



数学书籍汇总

读书笔记

作者：虞朝阳

组织：西北工业大学

版本：1.00

Wir müssen wissen, wir werden wissen. (我们必须知道，我们必将知道) - David.Hilbert

前言

这里收集了大量的数学书籍，大部分都是比较经典的，包含了代数，几何，分析，组合数学等各个分支的数学书籍。原著如果是英文的，将会被翻译成中文，所以收集整理的进度上不可能会太快。

我希望最终能形成一本书：尽早引入一些抽象代数的概念，能够尽量给出各种应用。初步设想从集合的一些基础知识出发，引入基本的群环域的概念，从自然数出发，构造整数，然后引入一些数论的基础知识，进一步构造有理数，实数，复数，然后开始讨论一些微积分。从线性代数和几何角度，再次出发。

目录

Preface	A
第一部分 近世代数概论	1
1 整数	3
1.1 交换环, 整环	3
1.2 交换环的基本性质	4
1.3 有序整环的性质	6
1.4 良序原则	7
1.5 数学归纳法, 指数定律	8
1.6 可除性	9
1.7 欧几里得算法	10
1.8 算术基本定理	12
1.9 同余式	13
1.10 环 \mathbb{Z}_n	15
1.11 集合, 函数, 关系	16
1.12 同构与自同构	17
2 有理数和域	19
2.1 域的定义	19
2.2 有理数域的构造	21
2.3 联立线性方程	24
2.4 有序域	26
2.5 正整数公设	28
2.6 皮亚诺公设	30
3 多项式	33
3.1 多项式形式	33
3.2 多项式函数	35
3.3 交换环的同态	38
3.4 多元多项式	39
3.5 辗转相除法	40
3.6 单位与相伴	42
3.7 不可约多项式	43
3.8 唯一因子分解定理	44

3.9 其他唯一因子分解整环	46
3.10 爱森斯坦不可约判别法则	48
3.11 部分分式	50
4 实数	52
4.1 毕达哥拉斯二难推论	52
4.2 上界与下界	53
4.3 实数公设	54
4.4 多项式方程的根	55
第四章习题	58
4.5 戴德金分割	58
第四章习题	60
5 复数	61
5.1 复数的定义	61
第五章习题	62
5.2 复平面	63
第五章习题	65
5.3 代数基本定理	65
第五章习题	67
5.4 共轭数与实多项式	68
第五章习题	69
5.5 二次方程与三次方程	69
第五章习题	71
5.6 四次方程的根式解法	72
第五章习题	73
5.7 稳定型方程	73
第五章习题	73
6 群	75
6.1 正方形的对称	75
第六章习题	76
6.2 变换群	76
第六章习题	79
6.3 其他例子	81
第六章习题	81
6.4 抽象群	82
第六章习题	84
6.5 同构	85

第六章习题	87
6.6 循环群	88
第六章习题	89
6.7 子群	90
第六章习题	92
6.8 拉格朗日定理	93
第六章习题	94
6.9 置换群	95
7 几何	98
8 几何	99
9 几何	100
10 几何	101
第二部分 代数	102
11 矩阵	104
11.1 基本运算	104
12 群	105
13 向量空间	106
14 线性算子	107
15 线性算子的应用	108
第三部分 基础代数	109
16 集合论里的概念 整数	111
17 么半群和群	112
18 环	113
19 主理想整环上的模	114
20 方程的 Galois 理论	115

第四部分 微积分	116
21 数的基本性质	118
第五部分 流形上的微积分	119
22 欧几里得空间上的函数	121
22.1 范数与内积	121
第二十二章 习题	123
22.2 欧几里得空间的子集	128
第二十二章 习题	130
22.3 函数与连续性	134
第二十二章 习题	135
23 微分	137
23.1 基本定义	137
第二十三章 习题	138
23.2 基本定理	139
第二十三章 习题	142
23.3 偏导数	144
第二十三章 习题	145
23.4 导数	147
24 积分	150
24.1 基本定义	150
24.2 测度零和容度零	150
24.3 可积函数	150
24.4 富比尼定理	150
第二十四章 习题	150
25 链上的积分	151
26 流形上的积分	152
第六部分 多元微积分	153
27 欧氏空间	155
27.1 向量空间	155

第七部分 数学分析	157
28 实数系与复数系	159
28.1 引言	159
28.2 域公理	159
28.3 序公理	159
29 集合论的一些基本概念	160
30 点集拓扑初步	161
第八部分 单复变函数	162
31 复数系	164
31.1 实数	164
31.2 复数域	164
31.3 复平面	165
31.4 复数的极坐标表示与复数的方根	167
31.5 复平面上的直线和半平面	168
31.6 扩充平面及其球面表示	169
32 度量空间与 \mathbb{C} 的拓扑	171
32.1 度量空间的定义和例子	171
32.2 连通性	174
32.3 序列与完备性	177
32.4 紧性	180
32.5 连续性	184
32.6 一致收敛性	188
33 解析函数的初等性质和例子	190
33.1 幂级数	190
33.2 解析函数	193
第三十三章 习题	202
33.3 作为映照得解析函数. Möbius 变换	203
第三十三章 习题	211
34 复积分	214
34.1 Riemann-Stieltjes 积分	214
第三十四章 习题	223
34.2 解析函数的幂级数表示	223

35 Runge 定理	224
35.1 Runge 定理	224
35.2 单连通性	224
35.3 Mittag-Leffler 定理	224
36 调和函数	225
 第九部分 数学分析	 226
37 实数系	228
37.1 整数, 有理数与无理数	228
37.2 Dedekind 分割	231
37.3 不等式	231
37.4 实数列	231
37.5 实数级数	231
37.6 有规则的小数	231
38 连续性	232
39 微分与积分	233
40 一致收敛性	234
41 度量空间	235

第一部分

近世代数概论

《近世代数概论》的作者是 G. 伯克霍夫和 S. 麦克莱恩. 参考: [1].

第一章 整数

1.1 交换环, 整环

近世代数第一次揭示了数学系统的多变性和丰富性. 本书从最基本也是最古老的正整数系统 (整数系统, 记为 \mathbb{Z}) 开始.

首先假定加法和乘法的八个公设, 这些公设不仅对整数成立, 而且对于很多数学系统都成立, 例如所有有理数, 所有实数, 所有复数, 所有多项式, 任意已知区间上的连续函数.

定义 1.1. 交换环

设 R 是由元素 a, b, c, \dots 组成的集合, 在 R 上定义了任意两个元素 a 与 b 的和 $a+b$ 及积 ab . 如果下列公设 (i)-(viii) 成立, 那么 R 称为交换环:

(i) 封闭性. 若 $a, b \in R$, 则 $a+b \in R, ab \in R$.

(ii) 唯一性. 若 R 中 $a = a'$ 且 $b = b'$, 则 $a+b = a'+b'$ 以及 $ab = a'b'$.

(iii) 交换律. 对 R 中一切 a 与 b ,

$$a+b = b+a, \quad ab = ba.$$

(iv) 对一切 $a, b, c \in R$,

$$a+(b+c) = (a+b)+c,$$

$$a(bc) = (ab)c.$$

(v) 分配律. 对一切 $a, b, c \in R$,

$$a(b+c) = ab+ac.$$

(vi) 零. R 中包含元素 0 , 使得对于一切 $a \in R$,

$$a+0 = a.$$

(vii) 单位元素. R 中包含元素 $1 \neq 0$, 使得对于一切 $a \in R$,

$$a1 = a.$$

(viii) 加法逆元素. 对于每个 $a \in R$, 方程

$$a+x = 0$$

在 R 中有解 x . x 称为 a 的逆元素, 并记为 $-a$.



首先定义中的 $1 \neq 0$, 排除只包含一个元素 0 的情形. 其次, 0 和 1 其实起着相似的作用, 所以可以分别称为加法和乘法单位元. 第三, 交换中只保证了加法存在逆元素, 对于乘法没有这个保证, 这样一来, 在整数集合 \mathbb{Z} 中, $c \neq 0$, 且 $ca = cb$, 则必有 $a = b$, 这个结论对于一般的交换环不成立 (例如区间上全体实函数组成的集合). 为此引入整环的概念.

定义 1.2. 整环

满足下面附加公设的交换环是整环:

(ix) 消去律. 若 $c \neq 0$ 且 $ca = cb$, 则 $a = b$.



整环并不保证每个非零元素存在乘法逆元素. 不过后面会证明 1 是有乘法逆元素的 (1 自身), -1 也有乘法逆元素 -1 .

这里应该多举一些交换环和整环的例子.

集合 $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} | a, b \in \mathbb{Z}\}$ 是一个整环, $a + b\sqrt{2} = c + d\sqrt{2}$ 当且仅当 $a = c$ 且 $b = d$, 加法和乘法分别定义为:

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2},$$

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}.$$

1.2 交换环的基本性质

当我们想要得到对于整个代数系统都正确的结论时, 必须多加小心, 我们必须确信, 所有的证明只用到明显列出的公设和一般逻辑法则, 其中最基本的逻辑法则是相等关系的三个基本定律: 对一切 a, b, c 有

- 自反律 $a = a$.
- 对称律若 $a = b$, 则 $b = a$.
- 传递律若 $a = b$ 且 $b = c$, 则 $a = c$.

下面任意交换环都成立的一些基本法则. 证明的时候只是需要注意只能使用公设或者前面证明的结论. 这里省略, 参考书本.

推论 1.1. 法则 1

对一切 $a, b, c \in R$, 有

$$(a + b)c = ac + bc.$$



这条法则可称为右分配律, 可与公设 (v) 对比, 公设 (v) 是左分配律.

推论 1.2. 法则 2

对一切 $a \in R$, $0 + a = a$ 且 $1a = a$.

**推论 1.3. 法则 3**

如果 $z \in R$ 满足: 对一切 $a \in R$, $a + z = a$, 那么 $z = 0$.



这个法则说明加法单位元素 0 的唯一性.

推论 1.4. 法则 4

对一切 $a, b, c \in R$ 成立: 由 $a + b = a + c$, 可推出 $b = c$.



这个法则称为加法消去律.

推论 1.5. 法则 5

对一切 $a \in R$, 存在唯一的 $x \in R$ 满足 $a + x = 0$.



公设 (viii) 只保证了存在性, 这个法则说明唯一性.

推论 1.6. 法则 6

对一切 $a, b \in R$, 存在唯一的 $x \in R$ 使得 $a + x = b$.



这个法则说明减法是可能的而且差是唯一的.

推论 1.7. 法则 7

对一切 $a \in R$, $a \cdot 0 = 0 = 0 \cdot a$.

**推论 1.8. 法则 8**

如果 $u \in R$ 满足: 对一切 $a \in R$, $au = a$, 那么 $u = 1$.



这个法则说明乘法单位元素 1 的唯一性.

推论 1.9. 法则 9

对一切 $a, b \in R$, $(-a)(-b) = ab$.



特别的有 $(-1)(-1) = 1$. 这个证明起来稍微麻烦一点, 不过只需要注意到 $-a, -b$ 的定义, 一步一步来还是可以得到的. 只需要考虑

$$[ab + a(-b)] + (-a)(-b) = ab + [a(-b) + (-a)(-b)]$$

即可. 中间的 $a(-b)$ 可以换成 $(-a)b$. 另外需要使用法则 7.

还有一条基本的代数定律是用于解二次方程的: 若 $ab = 0$, 则或者 $a = 0$ 或者 $b = 0$. 遗憾的是, 这个断语不是对一切交换环成立的. 但是在任意的整环 D 中成立 (可以根据乘法消去律证明). 反之, 在任意交换环中, 从这个断语可以得到消去律. 若 $a \neq 0$, 从 $ab = ac$ 有 $ab - ac = a(b - c) = 0$, 可得 $b - c = 0$ 从而 $b = c$. 于是我们有:

定理 1.1

在交换环中, 乘法消去律等价于“非零元素之积不为零”这个命题.



这里所谓“非零元素之积不为零”这个命题, 可以用符号表示为: $a \neq 0, b \neq 0$, 则必有 $ab \neq 0$. 我们把满足 $ab = 0$ 的非零元素 a, b 称为零因子. 因此交换环中的消去律等价于“ R 中不包含零因子”.

前面提到 $\mathbb{Z}[\sqrt{2}]$ 是整环, 需要证明在 $\mathbb{Z}[\sqrt{2}]$ 中成立消去律, 这个可以使用这个定理来完成. 证明过程参考书本, 需要注意, 这里需要用到结论 $\sqrt{2}$ 不是有理数, 也就是不能表示为 a/b 的形式, 这里 a, b 是整数.

如果承认 $\sqrt{2}$ 是实数, 并且承认所有实数的集合构成整环, 那么借助于子整环的概念可以非常容易证明 $\mathbb{Z}[\sqrt{2}]$ 是整环.

定义 1.3. 子整环

整环 D 的子整环是 D 的子集, 它对于同一种加法和乘法运算也是整环.



子集 S 是子整环的充分必要条件是: S 包含 0 和 1; S 包含其中任意元素 a 的加法逆元素; S 包含其中任意两个元素 a 与 b 的和 $a + b$ 以及积 ab . 换成集合语言, 可以描述如下:

- $0 \in S, 1 \in S$;
- 对任意 $a \in S$, 必有 $-a \in S$;
- 对任意 $a, b \in S$, 有 $a + b \in S, ab \in S$.

1.3 有序整环的性质

所有整数组成的环 \mathbb{Z} 在数学中起着独特的作用, 因此我们将研究它的特殊性质. 乘法交换律和消去律仅仅是其中两个, 许多其他性质都来源于整数有可能被排成通常的次序:

$$\cdots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \cdots$$

这个次序常用关系 $a < b$ 表示. 关系 $a < b$ 成立当且仅当差 $b - a$ 为正整数. 假设正整数 $1, 2, 3, \cdots$ 集合的下列三个性质作为公设.

- 加法律两个正整数的和是正整数.
- 乘法律两个正整数的积是正整数.
- 三分律对于已知整数 a , 下面三种情况中有且仅有一个成立: 或者 a 为正整数, 或者 $a = 0$, 或者 $-a$ 为正整数.

请注意, 这里相当于根据这三个公设定义了正整数集合, 也就是只要 \mathbb{Z} 的子集 \mathbb{Z}^+ 满足这三个公设的就可以作为 \mathbb{Z} 的正整数集合. 按照通常的加法, 乘法, 应该和我们以前学到的是一致的. 有必要给这样的整环一个单独的名称.

定义 1.4. 有序整环

如果整环 D 中存在某些被称为正元素的元素, 它们满足类似于上面对整数指出的加法, 乘法和三分律这三个公设, 那么称 D 为有序整环.



明显, 整数环 \mathbb{Z} , 有理数环 \mathbb{Q} , 实数环 \mathbb{R} 都是有序整环. 所有复数构成的集合是整环, 但是无法定义类似整数的序关系, 不是有序整环.

定理 1.2

在任意有序整环中, 一切非零元素的平方都是正的.



证明使用三分律以及前面的法则 9 即可. 注意所谓平方, 意指 $a^2 = a \cdot a$.

由此定理, 立即可以得到 $1 = 1^2$ 是正的. 从而可以证明在有序整环中 $x^2 + 1 = 0$ 无解, 也说明所有复数无法构成有序整环.

定义 1.5. 大于, 小于关系

在有序整环中, $a < b$ 和 $b > a$ 这两个等价的说法都意味着 $b - a$ 是正的, 还有 $a \leq b$ 的意思是 $a < b$ 或者 $a = b$.



根据这个定义, 正元素 a 可以描述为大于零的元素, 元素 $b < 0$ 称为负元素. 从定义还可以得出“小于关系”的传递律:

- 传递律若 $a < b$ 且 $b < c$, 则 $a < c$.

证明直接使用定义以及加法律即可. 事实上, 根据定义以及正元素的三个公设, 正好对应到不等式的三个性质:

- 不等式两边同时加上一个元素若 $a < b$, 则 $a + c < b + c$.
- 不等式两边同时乘以一个正元素若 $a < b$ 且 $c > 0$, 则 $ac < bc$.
- 三分律对任意 a 和 b , 三个关系式 $a < b$, $a = b$ 和 $a > b$ 中有且仅有一个成立.

证明不难, 需要注意加上一个元素的时候, 对这个元素没有限制, 但是乘以一个元素的时候, 要求这个元素必须是正元素, 事实上, 乘以负元素的话, 不等号反向.

定义 1.6. 绝对值

在有序整环中, 当元素 a 为 0 时, 它的绝对值 $|a|$ 是 0; 否则 $|a|$ 是元素对 $a, -a$ 中的正元素.



也就是 a 的绝对值可以表示如下:

$$|a| = \begin{cases} a, & a \geq 0 \\ -a, & a < 0 \end{cases}$$

适当的分情况讨论, 可以得到和的绝对值与积的绝对值的定律:

$$|a + b| \leq |a| + |b|; \quad |ab| = |a||b|. \quad (1.3.1)$$

和的绝对值的定律也可以这样证明:

$$-|a| \leq a \leq |a| \text{ 且 } -|b| \leq b \leq |b|$$

于是有

$$-(|a| + |b|) \leq a + b \leq |a| + |b|,$$

由此得证.

1.4 良序原则

如果有序整环的子集 S 的每个非空子集都包含最小元素, 那么 S 成为良序的. 利用这个概念我们可以阐述整数的重要性质, 这性质在特征上不是代数的, 并且是其他数系不具备的.

- 良序原则全体正整数的集合是良序的.

换句话说, 正整数的任意非空集合 C 包含某最小元素 $m \in C$, 使 C 中的 c 总有 $m \leq c$. 不过这里有一点疑惑, 本书中这个良序原理是作为公理来接受的吗? 还是需要证明? 看来

需要看其他书了解一下.

定理 1.3

0 和 1 之间没有整数.



这个证明有点意思: 假设存在适合 $0 < c < 1$ 的任意整数 c , 那么所有这种整数的集合 C 是非空的. 根据良序原则, 这个集合存在最小整数 m , 并且 $0 < m < 1$. 用正数 m 乘不等式两边, 得到 $0 < m^2 < m$, 于是 m^2 是集合 C 中的另一个整数, 它小于已假定的 C 中的最小元素 m , 这个矛盾导出定理成立.

定理 1.4

如果正整数的一个集合 S 包含 1, 并且当它包含 n 时必包含 $n+1$, 那么集合 S 包含任意正整数.



证明使用良序原则. 由那些不包含于 S 中的正数组成的集合 S' , 证明 S' 是空集即可.

1.5 数学归纳法, 指数定律

现在我们可以按加法, 乘法及序完整地列出全体整数集合的基本性质, 今后我们假定全体整数构成有序整环 \mathbb{Z} , 其中所有正元素的集合是良序的. 全体整数的集合的其他每个数学性质, 可以由此通过严格的逻辑推导来证明. 特别的, 可以导出非常重要的

- **数学归纳法原理** 设命题 $P(n)$ 与每个正整数 n 有关, 它或者正确, 或者错误. 如果 (i) $P(1)$ 是正确的, (ii) 对一切 k , 由 $P(k)$ 推出 $P(k+1)$, 那么 $P(n)$ 对一切正整数 n 都是正确的.

只需要考虑集合 $C = \{k | P(k) \text{ 成立}\}$, 这个集合满足前面的定理 1.4 的条件.

现在用归纳的方法来证明在任意交换环中成立的各种定律. 首先用它来形式地建立任意 n 个被加数的一般分配律.

$$a(b_1 + b_2 + \cdots + b_n) = ab_1 + ab_2 + \cdots + ab_n. \quad (1.5.1)$$

为明确起见, 定义累加和 $b_1 + b_2 + \cdots + b_n$ 如下:

$$b_1 + b_2 + b_3 = (b_1 + b_2) + b_3,$$

$$b_1 + b_2 + b_3 + b_4 = [(b_1 + b_2) + b_3] + b_4.$$

一般的通过递推公式:

$$b_1 + \cdots + b_k + b_{k+1} = (b_1 + \cdots + b_k) + b_{k+1}. \quad (1.5.2)$$

证明使用数学归纳法即可. 类似的但更为复杂的归纳论证将得到一般结合律, 它断言: 和 $b_1 + \cdots + b_k$ 或者积 $b_1 \cdots b_k$ 不管把括号括在哪里都有相同的值. 应用这个结果和 1.7.1, 可以建立双边一般的分配律:

$$\begin{aligned} & (a_1 + \cdots + a_m)(b_1 + \cdots + b_n) \\ &= a_1 b_1 + \cdots + a_1 b_n + \cdots + a_m b_1 + \cdots + a_m b_n. \end{aligned}$$

注意, 根据一般结合律和一般交换律, k 个项的和不管项的次序与分组如何总有相同的值.

任意交换环 R 中的正整指数也可以归纳定义. 如果 n 为正整数, 则幂 a^n 表示 n 个因子的积 $aa \cdots a$, 这也可以递归定义:

$$a^1 = a, a^{n+1} = a^n a. \quad (\forall a \in R) \quad (1.5.3)$$

由这些定义, 我们可以对任意正整指数 m 和 n 证明下面常用的定律:

$$a^m a^n = a^{m+n}, \quad (1.5.4)$$

$$(a^m)^n = a^{mn}, \quad (ab)^m = a^m b^m. \quad (1.5.5)$$

证明同样使用数学归纳法和递归定义即可.

最后, 我们证明二项公式在任意交换环 R 上成立. 首先用递推公式

$$0! = 1, \quad (n+1)! = n!(n+1),$$

定义非负整数上的阶乘函数 $n!$, 然后对 \mathbb{Z} 中的 $n \geq 0$, 类似的用

$$\binom{n}{0} = \binom{n}{n} = 1, \quad \binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$$

定义二项系数. 由这些定义, 再对 n 用归纳法, 得到

$$\begin{aligned} (x+y)^n &= x^n + nx^{n-1}y + \cdots + \binom{n}{k}x^{n-k}y^k + \cdots + y^n \\ &= \sum_{k=0}^n \binom{n}{k}x^{n-k}y^k. \end{aligned} \quad (1.5.6)$$

和

$$k!(n-k)!\binom{n}{k} = n! \quad (1.5.7)$$

也就是

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

数学归纳原理允许我们在证明 $P(n+1)$ 时, 随意假定 $P(n)$ 的正确性, 我们指出, 人们甚至可以对一切 $k \leq n$ 假定 $P(k)$ 的正确性, 这称为

- **数学归纳法第二原理** 设命题 $P(n)$ 与每个正整数 n 有关, 如果对每个 m , 由假设 " $P(k)$ 对一切 $k < m$ 是正确的", 可以推出 " $P(m)$ 本身是正确的", 那么 $P(n)$ 对一切 n 都是正确的.

令 S 表示使 $P(n)$ 错误的正整数集合, 使用良序原理即可. 注意, 在 $m=1$ 的情形中, 所有 $k < 1$ 的集合是空的, 因此必须暗含 $P(1)$ 的证明. 也就是在使用数学归纳法的时候, 都需要证明 $P(1)$ 成立.

1.6 可除性

整系数方程 $ax = b$ 不总是有整数解 x , 如果有整数解, 则称 b 可被 a 整除. 在任意整环中也有类似的可除性概念.

定义 1.7. 整除

在整环 D 中, 如果有 D 中某一 q , 使 $b = aq$, 则称元素 b 可被元素 a 整除. 当 b 可被 a 整除时, 记作 $a|b$, 我们说 a 是 b 的因子, b 是 a 的倍数. 1 的因子称为 D 的单位或可逆元素.



关系 $a|b$ 满足自反律和传递律:

- 自反律 $a|a$;
- 传递律由 $a|b$ 和 $b|c$ 可推出 $a|c$.

自反律可以通过 $a = a \cdot 1$ 得到, 至于第二个, 使用定义: $a|b$ 和 $b|c$ 意味着存在元素 d_1 和 d_2 , 满足 $b = ad_1$ 和 $c = bd_2$, 由此得到 $c = a(d_1d_2)$, $d_1d_2 \in D$, 按照定义 $a|c$.

对于全体整数集 \mathbb{Z} 组成的整环来说, 1 和 -1 都是 1 的因子, 因而都是 \mathbb{Z} 的单位或者可逆元素, 而且也只有这两个单位.

定理 1.5

\mathbb{Z} 中仅有的单位是 ± 1



对于整数 a 和 b , $ab = 1$ 意味着 $a = \pm 1$ 和 $b = \pm 1$. 这个证明需要使用到有序整环中的概念, 以及良序原则得到的定理 1.3: 从 $ab = 1$ 得到 $|a||b| = 1$, 而整环中不存在零因子, 可以知道 $|a| > 0$ 和 $|b| > 0$, 最后通过三分律以及不等式的性质可以知道 $|a|$ 和 $|b|$ 只能是 1.

推论 1.10

如果整数 a 和 b 彼此可整除, 即 $a|b$ 且 $b|a$, 那么 $a = \pm b$.



证明需要使用到消去律和上述定理.

因为 $a = a \cdot 1 = (-a) \cdot (-1)$, 任意整数 a 可被 $a, -a, 1$ 和 -1 整除, 我们有定义:

定义 1.8. 素数

如果整数 p 不为 0 或 ± 1 , 并且 p 只能被 ± 1 和 $\pm p$ 整除, 那么称 p 为素数.



这个概念应该是可以被推广到一般整环的. 到后面学到理想概念之后再对比整数里面的素数.

1.7 欧几里得算法

整数 a 除以 b 用普通的除法就得到商 q 和余数 r . 也就是

- **除法算式** 对于给定的整数 a 和 $b, b > 0$, 存在整数 q 和 r , 使得

$$a = bq + r, \quad 0 \leq r < b. \quad (1.7.1)$$

从几何上看, 说明 a 会在区间 $[bq, b(q+1)]$ 上, 去掉右端点. 证明使用良序原理, 考虑集合 $S = \{a - bx | a - bx \geq 0, x \in \mathbb{Z}\}$. 要使用良序原理, 我们需要证明 S 非空, 注意到 $b > 0$, 对于整数, 就有 $b \geq 1, -|a|b \leq -|a| \leq a$, 于是 $a - (-|a|b) \geq 0, S$ 非空.

推论 1.11

对给定的整数 a 和 b , 满足等式 1.7.1 的商 q 和余数 r 是唯一确定的.



反证法即可, 不过需要结论: $a|b$, 并且 $|b| < |a|$, 那么只能是 $b = 0$. 或者说 $a|b$ 时, 必有 $|a| \leq |b|$.

我们经常有必要不涉及单个整数, 而是去处理某整数集合. 如果集合 S 包含 S 中任意两个元素 a 与 b 的和 $a+b$ 及差 $a-b$, 则称集合 S 在加法与减法之下封闭. 所有偶数构成这样的集合. 更一般的, 任意固定的整数 m 的所有倍数 xm 的集合在加法与减法之下是封闭的, 反过来也成立, 也就是说: 这种倍数的集合是具有这些性质的唯一的整数集合.

定理 1.6

在加法与减法之下封闭的任意非空整数集合, 不是仅由零组成, 就是包含最小正整数并由这个整数的所有倍数组成.



证明参考书本, 只是提示一点: 对于这样的集合 S , 必有 $0 \in S$, 然后就有 $a \in S$, 必有 $-a \in S$, 从而必然有正整数. 由此得到最小的正整数 m , 然后归纳证明 S 包含所有 m 的倍数, 再证明除了 m 的倍数之外不能有其他.

定义 1.9

如果整数 d 是整数 a 与 b 的公因子, 并且是任何其他公因子的倍数, 那么称 d 为 a 与 b 的最大公因子 (g.c.d.). 也就是 d 满足

$$d|a; \quad d|b; \quad c|a \text{ 和 } c|b \text{ 可推出 } c|d.$$



例如 3 和 -3 都是 6 和 9 的最大公因子. 按照定义, 两个不同的最大公因子必彼此整除, 因此它们仅相差一个符号. a 和 b 中两个可能的最大公因子 $\pm d$ 中, 正的最大公因子常用符号 (a, b) 表示. 值得注意的是, 最大公因子定义中的“最大”, 主要不是指 d 的数值比其他公因子 c 大, 而是指 d 为任何这种数 c 的倍数.

定理 1.7

任意两个整数 $a \neq 0$ 和 $b \neq 0$ 有正的最大公因子 (a, b) , 它可表为 a 和 b 的具有整系数的 s 和 t 的线性组合, 形为

$$(a, b) = sa + tb. \quad (1.7.2)$$



考虑形为 $sa + tb$ 的所有数, 这些数组成的集合对加法和减法封闭, 从而存在最小正整数 d , 然后证明它就是正的最大公约数.

类似, a 和 b 的公倍数的集合 M 在加法和减法之下也是封闭的, 它的最小正元素 m 将是 a 和 b 的公倍数, 它整除每个公倍数, 于是 m 是最小公倍数 (l.c.m.).

定理 1.8

任意两个整数 $a \neq 0$ 和 $b \neq 0$ 有最小公倍数 $m = [a, b]$, 它是 a 和 b 的每个公倍数的因子, 并且它自己也是 a 和 b 的公倍数.



为找到两个整数 a 和 b 的最大公因子, 可应用所谓欧几里得算法. 由于 $(a, b) =$

$(a, -b)$, 我们可以假设 a 和 b 都是正整数. 除法公式给出:

$$a = bq_1 + r_1, \quad 0 \leq r_1 < b, \quad (1.7.3)$$

整除 a 和 b 的每个整数必整除余数 r_1 , 反之, b 和 r_1 的每个公因子是 a 的因子, 所以 a 与 b 的公因子和 b 与 r_1 的公因子相同, 从而 $(a, b) = (b, r_1)$. 于是我们可以在 b 和 r_1 继续执行类似操作:

$$\begin{aligned} b &= r_1q_2 + r_2, & 0 < r_2 < r_1 \\ r_1 &= r_2q_3 + r_3, & 0 < r_3 < r_2 \\ &\dots & \dots \\ r_{n-2} &= r_{n-1}q_n + r_n, & 0 < r_n < r_{n-1} \\ r_{n-1} &= r_nq_{n+1} \end{aligned} \quad (1.7.4)$$

因为余数不断减小, 最后必有余数 r_{n+1} 为零. 所要求的最大公因子是:

$$(a, b) = (b, r_1) = (r_1, r_2) = \dots = (r_{n-1}, r_n) = r_n.$$

利用欧几里得算法, 可以把最大公因子显式地表示为线性组合 $sa + tb$, 这只需要用 a 和 b 表示逐次的余数 r_i 即可.

$$\begin{aligned} r_1 &= a - bq_1 = a + (-q_1)b \\ r_2 &= b - q_2r_1 = (-q_2)a + (1 + q_1q_2)b \\ &\dots \end{aligned}$$

利用 $(a, b) = sa + tb$ 可以证明下面的定理:

定理 1.9

如果 p 为素数, 那么由 $p|ab$ 可推出 $p|a$ 或 $p|b$.



当 p 为素数的时候, 如果 $p|a$ 不成立, 那么必有 $(p, a) = 1$. 于是 $1 = sa + tp$, 两边乘以 b 即可得到结论.

如果 $(a, b) = 1$, 就称 a 和 b 互素. 用前面的方法可以证明:

定理 1.10

如果 $(c, a) = 1$ 且 $c|ab$, 那么 $c|b$.



运用定理 1.10, 再加上整除的定义, 可以证明下面的:

定理 1.11

如果 $(a, c) = 1$, $a|m$ 且 $c|m$, 那么 $ac|m$.



1.8 算术基本定理

现在可以证明整数唯一因子分解定理, 也成为算术基本定理.

定理 1.12. 算术基本定理

任意非零整数可表为单位 (± 1) 乘以正素数的积, 如果不计素因子出现的顺序, 这种表示是唯一的.



存在性证明使用数学第二归纳法, 至于唯一性, 使用上一节的定理 1.9.

数的因子分解中, 同一个素数 p 可以出现多次. 把所出现的相同的素数集中起来, 分解式可写为:

$$a = \pm p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \quad (1 < p_1 < p_2 < \cdots < p_k). \quad (1.8.1)$$

由唯一性可知, 每个素数 p_i 的指数 e_i 是由给定的 a 唯一确定的.

1.9 同余式

两个整数 a 和 b 对模 m 同余定义如下:

定义 1.10. 同余

$a \equiv b \pmod{m}$ 成立当且仅当 $m \mid (a - b)$.



我们也可以说 $a \equiv b \pmod{m}$ 的意思是差 $a - b$ 在 m 的所有倍数的集合中. 另外还可以根据下述事实来定义: 每个整数 a 除以 m 剩下唯一的余数.

定理 1.13

两个整数 a 和 b 对模 m 同余当且仅当它们除以 $|m|$ 时剩下相同的余数.



注意到 $a \equiv b \pmod{m}$ 当且仅当 $a \equiv b \pmod{m}$, 只需要对 $m > 0$ 进行证明即可. 证明使用定义即可.

固定模 m 的同余关系具有和相等类似的性质 (很多时候在知道模 m 的时候, 经常会省略 \pmod{m} , 就如下面所示):

- 自反律 $a \equiv a$.
- 对称律若 $a \equiv b$, 则 $b \equiv a$.
- 传递律若 $a \equiv b$ 且 $b \equiv c$, 则 $a \equiv c$.

证明使用定义即可完成.

固定模 m 的同余关系还具有“代换性质”, 这也是相等关系的性质之一, 即: 同余整数之和同余, 而且同余整数之积同余. 用同余式表示为: $a_1 \equiv b_1, a_2 \equiv b_2$, 那么 $a_1 + a_2 \equiv b_1 + b_2, a_1 a_2 \equiv b_1 b_2$.

定理 1.14

如果 $a \equiv b \pmod{m}$, 那么对一切整数 x , 有

$$a + x \equiv b + 1, \quad ax \equiv bx, \quad -a \equiv -b \pmod{m}$$



同样使用定义即可证明.

对于方程成立的消去律对于同余式不一定成立. 例如, 由 $2 \cdot 7 \equiv 2 \cdot 1 \pmod{12}$ 不能

推出 $7 \equiv 1 \pmod{12}$. 之所以不能这样推断, 是因为被消去的 2 是模的一个因子. 对于同余, 最好也只能得到修改的消去律:

定理 1.15

当 c 与 m 互素时, 由 $ca \equiv cb \pmod{m}$ 可推出 $a \equiv b \pmod{m}$.



这实际上是定理 1.10 的一个应用.

线性方程的讨论可以扩展到同余式上:

定理 1.16

如果 c 与 m 互素, 那同余式

$$cx \equiv b \pmod{m}$$

有整数解 x , 任意两个解 x_1 和 x_2 对模 m 同余.



证明提要: $(c, m) = 1$, 说明存在整数 s, t 使得 $1 = sc + tm$, 从而 $b = bsc + btm$, 于是 $b \equiv (bs)c \pmod{m}$, 也就是 $x = bs$ 是一个解. 第二个结论, 通过使用同余式的传递律和对称律, 由 $cx_1 \equiv b$ 和 $cx_2 \equiv b$ 可推出 $cx_1 \equiv cx_2$, 使用定理 1.15 可得 $x_1 \equiv x_2$.

当模 m 为素数时, 出现重要的特殊情形, 此时, 不能被 m 整除的一切整数都与 m 互素, 由此得出

推论 1.12

如果 p 为素数, 并且 $c \not\equiv 0 \pmod{p}$, 那么 $cx \equiv b \pmod{p}$ 有模 p 的唯一解.



这里所谓模 p 唯一解, 就是指任意两个解模 p 同余 (相等).

也可以解联立同余式.

定理 1.17

如果 m_1 与 m_2 互素, 那么同余式

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \end{aligned} \tag{1.9.1}$$

有公共解 x , 任意两个解 x_1 和 x_2 对模 $m_1 m_2$ 同余.



证明摘要: 对任意整数 y , $x = b_1 + ym_1$ 是第一个同余式的解, 这样的 x 又要满足第二个同余式, 当且仅当 $b_1 + ym_1 \equiv b_2 \pmod{m_2}$, 或者说 $ym_1 \equiv b_2 - b_1 \pmod{m_2}$, 根据定理 1.16, 这个方程有解 y , 从而 x 存在. 第二部分, 只需要注意到, 对于任意两个解 x_1 和 x_2 , 有 $x_1 - x_2 \equiv 0 \pmod{m_1}$, $x_1 - x_2 \equiv 0 \pmod{m_2}$, 而 $(m_1, m_2) = 1$, 于是 $x_1 - x_2$ 必然可以被 $m_1 m_2$ 整除.

上面同样的方法应用于形为

$$a_i x \equiv b_i \pmod{m_i}$$

的两个或多个同余式, 其中 $(a_i, m_i) = 1$, 并且各个不同的模两两互素.

书中没有这个过程, 这里简单对两个同余式的情形说明一下: 对于 $a_1 x \equiv b_1 \pmod{m_1}$ 来说, 从 $(a_1, m_1) = 1$ 可知存在 s_1, t_1 使得 $s_1 a_1 + t_1 m_1 = 1$, 从而可知 $x = b_1 s_1$ 是同余式

的一个解, 对于任意整数 y , $b_1s_1 + ym_1$ 都是其解, 代入第二个同余式 $a_2x \equiv b_2 \pmod{m_2}$, 有 $a_2(b_1s_1 + ym_1) \equiv b_2 \pmod{m_2}$, 或者 $a_2m_1y \equiv b_2 - b_1s_1a_2 \pmod{m_2}$, 而 $(a_2, m_2) = 1$, $(m_1, m_2) = 1$, 必有 $(a_2m_1, m_2) = 1$, 最后一个同余式有解 y , 从而存在 x .

定理 1.18. 费马 (Fermat) 小定理

如果 a 为整数, p 为素数, 那么

$$a^p \equiv a \pmod{p}$$



是用数学归纳法以及二项式公式, 二项式公式 $(n+1)^p$ 中, 除了第一项和最后一项, 其余每一项都能被 p 整除 (这个结论并不显然, 需要证明), 于是 $(n+1)^p \equiv n^p + 1 \pmod{p}$.

关于 $p \mid \binom{p}{k}$ 并不是特别明显, 这里 $0 < k < p$, 不过在 p 是素数的情形下, 还是比较容易的, 证明如下: 由于 p 是素数, 所以条件中的 k , 任意 $0 < l \leq k$ 满足 $(l, p) = 1$, 于是 $(k!, p) = 1$, 因为 $\binom{p}{k}$ 是整数, 于是应该有 $k! \mid (p-1) \cdots (p-k+1)$, 也就是

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1) \cdots (p-k+1)}{k!} = p \cdot \frac{(p-1) \cdots (p-k+1)}{k!}$$

由此得证.

1.10 环 \mathbb{Z}_n

人们很早就区分偶数和奇数, 并且熟知偶数和奇数如下规律:

$$\text{偶数} + \text{偶数} = \text{奇数} + \text{奇数} = \text{偶数}$$

$$\text{偶数} + \text{奇数} = \text{奇数}$$

$$\text{偶数} \cdot \text{偶数} = \text{偶数} \cdot \text{奇数} = \text{偶数}$$

$$\text{奇数} \cdot \text{奇数} = \text{奇数}$$

这些恒等式定义了一个新的整环 \mathbb{Z}_2 , 它仅有两个元素 0 (偶数) 和 1 (奇数) 组成, 并且有加法表和乘法表:

$$0 + 0 = 1 + 1 = 0, \quad 0 + 1 = 1 + 0 = 1,$$

$$0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0, \quad 1 \cdot 1 = 1.$$

类似的构造可用于对任意模 n 的全体剩余 $0, 1, 2, \dots, n-1$, 这样两个剩余的相加或相乘, 可以先简单的进行普通意义下 (\mathbb{Z} 下) 的相加或相乘, 然后将所得结果取模 n 的剩余. 对于这样的系统, 组成一个交换环, 也就是:

定理 1.19

在加法和乘法之下, 对任意固定的模 $n \geq 2$, 整数 $0, 1, \dots, n-1$ 的集合组成一个交换环.



证明也就是验证交换环的各个公设, 这里省略.

与整环定义唯一不相一致的公设是乘法消去律. 而乘法消去律在交换环中等价于: \mathbb{Z}_n 中无零因子, 及由 $ab = 0$ 推出 $a = 0$ 或者 $b = 0$, 在 \mathbb{Z}_n 中就是: 由 $ab \equiv 0 \pmod{n}$ 推

出 $a \equiv 0 \pmod{n}$ 或 $b \equiv 0 \pmod{n}$, 这等价于: 由 $n|ab$ 推出 $n|a$ 或 $n|b$, 这个结果对于 n 为素数的时候是成立的. n 不是素数的时候, 有非平凡分解 $n = ab$, 此时显然 $n|a$ 和 $n|b$ 都不成立, 因此我们有

定理 1.20

模 n 整数环 \mathbb{Z}_n 是整环当且仅当 n 是素数.



还有其他更系统的方法构造模 n 整数的代数. 用等式代替同余式的方法, 本质上意味着: 把所有用 n 去除而剩下同样余数的整数归在一组, 产生一个新的数. 每个这样的整数组称为“剩余类”, 也就是说, 对于任意模 n , 由余数 r ($0 \leq r < n$) 确定的剩余类 r_n , 是由所有用 n 去除而剩下余数 r 的整数 a 组成的. 每个整数属于一个且仅属于一个剩余类, 而且两个整数属于同一个剩余类当且仅当他们同余. 模 n 有 n 个剩余类: $0_n, 1_n, \dots, (n-1)_n$.

\mathbb{Z}_n 的代数可以直接在这些剩余类上进行: 两个剩余类相加 (或相乘), 可以在两个剩余类中任意选择代表元素 a 和 b , 并求出含有 $a+b$ (或者 ab) 的剩余类. 如果 a_n 表示包含 a 的剩余类, 可以表示为

$$(a+b)_n = a_n + b_n, \quad (ab)_n = a_n b_n.$$

后面还会回到这个剩余类.

1.11 集合, 函数, 关系

¹ 集合是一些数学对象完全任意的集体. 如果 A 是集合, 则我们记 $x \in A$ 表示对象 x 是集合 A 的元素, 当 x 不是 A 的元素时, 记作 $x \notin A$. 有限集合可以通过列出它的所有元素来确定. 任何集合由它的元素确定, 也就是, 两个集合 A 和 B 相等当且仅当它们有相同的元素. 这个原则 (称为外延公理) 也可用符号表示为: $A = B$ 的意思是, 对一切 x , $x \in A$ 当且仅当 $x \in B$. 集合的相等关系满足一般相等关系的自反律, 对称律和传递律.

集合 S 称为集合 A 的子集, 当且仅当 S 的每个元素 x 也在 A 中, 用符号 $S \subset A$ 表示. 如果 $T \subset S$ 和 $S \subset A$, 那么显然 $T \subset A$, 也就是关系 \subset 满足传递律. 集合相等也可以表述为: $A = B$ 当且仅当 $A \subset B$ 和 $B \subset A$ 两者都成立. 空集 \emptyset (没有元素的集合) 是每个集合的子集.

从任意集合出发, 可以选出各种不同的子集. 任何性质都给定一个子集; 已知任意集合 A 和性质 P , 可以构成一个子集

$$S = \{x | x \in A, \text{ 并且 } x \text{ 具有性质 } P\},$$

它是由 A 中具有性质 P 的所有元素组成.

一般地, 如果 A 和 B 都是集合, 则关于 A 到 B 的函数是这样规定的: 它对 A 中的每个元素 a 给定 B 中的一个元素, 把它记作 $a \mapsto a\phi$. 关系 $a \mapsto a\phi$ 有时写成 $a \mapsto \phi a$ 或 $a \mapsto \phi(a)$, 也就是把函数符号写在前面 (好像大部分书都是采取这后一种写法). 函数

¹这一节的内容, 应该想办法提前, 并且可以替换成其他书中的陈述.

$\phi: A \rightarrow B$ 也称为 A 到 B 的映射, 变换或对应, 集合 A 称为函数 ϕ 的定义域, 而集合 B 是函数 ϕ 的取值域.

函数 $\phi: A \rightarrow B$ 的象 (或 “值域”) 是所有函数 “值” 的集合, 即所有 $a\phi$ ($a \in A$) 的集合, 象是取值域 B 的子集, 而不一定是整个 B .

函数 $\phi: A \rightarrow B$, 当 B 的每个元素 b 是函数的象时, 也就是说象是整个取值域时, 称 ϕ 是满射 (映上).

函数 $\phi: A \rightarrow B$, 当 A 的不同元素总有不同的象, 也就是说由 $a\phi = a'\phi$ 总能推出 $a = a'$ 时, 称 ϕ 是单射 (一一映入).

函数 $\phi: A \rightarrow B$, 当它既是单射又是满射, 即对每个元素 $b \in B$, 有一个且仅有一个 $a \in A$ 具有象 b , 使 $a\phi = b$, 则称 ϕ 是双射 (一一映上). 双射 $\phi: A \rightarrow B$ 也称为 A 到 B 上的一一对应.

一般的, 集合 S 上的二元运算 \circ 是这样规定的: 它对 S 中每个有序元素对 a 和 b 给出同一集合 S 中的唯一确定的第三个元素 $c = a \circ b$, 这里我们用 “唯一” 表示代换性质:

$$a = a' \text{ 且 } b = b' \text{ 推出 } a \circ b = a' \circ b' \quad (1.11.1)$$

注意定义中是有序对, 所以这个定义没有保证 $a \circ b = b \circ a$.

为方便起见, 把所有有序元素对 (a, b) ($a \in S, b \in T$) 的集合记作 $S \times T$, 这称为 S 和 T 的笛卡尔积. 我们又把集合同自身的积 $S \times S$ 记作 S^2 , 那么二元运算同函数 $\circ: S^2 \rightarrow S$ 一样.

两个已知整数间有各种关系, 例如 $a = b, a < b, a \equiv b \pmod{7}, a|b$ 等. 为一般地讨论关系, 我们引进符号 R 表示任何关系, 形式上, 如果已知集合 S 中的任何两个元素 a 和 b , 不是 a 与 b 有关系 R (记作 aRb), 就是 a 与 b 没有关系 R (记作 $aR'b$), 那么 R 就表示集合 S 上的二元关系.

数学中特别重要的是像同于和相等那样的集合 S 上满足下面定律的关系:

- 自反律 $a = a$, 对一切 $a \in S$.
- 对称律若 $a = b$, 则 $b = a$, 对一切 $a, b \in S$.
- 传递律若 $a = b$ 且 $b = c$, 则 $a = c$, 对一切 $a, b, c \in S$.

满足自反律, 对称律和传递律的关系称为等价关系. 例如平面三角形的全等关系就是等价关系.

1.12 同构与自同构

近世代数最重要的概念之一是同构的概念. 现在对交换环定义这个概念:

定义 1.11. 同构

两个交换环 R 和 R' 之间的同构是 R 的元素 a 与 R' 的元素 a' 的一一对应 $a \leftrightarrow a'$, 并对所有元素 a 和 b 满足条件:

$$(a + b)' = a' + b', \quad (ab)' = a'b', \quad (1.12.1)$$

如果两个环 R 和 R' 之间存在这样的对应, 则称它们是同构的.



基于规律1.12.1我们可以说, 同构 $a \leftrightarrow a'$ “保持和与积”. 粗略地说, 两个交换环当它们的元素仅仅区别于记号时, 它们是同构的. 一个恰当的例子是“偶数”和“奇数”的代数同整环 \mathbb{Z}_2 比较, 一一对应

$$\text{偶数} \leftrightarrow 0 \quad \text{奇数} \leftrightarrow 1$$

是这两个整环之间的同构.

许多整环具有同它们自身的同构, 这样的同构是很重要的, 它称为自同构, 类似于几何图形中的对称性. 例如考虑整环 $\mathbb{Z}[\sqrt{2}]$, 在非平凡对应 $m + n\sqrt{2} \leftrightarrow m - n\sqrt{2}$ 之下, $\mathbb{Z}[\sqrt{2}]$ 与它自身同构. 这一点可以通过简单验证规律1.12.1即可. 这里省略.

任何同构 $a \leftrightarrow a'$ 不仅保持和与积, 而且保持差. 根据定义 $a - b$ 是方程 $b + x = a$ 的解, 所以 $b + (a - b) = a$, 因为对应保持和, 所以 $b' + (a - b)' = a'$, 这就是说 $(a - b)'$ 是方程 $b' + x = a'$ 的 (唯一) 解, 或者说

$$(a - b)' = a' - b'.$$

另一个法则是

$$0' = 0, \quad 1' = 1, \quad (-a)' = -a'. \quad (1.12.2)$$

总之 R 的零 (单位元素) 对应于 R' 的零 (单位元素).

同构的概念普遍应用于代数系统. 我们甚至可以说, 抽象代数是研究代数系统那些在同构之下仍保持不变的性质.

在把整数系描述为有序整环 (其中每个正整数集合具有最小元素) 时我们曾要求: 对于所有的数学意义, 这些公设完整地描述了全体整数. 现在我们可以把它叙述得更确切 (后面会证明). 任意有序整环当它所包含的全体正元素集合是良序的, 它就同构于整数环 \mathbb{Z} . \mathbb{Z} 的“精确到同构”的这个特征是最完全的了, 它可用我们已用过的任何形式的公设系得到. 因为一般地, 显然, 如果系统 S 满足这样的公设系, 而且 S' 是另一个同构于 S 的系统, 那么 S' 必也满足这些公设. 因此, 如果 S 满足加法交换律, 则对 S 中一切 a 和 b , $a + b = b + a$. 由于在已知同构之下, 它们的对应元素必相等, 所以 $(a + b)' = (b + a)'$. 因为同构保持和, 所以 $a' + b' = b' + a'$. 这就断言: 交换律在 S' 中也成立. 这种论证具有一般性, 可应用于我们的一切公设.

第二章 有理数和域

2.1 域的定义

全体有理数组成的整环 \mathbb{Q} 和全体实数组成的整环 \mathbb{R} 具有整数环 \mathbb{Z} 所不具备的极重要的代数特征：在它们之中，任何方程 $ax = b$ ($a \neq 0$) 是可解的。具有这个性质的交换环称为域。我们现在将证明：在任何交换环中，如果所有非零元素有乘法逆，那么除法是可能的，并具有一些熟知性质。

定义 2.1. 域

如果 F 是一个交换环，并且对每个元素 $a \neq 0$ ，它都包含一个逆元素 a^{-1} ，满足方程 $a^{-1}a = 1$ ，那么 F 是域。



在任何域中，消去律 (ix) 成立（证明难度不大，略），换句话说，每个域是一个整环。更一般的，是域的子整环（根据相同的理由）¹。相反，我们将在本节和下一节指出，任何整环都能够按照唯一的最小路径被扩展成域。我们通过把分数表示为整数之商的标准表示法来说明扩展的方法。

定理 2.1

在任何域中，除法（零除外）是可能的而且是唯一的。



实际上就是证明 $a \neq 0$ 时，方程 $ax = b$ 有唯一解：可以直接构造出这个解 $x = a^{-1}b$ ，至于唯一性，通过消去律保证。

我们用 $\frac{b}{a}$ (a 除 b 所得的商) 表示 $ax = b$ 的唯一解，特别的， $\frac{1}{a} = a^{-1}$ 。下面证明通常的商的运算法则（可以使用域的公设来证明）：

定理 2.2

在任何域中，商遵循下列法则（这里 $b \neq 0, d \neq 0$ ）：

- (i) $\frac{a}{b} = \frac{c}{d}$ 当且仅当 $ad = bc$,
- (ii) $\frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd}$,
- (iii) $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$,
- (iv) $\frac{a}{b} + (-\frac{a}{b}) = 0$,
- (v) $\frac{a}{b} \cdot \frac{b}{a} = 1$, 当 $\frac{a}{b} \neq 0$.



证明不难，严格使用各个公设和定义。例如对于 (i) $\frac{a}{b} = \frac{c}{d}$ 意味着： $ab^{-1} = cd^{-1}$ 。

$$ad = a(b^{-1}b)d = cd^{-1}(bd) = cd^{-1}db = bc,$$

反过来类似。

(ii) 的证明回到方程， $x = \frac{a}{b}$ 和 $y = \frac{c}{d}$ 分别表示 $bx = a$ 和 $dy = c$ 的解，于是有

$$dbx = da, bdy = bc, bd(x \pm y) = ad \pm bc,$$

¹这句话有点费解

也就是 $x \pm y$ 是方程 $bdz = ad \pm bc$ 的唯一解 $z = \frac{ad \pm bc}{bd}$.

(iii) 的证明和 (ii) 类似

$$(bd)(xy) = (bx)(dy) = ac,$$

(iv) 的证明利用前面的 (ii), 同时注意到 $0 \cdot x = 0$. (v) 的证明使用 (iii), 然后 $x = 1$ 是方程 $bax = ab$ 的唯一解.

还可以证明如下结论:

$$(bd)^{-1} = d^{-1}b^{-1}, (-b)^{-1} = -(b^{-1}), b, d \neq 0 \quad (2.1.1)$$

$$a \pm \frac{b}{c} = \frac{ac \pm b}{c}, a \frac{b}{c} = \frac{ab}{c}, c \neq 0 \quad (2.1.2)$$

$$\frac{a}{b} / \frac{c}{d} = \frac{ad}{bc}, \frac{a}{b} / c = \frac{a}{bc}, \frac{a}{1} = a, b, c, d \neq 0 \quad (2.1.3)$$

$$-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}, \frac{-a}{-b} = \frac{a}{b}, b \neq 0 \quad (2.1.4)$$

存在各种各样的域, 例如对于任意素数 p , 整环 \mathbb{Z}_p 是一个域, 这可由定理??的推论得到. 如果我们假定全体实数构成一个域, 那么我们利用子域的概念可以容易地构造出其他域的例子.

定义 2.2

如果一个给定的域 F 的子集在 F 中的加法和乘法运算之下构成一个域, 那么称这个子集为 F 的子域.



只要问题中的运算能进行, 那么所有在 F 中成立的恒等式 (即交换律, 结合律和分配律) 在 F 的任意子集中自然成立, 因此验证 F 的子集 S 是否是子域时, 可以不管那些恒等式的证明, 而只需要检验那些包含某个“存在性”的公设, 比如逆元素的存在性.

定理 2.3

如果域 F 的子集 S 包含着 F 中的零元素和单位元素, S 在加法和乘法之下是封闭的, S 中每个 a 在 S 中有它的负元素 $-a$ (加法逆元素) 和乘法逆元素 a^{-1} (假定 $a \neq 0$), 那么 S 是子域.



利用这个定理, 可以证明所有形如 $a + b\sqrt{2}$ 的实数的集合是实数域的一个子域, 其中系数 a 和 b 是有理数, 这个子域通常记为 $\mathbb{Q}(\sqrt{2})$, 这里 \mathbb{Q} 表示有理数域. 证明稍微麻烦一点是乘法逆元素的存在性 (通分, 分子分母乘以 $a - b\sqrt{2}$ 即可), 而这依赖于结论 $\sqrt{2}$ 是无理数, 从而 $a^2 - 2b^2$ 不能为零. 具体过程参考书本.

同样的可以证明, 所有实数 $a + b\sqrt[3]{5} + c\sqrt[3]{25}$ 的集合 $\mathbb{Q}(\sqrt[3]{5})$ 是一个域. 难点同样在于乘法逆元素的存在性, 需要去解一个线性方程组.

$$(a + b\sqrt[3]{5} + c\sqrt[3]{25})(x + y\sqrt[3]{5} + z\sqrt[3]{25}) = (1 + 0\sqrt[3]{5} + 0\sqrt[3]{25}).$$

从这里可以得到方程组.

如果我们假定存在一个由全体复数 $a + bi$ (这里 $i = \sqrt{-1}$, a 和 b 是实数) 构成的域, 那么我们还可以构造其他子域. 二次方程

$$\omega^2 + \omega + 1 = 0$$

在复数中有根 $\omega = \frac{-1+\sqrt{-3}}{2} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, 它是一个虚的单位立方根. 所有数 $a + b\omega$ (a, b 为有理数) 构成复数域的一个子域 $\mathbb{Q}(\omega)$. 验证不难, 至于乘法的封闭, 需要注意到 $\omega^2 = -\omega - 1$,

$$\begin{aligned}(a + b\omega)(c + d\omega) &= ac + (bc + ad)\omega + bd\omega^2 \\ &= (ac - bd) + (bc + ad - bd)\omega.\end{aligned}$$

至于乘法逆元素, 同样可以通过求解线性方程组得到. 这里直接给出

$$(a + b\omega)\left[\frac{-(b - a + b\omega)}{a^2 - ab + b^2}\right] = \frac{a^2 - ab + b^2}{a^2 - ab + b^2} = 1$$

分母 $a^2 - ab + b^2$ 不可能为零, 除非 $a = b = 0$,

$$a^2 - ab + b^2 = \frac{a^2 + b^2}{2} + \frac{(a - b)^2}{2}.$$

2.2 有理数域的构造

在第一节中, 假定了全体整数的良序整环 \mathbb{Z} 的存在, 现在我们将严格地证明, 有理数域 \mathbb{Q} (有序的) 能够由 \mathbb{Z} 构造出. 实际上, 更一般的, 我们将证明, 类似的构造可以应用到任何整环上.

仅仅由全体整数不能构成域, 由整数构造有理数在本质上恰是构造了包含全体整数在内的域. 显然这个域还必须包含所有方程 $bx = a$ 的解, 其中系数 $a, b, b \neq 0$ 是整数. 为了从这些方程抽象地构造“有理数”, 我们引入某些新记号 (或者数偶) $r = (a, b)$ ², 每个记号代表一个方程 $bx = a$ 的解, 为此, 我们必须说明, 这些新记号完全像域中的商 $\frac{a}{b}$ 那样可以相加, 相乘和相等 (定理 2.2 中的 (i) (ii) (iii)).

不管我们从整数环 \mathbb{Z} , 还是从其他一些整环 D 出发, 上述说明是很有意义的, 还可以确切地描述如下:

定义 2.3. 商域

设 D 是任意整环, D 的商域 $Q(D)$ 是由所有数偶组成. 其中 $a, b \in D$ 并且 $b \neq 0$. 这种数偶的相等由下面约定来确定:

$$(a, b) \equiv (a', b') \Leftrightarrow ab' = a'b, \quad (2.2.1)$$

而数偶的和与积分别由下列约定来确定:

$$(a, b) + (a', b') = (ab' + a'b, bb'), \quad (2.2.2)$$

$$(a, b) \cdot (a', b') = (aa', bb'). \quad (2.2.3)$$



注意, 因为 D 不包含零因子 (定理), 在 (2.2.2) 和 (2.2.3) 中的乘积 $bb' \neq 0$, 所以 $Q(D)$ 在加法和乘法之下是封闭的.

我们希望数偶之间的“ \equiv ”关系和相等关系一致, 其实, 通过直接验证可以证明“ \equiv ”满足相等的三个性质 (自反律, 对称律和传递律), 其次和与积在 \equiv 意义下是唯一确定的.

²其实分析中实数的构造有些类似, 既然我要想有理数极限存在, 我直接构造一个数作为极限, 但是需要证明这个极限唯一, 并且满足已有运算.

例如, 由 $(a, b) \equiv (a', b')$ 可以推出 $(a, b) + (a'', b'') = (a', b') + (a'', b'')$. 这一点同样可以直接使用定义完成验证 (参考书本). 类似的, 对于乘法的唯一性断言也是成立的. 我们得出结论, 由 (2.2.1) 式定义的相等具有所要求的性质.

现在可以验证 $Q(D)$ 中的各种代数定律. 例如分配律, 根据定义 (2.2.2) 和 (2.2.3), 按照下列方法一步一步简化定律的每一边. 设 r, r' 和 r'' 是任意三个数偶,

$$\begin{array}{ll} r(r' + r'') & rr' + rr'' \\ (a, b)[(a', b') + (a'', b'')] & (a, b)(a', b') + (a, b)(a'', b'') \\ (a, b)(a'b'' + a''b', b'b'') & (aa', bb') + (aa'', bb'') \\ (aa'b'' + aa''b', bb'b'') & (aa'bb'' + aa''bb', bb'bb'') \end{array}$$

最后一行的两边给出了在 (2.2.1) 意义下相等的数偶, 这是因为右边和左边的差别只是在右边所有项中多出现一个非零因子 b , 在数偶中这样一个额外因子使数偶总保持相等, 即 $(bx, by) = (x, y)$, 因为根据 (2.2.1) 式这个等式相等于恒等式 $bxy = bxy$.

和分配律证明类似, 我们可以证明结合律和交换律. 加法单位元素 (零) 是数偶 $(0, 1)$, 因为

$$(0, 1) + (a, b) = (0 \cdot b + 1 \cdot a, 1 \cdot b) = (a, b).$$

同样消去律也成立, 并且数偶 $(1, 1)$ 是乘法单位元素. (a, b) 的负元素 (加法逆元素) 是 $-(a, b) = (-a, b)$, 这就验证了关于整环的一切公设.

定理 2.4

对任意整环 D , 商域 $Q(D)$ 是一个域.



剩下只需证明每个方程 $rx = 1$ 其中 $r \neq 0$ 在 $Q(D)$ 中有一个解. 也就是说, 对于每个 $r \neq 0$, 在 $Q(D)$ 中存在 r 的乘法逆元素, 这是容易证明的 ((a, b) 的乘法逆元素应该是 (b, a)). 更一般的, 任意方程

$$(a, b)(x, y) \equiv (c, d), \quad (a, b) \not\equiv (0, 1), \quad (2.2.4)$$

都有解 (可以转化为有理数进行思考, 这样求解很方便)

$$(x, y) = (bc, ad).$$

条件 $(a, b) \not\equiv (0, 1)$ 保证了 $a \neq 0$, 于是解 (x, y) 中的 $ad \neq 0$, 从而满足定义.


我们现在希望证明, $Q(D)$ 实际上包含着原来的整环 D 作为它的子整环, 换句话说, $Q(D)$ 实际上是 D 的扩展. 严格说来这是不可能的³, 因为数偶 (a, b) 不像 D 中那样的元素, 不过我们可以把每个 $a \in D$ 与 $(a, 1)$ 联系起来, 在相等, 加法和乘法之下, $(a, 1)$ 具有的性质完全像 a 一样.

$$\begin{aligned} (a, 1) + (b, 1) &= (a \cdot 1 + b \cdot 1, 1 \cdot 1) = (a + b, 1), \\ (a, 1) \cdot (b, 1) &= (ac, b, 1 \cdot 1) = (ab, 1), \\ (a, 1) &\equiv (b, 1) \Leftrightarrow a = b. \end{aligned}$$

³所以这个是同构意义下的, 见后面的讨论.


我们可以断言, 一一对应 $a \leftrightarrow (a, 1)$ 是给定的整环 D 到域 $Q(D) = F$ 的子整环上的一个同构. 此外, 方程 (2.2.4) 表明, 任何数偶 $r = (a, b) \in Q(D)$ 是方程 $(b, 1)r = (a, 1)$ 或者 $br = a$ 的解, 因此 $r = (a, b)$ 是商 $\frac{a}{b}$, 这就证明了

定理 2.5

任何整环 D 能够同构地嵌入域 $Q(D)$ 中, $Q(D)$ 的每个元素是 D 中两个元素的商. 


特别的, 把定理 2.5 用到整数环 \mathbb{Z} 上. 事实上在上述论证中始终想到 $D = \mathbb{Z}$ 这一特殊情形, 因此 $Q(D) = Q(\mathbb{Z})$ 是全体普通分数的集合. 所以我们有

推论 2.1

整数环 \mathbb{Z} 可以作为子整环嵌入域 $\mathbb{Q} = Q(\mathbb{Z})$ 中, 域 \mathbb{Q} 的每个元素是整数的商 $\frac{a}{b}$, 其中 $b \neq 0$. 

我们现在指出, 有理数域 $\mathbb{Q} = Q(\mathbb{Z})$ 实际上已通过前面的论述被精确地表征出来 (精确到同构), 因为 \mathbb{Z} 是由它的公设所定义 (精确到同构), 所以这像我们所希望的那样是完备的表征. 事实上我们将证明, 任何整环 D 都有类似的结果.

定理 2.6

设整环 D 作为子整环包含在任意一个域 F 中, 那么 F 中所有形为 $\frac{a}{b}$ (其中 $a, b \in D$, $b \neq 0$) 的元素组成的集合是 F 的一个子域 S , 并且在对应 $\frac{a}{b} \leftrightarrow (a, b)$ 之下这个子域 S 与 $Q(D)$ 同构. 

两个域 F 和 F' 之间的同构是指, 把 F 和 F' 看作交换环时它们之间的同构, 特别, 它是 F 和 F' 之间满足下列性质的一一对应, 即如果 $x \leftrightarrow x'$ 和 $y \leftrightarrow y'$, 那么

$$(x + y) \leftrightarrow (x' + y'), \quad (xy) \leftrightarrow (x'y').$$


证明: 域 F 包含商 $\frac{a}{b}$, 这个商事方程 $bx = a$ 的解, 其系数 a 和 $b \neq 0$ 在 D 中, 所有这些商的集合 S 包含所有整数 $\frac{a}{1} = a$. 根据定理 2.2 中的法则, S 在加法, 减法, 乘法和除法之下是封闭的, 于是在 F 的这些运算之下, S 可以描述成 D 的闭包. 总之 S 是一个域 (定理 2.3).

这些商 $\frac{a}{b}$ 以定理 2.2 的 (i)-(iii) 所描述的方式进行相加, 相乘以及表示相等, 完全相同的法则用到数偶 (a, b) 上, 因此对应 $\frac{a}{b} \leftrightarrow (a, b)$ 是 D 的闭包 S 到 $Q(D)$ 上的一个同构.

特别注意, 这个对应把 D 中每个 a 映上到 $\frac{a}{1} \leftrightarrow (a, 1) = a$.

联合定理 2.6 和前面的推论, 我们得到

定理 2.7

整数环 \mathbb{Z} 可以按照一种且只有一种方式被嵌入域 $\mathbb{Q} = Q(\mathbb{Z})$ 中, 使得 \mathbb{Q} 的每个元素是两个整数的商. 

这就完成了由整数环 \mathbb{Z} 构造有理数域 \mathbb{Q} .

2.3 联立线性方程

一个域不一定由通常的“数”组成, 比如 p 为素数, 则所有模 p 的整数就构成一个只包含有限多个不同元素的域. 整环 \mathbb{Z}_p 是域这个事实是下面定理的推论.

定理 2.8

任何有限整环 D 是一个域.



整环和域就差一个非零元素的乘法逆元素的存在性. D 是有限的意味着 D 的元素全部可以列出来, 排成 b_1, b_2, \dots, b_n , 为证明 D 是域, 我们只须证明 D 的任意指定的元素 $a \neq 0$ 在 D 中有一个逆元素. 考察所有的乘积

$$ab_1, ab_2, \dots, ab_n, \quad (2.3.1)$$

这给出了 D 中几个全不相同的元素, 因为不然, 如果对某 $i \neq j$ 有 $ab_i = ab_j$, 则根据消去律, 得到 $b_i = b_j$, 这与假定 b_i 是不同元素相违背. 因为 D 中全部元素都在列表 (2.3.1), D 中单位元素 1 也必然出现在表中某个位置上, 比如 $1 = ab_i$, 那么相应的元素 b_i 就是所要求的 a 的逆元素.

根据上述证明, 为在 \mathbb{Z}_p 中精确地找出逆元素, 可以对 \mathbb{Z}_p 中所有可能的数 b_i 进行试验来得到. 逆元素还可以直接计算出, 这是因为 \mathbb{Z}_p 中方程 $ax = 1$ (其中 $a \neq 0$) 就是同余方程 $ax \equiv 1 \pmod{p}$, 后者可以根据欧几里得算法求出 x .

值得注意的是, 联立线性方程组的整个理论应用到一般域. 例如考虑两个联立方程

$$\begin{aligned} ax + by &= e, \\ cx + dy &= f, \end{aligned} \quad (2.3.2)$$

式中字母 a, \dots, f 表示域 F 的任意元素. 第一个方程乘以 d , 第二个方程乘以 b , 然后相减, 我们得到 $(ad - bc)x = de - bf$; 第二个方程乘以 a , 第一个方程乘以 c , 然后相减得到 $(ad - bc)y = af - ce$, 因此我们定义 (2.3.2) 的系数行列式为

$$\Delta = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc,$$

当 $\Delta \neq 0$ 时, 则方程 (2.3.2) 有解:

$$x = \frac{de - bf}{\Delta}, \quad y = \frac{af - ce}{\Delta},$$

而且没有其它解, 当 $\Delta = 0$ 时, 方程 (2.3.2) 或者没有解, 或者有无穷多解 (后者仅当 $c = ka, d = kb, f = ke$ 时发生, 也就是两个方程成比例).

高斯 (Gauss) 消去法 前面消去法的方法可以推广到形为

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n &= b_1, \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n &= b_2, \\ &\dots\dots\dots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n &= b_m \end{aligned} \quad (2.3.3)$$

的 n 个未知数的 m 个联立线性方程. 这里 a_{ij}, b_i, x_i 全部被限制在指定的域 F 上. 为求出

已知方程组的全部解, 我们现在将叙述称为高斯消去法的一般方法, 其想法是用简单的方程组代替已知方程组, 这个简单的方程组等价于已知方程组, 即它们是同解方程组.

采用缩写记号, 我们只写下第 i 个方程, 并把它表示成样本项 $a_{ij}x_j$, 对 $j = 1, \dots, n$ 求和, 即写成

$$\sum_{j=1}^n a_{ij}x_j = b_i, \quad i = 1, \dots, m; a_{ij} \in F.$$

我们分两种情况对未知数的个数 n 用归纳法进行论证.

情况 1 每个 $a_{i1} = 0$. 那么显然方程组等价于 $n - 1$ 个未知数 x_2, \dots, x_n 的 m 个方程的一个“较小”的方程组; 对于较小的方程组来说, x_1 是任意的.

情况 2 某一个 $a_{i1} \neq 0$. 通过两个方程的调换, 我们得到等价的方程组, 使得 $a_{11} \neq 0$. 当第一个方程乘以 a_{11}^{-1} 时, 我们则得到一个等价的方程组, 其中 $a_{11} = 1$, 然后依次从第 i 个方程 ($i = 2, \dots, m$) 减去新的第一个方程的 a_{i1} 倍, 我们便得到形如

$$\begin{aligned} x_1 + a'_{12}x_2 + a'_{13}x_3 + \dots + a'_{1n}x_n &= b'_1, \\ a'_{22}x_2 + a'_{23}x_3 + \dots + a'_{2n}x_n &= b'_2, \\ &\dots\dots\dots \\ a'_{m2}x_2 + a'_{m3}x_3 + \dots + a'_{mn}x_n &= b'_m \end{aligned} \quad (2.3.4)$$

的等价方程组. 例如在域 \mathbb{Z}_11 上, 方程组

$$\begin{aligned} 3x + 5y + 7z &\equiv 6, \\ 5x + 9y + 6z &\equiv 7, \\ 2x + y + 4z &\equiv 3, \end{aligned}$$

用这个方法转化为 (第一个方程乘以 4 即可转化为 $a_{11} = 1$)

$$\begin{aligned} x + 9y + 6z &\equiv 2, \\ 8y + 9z &\equiv 8, \\ 5y + 3z &\equiv 10, \end{aligned}$$

对 m 用归纳法进行论证, 我们得到

定理 2.9

任意 n 个未知数 m 个方程的联立线性方程组 (2.3.3) 可化为一个等价的方程组. 这个等价方程组的第 i 个方程具有形式

$$x_i + c_{i,i+1}x_{i+1} + c_{i,i+2}x_{i+2} + \dots + c_{in}x_n = d_i, \quad (2.3.5)$$

这里 i 属于 $\{1, 2, \dots, m\}$ 中 r 个数组成的某个子集, 然后再加上 $m - r$ 个形为 $0 = d_k$ 的方程.



如果总是出现情况 2, 则我们得到形为 (2.3.4) 的 m 个方程, 并且称原方程组是相容的. 如果出现情况 1, 则我们可以得到形为 $0 = d_k$ 的一组退化方程. 如果所有的 $d_k = 0$, 则可以不考虑 $0 = d_k$ 的那些方程, 如果有一个 $d_k \neq 0$, 则原方程组 (2.3.3) 是不相容的 (没有解).

详细写出方程组 (2.3.5) 如下

$$\begin{aligned}x_1 + c_{12}x_2 + c_{13}x_3 + \cdots + c_{1n}x_n &= d_1, \\x_2 + c_{23}x_3 + \cdots + c_{2n}x_n &= d_2, \\&\dots\dots\dots \\x_r + \cdots + c_{rn}x_n &= d_r \quad (r \leq m)\end{aligned}\tag{2.3.6}$$

可称为梯形方程组.

任何梯形方程组 (2.3.5) 的解法是容易描述的, 逐次考虑 x_n, x_{n-1}, \dots, x_1 . 如果在该序列中出现的 x_i 是方程组 (2.3.5) 中某个方程的第一个变量, 那么它可通过 x_n, \dots, x_{i+1} 由下列关系确定出来

$$x_i = d_i - c_{i,i+1}x_{i+1} - c_{i,i+2}x_{i+2} - \cdots - c_{in}x_n$$

否则, 这个 x_i 取任意值. 这就证明了

推论 2.2

在定理 2.9 所说的相容情况下, (2.3.3) 的全部解确定如下, 不出现在 (2.3.5) 各式首位的 $m-r$ 个变量 x_k 可以任意取值 (它们是自由变量). 任意选取这些 x_k 后, 代入 (2.4.1) 式并可逐步地算出剩下的变量 x_i .



前面 \mathbb{Z}_{11} 上的方程组可以通过消元法求解得出

$$\left. \begin{aligned}x + 9y + 6z &\equiv 2 \\y + 8z &\equiv 1 \\z &\equiv 7\end{aligned} \right\} \pmod{11}$$

最后得到 $x = 4, y = 0, z = 7$.

如果方程 (2.3.3) 右边的常数 b_i 全都为零, 则称方程组为齐次的. 这类方程组总有 (平凡) 解 $x_1 = x_2 = \cdots = x_n = 0$, 它可能不存在非平凡解, 但是如果变量的个数超过方程的个数, 那么方程组 (2.3.5) 的最后一个方程总还包含可任意取值的自由变量. 此外, 对于齐次方程组来说, 绝不会出现可能矛盾的方程 $0 = d_i$, 因此有

定理 2.10

n 个变量 m 个方程的齐次线性方程组, 当 $m < n$ 时, 总有非全为零的解.



2.4 有序域

如果域 F 包含“正”元素集合 P , 满足 3 中所列出的加法律, 乘法律和三分律, 则称域 F 是有序的. 换句话说, 当把域看成一个整环时, 它是一个有序整环, 则这个域是有序域. 根据经验知道, 全体有理数就构成这样的有序域, 现在我们从构造有理数为整数偶出发来证明这一点, 并进一步指出, 这种“自然”排序的方法, 是把有理数域作成有序域的唯一方法.

首先回忆一下, 任何有序整环中, 非零元素 b 的平方 b^2 总是正的. 如果商 $\frac{a}{b}$ 是正的,

则乘积 $(\frac{a}{b})^2 = ab$ 也必是正的, 反之也真. 因此在任意有序域中

$$\frac{a}{b} > 0 \Leftrightarrow ab > 0, \quad (2.4.1)$$

而有理数 (a, b) 表示商 $\frac{a}{b}$, 因此我们定义有理数 (a, b) 是正的当且仅当在 \mathbb{Z} 中乘积 ab 是正的.

定理 2.11

如果定义 $(a, b) > 0$ 意味着整数 ab 是正的, 则全体有理数构成一个有序域.



我们按前面的习惯 (32) 定义了相等之后, 必须证明与正元素相等的元素是正的⁴: 由 $(a, b) > 0$ 和 $(a, b) \equiv (c, d)$ 推出 $(c, d) > 0$. 这是正确的, 因为 cd 与 b^2cd 同号, ab 与 abd^2 同号, 根据假设 $ad = bc$, 有 $abd^2 = b^2cd$. 所需的加法律、乘法律和三分律也成立. 例如, 两个正的数偶 (a, b) 与 (c, d) 的和是正的, 这是因为, 由 $ab > 0$ 和 $cd > 0$ 推出 $d^2ab > 0$ 和 $b^2cd > 0$, 因此

$$bd(ad + bc) = d^2ab + b^2cd > 0.$$

这就是说和 $(ad + bc, bd)$ 是正的. 最后, 分数“正”元素的定义同表示整数的特殊分数 $(a, 1)$ 的自然顺序是一致的, 这是因为, 根据定义 (2.4.1), 只有当 $a \cdot 1 > 0$ 时, $(a, 1)$ 才是正的.

因为上述定理的证明中只用到“全体整数是有序整环”的假定, 所以它实际上建立了更一般的结果:

定理 2.12

在约定“ D 的元素 a, b 的商是正的当且仅当 ab 是正的”之下, 有序整环 D 的商域 $Q(D)$ 是有序的. 只有按这种方法可以扩展 D 的次序使 Q 成为有序域.



存在很多其他有序域: 实数域, 形为 $a + b\sqrt{2}$ 的域 $\mathbb{Q}(\sqrt{2})$ 和实数域的其他子域. 在任何这样的域中, 绝对值可按3那样定义, 在那里所建立的不等式的性质在这里同样成立. 在任何有序域上, 除任意有序整环上成立的法则之外, 我们还可以证明:

$$0 < \frac{1}{a} \Leftrightarrow a > 0 \quad (2.4.2)$$

$$\frac{a}{b} < \frac{c}{d} \Leftrightarrow abd^2 < b^2cd \quad (2.4.3)$$

$$0 < a < b \Rightarrow 0 < \frac{1}{b} < \frac{1}{a} \quad (2.4.4)$$

$$a < b < 0 \Rightarrow 0 > \frac{1}{a} > \frac{1}{b} \quad (2.4.5)$$

$$a_1^2 + a_2^2 + \cdots + a_n^2 \geq 0 \quad (2.4.6)$$

(2.4.4) 和 (2.4.5) 两个法则在不等式除法中是常见的. 法则 (2.4.6), 即平方和永远非负, 是特别有用的. 例如, 若 $a \neq b$, 则 $(a - b)^2 > 0$, 于是 $a^2 - 2ab + b^2 > 0$, 由此得出

⁴这段话需要这样来理解: 一个有理数其实可以有多种表示方法, 他们之间是相等的, 而前面正元素只对应其中一种表示方法. 例如假设 $\frac{1}{2}$ 是正的, 我们需要证明和它相等的 $\frac{2}{4}$, $\frac{3}{6}$ 之类都是正的, 从而说明相等的定义对于正元素也是合理的, 就是我们通常理解的相等

$a^2 + b^2 > 2ab$, 令 $x = a^2, y = b^2$, 并且两边除以 2, 那么

$$\frac{x+y}{2} > \sqrt{xy} \quad (x \neq y).$$

这表明, 两个不同实数 (正实数) 的算术平均值 $\frac{x+y}{2}$ 大于几何平均值 \sqrt{xy} .

