于(iii) , 设 $\sigma_1:V_1\longrightarrow V_2$, $\sigma_2:V_2\longrightarrow V_3$, 则 $\sigma_2\circ\sigma_1:V_1\longrightarrow V_3$ 是 1-1 映射, 且对任意 $\boldsymbol{a},\boldsymbol{b}\in V_1$ 有

$$\begin{aligned}\sigma_2\circ\sigma_1(\boldsymbol{a}+\boldsymbol{b})&=\sigma_2(\sigma_1(\boldsymbol{a})+\sigma_1(\boldsymbol{b}))=\sigma_2(\sigma_1(\boldsymbol{a}))+\sigma_2(\sigma_1(\boldsymbol{b}))\\&=\sigma_2\circ\sigma_1(\boldsymbol{a})+\sigma_2\circ\sigma_1(\boldsymbol{b})\\\sigma_2\circ\sigma_1(\lambda\boldsymbol{a})&=\sigma_2(\sigma_1(\lambda\boldsymbol{a}))=\sigma_2(\lambda\sigma_1(\boldsymbol{a}))=\lambda\sigma_2(\sigma_1(\boldsymbol{a}))\\&=\lambda\sigma_2\circ\sigma_1(\boldsymbol{a})\end{aligned}$$

对于(iv), 设 $\sigma: V_1 \longrightarrow V_2$ 是同构映射, $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$ 是 V_1 的一组线性无关向量. 那么对任意实数 $\lambda_1, \cdots, \lambda_m$, 如果

$$\lambda_1\sigma(\boldsymbol{a}_1) + \lambda_2\sigma(\boldsymbol{a}_2) + \cdots + \lambda_m\sigma(\boldsymbol{a}_m) = 0,$$

就有

$$\sigma(\lambda_1\boldsymbol{a}_1 + \lambda_2\boldsymbol{a}_2 + \cdots + \lambda_m\boldsymbol{a}_m) = 0,$$

因此

$$\lambda_1\boldsymbol{a}_1 + \lambda_2\boldsymbol{a}_2 + \cdots + \lambda_m\boldsymbol{a}_m = 0,$$

推出 $\lambda_1 = \lambda_2 = \cdots = \lambda_m = 0$, 即 V_2 中向量 $\sigma(\boldsymbol{a}_1), \sigma(\boldsymbol{a}_1), \cdots, \sigma(\boldsymbol{a}_m)$ 线性无关.

对于(v), 设 $\dim V_1 = n$, $\boldsymbol{e}_1, \cdots, \boldsymbol{e}_n$ 是 V_1 的一组基, $\sigma: V_1 \longrightarrow V_2$ 是同构映射, 根据(iv), V_2 中向量组 $\sigma(\boldsymbol{e}_1), \sigma(\boldsymbol{e}_2), \cdots, \sigma(\boldsymbol{e}_n)$ 线性无关.

对任意 $\boldsymbol{x}' \in V_2$, 有 $\boldsymbol{x} \in V_1$, 使得 $\boldsymbol{x}' = \sigma(\boldsymbol{x})$, 将 $\boldsymbol{x}$ 在 V_1 中由$\boldsymbol{e}_1, \cdots, \boldsymbol{e}_n$ 线性表示:

$$\boldsymbol{x} = \lambda_1\boldsymbol{e}_1 + \lambda_2\boldsymbol{e}_2 + \cdots + \lambda_n\boldsymbol{e}_n,$$

那么 V_2 中任意的 $\boldsymbol{x}'$ 就由 $\sigma(\boldsymbol{e}_1), \sigma(\boldsymbol{e}_2), \cdots, \sigma(\boldsymbol{e}_n)$ 线性表示:

$$\begin{aligned}\boldsymbol{x}' = \sigma(\boldsymbol{x}) &= \sigma(\lambda_1\boldsymbol{e}_1 + \lambda_2\boldsymbol{e}_2 + \cdots + \lambda_n\boldsymbol{e}_n)\\ &= \lambda_1\sigma(\boldsymbol{e}_1) + \lambda_2\sigma(\boldsymbol{e}_2) + \cdots + \lambda_n\sigma(\boldsymbol{e}_n),\end{aligned}$$

也就是 $\sigma(\boldsymbol{e}_1), \sigma(\boldsymbol{e}_2), \cdots, \sigma(\boldsymbol{e}_n)$ 是 V_2 的一组基. 所以 $\dim V_2 = \dim V_1$.

反之若 $\dim V_1 = \dim V_2$, 分别取 V_1 的一组基 $\{\boldsymbol{e}_1, \cdots, \boldsymbol{e}_n\}$ 和 V_2 的一组基 $\{\boldsymbol{e}'_1, \cdots, \boldsymbol{e}'_n\}$, 按下列方式定义一个映射 σ, 先令

$$\sigma(\boldsymbol{e}_1) = \boldsymbol{e}'_1, \cdots, \sigma(\boldsymbol{e}_n) = \boldsymbol{e}'_n.$$

再对任意 $\boldsymbol{a} = \lambda_1\boldsymbol{e}_1 + \cdots + \lambda_n\boldsymbol{e}_n \in V_1$, 定义

$$\sigma(\boldsymbol{a}) = \lambda_1\sigma(\boldsymbol{e}_1) + \cdots + \lambda_n\sigma(\boldsymbol{e}_n) = \lambda_1\boldsymbol{e}'_1 + \cdots + \lambda_n\boldsymbol{e}'_n \in V_2,$$

可以验证 σ 是同构映射. □

例 5.6.4 $\mathbb{R}$ 上任何 n 维向量空间 V 与数组空间 E_n （例5.6.1 ）同构. 当选定 V 的一组基 $\{\boldsymbol{e}_1, \cdots, \boldsymbol{e}_n\}$ 后, 那么对任意 $\boldsymbol{a} \in V$, 同构映射就是

$$\sigma: \boldsymbol{a} = a_1\boldsymbol{e}_1 + \cdots + a_n\boldsymbol{e}_n \longrightarrow (a_1, \cdots, a_n),$$

反之以 E_n 中数组作为坐标, 就唯一对应 V 中一个向量.

因此, 从同构角度看, $\mathbb{R}$ 上 n 维向量空间 V 本质上与 n 维数组空间 E_n 无异.

例 5.6.5 例5.6.3 中 $F_n[x]$ 与 $n+1$ 维数组空间 E_{n+1} 同构. 同构映射为

$$a_0 + a_1x + \cdots + a_nx^n \longmapsto (a_0, a_1, \cdots, a_n).$$

3° 向量空间的子空间

定义 5.20 设 V 是 $\mathbb{R}$ 上 n 维向量空间, W 是 V 的非空子集, 若 W 对 V 中的加法和数乘运算也形成 $\mathbb{R}$ 上一个向量空间, 则称 W 是 V 的**子空间**. 不难验证, W 是 V 子空间的充分必要条件是 W 对加法和数乘保持封闭:

$$\lambda\boldsymbol{a} + \mu\boldsymbol{b} \in W \quad \boldsymbol{a}, \boldsymbol{b} \in W,\ \lambda, \mu \in \mathbb{R}.$$

因为 W 的基也是 V 的线性无关向量组, 由定理5.17, 推出 $\dim W \leqslant \dim V$.

若取 V 一组向量 $\boldsymbol{a}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_l \subset V$, 则可验证

$$W = \{\lambda_1\boldsymbol{a}_1 + \lambda_2 a_2 + \cdots + \lambda\boldsymbol{a}_l \mid \lambda_i \in \mathbb{R},\ \boldsymbol{a}_i \in S,\ i = 1, \cdots, l,\ l \in \mathbb{N}\}$$

是 V 的子空间, 称为 **由 $\boldsymbol{a}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_l$ 生成的子空间**, 记为 $W =< \boldsymbol{a}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_l >$. 特别当 $\boldsymbol{a}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_l$ 线性无关时, $\dim W = l$.

例 5.6.6 设 $l < n$, 则 n 维数组空间 E_n 中下列元素构成的子集合

$$W = \{(a_1, \cdots, a_l, 0, \cdots, 0) \in E_n \mid a_1, \cdots, a_l \in \mathbb{R}\},$$

是 E_n 的子空间. 不难验证, W 与 E_l 同构. 它们可类比三维空间的坐标平面和坐标轴.

例 5.6.7 在向量空间 $F_n[x]$ 中, 设

$$W = \{p(x) \mid p(-x) = p(x),\ p(x) \in F_n[x]\},$$

不难验证 W 是 $F_n[x]$ 的子空间, 该子空间也是线性无关向量

$$1, x^2, x^4, \cdots, x^{2m}$$

生成的子空间, 这里 $m = \left[\dfrac{n}{2}\right]$, $[a]$ 表示不超过 a 的最大整数. 因此 $\dim W = m + 1$.

4° 内积与欧氏空间

在三维空间中, 向量之间的内积是通过几何方式定义的 (定义5.6). 但从代数上看, 内积实际上是任意一对向量与一个实数的函数关系, 并且满足性质5.7. 因此将具体内积代数性质抽象出来, 可给出下列定义:

定义 5.21 设 V 是$\mathbb{R}$ 上向量空间, 如果 V 中任意一对向量 $\boldsymbol{a},\ \boldsymbol{b}\in V$, 对应一个实数, 记为 $(\boldsymbol{a},\boldsymbol{b})\in\mathbb{R}$, 并满足:

(i) 对称性: $(\boldsymbol{a},\boldsymbol{b})=(\boldsymbol{b},\boldsymbol{a}),\quad \boldsymbol{a},\ \boldsymbol{b}\in V$;

(ii) 线性性: $(\mu\boldsymbol{a}+\nu\boldsymbol{b},\ \boldsymbol{c})=\mu(\boldsymbol{a},\boldsymbol{c})+\nu(\boldsymbol{b},\boldsymbol{c}),\quad \boldsymbol{a},\boldsymbol{b},\boldsymbol{c}\in V,\ \mu,\ \nu\in\mathbb{R}$;

(iii) 正定性: $(\boldsymbol{a},\ \boldsymbol{a})\geqslant 0,\quad \boldsymbol{a}\in V,$ 等号成立当且仅当 $a=0$.

那么称 $(\boldsymbol{a},\boldsymbol{b})$ 为向量 $\boldsymbol{a}$ 和 $\boldsymbol{b}$ 的***内积***. $\mathbb{R}$ 上定义了内积的向量空间 V 称为***欧氏空间***.

注意到内积定义中线性性实际上也是“双线性性”, 即由对称性可以推出

$$(\boldsymbol{a},\ \mu\boldsymbol{b}+\nu\boldsymbol{c})=\mu(\boldsymbol{a},\boldsymbol{b})+\nu(\boldsymbol{a},\boldsymbol{c}).$$

定理 5.22 (Cauchy-Schwarz 不等式) 设 V 是欧氏空间, $(\cdot,\cdot)$ 是V 的一个内积, 则对任意两个向量 $\boldsymbol{a},\boldsymbol{b}\in V$, 有

$$|(\boldsymbol{a},\boldsymbol{b})|\leqslant\sqrt{(\boldsymbol{a},\boldsymbol{a})(\boldsymbol{b},\boldsymbol{b})}.$$

证明 对任意实数 λ 和 $\boldsymbol{a},b\in V$, 有

$$0\leqslant(\lambda\boldsymbol{a}+\boldsymbol{b},\lambda\boldsymbol{a}+\boldsymbol{b})=(\boldsymbol{a},\boldsymbol{a})\lambda^2+2(\boldsymbol{a},\boldsymbol{b})\lambda+(\boldsymbol{b},\boldsymbol{b}),$$

因此根据 λ 的二次多项式判别式即可证得定理. □

根据内积, 可以定义 V 中任意向量 $\boldsymbol{a}$ 大小 (称为**模**)

$$|\boldsymbol{a}|=\sqrt{(\boldsymbol{a},\boldsymbol{a})},$$

以及通过

$$\cos\theta=\frac{(\boldsymbol{a},\boldsymbol{b})}{|\boldsymbol{a}||\boldsymbol{b}|}$$

定义任意两个非零向量 $\boldsymbol{a},\boldsymbol{b}\in V$ 夹角 θ. 若两个非零向量内积为零 $(\boldsymbol{a},\boldsymbol{b})=0$, 则称 $\boldsymbol{a}$ 和 $\boldsymbol{b}$ 相互**正交**或相互垂直. 从内积满足的Cauchy-Schwarz 不等式, 还可以得到下列推论

推论 5.23 对任意两个向量 $\boldsymbol{a},\boldsymbol{b}\in V$, 有

三角不等式: $|\boldsymbol{a}+\boldsymbol{b}|\leqslant|\boldsymbol{a}|+|\boldsymbol{b}|$;

平行四边形等式: $|\boldsymbol{a}+\boldsymbol{b}|^2+|\boldsymbol{a}-\boldsymbol{b}|^2=2(|\boldsymbol{a}|^2+|\boldsymbol{b}|^2)$.

证明

$$\begin{aligned}|\boldsymbol{a}+\boldsymbol{b}|^2&=(\boldsymbol{a}+\boldsymbol{b},\boldsymbol{a}+\boldsymbol{b})=|\boldsymbol{a}|^2+|\boldsymbol{b}|^2+2(\boldsymbol{a},\boldsymbol{b})\\&\leqslant|\boldsymbol{a}|^2+|\boldsymbol{b}|^2+2|\boldsymbol{a}||\boldsymbol{b}|=(|\boldsymbol{a}|+|\boldsymbol{b}|)^2,\end{aligned}$$

两边开方就得到三角不等式. 而由下列两式相加得到

$$\begin{aligned}|\boldsymbol{a}+\boldsymbol{b}|^2&=(\boldsymbol{a}+\boldsymbol{b},\boldsymbol{a}+\boldsymbol{b})=|\boldsymbol{a}|^2+|\boldsymbol{b}|^2+2(\boldsymbol{a},\boldsymbol{b})\\|\boldsymbol{a}-\boldsymbol{b}|^2&=(\boldsymbol{a}-\boldsymbol{b},\boldsymbol{a}-\boldsymbol{b})=|\boldsymbol{a}|^2+|\boldsymbol{b}|^2-2(\boldsymbol{a},\boldsymbol{b})\end{aligned}$$

就得到平行四边形等式 □

例 5.6.8 设 E_n 和 $\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_n$ 是例5.6.1 中给出的 n 维向量空间和它的一组基, 对任意一对向量 $\boldsymbol{a}, \boldsymbol{b} \in E_n$:

$$\boldsymbol{a} = a_1\boldsymbol{e}_1 + a_2\boldsymbol{e}_2 + \cdots + a_n\boldsymbol{e}_n, \quad \boldsymbol{b} = b_1\boldsymbol{e}_1 + b_2\boldsymbol{e}_2 + \cdots + b_n\boldsymbol{e}_n,$$

定义

$$(\boldsymbol{a}, \boldsymbol{b}) = a_1b_1 + a_2b_2 + \cdots + a_nb_n.$$

不难验证它是 E_n 上的一个内积. 因此 E_n 关于这个内积形成欧氏空间, 并特别记为 $\mathbb{R}^n$.

在上述内积的定义下, 基向量两两正交:

$$(\boldsymbol{e}_i, \boldsymbol{e}_j) = \delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j. \end{cases}$$

(i) 向量的模长:

$$|\boldsymbol{a}| = \sqrt{a_1^2 + a_2^2 + \cdots + a_n^2}.$$

(ii) 两向量的夹角:

$$\cos\theta = \frac{a_1b_1 + a_2b_2 + \cdots + a_nb_n}{\sqrt{a_1^2 + a_2^2 + \cdots + a_n^2}\sqrt{b_1^2 + b_2^2 + \cdots + b_n^2}}.$$

因此对任何实数 $a_1, \cdots, a_n$ 和 $b_1, \cdots, b_n$, 有

(iii) Cauchy-Schwarz 不等式:

$$(a_1b_1 + \cdots + a_nb_n)^2 \leqslant (a_1^2 + \cdots + a_n^2)(b_1^2 + \cdots b_n^2).$$

(iv) 三角不等式

$$\sqrt{(a_1 + b_1)^2 + \cdots + (a_n + b_n)^2} \leqslant \sqrt{a_1^2 + \cdots + a_n^2} + \sqrt{b_1^2 + \cdots + b_n^2}.$$

(v) 平行四边形等式:

$$\begin{aligned}&(a_1 + b_1)^2 + \cdots + (a_n + b_n)^2 + (a_1 - b_1)^2 + \cdots + (a_n - b_n)^2 \\ &= 2((a_1^2 + \cdots + a_n^2) + (b_1^2 + \cdots + b_n^2)).\end{aligned}$$

因此, 配备上述内积的数组空间 $\mathbb{R}^n$ 实际上是解析几何中三维空间的直接推广. 一般情况下, 设 V 是$\mathbb{R}$ 上 n 维向量空间, $(\cdot, \cdot)$ 是它的内积, $\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_n$ 是一组基. 记

$$g_{ij} = (\boldsymbol{e}_i, \boldsymbol{e}_j), \quad i, j = 1, 2, \cdots, n.$$

或表示成矩阵形式

$$G=\begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & & \vdots \\ g_{n1} & g_{n2} & \cdots & g_{nn} \end{pmatrix}=\begin{pmatrix} (\boldsymbol{e}_1,\boldsymbol{e}_1) & (\boldsymbol{e}_1,\boldsymbol{e}_2) & \cdots & (\boldsymbol{e}_1,\boldsymbol{e}_n) \\ (\boldsymbol{e}_2,\boldsymbol{e}_1) & (\boldsymbol{e}_2,\boldsymbol{e}_2) & \cdots & (\boldsymbol{e}_2,\boldsymbol{e}_n) \\ \vdots & \vdots & & \vdots \\ (\boldsymbol{e}_n,\boldsymbol{e}_1) & (\boldsymbol{e}_n,\boldsymbol{e}_2) & \cdots & (\boldsymbol{e}_n,\boldsymbol{e}_n) \end{pmatrix},$$

这样, V 中任意一对向量

$$\boldsymbol{a}=a_1\boldsymbol{e}_1+a_2\boldsymbol{e}_2+\cdots+a_n\boldsymbol{e}_n,\quad \boldsymbol{b}=b_1\boldsymbol{e}_1+b_2\boldsymbol{e}_2+\cdots+b_n\boldsymbol{e}_n,$$

的内积也就确定了:

$$(\boldsymbol{a},\boldsymbol{b})=\sum_{i,j=1}^{n} g_{ij}a_ib_j.$$

矩阵 G 称为内积 $(\cdot,\cdot)$ 在基 $\boldsymbol{e}_1,\boldsymbol{e}_2,\cdots,\boldsymbol{e}_n$ 下的**度量矩阵**. 它具有一系列特定的性质, 例如 G 中元素满足对称性: $g_{ij}=g_{ji}$ 等等. 反之, 任何满足这些性质的度量矩阵, 都可以定义 V 上的内积, 详情不再讨论.

§5.7 线性方程组

考察包含 n 个未知量 $x_1,x_2,\cdots,x_n$ 并由 m 个方程组成的线性方程组

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

其中系数 $a_{ij},i=1,\cdots,m,j=1,\cdots,n$ 以及 $b_i,\ i=1,\cdots,m$ 是给定实数. 把方程组系数按下列方式组成矩阵

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix},$$

称为$m\times n$ **矩阵**, 特别, 当 $m=n$ 时, $n\times n$ 矩阵 A 称为n **阶方阵**. 方程组 (1) 可简写为

$$A\boldsymbol{x}=\boldsymbol{b},\quad \boldsymbol{x}=\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix},\ \boldsymbol{b}=\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \tag{2}$$

这里把向量写成列的形式称为**列向量**, 而通常写成行的形式称为**行向量**. 对于 $A\boldsymbol{x}=\boldsymbol{b}$ 中矩阵与向量乘法, 理解为用矩阵 A 第一行每个分量与列向量 $\boldsymbol{x}$ 对应分量相乘后再相加就得到第一个方程, 其它类似. 称方程组 (1) 或 (2) 为**非齐次线性方程组**.

当 $b_i=0,\ i=1,\cdots,m$ （ $\boldsymbol{b}=0$) 时, 方程组

$$A\boldsymbol{x}=0 \tag{3}$$

称为**齐次线性方程组**. 这里不打算讨论 (2) 和 (3) 解的一般理论, 仅以例子做出说明.

1° 系数矩阵为方阵非齐次线性方程组的解

例 5.7.1 考虑下列线性方程组

$$\begin{cases} x+\ y+\ z=b_1, \\ x+2y+3z=b_2, \\ 2x\quad -\ z=b_3. \end{cases}$$

这里 b_1,b_2,b_3 是任意给定实数. 用矩阵表示, 该方程组为

$$A\boldsymbol{x}=\boldsymbol{b},\ A=\begin{pmatrix}1&1&1\\1&2&3\\2&0&-1\end{pmatrix},\ \boldsymbol{x}=\begin{pmatrix}x\\y\\z\end{pmatrix},\ \boldsymbol{b}=\begin{pmatrix}b_1\\b_2\\b_3\end{pmatrix}, \tag{4}$$

其中方程组的系数矩阵是 3 阶方阵.

从几何上看, 在 $Oxyz$ 坐标系中, 方程组 (4) 中三个方程分别表示三个平面, 方程组的解即是三个平面的交点 (x,y,z). 而三个平面相交于一点当且仅当三个平面法向量

$$\boldsymbol{v}_1=(1,1,1),\ \boldsymbol{v}_2=(1,2,3),\ \boldsymbol{v}_3=(2,0,-1)$$

不共面. 注意到三个法向量 $\boldsymbol{v}_1,\boldsymbol{v}_2,\boldsymbol{v}_3$ 正是矩阵 A 中三行构成的行向量.

从代数上看, 把矩阵 A 的三列分别记为 $\mathbb{R}^3$ 中三个列向量

$$\boldsymbol{a}_1=\begin{pmatrix}1\\1\\2\end{pmatrix},\ \boldsymbol{a}_2=\begin{pmatrix}1\\2\\0\end{pmatrix},\ \boldsymbol{a}_3=\begin{pmatrix}1\\3\\-1\end{pmatrix},$$

那么方程组 (4) 可以看成向量 $\boldsymbol{b}$ 由 $\boldsymbol{a}_1,\boldsymbol{a}_2,\boldsymbol{a}_3$ 线性表示:

$$x\boldsymbol{a}_1+y\boldsymbol{a}_2+z\boldsymbol{a}_3=\boldsymbol{b},$$

因此方程组有唯一解, 当且仅当 $\boldsymbol{a}_1,\boldsymbol{a}_2,\boldsymbol{a}_3$ 是 $\mathbb{R}^3$ 中线性无关向量.

不管是从几何上还是从代数上看, 不管是矩阵A 的行向量不共面, 还是列向量线性无关, 共同特点是矩阵对应的行列式不为零 (参见§5.2 的最后关于行列式部分)!

$$\det A = \begin{vmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 2 & 0 & -1 \end{vmatrix} = 1 \neq 0.$$

因此系数矩阵是方阵的非齐次线性方程组有唯一解, 当且仅当系数矩阵对应行列式不等于零. 当然, 对于 n 阶方阵A, 需要事先定义 A 的行列式, 这里就不再展开了.