2.5 正整数公设

虽然我们用了全体整数的整环 \mathbb{Z} 作为我们考察基本数系的出发点, 但是这一过程实际上很不严格, 因为它假定负数存在. 本节余下部分我们将指出怎样仅由我们熟悉的正整数的事实导出负整数及其性质. 由此我们指出, 负数存在性的假定如何可以避免.

为一致起见, 我们从列举所有正整数系 \mathbb{Z}^+ 的一些基本性质开始, 这些性质容易从 Section 2.2 的结果推出.

定理 2.13. 正整数性质

\mathbb{Z} 中所有正整数系 \mathbb{Z}^+ 具有下列性质:

- (i) 在所定义的加法和乘法二元运算之下, \mathbb{Z}^+ 是封闭的, 这两个运算满足结合律、交换律和分配律.
- (ii) 在 \mathbb{Z}^+ 中存在乘法单位元素 1, 适合对 \mathbb{Z}^+ 中一切 m 有 $m \cdot 1 = m$.
- (iii) 在 \mathbb{Z}^+ 中, 消去律成立

$$mx = nx \Rightarrow m = n. \quad (2.5.1)$$

- (iv) 对 \mathbb{Z}^+ 中任意两个元素 m 和 n , 下面三种关系恰有一个成立: 或者 $m = n$, 或者 $m + x = n$ 在 \mathbb{Z}^+ 中有一个解, 或者 $m = n + y$ 在 \mathbb{Z}^+ 中有一个解.
- (v) 在 \mathbb{Z}^+ 中数学归纳法原理成立: \mathbb{Z}^+ 的任意子集如果包含 1, 并且当他包含 n 时也包含 $n + 1$, 那么这个子集包含 \mathbb{Z}^+ 中每一个元素.



书中没有给出证明, 有机会尝试一下, 主要是保证每一步都有公设或者已经证明的定理作为依据.

相反的, 如果把这个定理中指出的 (i)~(v) 看作公设, 在下述意义下, 它们完整地描述了正整数: 我们先前定义过的正整数系具有这些性质, 并且可以证明任何其他满足这些公设的系统与这个正整数系同构. 特别注意, 在 \mathbb{Z}^+ 中如果 $m + x = n$, 那么

$$\begin{aligned} n + z &= (m + x) + z = m + (x + z) \\ &= m + (z + x) = (m + z) + x, \end{aligned}$$

因此由 (iv) 知 $m + z = n + z$ 是不可能的. 类似的, $m = n + y$ 同 $m + z = n + z$ 也是不相容的, 因此我们可以得到

$$m + z = n + z \Rightarrow m = n. \quad (2.5.2)$$

而且, 方程 $m + x = n$ 的三种可能性代替了正整数系的那些序的性质.

从这些公设给出的正整数系出发, 我们可以重新构造整数系 \mathbb{Z} . 构造的目的是为了得到一个比 \mathbb{Z}^+ 大的系统, 在这个系统中减法总是可能的. 因此, 作为新元素, 我们引进某

正整数偶 (m, n) ⁵, 这里每个数偶表示方程 $n + x = m$ 的解 (如果是解的话). 这个构造的详细过程类似于整数环构造有理数域 (32).

定义 2.4

一个整数定义为正整数 m 和 n 的一个数偶 (m, n) . 数偶的相等定义为

$$(m, n) \equiv (r, s) \Leftrightarrow m + s = n + r, \quad (2.5.3)$$

而和与积分别定义为

$$(m, n) + (r, s) = (m + r, n + s), \quad (2.5.4)$$

$$(m, n) \cdot (r, s) = (mr + ns, ms + nr), \quad (2.5.5)$$

最后, (m, n) 是“正”的当且仅当对某正整数 x 有 $n + x = m$.



由这些定义引进的数偶实际上满足我们已给出的所有关于整数的公设. 我们首先必须验证, 由 (2.5.3) 引进的“相等”满足自反律、对称律和传递律. 在这个相等意义下, 分别由 (2.5.4) 和 (2.5.5) 给出的和与积是唯一确定的. 把定义 (2.5.4) 和 (2.5.5) 系统地应用到整环的各种形式的定律上, 那么这些定律对于数偶也成立, 这同有理数的讨论几乎一样. 特别, 对刚刚定义的系统, $(2, 1)$ 是单位元素, $(1, 1)$ 是零元素, 并且加法逆元素存在, 这是因为

$$(m, n) + (n, m) \equiv (1, 1), \quad \forall (m, n).$$

下面只要证明数偶的乘法消去律, 就知道全体数偶构成整环. 乘法消去律的证明需要用到定理 2.13 的条件 (iv).

由定理 2.13 的公设 (iv), 每个数偶恰好可写成下面三种形式之一: (m, m) , $(m + x, m)$, $(m, m + x)$. 第一种形式的那些数偶等于零元素 $(1, 1)$; 第二种形式的数偶 $(m + x, m)$ 是正的数偶, 并且可以证明, 数偶具有有序整环的定义中所要求的加法律, 乘法律和三律. 此外,

$$(m + x, m) \equiv (n + y, n) \Leftrightarrow x = y.$$

因此, 如果把“ \equiv ”的数偶看作同一数偶, 那么对应 $x \mapsto (m + x, m)$ 是全体给定的正整数 x 的集合到全体新的正数偶 $(m + x, m)$ 的集合的一个单射. 它甚至是一个单一同态, 这因为由定义 (2.5.4) 和 (2.5.5),

$$\begin{aligned} (m + x, m) + (n + y, n) &= (m + n + x + y, m + n), \\ (m + x, m) \cdot (n + y, n) &= (mn + my + nx + mn + xy, mn + nx + mn + my). \end{aligned}$$

因此新的“正”数偶满足数学归纳法原理. 于是我们就粗略的给出了下面结果的一个证明.

⁵请和卡面有理数域构造那一节做个类比, 其实思路是一致的.

定理 2.14

通过定义 \mathbb{Z} 的任意元素为 \mathbb{Z}^+ 中两个正整数之差这种方式, 正整数系 \mathbb{Z}^+ 可以嵌入较大的系统 \mathbb{Z} 中, 在 \mathbb{Z} 中减法是可能的. 这样构造的系统 \mathbb{Z} 是一个有序整环, 它的正元素满足数学归纳法原理.



数学归纳法蕴含着良序原则. 值得注意的是, 上面粗略的证明只涉及到 \mathbb{Z}^+ 的公设, 反过来, 在包含 \mathbb{Z}^+ 的任意整环中, \mathbb{Z}^+ 的元素之差 $(a-b)$ 必须满足定义 (2.5.3) ~ (2.5.5), 这就证明了

定理 2.15

包含系统 \mathbb{Z}^+ 的任意整环包含一个与整数环 \mathbb{Z} 同构的子整环.



2.6 皮亚诺公设

在正整数集合 $P = \mathbb{Z}^+$ 上, 如果把加法和乘法当作未定义的运算, 我们可以用后继函数

$$S(n) = n + 1 \quad (2.6.1)$$

来定义它们.

定理 2.16

正整数集合 P 和后继函数 S 具有下列性质:

- (i) $1 \in P$,
- (ii) 若 $n \in P$, 则 $S(n) \in P$,
- (iii) P 中没有一个 n , 使得 $S(n) = 1$;
- (iv) 对 P 中 m 和 n , 由 $S(m) = S(n)$ 可推出 $m = n$;
- (v) P 的一个子集如果包含 1, 并且当它包含 n 时, 也包含 $S(n)$, 那么这个子集必等于 P .



这些性质直接从定理 2.13 得到, 特别注意, (v) 是数学归纳法原理.

性质 (i) ~ (v) 称为正整数集合的皮亚诺公设. 正如下面指出的那样, 它们足以证明正整数的所有性质. 我们现在用它们来证明, 原来的整数公设可确定整数集合 (精确到同构).

定理 2.17

在任意有序整环 D 中, 存在唯一的子集 P' 满足关于单位元素 $1'$ 和后继函数 $S'(a) = a + 1'$ 的皮亚诺公设.



直观的, 显然由 $2' = 1' + 1'$, $3' = 1' + 1' + 1'$, \dots 就是这样一个子集. 不过我们希望一个以有序整环公设为依据的正式证明.

D 的所有正元素的集合 D^+ 显然包含 $1'$, 并且满足 (i) 和 (ii), 现在令 Σ 是 D^+ 的所有

子集 T 组成的类, 而 T 具有性质 (i) 和 (ii), 我们定义 P' 是所有这些集合 T 的交集⁶.

由定义, 对于 P' , (i) 和 (ii) 成立, 因为 P' 只包含正元素, (iii) 成立; 因为 $a+1' = b+1'$ 意味着 $a = b$, 所以 (iv) 成立. 为证明 (v), 令 A 是 P' 的子集, 它包含 1, 并且当它包含 a 时也包含 $S(a)$. 那么 A 是前面用到的集合 T 的一个, 于是 P' 包含在 A 中, 因此 $P' = A$. 对 P' , 这就证明了 (v), 同时 (v) 表明 P' 是唯一可能的这样的集合, 因为 P' 满足 (i) 和 (ii).

定理 2.18

定理 2.17 的子集 P' 对于加法、乘法和序而言, 它同构于正整数集合 P .



非正式的, 显然 $1 \mapsto 1', 2 \mapsto 2', \dots$ 产生所要求的同构, 因为 $1' < 1'+1' < 1'+1'+1' < \dots$, 所以这个对应将保持次序. 证明过程就是把这个对应明确化 (对于自然数系来说, 自然应该考虑归纳定义).

首先, 令 $Q(n)$ 是如下命题: P 中整数 $1 \leq x \leq n$ 和 P' 中元素 $\phi_n(x)$ 之间存在唯一的对应 $x \mapsto \phi_n(x)$, 在这对应下:

$$\phi_n(1) = 1', \phi_n(S(x)) = S'(\phi_n(x)), 1 \leq x < n. \quad (2.6.2)$$

显然 $Q(1)$ 成立, 已知 $Q(n)$ 成立, 因此有一个 ϕ_n , 我们可以通过

$$\phi_{n+1}(x) = \phi_n(x), 1 \leq x \leq n; \phi_{n+1}(n+1) = S'(\phi_n(n)),$$

构造唯一的 ϕ_{n+1} , 因此由 $Q(n)$ 成立推出 $Q(n+1)$ 成立. 由归纳法这就证明了 $Q(n)$ 成立.

再有, 如果 $a \leq x \leq n < m$, 对 x 用归纳法, 我们可以证明 $\phi_n(x) = \phi_m(x)$, 因此当 $x \leq n$ 时, $\phi_n(x)$ 是不依赖于 n 的. 令 $\phi(x)$ 表示 P' 的元素, 这就给出了 P 到 P' 的对应 $x \mapsto \phi(x)$, 它具有性质:

$$\phi(1) = 1', \phi(S(x)) = S'(\phi(x)). \quad (2.6.3)$$

P' 的每个元素是 P 的某个元素 x 的对应元素 $\phi(x)$. 因为元素 $\phi(x)$ 的集合包含 $1'$, 并且如果包含任何 $\phi(x)$ 也一定包含 $\phi(x)$ 的后继, 因此根据 P' 的性质 (v), 这个集合就是整个 P' .

在两个集合 P 和 P' 中, 我们有

$$n+1 = S(n), \quad n + S(m) = S(n+m), \quad (2.6.4)$$

$$n \cdot 1 = n, \quad n \cdot S(m) = n \cdot m + m, \quad (2.6.5)$$

从这些方程和 (2.6.3) 式, 对 m 用归纳法, 容易证明

$$\phi(n+m) = \phi(n) + \phi(m),$$

$$\phi(n \cdot m) = \phi(n) \cdot \phi(m),$$

换句话说, ϕ 关于加法和乘法是一个同构.

其次, ϕ 保留次序, 即由 $m < n$, 可推出 $\phi(m) < \phi(n)$. 实际上, 由定义, $m < n$ 意味着

⁶请注意这种处理方式在数学中也是常见的, 为了构造具备某种的集合, 首先找出包含这种性质元素的集合, 然后做交集.

$n - m$ 是正的, 即

$$m < n \Leftrightarrow \exists k \in P, n = m + k. \quad (2.6.6)$$

因此由 $m < n$ 得出 $n = m + k$, 所以 $\phi(n) = \phi(m) + \phi(k)$, 因为 $\phi(k)$ 在 D 中是正的, 所以这就证明了 $\phi(m) < \phi(n)$.

最后 ϕ 是 P 到 P' 的双射, 因为已经知道 $\phi(x)$ 的集合包含整个 P' , 所以只需证明, 由 $n \neq m$ 可推出 $\phi(n) \neq \phi(m)$, 但是 $n \neq m$ 的意思是, 比如说是 $m < n$, 于是 $\phi(m) < \phi(n)$, 因此

$$\phi(n) \neq \phi(m).$$

为概括我们的结论, 我们定义两个有序整环之间的序-同构, 即保留次序的同构. 鉴于定理2.15, 从定理2.18得出下列推论:

推论 2.3

任意有序整环包含一个与 \mathbb{Z} 序-同构的子整环.



这个结果同定理2.6和定理2.7结合起来, 我们有

推论 2.4

任意有序域包含一个与有理数域 \mathbb{Q} 序-同构的子域.



这个结果给出作为最小有序域的有理数域的一个抽象特征.

最后, 在 D 中全体正元素集合是良序的情况下, 容易证明, 定理2.17的集合 P' 是由 D 的所有正元素组成. 这就证明了

推论 2.5

在序-同构意义下, 只存在一个有序整环 \mathbb{Z} , 它的正元素构成良序集合.



这就证明了, 在同构意义下, 整数公设唯一地确定整数集合.

可以不从良序整环公设开始论述整数集合, 而是从皮亚诺公设开始, 其要点是注意到可用递归方程 (2.6.4) 和 (2.6.5) 定义完备的加法表和乘法表. 同定理2.15的证明中几乎一样, 我们可以正式地证明存在唯一的满足 (2.6.4) 的二元运算---加法, 类似的, 存在唯一的满足 (2.6.5) 的乘法, 那么定理2.13中列举的各种性质可用归纳法证明. 然后从皮亚诺公设出发, 2.5节中给出的数偶构造产生全体有理数⁷.

⁷一般都是这个顺序, 从皮亚诺公设出发, 一步步构造整数, 有理数, 实数, 复数.

第三章 多项式

3.1 多项式形式

设 D 为任意整环, 设 x 是较大的整环 E 的任意元素, D 作为 E 的子整环包含在 E 中, 在 E 中, 我们能作 x 同 D 的元素或同 x 本身的和、差与积.

反复进行这些运算, 明显得到下面形式的一切表达式

$$a_0 + a_1x + \cdots + a_nx^n \quad (a_0, \cdots, a_n \in D; a_n \neq 0, \text{当 } n > 0), \quad (3.1.1)$$

这里 x^n 定义为 n 个因子的乘积 $xx \cdots x$. 而反过来, 只用整环公设, 我们可对形为 (3.1.1) 的任意两个表达式进行加、减与乘, 得到第三个这样的表达式. (书中后面举了一个乘法的例子, 这里省略, 毕竟很简单.)

事实上, 设

$$p(x) = a_0 + a_1x + \cdots + a_mx^m$$

$$q(x) = b_0 + b_1x + \cdots + b_nx^n$$

是形为 (3.1.1) 的任意两个表达式. 如果 $m > n$, 那么我们有

$$\begin{aligned} p(x) \pm q(x) &= (a_0 \pm b_0) + \cdots + (a_n \pm b_n)x^n + a_{n+1}x^{n+1} \\ &\quad + \cdots + a_mx^m. \end{aligned} \quad (3.1.2)$$

如果 $m < n$ 可得类似公式, 根据分配律,

$$p(x)q(x) = \sum_{i=0}^m \sum_{j=0}^n a_i b_j x^{i+j},$$

然后把指数相同的项集中在一起, 并将系数相加, 我们有

$$p(x)q(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + a_mb_nx^{m+n} \quad (3.1.3)$$

这个公式中, x^k 的系数为

$$\sum_i a_i b_{k-i}$$

这里对满足 $0 \leq i \leq m$ 和 $0 \leq k-i \leq n$ 的所有 i 求和.

于是我们就证明了下面的结果:

定理 3.1

假设存在一个整环 E , 包含一个与给定整环 D 同构的子整环, 并有元素 x 不在 D 中, 那么关于这个元素 x 的多项式 (3.1.1) 根据公式 (3.1.2) 和 (3.1.3) 相加、相减和相乘, 构成 E 的子整环.



为了证明这样的整环 E 总是存在的, 需要建立下面的定义.

定义 3.1

整环 D 上关于 x 的多项式是指形为 (3.1.1) 的表达式, 整数 n 成为多项式的次数. 两个多项式相等是指它们具有相同的次数, 并且对应的系数都相等.



因为关于符号 x 并没有给出什么假定, 所以表达式 (3.1.1) 也常称为多项式形式 (需要把它同多项式函数加以区别), 符号 x 本身称为未定元.

定理 3.2

如果加法和乘法分别由公式 (3.1.2) 和 (3.1.3) 定义, 那么整环 D 上关于 x 的全体不同的多项式形式构成一个包含 D 在内的新整环 $D[x]$.



证明过程只是去验证各个公设, 这里抄录下来.

由公式 (3.1.3) 推出没有零因子 (乘法消去律), 这是因为, 两个非零多项式形式乘积的首项系数 $a_m b_n$ 是它相应因子的非零首项系数 a_m 和 b_n 的乘积 (非零的). 0 和 1 的性质及加法逆元素的存在性不难从公式 (3.1.2) 和 (3.1.3) 得出.

为了证明交换律、结合律和分配律, 引进“哑”零系数是方便的, 这使得 (3.1.2) 和 (3.1.3) 变成简单形式

$$\sum_{k=0}^{\infty} a_k x^k + \sum_{k=0}^{\infty} b_k x^k = \sum_{k=0}^{\infty} (a_k + b_k) x^k, \quad (3.1.2')$$

$$\left(\sum_{k=1}^{\infty} x^k \right) \left(\sum_{k=0}^{\infty} b_k x^k \right) = \sum_{k=0}^{\infty} \left(\sum_{i+j=k} a_i b_j x^k \right), \quad (3.1.3')$$

这里除了有限多个系数之外全都是零. 那么任何一个定律, 比如分配律, 只要把定律的两边按照法则 (3.1.2') 和 (3.1.3') 乘起来就可以验证, 这因为,

$$\begin{aligned} & \left(\sum_k a_k x^k \right) \left(\sum_k b_k x^k + \sum_k c_k x^k \right) \\ &= \sum_k \left[\sum_{i+j=k} a_i (b_j + c_j) \right] x^k \\ & \left(\sum_k a_k x^k \right) \left(\sum_k b_k x^k \right) + \left(\sum_k a_k x^k \right) \left(\sum_k c_k x^k \right) \\ &= \sum_k \left[\left(\sum_{i+j=k} a_i b_j \right) + \left(\sum_{i+j=k} a_i c_j \right) \right] x^k \end{aligned}$$

并证明这两个等式右边的 x 的每个幂 x_i^k 的系数相等. 根据整环 D 的分配律, 两个表达式中 x 的 k 次幂的系数是相同的. 类似的论证可证其余定律, 从而完成定理 3.2 的其他证明.

现在回忆一下 32 节的定理 2.7, 我们会看到, 如果我们定义 D 上关于未定元 x 的有理形式为带有非零分母多项式形式的形式商,

$$\frac{p(x)}{q(x)} = \frac{a_0 + a_1 x + \cdots + a_m x^m}{b_0 + b_1 x + \cdots + b_n x^n},$$

$$(a_i, b_j \in D; a_m \neq 0, \text{ 当 } m > 0; b_n \neq 0)$$

并由 32 节的定义 (2.2.1), (2.2.2) 和 (2.2.3) 来分别定义相等, 加法和乘法, 这样我们便可得到一个域.

推论 3.1

任意整环 D 上关于未定元 x 的有理形式构成一个域, 这个域记作 $D(x)$.



这一节有几个习题是设计扩充知识: 多项式的形式导数.

练习 3.1 $p(x) = a_0 + a_1x + \cdots + a_nx^n$ 的“形式导数”定义为 $p'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}$. 证明, 在任意整环上,

(a) $(cp)' = cp'$ (c 为常数);

(b) $(p+q)' = p' + q'$;

(c) $(pq)' = p'q + pq'$;

(d) $(p^n)' = np^{n-1}p'$.

练习 3.2 设 $p(y)$ 和 $q(x)$ 分别是关于未定元 y 和 x 的多项式形式, 证明: 把 $y = q(x)$ 代入 $p(y)$, 产生一个多项式 $p(q(x))$. 根据习题 3.1 中定义的形式导数, 证明: $[p(q(x))]' = p'(q(x))q'(x)$.

3.2 多项式函数

设 D 为任意整环, 又设

$$f(x) = a_0 + a_1x + \cdots + a_mx^m$$

是 D 上关于 x 的任意多项式形式. 如果未定元 x 用一个元素 $c \in D$ 代替, $f(x)$ 就不再是一个虚的表达式, 它可以看作 D 中一个确定元素

$$a_0 + a_1c + \cdots + a_mc^m.$$

换句话说, 如果 x 被看作在微积分学意义下的一个独立变量, 而不是看作 D 外面的抽象符号, 那么 $f(x)$ 就成为普通的函数: “如果 x 已知 (值为 c), 那么 $f(x)$ 就被确定可 (值为 $f(c)$)”. 我们把它抽象化, 一般地定义变量在 D 上的“函数” f 是一个规则: 它给 D 上每个元素 x 确定一个“值” $f(x)$, 这个值也在 D 中. 我们定义两个这样的函数相等 (记作 $f = g$) 当且仅当对所有的 x , $f(x) = g(x)$. 两个函数的和 $h = f + g$, 差 $q = f - g$ 及积 $p = fg$ 分别通过对所有的 x 计算 $h(x) = f(x) + g(x)$, $q(x) = f(x) - g(x)$ 和 $p(x) = f(x)g(x)$ 来定义的. 常量函数是取值 b 与 x 无关的函数; 恒等函数是函数 j , 它满足对所有的 x , $j(x) = x$.

定义 3.2

多项式函数是可以写成形式 (3.1.1) 的函数.



因为推导公式 (3.1.2) 和 (3.1.3) 所用的法则在任何整环中都是成立的, 所以不管未定元 x 取什么值 c (在 D 中), 公式 (3.1.2) 和 (3.1.3) 都成立. 也就是说它们是恒等式, 因此多项式函数的和与积也可以通过公式 (3.1.2) 和 (3.1.3) 来计算. 后面将说明, D 上全体多项式函数构成一个交换环.

根据定义, 每个形式 (3.1.1) 都确定一个唯一的多项式函数, 每个多项式函数至少由一个这样的形势来确定. 因此无疑存在一个保持和与积德映射, 它把任意给定整环 D 上

的全体多项式形式的集合映射到全体多项式函数的集合。（这样的对应称为映上同态或满同态）

如果可以确定映射是一一的, 我们就知道它是一个同构. 因此, 从抽象代数的观点来看, 我们可以忽略多项式形式与多项式函数之间的差别. 可惜情况并非如此. 事实上, 在模 3 整数域 \mathbb{Z}_3 上, $f(x) = x^3 - x$ 和 $g(x) = 0$ 这两个不同的形式确定了同一个函数---这个函数恒等于零. 根据费马定理, 在 \mathbb{Z}_p 上, $x^p - x$ 与 0 是相同的. 因此在任意 \mathbb{Z}_p 上, 多项式函数相等不同于多项式形式相等.

我们现在将指出, 在上述例子中, 由于系数所在的整环是有限的, 发生这一事实并不奇怪. 在有理数域上, 我们并不能构造出一个这样的例子. 我们在说明此事之前先回忆一些基本定义. 所谓非零形式 (3.1.1) 的次数, 我们指的是它的最大指数, 即 n . 最高次项 $a_n x^n$ 称为它的首项, a_n 称为它的首项系数. 如果 $a_n = 1$, 多项式则称为首一多项式.

定理 3.3

整环 D 上的一个多项式形式 $r(x)$ 可被 $x - a$ 整除当且仅当 $r(a) = 0$.



这里“ $r(x)$ 可被 $x - a$ 整除”这句话的意思是 $r(x) = (x - a)s(x)$, 其中 $s(x)$ 是 D 上的某一个多项式形式.

设 $r(x) = c_0 + c_1 x + \cdots + c_n x^n$ ($c_n \neq 0$), 对每个 a , 我们有

$$\begin{aligned} \sum_{k=0}^n c_k x^k - \sum_{k=0}^n c_k a^k &= \sum_{k=0}^n (x^k - a^k) \\ &= \sum_{k=0}^n c_k [(x - a)(x^{k-1} + x^{k-2}a + \cdots + a^{k-1})]. \end{aligned}$$

因此 $r(x) - r(a) = (x - a)s(x)$, 这里 $s(x)$ 是 $n - 1$ 次多项式形式. 反之, 如果 $r(x) = (x - a)s(x)$ 中用 a 代替 x , 则得 $r(a) = 0$.

推论 3.2

整环 D 上的 n 次多项式 $r(x)$ 在 D 中至多有 n 个零点.



($r(x)$ 的零点是指方程 $r(x) = 0$ 的根, 即元素 $a \in D$ 使得 $r(a) = 0$.)

如果 a 是一个零点, 那么根据定理有 $r(x) = (x - a)s(x)$, 其中 $s(x)$ 的次数为 $n - 1$. 由归纳法, $s(x)$ 至多有 $n - 1$ 个零点, 可是根据 1.2 定理 1.1, $r(x) = 0$ 当且仅当 $x = a$ 或 $s(x) = 0$, 因此 $r(x) = 0$ 至多有 n 个零点.

定理 3.4

如果整环 D 是无限的, 那么 D 上定义同一个函数的两个多项式形式具有相等的系数.



像 (3.1.1) 那样, 设 $p(x)$ 和 $q(x)$ 是两个给定的关于未定元 x 的多项式形式. 如果它们确定同一个函数, 那么对于 D 中选取的每个元素 a 都有 $p(a) = q(a)$; 然而我们所希望的结论则是 $p(x)$ 和 $q(x)$ 的次数相等, 对应的系数相同. 如果用差 $r(x) = p(x) - q(x)$ 来表示, 这就是说, 对 D 中一切 a , $r(a) = c_0 + c_1 a + \cdots + c_n a^n = 0$ 可推出 $c_0 = c_1 = \cdots = c_n = 0$.

这个结论可由定理3.3的推论推出, 因为如果系数 c_i 不全为零, 那么在 D 中至多有 n 个 x 使多项式 $r(x)$ 为零, 因为 D 是无限的, 所以还剩下一些 x 值使 $r(x) \neq 0$, 这与 $r(x)$ 在 D 上为零相矛盾.

于是, 如果 D 是无限的, 则多项式函数和多项式形式这两个概念是等价的 (用代数学的术语说就是, 多项式函数环同构于多项式形式环).

另一方面, 如果 D 是包含元素 a_1, a_2, \dots, a_n 的有限整环, 则定理??一定不成立, 例如在这种情况下, n 次首一多项式形式 $(x - a_1)(x - a_2) \cdots (x - a_n)$ 同形式 0 确定了同一个函数.

因为同构于整环的任意系统本身也是一个整环, 所以定理3.4蕴含着下面的推论.

推论 3.3

任意无限整环上全体多项式函数构成一个整环.



如果 D 为无限域, 则不同的有利形式确定不同的有理函数, 所以 D 上全体有理函数构成一个域. (留心, 一个有理函数不是在一切点上都有定义, 只是使那些分母不为零的点上才有定义, 因此, 如果 D 是一个域, 那么除有限个点外的全部点上它是有定义的.)

我们常常希望找出一个次数最小的多项式 $p(x)$, 使它在域 F 中的 $n+1$ 个已知点 a_0, a_1, \dots, a_n 上分别取 F 中给定的值 y_0, y_1, \dots, y_n , 即

$$p(a_i) = y_i; (i = 0, \dots, n; a_i \neq a_j, \text{ 当 } i \neq j.) \quad (3.2.1)$$

这称为多项式插值问题.

为了解决这个问题, 考虑多项式

$$\begin{aligned} q_i(x) &= \prod_{j \neq i} (x - a_j) \\ &= (x - a_0) \cdots (x - a_{i-1})(x - a_{i+1}) \cdots (x - a_n) \end{aligned}$$

显然, 当 $j \neq i$ 时, $q_i(a_j) = 0$, 而

$$C_i = q_i(a_i) = \prod_{j \neq i} (a_i - a_j) \neq 0.$$

因此 C_i^{-1} 存在, 并且下面这个次数为 n 或低于 n 的多项式

$$p(x) = \sum_{i=0}^n C_i^{-1} y_i q_i(x) = \sum_{i=0}^n \frac{y_i \prod_{j \neq i} (x - a_j)}{\prod_{j \neq i} (a_i - a_j)} \quad (3.2.2)$$

满足方程 (3.2.1). 公式 (3.2.2) 成为拉格朗日 (Lagrange) 插值公式.

由定理3.3知, 至多有一个 n 次或低于 n 次的多项式能够满足方程 (3.2.1): 因为两个这样的多项式之差有 $n+1$ 个零点, 于是它必为零多项式. 这就证明了下面的结果:

定理 3.5

存在一个而且只存在一个 n 次或低于 n 次的多项式形式, 在 $n+1$ 个不同点上取给定的值.



3.3 交换环的同态

设 D 是任意给定的整环, 又 $D\langle x \rangle$ 设表示 D 上的多项式函数集合. 对所有 $x \in D$, $f(x) + g(x) = g(x) + f(x)$, $0 + f(x) = f(x)$, $1 \cdot f(x) = f(x)$, 等等. 因此, 加法和乘法满足交换律, 结合律和分配律; 加法和乘法的单位元素存在; 并且加法逆元素存在. 概括起来, $D\langle x \rangle$ 除乘法消去律外满足整环的所有公设. 当 D 为有限整环时, 消去律不成立, 这因为存在非零因子的乘积 $(x - a_1)(x - a_2) \cdots (x - a_n)$ 为零.

换句话说, $D\langle x \rangle$ 是一个交换环. 为方便起见, 我们在此重述这个定义.

定义 3.3. 交换环

交换环在称为加法和乘法的两种二元运算之下封闭的集合, 这两种运算满足交换律和结合律, 并且进一步有

- (i) 满足乘法对加法的分配律;
- (ii) 存在加法单位元素 (零) 0 , 并且存在加法逆元素;
- (iii) 存在乘法单位元素 1^a .

^a有些书没有这一条



任意整环 D 上的全体函数构成的系统 D^* , 为我们提供了另一个交换环的例子, 这里加法和乘法像 3.2 里那样定义. 甚至于定义在无限整环 D 上的全体函数集合 D^* 中也存在零因子. 例如, 如果 D 为任意有序整环, 我们定义 $f(x) = |x| + a$, $g(x) = |x| - 1$, 那么 $f \cdot g = h$, $h(x) = |x|^2 - x^2 = 0$, 对一切 x 成立. 但是 $f \neq 0$, $g \neq 0$. 另一方面, D^* 具有整环定义中所有其它性质. 我们只要在每步证明的右边简单写上“对一切 x ”, 根据 D 的定律便可得到 D^* 的相应定律的证明. (这里略). 再有, 如果我们定义 e 为一个常数函数, 即 $e(x) = 1$ 对一切 x , 那么 $e(x)f(x) = 1 \cdot f(x) = f(x)$ 对一切 x 和 f , 因此 $e \cdot f = f$, 于是 e 是 D^* 的乘法单位元素. (乘法消去律为什么不能按这种方式证明. 因为要想成立消去律, 必须对一切 x 成立, 可是对于两个函数 f 和 g , 完全可以做到 $f(x)$ 等于零的时候, $g(x)$ 不等于零, 反过来 $g(x)$ 等于零的时候, $f(x)$ 不等于零, 就像前面所举例子. 这样对于单个 x 来说, 消去律可以使用, 可是对于函数还是不成立.) 因为上面没有一处用到乘法消去律, 所以我们可以断言:

引理 3.1

任意交换环 A 上的全体函数构成一个交换环.



现在让我们定义交换环 A 的子环为 A 的这样的子集: 如果它包含任意两个元素 f 和 g , 则它包含 $f \pm g$ 和 fg , 并且还包含着 A 的单位元素.

由定理 3.1, 任意整环 D 上多项式函数集合 $D\langle x \rangle$, (i) 它是 D 上所有函数环 D^* 的子环, (ii) 它包含所有常数函数和恒等函数, (iii) 它包含在任何其他满足 (ii) 的 D^* 的子环之中. 按这种定义 $D\langle x \rangle$ 是由常数函数和恒等函数生成的 D^* 的子环, 这给出多项式函数概念的一个简单的代数特征.

下面将同构的概念一般化, 可以更深刻地认识交换环.

定义 3.4

一个函数 $\phi: a \mapsto a\phi$, 它把交换环 R 映射到交换环 R' , ϕ 称为同态, 当且仅当它满足下列条件: 对所有 $a, b \in R$ 有

$$(a+b)\phi = a\phi + b\phi, \quad (3.3.1)$$

$$(ab)\phi = (a\phi)(b\phi), \quad (3.3.2)$$

并且把 R 的单位元素映射到 R' 的单位元素.



这些条件表明, 同态保持加法和乘法. 它们是按照 1.11 和 1.12 中简洁的记号写出来的, 其中 $a\phi$ 表示用 ϕ 变换 a , 如果我们写 $\phi(a)$ 代替 $a\phi$, 则 (3.3.1) 和 (3.3.2) 分别写成 $\phi(a+b) = \phi(a) + \phi(b)$ 和 $\phi(ab) = \phi(a)\phi(b)$. 显然一个同构恰是一个双射的同态.

我们容易验证, 从 n 到包含 n 的剩余类 (对任意固定模 m) 的函数是一个同态 $\mathbb{Z} \mapsto \mathbb{Z}_m$, 它把整数环 \mathbb{Z} 映上模 m 剩余类环 \mathbb{Z}_m . 我们现在证明另一个容易的结果:

引理 3.2

设 ϕ 是从交换环 R 到交换环 R' 的同态, 那么 0ϕ 是 R' 的零元素, 并且对所有 $a, b \in R$, 有 $(a-b)\phi = a\phi - b\phi$.



由 (3.3.1) 式, $0\phi = (0+0)\phi = 0\phi + 0\phi$, 这就证明了 0ϕ 是 R' 的零元素. 类似的, 如果 $x = a - b$ 在 R 中, 那么 $b + x = a$ 并且 $a\phi = (b+x)\phi = b\phi + x\phi$, 于是 $x\phi = a\phi - b\phi$ 在 R' 中.

定理 3.6

从任意整环 D 上的多项式形式整环 $D[x]$ 到 D 上多项式函数环 $D\langle x \rangle$ 的对应 $p(x) \mapsto f(x)$ 是一个同态.



对 D 中任意元素 x , 在 D 中元素 $p(x)$ 和 $q(x)$ 的加法和乘法必须遵循恒等式 (3.1.2) 和 (3.1.3), 因为在 3.1 节中这些恒等式的推导只用到整环公设.

定理 3.4 的结果指出, 如果 D 是无限的, 那么定理 3.6 中的同态是一个同构.

3.4 多元多项式

前面讨论的都是单变量 (未定元) x 的多项式, 但是很多结果不难推广到多变量 (未定元) x_1, \dots, x_n 的情形.

定义 3.5

整环 D 上关于未定元 x_1, \dots, x_n 的多项式形式可递推地定义为整环 $D[x_1, \dots, x_{n-1}]$ 上关于变量 x_n 的多项式形式, 而 $D[x_1, \dots, x_{n-1}]$ 是 D 上关于变量 x_1, \dots, x_{n-1} 的多项式形式组成的整环 (简单地说, $D[x_1, \dots, x_n] = D[x_1, \dots, x_{n-1}][x_n]$). 整环 D 上关于变量 x_1, \dots, x_n 的多项式函数是由常数函数 $f(x_1, \dots, x_n) = c$ 和 n 个恒等函数 $f_i(x_1, \dots, x_n) = x_i$ ($i = 1, \dots, n$) 通过加

法、减法和乘法构造出来的。



根据定理3.4对 n 用归纳法得

定理 3.7

如果 D 是无限的, 那么 D 上关于变量 x_1, \dots, x_n 的每个多项式函数可按一种且只有一种方法表示为多项式形式. 不管 D 是无限的还是有限的, $D[x_1, \dots, x_n]$ 是一个整环.



从定义明显看出, 变量下标的每个置换, 引导出关于 $D\langle x_1, \dots, x_n \rangle$ 的一个自然的自同构, 其中 $D\langle x_1, \dots, x_n \rangle$ 是 n 个变量多项式函数的交换环. 如果 D 是无限的, 由定理3.7得到, 上述结论对多项式形式也是正确的 (这些定义对于变量不是对称的). 现在我们证明, 这个结论对任意整环 D 都是正确的.

定理 3.8

变量下标的每个置换, 引导出 $D[x_1, \dots, x_n]$ 上的不同自同构.



考虑两个未定元 x, y 的情况, $D[y, x]$ 的每个形式

$$p(y, x) = \sum_i \left(\sum_j a_{ij} y^j \right) x^i.$$

可以根据 $D[y, x]$ 中的分配律、交换律和结合律重新排列的出一个形为

$$p(y, x) = \sum_j \left(\sum_i a_{ij} x^i \right) y^j.$$

的表达式. 根据这个表达式的形式, 似乎可以把它解释为整环 $D[x, y]$ (先 x 后 y) 中的多项式 $p'(x, y)$, 这样建立的对应 $p(y, x) \mapsto p'(x, y)$ 是一对一的---每个非零元素 a_{ij} 的有限集合恰好对应 $D[y, x]$ 中一个元素, 也恰好对应 $D[x, y]$ 中一个元素. 最后, 因加法和乘法的法则 (3.1.2) 和 (3.1.3) 可以从整环的公设推出, 而 $D[y, x]$ 和 $D[x, y]$ 这两个是整环, 所以我们看到这个对应保持了和与积.

n 个未定元的情况可以用更复杂更一般的记号类似地处理, 或者从两个变量的情况出发用归纳法推导出.

于是 $D[x_1, \dots, x_n]$ 事实上对称地依赖于 x_1, \dots, x_n . 这就启发我们构造一种 $D[x_1, \dots, x_n]$ 的定义, 从这定义对称性是一目了然的. 在 $n = 2$ 情况下对于整环 $D'' = D[x, y]$, 可以粗略地说明如下. 第一, D'' 是由 x, y 和 D 的元素生成的 (D'' 的每个元素可以由 x, y 和 D 的元素反复进行求和与求积运算而得). 第二, 生成元 x 和 y 是 D 上并立未定元 (或者是在 D 上代数独立的). 这就意味着, 系数 a_{ij} 在 D 上的有限和 $\sum_{i,j} a_{ij} x^i y^j$ 可以为零当且仅当所有系数全为零. 这两个性质以对称的方式唯一确定整环 $D[x, y]$.

3.5 辗转相除法

多项式辗转相除法 (有时称为“多项式长除法”) 为下面的多项式相除提供了一个标准形式: 用一个多项式 $a(x)$ 去除另一个多项式 $b(x)$ 以便得到商式 $q(x)$ 和余式 $r(x)$, $r(x)$

的次数低于除式 $a(x)$ 的次数. 我们现在将证明, 这个辗转相除法, 虽然通常是在有理系数多项式上进行, 但实际上对于系数在任意域上的多项式都是可行的.

定理 3.9

如果 F 为任意域, $a(x) \neq 0$ 和 $b(x)$ 是 F 上的任意多项式, 那么我们可以找到 F 上的多项式 $q(x)$ 和 $r(x)$, 使得

$$b(x) = q(x)a(x) + r(x) \quad (3.5.1)$$

成立, 这里 $r(x)$ 或者为零或者它的次数低于 $a(x)$ 的次数.



证明概要: 从 $b(x)$ 中减去除式 $a(x)$ 与适当的单项式 cx^k 的乘积, 逐步消去被除式 $b(x)$ 的最高项. 如果 $a(x) = a_0 + a_1x + \cdots + a_mx^m$ ($a_m \neq 0$), $b(x) = b_0 + b_1x + \cdots + b_nx^n$ ($b_n \neq 0$), 并且 $b(x)$ 的次数 n 不低于 $a(x)$ 的次数 m , 则我们可以做差

$$\begin{aligned} b_1(x) &= b(x) - \frac{b_n}{a_m}x^{n-m}a(x) \\ &= 0 \cdot x^n + (b_{n-1} - \frac{a_{m-1}b_n}{a_m})x^{n-1} + \cdots \end{aligned} \quad (3.5.2)$$

$b_1(x)$ 的次数低于 n 或者为零. 然后我们可以重复这一过程直到余式的次数低于 m 为止.

辗转相除法的正式证明可以根据数学归纳法第二原理, 设 m 是 $a(x)$ 的次数. 任何次数 $n < m$ 的多项式 $b(x)$ 可表示成 $b(x) = 0 \cdot a(x) + b(x)$, 其商式 $q(x) = 0$. 对次数 $n \geq m$ 的多项式, 由 (3.5.2) 式得到

$$b(x) = b_1(x) + \frac{b_n}{a_m}x^{n-m}a(x), \quad (3.5.3)$$

其中 $b_1(x)$ 的次数 $k < n$, 除非 $b_1(x) = 0$, 由数学归纳法第二原理, 我们可以假定, 表达式 (3.5.1) 对于一切次数 $k < n$ 的多项式都成立. 于是我们有

$$b_1(x) = q_1(x)a(x) + r(x), \quad (3.5.4)$$

这里 $r(x)$ 的次数低于 m , 除非 $r(x) = 0$. 把 (3.5.4) 式代入 (3.5.3) 式中, 我们得到所要求的方程 (3.5.1).

$$b(x) + [q_1(x) + \frac{b_n}{a_m}x^{n-m}]a(x) + r(x).$$

特别是, 如果多项式 $a(x) = x - c$ 是线性首一的, 那么 (3.5.1) 中的余式是一个常数 $r = b(x) - (x - c)q(x)$, 如果我们令 $x = c$, 这个方程给出 $r = b(c) - 0q(c) = b(c)$. 因此我们有

推论 3.4

用 $x - c$ 去除多项式 $p(x)$, 其余数是 $p(c)$. (称为余数定理)



当 (3.5.1) 中的余式是零时, 我们就称 $b(x)$ 可被 $a(x)$ 整除. 更确切地说, 如果 $a(x)$ 和 $b(x)$ 是整环 D 上的两个多项式形式, 那么, 在 D 上 (或在 $D[x]$ 中) $b(x)$ 可被 $a(x)$ 整除当且仅当存在某个多项式形式 $q(x) \in D[x]$, 使得 $b(x) = q(x)a(x)$.

3.6 单位与相伴

我们可以得到关于多项式的完全类似于算术基本定理的定理（或称为唯一因子分解定理）。在这个类比中，“不可约多项式”扮演素数的角色，它的定义如下：

定义 3.6

一个多项式形式如果它可以分解出系数在 F 上，次数较低的多项式因子，则称它为 F 上可约多项式，否则称它为 F 上不可约多项式。



多项式 $x^2 + 4$ 在有理数域上是不可约的。如果不然， $(x^2 + 4 = (x + a)(x + b))$ 。令 $x = -b$ 代入上式得 $(-b)^2 + 4 = 0$ ，因此 $(-b)^2 = -4$ ，这显然是不可能的，因为在这个域中一个数的平方不可能是负的。因为在任意有序域中，同样的论证也成立，所以我们得出结论：在实数域或其他任意有序域上， $x^2 + 4$ 也是不可约的。

为了阐明不可约多项式和素数之间的类似，我们现在对任意整环 D 来定义某些整除性的概念，例如对多项式环 $Q[x]$ ，整数环 \mathbb{Z} 或者别的整环来定义。

D 的元素 a 可被 b 整除（记作 $b|a$ ）的定义是，在 D 中存在某个元素 c 使 $a = cb$ 。如果 $b|a$ 而且 $a|b$ ，则称两个元素 a 和 b 是相伴的。单位元素 1 的相伴称为单位。因为对一切 a ，有 $1|a$ ，所以 u 是 D 中的单位当且仅当它在 D 中有乘法逆元素 u^{-1} ，使得 $1 = uu^{-1}$ 。具有这个性质的元素也称为可逆元素。

如果 a 和 b 是相伴， $a = cb$ 并且 $b = c'a$ ，因此 $a = cc'a$ 。由消去律得 $1 = cc'$ ，于是 c 和 c' 都是单位。反过来，如果 u 是单位，则 $a = ub$ 是 b 的相伴。因此两个元素是相伴当且仅当其中每一个可以从另外一个乘以单位因子而得到。

例 3.1 在域中，每个 $a \neq 0$ 是单位。（因为每个非零元可逆，存在逆元素。）

例 3.2 在整数环 \mathbb{Z} 中，单位只有 ± 1 ，因此任何 a 的相伴元是 $\pm a$ 。

例 3.3 在未定元 x 的多项式环 $D[x]$ 中，乘积 $f(x) \cdot g(x)$ 的次数是这两个因子的次数之和。因此任何元素 $b(x)$ 如果有多项式逆（即 $a(x)b(x) = 1$ ），它必须是零次多项式 $b(x) = b$ 。这样常数多项式 b 有逆当且仅当 b 在 D 中有逆。因此 $D[x]$ 的单位都是 D 的单位。

如果 F 是域，那么多项式环 $F[x]$ 的单位恰是 F 的非零常数，因此两个多项式 $f(x)$ 和 $g(x)$ 在 $F[x]$ 中相伴当且仅当每一个是另外一个的常数倍。

例 3.4 在一切数 $a + b\sqrt{2}$ （ a, b 为整数）构成的整环 $\mathbb{Z}[\sqrt{2}]$ 中，由 $(a + b\sqrt{2})(x + y\sqrt{2}) = 1$ 得出 $x = \frac{a}{a^2 - 2b^2}$ ， $y = -\frac{b}{a^2 - 2b^2}$ ---这些都是整数当且仅当 $a^2 - 2b^2 = \pm 1$ 。于是 $1 \pm \sqrt{2}$ 和 $3 \pm 2\sqrt{2}$ 是 $\mathbb{Z}[\sqrt{2}]$ 中的单位，而 $2 + \sqrt{2}$ 不是 $\mathbb{Z}[\sqrt{2}]$ 中的单位。

任意整环 D 的元素 b 可被它的一切相伴整除，还可被一切单位整除。这些相伴和单位称为 b 的“假因子”。不是单位也不具有真因子的元素称为 D 中素元素或称它在 D 中是不可约的。

例 3.5 在任意域 F 上，线性多项式 $ax + b$ （ $a \neq 0$ ）是不可约的，这是因为它的因子只是常数（单位）或是它本身的常数倍（相伴）。

例 3.6 考虑“高斯整数”环 $\mathbb{Z}[\sqrt{-1}]$ ，它是由所有形为 $a + b\sqrt{-1}$ （其中 $a, b \in \mathbb{Z}$ ）的数组

成. 如果 $a + b\sqrt{-1}$ 是单位, 那么对某个 $c + d\sqrt{-1}$, 我们有

$$\begin{aligned} 1 &= (a + b\sqrt{-1})(c + d\sqrt{-1}) \\ &= (ac - bd) + (ad + bc)\sqrt{-1} \end{aligned}$$

因此 $ac - bd = 1, ad + bc = 0$, 并容易验证

$$1 = (ac - bd)^2 + (ad + bc)^2 = (a^2 + b^2)(c^2 + d^2)$$

因为 $a^2 + b^2, c^2 + d^2$ 都是非负整数, 所以我们推断 $a^2 + b^2 = c^2 + d^2 = 1$; 于是只可能是: $1, -1, \sqrt{-1}$ 和 $-\sqrt{-1}$ 给出四个单位.

引理 3.3

在任意整环 D 中, 关系 “ a 和 b 相伴” 是一个等价关系.



3.7 不可约多项式

多项式代数中的一个基本问题是寻求判别给定域上多项式可约性有效方法, 这种判别自然完全依赖于所考虑的域 F . 例如, 在复数域 \mathbb{C} 上, 多项式 $x^2 + 1$ 分解为 $x^2 + 1 = (x + \sqrt{-1})(x - \sqrt{-1})$. 事实上, 后面将指出, $\mathbb{C}[x]$ 中只有线性多项式是不可约的. 而 $x^2 + 1$ 在实数域 \mathbb{R} 上是不可约的.

再有, 因为 $x^2 - 28 = (x - \sqrt{28})(x + \sqrt{28})$, 所以多项式 $x^2 - 28$ 在实数域上是可约的, 但是这个多项式在有理数域上是不可约的. 后面我们将严格证明它.

引理 3.4

一个二次或三次多项式 $p(x)$ 在域 F 上是不可约的, 除非对某个 $c \in F$, 有 $p(c) = 0$.



把 $p(x)$ 任意分解成次数较低的多项式, 其中一个因子必是线性的, 这因为多项式乘积的次数等于全体因子的次数.

定理 3.10

设 $p(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ 是整系数多项式. 方程 $p(x) = 0$ 的任何有理根 $\frac{r}{s}$ 必满足 $r|a_n$ 和 $s|a_0$.



假设对某个分数 $x = \frac{r}{s}$ 满足 $p(x) = 0$. 约掉 b 和 c 的最大公因子后, 我们可以把 $\frac{r}{s}$ 表示成两个互素整数 r 和 s 的商 $\frac{r}{s}$, 把它代入 $p(x)$ 得

$$0 = s^n p\left(\frac{r}{s}\right) = a_0r^n + a_1r^{n-1}s + \cdots + a_ns^n, \quad (3.7.1)$$

因此

$$-a_0r^n = s(a_1r^{n-1} + \cdots + a_ns^{n-1})$$

所以 $s|a_0r^n$, 但是 $(s, r) = 1$, 因此有 $s|a_0$, 类似地, 因为,

$$-a_ns^n = r(a_0r^{n-1} + a_1r^{n-2}s + \cdots + a_{n-1}s^{n-1}),$$

所以有 $r|a_n$.

推论 3.5

整系数首一多项式的任意有理根都是整数.



现在容易证明 $x^2 - 28$ 在 \mathbb{Q} 上是不可约的. 根据推论, $x^2 = 28$ 意味着 $x = \frac{r}{s}$ 是一个整数. 但是, 当 $|x| \geq 6$ 时 $x^2 - 28 > 0$, 当 $|x| \leq 5$ 时 $x^2 - 28 < 0$, 因此没有一个整数可能是 $x^2 - 28 = 0$ 的根, 所以 $x^2 - 28$ 在有理数域上说不可约的.

有理数域 \mathbb{Q} 上多项式的不可约性的一般判别法是没有的.

3.8 唯一因子分解定理

整个这一节我们将研究整环 $F[x]$ 上的因子分解. $F[x]$ 是由域 F 上关于未定元 x 的多项式形式组成. 主要结果是: 因子分解 (分解成不可约 (素) 因子) 是唯一的. 其证明类似于算术基本定理, 实际上是形式上的重复. 这个类比包含着下面基本概念, 这个概念将在后面做系统讨论.

定义 3.7. 理想

交换环 R 的非空子集 C 称为理想是指 C 满足: 由 $a \in C$ 和 $b \in C$ 可推出 $a \pm b \in C$, 由 $a \in C$ 和 $r \in R$ 可推出 $ra \in C$.



对任意 $a \in R$, a 的所有倍数 ra 的集合是一个理想. 这因为对所有 $r, s \in R$ 有

$$ra \pm sa = (r \pm s)a, \quad s(ra) = (sr)a.$$

这样的理想称为主理想. 我们将指出, 任何 $F[x]$ 中的所有理想是主理想.

定理 3.11

在任何域 F 上, $F[x]$ 的任何理想 C , (i) 或者仅由零组成, (ii) 或者由任何次数最低的非零元素 $a(x)$ 的倍数 $q(x)a(x)$ 的集合组成.



证明 如果 $C \neq \{0\}$, 则 C 包含一个次数最低的非零多项式 $a(x)$, 其次数记作 $d(a)$, C 还包含 $a(x)$ 的所有倍数 $q(x)a(x)$. 这种情况下, 如果 $b(x)$ 是 C 的任一多项式, 根据定理 3.9, 有某个 $r(x) = b(x) - q(x)a(x)$ 的次数小于 $d(a)$, 但是根据假设, C 包含 $r(x)$, 由 C 的构造知 C 不包含次数小于 $d(a)$ 的非零多项式, 因此 $r(x) = 0$, 所以 $b(x) = q(x)a(x)$. 定理获证.

现在设 $a(x)$ 和 $b(x)$ 是任意两个多项式, 考虑以任意多项式 $r(x)$ 和 $s(x)$ 作为系数的 $a(x)$ 和 $b(x)$ 所有“线性组合” $s(x)a(x) + r(x)b(x)$ 构成的集合 C , 这个集合显然是非空的, 并且包含着该集合元素的任意和, 差或倍数, 这是因为

$$\begin{aligned} (sa + tb) \pm (s'a + t'b) &= (a \pm a')a + (t \pm t')b, \\ q(sa + tb) &= (qs)a + (qt)b, \end{aligned}$$

因此集合 C 是一个理想, 根据定理 3.11, 它是由某个次数最低的多项式 $d(x)$ 的倍数组成的.

这个多项式 $d(x)$ 将整除 $a(x) = 1 \cdot a(x) + 0 \cdot b(x)$ 和 $b(x) = 0 \cdot a(x) + 1 \cdot b(x)$, 并且可被 $a(x)$ 和 $b(x)$ 的任意公因子整除. 这因为 $d(x) = s_0(x)a(x) + t_0(x)b(x)$, 我们的结论是

定理 3.12

在 $F[x]$ 中, 任意两个多项式 a 和 b 具有最大公因子 d 满足 (i) $d|a$ 和 $d|b$, (i') 由 $c|a$ 和 $c|b$ 可推出 $c|d$, 并且 (ii) d 是 a 和 b 的“线性组合^a” $d = sa + tb$.

^a这里的线性组合之所以打引号, 那是和线性代数里面的线性组合还是略有差异.



我们注意, 可用欧几里得算法, 由 a 和 b 明确地计算出 d . (这就是上面辗转相除法可用来明显地计算多项式的余数的原因.)

还有, 如果 d 满足 (i), (i') 和 (ii), 那么 d 的一切相伴也满足 (i) (i') 和 (ii). 附带一句, 由 (i) 和 (ii) 可推出 (i').

最大公因子 $d(x)$ 除单位因子外是唯一的. 这因为, 如果 d 和 d' 都是多项式 a 和 b 的最大公因子, 那么由 (i) 和 (i'), 有 $d|d'$ 和 $d'|d$, 因此 d 和 d' 确是相伴. 反之, 如果 d 是最大公因子, 那么 d 的每个相伴也是最大公因子. 有时为方便起见, 把与 d 相伴的唯一的非零多项式说成最大公因子.

两个多项式 $a(x)$ 和 $b(x)$, 如果它们的最大公因子是单位及其相伴, 则称它们互素. 这意味着多项式互素当且仅当它们的公因子只能是 F 的非零常数 (整环 $F[x]$ 的单位).

定理 3.13

如果 $p(x)$ 是不可约的, 则由 $p(x)|a(x)b(x)$ 可推出 $p(x)|a(x)$ 或者 $p(x)|b(x)$.



因为 $p(x)$ 是不可约的, 所以 $p(x)$ 和 $a(x)$ 的最大公因子或者是 $p(x)$ 或者是单位元素 1. 在前一种情况, 有 $p(x)|a(x)$, 在后一种情况, 我们可写

$$1 = s(x)p(x) + t(x)a(x),$$

因此

$$b(x) = 1 \cdot b(x) = s(x)p(x)b(x) + t(x)[a(x)b(x)],$$

因为 $p(x)$ 整除乘积 $a(x)b(x)$, 所以 $p(x)$ 整除上式右边两项, 因此整除 $b(x)$.

定理 3.14

$F[x]$ 中任意非常数多项式 $a(x)$ 可表示成一个常数 c 乘以某些首一不可约多项式的乘积. 这种表示法除因子出现的顺序外是唯一的.



证明 首先这样的因子分解是可能的. 如果 $a(x)$ 是常数或者不可约, 那么定理显然成立. 否则 $a(x)$ 是低次多项式的乘积 $a(x) = b(x)b'(x)$. 根据数学归纳法第二原理, 我们可以假定

$$b(x) = cp_1(x) \cdots p_m(x)$$

$$b'(x) = c'p'_1(x) \cdots p'_n(x)$$

因此

$$a(x) = (cc')p_1(x) \cdots p_m(x)p'_1(x) \cdots p'_n(x).$$

这里 cc' 是一常数, $p_i(x)$ 和 $p'_j(x)$ 是首一不可约多项式.

为了证明唯一性, 假设 $a(x)$ 可能有两个这样的“素”因子分解.

$$a(x) = cp_1(x) \cdots p_m(x) = c'q_1(x) \cdots q_n(x),$$

显然 $c = c'$ 是 $a(x)$ 的首项系数 (因为 $a(x)$ 的首项系数是其因子首项系数之积). 再有, 因为 $p_1(x)$ 整除 $c'q_1(x) \cdots q_n(x)$, 所以根据定理 3.13, 它必整除某个 (非常数) 因子 $q_i(x)$; 因为 $q_i(x)$ 是不可约的, 所以商式 $\frac{q_i(x)}{p_1(x)}$ 必为常数, 又因为 $p_1(x)$ 和 $q_i(x)$ 都是首一多项式, 所以常数必为 1. 因此 $p_1(x) = q_i(x)$. 消去之后, $p_2(x) \cdots p_m(x)$ 等于 q_k ($k \neq i$) 的乘积, 并且次数低于 $a(x)$ 的次数, 因此再根据数学归纳法第二原理, $p_j(x)$ ($j \neq 1$) 和 $q_k(x)$ ($k \neq i$) 成对地分别相等. 这就完成了证明.

一个推论是, 作为 $a(x)$ 的因子出现的每个首一不可约多项式 $p_i(x)$ 的指数 e_i 是由 $a(x)$ 唯一确定的, 并且它是使得 $[p_i(x)]^e | a(x)$ 的最大的 e .

如果像定理 3.14 那样, 多项式 $a(x)$ 分解成不可约因子 $p_i(x)$ 的积, 但 $p_i(x)$ 不必是首一多项式, 那么这些因子不再是唯一的了. 然而, 每个因子 $p_i(x)$ 被它的首项系数来除而得出唯一的首一不可约因子, 因此在 $F[x]$ 上 $p_i(x)$ 是这个不可约因子的相伴, 所以任意两个这样的因子分解只要重新排序, 并由适当的相伴因子代替每个因子, 就可做到彼此一致. 综上所述, $F[x]$ 中多项式的因子分解, 除了相差次序和单位因子外 (或者说除了相差次序和用相伴因子替换外) 是唯一的.

3.9 其他唯一因子分解整环

考虑有理数域 \mathbb{Q} 上关于两个未定元的多项式形式构成的整环 $\mathbb{Q}[x, y]$. $a(x, y) = x$ 和 $b(x, y) = y^2 + x$ 的公因子只能是 1 及其相伴, 但是不存在多项式 $s(x, y)$ 和 $t(x, y)$, 满足关系式 $xs(x, y) + (y^2 + x)t(x, y) = 1$, 这因为不管怎么选取 s 和 t , 多项式 $xs + (y^2 + x)t$ 总没有非零常数项. 类似的, 在整系数多项式环 $\mathbb{Z}[x]$ 中, 2 和 x 的最大公因子是 1, 而关系式 $2s(x) + xt(x) = 1$ 无解. 于是这两个整环中定理 3.12 都不成立,

然而我们可以证明, 上述两种情况分解成素因子是可能的而且是唯一的 (定理 3.14 成立).

定义 3.8. 唯一因子分解整环

满足下列条件的整环称为唯一因子分解整环 (有时称为高斯整环):

- (i) 非单位的任意元素可分解成素因子;
- (ii) 除了相差次序和单位因子外, 这种因子分解是唯一的.



我们的主要结果是: 如果 G 是任意唯一因子分解整环, 那么 G 上任意多项式形式的整环 $G[x_1, \dots, x_n]$ 同样是唯一因子分解整环. 对 n 用归纳法, 显然可把问题归结为关于单个未定元的 $G[x]$ 的情形, 我们将考虑这种情况.

首先我们将 G 嵌入 F 中, $F = Q(G)$ 为 G 的形式商构成的域, 并同 $G[x]$ 一起考虑 $F[x]$. 我们可以典型地把 G 想象为整数环, 相应地把 F 想象为有理数域.

其次, $F[x]$ 的多项式如果满足下列条件, 我们就称它为本原多项式: (i) 它的系数在 G 中 (“整数”); (ii) 它的所有系数没有除 G 中单位外的公因子. 例如 $3 - 5x^2$ 是本原多

项式, $3 - 6x^2$ 就不是.

引理 3.5. 高斯

两个本原多项式的乘积是本原多项式.



证明 记

$$\sum_k c_k x^k = \sum_i a_i x^i \cdot \sum_j b_j x^j,$$

如果它不是本原多项式, 那么 G 中某素元素 p 将整除每个 c_k , 设 a_m 和 b_n 分别是 $\sum_i a_i x^i$ 和 $\sum_j b_j x^j$ 中第一个不能被 p 整除的系数 (它们确实存在, 因为这两个多项式都是本原的), 那么乘积的系数 c_{m+n} 的计算公式 (3.1.3) 给出

$$a_m b_n = c_{m+n} - [a_0 b_{m+n} + \cdots + a_{m-1} b_{n+1} + a_{m+1} b_{n-1} + \cdots + a_{m+n} b_0]$$

因为上式右边所有项都能被 p 整除, 所以乘积 $a_m b_n$ 能被 p 整除, 这就推出 p 必出现在 a_m 或者 b_n 的唯一因子分解式之中, 这与选取 a_m 和 b_n 为不能被 p 整除相矛盾.

引理 3.6

$F[x]$ 的任意非零多项式 $f(x)$ 可以写成 $f(x) = c_f f^*(x)$, 其中 c_f 在 F 中, $f^*(x)$ 是本原多项式. 此外对于给定的 $f(x)$, 常数 c_f 和本原多项式 $f^*(x)$ 除了相差一个可能的 G 的单位因子外是唯一的.



证明 首先记

$$f(x) = \frac{b_0}{a_0} + \frac{b_1}{a_1}x + \cdots + \frac{b_n}{a_n}x^n, a_i, b_i \in G(\text{“整数”})$$

设 $c = \frac{1}{a_0 a_1 \cdots a_n}$, 我们有 $f(x) = cg(x)$, 其中 $g(x)$ 的系数都在 G 中. 现在令 c' 是 $g(x)$ 的所有系数的最大公因子 (这是存在的, 因为 G 中唯一因子分解定理成立), 显然 $f^*(x) = \frac{g(x)}{c'}$ 是本原, 并且 $f(x) = (cc')f^*(x)$, 取 $c_f = cc'$, 这就是引理中的第一个结论.

为了证明 c_f 和 f^* 的唯一性, 只须证明 f^* 除了相差 G 的单位因子外是唯一的. 为此假定 $f^*(x) = cg^*(x)$, 其中 $f^*(x)$ 和 $g^*(x)$ 都是本原多项式, 并且 $c \in F$. 记 $c = \frac{u}{v}$, 其中 $u, v \in G$ 并且互素, 因此 $ug^*(x) = vf^*(x)$. 那么 v 就是 $ug^*(x)$ 的所有系数的公因子, 因为 u 和 v 互素, 所以 v 整除 $g^*(x)$ 的每个系数. 但是 $g^*(x)$ 是本原的, 因此 v 是 G 的单位. 由对称性, u 也是一个单位, 所以 $\frac{u}{v}$ 是 G 的单位. 这就完成了证明.

引理 3.6 的常数 c_f 称为 $f(x)$ 的容度, 除相差 G 中相伴元素外是唯一的.

引理 3.7

如果在 $G[x]$ 中或者甚至在 $F[x]$ 中有 $f(x) = g(x)h(x)$, 那么 $c_f \sim c_g c_h$, 并且 $f^*(x) \sim g^*(x)h^*(x)$, 这里的 “ \sim ” 表示 $G[x]$ 中的相伴关系.



证明 根据引理 3.5, $g^*(x)h^*(x)$ 是本原多项式, 显然它还是 $f^*(x)$ 得某常数倍. 根据引理 3.6, 两者仅相差 G 的一个单位因子 u (所以两者是相伴的), 因此 $c_f = u^{-1}c_g c_h$.

这个引理的一个推论是, 如果 $f(x)$ 在 $G[x]$ 中, 并且它在 $F[x]$ 是可约的, 那么 $f(x) = uc_f g^*(x)h^*(x)$. 这就给出下面关于定理 3.10 推论的一个推广.

定理 3.15

整系数多项式如果它能分解成有理系数多项式之积, 那么它一定能分解成同次数的整系数多项式.



更重要的是, 由引理3.7, 在 $G[x]$ 中任意 $f(x)$ 的因子分解式分离成两个独立的部分: 一个是它的“容度” c_f 的分解, 一个是它的“本原部分” $f^*(x)$ 的分解. 前者相当于 G 的因子分解, 因此根据假设这种分解是可能的而且是唯一的. 根据引理??, 后者本质上等价于 $F[x]$ 中的分解, 由定理3.14, 这种分解是可能的而且是唯一的. 这就提出了

引理 3.8

如果 G 是唯一因子分解整环, 那么 $G[x]$ 也是唯一因子分解整环.



证明 由引理3.6, 任何多项式 $f(x)$ 可分解成 $f(x) = c_f f^*(x)$, 因此 $G[x]$ 中的素元素 $f(x)$ 必然有因子 c_f 或者 f^* 中的一个为 $G[x]$ 的单位. 于是 $G[x]$ 的素元素分为两种类型: 一类是 G 的素元素 p , 一类是本原不可约多项式, 它不仅在 $G[x]$ 中而且在 $F[x]$ 中都是不可约的 (3.15).

现在考虑 $G[x]$ 中任意多项式 $f(x)$. 它在 $F[x]$ 中有一个因子分解, 因而它与 $G[x]$ 的某些本原不可约多项式的乘积相伴, 记作 $f(x) \sim q_1(x) \cdots q_m(x)$. 于是 $f(x) = dq_1(x) \cdots q_m(x)$, 其中 G 的元素 d 可分解成 G 的素因子 p_i 的乘积, 总之 $f(x)$ 可分解成

$$f(x) = p_1 \cdots p_r q_1(x) \cdots q_m(x),$$

这里每个 p_i 是 G 的素元素, 每个 q_j 是 $G[x]$ 的本原不可约多项式.

出现在这个因子分解式中的多项式 $q_j(x)$ 除相差 G 的单位外是唯一确定的, 它是作为 $F[x]$ 中的 $f(x)$ 的唯一不可约因子的本原部分. 因为 $q_j(x)$ 都是本原的, 所以乘积 $p_1 \cdots p_r$ 实质上是 $f(x)$ 的唯一的容度. 因此 p_1, \dots, p_r (实质上) 是 c_f 在给定整环 G 中的全部因子 (唯一的). 这就证明了 $G[x]$ 是唯一因子分解整环.

由引理3.8并对 n 用归纳法我们可得出结论

定理 3.16

如果 G 是任意唯一因子分解整环, 那么 G 上每个多项式整环 $G[x_1, \dots, x_n]$ 也是唯一因子分解整环.



后面我们将举出一个整环, 它不是唯一因子分解整环, 不论定理3.12还是定理3.14都不成立. (例如整环 $\mathbb{Z}[\sqrt{5}]$, 由一切数 $a + b\sqrt{5}$ ($a, b \in \mathbb{Z}$) 组成. 它不是唯一因子分解整环, 因为 $2 \cdot 2 = (3 + \sqrt{5})(3 - \sqrt{5})$.)

3.10 爱森斯坦不可约判别法则

显然方程 $x^n = 1$, 当 n 为奇数时, 除了 $x = 1$ 外没有有理根, 由此得出 $x^n - 1$ 在 \mathbb{Q} 上除了 $x - 1$ 外没有首一线性因子. 但是这还不能证明商

$$\phi(x) = \frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \cdots + x + 1, \quad (3.10.1)$$

是不可约的. 事实上这个多项式除 n 为素数外是可约的.

我们现在证明, 如果 $n = p$ 是素数, 那么由 (3.10.1) 定义的分圆多项式 $\phi(x)$ 是不可约的, 因此 $x^p - 1 = (x - 1)\phi(x)$ 给出 $x^p - 1$ 的 (唯一) 因子分解式 (分解成首一不可约因子). 这个结果将从下面关于不可约性的充分条件推出. 这个定理是由爱森斯坦 (Eisenstein) 给出的.

定理 3.17

对于给定的素数 p , 设

$$a(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0,$$

是一整系数多项式, 如果

$$a_n \not\equiv 0 \pmod{p}, a_{n-1} \equiv a_{n-2} \equiv \cdots \equiv a_0 \equiv 0 \pmod{p},$$

$$a_0 \not\equiv 0 \pmod{p^2},$$

那么 $a(x)$ 在有理数域上是不可约的.



证明 假定可能有一个因子分解 ($n = m + k$)

$$a(x) = (b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0)(c_k x^k + c_{k-1} x^{k-1} + \cdots + c_0),$$

根据定理 3.15, 我们可以假定这两个因子都是整系数的, 即 b_i, c_j 为整数. 因为 $a_0 = b_0 c_0$, 所以假设中的第三个条件 $a_0 \not\equiv 0 \pmod{p^2}$ 意味着 b_0 和 c_0 不能同时被 p 整除. 固定一种情况, 我们假设 $b_0 \not\equiv 0 \pmod{p}$, 而 $c_0 \equiv 0 \pmod{p}$. 但是 $b_m c_k = a_n \not\equiv 0 \pmod{p}$, 故 $c_k \not\equiv 0 \pmod{p}$, 选取最小的指标 r ($r \leq k$) 使得 $c_r \not\equiv 0 \pmod{p}$, 而 $c_{r-1} \equiv \cdots \equiv c_0 \equiv 0 \pmod{p}$. 那么

$$a_r = b_0 c_r + b_1 c_{r-1} + \cdots + b_r c_0 \equiv b_0 c_r \pmod{p}.$$

但是, 因为 p 是素数, 所以由 $b_0 \not\equiv 0$ 和 $c_r \not\equiv 0 \pmod{p}$ 得出 $a_r \not\equiv 0 \pmod{p}$. 根据假设, 这样的系数 a_r 只可能是 a_n , 故 $r = n$. 这表明第二个因子的次数必须是 n , 所以多项式 $f(x)$ 确实是不可约的. 证毕.

当 $n = p$ 时, 这个判别准则可应用于多项式 (3.10.1), 这时 (3.10.1) 式给出分圆多项式

$$\phi(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1. \quad (3.10.1')$$

实际上, 爱森斯坦判别准则还不能直接用于 (3.10.1'), 不过这可以做一个简单的变量替换 $y = x - 1$, 并由二项式展开得到

$$\frac{x^p - 1}{x - 1} = \frac{(y + 1)^p - 1}{y} = y^{p-1} + p y^{p-2} + \frac{p(p-1)}{1 \cdot 2} y^{p-2} + \cdots + p.$$

出现在上式右边的二项系数都是可被素数 p 整除的整数, 这是因为 p 作为因子出现在每个系数的分子中, 并且不能被分母中比它小的整数消去. 这样作为 y 的多项式满足爱森斯坦判别准则的假设条件, 因此是不可约的, 原来 (3.10.1') 式的分圆多项式 $\phi(x)$ 仍保持这种不可约性.

3.11 部分分式

多项式的唯一因子分解定理可以用于有理函数上, 以便得到某些简化的表达式, 例如在积分学中用到的部分分式展开. 现在我们就对此进行讨论, 这一节涉及到的多项式和有理分式都假定它们的系数是在某一固定的域 F 上.

首先考虑这样的有理式 $\frac{b(x)}{a(x)}$, 它的分母分解成互素的因子 $c(x)$ 和 $d(x)$, 即 $a(x) = c(x)d(x)$, 由定理给出多项式 $s(x)$ 和 $t(x)$ 适合 $1 = sc + td$, 因此

$$\frac{b(x)}{c(x)d(x)} = \frac{s(x)b(x)}{d(x)} + \frac{t(x)b(x)}{c(x)}. \quad (3.11.1)$$

这一结果可叙述成

引理 3.9

一个有理分式, 如果它的分母是两个互素多项式 $c(x)$ 和 $d(x)$ 的乘积, 那么它可以表示成分母分别为 $c(x)$ 和 $d(x)$ 的两个商式之和.



如果分母 $a(x)$ 是一个幂 $a(x) = [c(x)]^m, m > 1$, 那么这个方法还不能直接应用. 改换另法, 按照辗转相除法, 用 $c(x)$ 去除分子, 有

$$b(x) = q_0(x)c(x) + r_0(x),$$

然后再用 $c(x)$ 去除商 $q_0(x)$ 得

$$q_0(x) = q_1(x)c(x) + r_1(x),$$

两个不等式合起来便得

$$b(x) = q_1(x)[c(x)]^2 + r_1(x)c(x) + r_0(x).$$

重复这一过程 (注意, 这个说法隐含了归纳过程), 采用缩写记号我们得到

$$b(x) = q_{m-1}c^m + r_{m-1}c^{m-1} + \cdots + r_1c + r_0, \quad (3.11.2)$$

这里每个多项式 $r_i = r_i(x)$, 如果不为零, 则它的次数低于 $c(x)$ 的次数. 现在有理分式 $\frac{b(x)}{a(x)}$ 变成

$$\frac{b}{c^m} = q_{m-1} + \frac{r_{m-1}}{c} + \frac{r_{m-2}}{c^2} + \cdots + \frac{r_1}{c^{m-1}} + \frac{r_0}{c^m}. \quad (3.11.3)$$

这就证明了

引理 3.10

以幂 $[c(x)]^m$ 为分母的可理式可以表示成一个多项式加上一些有理分式之和, 每个有理分式的分母是 $c(x)$ 的幂, 分子的次数低于 $c(x)$ 的次数.



综合这些结果, 可把任意给定的分母 $a(x)$ 分解成首一不可约多项式的乘积. 如果把相同的不可约因子归在一起, 我们有

$$a(x) = a_0[p_1(x)]^{m_1}[p_2(x)]^{m_2} \cdots [p_k(x)]^{m_k}. \quad (3.11.4)$$

其中指数 m_i 为整数. 任意两个不同的首一不可约多项式 $p_1(x)$ 和 $p_2(x)$ 当然互素, 因此幂 $[p_1(x)]^{m_1}$ 和 $[p_2(x)]^{m_2}$ 除了单位外没有公因子, 所以是互素的. 因此可以应用引理 3.9 把

分母分解成其中一个因子是 $c_1(x) = [p_1(x)]^{m_1}$, 而另一个因子是 (??) 式除去 $[p_1(x)]^{m_1}$ 后余下的部分. 重复进行下去, 就可把 $\frac{b}{a}$ 表为一些分式的和, 每个分式的分母是 $[p_i(x)]^{m_i}$. 最后还可用 (??) 式把每个分式进一步化简.

定理 3.18

任意有理分式 $\frac{b(x)}{a(x)}$ 可以表示成一个 x 的多项式加上形为 $\frac{r(x)}{[p(x)]^m}$ 的 (“部分”) 分式之和, 这里 $p(x)$ 为不可约多项式, $r(x)$ 的次数低于 $p(x)$ 的次数. 所出现的分母 $[p(x)]^m$ 是原来分母 $a(x)$ 的一切因子.



如果要找到给定的有理函数 $\frac{b(x)}{a(x)}$ 的明显的部分分式表达式, 那么照定理 3.18 证明的每一步去做就可得到. 这样的证明称为 “构造性” 证明. 它总是可以用于有关对象的实际计算.

例如, 在有理数域 \mathbb{Q} 上考虑 $\frac{x+1}{x^3-1}$. 分母是 $(x-1)(x^2+x+1)$, 第二个因子是不可约的, 由辗转相除法得到 $x^2+x+1 = (x+2) \cdot (x-1) + 3$, 用原来分式的分子 $(x+1)$ 乘这个方程, 我们得到

$$3(x+1) = (x+1)(x^2+x+1) - (x^2+3x+2)(x-1);$$

$$\frac{3(x+1)}{x^3-1} = \frac{x+1}{x-1} - \frac{x^2+3x+2}{x^2+x+1}.$$

所得的每个分式可以通过辗转相除法进一步化简得出

$$\frac{3(x+1)}{x^3-1} = \frac{2}{x-1} - \frac{2x+1}{x^2+x+1}.$$

在实数域 \mathbb{R} 上, 不可约多项式只能是线性多项式核满足 $b^2 - 4ac < 0$ 的二次多项式 $ax^2 + bx + c$ (后面会证明). 因此, 在 \mathbb{R} 上任意有理函数可以表示成分母是线性多项式的幂和二次多项式的幂的分式之和. 这个事实在微积分学中用来证明: 任何有理函数的不定积分可以通过 “初等函数” (即代数函数, 三角函数, 指数函数以及它们的反函数) 来表示. 根据定理 3.18, 有理分式求积时, 本质上可化为 $\frac{c}{(x+a)^m}$ 和 $\frac{c(x+d)}{(x^2+ax+b)^m}$ 两种类型的项之和求积. 因此, 如果这两种类型的函数的积分可以通过初等函数表示 (这是可以做到的), 那么关于积分的命题就将被证明.