2° 系数矩阵为 $m \times n$ 矩阵的线性方程组的解

首先考虑齐次线性方程组 (3). 记所有解的集合为

$$V = \{\boldsymbol{x} = (x_1, x_2, \cdots, x_n) \mid A\boldsymbol{x} = 0\},$$

定理 5.24 *齐次线性方程组 (3) 解集 V 是 $\mathbb{R}^n$ (例5.6.8) 的子空间, 也称为方程组 (3) 解空间.*

证明 不难验证若 $\boldsymbol{x}_1 = (x_1, x_2, \cdots, x_n)$, $\boldsymbol{x}_2 = (x_1', x_2', \cdots, x_n')$ 分别是(3) 的解, 则 $\mu\boldsymbol{x}_1 + \nu\boldsymbol{x}_2, \mu, \nu \in \mathbb{R}$ 也是解, 因此 V 是 $\mathbb{R}^n$ 的子空间. □

设 $\boldsymbol{e}_1, \cdots, \boldsymbol{e}_m$ 是 V 中一组基 (因此基向量 $\boldsymbol{e}_i, i = 1, \cdots, m$ 都是 (3) 的解), 称为 (3) 的**基本解组**, 那么 (3) 的任何解可由基本解组线性表示 (也称为 (3) 的通解)

$$\boldsymbol{x} = \lambda_1\boldsymbol{e}_1 + \cdots + \lambda\boldsymbol{e}_m.$$

解空间 V 的维数与方程组的系数 a_{ij} 密切相关, 下面, 通过一个例子加以说明.

例 5.7.2 设齐次线性方程组

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = 0, \\ x_1 + 2x_2 + 3x_3 - 2x_4 = 0, \\ x_1 - x_3 + 4x_4 = 0. \end{cases} \tag{5}$$

利用消元法可得方程组的解有如下形式

$$\boldsymbol{x} = (\lambda - 4\mu,\ -2\lambda + 3\mu,\ \lambda,\ \mu) = \lambda\boldsymbol{e}_1 + \mu\boldsymbol{e}_2,$$

其中λ, μ 是任意实数,

$$\boldsymbol{e}_1 = (1, -2, 1, 0),\ \boldsymbol{e}_2 = (-4, 3, 0, 1).$$

是两个线性无关的解, 构成方程的基本解组. 因此解空间 V 是$\mathbb{R}^4$ 的 2 维子空间. 从另

一个角度看, 方程组的系数矩阵为

$$A=\begin{pmatrix}1&1&1&1\\1&2&3&-2\\1&0&-1&4\end{pmatrix}$$

其中的列向量为

$$\boldsymbol{a}_1=\begin{pmatrix}1\\1\\1\end{pmatrix},\ \boldsymbol{a}_2=\begin{pmatrix}1\\2\\0\end{pmatrix},\ \boldsymbol{a}_3=\begin{pmatrix}1\\3\\-1\end{pmatrix},\ \boldsymbol{a}_4=\begin{pmatrix}1\\-2\\4\end{pmatrix},$$

此时方程组 (5) 可表示为

$$x_1\boldsymbol{a}_1+x_2\boldsymbol{a}_2+x_3\boldsymbol{a}_3+x_4\boldsymbol{a}_4=0,$$

不难看出向量组 $\boldsymbol{a}_1,\boldsymbol{a}_2,\boldsymbol{a}_3,\boldsymbol{a}_4$ 中, $\boldsymbol{a}_1,\boldsymbol{a}_2$ 线性无关, 且$\boldsymbol{a}_3,\boldsymbol{a}_4$ 可由 $\boldsymbol{a}_1,\boldsymbol{a}_2$ 线性表示:

$$\boldsymbol{a}_3=2\boldsymbol{a}_2-\boldsymbol{a}_1,\ \boldsymbol{a}_4=4\boldsymbol{a}_1-3\boldsymbol{a}_2.$$

称这样的 $\boldsymbol{a}_1,\boldsymbol{a}_2$ 是$\boldsymbol{a}_1,\boldsymbol{a}_2,\boldsymbol{a}_3,\boldsymbol{a}_4$ 的**极大线性无关组**. 因此方程简化为

$$(x_1-x_3+4x_4)\boldsymbol{a}_1+(x_2+2x_3-3x_4)\boldsymbol{a}_2=0,$$

因为 $\boldsymbol{a}_1,\boldsymbol{a}_2$ 线性无关, 所以有

$$x_1-x_3+4x_4=0,\ x_2+2x_3-3x_4=0.$$

其中, x_3,x_4 可以取任意实数, $x_3=\lambda,\ x_4=\mu$. 而 x_1,x_2 分别为 $x_1=\lambda-4\mu,\ x_2=-2\lambda+3\mu$. 解空间维数等于 $\mathbb{R}^4$ 维数减去系数矩阵中列向量极大线性无关组向量的个数.

定义 5.25 *对一般的齐次方程组 (3), 系数矩阵 A 的 n 个 m 维列向量中, 极大线性无关组包含的向量个数, 称为 A 的**列秩**.*

定理 5.26 *齐次线性方程组 (3) 的解空间 V 的维数满足*

$$\dim V=n-A\text{的列秩}.$$

限于篇幅, 定理的证明从略.

注记: 同样可定义 A 的 m 个 n 维行向量的极大线性无关组和行秩. 虽然 A 的列向量与行向量的维数不等, 但列秩和行秩是相等的, 因此称为矩阵 A 的秩, 记为 $\operatorname{rank}(A)$, 详情不再赘述.

对于非齐次线性方程组 (2) , 它的任意两个解的差满足对应的齐次线性方程组, 即

$$\text{若 } A\boldsymbol{x}=\boldsymbol{b},\ A\boldsymbol{x}'=\boldsymbol{b},\ \text{则 } A(\boldsymbol{x}-\boldsymbol{x}')=0.$$

因此, 若 $\boldsymbol{x}_0=(x_1^0,x_2^0,\cdots,x_n^0)$ 是非齐次一个特解, $\boldsymbol{e}_1,\cdots,\boldsymbol{e}_m$ 是对应齐次线性方程的基本解组, 那么非齐次方程 (2) 所有解 (即通解) 为

$$\boldsymbol{x}=\boldsymbol{x}_0+\lambda_1\boldsymbol{e}_1+\cdots+\lambda\boldsymbol{e}_m,\quad \lambda_1,\cdots,\lambda_m\in\mathbb{R}.$$

当然, 并非所有非齐次线性方程组都存在解. 下面的例子给出解释

例 5.7.3 考虑方程组 (5) 的非齐次情形

$$\begin{cases} x_1+\ x_2+\ \ x_3+\ \ x_4=b_1,\\ x_1+2x_2+3x_3-2x_4=b_2,\\ x_1\qquad -\ \ x_3+4x_4=b_3. \end{cases}\tag{6}$$

该方程有解$(x_1^0,x_2^0,x_3^0,x_4^0)$, 当且仅当

$$x_1^0\boldsymbol{a}_1+x_2^0\boldsymbol{a}_2+x_3^0\boldsymbol{a}_3+x_4^0\boldsymbol{a}_4=\boldsymbol{b},\ \boldsymbol{b}=\begin{pmatrix}b_1\\b_2\\b_3\end{pmatrix},$$

这里 $\boldsymbol{a}_1,\boldsymbol{a}_2,\boldsymbol{a}_3,\boldsymbol{a}_4$ 同例5.7.2, $\boldsymbol{a}_1,\boldsymbol{a}_2$ 线性无关, 因此

$$(x_1^0-x_3^0+4x_4^0)\boldsymbol{a}_1+(x_2^0+2x_3^0-3x_4^0)\boldsymbol{a}_2=\boldsymbol{b},$$

因此 (6) 有解当且仅当 $\boldsymbol{b}$ 能由 $\boldsymbol{a}_1,\boldsymbol{a}_2$ 线性表示, 因此 $\boldsymbol{a}_1,\boldsymbol{a}_2$ 分别是 $\boldsymbol{a}_1,\boldsymbol{a}_2,\boldsymbol{a}_3,\boldsymbol{a}_4$ 和 $\boldsymbol{a}_1,\boldsymbol{a}_2,\boldsymbol{a}_3,\boldsymbol{a}_4,\boldsymbol{b}$ 的极大线性无关组. 把两组向量分别作为矩阵 A 和 $\widetilde{A}$ 的列向量

$$A=\begin{pmatrix}1&1&1&1\\1&2&3&-2\\1&0&-1&4\end{pmatrix},\quad \widetilde{A}=\begin{pmatrix}1&1&1&1&b_1\\1&2&3&-2&b_2\\1&0&-1&4&b_3\end{pmatrix}$$

那么 (6) 有解的充分必要条件是两个矩阵的列秩相等:

$$A\text{的列秩}=\widetilde{A}\text{的列秩}.$$

矩阵 $\widetilde{A}$ 称为矩阵 A 的**增广矩阵**. 对一般的线性方程组 (2), 它的增广矩阵就是在系数矩阵 A 中再添加一列 $\boldsymbol{b}$.

例 5.7.4 考虑单个方程的 n 元线性方程

$$a_1x_1+a_2x_2+\cdots+a_nx_n=b,\tag{7}$$

系数矩阵A 只有一行, 而每一列均是一个数. 因此 A 的列秩等于 1. 即对应的齐次方程

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0, \tag{8}$$

的解空间为 V 是 $\mathbb{R}^n$ 的 $n-1$ 维子空间.

注意到无论是非齐次方程 (7) 还是齐次方程 (8), 都是三维空间平面方程形式上的推广. 由于系数矩阵实际上是一个 n 维向量, 因此记为 $\boldsymbol{a} = (a_1, a_2, \cdots, a_n)$. 利用 $\mathbb{R}^n$ 中内积, 方程 (7) 和 (8) 可表示为

$$(\boldsymbol{a}, \boldsymbol{x}) = b \ \text{(非齐次方程)};$$
$$(\boldsymbol{a}, \boldsymbol{x}) = 0 \ \text{(齐次方程)}.$$

因此, 齐次方程的解空间 V 是$\mathbb{R}^n$ 中那些与已知向量 $\boldsymbol{a}$ 垂直的向量形成的子空间, 也称 V 为 $\mathbb{R}^n$ 中的 $n-1$ 维**超平面**. 因 $(0, 0, \cdots, 0) \in V$, 因此超平面过 $\mathbb{R}^n$ 中的 “原点” .

若 $\boldsymbol{x}_0 = (x_1^0, x_2^0, \cdots, x_n^0)$ 是非齐次方程 (7) 的一个特解 (特解显然存在), 则 (7) 的任意解 $\boldsymbol{x}$ 满足 $(\boldsymbol{x} - \boldsymbol{x}_0, \boldsymbol{a}) = \boldsymbol{b} - \boldsymbol{b} = 0$, 即 $\boldsymbol{x} - \boldsymbol{x}_0 \in V$, 因此非齐次方程 (7) 的解的集合可以看成是超平面 V “平移” 到过 $\boldsymbol{x}_0$ “点” 的 “超平面” .

注记: 对包含 m 个方程的齐次线性方程组 (3), 其中每一个方程的解空间都是一个 $n-1$ 维的超平面, 因此整个齐次线性方程组的解空间就是 m 个 $n-1$ 维的超平面的交, 因此是 ($n - A$的列秩) 维的超平面.

第 5 讲习题

1. 已知空间中三个向量满足 $\boldsymbol{a}+\boldsymbol{b}+\boldsymbol{c}=0$, 试证:

$$\boldsymbol{a}\times\boldsymbol{b}=\boldsymbol{b}\times\boldsymbol{c}=\boldsymbol{c}\times\boldsymbol{a}.$$

反之, 若上式成立, 且$\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}$ 不共线, 证明 $\boldsymbol{a}+\boldsymbol{b}+\boldsymbol{c}=0$.

2. 在 $\triangle ABC$ 中, D,E 分别是边 BC,AC 的中点, AD,BE 相交于点 G. 证明: $AG=\frac{2}{3}AD$.

3. 证明下列两条直线是异面直线 (即不平行也不相交的两条直线)

$$\begin{cases}x+y-z-1=0,\\ 2x+y-z-2=0\end{cases}\quad\text{和}\quad\begin{cases}x+2y-z-2=0,\\ x+2y+2z+4=0.\end{cases}$$

并求两条直线的距离 (即两直线的公垂线段之长度).

4. 试求 $\dfrac{\sin\theta+3}{\cos\theta+2}$ $(0\leqslant\theta\leqslant\pi)$ 的最大值和最小值.

提示: 可考虑平面上点 $(-2,-3)$ 到以原点为圆心的单位圆上点的直线的斜率.

5. 下面方程刻划的是什么图形?

$$4x^2+25y^2+4z^2-16x-50y-16z-43=0.$$

6. 过原点作圆 $x^2+y^2-2x-4y+4=0$ 的任意割线交圆于 P_1,P_2, 求 P_1P_2 的中点 P 的轨迹.

7. 考虑两平面 Π_1 和 Π_2 之间的投影映射 (见第 1 讲第 4 节), 试证明 Π_1 上的圆可投影为 Π_2 上的椭圆、抛物线和双曲线.
提示: 不妨取 Π_1 为 Oxz 平面, Π_2 为 Oxy 平面. 取空间中一点 $Q(0,-1,\lambda)$ 作为投影的中心点, 以及 Oxz 平面上的圆 $x^2+(z-c)^2=1$. 给出圆上任意一点 $P(x,0,z)$ 在Oxy 平面上的投影 $P'(x',y',0)$, 求出 $P'(x',y',0)$ 满足的方程, 并讨论 λ 的取值.

8. 试证明: 线性无关的向量组去掉若干个向量后, 余下的非零个向量仍然线性无关; 在线性相关组增加任何若干个向量组成的向量组, 仍然线性相关.

9. 证明: 在区间 $[a,b]$ 上函数构成的空间中, $\boldsymbol{e}^{k_1x}$, $\boldsymbol{e}^{k_2x}$ $(k_1\neq k_2)$ 线性无关.

10. 设 $\boldsymbol{e}_1=\boldsymbol{i}+\boldsymbol{j}$, $\boldsymbol{e}_2=\boldsymbol{j}+\boldsymbol{k}$ 是 $\mathbb{R}^3$ 中两个向量 (这里 $\boldsymbol{i},\boldsymbol{j},\boldsymbol{k}$ 为 $\mathbb{R}^3$ 中相互垂直的单位向量). 试证明 $V=\{\alpha\boldsymbol{e}_1+\beta\boldsymbol{e}_2\mid\alpha,\beta\in\mathbb{R}\}$ 是 $\mathbb{R}^3$ 中的 2 维子空间.

11. 设 $\boldsymbol{a},\boldsymbol{b}$ 是 $\mathbb{R}^n$ 中单位向量, $|\boldsymbol{a}+\boldsymbol{b}|=1$, 求 $|\boldsymbol{a}-\boldsymbol{b}|$ 的值.

12. 求下列齐次线性方程组的通解

$$\begin{aligned} x + z &= 0, \\ y + z &= 0, \\ x + y + 2z &= 0 \end{aligned}$$

并确定 V 的维数, 给出一组基向量.

第 6 讲　尺规作图

所谓**尺规作图**是指从一些已知图形出发, 仅限于用没有刻度直尺和圆规 (以下简称**尺规**) 作出新的图, 因此又称**几何作图**.

§6.1　尺规在作图中的功能

先从一个例子谈起.

例 6.1.1　作出已知直线段 AB 的垂直平分线 (当然也就得到它的平分点) .

具体做法是: 分别以 A 和 B 作为圆心, 以超过 AB 长度一半长度 r 为半径, 用圆规作两个相交圆, 再用直尺连接圆两个交点, 就得到 AB 垂直平分线和平分点 (图 6.1) .

类似问题统称为**作图问题**. 为了方便, 今后把能够用尺规作出的作图问题称为是**可解**的, 不能作出的称为是**不可解**的.

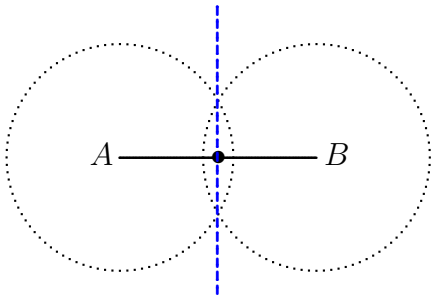


图 6.1

并不是每个作图问题都可解, 例如三等分角问题, 倍立方体问题, 求作正七边形问题以及化圆成方问题等等, 是无法用圆规和直尺来完成的 (将在§ 6.5 讨论) . 这样就产生了一个问题, 究竟哪些作图问题可解, 哪些不可解. 用什么方法判断一个作图问题可解还是不可解.

本专题主要从尺规作图问题, 如何发现它背后的数学, 并不讨论具体的作图过程.

尺规在作图中有如下基本功能:

(1) 过两个已知点作一条直线;

(2) 以已知点为圆心, 以已知长度为半径作一个圆;

(3) 作两条已知直线的交点;

(4) 作一个圆与已知圆或已知直线的交点.

功能 (1) 和 (2) 分别是直尺和圆规仅有的功能, 根据给定条件 (定点和定长) 用直尺或圆规直接完成. 后两种功能需要根据给定条件, 用尺规找出交点. 尺规作图正是按上述功能, 一个步骤接着一个步骤的过程, 也就是已知前面一步, 如何用尺规作出下一步的图形.

根据解析几何观点, 在平面上建立直角坐标系之后, 平面上点可由坐标表示, 知道了

点就知道了它的坐标, 知道了坐标就可以作出点. 而点的坐标是一对实数, 因此从给定点, 用尺规作出新的点, 就是从已知数用尺规作出新的数. 形象地说, 就是如何把尺规作图问题转化为 “数字化” 问题, 进而用代数方法研究作图的可解问题.

例 6.1.2 作已知角 $\angle AOB$ 的角平分线.

具体做法是: 不妨设 OA 和 OB 长度相等 (若不然, 可以通过以 O 为圆心, 用圆规以定长为半径, 在两直线上截出两点, 也就是圆与直线交点, 代替 A 和 B). 分别以 A 和 B 为圆心, 用圆规作半径相等两个圆交于 P (半径为已知). 最后用直尺连接 O 和 P, 就得到两直线夹角的平分线.

若在坐标系下考虑, 以 O 为原点, 以OA 作为 x 轴正向, OA 长度作为单位长度, 建立坐标系.

设已知角 $\angle AOB=\theta$, 则三个已知点坐标分别为 (图 6.2)

$$O(0,0),\ A(1,0),\ B(\cos\theta,\sin\theta),$$

用尺规作出点 P 的坐标为

$$P\left(r\cos\frac{\theta}{2},\ r\sin\frac{\theta}{2}\right),$$

就相当于根据已知点 O,A,B 的坐标作出 P 点的坐标, 或者说根据给定数 $1,\cos\theta,\sin\theta$ 用尺规作出新的数 $\cos\dfrac{\theta}{2},\sin\dfrac{\theta}{2}$.

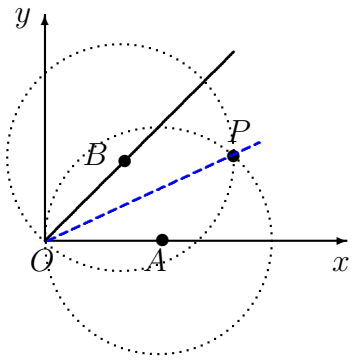


图 6.2

§6.2 作图的代数表示

于是, 尺规作图问题就转化为从已知数出发, 用尺规能够作出哪些数的问题.

1° 用尺规可实现已知数的四则运算

即任给两个数 a 和 b, 用尺规可以作出 $a\pm b,ra,ab$, 和 $\dfrac{a}{b}$. 这里 r 是任意有理数.

(a) 给定两个正实数 a 和 b 分别代表两个线段长度, 用直尺画一条数轴, 用圆规依次向数轴正向标出距离 $OA=a,\ AB=b$, 则线段 OB 的长度就是$a+b$, 若沿 OA 方向接连标出距离 a, 则可作长度为 na 的直线.

若沿相反方向标出 $AB=b$, 则 $OB=a-b$. 所以两个数 a 和 b 之间的加减法可由尺规作图来实现. 若 a,b 中有负数, 仍然以其绝对值为线段长度, 只是在数轴上丈量时, 取数轴正向的反方向即可.

(b) 设 q 为正整数, $OA=a$. 过 O 作另一条直线 OB, 使得 $OB=q$ 也就是数轴上单位长度 q 倍. 在OB 上取一点 D 使得 $OD=1$. 连接AB, 并过 D 点作 AB 平行线交 OA 与 C, 因此三角形 ΔOAB 与 ΔOCD 相似, 所以 $\dfrac{OC}{OD}=\dfrac{OA}{OB}$, 这样得 $OC=\dfrac{1}{q}a$ (图6.3) .

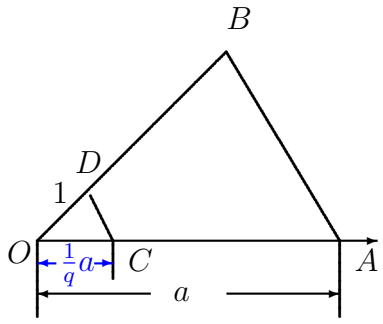


图 6.3

再将 OC 扩大 p 倍, 就得到长度为 $\dfrac{p}{q}a$ 的线段.

(c) 同样, 用尺规还可以实现两个数乘法和除法:

在任意角两边分别标出 $OA=a$, $OC=b$, 在 OA 上作 $OB=1$, 连接BC 并过 A 点作 BC 的平行线交 OC (或延长线) 于 D, 则 $OD=ab$ (图 6.4) .

若对任意角两边分别标出 $OA=a, OB=b$, 且在 OB 上标出 $OD=1$, 过 D 作平行于 AB 的直线交 OA(或延长线) 于 C, 则 $OC=\dfrac{a}{b}$ (图 6.5) .

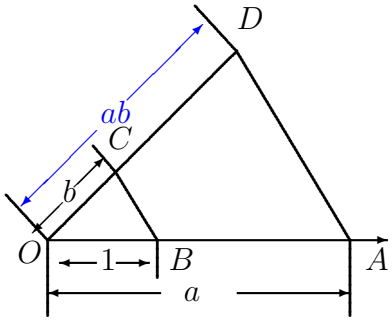


图 6.4

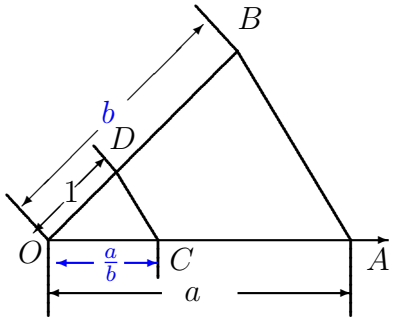


图 6.5

定义 6.1 设 $S=\{1,a,b,c,\cdots,\}$ 是包含 *1* 的数集, S中数经过任意有限次加减乘除得到所有可能数的集合记为 $\mathbb{F}(S)$, 不难验证 $\mathbb{F}(S)$ 满足第 *3* 讲中关于域的定义*3.3*, 因此是一个域, 称为***由 S 生成的数域***.

从已知数通过尺规, 逐步作出 $a\pm b, ra, ab, \dfrac{a}{b}$ 的过程说明如下结论:

定理 6.2 已知一个包含 *1* 的数集 $S=\{1,a,b,c,\cdots\}$, 那么用尺规可作出由 S 生成的数域 $\mathbb{F}(S)$ 中的任何数.

推论 6.3 从$S=\{1\}$ 出发, 用尺规可以作出有理数域 $\mathbb{Q}$ 中所有的有理数.

今后, 凡是说 “从数集S 或数域 $\mathbb{F}$ 出发”, 是指已经假设 S 或 $\mathbb{F}$ 中数是已知的, 或者已经通过尺规作出的数.

显然, 如果从任何有理数构成的集合出发, 用尺规按上述方式 (a), (b), (c), 得到的还是有理数, 自然要问, 能否用尺规作出有理数以外的数? 答案是肯定的, 而且是有决定意义的.

2° 用尺规作出已知数的平方根

设 $d>0$ (不妨设 $d>1$)是已知数, 在直线上标出 $OA=d, AB=1$ 以及$OB'=d-1$ 使得 A 是 $B'B$ 的平分点.

作直线段 OB 的平分点, 并以此为圆心, OB 为直径作圆; 再作 $B'B$ 垂直平分线, 该垂直平分线过 A 并交圆于 C (图 6.6) . 不难看出直角三角形 ΔOAC 和 ΔBAC 相似, 因此由

$$\frac{AC}{AB}=\frac{OA}{AC},$$

得

$$AC=\sqrt{d}.$$

因此, 用尺规可作出已知正数 d 的平方根 $\sqrt{d}$.

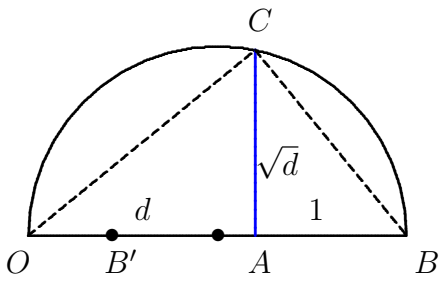


图 6.6

现在, 从 $\mathbb{F}$ 出发, 取 $d\in\mathbb{F}$ $(d>0)$, 作出 $\sqrt{d}$. 再从 $\mathbb{F}$ 和 $\sqrt{d}$ 出发, 进而可以用尺规作出所有下列形式的数

$$\alpha+\beta\sqrt{d},\ \alpha,\beta\in\mathbb{F}.$$

例如取 $d=2$, 就得到比有理数域 $\mathbb{Q}$ 范围更广的数 $\alpha+\beta\sqrt{2}$.

下面这个例子, 说明如何通过作出形如 $\alpha+\beta\sqrt{d}$ 的数,解决尺规作图问题.

例 6.2.1 单位圆内接正十边形的尺规作图问题是可解的.

这里, 只讨论上述尺规作图问题是否可解, 并不讨论内接正十边形具体作图过程.

假设圆心为 O 的单位圆内有一内接正十边形, 记某条边为 AB 长度为 x. $\triangle AOB$ 是等腰三角形, 圆心角 $\angle AOB=36°$, 其它两角 $\angle OAB=\angle OBA=72°$. 作角 $\angle OAB$ 的角平分线, 交 OB 于 C, 因此 AC 将 $\triangle AOB$ 分为两个等腰三角形 $\triangle ABC$ 和 $\triangle ACO$ (图 6.7) . 推得

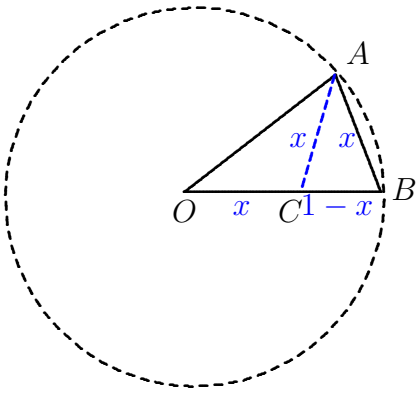


图 6.7

$$AB = AC = OC = x, BC = 1 - x.$$

又因为 $\triangle AOB$ 与 $\triangle ABC$ 相似, 这样就有

$$\frac{1}{x} = \frac{x}{1-x},$$

即 x 满足二次方程

$$x^2 + x - 1 = 0$$

因 $x > 0$, 所以

$$x = \frac{\sqrt{5}-1}{2},$$

这是一个有理数域添加了平方根 $\sqrt{5}$ 的数, 因此是可以用尺规作出, 这样用圆规从单位圆上一点出发, 以 x 为半径依次作与单位圆交点, 再用直尺连接这些交点就得到用尺规作出的内接正十边形.

顺便指出, $\dfrac{\sqrt{5}-1}{2} \simeq 0.618$ 正是所谓的 "黄金分割" , 人们认为如果矩形宽和长取成这样的比值, 从审美观点看是最好的. 早在公元前 6 世纪Pythagoras 学派就研究过正五边形和正十边形的作图问题, 由此推断他们应该触及并掌握了黄金分割.

利用简单的三角函数余弦定理, 还可以得到

$$\cos 36^\circ = \frac{\sqrt{5}+1}{4}, \ \cos 72^\circ = \frac{\sqrt{5}-1}{4}.$$

因此这些数也是通过尺规可以作出的.

归纳 1° 和 2°, 得出如下结论: **用尺规可以实现已知数的加减乘除以及开平方等代数运算.**

3° **尺规作图的代数性质**

现在要问, 假如仅从 $\mathbb{F}$ 出发, 除了 $\alpha + \beta\sqrt{d}$ 形式的数以外, 用尺规还能不能作出其它什么数? 答案是否定的.

定理 6.4 *若仅从一个已知数域 $\mathbb{F}$ 出发, 用尺规只能作出形如 $\alpha + \beta\sqrt{d}$ 的数, 其中$\alpha, \beta \in \mathbb{F}$.*

证明 为了证明上述结论, 从代数角度, 对尺规作图的基本功能分析如下:

(1)两已知点之间线段长度

设 (a_1, b_1), (a_2, b_2) 为两个已知点, $a_1, b_1, a_2, b_2 \in \mathbb{F}$, 那么连接 (a_1, b_1), (a_2, b_2) 两点线段长度为

$$\rho = \sqrt{(a_1 - a_2)^2 + (b_1 - b_2)^2},$$

它是 $\mathbb{F}$ 中数经过开平方所得到的数, 因此用尺规作出两已知点之间的线段长度仍然是形如 $\alpha+\beta\sqrt{d},\ \alpha,\beta\in\mathbb{F}$ 的数.

同时根据解析几何, 过已知两点的直线方程为

$$(b_1-b_2)x+(a_1-a_2)y+(a_1b_2-a_2b_1)=0,$$

由于 $\mathbb{F}$ 是数域, 所以上述方程的系数仍然属于$\mathbb{F}$.

(2)两条已知直线的交点.

设两条不平行直线的方程为

$$\begin{aligned}ax+by+c&=0,\\ a'x+b'y+c'&=0,\end{aligned}$$

其中系数 $a,b,c,a',b',c'\in\mathbb{F}$, 那么它们的交点坐标为

$$x_0=\frac{cb'-bc'}{ab'-ba'},\ y_0=\frac{ac'-a'c}{ab'-ba'}.$$

所以交点坐标是 $\mathbb{F}$ 中数经过加减乘除所得到的, 因此仍然是 $\mathbb{F}$ 中数, 也就是用直尺作出两条相交直线的交点坐标, 仍然是$\mathbb{F}$ 中数.

(3)已知圆和已知直线的交点.

设以 (ξ,η) 为圆心, 以 r 为半径, $\xi,\eta,r\in\mathbb{F}$, 那么圆的方程为

$$(x-\xi)^2+(y-\eta)^2=r^2$$

或表示成下列 2 次代数方程

$$x^2+y^2-2\xi x-2\eta y+\gamma=0.$$

其中 $\gamma=\xi^2+\eta^2-r^2\in\mathbb{F}$, 因此上述二次方程的系数仍然是 $\mathbb{F}$ 中的数.

圆与直线的交点坐标, 就是系数在 $\mathbb{F}$ 中圆和直线方程联立方程的解

$$\begin{aligned}x^2+y^2-2\xi x+2\eta y+\gamma&=0,\\ ax+by+c&=0,\end{aligned}$$

从联立方程中消去变量 y, 得到关于 x 的二次代数方程

$$Ax^2+Bx+C=0,$$

其中系数

$$A=a^2+b^2,\ B=2(ac-b^2\xi+ab\eta),\ C=c^2+2bc\eta+b^2\gamma,$$

因此$A, B, C \in \mathbb{F}$. 这样圆与直线相交就意味着上述二次代数方程有实数解

$$x = \frac{-B \pm \sqrt{\Delta}}{2A},$$

其中 $\Delta = B^2 - 4AC \in \mathbb{F}$. 因此 x 仍然是形如 $\alpha + \beta\sqrt{\Delta},\ p, q \in \mathbb{F}$ 的数.

对于y 也有类似结果 $y = p' + q'\sqrt{\Delta},\ p', q' \in \mathbb{F}$. 这样我们得到的结论是用尺规作出的圆与直线的交点坐标都是形如 $\alpha + \beta\sqrt{d},\ \alpha, \beta \in \mathbb{F}$ 的数.

(4)两个已知圆的交点.

设系数都是 $\mathbb{F}$ 中数的两个圆的代数方程为

$$x^2 + y^2 - 2\xi x - 2\eta y + \gamma = 0,$$

$$x^2 + y^2 - 2\xi' x - 2\eta' y + \gamma' = 0.$$

消去平方项得一次代数方程

$$2(\xi - \xi')x + 2(\eta - \eta')y - (\gamma - \gamma') = 0,$$

方程的系数都是$\mathbb{F}$ 中的数. 如同(3)一样, 通过上述方程与第一个圆的方程联立得到一个二次代数方程, 通过求解该方程, 得到用尺规作出的两个圆的交点, 其坐标也是形如 $\alpha + \beta\sqrt{d},\ \alpha, \beta \in \mathbb{F}$ 的数.

再以已知角平分线的作图问题为例. 不妨设所讨论的夹角为锐角$0 < \theta < \frac{\pi}{2}$, 因此以已知点 $A(1, 0)$ 和 $B(\cos\theta, \sin\theta)$ 为圆心(例6.1.2), 以1 为半径的两个圆有交点, 设交点坐标为 $P(x, y)$, 那么 x, y 满足方程

$$(x-1)^2 + y^2 = 1,$$
$$(x - \cos\theta)^2 + (y - \sin\theta)^2 = 1$$

或

$$x^2 - 2x + y^2 = 0,$$
$$x^2 - 2x\cos\theta + y^2 - 2y\sin\theta = 0,$$

消去平方项得

$$x(1 - \cos\theta) - y\sin\theta = 0,$$

与第一个圆的方程联立, 可解的交点坐标为

$$x = 1 + \cos\theta,\ y = \sin\theta = \sqrt{1 - \cos^2\theta}.$$

它们都是从已知数 $1, \cos\theta$ 出发, 通过加减乘除和开方运算得到的数.

总之, 从已知数 $\mathbb{F}$ 出发用尺规作出线段长度, 交点坐标只是形如 $\alpha+\beta\sqrt{d},\ \alpha,\beta\in\mathbb{F}$ 的数, 不会产生其它形式的数. □

注记 在尺规作图中, 有时会有“以任意一点为圆心”、“以任意长度为半径”、“作任意一条直线”等作图要求. 作图中出现这样或那样“任意”, 说明作图效果与这些任意值无关. 因此可以选择那些点或任意长度为有理点或有理数, 那些直线为一条由有理系数代数方程表示的直线.

§6.3 数域的扩张

由上节可知, 在坐标系中, 从已知条件出发, 用尺规作一个交点问题转化为从已知数作出新的数的问题, 并可实现数的四则运算. 这样, 当给定一些数 (这些数的集合记为 $S=\{1,a,b,c,\cdots,\}$), 能用尺规作出一个范围更广的数集 $\mathbb{F}$. 该数集对加法、乘法以及它们的逆运算封闭, 而且包含 0元和单位元 1. 根据定义3.3, $\mathbb{F}$ 是数域.

接下来关键的一步是用尺规可作出 $\mathbb{F}$ 中正数 d 的平方根 $\sqrt{d}$. 将 $\sqrt{d}$ 添加到 $\mathbb{F}$ 中去, 使得尺规可作出所有形如 $\alpha+\beta\sqrt{d}\ (\alpha,\beta\in\mathbb{F})$ 的数.

1° 扩域

如果 $\sqrt{d}\in\mathbb{F}$, 那么 $\alpha+\beta\sqrt{d}\in\mathbb{F}$, 因此用尺规作出的这些数仍然在 $\mathbb{F}$ 的范围内.

但是, 对 $d\in\mathbb{F},\ \sqrt{d}\notin\mathbb{F}$, 下列定理说明, 用尺规作出的形如 $\alpha+\beta\sqrt{d}$ 的数集不但扩大了 $\mathbb{F}$ 的范围, 而且仍然构成一个数域.

定理 6.5 从任意已知数域 $\mathbb{F}$ 出发,记用尺规作出的数集

$$\mathbb{F}(\sqrt{d})=\left\{\alpha+\beta\sqrt{d}\ \middle|\ d,\alpha,\beta\in\mathbb{F},\ \sqrt{d}\notin\mathbb{F}\right\}.$$

则 $\mathbb{F}(\sqrt{d})$ 满足:

(i) $\alpha+\beta\sqrt{d}=0$ 当且仅当 $\alpha=0,\beta=0$.

(ii) 当 $\beta\neq0$ 时, $\alpha+\beta\sqrt{d}\notin\mathbb{F}$.

(iii) $\mathbb{F}(\sqrt{d})$ 是一个包含 $\mathbb{F}$ 的数域.

证明 (i) : 设 $\alpha+\beta\sqrt{d}=0$, 若 $\beta=0$, 推出 $\alpha=0$, 若 $\beta\neq0$, 推出

$$\sqrt{d}=-\frac{\alpha}{\beta}\in\mathbb{F},$$

这与 $\sqrt{d}\notin\mathbb{F}$ 矛盾, 所以$\beta=0$. 反之显然.

(ii): 仍然采取反证法, 若 $\gamma=\alpha+\beta\sqrt{d}\in\mathbb{F},\ \beta\neq 0$, 解得

$$\sqrt{d}=\frac{\gamma-\alpha}{\beta}\in\mathbb{F},$$

仍然与$\sqrt{d}\notin\mathbb{F}$ 矛盾.

(iii): 仅需如下简单验证. 任取 $\mathbb{F}(\sqrt{d})$ 中两个数 $\alpha+\beta\sqrt{d},\ \alpha'+\beta'\sqrt{d}$, 那么

$$\begin{aligned}(\alpha+\beta\sqrt{d})\pm(\alpha'+\beta'\sqrt{d})&=(\alpha\pm\alpha')+(\beta\pm\beta'\sqrt{d})\in\mathbb{F}(\sqrt{d}),\\(\alpha+\beta\sqrt{d})\cdot(\alpha'+\beta'\sqrt{d})&=\alpha\alpha'+d\beta\beta'+(\alpha\beta'+\beta\alpha')\sqrt{d}\in\mathbb{F}(\sqrt{d}),\\\frac{\alpha+\beta\sqrt{d}}{\alpha'+\beta'\sqrt{d}}&=\frac{\alpha\alpha'-d\beta\beta'}{\alpha'^2-d\beta'^2}+\frac{\alpha\beta'-\beta\alpha'}{\alpha'^2-d\beta'^2}\sqrt{d}\in\mathbb{F}(\sqrt{d}).\end{aligned}$$

这里, 由于$\sqrt{d}\notin\mathbb{F}$, 所以第三式中的分母 $\alpha'^2-d\beta'^2\neq 0$, 否则就有$\sqrt{d}=\pm\dfrac{\alpha'}{\beta'}\in\mathbb{F}$, 这与 $\sqrt{d}\notin\mathbb{F}$ 相矛盾, 因此第三式中除法有意义. □

定义 6.6 设 $\mathbb{F}$ 是一个数域, $d\in\mathbb{F},\ \sqrt{d}\notin\mathbb{F}$. 称数域 $\mathbb{F}(\sqrt{d})$ 为数域 $\mathbb{F}$ 的一个扩域, $\mathbb{F}$ 为 $\mathbb{F}(\sqrt{d})$ 的子域 .

例 6.3.1 设 $\mathbb{F}=\mathbb{Q}$, 取 $2\in\mathbb{Q}$, 则 $\sqrt{2}\notin\mathbb{Q}$, 所以$\mathbb{Q}$ 的扩域为

$$\mathbb{Q}(\sqrt{2})=\left\{\alpha+\beta\sqrt{2}\ \middle|\ \alpha,\beta\in\mathbb{Q}\right\}.$$

显然 $\mathbb{Q}(\sqrt{2})$ 包含了有理数域 $\mathbb{Q}$, 但比实数域 $\mathbb{R}$ 范围要小(例如实数 $\sqrt{3}\notin\mathbb{Q}(\sqrt{2})$).

如果仍然把 $\mathbb{F}$ 的数当作已知数, 定理6.4 证明了用尺规能够作出的数也只能是形如 $\alpha+\beta\sqrt{d}$ 的数.

现在, 从一个已知数集 $S=\{1,a,b,c,\cdots,\}$ 出发, 用尺规作出数域 $\mathbb{F}_0=\mathbb{F}(S)$.

再从 $\mathbb{F}_0$ 出发, 取正数 $d_1\in\mathbb{F}_0$, 用尺规作出它的平方根, 并保证 $\sqrt{d_1}\notin\mathbb{F}_0$, 这样就得到 $\mathbb{F}_0$ 的一个扩域:

$$\mathbb{F}_1=\left\{\alpha+\beta\sqrt{d_1}\ \middle|\ d_1,\alpha,\beta\in\mathbb{F}_0,\ \sqrt{d_1}\notin\mathbb{F}_0\right\},$$

然后从 $\mathbb{F}_1$ 出发(即把 $\mathbb{F}_1$ 作为已知数域), 重复上述过程: 取 $d_2\in\mathbb{F}_1$, 但 $\sqrt{d_2}\notin\mathbb{F}_1$, 就得到 $\mathbb{F}_1$ 的一个扩域:

$$\mathbb{F}_2=\left\{\alpha+\beta\sqrt{d_2}\ \middle|\ d_2,\alpha,\beta\in\mathbb{F}_1,\ \sqrt{d_2}\notin\mathbb{F}_1\right\},$$

如此下去, 从 $\mathbb{F}_{i-1}$ 出发, 就得到 $\mathbb{F}_{i-1}$ 的一个扩域

$$\mathbb{F}_i=\left\{\alpha+\beta\sqrt{d_i}\ \middle|\ d_i,\alpha,\beta\in\mathbb{F}_{i-1},\ \sqrt{d_i}\notin\mathbb{F}_{i-1}\right\},$$

$i=1,\cdots n,\cdots$. 这一系列扩域满足下列包含关系

$$\mathbb{F}_0\subset\mathbb{F}_1\subset\cdots\subset\mathbb{F}_n\subset\cdots.$$

并统称为数域 $\mathbb{F}_0$ 的扩域.

定理 6.7 扩域 $\mathbb{F}_i,\ i=1,2,\cdots$ 中每个数都是可以用尺规通过逐步添加数的平方根一步一步作出的数.

例 6.3.2 下列集合

$$\mathbb{Q}(\sqrt{2})(\sqrt[4]{2})=\left\{\alpha+\alpha'\sqrt[4]{2}+\beta\sqrt[4]{2}^2+\beta'\sqrt[4]{2}^3 \;\middle|\; \alpha,\alpha',\beta,\beta'\in\mathbb{Q}\right\}$$

是一个扩域.

因为 $\mathbb{Q}(\sqrt{2})=\left\{\alpha+\beta\sqrt{2} \;\middle|\; \alpha,\beta\in\mathbb{Q}\right\}$ 是 $\mathbb{Q}$ 的一个扩域,

取 $\sqrt{2}\in\mathbb{Q}(\sqrt{2})$. 若 $\sqrt{\sqrt{2}}=\sqrt[4]{2}\in\mathbb{Q}(\sqrt{2})$, 则存在$\alpha,\beta\in\mathbb{Q}$ 使得

$$\sqrt[4]{2}=\alpha+\beta\sqrt{2},$$

两边平方得

$$\sqrt{2}=\alpha^2+2\beta^2+2\alpha\beta\sqrt{2},$$

根据定理6.5 中的(i), 推出 $\alpha^2+2\beta^2=0,\ 2\alpha\beta=1$, 这是不可能的. 因此 $\sqrt[4]{2}\notin\mathbb{F}_1$, 推得

$$\mathbb{Q}(\sqrt{2})(\sqrt[4]{2})=\left\{p+q\sqrt[4]{2} \;\middle|\; p,q\in\mathbb{Q}(\sqrt{2})\right\}$$

是$\mathbb{Q}(\sqrt{2})$ 的一个扩域. 令

$$p=\alpha+\beta\sqrt{2},\ q=\alpha'+\beta'\sqrt{2},\ \alpha,\beta,\alpha',\beta'\in\mathbb{Q},$$

则 $\mathbb{Q}(\sqrt{2})(\sqrt[4]{2})$ 中的数可表示为:

$$\mathbb{Q}(\sqrt{2})(\sqrt[4]{2})=\left\{\alpha+\alpha'\sqrt[4]{2}+\beta\sqrt[4]{2}^2+\beta'\sqrt[4]{2}^3 \;\middle|\; \alpha,\beta,\alpha',\beta'\in\mathbb{Q}\right\}.$$

例 6.3.3 取 $3=3+0\sqrt{2}\in\mathbb{Q}(\sqrt{2})$, 不难验证 $\sqrt{3}\notin\mathbb{Q}(\sqrt{2})$, 否则存在有理数 α,β 使得 $\alpha+\beta\sqrt{2}=\sqrt{3}$, 两边平方得

$$\alpha^2+2\beta^2+2\alpha\beta\sqrt{2}=3,$$

根据定理6.5 中的(i), 推出 $\alpha^2+2\beta^2=3,\ 2\alpha\beta=0$, 推出

$$\beta=0,\ \ \alpha=\pm\sqrt{3};\ \ 或\ \ \alpha=0,\ \ \beta=\pm\sqrt{\frac{3}{2}},$$

无论 $\alpha=\pm\sqrt{3}$ 还是 $\beta=\pm\sqrt{\dfrac{3}{2}}$ 都不是有理数(见第 3 讲习题 3), 推出矛盾. 因此 $\sqrt{3}\notin\mathbb{Q}(\sqrt{2})$, 且

$$\mathbb{Q}(\sqrt{2})(\sqrt{3})=\left\{p+q\sqrt{3} \;\middle|\; p,q\in\mathbb{Q}(\sqrt{2})\right\}$$

是 $\mathbb{Q}(\sqrt{2})$ 的一个扩域. 令

$$p=\alpha+\beta\sqrt{2},\ q=\alpha'+\beta'\sqrt{2}\ \ (\alpha,\beta,\alpha',\beta'\in\mathbb{Q})$$

就得到 $\mathbb{Q}(\sqrt{2})(\sqrt{3})$ 中的数的如下表示:

$$\mathbb{Q}(\sqrt{2})(\sqrt{3})=\left\{\alpha+\beta\sqrt{2}+\alpha'\sqrt{3}+\beta'\sqrt{6}\ \middle|\ \alpha,\beta,\alpha',\beta'\in\mathbb{Q}\right\}.$$

例如 $\alpha\sqrt{2}+\beta\sqrt{3}$ 也是 $\mathbb{Q}(\sqrt{2})(\sqrt{3})$ 中的数, 其中 $\alpha,\beta\in\mathbb{Q}$.