例题 3.1 分解下式成部分分式

第四章 实数

4.1 毕达哥拉斯二难推论

抽象代数虽然相当多地强调了一般的域和整环所具有的大量性质,但是实数域和复数域对于定量地描述我们生活的世界还是不可缺少的.例如,在代数和几何的关系中,不仅在初等解析几何而且再进一步讨论矢量和矢量分析中,这两个域都是很重要的.此外,它们还具有独特的代数性质,这些性质将在本书后几章中展示出来,特别重要的是实数域 \mathbb{R} 的序的完备性和复数域 \mathbb{C} 的代数完备性.

希腊人研究实数用的是纯几何方法.对他们来说,一个数只不过是两个线段 a 和 b 的长度之比 ($a:b$).他们直接给出关于比的相等以及比的加法,乘法,减法和除法的几何构造.全体实数构成有序域的公设在希腊人看来,是由平面几何一系列公设(包括平行公设)证明的一组几何定理.

古希腊哲学家毕达哥拉斯(Pythagoras)知道,正方形对角线长 d 与它的边长 s 之比 $r = \frac{d}{s}$ 一定满足方程

$$d^2 = (rs)^2 = r^2 s^2 = s^2 + s^2 \quad (\text{毕达哥拉斯定理}) \quad (4.1.1)$$

因此他推理,存在一个“数” r ,满足 $r^2 = 1 + 1 = 2$.

另一方面,他发现 r 不能表示成两个整数的商 $r = \frac{a}{b}$. 这是因为 $(\frac{a}{b})^2 = 2$ 意味着 $a^2 = 2b^2$, 根据素因子分解定理,2 每次整除 a 就恰有两次整除 a^2 , 因此 2 整除 a^2 偶数次,类似的,2 整除 $2b^2$ 奇数次,所以 $a^2 = 2b^2$ 没有整数解.

只要把不能表为整数之商的数设为无理数,我们就能避开上述“毕达哥拉斯二难推论”.

类似的论证指出,立方体 C 的对角线长与它的边长之比为 $\sqrt{3}$, C 的边长与具有一半体积的立方体的边长之比为 $\sqrt[3]{2}$, 这些都是无理数. 这些结果是 3.7 节定理 3.10 的特殊情况.

此外, π , e 及许多别的数都是无理数(因此 π 不会恰好是 $\frac{22}{7}$, 甚至 3.1416), 我们将证明,绝大多数的实数不仅是无理数,而且甚至不能满足一个代数方程(与 $\sqrt{2}$ 不同). 为了回答“什么是实数?”这个基本问题,我们要用到一些新的概念.

一个概念是连续性---如果实轴分成两段,那么这两段必在公共边界点上相接. 第二个概念是,有序有理数域 \mathbb{Q} 在实数域里稠密,因此,每个实数是一个或多个有理数序列(例如精确到 n 位的有限小数逼近序列)的极限. 这个概念还可表述为

$$x < y \quad \Rightarrow \quad \exists \frac{m}{n} \in \mathbb{Q}, x < \frac{m}{n} < y. \quad (4.1.2)$$

实数的这个性质首先被希腊数学家欧多克斯(Eudoxus)发现. 欧多克斯把 $x = a:b$ 和 $y = c:d$ 都看作线段长度之比,线段长度 a 的整数倍 na 可用几何方法做出,他规定 $(a:b) = (c:d)$ 当且仅当对一切正整数 m 和 n ,

$$\begin{aligned} na > mb & \Rightarrow nc > md, \\ na < mb & \Rightarrow nc < md. \end{aligned} \quad (4.1.3)$$

上述两个概念可以合并成一个完备性公设, 由这个公设我们可以通过有序域 \mathbb{Q} 的自然扩张来构造实数. 这个“完备性”公设类似于整数的良序公设, 二者都涉及无限集合的性质. 这种性质是非代数的. 我们将看到, 这个完备性公设对于建立实数域的某些重要代数性质 (例如每个正数都有平方根) 是必需的.

例题 4.1 给出 $\sqrt{3}$ 是无理数的直接证明.

例题 4.2 证明: $\sqrt[n]{a}$ 是无理数, 除非整数 a 是某一整数的 n 次幂.

例题 4.3 证明: $\log_{10} 3$ 是无理数.

例题 4.4 证明: $\sqrt{2} + \sqrt{5}$ 是无理数.

4.2 上界与下界

实数域可以最简单地被描述为具有下列性质的有序域, 即域中任意有界集合都有最大下界和最小上界. 我们现在就定义这两个概念, 它们类似于可除性理论中的最大公因子和最小公倍数的概念.

定义 4.1. 上界和最小上界

设 S 为有序整环 D 中某些元素构成的集合. 如果 D 中元素 b (它本身不一定在 S 中) 使得对 S 中每个元素 x , 有 $b \geq x$, 则称 b 为 S 的上界. 对于 S 的上界 b , 如果 D 中没有比 b 小的元素是 S 的上界, 也就是说, 如果对任意 $b' < b$, S 中都存在一个 x 适合 $b' < x$, 那么 b 就是 S 的最小上界.



把上面定义的“ $>$ ”换成“ $<$ ”, “ $<$ ”换成“ $>$ ”, 可定义 S 的下界和最大下界的概念.

由定义直接可知, D 的子集 S 至多有一个最小上界, 并且至多有一个最大下界. 因为如果 b_1 和 b_2 都是最小上界, 那么 $b_1 \leq b_2$ 且 $b_2 \leq b_1$, 于是 $b_1 = b_2$. 最大下界类似.

直观上, 把实数当作连续直线 (x 轴) 上的点来考虑, 并想象在这条直线上, 全体有理数密集地撒布在它们各自本来的位置上. 由此我们容易得出结论: 每个实数 a 可定义为所有适合 $r < a$ 的有理数 $r = \frac{m}{n}$ ($n > 0$) 的集合 S 的最小上界. 例如 $\sqrt{2}$ 是大于所有适合 $m^2 < 2n^2$ 的比 $\frac{m}{n}$ ($m > 0, n > 0$) 的最小实数, 也就是说, 数 $\sqrt{2}$ 是适合 $m^2 < 2n^2$ 的正有理数 $\frac{m}{n}$ 的集合的最小上界.

用无限小数表示实数的普通表达式直接包含着把实数看作有理数集合的最小上界的概念. 例如我们可以把 $\sqrt{2}$ 写成最小上界 (l.u.b) 和最大下界 (g.l.b) 的两种形式.

$$\begin{aligned}\sqrt{2} &= \text{l.u.b.}(1.4, 1.41, 1.414, 1.4142, \dots) \\ &= \text{g.l.b.}(1.5, 1.42, 1.415, 1.4143, \dots)\end{aligned}\tag{4.2.1}$$

由熟悉的小数表达式的性质很容易看出, 每个正实数非空集合 T 有最大下界, 如下所述.

考虑把 T 的元素只取前 n 位的 n 位小数, 它们中间必有一个最小的元素, 这是因为只有有限个非负 n 位小数, 比 T 的任何给定的元素都小. 设这个最小的 n 位小数是 $k + 0.d_1d_2 \cdots d_n$, 其中 k 为某整数, d_i 为数字. 最小的 $n+1$ 位小数其前 n 位与 $d_1d_2 \cdots d_n$ 相同, 因此有形式 $k + 0.d_1d_2 \cdots d_nd_{n+1}$, 这里添上一个数字 d_{n+1} , 所以上述构造定义了某

一个无限小数

$$c = k + 0.d_1d_2d_3\cdots$$

根据构造, c 就是 T 的下界 (因为 T 中没有一个 x 能比 c 的小数表达式小), 而且是最大下界 (任何比 c 大的小数就不再是 T 的下界).

但是如果把实数定义成无限小数, 那么很难证明中学代数中所承认的事实: 无限小数系统是有序域¹.

4.3 实数公设

我们现在将用一组简短的公设来描述实数. 后面我们会看到, 这些公设唯一地 (精确到同构) 确定全体实数.

定义 4.2

有序整环 D 是完备的当且仅当 D 的正元素的每个非空集合在 D 中有最大下界.



实数公设 实数构成完备的有序域 \mathbb{R} .

我们根据这个公设得出的实数性质, 确实可以导出全体实数的一切熟知的性质, 包括像洛尔 (Rolle) 定理那样的结果, 这个定理在微积分学中, 对于泰勒 (Taylor) 定理的证明或其他方面是基本的.

但是我们只限于讨论几个简单的应用.

定理 4.1

在实数域 \mathbb{R} 中, 每个具有下界的非空子集 S 有最大下界, 每个具有上界的非空子集 T 具有最小上界.



证明 假设 S 有下界 b , 如果把 $1-b$ 加在 S 的每个元素 x 上, 则得到正数 $x-b+1$ 的集合 S' . 根据实数公设, 这个集合 S' 具有最大下界 c' , 因此数 $c = c' + b - 1$ 是原来集合 S 的最大下界, 这很容易验证.

对偶的, 如果集合 T 有上界 a , 则 T 的所有元素的负元素 $-y$ 组成的集合具有下界 $-a$, 因此根据上述证明, 它有最大下界 b^* . 那么可以证明, 数 $a^* = -b^*$ 就是已知集合 T 的最小上界. 证毕.

实数公设保证全体实数构成有序域 \mathbb{R} , 所以 2.6 节定理 2.18 的推论 2.4 指出, \mathbb{R} 必包含同构于有理数域 \mathbb{Q} 的子域. 因为在第二节里, \mathbb{Q} 仅在同构意义下定义, 所以我们也同样假定实数域 \mathbb{R} 包含所有有理数, 因而包含所有整数. 这个约定使上述公设适应于习惯用法, 并可使我们证明下面的实数性质 (常称为阿基米德定律).

定理 4.2. 阿基米德定律

在所有实数组成的域 \mathbb{R} (由实数公设定义的) 中, 对任意两个数 $a > 0$ 和 $b > 0$, 存在整数 n 使得 $na > b$.



¹困难在于两个不同的小数实际上是相等的, 例如 $0.199999\cdots = 0.200000\cdots$. 详细请看 J.F.Ritt, Theory of Functions. 可能的话后面收录这本书.

证明 假定对于两个特定的实数 a 和 b , 上述结论是错误的, 因而对每个 $n, b \geq na$. 则所有倍数 na 的集合 S 有上界 b , 从而它也有最小上界 b^* , 所以对每个 $n, b^* \geq na$, 因此对每个 m , 也有 $b^* \geq (m+1)a$. 这推出 $b^* - a \geq ma$, 所以 $b^* - a$ 也是 a 的所有倍数的集合的上界, 但是它小于已知的最小上界, 得出矛盾.

推论 4.1

对已知实数 a 和 $b, b > 0$, 总存在整数 q 适合 $a = bq + r, 0 \leq r < b$.



这是除法算式的推广.

这样建立的“阿基米德性质”可以证明欧多克斯条件 (参考4.1节的 (4.1.3)) 是合理的.

定理 4.3

任意两个实数 c 和 d 之间 ($c > d$), 存在有理数 $\frac{m}{n}$ 适合 $c > \frac{m}{n} > d$.



像前面那样, 这个定理由“实数构成完备的有序域”的公设就可证明. 根据假设, $c - d > 0$, 所以由阿基米德定律有正整数 n 使得 $n(c - d) > 1$, 即 $\frac{1}{n} < c - d$. 现在设 m 为适合 $m > nd$ 的最小整数, 那么 $\frac{m-1}{n} \leq d$, 因此

$$\frac{m}{n} = \frac{m-1}{n} + \frac{1}{n} < d + (c - d) = c.$$

因为 $\frac{m}{n} > d$, 这就完成了证明.

我们可以对上面的证明直观说明如下. 具有固定分母 n 的不同分数 $0, \pm\frac{1}{n}, \pm\frac{2}{n}, \dots$, 以长度 $\frac{1}{n}$ 为间隔沿实轴隔开. 为确保一个这样的点能落在 c 和 d 之间, 我们只需使间隔 $\frac{1}{n}$ 小于已知的差 $c - d$.

这个定理可用来正式地证明像 (4.2.1) 式那样把实数表示成有理数集合的最小上界的直观想法.

推论 4.2

每个实数是某有理数集合的最小上界.



证明: 对于已知实数 c , 设 S 表示所有有理数 $\frac{m}{n} \leq c$ 的集合. 那么 c 是 S 的上界, 根据定理4.3, 没有比 c 小的实数 d 可以是 S 的界, 因此 c 是 S 的最小上界.

练习 4.1 证明: 不存在这样的有序整环 D , 其中每个非空集合具有最小上界. (提示: D 本身可以没有上界.)

练习 4.2 证明: 有序整环 \mathbb{Z} 是完备的.

4.4 多项式方程的根

我们现在将指出怎样利用最小上界的存在性来证明实数系 \mathbb{R} 的各种性质, 首先包括像 $x^2 = 2$ 这样方程解的存在性.

定理 4.4

如果 $p(x)$ 为实系数多项式, $a < b$, 并且 $p(a) < p(b)$, 那么对满足 $p(a) < C < p(b)$ 的每个常数 C , 方程 $p(x) = C$ 在 a 和 b 之间有根.



几何上, 定理的假设意味着 $y = p(x)$ 的曲线与水平直线 $y = p(a)$ 在 $x = a$ 处相交, 并与水平直线 $y = p(b)$ 在 $x = b$ 处相交; 定理的结论是说: 曲线也必与每条中间的水平直线 $y = C$ 在某点相交², 这点的 x 坐标在 a 和 b 之间.

证明依赖于下面两个引理.

引理 4.1

对任意实数 x 和 h , 我们有

$$p(x+h) - p(x) = hg(x, h),$$

式中 $g(x, h)$ 是只依赖于 $p(x)$ 的多项式.



证明 根据二项定理, 对于 $p(x)$ 的每个单项 $a_k x^k$, 这是正确的. 现在对 k 求和并且提出公因子 h , 我们便得到所需要的结论.

引理 4.2

对于已知的 a, b 和 $p(x)$, 存在实常数 M , 使得满足 $a \leq x \leq b, a \leq x+h \leq b$ 的一切 x 和一切正的 h , 有

$$|p(x+h) - p(x)| \leq Mh.$$



证明 根据引理 4.1, 只须证明当 $x \leq |a| + |b|, |h| \leq |b-a|$ 时, 有 $|g(x, h)| \leq M$. 但是, 如果我们把 $g(x, h)$ 的每项用它的绝对值代替, 根据 1.3.1, 则使 $|g(x, h)|$ 增大或保持不变. 如果我们再分别用 $|a| + |b|$ 和 $|b-a|$ 代替 $|x|$ 和 $|h|$, 那么又使得到的结果增大或保持不变. 然而, 这个替换给我们一个只依赖于 $p(x)$ 的系数和区间 $a \leq x \leq b$ 的实常数 M .

有了引理 4.2, 我们准备证明定理 4.4, 设 S 表示 a 和 b 之间满足 $p(x) \leq C$ 的实数的集合. 因为 $p(a) < C$, 所以 S 是不空的, 并且它以 b 为上界. 因此 S 有实的最小上界 c , 我们来证明 $p(c) = C$.

为此目的, 显然只须排除 $p(c) < C$ 和 $p(c) > C$ 两种可能. 但是, 根据引理 4.2 由 $p(c) < C$ 可推出, 对 $h = \frac{C-p(c)}{M}$, $p(c+h) \leq C$. 因此 $(c+h) \in S$. 这与 c 是 S 的上界的定义矛盾. (引理 4.2 可以应用是因为 $c+h \geq b$ 显然是不可能的.)

现在剩下 $p(c) > C$ 这种可能. 但是在这种情形下, 再根据引理 4.2, 对一切正的 $h \leq \frac{p(c)-C}{2M}$, 有 $p(c-h) > C$, 这与 c 是 S 的最小上界的定义矛盾³: $c - \frac{p(c)-C}{2M}$ 将给出比 c 小的上界. 因此只留下 $p(c) = C$.

根据这个定理我们容易证明:

²数学分析中有一个一般性的定理, 它断言这个结论不仅对于多项式函数 $p(x)$ 成立, 而且对于任意连续函数也成立.

³这里似乎有问题, 按照目前 S 的选取方法, 这里无法成立, 因为目前的选择方法无法保证小于 c 数必有 $p(c) \leq C$, 所以这里需要修改 S 的构造方式: $S = \{x : \forall y \in [a, x], p(y) \leq C\}$

推论 4.3

如果 $p(x)$ 为正系数多项式, 而且没有常数项, $C > 0$, 那么 $p(x) = C$ 有正实根.

**推论 4.4**

如果 $p(x)$ 为奇次多项式, 那么对每个实数 C , $p(x) = C$ 有实根.



定理 4.4 没有给出 $p(x) = C$ 的小数形式的根的实际计算方法, 但这是容易做到的. 例如我们可以设 $c_1 = \frac{a+b}{2}$, 则或 $p(c_1) = C$, 或 $p(c_1) > C$, 或 $p(c_1) < C$. 在第一种情形下, 方程的根就找到了; 在第二三种情形下, 分别在区间 $a \leq x \leq c_1$ 和 $c_1 \leq x \leq b$ 中有根, 这个区间长度为原来的一半. 重复这一过程便可得到 $p(x) = C$ 的根的任何精度的近似值.

如果我们采用线性内插法, 且令

$$c_1 = a + \frac{[C - p(a)](b - a)}{p(b) - p(a)},$$

则收敛得更快.

其他计算方程根的有效方法在数学分析里讨论. 例如, 当 $|x| < 1$, 我们可以运用无穷级数

$$\sqrt{1+x} = 1 + \frac{1}{2}x + \frac{1}{2}\left(-\frac{1}{2}\right)\frac{x^2}{2!} + \frac{1}{2}\left(-\frac{1}{2}\right)\left(-\frac{3}{2}\right)\frac{x^3}{3!} + \cdots. \quad (4.4.1)$$

附录 三次方程的三角解法

在三次方程

$$a_3x^3 + a_2x^2 + a_1x + a_0 = 0, \quad a_3 \neq 0 \quad (4.4.2)$$

的情况下, 方程实根可按下法求得. 我们用 a_3 去除方程各项把 (4.4.2) 化简成 $a_3 = 1$ 的情形. 现在作变量替换 $x = y - \frac{a_2}{3}$, 并移动常数项, 把 (4.4.2) 化为

$$y^3 + py = q. \quad (4.4.3)$$

当 $p = 0$ 时, 答案立即可得.

否则, 令 $y = hz$, 并用 k 乘 (4.4.3) 的各项, 其中 $h = \sqrt{\frac{4|p|}{3}}$, $k = \frac{3}{h|p|}$, 我们可把 (4.4.3) 化为下列两个方程之一:

$$4z^3 = 3z = C \text{ 或 } 4z^3 - 3z = C. \quad (4.4.4)$$

为了解第一个方程, 我们可用熟悉的三角恒等式

$$\operatorname{sh} 3\theta = 4 \operatorname{sh}^3 \theta + 3 \operatorname{sh} \theta,$$

因此⁴,

$$z = \operatorname{sh} \left(\frac{1}{3} \operatorname{argsh} C \right). \quad (4.4.5)$$

为了解第二个方程, 当 $D \geq 1$, 我们利用类似的公式

$$\operatorname{ch} 3\theta = 4 \operatorname{ch}^3 \theta - 3 \operatorname{ch} \theta,$$

⁴书中几个反函数使用的符号是 Arsh , Arch 和 Arcos , 应该想办法统一这些三角函数的表示方法, 包括双曲函数的表示.

得到

$$z = \operatorname{ch} \frac{1}{3} \operatorname{argch} C.$$

当 $C \leq -1$, 改变 z 的符号后再应用同样的方法求解. 为了解当 $|C| < 1$ 时的第二个方程 (这就是 15.8 的不可约情形), 利用相似的公式

$$\cos 3\theta = 4 \cos^3 \theta - 3 \cos \theta,$$

得到

$$z = \cos \frac{1}{3} \arccos C.$$

在这种情形下, z 取三个值, 这是因为 $\frac{1}{3} \arccos C$ 有三个值, 它们之间相差 120° 的倍数.

第四章 习题

1. 证明: 每个正实数有实平方根.
2. 证明: 对任意正实数 a 和任意整数 n , 方程 $x^n = a$ 有且仅有一个正实根 $\sqrt[n]{a}$.
3. 证明: 对每个 $C > -\frac{3}{8}$, $x^4 - x = C$ 有两个实根.
4. 利用正文中的 (4.4.1) 式和 $(\frac{\sqrt{5}}{2})^2 = 1 + \frac{1}{4}$, 求 $\sqrt{5}$ 得四位小数近似值.
5. 利用 (4.4.1) 式和 $(\frac{5\sqrt{2}}{7})^2 = 1 + \frac{1}{49}$, 求 $\sqrt{2}$ 得六位小数近似值.
6. 证明: 偶次首一多项式达到最小值 K , 并且对每个值 $C > K$, 多项式两次取值 C .
7. (a) 设 a 和 b 为正实数, $n \geq -1$ 为整数, 证明, 对一切充分大的正值 x , 有 $ax^{n+1} > bx^n$.
(b) 已知多项式具有正的首项系数, 求出一个实数 M , 使得对一切 $x > M$, 有 $p(x) > 0$.
8. 证明推论 4.3.
9. 证明推论 4.4.
10. 求下列方程的实根 (取小数三位):
(a) $3x^3 - x = \frac{1}{9}$,
(b) $x^3 - 3x^2 + 6x = 7$,
(c) $x^3 + 3x^2 + 2 = 0$.

4.5 戴德金分割

想象在 x 轴上, 有理数撒布在它们各自本来的位置上, 但是当分割 x 轴时 (比如说, 用剪刀剪开), 我们就把全体有理数分成两类, 一类在左边, 记作 L , 一类在右边, 记作 U . 每个有理数落入这两类中, 而仅当在点 $x = \frac{m}{n}$ 处分割 x 轴时, 有理数 $\frac{m}{n}$ 同时落在这两类中. 特别注意, 如果 x 在 L 中, 那么对 U 的每个 y , 有 $x \leq y$; 反过来, 如果对 U 中一切 y , 有 $x \leq y$, 那么 x 必落在 L 中. 由此引出戴德金 (Dedekind) 分割的想法.

一般地, 设 F 为任意有序域. 我们用 F 中的“戴德金分割”表示适合下列条件的一对非空子集 L 和 U :

- (i) L 是 U 的全体元素的所有下界的集合;
- (ii) U 是 L 的全体元素的所有上界的集合.

引理 4.3

戴德金分割的 L 部分和 U 部分合在一起包含 F 的一切元素；它们至多有一个公共元素。



证明 设已知 $x \in F$, 如果对某 $a \in L$, 有 $x \leq a$, 那么对一切 $y \in U$, 有 $x \leq a \leq y$, 因此 $x \in L$, 否则, 由三分律, 对一切 $a \in L$, 有 $x > a$, 所以 $x \in U$. 这就证明了第一个结论: F 的每个元素不在 L 中就在 U 中. 再有, 设 a 和 b 都既在 L 中又在 U 中, 则 $a \geq b$ (因为 $a \in U, b \in L$), 并且 $a \leq b$ (因为 $a \in L, b \in U$), 因此 $a = b$, 这就证明了第二个结论.

如果 L 和 U 有一个公共元素 a , 则称该分割是通过 a 的. 显然, 如果 L_a 是所有适合 $x \leq a$ 的 x 的集合, 并且 U_a 是所有适合 $x \geq a$ 的 x 的集合, 那么分割 (L_a, U_a) 通过 a .

戴德金分割公理 (在有序域 F 上) 每个分割通过某元素 a .

定理 4.5

戴德金分割公理在有序域中成立当且仅当 F 是完备的有序域.



证明 设 (L, U) 是任意分割, 如果最小上界的存在性是已知的, 则 L 具有最小上界 a . 因为 a 是 L 的上界, 所以 a 必在 U 中; 因为它是最小上界, 所以它是一切上界的下界, 因此是 U 的所有元素的下界. 根据分割定义, 意味着 a 在 L 中, 所以给定的分割通过元素 a .

反过来, 假定戴德金分割公理成立, 并设 S 为非空有界集合. 设 U 是 S 的所有上界的集合, L 是 U 的所有下界的集合 (显然, L 包含 S). 为证明 (L, U) 是一分割, 我们只须确定 U 是 L 的所有上界的集合. 但是根据 L 的构造, U 的每个元素是 L 的上界 (对一切 $x \in L, y \in U$, 有 $x \leq y$); 而因为 L 包含 S , 所以 U 包含 L 的一切上界. 现在根据戴德金公理, 分割线 (L, U) 通过某元素 a , 因为它是 U 的元素, 所以它是 S 的上界, 又因为它是 L 的元素, 所以它是 S 的最小上界 (即对一切 $x \in U$, 有 $a \leq x$). 这就完成了证明.

我们现在概述一下实数公设“实数系是完备的有序域”有关分类性质的证明.

定理 4.6

任意两个完备的有序域同构.



证明 设 F' 和 F'' 为任意两个这样的域, 根据 2.6 定理 2.18 的推论 2.4, 它们分别包含同构的“有理数”子域 Q' 和 Q'' , 我们把 Q' 和 Q'' 之间的同构 (保持和与积, 并保持次序的同构) 扩张到 F' 和 F'' 之间的同构.

的确, 每个 $a' \in F'$ 定义了 F' 中的一个分割, 从而定义了 Q' (有理数子域) 中的分割. 但根据定理 4.3, a' 由 Q' 中这个分割所确定---并且 Q' 中每个分割 (L_R, U_R) 用这个方法确定 $a' = l.u.b.L_R = g.l.b.U_R$. Q'' 中分割的情况类似, 因此 F' 和 F'' 的元素分别双射到 Q' 和 Q'' 的分割. 这种双射显然保持次序.

最后, F' 和 F'' 中的运算可由 Q' 和 Q'' 的那些运算定义, 以便把 Q' 和 Q'' 的同构扩张. 更确切地说, 设 a 和 b 分别对应于 Q' 中分割 (L_a, U_a) 和 (L_b, U_b) . 那么 $a + b$ 对应于分割⁵ $(L_a + L_b, U_a + U_b)$, 其中 $L_a + L_b$ 是所有和 $x + y$ ($x \in L_a, y \in L_b$) 的集合, 而 $U_a + U_b$

⁵在某些情况下, $(L_a + L_b, U_a + U_b)$ 不会是分割, 因为数 $a + b$ 不在 L 中, 也不在 U 中; 但是如果把遗漏的数添到 L 和 U 上去, 我们便得到分割, 类似的情况适合于下面的 $L_a L_b$.

可类似地描述. 把正元素 a 和 b 相乘, 构成正有理系数中类似的分割, 那么 ab 对应于分割 $(L_a L_b, U_a U_b)$, 其中 $L_a L_b$ 是所有积 xy ($x \in L_a, y \in L_b$) 的集合, $U_a U_b$ 也类似地定义. 因为 $(-a)b = a(-b) = -ab$ 和 $(-a)(-b) = ab$, 因此这可扩充到一切乘积, 我们不再详细论述.

反过来, 我们可以利用分割通过整数或正整数构造实数. 我们首先证明全体有理数构成具有阿基米德性质 (定理4.2中所指出的) 的有序域. 用上段叙述的方式定义 \mathbb{Q} 中分割的加法和乘法, 我们可以证明 \mathbb{Q} 中分割构成满足戴德金分割公理的有序域, 因而给出完备的有序域. 但是证明很长, 会把我们引入迷途, 因此我们只是叙述一下结果.

定理 4.7

有一个且仅有一个 (同构的域除外) 完备的有序域.



不用戴德金分割, 而通过有理数, 把实数看作有理数序列的极限, 也可以构造实数⁶.

第四章习题

- 证明: 如果 (L, U) 和 (L', U') 是有理数域中的分割, 那么每个有理数 (至多有一个例外) 都能表为 $x + y$ ($x \in L, y \in L'$), 或者表为 $u + v$ ($u \in U, v \in U'$).
- 叙述并证明对于正有理数在乘法下的类似于习题1的一个定理.
- 为什么这个定理对于负有理数不成立?
- 证明: 对于每个 $\epsilon > 0$, 存在充分大的 n 使得 $10^{-n} < \epsilon$.
- 有序域 F 中的戴德金分割有时定义为 F 的一对子集 L' 和 U' , 它们适合: F 的每个元素或者在 L' 中或者在 U' 中, 并且当 $x \in L', y \in U'$ 时, 有 $x < y$. 通过添加或删除相应的单个元素, 可以证明: 这种类型的每个分割给出正文中定义的分割 (L, U) , 反之亦然.
- 设 t 为有序整环 D 中的元素, $0 < t < 1$, 证明: $s = 2 - t$ 具有性质 $s > 1, st \leq 1$.
- 设 D 为不同构于 \mathbb{Z} 的完备的有序整环. 证明: D 包含适合 $0 < t < 1$ 的元素. 设 b 和 c 为 D 的任意正元素, 证明: 对某整数 $n, t^n b < c$.
- 利用习题6和习题7. 证明: 任意完备的有序整环或者同构于 \mathbb{Z} , 或者同构于 \mathbb{R} . (提示: 求出 $b > 1$ 的逆元素, 考虑满足 $xb \leq 1$ 的所有的 x .)
- (a) 证明: \mathbb{R} 的任意自同构保持关系 $x \leq y$. (提示: $x \leq y$ 当且仅当 $z^2 = y - x$ 有解.)
(b) 利用 (a) 证明: \mathbb{R} 唯一的自同构是平凡自同构 $x \mapsto x$.
- 证明: 如果 $D = F$ 为有序域, 并且对每个有理函数

$$R(x) = \frac{b_0 + b_1 x + \cdots + b_r x^r}{a_0 + a_1 x + \cdots + a_n x^n} \neq 0, \quad a_n b_r \neq 0,$$
 我们规定 $R(x) > 0$ 的意思是 $a_n b_r > 0$, 那么 $F(x)$ 成为有序域.
- 证明: 在习题10中, $R(x) > 0$ 当且仅当对 F 中一切充分大的 t , 有 $R(t) > 0$.

⁶参看 C.C.MacDuffee, Introduction to Abstract Algebra(New York, Wiley, 1940) 的第 VI 章的论述.

第五章 复数

5.1 复数的定义

如果我们把实数系 \mathbb{R} 扩张成较大的复数域 \mathbb{C} , 那么在解析函数论和微分方程论中, 特别是代数学中, 很多代数定理的描述将更为简洁. 我们现在就来定义复数域, 并且指出, 如果我们想要使每个多项式方程都有根, 由实数域扩张而得到的域就是复数域.

定义 5.1

复数就是实数偶 (x, y) — x 称为 (x, y) 的实分量, y 称为 (x, y) 的虚分量. 根据法则

$$(x, y) + (x', y') = (x + x', y + y'), \quad (5.1.1)$$

$$(x, y) \cdot (x', y') = (xx' - yy', xy' + yx'), \quad (5.1.2)$$

施行复数相加和相乘. 这样定义的复数系记作 \mathbb{C} .



我们认为上面的定义不是靠神灵的力量, 而是通过简单的代数运算而得到的. 首先, 观察出方程 $x^2 = -1$ 没有实根 (x^2 决不能是复数). 这就暗示我们要引进一个虚数 i , 它满足 $i^2 = -1$, 此外还满足普通的代数定律. 用确切的话来说, 它提出一个表面上讲得通的假设: 存在一个包含元素 i 同时包含实数域 \mathbb{R} 的整环 D .

在 D 中, 任意形为 $x + yi$ (x, y 为实数) 的表达式将表示一个元素. 此外, 由整环的定义 (普通的代数定律) 有

$$(x + yi) \pm (x' + y'i) = (x \pm x') + (y \pm y')i, \quad (5.1.1')$$

$$(x + yi) \cdot (x' + y'i) = xx' + (xy' + yx')i + yy'i^2. \quad (5.1.2')$$

因为 $i^2 = -1$, 我们由 (5.1.2') 得

$$(x + yi) \cdot (x' + y'i) = (xx' - yy') + (xy' + yx')i. \quad (5.1.2'')$$

于是我们得到一个推论是, 由 \mathbb{R} 和 i 生成的 D 的子整环包含一切形为 $x + yi$ 的元素, 而不包含其他任何元素.

再有, $x + yi = x' + y'i$ 推出 $x - x' = (y' - y)i$, 因此两边平方得 $(x - x')^2 = -(y' - y)^2$, 又因 $(x - x')^2 \geq 0$, $-(y' - y)^2 \leq 0$, 除非 $x = x'$, $y = y'$, 上面等式不成立. 总之, 不同的实数偶 (x, y) 确定 D 中不同的元素 $x + yi$, 这就建立了, \mathbb{C} 中的元素和由 \mathbb{R} 与 i 生成的 D 的子整环中元素之间的一一对应 $(x, y) \leftrightarrow x + yi$. 比较公式 (5.1.1')~(5.1.2') 和 (5.1.1)~(5.1.2), 我们看到这种对应保持和与积, 因此是一个同构. 这就证明了

定理 5.1

设 D 为包含实数系 \mathbb{R} 和 -1 的平方根 i 的任意整环, 那么由 \mathbb{R} 和 i 生成的 D 的子整环与 \mathbb{C} 同构.



我们现在证明我们的猜想, 确实存在一个整环 D , 它包含全体实数和 -1 的平方根.

定理 5.2

按上面定义的复数系是一个域, 它包含一个与 \mathbb{R} 同构的子域, 并包含方程 $x^2 + 1 = 0$ 的根.



证明 对于实数偶 (x, y) , 加法的交换律和结合律成立, $(0, 0)$ 是加法单位元素, $(-x, -y)$ 是 (x, y) 的加法逆元素, 这些都是下述事实的直接结论: 数偶的实分量和虚分量是独立相加的, 而相应的定律对于它们都是成立的.

类似的, 乘法的交换律和结合律成立, $(1, 0)$ 是乘法单位元素, 每个 $(x, y) \neq (0, 0)$ 都有乘法逆元素

$$(x, y)^{-1} = \left(\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2} \right). \quad (5.1.3)$$

这可由 5.2 中建立的事实得到, 在 5.2 中指出, 几个复数相乘时, 它们的“辐角”和“绝对值”是分开来进行运算的, 这些运算本身满足交换律和结合律. 可是在这里, 检验这些定律所采用的办法是直接代入定义 (5.1.2), 只有结合律的计算比较冗长, 我们略去了它们的详细验证.

最后, 类似地直接代入定义, 我们可以验证分配律. 设 $z = (x, y)$, $z' = (x', y')$, $z'' = (x'', y'')$. 那么代入 (5.1.1) 和 (5.1.2), 有

$$\begin{aligned} z(z' + z'') &= (x, y)(x' + x'', y' + y'') \\ &= (x(x' + x'') - y(y' + y''), x(y' + y'') + y(x' + x'')), \\ zz' + zz'' &= (xx' - yy', xy' + yx') + (xx'' - yy'', xy'' + yx'') \\ &= (xx' - yy' + xx'' - yy'', xy' + yx' + xy'' + yx''). \end{aligned}$$

从这两个表达式可以直接验证 $z(z' + z'') = zz' + zz''$.

在这个由数偶组成的域 \mathbb{C} 中, 我们利用定理 5.1 中所用过的对应 $(x, y) \leftrightarrow x + yi$, 可以在 \mathbb{C} 中找到一个实数子域. 按照这种对应, 实数 x 对应于第二项为零的数偶, $(0, 1)$ 对应于 i . 特别是, 如果定义 (5.1.1) 和 (5.1.2) 中的第二个分量 y 和 y' 都是零时, 那么第一个分量 x 和 x' 的相加和相乘恰好与实数 x 和 x' 的相加和相乘一样. 这正是我们所要认识的: 对应 $x \leftrightarrow (x, 0)$ 是实数域 \mathbb{R} 到 \mathbb{C} 的子域的一个同构. 在上面这种情况下, 我们认为, 每个这样特殊的复数 $(x, 0)$ 至与相应的实数 x 等同.

最后, 我们希望 -1 的平方根相当于数偶 $(0, 1)$. 事实上, 定义 (5.1.2) 的特殊情况表明, $(0, 1)^2 = (-1, 0) = -1$. 因此我们定义 i 是数偶 $(0, 1)$. 那么任意数偶 (x, y) 具有形式

$$(x, y) = (x, 0) + (0, y) = (x, 0) + (y, 0)(0, 1) = x + yi. \quad (5.1.4)$$

记号 $x + yi$ 是很方便的, 后面我们都用它来代替 (x, y) . 为简洁起见, 我们还常常写作 $z = (x, y) = x + yi$, $w = (u, v) = u + vi$, $c = (a, b) = a + bi$, 等等---换句话说, 我们用单个字母表示复数, 用字母表中紧靠着它的前两个字母分别表示这个复数的实分量和虚分量.

第五章 习题

1. 验证复数乘法满足交换律和结合律。
2. 用公式 (5.1.3) 验证 $(x, y)(x, y)^{-1} = (1, 0)$ 。
3. 解方程 $(1, 1)(x, y) = (2, 1)$.
 - (a) 化为一对关于变量 x, y 的联立线性方程;
 - (b) 用公式 (5.1.3)。
4. 分别求出满足下列关系的复数 $z = x + yi$ 和 $w = u + vi$:
 - (a) $z + iw = 1, iz + w = 1 + i$;
 - (b) $(1 + i)z - iw = 3 + i, (2 + i)z + (2 - i)w = 2i$.
5. 求出方程 $z^2 = -a$ (a 为任意正实数) 的全部复根, 并验证你的答案。
6. 描述由 i 和全体有理数生成的 \mathbb{C} 的子域。
7. 如果 D 是交换环, 定理 5.1 还成立吗? 给出详细证明。
8. (a) 证明: $z^2 = a + bi$ 有解 $x + yi$, 其中 $x = \left[\frac{a + \sqrt{a^2 + b^2}}{2} \right]^{\frac{1}{2}}, y = \frac{b}{2x}$.
 (b) 证明: 方程的解还可表成

$$y = \left[\frac{\sqrt{a^2 + b^2} - a}{2} \right]^{\frac{1}{2}}, \quad x = \frac{b}{2y}.$$

(注意, 当 a 是负数, 并且 $\frac{b}{a}$ 很小时, 这组公式在数值计算中更为精确。)

9. 方程 $z^3 + 3iz = 3 + i$ 有一个根 $-i$, 计算另一个根, 并表示成小数形式。
10. 证明: 如果 F 为任意有序域, 那么存在一个比它大的域 F^* , 包含着与 F 同构的子域和 -1 的平方根。
11. 用定理 5.1 和定理 5.2 的方法, 不借助于实数, 证明: 有理数域 \mathbb{Q} 可以扩张到较大的域 $\mathbb{Q}\sqrt{2}$, 该域包含 \mathbb{Q} 和 2 的平方根。
12. 证明: 不可能存在“正复数”的定义, 使 \mathbb{C} 构成有序域。

5.2 复平面

全体复数到笛卡尔平面的全体点上有一个基本的一一映射, 即每个复数 $z = x + yi$ 映射到点 $P = (x, y)$ 上, 这个点以 z 的实分量 x 为横坐标, 以虚分量 y 为纵坐标。

极坐标可以用在这个平面上。我们回忆一下, 平面上的每个点 P , 因此每个复数是由两个极坐标 r 和 θ 唯一确定的, 这里 r 是联结点 P 到原点的线段 \overline{Oz} 的长度 (非负的), 而 θ 是由 x 轴到线段 \overline{Oz} 的夹角, 所以

$$\begin{aligned} |z| &= r = (x^2 + y^2)^{\frac{1}{2}}, \\ \arg z &= \theta = \arctan \frac{y}{x}. \end{aligned} \quad (5.2.1)$$

我们把 r 称为复数 z 的绝对值, 把 θ 称为 z 的辐角。 r 和 θ 按下式确定 x 和 y

$$x = r \cos \theta, y = r \sin \theta, z = r(\cos \theta + i \sin \theta). \quad (5.2.2)$$

这就是通常由极坐标到直角坐标的变换公式。我们还可以把 (5.2.2) 式写成 $z = re^{i\theta}$, 这是因为, 由通常的泰勒级数展开式得到

$$e^{i\theta} = 1 + i\theta + \frac{(-1)\theta^2}{2!} + \frac{(-i)\theta^3}{3!} + \cdots = \cos \theta + i \sin \theta.$$

绝对值和辐角的重要性主要反映在棣莫弗 (De Moivre) 公式, 这个公式叙述如下:

定理 5.3

复数乘积的绝对值等于因子的绝对值之积, 乘积的辐角等于因子的辐角之和, 换句话说,

$$|zz'| = |z||z'|, \quad \arg zz' = \arg z + \arg z'. \quad (5.2.3)$$

证明 因为按 (5.2.2) 式, 有 $z = r(\cos \theta + i \sin \theta)$, $z' = r'(\cos \theta' + i \sin \theta')$, 代入定义 (5.1.2) 中我们得到

$$\begin{aligned} zz' &= rr'[(\cos \theta \cos \theta' - \sin \theta \sin \theta') \\ &\quad + i(\cos \theta \sin \theta' + \sin \theta \cos \theta')]; \end{aligned}$$

由熟知的三角公式, 这就是

$$zz' = rr'[\cos(\theta + \theta') + i \sin(\theta + \theta')].$$

这就给出了结论 (5.2.3)。

复数绝对值的乘法性质与加法性质 (不等式) 其表达形式同实数一样, 即

$$|z| > 0, \text{ 除非 } z = 0, |0| = 0; \quad (5.2.4)$$

$$|z + z'| \leq |z| + |z'|. \quad (5.2.5)$$

为了证明这些, 注意公式 (5.1.1) 意味着 $z + z'$ 可以通过画以 z, O 和 z' 为三个顶点的平行四边形来求得, 第四个顶点就是 $z + z'$, 由于复数的绝对值等于相应线段的几何长度, 现在可以推出公式 (5.2.4) 和 (5.2.4)。

复 n 次单位根可以用三角方法求得。从棣莫弗公式 (5.2.3) 直接得出

$$[r(\cos \theta + i \sin \theta)]^{-1} = \frac{1}{r}[\cos(-\theta) + i \sin(-\theta)].$$

进一步得到, $z^n = 1$ 当且仅当 $|z|^n = 1$, 并且 $n \cdot \arg z$ 是 2π 的整数倍 $2k\pi$. 因为 $|z| \geq 0$, 所以 $|z| = 1$. 因为 $\arg z$ 在 $0 \leq \theta < 2\pi$ 上是单值的, 所以 $z^n = 1$ 确有 n 个解。在直角坐标这, 它们是

$$1, \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}, \dots, \cos \frac{2\pi(n-1)}{n} + i \sin \frac{2\pi(n-1)}{n}.$$

如果我们用 ω 表示 $\cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$, 则可得到这些 n 次单位根的另一种表示: $1, \omega, \omega^2, \dots, \omega^{n-1}$. 用几何语言叙述就是

定理 5.4

全体复 n 次单位根是单位圆 $|z| = 1$ 内接正 n 边形的 n 个顶点。

更一般地, 考虑方程 $z^n = c$, 其中 $c \neq 0$ 为任意复数。在极坐标中, 方程的一个解是

$$z_0 = |c|^{\frac{1}{n}}(\cos \theta + i \sin \theta), \text{ 其中 } \theta = \frac{1}{n} \arg c.$$

此外, ωz_0 是 $z^n = c$ 的根当且仅当 $c = (\omega z_0)^n = \omega^n z_0^n = \omega^n c$, 因此 $\omega^n = 1$. 于是 c 的 n 次根是 $z_0, \omega z_0, \omega^2 z_0, \dots, \omega^{n-1} z_0$, 这里 ω 是上面定义的复 n 次单位根。特别, 它们也可以用正多边形的 n 个顶点表示。

对 $c = a + bi$ 的 n 次根 $z_0, \omega z_0, \omega^2 z_0, \dots, \omega^{n-1} z_0$, 我们可以借助于三角函数表和对数表, 很容易地计算出它们的数值。从恒等式

$$\log |z_0| = \log |c|^{\frac{1}{n}} = \frac{1}{n} \log (a^2 + b^2)^{\frac{1}{2}} = \frac{1}{2n} \log (a^2 + b^2)$$

出发, 我们可以计算 $|z_0|$. 根据棣莫弗公式 (5.2.3), 有 $\arg z_0 = \frac{1}{n} \arctan \frac{b}{a}$, 和 $\arg \omega^k z_0 = \frac{1}{n} \arctan \frac{b}{a} + \frac{360k}{n}$. 这里的单位是度。最后由公式

$$z = r(\cos \theta + i \sin \theta) = |z| \cos(\arg z) + i|z| \sin(\arg z)$$

完成计算。

每个复 n 次单位根 ω 满足一个有理数域上不可约的有理系数多项式方程。这些方程称为“分圆”方程, 在方程式理论中起着重要作用。

由定义, 每个 n 次单位根满足方程 $z^n - 1 = 0$, 此外, 除了 $z = 1$ 的其他所有根满足

$$q_n(z) = \frac{z^n - 1}{z - 1} = z^{n-1} + z^{n-2} + \dots + z + 1 = 0. \quad (5.2.6)$$

在 3.10 中用爱森斯坦判别准则证明当 $n = p$ 为素数时, $q_p(z)$ 是不可约的。

如果 n 不是素数, 那么情况就复杂了。例如, 当 $n = 4$, $z^3 + z^2 + z + 1 = (z+1)(z^2+1)$ 是可约的。一般地, 我们可以从 (5.2.6) 中分解出 k 次单位根所满足的分圆多项式, 这里 k 取遍 n 的所有真因子。 n 次单位根, 如果对所有的 $k < n$, 它不是 k 次单位根, 则称它为 n 次本原单位根。(例如, 四次本原单位根是 i 和 $-i$.) n 次本原单位根是 ω^m , 其中 m 与 n 互素, 它们都满足有理数域上同一个不可约方程。但是这一结论的证明和这个方程次数的计算, 需要更多的数论知识。

第五章 习题

1. 用棣莫弗公式证明复数乘法的交换律和结合律, 以及乘法逆元素的存在性。
2. 描述对应关系 $z \mapsto zi$ 的几何意义。
3. 求三次单位根和五次单位根的实分量和虚分量, 计算到小数点后四位 (用三角函数表)。
4. 求 $2 + 2i$ 得立方根和四次根, 计算到小数点后四位。
5. 列出全部 12 次本原单位根, 并在图纸上把它们画在一个大单位圆上。
6. 用几何语言描述变换 $z \mapsto cz + d$ ($c, d \in \mathbb{C}, c \neq 0$) 的效果, 当 $|c| = 1$ 时是什么情况? (提示: 使用“平移”, “旋转”和“放大”等词。)
7. 找出 $z^6 - 1$ 在有理数域 \mathbb{Q} 上的不可约因子。
8. (a) 证明: $\omega = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$ 是 n 次本原单位根。
(b) 证明: ω^m 是 n 次本原单位根当且仅当 m 与 n 互素。

5.3 代数基本定理

我们在 5.1 中看到, 实数系 \mathbb{R} 添加方程 $z^2 + 1 = 0$ 的一个虚根 i 就得到复数系。但是为什么就到此为止了呢? 为什么不打算添加其他多项式方程的“虚”根以便得到更大的

域呢？所谓代数基本定理就回答了这个问题：一旦添加上 i ，那么每个多项式方程就必有（复）根，所以为解方程我们就不需要再选另外的虚根。

定理 5.5. 欧拉-高斯

每个正次数的复系数多项式必有复根。



已经知道这个著名定理的很多证明方法¹。所有的证明都包含着像第4章引进的那些非代数概念；这里我们选择了一个证明，它的非代数部分在直观上好像特别容易说明。我们从不从第4章有关的公理来详细证明非代数部分。

证明 因为多项式

$$p(z) = a_m z^m = a_{m-1} z^{m-1} + \cdots + a_0, a_m \neq 0$$

与多项式

$$\begin{aligned} q(z) &= z^m + \frac{a_{m-1}}{a_m} z^{m-1} + \cdots + \frac{a_0}{a_m} \\ &= z^m + c_{m-1} z^{m-1} + \cdots + c_0 \end{aligned}$$

有相同的根，所以只须讨论首项系数为 1 的情况。

这种情况下，我们画两个复平面，一个标记为“ z -平面”，另一个标记为“ w -平面”。已知函数 $q(z)$ 把 z -平面的每个点 $z_0 = (x_0, y_0)$ 映射到 w -平面的点 $w_0 = q(z_0)$ 上。此外，如果 z 描绘 z -平面上的一条连续曲线，那么 $q(z)$ （是可微的）将描绘 w -平面上的一条连续曲线。我们的目的是证明， w -平面的原点 O 是 z -平面上某个点 z 的“像” $q(z)$ ，或者与之同样的是证明 z -平面上某个圆的像通过 w -平面的原点 O 。

对每个固定的 $r > 0$ ，函数 $w = q(re^{i\theta})$ 确定了 w -平面上的一条闭曲线 γ'_r ，即 z -平面上以原点 O 为中心， r 为半径的圆 $\gamma_r: |z| = r$ ($z = re^{i\theta}$) 的像。对每个固定的 r ，考虑线积分²

$$\phi(r, \theta) = \int_0^\theta d(\arg w) = \int_0^\theta \frac{u dv - v du}{u^2 + v^2},$$

这是对任何不通过原点 $w = 0$ 的曲线 γ'_r 来定义的。（如果 γ'_r 通过 $w = 0$ ，那么定理 5.5 的结论就立即可得。）几何上显然有 $\phi(r, 2\pi) = 2\pi n(r)$ ，这里分支数 $n(r)$ 是曲线 γ'_r 绕原点反时针旋转的次数。例如，在图中描绘的曲线，其 $n(r) = 2$ 。

现在考虑 $n(r)$ 随 r 的变化情况。因为 $q(re^{i\theta})$ 是连续函数，所以除了 γ'_r 通过原点外， $n(r)$ 也是随 r 连续变化的。再有， $n(0) = 0$ （除非 $c_0 = 0$ ，这时 0 是方程的根），现在假

¹例如参见，L. E. Dickson, *New First Course in the Theory of Equations* (New York: Wiley, 1939). 附录，或 L. Weisner, *Introduction to the theory of Equations* (New York: Macmillan, 1938), p.145

²在证明线积分的存在时，必须用到 \mathbb{R} 的完备性。恒等式

$$d(\arg w) = \frac{u dv - v du}{u^2 + v^2}$$

成立是因为 $\arg w = \arctan \frac{v}{u}$ 。

定 $c_0 \neq 0$, 我们将证明, 当 r 充分大时, $n(r)$ 就是 $q(z)$ 的次数 m 。实际上, 设

$$\begin{aligned} q(z) &= z^m + c_{m-1}z^{m-1} + \cdots + c_1z + c_0 \\ &= z^m \left(1 + \sum_{k=1}^m c_{m-k}z^{-k} \right) \end{aligned}$$

根据棣莫弗公式 (5.2.3), 有

$$\arg q(z) = m \arg z + \arg \left(1 + \sum_{k=1}^m c_{m-k}z^{-k} \right)$$

因此, 当 z 沿着圆 γ_r 作反时针方向变化一周时, $\arg q(z)$ 得到的改变量是 $\arg z$ 的改变量的 m 倍 (即 $m \cdot 2\pi$) 加上 $\arg \left(1 + \sum_{k=1}^m c_{m-k}z^{-k} \right)$ 的改变量。可是当 $|z| = r$ 充分大时, 由公式 (5.2.4) 和 (5.2.5) 可知,

$$1 + \sum_{k=1}^m c_{m-k}z^{-k} = u$$

停留在圆 $|u - 1| < \frac{1}{2}$ 中, 因此绕原点只转了零次 (画个图加以解释)。

我们得出结论: 当 r 充分大时, $n(r) = m$, $\arg q(z)$ 的总改变量是 $2\pi m$ 。但是当 r 变化时, γ'_r 是连续变形的 (因为 $q(z)$ 是连续的)。然而, 几何上显然有³: 一条绕原点 m ($\neq 0$) 次的曲线, 如果不是它变形的某一步通过原点, 这条曲线就不能连续地变形成一点。由此推出, 对某个 r , γ'_r 必通过原点, 这就出现 $q(z) = 0$! 证毕。

作为推论, 我们注意, 如果 $p(z_1) = 0$, 那么根据余数定理 (3.5), 我们可以写成 $p(z) = (z - z_1)r(z)$ 。如果 $p(z)$ 的次数为 m , $m > 1$, 则商式 $r(z)$ 具有正次数, 因此它也有一个复根 $z = z_2$, 如此进行下去, 我们就找到 $p(z)$ 的 m 个线性因子, 如

$$p(z) = c(z - z_1)(z - z_2) \cdots (z - z_m). \quad (5.3.1)$$

由此得到, \mathbb{C} 上的不可约多项式只能是线性的。这个推论和第3章的唯一因子分解定理合在一起得出

定理 5.6

任意复系数多项式可按一种且仅按一种方式写成 (5.3.1) 的形式。



在 (5.3.1) 中 $p(z)$ 的根显然是 z_1, \dots, z_m , 这是因为乘积为零当且仅当它其中一个因子为零。如果因子 $(z - z_i)$ 重复出现, 那么它重复出现的次数称为根 z_i 的重数。在微积分学中, 这个可以定义为 $p(z)$ 在 z_i 点为零的“阶数”: 使得 $p(z)$ 和它的前 $v - 1$ 阶导数在 z_i 点都为零的最大整数 v 。

第五章习题

1. 不用3.8一般的唯一性定理, 证明: 分解式 (5.3.1) 的唯一性。
2. 证明: 任何有理复函数, 如果对所有的 z 都取有限值, 则它是多项式。
3. 所有复数偶 (w, z) , 当相加和相乘遵循法则 (5.1.1) 和 (5.1.2) 时, 它构成含有单位元素的交换环吗? 构成域吗?

³这作为平面拓扑学中的一个定理已经证明了。例如参看 S. Lefschetz. Introduction to Topology (Princeton University Press, 1949), p. 127

4. 证明：任意二次多项式可以通过 $\mathbb{C}[z]$ 的适当的自同构得到形式 $cz(z-1)$ 或 cz^2 。
5. (a) 用马克劳林 (Maclaurin) 级数证明公式 $e^{ix} = \cos x + i \sin x$ 。
 (b) 证明每个复数可以写成 $re^{i\theta}$ 。
 (c) 推导恒等式

$$\cos z = \frac{e^{iz} + e^{-iz}}{2}, \quad \sin z = \frac{e^{iz} - e^{-iz}}{2i}.$$

6. 利用部分分式证明：域 \mathbb{C} 上的任意有理函数可以写成一个多项式加上一些有理函数之和，这些有理函数的分子是常数，分母是线性函数的幂。
7. 分解 $z^2 + z + 1 + i$ 。

5.4 共轭数与实多项式

在复数域 \mathbb{C} 上，方程 $z^2 = -1$ 有两个根 i 和 $-i = 0 + (-1)i$ 。对应 $x + yi \mapsto x + y(-i) = x - yi$ 把第一个根映射到第二个根，反过来把第二个根映射到第一个根，而它们保持所有实数不变。而且这个对应把和映射到和，把积映射到积，这可以通过直接代入公式 (5.1.1) 和 (5.1.2) 或者应用定理 5.1 来验证。换句话说，这个对应是 \mathbb{C} 的一个自同构 (\mathbb{C} 到自身的同构)。

我们可以更简洁地把这个对应叙述如下。把数 $x - yi$ 称为复数 $x + yi$ 的“共轭” z^* 。对应 $z \mapsto z^*$ 是 \mathbb{C} 上周期为 2 的自同构，这是因为

$$(z_1 + z_2)^* = z_1^* + z_2^*, (z_1 z_2)^* = z_1^* z_2^*, (z^*)^* = z. \quad (5.4.1)$$

在几何上这个对应相当于复平面关于 x 轴的一个反射；与其共轭相等的数只有实数。

共轭复数在数学中和物理学中（特别在波动力学中）是很有用的。在使用它们的时候，记住下面一些简单公式是方便的：

$$|z|^2 = zz^*, \quad z^{-1} = \frac{z^*}{|z|^2}.$$

用这些公式可使我们从定理 5.6 很容易地推出实系数多项式的分解定理。

引理 5.1

实系数多项式的非实复根是以一对共轭复数的形式出现。



这推广了下面熟知的事实：二次多项式 $ax^2 + bx + c$ ，当判别式 $b^2 - 4ac < 0$ 时，有两个共轭复根 $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ 。

证明 设 $p(z)$ 为已知多项式，我们可以把它写成 (5.3.1) 的形式，其中 z_i 是复数（不是通常的实数）。因为作用在这些根 z_i 上的一个对应 $z_i \mapsto z_i^*$ 是自同构，所以它把 $p(z)$ 映射到另一个多项式

$$p^*(z) = c^*(z - z_1^*)(z - z_2^*) \cdots (z - z_m^*).$$

这个多项式的每个系数是 $p(z)$ 中相应系数的共轭⁴。但因 $p(z)$ 的全体系数都是实数，所

⁴这一步不明白？能有这样的结论吗？后面几步依赖于这一步，所以需要搞清楚这一步。或者应该这样理解， $\forall z$,

$$(p(z))^* = c^*(z^* - z_1^*)(z^* - z_2^*) \cdots (z^* - z_m^*).$$

以 $p(z) = p^*(z)$. 因此分解式 (5.3.1) 是唯一的, $c = c^*$ 是实数, 并且 z_i 是实数或者是成对出现的共轭复数。

定理 5.7

任意实系数多项式可以分解成(实)线性多项式和判别式为负的(实)二次多项式。♡

证明 上面引理中的实根 z_i 给出(实)线性因子 $(z - z_i)$. 一对共轭复根 $z + bi$ 和 $a - bi$ ($b \neq 0$) 可以合并起来有

$$[z - (a + bi)][z - (a - bi)] = z^2 - 2az + (a^2 + b^2).$$

它给出 $p(z)$ 的一个实系数二次因子, 其判别式为

$$4a^2 - 4(a^2 + b^2) = -4b^2 < 0.$$

反过来, 线性多项式和判别式为负的二次多项式在实数域上是不可约的(后者是因为它们只有复数根, 因此没有线性因子)。定理 5.7 所描述的因子分解是唯一的, 这可作为一个推论。

第五章习题

1. 解方程:

- (a) $(1 + i)z + 3iz^* = 2 + i$,
- (b) $zz^* + 2z = 3 + i$,
- (c) $zz^* = 3(z - z^*) = 4 - 3i$.

2. 解方程:

- (a) $zz^* + 3(z + z^*) = 7$,
- (b) $zz^* + 3(z + z^*) = 3i$.

3. 解联立方程:

$$\begin{cases} iz + (1 + i)w = 3 + i, \\ (1 + i)z^* - (6 + i)w^* = 4. \end{cases}$$

- 4. 给出 4.4 定理 4.4 推论 4.4 的独立的证明。
- 5. 证明: 如果我们在实数系上添加一个任意的非线性不可约的实系数多项式的虚根, 则可得到一个与 \mathbb{C} 同构的域。
- 6. 证明: 在任意有序域上, 如果 $b^2 - 4ac < 0$, 则 $ax^2 + bx + c$ 是不可约的。
- 7. 证明: 保持所有实数都不变的 \mathbb{C} 的每个自同构或者是恒等自同构 $z \mapsto z$, 或者是自同构 $z \mapsto z^*$ 。

5.5 二次方程与三次方程

5.3 中我们证明了任意复系数多项式根的存在性, 但没有指出如何有效地把根计算出来。在 5.5 和 5.6 中, 我们将指出如何计算二次方程, 三次方程和四次方程的根。计算过程

那么由于 z 的任意性, 我们有多项式 $P(z) = c^*(z - z_1^*)(z - z_2^*) \cdots (z - z_m^*)$ 和 $(p(z))^*$ 表示的是同一个多项式。

中只包含四种有理运算（加、乘、减、除）和开 n 次方根运算。[5.1](#)和[5.2](#)中我们已指出如何进行复数的这些运算。下面讲的计算过程也可用于任何别的域上，在这些域上，任意元素的 n 次根是可以构造的，而且 $1 + 1 \neq 0$, $1 + 1 + 1 \neq 0$ 。

二次方程可以用中学代数的“配方”方法求解。方程

$$az^2 + bz + c = 0, \quad (a \neq 0) \quad (5.5.1)$$

等价于（具有同样的根）较简单的方程

$$z^2 + Bz + C = 0, \quad (B = \frac{b}{a}, C = \frac{c}{a}). \quad (5.5.2)$$

如果令 $w = z + \frac{B}{2}$ (即 $z = w - \frac{B}{2}$)，以便配成完全平方，我们可以看到 [\(5.5.2\)](#) 式等价于

$$w^2 = \frac{B^2}{4} - C. \quad (5.5.3)$$

对 w, B, C 代回 z, a, b, c ，这就得出

$$z = w - \frac{B}{2} = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \quad (5.5.4)$$

根据[5.2](#)，所以有两个解。

三次方程可以类似地求解。首先像[4.4](#)那样，把三次方程化为形式

$$z^3 + pz + q = 0, \quad (5.5.5)$$

然后做维特 (Vieta) 变换 $z = w - \frac{p}{3w}$ ，结果得到（有些项已消去）

$$w^3 - \frac{p^3}{27w^3} + q = 0. \quad (5.5.6)$$

用 w^3 乘以各项，我们得到关于 w^3 的二次方程。这个方程可以根据公式 [\(5.5.4\)](#) 求解，得出

$$w^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \quad (\text{两个值}). \quad (5.5.7)$$

这给出 w 的 6 个三次根形式的解。把这些解代入公式 $z = w - \frac{p}{3w}$ ，我们就得到 z 的三对解，成对的两个解是相等的。

阐述一下前面定理 6 中的公式是有趣的。例如，二次多项式的情形，记

$$z^2 + Bz + C = (z - z_1)(z - z_2),$$

我们有

$$z_1 + z_2 = -B, z_1 z_2 = C, \quad (5.5.8)$$

因而

$$(z_1 - z_2)^2 = B^2 - 4C. \quad (5.5.9)$$

$B^2 - 4C = D$ 这个量是 [\(5.5.2\)](#) 的判别式。用原来 [\(5.5.1\)](#) 式中的系数表示： $D = \frac{b^2 - 4ac}{a^2}$ 。

类似的，设 z_1, z_2, z_3 是简化的三次方程 [\(5.5.5\)](#) 的根，则

$$z_1 + z_2 + z_3 = 0, z_1 z_2 + z_2 z_3 + z_3 z_1 = p, z_1 z_2 z_3 = -q, \quad (5.5.10)$$

合并前两个关系式, 我们得到公式

$$\begin{aligned} p &= z_1 z_2 - z_3^2, (z_1 - z_2)^2 = -4p - 3z_3^2, \\ z_1^2 + z_2^2 + z_3^2 &= -2p. \end{aligned} \quad (5.5.11)$$

我们现在用

$$\begin{aligned} D &= \prod_{i < j} (z_i - z_j)^2 = P^2, \\ \text{这里 } P &= (z_1 - z_2)(z_2 - z_3)(z_3 - z_1) \end{aligned} \quad (5.5.12)$$

来定义三次方程的判别式, 把 P 平方, 再利用 (5.5.11) 式的第二个关系式, 通过一些计算后我们就得到

$$D = -4p^3 - 27q^2, \quad (5.5.13)$$

它可以用来简化 (5.5.7), 得 $w = -\frac{q}{2} + \frac{\sqrt{-D}}{6}$.

定理 5.8

实系数二次方程或三次方程, 如果它的判别式非负则它有实根; 如果它的判别式是负的, 则它有两个虚根。



证明 根据定理 5.7 的推论, 或者所有的根都是实根, 或者有两个共轭虚根 $z_1 = x_1 + yi$ 和 $z_2 = x_1 - yi$. 如果所有的根都是实根, 则对所有的 $i \neq j$, 有 $(z_i - z_j)^2 \geq 0$, 因此 $D \geq 0$. 对第二种情况, 有 $(z_1 - z_2)^2 = -4y^2 < 0$, 又因为 $z_3 = x_3$ 是实的, 所以 $(z_1 - z_3)(z_2 - z_3) = (x_1 - x_3)^2 + y^2 > 0$, 因此 $D < 0$. 证毕。

由 (5.5.12) 式, 条件 $D = 0$ 给出了检验方程有重根的简单判别法。

可惜的是, 在 $D > 0$ 的情况下, 方程 $z^3 + pz + q = 0$ 的三个根全部是实根, 但公式 (5.5.7) 却是用复数把它们表示出来。我们在??中将指出这是毫无助益的。

第五章习题

- 证明: 对任意复数 y, p , 存在 z 满足 $y = z - \frac{p}{3z}$. 存在多少个 z ?
- 用根式表出方程的解:
 - $z^2 + iz = 2$,
 - $z^3 + 3iz = 1 + i$,
 - $z^3 + 3iz^2 = 10i$.
- 把习题 2.(a) - (c) 每个方程中的一个根改写成小数形式。
- (a) 证明 (5.5.11) 式; (b) 证明 (5.5.13) 式。
- (a) 证明: $\operatorname{sh} 3\gamma = \operatorname{sh}(3\gamma + 2\pi i)$.
(b) 利用 4.4 中的公式 (4.4.5) 证明: 方程 $4z^3 + 3z = C$ 除有实根 $\operatorname{sh} [\frac{1}{3} \operatorname{Arsh} C]$ 外, 还有复根 $-\frac{1}{3} \operatorname{ch} \gamma \pm \frac{i\sqrt{3}}{2} \operatorname{sh} \gamma$.
- 设 $\omega = e^{\frac{2\pi i}{5}}$ 是五次本原单位根, 且设 $\zeta = \omega + \frac{1}{\omega}$.
 - 证明: $\zeta^2 + \zeta = 1$.
 - 推断: 中心在 $(0, 0)$, 一个顶点在 $(1, 0)$ 的一个正五边形中, 与这个顶点相邻的顶点的 x 坐标是 $\frac{\sqrt{5}-1}{4}$.

7. 用公式 $\cos \theta = \frac{e^{i\theta} + e^{-i\theta}}{2}$ 证明: $\cos n\theta = T_n(\cos \theta)$, 其中 T_n 为一个适当的 n 次多项式, 并计算 T_1, T_2, T_3, T_4 .

5.6 四次方程的根式解法

任何一种把代数方程的求解化为一系列有理运算和对某数开 n 次方根的运算的方法称为“根式解法”。

定理 5.9

任意 $n \leq 4$ 次实系数或复系数多项式方程可用根式求解。



证明 因为 $n = 1$ 的情形在任意域上都是可解的, 而 $n = 2, 3$ 的情形在 5.5 中已作了处理, 所以我们只须考虑

$$ax^4 + bx^3 + cx^2 + dx + e = 0, \quad (a \neq 0).$$

再有, 用 a 去除每一项, 并用 $z = x + \frac{b}{4a}$ 代替 x (以便配成“完全”四次方), 我们得到方程

$$z^4 + pz^2 + qz + r = 0, \quad (5.6.1)$$

它的根与原方程的根相差 $\frac{b}{4a}$. 但是, 对所有的 u , (5.6.1) 式等价于

$$\begin{aligned} z^4 + z^2u + \frac{u^2}{4} - z^2u - \frac{u^2}{4} + pz^2 + qz + r &= 0, \\ \left(z^2 + \frac{u}{2}\right)^2 - \left[(u-p)z^2 - qz + \left(\frac{u^2}{4} - r\right)\right] &= 0, \end{aligned} \quad (5.6.2)$$

第一项是一个完全平方 P^2 , 这里 $P = z^2 + \frac{u}{2}$. 方括号中的项当选取 u 满足 (相当于判别式等于零)

$$q^2 = 4(u-p)\left(\frac{u^2}{4} - r\right) \quad (5.6.3)$$

时, 是一个完全平方 Q^2 . 应用定理 5.8, 这个关于 u 的三次方程可用根式求解. 如果 (5.6.1) 式的系数是实数, 我们甚至可以证明, 至少有一个实数 $u_1 \geq p$ 满足 (5.6.3) 式, 这是因为, 当 $u = p$ 时, (5.6.3) 式的右边为零, 并且当 $u > 0$ 充分大时, (5.6.3) 式的右边大于 q^2 , 或大于另一个任意预先给定的常数. 因此根据 4.4 定理 ??, (5.6.3) 式有所要求的实根 u .

把这个常数 u_1 代入 (5.6.2) 式, 则 (5.6.1) 式的左边采取形式 $P^2 - Q^2 = (P+Q)(P-Q)$, 或者

$$\left(z^2 + \frac{u_1}{2} + Q\right)\left(z^2 + \frac{u_1}{2} - Q\right), \quad (5.6.4)$$

这里

$$Q = Az - B, A = \sqrt{u_1 - p}, B = \frac{q}{2A}. \quad (5.6.5)$$

(5.6.1) 式的根显然是 (5.6.4) 式两个二次因子的根, 后者可根据 (5.5.4) 式求出. 注意, 如果原方程的系数 a, b, c, d, e 都是实数, 那么这两个因子也是实系数的。

回顾一下方程根式解法的历史是有意义的。二次方程的求解由 Hindus 发现。而它的

几何形式由希腊人给出 (4.1). 三次方程和四次方程的求解是由文艺复兴时期意大利数学家 Scipio del Ferro(1515) 和 Ferrari(1545) 给出。此外, 十八世纪末, 阿贝尔 (Abel) 和伽罗华 (Galois) 证明了所有次数 $n \geq 5$ 的多项式方程用根式求解是不可能的。

第五章习题

1. 用根式求解 $z^4 - 4z^3 + (1+i)z = 3i$.
2. 不用代数基本定理证明: 每个次数 $n < 6$ 的实系数多项式有复根。
3. 解联立方程

$$\begin{cases} zw = 1 + i, \\ z^2 + w^2 = 3 - i. \end{cases}$$

5.7 稳定型方程

很多物理系统是稳定的当且仅当相应的多项式方程的全部根具有负的实部。因此具有这种性质的方程称为“稳定型”方程。

在实二次方程 $z^2 + Bz + C = 0$ 的情形中, 容易检验它的稳定性。如果 $4C \leq B^2$, 则两个根都是实数。它们具有相同符号当且仅当 $z_1 z_2 = C > 0$, 符号是负的当且仅当 $B = -(z_1 + z_2) > 0$ 。如果 $4C > B^2$, 则方程的根是两个共轭复数, 它们两个具有负的实部 $x_1 = x_2$ 当且仅当 $B = -2x_1 = -2x_2 > 0$, 这种情形中也有 $C > \frac{B^2}{4} > 0$ 。因此这两种情形的“稳定性”条件是 $B > 0, C > 0$ 。

在实三次方程 $z^3 + Az^2 + Bz + C = 0$ 的情形中, 稳定性条件也不难找到。(当然, 只考虑简化形式 (5.5.5) 还不够。) 事实上, 如果所有的根具有负实部, 那么因为一个根 $z = -a$ 是实的, 所以我们有分解式

$$z^3 + Az^2 + bz + c = (z + a)(z^2 + bz + c), \quad (5.7.1)$$

这里 $a > 0$, 并由上述情况知 $b > 0, c > 0$ 。因此稳定性的必要条件是 $A = a + b > 0$, $B = (ab + c) > 0$ 和 $C = ac > 0$, 此外 $AB - C = b(a^2 + ab + c) > 0$ 。

反之, 假定 $A > 0, B > 0, C > 0, AB - C > 0$, 并考虑实分解式 (5.7.1), 根据定理 5.7 这个分解总是存在的。因为 $ac = C > 0$, 所以 a 和 c 有相同的符号。但是如果它们两个都是负的, 那么 b 必须是负的才能使 $ab + c > 0$, 因此 $A = a + b < 0$, 同假定矛盾, 因此 $a > 0, c > 0$, 并推出 $a^2 + ab + c = a(a + b) + c > 0$ 。但是这就推出 $b = \frac{AB - C}{a^2 + ab + c} > 0$ 。因此 (5.7.1) 式的两个因子是稳定的。因此我们证明了下面结果。

定理 5.10

实二次方程 $z^2 + Bz + C = 0$ 是稳定型方程当且仅当 $B > 0$ 和 $C > 0$ 。实三次方程 $z^3 + Az^2 + Bz + C = 0$ 是稳定型方程当且仅当 $A > 0, B > 0, C > 0$ 和 $AB > C$ 。

第五章习题

1. 检验下列多项式的稳定性:

- (a) $z^3 + z^2 + 2z + 1$,
(b) $z^3 + z^2 + 2z + 2$.
2. 证明: n 次首一实系数多项式是稳定型的, 那么它的所有系数都必须都是正的。
3. 证明: 实系数多项式 $z^4 + Az^3 + Bz^2 + Cz + D$ 是稳定型的当且仅当它的所有系数都是正的, 并且 $ABC > A^2D + C^2$.
4. 利用习题3, 求出复系数二次方程 $z^2 + Bz + C = 0$ 是稳定型方程的充分必要条件。(提示: 考虑 $(z^2 + Bz + C)(z^2 + B^*z + C^*) = 0$.)

第六章 群

6.1 正方形的对称

“对称”的概念对每个受过教育的人来说都是熟悉的，但是由对称产生的对称代数却只有少数人了解。我们将通过具体的正方形对称来引出这个代数。

我们设想一个正方形硬纸板放在有固定轴的平面上，使得正方形的中心落在坐标原点上，正方形的一个边是水平的。显然，这个正方形具有旋转对称：它通过下面的刚体运动可旋转成自身。

R : 围绕中心 O 顺时针旋转 90° .

R', R'' : 以同样的方式旋转 180° 和 270° .

这个正方形还有反射对称：它可以通过下面的刚体反射变为自身。

H : 关于过原点 O 的水平轴的反射.

V : 关于过原点 O 的垂直轴的反射.

D : 关于 I, III 象限中的对角线的反射.

D' : 关于 II, IV 象限中的对角线的反射.