2° 从代数角度看扩域

在扩域中, 添加一个数的平方根 $\sqrt{d}$ 使数域 $\mathbb{F}$ 扩大到$\mathbb{F}(\sqrt{d})$ 的关键条件是:

$$d\in\mathbb{F},\ \sqrt{d}\notin\mathbb{F}.$$

从代数上看, 该条件表示代数方程 $x^2-d=0$ 在数域 $\mathbb{F}$ 中没有根, 或者说 x^2-d 是 $\mathbb{F}$ 上不可约多项式 (见第 2 讲§2.8 中定义2.37和推论2.42) .

推而广之, 给定数域 $\mathbb{F}$ 上任意 n $(n\geqslant 2)$ 次不可约多项式

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0\ \ (a_n,a_{n-1},\cdots,a_0\in\mathbb{F}).$$

设 a 是方程 $f(x)=0$ 的一个根, 则 $a\notin\mathbb{F}$ (否则在 $\mathbb{F}$ 上有 $f(x)=(x-a)g(x)$, 这与 $f(x)$ 不可约矛盾) . 作集合

$$\mathbb{F}(a)=\left\{b_{n-1}a^{n-1}+b_{n-2}a^{n-2}+\cdots+b_0\ \middle|\ b_{n-1},b_{n-2},\cdots,b_0\in\mathbb{F}\right\},$$

利用

$$a_na^n+a_{n-1}a^{n-1}+\cdots+a_0=0,$$

可以验证 $\mathbb{F}(a)$ 是一个包含 $\mathbb{F}$ 的数域, 称为 $\mathbb{F}$ 的扩域. 这种通过对数域 $\mathbb{F}$ 添加 $\mathbb{F}$ 上不可约多项式的根得到扩域的过程也称为**代数扩张**.

例 6.3.4 x^2-2 是 $\mathbb{Q}$ 上不可约多项式, 它的一个根 $a=\sqrt{2}\notin\mathbb{Q}$, 因此扩域为

$$\mathbb{Q}(\sqrt{2})=\left\{\alpha+\beta\sqrt{2}\ \middle|\ \alpha,\beta\in\mathbb{Q}\right\}.$$

在域 $\mathbb{Q}(\sqrt{2})$ 上, x^2-2 不再是不可约多项式, 并可分解为一次因式的乘积:

$$x^2-d=(x-\sqrt{d})(x+\sqrt{d}).$$

例 6.3.5 对 $\mathbb{R}$ 上不可约多项式 x^2+1, 取它的一个根 $a=\mathrm{i}\notin\mathbb{R}$, 因此扩域就是复数域

$$\mathbb{C}=\left\{\alpha+\mathrm{i}\beta\ \middle|\ \alpha,\beta\in\mathbb{R}\right\},$$

从而使得 x^2+1 在$\mathbb{C}$上可以分解为

$$x^2+1=(x-\mathrm{i})(x+\mathrm{i}).$$

例 6.3.6 x^4-2 是 $\mathbb{Q}$ 上不可约多项式, 取 $a=\sqrt[4]{2}$, 则扩域为

$$\left\{\alpha+\alpha'\sqrt[4]{2}+\beta\sqrt[4]{2}^2+\beta'\sqrt[4]{2}^3 \;\middle|\; \alpha,\beta,\alpha',\beta'\in\mathbb{Q}\right\}.$$

它也是 $\mathbb{Q}$ 通过添加$\sqrt{2}$ 得到扩域 $\mathbb{Q}(\sqrt{2})$ 后 , 添加 $\sqrt{\sqrt{2}}$ 得到的扩域 $\mathbb{Q}(\sqrt{2})(\sqrt[4]{2})$ (例6.3.2). 如果再添加 i, 则得到扩域 $\mathbb{Q}(\sqrt{2})(\sqrt[4]{2})(\mathrm{i})$, 多项式$x^4-2$ 在扩域上可不断分解因式, 直至分解为一次因式的乘积:

$$\begin{aligned}
&\text{在 } \mathbb{Q}(\sqrt{2}) \text{ 上 :} && x^4-2=(x^2-\sqrt{2})(x^2+\sqrt{2});\\
&\text{在 } \mathbb{Q}(\sqrt{2})(\sqrt[4]{2}) \text{ 上 :} && x^4-2=(x-\sqrt[4]{2})(x+\sqrt[4]{2})(x^2+\sqrt{2});\\
&\text{在 } \mathbb{Q}(\sqrt{2})(\sqrt[4]{2})(\mathrm{i}) \text{ 上 :} && x^4-2=(x-\sqrt[4]{2})(x+\sqrt[4]{2})(x-\mathrm{i}\sqrt{2})(x+\mathrm{i}\sqrt{2}).
\end{aligned}$$

例 6.3.7 多项式

$$x^4-10x^2+1$$

在有理数域 $\mathbb{Q}$ 上是不可约的, 但是在扩域 $\mathbb{Q}(\sqrt{2})$ 上是可约的, 且有因式分解:

$$x^4-10x^2+1=(x^2-2\sqrt{2}x-1)(x^2+2\sqrt{2}x-1),$$

其中两个因子 $x^2\pm2\sqrt{2}x-1$ 的系数属于 $\mathbb{Q}(\sqrt{2})$, 但是在 $\mathbb{Q}(\sqrt{2})$ 上不可约 (不能继续分解). 如果将扩域 $\mathbb{Q}(\sqrt{2})$ 继续进行扩张, 得 $\mathbb{Q}(\sqrt{2})(\sqrt{3})$ (见例6.3.3), 那么在 $\mathbb{Q}(\sqrt{2})(\sqrt{3})$ 上可继续因式分解

$$\begin{aligned}
x^4-10x^2+1&=(x^2-2\sqrt{2}x-1)(x^2+2\sqrt{2}x-1)\\
&=(x-\sqrt{2}-\sqrt{3})(x-\sqrt{2}+\sqrt{3})(x+\sqrt{2}-\sqrt{3})(x+\sqrt{2}+\sqrt{3})
\end{aligned}$$

可见域 $\mathbb{F}$ 上一个不可约多项式, 通过不断地进行代数扩张, 使得该多项式在扩域可进行因式分解, 最终给出对应的代数方程的根. 例6.3.6通过扩域给出$x^4-2=0$ 在扩域 $\mathbb{Q}(\sqrt{2})(\sqrt[4]{2})(\mathrm{i})$ 上的四个根: $\pm\sqrt[4]{2},\ \pm\mathrm{i}\sqrt{2}$. 例6.3.7通过扩域, 给出 $x^4-10x^2+1=0$ 在 $\mathbb{Q}(\sqrt{2})(\sqrt{3})$ 上的四个根: $\sqrt{2}\pm\sqrt{3},\ -\sqrt{2}\pm\sqrt{3}$.

注记 本专题主要目的是通过扩域解决尺规作图是否可解问题. 事实上, 扩域在研究代数方程

$$f(x)=0,\ f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$$

的根能否通过其系数 $S=\{a_n,a_{n-1},\cdots,a_0\}$ 的加减乘除和各类开方表示的问题时, 也扮演重要角色. 大致上说, 首先通过加减乘除将 S 扩张成数域 $\mathbb{F}$, 若能通过有限次添加根式得到某个扩域, 使 $f(x)$ 在该扩域上能够分解成一次因式, 那么也就证明了 $f(x)=0$ 的根可由系数的加减乘除和各类开方表示. 具体内容这里就不再涉及了, 感兴趣的读者可以参考有关抽象代数的教材.

§6.4 尺规作图与三次代数方程的根

用尺规作出的图形仅是直线或圆, 而直线或圆的代数方程是以系数属于已知数域 $\mathbb{F}$ 中的一次或二次代数方程, 通过尺规作图得到交点坐标也不会越过数域 $\mathbb{F}$ 和其中数开平方根的范围. 例如用尺规作出已知圆与直线的交点问题, 实际上归结于用尺规作出一个二次代数方程

$$Ax^2 + Bx + C = 0$$

的根问题, 其中系数 A, B, C 都是数域已知的数域 $\mathbb{F}$. 因此交点坐标是方程的系数通过加减乘除和开平方根得到的, 也就是可以用尺规作出方程的根. 例6.2.1也是把用尺规作出单位元内接正十边形的问题, 转化为用尺规作出二次代数方程

$$x^2 + x - 1 = 0$$

根的问题.

定义 6.8 对于数域 $\mathbb{F}$ 上多项式

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \quad (a_n, \cdots, a_0 \in \mathbb{F}),$$

若方程 $f(x) = 0$ 的一个根 $x_0 \in \mathbb{F}_n$, 则称 x_0 是可以用尺规作出的. 这里 $\mathbb{F}_n$ 是 $\mathbb{F}$ 经过有限次逐步添加平方根得到的扩域.

现在转而讨论一个新的问题, 哪些代数方程的实根可以由尺规作出.

下面只讨论三次代数方程的情形. 设

$$f(x) = x^3 + ax^2 + bx + c \quad (a, b, c \in \mathbb{F})$$

是数域 $\mathbb{F}$ 上三次多项式. 从第 2 讲中的代数基本定理可知, 3 次代数方程 $f(x) = 0$ 有三个根 x_1, x_2, x_3, 且根与系数的关系为

$$a = -(x_1 + x_2 + x_3),$$

$$b = x_1x_2 + x_2x_3 + x_1x_3,$$

$$c = -x_1x_2x_3.$$

引理 6.9 设 $f(x) = x^3 + ax^2 + bx + c$ 是数域 $\mathbb{F}$ 上三次多项式, 如果 $f(x) = 0$ 有形如 $\alpha + \beta\sqrt{d}$ 的根, 这里 $\alpha, \beta \in \mathbb{F}$, $\beta \neq 0$, $d \in \mathbb{F}$ 但 $\sqrt{d} \notin \mathbb{F}$, 那么

(i) $\alpha - \beta\sqrt{d}$ 也是方程 $f(x) = 0$ 的根.

(ii) 方程 $f(x) = 0$ 一定有属于 $\mathbb{F}$ 的根.

证明 设 $x_1 = \alpha + \beta\sqrt{d}$ $(\beta \neq 0)$ 是 $f(x) = 0$ 的根, 令 $x_2 = \alpha - \beta\sqrt{d}$. 那么二次多项式

$$g(x) = (x - x_1)(x - x_2) = x^2 - 2\alpha x + \alpha^2 + d\beta^2,$$

也是数域 $\mathbb{F}$ 上的多项式, 用 $g(x)$ 除 $f(x)$ 得 (参见第 2 讲多项式的带余除法)

$$f(x)=g(x)q(x)+r(x),$$

这里商式和余式 $q(x),r(x)\in\mathbb{F}[x]$ (即它们是 $\mathbb{F}$ 上的多项式).

因为除式 $g(x)$ 是二次多项式, 所以余式 $r(x)$ 的次数不超过 1, 不妨设

$$r(x)=\lambda x+\rho\ \ (\lambda,\rho\in\mathbb{F}).$$

将 $x=x_1$ 代入 $f(x)=g(x)q(x)+r(x)$, 并注意到 $f(x_1)=g(x_1)=0$, 推出

$$r(x_1)=\lambda x_1+\rho=0.$$

如果 $\lambda\neq 0$, 那么

$$x_1=-\frac{\rho}{\lambda}\in\mathbb{F},$$

推出 $\sqrt{d}=\dfrac{1}{\beta}(x_1-\alpha)\in\mathbb{F}$, 矛盾. 所以$\lambda=0$, 进而 $\rho=0$. 这样就有

$$f(x)=g(x)q(x),$$

即 $x_2=\alpha-\beta\sqrt{d}$ 也是方程 $f(x)=0$ 的根.

再利用根与系数的关系, $f(x)=0$ 的第三个根 x_3 满足

$$a=-(x_1+x_2+x_3)=-(2\alpha+x_3),$$

即 $x_3=-a-2\alpha\in\mathbb{F}$. 这样就完成了引理的证明. □

定理 6.10 设 $f(x)=x^3+ax^2+bx+c$ 是数域 $\mathbb{F}$ 上三次多项式. 如果方程 $f(x)=0$ 在数域 $\mathbb{F}$ 内没有根, 那么方程 $f(x)=0$ 在从 $\mathbb{F}$ 出发的任何扩域 $\mathbb{F}_i,\ i=1,2,\cdots$ 中也没有根. 也就是说, 只要三次方程在 $\mathbb{F}$ 中没有根, 那么方程的任何根都不可能是用尺规可以作出的数.

证明 反证法: 假设方程 $f(x)=0$ 存在一个根 $x_n\in\mathbb{F}_n$. 设 $\mathbb{F}_0,\ \mathbb{F}_1,\ \cdots,\ \mathbb{F}_n$. 是从 $\mathbb{F}$ 出发, 经过逐一对 $d_1,d_2,\cdots,d_n$ 进行开平方得到的一串扩域 .

根据假设, 方程的根 $x_n\in\mathbb{F}_n$ 推得

$$x_n=\alpha_n+\beta_n\sqrt{d_n}\in\mathbb{F}_n,$$

这里 $\alpha_n,\beta_n\in\mathbb{F}_{n-1}$, $d_n\in\mathbb{F}_{n-1}$ 但 $\sqrt{d_n}\notin\mathbb{F}_{n-1}$.

根据引理6.9中 (ii), 方程 $f(x)=0$ 一定有属于数域 $\mathbb{F}_{n-1}$ 的根, 记为

$$x_{n-1}=\alpha_{n-1}+\beta_{n-1}\sqrt{d_{n-1}}\in\mathbb{F}_{n-1},$$

其中 $\alpha_{n-1},\beta_{n-1}\in\mathbb{F}_{n-2}$, $d_{n-1}\in\mathbb{F}_{n-2}$ 但 $\sqrt{d_{n-1}}\notin\mathbb{F}_{n-2}$.

同理再根据引理6.9中 (ii), 可得方程 $f(x)=0$ 在 $\mathbb{F}_{n-2}$ 中有根, 以此类推, 最终得到方程在 $\mathbb{F}_0=\mathbb{F}$ 中有根, 因此与定理条件相矛盾. □

§6.5 尺规作图中三个不可解问题

有了上面准备, 可以把尺规作图问题转化成一个代数问题. 例如, 根据定理6.10, 从有理数域 $\mathbb{Q}$ 出发, 一个尺规作图问题是否可解, 就转化为一个代数方程在 $\mathbb{Q}$ 内是否存在根的问题.

现在可以讨论历史上关于尺规作图的三个不可解的著名问题了.

1° 倍立方问题

所谓倍立方问题即是给定边长为 1 的立方体, 能否用尺规作出一个体积是它二倍的正立方体. 设新的立方体的边长为 $x>0$, 问题归结为

已知 1, 用尺规是否能作出数 x 使得 $x^3=2$.

从已知数 1 出发, 可以用尺规作出有理数域 $\mathbb{F}_0=\mathbb{Q}$. 由于方程

$$x^3-2=0$$

唯一的实根 $x=\sqrt[3]{2}$ 不是有理数, 所以方程在 $\mathbb{Q}$ 中没有根, 根据定理6.10, 推出 $x^3-2=0$ 在从 $\mathbb{Q}$ 出发的任何扩域 $\mathbb{F}_i,\ i=1,2,\cdots$ 中没有根, 即方程 $x^3-2=0$ 的实根不可能用尺规作出, 所以尺规作图的倍立方问题不可解!

为了更好地解释定理6.10, 这里不妨以倍立方问题作为具体例子, 重复定理6.10 证明过程.

假设这个实根 x 可以用尺规作出, 那么它一定需要经过有限次开平方运算才能得到. 设 x 可经过 n 次开平方运算得到, 并记第 n 次开平方的数为 d, 因此

$$x=\alpha+\beta\sqrt{d}\in\mathbb{F}_n,\ \alpha,\beta,d\in\mathbb{F}_{n-1},\ \text{但}\ \sqrt{d}\notin\mathbb{F}_{n-1}.$$

根据引理6.9中 (i),

$$x'=\alpha-\beta\sqrt{d}$$

也是方程 $x^3-2=0$ 的实根.

但是方程只有一个实根 $\sqrt[3]{2}$, 所以 $x=x'=\sqrt[3]{2}$ 推出 $\beta=0$, 且

$$x=x'=\sqrt[3]{2}=\alpha\in\mathbb{F}_{n-1}.$$

也就是这个实根 x 是 $\mathbb{F}_{n-1}$ 中的数, 记为

$$x=\alpha'+\beta'\sqrt{d'},\ \alpha',\beta'\ d'\in\mathbb{F}_{n-2},\ \text{但}\ \sqrt{d'}\notin\mathbb{F}_{n-2}.$$

重复上述推导, 并一步一步继续下去, 最后得到一个荒谬的结论: $x=\sqrt[3]{2}\in\mathbb{F}_0=\mathbb{Q}$. 因此假设是错误的, 从而证明了方程 $x^3-2=0$ 的根不可能用尺规作出, 也就是倍立方问题不可解!

2° 三等分任意角问题

现在证明用尺规三等分任意角一般来说是不可能的. 当然, 对一些特殊情况, 如像 $90°$, $180°$ 等是可以用尺规三等分的.

设给定一个角 θ 的余弦 $\cos\theta$, 要从已知数集 $S=\{1,\cos\theta\}$ 出发, 用尺规作出数 $\cos\left(\dfrac{\theta}{3}\right)$. 利用三角函数的有关公式, 有

$$\cos\theta=4\cos^3\left(\frac{\theta}{3}\right)-3\cos\left(\frac{\theta}{3}\right)$$

因此从已知数 $\cos\theta$ 出发, 用尺规作出 $x=\cos\left(\dfrac{\theta}{3}\right)$ 相当于用尺规作出三次代数方程

$$4x^3-3x-\cos\theta=0$$

的根. 这里, 我们取一种特殊情况来说明三等分角问题不可解.

设 $\theta=60°$, 则 $\cos\theta=\dfrac{1}{2}$. 因此从数集 $S=\left\{1,\dfrac{1}{2}\right\}$ 出发, 用尺规可作出有理数域 $\mathbb{Q}$. 而方程简化为

$$8x^3-6x-1=0.$$

或经过简单变换 $v=2x$, 方程变换为

$$v^3-3v-1=0$$

根据定理6.10, 只需说明上述方程在 $\mathbb{Q}$ 中没有根, 就推出相应的三等分角问题不可解.

假设该方程有有理根 $v=\dfrac{p}{q}$, 其中 $(p,q)=1$. 代入方程有

$$p^3-3q^2p-q^3=0$$

由此推出

$$q^3=p(p^2-3q^2),\ \ \text{以及}\ \ p^3=q^2(3p+q)$$

从$q^3=p(p^2-3q^2)$ 看出, q^3 能被 p 整除 , 因此 p,q 有公因子, 除非 $p=\pm1$.

从 $p^3=q^2(3p+q)$ 看出 p^3 能被 q 整除, 因此 p,q 有公因子, 除非 $q=\pm1$.

所以方程的有理根只可能是 $v=\pm 1$, 这显然是不成立的. 所以方程没有有理根, 当然对$\theta=60^\circ$ 的角, 也就不可能有用尺规进行三等分.

3° 正七边形的作图问题

考虑单位圆的内接正七边形问题, 类似正十边形情形 (例6.2.1), 设每边对应的圆心角为 $\theta=\dfrac{360^\circ}{7}$, 那么问题归结为

已知 1, 用尺规是否可以作出 $\cos\theta$ (如果作出 $\cos\theta$, 自然也就能作出 $\sin\theta=\sqrt{1-\cos^2\theta}$) .

借助第 4 讲中的复数, 正七边形的顶点正是方程

$$z^7-1=0,$$

的单位根. 由于方程有一个显然的根 $z=1$, 而其余的根都满足

$$\frac{z^7-1}{z-1}=z^6+z^5+z^4+z^3+z^2+z+1=0.$$

在上述方程中除以 z^3 得

$$z^3+\frac{1}{z^3}+z^2+\frac{1}{z^2}+z+\frac{1}{z}+1=0,$$

或写成

$$\left(z+\frac{1}{z}\right)^3+\left(z+\frac{1}{z}\right)^2-2\left(z+\frac{1}{z}\right)-1=0$$

设

$$z=\cos\theta+\mathrm{i}\sin\theta,\ \theta=\frac{360^\circ}{7}$$

推出

$$x=z+\frac{1}{z}=2\cos\theta,$$

则 x 是整系数三次代数方程

$$x^3+x^2-2x-1=0.$$

的实根.

现在从 1 出发, 得到有理数域 $\mathbb{Q}$. 能否用尺规作出正七边形, 就是能否用尺规作出数 x, 也就是上述方程是否存在有理根.

下面用反证法证明上述方程不存在有理根, 也就推出正七边形作图问题不可解.

假设方程有有理根 $x=\dfrac{p}{q},\ (p,q)=1$, 那么

$$p^3+p^2q-2pq^2-q^3=0,$$

上式分别导出

$$p^3 = q(q^2 + 2pq - p^2),$$
$$q^3 = p(p^2 + pq - 2q^2),$$

因此 p 和 q 有公因子, 这与 $(p, q) = 1$ 矛盾.

注记 尺规作图另一个著名例子是“化圆成方”问题, 即能否用尺规作出与一个单位圆面积相等正方形. 也就是问能否用尺规作出一个满足方程

$$x^2 = \pi$$

的数. 这个问题已经被证明是不可解的. 但证明过程需要用到 π 是超越数这个事实. 所谓超越数是那些不可能成为任何一个整系数(或有理系数)代数方程根的数(可对比习题 3 中所给出的“代数数”的定义), 具体内容不再展开.

§6.6 等分圆周的尺规作图问题*

除了上节讨论的三个著名问题外, 还有一个饶有兴趣的历史悠久问题, 就是用尺规作圆周的任意 n 等分问题. 依序连接等分点, 因此等分圆周问题等价于圆周内接正n 边形的尺规作图问题.

我们已经看到, 内接正十边形问题可解, 但是内接正七边形不可解. 即十等分圆周可解, 但七等分圆周不可解. 自然要问, 对于什么样的 n, 等分圆周问题可解.

等分圆周, 就是要 n 等分圆周角 $360°$. 与三等分角问题相比较, 前者只是等分固定圆周角, 但等分的份数 n 可以不同; 而后者虽是三等分, 但是角度却是任意的. 可类比的是, n 等分圆周问题, 就是从已知 $\cos 360° = 1$ 出发, 用尺规作出 $\cos\dfrac{360°}{n}$ 的问题. 或者说, 当 n 满足什么条件时, 用尺规可以作出 $\cos\dfrac{360°}{n}$.

1° 几种特殊情形

例 6.6.1 当 $n = 2^k$ 时, n 等分圆周尺规作图问题可解.

证明 显然 2 等分圆周非常简单, 只要过圆心, 用直尺作直线就可以了. 紧接着按例6.1.1 作该直线垂直平分线, 则可将圆周 4 等分. 根据例6.1.2, 用尺规可平分对应的等分角, 因此可 8 等分圆周. 这样一直做下去, 就可将圆周 2^k 等分.