至此，我们列举的这些情形包括了七种对称。

对称代数起源于下述事实：我们通过相继完成两个运动可以把两个运动相乘。例如，乘积 HR 可分两步得到：首先把正方形关于水平轴反射，然后再把正方形顺时针旋转 90° 。通过正方形硬纸板的实验，我们可以验证， HR 的最终效果与 D' 是一样的，这里是关于从左上角到右下角的对角线的反射。另一方面，等式 $HR = D'$ 可以通过观察正方形的每个顶点的变化来验证，如果等式两边具有同一个效果，则等式成立。例如，在图 1 中， HR 是先通过 H 把 1 送到 4，然后通过 R 把 4 送到 3，因此就把 1 送到 3，这恰好与 D' 的效果一样。

类似地， RH 定义为先顺时针旋转 90° 随后关于水平轴反射。（注意：图 6.1 的平面包含反射轴，这个平面可以想象成不随正方形而旋转。）

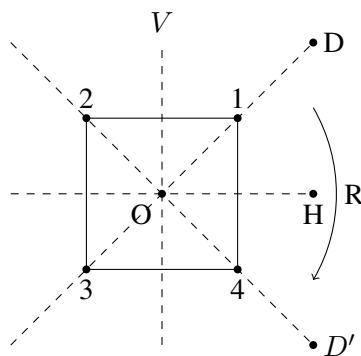


图 6.1

由计算表明 $RH = D \neq HR$ ，由此我们顺便得到这里所说的“乘法”一般不满足交换律！但是它满足结合律，我们在 6.2 中将看到这一点。

读者计算正方形对称的其他乘积 (6.4 的表 1 中给出的一个完整的乘法表) 是有意义的。当你做完这些乘积之后将会发现, 一般地, 逐次地把任意两个对称乘起来便得到第三个对称, 但有个例外, 例如, 当 R 和 R' 相乘时, 就会看到它的积是一个使正方形每个点都保持原来位置的运动, 这就是所谓的“恒等”运动 I 。这通常不被非数学家认为是对称; 尽管如此, 为了能使所有的对称两两相乘, 我们还是把 I 看作一个 (退化的) 对称。

一般地, 根据定义, 几何图形的对称是图形上的点保持距离不变的一一变换。容易看出, 正方形的任意对称一定把顶点 1 变换到四个可能的顶点之一, 而且对每个这样的选择正好有两个对称, 于是总共只有八个对称, 就是我们已经列出来的那些。

不仅正方形, 而且每个正多边形和正多面体 (例如立方体和正二十面体) 都存在有趣的对称群, 可以用上面概述的出等方法找到。

类似的, 很多装饰品有有趣的对称。例如我们考虑一个无限长的装饰图案



在这个图案中, 箭头是沿着直线以一英寸间隔均匀分布的。这个图形的三个简单的对称是: T , 向右平移一英寸; T' , 向左平移一英寸; H , 图形关于水平轴反射。其他对称 (事实上是一切对称) 可以由这三个对称反复相乘而得到。

第六章 习题

1. 计算 $HV, HD', D'H, R'D', D'R', R'R''$.
2. 在“箭头”装饰图案中, 描述对称 TH 和 HT .
3. 列出等边三角形的所有对称, 并计算五种具有代表性的乘积。
4. 列出普通矩形的所有对称, 并计算它们的所有乘积。
5. 正四面体有多少对称? 正八面体有多少对称? 画图说明。
6. 证明: 正文中的装饰图案的任意对称可通过 H, T 和 T' 反复相乘而得到。

6.2 变换群

对称代数可以推广到无论什么元素的任意集合 S 的一一变换。虽然常常把集合 S 看作“空间” (例如平面或球), 把 S 的元素看作“点”, 并且把双射看作 S 的相对于适当性质的“对称”, 然而在任何情况下, S 的双射还满足一些非平凡的代数定律。

为了理解这些定律, 我们必须清楚地记住 1.11 中给出的关于函数、单射、满射和双射的定义。为了重新解释它们, 我们给出一些新的例子。同 1.11 一样, 我们通常用缩写记号 xf 代替 $f(x)$ (读作“ x 通过 f 的变换”), 用 xg 代替 $g(x)$, 等等。

函数 $f(x) = e^{2\pi ix}$ 把实数域 \mathbb{R} 映入复数域 \mathbb{C} , 它的值域 (像) 是单位圆。类似的, $g(z) = |z|$ 是函数 $g: \mathbb{C} \rightarrow \mathbb{R}$, 它的像是所有非负实数的集合。

再有, 考虑下列整数环 \mathbb{Z} 到自身的函数 $\phi_0: \mathbb{Z} \rightarrow \mathbb{Z}$ 和 $\psi_0: \mathbb{Z} \rightarrow \mathbb{Z}$:

$$n\phi_0 = 2n, m\psi_0 = \begin{cases} \frac{m}{2}, & m \text{ 为偶数,} \\ 0, & m \text{ 为奇数.} \end{cases}$$

根据乘法消去律, ϕ_0 是一一的; 然而它的值域仅由偶数组成, 所以 ϕ_0 没有把 \mathbb{Z} 变换到 \mathbb{Z} 上。另一方面, ψ_0 不是一一的, 这因为所有奇数都映射到零, 但是它把 \mathbb{Z} 映到 \mathbb{Z} 上, 于是 ψ_0 是满射, 而不是单射。

我们现在转到变换代数。具有相同的定义域 S 和相同的取值域 T 的两个变换 $\phi : S \rightarrow T$ 和 $\phi' : S \rightarrow T$, 如果它们作用到 S 的每一点上都有相同的效果, 则称它们相等, 即

$$\phi = \phi' \text{ 的意思是, 对每个 } p \in S, p\phi = p\phi'. \quad (6.2.1)$$

再定义两个变换 ϕ 和 ψ 的乘积或合成 $\phi\psi$ 为它们相继作用的结果, 先 ϕ 后 ψ , 然而这里应假定 ϕ 的取值域是 ψ 的定义域, 换句话说, 如果

$$\phi : S \rightarrow T, \psi : T \rightarrow U,$$

那么 $\phi\psi$ 是由等式

$$p(\phi\psi) = (p\phi)\psi \quad (6.2.2)$$

给出的由 S 到 U 中的变换, 式中规定 $\phi\psi$ 作用到任意点 $p \in S$, 特别是, S (到自身) 的两个变换的乘积总是可以定义的。我们现在只考虑这种情况, 只要假定所包含的乘积有定义, 下面证明的恒等式几乎所有都可以用于一般情况。

变换的乘法适合

结合律

$$(\phi\psi)\theta = \phi(\psi\theta),$$

这里假定所包含的乘积都有定义, 直观上这是显然的: $(\phi\psi)\theta$ 和 $\phi(\psi\theta)$ 两者都是按照先 ϕ 后 ψ 最后 θ 的顺序作用的。正式地, 对每个 $p \in S$, 我们有

$$p[\phi(\psi\theta)]_{\phi(\psi\theta)} = (p\phi)(\psi\theta)_{\psi\theta} = [(p\phi)\psi]_{\phi\psi} \theta_{\phi\psi} = [p(\phi\psi)]_{(\phi\psi)\theta} \theta_{(\phi\psi)\theta} = p[(\phi\psi)\theta],$$

这里每步都依赖于乘法的定义 (6.2.2), 也就是把定义 (6.2.2) 用到与每步相对应的等号下面标出的乘积上。根据变换相等的定义 (6.2.1), 这就证明了结合律 $\phi(\psi\theta) = (\phi\psi)\theta$ 。

集合 S 上的恒等变换 $I = I_S$ 是使 S 上每个点保持固定的变换 $I : S \rightarrow S$ 。代数上, 这可叙述成等式

$$pI = p, \text{ 对每个 } p \in S. \quad (6.2.3)$$

从上面的定义, 直接推出 **同一律**

$$I\phi = \phi I = \phi, \text{ 对一切 } \phi.$$

为了验证这一点, 我们注意, 对所有的 p , 有 $p(I\phi) = (pI)\phi = p\phi$, 类似的, $p(\phi I) = (p\phi)I = p\phi$ 。

现在回到前面定义在集合 Z 上的特殊变换 ϕ_0 和 ψ_0 , 并计算它们的乘积。显然

$$m\psi_0\phi_0 = \begin{cases} m, & \text{当 } m \text{ 为偶数,} \\ 0, & \text{当 } m \text{ 为奇数.} \end{cases}$$

因此 $\psi_0\phi_0 \neq I$ 。另一方面, 对一切 $m \in \mathbb{Z}$, 有 $m\phi_0\psi_0 = m$, 因此 $\phi_0\psi_0 = I$ 。于是我们称 ψ_0 是 ϕ_0 的右逆元素 (而不是左逆元素)。

一般地, 如果变换 $\phi: S \rightarrow S$ 和 $\psi: S \rightarrow S$ 具有 $\phi\psi = I: S \rightarrow S$, 那么称 ϕ 是 ψ 的左逆元素, 而 ψ 是 ϕ 的右逆元素。这些定义同以前定义的是“一一映入的 (单射)”和“映上的 (满射)”等概念有密切关系。

定理 6.1

变换 $\phi: S \rightarrow S$ 是一一的当且仅当它有右逆元素, ϕ 是映上的当且仅当它有左逆元素。



证明 如果 ϕ 有右逆元素 ψ , $\phi\psi = I$, 并且 $p\phi = p'\phi$, 那么

$$p = p(\phi\psi) = (p\phi)\psi = (p'\phi)\psi = p'(\phi\psi) = p'.$$

于是由 $p\phi = p'\phi$ 可推出 $p = p'$, 因此 ϕ 是一一的。类似的, 如果 ϕ 有左逆元素 ψ' , 则 $\psi'\phi = I$ 。因此 S 中的任何元素 q 都可写成

$$q = qI = q(\psi'\phi) = (q\psi')\phi,$$

这表明 q 是某一点 $p = q\psi'$ 的 ϕ -像。因此 ϕ 是映上的。

反过来, 已知任意 $\phi: S \rightarrow S$, 我们首先如下构造第二个变换 $\psi: S \rightarrow S$ 。 S 中有一些点, 其中每个点 q 是 S 的一个或多个点 p 在 ϕ 之下的像。对每个点 q , 在这些点 p 中任意选出一个点作为像 $q\psi$, 那么, 对形为 $p\phi$ 的任何一个 q , 有

$$q(\psi\phi) = (q\psi)\phi = p\phi = q.$$

再令 ψ 随便按什么方式映射 S 中其余的点 q , 譬如说映射到 (非空) 集合 S 的某个固定点上。

现在, 如果 ϕ 是映上的, 那么每个 q 都有形式 $p\phi$, 因此 $\psi\phi = I$, 所以 ϕ 有 ψ 作为它的左逆元素。另一方面, 如果 ϕ 是一对一的, 那么, 对每个 p , $(p\psi)\phi$ 一定是唯一的 p , 即上面所说的 $q = p\phi$ 中的 p 。因此 $\phi\psi = I$, 所以 ψ 是 ϕ 的右逆元素, 如断言所述。

注 微积分学中函数记号 $y = \phi(x)$ 暗示记成 $y = \phi x$, 而前面我们写成 $y = x\phi$; 按照这种记号, ϕ 和 $z = \psi(y)$ 的合成自然写成 $z = (\psi\phi)x$, 它是作为 $z = \psi(\phi(x))$ 的缩写记号, 并代替 $z = x\phi\psi$ 。因此 $\psi\phi$ 的意思是“先执行 ϕ , 后执行 ψ ”, 而右逆元素和左逆元素的概念应相互对换。虽然上述两种记号用任何一种都是可以的, 但是一定要避免他们之间的混淆。然而, 双边逆元素的意思保持不变, 正如下面推论所述。

推论 6.1

变换 $\phi: S \rightarrow S$ 是双射当且仅当它既有右逆元素又有左逆元素。如果 ϕ 是双射, 那么 ϕ 的任意右逆元素等于 ϕ 的任意左逆元素。



事实上, 如果 ϕ 有右逆元素 θ 和左逆元素 ψ , 那么

$$\theta = I\theta = (\psi\phi)\theta = \psi(\phi\theta) = \psi I = \psi.$$

把变换 $\phi: S \rightarrow S$ 的 (双边) 逆元素定义为满足

逆律

$$\phi\phi^{-1} = \phi^{-1}\phi = I$$

的任意变换 ϕ^{-1} . 这些等式也表明 ϕ^{-1} 是 ϕ 的 (双边) 逆元素, 因此进一步有

推论 6.2

变换 $\phi: S \rightarrow S$ 是双射当且仅当 ϕ 有 (双边) 逆元素 ϕ^{-1} . 如果 ϕ 是双射, 那么 ϕ 的任何两个逆元素是相等的, 并有

$$(\phi^{-1})^{-1} = \phi. \quad (6.2.4)$$

这个推论后面将要用到. 它可以直接证明, 因为 ϕ^{-1} 只不过是这样一个变换, 它把 S 的每个点 $q = p\phi$ 变回原来唯一的点 p . 在 S 是有限的特殊情况下, ϕ 是一一的当且仅当 ϕ 是映上的, 因此在这种情况下左逆元素和右逆元素的更细致的讨论是没有意义的.

对于集合 S 到另一个集合 T 的函数 $\phi: S \rightarrow T$ 来说, 定理 6.1 及其推论以及它们的证明也都成立. 我们只需注意, 左逆元素 ψ 或者右逆元素 θ 是第二个集合 T 到集合 S 中的变换, 并注意

$$\psi\phi = I_T: T \rightarrow T, \quad \phi\theta = I_S: S \rightarrow S.$$

这里 I_S 和 I_T 分别是 S 和 T 上的恒等变换.

我们现在准备定义变换群这一重要概念. “空间” S 上的变换群是指满足下列条件的把 S 映上 S 的一一变换 ϕ 组成的任意集合 G :

- (i) S 的恒等变换在 G 中;
- (ii) 如果 ϕ 在 G 中, 则它的逆元素也在 G 中;
- (iii) 如果 ϕ 和 ψ 在 G 中, 则它们的积也在 G 中.

定理 6.2

任意空间 S 到自身的所有双射所组成的集合 G 是一个变换群.

证明 因为 $II = I, S$ 上的恒等变换 I 是双射, 因此 I 在集合 G 中, 上面的条件 (I) 满足. 如果 ϕ 在 G 中, 由前面的推论 6.2 得 ϕ^{-1} 也是双射, 因此它同样在 G 中, 条件 (II) 满足. 最后, 任意两个把 S 映上 S 的一一变换 ϕ 和 ψ , 它们的乘积有逆元素, 因为根据假设

$$\begin{aligned} (\phi\psi)(\psi^{-1}\phi^{-1}) &= \phi(\psi\psi^{-1})\phi^{-1} = \phi I \phi^{-1} = \phi\phi^{-1} = I, \\ (\psi^{-1}\phi^{-1})(\phi\psi) &= \psi^{-1}(\phi^{-1}\phi)\psi = \psi^{-1} I \psi = \psi^{-1}\psi = I, \end{aligned}$$

因此 $\phi\psi$ 也是双射, 并且有逆元素

$$(\phi\psi)^{-1} = \psi^{-1}\phi^{-1}. \quad (6.2.5)$$

口头上说就是, 乘积的逆元素等于逆元素颠倒次序相乘.

有限集 S 到自身的双射通常称为 S 的置换. n 个元素的所有置换组成的群称为 n 次对称群; 显然它包含 $n!$ 个置换, 这因为第一个元素的像 k_1 , 可以有 n 种方式选取, 然后, 第二个元素的像可从去掉 k_1 剩下的元素中以 $n-1$ 种方法选取, 等等.

第六章习题

1. 在正方形对称群中计算 $VD, (VD)R'', DR'', V(DR'')$.
2. 类似习题1., 计算 $HR, R'(HR), R'H, (R'H)R$.
3. 设 S 由所有实数组成 (或由直线上的所有点 x 组成), 所考察的变换具有形式 $x\phi = ax + b$. 在下列各种情况中, 以所指定类型的 a 和 b 为系数的所有可能的变换 ϕ 组成的集合, 哪些是变换群, 并给出证明.
 - (a) a 和 b 是有理数;
 - (b) $a = 1, b$ 是奇数;
 - (c) $a = 1, b$ 是正整数或零;
 - (d) $a = 1, b$ 是偶数;
 - (e) a 是整数, $b = 0$;
 - (f) $a \neq 0, a$ 和 b 是实数;
 - (g) $a \neq 0, a$ 是整数, b 是实数;
 - (h) $a \neq 0, a$ 是实数, b 是整数;
 - (i) $a \neq 0, a$ 是整数, b 是无理数;
 - (j) $a \neq 0, a$ 是有理数, b 是实数.

在这些变换群中, 哪些群的乘法满足交换律?

4. 找出恰有三个“点”的“空间” S 上的所有变换, 共有多少个变换? 其中有多少是一一变换?
5. 证明: 所有正整数的集合上的变换 $n \mapsto n^2$ 没有左逆元素. 并列两个明显的右逆元素.
6. 列出正文中定义的变换 $\psi_0: \mathbb{Z} \rightarrow \mathbb{Z}$ 的两个不同的左逆元素, 并列 ϕ_0 的两个不同的右逆元素.
7. 证明: 如果 ϕ 和 ψ 二者都有右逆元素, 那么 $\phi\psi$ 也有右逆元素.
8. 对于正方形对称群, 计算 $[R^{-1}(VR)]^{-1}[(R^{-1}D)R]$.
9. 对正方形对称群. 解方程 $RXR' = D$.
10. 在正方形对称群中, 验证

$$(RH)^{-1} = H^{-1}R^{-1} \neq R^{-1}H^{-1}.$$

11. 求出矩形每个对称的逆元素, 并验证公式 (6.2.5)。
12. 证明: 如果 $\phi_1, \phi_2, \dots, \phi_n$ 是一一的, 那么 $\phi_1\phi_2 \cdots \phi_n$ 也是一一的, 且有逆元素

$$(\phi_1\phi_2 \cdots \phi_n)^{-1} = \phi_n^{-1} \cdots \phi_2^{-1}\phi_1^{-1}.$$
13. 证明: 对任意 $\phi: S \rightarrow S$. 由定理6.1证明的第二部分所构造的变换 ψ 满足 $\phi\psi\phi = \phi$.
14. 证明: 具有唯一右逆元素或唯一左逆元素的变换 $\phi: S \rightarrow S$, 必是 S 到 S 上的一一变换。

6.3 其他例子

立方体的所有对称构成另一个有趣的群。用几何语言来说，这些对称是保持立方体上距离不变的一一变换。它们被称为“等距变换”，共有 48 个。为了说明这一点，我们注意到，任意一个初始顶点可以变换到八个顶点中的任意一点。任意顶点的变换固定之后，这个顶点的三个相邻顶点可以有六种方式进行排列，于是给出 $6 \cdot 8 = 48$ 种可能性。当一个顶点和它的三个相邻顶点的位置确定时，立方体上任何一点的位置也就固定下来，所以整个对称就知道了。因此立方体恰有 48 个对称。它们中间很多都具有特殊的几何性质，例如，其中一个对称是把立方体的每个点反射成对径点。

包含着无穷多个变换的一个熟悉的群是所谓欧几里得群。这个群由平面的所有“等距变换”组成，或者用初等几何的语言来说，在这些变换下，平面同自身是全等的。这个群由平移、刚体旋转和反射的乘积组成。我们将在第 7 章详细讨论它。

另一个群是由空间的所有“相似变换”组成，即由那些使一切距离扩大常数 k ($k > 0$ ，称为比例因子) 倍的一一变换组成。任意球面变为自身的所有刚体运动又构成一个群。使平面上正六边形网络保持不变的所有“等距变换”构成另一个有趣的群。

再有，一条橡皮绳沿一直线摆放着，绳的两端分别固定在 P, Q 两点，它可以沿着这条直线以很多种方式变形。所有这些变形构成一个群（通常称为线段 PQ 的同胚群）。

一般地说，任意集合的一一变换，如果保持集合中元素的某个或某些任意给定的性质，那么这些一一变换构成一个群。克莱茵 (Felix Klein) (Erlanger 纲领, 1872) 雄辩地描述了，不同的几何分支可以看作是研究相应空间的那些在适当的变换群下保持不变的性质。例如，欧几里得几何是研究空间的那些在所有等距变换下保持不变的性质，拓扑学是研究空间的那些在所有同胚变换下保持不变的性质。类似的，射影几何和仿射几何分别研究空间在射影群和仿射群下保持不变的性质。射影群和仿射群的定义将在第 7 章给出。

第六章 习题

1. 描述带有六个等间隔辐条的车轮的全部对称。
2. 描述一个顶点固定的立方体的六个对称。
3. 设 S, T 是立方体关于平面的反射，这两个平面分别平行于立方体的两个不同的侧面。描述 ST 的几何意义。
4. 描述一些把图 2 的正六边形网络变到自身的平面等距变换。
5. 对正方形网络作习题 4。你能数出所有这样的变换吗（这是困难的）？
6. 对正三角形网络作习题 4。并说明这些变换与习题 1 的变换群的关系。
7. 对下述几种情况作习题 4：
 - (a) 无限圆柱体。
 - (b) 有限圆柱体，
 - (c) 圆柱螺旋线，即一条围绕柱面并与圆柱轴线成定角的螺旋线。
8. 证明：所有变换 $x \mapsto x' = \frac{ax+b}{cx+d}$ （其中系数 a, b, c, d 在任意域 F 中，并且 $ad-bc=1$ ）组成一个群，这些变换作用在由域 F 的全体元素和符号元素 ∞ 组成的集合上。

6.4 抽象群

变换群绝不是其乘法满足6.2中所说的结合律、同一律和逆律的唯一系统。例如，任意域（如有理数域，实数域和复数域）的全体非零元素都满足这些定律。因为任意两个非零元素的乘积是一个非零元素；结合律成立；域的单位元素1满足同一律，并且 $\frac{1}{x} = x^{-1}$ 满足逆律。

类似的，任意整环的全体元素（这次包括零）在加法运算之下满足上述三个定律。例如，任意两个元素有唯一确定的和；加法满足结合律；对于加法运算，零满足同一律， $-x$ 满足逆律。换句话说，任意整环的全体元素在加法之下构成一个群。

为方便起见，我们引进包含上述和其他一些例子的群的抽象概念。

定义 6.1. 群 (Group)

具有二元运算的元素集合 G , (i) 运算满足结合律；(ii) 有一个满足同一律的单位元素；(iii) 对每个元素 a , 有元素 a^{-1} （称为 a 的逆）满足逆律，则这个集合 G 称为群。

我们可以不提变换，用许多方式抽象地给出群的定义，这样定义的群常常称为抽象群。

在讨论抽象群的时候，元素用小写拉丁字母 a, b, c, \dots 来表示。乘积记号“ ab ”通常用来表示 G 的两个元素 a 和 b 在群的运算之下而得的结果，但是其他记号，像“ $a + b$ ”和“ $a \circ b$ ”也同样适用。在乘积记号中，用“ e ”表示单位元素，定义群的三个定律变为结合律 $a(bc) = (ab)c$, 对一切 a, b, c .

同一律 $ae = ea = a$, 对一切 a .

逆律 $aa^{-1} = a^{-1}a = e$, 对每个 a 和某个 a^{-1} .

其运算满足交换律的群称为交换群或阿贝尔群。利用这个概念我们可以把域的定义简化如下。

定义 6.2. 域

集合 F 满足下列条件时称为域， F 在两个唯一确定的二元运算——加法和乘法之下是封闭的，并有

- (i) 在加法之下， F 是具有单位元素零的交换群；
- (ii) 在乘法之下， F 中非零元素构成交换群；
- (iii) 分配律成立： $a(b + c) = ab + ac$.

为证明这个定义同2.1中给出的定义是等价的，我们注意，这里给出的公设，除了含有因子零的乘法结合律外，包含前面对域所描述的一切公设。这可以详细地验证。

第1、2章的第一节中的一些结果现在将表现为下面关于群的定理的推论。

定理 6.3

在任意群中， $xa = b$ 和 $ay = b$ 有唯一解，分别为 $x = ba^{-1}$ 和 $y = a^{-1}b$ 。因此由 $ca = da$ 可推出 $c = d$ ，同样由 $ac = ad$ 可推出 $c = d$ （消去律）。

证明 如果 a^{-1} 是在逆律中确定的元素，显然， $(ba^{-1})a = b(a^{-1}a) = be = b$ 。类似的，

$a(a^{-1}b) = b$ 。反过来, 由 $xa = b$ 可推出 $x = xe = xaa^{-1} = ba^{-1}$, 同样地, 由 $ay = b$ 可推出 $y = a^{-1}b$ 。

注意, 在这个证明中并没有假定 a^{-1} 是满足 $xa = e$ 的唯一的元素。但 a^{-1} 确是唯一的, 这是因为, 若 $xa = e$, 则

$$x = xe = x(aa^{-1}) = (xa)a^{-1} = ea^{-1} = a^{-1}.$$

类似地, a^{-1} 是使得 $ay = e$ 的唯一元素。

因为根据定理6.3, 在任意群 G 中方程 $ex = e$ 和 $ay = e$ 有唯一解分别为 $x = e$ 和 $y = a^{-1}$, 因此, 我们得到

推论 6.3

群有唯一的单位元素, 并且对每个元素 a 有唯一的逆 a^{-1} .



定理 6.4

前面所述的群的定义中, 同一律和逆律可以用较弱的形式来代替。

左同一律 对所有的元素 a , 存在某元素 e , 满足 $ea = a$.

左逆律 对给定的元素 a , 存在某元素 a^{-1} , 满足 $a^{-1}a = e$.



证明 如果这些弱的定律成立, 则左消去律也成立, 即由 $ca = cb$ 可推出 $a = b$ 。因为我们只须用 c^{-1} 左乘等式 $ca = cb$ 的两边, 再用结合律得到 $(c^{-1}c)a = (c^{-1}c)b$, 这就是 $ea = eb$, 故得 $a = b$ 。

给出的这个左单位元素也是右单位元素, 这是因为

$$a^{-1}ae = ee = e = a^{-1}a$$

再根据左消去律, 因此对所有的 a , 有 $ae = a$ 。最后, 左逆元素也是右逆元素, 因为由于左单位元素也是右单位元素, 则有

$$a^{-1}(aa^{-1}) = (a^{-1}a)a^{-1} = ea^{-1} = a^{-1} = a^{-1}e,$$

现在再用左消去律, 得 $aa^{-1} = e$ 。这就完成了我们的证明。

还有很多其他的群公设系统, 常用的一个是按照除法的可能性来建立的, 如下所述:

定理 6.5

如果 G 是一个非空集合, 在满足结合律的乘法之下是封闭的, 对于这个集合所有的方程 $xa = b$ 和 $ay = b$ 在 G 中有解 x 和 y , 那么 G 是一个群。



证明留做习题。

除了对任意群 G 把有关乘法的代数定律系统化以外, 当 G 的元素有限时, 我们还可以用“乘法表”的形式给出 G 中任意两个元素乘积的特殊构成法则。这个乘法表是一些元素的正方形阵列, 表的最左一列和最上一行列出群的所有元素。表中对对应着最左列上的 a 和最上行的 b 的那个元素是乘积 ab (按此次序)。

为举例说明, 我们在表6.1中绘制了正方形对称群的乘法表。这个表的计算可以按照6.1中证明的 $HR = D'$ 和 $RH = D$ 的模式来进行。其他方法将在6.6中描述。

表 6.1: 正方形对称群

	I	R	R'	R''	H	V	D	D'
I	I	R	R'	R''	H	V	D	D'
R	R	R'	R''	I	D	D'	V	H
R'	R'	R''	I	R	V	H	D'	D
R''	R''	I	R	R'	D'	D	H	V
H	H	D'	V	D	I	R'	R''	R
V	V	D	H	D'	R'	I	R	R''
D	D	H	D'	V	R	R''	I	R'
D'	D'	V	D	H	R''	R	R'	I

关于群的大部分性质可以直接从表中看到。例如，单位元素的存在表明，某一行和相应的列一定分别是顶头一行和最左边一列的复制品。方程 $ay = b$ 可解意味着 a 所在的那一行一定包含元素 b ；因为解是唯一的，所以 b 在这一行中只能出现一次。一个群是交换群当且仅当它的乘法表关于主对角线（即左上角到右下角的连线）是对称的。遗憾的是，结合律不容易从这个表中直观地看出。

第六章 习题

1. 设 a, b, c 是群的固定元素，证明方程 $axaxba = xbc$ 有唯一解。
2. 证明：在 $2n$ 个元素的群中，除单位元素外还存在一个元素同它的逆相等。
3. 全体正实数在加法下构成一个群吗？在乘法下构成群吗？全体偶数在加法下构成群吗？全体奇数呢？为什么？
4. 在模 11 整数域 \mathbb{Z}_{11} 中，下列集合中哪些在乘法下构成群：
 - (a) $\{1, 3, 4, 5, 9\}$,
 - (b) $\{1, 3, 5, 7, 8\}$,
 - (c) $\{1, 8\}$,
 - (d) $\{1, 10\}$.
5. 证明：含有四个元素或少于四个元素的群一定是阿贝尔群。（提示： ba 是 e, a, b, ab 中的一个，显然的情形除外。）
6. 证明：如果在一个群中 $xx = x$ ，则 $x = e$ 。
7. 下列乘法表描述一个群吗？

	a	b	c	d
a	b	d	a	c
b	d	c	b	a
c	a	b	c	b
d	c	a	d	a

	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	a
d	d	c	b	b

8. 证明：1.2 中法则 2(单位元)，4(消去律)，和 6(逆元唯一性) 在任意交换群中都成立。
9. 下列数集中哪一些是群？为什么？

- (a) 所有有理数, 在加法运算之下; 在乘法运算之下;
 - (b) 所有无理数, 在乘法运算之下;
 - (c) 所有绝对值为 1 的复数, 在乘法运算之下;
 - (d) 所有绝对值为 1 的复数, 在运算 $z \circ z' = |z| \cdot z'$ 之下;
 - (e) 所有整数, 在减法运算之下;
 - (f) 任意整环的全体单位 (3.6), 在乘法运算之下;
10. 证明: 下列公设系统描述一个阿贝尔群:
- (i) 对一切 a, b, c 有 $(ab)c = a(bc)$;
 - (ii) 定理 6.4 的“左同一律”成立;
 - (iii) 定理 6.4 的“左逆律”成立;
11. 证明: 如果对群 G 中所有元素有 $x^2 = e$, 那么 G 是交换群。
12. 证明定理 6.5。(提示: 如果 $ax = a$, 那么 x 是右单位元素, 并且任意右单位元素等于左单位元素。)
13. 设 S 是一个非空集合, 在乘法运算之下是封闭的, 并且满足 $ab = ba, a(bc) = (ab)c$, 由 $ax = ay$ 可推出 $x = y$.
- (a) 证明: 若 S 有限, 则 S 是群。
 - (b) 证明: 若 S 有限或无限, 则 S 可以嵌入一个群中。

6.5 同构

考虑实数整环上的变换 $x \mapsto \log x$. 我们知道, 当 x 在区间 $0 < x < +\infty$ 上增加时, $\log x$ 就在区间 $-\infty < x < +\infty$ 上连续增加; 也就是说, 这个对应是正实数系和全体实数系之间的一一对应 (逆变换是 $y \mapsto e^y$)。而且对所有的 x, y , 有 $\log xy = \log x + \log y$, 于是我们可以用相应的和的计算代替乘积的计算。事实上, 这是对数主要的实际用途。

其次, 设 \mathbb{Z}_3 是模 3 整数构成的域 (3.10), 并设 G 是等边三角形到自身的刚体旋转群。如果 I, R 和 R' 分别表示转过 $0^\circ, 120^\circ$ 和 240° 的旋转, 那么把整数同旋转联系起来的对应 $0 \leftrightarrow I, 1 \leftrightarrow R, 2 \leftrightarrow R'$ 是一个把 \mathbb{Z}_3 中元素的和映射成 G 中相应旋转的乘积的双射。例如, 考虑对应

$$\begin{aligned} 1 + 2 &\equiv 0 \pmod{3} &\leftrightarrow & RR' = I \\ 2 + 2 &\equiv 1 \pmod{3} &\leftrightarrow & R'R' = R \end{aligned}$$

这些都是 1.12 中所谈到的“同构”一般概念的例子, 这个概念对群来说比对整环更简单也更重要。

定义 6.3

两个群 G 和 G' 之间的同构指的是它们元素之间保持群的乘法的双射 $a \leftrightarrow a'$, 即它满足, 若 $a \leftrightarrow a'$ 和 $b \leftrightarrow b'$, 则 $ab \leftrightarrow a'b'$.



例如, 在第一个例子中我们描述了正实数乘法群与实数加法群之间的同构, 在第二

个例子中，我们指出一个模 3 整数加法群与正三角形旋转对称群之间的同构。

类似的，映射 $0 \mapsto 1, 1 \mapsto 2, 2 \mapsto 4, 3 \mapsto 3$ 是模 4 整数加法群与模 5 非零整数乘法群之间的同构。通过比较模 4 整数加法群的加发表和模 5 非零整数乘法群的乘法表来验证这个结果是方便的。见表 6.2 和表 6.3。

表 6.2

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

表 6.3

×	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

依次我们有，模 4 整数加法群同构于正方形旋转对称群。通过比较表 6.2 和表 6.1 (6.4) 的旋转部分可以验证，双射 $0 \leftrightarrow I, 1 \leftrightarrow R, 2 \leftrightarrow R', 3 \leftrightarrow R''$ 是一个同构。

同构的概念很重要，因为它使我们认识到，完全不同的群从抽象群论的观点看可以看成同一个群。同构的群抽象地认为是同一个群（它们的差别仅在于它们元素符号的不同），这个事实可以在很多情况下看到。

例如，根据定义，两个有限群 G 和 G' 同构当且仅当通过适当的替换，从 G 的群表可以得出 G' 的群表，从 6.4 的倒数第二句可以得出， G' 是阿贝尔群当且仅当 G 是阿贝尔群，也就是说，一个有限阿贝尔群的任何同构像是阿贝尔群，还有，在其他方面，同构的性质很像相等。

定理 6.6

关系“群 G 同构于群 G' ”满足群之间的自反的，对称的和传递的关系。



证明 自反性是显然的（每个群通过恒等变换同它自身同构）。对于对称性，设 $a \leftrightarrow aT$ 是 G 和 G' 之间的任意同构对应，因为 T 是双射，所以 T 有逆元素 T^{-1} ， T^{-1} 是 G' 到 G 上的同构。最后，如果 T 把 G 同构地映射到 G' 上，而 T' 把 G' 同构地映射到 G'' 上，那么 TT' 就是 G 和 G'' 之间的同构。

值得注意的是，定理 6.6 及其证明对于整环之间的同构同样成立，而且对于任何类型的代数系统之间的同构也都成立。

定理 6.7

在两个群同构之下，它们的单位元素相互对应，相应元素的逆元素相互对应。



证明 方程 $ax = a$ 的唯一解 e 对应到 $a'x = a'$ 的唯一解 e' ，因此单位元素相互对应。所以， G 中方程 $ax = e$ 的唯一解 a^{-1} 对应到 G' 中方程 $a'x = e'$ 的唯一解 a'^{-1} 。这就完成了证明。

我们最后证明著名的凯莱 (Cayley) 定理，这个定理可被解释为是证明变换乘法有关公设的完备性。

定理 6.8

任意抽象群 G 与一个变换群同构。



证明 把由 G 的所有元素组成的“空间”上的每个变换 $\phi_a: x \rightarrow xa = x\phi_a$ 同 G 的元素 a 联系起来。因为由 $e\phi_a = e\phi_b$ 可推出 $a = ea = eb = b$, 所以 G 的不同元素对应着不同的变换, 因为对所有的 x , 有

$$x(\phi_a\phi_b) = (x\phi_a)\phi_b = (xa)\phi_b = (xa)b = x(ab) = x\phi_{ab}, \quad (6.5.1)$$

所以乘积 $\phi_a\phi_b = \phi_{ab}$, 因而所有 ϕ_a 的集合 G' 包含任意两个变换, 就一定包含它们的乘积。再有, 因为对所有的 x 有 $x\phi_e = xe = x$, 所以 G' 包含单位元素。我们可以类似地证明, 对所有的 a , $(\phi_a)^{-1}$ 存在, 并在 G' 中, 实际上它就是 $\phi_{a^{-1}}$, 因此 G' 是一个变换群, 根据 (6.5.1), 它与 G 同构。

第六章 习题

1. 下列群中, 任意两个群都同构吗?
 - (a) 等边三角形的对称群;
 - (b) 正方形对称群;
 - (c) 正六边形的旋转群;
 - (d) 模 6 整数加法群。
2. 与习题 1 同样的问题。
 - (a) 正方形的旋转群;
 - (b) 矩形的对称群;
 - (c) 菱形 (等边平行四边形) 的对称群;
 - (d) 模 13 整数 1, 5, 8, 12 的乘法群;
 - (e) 模 12 整数 1, 5, 7, 11 的乘法群。
3. (a) 证明: “高斯整数” $m + n\sqrt{-1}$ ($m, n \in \mathbb{Z}$) 的加法群同形为 $2^n 3^m$ ($m, n \in \mathbb{Z}$) 的有理因子的乘法群同构。
 (b) 给出两个与矩形网络的变换群同构的群。
4. 非零实数构成的乘法群与所有实数构成的加法群同构吗?
5. 确定 \mathbb{Z}_4 的加法群与正方形的旋转群之间的所有同构。
6. (a) 列出正方形对称群与正方形四个顶点 1, 2, 3, 4 上的变换群之间的同构。
 (b) 像定理 6.7 那样明显地指出, 两个群中的逆元素在这个同构之下是如何对应的。
7. 对正六边形的旋转群做习题 6.
8. 列出与下列每个群同构的变换群, 说明定理 6.8
 - (a) 所有实数构成的加法群;
 - (b) 所有非零实数构成的乘法群;
 - (c) 模 8 整数加法群。

6.6 循环群

在任意群中, 元素 a 的整数幂 a^m 可以分别对正指数、零指数和负指数来定义。当 $m > 0$ 时, 我们定义

$$a^m = a \cdot a \cdots a (m \text{ 个因子}), a^0 = e, a^{-m} = (a^{-1})^m. \quad (6.6.1)$$

两个普通的指数定律成立:

$$a^r a^s = a^{r+s}, \quad (a^r)^s = a^{rs}. \quad (6.6.2)$$

另一方面, 一般说来, $(ab)^r \neq a^r b^r$ (参见习题2).

如果两个指数 r 和 s 都是正的, 那么定律 (6.6.2) 可由定律 (6.6.1) 直接推出¹。对于 (??) 式的第一个定律的其他情形, 当 r 和 s 中有一个可能为零时, (6.6.2) 式立即得出; 当 r 和 s 两者都可能为负的时, (6.6.2) 式可从定义 (6.6.1) 的最后一个公式直接推出。剩下的情形就是一个指数为负一个指数为正, 比如 $r = -m, s = n$, 其中 $m > 0, n > 0$ 。这时

$$a^{-m} a^n = (a^{-1})^m a^n = (a^{-1} \cdots a^{-1})(a \cdots a).$$

根据结合律, 我们可以相继消去一些 a 和 a 的逆 a^{-1} , 当 $n \geq m$ 时, 留下 a^{n-m} , 而当 $n < m$ 时, 留下某些逆, 即 $(a^{-1})^{m-n}$ 或 $a^{-(m-n)}$ 。这两种情形我们都得到所要求的 $a^{-m} a^n = a^{n+(-m)}$ 。

(6.6.2) 式的第二个定律可以更简单地证明。如果 s 为正, 则由 (6.6.2) 式的第一个定律有

$$a^r a^r \cdots a^r = a^{r+r+\cdots+r} = a^{rs}.$$

如果 s 为负, 注意不管 r 是正的, 零和负的, 都有 $(a^r)^{-1} = a^{-r}$, 我们可以做类似的展开。如果 s 为零, 则立即可得结论。

定义 6.4

群中元素 a 的阶是指使得 $a^m = e$ 成立的最小正整数^a m 。如果找不到 a 的正次幂等于 e , 则定义 a 的阶位无穷。如果群 G 包含某一个元素 x , G 的元素都由 x 的幂组成, 那么称 G 为循环群; 这个元素 x 称为群 G 的生成元。

^a良序原理保证这个 m 一定存在。



例如, 正方形的所有到自身的旋转构成的群是由 R 的四个幂 R, R^2, R^3 和 $R^4 = I$ 组成, 这里 R 表示顺时针旋转 90° 。这个群完全等同的可以由 R^3 生成 (R^3 表示逆时针旋转 90°), 这因为 $R^2 = (R^3)^2, R = (R^3)^3, I = (R^3)^4$, 同 R^3 一起组成这个群。

定理 6.9

如果元素 a 生成循环群 G , 那么 a 的阶可以确定群 G (在同构意义下)。事实上, 如果 a 的阶是无穷, 那么 G 同构于整数加法群; 如果 a 的阶是某有限整数 n , 那么

¹ r 个因子“ a ”后跟着 s 个因子 a , 共有 $r + s$ 个因子。再有, 每组有 r 个因子“ a ”, s 组共有 rs 个因子。

G 同构于模 n 整数加法群。



证明 首先, $a^r = a^s$, 当且仅当

$$e = a^r(a^s)^{-1} = a^r a^{-s} = a^{r-s}, \quad (6.6.3)$$

这里用了公式 (6.6.2)。再看, 若 $r \neq s$, 则或 $r > s$, 或 $s > r$, 因此, 如果 a 的阶是无穷, 那么不存在整数 $r > s$ 使得 $a^{r-s} = e$, 所以不存在 a 的两个不同的幂是相等的。此外, 由 (6.6.2) 有 $a^s a^t = a^{s+t}$, 因此对应 $a^s \mapsto s$ 使群 G 与整数加法群同构, 这就证明了定理的第一个结论。

如果 a 的阶是有限的, 那么使得 $a^t = e$ 的整数 t 的集合包含零, 由 (6.6.2) 可知这个集合还包含它的任意两个元素的和与差。因此, 根据 1.7 定理 1.6, $a^t = e$ 当且仅当 t 是 a 的阶的倍数, 所以根据公式 (6.6.3), $a^r = a^s$ 当且仅当 $n|(r-s)$; 也就是说, $a^r = a^s$ 当且仅当 $r \equiv s \pmod{n}$ 。最后, 再由 (6.6.2), 有 $a^r a^s = a^{r+s}$, 所以对应 $a^r \mapsto r$ 是 G 到模 n 整数加法群的同构。

定理 6.9 的一个推论是, 任意循环群 G 的元素个数 (称为群 G 的阶) 等于 G 的任意一个生成元的阶, 任意两个同阶循环群同构。

正方形对称群不是循环群, 不过它是由两个元素 R 和 H 生成的; 事实上, 表 6.1 (6.4) 指出

$$\begin{aligned} R^0 &= I, R = R, R^2 = R', R^3 = R''; \\ H &= H, HR = D', HR^2 = V, HR^3 = D. \end{aligned}$$

于是这个群的全体元素都可唯一地表示成 $H^i R^j$, 其中 $i = 0, 1, j = 0, 1, 2, 3$ 。此外, R 和 H 还满足

$$R^4 = I, H^2 = I, RH = HR^3.$$

这些等式称为“定义关系”, 因为这些关系可以使任意两个元素的乘积 $H^i R^j$ ($i = 0, 1$) 化成同样的形式。例如

$$D'V = HRHR^2 = HHR^3R^2 = IR = R,$$

类似的计算将给出正方形对称群的整个乘法表 (6.1)。

第六章 习题

1. 利用定义 $a^1 = a, a^{m+1} = a^m a$, 对正指数用归纳法来证明公式 (6.6.2)。
2. 证明: 如果对 G 中一切 a, b , 及一切正整数 n , 有 $(ab)^n = a^n b^n$, 那么 G 是交换群, 反之也真。
3. 6 阶循环群有几个不同的生成元?
4. 证明: 如果 6 元素的交换群包含一个 3 阶元素, 那么这个群是循环群。
5. (a) 模 7 整数 $1, 2, \dots, 6$ 组成的乘法群是循环群吗?
(b) 模 8 整数 $1, 3, 5, 7$ 组成的乘法群是循环群吗?
(c) 模 9 整数 $1, 2, 4, 5, 7, 8$ 组成的乘法群是循环群吗?

6. 设循环群 G 是由 m 阶元素 a 生成, 证明: a^k 生成 G 当且仅当 k 与 m 互素。
7. 在习题6.的假定之下, 求 G 的任意元素 a^k 的阶。
8. 求正方形对称群中每个元素的阶。
9. 给出满足定义关系 $x^2 = y^2 = e$, $xy = yx$ 的两个元素 x 和 y 生成群 G 所有元素和乘法表。
10. 二面体群 D_n 是正 n 边形的所有对称构成的群 (当 $n = 4$ 时, D_n 就是正方形对称群)。证明: D_n 包含 $2n$ 个元素, 并由两个元素 R 和 H 生成, 这里 R 和 H 满足 $R^n = I$, $H^2 = I$, $RH = HR^{n-1}$ 。
11. 分别找出下面三个无限图案的对称群的生成元和定义关系。三个群中任意两个同构吗?
想象图形沿两个方向无限延伸下去。
12. 对6.3中的习题1.,2.,4.和5.进行与上题类似的讨论。

6.7 子群

很多群都包含在较大的群之中。例如, 正方形的旋转群是正方形对称群的一部分。再有, 根据对称性诱导出的正方形顶点的八个置换构成的群, 是这些顶点的所有 $4! = 24$ 个置换组成的置换群的一部分。偶数加法群是整数加法群的一部分。

这些例子提出子群的概念。群 G 的一个子集 S , 如果关于 G 的二元运算 (乘法) S 本身也是一个群, 那么称 S 为 G 的子群。

在任意群 G 中, 仅由单位元素 e 组成的集合是一个子群。整个群 G 也是它自己的一个子群。 G 中不是平凡 (“伪”) 子群 e 和 G 的子群称为真子群。

定理 6.10

群 G 的非空子集 S 是子群当且仅当 (i) 由 a 和 b 在 S 中推出 ab 在 S 中; (ii) 由 a 在 S 中推出 a^{-1} 在 S 中。



证明 在这些假设之下, 显然 S 是一个子群: 结合律是显然的; 因为至少有一个元素 a 在 S 中, 所以 G 的单位元素 $e = aa^{-1}$ 在 S 中; 群的其他公设已被假定。反过来, 我们必须证明在任一子群中 (i) 和 (ii) 成立。 G 的任意子群的单位元素 $x = e'$ 满足 $xx = x$, 因此它是 G 的单位元素 (6.4习题6.)。由此可以推出, 因为对任何元素 a , G 有且仅有一个逆元素, 所以在子群中任何元素 a 的逆元素与它作为 G 中元素的逆元素是同一个元素, 故 (ii) 成立。条件 (i) 是显然的。

对于有限阶 (m) 元素 a , 显然有 $a^{m-1}a = a^m = e$, 因此 $a^{-1} = a^{m-1}$. 于是我们有下面简化的条件。

定理 6.11

有限群 G 的非空子集 S 是群 G 的子群当且仅当 S 中任意两个元素的乘积仍在 S 中。



在已知的非阿贝尔群 G 的所有子群中间, 最重要的一个子群是 G 的中心。它定义

为, 对一切 $x \in G$ 满足关系 $ax = xa$ 的所有元素 $a \in G$ 的集合。我们留给读者验证。实际上, 群的中心总是 G 的子群。

确定一个特定群 G 的全部子群, 一般来说是很困难的。在 G 是循环群的情况下, 我们现在来确定它的全部子群。

定理 6.12

循环群 G 的任何子群是循环群。



证明 设 G 由元素 a 的幂组成, 如果 a^s 和 a^t 在 S 中, 则由定理 6.10, $a^{s+t} = a^s a^t$ 和 $a^{s-t} = a^s (a^t)^{-1}$ 都在 S 中。因此, 使 a^s 在 S 中的整数 s 组成的集合在加法和减法之下是封闭的, 所以²这个集合由某一个最小正指数 r 的所有倍数组成 (1.7 定理 1.6)。因而 S 由所有幂 $a^{kr} = (a^r)^k$ 组成, 因此 S 是以 a^r 为生成元的循环群。

在 G 为无限的情况下, 每个 $r > 0$ 确定不同的子群。如果 G 有 n 个元素, 那么, 因为 $a^n = e$ 一定在 S 中, 所以只有那些 n 的因子 $r > 0$ 才能用这种方法确定出 G 的子群, 而这些子群全不相同。

为得到进一步研究子群的材料, 我们现在列出正方形对称群的全部子群。通过验证 6.1 给出的这个群运算的定义, 我们找到了全部真子群, 每个子群保持八种构形中的一种不变性:

一对角线	一轴	一面
$[I, D, D', R']$	$[I, H, V, R']$	$[I, R, R', R'']$
一轴和一对角线	顶点 1(或 3)	顶点 2(或 4)
$[I, R']$	$[I, D]$	$[I, D']$
一垂直边	一水平边	
$[I, H]$	$[I, V]$	

这里保持面不变的变换, 我们理解为正方形没有翻转的那些变换。所有这些子群可以在一个表上按它们相互之间的关系表示出来, 其中每个群用向下的线或一串线同它的所有子群连接起来, 如图所示。

不用几何方法我们也可以找出所有这些子群。事实上, 把群的元素看作纯抽象的元素, 可以最有效的确定一个特定有限群 G 的全部子群, 如下所述。

首先注意, 如果 G 的子群 S 包含元素 a , 则 S 也包含由 a 的所有幂组成的循环子群 $\{a\}$ (证明它是子群!)。在上述例子中, 这个方法给出列出的除前两个子群以外的所有子群。其次注意, 任何子群不仅包含两个循环子群 $\{a\}$ 和 $\{b\}$, 而且必包含 a 和 b 的幂的所有乘积 (例如 $a^2 b^{-3} a$ 所组成的集合 $\{a, b\}$)。(用定理 6.11 证明这个集合构成一个子群!) 在上述例子中, 这种方法给出了剩下的子群。(在 6.8 我们将看到, 为什么这些子群都是含有 2 个或 4 个元素。) 一般来说, 我们还可以进一步对由三个或更多的元素生成的子群

²当集合 S 仅由零组成时, 取 $r = 0$, 这个结论还成立。

$\{a, b, c\}$ 进行检验, 但是这时群中元素的个数应至少是四个不同素数之积, 否则绝不会出现这种情况。

两个子群 (实际上也可以是任意两个集合!) S 和 T 的交 $S \cap T$ 是由既属于 S 又属于 T 的所有元素组成的集合。

定理 6.13

群 G 中两个子群 S 和 T 的交 $S \cap T$ 是 G 的子群。



证明 根据定理 6.10, a 在 $S \cap T$ 中意味着 a 在 S 中, 因此 a^{-1} 在 S 中, 同样可推出 a^{-1} 在 T 中, 所以 a^{-1} 在 $S \cap T$ 中。类似的, a 和 b 都在 $S \cap T$ 中意味着 ab 既在 S 中又在 T 中, 所以 ab 在 $S \cap T$ 中。因此根据定理 6.10, $S \cap T$ 是一个子群。还有, $S \cap T$ 包含 e , 所以 $S \cap T$ 是非空的。

显然, $S \cap T$ 是包含在 S 和 T 中的最大子群。对偶的, 存在包含 S 和 T 的最小子群。它由 S 和 T 中元素的正幂和负幂的所有乘积组成, 称它为 S 和 T 的并, 记作 $S \cup T$ ³。在第 9 章中我们将再讨论这些概念。

第六章习题

1. 在正六边形对称群中, 保持对角线不变的子群是什么?
2. 证明: 如果 T 是 S 的子群, S 又是 G 的子群, 那么 T 是 G 的子群。
3. 在四个数字 1, 2, 3, 4 的置换群中 (置换记作 ϕ), 找出下列子群:
 - (a) 所有把集合 $\{1, 2\}$ 变为 $\{1, 2\}$ 的置换 ϕ 。
 - (b) 所有适合 “对集合 $\{1, 2, 3, 4\}$ 中任意两个数字 a, b , 由 $a \equiv b \pmod{2}$ 可推出 $a\phi \equiv b\phi \pmod{2}$ ” 的置换 ϕ 。
4. 证明: 当 G 是无限的, 但 G 的所有元素有有限阶, 定理 ?? 仍然成立。说明 $\mathbb{Z}_p[x]$ 的加法群就是这样一个群。
5. 列出下列各群的所有子群:
 - (a) 模 12 整数加法群;
 - (b) 正五边形对称群;
 - (c) 正六边形对称群;
 - (d) 四个字母的置换群。
6. 设 $a \leftrightarrow a'$ 是两个置换群 G 和 G' 之间的同构, 又设 S 是 G 中保留一个字母固定的那些置换组成的集合。 G' 中与所有 $a \in S$ 对应的那些元素组成的集合 S' , 一定是 G' 的子群吗? 集合 S' 一定保留一个字母固定吗? 说明一下。
7. 证明: 任意群 G 的中心是 G 的子群。
8. 找出下列各群的中心:
 - (a) 正方形对称群;
 - (b) 等边三角形对称群。
9. 找出正 n 边形对称群的中心。

³注意这个并和集合的并集不一样。

10. 证明：任意交换群 G 中的全体有限阶元素构成 G 的一个子群。

6.8 拉格朗日定理

我们现在来讨论抽象群理论中一个具有重要意义的概念：群 G 的任意子群 S 分解 G 成陪集。

定义 6.5

群或子群的阶指的是它的元素的个数。设 S 是群 G 的一个子群， a 是 G 中一个固定元素，则 S 的所有元素 s 用 a 右 (左) 乘的右 (左) 倍数 $sa(as)$ 所组成的集合 $Sa(aS)$ 称为 G 的子群 S 在 G 中的一个右 (左) 陪集。 S 的不同右陪集的个数称为子群 S 在 G 中的“指数”。



因为 $Se = S$ ，所以 S 是它本身的一个右陪集。此外我们有

引理 6.1

如果 S 是有限的，则 S 的每个右陪集 Sa 中元素的个数同 S 的元素一样多。



这是因为，变换 $s \mapsto sa$ 是双射：右陪集 Sa 的每个元素 $t = sa$ 是 S 的元素 $s = ta^{-1}$ 的像，这个元素是唯一的。（参见定理 6.8。）

引理 6.2

S 的两个右陪集 Sa 和 Sb ，或者相等，或者没有公共元素。



这是因为，假定 Sa 和 Sb 有一个公共元素 $c = s'a = a''b$ (s', s'' 在 S 中)。那么 Sb 包含 Sa 的每个元素 $sa = ss'^{-1}s'a = ss'^{-1}s''b = (ss'^{-1}s'')b$ 。类似的， Sa 包含 Sb 的每个元素，所以 $Sa = Sb$ 。

举例说明这些引理是容易的。例如，如果 G 是正方形对称群，则子群 $S = [I, H]$ 有四个右陪集：

$$\begin{aligned} [I, H]I &= [I, H], \\ [I, H]R &= [R, HR] = [R, D'], \\ [I, H]R' &= [R', HR'] = [R'V], \\ [I, H]R'' &= [R'', HR''] = [R'', D]. \end{aligned}$$

每个陪集有两个元素，并且对称群中的每个元素都落入这四个右陪集中的一个。

再有，如果 G 是整数加法群，则由 5 的倍数 $\pm 5n$ 组成的子群，它的所有右陪集就是模 5 的不同剩余类。最后，设 G 是数字 $1, 2, \dots, 6$ 的所有置换组成的对称群，而 S 是保持数字 1 固定的置换组成的子群。那么由 $1\phi = k$ 可推出，对所有的 $\psi \in S$ ，有 $1(\psi\phi) = (1\psi)\phi = 1\phi = k$ 。因此陪集 $S\phi$ 只包含 $5!$ 个把 1 变为 k 的置换（根据引理 6.1，这是 $S\phi$ 的全部元素）。所以 S 的右陪集是 G 中分别使 $1 \mapsto 1, 1 \mapsto 2, \dots, 1 \mapsto 6$ 的子集合。

从上述这些引理我们得到一个经典的结果，这个结果对有限群的理论来说是基本的和重要的。因为任意右陪集 Sa 总包含 $a = ea$ ，所以任意群 G 的每个元素都包含在某一

个右陪集中。因此 G 可用 S 分解成一些不重叠的子集合，每个子集合的元素恰恰同 S 的元素一样多。如果 G 是有限的⁴，这个结论就是

定理 6.14. 拉格朗日

有限群 G 的阶是它的每个子群的阶的倍数。



G 的每个元素 a 生成一个循环子群，它的阶就是 a 的阶（定理 6.9 的推论）。因此我们有

推论 6.4

有限群 G 的每个元素的阶都是 G 的阶的因子。



推论 6.5

具有素数阶 p 的群是循环群。



这是因为，在有限群中，由任意元素 $a \neq e$ 生成的循环子群 A 的阶 $n > 1$ ，可整除 p ，而这就意味着 $n = p$ 。因此 $G = A$ 是循环群。

更一般地，拉格朗日定理可以用来确定（精确到同构）所有任意低阶的抽象群。例如，四群是定义为由四个可交换元素： e （单位元素）和 $a, b, c = ab$ 组成的群，后面三个元素的阶都是 2。6.9 中我们将证明这个群与矩形对称群同构。我们现在证明

推论 6.6

四阶抽象群只有四阶循环群和四群两种。



换句话说，每个四阶群或者同构于四阶循环群，或者同构于四群。

证明 当四阶群包含一个四阶元素时，这个群是循环群。否则，由推论 6.4 知， G 的元素除 e 外，它们的阶一定都是 2。记它们为 a, b, c 。根据消去律， ab 不可能是 $ae = a$ ， $eb = b$ 或 $aa = e$ ，因此 $ab = c$ 。类似的， $ba = c$ ， $ac = ca = b$ ， $bc = cb = a$ 。而这些等式连同 $a^2 = b^2 = c^2 = e$ ，和对一切 x ，有 $ex = xe = x$ 一起给出四群的乘法表。

拉格朗日定理也可以应用到数论中。

推论 6.7. 费马

如果 a 是整数， p 是素数，那么 $a^p \equiv a \pmod{p}$ 。



证明 模 p 整数（零除外）乘法群有 $p-1$ 个元素。那么根据推论 6.4，这个群的任意元素 a 的阶是 $p-1$ 的因子，所以对任何元素 $a \not\equiv 0 \pmod{p}$ 有 $a^{p-1} \equiv 1 \pmod{p}$ 。如果我们用 a 乘同余式两边，我们就得到所要求的同余式。对于 $a \equiv 0 \pmod{p}$ 的情况，结论显然正确。

第六章 习题

1. 对 $p = 7$ ，和 $a = 2, 3, 6$ 验证费马定理。
2. (a) 列出 26 阶二面体群（6.6 的习题 10）的全部子群。共有多少子群？

⁴推广到无限的情况，可从第 10 章的讨论中立即得到，但这并不重要。

- (b) 推广你的结果。
3. 证明：有限群的任意子群的右陪集的个数等于它的左陪集的个数。（提示：利用对应 $x \mapsto x^{-1}$ 。）
 4. 确定正方形对称群的子群 $[I, D]$ 的陪集。
 5. 设 S 是群 G 的任意子群。又设 SaS 表示由所有乘积 sas' (s, s' 在 S 中) 组成的集合。证明：对任意 $a, b \in G$, 或者 $SaS \cap SbS$ 是空集, 或者 $SaS = SbS$ 。
 6. 对任意子群 S , 设 $x \equiv y \pmod{S}$ 是指 $xy^{-1} \in S$.
 - (a) 证明：这个关系满足自反律、对称律和传递律。并证明： $x \equiv y \pmod{S}$ 当且仅当 x 和 y 在 S 的同一个右陪集中。
 - (b) 证明：由 $x \equiv y \pmod{S}$ 可推出，对一切 a 有 $xa \equiv ya \pmod{S}$ 。
 7. 设 G 是正六边形对称群， S 是保持一个顶点固定的子群。求出 S 的右陪集和左陪集。
 8. 证明： p^m 阶群（这里 p 为素数）一定包含一个 p 阶子群。
 9. (a) 设 G 是 \mathbb{R} 上所有变换 $x \mapsto ax + b$ （其中 $a \neq 0$ 和 b 为实数）构成的群，而 S 是 $a = 1$ 的所有这样的变换构成的子群。描述 S 在 G 中的右陪集和左陪集。
 (b) 又设 T 是 $b = 0$ 的所有这样的变换构成的子群，描述 T 在 G 中的右陪集和左陪集。
 10. (a) 证明：在任意交换环 R 中，所有单位（具有乘法逆元素的那些元素）构成一个群 G 。
 (b) 证明：如果 $R = \mathbb{Z}_n$, 那么 G 是由所有与 n 互素的正整数 $k < n$ 组成。
 (c) 在 $R = \mathbb{Z}_n$ 的情况下， G 的阶记作 ϕ_n , 并称为欧拉函数。证明：当 $n = p$ 为素数时， $\phi(p) = p - 1$ 。计算 $\phi(12), \phi(16), \phi(30)$ 。
 (d) 用拉格朗日定理证明：如果 $(k, n) = 1$, 那么 $k^{\phi(n)} \equiv 1 \pmod{n}$ 。
 11. 证明：如果 S 和 T 分别是群 G 的 s 阶和 t 阶子群，并且 $S \cap T$ 和 $S \cup T$ 的阶分别为 u 和 v , 那么 $st \leq uv$ 。
 12. 证明：6 阶抽象群只有 6 阶循环群和三字母的对称群。
 13. 设 $2^h + 1$ 是素数 p 。
 - (a) 证明：模 p 整数乘法群中，2 的阶是 $2h$ 。
 - (b) 利用费马定理推证： $2h$ 可整除 $p - 1 = 2^h$ 。
 - (c) 导出结论 h 是 2 的幂。

6.9 置换群

置换是有限集到自身的一一变换。例如由 1, 2, 3, 4, 5 五个数字可以组成一个集合。一个置换可以是一个变换 ϕ :

$$1\phi = 2, 2\phi = 3, 3\phi = 4, 4\phi = 5, 5\phi = 1. \quad (6.9.1)$$

另一个置换可以是变换 ϕ' :

$$1\phi' = 2, 2\phi' = 3, 3\phi' = 1, 4\phi' = 5, 5\phi' = 4. \quad (6.9.2)$$

一个置换，像上面定义的置换 ϕ 那样，如果它给出置换符号的一个循环排列，那么这个置换称为循环置换或称为循环。为表示循环置换，有一个含蓄的记号---仅仅把字母写到括号里边，首先写出所包含的任何一个字母，然后写出它变换后的字母，...，最后写出能变换成原来第一个字母的那个字母。例如，(6.9.1) 式表示的置换 ϕ 可以写成下列等价形式中的任何一个：

$$(12345), (23451), (34512), (45123), (51234).$$

定理 6.15

n 个符号的循环置换的阶是 n .



证明 循环置换 $\gamma = (a_1 a_2 \cdots a_n)$ 把 a_i 变成 a_{i+1} . 因此 γ^2 的效果相当于 γ 作用两次，把每个 a_i 变成 a_{i+2} . 一般的， γ^k 把 a_i 变成 a_{i+k} ，这里所有下标都按模 n 化简了。 γ^k 为单位元素 I 当且仅当 $a_{i+k} = a_i$. 即当且仅当 $k \equiv 0 \pmod{n}$. 因为使得 $\gamma^k = I$ 的最小整数 k 是 n 本身，所以 γ 的阶是 n (见 6.6 中的定义)。这时我们说循环 γ 的长度是 n .

循环置换的记号可以推广到任意置换的情形。例如：(6.9.2) 式中表示的置换 ϕ' ，把数字 1, 2 和 3 循环排列，并且把 4 和 5 循环排列。于是 ϕ' 是这两个循环的积

$$(123)(45) = (45)(123).$$

这个乘积可以按两种次序写，是因为由 (1, 2, 3) 置换过的符号在 (4, 5) 作用下保持不变，这表示按两种次序相继使用这两个置换，其结果一样。

定理 6.16

任意置换 ϕ 可写成几个循环的乘积，这些循环分别作用在不相交的符号集上（更简洁地说，任意置换 ϕ 可写成几个不相交的循环之积）。



证明 选择任意一个符号记作 a_1 ，再用 a_2 表示 $a_1\phi$. 用 a_3 表示 $a_2\phi$, ..., 用 a_n 表示 $a_{n-1}\phi$, 直到 $a_n\phi = a_1$ 是前面某一个已经命名了的元素。因为任意 $a_i (i > 1)$ 前面一个元素是 a_{i-1} ，所以 $a_n\phi$ 一定是 a_1 . 于是 ϕ 作用到字母 a_1, a_2, \dots, a_n 上的结果是循环 $(a_1 a_2 \cdots a_n)$. 此外，循环 $(a_1 a_2 \cdots a_n)$ 当它包含任意字母 a_i 时就一定包含前一个字母 a_{i-1} ，因此 ϕ 还要置换这 n 个字母外剩下来的字母。现在对符号的个数用归纳法就可推出定理的结论。特别， m 个字母的恒等置换可表示成 m 个循环之积，每个循环的长度为 1.

反之，显然任意不相交循环之积是一个置换。此外，我们可以证明：

定理 6.17

任意置换 ϕ 的阶等于 ϕ 的不相交循环之长度的最小公倍数。



证明 把置换 ϕ 写成不相交循环 $\gamma_1, \dots, \gamma_r$ 的乘积 $\phi = \gamma_1 \cdots \gamma_r$. 如果 $i \neq j$, 则 γ_i 和 γ_j 是不相交的；因此 $\gamma_i \gamma_j = \gamma_j \gamma_i$, 并且因子 γ_i 可以在 ϕ 和它的幂中重新排列，从而对所有整数 n , 得到 $\phi^n = \gamma_1^n \cdots \gamma_r^n$. 所以 $\phi^n = I$ 当且仅当每个 γ_i^n 是恒等置换。而根据定理 6.15, 由此可推出， $\phi^n = I$ 当且仅当 n 是 $\gamma_1, \dots, \gamma_r$ 的长度的公倍数，由此立即得到定理 6.17 的结论。

根据 6.5 的定理 6.8，每个有限群同构于一个或多个置换群。特别，这对于由几何图形

的对称构成的有限群是正确的，我们现在用两个例子来说明这一点。

考虑矩形对称群（图）。在这个群中，由下列四个置换

$$I = (1)(2)(3)(4), \quad R = (14)(23),$$

$$H = (13)(24), \quad V = (12)(34)$$

来变换它的顶点。这个群被称为四群。根据定理6.8，它同构于置换群

$$\phi_I = (I)(R)(V)(H), \quad \phi_R = (IR)(HV),$$

$$\phi_H = (IH)(RV), \quad \phi_V = (IV)(RH).$$

第七章 几何

第八章 几何

第九章 几何

第十章 几何

第二部分

代数

《代数》的作者是 M. 阿廷。参考：[2]。

第十一章 矩阵

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

11.1 基本运算

设 m 和 n 是正整数，

第十二章 群

第十三章 向量空间

第十四章 线性算子

第十五章 线性算子的应用

第三部分

基础代数

《基础代数》(Basic Algebra) 的作者是 N.Jacobson。参考: [3]。

第十六章 集合论里的概念 整数

第十七章 么半群和群

第十八章 环

第 十九 章 主理想整环上的模

第 二十 章 方程的 Galois 理论

第四部分

微积分

《微积分》(Calculus) 的作者是 M. 斯皮瓦克 (M. Spivak)。参考: [4]。

第二十一章 数的基本性质

本章的标题简单地表达了阅读本书所需要的数学知识。

第五部分

流形上的微积分

《流形上的微积分》的作者是 M.Spivak. 参考: [?].

第二十二章 欧几里得空间上的函数

22.1 范数与内积

欧几里得 (Euclid) n 维空间 (也简称欧氏空间) \mathbb{R}^n 定义为一切实数 x^i 的 n 数组 (x_1, \dots, x_n) (一个“1数组”就是一个数, 而 $\mathbb{R}^1 = \mathbb{R}$ 则是一切实数的集) 的集合. \mathbb{R}^n 的元素通常称为 \mathbb{R}^n 的点, 而 $\mathbb{R}^1, \mathbb{R}^2, \mathbb{R}^3$ 通常分别称为直线、平面和空间. 如 x 表示 \mathbb{R}^n 的一元素, 则 x 是一个 n 数组, 其中第 i 个记作 x^i ; 于是我们可以写成

$$x = (x_1, \dots, x_n).$$

\mathbb{R}^n 中的点也常常称为 \mathbb{R}^n 中的向量, 因为, 按照 $x + y = (x_1 + y_1, \dots, x_n + y_n)$ 以及 $ax = (ax_1, \dots, ax_n)$ 作为运算, \mathbb{R}^n 是一个向量空间 (在实数域上, 维数为 n). 在这向量空间中, 向量 x 的长度的概念, 通常称为 x 的范数 $|x|$, 并定义为 $|x| = \sqrt{(x_1)^2 + \dots + (x_n)^2}$. 如 $n = 1$, 则 $|x|$ 就是 x 的通常的绝对值. 范数和 \mathbb{R}^n 的向量空间结构间的下一关系极为重要.

定理 22.1

如 $x, y \in \mathbb{R}^n$ 且 $a \in \mathbb{R}$, 则

- (1) $|x| \geq 0$, 当且仅当 $x = 0$ 时, $|x| = 0$.
- (2) $\left| \sum_{i=1}^n x_i y_i \right| \leq |x| \cdot |y|$, 当且仅当 x 与 y 线性相关时等式成立.
- (3) $|x + y| \leq |x| + |y|$.
- (4) $|ax| = |a| \cdot |x|$.



证明

- (1) 根据定义, 显然有 $|x| \geq 0$, 而且 $|x| = 0$ 时, 必有各个 $x_i = 0$, 也就是 $x = 0$, 反过来, 如果 $x = 0$, 显然有 $|x| = 0$. 而 $x \neq 0$ 时, 至少存在一个 $x_i \neq 0$, 于是 $|x| \geq |x_i| > 0$.
- (2) 如 x 与 y 线性相关, 等式明显成立. 如不是这样, 则对一切 $\lambda \in \mathbb{R}, \lambda y - x \neq 0$, 因此

$$\begin{aligned} 0 < |\lambda y - x|^2 &= \sum_{i=1}^n (\lambda y_i - x_i)^2 \\ &= \lambda^2 \sum_{i=1}^n (y_i)^2 - 2\lambda \sum_{i=1}^n x_i y_i + \sum_{i=1}^n (x_i)^2. \end{aligned}$$

所以右方是 λ 的没有实根的二次式, 其判别式必须为负. 于是

$$4 \left(\sum_{i=1}^n x_i y_i \right)^2 - 4 \sum_{i=1}^n (x_i)^2 \sum_{i=1}^n (y_i)^2 < 0.$$

(3)

$$\begin{aligned}
|x+y|^2 &= \sum_{i=1}^n (x_i + y_i)^2 \\
&= \sum_{i=1}^n (x_i)^2 + \sum_{i=1}^n (y_i)^2 + 2 \sum_{i=1}^n x_i y_i \\
&\leq |x|^2 + |y|^2 + 2|x| \cdot |y| \\
&= (|x| + |y|)^2.
\end{aligned}$$

$$(4) |ax| = \sqrt{\sum_{i=1}^n (ax_i)^2} = \sqrt{a^2 \sum_{i=1}^n (x_i)^2} = |a| \cdot |x|.$$

在 (2) 中出现的量 $\sum_{i=1}^n x_i y_i$ 称为 x 与 y 的内积并记作 $\langle x, y \rangle$ 。内积的一些最重要的性质如下。

定理 22.2

如 x, x_1, x_2 与 y, y_1, y_2 是 \mathbb{R}^n 中的向量, 且 $a \in \mathbb{R}$, 则

(1) $\langle x, y \rangle = \langle y, x \rangle$ (对称性).

(2) (双线性)

$$\langle ax, y \rangle = \langle x, ay \rangle = a \langle x, y \rangle$$

$$\langle x_1 + x_2, y \rangle = \langle x_1, y \rangle + \langle x_2, y \rangle$$

$$\langle x, y_1 + y_2 \rangle = \langle x, y_1 \rangle + \langle x, y_2 \rangle$$

(3) $\langle x, x \rangle \geq 0$, 且 $\langle x, x \rangle = 0$ 当且仅当 $x = 0$ (正定性)。

(4) $|x| = \sqrt{\langle x, x \rangle}$.

(5) 极化等式

$$\langle x, x \rangle = \frac{|x+y|^2 - |x-y|^2}{4}.$$



证明

$$(1) \langle x, y \rangle = \sum_{i=1}^n x_i y_i = \sum_{i=1}^n y_i x_i = \langle y, x \rangle.$$

(2) 由 (1) 只须证明

$$\langle ax, y \rangle = a \langle x, y \rangle,$$

$$\langle x_1 + x_2, y \rangle = \langle x_1, y \rangle + \langle x_2, y \rangle.$$

这些可由下列等式得出:

$$\langle ax, y \rangle = \sum_{i=1}^n (ax_i) y_i = a \sum_{i=1}^n x_i y_i = a \langle x, y \rangle,$$

$$\langle x_1 + x_2, y \rangle = \sum_{i=1}^n (x_1^i + x_2^i) y_i = \sum_{i=1}^n x_1^i y_i + \sum_{i=1}^n x_2^i y_i$$

$$= \langle x_1, y \rangle + \langle x_2, y \rangle.$$

(3) 和 (4) 留给读者.

(5)

$$\begin{aligned}
& \frac{|x+y|^2 - |x-y|^2}{4} \\
&= \frac{1}{4}[\langle x+y, x+y \rangle - \langle x-y, x-y \rangle] \\
&= \frac{1}{4}[\langle x, x \rangle + 2\langle x, y \rangle + \langle y, y \rangle - \\
&\quad (\langle x, x \rangle - 2\langle x, y \rangle + \langle y, y \rangle)] = \langle x, y \rangle.
\end{aligned}$$

我们对记号作一些重要注解以结束本节。向量 $(0, \dots, 0)$ 通常简记为 0 。 \mathbb{R}^m 的通常基底是 e_1, \dots, e_n , 其中 $e_i = (0, \dots, 1, \dots, 0)$, 在第 i 个位置上是 1. 如 $T: \mathbb{R}^n \rightarrow \mathbb{R}^m$ 是一个线性变换, T 关于 \mathbb{R}^n 与 \mathbb{R}^m 的通常基底的矩阵是 $m \times n$ 矩阵 $A = (a_{ij})$, 其中 $T(e_i) = \sum_{j=1}^n a_{ji}e_j$ — $T(e_i)$ 的系数出现在矩阵的第 i 列。如 $S: \mathbb{R}^m \rightarrow \mathbb{R}^p$ 有 $p \times m$ 矩阵 B , 则 $S \circ T$ 有 $p \times n$ 矩阵 BA [这里 $S \circ T(x) = S(T(x))$]; 绝大多数线性代数书籍把 $S \circ T$ 简记为 ST]. 为要找出 $T(x)$, 我们来计算 $m \times 1$ 矩阵.

$$\begin{pmatrix} y^1 \\ \vdots \\ y^m \end{pmatrix} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x^1 \\ \vdots \\ x^n \end{pmatrix};$$

则 $T(x) = (y^1, \dots, y^m)$. 下一习惯记法大大简化许多公式: 如 $x \in \mathbb{R}^n$ 与 $y \in \mathbb{R}^m$, 则 (x, y) 表示

$$(x^1, \dots, x^n, y^1, \dots, y^m) \in \mathbb{R}^{n+m}.$$

第二十二章 习题

1. 求证 $|x| \leq \sum_{i=1}^n |x^i|$.

注意到不等式两边都大于等于 0, 两边平方, 展开, 就会发现等式成立。

$$\left(\sum_{i=1}^n |x^i|\right)^2 = \sum_{i=1}^n |x^i|^2 + 2 \sum_{i \neq j} |x^i||x^j| = |x|^2 + 2 \sum_{i \neq j} |x^i||x^j|$$

2. 定理 22.1(3) 中的等式何时成立? 提示: 重新检查证明; 答案不是“当 x 与 y 线性相关”。

在证明过程中, 等式成立首先要求 x 与 y 线性相关, 然后要求 $\sum_{i=1}^n x^i y^i \geq 0$, 把线性相关代入, 可以得出等号成立当且仅当: $ax + by = 0$ 且 $ab \leq 0$, 也就是 x 和 y 同方向。

3. 求证 $|x - y| \leq |x| + |y|$, 何时等式成立?

和上一道题目类似, 这一次要求 x 与 y 共线, 但是需要相反方向才能取等号。

4. 求证 $||x| - |y|| \leq |x - y|$.

$$|x| = |x - y + y| \leq |x - y| + |y|$$

$$|x| - |y| \leq |x - y|$$

由对称性可以得出另一个不等式: $|y| - |x| \leq |x - y|$, 结合起来就是所要证的不等式。

5. 量 $|y - x|$ 称为 x 与 y 间的距离, 求证并在几何上解释 “三角形不等式”:

$$|z - x| \leq |z - y| + |y - x|.$$

只要注意到, 对于三个点 x, y 和 z 构成的三角形来说, 不等式中的恰好就是三条边长, 几何上三角形两边之和大于第三边. 至于代数证明很简单.

$$|z - x| = |z - y + y - x| \leq |z - y| + |y - x|.$$

6. 设 f 与 g 在 $[a, b]$ 上平方可积.

(a) 求证: $\left| \int_a^b fg \right| \leq \left(\int_a^b f^2 \right)^{1/2} \left(\int_a^b g^2 \right)^{1/2}$, 提示: 分别考虑下面二情况: 对某一 $\lambda \in \mathbb{R}$, $0 = \int_a^b (f - \lambda g)^2$; 对一切 $\lambda \in \mathbb{R}$, $0 < \int_a^b (f - \lambda g)^2$.

(b) 如等式成立, $f = \lambda g$ 必定对某个 $\lambda \in \mathbb{R}$ 成立吗? 如 f 与 g 连续又怎样?

(c) 证明定理 22.2 是 (a) 的一个特殊情形.

(a) f 与 g 平方可积, 说明 $(f - \lambda g)$ 也是平方可积的, 假设存在一 $\lambda \in \mathbb{R}$ 使得 $0 = \int_a^b (f - \lambda g)^2$, 那么说明除了一个零测集 Λ 之外, 有 $f - \lambda g = 0$. 也就是几乎处处有 $f = \lambda g$, 从而几乎处处 $fg = \lambda g^2$, 由此不等式左边 $\left| \int_a^b fg \right| = \left| \int_a^b \lambda g^2 \right| = |\lambda| \int_a^b g^2$, 不等式右边: $\left(\int_a^b f^2 \right)^{1/2} \left(\int_a^b g^2 \right)^{1/2} = |\lambda| \int_a^b g^2$, 不等式成立等号. 如果对于所有 $\lambda \in \mathbb{R}$,

$$\begin{aligned} 0 &< \int_a^b (f - \lambda g)^2 = \int_a^b (f^2 - 2\lambda fg + \lambda^2 g^2) \\ &= \int_a^b f^2 - 2\lambda \int_a^b fg + \lambda^2 \int_a^b g^2. \end{aligned}$$

如果 $\int_a^b g^2 = 0$, 那么讨论和前面类似, 只是此时是 g 几乎处处等于 0, 从而 fg 几乎处处等于 0, 于是 $\int_a^b fg = 0$, 所以只需考虑 $\int_a^b g^2 > 0$ 的情形, 此时二次型的系数大于零, 只有判别式小于 0

$$\Delta = 4 \left(\int_a^b fg \right)^2 - 4 \int_a^b f^2 \int_a^b g^2 < 0,$$

获证.

(b) 等式成立, 说明存在 $\lambda \in \mathbb{R}$, 在除了某个零测集之外有 $f = \lambda g$, 或者 f 和 g 至少有一个几乎处处等于 0, 如果 f 和 g 连续, 那么在 $g \neq 0$ 的情形下, 必然存在一 $\lambda \in \mathbb{R}$ 使得 $f = \lambda g$. 因为对于非负连续函数, 如果存在某点不等于 0, 那么由于连续函数的保号性, 必然在区间上的积分大于 0.

(c) 考虑如下定义在 $[0, n]$ 区间上的阶梯函数 $f(x)$ 和 $g(x)$:

$$f(x) = \begin{cases} x_1, & 0 \leq x \leq 1, \\ x_2, & 1 < x \leq 2, \\ \dots, & \\ x_n, & (n-1) < x \leq n. \end{cases}$$

$g(x)$ 类似, 只是在相同区间上, x_i 换成 y_i , 那么显然 $f(x)$ 和 $g(x)$ 都是平方可积的,

并且

$$\begin{aligned}\int_0^n fg &= \sum_{i=1}^n x_i y_i, \\ \int_0^n f^2 &= \sum_{i=1}^n (x_i)^2 \\ \int_0^n g^2 &= \sum_{i=1}^n (y_i)^2.\end{aligned}$$

7. 一线性变换 $T: \mathbb{R}^n \rightarrow \mathbb{R}^n$, 如果 $|T(x)| = |x|$, 则称为保范数的. 如果 $\langle Tx, Ty \rangle = \langle x, y \rangle$, 则称为保内积的.

(a). 求证 T 是保范数的当且仅当 T 是保内积的.

(b). 求证这种线性变换 T 是 1-1 的, 而且 T^{-1} 也是同一种变换.

使用定理 22.2 中的 (5) 极化等式和线性变换的性质即可. 从保范数和保内积的定义就可以得到.

$$\begin{aligned}|T(x)| = |x| &\Rightarrow \langle Tx, Ty \rangle = \frac{1}{4} [|Tx + Ty|^2 - |Tx - Ty|^2] \\ &= \frac{1}{4} [|T(x+y)|^2 - |T(x-y)|^2] \\ &= \frac{1}{4} [|x+y|^2 - |x-y|^2] = \langle x, y \rangle\end{aligned}$$

反过来, 保内积的话, 只需要令 $x = y$, 立即可得 $|Tx| = |x|$.

至于要证明 T 是一一的, 也就是要证明它既是单射又是满射.