例 6.6.2 若 m 等分圆周问题可解, 则 $m2^k$ 等分圆周问题也可解. 若 m 等分圆周问题不可解, 则对 m 的任何倍数 mk, 对应的等分问题也不可解.

证明 从前一个例子可以看出, 若尺规能够 m 等分圆周, 再对等分角不断进行二等分, 那么就会得到圆周的 $m2^k$ 等分.

设对于 m, 等分问题不可解, 如果存在 k, 使得 mk 等分问题可解, 那么将相邻的 k 等分合并, 就得到 m 等分的圆周, 这与条件是矛盾的, 因此第二个结论也成立.

例 6.6.3 对$m = 3, 5$, 尺规是可以等分圆周的, 因此也可 $3 \cdot 2^k$ 和 $5 \cdot 2^k$ 等分圆周, 例如可 6 等分圆周等. 但对 7 和 9, 尺规无法等分, 因此对 7 和 9 的倍数 $n = 7m$, 或 $n = 9m$ 的等分问题也是不可解的 .

证明 三等分圆周对应的圆周角为 $\cos\dfrac{360^\circ}{3} = \cos 120^\circ = -\dfrac{1}{2}$, 因此 3 等分圆周的尺规作图问题是可解的.

注意, 这里三等分的是一个特殊值的圆心角 $\theta = 360^\circ$, 因此与三等分任意角问题不可解的结论并不矛盾.

对于 5 等分问题, 只要在例6.2.1 十个等分点中, 间隔选择五个等分点即可, 因此 5 等分问题可解.

7 等分问题如同内接正 7 边形的尺规作图问题, 因此不可解.

对于 9 等分问题, 可仿照 7 等分问题证明, 从已知数 1 出发, 用尺规作出有理数域 $\mathbb{Q}$, 接下来的问题就是对 9 等分角 $\theta = \frac{360^\circ}{9}$, $\cos\theta$ 可否能用尺规作出的问题. 设

$$z = \cos\theta + \mathrm{i}\sin\theta, \quad \theta = \frac{360^\circ}{9}.$$

那么 z 满足

$$z^9 - 1 = (z^3 - 1)(z^6 + z^3 + 1) = 0,$$

因 $z^3 - 1 \neq 0$, 所以

$$z^6 + z^3 + 1 = 0,$$

同除 z^3 得

$$z^3 + 1 + z^{-3} = 0.$$

令 $x = z + z^{-1} = 2\cos\theta$, 则 $z^3 + z^{-3} = x^3 - 3x$, 因此

$$x^3 - 3x + 1 = 0.$$

如果该方程有有理根 $x = \frac{p}{q}$, $(p, q) = 1$, 则导致

$$p^3 - pq^2 + q^3 = 0,$$

或

$$p^3 = q^2(p - q), \ q^3 = p(p^2 - q^2)$$

无论哪种情况都与 $(p,q)=1$ 矛盾, 因此没有有理解, 根据定理6.10, 尺规 9 等分圆周问题不可解.

2° 17等分圆周问题

也是圆内接正 17 边形的尺规作图问题. 这是一个著名的等分问题, 它是由Gauss在他19岁那年完成的.

例 6.6.4 17 等分圆周问题是可解的.

证明 考虑方程

$$z^{17}-1=0$$

则方程的 17 个根对应单位圆上 17 个等分点.其中, $z_0=1$ 对应的等分点的坐标为 $P_0(1,0)$, 记

$$\theta=\frac{360^\circ}{17},$$

则其他 16个等分点用复数表示分别为

$$z_k=z_1^k=\cos k\theta+\mathrm{i}\sin k\theta=\boldsymbol{e}^{\mathrm{i}k\theta},\ k=2,\cdots,16.$$

这里用到了复数的 Euler 表示(第 4 讲§4.2). 除 $z_0=1$ 外, 其它 16 个解共轭成对出现.

$$\overline{z}_k=z_{17-k},\ k=1,\cdots,16.$$

或者说, 对$\theta=\dfrac{360^\circ}{17}$, 有

$$\cos m\theta=\cos k\theta,\quad (m+k=17)$$

根据根与系数关系, 有

$$\sum_{k=0}^{16}z_k=0,$$

或

$$\sum_{k=1}^{8}(z_k+\overline{z}_k)=2\sum_{k=1}^{8}\cos k\theta=-1.$$

现在从已知的 1 出发, 用尺规作出有理数域 $\mathbb{Q}$. 如果能证明 $\cos\theta$ 是能够通过尺规作出的数, 那么

$$\sin\theta=\sqrt{1-\cos^2\theta}$$

是通过加减乘除运算和已知数开平方运算得到的数, 因此也是可以通过尺规作出的. 这样就得到对应 z 的等分点的坐标

$$P_1(\cos\theta,\ \sin\theta),$$

因此线段 P_0P_1 的长度也是可以通过尺规作出的数. 从 P_1 开始以该长度为半径, 依次作圆交单位圆的交点就是其它的等分点. 这样就完成了用尺规解决 17 等分圆周的问题.

要证明从已知有理数域 $\mathbb{Q}$ 出发, , 能够用尺规作出数 $\cos\theta$. 过程虽然繁琐, 但基本上是初等的. 具体思路如下：把 $\cos\theta, \cos 2\theta, \cdots, \cos 8\theta$ 分为如下两组

$$a_1 = 2(\cos\theta + \cos 2\theta + \cos 4\theta + \cos 8\theta),$$
$$a_2 = 2(\cos 3\theta + \cos 5\theta + \cos 6\theta + \cos 7\theta),$$

由根与系数关系直接得到

$$a_1 + a_2 = -1.$$

利用三角函数的和差化积公式, 和

$$\cos m\theta = \cos k\theta, \quad (m + k = 17).$$

可以证明

$$\begin{aligned} a_1a_2 &= 4(\cos\theta + \cos 2\theta + \cos 4\theta + \cos 8\theta)(\cos 3\theta + \cos 5\theta + \cos 6\theta + \cos 7\theta) \\ &= -4. \end{aligned}$$

综合上述结果, 实数 a_1, a_2 满足

$$a_1 + a_2 = -1, \quad a_1a_2 = -4$$

因此是数域 $\mathbb{Q}$ 上二次方程的解

$$x^2 + x - 4 = 0$$

该方程的判别式为 $\Delta = 17 > 0$, 因此两个实解可通过有理数的加减乘除和开平方根得到, 即 a_1, a_2 可以用尺规作出.

再将 $a_1 = 2(\cos\theta + \cos 2\theta + \cos 4\theta + \cos 8\theta)$ 中求和项分为以下两组

$$b_1 = 2(\cos\theta + \cos 4\theta),$$
$$b_2 = 2(\cos 2\theta + \cos 8\theta),$$

因此, 首先有

$$b_1 + b_2 = a_1,$$

同时用类似证明 $a_1a_2 = -4$ 的方法得

$$b_1b_2 = 4(\cos\theta + \cos 4\theta)(\cos 2\theta + \cos 8\theta) = -1,$$

因此 b_1, b_2 满足数域 $\mathbb{Q}(\sqrt{17})$ 上的二次方程

$$x^2 - a_1 x - 1 = 0$$

其判别式 $\Delta = a_1^2 + 1 > 0$, 因此两个实根可以通过 $\mathbb{Q}(\sqrt{17})$ 中的数经过加减乘除和开平方根得到, 所以是可以用尺规作出的数.

同理把 $a_2 = 2(\cos 3\theta + \cos 5\theta + \cos 6\theta + \cos 7\theta)$ 中求和项分为以下两组

$$c_1 = 2(\cos 3\theta + \cos 5\theta),$$

$$c_2 = 2(\cos 6\theta + \cos 7\theta),$$

得

$$c_1 + c_2 = a_2,\ c_1 c_2 = -1.$$

所以 c_1, c_2 是 $\mathbb{Q}(\sqrt{17})$ 上方程

$$x^2 - a_2 x - 1 = 0,\ \Delta = a_2^2 + 1 > 0$$

的两个解, 它们也是可以用尺规作出的数.

注意到 c_1 的定义, 通过和差化积有

$$c_1 = 2(\cos 3\theta + \cos 5\theta) = 4\cos\theta\cos 4\theta,$$

将该方程与

$$b_1 = 2(\cos\theta + \cos 4\theta)$$

联立, 不难发现数 $2\cos\theta$ 和 $2\cos 4\theta$ 是下列二次方程

$$x^2 - b_1 x + c_1 = 0$$

的解, 该方程系数都是可用尺规作出的数, 且判别式 $\Delta = b_1^2 + c_1^2 > 0$, 因此 $2\cos\theta$ 和 $2\cos 4\theta$ 是在用尺规作出的已知数的基础上, 再次通过加减乘除和开平方根运算得到, 因此也可以用尺规作出. 这样, 最终证明了用尺规可以作出 $\cos\theta,\ \theta = \dfrac{260^\circ}{17}$. □

注记 这里只关心用尺规作出 $\cos\theta$ 的问题, 如果要具体算出每一步得到的一对根, 只需要利用求根公式, 并比较一对根之间大小即可.

3° 一般性结论

引理 6.11 设正整数 m, n 互素 $(m, n) = 1$, 若 m 等分圆周和 n 等分圆周问题可解, 则 mn 等分圆周问题也可解.

证明 因为 $(m,n)=1$, 根据 Bezout 定理2.9（第 2 讲§2.4 ）, 存在两个整数 l,k, 使得

$$lm+kn=1.$$

因此

$$\frac{1}{mn}=\frac{l}{n}+\frac{k}{m}.$$

记

$$\theta=\frac{360^\circ}{mn},\ \theta_1=\frac{360^\circ}{m},\ \theta_2=\frac{360^\circ}{n}$$

这样用复数的 Euler 表示, 有

$$\boldsymbol{e}^{\theta}=\boldsymbol{e}^{k\theta_1}\boldsymbol{e}^{l\theta_2}$$

两边取实部得

$$\cos\theta=\mathrm{Re}\left((\cos\theta_1+\mathrm{i}\sin\theta_1)^k(\cos\theta_2+\mathrm{i}\sin\theta_2)^l\right).$$

根据引理条件, $\cos\theta_1$ $\cos\theta_2$ 用尺规是可以作出的数, 因此,

$$\sin\theta_1=\sqrt{1-\cos^2\theta_1},\ \sin\theta_2=\sqrt{1-\cos^2\theta_2}$$

也是可用尺规作出的数. 进而得出 $\cos\theta$ 是通过 $\cos\theta_1$ $\cos\theta_2$ 加减乘除和开平方根运算得到, 因此也是可以用尺规作出的数. □

例如 15 等分圆周问题是可解的, 这是因为 3 和 5 等分圆周问题可解, 且 $(3,5)=1$.

现在总结如下：

根据引理6.11, 如果两个素数 p_1,p_2 对应等分问题可解, 那么 p_1p_2 对应等分问题也可解. 但是, 一些素数对应的等分问题是可解的, 如 2, 3, 5, 17 等等, 一些素数对应的等分问题不可解, 如 7, 9.

从 2, 3, 5, 17 等分圆周问题可解性看出, 除 2 外, 素数 3, 5, 17 有其特殊性:

$$3=2^{2^0}+1,\ 5=2^{2^1}+1,\ 17=2^{2^2}+1$$

这些数正是 Fermat 素数（第 2 讲§2.4）. 虽然形如 $2^{2^n}+1$ 的 Fermat 数并不都是素数, 但是对 Fermat 素数, 对应的等分问题是可解的. 结合引理和例6.6.2, 有下列结论.

定理 6.12 *n 等分圆周（即圆内接正 n 边形）的尺规作图问题可解的充分必要条件是*

$$n=2^kp_1p_2\cdots p_m,$$

这里 $p_1,p_2,\cdots,p_m$ 是不同的 Fermat 素数.

详细证明不再赘述.

第 6 讲习题

1. 设 $p=1+\sqrt{2},\ q=2-\sqrt{2}$, 把 $\dfrac{p}{q},\ p+p^2$ 表示成 $a+b\sqrt{2}$ 的形式 .

2. 取 $d=1+\sqrt{2}\in\mathbb{Q}(\sqrt{2})$, 证明: $\sqrt{1+\sqrt{2}}\notin\mathbb{Q}(\sqrt{2})$. 因此有扩域

$$\mathbb{Q}(\sqrt{2})(\sqrt{1+\sqrt{2}})=\left\{\alpha+\beta\sqrt{2}+\alpha'\sqrt{1+\sqrt{2}}+\beta'\sqrt{2+2\sqrt{2}}\ \middle|\ \alpha,\beta,\alpha',\beta'\in\mathbb{Q}\right\}$$

3. 设 $\mathbb{F}_0=\mathbb{Q}$, 证明

(1) $\mathbb{Q}$ 的扩域

$$\mathbb{Q}(\sqrt{d_1})=\left\{\alpha+\beta\sqrt{d_1}\ \middle|\ d_1,\alpha,\beta\in\mathbb{Q},\ \sqrt{d_1}\notin\mathbb{Q}\right\}$$

中任何数都是某个有理系数 2 次代数方程的根.

(2) $\mathbb{Q}(\sqrt{d_1})$ 的扩域

$$\mathbb{Q}(\sqrt{d_1})(\sqrt{d_2})=\left\{p+q\sqrt{d_2}\ \middle|\ d_2,p,q\in\mathbb{Q}(\sqrt{d_1}),\ \sqrt{d_2}\notin\mathbb{Q}(\sqrt{d_1})\right\}$$

中任何数也是某个有理系数的 4 次代数方程的根.

提示 取 $x=p+q\sqrt{d_2}\in\mathbb{Q}(\sqrt{d_1})(\sqrt{d_2})$, 并记

$$p=\alpha_1+\beta_1\sqrt{d_1},\ q=\alpha_2+\beta_2\sqrt{d_1},\ d_2=\alpha_3+\beta_3\sqrt{d_1}.$$

其中$\alpha_i,\beta_i,\ i=1,2,3$ 都是有理数. 则

$$x^2-2px+p^2=d_2q^2$$

代入得

$$x^2-2(\alpha_1+\beta_1\sqrt{d_1})x+(\alpha_1+\beta_1\sqrt{d_1})^2=(\alpha_3+\beta_3\sqrt{d_1})(\alpha_2+\beta_2\sqrt{d_1})^2.$$

合并包含 $\sqrt{d_1}$ 的项有

$$x^2-2\alpha_1x+u=\sqrt{d_1}(-2\beta_1x+v),$$

其中 u,v 是有理数. 两边再平方就推出 x 满足的四次方程.

注记 一个数 x, 如果是某个整系数代数方程

$$a_nx^n+a_{n-1}x^{n-1}+\cdots a_1x+a_0=0\ \ (a_n,\cdots,a_0\in\mathbb{Z})$$

的根, 则称x 是***代数数***.

显然, 任何有理数 $x=\dfrac{p}{q}$ 是整系数一次代数方程

$$qx-p=0$$

的根. 因此有理数是代数数. $x=\sqrt{2}$ 满足 $x^2-2=0$ 因此 $\sqrt{2}$ 也是代数数.

由于有理系数的代数方程, 通过通分都等价于整系数的代数方程, 因此有理系数代数方程的根也是代数数.

本题目中, 实际上要证明对于有理数域 $\mathbb{F}_0=\mathbb{Q}$ 的扩域 $\mathbb{F}_1=\mathbb{F}_0(\sqrt{d_1})$ 以及 $\mathbb{F}_2=\mathbb{F}_1(\sqrt{d_2})$, 其中的数都是代数数.

进一步用数学归纳法可证明: 扩域 $\mathbb{F}_n$ 中任何数 x, 都是系数属于 $\mathbb{F}_{n-k}$ 的一个 2^k 次代数方程的根, $0<k\leqslant n$. 当 $k=n$ 时, 就可证明 $\mathbb{F}_n$ 中的数任何数 x 都是代数数. 用尺规作图的语言说, 就是从有理数域出发, 经过尺规作出的数都是代数数.

不是代数数的数称为***超越数***. 事实上, 超越数是存在的, 典型的例子是 π. 有关讨论已超出本专题的范围, 不再赘述.

第 7 讲　有限群

代数学的基本问题之一是研究各类代数方程的求解问题. 大家知道, 二次代数方程

$$ax^2 + bx + c = 0, \quad (a \neq 0)$$

的根可以通过对系数 a, b, c 进行有限次加、减、乘、除和开平方根运算给出. 事实上, 古代巴比伦人就已经用上述方法求解 (实系数) 二次代数方程了. 但是对于三次、四次乃至更高次数的代数方程, 能否通过系数的加、减、乘、除和开平方根、开立方根或开四次方根、甚至开更高次方根等代数方法求解. 这个问题直到16世纪中叶才解决了三次、四次代数方程求根问题. 时间跨度上千年. 人们自然希望能够继续下去, 对五次及以上方程, 也能够找到一个公式, 使得方程的根能用方程系数的代数式表示出来. 但遗憾的是, 在随后的两百多年时间里毫无进展.

正是这种“遗憾”, 人们开始意识到对五次及五次以上代数方程, 类似求根公式也许不存在. 十九世纪早期, 两位年轻数学家 Galois 和 Abel 考虑了代数方程根的置换, 用一种全新的思想揭示了五次及五次以上方程用代数求解方法不可解深层次原因. 由此开辟了一个崭新的数学领域–群论. 现如今群论不但是数学的基本知识, 在物理、化学、力学等领域也同样发挥了重要作用.

本专题仅限于如何从求解代数方程引进群的概念, 以及关于群的一些基本内容.

§7.1　代数方程的求解

在第 4 讲 §4.3 中, 从代数基本定理可知: 任何实系数或复系数 n 次代数方程在复数域中一定有 n 个根. 但是, 代数基本定理只是指出方程根存在性, 并没有给出具体求法. 为了进一步研究类似二次代数方程求根公式问题, 首先给出一般性定义

定义 7.1　对 n 次代数方程

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots a_0 = 0, \ (a_0 \neq 0),$$

这里, 方程系数 $a_n, a_{n-1}, \cdots, a_0$ 为复数或实数.

如果一个数 a 是通过方程系数 $a_n, a_{n-1}, \cdots, a_0$ 的加、减、乘、除以及各种次数的开方得到, 那么称这个数***由方程的系数代数表示 (简称“代数表示”)***.

如果通过某种方法使得方程的根由方程系数代数表示, 则称为方程***代数求解方法***.

1° 二次方程的代数求解

不失一般性, 取二次方程首项系数为 1, 因此有

$$x^2+px+q=0.$$

通过配方, 该方程可以化为

$$\left(x+\frac{p}{2}\right)^2+q-\frac{p^2}{4}=0,$$

因此方程两个根可以由系数 p,q 代数表示

$$x_1=\frac{-p+\sqrt{p^2-4q}}{2},\quad x_2=\frac{-p-\sqrt{p^2-4q}}{2}.$$

记 $\Delta=p^2-4q$, 根据 Δ 的取值, 可以判断方程的两个根是两个实根、重根还是一对互为共轭复根.

2° 三次方程的代数求解

关于三次代数方程

$$x^3+ax^2+bx+c=0,$$

仍然可以用代数求解方法求解. 令 $y=x+\dfrac{a}{3}$, 方程化为

$$y^3+\frac{3b-a^2}{3}y+\frac{2a^3-9ab+27c}{27}=0,$$

因此, 一般三次代数方程求解问题可归结为对下列方程求解问题

$$x^3+px+q=0.$$

若 $p=0$, 在复数范围内 $-q$ 的三个立方根就是方程 $x^3+q=0$ 的解.

若 $p\neq 0$, 则对该方程作如下变换

$$x=u-\frac{p}{3u},$$

就有

$$u^3-\frac{p^3}{27u^3}+q=0,$$

或转化成一个关于 u^3 的二次方程

$$u^6+qu^3-\frac{p^3}{27}=0$$

根据二次方程求根公式, u 满足下列方程

$$u^3=\frac{-q\pm\sqrt{\Delta}}{2},\quad \Delta=q^2+\frac{4}{27}p^3.$$

取 u 为 $\dfrac{-q+\sqrt{\Delta}}{2}$ 一个立方根, 那么 $\dfrac{-q+\sqrt{\Delta}}{2}$ 的三个立方根为

$$u_1 = u,\ u_2 = \omega u,\ u_3 = \omega^2 u,$$

其中

$$\omega = -\frac{1}{2} + \mathrm{i}\frac{\sqrt{3}}{2},\ \omega^2 = -\frac{1}{2} - \mathrm{i}\frac{\sqrt{3}}{2}$$

是 $z^3 = 1$ 的单位根,

注意到当 u 是 $\dfrac{-q+\sqrt{\Delta}}{2}$ 的立方根时, $v = -\dfrac{p}{3u}$ 是 $\dfrac{-q-\sqrt{\Delta}}{2}$ 的立方根:

$$v^3 = -\frac{p^3}{27}\frac{2}{-q+\sqrt{\Delta}} = \frac{-q-\sqrt{\Delta}}{2},$$

因此 $\dfrac{-q-\sqrt{\Delta}}{2}$ 的三个立方根为

$$v_1 = v = -\frac{p}{3u},\ v_2 = -\frac{p}{3u_2} = \omega^2 v,\ v_3 = -\frac{p}{3u_3} = \omega v,$$

这里用到了 $\omega^3 = 1$. 因此方程 $x^3 + px + q = 0$ $(p \neq 0)$ 的三个根为

$$\begin{aligned}
x_1 &= u_1 - \frac{p}{3u_1} = u + v,\\
x_2 &= u_2 - \frac{p}{3u_2} = \omega u + \omega^2 v = -\frac{1}{2}(u+v) + \mathrm{i}\frac{\sqrt{3}}{2}(u-v),\\
x_3 &= u_3 - \frac{p}{3u_3} = \omega^2 u + \omega v = -\frac{1}{2}(u+v) - \mathrm{i}\frac{\sqrt{3}}{2}(u-v),
\end{aligned}$$

其中u 是$\dfrac{-q+\sqrt{\Delta}}{2}$ 一个立方根, $v = -\dfrac{p}{3u}$ 是 $\dfrac{-q-\sqrt{\Delta}}{2}$ 的立方根.

这就是方程 $x^3 + px + q = 0$ 的求根公式, 三个根均可由系数 p, q 代数表示.

类似二次方程情形, 当 p, q 为实数时, 由$\Delta = q^2 + \dfrac{4}{27}p^3$ 可对方程的根做如下判断.

当 $\Delta > 0$ 时, 取 $u,\ v$ 是实立方根, $u \neq v$. 因此 x_1 是实根, x_2, x_3 是互为共轭的一对复根.

当 $\Delta = 0$ 时, 取 $u,\ v$ 是 $-\dfrac{q}{2}$ 实立方根, 因此 $u = v$, $x_1 = 2u,\ x_2 = x_3 = u$ 为三个实根, 其中x_2, x_3 是一对重根.

当 $\Delta < 0$ 时, 此时 $p < 0$, 所以 u 是$\dfrac{-q+\sqrt{\Delta}}{2}$ 的复立方根, 记 $u = \alpha + \mathrm{i}\beta$ $(\beta \neq 0)$. 但

$$(u\overline{u})^3 = |u|^6 = \frac{q^2 - \Delta}{4} = -\frac{p^3}{27},$$

因 $|u|^2$ 是实数, 推出 $|u|^2 = -\dfrac{p}{3} = uv$, 所以 $v = \overline{u} = \alpha - \mathrm{i}\beta$, 那么三个根

$$x_1 = 2\alpha,\ x_2 = -\alpha - \sqrt{3}\beta,\ x_3 = -\alpha + \sqrt{3}\beta$$

为互不相等的实根.