(1) T 是单射, 也就是如果 $T(x_1) = T(x_2)$, 则 $x_1 = x_2$.

$$0 = |T(x_1) - T(x_2)| = |T(x_1 - x_2)| = |x_1 - x_2|.$$

(2) T 是满射. 证明 T 的矩阵 A 可逆即可, 也就是证明 A 的任意两列正交. 这一点只需要注意到

$$\langle T(e_i), T(e_j) \rangle = \langle e_i, e_j \rangle = \delta_{ij},$$

而 $T(e_i)$ 的系数就是 A 的第 i 列, 从而 A 是正交矩阵, 可逆. 至于说 T^{-1} 也是保范的, 可以从下列等式得到

$$|T(T^{-1}(x))| = |T^{-1}(x)| = |x|.$$

8. 如 $x, y \in \mathbb{R}^n$ 不为零, x 与 y 间的夹角记作 $\angle(x, y)$ 定义为 $\arccos(\langle x, y \rangle / |x| \cdot |y|)$. 由定理 22.1 的 (2), 这是有意义的. 线性变换 T 称为是保角的, 如 T 是 1-1 的, 且对 $x, y \neq 0$, 我们有 $\angle(Tx, Ty) = \angle(x, y)$.

(a) 求证: 如 T 是保范数的, 则 T 是保角的.

(b) 如 \mathbb{R}^n 有一基底 x_1, \dots, x_n , 又有数 $\lambda_1, \dots, \lambda_n$ 使得 $Tx_i = \lambda_i x_i$, 求证 T 是保角的, 当且仅当所有 $|\lambda_i|$ 皆相等.

(c) 所有保角的 $T: \mathbb{R}^n \rightarrow \mathbb{R}^n$ 是些什么?

(a) 首先从上一道题目可知, 保范数意味着 T 是一一的, 且保内积, 于是 $\langle Tx, Ty \rangle =$

$\langle x, y \rangle$. 于是 $x \neq y$ 时

$$\angle(Tx, Ty) = \arccos\left(\frac{\langle Tx, Ty \rangle}{|Tx||Ty|}\right) = \arccos\frac{\langle x, y \rangle}{|x||y|} = \angle(x, y).$$

(b) 我怎么感觉这道题目的结论有点问题, 应该是所有 λ_i 都相等才是合理的。下面的证明方法来自微信网友枫树 (gusongduping)

充分性: 若 $\lambda_1 = \lambda_2 = \cdots = \lambda_n \neq 0$, 则 $\forall x \in \mathbb{R}^n$ 有 $Tx = \lambda_1 x$, 于是 $\forall x, y \in \mathbb{R}^n$ 有

$$\angle Tx, Ty = \arccos\frac{\langle Tx, Ty \rangle}{|Tx||Ty|} = \arccos\frac{\lambda_1^2 \langle x, y \rangle}{|\lambda_1|^2 |x||y|} = \angle(x, y).$$

因而 T 是保角的。

必要性: 若 T 是保角的, 从而是一一的, 于是 $\lambda_i \neq 0$, 对于给定的 λ_k 与 λ_s , 我们考虑 (x_k, x_s) ,

若 $(x_k, x_s) = 0$, 也就是两个向量正交, 则对于 $\alpha = x_k + x_s$, $\beta = -(x_s, x_s)x_k + (x_k, x_k)x_s$, 有 $(\alpha, \beta) = 0$, 于是

$$(T\alpha, T\beta) = (\alpha, \beta) = 0 \Leftrightarrow \lambda_k^2 = \lambda_s^2.$$

又由于 $\angle(Tx_k, Tx_s) = \angle(x_k, x_s)$, 可得 $\lambda_k \lambda_s > 0$, 从而 $\lambda_k = \lambda_s$.

若 $(x_k, x_s) \neq 0$, 则对于 $\alpha = x_k$, $\beta = -(x_k, x_s)x_k + (x_k, x_k)x_s$, 有 $(\alpha, \beta) = 0$, 于是

$$(T\alpha, T\beta) = 0 \Leftrightarrow \lambda_k = \lambda_s.$$

获证。

上面的证明过程, 主要是 α 和 β 的构造, 我原来有一些思路, 不过傻了, 使用了一般情形进行讨论, 没有想到构造正交向量。上面 x_k 和 x_s 正交的时候, 要想得到 $\lambda_k = \lambda_s$, 似乎需要依赖直观, 也就是 λ_k 和 λ_s 同号这一步有些麻烦, 好像不成立, 只能推到 $\lambda_k^2 = \lambda_s^2$. 可以试试相似三角形的概念。正交的时候, 最多得到绝对值相等。

(c) 由 (b), 首先必然存在一组基底 x_1, \cdots, x_n 使得 $Tx_i = \lambda x_i$, 从而 $\forall x \in \mathbb{R}^n$ 有 $Tx = \lambda x$, 那么对于标准基底来说, 由于 x_1, \cdots, x_n 和标准基底之间存在一一变换, 也就是存在可逆矩阵 A 使得 $x_i = Ae_i$, 于是, 对于标准基底, 就有 $Tx = \lambda Ax$, 从几何上, 应该是平移, 旋转, 伸缩以及它们的组合的结果。这个做法似乎也不严格, 没有证明除了这个变换, 就不存在其他的保角变换。

9. 如果 $0 \leq \theta < \pi$, 设 $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ 有矩阵

$$\begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix},$$

求证 T 是保角的, 且若 $x \neq 0$, 则 $\angle(x, Tx) = \theta$.

比较笨，直接计算。点 $(x_1, x_2) \in \mathbb{R}^2$, 有

$$\begin{aligned} |T(x_1, x_2)|^2 &= \left| \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \right|^2 \\ &= \left| \begin{pmatrix} x_1 \cos \theta + x_2 \sin \theta \\ -x_1 \sin \theta + x_2 \cos \theta \end{pmatrix} \right|^2 \\ &= (x_1 \cos \theta + x_2 \sin \theta)^2 + (-x_1 \sin \theta + x_2 \cos \theta)^2 \\ &= x_1^2 + x_2^2 = |(x_1, x_2)|^2. \end{aligned}$$

这里省略了展开，合并的过程，展开后刚好抵消一部分，留下部分使用 $\cos^2 \theta + \sin^2 \theta = 1$ 即可。上述等式说明这是一个保范数的线性变换，从而是保角的。至于后面部分，也是直接计算 $\langle x, Tx \rangle / |x| \cdot |Tx|$ ，并注意到 $|Tx| = |x|$ ，于是就有

$$\begin{aligned} \frac{\langle x, Tx \rangle}{|x| \cdot |Tx|} &= \frac{x_1(x_1 \cos \theta + x_2 \sin \theta) + x_2(-x_1 \sin \theta + x_2 \cos \theta)}{x_1^2 + x_2^2} \\ &= \frac{(x_1^2 + x_2^2) \cos \theta}{x_1^2 + x_2^2} = \cos \theta, \end{aligned}$$

因而 $\angle(x, Tx) = \theta$.

10. 如 $T: \mathbb{R}^m \rightarrow \mathbb{R}^n$ 是一线性变换，证明有这样的数 M 使得对于 $h \in \mathbb{R}^m$ 有 $|T(h)| \leq M|h|$. 提示：用 $|h|$ 以及 T 的矩阵中的元估计 $|T(h)|$.

设 T 的矩阵为 $A = (a_{ij})$ 是一 $n \times m$ 矩阵，令 $a = \max |a_{ij}|$ ，则

$$\begin{aligned} |T(h)|^2 &= \langle Th, Th \rangle = \sum_{i=1}^n \left(\sum_{j=1}^m a_{ij} h_j \right)^2 \\ &\leq \sum_{i=1}^n \left(\sum_{j=1}^m a_{ij}^2 \right) \left(\sum_{j=1}^m h_j^2 \right) \\ &\leq \sum_{i=1}^n m a^2 \sum_{j=1}^m h_j^2 = m n a^2 \sum_{j=1}^m h_j^2 = m n a^2 |h|^2 \end{aligned}$$

于是，只要取 $M = \sqrt{mna}$ ，这里 $a = \max |a_{ij}|$ 就有 $|Th| \leq M|h|$.

11. 如果 $x, y \in \mathbb{R}^n, z, w \in \mathbb{R}^m$ ，证明： $\langle (x, z), (y, w) \rangle = \langle x, y \rangle + \langle z, w \rangle$ 以及 $|(x, z)| = \sqrt{|x|^2 + |z|^2}$. 注意 (x, z) 与 (y, w) 表示 \mathbb{R}^{n+m} 中的点。

直接展开

$$\begin{aligned} \langle (x, z), (y, w) \rangle &= (x_1 y_1 + \cdots + x_n y_n) + (z_1 w_1 + \cdots + z_m w_m) \\ &= \langle x, y \rangle + \langle z, w \rangle, \\ |(x, z)|^2 &= \langle (x, z), (x, z) \rangle = \langle x, x \rangle + \langle z, z \rangle \\ &= |x|^2 + |z|^2. \end{aligned}$$

12. 设 $(\mathbb{R}^n)^*$ 表示向量空间 \mathbb{R}^n 的对偶空间，如 $x \in \mathbb{R}^n$ ，用 $\varphi_x(y) = \langle x, y \rangle$ 定义 $\varphi_x \in (\mathbb{R}^n)^*$. 用 $T(x) = \varphi_x$ 定义 $T: \mathbb{R}^n \rightarrow (\mathbb{R}^n)^*$. 证明 T 是一个 1-1 线性变换，并作出结论：每一个 $\varphi \in (\mathbb{R}^n)^*$ 是关于唯一的一个 $x \in \mathbb{R}^n$ 的 φ_x .

(1) T 是线性变换, 这一点因为内积是双线性函数。 $\forall z \in \mathbb{R}^n$,

$$\begin{aligned} T(\alpha x + \beta y)(z) &= \varphi_{\alpha x + \beta y}(z) = \langle \alpha x + \beta y, z \rangle \\ &= \alpha \langle x, z \rangle + \beta \langle y, z \rangle = \alpha \varphi_x(z) + \beta \varphi_y(z) \\ &= \alpha T x(z) + \beta T y(z). \end{aligned}$$

(2) T 是单射. 也就是需要从 $Tx_1 = Tx_2$ 推出 $x_1 = x_2$. 从 $Tx_1 = Tx_2$ 可知, 对于任意的 $y \in \mathbb{R}^n$ 有 $\langle x_1, y \rangle = \langle x_2, y \rangle$, 分别令 $y = x_1$ 和 $y = x_2$, 可以得到

$$\langle x_1, x_1 \rangle = \langle x_2, x_1 \rangle = \langle x_1, x_2 \rangle = \langle x_2, x_2 \rangle,$$

由此可得 $x_1 = x_2$.

(3) T 是满射. 也就是对于任一元素 $\varphi \in (\mathbb{R}^n)^*$, 我们需要找到一个 x 使得 $Tx = \varphi$. 那么如何构造这个 φ 呢? 首先回忆一下什么是线性空间的对偶空间, 所谓对偶空间, 是所有 \mathbb{R}^n 上的线性泛函构成的线性空间, 所谓线性泛函, 实际上就是 $L: \mathbb{R}^n \rightarrow \mathbb{R}$ 的线性变换. 既然是线性空间, 我们考虑 \mathbb{R}^n 的标准基底 $\{e_1, \dots, e_n\}$, 在 φ 作用下的值分别记为 α_i , 也就是 $\varphi(e_i) = \alpha_i$. 于是对于任一 $x \in \mathbb{R}^n$, 有 $x = \sum_{i=1}^n x_i e_i$, 从而

$$\varphi(x) = \varphi\left(\sum_{i=1}^n x_i e_i\right) = \sum_{i=1}^n x_i \varphi(e_i) = \sum_{i=1}^n x_i \alpha_i,$$

这一点提示我们, 我们如果记 $\alpha = (\alpha_1, \dots, \alpha_n)$, 那么 $\varphi(x) = \langle x, \alpha \rangle$. 也就是 $T\alpha = \varphi$.

13. 如 $x, y \in \mathbb{R}^n$, 则若 $\langle x, y \rangle = 0$, 就称 x 与 y 垂直 (或正交). 如 x 与 y 垂直, 求证: $|x + y|^2 = |x|^2 + |y|^2$.

直接展开并利用对称性以及正交的定义即可。

$$|x + y|^2 = \langle x + y, x + y \rangle = \langle x, x \rangle + 2\langle x, y \rangle + \langle y, y \rangle = |x|^2 + |y|^2.$$

22.2 欧几里得空间的子集

闭区间 $[a, b]$ 在 \mathbb{R}^2 中有一自然的类比. 这就是闭矩形 $[a, b] \times [c, d]$, 定义为一切数对 (x, y) 的全体, 其中 $x \in [a, b], y \in [c, d]$. 更一般的, 如 $A \subset \mathbb{R}^m, B \subset \mathbb{R}^n$, 则 $A \times B \subset \mathbb{R}^{m+n}$ 定义为一切 $(x, y) \in \mathbb{R}^{m+n}$ 的集, 其中 $x \in A, y \in B$. 特别, $\mathbb{R}^{m+n} = \mathbb{R}^m \times \mathbb{R}^n$. 如 $A \subset \mathbb{R}^m, B \subset \mathbb{R}^n$, 和 $C \subset \mathbb{R}^p$, 则 $(A \times B) \times C = A \times (B \times C)$, 二者皆简记为 $A \times B \times C$; 这一记法也推广到任意个数的集的乘积. 集 $[a_1, b_1] \times \dots \times [a_n, b_n] \subset \mathbb{R}^n$ 称作 \mathbb{R}^n 中的闭矩形, 而集 $(a_1, b_1) \times \dots \times (a_n, b_n) \subset \mathbb{R}^n$ 称作开矩形. 更一般地, 一个集 $U \subset \mathbb{R}^n$ 称作开集, 如果对每一个 $x \in U$, 有一个开矩形 A 使得 $x \in A \subset U$.

\mathbb{R}^n 的一个子集 C 称为闭集如 $\mathbb{R}^n - C$ 是开集. 例如, 如 C 只含有限多个点, 则 C 是闭. 读者应该补充证明: \mathbb{R}^n 中的闭矩形确为一闭集.

如 $A \subset \mathbb{R}^n$ 且 $x \in \mathbb{R}^n$, 则下列三种可能性之一必成立。

1. 存在一个开矩形 B 使得 $x \in B \subset A$.
2. 存在一个开矩形 B 使得 $x \in B \subset \mathbb{R}^n - A$.
3. 如 B 是任一个开矩形使得 $x \in B$ 者, 则 B 同时含有 A 与 $\mathbb{R}^n - A$ 的点.

满足 (1) 的那些点构成 A 的内域, 满足 (2) 的那些点构成 A 的外域, 满足 (3) 的那些

点构成 A 的边界。习题 1-16 到 1-18 表明这些术语有时可能有意想不到的意义。

不难看出,任何集 A 的内域是开的;对 A 的外域,它实际上是 $\mathbb{R}^n - A$ 的内域,所以也是如此。于是(习题 1-14)它们的并集是开的,而所剩下的,即其边界,必定是闭得。

我们把一组开集称为 A 的一个开覆盖(或简称覆盖 A)¹ \mathcal{O} . 如果任一点 $x \in A$ 是在 \mathcal{O} 的某开集中。例如,如 \mathcal{O} 是一切开区间 $(a, a+1)$ 的集合,其中 $a \in \mathbb{R}$, 则 \mathcal{O} 是 \mathbb{R} 的一(开)覆盖。很明显, \mathcal{O} 的有限个开集不能覆盖 \mathbb{R} , 也不能覆盖 \mathbb{R} 的任一无界集。类似情况对有界集也可能发生。设对一切正整数 $n > 1$, \mathcal{O} 是一切开区间 $(1/n, 1 - 1/n)$ 的集合, 则 \mathcal{O} 是 $(0, 1)$ 的一开覆盖, 但 \mathcal{O} 中的有限个集仍不能覆盖 $(0, 1)$ 。虽然这一现象可能不会出现特别的坏处, 但这种状况不会发生的集至为重要, 它们有一个特殊的名称: 一集 A 称为紧的, 如它的任何开覆盖 \mathcal{O} 包含着一个有限个开集的组仍能覆盖 A 。

只有有限个点的集显然是紧的, 包含 0 以及数 $1/n$ (对一切整数 n) 的无限集 A 也是紧的(理由: 如 \mathcal{O} 是一覆盖: 则对 \mathcal{O} 中某一开集 U 有 $0 \in U$; A 中只有有限个别的点不在 U 中, 每个这样的点至多只要再加上一个开集)。

下列几个结果使对紧集的认识大大简化了, 其中只有第一个结果有一定的深度(也就是, 用到了有关实数的一些事实)。

定理 22.3. 海涅-波雷耳 (Heine-Borel)

闭区间 $[a, b]$ 是紧的。



证明 若 \mathcal{O} 是 $[a, b]$ 的一个开覆盖, 设 $A = \{x : a \leq x \leq b \text{ 且 } [a, x] \text{ 能被 } \mathcal{O} \text{ 中某有限个开集所覆盖}\}$. 注意 $a \in A$, 且 A 显然有上界(以 b 为上界)。我们希望证明 $b \in A$ 。这只要对 $\alpha = A$ 的上确界 ($\alpha = \sup A$) 证明两件事: (1) $\alpha \in A$, (2) $b = \alpha$ 就行了。

因 \mathcal{O} 是一覆盖, 故对某一 U 有 $\alpha \in U$. 那么在某区间中 α 左边的一切点也在 U 中。因为 α 是 A 的上确界, 故在这区间中有一 $x \in A$. 于是 $[a, x]$ 能被 \mathcal{O} 中某有限个开集所覆盖, 而 $[x, \alpha]$ 被一个集 U 所覆盖。所以 $[a, \alpha]$ 能被 \mathcal{O} 中有限个开集所覆盖, 即 $\alpha \in A$ 。这就证明了 (1)。

要证 (2) 为真, 假设不然: $\alpha < b$. 因此在 α 与 b 之间有一点 x' 使 $[\alpha, x'] \subset U$. 因 $\alpha \in A$, 区间 $[a, \alpha]$ 能被 \mathcal{O} 中有限个开集所覆盖, 而 $[\alpha, x']$ 已被 U 覆盖。所以 $x' \in A$, 这和 α 是 A 的上确界相矛盾。

若 $B \subset \mathbb{R}^m$ 是紧的且 $x \in \mathbb{R}^n$, 易见 $\{x\} \times B \subset \mathbb{R}^{n+m}$ 是紧的。但是, 可以作出一个强得多的论断。

定理 22.4

若 B 是紧的, \mathcal{O} 是 $\{x\} \times B$ 的一开覆盖, 则有包含 x 的一开集 $U \subset \mathbb{R}^n$ 使得 $U \times B$ 能被 \mathcal{O} 中有限个集所覆盖。



证明 因为 $\{x\} \times B$ 是紧的, 我们可以一开始就认为 \mathcal{O} 是有限的, 我们只要找出开集 U 使 $U \times B$ 被 \mathcal{O} 所覆盖。

¹原文意思是若一个集族 \mathcal{O} 是 A 的覆盖, 就说 \mathcal{O} 覆盖 A . 而不是说开覆盖可以简称为覆盖, 而应说开集族 \mathcal{O} 覆盖 A

对每一个 $y \in B$, 点 (x, y) 在 \mathcal{O} 的某开集 W 中. 因 W 是开的, 对某一开矩形 $U_y \times V_y$ 我们有 $(x, y) \in U_y \times V_y \subset W$. 这些集 V_y 覆盖了紧集 B , 所以有限个 V_{y_1}, \dots, V_{y_k} 也覆盖 B . 令 $U = U_{y_1} \cap \dots \cap U_{y_k}$. 于是, 若 $(x', y') \in U \times B$, 对某一 i 我们有 $y' \in V_{y_i}$, 当然 $x' \in U_{y_i}$. 所以 $(x', y') \in U_{y_i} \times V_{y_i}$, 它包含在 \mathcal{O} 的某个 W 中.

推论 22.1

若 $A \subset \mathbb{R}^n$ 与 $B \subset \mathbb{R}^m$ 是紧的, 则 $A \times B \subset \mathbb{R}^{n+m}$ 也是紧的.



证明 若 \mathcal{O} 是 $A \times B$ 的一开覆盖, 则对每一个 $x \in A$, \mathcal{O} 覆盖了 $\{x\} \times B$. 由定理 22.4, 有一个包含 x 的开集 U_x , 使得 $U_x \times B$ 能被 \mathcal{O} 中有限个集覆盖. 因为 A 是紧的, U_x 中的有限个 U_{x_1}, \dots, U_{x_m} 覆盖 A . 因为 \mathcal{O} 中有限个集覆盖每一个 $U_{x_i} \times B$, 所以 \mathcal{O} 中有限个集也就整个覆盖了 $A \times B$.

推论 22.2

若每一个 A_i 是紧的, 则 $A_1 \times \dots \times A_k$ 也是紧的. 特别, \mathbb{R}^k 中的闭矩形是紧的.

**推论 22.3**

\mathbb{R}^n 中的有界闭集是紧的.



(逆定理也真)

证明 若 $A \subset \mathbb{R}^n$ 是有界闭的, 则对某一个闭矩形 $B, A \subset B$, 若 \mathcal{O} 是 A 的一个开覆盖, 则 \mathcal{O} 是 \mathcal{O} 与 $\mathbb{R}^n - A$ 一起是 B 的一个开覆盖. 所以 \mathcal{O} 中有限个集 U_1, \dots, U_n , 可能再加上 $\mathbb{R}^n - A$, 覆盖了 B , 因此, U_1, \dots, U_n 覆盖了 A .

第二十二章 习题

1. 求证任何一个 (即使是无穷多个) 开集的并集是开的. 求证两个 (从而是有有限个) 开集的交集是开的, 给出对于无穷多个开集的一个反例.

设 $U = \bigcup_{i \in I} U_i$, 这里 U_i 为开集, I 是指标集, 需要证明 U 是开集. 对于任意的 $a \in U$, 存在 $i \in I$, 使得 $a \in U_i$, 由于 U_i 是开集, 从而存在开矩形 B 使得 $a \in B \subset U_i \subset U$, 于是 U 为开集.

对于交集, 设 $U = U_1 \cap U_2$, 那么对于 $x \in U$, 于是 $x \in U_i, i = 1, 2$, 存在开矩形 B_i , 使得 $x \in B_i$, 我们记开矩形 $B_i = (a_i^{(1)}, b_i^{(1)}) \times \dots \times (a_i^{(n)}, b_i^{(n)})$, 那么只需要取

$$a^{(j)} = \max(a_1^{(j)}, a_2^{(j)}), b^{(j)} = \min(b_1^{(j)}, b_2^{(j)}), j = 1, \dots, n,$$

即可, 这样的 $B = (a^{(1)}, b^{(1)}) \times \dots \times (a^{(n)}, b^{(n)})$ 包含 x , 并且是 $B_1 \cap B_2$ 的子集. 从而是 $U_1 \cap U_2$ 的子集, 也就是 U 的子集.

至于反例, 考虑集合 $U_i = (-\frac{1}{i}, 1 + \frac{1}{i})$, 这里 $i = 2, 3, \dots$, 显然每一个都是开集, 但是它们的交集等于 $[0, 1]$ 是闭集.

2. 求证 $\{x \in \mathbb{R}^n : |x - a| < r\}$ 是开的 (参见习题 5.).

书中是使用开矩形来定义开集的, 所以需要找到开矩形属于这个集合 U . 对于任意一点 $y \in U$, 记 $s = \min(|y - a|, r - |y - a|)$, 于是考虑以 y 为中心, 边长是 $s/\sqrt{2}$ 的

开矩形 B , 那么对于任意一点 $z \in B$, 有 $|z - y| < s$, 于是

$$|z - a| < |z - y| + |y - a| < s + |y - a| < r - |y - a| + |y - a| = r,$$

说明 $z \in U$, 也就是 $B \subset U$, 因而 U 是开集。

有了这个结论, 后面的证明中, 有时会这样使用开集: 如果 U 是开集, $\forall a \in U$, 那么存在 $r > 0$, 使得 $U(a, r) = \{x \in \mathbb{R}^n : |x - a| < r\} \subset U$.

3. 求下列集的内域, 外域和边界:

$$\{x \in \mathbb{R}^n : |x| \leq 1\}$$

$$\{x \in \mathbb{R}^n : |x| = 1\}$$

$$\{x \in \mathbb{R}^n : \text{每一 } x_i \text{ 是有理数}\}.$$

上述三个集合分别记作 A, B, C ,

(1) A 是一个特别常见的集合, 它的内域是集合

$$\{x \in \mathbb{R}^n : |x| < 1\},$$

外域是

$$\{x \in \mathbb{R}^n : |x| > 1\},$$

边界是

$$\{x \in \mathbb{R}^n : |x| = 1\},$$

(2) B 是一个闭集, 其内域是空集 \emptyset , 外域为

$$\{x \in \mathbb{R}^n : |x| \neq 1\},$$

边界就是它自身.

$$\{x \in \mathbb{R}^n : |x| = 1\}.$$

(3) 这个集合比较特殊, 需要使用有理数的稠密性。它的内域和外域都是空集, 边界是 \mathbb{R}^n , 全集。

4. 求作一个集 $A \subset [0, 1] \times [0, 1]$, 使得 A 在每一条水平线和铅直线上至多只含一点, 但 A 的边界 $= [0, 1] \times [0, 1]$ 。提示: 只要能保证 A 在正方形 $[0, 1] \times [0, 1]$ 的每四分之一中含有点, 又在每十六分之一中含有点, 如此等等, 这就够了。

按照提示操作, 需要使用不可数集和可数集的概念, 这样来选择: 首先把 $[0, 1] \times [0, 1]$ 四等分, 也就是把 $[0, 1]$ 二等分, 分别在四个区域正方形区域中各自选择一个点, 记为 $a_1^1, a_1^2, a_1^3, a_1^4$, 要求, 任意两个点不在同一水平线或者铅直线上, 然后把 $[0, 1] \times [0, 1]$ ($16=4^2$) 等分, 也就是把 $[0, 1]$ 四等分 (2^2), 然后分别在 16 个正方形区域各自选择一个点, 记作 $a_2^1, a_2^2, \dots, a_2^{16}$, 要求是: 所有点不能在同一水平线或者铅直线上, 如此继续, 4^3 等分, 等等, 第 n 次操作, 需要 4^n 等分, 得到 $a_n^1, a_n^2, \dots, a_n^{4^n}$ 个点, 要求还是: 所有的点不能在同一水平线或者铅直线上, 这个是可以办到的, 因为无论是线段还是正方形区域, 里面都是不可数个点, 而前面选择的只有最多可数个点。这样得到无穷多个点, 可数多个点, 用 A 表示所有这些点的集合。这个集合的边界是 $[0, 1] \times [0, 1]$ 。

首先, 根据 A 中点的构造过程可知, 每一条水平线或者铅直线上最多只含一个 A 中的点。其次, 对于任意一点 $(x, y) \in [0, 1] \times [0, 1]$, 对于任意包含 (x, y) 的开矩形 $B = (x_1, y_1) \times (x_2, y_2)$ 来说, 令 $d = \min\{x_2 - x_1, y_2 - y_1\}$, 那么只要 n 足够大, 使得 $\frac{1}{2^n} < d$, 那么第 n 操作中, 分成了 4^n 个边长为 $\frac{1}{2^n}$ 个正方形的时候, 至少有一个正方形落入上述开矩形 B 之中, 从而必然有 B 中一点 $(x', y') \in A$, 另外由于 B 中的点是不可数的, 而 A 中只有可数个点, 因而也必有 B 中的点不属于 A . 所以 (x, y) 是 A 的边界上的点。

5. 如 $A \subset [0, 1]$ 是这样一些开区间 (a_i, b_i) 的并集, 使得 $(0, 1)$ 中的每一有理数包含在某个 (a_i, b_i) 内, 求证 A 的边界 $= [0, 1] - A$.

首先 A 是开区间的并集, 从而使开集。其次, 从有理数的稠密性可知, 对于任一点 $x_0 \in [0, 1] - A$, 包含 x_0 的任意一个开区间, 必然包含某个有理数, 而有理数属于 A , 于是 x_0 是 A 的边界点。至于 $[0, 1]$ 之外的点, 首先 $\mathbb{R} - [0, 1]$ 是开集, 从而属于 A 的外域。

6. 如 A 是包含任何有理数 $r \in [0, 1]$ 的一个闭集, 求证 $[0, 1] \subset A$.

这道题目还是因为有理数的稠密性。对于任意的 $x \in [0, 1]$, 由于 $[0, 1]$ 中的所有有理数属于 A , 从而 x 是 A 的聚点 (x 的任意邻域内, 存在 A 的点) 又因为 A 是闭集, 因而 $x \in A$.

7. 求证推论22.3的逆: \mathbb{R}^n 的紧集是闭有界集 (参见习题6.)。

设 $T \subset \mathbb{R}^n$ 是紧集。

(1) 考虑 T 的开覆盖: $U_m = \{x \in \mathbb{R}^n : |x| < m\}$, 这里 $m \in \mathbb{Z}^+$, 由于 T 是紧集, 存在有限个开集 U_{m_1}, \dots, U_{m_k} 覆盖 T , 令 $M = \max\{m_1, \dots, m_k\}$, 那么 $T \subset U_M$, 从而是有界的。

(2) 要证明 T 是闭集, 也就是证明 $\mathbb{R}^n - T$ 是开集。对于任意一点 $x \in \mathbb{R}^n - T$, 对于任意一点 $a \in T$, 如果记 $r_a = |x - a|/2$, 那么开球 $U_a = \{x \in \mathbb{R}^n : |x - a| < r_a\}$ 为一开集, 考虑所有这样的开球 $U_a, a \in T$, 显然它们构成 T 的一个开覆盖, 从而存在有限个开球 U_{a_1}, \dots, U_{a_k} 覆盖 T . 我们把这些半径中最小的那个记为 r , 也就是 $r = \min\{r_{a_1}, \dots, r_{a_k}\}$, 我们来看看集合 $U(x, r) = \{y \in \mathbb{R}^n : |y - x| < r\}$. 我们希望证明 $U(x, r) \cap T = \emptyset$. 那么对于任一点 $y \in T$, 存在 a_i , 使得 $y \in U_{a_i}$, 也就是有

$$|y - a_i| < r_{a_i},$$

于是

$$|y - x| \geq ||y - a_i| - |a_i - x|| = |2r_{a_i} - |y - a_i|| = 2r_{a_i} - |y - a_i| > r_{a_i} > r,$$

因而 $y \notin U(x, r)$. 于是 $U(x, r) \subset \mathbb{R}^n - T$, $\mathbb{R}^n - T$ 为开集, T 是闭集。

8. (a) 如 A 是闭的且 $x \notin A$, 求证存在一数 $d > 0$ 使对一切 $y \in A$ 有 $|y - x| \geq d$.
 (b) 如 A 是闭的, B 是紧的, 且 $A \cap B = \emptyset$, 求证存在 $d > 0$ 使对一切 $y \in A$ 与 $x \in B$ 有 $|y - x| \geq d$. 提示: 对每一个 $b \in B$ 找出包含 b 的一开集 U 使得这一关系式对 $x \in U \cap B$ 成立。
 (c) 若 A 与 B 都是闭的但都不是紧的, 试在 \mathbb{R}^2 中给出一个反例。

(a) A 为闭集, 那么 $\mathbb{R}^n - A$ 为开集, 而 $x \in \mathbb{R}^n - A$, 从而存在开球 $U(x, r) \subset \mathbb{R}^n - A$, 选择 $d = r$ 即可, 此时, 对于所有的 $y \in A$, 有 $|y - x| \geq d$.

(b) 从 (a) 可知, 对于任一 $b \in B$, 存在 d_b 使得 $\forall a \in A, |a - b| \geq d_b$, 那么考虑开球 $U_b = \{x \in \mathbb{R}^n : |x - b| < d_b/2\}$, U_b 具有如下性质: 任意点 $a \in A, x \in U_b$ 有 $|x - a| \geq d_b/2$. 理由如下: $|a - b| \geq d_b, |x - b| < d_b/2$, 于是

$$|x - a| \geq ||x - b| - |b - a|| = |b - a| - |x - b| \geq d_b - d_b/2 = d_b/2.$$

于是所有的 $U_b, b \in B$ 构成 B 的一个开覆盖, 由于 B 的紧性, 存在有限个 U_{b_1}, \dots, U_{b_k} 覆盖 B . 此时选取 $d = \min\{d_{b_1}/2, \dots, d_{b_k}/2\}$, 此时, $\forall y \in A, \forall x \in B$ 有 $|y - x| \geq d$. 证明方法和前面 U_b 类似.

(c) 可以考虑由孤立点组成的两个集合

$$A = \{(n, \frac{1}{n}) : n = 2, 3, \dots\},$$

$$B = \{(n, -\frac{1}{n}) : n = 2, 3, \dots\}.$$

这两个集合都是闭集, 但不是紧集. 它们之间的距离可以任意接近.

9. 如 U 是开的且 $C \subset U$ 是紧的, 证明存在一紧集 D 使得 $C \subset D$ 的内域且 $D \subset U$. 这里需要使用上一题的结论. U 为开集, 那么 $\mathbb{R}^n - U$ 为闭集. C 为紧集, 那么存在 $d > 0$, 使得 $\forall x \in C, \forall y \in \mathbb{R}^n - U$, 有 $|x - y| \geq d$. 由此, 我们这样来构造 D :

$$D = \{x \in \mathbb{R}^n : \exists y \in C, |y - x| \leq d/2\}.$$

(1) 由于 C 是紧集, 从而是有界, 根据 D 的构造, D 也是有界的, 事实上, $\forall x \in D$, 存在 $y \in C, |x - y| \leq d/2$, 于是

$$|x| \leq |x - y| + |y| < M + d/2.$$

(2) D 是闭集, 我们证明 $\mathbb{R}^n - D$ 是开集. 对于任一 $x \in \mathbb{R}^n - D$, 根据 D 的定义, $\forall y \in C, |y - x| > d/2$. 我们希望找到开球 $U(x, r) \cap D = \emptyset$. 我们这样来选取这个 r : 根据上一题的结论, 存在 d_x , 使得对于任意 $y \in C$, 有 $|y - x| \geq d_x$, 显然可以认为 $d_x \geq d/2$, 是否可以更强一点, $d_x > d/2$ 呢, 对于紧集 C 来说, 这是可以的 (需要后面一节中, 紧集上连续函数可以取到最大值和最小值), 我们取 $r = d_x - d/2$, 于是 $\forall z \in U(x, r)$, 对于任一 $y \in C$, 有

$$|y - z| \geq ||y - x| - |z - x|| = |y - x| - |z - x| > d_x - r = d/2,$$

因此 $z \in \mathbb{R}^n - D$, 从而 $\mathbb{R}^n - D$ 为开集.

(3) 还需要证明最后一步 $D \subset U$. $\forall x \in D, y \in \mathbb{R}^n - U$, 存在 $a \in C, |x - a| \leq d/2, |y - a| \geq d$, 于是

$$|y - x| \geq ||y - a| - |x - a|| = |y - a| - |x - a| \geq d - d/2 = d/2.$$

它说明 D 中的点不可能属于 $\mathbb{R}^n - U$, 因此 $D \subset U$.

22.3 函数与连续性

从 \mathbb{R}^n 到 \mathbb{R}^m 的一个函数 (有时称为 n 个变元的 (向量值) 函数) 是一个规则, 它把 \mathbb{R}^n 中的每一点对应到 \mathbb{R}^m 中的某一点; 一个函数 f 使 x 所对应的点记作 $f(x)$. 我们写 $f: \mathbb{R}^n \rightarrow \mathbb{R}^m$ (按上下文读作 “ f 把 \mathbb{R}^n 映入 \mathbb{R}^m ” 或 “ f 映 \mathbb{R}^n 入 \mathbb{R}^m ”) 表明 $f(x) \in \mathbb{R}^m$ 是对 $x \in \mathbb{R}^n$ 定义的. 记号 $f: A \rightarrow \mathbb{R}^m$ 表示 $f(x)$ 仅对集 A 中的 x 有意义, A 称为 f 的定义域. 如 $B \subset A$, 我们把 $f(B)$ 定义为对 $x \in B$ 的一切 $f(x)$ 的集. 又若 $C \subset \mathbb{R}^m$, 我们定义 $f^{-1}(C) = \{x \in A: f(x) \in C\}$. 记号 $f: A \rightarrow B$ 表示 $f(A) \subset B$.

通过作出一函数 $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ 的图, 我们可以得到它的一方便的表示, 这个图就是一切形如 $(x, y, f(x, y))$ 的 3 数组的集, 它实际上是 3 维空间中的一个图形 (例如, 见第 23 章图).

若 $f, g: \mathbb{R}^n \rightarrow \mathbb{R}$, 则函数 $f+g, f-g, f \cdot g$ 与 f/g 可以确切地像单变量情况一样来定义. 如 $f: A \rightarrow \mathbb{R}^m, g: B \rightarrow \mathbb{R}^p$, 其中 $B \subset \mathbb{R}^m$, 则复合函数 $g \circ f$ 定义为 $g \circ f(x) = g(f(x))$; $g \circ f$ 的定义域是 $A \cap f^{-1}(B)$. 如 $f: A \rightarrow \mathbb{R}^m$ 是 1-1 的, 也就是, 当 $x \neq y$ 时 $f(x) \neq f(y)$, 我们定义 $f^{-1}: f(A) \rightarrow \mathbb{R}^n$, 这里要求 $f^{-1}(z)$ 是唯一的 $x \in A$ 并且 $f(x) = z$.

一个函数 $f: A \rightarrow \mathbb{R}^m$ 用 $f(x) = (f_1(x), \dots, f_m(x))$ 确定 m 个分量函数 $f_1, \dots, f_m: A \rightarrow \mathbb{R}$. 反过来, 如果已给 m 个函数 $g_1, \dots, g_m: A \rightarrow \mathbb{R}$, 则有唯一的函数 $f: A \rightarrow \mathbb{R}^m$ 使得 $f_i = g_i$, 即 $f(x) = (g_1(x), \dots, g_m(x))$. 这个函数 f 将记作 (g_1, \dots, g_m) , 所以我们总有 $f = (f_1, \dots, f_m)$. 如 $\pi: \mathbb{R}^n \rightarrow \mathbb{R}^n$ 是恒等函数, $\pi(x) = x$, 则 $\pi_i(x) = x_i$; 函数 π_i 称作第 i 个投影函数.

和单变量情况一样, 记号 $\lim_{x \rightarrow a} f(x) = b$ 表示, 当选取 x 足够接近于 a 但不等于 a 时, 我们可以使 $f(x)$ 任意地接近于 b . 用数学术语讲, 这表明: 对任一数 $\epsilon > 0$, 存在一数 $\delta > 0$ 使对 f 的定义域中的一切满足 $0 < |x - a| < \delta$ 的 x 有 $|f(x) - b| < \epsilon$. 函数 $f: A \rightarrow \mathbb{R}^m$ 称为在 $a \in A$ 连续, 如果 $\lim_{x \rightarrow a} f(x) = f(a)$. $f: A \rightarrow \mathbb{R}^m$ 在每一 $a \in A$ 处连续就简称 f 是连续的. 关于连续性概念的有趣的意想不到的点之一是, 它可以不用极限来定义. 由下一定理得知, $f: \mathbb{R}^n \rightarrow \mathbb{R}^m$ 连续, 当且仅当只要 $U \subset \mathbb{R}^m$ 是开的 $f^{-1}(U)$ 就是开的; 如 f 的域不是 \mathbb{R}^n 的全部, 则需要一稍微复杂的条件.

定理 22.5

如 $A \subset \mathbb{R}^n$, 函数 $f: A \rightarrow \mathbb{R}^m$ 连续当且仅当对任一开集 $U \subset \mathbb{R}^m$ 存在某开集 $V \subset \mathbb{R}^n$ 使得 $f^{-1}(U) = V \cap A$.



证明 设 f 连续. 如 $a \in f^{-1}(U)$, 则 $f(a) \in U$. 因 U 是开的, 故有开矩形 B 使 $f(a) \in B \subset U$. 因 f 在 a 点连续, 我们只要把 x 选取在包含 a 的某充分小的矩形 C 内, 就能保证 $f(x) \in B$. 对每一 $a \in f^{-1}(U)$ 这样做, 并令 V 为所有这些 C 的并集. 显然 $f^{-1}(U) = V \cap A$. 其逆也类似, 留给读者去证明.

定理 22.5 的下一推断极为重要.

定理 22.6

如 $f: A \rightarrow \mathbb{R}^m$ 是连续的, 其中 $A \subset \mathbb{R}^n$, 而 A 是紧的, 则 $f(A)$ 也是紧的。



证明 设 \mathcal{O} 是 $f(A)$ 的一个开覆盖。对于 \mathcal{O} 中每一个开集 U 存在一个开集 V_U 使得 $f^{-1}(U) = V_U \cap A$. 一切 V_U 的集合是 A 的一开覆盖。因 A 是紧的, 故有有限个 V_{U_1}, \dots, V_{U_n} 覆盖 A . 于是 U_1, \dots, U_n 覆盖 $f(A)$.

若 $f: A \rightarrow \mathbb{R}$ 有界, 则 f 在 $a \in A$ 处不连续的程度可以用一个确切的方法加以度量。对 $\delta > 0$ 令

$$M(a, f, \delta) = \sup\{f(x) : x \in A \text{ 且 } |x - a| < \delta\}$$

$$m(a, f, \delta) = \inf\{f(x) : x \in A \text{ 且 } |x - a| < \delta\}.$$

f 在 a 处的振幅 $o(f, a)$ 定义为 $o(f, a) = \lim_{\delta \rightarrow 0} [M(a, f, \delta) - m(a, f, \delta)]$. 因为 $M(a, f, \delta) - m(a, f, \delta)$ 当 δ 下降时也下降, 所以这一极限恒存在。关于 $o(f, a)$ 有两个重要事实。

定理 22.7

有界函数 f 当且仅当 $o(f, a) = 0$ 时在 a 点连续。



证明 设 f 在 a 点连续, 对任一数 $\epsilon > 0$ 我们可以选取一数 $\delta > 0$ 使对一切 $x \in A$ 且 $|x - a| < \delta$ 者恒有 $|f(x) - f(a)| < \epsilon$; 于是 $M(a, f, \delta) - m(a, f, \delta) \leq 2\epsilon$. 因这对任意 ϵ 为真, 故有 $o(f, a) = 0$. 其逆类似, 并留给读者。

定理 22.8

设 $A \subset \mathbb{R}^n$ 是闭的。如 $f: A \rightarrow \mathbb{R}$ 是任一有界函数, 又 $\epsilon > 0$, 则 $\{x \in A : o(f, x) \geq \epsilon\}$ 是闭的。



证明 设 $B = \{x \in A : o(f, x) \geq \epsilon\}$. 我们要证明 $\mathbb{R}^n - B$ 是开的。如果 $x \in \mathbb{R}^n - B$, 那么或者有 $x \notin A$, 不然的话, 就有 $x \in A$ 以及 $o(f, x) < \epsilon$. 在第一种情况下, 因 A 是闭的, 故存在包含 x 的开矩形 C 使得 $C \subset \mathbb{R}^n - A \subset \mathbb{R}^n - B$. 在第二种情况下, 存在一 $\delta > 0$ 使得 $M(x, f, \delta) - m(x, f, \delta) < \epsilon$. 令 C 是一包含 x 的开矩形, 使得对一切 $y \in C$, 有 $|x - y| < \delta$. 则若 $y \in C$, 就有一 δ_1 , 使对所有满足 $|z - y| < \delta_1$ 的 z 有 $|x - z| < \delta$. 于是 $M(y, f, \delta_1) - m(y, f, \delta_1) < \epsilon$, 从而 $o(y, f) < \epsilon$. 所以 $C \subset \mathbb{R}^n - B$.

第二十二章 习题

1. 若 $f: A \rightarrow \mathbb{R}^m$ 且 $a \in A$, 证明 $\lim_{x \rightarrow a} f(x) = b$ 当且仅当对于 $i = 1, \dots, m$ 有 $\lim_{x \rightarrow a} f_i(x) = b_i$.
2. 求证 $f: A \rightarrow \mathbb{R}^m$ 在 a 点连续当且仅当每一个 f_i 都如此。
3. 求证线性变换 $T: \mathbb{R}^n \rightarrow \mathbb{R}^m$ 是连续的。提示: 利用习题10..
4. 设 $A = \{(x, y) \in \mathbb{R}^2 : x > 0 \text{ 且 } 0 < y < x^2\}$.
 - (a) 证明通过 $(0, 0)$ 的任一直线包含一个围绕 $(0, 0)$ 的在 $\mathbb{R}^2 - A$ 中的区间。
 - (b) 这样定义 $f: \mathbb{R}^2 \rightarrow \mathbb{R}$, 当 $x \notin A$ 时, $f(x) = 0$, 当 $x \in A$ 时 $f(x) = 1$. 对 $h \in \mathbb{R}^2$ 定义 $g_h: \mathbb{R} \rightarrow \mathbb{R}$, $g_h(t) = f(th)$. 求证每个 g_h 在 0 点连续, 但 f 在 $(0, 0)$ 点不连续。

5. 由考察 $f(x) = |x - a|$ 确定的 $f: \mathbb{R}^n \rightarrow \mathbb{R}^1$ 来证明 $\{x \in \mathbb{R}^n : |x - a| < r\}$ 是开的。
6. 如 $A \subset \mathbb{R}^n$ 不是闭的, 证明存在一无界的连续函数 $f: A \rightarrow \mathbb{R}$. 提示: 如 $x \in \mathbb{R}^n - A$ 但 $x \notin [(\mathbb{R}^n - A) \text{ 的内域}]$, 令 $f(y) = 1/|y - x|$.
7. 如 A 是紧的, 求证任何连续函数 $f: A \rightarrow \mathbb{R}$ 有最大值和最小值。
8. 设 $f: [a, b] \rightarrow \mathbb{R}$ 是一增函数。如 $x_1, \dots, x_n \in [a, b]$, 证明

$$\sum_{i=1}^n o(f, x_i) < f(b) - f(a).$$

第二十三章 微分

23.1 基本定义

回想一函数 $f: \mathbb{R} \rightarrow \mathbb{R}$ 在 $a \in \mathbb{R}$ 处可微是指：有一数 $f'(a)$ 使得

$$\lim_{h \rightarrow 0} \frac{f(a+h) - f(a)}{h} = f'(a). \quad (23.1.1)$$

对一般情形的函数 $f: \mathbb{R}^n \rightarrow \mathbb{R}^m$ 这个式子当然没有意义，但可以用一种方式将其重写使之有意义。如 $\lambda: \mathbb{R}^n \rightarrow \mathbb{R}^m$ 是由 $\lambda(h) = f'(a) \cdot h$ 定义的线性变换，则 (23.1.1) 式等价于

$$\lim_{h \rightarrow 0} \frac{f(a+h) - f(a) - \lambda(h)}{h} = 0. \quad (23.1.2)$$

(23.1.2) 式常常可解释为 $\lambda + f(a)$ 是 f 在 a 处的一个好的近似（见习题）。因而我们集中注意力于线性变换 λ ，而把可微性重述如下：

函数 $f: \mathbb{R}^n \rightarrow \mathbb{R}^m$ 在 $a \in \mathbb{R}^n$ 点可微，如果有一线性变换 $\lambda: \mathbb{R}^n \rightarrow \mathbb{R}^m$ 使得

$$\lim_{h \rightarrow 0} \frac{f(a+h) - f(a) - \lambda(h)}{h} = 0.$$

在这一形式下，这个定义对于高维有简单的推广：

定义 23.1

函数 $f: \mathbb{R}^n \rightarrow \mathbb{R}^m$ 在 $a \in \mathbb{R}^n$ 点可微，如果存在一线性变换 $\lambda: \mathbb{R}^n \rightarrow \mathbb{R}^m$ 使得

$$\lim_{h \rightarrow 0} \frac{|f(a+h) - f(a) - \lambda(h)|}{|h|} = 0.$$



注意 h 是 \mathbb{R}^n 中的点， $f(a+h) - f(a) - \lambda(h)$ 是 \mathbb{R}^m 中的点，所以范数记号是不可少的，这个线性变换 λ 记作 $Df(a)$ ，称作 f 在 a 点的导数¹。短语“这个线性变换 λ ”的正确性证明如下。

定理 23.1

如 $f: \mathbb{R}^n \rightarrow \mathbb{R}^m$ 在 $a \in \mathbb{R}^n$ 点可微，则存在一个唯一的线性变换 $\lambda: \mathbb{R}^n \rightarrow \mathbb{R}^m$ 使得

$$\lim_{h \rightarrow 0} \frac{|f(a+h) - f(a) - \lambda(h)|}{|h|} = 0.$$



证明 假定 $\mu: \mathbb{R}^n \rightarrow \mathbb{R}^m$ 也满足

$$\lim_{h \rightarrow 0} \frac{|f(a+h) - f(a) - \mu(h)|}{|h|} = 0.$$

¹这里不同的书略有差异，从而会给人造成混淆，有些书把这个称为微分，而作为线性函数，给定一组基底之后，是存在一个对应的矩阵的，把这个矩阵称为导数。

如 $d(h) = f(a+h) - f(a)$, 则

$$\begin{aligned} & \lim_{h \rightarrow 0} \frac{|\lambda(h) - \mu(h)|}{|h|} \\ &= \lim_{h \rightarrow 0} \frac{|\lambda(h) - d(h) + d(h) - \mu(h)|}{|h|} \\ &\leq \lim_{h \rightarrow 0} \frac{|\lambda(h) - d(h)|}{|h|} + \lim_{h \rightarrow 0} \frac{|d(h) - \mu(h)|}{|h|} \\ &= 0. \end{aligned}$$

另一方面, 因 $\frac{|\lambda(h) - \mu(h)|}{|h|} \geq 0$, 所以 $\lim_{h \rightarrow 0} \frac{|\lambda(h) - \mu(h)|}{|h|} = 0$. 如 $x \in \mathbb{R}^n$, 则当 $t \rightarrow 0$ 时 $tx \rightarrow 0$. 因此对 $x \neq 0$ 我们有

$$0 = \lim_{t \rightarrow 0} \frac{|\lambda(tx) - \mu(tx)|}{|tx|} = \frac{|\lambda(x) - \mu(x)|}{|x|}$$

所以 $\lambda(x) = \mu(x)$.

我们以后将会发现求 $Df(a)$ 的一个简单方法. 目前我们来考察由 $f(x, y) = \sin x$ 定义的函数 $f: \mathbb{R}^2 \rightarrow \mathbb{R}$. 那么 $Df(a, b) = \lambda$ 满足 $\lambda(x, y) = (\cos a) \cdot x$. 为要证明它, 注意

$$\lim_{(h,k) \rightarrow 0} \frac{|f(a+h, b+k) - f(a, b) - \lambda(h, k)|}{|(h, k)|} = \lim_{(h,k) \rightarrow 0} \frac{|\sin(a+h) - \sin a - (\cos a) \cdot h|}{|(h, k)|}$$

因为 $\sin'(a) = \cos a$, 我们有

$$\lim_{h \rightarrow 0} \frac{|\sin(a+h) - \sin a - (\cos a) \cdot h|}{|h|} = 0.$$

因为 $|(h, k)| \geq |h|$, 所以还有

$$\lim_{(h,k) \rightarrow 0} \frac{|\sin(a+h) - \sin a - (\cos a) \cdot h|}{|(h, k)|} = 0.$$

考察 $Df(a): \mathbb{R}^n \rightarrow \mathbb{R}^m$ 关于 \mathbb{R}^n 与 \mathbb{R}^m 的通常基底的矩阵, 常常是方便的. 这个 $m \times n$ 矩阵称为 f 在 a 处的雅可比 (Jacobi) 矩阵, 记作 $f'(a)$. 如 $f(x, y) = \sin x$, 则 $f'(a, b) = (\cos a, 0)$. 如 $f: \mathbb{R} \rightarrow \mathbb{R}$, 则 $f'(a)$ 是 1×1 矩阵, 其唯一元就是在初等微积分中记作 $f'(a)$ 的那个数.

如果 f 仅在包含 a 的某个开集上定义, 那么还可以定义 $Df(a)$. 为使定理的叙述流畅而又不失其普遍性, 我们只考虑定义在 \mathbb{R}^n 上的函数. 设有 $f: \mathbb{R}^n \rightarrow \mathbb{R}^m$, 如果 f 在每一个 $a \in A$ 处可微就称 f 在 A 上可微. 如 $f: A \rightarrow \mathbb{R}^m$, 又若 f 可以扩张为在包含 A 的某开集上的可微函数, 则称 f 是可微的.

第二十三章 习题

1. 求证: 如 $f: \mathbb{R}^n \rightarrow \mathbb{R}^m$ 在 $a \in \mathbb{R}^n$ 处可微, 则它在 a 点连续. 提示, 利用习题10..
2. 一函数 $f: \mathbb{R}^2 \rightarrow \mathbb{R}$, 如对每一 $x \in \mathbb{R}$, 对所有 $y_1, y_2 \in \mathbb{R}$ 我们都有 $f(x, y_1) = f(x, y_2)$, 则称 f 与第二变元无关. 试证 f 与第二变元无关当且仅当存在一函数 $g: \mathbb{R} \rightarrow \mathbb{R}$ 使得 $f(x, y) = g(x)$. $f'(a, b)$ 用 g' 表示时是什么?
3. 试决定何时一函数 $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ 与第一变元无关, 并对这种 f 求出 $f'(a, b)$. 什么样的函数即与第一变元无关也与第二变元无关?
4. 设 g 是单位圆周 $\{x \in \mathbb{R}^2 : |x| = 1\}$ 上的连续函数且有 $g(0, 1) = g(1, 0) = 0$,

$g(-x) = -g(x)$. 定义 $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ 为:

$$f(x) = \begin{cases} |x| \cdot g\left(\frac{x}{|x|}\right) & x \neq 0, \\ 0 & x = 0. \end{cases}$$

(a) 如 $x \in \mathbb{R}^2$ 且 $h: \mathbb{R} \rightarrow \mathbb{R}$ 定义为 $h(t) = f(tx)$, 证明 h 是可微的。

(b) 证明 f 在 $(0,0)$ 处不可微, 除非 $g = 0$. 提示: 当 $k = 0$ 时 (再当 $h = 0$ 时) 考察 (h, k) , 先证明 $Df(0,0)$ 必须为零。

5. 设 $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ 用下式定义:

$$f(x, y) = \begin{cases} \frac{x|y|}{\sqrt{x^2 + y^2}} & (x, y) \neq 0, \\ 0 & (x, y) = 0. \end{cases}$$

证明 f 是习题4.中考虑过的那种函数, 所以 f 在 $(0,0)$ 处不可微。

6. 设 $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ 定义为 $f(x, y) = \sqrt{|xy|}$. 求证 f 在 $(0,0)$ 处不可微。

7. 设 $f: \mathbb{R}^n \rightarrow \mathbb{R}$ 是一函数使得 $|f(x)| \leq |x|^2$. 证明 f 在 0 处可微。

8. 设 $f: \mathbb{R} \rightarrow \mathbb{R}^2$. 求证: 当且仅当 f_1 与 f_2 在 $a \in \mathbb{R}$ 处可微时, f 在 a 处可微, 且这时

$$f'(a) = \begin{pmatrix} (f_1)'(a) \\ (f_2)'(a) \end{pmatrix}.$$

9. 两函数 $f, g: \mathbb{R} \rightarrow \mathbb{R}$ 称为在 a 点直到 n 阶相等, 如果

$$\lim_{h \rightarrow 0} \frac{f(a+h) - g(a+h)}{h^n} = 0.$$

(a) 试证: f 在 a 点可微, 当且仅当 f 在 a 点连续, 且存在形如 $g(x) = a_0 + a_1(x-a)$ 的函数 g 使得 f 与 g 在 a 点直到一阶相等。

(b) 如 $f'(x), \dots, f^{(n)}(x)$ 在 $x = a$ 附近存在, $f^{(n)}(x)$ 在 a 点连续, 试证 f 与下式

$$g(x) = \sum_{i=0}^n \frac{f^{(i)}(a)}{i!} (x-a)^i$$

定义的函数 g 在 a 点直到 n 阶相等。提示: 极限

$$\lim_{x \rightarrow a} \frac{f(x) - \sum_{i=0}^n \frac{f^{(i)}(a)}{i!} (x-a)^i}{(x-a)^n}$$

可用洛必达 (L'Hospital) 法则计算。

23.2 基本定理

定理 23.2. 锁链法则

如 $f: \mathbb{R}^n \rightarrow \mathbb{R}^m$ 在 a 点可微, $g: \mathbb{R}^m \rightarrow \mathbb{R}^p$ 在 $f(a)$ 点可微, 则其复合 $g \circ f: \mathbb{R}^n \rightarrow \mathbb{R}^p$ 在 a 点可微, 且

$$D(g \circ f)(a) = Dg(f(a)) \circ Df(a).$$



注。此式可写成

$$(g \circ f)'(a) = g'(f(a)) \circ f'(a).$$

如 $m = n = p = 1$, 我们便得到老的锁链规则。

证明 令 $b = f(a)$, $\lambda = Df(a)$, $\mu = Dg(f(a))$. 如果我们定义

$$\varphi(x) = f(x) - f(a) - \lambda(x - a), \quad (23.2.1)$$

$$\psi(x) = g(y) - g(b) - \mu(y - b), \quad (23.2.2)$$

$$\rho(x) = g \circ f(x) - g \circ f(a) - \mu \circ \lambda(x - a), \quad (23.2.3)$$

则

$$\lim_{x \rightarrow a} \frac{|\varphi(x)|}{|x - a|} = 0, \quad (23.2.4)$$

$$\lim_{y \rightarrow b} \frac{|\psi(y)|}{|y - b|} = 0, \quad (23.2.5)$$

而我们必须证明

$$\lim_{x \rightarrow a} \frac{|\rho(x)|}{|x - a|} = 0.$$

现在

$$\begin{aligned} \rho(x) &= g(f(x)) - g(b) - \mu(\lambda(x - a)) \\ &= g(f(x)) - g(b) - \mu(f(x) - f(a) - \varphi(x)) \quad \text{由 (23.2.1)} \\ &= [g(f(x)) - g(b) - \mu(f(x) - f(a))] + \mu(\varphi(x)) \\ &= \psi(f(x)) + \mu(\varphi(x)) \quad \text{由 (23.2.2)} \end{aligned}$$

于是我们必须证明

$$\lim_{x \rightarrow a} \frac{|\psi(f(x))|}{|x - a|} = 0, \quad (23.2.6)$$

$$\lim_{x \rightarrow a} \frac{|\mu(\varphi(x))|}{|x - a|} = 0. \quad (23.2.7)$$

(23.2.7) 式容易从 (23.2.4) 式和习题10.推得。如果 $\epsilon > 0$, 从 (23.2.5) 式推知, 对某一个 $\delta > 0$, 我们有

$$|\psi(f(x))| < \epsilon |f(x) - b|, \text{ 只要 } |f(x) - b| < \delta,$$

而这一点只要对某个 δ_1 , 由 $|x - a| < \delta_1$ 就总成立, 于是, 由习题10., 对某个 M ,

$$\begin{aligned} |\psi(f(x))| &< \epsilon |f(x) - b| \\ &= \epsilon |\varphi(x) + \lambda(x - a)| \\ &= \epsilon |\varphi(x)| + \epsilon M |x - a|. \end{aligned}$$

(23.2.6) 式现就容易得出。

定理 23.3

(a) 如 $f: \mathbb{R}^n \rightarrow \mathbb{R}^m$ 是一常值函数 (也就是, 若对某 $y \in \mathbb{R}^m$, 我们有: 对一切 $x \in \mathbb{R}^n$, $f(x) = y$), 那么

$$Df(a) = 0.$$

(2) 如 $f: \mathbb{R}^n \rightarrow \mathbb{R}^m$ 是一个线性变换, 则

$$Df(a) = f.$$

(3) 如 $f: \mathbb{R}^n \rightarrow \mathbb{R}^m$, 则 f 在 $a \in \mathbb{R}^n$ 处可微当且仅当每个 f_i 是如此, 且

$$Df(a) = (Df_1(a), \dots, Df_m(a)).$$

于是 $f'(a)$ 是 $m \times n$ 矩阵, 其第 i 行是 $f'_i(a)$.

(4) 如 $s: \mathbb{R}^2 \rightarrow \mathbb{R}$ 定义为 $s(x, y) = x + y$, 则

$$Ds(a, b) = s.$$

(5) 如 $p: \mathbb{R}^2 \rightarrow \mathbb{R}$ 定义为 $p(x, y) = x \cdot y$, 则

$$Dp(a, b)(x, y) = bx + ay.$$

于是 $p'(a, b) = (b, a)$.



证明

(1)

$$\lim_{h \rightarrow 0} \frac{|f(a+h) - f(a) - 0|}{|h|} = \lim_{h \rightarrow 0} \frac{|y - y - 0|}{|h|} = 0.$$

(2)

$$\lim_{h \rightarrow 0} \frac{|f(a+h) - f(a) - f(h)|}{|h|} = \lim_{h \rightarrow 0} \frac{|f(a) = f(h) - f(a) - f(h)|}{|h|} = 0.$$

(3) 如每一个 f_i 在 a 处可微, 且

$$\lambda = (Df_1(a), \dots, Df_m(a)),$$

则

$$\begin{aligned} f(a+h) - f(a) - f(h) \\ &= (f_1(a+h) - f_1(a) - Df_1(a)(h), \dots, \\ &\quad f_m(a+h) - f_m(a) - Df_m(a)(h)). \end{aligned}$$

所以

$$\begin{aligned} &\lim_{h \rightarrow 0} \frac{|f(a+h) - f(a) - \lambda(h)|}{|h|} \\ &\leq \lim_{h \rightarrow 0} \sum_{i=1}^m \frac{|f_i(a+h) - f_i(a) - Df_i(a)(h)|}{|h|} \\ &= 0. \end{aligned}$$

另一方面, 如 f 在 a 处可微, 则由 (2) 与定理 23.2, $f_i = \pi_i \circ f$ 在 a 处可微。

(4) 由 (2) 推得。

(5) 令 $\lambda(x, y) = bx + ay$. 那么

$$\begin{aligned} &\lim_{(h,k) \rightarrow 0} \frac{|p(a+h, b+k) - p(a, b) - \lambda(h, k)|}{|(h, k)|} \\ &= \lim_{(h,k) \rightarrow 0} \frac{|hk|}{|(h, k)|}. \end{aligned}$$

现在

$$|hk| \leq \begin{cases} |h|^2 & \text{如 } |k| \leq |h|, \\ |k|^2 & \text{如 } |h| \leq |k|, \end{cases}$$

因此 $|hk| \leq |h|^2 + |k|^2$. 所以

$$\frac{|hk|}{|(h, k)|} \leq \frac{h^2 + k^2}{\sqrt{h^2 + k^2}} = \sqrt{h^2 + k^2},$$

因而

$$\lim_{(h,k) \rightarrow 0} \frac{|hk|}{|(h, k)|} = 0.$$

推论 23.1

如 $f, g: \mathbb{R}^n \rightarrow \mathbb{R}$ 在 a 处可微, 则

$$D(f+g)(a) = Df(a) + Dg(a),$$

$$D(f \cdot g)(a) = g(a)Df(a) + f(a)Dg(a).$$

此外, 如果 $g(a) \neq 0$, 则

$$D(f/g)(a) = \frac{g(a)Df(a) - f(a)Dg(a)}{[g(a)]^2}.$$



证明 我们将证明第一式而把其余的留给读者。因为 $f+g = s \circ (f, g)$, 我们有

$$\begin{aligned} D(f+g)(a) &= Ds(f(a), g(a)) \circ D(f, g)(a) \\ &= s \circ (Df(a), Dg(a)) \\ &= Df(a) + Dg(a). \end{aligned}$$

下面这样的函数 $f: \mathbb{R}^n \rightarrow \mathbb{R}^m$ 的可微性现在得到了保证。其各分量函数可以从函数 π_i (它们是线性变换) 以及我们在初等微积分中早已会求导的函数经过加法、乘法、除法 and 复合而获得。但是, 求 $Df(x)$ 或 $f'(x)$ 可能是一项相当艰巨的工作。例如, 设 $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ 定义为 $f(x, y) = \sin(xy^2)$. 因为 $f = \sin \circ (\pi_1 \cdot [\pi_2]^2)$, 我们有

$$\begin{aligned} f'(a, b) &= \sin'(ab^2) \cdot [b^2(\pi_1)'(a, b) + a([\pi_2]^2)'(a, b)] \\ &= \sin'(ab^2) \cdot [b^2(\pi_1)'(a, b) + 2ab(\pi_2)'(a, b)] \\ &= (\cos(ab^2)) \cdot [b^2(1, 0) + 2ab(0, 1)] \\ &= (b^2 \cos(ab^2), 2ab \cos(ab^2)). \end{aligned}$$

幸而我们很快将会发现计算 f' 的一种简单得多的方法。

第二十三章 习题

1. 利用本节定理求以下的 f' :

- (a) $f(x, y, z) = x^y$.
- (b) $f(x, y, z) = (x^y, z)$.
- (c) $f(x, y) = \sin(x \sin y)$.
- (d) $f(x, y, z) = \sin(x \sin(y \sin z))$.

- (e) $f(x, y, z) = x^{y^z}$.
 (f) $f(x, y, z) = x^{y+z}$.
 (g) $f(x, y, z) = (x + y)^z$.
 (h) $f(x, y) = \sin(xy)$.
 (i) $f(x, y) = [\sin(xy)]^{\cos^3}$.
 (j) $f(x, y) = (\sin(xy), \sin(x \sin y), x^y)$.
2. 求以下的 f' (其中 $g: \mathbb{R} \rightarrow \mathbb{R}$ 是连续的):
 (a) $f(x, y) = \int_a^{x+y} g$.
 (b) $f(x, y) = \int_a^{x \cdot y} g$.
 (c) $f(x, y, z) = \int_{xy}^{\sin(x \sin(y \sin z))} g$.
3. 一函数 $f: \mathbb{R}^n \times \mathbb{R}^m \rightarrow \mathbb{R}^p$, 如果对 $x, x_1, x_2 \in \mathbb{R}^n, y, y_1, y_2 \in \mathbb{R}^m$ 以及 $a \in \mathbb{R}$, 我们有

$$\begin{aligned} f(ax, y) &= af(x, y) = f(x, ay), \\ f(x_1 + x_2, y) &= f(x_1, y) + f(x_2, y), \\ f(x, y_1 + y_2) &= f(x, y_1) + f(x, y_2), \end{aligned}$$

则称 f 是双线性的。

- (a) 求证若 f 是双线性的, 则
- $$\lim_{(h,k) \rightarrow 0} \frac{|f(h, k)|}{|(h, k)|} = 0.$$
- (b) 求证 $Df(a, b)(x, y) = f(a, y) + f(x, b)$.
 (c) 证明定理 23.3 中 $Dp(a, b)$ 的公式是 (b) 的一特殊情况。
4. 定义 $IP: \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}$ 为 $IP(x, y) = \langle x, y \rangle$.
 (a) 求 $D(IP)(a, b)$ 与 $(IP)'(a, b)$.
 (b) 如 $f, g: \mathbb{R} \rightarrow \mathbb{R}^n$ 可微且 $h: \mathbb{R} \rightarrow \mathbb{R}$ 定义为 $h(t) = \langle f(t), g(t) \rangle$, 证明

$$h'(a) = \langle f'(a)^T, g(a) \rangle + \langle f(a), g'(a)^T \rangle.$$

(注意 $f'(a)$ 是一 $n \times 1$ 矩阵; 其转置矩阵 $f'(a)^T$ 是一 $1 \times n$ 矩阵, 我们把它看作 \mathbb{R}^n 的元.)

- (c) 如 $f: \mathbb{R} \rightarrow \mathbb{R}^n$ 可微且对一切 $t, |f(t)| = 1$, 证明 $\langle f'(t)^T, f(t) \rangle = 0$.
 (d) 举出一可微函数 $f: \mathbb{R} \rightarrow \mathbb{R}$ 使得 $|f|(t) = |f(t)|$ 定义的函数 $|f|$ 不可微。
5. 设 $E_i (i = 1, \dots, k)$ 是各维数不必相同的欧氏空间。一函数 $f: E_1 \times \dots \times E_k \rightarrow \mathbb{R}^p$ 称为重线性的, 如果对于每个选定的 $x_j \in E_j (j \neq i)$, 由 $g(x) = f(x_1, \dots, x_{i-1}, x, x_{i+1}, \dots, x_k)$ 定义的函数 $g: E_i \rightarrow \mathbb{R}^p$ 是一个线性变换。
- (a) 如果 f 是重线性的而且 $i \neq j$, 证明对于 $h = (h_1, \dots, h_k)$, 其中 $h_l \in E_l$, 我们有

$$\lim_{h \rightarrow 0} \frac{|f(a_1, \dots, h_i, \dots, h_j, \dots, a_k)|}{|h|} = 0.$$

提示: 如果 $g(x, y) = f(a_1, \dots, x, \dots, y, \dots, a_k)$, 则 g 是双线性的。

(b) 求证

$$Df(a_1, \dots, a_k)(x_1, \dots, x_k) = \sum_{i=1}^k f(a_1, \dots, a_{i-1}, x_i, a_{i+1}, \dots, a_k).$$

6. 把一个 $n \times n$ 矩阵的每一列视作 \mathbb{R}^n 的一元从而把矩阵本身当作 n 重乘积 $\mathbb{R}^n \times \dots \times \mathbb{R}^n$ 中的一个点。

(a) 求证 $\det : \mathbb{R}^n \times \dots \times \mathbb{R}^n \rightarrow \mathbb{R}$ 可微且

$$D(\det)(a_1, \dots, a_n)(x_1, \dots, x_n) = \sum_{i=1}^n \det \begin{bmatrix} a_1 \\ \vdots \\ x_i \\ \vdots \\ a_n \end{bmatrix}.$$

(b) 如果 $a_{ij} : \mathbb{R} \rightarrow \mathbb{R}$ 可微而 $f(t) = \det(a_{ij}(t))$, 试证

$$f'(t) = \sum_{j=1}^n \det \begin{bmatrix} a_{11}(t) & \dots & a_{1n}(t) \\ \vdots & & \vdots \\ a'_{j1}(t) & \dots & a'_{jn}(t) \\ \vdots & & \vdots \\ a_{n1}(t) & \dots & a_{nn}(t) \end{bmatrix}.$$

(c) 如对一些 t , $\det(a_{ij}(t)) \neq 0$, 且 $b_1, \dots, b_n : \mathbb{R} \rightarrow \mathbb{R}$ 都是可微的, 又设 $s_1, \dots, s_n : \mathbb{R} \rightarrow \mathbb{R}$ 是这样的一些函数使得 $s_1(t), \dots, s_n(t)$ 是方程组

$$\sum_{j=1}^n a_{ij} s_j(t) = b_i(t), \quad i = 1, \dots, n$$

的解。求证 s_i 可微并求出 $s'_i(t)$,

7. 设 $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$ 可微且有可微的逆 $f^{-1} : \mathbb{R}^n \rightarrow \mathbb{R}^n$. 证明: $(f^{-1})'(a) = [f'(f^{-1}(a))]^{-1}$.
提示: $f \circ f^{-1}(x) = x$.

23.3 偏导数

我们从讨论“每次对一个变元”求导数的问题开始, 如 $f : \mathbb{R}^n \rightarrow \mathbb{R}$ 且 $a \in \mathbb{R}^n$, 如极限

$$\lim_{h \rightarrow 0} \frac{f(a_1, \dots, a_i + h, \dots, a_n) - f(a_1, \dots, a_n)}{h}$$

存在, 就记作 $D_i f(a)$, 称为 f 在 a 点的偏导数。注意 $D_i f(a)$ 是某函数的通常导数, 这很重要; 实际上, 如 $g(x) = f(a_1, \dots, x, \dots, a_n)$, 则 $D_i f(a) = g'(a)$. 这表明, $D_i f(a)$ 是 f 的图形和平面 $x_j = a_j (j \neq i)$ 的交线在 $(a, f(a))$ 点切线的斜率 (图)。这也表明, 计算 $D_i f(a)$ 是我们早已会做的问题。如 $f(x_1, \dots, x_n)$ 已由含有 x_1, \dots, x_n 的某公式给出, 则我们可这样来求 $D_i f(x_1, \dots, x_n)$, 即把所有 $x_j (j \neq i)$ 都看作常数, 而对所得的 x_i 的函数在 x_i 求导。例如, $f(x, y) = \sin(xy^2)$, 则 $D_1 f(x, y) = y^2 \cos(xy^2)$, $D_2 f(x, y) = 2xy \cos(xy^2)$. 又如, $f(x, y) = x^y$, 则 $D_1 f(x, y) = yx^{y-1}$, $D_2 f(x, y) = x^y \ln x$.

稍经练习 (例如, 作本节末的习题), 就和已经会计算的通常导数一样, 也会很容易

地计算 $D_i f$.

如果一切 $x \in \mathbb{R}^n$, $D_i f(x)$ 存在, 我们便得到一个函数 $D_i f: \mathbb{R}^n \rightarrow \mathbb{R}$. 这个函数在 x 点的第 j 个偏导数, 也就是 $D_j(D_i f)(x)$, 常常记作 $D_{i,j} f(x)$. 注意这个记号把 i 和 j 的次序颠倒了. 实际上, 这个次序通常是没有关系的, 因为绝大多数函数 (在习题中给出例题) 满足 $D_{i,j} f = D_{j,i} f$. 有好些细致的定理保证这个等式: 下面这个定理已经完全够用了. 我们把它的陈述放在这里面而把证明放在后面 (习题1.).

定理 23.4

如 $D_{i,j} f$ 与 $D_{j,i} f$ 在包含 a 的一开集中连续, 则

$$D_{i,j} f(a) = D_{j,i} f(a).$$



函数 $D_{i,j} f$ 叫做 f 的二阶 (混合) 偏导数. 高阶 (混合) 偏导数可用明显的方式来定义. 显然定理23.4能用来证明在适当条件下高阶混合偏导数的相应等式. 如 f 有一切阶的偏导数, 则 $D_{i_1, \dots, i_k} f$ 中 i_1, \dots, i_k 的次序是完全无所谓的. 具有这种性质的函数称为 C^∞ 函数. 在以下各章中, 为方便起见, 经常仅限于讨论 C^∞ 函数.

在下节, 将用偏导数来求导数. 它们还有另外一个重要的用处---求函数的极大值和极小值.

定理 23.5

设 $A \subset \mathbb{R}^n$, 如 $f: A \rightarrow \mathbb{R}$ 在 A 的内域中点 a 处达到极大 (或极小), 且 $D_i f(a)$ 存在, 则 $D_i f(a) = 0$.



证明 设 $g_i(x) = f(a_1, \dots, x, \dots, a_n)$. 显然 g_i 在 a_i 处有极大值 (或极小值), 且 g_i 在包含 a_i 的一开区间中有定义. 因此 $0 = g'_i(a_i) = D_i f(a)$.

提醒读者, 定理23.5的逆即使当 $n = 1$ 时已不成立 (如 $f: \mathbb{R} \rightarrow \mathbb{R}$ 由 $f(x) = x^3$ 定义, 则 $f'(0) = 0$, 但 0 点甚至不是一个局部极大值或极小值). 如 $n > 1$, 定理23.5的逆可以在一种更为奇特的方式下不再为真. 例如, 设 $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ 由 $f(x, y) = x^2 - y^2$ 定义 (图). 则因 g_1 在 0 处有一极小值, 故 $D_1 f(0, 0) = 0$; 而因 g_2 在 0 处有一个极大值, 故 $D_2 f(0, 0) = 0$. 显然 $(0, 0)$ 既不是相对极大点也不是相对极小点.

如用定理23.5来寻求 f 在 A 上的最大值或最小值, 那么还必须单另检查 f 在边界点上的值---这是一件可怕的事情, 因为 A 的边界可能是整个 A ! 习题11.指明一种作法, 习题??陈述了一个经常可用的好方法.

第二十三章 习题

1. 求下列函数的偏导数:

- (a) $f(x, y, z) = x^y$.
- (b) $f(x, y, z) = z$.
- (c) $f(x, y) = \sin(x \sin y)$.
- (d) $f(x, y, z) = \sin(x \sin(y \sin z))$.
- (e) $f(x, y, z) = x^{y^z}$.

- (f) $f(x, y, z) = x^{y+z}$.
- (g) $f(x, y, z) = (x + y)^z$.
- (h) $f(x, y) = \sin(xy)$.
- (i) $f(x, y) = [\sin(xy)]^{\cos 3}$.
2. 求下列函数的偏导数 (其中 $g: \mathbb{R} \rightarrow \mathbb{R}$ 连续):
- (a) $f(x, y) = \int_a^{x+y} g$.
- (b) $f(x, y) = \int_y^x g$.
- (c) $f(x, y) = \int_a^{xy} g$.
- (d) $f(x, y, z) = \int_g^{xy} g$.
3. 如 $f(x, y) = x^{x^{x^y}} + (\ln x)(\arctan(\arctan(\arctan(\sin(\cos xy) - \ln(x + y))))))$, 求 $D_2 f(1, y)$. 提示: 有一很容易的做法。
4. 通过 g 与 h 的导数求 f 的偏导数, 如果
- (a) $f(x, y) = g(x)h(y)$.
- (b) $f(x, y) = g(x)^{h(y)}$.
- (c) $f(x, y) = g(x)$.
- (d) $f(x, y) = g(y)$.
- (e) $f(x, y) = g(x + y)$.
5. 设 $g_1, g_2: \mathbb{R}^2 \rightarrow \mathbb{R}$ 连续, 定义 $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ 为
- $$f(x, y) = \int_0^x g_1(t, 0)dt + \int_0^y g_2(x, t)dt.$$
- (a) 证明 $D_2 f(x, y) = g_2(x, y)$.
- (b) f 应怎样定义使得 $D_1 f(x, y) = g_1(x, y)$?
- (c) 求一函数 $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ 使得 $D_1 f(x, y) = x$, $D_2 f(x, y) = y$. 再求一个使得 $D_1 f(x, y) = y$, $D_2 f(x, y) = x$.
6. 如 $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ 且 $D_2 f = 0$, 证明 f 与第二个变元无关。如果 $D_1 f = D_2 f = 0$, 证明 f 是常数。
7. 设 $A = \{(x, y): x < 0 \text{ 或者 } x \geq 0 \text{ 且 } y \neq 0\}$.
- (a) 如果 $f: A \rightarrow \mathbb{R}$ 且 $D_1 f = D_2 f = 0$, 证明 f 是一个常数, 提示: 注意, A 中任两点可用一串直线段联结, 每一段平行于坐标轴之一。
- (b) 求一函数 $f: A \rightarrow \mathbb{R}$ 使得 $D_2 f = 0$, 但 f 不是与第二变元无关。
8. 定义 $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ 为
- $$f(x, y) = \begin{cases} xy \frac{x^2 - y^2}{x^2 + y^2} & (x, y) \neq 0, \\ 0 & (x, y) = 0, \end{cases}$$
- (a) 试证: 对一切 x , $D_2 f(x, 0) = x$; 对一切 y , $D_1 f(0, y) = -y$.
- (b) 试证 $D_{1,2} f(0, 0) \neq D_{2,1} f(0, 0)$.
9. 定义 $f: \mathbb{R} \rightarrow \mathbb{R}$ 为
- $$f(x) = \begin{cases} e^{-x^{-2}} & x \neq 0, \\ 0 & x = 0. \end{cases}$$

证明 f 是一 C^∞ 函数, 且对一切 $i, f^{(i)}(0) = 0$. 提示: 极限

$$f'(0) = \lim_{h \rightarrow 0} \frac{e^{-h^{-2}}}{h} = \lim_{h \rightarrow 0} \frac{1/h}{e^{h^{-2}}}$$

可用洛必达法则计算. 对 $x \neq 0$ 求 $f'(x)$ 非常容易, 然后 $f''(0) = \lim_{h \rightarrow 0} f'(h)/h$ 可用洛必达法则求得.

10. 设

$$f(x) = \begin{cases} e^{-(x-1)^{-2}} \cdot e^{-(x+1)^{-2}} & x \in (-1, 1), \\ 0 & x \notin (-1, 1). \end{cases}$$

- (a) 证明 $f: \mathbb{R} \rightarrow \mathbb{R}$ 是一 C^∞ 函数, 它在 $(-1, 1)$ 内为正, 在其它处为 0,
 (b) 证明存在一 C^∞ 函数 $g: \mathbb{R} \rightarrow [0, 1]$ 使得当 $x \leq 0$ 时 $g(x) = 0$, 当 $x \geq \epsilon$ 时 $g(x) = 1$. 提示: 如果 f 是一个 C^∞ 函数, 在 $(0, \epsilon)$ 内为正, 在其它处为 0, 令

$$g(x) = \int_0^x f / \int_0^\epsilon f.$$

- (c) 如 $a \in \mathbb{R}^n$, 定义 $g: \mathbb{R}^n \rightarrow \mathbb{R}$ 为

$$g(x) = f([x_1 - a_1]/\epsilon) \cdots f([x_n - a_n]/\epsilon).$$

证明 g 是一个 C^∞ 函数, 它在

$$(a_1 - \epsilon, a_1 + \epsilon) \times \cdots \times (a_n - \epsilon, a_n + \epsilon)$$

内为正, 在其它处为零.

- (d) 如 $A \subset \mathbb{R}^n$ 是开的且 $C \subset A$ 是紧的, 证明存在一个非负 C^∞ 函数 $f: A \rightarrow \mathbb{R}$ 使当 $x \in C$ 时 $f(x) > 0$, 而在含于 A 内的某闭集之外 $f = 0$.
 (e) 证明可以选取这样的 f 使得 $f: A \rightarrow [0, 1]$, 且对 $x \in C, f(x) = 1$. 提示: 如果 (d) 中的函数 f 当 $x \in C$ 时 $f(x) \geq \epsilon$, 考察 $g \circ f$, 其中 g 是 (b) 中的函数.

11. 定义 $g, h: \{x \in \mathbb{R}^2: |x| \leq 1\} \rightarrow \mathbb{R}^3$ 为

$$g(x, y) = (x, y, \sqrt{1 - x^2 - y^2}), h(x, y) = (x, y, -\sqrt{1 - x^2 - y^2}).$$

证明 f 在 $\{x \in \mathbb{R}^2: |x| = 1\}$ 上的最大值或者是 $\{x \in \mathbb{R}^2: |x| \leq 1\}$ 上 $f \circ g$ 的最大值, 或者是它上面 $f \circ h$ 的最大值.

23.4 导数

比较过习题1.和1.的读者已经猜到下面的

定理 23.6

如果 $f: \mathbb{R}^n \rightarrow \mathbb{R}^m$ 在 a 点可微, 则对于 $1 \leq i \leq m, 1 \leq j \leq n, D_j f_i(a)$ 存在, 且 $f'(a)$ 是 $m \times n$ 矩阵 $(D_j f_i(a))$.



证明 先假定 $m = 1$, 故 $f: \mathbb{R}^n \rightarrow \mathbb{R}$. 用 $h(x) = (a_1, \cdots, x, \cdots, a_n)$ 定义 $h: \mathbb{R} \rightarrow \mathbb{R}^n$, 其

中 x 在第 j 个位置。则 $D_j f(a) = (f \circ h)'(a_j)$. 因此, 由定理 23.2,

$$\begin{aligned} (f \circ h)'(a_j) &= f'(a) \cdot h'(a_j) \\ &= f'(a) \cdot \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix} \leftarrow \text{第 } j \text{ 个位置.} \end{aligned}$$

因为 $(f \circ h)'(a_j)$ 有唯一的元素 $D_j f(a)$, 这就表明 $D_j f(a)$ 存在且就是 $1 \times n$ 矩阵 $f'(a)$ 的第 j 个元素。

因为由定理 23.3, 每一 f_i 可微, 且 $f'(a)$ 的第 i 行是 $(f_i)'(a)$, 所以现在本定理就对任意的 m 都成立。

在习题中有几个例子表明定理 23.6 的逆不成立。但若添加一个假设, 它还是对的。

定理 23.7

如 $f: \mathbb{R}^n \rightarrow \mathbb{R}^m$, 则若所有 $D_j f_i(x)$ 在包含 a 的一开集中存在且每一函数 $D_j f_i$ 在 a 点连续, 则 $Df(a)$ 存在。(这样的函数 f 称为在 a 点连续可微。)



证明 和定理 23.6 的证明一样, 只要考察 $m = 1$ 的情况就够了, 所以 $f: \mathbb{R}^n \rightarrow \mathbb{R}$, 于是

$$\begin{aligned} f(a+h) - f(a) &= f(a_1+h_1, a_2, \dots, a_n) - f(a_1, \dots, a_n) \\ &\quad + f(a_1+h_1, a_2+h_2, a_3, \dots, a_n) \\ &\quad - f(a_1+h_1, a_2, \dots, a_n) + \dots \\ &\quad + f(a_1+h_1, \dots, a_n+h_n) \\ &\quad - f(a_1+h_1, \dots, a_{n-1}+h_{n-1}, a_n). \end{aligned}$$

回想 $D_1 f$ 是由 $g(x) = f(x, a_2, \dots, a_n)$ 定义的函数 g 的导数。对 g 应用中值定理, 便得

$$\begin{aligned} f(a_1+h_1, a_2, \dots, a_n) - f(a_1, \dots, a_n) \\ = h_1 \cdot D_1 f(b_1, a_2, \dots, a_n), \end{aligned}$$

这里 b_1 是 a_1 与 a_1+h_1 间的某数。同样, 在和式中第 i 项等于 (对某 c_i)

$$h_i \cdot D_i f(a_1+h_1, \dots, a_{i-1}+h_{i-1}, b_i, \dots, a_n) = h_i D_i f(c_i).$$

于是,

$$\begin{aligned} \lim_{h \rightarrow 0} \frac{\left| f(a+h) - f(a) - \sum_{i=1}^n D_i f(a) \cdot h_i \right|}{|h|} \\ = \lim_{h \rightarrow 0} \frac{\left| \sum_{i=1}^n [D_i f(c_i) - D_i f(a)] \cdot h_i \right|}{|h|} \\ \leq \lim_{h \rightarrow 0} \sum_{i=1}^n |D_i f(c_i) - D_i f(a)| \cdot \frac{|h_i|}{|h|} \end{aligned}$$

$$\begin{aligned}
&\leq \lim_{h \rightarrow 0} \sum_{i=1}^n |D_i f(c_i) - D_i f(a)| \\
&= 0,
\end{aligned}$$

因为 $D_i f$ 在 a 点连续。

虽然在证明定理23.6时应用了锁链规则,但能容易地把它去掉。对可微函数有定理23.7,对它们的导数有定理23.6,所以锁链规则看来似乎是多余的。但是,它有一个关于偏导数的极端重要的结论。

定理 23.8

设 $g_1, \dots, g_m : \mathbb{R}^n \rightarrow \mathbb{R}$ 在 a 点连续可微, 并设 $f : \mathbb{R}^m \rightarrow \mathbb{R}$ 在 $(g_1(a), \dots, g_m(a))$ 点连续可微。用 $F(x) = f(g_1(x), \dots, g_m(x))$ 定义 $F : \mathbb{R}^n \rightarrow \mathbb{R}$ 。则

$$D_i F(a) = \sum_{j=1}^m D_j f(g_1(a), \dots, g_m(a)) \cdot D_i g_j(a).$$



证明 函数 F

第二十四章 积分

24.1 基本定义

24.2 测度零和容度零

24.3 可积函数

24.4 富比尼定理

第二十四章 习题

1. 设 $D_{1,2}f$ 与 $D_{2,1}f$ 都连续, 应用富比尼定理对 $D_{1,2}f = D_{2,1}f$ 给一简证。提示:

第 二十五 章 链上的积分

第二十六章 流形上的积分

第六部分

多元微积分

《多元微积分》的作者是 C.Goffman。参考：[5]。

第二十七章 欧氏空间

欧氏空间是一个向量空间，它具有满足某些条件的距离函数。在这一章中，我们给出这些空间的定义和主要性质，还要讨论向量空间之间的线性映射及其性质，然后给出欧氏空间拓扑的一个简洁的处理。

27.1 向量空间

实数域 \mathbb{R} 上的向量空间是一个集合 S ，它带有映射

$$g : S \times S \rightarrow S$$

和

$$v : \mathbb{R} \times S \rightarrow S,$$

通常用记号 $g(x, y) = x + y$ 和 $v(a, x) = ax$ 记这两个映射，并假定下列条件成立：

(a) S 对于映射 g 成一 Abel 群。

(b₁) 对于每个 $x \in S$ 和 $a, b \in \mathbb{R}$ ， $(ab)x = a(bx)$ 。

(b₂) 对于每个 $x \in S$ 和 $a, b \in \mathbb{R}$ ， $(a + b)x = ax + bx$ 。

(b₃) 对于每个 $x, y \in S$ 和 $a \in \mathbb{R}$ ， $a(x + y) = ax + ay$ 。

(b₄) 对于每个 $x \in S$ ， $1 \cdot x = x$ 。

我们用记号 θ 记 S 中群的恒等元。容易证明 $0 \cdot x = \theta$ 对每个 $x \in S$ 成立。不难看出，群的逆元是 $(-1)x$ ，记为 $-x$ 。我们把 $y + (-x)$ 写为 $y - x$ 。

我们只给出向量空间的两个例子。

例 27.1 设 S 是 n -实数组的集合。对于

$$x = (x_1, \dots, x_n) \in S,$$

$$y = (y_1, \dots, y_n) \in S,$$

命

$$x + y = (x_1 + y_1, \dots, x_n + y_n).$$

对于

$$x = (x_1, \dots, x_n) \in S$$

和 $a \in \mathbb{R}$ ，命

$$ax = (ax_1, \dots, ax_n).$$

例 27.2 设 A 是任一集合， X 是一向量空间。命 X^A 是 A 到 X 的全体映射所成的集合。对于任意 $f, g \in X^A$ ，定义 $f + g$ 是这样的映射：对于每个 $\alpha \in A$ ，

$$(f + g)(\alpha) = f(\alpha) + g(\alpha).$$

对每个 $f \in X^A$ 和 $a \in \mathbb{R}$, 定义 af 为这样的映射: 对于每个 $\alpha \in A$,

$$(af)(\alpha) = af(\alpha).$$

设 A, B 是两个集合, 映射 $f: A \rightarrow B$ 叫做单射的 (injective), 如果它是一对一的; 叫做满射的 (surjective), 如果它是 A 到整个 B 上的映射; 叫做双射 (bijective), 如果它是 A 到整个 B 上的映射, 而且是一对一的。这就是说, 如果 $x, y \in A$, 只要 $x \neq y$ 就有 $f(x) \neq f(y)$, f 就是单射的; 如果对于每个 $u \in B$, 存在 $x \in A$ (可以多于一个), 使得 $u = f(x)$, f 就是满射的。

设 S, T 是两个向量空间, 映射

$$f: S \rightarrow T$$

叫做一个同态映射, 如果对任意 $x, y \in S$ 有 $f(x+y) = f(x) + f(y)$, 对每个 $x \in S$, $a \in \mathbb{R}$ 有 $f(ax) = af(x)$ 。

同态映射称为同构映射, 如果它是双射的。向量空间 S 和 T 称为同构的, 如果存在一个同构映射 $f: S \rightarrow T$ 。

注意 向量空间之间的同态映射也叫做线性映射。今后我们就采用这后一术语。

设 S 是一向量空间, 子集 $T \subset S$ 称为一个子空间, 如果

第七部分

数学分析

《数学分析》的作者是 Tom.M.Apostol。参考: [6]。

第二十八章 实数系与复数系

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

28.1 引言

28.2 域公理

28.3 序公理

第二十九章 集合论的一些基本概念

第 三十 章 点集拓扑初步

第八部分

单复变函数

《单复变函数》(Functions of One Complex Variable) 的作者是 J.B. 康威 (John B. Conway). 参考: [7].

第三十一章 复数系

31.1 实数

我们用 \mathbb{R} 表示所有实数组成的集. 假定读者熟悉实数系及其性质, 特别地, 假定读者具备下面的知识: \mathbb{R} 的序, 上确界和下确界的定义和性质, 以及 \mathbb{R} 的完备性 (\mathbb{R} 中的每一个有上界的集必有上确界). 我们也假定读者熟知 \mathbb{R} 中的序列的收敛性与无穷级数. 最后, 一个人只有在单变量实函数方面有了坚实的基础之后, 才可以着手学习复变函数. 虽然在学习解析函数理论之前, 传统上是先学习多变数实函数. 但是对于本书来说, 本质上这不是必要的条件, 因为本书中任何地方都不需要这个领域里深入的结果.

31.2 复数域

我们把复数集 \mathbb{C} 定义为所有有序数对 (a, b) 的集, 其中 a, b 是实数. 加法和乘法由下式定义:

$$(a, b) + (c, d) = (a + c, b + d),$$

$$(a, b)(c, d) = (ac - bd, bc + ad).$$

容易验证, 这样定义后, \mathbb{C} 满足域 (field) 的所有公理. 这就是说, \mathbb{C} 满足加法和乘法的结合律、交换律、分配了; $(0, 0)$ 和 $(1, 0)$ 分别是加法和乘法的单位元素, 并且 \mathbb{C} 内的每一个非零元素有加法和乘法的逆元素.

对于复数 $(a, 0)$, 我们将写为 a , 这个映照 $a \mapsto (a, 0)$ 定义了一个 \mathbb{R} 到 \mathbb{C} 的域同构¹, 所以我们可以把 \mathbb{R} 考虑为 \mathbb{C} 的一个子集. 如果令 $i = (0, 1)$, 那么 $(a, b) = a + ib$, 从现在起, 我们对复数就不再使用有序数对的记号了.

注意到 $i^2 = -1$, 所以方程 $z^2 + 1 = 0$ 在 \mathbb{C} 内有根. 事实上, 对于 \mathbb{C} 内的每个 z , $z^2 + 1 = (z + i)(z - i)$. 更一般地, 如果 z 和 w 是复数, 我们得到

$$z^2 + w^2 = (z + iw)(z - iw),$$

令 z 和 w 是实数 a 和 b (a 和 b 都不为 0²), 我们得到

$$\frac{1}{a + bi} = \frac{a - bi}{a^2 + b^2} = \frac{a}{a^2 + b^2} - i\left(\frac{b}{a^2 + b^2}\right),$$

这样我们就有了一个复数的倒数的公式.

当我们写 $z = a + bi$ ($a, b \in \mathbb{R}$) 时, 我们称 a, b 为 z 的实部和虚部, 并且用 $a = \Re z$, $b = \Im z$ 表示.

作为本节的结尾, 我们在 \mathbb{C} 内引进两个运算. 这两个运算不是域的运算. 如果 $z = x + iy$ ($x, y \in \mathbb{R}$), 那么我们定义 $|z| = (x^2 + y^2)^{\frac{1}{2}}$ 为 z 的绝对值, $\bar{z} = x - iy$ 为 z 的共轭

¹这恐怕不能说是同构, 因为明显不是一一映射, 应该是 \mathbb{R} 和 \mathbb{C} 的一个子集同构

²这里只需要 a 和 b 不全为 0 即可.

数. 注意:

$$|z|^2 = z\bar{z}, \quad (31.2.1)$$

特别地, 如果 $z \neq 0$, 那么

$$\frac{1}{z} = \frac{\bar{z}}{|z|^2}.$$

下面是绝对值和共轭数的基本性质, 其证明留给读者.

$$\Re z = \frac{1}{2}(z + \bar{z}), \quad \Im z = \frac{1}{2i}(z - \bar{z}). \quad (31.2.2)$$


$$(z + w) = \bar{z} + \bar{w}, \quad z\bar{w} = \bar{z}w. \quad (31.2.3)$$

$$|zw| = |z||w|. \quad (31.2.4)$$

$$|z/w| = |z|/|w|. \quad (31.2.5)$$


$$|\bar{z}| = |z|. \quad (31.2.6)$$

读者证明后面三个式子的时候, 应当尽量避免将 z 和 w 展开为它们的实部和虚部, 而最好利用 (31.2.1), (31.2.2) 和 (31.2.3).

 **练习 31.1** 求下列各复数的实部和虚部:

$$\frac{1}{z}; \frac{z-a}{z+a} (a \in \mathbb{R}); z^2; \frac{3+5i}{7i+1}; \left(\frac{-1+i\sqrt{3}}{2}\right)^3;$$


$$\left(\frac{-1-i\sqrt{3}}{2}\right)^6; i^n; \left(\frac{1+i}{\sqrt{2}}\right)^n, 2 \leq n \leq 8.$$

 **练习 31.2** 求下列各复数的绝对值和共轭数:

$$-2+i; -3; (2+i)(4+3i); \frac{3-i}{\sqrt{2}+3i}; \frac{i}{i+3};$$

$$(1+i)^6; i^{17}.$$


 **练习 31.3** 证明: 当且仅当 $z = \bar{z}$ 时, z 才是实数.

 **练习 31.4** 若 z 和 w 是复数, 证明下列等式:


$$|z+w|^2 = |z|^2 + 2\Re z\bar{w} + |w|^2$$

$$|z-w|^2 = |z|^2 - 2\Re z\bar{w} + |w|^2$$

$$|z+w|^2 + |z-w|^2 = 2(|z|^2 + |w|^2)$$

 **练习 31.5** 设 $z = z_1 + \cdots + z_n$, $w = w_1 + \cdots + w_n$, 利用归纳法证明:

$$|w| = |w_1| \cdots |w_n|; \bar{z} = \bar{z}_1 + \cdots + \bar{z}_n; \bar{w} = \bar{w}_1 \cdots \bar{w}_n.$$

 **练习 31.6** 设 $R(z)$ 是 z 的有理函数, 如果 $R(z)$ 的所有系数是实数, 则 $\overline{R(z)} = R(\bar{z})$.

31.3 复平面

从复数的定义易见, \mathbb{C} 中每一点 z 都可以和平面 \mathbb{R}^2 上唯一确定的点 $(\Re z, \Im z)$ 相等. 复数的加法恰好就是向量空间 \mathbb{R}^2 的加法, 如果 z 和 w 是 \mathbb{C} 中的点, 那么从 z 和 w 到 $0 (= (0, 0))$ 画两条直线, 这两条直线形成了以 0 、 z 、 w 为三个顶点的平行四边形的两条边, 平行四边形的第四个顶点就是 $z+w$.

注意, $|z - w|$ 恰好是 z 和 w 之间的距离, 理会到这一点, 上节习题31.4中的最后一个等式说的就是平行四边形法则: 平行四边形各边长的平方和等于其对角线的平方和.

距离函数的基本性质是它满足三角不等式 (见下一章). 在这种情况下, 对复数 z_1, z_2, z_3 , 这个不等式变为

$$|z_1 - z_2| \leq |z_1 - z_3| + |z_3 - z_2|.$$

利用 $z_1 - z_2 = (z_1 - z_3) + (z_3 - z_2)$, 容易看出, 我们只需证明

$$|z + w| \leq |z| + |w| \quad (z, w \in \mathbb{C}) \quad (31.3.1)$$

为了证明这个不等式, 首先看出, 对于 \mathbb{C} 中任意 z ,

$$\begin{aligned} -|z| &\leq \Re z \leq |z|, \\ -|z| &\leq \Im z \leq |z|. \end{aligned} \quad (31.3.2)$$

因此, $\Re z\bar{w} \leq |z\bar{w}| = |z||w|$. 于是

$$\begin{aligned} |z + w|^2 &= |z|^2 + 2\Re z\bar{w} + |w|^2 \\ &\leq |z|^2 + 2|z||w| + |w|^2 = (|z| + |w|)^2, \end{aligned}$$

由此推出31.3.1. (这个式子称为三角不等式, 因为如果我们把 z 和 w 表示在平面上, (31.3.1) 式表明, 三角形 $[0, z, z + w]$ 的一边的长度小于另外两边长度的和. 或者说两点间的最短距离是直线). 在遇到一个不等式时, 人们总应当问一问等号成立的必要充分条件是什么, 考察一个三角形并考虑到 (31.3.1) 的几何意义, 我们就引出条件 $z = tw$, 对某一 $t \in \mathbb{R}, t \geq 0$. (或者如果 $w = 0$, 则 $w = tz$). 显然, 当这两点和原点共线时, 等号成立. 事实上, 如果我们看一下 (31.3.1) 式的证明, 便知道 $|z + w| = |z| + |w|$ 成立的必要充分条件是 $|z\bar{w}| = \Re(z\bar{w})$. 这等价于 $z\bar{w} \geq 0$ (即 $z\bar{w}$ 是非负实数). 如果 $w \neq 0$, 两边乘以 w/w , 我们得到 $|w|^2(z/w) \geq 0$, 令

$$t = z/w = \left(\frac{1}{|w|^2}\right)|w|^2(z/w),$$

那么 $z = tw, t \geq 0$.

由归纳法, 我们也有

$$|z_1 + z_2 + \cdots + z_n| \leq |z_1| + |z_2 + \cdots + z_n|, \quad (31.3.3)$$

不等式

$$||z| - |w|| \leq |z - w| \quad (31.3.4)$$

也是有用的.

既然我们给出了绝对值的几何解释, 让我们再来看一看, 平面上一点的共轭复数是什么, 这是容易的, 事实上, \bar{z} 是 z 关于 x 轴 (即实轴) 的对称点.

练习 31.7 证明 (31.3.4) 并给出等号成立的必要充分条件.

练习 31.8 证明: (31.3.2) 中的等号成立, 当且仅当, 对任意整数 k 和 $l, 1 \leq k, l \leq n$, 只要 $z_l \neq 0$, 就有 $z_k/z_l \leq 0$.

练习 31.9 设 $a \in \mathbb{R}, c > 0$ 是固定的. 对于每个可能选取的 a 和 c , 试描画出满足条件

$$|z - a| - |z + a| = 2c$$

的点集. 现在设 a 为任意复数, 利用平面的旋转画出满足上述方程的点的轨迹.

31.4 复数的极坐标表示与复数的方根

考虑复平面 \mathbb{C} 的点 $z = x + iy$. 这个点有极坐标 (r, θ) : $x = r \cos \theta$, $y = r \sin \theta$. 显然 $r = |z|$, θ 是正实轴与从 0 到 z 的直线段的夹角. 注意, 在上述等式中的 θ 可以代之以 θ 加上 2π 的任意整数倍, 角 θ 称为 z 的幅 (还是这个“辐”) 角, 记为 $\theta = \arg z$. 由于 θ 的不确定性, “arg” 不是一个函数. 我们引进记号

$$\operatorname{cis} \theta = \cos \theta + i \sin \theta. \quad (31.4.1)$$

设 $z_1 = r_1 \operatorname{cis} \theta_1$, $z_2 = r_2 \operatorname{cis} \theta_2$, 那么

$$\begin{aligned} z_1 z_2 &= r_1 r_2 \operatorname{cis} \theta_1 \operatorname{cis} \theta_2 = r_1 r_2 [(\cos \theta_1 \cos \theta_2 - \sin \theta_1 \sin \theta_2) \\ &\quad + i(\sin \theta_1 \cos \theta_2 + \sin \theta_2 \cos \theta_1)] \end{aligned}$$

由正弦和余弦的和角公式, 我们得到

$$z_1 z_2 = r_1 r_2 \operatorname{cis} (\theta_1 + \theta_2). \quad (31.4.2)$$

换句话说 $\arg z_1 z_2 = \arg z_1 + \arg z_2$ (什么实函数把成绩变为和? ³). 由归纳法, 对于 $z_k = r_k \operatorname{cis} \theta_k$, $1 \leq k \leq n$, 我们有

$$z_1 z_2 \cdots z_n = r_1 r_2 \cdots r_n \operatorname{cis} (\theta_1 + \theta_2 + \cdots + \theta_n). \quad (31.4.3)$$

特别地, 对于每个整数 $n \geq 0$, 有

$$z^n = r^n \operatorname{cis} (n\theta). \quad (31.4.4)$$

进而若 $z \neq 0$, 则 $z[r^{-1} \operatorname{cis} (-\theta)] = 1$; 所以如果 $z \neq 0$, 那么对于一切整数 n , 正的, 负的, 或 0, (31.4.4) 也成立. 作为 (31.4.4) 的一个特别情形, 我们得到棣莫佛 (de Moivre) 公式:

$$(\cos \theta + i \sin \theta)^n = \cos n\theta + i \sin n\theta.$$

现在我们可以来考虑下面的问题了. 对于给定的一个复数 $a \neq 0$, 和一个整数 $n \geq 2$, 你能否找到满足 $z^n = a$ 的数 z ? 这样的 z 你能找到多少个? 由于 (31.4.4) 式, 解答这个问题是容易的. 设 $a = |a| \operatorname{cis} \alpha$; 由 (31.4.4), $z = |a|^{\frac{1}{n}} \operatorname{cis} (\alpha/n)$ 就满足要求. 但是这个解不是唯一解, 因为 $z' = |a|^{\frac{1}{n}} \operatorname{cis} \frac{1}{n}(\alpha + 2\pi)$ 也满足 $(z')^n = a$. 事实上, 每一个数

$$|a|^{\frac{1}{n}} \operatorname{cis} \frac{1}{n}(\alpha + 2\pi k), \quad 0 \leq k \leq n-1. \quad (31.4.5)$$

都是 a 的 n 次方根. 借助 (31.4.4) 我们得到下述结果: 对于 \mathbb{C} 中的每一个不等于零的数 a , 都有 a 的 n 个不同的 n 次方根, 它们由公式 (31.4.5) 给出.

例子 计算 n 次单位根. 由于 $1 = \operatorname{cis} 0$, (31.4.5) 式给出如下这些根:

$$1, \operatorname{cis} \frac{2\pi}{n}, \operatorname{cis} \frac{4\pi}{n}, \dots, \operatorname{cis} \frac{2\pi}{n}(n-1).$$

³对数函数 $\ln(ab) = \ln a + \ln b$


特别地, 立方单位根是

$$1, \frac{1}{2}(-1 + i\sqrt{3}), \frac{1}{2}(-1 - i\sqrt{3}).$$

 **练习 31.10** 求出 6 次单位根.

 **练习 31.11** 计算:

- (a) i 的平方根;
- (b) i 的立方根;
- (c) $\sqrt{3} + 3i$ 的平方根.

 **练习 31.12** n 次单位原根是一复数 a , 使得 $1, a, a^2, \dots, a^{n-1}$ 是 n 个不同的 n 次单位根. 证明: 如果 a, b 分别是 n 次和 m 次单位原根, 则 ab 是 k 次单位根, k 是某一整数. k 的最小值是什么? 如果 a, b 是非单位原根, 你能说些什么?


 **练习 31.13** 试利用二项式


$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k,$$


其中 $\binom{n}{k} = \frac{n!}{k!(n-k)!}$, 并比较棣莫佛公式两边的实部和虚部, 得到公式

$$\cos n\theta = \cos^n \theta - \binom{n}{2} \cos^{n-2} \theta \sin^2 \theta + \binom{n}{4} \cos^{n-4} \theta \sin^4 \theta - \dots$$

$$\sin n\theta = \binom{n}{1} \cos^{n-1} \theta \sin \theta - \binom{n}{3} \cos^{n-3} \theta \sin^3 \theta + \dots$$

 **练习 31.14** 设 $z = \operatorname{cis} \frac{2\pi}{n}$, 整数 $n \geq 2$. 证明: $1 + z + \dots + z^{n-1} = 0$.

 **练习 31.15** 证明: $\phi(t) = \operatorname{cis} t$ 是加法群 \mathbb{R} 到乘法群 $T = \{z : |z| = 1\}$ 上的群同态.

 **练习 31.16** 如果 $z \in \mathbb{C}$, 并且对于每个正整数 n , $\Re z^n \geq 0$, 证明: z 是正实数.

31.5 复平面上的直线和半平面

设 L 表示 \mathbb{C} 中的直线. 从初等解析几何知道, L 是由 L 上的一个点和一个方向向量决定的. 于是, 如果 a 是 L 上任一点, b 是它的方向向量, 那么

$$L = \{z = a + tb : -\infty < t < \infty\}.$$

由于 $b \neq 0$, 这就给出, 对于 L 上的 z , 有

$$\Im\left(\frac{z-a}{b}\right) = 0.$$

事实上, 如果 z 满足等式

$$0 = \Im\left(\frac{z-a}{b}\right),$$

那么

$$t = \frac{z-a}{b},$$

蕴含 $z = a + tb$, $-\infty < t < \infty$. 这就是说

$$L = \left\{z : \Im\left(\frac{z-a}{b}\right) = 0\right\}. \quad (31.5.1)$$

集合

$$\begin{aligned} &\{z : \Im(\frac{z-a}{b}) > 0\}, \\ &\{z : \Im(\frac{z-a}{b}) < 0\}. \end{aligned}$$


的轨迹是什么呢? 作为回答这个问题的第一步, 注意到 b 是一个方向, 我们可以假定 $|b| = 1$. 我们暂时考虑 $a = 0$ 的情形. 并且令 $H_0 = \{z : \Im(z/b) > 0\}$, $b = \operatorname{cis} \beta$. 如果 $z = r \operatorname{cis} \theta$, 那么 $z/b = r \operatorname{cis}(\theta - \beta)$. 于是 z 在 H_0 中, 当且仅当 $\sin(\theta - \beta) > 0$, 即 $\beta < \theta < \pi + \beta$. 所以, 如果我们“按照 b 的方向沿着 L 前进”, H_0 是位于 L 左边的半平面. 如果我们令

$$H_a = \{z : \Im(\frac{z-a}{b}) > 0\},$$

那么容易看出, $H_a = a + H_0 \equiv \{a + w : w \in H_0\}$; 即 H_a 是由 H_0 平移 a 而得到的, 因此, H_a 是位于 L 的左边的半平面. 类似地,

$$K_a = \{z : \Im(\frac{z-a}{b}) < 0\}$$

是位于 L 的右边的半平面.

 **练习 31.17** 设 C 是圆周 $\{z : |z - c| = r\}$, $r > 0$, $a = c + r \operatorname{cis} \alpha$; 并且令

$$L_\beta = \{z : \Im(\frac{z-a}{b}) = 0\},$$

其中 $b = \operatorname{cis} \beta$. 找出 L_β 在 a 处切于圆周 C 的关于 β 的充分必要条件.

31.6 扩充平面及其球面表示

在复分析中, 我们常常涉及到这样一些函数, 当自变量趋于给定点时, 它们趋于无穷. 为了讨论这种情形, 我们引进扩充平面 $\mathbb{C}_\infty \equiv \mathbb{C} \cup \{\infty\}$. 同时为了讨论到取到无穷作为它的值的函数的连续性. 我们也希望在 \mathbb{C}_∞ 内引进距离函数. 为了这个目的以及为了给出 \mathbb{C}_∞ 的具体图像, 我们把 \mathbb{C}_∞ 表示为 \mathbb{R}^3 中的单位球面

$$S = \{(x_1, x_2, x_3) \in \mathbb{R}^3 : x_1^2 + x_2^2 + x_3^2 = 1\}.$$

设 $N = (0, 0, 1)$; 即 N 是 S 上的北极. 同时, 把 \mathbb{C} 等同于 $\{(x_1, x_2, 0) : x_1, x_2 \in \mathbb{R}\}$, 于是 \mathbb{C} 沿赤道切割 S . 现在对于 \mathbb{C} 中每个点 z , 考虑 \mathbb{R}^3 中通过 z 和 N 的直线. 这条直线与球面恰好交于一点 $Z \neq N$. 如果 $|z| > 1$, 那么 Z 在北半球面上; 如果 $|z| < 1$, 那么 Z 在南半球面上; 如果 $|z| = 1$, 那么 $Z = z$. 当 $|z| \rightarrow \infty$ 时, Z 怎样呢? 很清楚, Z 趋于 N . 因此, 我们就把 N 与 \mathbb{C}_∞ 中的 ∞ 等同起来. 这样一来, \mathbb{C}_∞ 就被表示为球面 S 了.

让我们来考察这种表示法. 令 $z = x + iy$, 设 $Z = (x_1, x_2, x_3)$ 是 S 上相应的点, 我们要找出用 x, y 表示 x_1, x_2, x_3 的方程. 在 \mathbb{R}^3 中通过 z 和 N 的直线由 $\{tN + (1-t)z : -\infty < t < \infty\}$ 或

$$\{((1-t)x, (1-t)y, t) : -\infty < t < \infty\} \quad (31.6.1)$$

给出. 因此, 如果能够找到直线和 S 的交点的 t 值, 我们就能够找到 Z 的坐标. 如果 t 是这个值, 那么

$$1 = (1-t)^2 x^2 + (1-t)^2 y^2 + t^2 = (1-t)^2 |z|^2 + t^2.$$

由此注意到

$$1 - t^2 = (1 - t)^2 |z|^2.$$

因为 $t \neq 1$ ($z \neq \infty$), 所以

$$t = \frac{|z|^2 - 1}{|z|^2 + 1}.$$

于是

$$x_1 = \frac{2x}{|z|^2 + 1}, x_2 = \frac{2y}{|z|^2 + 1}, x_3 = \frac{|z|^2 - 1}{|z|^2 + 1}. \quad (31.6.2)$$

这就给出

$$x_1 = \frac{z + \bar{z}}{|z|^2 + 1}, x_2 = \frac{-i(z - \bar{z})}{|z|^2 + 1}, x_3 = \frac{|z|^2 - 1}{|z|^2 + 1}. \quad (31.6.3)$$

如果 Z 是给定的 ($Z \neq N$), 我们希望找 z . 这时, 通过令 $t = x_3$ 并利用 (31.6.1), 我们得到

$$z = \frac{x_1 + ix_2}{1 - x_3} \quad (31.6.4)$$

现在让我们用下面的方式定义扩充平面上点之间的距离函数: 对于 \mathbb{C}_∞ 中的 z, z' , 定义 z 到 z' 的距离 $d(z, z')$ 为它们在 \mathbb{R}^3 中相应两点 Z 和 Z' 的距离. 如果 $Z = (x_1, x_2, x_3)$, $Z' = (x'_1, x'_2, x'_3)$, 那么

$$d(z, z') = [(x_1 - x'_1)^2 + (x_2 - x'_2)^2 + (x_3 - x'_3)^2]^{\frac{1}{2}}. \quad (31.6.5)$$

利用 Z 和 Z' 在 S 上这一事实, (31.6.5) 给出

$$[d(z, z')]^2 = 2 - 2(x_1 x'_1 + x_2 x'_2 + x_3 x'_3). \quad (31.6.6)$$

由 (31.6.3), 我们得到


$$d(z, z') = \frac{2|z - z'|}{[(1 + |z|^2)(1 + |z'|^2)]^{\frac{1}{2}}}, \quad (z, z' \in \mathbb{C}). \quad (31.6.7)$$


用类似的方法, 对于 \mathbb{C} 中的 z , 我们得到


$$d(z, \infty) = \frac{2}{(1 + |z|^2)^{\frac{1}{2}}}, \quad (31.6.8)$$

球面 S 和 \mathbb{C}_∞ 的点之间这种对应关系称为球极平面投影.

 **练习 31.18** 给出 (31.6.7) 和 (31.6.8) 的详细推导.


 **练习 31.19** 对于下列 \mathbb{C} 中的点给出 S 上对应的点: $0, 1 + i, 3 + 2i$.

 **练习 31.20** S 上哪些子集对应 \mathbb{C} 中的实轴和虚轴.

 **练习 31.21** 设 Λ 是 S 上的一个圆周, 那么在 \mathbb{R}^3 中有唯一的平面 P , 使得 $P \cap S = \Lambda$. 由解析几何知道

$$P = \{(x_1, x_2, x_3) : x_1 \beta_1 + x_2 \beta_2 + x_3 \beta_3 = l\},$$

其中 $(\beta_1, \beta_2, \beta_3)$ 是与 P 正交的一个向量, l 是某一实数. 可以假设 $\beta_1^2 + \beta_2^2 + \beta_3^2 = 1$. 利用这一事实, 证明: 如果 Λ 包含点 N , 则它在 \mathbb{C} 上的投影是一直线. 否则, Λ 投影到 \mathbb{C} 中的一个圆周上.

 **练习 31.22** 设 Z 和 Z' 是 S 上分别与 z 和 z' 相应的两点. W 是 S 上与 $z + z'$ 对应的点. 试用 Z 和 Z' 的坐标表示出 W 的坐标.

第三十二章 度量空间与 \mathbb{C} 的拓扑

32.1 度量空间的定义和例子

一个度量空间是一个序偶 (X, d) , 这里 X 是一个集, d 是一个从 $X \times X$ 到 \mathbb{R} 的函数, 称之为距离函数或度量, 它满足下列条件:

$$d(x, y) \geq 0;$$

当且仅当 $x = y$ 时, $d(x, y) = 0$;

$$d(x, y) = d(y, x) \quad (\text{对称性});$$

$$d(x, z) \leq d(x, y) + d(y, z) \quad (\text{三角不等式}).$$

如果 x 和 $r > 0$ 是固定的, 那么定义

$$B(x; r) = \{y \in X : d(x, y) < r\},$$

$$\bar{B}(x; r) = \{y \in X : d(x, y) \leq r\}.$$

$B(x; r)$ 和 $\bar{B}(x; r)$ 分别称为以 x 为中心, r 为半径的开球和闭球.

例子

例 32.1 设 $X = \mathbb{R}$ 或 \mathbb{C} , 定义 $d(z, w) = |z - w|$, 这就使 (\mathbb{R}, d) 和 (\mathbb{C}, d) 都成为度量空间. 事实上, (\mathbb{C}, d) 将是我们最感兴趣的例子. 如果读者在此以前从来未接触过度量空间的概念, 那么在学习这一章的过程中应当时常想到 (\mathbb{C}, d) .

例 32.2 设 (X, d) 是一个度量空间, $Y \subset X$; 那么 (Y, d) 也是一个度量空间.

例 32.3 设 $X = \mathbb{C}$, 定义 $d(x + iy, a + ib) = |x - a| + |y - b|$. 那么 (\mathbb{C}, d) 是一个度量空间.

例 32.4 设 $X = \mathbb{C}$, 定义 $d(x + iy, a + ib) = \max |x - a|, |y - b|$.

例 32.5 设 X 是任意一个集, 定义 $d(x, y) = 0$, 如果 $x = y$; $d(x, y) = 1$, 如果 $x \neq y$. 为了证明函数 d 满足三角不等式, 只要考虑在 x, y, z 当中出现相等的各种可能情形. 注意, 如果 $r \leq 1$, 则 $B(x; r)$ 只由一个点 x 所组成; 如果 $r > 1$, 则 $B(x; r) = X$. 这个度量空间在解析函数论的研究中并不出现.

例 32.6 设 $X = \mathbb{R}^n$, 对于 \mathbb{R}^n 中的 $x = (x_1, \dots, x_n)$ 和 $y = (y_1, \dots, y_n)$ 定义

$$d(x, y) = \left[\sum_{j=1}^n (x_j - y_j)^2 \right]^{\frac{1}{2}}.$$

例 32.7 设 S 是任意一个集, $B(S)$ 表示满足条件

$$\|f\|_{\infty} = \sup \{|f(s)| : s \in S\} < \infty$$

的函数 $f : S \rightarrow \mathbb{C}$ 的集. 这就是说, $B(S)$ 由所有其值域位于某一有穷半径的圆内的复值函数所构成. 对于 $B(S)$ 中的 f 和 g 定义 $d(f, g) = \|f - g\|_{\infty}$. 我们来证明 d 满足三角不等式. 事实上, 如果 f, g 和 h 在 $B(S)$ 中, s 是 S 中的任意一点, 那么 $|f(s) - g(s)| = |f(s) - h(s) + h(s) - g(s)| \leq |f(s) - h(s)| + |h(s) - g(s)| \leq \|f - h\|_{\infty} + \|h - g\|_{\infty}$. 于是若对于 S 中所有的 s 取上确界, 则有 $\|f - g\|_{\infty} \leq \|f - h\|_{\infty} + \|h - g\|_{\infty}$, 这就是对于 d

的三角不等式.

定义 32.1. 开集

对于度量空间 (X, d) , 一个集 $G \subset X$ 是开集, 如果 G 内的每一个 x , 都存在一个 $\epsilon > 0$, 使得 $B(x; \epsilon) \subset G$.



于是, 一个集在 \mathbb{C} 内是开的, 如果它没有“边”. 例如,

$$G = \{z \in \mathbb{C} : a < \Re(z) < b\}$$

是开的; 但是 $\{z : \Re(z) < 0\} \cap \{0\}$ 不是开的, 因为不管我们把 ϵ 取得多么小, $B(0; \epsilon)$ 都不能包含在这个集内.

我们用 \emptyset 表示空集, 就是一个元素也没有的集.

命题 32.1

设 (X, d) 是一个度量空间, 那么:

- (a) 集 X 和 \emptyset 是开集.
- (b) 如果 G_1, \dots, G_n 是 X 中的开集, 则 $\bigcap_{k=1}^n G_k$ 也是 X 中的开集.
- (c) 如果 $\{G_j : j \in J\}$ 是 X 中的开集族, J 是任一指标集, 则 $G = \bigcup \{G_j : j \in J\}$ 也是开集.



证明 (a) 的证明是平凡的. 为了证明 (b), 设 $x \in G = \bigcap_{k=1}^n G_k$; 那么 $x \in G_k$, $k = 1, 2, \dots, n$. 于是由定义, 对于每个 k 有 $\epsilon_k > 0$, 使得 $B(x; \epsilon_k) \subset G_k$. 如果取 $\epsilon = \min(\epsilon_1, \epsilon_2, \dots, \epsilon_n)$, 那么, 对于 $1 \leq k \leq n$, $B(x; \epsilon) \subset B(x; \epsilon_k) \subset G_k$, 于是 $B(x; \epsilon) \subset G$, G 是开集.

(c) 的证明留给读者作为习题.

在度量空间里还有另一类著名的子集. 这类子集包含它们的全部“边”, 换一个说法, 它们的余集没有“边”.

定义 32.2. 闭集

一个集 $F \subset X$ 是闭的, 如果它的余集 $X - F$ 是开的.



下面的命题是命题32.1的补命题. 对于前一命题应用 Morgan 法则便可完成其证明, 我们把它留给读者.

命题 32.2

设 (X, d) 是一个度量空间, 那么:

- (a) 集 X 和 \emptyset 是闭的.
- (b) 如果 F_1, \dots, F_n 是 X 中的闭集, 则 $\bigcup_{k=1}^n F_k$ 也是 X 中的闭集.
- (c) 如果 $\{F_j : j \in J\}$ 是 X 中的闭集族, J 是任一指标集, 则 $F = \bigcap \{F_j : j \in J\}$ 也是闭集.



在学习开集和闭集时, 最普遍的错误是把闭集的定义解释为一个集不是开集便是闭集. 这种理解当然是错误的. 只要看集 $\{z \in \mathbb{C} : \Re(z) > 0\} \cup \{0\}$ 就清楚了, 这个集既不是

开的,也不是闭的.

定义 32.3

设 A 是 X 的子集, 那么, A 的内部 $\text{int } A$ 就是集合 $\bigcup\{G : G \text{ 是开集, 且 } G \subset A\}$. A 的闭包 A^- 就是集 $\bigcap\{F : F \text{ 是闭集, 且 } F \supset A\}$. 注意, $\text{int } A$ 可以是空集, A^- 可以是 X . 如果 $A = \{a + ib : a \text{ 和 } b \text{ 是有理数}\}$, 那么同时有 $A^- = \mathbb{C}$ 和 $\text{int } A = \emptyset$. 根据命题 32.1 和 32.2, A^- 是闭集, $\text{int } A$ 是开集. A 的边界记为 ∂A , 定义为 $\partial A = A^- \cap (X - A)^-$.



命题 32.3

设 A 和 B 是度量空间 (X, d) 的子集, 那么:

- (a) 当且仅当 $A = \text{int } A$ 时 A 是开集.
- (b) 当且仅当 $A = A^-$ 时 A 是闭集.
- (c) $\text{int } A = X - (X - A)^-$; $A^- = X - \text{int}(X - A)$; $\partial A = A^- - \text{int } A$.
- (d) $(A \cup B)^- = A^- \cup B^-$.
- (e) 当且仅当存在 $\epsilon > 0$, 使得 $B(x_0; \epsilon) \subset A$ 时, $x_0 \in \text{int } A$.
- (f) 当且仅当, 对每一 $\epsilon > 0$, $B(x_0; \epsilon) \cap A \neq \emptyset$ 时, $x_0 \in A^-$.



证明 (a) 至 (e) 的证明留给读者. 为了证明 (f), 假设 $x_0 \in A^- = X - \text{int}(X - A)$; 于是, $x_0 \notin \text{int}(X - A)$. 由 (e), 对于每一 $\epsilon > 0$, $B(x_0; \epsilon)$ 不包含在 $X - A$ 内, 这就是说, 存在一个点 $y \in B(x_0; \epsilon)$, y 不在 $X - A$ 内. 所以 $y \in B(x_0; \epsilon) \cap A$. 现在设 $x_0 \notin A^- = X - \text{int}(X - A)$, 那么 $x_0 \in \text{int}(X - A)$, 由 (e), 存在 $\epsilon > 0$, 使得 $B(x_0; \epsilon) \subset X - A$. 即 $B(x_0; \epsilon) \cap A = \emptyset$, 所以 x_0 不满足条件.

最后, 再定义一类著名的集合.

定义 32.4. 稠密

度量空间 X 的一个子集 A 是稠密的, 如果 $A^- = X$.



有理数集 \mathbb{Q} 在 \mathbb{R} 中是稠密的, $\{x + iy : x, y, \in \mathbb{Q}\}$ 在 \mathbb{C} 中是稠密的.

练习 32.1 证明: (32.2) 至 (32.6) 中给出的那些例子都确实是度量空间, 只有例子 (32.6) 的证明可能会有些困难, 对于这些例子给出 $B(x; r)$.

练习 32.2 \mathbb{C} 的下列子集, 哪些是开集, 哪些是闭集?

- (a) $\{z : |z| < 1\}$;
- (b) 实轴;
- (c) $\{z : z^n = 1, \text{ 对某一整数 } n \geq 1\}$;
- (d) $\{z \in \mathbb{C} : z \text{ 是实数, 且 } 0 \leq z < 1\}$;
- (e) $\{z \in \mathbb{C} : z \text{ 是实数, 且 } 0 \leq z \leq 1\}$.

- 练习 32.3 如果 (X, d) 是任一度量空间, 证明: 每一个开球是开集, 每一个闭球是闭集.
- 练习 32.4 给出 (32.1c) 的详细证明.
- 练习 32.5 证明命题 32.2.
- 练习 32.6 证明: 一个集 $G \subset X$ 是开的, 当且仅当 $X - G$ 是闭的.
- 练习 32.7 证明: (\mathbb{C}_∞, d) 是一度量空间, 其中 d 是由第一章的 (31.6.7), (31.6.8) 给出的.
- 练习 32.8 设 (X, d) 是一度量空间, $Y \subset X$, 又设 $G \subset X$ 是开的, 证明 $G \cap Y$ 是 (Y, d) 中的开集. 反之, 如果 $G_1 \subset Y$ 是 (Y, d) 中的开集, 则存在开集 $G \subset X$, 使得 $G_1 = G \cap Y$.
- 练习 32.9 在上题中用“闭的”代替“开的”.
- 练习 32.10 证明命题 32.3
- 练习 32.11 证明: $\{\operatorname{cis} k : k \geq 0\}$ 在 $T = \{z \in \mathbb{C} : |z| = 1\}$ 中是稠密的. 对于哪些 θ 的值, $\{\operatorname{cis}(k\theta) : k > 0\}$ 在 T 中是稠密的?

32.2 连通性

作为这一节的开始, 让我们先给出一个例子. 设 $X = \{x \in \mathbb{C} : |z| \leq 1\} \cup \{z : |z - 3| < 1\}$, 并且把 \mathbb{C} 的度量赋于 X (今后, 当我们把 \mathbb{R} 或 \mathbb{C} 的子集 X 看作一个度量空间时, 如果不作相反的声明, 总假定 X 继承度量 $d(z, w) = |z - w|$), 那么集合 $A = \{z : |z| \leq 1\}$ 既是开的, 又是闭的. 它是闭的, 因为它在 X 中的余集 $B = X - A = \{z : |z - 3| < 1\}$ 是开的; A 是开的, 因为如果 $a \in A$, 那么 $B(a; 1) \subset A$ (注意: $\{z \in \mathbb{C} : |z - a| < 1\}$ 并不总包含在 A 中, 当 $a = 1$ 时就是一例. 但当按定义, $B(a; 1)$ 是 $z \in X : |z - a| < 1$, 它是包含在 A 中的). 类似的, B 在 X 中也是既开又闭的.

这是一个非连通空间的例子.

定义 32.5. 连通

一个度量空间 (X, d) 是连通的, 如果只有 \emptyset 和 X 既是开的又是闭的. 设 $A \subset X$, 如果度量空间 (A, d) 是连通的, 那么 A 是 X 的连通子集.

连通性的一个等价说法是: X 是不连通的, 如果存在 X 中的互不相交的非空开集 A 和 B , 使得 $X = A \cup B$. 事实上, 如果这个条件成立, 那么 $A = X - B$ 也是闭的.

命题 32.4

一个集 $X \subset \mathbb{R}$ 是连通的, 当且仅当 X 是一个区间.

证明 设 $X = [a, b]$, a, b 是 \mathbb{R} 的元素. 设 $A \subset X$ 是 X 的开子集, 满足 $a \in A$, $A \neq X$. 我们将证明 A 不可能也是闭的, 因此 X 必是连通的. 因为 A 是开的, $a \in A$, 所以存在 $\epsilon > 0$, 使得 $[a, a + \epsilon) \subset A$, 设

$$r = \sup\{\epsilon : [a, a + \epsilon) \subset A\}.$$

则有断言: $[a, a + r) \subset A$. 事实上, 如果 $a \leq x < a + r$, 令 $h = a + r - x > 0$, 由上确界的定义, 存在 ϵ , $r - h < \epsilon < r$ 且 $[a, a + \epsilon) \subset A$. 但是 $a \leq x = a + (r - h) < a + \epsilon$ 蕴含 $x \in A$. 断言得证.

但是 $a+r \notin A^1$, 因为在相反的情形, $a+r \in A$, 那么由于 A 是开的, 存在 $\delta > 0$, 使得 $[a+r, a+r+\delta) \subset A$. 但这就给出 $[a, a+r+\delta) \subset A$. 这与 r 的定义相矛盾. 现在假定 A 也是闭的, 那么 $a+r \in B = X - A$, B 是开的, 因此我们可以找到 $\delta > 0$, 使得 $(a+r-\delta, a+r] \subset B$. 这和上述断言矛盾.

其他类型的区间的连通性的证明是类似的, 留给读者作为习题.

\mathbb{R} 中的连通集必是一区间, 其证明留做习题.

如果 w 和 z 是 \mathbb{C} 中的两点, 那么我们用

$$[z, w] = \{tw + (1-t)z : 0 \leq t \leq 1\}$$

表示从 z 到 w 的直线段, 从 a 到 b 的折线是集 $P = \bigcup_{k=1}^n [z_k, w_k]$. 其中 $z_1 = a, w_n = b$, 并且对于 $1 \leq k \leq n-1, w_k = z_{k+1}$; 或者写成 $P = [a, z_1, \dots, z_n, b]$.

定理 32.1

一个开集 $G \subset \mathbb{C}$ 是连通的, 当且仅当, 对于 G 的任意两点 a, b , 存在一条从 a 到 b 的折线, 这一折线整个地位于 G 内.



证明 设 G 满足定理的条件, 假定 G 不是连通的, 我们将得到一个矛盾. 由定义, $G = A \cup B$, 其中 A, B 既是开集又是闭集, 且 $A \cap B = \emptyset$, A, B 都是非空的, 设 $a \in A, b \in B$; 按照假定, 存在从 a 到 b 的一条折线 $P, P \subset G$. 稍加考虑, 便可看出, 在组成 P 的某一线段上, 有一点在 A 内, 而另一点在 B 内, 所以我们可以假定 $P = [a, b]$. 我们定义

$$S = \{s \in [0, 1] : sb + (1-s)a \in A\},$$

$$T = \{t \in [0, 1] : tb + (1-t)a \in B\}.$$

那么, $S \cap T = \emptyset, S \cup T = [0, 1], 0 \in S, 1 \in T$. 但是能够证明 S 和 T 都是开集 (习题 32.13), 这就和 $[0, 1]$ 的连通性矛盾. 于是 G 一定是连通的.

现在设 G 是连通的, 并且在 G 内固定一点 a , 要指出如何构造从 a 到 b 的折线 (在 G 内!) 是困难的, 但是我们并不需要实现这种构造, 而只要证明这一折线是存在的. 对于 G 内固定的一点 a , 定义

$$A = \{b \in G : \text{存在 } a \text{ 到 } b \text{ 的折线 } P \subset G\}.$$

我们要证明 A 在 G 内既是开的又是闭的. 由于 $a \in A$ 和 G 是连通的, 所以 $A = G$, 定理便得证.

为了证明 A 是开的, 设 $b \in A, P = [a, z_1, \dots, z_n, b]$ 是从 a 到 b 的折线, $P \subset G$. 由于 G 是开的 (这对于定理的前半部分并不需要), 存在 $\epsilon > 0$, 使得 $B(b; \epsilon) \subset G$, 但是如果 $z \in B(b; \epsilon)$, 那么 $[b, z] \subset B(b; \epsilon) \subset G$, 因此, $Q = P \cup [b, z]$ 是 G 内从 a 到 z 的折线, 这就表明 $B(b; \epsilon) \subset A$, 所以 A 是开的.

为了证明 A 是闭的, 假设在 $G - A$ 内有一点 z , 及 $\epsilon > 0$ 使得 $B(z; \epsilon) \subset G$. 如果 $A \cap B(z; \epsilon)$ 内存在一点 b , 那么如上所述, 我们能够构造一条从 a 到 z 的折线. 于是我们必有 $B(z; \epsilon) \cap A = \emptyset$, 或者 $B(z; \epsilon) \subset G - A$. 即 $G - A$ 是开的, 所以 A 是闭的.

¹这里有两种可能: (1) $a+r = b$; (2) $a+r < b$. 当 $a+r = b$ 时, $a+r \in A$ 导致 $A = X$, 与原来的假定 $A \neq X$ 矛盾; 作者忽略了这种情况.

推论 32.1

如果 $G \subset \mathbb{C}$ 是开的, 连通的, a, b 是 G 内的点, 那么在 G 内存在一条从 a 到 b 的折线, 这一折线由平行于实轴和平行于虚轴的线段所组成.



证明 证明这个推论的方法有两个. 一个方法是先在 G 内求得一条从 a 到 b 的折线. 然后修改其每一线段, 使得新的折线具有所要的性质. 利用紧性比较容易实现这个证明 (见本章 32.5 节习题 32.37). 另一个证明可以由修改定理 32.1 的证明而得到. 和定理 32.1 的证明一样, 定义集 A , 但附加一个限制, 就是折线的线段都平行于一个坐标轴. 往下的证明仍然有效, 只有一点例外, 就是如果 $z \in B(b; \epsilon)$, 那么 $[b, z]$ 可能不平行于坐标轴, 但是容易看出, 如果 $z = x + iy, b = p + iq$, 那么折线 $[b, p + iy] \cup [p + iy, z] \subset B(b; \epsilon)$, 且它的线段平行于坐标轴.

现在我们将证明, 度量空间的任意一个集可以用典型的方法表示为连通块的和.

定义 32.6

度量空间 X 的子集 D 是 X 的一个分支, 如果它是 X 的最大连通子集. 即 D 是连通的, 并且不存在 X 的连通子集, D 是它的真子集.



如果读者考察这一节一开始给出的例子, 就会发现 A, B 都是分支. 并且 X 只有这两个分支. 作为另一个例子, 设 $X = \{0, 1, \frac{1}{2}, \frac{1}{3}, \dots\}$, 这时显然 X 的每一个分支都是一个点, 并且它的每一个点都是一个分支. 注意, 分支 $\{\frac{1}{n}\}$ 都是 X 中的开集, 分支 $\{0\}$ 不是 X 中的开集.

引理 32.1

设 $x_0 \in X, \{D_j : j \in J\}$ 是 X 的连通子集族, 对于 J 中的每一个 $j, x_0 \in D_j$. 则 $D = \bigcup \{D_j : j \in J\}$ 是连通的.



证明 设 A 是度量空间 (D, d) 的子集, 它既是开的又是闭的, 且设 $A \neq \emptyset$. 那么对于每个 $j, A \cap D_j$ 是 (D_j, d) 中的开集, 也是 (D_j, d) 中的闭集 (见 ?? 节中的习题 32.8 和习题 32.9). 由于 D_j 是连通的, 所以, 或者 $A \cap D_j = \emptyset$, 或者 $A \cap D_j = D_j$. 因为 $A \neq \emptyset$, 所以至少存在一个 k , 使得 $A \cap D_k \neq \emptyset$; 因此 $A \cap D_k = D_k$, 特别地, $x_0 \in A$. 所以, 对于每个 $j, x_0 \in A \cap D_j$, 于是对于每个 $j, A \cap D_j = D_j$, 或者说 $D_j \subset A$. 这就得到 $D = A$, 所以 D 是连通的.

定理 32.2

设 (X, d) 是一个度量空间, 则

- (a) X 中的每一个 x_0 包含在 X 的一分支中;
- (b) X 的不同分支是互不相交的.



注意, (a) 表示 X 是它的分支的和.

证明 (a) 设 \mathcal{D} 是包含 x_0 的 X 的连通子集族. 注意到 $\{x_0\} \in \mathcal{D}$, 所以 $\mathcal{D} \neq \emptyset$. 也注意到上述引理的假设适用于族 \mathcal{D} , 因此 $C = \bigcup \{D; D \in \mathcal{D}\}$ 是连通的, 且 $x_0 \in C$. C 必定是一个分支. 事实上, 如果 D 是连通的, $C \subset D$, 那么 $x_0 \in D$, 所以 $D \in \mathcal{D}$. 但是这样一

来, $D \subset C$, 所以 $C = D$. 于是 C 是最大的. (a) 得证.

(b) 设 C_1, C_2 是两个分支, $C_1 \neq C_2$, 假定在 $C_1 \cap C_2$ 内存在一点 x_0 , 再由引理, $C_1 \cup C_2$ 是连通的, 由于 C_1, C_2 都是分支, 这就给出 $C_1 = C_1 \cup C_2 = C_2$, 矛盾.

命题 32.5

(a) 如果 $A \subset X$ 是连通的, $A \subset B \subset A^-$, 那么 B 是连通的; (b) 如果 C 是 X 的一分支, 那么 C 是闭的.



证明留给读者作为习题.


定理 32.3

设 G 是 \mathbb{C} 中的开集, 那么 G 的分支是开集, 并且 G 只有可数个分支.



证明 设 C 是 G 的一分支, $x_0 \in C$. 由于 G 是开集, 所以存在 $\epsilon > 0$, 使得 $B(x_0; \epsilon) \subset G$. 根据引理, $B(x_0; \epsilon) \cup C$ 是连通的, 所以它必是 C . 即 $B(x_0; \epsilon) \subset C$, 所以 C 是开的.

为了看出分支的个数是可数的, 设 $S = \{a + ib : a, b \text{ 是有理数, 且 } a + ib \in G\}$, 那么 S 是可数的. G 的每个分支包含 S 的一点, 所以分支的个数是可数的.

 **练习 32.12** 本习题的目的在于证明 \mathbb{R} 的连通子集是一个区间.

(a) 证明: 当且仅当对于 A 中的任意两点 $a, b, a < b$, 有 $[a, b] \subset A$ 时, 集 $A \subset \mathbb{R}$ 是一个区间.

(b) 利用 (a) 证明: 如果 $A \subset \mathbb{R}$ 是连通的, 那么 A 是一个区间.


 **练习 32.13** 证明定理 32.1 的证明中的集 S 和 T 是开集.


 **练习 32.14** \mathbb{C} 中的下列子集 X , 哪些是连通的? 如果 X 不是连通的, 它的分支是什么?

(a) $X = \{z : |z| \leq 1\} \cup \{z : |z - 2| < 1\}$;

(b) $X = [0, 1] \cup \{1 + \frac{1}{n} : n > 1\}$;

(c) $X = \mathbb{C} - (A \cup B)$, 其中 $A = [0, \infty)$, $B = \{z = r \operatorname{cis} \theta : r = \theta, 0 \leq \theta \leq \infty\}$.

 **练习 32.15** 证明引理 32.1 的下述推广: 如果 $\{D_j : j \in J\}$ 是 X 的连通子集族, 且对于 J 中的每个 j 和 k , 有 $D_j \cap D_k \neq \emptyset$, 那么 $D = \bigcup \{D_j : j \in J\}$ 是连通的.

 **练习 32.16** 证明: 如果 $F \subset X$ 是闭的、连通的, 那么对于 F 中的每对点 a, b 和每个 $\epsilon > 0$, 在 F 中存在点 $z_0, z_1, \dots, z_n, z_0 = a, z_n = b$, 且对于 $1 \leq k \leq n, d(z_{k-1}, z_k) < \epsilon$, F 是闭的这个假定是必要的吗? 如果 F 是一个满足这个性质的集, 即使 F 是闭的, 也不一定是连通的. 试举例说明之.

32.3 序列与完备性

在度量空间中, 最有用的概念之一是收敛序列的概念, 这一概念在度量空间和复分析中与在微积分中一样起着中心的作用.

定义 32.7

设 $\{x_1, x_2, \dots\}$ 是度量空间 (X, d) 中的一个序列, 说 $\{x_n\}$ 收敛到 x , 如果对于每个 $\epsilon > 0$, 存在正整数 N , 使得 $n > N$ 时, $d(x, x_n) < \epsilon$, 记为 $x = \lim x_n$ 或 $x_n \rightarrow x$.



换言之, $x = \lim x_n$, 如果 $0 = \lim d(x, x_n)$.

如果 $X = \mathbb{C}$, 那么 $z = \lim z_n$ 意味着, 对于每个 $\epsilon > 0$, 存在正整数 N , 使得当 $n > N$ 时, $|z - z_n| < \epsilon$.

在度量空间的理论中, 许多概念可以借助于序列来叙述. 下面是一个例子.

命题 32.6

一个集 $F \subset X$ 是闭的, 当且仅当对于 F 中的每个序列 $\{x_n\}$, 若 $x = \lim x_n$, 则 $x \in F$.



证明 设 F 是闭的, $x = \lim x_n$, 其中每个 x_n 在 F 中. 所以对于每个 $\epsilon > 0$, 在 $B(x; \epsilon)$ 中有一点 x_n ; 即 $B(x; \epsilon) \cap F \neq \emptyset$. 所以由命题 32.3(f), $x \in F^- = F$.

现在设 F 不是闭的, 所以在 F^- 中有 x_0 , x_0 不在 F 中. 由命题 32.3(f), 对于每个 $\epsilon > 0$, 有 $B(x_0; \epsilon) \cap F \neq \emptyset$. 特别地, 对于每个正整数 n , 在 $B(x_0; \frac{1}{n}) \cap F$ 中有点 x_n . 于是 $d(x_0, x_n) < \frac{1}{n}$, 这就蕴含 $x_n \rightarrow x_0$. 由于 $x_0 \notin F$, 这就是说定理的条件不满足.

定义 32.8

设 $A \subset X$. 那么 X 中的点 x 是 A 的极限点, 如果在 A 中存在由不同点构成的序列 $\{x_n\}$, 使得 $x = \lim x_n$.



在这个定义中“不同”二字的理由可由下面的例子得到解释. 设 $X = \mathbb{C}$, $A = [0, 1] \cup \{i\}$; $[0, 1]$ 中的每一点是 A 的极限点, 但 i 不是 A 的极限点, 我们不能指望把 i 这样的点叫做极限点. 但是如果把“不同”二字从定义中删去, 我们就可以对每个 n 取 $x_n = i$, 有 $i = \lim x_n$.

命题 32.7

(a) 一个集合是闭的, 当且仅当, 它包含它的所有极限点; (b) 如果 $A \subset X$, 那么 $A^- = A \cup \{x : x \text{ 是 } A \text{ 的极限点}\}$.



证明留做习题.

从实分析中我们知道, \mathbb{R} 的基本性质是: 任意一个序列, 当 n 增大时它的项变得越来越接近, 则它一定是收敛的. 这种序列称为 Cauchy 序列. 这种序列的属性之一是它的极限一定存在, 尽管你不能求出它.

定义 32.9. Cauchy 序列

序列 $\{x_n\}$ 称为 Cauchy 序列, 如果对于每个 $\epsilon > 0$, 都存在一个正整数 N , 使得对所有的 $n, m \geq N$, 有 $d(x_n, x_m) < \epsilon$.



如果 (X, d) 有性质: 每个 Cauchy 序列在 X 中有极限, 那么 (X, d) 是完备的.

命题 32.8

\mathbb{C} 是完备的.



证明 如果 $\{x_n + iy_n\}$ 是 \mathbb{C} 中的 Cauchy 序列, 那么 $\{x_n\}$ 和 $\{y_n\}$ 是 \mathbb{R} 中的 Cauchy 序列, 由于 \mathbb{R} 是完备的, 所以 $x_n \rightarrow x$, $y_n \rightarrow y$, x, y 在 \mathbb{R} 中. 由此推出, $x + iy = \lim (x_n + iy_n)$,

所以 \mathbb{C} 是完备的.

考虑具有度量 d (见第31章的31.6.8和31.6.7) 的 C_∞ . 设 z_n, z 是 \mathbb{C} 中的点, 可以证明 $d(z_n, z) \rightarrow 0$, 当且仅当 $|z_n - z| \rightarrow 0$. 尽管如此, 注意序列 $\{z_n\}$, $\lim |z_n| = \infty$ 是 C_∞ 中的 Cauchy 序列, 但是它不是 \mathbb{C} 中的 Cauchy 序列.

如果 $A \subset X$, 我们把 $\text{diam } A = \sup \{d(x, y) : x \text{ 和 } y \text{ 在 } A \text{ 中}\}$ 定义为 A 的直径.

定理 32.4. Cantor 定理

度量空间 (X, d) 是完备的, 当且仅当, 任意满足条件 $F_1 \supset F_2 \supset \cdots$ 和 $\text{diam } F_n \rightarrow 0$, 非空闭集序列 $\{F_n\}$, 其交集 $\bigcap_{n=1}^\infty F_n$ 是由一个点所组成.



证明 设 (X, d) 是完备的, $\{F_n\}$ 是一个闭集序列, 具有性质: (i) $F_1 \supset F_2 \supset \cdots$; (ii) $\lim \text{diam } F_n = 0$. 对于每个 n , 设 x_n 是 F_n 种的任意一点, 如果 $n, m \geq N$, 那么 x_n, x_m 在 F_N 中, 由定义, $d(x_n, x_m) \leq \text{diam } F_N$. 由假定, N 可玄德充分大, 使得 $\text{diam } F_N < \epsilon$; 这就表明 $\{x_n\}$ 是 Cauchy 序列. 由于 X 是完备的, 所以 $x_0 = \lim x_n$ 存在. 又对于所有的 $n \geq N$, 因为 $F_n \subset F_N$, 所以 x_n 在 F_N 中; 因此, 对于每个 N, x_0 在 F_N 中, 这就给出 $x_0 \in \bigcap_{n=1}^\infty F_n = F$. 所以 F 至少包含一个点. 如果 y 也在 F 中, 那么对于每个 n, x_0 和 y 都在 F_n 中, 这就给出 $d(x_0, y) \leq \text{diam } F_n \rightarrow 0$, 所以 $d(x_0, y) = 0$, 或者 $x_0 = y$.

现在, 如果 X 满足所述的条件, 我们来证明 X 是完备的. 设 $\{x_n\}$ 是 X 中的 Cauchy 序列, 又设 $F_n = \{x_n, x_{n+1}, \cdots\}^-$; 那么 $F_1 \supset F_2 \supset \cdots$. 如果 $\epsilon > 0$, 选取 N , 使得对于每个 $n, m \geq N$, 都有

$$d(x_n, x_m) < \epsilon;$$

这就表示对于 $n \geq N$, $\text{diam}\{x_n, x_{n+1}, \cdots\} \leq \epsilon$, 所以对于 $n \geq N$, $\text{diam } F_n \leq \epsilon$ (习题32.19). 于是 $\text{diam } F_n \rightarrow 0$, 并且, 按照假设, 在 X 中存在点 x_0 , $\{x_0\} = F_1 \cap F_2 \cap \cdots$. 特别地, x_0 在 F_n 中, $d(x_0, x_n) \leq \text{diam } F_n \rightarrow 0$, 所以 $x_0 = \lim x_n$.

有一个典型习题与这个定理有联系, 就是在 \mathbb{R} 中找一个集序列 $\{F_n\}$, 它满足下面的条件中的两个条件:

- (a) 每个 F_n 是闭的;
- (b) $F_1 \supset F_2 \supset \cdots$;
- (c) $\text{diam } F_n \rightarrow 0$.

但是 $F = F_1 \cap F_2 \cap \cdots$ 或者是空的, 或者多于一点, 对于两个条件的各种可能选择, 读者都应举出相应的例子.

命题 32.9

设 (X, d) 是一个完备的度量空间, $Y \subset X$, 当且仅当 Y 在 X 中是闭时 (Y, d) 是一个完备度量空间.



证明 当 Y 是闭子集时, (Y, d) 是完备的. 其证明留给读者作为习题. 现在设 (Y, d) 是完备的, x_0 是 Y 的极限点, 那么在 Y 中有序列 $\{y_n\}$, 使得 $x_0 = \lim y_n$. 因此 $\{y_n\}$ 是 Cauchy 序列 (习题32.21), 并且因为 (Y, d) 是完备的, 所以 $\{y_n\}$ 一定收敛到 Y 中的 y_0 . 由此推得

$y_0 = x_0$, 所以 Y 包含它的所有极限点. 由命题 32.7, Y 是闭的.

练习 32.17 证明命题 32.7.

练习 32.18 完成命题 32.9 的详细证明.

练习 32.19 证明: $\text{diam } A = \text{diam } A^-$.

练习 32.20 设 z_n, z 是 \mathbb{C} 中的点, d 是 \mathbb{C}_∞ 中的度量, 证明 $|z_n - z| \rightarrow 0$, 当且仅当, $d(z_n, z) \rightarrow 0$. 证明: 如果 $|z_n| \rightarrow \infty$, 那么 $\{z_n\}$ 是 \mathbb{C}_∞ 中的 Cauchy 序列. ($\{z_n\}$ 在 \mathbb{C}_∞ 中一定收敛吗?)

练习 32.21 证明: (X, d) 中的每个收敛序列一定是 Cauchy 序列.

练习 32.22 给出三个不完备度量空间的例子.

练习 32.23 在 \mathbb{R} 上作一度量 d , 满足条件: $|x_n - x| \rightarrow 0$, 当且仅当, $d(x_n, x) \rightarrow 0$, 而当 $|x_n| \rightarrow \infty$ 时, $\{x_n\}$ 是 (\mathbb{R}, d) 中的 Cauchy 序列. (提示: 从 \mathbb{C}_∞ 得到启示.)

练习 32.24 设 $\{x_n\}$ 是 Cauchy 序列, 且 $\{x_{n_k}\}$ 是收敛子序列, 证明: $\{x_n\}$ 一定是收敛的.

32.4 紧性

紧性的概念是把有限集中一些好的性质推广到无穷集去, 紧集的大部分性质类似于有限集的性质, 这些性质在有限集是很平凡的. 例如, 有限集的每个序列有收敛子序列. 这是平凡的, 因为至少有一点重复无穷多次. 当我们把“有限”代之以“紧”时, 这个结果仍然成立.

定义 32.10. 紧集

度量空间 X 的子集 K 是紧的, 如果对于 X 中的每个具有性质

$$K \subset \bigcup \{G : G \in \mathcal{G}\}, \quad (32.4.1)$$

的开集族 \mathcal{G} 都可在 \mathcal{G} 中找到有限个集 G_1, G_2, \dots, G_n , 使得 $K \subset G_1 \cup G_2 \cup \dots \cup G_n$. 满足 (32.4.1) 的集族 \mathcal{G} 称为 K 的覆盖; 如果 \mathcal{G} 的每个集是开的, 则称它是 K 的开覆盖.

显然, 空集和所有的有限集是紧的. $D = \{z \in \mathbb{C} : |z| < 1\}$ 是一个非紧集的例子. 如果 $G_n = \{z : |z| < 1 - \frac{1}{n}\}$, $n = 2, 3, \dots$, 那么 $\{G_2, G_3, \dots\}$ 是 D 的一个开覆盖, 但它没有有限子覆盖.

命题 32.10

设 K 是 X 的一个紧子集, 那么

- (a) K 是闭的;
- (b) 如果 F 是闭的, 且 $F \subset K$, 则 F 是紧的.

证明 为了证明 (a), 我们要证明 $F = F^-$. 设 $x_0 \in K^-$, 由命题 32.3(f), 对于每个 $\epsilon > 0$, $B(x_0; \epsilon) \cap K \neq \emptyset$. 设

$$G_n = X - \bar{B}(x_0; \frac{1}{n}),$$

并假定 $x_0 \notin K$, 那么每个 G_n 是开集, 且 $K \subset \bigcup_{n=1}^{\infty} G_n$ (因为 $\bigcap_{n=1}^{\infty} \bar{B}(x_0; \frac{1}{n}) = \{x_0\}$)

. 因为 K 是紧的, 所以存在正整数 m , 使得 $K \subset \bigcup_{n=1}^m G_n$. 但是 $G_1 \subset G_2 \subset \cdots$, 所以 $K \subset G_m = X - \bar{B}(x_0; \frac{1}{m})$. 但这就给出 $B(x_0; \frac{1}{m}) \cap K = \emptyset$, 从而得到一个矛盾. 于是 $K = K^-$.

为了证明 (b), 设 \mathcal{G} 是 F 的一个开覆盖. 那么由于 F 是闭的, $\mathcal{G} \cup \{X - F\}$ 是 K 的开覆盖. 设 G_1, G_2, \dots, G_n 是 \mathcal{G} 中的集, 使得 $K \subset G_1 \cup \cdots \cup G_n \cup (X - F)$. 显然, $F \subset G_1 \cup \cdots \cup G_n$, 所以 F 是紧的.

设 \mathcal{F} 是 X 的子集族, 我们说 \mathcal{F} 有有限交性质 (f, i, p) 如果, 只要 $\{F_1, F_2, \dots, F_n\} \subset \mathcal{F}$, 总有 $F_1 \cap F_2 \cap \cdots \cap F_n \neq \emptyset$. 这种子集族的一个例子是 $\{D - G_2, D - G_3, \dots\}$, 其中集 G_n 是命题 32.10 之前所述例子中的集.

命题 32.11

一个集合 $K \subset X$ 是紧的, 当且仅当, K 中每个具有 (f, i, p) 的闭子集^a族 \mathcal{F} , 都有 $\bigcap \{F : F \in \mathcal{F}\} \neq \emptyset$.

^a这里的“闭子集”应是“相对于集合 K 的闭子集”. 否则命题的充分性不真, 必要性的证明应作相应的修改.



证明 设 K 是紧的, \mathcal{F} 是具有 (f, i, p) 的 K 中的闭子集族. 假设 $\bigcap \{F : F \in \mathcal{F}\} = \emptyset$. 令 $\mathcal{D} = \{X - F : F \in \mathcal{F}\}$, 那么由假设 $\bigcup \{X - F : F \in \mathcal{F}\} = X - \bigcap \{F : F \in \mathcal{F}\} = X$. 特别地, \mathcal{D} 是 K 的开覆盖, 于是存在 $F_1, \dots, F_n \in \mathcal{F}$, 使得 $K \subset \bigcup_{k=1}^n (X - F_k) = X - \bigcap_{k=1}^n F_k$. 但这就给出 $\bigcap_{k=1}^n F_k = X - K$, 由于每个 F_k 是 K 的子集, 所以必有 $\bigcap_{k=1}^n F_k = \emptyset$. 这与 \mathcal{F} 具有 (f, i, p) 相矛盾.

条件的充分性的证明留给读者作为习题.

推论 32.2

每个紧的度量空间是完备的.



证明 这容易由上面的命题和定理 32.4 推出.

推论 32.3

如果 X 是紧的, 那么每个无穷集在 X 中至少有一个极限点.