以上分别给出二次和三次代数方程代数求解详细过程. 下面将转变思路, 探讨对代数方程求解问题新的认识.

§7.2 对称多项式

设 $x_1, x_2, \cdots, x_n$ 是 n 个不定元, 称

$$F(x_1, \cdots, x_n) = \sum_{i_1, \cdots, i_n} a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}$$

为 n 元多项式. 这里求和都是有限求和: $i_k = 1, \cdots, d_k$, d_k 为正整数, $k = 1, \cdots, n$.

1° 对称多项式

定义 7.2 对 n 元多项式 $F(x_1, \cdots, x_n)$, 若对不定元 $x_1, x_2, \cdots, x_n$ 进行任意置换, $F(x_1, \cdots, x_n)$ 不变, 则称为是 $x_1, x_2, \cdots, x_n$ 的***对称多项式***.

例如, 两个不定元 x_1, x_2 的多项式

$$F(x_1, x_2) = x_1^2 + x_2^2$$

满足 $F(x_1, x_2) = F(x_2, x_1)$, 因此是对称多项式.

设 $x_1, \cdots, x_n$ 是不定元, 引进新的不定元 x, 作 x 多项式

$$\begin{aligned} f(x) &= (x - x_1)(x - x_2) \cdots (x - x_n) \\ &= x^n - \lambda_1 x^{n-1} + \lambda_2 x^{n-2} - \cdots + (-1)^n \lambda_n \end{aligned}$$

则对 $x_1, x_2, \cdots, x_n$ 任意置换, $f(x)$ 不变, 因此 $f(x)$ 系数

$$\begin{aligned} \lambda_1(x_1, \cdots, x_n) &= x_1 + x_2 + \cdots + x_n, \\ \lambda_2(x_1, \cdots, x_n) &= x_1x_2 + x_1x_3 + \cdots + x_2x_3 + \cdots + \cdots + x_{n-1}x_n, \\ &\vdots \\ \lambda_n(x_1, \cdots, x_n) &= x_1x_2 \cdots x_n. \end{aligned}$$

是 $x_1, x_2, \cdots, x_n$ 对称多项式. 称 $\lambda_1, \lambda_2, \cdots, \lambda_n$ 为 $x_1, x_2, \cdots, x_n$ **初等对称多项式**.

定理 7.3 (对称多项式基本定理) 设 $F(x_1, x_2, \cdots, x_n)$ 是 $x_1, x_2, \cdots, x_n$ 对称多项式, 则 $F(x_1, x_2, \cdots, x_n)$ 可表示为 $\lambda_1, \lambda_2, \cdots, \lambda_n$ 的多项式, 即存在一个 n 元多项式

$G(y_1, y_2, \cdots, y_n)$, 使得

$$F(x_1, x_2, \cdots, x_n) = G(\lambda_1, \lambda_2, \cdots, \lambda_n)$$

证明 这里只证明 $n = 2$ 的情形, 其它情形证明类似. 此时两个基本对称多项式为

$$\lambda_1(x_1, x_2) = x_1 + x_2,\ \lambda_2(x_1, x_2) = x_1 x_2.$$

设 $F(x_1, x_2)$ 是 x_1, x_2 的对称多项式. 对 $F(x_1, x_2)$ 中每一项, 按 x_1 幂次从高到低排列. 设 $F(x_1, x_2)$ 中 x_1 最高次幂项为 $ax_1^n x_2^m$, 其中 a 为该项系数.

首先断定 : $n \geqslant m$. 若不然, 根据对称性 $F(x_1, x_2) = F(x_2, x_1)$, $F(x_1, x_2)$ 中还包含 $ax_1^m x_2^n$, 这与 $ax_1^n x_2^m$ 是x_1 最高次幂项矛盾.

另一方面, 注意到

$$a\lambda_1^{n-m}\lambda_2^m = (x_1 + x_2)^{n-m}(x_1 x_2)^m$$

也是x_1, x_2 的对称多项式, 且 x_1 的最高次幂项为 $ax_1^n x_2^m$, 所以在

$$F_1(x_1, x_2) = F(x_1, x_2) - a\lambda_1^{n-m}\lambda_2^m$$

中, 关于 x_1 的最高次幂项的次数一定小于 n, 并且$F_1(x_1, x_2)$ 仍然是对称多项式. 重复上述过程就可把 $F(x_1, x_2)$ 表示为 λ_1, λ_2 的多项式. □

2° Viete 公式

当 $x_1, x_2, \cdots, x_n$ 是 n 次代数方程的根时, 就有如下的根与系数关系, 也就是下列 Viete（韦达, 1540-1603）公式.

定理 7.4 (Viete 公式) 如果 $x_1, x_2, \cdots, x_n$ 是实系数 n 次代数方程

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

的 n 个根, 那么根 $x_1, x_2, \cdots, x_n$ 的 n 个初等对称多项式可由多项式系数代数表示:

$$\begin{aligned}
&\lambda_1(x_1, \cdots, x_n) = x_1 + x_2 + \cdots + x_n = -a_{n-1},\\
&\lambda_2(x_1, \cdots, x_n) = x_1x_2 + x_1x_3 + \cdots + x_2x_3 + \cdots + \cdots + x_{n-1}x_n = a_{n-2},\\
&\qquad\qquad \vdots\\
&\lambda_n(x_1, \cdots, x_n) = x_1x_2\cdots x_n = (-1)^n a_0.
\end{aligned}$$

只要根据代数学基本定理的推论（见第 4 讲）, 作如下因式分解

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = (x - x_1)(x - x_2)\cdots(x - x_n),$$

通过比较 x 各次幂系数就得到多项式根与系数关系（Viete 公式）.

由对称多项式基本定理和 Viete 公式, 就得到如下推论

推论 7.5 设 $x_1, x_2, \cdots, x_n$ 是实系数 n 次代数方程

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

的根, 则根 $x_1, x_2, \cdots, x_n$ 的任意对称多项式 $F(x_1, \cdots, x_n)$ 可由多项式系数代数表示.

§7.3 代数方程根的置换

现在, 从一个新的角度重新审视代数方程求解问题.

1° 二次代数方程根的置换

设 x_1, x_2 是二次代数方程

$$x^2 + px + q = 0,$$

两个根, 那么二次方程的 Viete 公式为

$$\lambda_1(x_1, x_2) = x_1 + x_2 = -p,$$
$$\lambda_2(x_1, x_2) = x_1 x_2 = q.$$

对于 x_1, x_2 的对称多项式 $F(x_1, x_2)$, 将 x_1 换作 x_2, x_2 换作 x_1 的置换简记为

$$\begin{pmatrix} x_1 & x_2 \\ x_2 & x_1 \end{pmatrix} \quad 或 \quad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix},$$

因此对任意对称多项式$F(x_1, x_2)$, 在置换下是不变的:

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} : F(x_1, x_2) \longrightarrow F(x_2, x_1) = F(x_1, x_2).$$

将推论7.5 具体应用到二次代数方程, 那么任何根的对称多项式 $F(x_1, x_2)$ 都可由二次代数方程的系数 p, q 代数表示.

例 7.3.1 设 x_1, x_2 是二次代数方程两个根, 则

$$x_1^2 + x_2^2 = \lambda_1^2 - 2\lambda_2 = p^2 - 2q;$$
$$x_1^3 + x_2^3 = \lambda_1^3 - 3\lambda_1\lambda_2 = -p^3 + 3pq;$$
$$(x_1 - x_2)^2 = \lambda_1^2 - 4\lambda_2 = p^2 - 4q.$$

注意到对称多项式

$$(x_1 - x_2)^2 = (x_1 + \omega x_2)^2 = p^2 - 4q,$$

其中 $\omega=-1$ 是 $z^2=1$ 单位根. 对 $(x_1-x_2)^2$ 开平方根后与 $x_1+x_2=-p$ 联立

$$x_1+x_2=-p,\ x_1-x_2=\pm\sqrt{p^2-4q},$$

解出两个根

$$x_1=\frac{-p+\sqrt{p^2-4q}}{2},\ x_2=\frac{-p-\sqrt{p^2-4q}}{2}.$$

这样就把二次代数方程的两个根 x_1,x_2 由方程系数 p,q 代数表示, 即通过 p,q 的加减乘除和开平方根等运算得到. 这里关键是通过对称多项式 $(x_1-x_2)^2$ 找到了 $x_1-x_2=x_1+\omega x_2$.

2° 三次代数方程根的置换

如果说通过二次方程, 还难以体会利用根的置换在求解方程中的作用, 那么我们用同样的方法, 考察三次代数方程

$$x^3+px^2+qx+r=0,$$

和 Viete 公式

$$\begin{aligned}\lambda_1(x_1,x_2,x_n)&=x_1+x_2+x_3=-p,\\ \lambda_1(x_1,x_2,x_n)&=x_1x_2+x_2x_3+x_3x_1=q,\\ \lambda_1(x_1,x_2,x_n)&=x_1x_2x_3=-r.\end{aligned}$$

关于根的任何一个置换 $(x_1,x_2,x_3)\longrightarrow(x_{i_1},x_{i_2},x_{i_3})$ 就是对根的编号 $(1,2,3)$ 进行一次重新排列. 这样的排列共有六种, 记为:

$$\sigma_0=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\ \sigma_1=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\ \sigma_2=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},$$
$$\sigma_3=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\ \sigma_4=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\ \sigma_5=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}.$$

其中 σ_0 是恒等置换. 与二次方程情形相同, 三次方程根 x_1,x_2,x_3 的任何对称多项式$P(x_1,x_2,x_3)$, 都可以表示为 $\lambda_1,\lambda_2,\lambda_3$ 的多项式, 进而可以由方程系数 p,q,r 代数表示.

现在需要找到一个与二次方程情形中$x_1-x_2=x_1+\omega x_2$, ($\omega=-1$ 满足方程 $z^2=1$) 类似多项式. 因此, 借助方程 $z^3=1$ 的三次单位根 $1,\omega,\omega^2$, 其中 $\omega\neq1$, 所以 ω 还满足方程 $z^2+z+1=0$. 设

$$\psi_0=x_1+\omega x_2+\omega^2x_3,$$

但是,不难发现, ψ_0 并不是 x_1, x_2, x_3 的对称多项式. 在六种置换下, 记 ψ_0 分别变换为 $\psi_0, \psi_1, \psi_2, \psi_3, \psi_4, \psi_5$, 它们可具体表示为

$$\sigma_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} : \psi_0 \longrightarrow x_1 + \omega x_2 + \omega^2 x_3 = \psi_0,$$

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} : \psi_0 \longrightarrow x_1 + \omega x_3 + \omega^2 x_2 = \psi_1,$$

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} : \psi_0 \longrightarrow x_3 + \omega x_1 + \omega^2 x_2 = \psi_2,$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} : \psi_0 \longrightarrow x_3 + \omega x_2 + \omega^2 x_1 = \psi_3$$

$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} : \psi_0 \longrightarrow x_2 + \omega x_1 + \omega^2 x_3 = \psi_4,$$

$$\sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} : \psi_0 \longrightarrow x_2 + \omega x_3 + \omega^2 x_1 = \psi_5.$$

利用 $\omega^3 = 1$, 容易验证 $\psi_0, \psi_1, \psi_2, \psi_3, \psi_4, \psi_5$ 中只有 ψ_0, ψ_1 是独立的, 其余的均可由 ψ_0 或 ψ_1 表示:

$$\psi_2 = \omega^2\psi_0,\ \psi_5 = \omega\psi_0,\ \psi_3 = \omega\psi_1,\ \psi_4 = \omega^2\psi_1.$$

因此, 在六种置换下, ψ_0 分别变换为

$$\sigma_0 :\ \psi_0 \longrightarrow \psi_0,\quad \sigma_2 :\ \psi_0 \longrightarrow \omega^2\psi_0,\quad \sigma_5 :\ \psi_0 \longrightarrow \omega\psi_0,$$
$$\sigma_1 :\ \psi_0 \longrightarrow \psi_1,\quad \sigma_3 :\ \psi_0 \longrightarrow \omega\psi_1,\quad \sigma_4 :\ \psi_0 \longrightarrow \omega^2\psi_1,$$

类似地, 可以验证在六种置换下, ψ_1 分别变换为

$$\sigma_0 :\ \psi_1 \longrightarrow \psi_1,\quad \sigma_2 :\ \psi_1 \longrightarrow \omega\psi_1,\quad \sigma_5 :\ \psi_0 \longrightarrow \omega^2\psi_1,$$
$$\sigma_1 :\ \psi_1 \longrightarrow \psi_0,\quad \sigma_3 :\ \psi_1 \longrightarrow \omega^2\psi_0,\quad \sigma_4 :\ \psi_1 \longrightarrow \omega\psi_0,$$

由此推出, 在所有置换下, 作为集合 $\{\psi_0, \psi_1, \psi_2, \psi_3, \psi_4, \psi_5\}$ 是不变的, 只不过秩序重新排列了而已. 例如

$$\psi_4 = \omega^2\psi_1 \xrightarrow{\sigma_3} \omega^2(\omega^2\psi_0) = \omega\psi_0 = \psi_5.$$

这样就有下列性质.

性质 7.6 *关于 t 的多项式*

$$f(t) = (t - \psi_0)(t - \psi_1)(t - \psi_2)(t - \psi_3)(t - \psi_4)(t - \psi_5)$$

在 x_1, x_2, x_3 的任何置换下不变, 因此 $f(t)$ 系数是 x_1, x_2, x_3 的对称多项式.

将由 ψ_0 和 ψ_1 表示的 $\psi_2,\psi_3,\psi_4,\psi_5$ 带入多项式 $f(t)$, 并利用 $\omega^3=1$（因为 $\omega\neq 1$, 因此也有$\omega^2+\omega+1=0$）得

$$\begin{aligned} f(t) &= (t-\psi_0)(t-\omega\psi_0)(t-\omega^2\psi_0)(t-\psi_1)(t-\omega\psi_1)(t-\omega^2\psi_1)\\ &= (t^3-\psi_0^3)(t^3-\psi_1^3)\\ &= t^6-(\psi_0^3+\psi_1^3)t^3+\psi_0^3\psi_1^3. \end{aligned}$$

性质 7.7 多项式 $f(t)$ 可表示为

$$f(t)=t^6-(\psi_0^3+\psi_1^3)t^3+\psi_0^3\psi_1^3,$$

其系数为 $\psi_0^3+\psi_1^3$ 和 $\psi_0^3\psi_1^3$, 是 x_1,x_2,x_3 的对称多项式, 因此能够用三次多项式 $x^3+px^2+qx+r=0$ 的系数 p,q,r 代数表示:

$$\begin{aligned} \psi_0^3+\psi_1^3 &= -2p^3+9pq-27r,\\ \psi_0^3\psi_1^3 &= (p^2-3q)^3. \end{aligned}$$

在推导上面具体表达式时, 只要把 $\psi_0=x_1+\omega x_2+\omega^2x_3$, $\psi_1=x_1+\omega x_3+\omega^2x_2$ 代入并利用三次多项式 Viete 公式和 $\omega^3=1$, $\omega^2+\omega+1=0$ 即可.

根据性质7.7, $f(t)=0$, 的 6 个根 $\psi_0,\psi_1,\psi_2,\psi_3,\psi_4,\psi_5$ 可以通过

$$\begin{aligned} t^3 &= \frac{(\psi_0^3+\psi_1^3)\pm\sqrt{(\psi_0^3+\psi_1^3)^2-4(\psi_0^3\psi_1^3)}}{2}\\ &= \frac{(-2p^3+9pq-27r)\pm\sqrt{(-2p^3+9pq-27r)^2-4(p^2-3q)^3}}{2} \end{aligned}$$

开立方根得到, 因此它们都可以由 p,q,r 代数表示（即通过系数 p,q,r 的加减乘除以及开平方根、开立方根得到）.

由于方程 $f(t)=0$ 中 6 个根只有 ψ_0, ψ_1 是独立的, 再从 Viete 公式中取 $x_1+x_2+x_3=-p$,并考虑下列三元一次线性方程组

$$\begin{cases} x_1+x_2+x_3 & =-p,\\ x_1+\omega x_2+\omega^2x_3 & =\psi_0,\\ x_1+\omega x_3+\omega^2x_2 & =\psi_1. \end{cases}$$

根据第 5 讲 §5.6 中讨论结果, 上述方程组系数行列式

$$\begin{vmatrix} 1 & 1 & 1\\ 1 & \omega & \omega^2\\ 1 & \omega^2 & \omega \end{vmatrix} = 3\omega(\omega-1)\neq 0$$

因此有唯一的解：

$$\begin{cases} x_1 = \frac{1}{3}(-p + \psi_0 + \psi_1), \\ x_2 = \frac{1}{3}(-p + \omega^2\psi_0 + \omega\psi_1), \\ x_3 = \frac{1}{3}(-p + \omega\psi_0 + \omega^2\psi_1), \end{cases}$$

即三次方程的三个根 x_1, x_2, x_3 可用方程系数 p 和 ψ_0, ψ_1 代数表示, 而 ψ_0, ψ_1 可由系数 p, q, r 代数表示, 因此最终得到三次方程的根 x_1, x_2, x_3 可由其系数 p, q, r 代数表示 .

三次代数方程根的置换共有 6 种

$$S_6 = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$$

其中一组, 记为

$$A_3 = \{\sigma_0, \sigma_2, \sigma_5\},$$

A_3 中的置换把 ψ_0 分别变换到 $\psi_0, \omega^2\psi_0, \omega\psi_0$, 把 ψ_1 分别变换到 $\psi_1, \omega\psi_1, \omega^2\psi_1$, 如果在置换中定义一种代数结构（下面将重点讨论）, 那么将会发现, S_3 中子集合 $A_3 = \{\sigma_0, \sigma_2, \sigma_5\}$ 具有特殊性质.

推而广之, 四次代数方程根的置换共有 24 种, 置换的集合记为 S_4, 我们发现 S_4 与 S_3 有类似的性质, 但是对一般的 n $(n \geqslant 5)$ 次代数方程, 根的置换种类达到 $n!$ 种, 这 $n!$ 种置换的集合记为 S_n, 远比 S_3, S_4 要复杂. 这就需要对 S_n 代数性质作进一步研究, 因此也就产生了数学中一个十分重要领域–群的理论, 并为最终解决 5 次及 5 次以上一般代数方程不可能用代数方法求解奠定了数学基础.

§7.4 置换及其性质

首先从置换出发, 并通过置换满足的代数结构, 引进群的定义, 并以置换为模型, 讨论群基本性质.

抽象地看, 所谓置换实际上是一个有 n 个元素有限集合

$$X = \{x_1, x_2, \cdots, x_n\}$$

自身到自身的 1-1 对应（1-1 映射）:

$$\sigma : X \longrightarrow X,$$

这里集合 X 中元素不一定是某个方程的根, 可以是任何元素, 例如 $X = \{1, 2, \cdots, n\}$. 因为是 1-1 对应, 所以可以具体表示为

$$\sigma(x_1) = x_{\alpha_1},\ \sigma(x_2) = x_{\alpha_2},\ \cdots,\ \sigma(x_n) = x_{\alpha_n},$$

这里 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 是 $1, 2, \cdots, n$ 的一个排列.

称 n 个元素的置换为n **阶置换**, 显然 n 阶置换共有 $n!$ 种.

因为 σ 是 n 个元素之间的1-1 对应, 有时我们干脆将它记为

$$\sigma(1) = \alpha_1,\ \sigma(2) = \alpha_2,\ \cdots,\ \sigma(n) = \alpha_n,$$

并按列表的方法, 将它表示为上下对应

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_n \end{pmatrix}$$

一般来说, 习惯上将置换中列的顺序按第一行 1 到n 排列 , 但是, 只要上下对应不变, 列与列先后顺序并没有任何关系. 例如

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

正如一个班级同学与学号的 1-1 对应, 与同学座次没有关系.

记 n 个元素的置换的全体为

$$S_n = \left\{ \sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_n \end{pmatrix} \;\middle|\; (\alpha_1, \cdots, \alpha_n) \text{ 是 } (1, \cdots, n) \text{ 的一个排列} \right\}$$

1° **置换的乘积**

设有两个置换

$$\sigma_1 = \begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \end{pmatrix},\quad \sigma_2 = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \beta_1 & \beta_2 & \cdots & \beta_n \end{pmatrix},$$

它们的乘积定义为两个置换的复合, 即先进行σ_1 置换, 再进行 σ_2 置换 :

$$X \xrightarrow{\sigma_1} X \xrightarrow{\sigma_2} X$$

或者表示为

$$\sigma_2\sigma_1 = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \beta_1 & \beta_2 & \cdots & \beta_n \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & n \\ \beta_1 & \beta_2 & \cdots & \beta_n \end{pmatrix} = \sigma_3.$$

也就是, 在 σ_1 的第一行任何一个 i, 对应的列找到 α_i, 再在 σ_2 的第一行中 α_i 找到同一列对应的 β_i, 这样就得到两个置换乘积将 i 置换到 β_i.

注意到置换的乘积未必具有交换性, 例如

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix},$$

但是

$$\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}=\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix},$$

两者是不相等的. 虽然置换乘法不满足交换律, 但是满足结合律, 即对于任意三个置换 σ,ρ,τ, 有

$$\tau(\rho\sigma)=(\tau\rho)\sigma.$$

2° **恒等置换**

在所有置换中, 下列置换称为恒等置换

$$e=\begin{pmatrix}1&2&\cdots&n\\1&2&\cdots&n\end{pmatrix}$$

它的特点是与任意置换 σ 相乘, 结果不变

$$e\sigma=\sigma e=\sigma.$$

3° **逆置换**

任意置换

$$\sigma=\begin{pmatrix}1&2&\cdots&n\\\alpha_1&\alpha_2&\cdots&\alpha_n\end{pmatrix},$$

必存在逆置换

$$\sigma^{-1}=\begin{pmatrix}\alpha_1&\alpha_2&\cdots&\alpha_n\\1&2&\cdots&n\end{pmatrix},$$

使得

$$\sigma^{-1}\sigma=\sigma\sigma^{-1}=e.$$

例如

$$\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}^{-1}=\begin{pmatrix}4&2&1&3\\1&2&3&4\end{pmatrix},$$

就是将 σ 的两行对调. 如果将列重新排列, 即把第 3 列调到第 1 列, 第 1 列调到第 4 列, 就有

$$\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}^{-1}=\begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix}.$$

4° **轮换与对换**

设 $\alpha_1, \alpha_2, \cdots, \alpha_d$ 是$\{1, 2, \cdots, n\}$ 中 d 个不相等的整数. 若一个置换 σ 满足

$$\sigma(\alpha_1) = \alpha_2,\ \sigma(\alpha_2) = \alpha_3,\ \cdots,\ \sigma(\alpha_{d-1}) = \alpha_d,\ \sigma(\alpha_d) = \alpha_1,$$

并且$\sigma(\beta) = \beta,\ \beta \neq \alpha_1, \alpha_2, \cdots, \alpha_d$. 则称置换为一个$d-$ **轮换**, d 称为轮换**长度**. 简记为

$$\sigma = (\alpha_1\alpha_2\cdots\alpha_d) = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_{d-1} & \alpha_d & \beta_1 & \beta_2 & \cdots & \beta_r \\ \alpha_2 & \alpha_3 & \cdots & \alpha_d & \alpha_1 & \beta_1 & \beta_2 & \cdots & \beta_r \end{pmatrix}.$$

其中 $d+r = n$. 因为置换与列的排序无关, 所以把通过置换发生变化的排在前面, 而那些在置换下不变的排在后面. 当然, 这样的记号不唯一, 例如 $(\alpha_2\alpha_3\cdots\alpha_d\alpha_1), (\alpha_3\alpha_4\cdots\alpha_d\alpha_1\alpha_2)$ 等等都表示同一个轮换.

如果轮换 σ_1 中出现数字在另一个轮换 σ_2 中不再出现, 那么就称这两个轮换**不相交**, 否则称为**相交**. 例如 (134) 与 (589) 不相交, 但 (134) 与 (247) 相交.

所谓**对换** 是指最简单的轮换, 即

$$\sigma = (\alpha\beta) = \begin{pmatrix} \cdots & \alpha & \cdots & \beta & \cdots \\ \cdots & \beta & \cdots & \alpha & \cdots \end{pmatrix}.$$

它表示

$$\sigma(\alpha) = \beta,\ \sigma(\beta) = \alpha,\ \sigma(j) = j,\ j \neq \alpha, \beta.$$

轮换具有下列简单性质:

性质 7.8

(i) 长度为 d 的轮换 $\sigma = (\alpha_1\alpha_2\cdots\alpha_d)$ 满足 $\sigma^d = e,\ \sigma^r \neq e\ (r \neq d)$.

(ii) 不相交轮换的乘积可交换:

$$(\alpha_1\alpha_2\cdots\alpha_d)(\beta_1\beta_2\cdots\beta_r) = (\beta_1\beta_2\cdots\beta_r)(\alpha_1\alpha_2\cdots\alpha_d),$$

这里 $\alpha_k \neq \beta_l,\ k = 1, 2, \cdots, d,\ l = 1, 2, \cdots, r$.

引进轮换后, 有下列结果:

定理 7.9 除恒等置换外, 任意置换都可以分解为若干个不相交轮换乘积. 任意置换都可以分解为若干个对换 (可以相交) 乘积.

该定理实际上给出了置换的另一种表示, 这种表示方法在某些场合更加方便.

证明 取 $\alpha_1 = 1$, 若 $\sigma(\alpha_1) = \alpha_1$, 即 α_1 在置换下不发生变化, 则考虑 $\alpha_1 = 2$, 搜索下去直到出现 $\sigma(\alpha_1) \neq \alpha_1$. 记$\alpha_2 = \sigma(\alpha_1)$. 显然 $\sigma(\alpha_2) \neq \alpha_2$, 否则与 1-1 对应矛盾.

若 $\sigma(\alpha_2) = \alpha_1$, 则 $(\alpha_1\alpha_2)$ 是一个对换, 剩余的是不再出现 α_1 和 α_2 的置换;

若 $\sigma(\alpha_2) \neq \alpha_1$, 则记$\alpha_3 = \sigma(\alpha_2)$. 如此下去直到出现 $\sigma(\alpha_{d_1}) = \alpha_1$, 这样 $(\alpha_1\alpha_2\cdots\alpha_{d_1})$ 就是一个轮换. 剩余部分是不再包含 $\alpha_1, \alpha_2, \cdots, \alpha_{d_1}$ 的置换.

对剩余部分继续实施上述过程, 经过有限步就可以把 σ 分解成不相交轮换乘积.

关于第二个结论, 只要考虑任意轮换可以分解成对换乘积即可, 事实上, 对于任意轮换, 有

$$(\alpha_1\alpha_2\cdots\alpha_d)=(\alpha_1\alpha_2)(\alpha_2\alpha_3)\cdots(\alpha_{d-2}\alpha_{d-1})(\alpha_{d-1}\alpha_d),$$

例如

$$\begin{aligned}(1234)&=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}\\&=\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}\\&=(12)(23)(34).\end{aligned}$$

这样就证明了定理. □

§7.5 有限群及其性质

上节定义了置换的乘法、单位置换以及置换的逆, 同时讨论了乘法、单位元以及逆元所满足的算术性质, 把这些性质抽象出来就得到了“群”的定义.

1° 有限群

定义 7.10 一个集合 G , 如果满足如下条件, 那么称 G 是一个***群***:

(i) G 有一种运算, 称为“乘法”, 即对任意 $a,b\in G$, 有$ab\in G$, 乘法运算满足结合律

$$(ab)c=a(bc),\ a,b,c\in G.$$

(ii) G 中包含“单位元”, 通常记为 e, 它满足: 对任意 $a\in G$,

$$ea=ae=a.$$

(iii) G 中任意元素 a 均可逆, 即 $xa=e$ 在 G 中可解, 记 $x=a^{-1}\in G$, 称为 a 的***逆元*** , 它满足

$$aa^{-1}=a^{-1}a=e.$$

若 G 中乘法可交换, 即对任意 $a,b\in G$, 有 $ab=ba$, 则称 G 为***交换群*** 或 *Abel* ***群***.

若群 G 元素个数有限, 则称为***有限群***. 元素个数称为群的***阶***.

由定义, 直接得到如下定理.

定理 7.11 (消去律) *若群 G 中元素 a,b,c 满足 $ab=ac$, 或 $ba=ca$, 则 $b=c$.*

证明 设 $ab=ac$, 两边左乘 a^{-1} 得 $a^{-1}(ab)=a^{-1}(ac)$, 利用结合律得 $(a^{-1}a)b=(a^{-1}a)c$, 也就是 $b=eb=ec=c$. 对于右乘 $ba=ca$, 证明类似 □

其实, 在前面各专题中, 已经出现了群的例子, 这里连同一些新例子一并展示.

例 7.5.1 所有正有理数集合 $\mathbb{Q}_+=\{r\mid r>0,\ r\in\mathbb{Q}\}$ 是群, 其中单位元为 1, 但不是有限群.

例 7.5.2 模 m 同余类 $\mathbb{Z}_m$ 的子集合 (第 2 讲 §2.6)

$$\mathbb{Z}_m^*=\{[a]\mid [a]\in\mathbb{Z}_m,\ (a,m)=1\},$$

是一个可交换的, 阶数为 $\varphi(m)$ (Euler 函数, 见第 2 讲§ 2.5) 的有限群. 例如当 $m=8$ 时,

$$\mathbb{Z}_8^*=\{[1],[3],[5],[7]\}$$

是一个 4 阶有限群.

例 7.5.3 n 次的单位根组成的集合 $D_n=\{\xi_1,\xi_2,\cdots,\xi_n\}$ 在复数乘法运算下是一个群 (第 4 讲§4.4). 特别当 $n=4$ 时, 四个单位根 $\{1,-1,\mathrm{i},-\mathrm{i}\}$ 的集合是一个群.

例 7.5.4 考虑等边三角形对称不变性. 设 $\{e,a_1,a_2\}$ 分别是三角形以中心点为圆心顺时针旋转 $0^\circ,120^\circ,\ 240^\circ$ 的旋转, $\{a_3,a_4,a_5\}$ 分别是以三个角平分线 K,L,M 的反射 (图 7.1) . 则等边三角形在上述旋转和反射下不变.

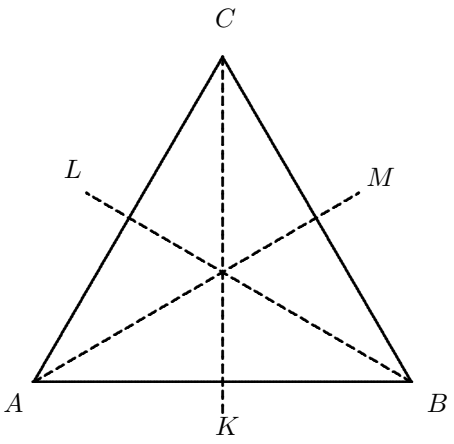


图 7.1

在六个元素集合中

$$S=\{e,a_1,a_2,a_3,a_4,a_5\}$$

将连续作用定义为乘法, 那么 S 是一个群, 元素之间的乘积以及单位元和逆元等信息均可从下列乘法表中反映.例如 $a_1a_2 = a_2a_1 = e$, 因此 a_1, a_2 互为逆元.

乘法	e	a_1	a_2	a_3	a_4	a_5
e	e	a_1	a_2	a_3	a_4	a_5
a_1	a_1	a_2	e	a_5	a_3	a_4
a_2	a_2	e	a_1	a_4	a_5	a_3
a_3	a_3	a_4	a_5	e	a_1	a_2
a_4	a_4	a_5	a_3	a_2	e	a_1
a_5	a_5	a_3	a_4	a_1	a_2	e

例 7.5.5 对下列六个函数

$$f_0(x) = x, \quad f_1(x) = \tfrac{1}{1-x}, \quad f_2(x) = \tfrac{x-1}{x},$$
$$f_3(x) = \tfrac{1}{x}, \quad f_4(x) = 1 - x, \quad f_5(x) = \tfrac{x}{x-1},$$

定义它们之间的乘法如下

$$(f_i \circ f_j)(x) = f_i(f_j(x)),$$

也就是函数的复合, 那么不难验证在该乘法定义下, 六个函数的集合满足群的定义. 例如,

$$(f_5 \circ f_2)(x) = f_5(f_2(x)) = \frac{(x-1)/x}{(x-1)/x - 1} = 1 - x = f_4(x),$$
$$(f_2 \circ f_5)(x) = f_2(f_5(x)) = \frac{x/(x-1) - 1}{x/(x-1)} = \frac{1}{x} = f_3(x),$$

各项之间的乘法由下面乘法表给出.

乘法	f_0	f_1	f_2	f_3	f_4	f_5
f_0	f_0	f_1	f_2	f_3	f_4	f_5
f_1	f_1	f_2	f_0	f_5	f_3	f_4
f_2	f_2	f_0	f_1	f_4	f_5	f_3
f_3	f_3	f_4	f_5	f_0	f_1	f_2
f_4	f_4	f_5	f_3	f_2	f_0	f_1
f_5	f_5	f_3	f_4	f_1	f_2	f_0

其中, f_0 是单位元.每个元素的逆元也在表中给出, 例如 f_2 的逆元为 f_1:

$$f_2 \circ f_1 = f_1 \circ f_2 = f_0.$$

例7.5.4和例7.5.5虽然是完全不同两个例子, 但是如果做一个对应

$$\{e, a_1, a_2, a_3, a_4, a_5\} \longrightarrow \{f_0, f_1, f_2, f_3, f_4, f_5\}$$

不难发现它们的乘法表完全一样, 称这种现象为群的同构.

定义 7.12 设有两个群 G_1 和 G_2, 分别以e_1 和 e_2 为各自单位元. 如果存在一个 *1-1* 映射 $\varphi : G_1 \longrightarrow G_2$ 使得

$$\varphi(ab) = \varphi(a)\varphi(b) \quad \text{对任意 } a, b \in G_1 \text{ 成立}$$

那么称 φ 为群 G_1 和 G_2 的同构. 上式中 ab 是 G_1 中乘法, $\varphi(a)\varphi(b)$ 是 G_2 中乘法.

如果两个群 G_1 和 G_2 之间存在一个同构, 那么称这两个群是同构的, 记为

$$G_1 \cong G_2.$$

根据定义, 若存在 G_1 和 G_2 的同构 φ, 则一定有

$$\varphi(e_1) = e_2, \quad (\varphi(a))^{-1} = \varphi(a^{-1}) \quad a \in G_1.$$

例7.5.4和例7.5.5分别给出的两个群同构.

顾名思义, 两个同构的群意味着它们有相同群结构, 与群无关其它性质可以忽略不计. 例如不管是例7.5.4三角形旋转或反射, 还是例7.5.5中定义的函数, 在各自的运算下, 群的结构完全一样.

2° 子群

定义 7.13 设 G 是一个群, H 是G 子集合. 如果 H 对G 中运算也构成一个群, 那么称 H 为 G 的***子群***.

显然, 只有单位元的集合 $E = \{e\}$ 以及 G 自身一定是 G 的子群, 称为**平凡子群**.其它子群为**非平凡子群**. 一般情况下, 所讨论子群都是指非平凡子群.

例 7.5.6 在例7.5.4中, 记等边三角形旋转的集合为 $H = \{e, a_1, a_2\} \subset S$, 则 H 满足群的定义, 因此是 S 的子群. 元素之间乘法由下表给出

乘法	e	a_1	a_2
e	e	a_1	a_2
a_1	a_1	a_2	e
a_2	a_2	e	a_1

有限群和子群之间有下列著名的 Lagrange（拉格朗日, 1736-1813）定理.

定理 7.14 (Lagrange) 设 G 是有限群, H 是 G 非平凡子群（当然也是有限群）, 那么 H 的阶一定能够整除 G 的阶. 若 G 的阶为素数, 则 G 不存在非平凡子群.

证明 设 G 的阶为 n, H 的阶为 r, 因为 H 是非平凡子群, 所以 $n > r > 1$.

证明的思路是利用 H 将 G 分解成若干个元素个数都是 r , 但两两不相交子集的并, 因此推出定理的结果. 具体做法如下: 记非平凡子群 H 的元素为

$$H = \{h_1, h_2, \cdots, h_r\}.$$

取 $a_1 \in G,\ a_1 \notin H$ （所以$a_1 \neq e$, 因为 $e \in H$ ）, 令

$$a_1H = \{a_1h_1, a_1h_2, \cdots, a_1h_r\} \subset G$$

则集合 a_1H 中 r 个元素互不相等. 否则, 必有 $a_1h_i = a_1h_j$, 根据消去率, 推出 $h_i = h_j$, 这与 H 的元素个数是 r 相矛盾.

同时, $a_1H \cap H = \phi$ (ϕ 表示空集), 即a_1H 和 H 中元素相异. 否则, 必有某个 a_1h_i 与 H 中某个元素相等 $a_1h_i = h_j$, 推出 $a_1 = h_jh_i^{-1} \in H$, 这与 a_1 选取相矛盾. 因此

$$G \supseteq H \cup a_1H,$$

若等号成立: $G = H \cup a_1H$ 推出$n = 2r$, 定理得证.

反之取$a_2 \in G,\ a_2 \notin a_1H \cup H$, 并令

$$a_2H = \{a_2h_1, a_2h_2, \cdots, a_2h_r\} \subset G,$$

如同对 a_1H 的讨论, a_2H 中元素互不相等, 因此 a_2H 中元素个数仍然是 r 个.

如果存在某个 a_2h_i 使得 $a_2h_i = h_j$, 则推出 $a_2 = h_jh_i^{-1} \in H$.

如果存在某个 a_2h_i 使得 $a_2h_i = a_1h_j$, 则推出 $a_2 = a_1h_jh_i^{-1}$, 因为 $h_jh_i^{-1} \in H$, 所以必有 $h_jh_i^{-1} = h_k$, 推出 $a_2 = a_1h_k \in a_1H$.

上述两种情况都与 a_2 的选取矛盾, 所以 $a_2H \cap H = a_2H \cap a_1H = \phi$, 且

$$G \supseteq H \cup a_1H \cup a_2H.$$

若等号成立, 则 $n = 3r$, 否则继续上述过程. 经过有限步可得 l 个元素个数为 r 的子集合 $a_1H,\ a_2H,\ \cdots,\ a_lH$ 使得

$$G = H \cup a_1H \cup a_2H \cup \cdots \cup a_lH,$$

且

$$a_iH \cap a_jH = \phi\ (1 \leqslant i \neq j \leqslant l)$$

因此 $n = lr$, 即 $r \mid n$. □

在上述证明过程中, 对 $a \in G$, $aH = \{ah \mid h \in H\}$ 称为 G 关于子群 H 的**陪集**. 因此也就得到

定理 7.15 设 G 是有限群, H 是 G 非平凡子群, 则 G 能分解为两两不相交陪集的并.

3° 对称群与置换群

定义 7.16 所有n 阶置换构成集合 S_n 满足群的定义, 其中单位元 $e=\sigma_0$,因此 S_n 是$n!$ 阶有限群, 称为***对称群***. 由于置换乘积不可交换, 所以对称群是非 $Abel$ 群.

对称群 S_n 中任何子群称为***置换群***.

虽然对称群 (置换群) 是从代数方程根的置换开始, 但并不局限于此. 例如几何图形对称性就是一个重要的例子.

例 7.5.7 考虑对称群 S_3, 它由六个置换组成

$$\sigma_0=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\ \sigma_1=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\ \sigma_2=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},$$
$$\sigma_3=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\ \sigma_4=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\ \sigma_5=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}.$$

不难看出, 在例7.5.4 中, 若将等边三角形的三个顶点分别用 A,B,C 表示, 那么任何保持等边三角形不变的变换, 都对应于三个顶点 (A,B,C) 的一个置换：

$$e=\sigma_0,\ a_1=\sigma_5,\ a_2=\sigma_2,\ a_3=\sigma_4,\ a_4=\sigma_3,\ a_5=\sigma_1.$$

因此例7.5.4中的 S 就是对称群 S_3.

例 7.5.8 S_3 的子集合 $\{\sigma_0,\ \sigma_1\}$, $\{\sigma_0,\ \sigma_3\}$, $\{\sigma_0,\ \sigma_4\}$ 和 $\{\sigma_0,\ \sigma_2,\ \sigma_5\}$ 是它的子群, 即它们分别有单位元$e=\sigma_0$, 对置换的乘法封闭, 且包含任何元素的逆元. 因此是置换群. 从几何上看, 子群 $\{\sigma_0,\ \sigma_1\}$, $\{\sigma_0,\ \sigma_3\}$, $\{\sigma_0,\ \sigma_4\}$ 正是等边三角形沿对称轴的反射变换, 而子群 $A_3=\{\sigma_0,\ \sigma_2,\ \sigma_5\}$ 是等边三角形的旋转变换.

继续考虑

$$A_3=\{\sigma_0,\ \sigma_2,\ \sigma_5\}=\left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\ \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\ \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\right\},$$

它的一个典型特征是下列多项式

$$\phi=(x_1-x_2)(x_1-x_3)(x_2-x_3)$$

仅在A_3中置换下不变:

$$\sigma_i:\phi\longrightarrow\phi,\ i=0,2,5,$$

但是在 S_3 中其它置换下是变化的:

$$\sigma_i : \phi \longrightarrow -\phi,\ i = 1, 3, 4.$$

一般地, 考虑 n 个未定元多项式

$$\phi(x_1, x_2, \cdots, x_n) = \prod_{i<j}^{n} (x_i - x_j)$$

即所有$(x_i - x_j),\ i < j$ 因子的乘积, 不难看出任何一个置换 $\sigma \in S_n$, 必有

$$\sigma :\ \phi(x_1, x_2, \cdots, x_n) \longrightarrow \pm\phi(x_1, x_2, \cdots, x_n).$$

若 $\sigma : \phi \longrightarrow \phi$, 则称 σ 为**偶置换**, 若 $\sigma : \phi \longrightarrow -\phi$, 则称 σ 为**奇置换**. 因此当 $n = 3$ 时, S_3 中置换 $A_3 = \{\sigma_0,\ \sigma_2,\ \sigma_5\}$ 是偶置换, 其余的 $\{\sigma_1,\ \sigma_3,\ \sigma_4\}$ 是奇置换.

定理 7.17 对于 S_n 中置换, 有

(i) 任意对换一定是奇置换.

(ii) 长度为奇数的轮换是偶置换, 长度为偶数的轮换为奇置换.

(iii) 任意偶置换可以分解为偶数个对换乘积, 任意奇置换可以分解为奇数个对换乘积.

(iv) S_n 中偶置换和奇置换个数各为 $\dfrac{n!}{2}$.

证明 (i) 是显然的. 根据定理7.9, 直接可以得到(ii) 和 (iii). 关于 (iv) 的证明, 作偶置换和奇置换的如下对应:设 σ 是一个偶置换, 那么 $(12)\sigma$ 就是一个奇置换, 而且这样的对应是一对一的, 因此偶置换与奇置换的个数相等, 各等于 S_n 的一半. □

类似 A_3, 对一般的 n, 有

定理 7.18 记 S_n 中偶置换全体为 A_n, 则 A_n 是 S_n 的子群, 称为***交错群***.

证明 设 $\sigma,\ \tau$ 是任意两个偶置换, 那么

$$\phi(x_1, \cdots, x_n) \xrightarrow{\sigma} \phi(x_1, \cdots, x_n) \xrightarrow{\tau} \phi(x_1, \cdots, x_n),$$

所以$\tau\sigma$ 还是偶置换. 偶置换的逆 $\sigma^{-1} : \phi \Rightarrow \phi$ 仍是偶置换, 恒等置换当然是偶置换, 所以A_n 是一个群. □

为了更好地掌握交错群, 利用置换可分解为对换乘积这样的特点, 进一步分析交错群中元素的特征.

定理 7.19 除恒等置换外, 交错群 A_n 中任意置换 σ 均可分解为长度为 3 (可相交) 轮换乘积.

证明 根据定理7.9, 对 $\sigma \in A_n$, 可以分解为对换的乘积, 而每个对换是奇置换, 因此分解式中一定包含偶数个对换:

$$\sigma = \sigma_1\sigma_2\cdots\sigma_{2r},$$

将偶数个对换依次分为两两一组. 对 $\sigma_1\sigma_2$, 有下列三种情况:

(1)若 $\sigma_1 = \sigma_2$, 则 $\sigma_1\sigma_2 = e$ 是一个恒等置换.

(2)若 σ_1 和 σ_2 有一个字符相同, 不妨设 $\sigma_1 = (\alpha\beta)$, $\sigma_2 = (\beta\gamma)$, 则

$$\begin{aligned}\sigma_1\sigma_2 &= (\alpha\beta)(\beta\gamma)\\ &= \begin{pmatrix}\alpha & \beta & \gamma & \cdots\\ \beta & \alpha & \gamma & \cdots\end{pmatrix}\begin{pmatrix}\alpha & \beta & \gamma & \cdots\\ \alpha & \gamma & \beta & \cdots\end{pmatrix}\\ &= \begin{pmatrix}\alpha & \beta & \gamma & \cdots\\ \beta & \gamma & \alpha & \cdots\end{pmatrix} = (\alpha\beta\gamma).\end{aligned}$$

因此是一个长度为 3 的轮换, 这里省略号表示上下不发生变化的对应.

(3)若 σ_1 和 σ_2 无相同字符, 不妨设 $\sigma_1 = (\alpha\beta)$, $\sigma_2 = (\gamma\delta)$, 则

$$\sigma_1\sigma_2 = (\alpha\beta)(\gamma\delta) = (\alpha\beta)(\beta\gamma)(\beta\gamma)(\gamma\delta) = (\alpha\beta\gamma)(\beta\gamma\delta),$$

因此是两个长度为 3 轮换的乘积, 这里插入的对换满足 $(\beta\gamma)(\beta\gamma) = e$.