证明 设 S 是 X 的一无穷子集, 假设 S 没有极限点. 设 $\{a_1, a_2, \dots\}$ 是 S 中不同点的序列, 那么 $F_n = \{a_n, a_{n+1}, \dots\}$ 也没有极限点. 但是如果一个集合没有极限点, 那么也可以说它包含了它的所有极限点, 因而它是闭集! 于是每个 F_n 是闭的, 且 $\{F_n : n \geq 1\}$ 具有 (f, i, p) . 但是由于点 a_1, a_2, \dots 是不同的, 所以 $\bigcap_{n=1}^{\infty} F_n = \emptyset$. 这与上面的命题 32.11 相矛盾.

定义 32.11. 列紧性

称一个度量空间 (X, d) 是列紧的, 如果 X 中的每个序列都有收敛子序列.



我们将证明度量空间的紧性和列紧性是一回事, 为此需要下面的引理.

引理 32.2. Lebesgue 覆盖引理

如果 (X, d) 是列紧的, \mathcal{G} 是 X 的开覆盖, 那么存在 $\epsilon > 0$, 使得 X 中的每个 x , 都存在 \mathcal{G} 中的一个集 G , 满足 $B(x; \epsilon) \subset G$.



证明 用反证法, 设 \mathcal{G} 是 X 的开覆盖, 而这样的 ϵ 不存在. 特别地, 对于每个正整数 n , 在 X 中有点 x_n , 使得 $B(x_n; \frac{1}{n})$ 不包含在 \mathcal{G} 中任一个集 G 内. 因为 X 是列紧的, 所以在 X 中存在点 x_0 和序列 $\{x_{n_k}\}$, 使得 $x_0 = \lim x_{n_k}$. 设 $G_0 \in \mathcal{G}$, $x_0 \in G_0$; 选取 $\epsilon > 0$ 使得 $B(x_0; \epsilon) \subset G_0$. 现在设 N 是这样的正整数, 对于所有的 $n_k \geq N$, 都有 $d(x_0; x_{n_k}) \leq \epsilon/2$. 设 n_k 是比 N 和 $2/\epsilon$ 都大的任意正整数, $y \in B(x_{n_k}; \frac{1}{n_k})$, 那么 $d(x_0, y) \leq d(x_0, x_{n_k}) + d(x_{n_k}, y) < \epsilon/2 + 1/n_k < \epsilon$. 即 $B(x_{n_k}; \frac{1}{n_k}) \subset B(x_0; \epsilon) \subset G_0$, 这和 x_{n_k} 的取法相矛盾.

对于 Lebesgue 覆盖引理通常有两种误解. 一是言之未及, 一是言过其实. 由于 \mathcal{G} 是 X 的开覆盖, 所以 X 的每个 x 包含在 \mathcal{G} 的某一个 G 内; 因为 G 是开集, 于是存在 $\epsilon > 0$ 使得 $B(x; \epsilon) \subset G$. 但是引理所给出的 $\epsilon > 0$ 是使得对于任意的 x , $B(x; \epsilon)$ 都包含在 \mathcal{G} 的某一集内. 另一种误解是, 以为对于引理中所得到的 $\epsilon > 0$, $B(x; \epsilon)$ 包含在 \mathcal{G} 中含有 x 的每个 G 内.

定理 32.5

设 (X, d) 是一个度量空间, 那么下列条件是等价的:

- (a) X 是紧的;
- (b) X 中的每个无穷集至少有一个极限点;
- (c) X 是列紧的;
- (d) X 是完备的, 并且对于每个 $\epsilon > 0$, X 内存在有穷多个点 x_1, x_2, \dots, x_n , 使得

$$X = \bigcup_{k=1}^n B(x_k; \epsilon).$$

((d) 中所述的性质称为完全有界性.)



证明 由推论 32.3, (a) 蕴含 (b).

(b) 蕴含 (c). 设 $\{x_n\}$ 是 X 中的一个序列, 不失一般性, 假定点 x_1, x_2, \dots 是不同的. 由 (b), 集合 $\{x_1, x_2, \dots\}$ 有一个极限点 x_0 . 于是有点 $x_{n_1} \in B(x_0; 1)$, 类似的, 有正整数 $n_2 > n_1$, $x_{n_2} \in B(x_0; \frac{1}{2})$, 如此继续下去, 我们得到正整数 $n_1 < n_2 < \dots$, $x_{n_k} \in B(x_0; \frac{1}{k})$. 于是 $x_0 = \lim x_{n_k}$. 所以 X 是列紧的.

(c) 蕴含 (d). 设 $\{x_n\}$ 是 Cauchy 序列, 应用列紧性的定义和借助于 32.3 节的习题 32.24, 便可看出 X 是完备的.

现在设 $\epsilon > 0$, 固定 $x_1 \in X$. 如果 $X = B(x_1; \epsilon)$, 那么结论得证. 否则选取 $x_2 \in X - B(x_1; \epsilon)$. 如果 $X = B(x_1; \epsilon) \cup B(x_2; \epsilon)$, 结论也得证. 否则设 $x_3 \in X - [B(x_1; \epsilon) \cup B(x_2; \epsilon)]$. 如果这个过程不会终止, 我们就得到一序列 $\{x_n\}$, 使得

$$x_{n+1} \in X - \bigcup_{k=1}^n B(x_k; \epsilon).$$

但是这蕴含对于 $n \neq m$, $d(x_n, x_m) \geq \epsilon > 0$. 于是 $\{x_n\}$ 没有收敛子列, 这与 (c) 相矛盾.

(d) 蕴含 (c). 这部分证明用到“鸽巢原理”, 这个原理可表述为: 如果物件数多于容器数, 那么至少有一个容器里装的物件多于一个. 进而, 如果无穷多个点包含在有穷多个球里, 那么有一个球包含无穷多个点, 所以 (d) 是说, 对于每个 $\epsilon > 0$ 和 X 中的无穷集, 存在点 $y \in X$, 使得 $B(y; \epsilon)$ 包含这个集的无穷多个点. 设 $\{x_n\}$ 是一个由不同点组成的序列. 在 X 中存在点 y_1 和 $\{x_n\}$ 的子序列 $\{x_n^{(1)}\}$, 使得 $\{x_n^{(1)}\} \subset B(y_1; 1)$. 又存在 X 中的 y_2 和 $\{x_n^{(1)}\}$ 的子序列 $\{x_n^{(2)}\}$, 使得 $\{x_n^{(2)}\} \subset B(y_2; 1/2)$. 如此继续下去, 对于每个正整数 $k \geq 2$, 存在 X 中的 y_k 和 $\{x_n^{(k-1)}\}$ 的子序列 $\{x_n^{(k)}\}$, 使得 $\{x_n^{(k)}\} \subset B(y_k; 1/k)$. 设 $F_k = \{x_n^{(k)}\}$, 那么 $\text{diam } F_k \leq 2/k$, 且 $F_1 \supset F_2 \supset \cdots$. 根据定理??, $\bigcap_{k=1}^{\infty} F_k = \{x_0\}$. 我们断言 $x_k^{(k)} \rightarrow x_0$ ($x_k^{(k)}$ 是 $\{x_n\}$ 的子序列). 事实上, $x_0 \in F_k$, 所以 $d(x_0; x_k^{(k)}) \leq \text{diam } F_k \leq 2/k$, $x_0 = \lim x_k^{(k)}$.

(c) 蕴含 (a). 设 \mathcal{G} 是 X 的一个开覆盖. 上面的引理给出一个 $\epsilon > 0$, 使得对于每个 $x \in X$, \mathcal{G} 中存在一个集 G , $B(x; \epsilon) \subset G$. 现在已知 (c) 蕴含 (d), 因此, 在 X 中存在点 x_1, \cdots, x_n , 使得 $X = \bigcup_{k=1}^n B(x_k; \epsilon)$. 现在对于 $1 \leq k \leq n$, 存在集 $G_k \in \mathcal{G}$, $B(x_k; \epsilon) \subset G_k$. 因此 $X = \bigcup_{k=1}^n G_k$, 即 $\{G_1, \cdots, G_n\}$ 是 \mathcal{G} 的有限子覆盖.

定理 32.6. Heine-Borel 定理

当且仅当 K 是有界闭集时, \mathbb{R}^n ($n \geq 1$) 中的一个集 K 是紧的.



证明 如果 K 是紧的, 那么由前一定理的 (d), K 是完全有界的. 由命题 32.10 推出 K 一定是闭的. 容易证明完全有界的集也是有界的.

现在假设 K 是有界闭集. 因此存在实数 a_1, a_2, \cdots, a_n 和 b_1, b_2, \cdots, b_n , 使得 $K \subset F = [a_1, b_1] \times \cdots \times [a_n, b_n]$. 如果能够证明 F 是紧的, 那么因为 K 是闭的, 就可推知 K 是紧的 (命题 32.10(b)). 由于 \mathbb{R}^n 是完备的和 F 是闭的, 推知 F 是完备的. 因此, 再次应用前一定理中的 (d), 我们只需证明 F 是完全有界的. 这是容易的, 虽然写起来有点繁. 设 $\epsilon > 0$; 现在我们将 F 写成 n 维矩形的和, 其中每个矩形的直径小于 ϵ . 这样, 我们有 $F \subset \bigcup_{k=1}^{\infty} B(x_k; \epsilon)$, 其中每个 x_k 属于前面提到的矩形中的某一个. 这个做法的细节留给读者作为习题去完成 (习题 32.27).

练习 32.25 完成命题 32.28 的证明.

练习 32.26 设 $p = (p_1, p_2, \cdots, p_n)$, $q = (q_1, q_2, \cdots, q_n)$ 是 \mathbb{R}^n 中的点, 并且对于每个 k , $p_k < q_k$. 设 $R = [p_1, q_1] \times \cdots \times [p_n, q_n]$. 证明


$$\text{diam } R = d(p, q) = \left[\sum_{k=1}^n (q_k - p_k)^2 \right]^{\frac{1}{2}}.$$

练习 32.27 设 $F = [a_1, b_1] \times \cdots \times [a_n, b_n] \subset \mathbb{R}^n$, $\epsilon > 0$, 利用习题 32.26 证明: 存在矩形 R_1, R_2, \cdots, R_m , 使得 $F = \bigcup_{k=1}^m R_k$, 并且对于每个 k , $\text{diam } R_k < \epsilon$. 如果 $x_k \in R_k$, 那么由此推出 $R_k \subset B(x_k; \epsilon)$.

练习 32.28 证明: 有穷多个紧集的和是紧的.

练习 32.29 设 X 是所有有界复数序列的集. 也就是 $\{x_k\} \in X$, 当且仅当, $\sup\{|x_n| : n \geq 1\} < \infty$. 如果 $x = \{x_n\}$ 和 $y = \{y_n\}$, 定义 $d(x, y) = \sup\{|x_n - y_n| : n \geq 1\}$. 证明: 对于 X 中的每个 x 和 $\epsilon > 0$, $\bar{B}(x; \epsilon)$ 不是完全有界的, 尽管它是完备的. (提示: 如果首先证明

可以假定 $x = (0, 0, \dots, 0)$, 事情就容易了).

 **练习 32.30** 证明: 完全有界的集的闭包是完全有界的.

32.5 连续性

函数最基本的性质之一是连续性. 有了连续性就保证了一定程度的正则性和光滑性. 否则, 要得到度量空间上的任何函数理论是困难的. 由于本书的主题是具有导数的 (所以也是连续的) 一个复变数的函数论, 所以连续性的研究是基本的.

定义 32.12. 连续

设 (X, d) 和 (Ω, ρ) 是度量空间, $f: X \rightarrow \Omega$ 是一个函数. 设 $a \in X, \omega \in \Omega$, 如果对于每个 $\epsilon > 0$, 都存在 $\delta > 0$, 使得只要 $0 < d(x, a) < \delta$ 就有 $\rho(f(x), \omega) < \epsilon$, 那么就说 $\lim_{x \rightarrow a} f(x) = \omega$. 如果 $\lim_{x \rightarrow a} f(x) = f(a)$ 就说函数 f 在点 a 是连续的, 如果 f 在 X 的每一点都是连续的, 那么就称 f 是从 X 到 Ω 的连续函数.



命题 32.12

设 $f: (X, d) \rightarrow (\Omega, \rho)$ 是一个函数, $a \in X, \alpha = f(a)$. 下列事实是等价的:

- (a) f 在 a 点是连续的;
- (b) 对于每个 $\epsilon > 0$, $f^{-1}(B(\alpha; \epsilon))$ 包含一个以 a 为中心的球;
- (c) $\alpha = \lim f(x_n)$, 只要 $a = \lim x_n$.



证明留给读者作为习题.

这是关于函数在一点的连续性的最后一个命题, 从现在起, 我们将只涉及在 X 的所有点上连续的函数.

命题 32.13

设 $f: (X, d) \rightarrow (\Omega, \rho)$ 是一个函数, 下列事实是等价的:

- (a) f 是连续的;
- (b) 如果 Δ 是 Ω 中的开集, 那么 $f^{-1}(\Delta)$ 是 X 中的开集;
- (c) 如果 Γ 是 Ω 中的闭集, 那么 $f^{-1}(\Gamma)$ 是 X 中的闭集.



证明 (a) 蕴含 (b). 设 Δ 是 Ω 中的开集, $x \in f^{-1}(\Delta)$. 如果 $\omega = f(x)$, 那么 ω 在 Δ 内; 由定义, 存在 $\epsilon > 0$, 使得 $B(\omega, \epsilon) \subset \Delta$. 由于 f 是连续的, 所以由上一命题的 (b) 给出一 $\delta > 0$, 使得 $B(x, \delta) \subset f^{-1}(B(\omega; \epsilon)) \subset f^{-1}(\Delta)$. 因此 $f^{-1}(\Delta)$ 是开的.

(b) 蕴含 (c). 如果 $\Gamma \subset \Omega$ 是闭的, 那么 $\Delta = \Omega - \Gamma$ 是开的. 由 (b), $f^{-1}(\Delta) = X - f^{-1}(\Gamma)$ 是开的, 所以 $f^{-1}(\Gamma)$ 是闭的.

(c) 蕴含 (a). 假设在 X 中存在一点 x , f 在这点不连续, 那么存在 $\epsilon > 0$, 和一个序列 $\{x_n\}$, 使得 $x = \lim x_n$, 但是对于每个 n , 都有 $\rho(f(x_n), f(x)) \geq \epsilon$. 令 $\Gamma = \Omega - B(f(x); \epsilon)$, 那么 Γ 是闭的, 并且 x_n 在 $f^{-1}(\Gamma)$ 中. 由于 $f^{-1}(\Gamma)$ 是闭的 (根据 (c)), 我们有 $x \in f^{-1}(\Gamma)$. 但这就蕴含 $\rho(f(x); f(x)) \geq \epsilon > 0$, 故矛盾.

下述类型的结果大概易为读者所理解, 所以证明留给读者作为习题.

命题 32.14

设 f 和 g 是 X 到 \mathbb{C} 内的连续函数, $\alpha, \beta \in \mathbb{C}$. 那么 $\alpha f + \beta g$ 和 fg 也是连续的. 如果对于 X 中的每个 $x, g(x) \neq 0$, 那么 f/g 也是连续的.

**命题 32.15**

设 $f: X \rightarrow Y$ 及 $g: Y \rightarrow Z$ 是连续函数, 那么 $g \circ f$ (这里 $g \circ f(x) = g(f(x))$) 是 X 到 Z 内的一个连续函数.



证明 如果 U 是 Z 中的开集, 那么 $g^{-1}(U)$ 是 Y 中的开集. 因此 $f^{-1}(g^{-1}(U)) = (g \circ f)^{-1}(U)$ 是 X 中的开集.

定义 32.13. 一致连续

函数 $f: (X, d) \rightarrow (Y, \rho)$ 是一致连续的, 如果对于每个 $\epsilon > 0$, 存在 $\delta > 0$ (只依赖于 ϵ), 使得当 $d(x, y) < \delta$ 时, 就有 $\rho(f(x), f(y)) < \epsilon$. 我们称 f 是一个 Lipschitz 函数. 如果存在常数 $M > 0$, 使得对于 X 中的所有 x 和 y , 都有 $\rho(f(x), f(y)) \leq Md(x, y)$.



容易看出, 每个 Lipschitz 函数是一致连续的. 事实上, 如果给定 $\epsilon > 0$, 取 $\delta = \epsilon/M$ 即可. 也容易看出每个一致连续的函数是连续的. 上述诸类函数有些什么例子呢? 如果 $X = \Omega = \mathbb{R}$, 那么 $f(x) = x^2$ 是连续的, 但不是一致连续的. 如果 $X = \Omega = [0, 1]$, 那么 $f(x) = x^{\frac{1}{2}}$ 是一致连续的, 但不是 Lipschitz 函数. 下述命题为 Lipschitz 函数提供了一个丰富的来源.

设 $A \subset X, x \in X$. 我们定义 x 到集 A 的距离 $d(x, A)$ 为

$$d(x, A) = \inf\{d(x, a) : a \in A\}.$$

命题 32.16

设 $A \subset X$, 那么:

- (a) $d(x, A) = d(x, A^-)$.
- (b) $d(x, A) = 0$, 当且仅当, $x \in A^-$.
- (c) 对于 X 中的所有 x , 有 $|d(x, A) - d(y, A)| \leq d(x, y)$.



证明 (a) 如果 $A \subset B$, 那么由定义显然有 $d(x, B) \leq d(x, A)$. 因此 $d(x, A^-) \leq d(x, A)$. 另一方面, 如果 $\epsilon > 0$, 则存在 A^- 中的一点 y , 使得 $d(x, A^-) \geq d(x, y) - \epsilon/2$. 再在 A 中找一点 a , 满足 $d(y, a) < \epsilon/2$. 但是由三角不等式 $|d(x, y) - d(x, a)| \leq d(y, a) < \epsilon/2$. 特别地, $d(x, y) > d(x, a) - \epsilon/2$. 这就给出 $d(x, A^-) \geq d(x, a) - \epsilon \geq d(x, A) - \epsilon$. 因为 ϵ 是任意的, 所以 $d(x, A^-) \geq d(x, A)$. (a) 得证.

(b) 如果 $x \in A^-$, 那么 $0 = d(x, A^-) = d(x, A)$. 现在对于 X 中的任意 x , 在 A 中存在一最小序列 $\{a_n\}$, 使得 $d(x, A) = \lim d(x, a_n)$. 所以如果 $d(x, A) = 0$, 那么 $\lim d(x, a_n) = 0$, 即 $x = \lim a_n, x \in A^-$.

(c) 对于 A 中的 a , $d(x, a) \leq d(x, y) + d(y, a)$, 因此 $d(x, A) = \inf\{d(x, a) : a \in A\} \leq \inf\{d(x, y) + d(y, a) : a \in A\} = d(x, y) + d(y, A)$. 这就给出了 $d(x, A) - d(y, A) \leq d(x, y)$. 类似的, $d(y, A) - d(x, A) \leq d(x, y)$. 所以不等式得证.

注意, 命题的 (c) 是说: 由 $f(x) = d(x, A)$ 所定义的函数 $f: X \rightarrow \mathbb{R}$ 是一个 Lipschitz 函数. 如果我们变动集 A , 便得到许多这种函数.

两个一致连续的 (Lipschitz) 函数的乘积仍是一致连续的 (Lipschitz) 函数, 这一命题是不真的. 例如, $f(x) = x$ 是 Lipschitz 函数, 但是 $f \cdot f$ 甚至都不是一致连续的. 不过如果 f 和 g 都是有界的, 那么命题就成立了 (见习题 32.33).

下面的定理包含连续函数的两个最重要的性质.

定理 32.7

设 $f: (X, d) \rightarrow (\Omega, \rho)$ 是一个连续函数. (a) 如果 X 是紧的, 那么 $f(X)$ 是 Ω 种的紧子集; (b) 如果 X 是连通的, 那么 $f(X)$ 是 Ω 中的连通子集.

证明 为了证明 (a) 和 (b), 不失一般性, 可以假设 $f(X) = \Omega$. (a) 设 $\{\omega_n\}$ 是 Ω 中的一个序列, 那么对于每个 $n \geq 1$, 在 X 中存在一点 x_n , 使得 $\omega_n = f(x_n)$. 由于 X 是紧的, 所以在 X 中存在一点 x 和一个子序列 $\{x_{n_k}\}$, 使得 $x = \lim x_{n_k}$. 设 $\omega = f(x)$, 那么由 f 的连续性, $\omega = \lim \omega_{n_k}$, 因此根据定理 32.5, Ω 是紧的. (b) 设 $\Sigma \subset \Omega$ 在 Ω 中既是开的, 又是闭的, 且 $\Sigma \neq \emptyset$, 那么因为 $f(X) = \Omega$, 所以 $\emptyset \neq f^{-1}(\Sigma)$. 因为 f 是连续的, 所以 $f^{-1}(\Sigma)$ 也既是开的, 又是闭的. 根据 X 的连通性, $f^{-1}(\Sigma) = X$, 这就给出 $\Omega = \Sigma$, 于是 Ω 是连通的.

推论 32.4

如果 $f: X \rightarrow \Omega$ 是连续的, K 是 X 中的紧集或连通集, 那么相应地 $f(K)$ 是 Ω 中的紧集或连通集.

推论 32.5

如果 $f: X \rightarrow \mathbb{R}$ 是连续的, X 是连通的, 那么 $f(X)$ 是一个区间.

这可由 \mathbb{R} 的连通子集的特征是区间这一事实推出.

定理 32.8. 中值定理

如果 $f: [a, b] \rightarrow \mathbb{R}$ 是连续的, 且 $f(a) \leq \xi \leq f(b)$, 那么存在一点 x , $a \leq x \leq b$, 使得 $f(x) = \xi$.

推论 32.6

如果 $f: X \rightarrow \mathbb{R}$ 是连续的, $K \subset X$ 是紧的, 那么在 K 中存在点 x_0 和 y_0 , 使得 $f(x_0) = \sup\{f(x) : x \in K\}$, $f(y_0) = \inf\{f(x) : x \in K\}$.

证明 如果 $\alpha = \sup\{f(x) : x \in K\}$, 那么因为 $f(K)$ 在 \mathbb{R} 中是有界闭集, 所以 α 在 $f(K)$ 内. 类似地, $\beta = \inf\{f(x) : x \in K\}$ 在 $f(K)$ 内.

推论 32.7

如果 $K \subset X$ 是紧的, $f: X \rightarrow \mathbb{C}$ 是连续的, 那么在 K 内存在点 x_0 和 y_0 , 使得

$$|f(x_0)| = \sup\{|f(x)| : x \in K\},$$

$$|f(y_0)| = \inf\{|f(x)| : x \in K\}.$$

证明 这个系由上一系推出, 因为 $g(x) = |f(x)|$ 定义一个从 X 到 \mathbb{R} 的连续函数.

推论 32.8

如果 K 是 X 的紧子集, x 在 X 内, 那么在 K 内存在一点 y , 使得 $d(x, y) = d(x, K)$. 

证明 定义 $f: X \rightarrow \mathbb{R}$ 为 $f(y) = d(x, y)$, 那么 f 是连续的, 并且由系 32.6, 在 K 上取到最小值. 这就是说, 在 K 内存在一点 y , 使得对于每个 $z \in K$, 都有 $f(y) \leq f(z)$. 这就给出了 $d(x, y) = d(x, K)$.

下面的两个定理极为重要, 在全书中将反复用到它, 用时不再注明.

定理 32.9

设 $f: X \rightarrow \Omega$ 是连续的, X 是紧的, 那么 f 是一致连续的. 

证明 设 $\epsilon > 0$, 我们要找一个 $\delta > 0$, 使得 $d(x, y) < \delta$ 蕴含 $\rho(f(x), f(y)) < \epsilon$. 假如不存在这样的 δ ; 特别地, 每个 $\delta = \frac{1}{n}$ 都不满足上述要求. 那么对于每个 $n \geq 1$, 在 X 内有点 x_n, y_n , 使得 $d(x_n, y_n) < \frac{1}{n}$, 但是 $\rho(f(x_n), f(y_n)) \geq \epsilon$. 因为 X 是紧的, 所以存在子序列 $\{x_{n_k}\}$ 和点 $x \in X$, 使得 $x = \lim x_{n_k}$.

我们断言 $x = \lim y_{n_k}$. 事实上, $d(x, y_{n_k}) \leq d(x, x_{n_k}) + \frac{1}{n_k}$; 当 k 趋于 ∞ 时, 它是趋于零的.


设 $\omega = f(x)$, 那么 $\omega = \lim f(x_{n_k}) = \lim f(y_{n_k})$, 所以不等式

$$\epsilon \leq \rho(f(x_{n_k}), f(y_{n_k})) \leq \rho(f(x_{n_k}), \omega) + \rho(\omega, f(y_{n_k})),$$

的右边趋于零. 这是一个矛盾. 因而定理得证.

定义 32.14

如果 A, B 是 X 的子集, 那么定义 A 到 B 的距离 $d(A, B)$ 为

$$d(A, B) = \inf\{d(a, b) : a \in A, b \in B\}.$$



注意, 如果 B 是一个点所组成的集 $\{x\}$, 那么 $d(A, \{x\}) = d(x, A)$. 如果 $A = \{y\}$, $B = \{x\}$. 那么 $d(\{x\}, \{y\}) = d(x, y)$. 又如果 $A \cap B \neq \emptyset$, 那么 $d(A, B) = 0$. 但是 A, B 不相交, 我们也可能有 $d(A, B) = 0$. 最典型的例子是取 $A = \{(x, 0) : x \in \mathbb{R}\}$, $B = \{(x, e^x) : x \in \mathbb{R}\}$. 注意 A, B 都是闭的且不相交, 但仍有 $d(A, B) = 0$.


定理 32.10

如果 A, B 是 X 中不相交的集合, B 是闭的, A 是紧的, 那么 $d(A, B) > 0$. 


证明 定义 $f: X \rightarrow \mathbb{R}$ 为 $f(x) = d(x, B)$. 因为 $A \cap B = \emptyset$ 及 B 是闭集, 所以对于 A 内的每一个 a , $f(a) > 0$. 但是因为 A 是紧的, 所以在 A 内存在一点 a , 使得 $0 < f(a) = \inf\{f(x) : x \in A\} = d(A, B)$.


 **练习 32.31** 证明命题 32.12.


 **练习 32.32** 如果 f 和 g 是从 X 到 \mathbb{C} 的一致连续 (Lipschitz) 函数, 那么 $f + g$ 也是一致连续 (Lipschitz) 函数.


 **练习 32.33** 我们说 $f: X \rightarrow \mathbb{C}$ 是有界的, 如果存在一常数 $M > 0$, 使得对于 X 中的所有


x , 有 $|f(x)| \leq M$. 证明: 如果 f 和 g 是从 X 到 \mathbb{C} 的有界的, 一致连续的 (Lipschitz) 函数, 则 fg 也是这样的函数.


 **练习 32.34** 两个一致连续的 (Lipschitz) 函数的复合函数仍然是一致连续 (Lipschitz) 函数吗?


 **练习 32.35** 设 $f: X \rightarrow \Omega$ 是一致连续的. 证明: 如果 $\{x_n\}$ 是 X 中的 Cauchy 序列, 则 $\{f(x_n)\}$ 是 Ω 中的 Cauchy 序列. 如果我们只假定 f 是连续的, 结论仍对吗? (证明或举出反例)

 **练习 32.36** 回忆稠密集的定义 (32.4). 设 Ω 是完备的度量空间, $f: (D, d) \rightarrow (\Omega, \rho)$ 是一致连续的, 其中 D 在 (X, d) 中稠密. 利用上题证明存在一致连续的函数 $g: X \rightarrow \Omega$, 使得对 D 内的每一点, $g(x) = f(x)$.

 **练习 32.37** 设 G 是 \mathbb{C} 中的一个开子集, P 是 G 内一条从 a 到 b 的折线. 用定理 32.9 和 32.10 证明: 在 G 内存在一条从 a 到 b 的折线, 它由平行于实轴或虚轴的线段所组成.

 **练习 32.38** 利用 Lebesgue 覆盖引理 32.2 给出定理 32.9 的另一个证明.

 **练习 32.39** 证明 ?? 节的习题 32.16 的下述逆命题. 设 (X, d) 是紧的度量空间, 具有性质: 对于每个 $\epsilon > 0$, 及 X 中的任意点 a 和 b , 在 X 中存在点 z_0, z_1, \dots, z_n , $z_0 = a, z_n = b$, 使得对于 $1 \leq k \leq n$, 有 $d(z_{k-1}, z_k) < \epsilon$, 则 (X, d) 是连通的. (提示: 利用定理 32.10)

 **练习 32.40** 设 f 和 g 是从 (X, d) 到 (Ω, ρ) 的连续函数, D 是 X 中的稠密子集. 证明: 如果对于 D 内的 x , $f(x) = g(x)$, 则 $f = g$. 利用这一事实证明第 32.36 题中所得到的函数是唯一的.

32.6 一致收敛性

设 X 是一个集, (Ω, ρ) 是一个度量空间, f, f_1, f_2, \dots 是 X 到 Ω 内的函数. 我们说序列 $\{f_n\}$ 一致收敛到 f , 记成 $f = \text{u-lim } f_n$, 如果对于每个 $\epsilon > 0$, 存在正整数 N (只依赖于 ϵ), 使得当 $n \geq N$ 时, 对 X 中的所有 x , 都有 $\rho(f(x), f_n(x)) < \epsilon$. 因此, 只要 $n \geq N$, 就有

$$\sup\{\rho(f(x), f_n(x)) : x \in X\} \leq \epsilon.$$

第一个问题是: 如果 X 不仅是一个集, 而且还是一个度量空间, 并且每一个 f_n 是连续的, 那么 f 是连续的吗? 回答是肯定的.

定理 32.11

设 $f_n: (X, d) \rightarrow (\Omega, \rho)$ 对于每个 n 是连续的, $f = \text{u-lim } f_n$, 则 f 是连续的.

证明 在 X 中固定 x_0 , 且取定 $\epsilon > 0$, 我们希望找出一个 $\delta > 0$, 使得当 $d(x_0, x) < \delta$ 时, $\rho(f(x_0), f(x)) < \epsilon$. 因为 $f = \text{u-lim } f_n$, 所以存在一个函数 f_n , 使得对于 X 中的所有 x , $\rho(f(x), f_n(x)) < \epsilon/3$. 因为 f_n 是连续的, 所以存在 $\delta > 0$, 使得当 $d(x_0, x) < \delta$ 时, $\rho(f_n(x_0), f_n(x)) < \epsilon/3$. 所以如果 $d(x_0, x) < \delta$, 则有 $\rho(f(x_0), f(x)) \leq \rho(f(x_0), f_n(x_0)) + \rho(f_n(x_0), f_n(x)) + \rho(f_n(x), f(x)) < \epsilon$,

让我们来考虑特别情形 $\Omega = \mathbb{C}$. 如果 $u_n: X \rightarrow \mathbb{C}$, 令 $f_n(x) = u_1(x) + \dots + u_n(x)$,

我们说 $f(x) = \sum_{n=1}^{\infty} u_n(x)$, 当且仅当, $f(x) = \lim f_n(x)$ 对于 X 中的所有 x 成立。称级数 $\sum_{n=1}^{\infty} u_n(x)$ 一致收敛到 f , 当且仅当, $f = \text{u-lim } f_n$.

定理 32.12. Weierstrass M-判别法

设函数 $u_n : X \rightarrow \mathbb{C}$ 对于 X 中的每个 x 有 $|u_n(x)| \leq M_n$, 而这些常数满足 $\sum_{n=1}^{\infty} M_n < \infty$, 那么 $\sum_{n=1}^{\infty} u_n$ 是一致收敛的。



证明 设 $f_n(x) = u_1(x) + \cdots + u_n(x)$, 那么当 $n \geq m$ 时, 对于每个 x , 有


$$|f_n(x) - f_m(x)| = |u_{m+1}(x) + \cdots + u_n(x)| \leq \sum_{k=m+1}^n M_k.$$

因为 $\sum_{k=1}^{\infty} M_k$ 收敛, 所以 $\{f_n(x)\}$ 是 \mathbb{C} 中的 Cauchy 序列, 于是存在一点 $\xi \in \mathbb{C}$, 使得 $\xi = \lim f_n(x)$. 定义 $f(x) = \xi$. 这就给出了一个函数 $f : X \rightarrow \mathbb{C}$. 现在有

$$\begin{aligned} |f(x) - f_n(x)| &= \left| \sum_{k=n+1}^{\infty} u_k(x) \right| \\ &\leq \sum_{k=n+1}^{\infty} |u_k(x)| \leq \sum_{k=n+1}^{\infty} M_k; \end{aligned}$$

因为 $\sum_{k=1}^{\infty} M_k$ 是收敛的, 所以对于任意的 $\epsilon > 0$, 存在正整数 N , 使得当 $n \geq N$ 时,

$\sum_{k=n+1}^{\infty} M_k < \epsilon$. 这就给出了当 $n \geq N$ 时, 对于 X 中的所有 x , $|f(x) - f_n(x)| < \epsilon$.

 **练习 32.41** 设 $\{f_n\}$ 是从 (X, d) 到 (Ω, ρ) 内的一致连续的函数所组成的序列, 并且 $f = \text{u-lim } f_n$, 证明: f 是一致连续的。如果每一个 f_n 是带有常数 M_n 的 Lipschitz 函数, 且 $\sup M_n < \infty$, 则 f 是 Lipschitz 函数。如果 $\sup M_n = \infty$, 说明 f 可能不是 Lipschitz 函数。

第三十三章 解析函数的初等性质和例子

33.1 幂级数

在这一节里,我们将给出幂级数的定义和基本性质。然后利用幂级数来给出解析函数的例子。为此有必要先给出有关 \mathbb{C} 内无穷级数的某些初等事实。对 \mathbb{R} 内的无穷级数,这些事实读者应该是熟知的。设对于每个 $n \geq 0$, a_n 在 \mathbb{C} 内,称级数 $\sum_{n=0}^{\infty} a_n$ 收敛到 z ,当且仅当,对于每一个 $\epsilon > 0$,存在一正整数 N ,使得当 $m \geq N$ 时, $|\sum_{n=0}^m a_n - z| < \epsilon$ 。如果 $\sum_{n=0}^{\infty} |a_n|$ 收敛,则称级数 $\sum_{n=0}^{\infty} a_n$ 绝对收敛。

命题 33.1

如果 $\sum a_n$ 绝对收敛,那么 $\sum a_n$ 收敛。

证明 设 $\epsilon > 0$, 令 $z_n = a_0 + a_1 + \cdots + a_n$, 因为 $\sum |a_n|$ 收敛, 所以存在正整数 N , 使得 $\sum_{n=N}^{\infty} |a_n| < \epsilon$ 。于是, 如果 $m \geq k \geq N$,

$$|z_m - z_k| = \left| \sum_{n=k+1}^m a_n \right| \leq \sum_{n=N}^{\infty} |a_n| < \epsilon.$$

即 $\{z_n\}$ 是 Cauchy 序列。所以在 \mathbb{C} 内有一点 z , $z = \lim z_n$ 。因此 $\sum z_n = z$ 。

回顾 \mathbb{R} 内的序列上极限和下极限的定义。如果 $\{a_n\}$ 是 \mathbb{R} 内的序列, 那么定义

$$\liminf a_n = \lim_{n \rightarrow \infty} [\inf \{a_n, a_{n+1}, \cdots\}],$$

$$\limsup a_n = \lim_{n \rightarrow \infty} [\sup \{a_n, a_{n+1}, \cdots\}],$$

$\liminf a_n$ 和 $\limsup a_n$ 的另一个记号是 $\underline{\lim} a_n$ 和 $\overline{\lim} a_n$ 。如果 $b_n = \inf \{a_n, a_{n+1}, \cdots\}$, 那么 $\{b_n\}$ 是实的递增序列, 或是 $\{-\infty\}$ 。因此, $\liminf a_n$ 总是存在的, 虽然它可能是 $\pm\infty$ 。类似地, $\limsup a_n$ 总存在, 虽然它可能是 $\pm\infty$ 。

\liminf 和 \limsup 的若干性质包含在这一节的习题中。在 a 点附近的幂级数是形如 $\sum_{n=0}^{\infty} a_n(z-a)^n$ 的无穷级数。幂级数的一个最容易的例子(也是最有用的)是几何级数 $\sum_{n=0}^{\infty} z^n$ 。对于 z 的哪些值这个级数是收敛的? 什么时候这个级数是发散的? 容易看出, $1 - z^{n+1} = (1-z)(1+z+z^2+\cdots+z^n)$, 所以

$$1 + z + \cdots + z^n = \frac{1 - z^{n+1}}{1 - z}. \quad (33.1.1)$$

如果 $|z| < 1$, 那么 $0 = \lim z^n$ 。所以几何级数是收敛的, 并且有

$$\sum_{n=0}^{\infty} z^n = \frac{1}{1-z}.$$

如果 $|z| > 1$, 那么 $\lim z^n = \infty$, 级数发散。这个结果不仅是一般幂级数的收敛情况的模型, 而且是探讨幂级数的收敛性质的工具。

定理 33.1

对于给定的幂级数 $\sum_{n=0}^{\infty} a_n(z-a)^n$, 由

$$\frac{1}{R} = \limsup |a_n|^{\frac{1}{n}},$$

定义数 R , $0 \leq R \leq \infty$. 那么:

- (a) 如果 $|z-a| < R$, 则级数绝对收敛;
- (b) 如果 $|z-a| > R$, 则级数的项无界, 所以级数发散;
- (c) 如果 $0 < r < R$, 则级数在 $\{z: |z-a| \leq r\}$ 上一致收敛. 并且具有性质 (a) 和 (b) 的数 R 是唯一的.



证明 我们可以假定 $a=0$. 如果 $|z| < R$, 那么有一 r , 满足 $|z| < r < R$. 于是存在正整数 N , 使得 $|a_n|^{\frac{1}{n}} < \frac{1}{r}$, 对于所有的 $n > N$ 成立 (因为 $\frac{1}{r} > \frac{1}{R}$). 但是这时, $|a_n| < \frac{1}{r^n}$, 所以对于所有的 $n \geq N$, $|a_n z^n| < (\frac{|z|}{r})^n$. 这就是说, 余项 $\sum_{n=N}^{\infty} a_n z^n$ 围于级数 $\sum (\frac{|z|}{r})^n$, 并且因为 $\frac{|z|}{r} < 1$, 所以对于每个 z , $|z| < R$, 这个幂级数绝对收敛.

现在设 $r < R$, 选取 ρ , 使得 $r < \rho < R$, 与上面一样, 设 N 是一正整数, 使得对于所有的 $n \geq N$, $|a_n| < \frac{1}{\rho^n}$, 那么, 如果 $|z| < r$, 便有 $|a_n z^n| < (\frac{r}{\rho})^n$, $(\frac{r}{\rho}) < 1$, 因此由 Weierstrass M-判别法, 幂级数在 $\{z: |z| \leq r\}$ 上一致收敛. 这就证明了 (a) 和 (c).

为了证明 (b), 设 $|z| > R$. 选取 r , 使得 $|z| > r > R$. 因此 $\frac{1}{r} < \frac{1}{R}$, 由 \limsup 的定义, 有无穷多个 n 使得 $\frac{1}{r} < |a_n|^{\frac{1}{n}}$. 由此推出 $|a_n z^n| > (\frac{|z|}{r})^n$. 因为 $(\frac{|z|}{r}) > 1$, 所以这些项是无界的.

数 R 称为幂级数的收敛半径.

命题 33.2

如果 $\sum a_n(z-a)^n$ 是一个给定的幂级数, 收敛半径为 R , 则

$$R = \lim |a_n/a_{n+1}|,$$

如果右边的极限存在.



证明 仍然假定 $a=0$. 设 $\alpha = \lim |a_n/a_{n+1}|$, 我们假定这个极限存在. 设 $|z| < r < \alpha$, 并且取正整数 N , 使得对于所有的 $n \geq N$, 有 $r < |a_n/a_{n+1}|$, 令 $B = |a_N| r^N$, 那么 $|a_{N+1}| r^{N+1} = |a_{N+1}| r r^N < |a_N| r^N = B$; $|a_{N+2}| r^{N+2} = |a_{N+2}| r \cdot r^{N+1} < |a_{N+1}| r^{N+1} < B$; 如此继续下去, 我们得到 $|a_n r^n| \leq B$ 对于所有的 $n \geq N$ 成立. 但是这时对于所有的 $n \geq N$, $|a_n z^n| = |a_n r^n| \frac{|z|^n}{r^n} \leq B \frac{|z|^n}{r^n}$. 因为 $|z| < r$, 所以我们得到 $\sum_{n=1}^{\infty} |a_n z^n|$ 围于一收敛级数, 因此是收敛的. 由于 $r < \alpha$ 是任意的, 所以 $\alpha \leq R$.

另一方面, 如果 $|z| > r > \alpha$, 那么对于大于某一正整数 N 的所有的 n , $|a_n| < r |a_{n+1}|$. 如前所述, 我们得到, 对于 $n \geq N$, 有 $|a_n r^n| \geq B = |a_N r^N|$, 这就给出 $a_n z^n > B \frac{|z|^n}{r^n}$, 它当 n 趋于 ∞ 时趋于 ∞ . 因此级数 $\sum a_n z^n$ 发散. 所以 $R \leq \alpha$, 于是 $R = \alpha$.

考虑级数 $\sum_{n=0}^{\infty} \frac{z^n}{n!}$, 由命题 33.2, 这个级数的收敛半径是 ∞ , 因此对于每个复数, 它是收敛的, 并且在 \mathbb{C} 内的每个紧子集上一致收敛. 为了和微积分学一致, 我们把这个级

数称为指数级数或指数函数

$$e^z = \exp z = \sum_{n=0}^{\infty} \frac{z^n}{n!}.$$

回顾无穷级数理论中的下述命题（不予证明）。

命题 33.3

设 $\sum a_n$ 和 $\sum b_n$ 是两个绝对收敛的级数，令

$$c_n = \sum_{k=0}^n a_k b_{n-k},$$

那么 $\sum c_n$ 是绝对收敛的，其和为 $(\sum a_n)(\sum b_n)$.



命题 33.4

设 $\sum a_n(z-a)^n$, $\sum b_n(z-a)^n$ 是收敛半径 $\geq r > 0$ 的两个幂级数，令

$$c_n = \sum_{k=0}^n a_k b_{n-k},$$

那么幂级数 $\sum (a_n + b_n)(z-a)^n$ 和 $\sum c_n(z-a)^n$ 的收敛半径都大于或等于 r ，并且对于 $|z-a| < r$ ，有

$$\begin{aligned} \sum (a_n + b_n)(z-a)^n &= [\sum a_n(z-a)^n + \sum b_n(z-a)^n], \\ \sum c_n(z-a)^n &= [\sum a_n(z-a)^n][\sum b_n(z-a)^n]. \end{aligned}$$



证明 我们只给出证明的梗概。如果 $0 < s < r$ ，那么对于 $|z| < s$ ，我们得到 $\sum |a_n + b_n||z|^n \leq \sum |a_n|s^n + \sum |b_n|s^n < \infty$ ； $\sum |c_n||z|^n \leq (\sum |a_n|s^n)(\sum |b_n|s^n) < \infty$ 。由此容易完成命题的证明。

练习 33.1 证明命题 33.3

练习 33.2 给出命题 33.4 的详细证明。

练习 33.3 设 $\{a_n\}$, $\{b_n\}$ 是实数序列，证明： $\limsup (a_n + b_n) \leq \limsup a_n + \limsup b_n$ ， $\liminf (a_n + b_n) \geq \liminf a_n + \liminf b_n$ 。

练习 33.4 证明：对于 \mathbb{R} 中的任意序列，有 $\limsup a_n \geq \liminf a_n$ 。

练习 33.5 如果 $\{a_n\}$ 是 \mathbb{R} 中的收敛序列， $a = \lim a_n$ ，证明 $a = \liminf a_n = \limsup a_n$ 。

练习 33.6 求下列幂级数的收敛半径：

- (a) $\sum_{n=0}^{\infty} a^n z^n, a \in \mathbb{C}$;
- (b) $\sum_{n=0}^{\infty} a^{n^2} z^n, a \in \mathbb{C}$;
- (c) $\sum_{n=0}^{\infty} k^n z^n$, 整数 $k \neq 0$;
- (d) $\sum_{n=0}^{\infty} z^{n!}$.

练习 33.7 证明幂级数

$$\sum_{n=1}^{\infty} \frac{(-1)^n}{n} z^{n(n+1)}$$

的收敛半径等于 1. 讨论 $z-1, -1, i$ 时幂级数的收敛性。（提示：这个幂级数的第 n 个系

数不是 $\frac{(-1)^n}{n}$.)

33.2 解析函数

在这节里, 我们将定义解析函数并给出某些例子。还要证明解析函数的实部和虚部满足 Cauchy-Riemann 方程。

定义 33.1

设 G 是 \mathbb{C} 中的开集, $f: G \rightarrow \mathbb{C}$ 。说 f 在 G 内的一点 a 是可微的, 如果

$$\lim_{h \rightarrow 0} \frac{f(a+h) - f(a)}{h}$$

存在。这个极限值用 $f'(a)$ 来表示, 称为 f 在 a 点的导数。如果 f 在 G 的每一点是可微的, 我们就称 f 在 G 内是可微的。注意, 如果 f 在 G 内是可微的, 那么 $f'(a)$ 就定义了一个函数 $f': G \rightarrow \mathbb{C}$ 。如果 f' 是连续的, 那么我们就说 f 是连续可微的。如果 f' 是可微的, 那么就说 f 是二次可微的; 如此等等, 一个可微函数, 如果它的各阶导数都是可微的, 就称它是无穷次可微的。



(今后, 除非作相反的声明, 我们将假定所有的函数都在 \mathbb{C} 中取值。)

读者一定预料到下面的事实:

命题 33.5

如果 $f: G \rightarrow \mathbb{C}$ 在 G 内的 a 点是可微的, 那么 f 在 a 点连续。



证明 事实上

$$\begin{aligned} \lim_{z \rightarrow a} |f(z) - f(a)| &= \left[\lim_{z \rightarrow a} \frac{|f(z) - f(a)|}{|z - a|} \right] \cdot \left[\lim_{z \rightarrow a} |z - a| \right] \\ &= |f'(a)| \cdot 0 = 0. \end{aligned}$$

定义 33.2

称函数: $f: G \rightarrow \mathbb{C}$ 是解析的, 如果 f 在 G 内是连续可微的。



如同在微积分学中一样, 容易推知, 在 G 内的解析函数的和, 乘积仍是解析函数。还有, 如果 f 和 g 在 G 内是解析的, G_1 是 G 内的点集, g 在 G_1 内不等于零, 那么 f/g 在 G_1 内是解析的。

由于常数函数与函数 $f(z) = z$ 显然是解析的。由此推出, 所有的有理函数在分母的零点集的余集内是解析的。

此外, 对于和, 积, 商的导数的通常法则仍然成立。

命题 33.6. 链式法则

设 f 和 g 分别在 G 和 Ω 内解析, $f(G) \subset \Omega$, 那么 $g \circ f$ 在 G 内是解析的, 并且对于 G 内的所有 z , 有

$$(g \circ f)'(z) = g'(f(z))f'(z).$$



证明 在 G 内固定 z_0 并选取正数 r 使得 $B(z_0; r) \subset G$ 。我们必须证明, 如果 $0 < |h_n| < r$, $\lim h_n = 0$, 则 $\lim\{h_n^{-1}[g(f(z_0 + h_n)) - g(f(z_0))]\}$ 存在且等于 $g'(f(z_0))f'(z_0)$ 。(为什么这对于证明是充分的?)

情形 1 设对于所有的 n , $f(z_0) \neq f(z_0 + h_n)$ 。在这种情形,

$$\begin{aligned} & \frac{g \circ f(z_0 + h_n) - g \circ f(z_0)}{h_n} \\ &= \frac{g \circ f(z_0 + h_n) - g \circ f(z_0)}{f(z_0 + h_n) - f(z_0)} \cdot \frac{f(z_0 + h_n) - f(z_0)}{h_n} \end{aligned}$$

因为根据 (33.5) $\lim [f(z_0 + h_n) - f(z_0)] = 0$, 所以我们有

$$\lim h_n^{-1}[g \circ f(z_0 + h_n) - g \circ f(z_0)] = g'(f(z_0))f'(z_0).$$

情形 2 设对于无穷多个 n 的值, $f(z_0) = f(z_0 + h_n)$ 。将 h_n 表示为两个序列 $\{k_n\}$ 和 $\{l_n\}$ 的和, 其中 $f(z_0) \neq f(z_0 + k_n)$ 和 $f(z_0) = f(z_0 + l_n)$ 对所有的 n 成立。由于 f 是可微的, 所以 $f'(z_0) = \lim l_n^{-1}[f(z_0 + l_n) - f(z_0)] = 0$ 。也有 $\lim l_n^{-1}[g \circ f(z_0 + l_n) - g \circ f(z_0)] = 0$ 。由情形 1, $\lim k_n^{-1}[g \circ f(z_0 + k_n) - g \circ f(z_0)] = g'(f(z_0))f'(z_0) = 0$, 所以

$$\lim h_n^{-1}[g \circ f(z_0 + h_n) - g \circ f(z_0)] = 0 = g'(f(z_0))f'(z_0) = 0.$$

一般情形容易由上面两种情形推出。

为了定义导数, 我们假定函数是定义在开集内的。如果我们说 f 是在集 A 上解析的, 而 A 不是开集, 我们的意思是指 f 在包含 A 的一个开集内是解析的。

解析函数的这个定义也许对许多读者来说有点反常。但是, 在看过解析函数论的书籍, 并且上了一年解析函数的课程和讨论班之后, 他们会发现这个定义在微积分学中已经出现过, 从而会解除一定的疑虑。但这个理论是微积分学的简单推广吗? 回答是否定的。为了表明这两者之间有多么巨大的差别, 让我们提一下, 我们以后将证明**可微函数是解析的**。这的确是一个奇特的结果, 在实变数函数的理论中是没有与此相应的结果的(例如考虑 $x^2 \sin \frac{1}{x}$)。另一个同样值得注意的结果是:**每个解析函数是无穷次可微的, 并且在它的域内的每一点有幂级数展开式**。为什么如此弱的假设竟有如此深刻的结论呢? 如果考虑一下导数的定义, 便可从中找到出现这种现象的某些征兆。

在复变数的情形, 变数可以沿无穷多个方向趋于一点 a , 但在实变数的情形, 只有两个趋近的途径。例如, 定义在 \mathbb{R} 上的函数的连续性, 可以通过它的左连续性和右连续性来讨论。这与复变数函数的情形是大不相同的。所以复变数函数有导数这句话比说实变数函数有导数更强。甚至, 如果我们令 $g(x, y) = f(x + iy)$, 把定义在 $G \subset \mathbb{C}$ 内的函数 f 看作为两个实变数的函数, 那么, 即使要求 f 是 Frechet 可微的¹, 也不能保证 f 在我们的意义下有导数。

在习题中, 我们要求读者证明 $f(z) = |z|^2$ 仅在 $z = 0$ 有导数; 但是 $g(x, y) = f(x + iy) = x^2 + y^2$ 是 Frechet 可微的。

可微性蕴含解析性在第 34 章中证明。现在我们来证明幂级数表示的函数是解析的。

¹应该是多元函数中的微分定义, 等涉及到之后补上这里的参考资料。

命题 33.7

设 $f(z) = \sum_{n=0}^{\infty} a_n(z-a)^n$ 的收敛半径 $R > 0$, 那么:

(a) 对于每个 $k \geq 1$, 级数

$$\sum_{n=k}^{\infty} n(n-1)\cdots(n-k+1)a_n(z-a)^{n-k} \quad (33.2.1)$$

的收敛半径为 R ;

(b) 函数 f 在 $B(a; R)$ 内是无穷次可微的, 并且对于所有的 $k \geq 1$ 及 $|z-a| < R$, $f^{(k)}(z)$ 由级数 (33.2.1) 给出;

(c) 对于 $n \geq 0$,

$$a_n = \frac{1}{n!} f^{(n)}(a). \quad (33.2.2)$$



证明 仍假定 $a = 0$.

(a) 我们首先注意到, 如果对于 $k = 1$, (a) 被证明了, 那么 (a) 在 $k = 2, \dots$ 时也将随之成立。事实上, (a) 在 $k = 1$ 的情形应用到级数 $\sum n a_n(z-a)^{n-1}$ 上, 便得到 $k = 2$ 的情形。我们已知 $R^{-1} = \limsup |a_n|^{\frac{1}{n}}$, 而希望证明 $R^{-1} = \limsup |n a_n|^{\frac{1}{n-1}}$ 。由 l'Hôpital 法则², $\lim_{n \rightarrow \infty} \frac{\log n}{n-1} = 0$, 所以 $\lim_{n \rightarrow \infty} n^{\frac{1}{n-1}} = 1$ 。如果能够证明

$$\limsup |a_n|^{\frac{1}{n-1}} = R^{-1},$$

我们的结果便从习题2.推出。

设 $(R')^{-1} = \limsup |a_n|^{\frac{1}{n-1}}$, 那么 R' 是 $\sum_1^{\infty} a_n z^{n-1} = \sum_0^{\infty} a_{n+1} z^n$ 的收敛半径, 注意到 $z \sum a_{n+1} z^n + a_0 = \sum a_n z^n$, 所以如果 $|z| < R'$, 那么 $\sum |a_n z^n| \leq |z_0| + |z| \sum |a_{n+1} z^n| < \infty$ 。这就给出 $R' \leq R$ 。如果 $|z| < R$, 且 $z \neq 0$, 那么 $\sum |a_n z^n| < \infty$, $\sum |a_{n+1} z^n| \leq \frac{1}{|z|} \cdot \sum |a_n z^n| + \frac{1}{|z|} |a_0| < \infty$, 所以 $R \leq R'$ 。这就得到 $R = R'$ 。(a) 证毕。

(b) 对于 $|z| < R$, 设 $g(z) = \sum_{n=1}^{\infty} n a_n z^{n-1}$, $s_n(z) = \sum_{k=0}^n a_k z^k$, $R_n(z) = \sum_{k=n+1}^{\infty} a_k z^k$ 。固定 $B(0; R)$ 内的一点 w , 固定 r 使得 $|w| < r < R$ 。我们要证明 $f'(w)$ 存在且等于 $g(w)$ 。为此, 设 $\delta > 0$ 是任意的, 只要使得 $\bar{B}(w; \delta) \subset B(0; r)$ (在后面的证明中我们将进一步限定 δ), 设 $z \in B(w; \delta)$, 那么

$$\begin{aligned} & \frac{f(z) - f(w)}{z - w} - g(w) \\ &= \left[\frac{s_n(z) - s_n(w)}{z - w} = s'_n(w) \right] + [s'_n(w) - g(w)] \\ & \quad + \left[\frac{R_n(z) - R_n(w)}{z - w} \right], \end{aligned} \quad (33.2.3)$$

现在

$$\frac{R_n(z) - R_n(w)}{z - w} = \frac{1}{z - w} \sum_{k=n+1}^{\infty} a_k (z^k - w^k) = \sum_{k=n+1}^{\infty} a_k \left(\frac{z^k - w^k}{z - w} \right).$$

²l'Hôpital, 洛必达。

而

$$\left| \frac{z^k - w^k}{z - w} \right| = |z^{k-1} + z^{k-2}w + \cdots + zw^{k-2} + w^{k-1}| \leq kr^{k-1}.$$

因此

$$\left| \frac{R_n(z) - R_n(w)}{z - w} \right| \leq \sum_{k=n+1}^{\infty} |a_k| kr^{k-1}.$$

因为 $r < R$, 所以 $\sum_{k=1}^{\infty} |a_k| kr^{k-1}$ 收敛, 于是对于任意的 $\epsilon > 0$, 存在正整数 N_1 , 使得当 $n \geq N_1$ 时,

$$\left| \frac{R_n(z) - R_n(w)}{z - w} \right| < \epsilon/3, \quad (z \in B(w; \delta))$$

又 $\lim s'_n(w) = g(w)$, 所以存在正整数 N_2 , 使得当 $n \geq N_2$ 时, $|s'_n(w) - g(w)| < \epsilon/3$. 设 $n = \max(N_1, N_2)$, 这时我们可选取 $\delta > 0$, 使得当 $0 < |z - w| < \delta$ 时,

$$\left| \frac{s_n(z) - s_n(w)}{z - w} - s'_n(w) \right| < \epsilon/3.$$

把这些不等式代入 (33.2.3), 便得到

$$\left| \frac{f(z) - f(w)}{z - w} - g(w) \right| < \epsilon.$$

只要 $0 < |z - w| < \delta$. 这就是 $f'(w) = g(w)$.

(c) 直接计算, 我们得到 $f(0) = f^{(0)}(0) = a_0$. 利用 (33.2.1) (当 $a = 0$ 时), 我们得到 $f^{(k)}(0) = k!a_k$, 这就给出了公式 (33.2.2).

推论 33.1

如果级数 $\sum_{n=0}^{\infty} a_n(z-a)^n$ 的收敛半径 $R > 0$, 那么 $f(z) = \sum_{n=0}^{\infty} a_n(z-a)^n$ 在 $B(a; R)$ 内是解析的.

因此 $\exp z = \sum_{n=0}^{\infty} z^n/n!$ 在 \mathbb{C} 内是解析的. 在进一步考察指数函数与定义 $\cos z, \sin z$ 以前, 必须证明下面的结果.

命题 33.8

如果 G 是连通开集, $f: G \rightarrow \mathbb{C}$ 是可微的, 并且对于 G 内所有的 z , $f'(z) = 0$, 那么 f 是常数.

证明 在 G 内固定 z_0 , 设 $w_0 = f(z_0)$, $A = \{z \in G : f(z) = w_0\}$. 我们将通过证明 A 在 G 内既是开的, 又是闭的, 来证明 $A = G$. 设 $z \in G$, $\{z_n\} \subset A$, $z = \lim z_n$, 因为 $f(z_n) = w_0$ 对于每个 $n \geq 1$ 成立, 以及 f 是连续的, 所以我们得到, $f(z) = w_0$, 或者说 $z \in A$. 于是 A 在 G 内是闭的. 现在在 A 内固定 a , 设 $\epsilon > 0$, 使得 $B(a; \epsilon) \subset G$. 如果 $z \in B(a; \epsilon)$, 令 $g(t) = f(tz + (1-t)a)$, $0 \leq t \leq 1$, 那么

$$\frac{g(t) - g(s)}{t - s} = \frac{g(t) - g(s)}{(t-s)z + (s-t)a} \cdot \frac{(t-s)z + (s-t)a}{t-s}. \quad (33.2.4)$$

如果我们令 $t \rightarrow s$, 便得到

$$\lim_{t \rightarrow s} \frac{g(t) - g(s)}{t - s} = f'(sz + (1-s)a) \cdot (z - a) = 0.$$

即对于 $0 \leq s \leq t$, $g'(s) = 0$, 因此 g 是一个常数. 所以 $f(z) = g(1) = g(0) = f(a) = w_0$.

即 $B(a; \epsilon) \subset A$, A 也是开集。

现在对 $f(z) = e^z$, 求导数, 由命题33.7,

$$\begin{aligned} f'(z) &= \sum_{n=1}^{\infty} \frac{n}{n!} z^{n-1} = \sum_{n=1}^{\infty} \frac{1}{(n-1)!} z^{n-1} \\ &= \sum_{n=0}^{\infty} \frac{z^n}{n!} = f(z). \end{aligned}$$

于是复的指数函数和实的情形有相同的性质, 即

$$\frac{d}{dz} e^z = e^z. \quad (33.2.5)$$

对于 \mathbb{C} 内某一固定的 a , 设 $g(z) = e^z e^{a-z}$, 那么 $g'(z) = e^z e^{a-z} + e^z (-e^{a-z}) = 0$, 因此对于 \mathbb{C} 中的所有 z 和某一常数 ω , $g(z) = \omega$. 特别地, 利用 $e^0 = 1$, 我们得到 $\omega = g(0) = e^a$. 所以对于所有的 z , $e^z e^{a-z} = e^a$. 于是对于 \mathbb{C} 中所有的 a, b , $e^{a+b} = e^a \cdot e^b$. 这也给出 $1 = e^z e^{-z}$, 它蕴含对于任意的 z , $e^z \neq 0$ 以及 $e^{-z} = 1/e^z$. 我们再回到 e^z 的幂级数. 因为这个级数的所有系数是实的, 所以我们得到 $\exp \bar{z} = \overline{\exp z}$. 特别地, 对于实数 θ , 我们得到 $|e^{i\theta}|^2 = e^{i\theta} e^{-i\theta} = e^0 = 1$. 更一般地, $|e^z|^2 = e^z e^{\bar{z}} = e^{z+\bar{z}} = \exp(2\Re z)$, 于是

$$|\exp z| = \exp(\Re z). \quad (33.2.6)$$

所以我们看出 e^z 和实函数 e^x 有同样的性质. 仍和实的幂级数类似, 我们也用幂级数定义 $\cos z$ 和 $\sin z$.

$$\begin{aligned} \cos z &= 1 - \frac{z^2}{2!} + \frac{z^4}{4!} - \cdots + (-1)^n \frac{z^{2n}}{(2n)!} + \cdots, \\ \sin z &= z - \frac{z^3}{3!} + \frac{z^5}{5!} - \cdots + (-1)^n \frac{z^{2n+1}}{(2n+1)!} + \cdots. \end{aligned}$$

这两个幂级数的收敛半径都是 ∞ , 所以 $\cos z$ 和 $\sin z$ 在 \mathbb{C} 内是解析的. 利用命题33.7, 我们得到 $(\cos z)' = -\sin z$, $(\sin z)' = \cos z$. 通过幂级数的运算 (因为幂级数是绝对收敛的, 这是允许的), 得到

$$\cos z = \frac{1}{2}(e^{iz} + e^{-iz}), \quad \sin z = \frac{1}{2i}(e^{iz} - e^{-iz}). \quad (33.2.7)$$

这就得到, 对于 \mathbb{C} 中的 z , 有 $\cos^2 z + \sin^2 z = 1$ 以及

$$e^{iz} = \cos z + i \sin z. \quad (33.2.8)$$

特别地, 如果在 (33.2.8) 中设 z 是实数 θ , 我们得到 $e^{i\theta} = \operatorname{cis} \theta$. 因此, 对于 \mathbb{C} 中的 z

$$z = |z|e^{i\theta}, \quad (33.2.9)$$

其中 $\theta = \arg z$. 因为 $e^{x+iy} = e^x + e^{iy}$, 所以我们有 $|e^z| = \exp(\Re z)$ 及 $\arg e^z = \Im z$.

说 f 是以 c 为周期的周期函数, 如果 $f(z+c) = f(z)$ 对于 \mathbb{C} 中的所有 z 成立. 如果 c 是 e^z 的周期, 那么 $e^z = e^{z+c} = e^z e^c$ 蕴含 $e^c = 1$. 因为 $1 = |e^c| = \exp(\Re c)$, $\Re(c) = 0$. 于是对于 \mathbb{R} 中的某一 θ , $c = i\theta$. 但是由于 $1 = e^c = e^{i\theta} = \cos \theta + i \sin \theta$, 给出 e^z 的周期是 $2\pi i$ 的倍数. 于是如果我们用直线 $\Im z = \pi(2k-1)$, k 是任意整数, 把平面分成无穷多个水平带形, 指数函数在每个带形内有相同的性质. 这个周期性是实指数所不具备的一个性质. 注意, 通过考察复函数, 我们证明了指函数和三角函数之间的关系式 (33.2.8). 这个关系式单凭我们关于实函数的知识是料想不到的。

现在我们来定义 $\log z$, 我们可以采取和前面一样的办法, 设 $\log z$ 是实对数函数在某点附近的幂级数展开式。但是这仅给出在某一圆内的 $\log z$ 。定义对数为 t^{-1} 从 1 到 x ($x > 0$) 的积分, 这个方法是可行, 但在复的情形, 这样定义有点冒险, 并且是不能令人满意的。又因为与实的情形不同, e^z 并不是一一的映照, 所以 $\log z$ 不能定义为 e^z 的反函数。但是我们可以有与此类似的做法。

我们要这样定义 $\log w$, 使得当 $z = \log w$ 时, $w = e^z$ 。现在, 因为对于任意 z , $e^z \neq 0$, 所以我们不能定义 $\log 0$, 设 $e^z = w$, $w \neq 0$; 如果 $z = x + iy$, 那么 $|w| = e^x$, 且对于某个 k , $y = \arg w + 2\pi k$. 因此

$$\{\log |w| + i(\arg w + 2\pi k) : k \text{ 是任意整数}\} \quad (33.2.10)$$

是 $e^z = w$ 的解的集。(注意: $\log |w|$ 是通常实的对数。)

定义 33.3

如果 G 是 \mathbb{C} 中的连通开集, $f: G \rightarrow \mathbb{C}$ 是一个连续函数, 使得对于 G 内的所有 z , $z = \exp f(z)$, 那么 f 是对数的一个分支。



注意 $0 \notin G$ 。

设 f 是连通集 G 内的一个给定的对数分支, k 是整数。 $g(z) = f(z) + 2\pi ki$, 那么 $\exp g(z) = \exp f(z) = z$, 所以 g 也是一个对数分支。反之, 如果 f, g 都是 $\log z$ 的分支, 那么对于 G 内的每个 z , $f(z) = g(z) + 2\pi ki$, k 是依赖于 z 的某一整数。对于 G 内的每个 z , k 是相同的吗? 回答是肯定的。事实上, 如果 $h(z) = \frac{1}{2\pi i}[f(z) - g(z)]$, 那么 $h(z)$ 在 G 内是连续的, 并且 $h(G) \subset \mathbb{Z}$ (整数集)。因为 G 是连通的, 所以 $h(G)$ 也是连通的 (第??章定理32.7)。因此在 \mathbb{Z} 中有一个整数 k , 使得 $f(z) + 2\pi ik = g(z)$ 对于 G 内的所有 z 都成立。这就得到下面的命题。

命题 33.9

如果 $G \subset \mathbb{C}$ 是连通开集, f 是 G 内 $\log z$ 的一个分支, 那么 $\log z$ 的所有分支可表示为 $f(z) + 2\pi ki$, $k \in \mathbb{Z}$ 。



现在让我们在某一个连通开集内至少作出 $\log z$ 的一个分支。设

$$G = \mathbb{C} - \{z : z \leq 0\};$$

即, 沿负实轴“切开”平面。显然 G 是连通的, 并且对于 G 内的每个 z , 能够唯一地表示为 $z = |z|e^{i\theta}$, 其中 $-\pi < \theta < \pi$, 对于 θ 在这个范围内, 定义 $f(re^{i\theta}) = \log r + i\theta$ 。我们把连续性的证明留给读者 (习题9.), 由此推出 f 是 G 内对数的一个分支。

f 是解析的吗? 为了回答这个问题, 我们先证明一个一般性的事实。

命题 33.10

设 G 和 Ω 是 \mathbb{C} 的开子集。假定 $f: G \rightarrow \mathbb{C}$, $g: \Omega \rightarrow \mathbb{C}$ 是连续函数, 使得 $f(G) \subset \Omega$, 且 $g(f(z)) = z$ 对于 G 内的所有 z 成立。如果 g 是可微的, 且 $g'(z) \neq 0$, 那么 f 是

可微的, 且

$$f'(z) = \frac{1}{g'(f(z))}.$$

如果 g 是解析的, 那么 f 也是解析的。



证明 在 G 内固定一点 a . 设 $h \in \mathbb{C}$, $h \neq 0$, 使得 $a + h \in G$. 因此 $a = g(f(a))$, $a + h = g(f(a + h))$ 蕴含 $f(a) \neq f(a + h)$. 又

$$\begin{aligned} 1 &= \frac{g(f(a + h)) - g(f(a))}{h} \\ &= \frac{g(f(a + h)) - g(f(a))}{f(a + h) - f(a)} \cdot \frac{f(a + h) - f(a)}{h}. \end{aligned}$$

现在当 $h \rightarrow 0$ 时, 左边的极限当然是 1, 所以右边的极限也存在。因为 $\lim_{h \rightarrow 0} [f(a + h) - f(a)] = 0$, 所以

$$\lim_{h \rightarrow 0} \frac{g(f(a + h)) - g(f(a))}{f(a + h) - f(a)} = g'(f(a)).$$

因此, 由 $g'(f(a)) \neq 0$ 可知

$$\lim_{h \rightarrow 0} \frac{f(a + h) - f(a)}{h}$$

存在, 并且 $1 = g'(f(a))f'(a)$ 。

于是 $f'(z) = [g'(f(a))]^{-1}$ 。如果 g 是解析的, 那么 g' 是连续的, 由此得到 f 是解析的。

推论 33.2

对数函数的分支是解析的, 它的导数是 z^{-1} 。



我们把上面定义在 $\mathbb{C} - \{z : z \leq 0\}$ 的对数的特殊分支, 称为对数的主分支 (principal branch)。如果不作别的声明, 我们总是把 $\log z$ 当作对数的主分支。

如果 f 是对数函数在连通开集 G 内的分支, b 是 \mathbb{C} 中的固定点, 那么定义 $g : G \rightarrow \mathbb{C}$ 为 $g(z) = \exp(bf(z))$ 。如果 b 是一个整数, 那么 $g(z) = z^b$ 。对于具有 $\log z$ 的分支的连通开集, 我们用这种方式定义 z^b 的分支, 其中 b 在 \mathbb{C} 中。如果我们把 $g(z) = z^b$ 作为一个函数, 我们总是把这个函数理解为 $z^b = \exp b \log z$, 其中 $\log z$ 是对数的主分支, 因为 $\log z$ 是解析的, 所以 z^b 也是解析的。

从刚才的考虑可以明显看出, 连通性在解析函数论中起着重要作用。例如, 如果 G 不是连通的, 那么命题 33.8 是不对的。连通性在这里所起的作用类似于区间在微积分中所起的作用。因为这个原因, 引进术语“域³”是方便的。一个域是平面上的一个连通开子集。

这一节以讨论 Cauchy-Riemann 方程作为结束。设 $f : G \rightarrow \mathbb{C}$ 是解析的。对于 G 内的 $x + iy$, 令 $u(x, y) = \Re f(x + iy)$, $v(x, y) = \Im f(x + iy)$ 。我们用两种不同的方法计算极限

$$f'(z) = \lim_{h \rightarrow 0} \frac{f(z + h) - f(z)}{h}.$$

³这个域不是代数中的域, 这里的域应该对应英文 domain, 而代数中的域对应 field。

先让 h 取实值趋于零。对于 $h \neq 0$, h 是实的, 我们得到

$$\begin{aligned}\frac{f(z+h)-f(z)}{h} &= \frac{f(x+h+iy)-f(x+iy)}{h} \\ &= \frac{u(x+h,y)-u(x,y)}{h} \\ &\quad + i \frac{v(x+h,y)-v(x,y)}{h}\end{aligned}$$

令 $h \rightarrow 0$, 得到

$$f'(z) = \frac{\partial u}{\partial x}(x,y) + i \frac{\partial v}{\partial x}(x,y). \quad (33.2.11)$$

现在让 h 取纯虚值趋于零, 即对于 $h \neq 0$, h 是实的,

$$\begin{aligned}\frac{f(z+ih)-f(z)}{ih} &= -i \frac{u(x,y+h)-u(x,y)}{h} \\ &\quad + \frac{v(x,y+h)-v(x,y)}{h}\end{aligned}$$

于是

$$f'(z) = -i \frac{\partial u}{\partial y}(x,y) + \frac{\partial v}{\partial y}(x,y). \quad (33.2.12)$$

令 (33.2.11) 和 (33.2.12) 的实部虚部相等, 我们便得到 Cauchy-Riemann 方程

$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y}, \quad \frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x} \quad (33.2.13)$$

假定 u 和 v 有二阶连续偏导数 (我们最终将证明它们是无穷次可微的)。对 Cauchy-Riemann 方程求微商, 我们得到

$$\frac{\partial^2 u}{\partial x^2} = \frac{\partial^2 v}{\partial x \partial y}, \quad \frac{\partial^2 u}{\partial y^2} = -\frac{\partial^2 v}{\partial y \partial x}.$$

因此

$$\frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2} = 0, \quad (33.2.14)$$

满足 (33.2.14) 的任意一个具有连续的二阶偏导数的函数称为调和函数。类似地, v 也是调和的。我们将在第36章中研究调和函数。

设 G 是平面上的一个域, u 和 v 是定义在 G 内具有连续偏导数的函数。进而设 u, v 满足 Cauchy-Riemann 方程。为此, 设 $z = x+iy \in G, B(z;r) \subset G$. 如果 $h = s+it \in B(0;r)$, 那么

$$\begin{aligned}u(x+s,y+t)-u(x,y) &= [u(x+s,y+t)-u(x,y+t)] \\ &\quad + [u(x,y+t)-u(x,y)].\end{aligned}$$

把一元函数导数的中值定理应用到这两个括号内的式子上, 那么对于 $B(0;r)$ 内的每个 $s+it$, 都有数 s_1 和 $t_1, |s_1| < |s|, |t_1| < |t|$, 使得

$$\begin{cases} u(x+s,y+t)-u(x,y+t) = u_x(x+s_1,y+t)s, \\ u(x,y+t)-u(x,y) = u_y(x,y+t_1)t. \end{cases} \quad (33.2.15)$$

令 $\varphi(s,t) = [u(x+s,y+t)-u(x,y)] - [u_x(x,y)s + u_y(x,y)t]$, 由 (33.2.15) 得到

$$\begin{aligned}\frac{\varphi(s,t)}{s+it} &= \frac{s}{s+it} [u_x(x+s_1,y+t)-u_x(x,y)] \\ &\quad + \frac{t}{s+it} [u_y(x,y+t_1)-u_y(x,y)].\end{aligned}$$

但是由 $|s| < |s + it|$, $|t| < |s + it|$, $|s_1| < |s|$, $|t_1| < |t|$, 以及 u_x, u_y 是连续的, 得到

$$\lim_{s+it \rightarrow 0} \frac{\varphi(s, t)}{s + it} = 0. \quad (33.2.16)$$

因此

$$\begin{aligned} u(x + s, y + t) - u(x, y) &= u_x(x, y)s + u_y(x, y)t \\ &\quad + \varphi(s, t), \end{aligned}$$

其中 φ 满足 (33.2.16)。类似地,

$$v(x + s, y + t) - v(x, y) = v_x(x, y)s + v_y(x, y)t + \psi(s, t).$$

其中 ψ 满足

$$\lim_{s+it \rightarrow 0} \frac{\psi(s, t)}{s + it} = 0. \quad (33.2.17)$$

利用 u, v 满足 Cauchy-Riemann 方程这个事实, 容易看出

$$\frac{f(z + s + it) - f(z)}{s + it} = u_x(z) + iv_x(z) + \frac{\varphi(s, t) + i\psi(s, t)}{s + it}.$$

根据 (??) 和 (??), f 是可微的, 并且 $f'(z) = u_x(z) + iv_x(z)$. 因为 u_x, v_x 是连续的, 所以 f' 是连续的, f 是解析的。我们把这些结果总结如下。

定理 33.2

设 u, v 是定义在区域 G 内的实值函数, 假定 u, v 有连续的偏导数。 $f: G \rightarrow \mathbb{C}$ 定义为 $f(z) = u(z) + iv(z)$ 。当且仅当 u, v 满足 Cauchy-Riemann 方程时, f 是解析的。



例子 $u(x, y) = \log(x^2 + y^2)^{\frac{1}{2}}$ 在 $G = \mathbb{C} - \{0\}$ 内是调和的吗? 回答是肯定的。对 u 求微商可看出它满足 (??)。但是也可通过观察下述事实来证明: 在 G 内的每一点的邻域内, u 是定义在该邻域的一个解析函数 (哪个函数?) 的实部。

下面是关于调和函数的另一个问题。这个问题将在第35章35.3中作详细的研究。设 G 是平面上的一个域, $u: G \rightarrow \mathbb{R}$ 是调和的。是否存在一个调和函数 $v: G \rightarrow \mathbb{R}$, 使得 $f = u + iv$ 在 G 内是解析的? 如果这样的函数 v 存在, 就称它是 u 的共轭调和函数。如果 v_1 和 v_2 是 u 的两个共轭调和函数, 那么 $i(v_1 - v_2) = (u + iv_1) - (u + iv_2)$ 在 G 内是解析的, 并且仅取纯虚值。由此推出, 一个调和函数的两个共轭调和函数相差为一常数 (习题14.)。

回到共轭调和函数的存在性问题上。在域 $G = \mathbb{C} - \{0\}$ 内调和函数的上述例子 $u(z) = \log|z|$, 没有共轭调和函数。事实上, 如果它有共轭调和函数, 那么便可在 G 内定义对数函数的一个解析分支, 而这是办不到的 (习题21.)。但是存在一些区域, 在这些区域内每个调和函数有共轭调和函数。特别地, 现在证明, 当 G 是任意圆或是整个平面时, 就是这种情形。

定理 33.3

设 G 或者是整个平面, 或者是某一个开圆。如果 $u: G \rightarrow \mathbb{R}$ 是一个调和函数, 那么 u 有共轭调和函数。



证明 为了完成定理的证明, 需要用到积分号下求微商的 Leibniz 法则 (这个法则将在第34章的34.7的命题中叙述和证明), 设 $G = B(0; R)$, $0 < R \leq \infty$. 又设 $u : G \rightarrow \mathbb{R}$ 是调和函数。我们通过寻求调和函数 v , 使得 u, v 满足 Cauchy-Riemann 方程, 来完成定理的证明。为此定义

$$v(x, y) = \int_0^y u_x(x, t) dt + \varphi(x),$$

并确定 φ , 使得 $v_x = -u_y$ 。上述等式两边对 x 求微商, 得到

$$\begin{aligned} v_x(x, y) &= \int_0^y u_{xx}(x, t) dt + \varphi'(x) = - \int_0^y u_{yy}(x, t) dt + \varphi'(x) \\ &= -u_y(x, y) + u_y(x, 0) + \varphi'(x). \end{aligned}$$

所以, 必定有 $\varphi'(x) = -u_y(x, 0)$ 。容易验证 u 和

$$v(x, y) = \int_0^y u_x(x, t) dt - \int_0^x u_y(s, 0) ds$$

确实满足 Cauchy-Riemann 方程。

G 是圆或是 \mathbb{C} 这个条件用在何处? 这个证明方法为什么不能作足够的修改使之适用于一般的域? 当 $G = \mathbb{C} - \{0\}$, $u = \log |z|$ 时, 这个证明在何处失效?