继续对余下对换的乘积 $\sigma_3\sigma_4\cdots\sigma_{2r}$ 进行类似讨论, 就得到定理结果. □

例 7.5.9 根据上述讨论, 可以简洁地把交错群 A_4 中12 个元素表示出来.

$$\begin{aligned}A_4 =\{&(1),\ (12)(34),\ (13)(24),\ (14)(23),\\ &(123),\ (124),\ (134),\ (234),\ (132),\ (142),\ (143),\ (243)\}.\end{aligned}$$

这里用 (1) 表示恒等置换, 两个无相同字符的对换乘积, 符合情况(3), 因此可以表示成长度为 3 的(可相交)轮换的乘积.

4° **循环群**

一般地, 对 n 阶有限群 G, 任取 $a \in G$, $a \neq e$, 那么

$$a,\ a^2,\ a^3,\cdots a^{n+1} \in G,$$

因 G 中只有 n 个元素, 所以上面 $n+1$ 个元素必有两个相等, 不妨设$a^i = a^j$, $i < j$, 推得 $a^{j-i} = e$, 也就是说, 对于有限群 G 中任何元素$a \neq e$, 一定存在正整数 m, 使得 a^m 是单位元. 根据最小数原理(第 1 讲§1.1), 一定存在最小正整数 r, 使得 $a^r = e$. 称 r 为 a 的**周期**. 一般来说, 不同元素有不同周期.

例 7.5.10 在 S_3 中, σ_2, σ_5 的周期为 3, $\sigma_2, \sigma_3, \sigma_4$ 周期为 2.

定理 7.20 *设 G 是 n 阶有限群, $a \in G$, $a \neq e$, r 是 a 的周期, 那么 $\{e, a, a^2, \cdots, a^{r-1}\}$ 是 G 的 r 阶的子群 (因此 $r \leqslant n$).*

证明 只要按定义验证即可. 例如对 $0 \leqslant i, j \leqslant r-1, a^i a^j = a^{i+j} = a^k$, $0 \leqslant k \leqslant r-1$ 满足 $(i+j) \equiv k \pmod{r}$. 而 a^i 的逆元为 a^{r-i}. □

定义 7.21 *设 G 是 n 阶有限群, $a \in G$, $a \neq e$, r 是 a 的周期, 称 $\{e, a, a^2, \cdots, a^{r-1}\}$ 是**由 a 生成 G 的循环子群**. 如果存在一个元素 a, 使得 a 的周期 $r = n$, 即*

$$G = \{e, a, a^2, \cdots, a^{n-1}\},$$

*那么称 G 为**循环群**.*

例 7.5.11 若 ξ 是 $z^n - 1 = 0$ 的本原单位根, 则 n 次单位根集合 D_n 中所有n 次单位根可由 ξ 的幂次生成:

$$D_n = \{\xi^0, \xi, \xi^2, \cdots, \xi^{n-1}\}.$$

因此 D_n 是循环群.

定理 7.22 *若群 G 的阶是素数, 则 G 一定是循环群.*

证明 设 $a \in G$, $a \neq e$ 并以 $r > 1$ 为周期, 因此$\{e, a, a^2, \cdots, a^{r-1}\}$ 是 G 的循环子群, 根据定理7.14 , $r \mid n$, 但 n 是素数, 所以$r = n$, 即 $G = \{e, a, a^2, \cdots, a^{n-1}\}$, 因此是循环群. □

例 7.5.12 在 S_n 中, 单位元 e 周期为1. 一个对换 (ij) 周期为 2: $(ij)^2 = e$. 一个轮换 $(i_1 i_2 \cdots i_d)$ 周期为 d: $(i_1 i_2 \cdots i_d)^d = I$. 置换

$$a = (12\cdots n) = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 2 & 3 & 4 & \cdots & n & 1 \end{pmatrix}$$

的周期是 n, $\{e, a, a^2, \cdots, a^{n-1}\}$ 是 S_n 的循环子群. 但是对 $n \geqslant 3$, S_n 的阶数 $n!$ 不可能是素数, 因此 S_n $(n \geqslant 3)$ 不会是循环群.

4° 正规子群

定义 7.23 *设 H 是 G 非平凡子群, 若对于任意的 $g \in G$, $h \in H$, 有 $g^{-1}hg \in H$, 则称 H 为 G 的**正规子群**.*

显然, 如果 G 是交换群, 那么 $g \in G$, $h \in H$, 有 $g^{-1}hg = h \in H$, 所以交换群的任何子群都是正规子群.

例 7.5.13 对称群 S_3 的子群 $A_3=\{\sigma_0,\sigma_2,\sigma_5\}$ 是正规子群. 只要对于 S_3 中其它3个元素

$$\sigma_1=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\ \sigma_3=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\ \sigma_4=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},$$

逐一验证 $g^{-1}hg\in A_3$ 对 $g=\sigma_1,\sigma_3,\sigma_4$ 和 $h=\sigma_0,\sigma_2,\sigma_5$ 成立, 那么就推出 A_3 是 S_3 的正规子群. 经验证有

$$\sigma_1^{-1}\sigma_2\sigma_1=\sigma_5,\ \sigma_1^{-1}\sigma_5\sigma_1=\sigma_2,\ \sigma_3^{-1}\sigma_2\sigma_3=\sigma_5,$$
$$\sigma_3^{-1}\sigma_5\sigma_3=\sigma_2,\ \sigma_4^{-1}\sigma_2\sigma_4=\sigma_5,\ \sigma_4^{-1}\sigma_5\sigma_4=\sigma_2,$$

例如,

$$\sigma_1^{-1}=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}^{-1}=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},$$

$$\begin{aligned}\sigma_1^{-1}\sigma_2\sigma_1&=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}^{-1}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\\&=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\sigma_5,\end{aligned}$$

所以 A_3 是 S_3 的正规子群.

其实, 一般情况下无需验证, 直接可证明下列结论.

定理 7.24 *交错群 A_n 是对称群 S_n 的正规子群.*

证明 对任意的 $\tau\in S_n$, $\sigma\in A_n$, τ 和 τ^{-1} 要么同是偶置换, 要么同是奇置换, 所以当 σ 是偶置换时, $\tau^{-1}\sigma\tau$ 一定是偶置换, 即 $\tau^{-1}\sigma\tau\in A_n$. □

定义 7.25 *若 H 是 G 的正规子群, 且 G 中不再存在包含 H 的非平凡正规子群, 则称 H 是G 的**极大正规子群**.*

例7.5.13中, 因为 A_3 的阶是 3, S_3 的阶是 6, 如果存在另一个正规子群 F, 使得 $A_3\subset F\subset S_3$, 那么 F 的阶 r 一定满足 $3<r<6$, 且 3 必须整除 r, r 必须整除 6, 这是不可能的, 所以 A_3 是 S_3 的极大正规子群. 一般情况下, 有

定理 7.26 *交错群 A_n 是对称群 S_n 的极大正规子群.*

证明 由于 A_n 的阶是$\dfrac{n!}{2}$, 所以

$$\frac{S_n\text{的阶}}{A_n\text{的阶}}=\frac{n!}{n!/2}=2,$$

如果存在另一个正规子群 F, 使得 $A_n\subset F\subset S_n$, 那么 F 的阶 r 一定满足

$$\frac{n!}{2}<r<n!,$$

并且r 能整除 $n!$, 但

$$\frac{n!}{r} < \frac{n!}{n!/2} = 2$$

推出 $r = n!$, 即 $F = S_n$. 因此不存在包含 A_n 的 S_n 的任何非平凡子群, 这样就得出 A_n 是 S_n 的极大正规子群. □

6° **可解群**

对于一个有限群 G, 如果 G_1 是 G 的极大正规子群, G_2 是 G_1 的极大正规子群, G_3 是 G_2 的极大正规子群, $\cdots$, 这样得到

$$G \supset G_1 \supset G_2 \supset \cdots \supset E,$$

其中 $E = \{e\}$ 必定是一个只包含单位元的群. 这样的一列群, 称为 G 的**合成群列**.

这里需要特别指出, 若 G_1 是 G 的正规子群, G_2 是 G_1 的正规子群, 并不能推出 G_2 是 G 的正规子群!

定义 7.27 设 G 的合成群列为

$$G \supset G_1 \supset G_2 \supset \cdots \supset E,$$

$n, n_1, n_2, \cdots, 1$ 分别是 $G, G_1, G_2, \cdots$, 的阶. 根据定理*7.14*,

$$\frac{n}{n_1},\ \frac{n_1}{n_2},\ \frac{n_2}{n_3}, \cdots$$

是一列正整数, 称为 G 的***组合因数***.

如果一个有限群 G 组合因数都是素数, 那么称 G 为***可解群***.

例 7.5.14 S_3 和 S_4 是可解群.

这是因为 A_3 是 S_3 极大正规子群, A_3 中不再包含任何非平凡正规子群, 因此 S_3 的合成群列为

$$S_3 \supset A_3 \supset E,$$

组合因数

$$\frac{S_3\text{的阶}}{A_3\text{的阶}} = \frac{6}{3} = 2, \quad \frac{A_3\text{的阶}}{E\text{的阶}} = 3,$$

都是素数, 所以S_3 是可解群.

在例7.5.9 中, A_4 是 S_4 极大正规子群, 可以验证, A_4 中子集合

$$K = \{(1),\ (12)(34),\ (13)(24),\ (14)(23)\}$$

是 A_4 极大正规子群, 而

$$H = \{(1),\ (12)(34)\}$$

是 K 极大正规子群. 注意以下两点, 一是 H 是 K 的正规子群, 但不是 A_4 的正规子群, 二是K 中与 H 的同阶的正规子群不唯一. 这样就有

$$S_4 \supset A_4 \supset K \supset H \supset E$$

它们的组合因数

$$\frac{S_4\text{的阶}}{A_4\text{的阶}}=2,\quad \frac{A_4\text{的阶}}{K\text{的阶}}=3,\ \frac{K\text{的阶}}{H\text{的阶}}=2,\ \frac{H\text{的阶}}{E\text{的阶}}=2,$$

都是素数, 而且在 S_4, A_4, K, H, E 不可能再插入任何正规子群, 所以它们是 S_4 的合成群列, S_4 是可解群.

定义 7.28 *若群 G 中无非平凡正规子群, 则称 G 为**单群**.*

显然, 若群 G 的阶是素数, 那么由定理7.14, G 没有非平凡子群, 当然也不会有非平凡正规子群. 例如 A_3 的阶是 3, 所以一定是单群. A_4 不是单群. 但是, 并非有限单群的阶数一定是素数.

定理 7.29 *当 $n \geqslant 5$ 时, A_n 是单群.*

由此很快推出

定理 7.30

当 $n \leqslant 4$ 时, 对称群 S_n 是可解的.

当 $n \geqslant 5$ 时, 对称群 S_n 是不可解的.

定理中关于 $n \leqslant 4$ 的情形已经在例7.5.14中给出. 当 $n \geqslant 5$ 时, 因为 A_n 是 S_n 的极大正规子群, 由定理7.29 知, A_n 又是单群, 即 A_n 中不存在非平凡的正规子群. 这样 S_n 的合成群列只有

$$S_n \supset A_n \supset E,$$

(E 是只包含单位元的平凡群), 它们的阶分别为 $n!,\ \dfrac{n!}{2},\ 1$, 因而组合因数为

$$\frac{S_n\text{的阶}}{A_n\text{的阶}}=2,\quad \frac{A_n\text{的阶}}{E\text{的阶}}=\frac{n!}{2},$$

显然, 当 $n \geqslant 5$ 时, $\dfrac{n!}{2}$ 不可能是素数, 所以得到 S_n 不可解.

定理7.29 和定理7.30 是最终解决五次及五次以上代数方程不能够用代数方法求解的关键定理. 虽然在§7.3 中用置换求解三次代数方程时, 已经体会到S_3 的可解性 $S_3 \supset A_3 \supset E$ 在求解中扮演的特殊角色. 但是对于彻底解决代数方程求解问题还有很长路要走. 本专题目的也就仅限于从求解这样具体问题出发, 如何引进群的概念, 进一步理论可参考有关书籍. 最后以定理7.29 的证明作为本专题的结束.

定理7.29 的证明 设 $n \geqslant 5$, 为了证明 A_n 没有非平凡正规子群 , 我们将充分利用置换分解为轮换乘积这个事实.

假设 A_n 有E 以外正规子群 H, 下面将证明 H 只能等于 A_n 自身.

取 $h \in H,\ h \neq e$, 并设 h 是使得 $\{1,2,\cdots,n\}$ 中数字发生变化最少一个置换. 根据定理7.9, h 能够分解为不相交轮换的乘积.

$$h = \sigma_1 \cdots \sigma_r$$

其中 $\sigma_j,\ j = 1,\cdots,r$ 是互不相交轮换. 下面将分成几个步骤进行讨论.

（1）在 h 的上述分解中, 各轮换长度一定相等.

采用反证法, 若不然, 在轮换 $\sigma_j,\ j = 1,\cdots,r$ 中, 必有一个长度最小, 因为各轮换不相交, 因此可以将长度最小的交换到最左边, 因此不妨设 $\sigma_1 = (\alpha_1\alpha_2\cdots\alpha_k)$ 为长度最小的轮换, 长度为 k. 利用性质7.8, 有

$$h^k = \sigma_1^k\sigma_2^k\cdots\sigma_r^k = \sigma_2^k\cdots\sigma_r^k = h_1,$$

这里 $h_1 = \sigma_2^k\cdots\sigma_r^k$ 表示h 中不相交其他轮换 k 次方的乘积. 因为 σ_1 长度最小, 所以在 $\sigma_2,\cdots,\sigma_r$ 中, 至少有一个使得 $\sigma_j^k \neq e$. 所以 $h_1 \neq e$. 因为 H 是子群, 所以$h_1 = h^k \in H$, 但是 h_1 使得 $\{1,2,\cdots,n\}$ 中数字发生变化的个数比 h 使得 $\{1,2,\cdots,n\}$ 中数字发生变化至少少了 $\alpha_1,\alpha_2,\cdots\alpha_k$ 等 k 个,这与 h 的选取矛盾, 因此在 h 分解为不相交轮换乘积中, 各轮换长度一定相等.

（2） 在 h 分解为不相交轮换乘积中, 各轮换长度不会超过 3.

仍然采取反证法, 若不然, 在 $h = \sigma_1\cdots\sigma_r$ 中, 有一个轮换长度超过 3, 不妨设 $\sigma_1 = (1234\cdots)$（对一般情况 $\sigma_1 = (\alpha_1\alpha_2\alpha_3\alpha_4\cdots)$, 证明完全类似）, 记 $h = (1234\cdots)h_1$ 这里 h_1 是与 $(1234\cdots)$ 不相交其他轮换的乘积. 令偶置换 $g = (234) \in A_n$, 那么 g 与 h_1 不相交因此乘法可交换, 令

$$\begin{aligned} h_2 = g^{-1}hg &= g^{-1}(1234\cdots)h_1g = g^{-1}(1234\cdots)gh_1 \\ &= (243)(1234\cdots)(234)h_1 = (1423\cdots)h_1 \end{aligned}$$

这里 $h_2 = g^{-1}hg \in H$, 所以 $hh_2^{-1} \in H$, 但是

$$hh_2^{-1} = (1234\cdots)h_1((1423\cdots)h_1)^{-1} = (1234\cdots)(1423\cdots)^{-1} = (143),$$

所以置换 hh_2^{-1} 改变的数字少于 h 改变的数字, 这与 h 的定义矛盾.

（3）h 只能是一个轮换, 而不可能是多个轮换的乘积.

由前面两步, 我们已经知道 h 的分解只能由两种可能, 一是分解为长度为2 不相交轮换（对换）乘积, 二是分解为长度为3 不相交轮换乘积. 我们将逐一排除上述两种可能性.

第一种可能性的排除: 不妨设 $h = (12)(34)$, 也就是h 使得 $\{1,2,\cdots,n\}$ 中4个数字

发生变化. 因 $n>4$, 取偶置换 $g=(125)\in A_n$, 有

$$hg^{-1}hg=(12)(34)(152)(12)(34)(125)=(152),$$

它使得 $\{1,2,\cdots,n\}$ 中3个数字发生变化. 但是 $hg^{-1}hg\in H$, 因此与 h 的选取矛盾.

第二种可能性的排除: 不妨设 $h=(123)(456)$, 也就是h 使得 $\{1,2,\cdots,n\}$ 中6个数字发生变化. 仍然取偶置换 $g=(125)\in A_n$, 则

$$hg^{-1}hg=(24356)\in H,$$

它使得 $\{1,2,\cdots,n\}$ 中5个数字发生变化, 因此与 h 的选取矛盾.

一般情况下排除上述两种可能的方法完全类似.

总结上面讨论, 我们证明了如果 h 是 H 中使得 $\{1,2,\cdots,n\}$ 改变最少者, 那么 h 只能是

$$h=(\alpha_1\alpha_2),\ \text{或}\ h=(\alpha_1\alpha_2\alpha_3),$$

但是 $h\in H\subset A_n$ 是一个偶置换, 所以 h 只能是

$$h=(\alpha_1\alpha_2\alpha_3).$$

对于任意一个长度为 3 的轮换 $(\beta_1\beta_2\beta_3)$, 设偶置换

$$g=\begin{pmatrix}\alpha_1&\alpha_2&\alpha_3\\ \beta_1&\beta_2&\beta_3\end{pmatrix}$$

因为 H 是A_n 规范子群, 所以 $g^{-1}hg\in H$, 这样就推出

$$(\beta_1\beta_2\beta_3)=\begin{pmatrix}\beta_1&\beta_2&\beta_3\\ \alpha_1&\alpha_2&\alpha_3\end{pmatrix}\begin{pmatrix}\alpha_1&\alpha_2&\alpha_3\\ \alpha_2&\alpha_3&\alpha_1\end{pmatrix}\begin{pmatrix}\alpha_1&\alpha_2&\alpha_3\\ \beta_1&\beta_2&\beta_3\end{pmatrix}=g^{-1}hg$$

所以, 任何一个长度为 3 的轮换属于 H. 再根据定理7.19, A_n 中置换可分解为长度为3轮换的乘积, 因此也属于 H. 最终就证明了 $H=A_n$. □

第 7 讲习题

1. 设 G 是一个有限群, H 是 G 的非空子集. 若对任意的 $a,b\in H$, 有 $ab\in H$, 则 H 一定是 G 的子群.

   提示: 要证明 H 是 G 的子群, 就是要根据已知条件, 证明单位元 $e\in H$, 以及 $a^{-1}\in H$ 对任意的 $a\in H$ 成立. 取 $a\in H$, 若 $a=e$, 显然 e 和 $e^{-1}=e\in H$. 若 $a\neq e$, 根据条件 $a\cdot a=a^2\in H$, 进而推出 $\{a,a^2,\cdots,a^n,\cdots\}\subset H$. 再根据 G 是有限群的条件, 推出 e 和 $a^{-1}\in H$.

2. 证明群 G 的两个正规子群的交仍是正规子群.

3. 设 G 是一个群, $g\in G$, 试证下列 $G\longrightarrow G$ 的映射是同构映射 (称为 G 的自同构)

$$a\longmapsto\varphi(a)=g^{-1}ag,\quad a\in G.$$

4. 设 G 是有限群, $a,b\in G$, 满足 $ab=ab^{-1}$. 若 a 的周期为奇数, 求证: $b^2=e$ (e 为 G 中单位元) .

   提示: 设有非负整数 k, 使得 $a^{2k+1}=e$, 由条件可知

$$a=bab,\ a=b^{-1}ab^{-1},$$

   因此 $a^2=ba^2b^{-1}$ 即可证得.

5. 设 $G=\{a_1,a_2,\cdots,a_n\}$ 是一个有限 Abel 群, 证明元素 $a=a_1a_2\cdots a_n$ 满足 $a^2=e$.

   提示: 注意到 G 是有限群, 所以

$$\{a_1^{-1},a_2^{-1},\cdots,a_n^{-1}\}=\{a_1,a_2,\cdots,a_n\}$$

   再利用可交换性即可征得.

6. 设 G 是一个阶超过 3 的有限群, 对任意的 $g\in G$, 都有 $g^2=e$, 证明: G 是一个 Abel 群, 且 G 中所有元素的乘积等于 e.

   提示: 根据条件可知任意 $g\in G$, 都有 $g=g^{-1}$, 因此

$$g_1g_2=(g_1g_2)^{-1}=g_2^{-1}g_1^{-1}=g_2g_1.$$

   又因为 G 中元素个数超过 3, 所以存在 $a,b\in G$, 且 $a\neq b$, $a\neq e,b\neq e$. 记 $c=ab$, 那么可以验证 $c\neq a,c\neq b,c\neq e$. 且 $H=\{e,a,b,c\}$ 是 G 的子群. 若 $G=H$, 可直接验证 G 的所有元素乘积等于 e; 若 H 是 G 的非平凡子群, 根据定理7.15, G 可分解为两两不交的若干个陪集的并. 注意到利用交换性, 每个陪集 $gH=\{g,ga,gb,gc\}$ 的元素相乘 $g\cdot ga\cdot gb\cdot gc=g^4=e^2=e$, 所以可得本题结果.

7. 证明: 正有理数构成的群 (见例7.5.1) $\mathbb{Q}_+ = \{r \mid r > 0,\ r \in \mathbb{Q}\}$ 同构于自己的真子群.

   提示: 考虑 $\mathbb{Q}_+$ 的子集合 $A = \{r^2 \mid r \in \mathbb{Q}_+\}$. 首先验证$A$ 是 $\mathbb{Q}_+$ 真子集. 其次验证 A 是 $\mathbb{Q}_+$ 的子群. 最后验证

$$\varphi : x \longmapsto x^2 \ (x \in \mathbb{Q}_+)$$

   是$\mathbb{Q}_+ \longrightarrow A$ 的同构映射.

8. 类似例7.5.4, 试证保持正四边形不变的变换所构成的群是 S_4 的子群, 阶数为 $2 \cdot 4 = 8$.

   提示: 如图 *7.1*, 不难发现保持正四边形不变的变换就是四个角 A, B, C, D 之间的置换, 其中旋转变换可表示为 A, B, C, D 的轮换, 而关于对称轴的反射可表示为对换的乘积, 例如关于对称轴X 的反射为 $(1, 4)(2, 3)$.

   注意, 表示正四边形对称性的群是 S_4 的子群, 而 S_4 表示的是空间正四面体的对称性.

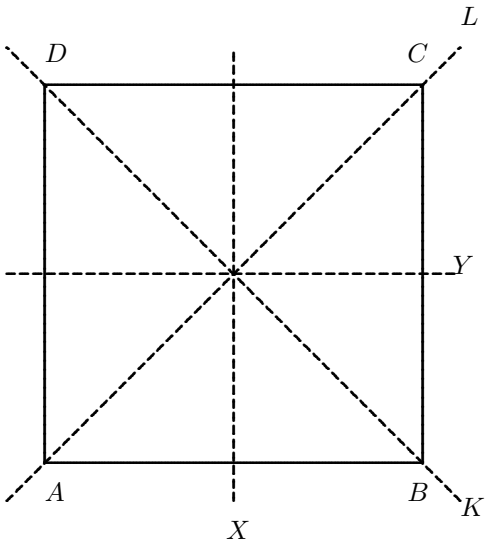


图 7.2

9. 求证不等边长的长方形的对称群有四个元素.