第三十三章 习题

1. 证明: $f(z) = |z|^2 = x^2 + y^2$ 仅在原点有导数。
2. 证明: 如果 b_n, a_n 是正实数, $0 < b = \lim b_n, a = \limsup a_n$, 则 $ab = \limsup (a_n b_n)$. 如果正德这一要求去掉, 结论仍成立吗?
3. 证明: $\lim n^{\frac{1}{n}} = 1$.
4. 证明: $(\cos z)' = -\sin z, (\sin z)' = \cos z$.
5. 导出公式 (33.2.7)。
6. 描画出下列各集: $\{z : e^z = i\}, \{z : e^z = -1\}, \{z : e^z = -i\}, \{z : \cos z = 0\}, \{z : \sin z = 0\}$.
7. 证明对于 $\cos(z+w), \sin(z+w)$ 的公式。
8. 定义 $\tan z = \frac{\sin z}{\cos z}$; 这个函数在何处有定义? 在何处是解析的?
9. 设 $z_n, z \in G = \mathbb{C} - \{z : z \leq 0\}$, 且 $z_n = r_n e^{i\theta_n}, z = r e^{i\theta}$, 其中 $-\pi < \theta, \theta_n < \pi$. 证明: 如果 $z_n \rightarrow z$, 那么 $\theta_n \rightarrow \theta, r_n \rightarrow r$.
10. 证明命题33.10的下述推广: 设 G 和 Ω 是 \mathbb{C} 中的开集又设 f 和 h 是定义在 G 内的函数, $g : \Omega \rightarrow \mathbb{C}, f(G) \subset \Omega, g$ 和 h 是解析的, 对于任意 $w, g'(w) \neq 0, f$ 是连续的, h 是一一的, 并且对于 G 内的 z , 它们满足 $h(z) = g(f(z))$. 证明 f 是解析的, 给出 $f'(z)$ 的公式。
11. 设 $f : G \rightarrow \mathbb{C}$ 是对数函数的一个分支, n 是一个整数, 证明对于 G 内的所有的 z , $z^n = \exp(nf(z))$.
12. 证明: 函数 $z^{\frac{1}{2}}$ 的实部总是正的。
13. 设 $G = \mathbb{C} - \{z : z \leq 0\}, n$ 是正整数。试求出所有的解析函数 $f : G \rightarrow \mathbb{C}$, 使得对于所有的 $z \in G, z = (f(z))^n$.

14. 设 $f: G \rightarrow \mathbb{C}$ 是解析的, G 是连通的, 证明: 如果 $f(z)$ 对于 G 内的所有 z 是实的, 那么 f 是常数。
15. 对于 $r > 0$, 设 $A = \{w: w = \exp(\frac{1}{z}), 0 < |z| < r\}$, 试确定这个集 A 。
16. 找出一个连通开集 $G \subset \mathbb{C}$ 和 G 内的两个连续函数 f 和 g , 使得 $f(z)^2 = g(z)^2 = 1 - z^2$ 对于 G 内的所有 z 都成立。你能使 G 最大吗? f 和 g 是解析的吗?
17. 给出 $\sqrt{1-z}$ 的主分支。
18. 设 f 和 g 分别是 z^a 和 z^b 的分支。证明: fg 是 z^{a+b} 的分支, f/g 是 z^{a-b} 的分支。设 $f(G) \subset G, g(G) \subset G$, 证明: $f \circ g$ 和 $g \circ f$ 都是 z^{ab} 的分支。
19. 设 G 是一个域, 定义 $G^* = \{z: \bar{z} \in G\}$ 。如果 $f: G \rightarrow \mathbb{C}$ 是解析的, 证明: $f^*: G^* \rightarrow \mathbb{C}, f^*(z) = \overline{f(\bar{z})}$ 也是解析的。
20. 设 z_1, z_2, \dots, z_n 是复数, 并且对于 $1 \leq k \leq n, \Re z_k > 0, \Re(z_1 \cdots z_n) > 0$ 。证明 $\log(z_1 \cdots z_n) = \log z_1 + \cdots + \log z_n$, 其中 $\log z$ 是对数函数的主分支。如果关于 z_k 的限制取消, 这个公式仍成立吗?
21. 证明: 不存在定义于 $G = \mathbb{C} - \{0\}$ 的对数分支。(提示: 假如这样的分支存在, 将它与主分支比较。)

33.3 作为映照得解析函数. Möbius 变换

考虑函数 $f(z) = z^2$ 。如果 $z = x + iy, \mu + i\nu = f(z)$, 那么 $\mu = x^2 - y^2, \nu = 2xy$ 。因此双曲线 $x^2 - y^2 = c$ 和 $2xy = d$ 由 f 映为直线 $\mu = c$ 和 $\nu = d$ 。一个有趣的事实是: 当 c 和 d 不为 0 时, 这些双曲线正如它们的像一样是正交的。这个事实并不是孤立的现象。在这一节稍后, 我们将对这个性质作一般性的探讨。

现在考察直线 $x = c$ 和 $y = d$ 变成什么。先考察 $x = c$ (y 任意); f 把这条直线映为 $\mu = c^2 - y^2, \nu = 2cy$ 。消去 y , 我们得到 $x = c$ 被映为抛物线 $\nu^2 = -4c^2(\mu - c^2)$ 。类似地, f 把 $y = d$ 映为抛物线 $\nu^2 = 4d(\mu + d^2)$ 。这些抛物线在 $(c^2 - d^2, \pm 2|cd|)$ 相交。应当指出, 当 $c \rightarrow 0$ 时, 抛物线 $\nu^2 = -4c^2(\mu - c^2)$ 逐渐合拢, 而接近于负实轴。这与函数 $z^{\frac{1}{2}}$ 把 $G = \mathbb{C} - \{z: z \leq 0\}$ 映为 $\{z: \Re z > 0\}$ 这一事实相吻合。还要注意, $x = c$ 和 $x = -c$ ($y = d$ 和 $y = -d$) 被映为同一抛物线。

中心在原点的圆周变成什么呢? 若 $z = re^{i\theta}$, 那么 $f(z) = r^2 e^{2i\theta}$ 。于是以原点为中心, 半径为 r 的圆周被映为半径为 r^2 的圆周, 两个点映为同一点⁴。

最后, 扇形 $S(\alpha, \beta) = \{z: \alpha < \arg z < \beta\}, \alpha < \beta$ 变为什么? 容易看出 $S(\alpha, \beta)$ 的像是扇形 $S(2\alpha, 2\beta)$, 当 $\beta - \alpha < \pi$ 时, f 限制在 $S(\alpha, \beta)$ 上是一一的。

上面的讨论阐明了 $f(z) = z^2$ 的性质, 而且对于研究其他解析函数的映照性质也是有用的。在解析函数的理论中, 下述问题占有重要的地位: 给定两个连通集 G 和 Ω , 是否存在定义在 G 内的解析函数, 使得 $f(G) = \Omega$? 除了本身的兴趣外, 这个问题的解 (或者宁可说是关于解的存在性问题) 是很有用的。

⁴ (r, θ) 和 $(r, \theta + \pi)$ 映为同一个点

定义 33.4

域 $G \subset \mathbb{C}$ 内的一条路径是一个连续函数 $\gamma : [a, b] \rightarrow G$, $[a, b]$ 是 \mathbb{R} 中的某一区间。如果对于 $[a, b]$ 内的每一个 t , $\gamma'(t)$ 存在, 并且 $\gamma' : [a, b] \rightarrow \mathbb{C}$ 是连续的, 那么 γ 是光滑路径。 γ 是分段光滑的, 如果存在 $[a, b]$ 的一个分割, $a = t_0 < t_1 < \cdots < t_n = b$, 使得 γ 在每个子区间 $[t_{j-1}, t_j]$ 上, $1 \leq j \leq n$, 是光滑的。



称函数 $\gamma : [a, b] \rightarrow \mathbb{C}$ 对于 $[a, b]$ 内的每个 t 都有导数 $\gamma'(t)$, 意思是指: 对于 $a < t < b$,

$$\lim_{h \rightarrow 0} \frac{\gamma(t+h) - \gamma(t)}{h} = \gamma'(t)$$

存在; 对于 $t = a$ 和 $t = b$ 分别存在右极限和左极限。当然, 这等价于说 $\Re(\gamma)$ 和 $\Im(\gamma)$ 有导数。

设 $\gamma : [a, b] \rightarrow G$ 是光滑路径, 并且对于 (a, b) 内的某一 t_0 , $\gamma'(t_0) \neq 0$, 那么 γ 在点 $z_0 = \gamma(t_0)$ 有切线。这条切线通过点 z_0 , 方向是 (向量) $\gamma'(t_0)$ 的方向, 或者说这条线的斜率是 $\tan \arg \gamma'(t_0)$ 。如果 γ_1 和 γ_2 是两条光滑路径, $\gamma_1(t_1) = \gamma_2(t_2) = z_0$, $\gamma'_1(t_1) \neq 0$, $\gamma'_2(t_2) \neq 0$, 那么路径 γ_1 和 γ_2 在 z_0 的夹角定义为

$$\arg \gamma'_2(t_2) - \arg \gamma'_1(t_1).$$

设 γ 是 G 内的光滑路径, $f : G \rightarrow \mathbb{C}$ 是解析的, 那么 $\sigma = f \circ \gamma$ 也是一条光滑路径, 并且 $\sigma'(t) = f'(\gamma(t))\gamma'(t)$ 。设 $z_0 = \gamma(t_0)$, 假定 $\gamma'(t_0) \neq 0$, $f'(z_0) \neq 0$, 那么 $\sigma'(t_0) \neq 0$, 并且 $\arg \sigma'(t_0) = \arg f'(z_0) + \arg \gamma'(t_0)$, 即

$$\arg \sigma'(t_0) - \arg \gamma'(t_0) = \arg f'(z_0). \quad (33.3.1)$$

现在设 γ_1, γ_2 是光滑路径, $\gamma_1(t_1) = \gamma_2(t_2) = z_0$, 并且 $\gamma'_1(t_1) \neq 0 \neq \gamma'_2(t_2)$ 。设 $\sigma_1 = f \circ \gamma_1, \sigma_2 = f \circ \gamma_2$ 。还假定路径 γ_1 和 γ_2 在 z_0 彼此不相切, 即假定 $\arg \gamma_1(t_1) \neq \arg \gamma_2(t_2)$ 。由等式 (33.3.1) 得到

$$\arg \gamma'_2(t_2) - \arg \gamma'_1(t_1) = \arg \sigma'_2(t_2) - \arg \sigma'_1(t_1). \quad (33.3.2)$$

这就是说, 任意给定过 z_0 的两条路径, f 把这两条路径映过 $w_0 = f(z_0)$ 的两条路径, 当 $f'(z) \neq 0$ 时, 曲线的夹角的大小和方向都是保持不变的。综上所述有下面的定理。

定理 33.4

如果 $f : G \rightarrow \mathbb{C}$ 是解析的, 那么在 $f'(z_0) \neq 0$ 的每一点 z_0 , f 保持角度不变。



函数 $f : G \rightarrow \mathbb{C}$ 保持角度不变, 并且

$$\lim_{z \rightarrow a} \frac{|f(z) - f(a)|}{|z - a|}$$

也存在, 这种函数称为共形映照。如果 f 是解析的, 且对于任意 z , $f'(z) \neq 0$, 则 f 是共形的, 反之亦然。

如果 $f(z) = e^z$, 那么 f 在整个 \mathbb{C} 中是共形的。让我们进一步察看一下指数函数。若 $z = c + iy$, c 是固定的。那么 $f(z) = re^{iy}$, $r = e^c$, 即 f 把直线 $x = c$ 映为中心在原点, 半径为 e^c 的圆周, 又, f 把直线 $y = d$ 映为无穷射线 $\{re^{id} : 0 < r < \infty\}$ 。

我们已经看到, 在任何宽度 $< 2\pi$ 的水平带形上, e^z 是一一的, 设 $G = \{z : -\pi <$

$\Im z < \pi$, 那么 $f(G) = \Omega = \mathbb{C} - \{z : z \leq 0\}$. f 也把垂直线段 $\{z = c + iy, -\pi < y < \pi\}$ 映为部分圆周 $\{e^{i\theta}, -\pi < \theta < \pi\}$. 把水平直线 $y = d, -\pi < d < \pi$, 映为和正实轴的夹角等于 d 的射线。

注意, 对数的主分支 $\log z$ 则反过来, 它把 Ω 映为带形 G , 把圆周映为 G 内的垂直线段, 把射线映为 G 内的水平直线。

$\cos z, \sin z$ 以及其他解析函数的映照性质的研究将在习题中进行。现在着手研究一类奇特的映照—Möbius 映照。

定义 33.5

形如 $S(z) = \frac{az+b}{cz+d}$ 的映照称为分式线性变换。如果 a, b, c, d 满足 $ad - bc \neq 0$, 那么 $S(z)$ 称为 Möbius (麦比乌斯) 变换。



如果 S 是 Möbius 变换, 那么 $S^{-1} = \frac{dz-b}{-cz+a}$ 满足 $S(S^{-1}(z)) = S^{-1}(S(z)) = z$, 即 S^{-1} 是 S 的逆映照, 如果 S 和 T 都是分式线性变换, 那么 $S \circ T$ 也是分式线性变换, 因此, Möbius 变换的集在复合变换下构成一个群。如果不作别的声明, 我们考虑的分式线性变换总是 Möbius 变换。

设 $S(x) = \frac{az+b}{cz+d}$, 如果 λ 是任意非零复数, 那么

$$S(z) = \frac{(\lambda a)z + (\lambda b)}{(\lambda c)z + (\lambda d)}.$$

即系数 a, b, c, d 不是唯一的 (见习题 20.)。

我们也可以把 S 看作是定义在 \mathbb{C}_∞ 上的, 它满足 $S(\infty) = a/c, S(-d/c) = \infty$. (注意, 我们不可能有 $a = 0 = c$, 或 $d = 0 = c$, 因为在这两种情形下都和 $ad - bc \neq 0$ 相矛盾) 因为 S 有逆变换, 所以 S 把 \mathbb{C}_∞ 映为 \mathbb{C}_∞ 。

如果 $S(z) = z + a$, 那么 S 称为平移; 如果 $S(z) = az, a \neq 0$, 那么 S 是一伸缩; 如果 $S(z) = e^{i\theta}z$ ⁵, 那么它是一个旋转。最后, 如果 $S(z) = 1/z$, 那么它是一个反演。

命题 33.11

如果 S 是一个 Möbius 变换, 那么 S 是平移, 伸缩^a, 反演的复合。(当然, 其中有的可能不出现。)

^a从这个命题看, 旋转是包含在伸缩里面的。



证明 首先, 设 $c = 0$, 因此 $S(z) = (a/d)z + (b/d)$, 所以如果 $S_1(z) = (a/d)z, S_2(z) = z + (b/d)$, 那么 $S_2 \circ S_1 = S$, 命题得证。

现在设 $c \neq 0$, 那么令 $S_1(z) = z + d/c, S_2(z) = 1/z, S_3(z) = \frac{bc-ad}{c^2}z, S_4(z) = z + a/c$, 那么 $S = S_4 \circ S_3 \circ S_2 \circ S_1$ 。

S 的不动点是什么呢? 即哪些点满足 $S(z) = z$. 如果 z 满足这个条件, 那么

$$cz^2 + (d - a)z - b = 0.$$

因此, 一个 Möbius 变换至多有两个不动点。除非 $S(z) = z$ 对所有的 z 成立。

⁵奇怪, 从这个定义来看, 前面的 az 中的 a 应该是实数才是合理的。

现在设 S 是一个 Möbius 变换, a, b, c 是 \mathbb{C}_∞ 中的不同点. $\alpha = S(a)$, $\beta = S(b)$, $\gamma = S(c)$. 假定 T 是另一个具有这种性质的变换. 那么 $T^{-1} \circ S$ 以 a, b, c 作为不动点, 所以 $T^{-1} \circ S = I =$ 恒同变换, 即 $S = T$. 因此一个 Möbius 变换由 \mathbb{C}_∞ 中的任意给定的三个点唯一确定。

设 z_2, z_3, z_4 是 \mathbb{C}_∞ 中的点. 定义 $S: \mathbb{C}_\infty \rightarrow \mathbb{C}_\infty$ 为:

$$S(z) = \left(\frac{z - z_3}{z - z_4} \right) / \left(\frac{z_2 - z_3}{z_2 - z_4} \right), \quad z_2, z_3, z_4 \in \mathbb{C};$$

$$S(z) = \frac{z - z_3}{z - z_4}, \quad z_2 = \infty;$$

$$S(z) = \frac{z_2 - z_4}{z - z_4}, \quad z_3 = \infty;$$

$$S(z) = \frac{z - z_3}{z_2 - z_3}, \quad z_4 = \infty.$$

在任意情况下, $S(z_2) = 1, S(z_3) = 0, S(z_4) = \infty$. 并且 S 是具有这种性质的唯一变换。

定义 33.6. 交比

如果 $z_1 \in \mathbb{C}_\infty$, 那么 (z_1, z_2, z_3, z_4) (z_1, z_2, z_3, z_4 的交比) 是使 z_2 变为 1, z_3 变为 0, z_4 变为 ∞ 这一唯一的 Möbius 变换下 z_1 的像。



例如, $(z_2, z_2, z_3, z_4) = 1, (z, 1, 0, \infty) = z$. 如果 M 是任意 Möbius 映照, w_2, w_3, w_4 是使得 $Mw_2 = 1, Mw_3 = 0, Mw_4 = \infty$ 的点, 那么 $Mz = (z, w_2, w_3, w_4)$.

命题 33.12

如果 z_2, z_3, z_4 是不同的点, T 是任意 Möbius 变换, 那么对于任意点 z_1 ,

$$(z_1, z_2, z_3, z_4) = (Tz_1, Tz_2, Tz_3, Tz_4).$$



证明 设 $S(z) = (z, z_2, z_3, z_4)$, 那么 S 是一个 Möbius 映照. 如果 $M = ST^{-1}$, 那么 $M(Tz_2) = 1, M(Tz_3) = 0, M(Tz_4) = \infty$, 因此 $ST^{-1} = (z, Tz_2, Tz_3, Tz_4)$ 对于 \mathbb{C}_∞ 中的所有 z 成立. 特别地, 令 $z = Tz_1$ 便得到所要求的结果。

命题 33.13

如果 z_2, z_3, z_4 是 \mathbb{C}_∞ 中的不同点, $\omega_2, \omega_3, \omega_4$ 也是 \mathbb{C}_∞ 中的不同点, 那么有且只有一个 Möbius 变换, 使得 $Sz_2 = \omega_2, Sz_3 = \omega_3, Sz_4 = \omega_4$.



证明 设 $Tz = (z, z_2, z_3, z_4), Mz = (z, \omega_2, \omega_3, \omega_4), S = M^{-1}T$. 显然 S 具有所要求的性质. 如果 R 是另一个 Möbius 变换, 使得 $Rz_j = \omega_j, j = 2, 3, 4$, 那么 $R^{-1} \circ S$ 有三个不动点 (z_2, z_3 和 z_4), 因此 $R^{-1} \circ S = I$, 或者说 $S = R$.

从中学几何中已经熟知, 平面上的三点决定一个圆周。(注意 \mathbb{C}_∞ 中过 ∞ 的圆周相应于 \mathbb{C} 中的直线, 因此, 在上面的叙述中不需要预先声明三点“不共线”, 平面上的直线将称为圆周。) 下述结果说明在什么时候四点位于一个圆周上。

命题 33.14

设 z_1, z_2, z_3, z_4 是 \mathbb{C}_∞ 中的四个不同点, 那么 (z_1, z_2, z_3, z_4) 是实数, 当且仅当, 这四个点位于一个圆周上。



证明 设 $S: \mathbb{C}_\infty \rightarrow \mathbb{C}_\infty$ 定义为 $Sz = (z, z_2, z_3, z_4)$, 那么 $S^{-1}(\mathbb{R}) =$ 使得 (z, z_2, z_3, z_4) 是实数的 z 的集。因此, 如果我们能够在 Möbius 变换下, \mathbb{R}_∞ 的像是一个圆周, 命题就得证。

设 $Sz = \frac{az+b}{cz+d}$, 如果 $z = x \in \mathbb{R}$, $\omega = S^{-1}(x)$, 那么 $x = S\omega$ 九蕴含 $S(\omega) = \overline{S(\omega)}$, 即

$$\frac{a\omega + b}{c\omega + d} = \frac{\overline{a\omega + b}}{\overline{c\omega + d}}$$

交叉相乘得到

$$\begin{aligned} (a\bar{c} - \bar{a}c)|\omega|^2 + (a\bar{d} - \bar{a}d)\omega \\ + (b\bar{c} - \bar{b}c)\bar{\omega} + (b\bar{d} - \bar{b}d) = 0. \end{aligned} \quad (33.3.3)$$

如果 $a\bar{c}$ 是实的, 那么 $a\bar{c} - \bar{a}c = 0$, 令 $\alpha = 2(a\bar{d} - \bar{a}d)$, $\beta = i(b\bar{d} - \bar{b}d)$. 用 i 乘 (33.3.3), 因为 β 是实的, 所以得到

$$0 = \Im(\alpha\omega) - \beta = \Im(\alpha\omega - \beta). \quad (33.3.4)$$

即 ω 位于由 (33.3.4) 决定的直线上, α, β 是固定的。如果 $a\bar{c}$ 不是实的, 那么 (33.3.3) 变成

$$|\omega|^2 + \bar{\gamma}\omega + \gamma\bar{\omega} - \delta = 0,$$

其中 γ 是某一个复常数, δ 是某一个实常数。因此

$$|\omega + \gamma| = \lambda, \quad (33.3.5)$$

其中

$$\lambda = (|\gamma|^2 + \delta)^{\frac{1}{2}} = \left| \frac{ad - bc}{ac - a\bar{c}} \right| > 0.$$

因为 γ 和 λ 不依赖于 x , (33.3.5) 是圆周的方程, 所以命题得证。

定理 33.5

Möbius 变换把圆周变为圆周。



证明 设 Γ 是 \mathbb{C}_∞ 中的任意的一个圆周, S 是任意一个 Möbius 变换。 z_2, z_3, z_4 是 Γ 上的三个不同的点, 记 $\omega_j = Sz_j, j = 2, 3, 4$, 那么 $\omega_2, \omega_3, \omega_4$ 决定一圆周 Γ' 。我们断言 $S(\Gamma) = \Gamma'$ 。事实上, 对于 \mathbb{C}_∞ 中的任意一点 z , 由命题 33.12 得到

$$(z, z_2, z_3, z_4) = (Sz, \omega_2, \omega_3, \omega_4). \quad (33.3.6)$$

根据上面的命题, 如果 z 在 Γ 上, 那么 (33.3.6) 的两边是实的, 但这就是说 $Sz \in \Gamma'$ 。

现在设 Γ 和 Γ' 是 \mathbb{C}_∞ 中的两个圆周。 $z_2, z_3, z_4 \in \Gamma, \omega_2, \omega_3, \omega_4 \in \Gamma'$ 。令 $Rz = (z, z_2, z_3, z_4)$, $Sz = (z, \omega_2, \omega_3, \omega_4)$, 那么 $T = S^{-1} \circ R$ 把 Γ 映为 Γ' 。事实上, $Tz_j = \omega_j, j = 2, 3, 4$, 和上面的证明一样, 推出 $T(\Gamma) = \Gamma'$ 。

命题 33.15

对于 \mathbb{C}_∞ 中任意给定的圆周 Γ 和 Γ' , 存在一个 Möbius 变换 T , 使得 $T(\Gamma) = \Gamma'$. 并且我们能够指定 Γ 上的任意三点变为 Γ' 上的任意三点. 如果我们指定 $Tz_j, j = 2, 3, 4$ (Γ 上的 z_j 互不相同), 那么 T 是唯一的.



证明 除了唯一性外, 其余的已在上段中给出了. 唯一性的证明对于读者来说是一个简单的习题.

现在我们知道 Möbius 变换把圆周变为圆周. 下一个问题是这些圆周的内部和外部变为什么? 为了回答这个问题, 我们引进一些新的概念.

定义 33.7

设 Γ 是通过 z_2, z_3, z_4 的圆周, \mathbb{C}_∞ 中的点 z 和 z^* 称为关于 Γ 是对称的, 如果

$$(z^*, z_2, z_3, z_4) = \overline{(z, z_2, z_3, z_4)}. \quad (33.3.7)$$



这个式子表示, 这个定义不仅依赖于圆周, 而且也依赖于圆周上的点 z_2, z_3, z_4 , 作为一个习题 (习题 11.), 留给读者去证明对称性和这些点的选取无关.

由命题 33.14, z 关于圆周 Γ 与自己对称, 当且仅当, $z \in \Gamma$.

让我们来研究 z 和 z^* 是对称的意味着什么. 设 Γ 是一条直线, 那么顾名思义, 我们相信 z 和 z^* 关于 Γ 是对称的, 如果通过 z 和 z^* 的直线垂直于 Γ , 并且 z 和 z^* 在 Γ 的两侧, 到 Γ 的有相同的距离. 事实正是如此.

设 Γ 是一直线. 取 $z_4 = \infty$. 等式 (33.3.7) 变成

$$\frac{z^* - z_3}{z_2 - z_3} = \frac{\bar{z} - \bar{z}_3}{\bar{z}_2 - \bar{z}_3}.$$

这就得到 $|z^* - z_3| = |z - z_3|$; 因为 z_3 是不确定的, 所以 z, z^* 到 Γ 上每一点的距离相同. 又

$$\Im \frac{z^* - z_3}{z_2 - z_3} = \Im \frac{\bar{z} - \bar{z}_3}{\bar{z}_2 - \bar{z}_3} = -\Im \frac{z - z_3}{z_2 - z_3}.$$

因此, 我们得到 (除非 $z \in \Gamma$), z, z^* 位于 Γ 确定的不同的半平面内. 由此推出, $[z, z^*]$ 垂直于 Γ .

现在设 $\Gamma = \{z : |z - a| = R\}$ ($0 < R < \infty$), z_2, z_3, z_4 在 Γ 上. 根据 (33.3.7), 并对若干 Möbius 变换多次应用命题 33.12, 得到

$$\begin{aligned} (z^*, z_2, z_3, z_4) &= \overline{(z, z_2, z_3, z_4)} \\ &= \overline{(z - a, z_2 - a, z_3 - a, z_4 - a)} \\ &= (\bar{z} - \bar{a}, \frac{R^2}{z_2 - a}, \frac{R^2}{z_3 - a}, \frac{R^2}{z_4 - a})^6 \\ &= (\frac{R^2}{\bar{z} - \bar{a}}, z_2 - a, z_3 - a, z_4 - a) \\ &= (\frac{R^2}{\bar{z} - \bar{a}} + a, z_2, z_3, z_4). \end{aligned}$$

⁶第一个等式是对称的定义, 第二个等式使用变换 $Tz = z - a$, 第三个等式是把共轭作用于每一项, 这个是成立的, 第四个等式是使用变换 $Tz = R^2/\bar{z}$, 第五个等式是使用变换 $Tz = z + a$.

因此。 $z^* = a + R^2(\bar{z} - \bar{a})^{-1}$, 或者 $(z^* - a)(\bar{z} - \bar{a}) = R^2$. 由此得到

$$\frac{z^* - a}{z - a} = \frac{R^2}{|z - a|^2} > 0;$$

所以 z^* 位于从 a 出发, 通过 z 的射线 $\{a + t(z - a) : 0 < t < \infty\}$ 上。利用 $|z - a||\bar{z} - \bar{a}| = R^2$ 这一事实, 如下图所示, 我们能够由 z 得到 z^* (若 z 位于 Γ 内部)。设 L 是从 a 出发, 通过 z 的射线, 过 z 点作一条直线 P 垂直于 L , 在 P 和 Γ 的交点处作 Γ 的切线, 这条切线和 L 的交点就是 z^* . 点 a 和 ∞ 关于 Γ 是对称的。

定理 33.6. 对称原理

如果 Möbius 变换 T 把圆周 Γ_1 变为圆周 Γ_2 , 那么关于 Γ_1 的一对对称点被 T 映为关于 Γ_2 的一对对称点。



证明 设 $z_2, z_3, z_4 \in \Gamma_1$, 如果 z, z^* 关于 Γ_1 是对称的, 那么由命题 33.12 得到

$$\begin{aligned} (Tz^*, Tz_2, Tz_3, Tz_4) &= (z^*, z_2, z_3, z_4) \\ &= \overline{(z, z_2, z_3, z_4)} \\ &= \overline{(Tz, Tz_2, Tz_3, Tz_4)}. \end{aligned}$$

因此 Tz^* 和 Tz 关于 Γ_2 是对称的。

现在我们讨论在 \mathbb{C}_∞ 中圆周的定向。这将能够使我们去区分 \mathbb{C}_∞ 中圆周的“内部”和“外部”。注意, 在 \mathbb{C}_∞ (球面) 上, 对于圆周的内部和外部没有明显的选择。

定义 33.8

如果 Γ 是一个圆周, 那么 Γ 的定向是 Γ 上的有序的三个点 (z_1, z_2, z_3) 。



直观上, 这三个点给了 Γ 的一个方向。这就是我们从 z_1 “走”到 z_2 再到 z_3 , 如果只给定两个点, 当然意思就含糊了。

设 $\Gamma = \mathbb{R}$, $z_1, z_2, z_3 \in \mathbb{R}$, 又设 $Tz = (z, z_1, z_2, z_3) = \frac{az+b}{cz+d}$. 由于 $T(\mathbb{R}_\infty) = \mathbb{R}_\infty$, 由此推出, a, b, c, d 可以取为实数 (见习题 8.), 因此

$$\begin{aligned} Tz &= \frac{az+b}{cz+d} = \frac{az+b}{|cz+d|^2}(c\bar{z}=d) \\ &= \frac{1}{|cz+d|^2}[ac|z|^2 + bd + bc\bar{z} + adz]. \end{aligned}$$

所以

$$\Im(z, z_1, z_2, z_3) = \frac{(ad-bc)}{|cz+d|^2} \Im z.$$

于是, $\{z : \Im(z, z_1, z_2, z_3) < 0\}$ 或者是上半平面, 或者是下半平面, 取决于 $(ad-bc) < 0$ 还是 $(ad-bc) > 0$. (注意, $ad-bc$ 是 T 的“行列式”。)

现在设 Γ 是任意的, z_1, z_2, z_3 在 Γ 上。对于任意的 Möbius 变换 S , 我们有 (根据命题 33.12)

$$\begin{aligned} \{z : \Im(z, z_1, z_2, z_3) > 0\} &= \{z : \Im(Sz, Sz_1, Sz_2, Sz_3) > 0\} \\ &= S^{-1}\{z : \Im(z, Sz_1, Sz_2, Sz_3) > 0\}. \end{aligned}$$

特别地, 如果选取 S , 使得 S 把 Γ 映为 \mathbb{R}_∞ , 那么 $\{z : \Im(z, z_1, z_2, z_3) > 0\}$ 等于上半平

面或下半平面在 S^{-1} 下的像。

如果 (z_1, z_2, z_3) 是 Γ 的定向, 那么我们定义 Γ (关于 (z_1, z_2, z_3)) 的右边为

$$\{z : \Im(z, z_1, z_2, z_3) > 0\}.$$

类似地, 我们定义 Γ 的左边为

$$\{z : \Im(z, z_1, z_2, z_3) < 0\}.$$

下述定理的证明留给读者作为习题。

定理 33.7. 定向原理

设 Γ_1 和 Γ_2 是 \mathbb{C}_∞ 中的两个圆周, T 是 Möbius 变换, $T(\Gamma_1) = \Gamma_2$, (z_1, z_2, z_3) 是 Γ_1 的定向, 那么 T 把 Γ_1 的右边和左边变为 Γ_2 关于定向 (Tz_1, Tz_2, Tz_3) 的右边和左边。



考虑 \mathbb{R} 的定向 $(1, 0, \infty)$ 。由交比的定义, $(z, 1, 0, \infty) = z$ 。因此, \mathbb{R} 关于 $(1, 0, \infty)$ 的右边是上半平面。这和我们的直观是一致的“当我们沿 \mathbb{R} 从 1 走到 0, 再到 ∞ , 上半平面在我们的右边。

作为例子, 考虑下述问题: 找出一个解析函数 $f: G \rightarrow \mathbb{C}$, $G = \{z : \Re z > 0\}$, 使得 $f(G) = D = \{z : |z| < 1\}$ 。我们是通过寻找一个 Möbius 变换来解决这个问题的。这个变换把虚轴变为单位圆周。由定向原理, 它把 G 变为 D (即我们必须细心选取这个映照, 使得它不是把 D 变为 $\{z : |z| > 1\}$)。

如果我们给定虚轴的定向为 $(-i, 0, i)$, 那么 $\{z : \Re z > 0\}$ 是虚轴的右边。事实上,

$$\begin{aligned} (z, -i, 0, i) &= \frac{2z}{z-i} = \frac{2z}{z-i} \cdot \frac{\bar{z}+i}{\bar{z}+i} \\ &= \frac{2}{|z-i|^2}(|z|^2 + iz). \end{aligned}$$

因此, $\{z : \Im(z, -i, 0, i) > 0\} = \{z : \Im iz > 0\} = \{z : \Re z > 0\}$ 。给 Γ 以定向 $(-i, -1, i)$, 我们得到 D 位于 Γ 的右边。又

$$(z, -i, -1, i) = \frac{2i}{i-1} \cdot \frac{z+1}{z-i}.$$

如果

$$Sz = \frac{2z}{z-i}, Rz = \left(\frac{2i}{i-1}\right)\left(\frac{z+1}{z-i}\right),$$

那么 $T = R^{-1}S$ 把 G 映为 D (并把虚轴映为 Γ)。由代数运算, 我们有

$$Tz = \frac{z-1}{z+1}.$$

把这个结果和前面的结果结合起来, 我们得到, $g(z) = \frac{e^z-1}{e^z+1}$ 把无穷带形 $\{z : |\Im z| < \pi/2\}$ 映为开单位圆 D 。(值得一提的是 $\frac{e^z-1}{e^z+1} = \tanh(\frac{z}{2})$)。

设 G_1, G_2 是连通开集, 为了找出一个解析函数 f , 使得 $f(G_1) = G_2$, 我们试图把 G_1, G_2 都映为开单位圆。如果这一点能够办到, f 就能由一个函数和另一个函数的反函数的符合而得到。

作为一个例子, 设 G 是两个相交于 a, b ($a \neq b$) 的圆周的内部开集, L 是过 a, b 的直线, 其定向是 (∞, a, b) 。那么 $Tz = (z, \infty, a, b) = \frac{z-a}{z-b}$ 把 L 映为实轴 ($T\infty = 1, Ta =$

$0, Tb = \infty$). 由于 T 把圆周映为圆周, 所以 T 把 Γ_1 和 Γ_2 映为过 0 和 ∞ 的圆周, 即 $T(\Gamma_1)$, $T(\Gamma_2)$ 是直线. 利用定向, 我们有 $T(G) = \{\theta_0 - \alpha < \arg \omega < \theta_0\}$ ⁷, $\alpha > 0$, 或者是某一这种闭扇形的余集. 利用幂函数, 或许还有一个旋转, 我们可以把这个楔形映为右半平面. 现在与 $\frac{z-1}{z+1}$ 复合起来, 就得到 G 到 $D = \{z : |z| < 1\}$ 的映照.

第三十三章 习题

1. 求 $\{z : \Re z < 0, |\Im z| < \pi\}$ 在指数函数下的像.
2. 对于集 $\{z : |\Im z| < \pi/2\}$ 做上一习题
3. 讨论 $\cos z$ 和 $\sin z$ 的映照性质.
4. 讨论 z^n 和 $z^{1/n}$, $n > 2$ 的映照性质. (提示: 利用极坐标.)
5. 求出 \mathbb{C}_∞ 中伸缩、平移、反演的不动点.
6. 计算下列交比: (a) $(7+i, 1, 0, \infty)$; (b) $(2, 1-i, 1, 1+i)$; (c) $(0, 1, i, -1)$; (d) $(i-1, \infty, 1+i, 0)$.
7. 如果 $Tz = \frac{az+b}{cz+d}$, 求出 z_2, z_3, z_4 (用 a, b, c, d 表示), 使得 $Tz = (z, z_2, z_3, z_4)$.
8. 如果 $Tz = \frac{az+b}{cz+d}$, 证明: 当且仅当我们可以选取 a, b, c, d 为实数时 $T(\mathbb{R}) = \mathbb{R}$.
9. 如果 $Tz = \frac{az+b}{cz+d}$, 求出 $T(\Gamma) = \Gamma$ 的充分必要条件, 其中 Γ 是单位圆周 $\{z : |z| = 1\}$.
10. 设 $D = \{z : |z| < 1\}$, 求出所有满足 $T(D) = D$ 的 Möbius 变换.
11. 证明: 对称的定义 (33.7) 不依赖于 z_2, z_3, z_4 的选取, 即证明: 如果 $\omega_2, \omega_3, \omega_4$ 也在 Γ 上, 那么它们满足等式 (33.3.7), 当且仅当 $(z^*, \omega_2, \omega_3, \omega_4) = \overline{(z, \omega_2, \omega_3, \omega_4)}$. (提示: 利用习题8.)
12. 证明定理33.4.
13. 讨论映照 $f(z) = \frac{1}{2}(z + \frac{1}{z})$.
14. 设一个圆包含在另一个圆内, 并在一点 a 相切, G 是这两个圆周之间的域, 将 G 共形映照为开单位圆. (提示: 先用 $(z-a)^{-1}$).
15. 设 $G = \{z : 0 < |z| < 1\}$. 能否将 G 共形映照为开单位圆?
16. 试用解析函数 f 把 $G = \mathbb{C} - \{z : -1 \leq z \leq 1\}$ 映为开单位圆, f 能是一一的吗?
17. 设 G 是一个域, $f : G \rightarrow \mathbb{C}$ 是解析的, $f(G)$ 是圆周的一子集, 证明: f 是一常数.
18. 设 $-\infty < a < b < \infty$. $Mz = \frac{z-ia}{z-ib}$. 定义直线 $L_1 = \{z : \Im z = b\}$, $L_2 = \{z : \Im z = a\}$, $L_3 = \{z : \Re z = 0\}$. 确定图中的 A, B, C, D, E, F 中的哪一个能被 M 映为图中的 U, V, W, X, Y, Z .
19. 设 a, b, M 如上题所述, $\log z$ 是对数的主分支.
 - (a) 证明: $\log(Mz)$ 对于所有的 z , 除去 $z = ic, a < c < b$ 外有定义. 并且如果 $h(z) = \Im[\log Mz]$, 那么对于 $\Re z > 0$, 有 $0 < h(z) < \pi$.
 - (b) 证明: 对于 $\Re z > 0$ 及任意实数 c , $\log(z-ic)$ 有定义, 并证明: 如果 $\Re z > 0$, 有 $|\Im \log(z-ic)| < \pi/2$.
 - (c) 设 h 如 (a) 中所述, 证明: $h(z) = \Im[\log z - ia - \log(z-ib)]$.

⁷原书误为 $T(G) = \{\omega - \alpha < \arg \omega < \alpha\}$, $\alpha > 0$.---译注

(d) 证明:

$$\int_a^b \frac{dt}{z - it} = i[\log(z - ib) - \log(z - ia)].$$

(提示: 利用微积分学的基本定理。)

(e) 结合 (c) 和 (d), 得到

$$h(x + iy) = \int_a^b \frac{dt}{x^2 + (y - t)^2} = \arctan\left(\frac{y - a}{x}\right) - \arctan\left(\frac{y - b}{x}\right).$$

(f) 解释 (e) 的几何意义, 并证明: 当 $\Re z > 0$ 时, $h(z)$ 是图中所画的角度。

20. 设 $Sz = \frac{az+b}{cz+d}$, $Tz = \frac{\alpha z+\beta}{\gamma z+\delta}$, 证明: 当且仅当存在非零复数 λ , 使得 $\alpha = \lambda a$, $\beta = \lambda b$, $\gamma = \lambda c$, $\delta = \lambda d$ 时 $S = T$.
21. 设 T 是具有不动点 z_1 和 z_2 的 Möbius 变换。如果 S 是一个 Möbius 变换, 证明: $S^{-1}TS$ 有不动点 $S^{-1}z_1$ 和 $S^{-1}z_2$.
22. (a) 证明: 一个 Möbius 变换, 当且仅当它是一个伸缩时, 仅以 0 和 ∞ 为它的不动点。
(b) 证明: 一个 Möbius 变换, 当且仅当它是一个平移时, 仅以 ∞ 为它的不动点。
23. 证明: 一个 Möbius 变换 T , 当且仅当, $Tz = a/z$, $a \in \mathbb{C}$ 时, 满足 $T(0) = \infty$, $T(\infty) = 0$.
24. 设 T 是一个 Möbius 变换, 且不失恒同变换。证明: 一个 Möbius 变换 S , 当且仅当 S 和 T 有相同的不动点时, 满足 $ST = TS$ 。(提示: 利用习题 21 和 22.)
25. 求出 Möbius 变换群的所有 Abel 子群。
26. (a) 设 $GL_2(\mathbb{C}) =$ 所有的 2×2 可逆复数矩阵。 \mathcal{M} 是 Möbius 变换群。 $\varphi: GL_2(\mathbb{C}) \rightarrow \mathcal{U}$ 定义为

$$\varphi \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \frac{az + b}{cz + d}.$$

证明: φ 是 $GL_2(\mathbb{C})$ 到 \mathcal{M} 上的群同态。求出 φ 的核。

(b) 设 $SL_2(\mathbb{C})$ 是 $GL_2(\mathbb{C})$ 的子群, 它是由行列式为 1 的所有矩阵所组成的。证明: $SL_2(\mathbb{C})$ 在 φ 下的像是 \mathcal{M} 的全体。 φ 的核的哪部分在 $SL_2(\mathbb{C})$ 中?

27. 如果 \mathcal{G} 是一个群, \mathcal{N} 是一个子群, 那么 \mathcal{N} 称为 \mathcal{G} 的正规子群, 如果当 $T \in \mathcal{N}$, $S \in \mathcal{G}$ 时 $S^{-1}TS \in \mathcal{N}$ 。如果 \mathcal{G} 的仅有的正规子群是 $\{I\}$ (I 是 \mathcal{G} 的单位) 和 \mathcal{G} 本身, 则称 \mathcal{G} 是单纯群。证明: Möbius 变换群 \mathcal{M} 是一个单纯群。
28. 讨论 $(1 - z)^i$ 的映照性质。
29. 对于复数 α 和 β , $|\alpha|^2 + |\beta|^2 = 1$,

$$u_{\alpha, \beta} = \frac{\alpha z - \bar{\beta}}{\beta z - \bar{\alpha}}, U = \{u_{\alpha, \beta} : |\alpha|^2 + |\beta|^2 = 1\}.$$

(a) 证明: 在变换的复合运算下 U 构成一个群。

(b) 如果 SU_2 是所有的行列式为 1 的酉矩阵所构成的集, 证明: SU_2 在矩阵的乘法下是一个群, 并且对于 SU_2 中的每一个 A , 有唯一的复数 α, β , 它们满足 $|\alpha|^2 + |\beta|^2 = 1$,

$$\text{使得 } A = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}.$$

- (c) 证明: $\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \rightarrow u_{\alpha,\beta}$ 是群 SU_2 到 U 上的同构。
- (d) 如果 $l \in \{0, \frac{1}{2}, 1, \frac{3}{2}, \dots\}$, 设 $H_l =$ 所有其次数 $\leq 2l$ 的多项式。对于 U 中的 $u_{\alpha,\beta}$ 定义 $T_u^{(l)} : H_l \rightarrow H_l$ 为 $(T_u^{(l)} f)(z) = (\beta z + \bar{\alpha})^{2l} f(u(z))$. 证明: $T_u^{(l)}$ 是 H_l 上的一个可逆的线性变换。并且 $u \mapsto T_u^{(l)}$ 是 U 到一个可逆线性变换群里 (H_l 到 H_l 上) 的一一同态。

30. 对于 $|z| < 1$ 定义 $f(z)$ 为

$$f(z) = \exp\{-i \log [i(\frac{1+z}{1-z})]^{1/2}\}.$$

- (a) 证明: f 将 $D = \{z : |z| < 1\}$ 共形映照为一个圆环 G .
- (b) 求出所有把 D 映为 D 的 Möbius 变换 $S(z)$, 使得当 $|z| < 1$ 时, $f(S(z)) = f(z)$.

第三十四章 复积分

本章导出的结果在解析函数的研究中是基本的, 这里给出的定理是整个数学知识的基础之一, 并且具有一系列范围广泛的应用。

34.1 Riemann-Stieltjes 积分

为了定义函数沿 \mathbb{C} 内一条路径的积分, 我们首先来定义 Riemann-Stieltjes 积分。这种积分的讨论是远不完备的, 而仅限于讨论为了有力的解释线积分是必需的那些结果。

定义 34.1. 有界变差函数

设 $[a, b] \subset \mathbb{R}$, 称函数 $\gamma: [a, b] \rightarrow \mathbb{C}$ 是有界变差函数, 如果存在一个常数 $M > 0$, 使得对于 $[a, b]$ 的每一个分割 $P = \{a = t_0 < t_1 < \cdots < t_m = b\}$, 总有

$$v(\gamma: P) = \sum_{k=1}^m |\gamma(t_k) - \gamma(t_{k-1})| \leq M.$$

γ 的全变差 $V(\gamma)$ 定义为

$$V(\gamma) = \sup\{v(\gamma: P) : P \text{ 是 } [a, b] \text{ 的任一个分割}\}.$$

显然, $V(\gamma) \leq M < \infty$.



容易看出。当且仅当, $\Re\gamma$ 和 $\Im\gamma$ 是有界变差函数时, γ 才是有界变差函数。当 γ 是实的, 非减函数时, 那么 γ 是有界变差函数, 并且 $V(\gamma) = \gamma(b) - \gamma(a)$ (习题1.)。我们还要给出别的例子, 但首先给出这种函数的一些容易导出的性质。

命题 34.1

设 $\gamma: [a, b] \rightarrow \mathbb{C}$ 是有界变差函数, 那么:

(a) 如果 P 和 Q 是 $[a, b]$ 的分割, 且 $P \subset Q$, 则

$$v(\gamma: P) \leq v(\gamma: Q);$$

(b) 如果 $\sigma: [a, b] \rightarrow \mathbb{C}$ 也是有界变差函数, 且 $\alpha, \beta \in \mathbb{C}$, 则 $\alpha\gamma + \beta\sigma$ 是有界变差函数, 且

$$V(\alpha\gamma + \beta\sigma) \leq |\alpha|V(\gamma) + |\beta|V(\sigma).$$



证明留给读者。

下面的命题给出一类广泛的有界变差函数, 实际上, 这是我们主要考虑的一类函数。

命题 34.2

如果 $\gamma: [a, b] \rightarrow \mathbb{C}$ 是分段光滑函数, 则 γ 是有界变差函数, 且

$$V(\gamma) = \int_a^b |\gamma'(t)| dt.$$



证明 设 γ 是光滑的 (对于分段光滑情形的证明容易由此推出), 我们记得, 当我们说 γ

是光滑时, 就意味着 γ' 是连续的。设 $P = \{a = t_0 < t_1 < \cdots < t_m = b\}$, 那么, 由定义,

$$\begin{aligned} v(\gamma; P) &= \sum_{k=1}^m |\gamma(t_k) - \gamma(t_{k-1})| = \sum_{k=1}^m \left| \int_{t_{k-1}}^{t_k} \gamma'(t) dt \right| \\ &\leq \sum_{k=1}^m \int_{t_{k-1}}^{t_k} |\gamma'(t)| dt = \int_a^b |\gamma'(t)| dt. \end{aligned}$$

因此 $V(\gamma) \leq \int_a^b |\gamma'(t)| dt$, γ 是有界变差函数。

由于 γ' 连续, 因而一致连续; 所以, 如果给定 $\epsilon > 0$, 我们可以选取 $\delta_1 > 0$, 使得当 $|s - t| < \delta_1$ 时, 有 $|\gamma'(s) - \gamma'(t)| < \epsilon$, 又可选取 $\delta_2 > 0$, 使得如果 $P = \{a = t_0 < t_1 < \cdots < t_m = b\}$, $\|P\| = \max\{(t_k - t_{k-1}) : 1 \leq k \leq m\} \leq \delta_2$ 时, 有

$$\left| \int_a^b |\gamma'(t)| dt + \sum_{k=1}^m |\gamma'(\tau_k)|(t_k - t_{k-1}) \right| < \epsilon,$$

其中 τ_k 是 $[t_{k-1}, t_k]$ 中的任意一点。因此,

$$\begin{aligned} \int_a^b |\gamma'(t)| dt &\leq \epsilon + \sum_{k=1}^m |\gamma'(\tau_k)|(t_k - t_{k-1}) \\ &= \epsilon + \sum_{k=1}^m \left| \int_{t_{k-1}}^{t_k} \gamma'(\tau_k) dt \right| \\ &\leq \epsilon + \sum_{k=1}^m \left| \int_{t_{k-1}}^{t_k} [\gamma'(\tau_k) - \gamma'(t)] dt \right| \\ &\quad + \sum_{k=1}^m \left| \int_{t_{k-1}}^{t_k} \gamma'(t) dt \right|. \end{aligned}$$

如果 $\|P\| \leq \delta = \min(\delta_1, \delta_2)$, 那么对于 $[t_{k-1}, t_k]$ 中的 τ_k , 有 $|\gamma'(t_k) - \gamma'(t_{k-1})| < \epsilon$, 且

$$\begin{aligned} \int_a^b |\gamma'(t)| dt &\leq \epsilon + \epsilon(b-a) + \sum_{k=1}^m |\gamma(t_k) - \gamma(t_{k-1})| \\ &= \epsilon[1 + (b-a)] + v(\gamma; P) \\ &\leq \epsilon[1 + (b-a)] + V(\gamma). \end{aligned}$$

令 $\epsilon \rightarrow 0+$, 给出

$$\int_a^b |\gamma'(t)| dt \leq V(\gamma),$$

这就得到了要证明的等式。

定理 34.1

设 $\gamma: [a, b] \rightarrow \mathbb{C}$ 是有界变差函数, $f: [a, b] \rightarrow \mathbb{C}$ 是连续函数, 则存在一个复常数 I , 使得对于每个 $\epsilon > 0$, 存在 $\delta > 0$, 当 $P = \{t_0 < t_1 < \cdots < t_m\}$ 是 $[a, b]$ 的一个分割, 且 $\|P\| = \max\{(t_k - t_{k-1}) : 1 \leq k \leq m\} < \delta$ 时,

$$\left| I - \sum_{k=1}^m f(\tau_k) [\gamma(t_k) - \gamma(t_{k-1})] \right| < \epsilon$$

其中 τ_k 可以在 $[t_{k-1}, t_k]$ 上任意选择。

数 I 就称为 f 在 $[a, b]$ 上关于 γ 的积分, 记为

$$I = \int_a^b f d\gamma = \int_a^b f(t) d\gamma(t).$$



证明 由于 f 是连续的, 因而是一致连续的; 于是我们可以 (归纳地) 取到正数 $\delta_1 > \delta_2 > \delta_3 > \dots$, 使得当 $|s - t| < \delta_m$ 时, 有 $|f(s) - f(t)| < \frac{1}{m}$. 对每一个 $m \geq 1$, 设 \mathcal{P}_m 是 $[a, b]$ 的满足 $\|P\| < \delta_m$ 的所有分割 P 作成的集, 那么 $\mathcal{P}_1 \supset \mathcal{P}_2 \supset \dots$, 再定义 F_m 是集

$$\left\{ \sum_{k=1}^m f(\tau_k) [\gamma(t_k) - \gamma(t_{k-1})] : P \in \mathcal{P}_m, t_{k-1} \leq \tau_k \leq t_k \right\} \quad (34.1.1)$$

的闭包。

我们先假定下述断言成立。

$$\begin{cases} F_1 \supset F_2 \supset F_3 \supset \dots, \\ \text{diam } F_m \leq \frac{2}{m} V(\gamma). \end{cases} \quad (34.1.2)$$

这时由 Cantor 定理 (第32章32.4), 恰好存在一个复数 I , 使得对每一个 $m \geq 1$ 都有 $I \in F_m$. 让我们来说明, 这将完成定理的证明。如果 $\epsilon > 0$, 令 $m > \frac{2}{\epsilon} V(\gamma)$, 则 $\epsilon > \frac{2}{m} V(\gamma) \leq \text{diam } F_m$, 由于 $I \in F_m$, 所以 $F_m \subset B(I; \epsilon)$. 于是取 $\delta = \delta_m$, 定理便得证。

现在来证明断言 (34.1.2)。显然由 $\mathcal{P}_1 \supset \mathcal{P}_2 \supset \dots$ 可推出 $F_1 \supset F_2 \supset \dots$. 为了证明 $\text{diam } F_m \leq \frac{2}{m} V(\gamma)$, 只要证明 (34.1.1) 中的集的直径 $\leq \frac{2}{m} V(\gamma)$. 为此分作两步进行, 每一步都是容易的, 虽然第一步较为冗长。

设 $P = \{t_0 < t_1 < \dots < t_m\}$ 是一个分割, 我们用 $S(P)$ 表示形如 $\sum f(\tau_k) [\gamma(t_k) - \gamma(t_{k-1})]$ 的和数, 其中 τ_k 是 $[t_{k-1}, t_k]$ 上的任意一点。固定 $m \geq 1$ 且设 $P \in \mathcal{P}_m$. 第一步证明, 如果 $P \subset Q$ ($Q \in \mathcal{P}_m$), 则 $|S(P) - S(Q)| < \frac{1}{m} V(\gamma)$. 设 Q 是由 P 添上一个分点得到的, 我们仅就这一情形给出证明。设 $1 \leq p \leq m$, $t_{k-1} < t^* < t_p$; 又设 $P \cup \{t^*\} = Q$. 假如 $t_{p-1} \leq \sigma \leq t^*, t^* \leq \sigma' \leq t_p$,

$$S(Q) = \sum_{k \neq p} f(\sigma_k) [\gamma(t_k) - \gamma(t_{k-1})] + f(\sigma) [\gamma(t^*) - \gamma(t_{p-1})] + f(\sigma') [\gamma(t_p) - \gamma(t^*)].$$

因为当 $|\tau - \sigma| < \delta_m$ 时, $|f(\tau) - f(\sigma)| < \frac{1}{m}$, 所以便有

$$\begin{aligned}
 |S(P) - S(Q)| &= \left| \sum_{k \neq p} [f(\tau_k) - f(\sigma_k)] [\gamma(t_k) - \gamma(t_{k-1})] \right. \\
 &\quad + f(\tau_p) [\gamma(t_p) - \gamma(t_{p-1})] \\
 &\quad - f(\sigma) [\gamma(t^*) - \gamma(t_{p-1})] \\
 &\quad \left. - f(\sigma') [\gamma(t_p) - \gamma(t^*)] \right| \\
 &\leq \frac{1}{m} \sum_{k \neq p} |\gamma(t_k) - \gamma(t_{k-1})| \\
 &\quad + |[f(\tau_p) - f(\sigma)] [\gamma(t^*) - \gamma(t_{p-1})]| \\
 &\quad + [f(\tau_p) - f(\sigma')] [\gamma(t_p) - \gamma(t^*)]| \\
 &\leq \frac{1}{m} \sum_{k \neq p} |\gamma(t_k) - \gamma(t_{k-1})| \\
 &\quad + \frac{1}{m} |\gamma(t^*) - \gamma(t_{p-1})| \\
 &\quad + \frac{1}{m} |\gamma(t_p) - \gamma(t^*)| \leq \frac{1}{m} V(\gamma).
 \end{aligned}$$

第二步, 设 P 和 R 是 \mathcal{P}_m 中的任意两个分割, 那么 $Q = P \cup R$ 是既包含 P 也包含 R 的分割, 利用第一步我们得到

$$\begin{aligned}
 |S(P) - S(R)| &\leq |S(P) - S(Q)| + |S(Q) - S(R)| \\
 &\leq \frac{2}{m} V(\gamma).
 \end{aligned}$$

由此便推出 (34.1.1) 中的集的直径 $\leq \frac{2}{m} V(\gamma)$.

通过 $\epsilon - \delta$ 论证方法, 从定义可推出下面的结果。

命题 34.3

设 f 和 g 是 $[a, b]$ 上的连续函数, γ 和 σ 是 $[a, b]$ 上的有界变差函数, 则对于任意两个数 α, β , 有

- (a) $\int_a^b (\alpha f + \beta g) d\gamma = \alpha \int_a^b f d\gamma + \beta \int_a^b g d\gamma$;
- (b) $\int_a^b f d(\alpha \gamma + \beta \sigma) = \alpha \int_a^b f d\gamma + \beta \int_a^b f d\sigma$.



下面的命题对于计算这种积分是很有用的,

命题 34.4

设 $\gamma: [a, b] \rightarrow \mathbb{C}$ 是有界变差函数, $f: [a, b] \rightarrow \mathbb{C}$ 是连续函数, 如果 $a = t_0 < t_1 < \dots < t_m = b$, 则

$$\int_a^b f d\gamma = \sum_{k=1}^m \int_{t_{k-1}}^{t_k} f d\gamma.$$



证明留做习题。

前面已经提到, 我们将主要考虑分段光滑的 γ . 下面的定理说明, 在这种情形下我们能够通过微积分学中已经学过的积分法来计算 $\int f d\gamma$.

定理 34.2

如果 γ 是分段光滑的, $f: [a, b] \rightarrow \mathbb{C}$ 是连续函数, 则

$$\int_a^b f d\gamma = \int_a^b f(t) \gamma'(t) dt.$$



证明 我们仍然只考虑 γ 是光滑的情形。通过考虑 γ 的实部和虚部, 把证明归结为对于 $\gamma([a, b]) \subset \mathbb{R}$ 的情形。设 $\epsilon > 0$, 且可取 $\delta > 0$, 使得当 $P = \{a = t_0 < t_1 < \cdots < t_n = b\}$, 满足 $\|P\| < \delta$ 时

$$\left| \int_a^b f d\gamma - \sum_{k=1}^n f(\tau_k) [\gamma(t_k) - \gamma(t_{k-1})] \right| < \epsilon/2, \quad (34.1.3)$$

$$\left| \int_a^b f(t) \gamma'(t) dt - \sum_{k=1}^n f(\tau_k) \gamma'(\tau_k) (t_k - t_{k-1}) \right| < \epsilon/2. \quad (34.1.4)$$

对于 $[t_{k-1}, t_k]$ 上的任意 τ_k 成立。如果我们应用导数的中值定理, 得到在 $[t_{k-1}, t_k]$ 内存在 τ_k , 使得 $\gamma'(t_k) = [\gamma(t_k) - \gamma(t_{k-1})](t_k - t_{k-1})^{-1}$ (注意: 应用中值定理时, γ 必需是实的)。于是

$$\sum_{k=1}^n f(\tau_k) [\gamma(t_k) - \gamma(t_{k-1})] = \sum_{k=1}^n f(\tau_k) \gamma'(\tau_k) (t_k - t_{k-1}).$$

联系到不等式 (34.1.3) 和 (34.1.4) 就得到

$$\left| \int_a^b f d\gamma - \int_a^b f(t) \gamma'(t) dt \right| < \epsilon.$$

由于 ϵ 是任意的, 所以定理得证。

我们已经定义路径为一个连续函数 $\gamma: [a, b] \rightarrow \mathbb{C}$. 如果 γ 是一条路径, 那么集合 $\gamma(t): a \leq t \leq b$ 称为 γ 的迹 (trace), 用 $\{\gamma\}$ 表示。应当注意, 路径的迹总是紧集。当 γ 是有界变差函数时, γ 是可求长路径。如果 P 是 $[a, b]$ 的一个分割, 那么 $v(\gamma; P)$ 正好就是连接 γ 的迹上的分点的线段的长度的和。说 γ 是可求长的就是说 γ 有有穷长度, 且它的长度是 $V(\gamma)$. 特别地, 如果 γ 是分段光滑的, 那么 γ 是可求长的, 它的长度等于 $\int_a^b |\gamma'(t)| dt$.

如果 $\gamma: [a, b] \rightarrow \mathbb{C}$ 是可求长路径, 且 $\{\gamma\} \subset E \subset \mathbb{C}$, $f: E \rightarrow \mathbb{C}$ 是连续函数, 那么 $f \circ \gamma$ 是 $[a, b]$ 上的连续函数。记住这点, 有助于理解下面的定义。

定义 34.2

如果 $\gamma: [a, b] \rightarrow \mathbb{C}$ 是可求长路径, f 是定义在 γ 的迹上的连续函数, 那么 f 沿 γ 的 (线) 积分是

$$\int_a^b f[\gamma(t)] d\gamma(t).$$

这个线积分也可以表示为 $\int_\gamma f = \int_\gamma f(z) dz$.



作为例子, 我们将 $\gamma: [a, b] \rightarrow \mathbb{C}$ 取为 $\gamma(t) = e^{it}$, 对于 $z \neq 0$, 定义 $f(z) = \frac{1}{z}$. γ 是光滑的, 所以由定理 34.2,

$$\int_\gamma \frac{1}{z} dz = \int_0^{2\pi} e^{-it} (ie^{it}) dt = 2\pi i.$$

利用 γ 的同一定义, 并设 $m \geq 0$ 是任意整数, 得到

$$\begin{aligned}\int_{\gamma} z^m dz &= \int_0^{2\pi} e^{imt} (ie^{it}) dt = \int_0^{2\pi} \exp(i(m+1)t) dt \\ &= \int_0^{2\pi} \cos(m+1)t dt + i \int_0^{2\pi} \sin(m+1)t dt = 0.\end{aligned}$$

现在设 $a, b \in \mathbb{C}$, 令 $\gamma(t) = tb + (1-t)a$, $0 \leq t \leq 1$, 那么 $\gamma'(t) = b - a$, 利用微积分学的基本定理, 我们便得到

$$\int_{\gamma} z^n dz = (b-a) \int_0^1 [tb + (1-t)a]^n dt = \frac{1}{n+1} (b^{n+1} - a^{n+1}),$$

其中 $n \geq 0$. 在习题中将举出更多的例子. 但现在我们将证明某个“不变性”的结果, 这个结果除了可用于计算外, 也构成了我们曲线定义的基础.

如果 $\gamma: [a, b] \rightarrow \mathbb{C}$ 是可求长路径, $\varphi: [c, d] \rightarrow [a, b]$ 是连续非减函数, 它的像是整个 $[a, b]$ (即 $\varphi(c) = a$, $\varphi(d) = b$), 则 $\gamma \circ \varphi: [c, d] \rightarrow \mathbb{C}$ 是一条路径, 它与 γ 有相同的迹. 而且 $\gamma \circ \varphi$ 是可求长的, 因为如果 $c = a_0 < s_1 < \cdots < s_n = d$, 那么 $a = \varphi(s_0) \leq \varphi(s_1) \leq \cdots \leq \varphi(s_n) = b$ 是 $[a, b]$ 的一个分割, 因此

$$\sum_{k=1}^n |\gamma(\varphi(s_k)) - \gamma(\varphi(s_{k-1}))| \leq V(\gamma),$$

所以 $V(\gamma \circ \varphi) \leq V(\gamma) < \infty$, 如果 f 是 $\{\gamma\} = \{\gamma \circ \varphi\}$ 上的连续函数, 那么 $\int_{\gamma \circ \varphi} f$ 也是有定义的.

命题 34.5

如果 $\gamma: [a, b] \rightarrow \mathbb{C}$ 是可求长路径, $\varphi: [c, d] \rightarrow [a, b]$ 是连续非减函数, 且 $\varphi(c) = a$, $\varphi(d) = b$, 则对于 $\{\gamma\}$ 上的任意一个连续函数 f , 有

$$\int_{\gamma} f = \int_{\gamma \circ \varphi} f.$$

证明 设 $\epsilon > 0$, 选取 $\delta_1 > 0$, 使得对于满足 $(s_k - s_{k-1}) < \delta_1$ 的 $[c, d]$ 的分割 $\{s_0 < s_1 < \cdots < s_n\}$ 及 $s_{k-1} \leq \sigma_k \leq s_k$, 有

$$\left| \int_{\gamma \circ \varphi} f - \sum_{k=1}^n f(\gamma \circ \varphi(\sigma_k)) [\gamma \circ \varphi(s_k) - \gamma \circ \varphi(s_{k-1})] \right| < \epsilon/2. \quad (34.1.5)$$

类似地, 选取 $\delta_2 > 0$, 使得对于满足 $(t_k - t_{k-1}) < \delta_2$ 的 $[a, b]$ 的分割 $\{t_0 < t_1 < \cdots < t_n\}$ 及 $t_{k-1} \leq \tau_k \leq t_k$, 有

$$\left| \int_{\gamma} f - \sum_{k=1}^n f(\gamma(\tau_k)) [\gamma(t_k) - \gamma(t_{k-1})] \right| < \epsilon/2. \quad (34.1.6)$$

但是 φ 在 $[c, d]$ 上是一致连续的, 因此存在 $\delta > 0$, $\delta < \delta_1$, 使得当 $|s - s'| < \delta$ 时, 就有 $|\varphi(s) - \varphi(s')| < \delta_2$, 所以, 如果 $\{s_0 < s_1 < \cdots < s_n\}$ 是 $[c, d]$ 的一个分割, 满足 $(s_k - s_{k-1}) < \delta < \delta_1$, 令 $t_k = \varphi(s_k)$, 那么 $\{t_0 < t_1 < \cdots < t_n\}$ 是 $[a, b]$ 的一个分割, 满足 $(t_k - t_{k-1}) < \delta_2$. 如果 $s_{k-1} \leq \sigma_k \leq s_k$, 令 $\tau_k = \varphi(\sigma_k)$, 那么 (34.1.5) 和 (34.1.6) 都成立, 而且这两个差式的第二项是相同的, 由此推出

$$\left| \int_{\gamma} f - \int_{\gamma \circ \varphi} f \right| < \epsilon.$$

因为 $\epsilon > 0$ 是任意的, 所以等式得证。

我们希望在可求长路径的集合上定义一个等价关系, 使得等价类中的每一条路径有相同的迹, 并且在这个迹上的连续函数的线积分, 对于这个类中的每一条路径来说都是相同的。如果对于某一个像上面那样的¹ φ , $\sigma = \gamma \circ \varphi$, 我们似乎就应当定义 σ 和 γ 是等价的, 但这并不是等价关系!

定义 34.3

设 $\sigma: [c, d] \rightarrow \mathbb{C}$ 和 $\gamma: [a, b] \rightarrow \mathbb{C}$ 都是可求长路径。称路径 σ 和 γ 等价, 如果存在连续、严格增函数 $\varphi: [c, d] \rightarrow [a, b]$, 且 $\varphi(c) = a, \varphi(d) = b$, 使得 $\sigma = \gamma \circ \varphi$. 我们称函数 φ 为一个参数变换。



一条曲线是路径的一个等价类。一条曲线的迹是其等价类中任意一条路径的迹。如果 f 在曲线的迹上连续, 那么 f 在曲线上的积分定义为 f 在等价类中任意一条路径上的积分。

曲线是光滑的 (分段光滑的), 当且仅当, 它的等价类中某一个路径是光滑的 (分段光滑的)。

今后, 曲线和它的等价类中的路径我们将不加区别。假如 “设 γ 是按照反时针方向通过一次的单位圆周” 就表示一条曲线。读者应当相信, 今后所叙述的关于曲线的结果, 与具体路径的取法无关。

设 $\gamma: [a, b] \rightarrow \mathbb{C}$ 是一个可求长路径, 且对于 $a \leq t \leq b$, 令 $|\gamma|(t)$ 为 $V(\gamma; [a, t])$, 即

$$|\gamma|(t) = \sup \left\{ \sum_{k=1}^n |\gamma(t_k) - \gamma(t_{k-1})| : \{t_0 < t_1 < \cdots < t_n\} \text{ 是 } [a, t] \text{ 的分割} \right\}.$$

显然, $|\gamma|(t)$ 是增函数, 所以 $|\gamma|: [a, b] \rightarrow \mathbb{C}$ 是有界变差函数。如果 f 在 $\{\gamma\}$ 上连续, 定义

$$\int_{\gamma} f|dz| = \int_a^b f(\gamma(t))d|\gamma|(t).$$

如果 γ 是可求长曲线, 那么用 $-\gamma$ 表示由 $(-\gamma)(t) = \gamma(-t)$ 定义的曲线, $-b \leq t \leq -a$. 其另一个记号是 γ^{-1} . 此外, 如果 $c \in \mathbb{C}$, $\gamma + c$ 表示由 $(\gamma + c)(t) = \gamma(t) + c$ 定义的曲线。下面的命题给出线积分的许多基本性质。

命题 34.6

设 γ 是可求长曲线, f 是 $\{\gamma\}$ 上的连续函数, 则

- (a) $\int_{\gamma} f = -\int_{-\gamma} f$;
- (b) $|\int_{\gamma} f| \leq \int_{\gamma} |f||dz| \leq V(\gamma) \sup\{|f(z)| : z \in \{\gamma\}\}$;
- (c) 如果 $c \in \mathbb{C}$, 那么 $\int_{\gamma} f(z)dz = \int_{\gamma+c} f(z)dz$.



证明留作习题。

下面的结果类似于关于线积分的微积分学的基本定理。

¹所谓 “像上面那样的 φ ” 是指不减的 φ ---校者注

定理 34.3

设 G 是 \mathbb{C} 中的开集, γ 是 G 内的可求长路径, 其起点和终点分别是 α 和 β . 如果 $f: G \rightarrow \mathbb{C}$ 是连续函数, 且具有原函数 $F: G \rightarrow \mathbb{C}$. 则

$$\int_{\gamma} f = F(\beta) - F(\alpha).$$

(我们记得, 当 $F' = f$ 时, 则称 F 是 f 的原函数。)



在这个定理的证明中, 需要下面有用的事实。

引理 34.1

如果 G 是 \mathbb{C} 中的开集, $\gamma: [a, b] \rightarrow G$ 是可求长路径, $f: G \rightarrow \mathbb{C}$ 是连续的, 则对于每个 $\epsilon > 0$, 存在 G 内的折线 Γ , 使得 $\Gamma(a) = \gamma(a)$, $\Gamma(b) = \gamma(b)$, 并且 $\left| \int_{\gamma} f - \int_{\Gamma} f \right| < \epsilon$.



证明 情形 I 设 G 是一个开圆。由于 $\{\gamma\}$ 是紧集, $d = \text{dist}(\{\gamma\}, \partial G) > 0$. 由此推出, 如果 $G = B(c; r)$, 那么 $\{\gamma\} \subset B(c; \rho)$, 其中 $\rho = r - \frac{1}{2}d$. 过渡到这个较小的圆的理由是, f 在 $\bar{B}(c; \rho) \subset G$ 上是一致连续的, 因此, 不失一般性, 可以假定 f 在 G 内是一致连续的。选取 $\delta > 0$, 使得当 $|z - w| < \delta$ 时, $|f(z) - f(w)| < \epsilon$. 如果 $\gamma: [a, b] \rightarrow \mathbb{C}$, 那么 γ 是一致连续的。于是存在 $[a, b]$ 的分割 $\{t_0 < t_1 < \cdots < t_n\}$ 使得当 $t_{k-1} \leq s, t \leq t_k$ 时,

$$|\gamma(s) - \gamma(t)| < \delta. \quad (34.1.7)$$

并且对于 $t_{k-1} \leq \tau_k \leq t_k$, 有

$$\left| \int_{\gamma} f - \sum_{k=1}^n f(\gamma(\tau_k)) [\gamma(t_k) - \gamma(t_{k-1})] \right| < \epsilon. \quad (34.1.8)$$

我们定义 $\Gamma: [a, b] \rightarrow \mathbb{C}$ 为

$$\Gamma(t) = \frac{1}{t_k - t_{k-1}} [(t_k - t)\gamma(t_{k-1}) + (t - t_{k-1})\gamma(t_k)],$$

$$t_{k-1} \leq t \leq t_k.$$

所以在 $[t_{k-1}, t_k]$ 上, $\Gamma(t)$ 是从 $\gamma(t_{k-1})$ 到 $\gamma(t_k)$ 的线段, 即 Γ 是 G 内的折线路径。由 (34.1.7) 得到

$$|\Gamma(t) - \gamma(\tau_k)| < \delta, t_{k-1} \leq t \leq t_k. \quad (34.1.9)$$

由于 $\int_{\Gamma} f = \int_a^b f[\Gamma(t)]\Gamma'(t)dt$, 所以

$$\int_{\Gamma} f = \sum_{k=1}^n \frac{\gamma(t_k) - \gamma(t_{k-1})}{t_k - t_{k-1}} \int_{t_{k-1}}^{t_k} f(\Gamma(t))dt.$$

利用 (34.1.8), 我们得到

$$\begin{aligned} \left| \int_{\gamma} f - \int_{\Gamma} f \right| &\leq \epsilon + \left| \sum_{k=1}^n f(\gamma(\tau_k)) \right. \\ &\quad \cdot [\gamma(t_k) - \gamma(t_{k-1})] - \int_{\Gamma} f \left| \right. \\ &\leq \epsilon + \sum_{k=1}^n |\gamma(t_k) - \gamma(t_{k-1})| (t_k - t_{k-1})^{-1} \\ &\quad \cdot \int_{t_{k-1}}^{t_k} |f(\Gamma(t)) - f(\gamma(\tau_k))| dt. \end{aligned}$$

应用 (34.1.9) 于被积函数, 得到

$$\left| \int_{\gamma} f - \int_{\Gamma} f \right| \leq \epsilon + \epsilon \sum_{k=1}^n |\gamma(t_k) - \gamma(t_{k-1})| \leq \epsilon(1 + V(\gamma)).$$

情形 I 得证。

情形 II G 是任意的。由于 $\{\gamma\}$ 是紧集, 所以存在数 $r > 0, 0 < r < \text{dist}(\{\gamma\}, \partial G)$. 选取 $\delta > 0$, 使得当 $|s - t| < \delta$ 时, $|\gamma(s) - \gamma(t)| < r$. 如果 $P = \{t_0 < t_1 < \cdots < t_n\}$ 是 $[a, b]$ 的一个分割, 且 $\|P\| < \delta$, 那么对于 $t_{k-1} \leq t \leq t_k$, 有 $|\gamma(t) - \gamma(t_{k-1})| < r$. 即, 如果 $\gamma_k : [t_{k-1}, t_k] \rightarrow \mathbb{C}$ 定义为 $\gamma_k(t) = \gamma(t)$, 那么 $\{\gamma_k\} \subset B(\gamma(t_{k-1}); r), 1 \leq k \leq n$. 由情形 I, 存在一条折线路径 $\Gamma_k : [t_{k-1}, t_k] \rightarrow B(\gamma(t_{k-1}); r)$ 使得 $\Gamma(t_{k-1}) = \gamma(t_{k-1}), \Gamma(t_k) = \gamma(t_k)$, 且 $\left| \int_{\gamma_k} f - \int_{\Gamma_k} f \right| < \epsilon/n$. 在 $[t_{k-1}, t_k]$ 上让 $\Gamma(t) = \Gamma_k(t)$, 那么 Γ 具有所要求的性质。

定理 34.3 的证明 情形 I $\gamma : [a, b] \rightarrow \mathbb{C}$ 是分段光滑的。这时由微积分学的基本定理,

$$\begin{aligned} \int_{\gamma} f &= \int_a^b f(\gamma(t)) \gamma'(t) dt = \int_a^b F'(\gamma(t)) \gamma'(t) dt \\ &= \int_a^b (F \circ \gamma)'(t) dt = F(\gamma(b)) - F(\gamma(a)) \\ &= F(\beta) - F(\alpha). \end{aligned}$$

情形 II 一般情形, 若 $\epsilon > 0$, 由引理 34.1, 存在从 α 到 β 的折线路径 Γ , 使得 $\left| \int_{\gamma} f - \int_{\Gamma} f \right| < \epsilon$, 但是 Γ 是分段光滑的, 所以由情形 I, $\int_{\Gamma} f = F(\beta) - F(\alpha)$. 因此 $\left| \int_{\gamma} f - [F(\beta) - F(\alpha)] \right| < \epsilon$; 由于 ϵ 是任意的。我们所要求的等式得证。

在定理 34.3 的证明中, 利用引理 34.1, 从分段光滑的情形过渡到可求长的情形, 这种方法在关于线积分许多结果的证明中是有代表性的。今后我们还会看到引理 34.1 的应用。

称一条曲线 $\gamma : [a, b] \rightarrow \mathbb{C}$ 是闭的, 如果 $\gamma(a) = \gamma(b)$.

推论 34.1

设 G, γ 和 f 满足定理 34.3 中的假定, 如果 γ 是闭曲线, 则

$$\int_{\gamma} f = 0.$$



微积分学的基本定理告诉我们, 每一个连续函数必有原函数。对于复变函数来说, 情况远非如此, 例如, 设 $f(z) = x^2 + y^2$, 如果 F 是 f 的原函数。现在由 Cauchy-Riemann

方程, 得到

$$\frac{\partial U}{\partial x} = \frac{\partial V}{\partial y} = x^2 + y^2, \quad \frac{\partial U}{\partial y} = \frac{\partial V}{\partial x} = 0.$$

但是 $\frac{\partial U}{\partial y} = 0$ 蕴含着 $U(x, y) = u(x)$, $u(x)$ 是某一个可微的函数, 所以 $x^2 + y^2 = \frac{\partial U}{\partial x} = u'(x)$, 这是一个明显的矛盾. 应用定理34.3也可以看出 $|z|^2$ 没有原函数 (见习题8.).

第三十四章 习题

1. 设 $\gamma: [a, b] \rightarrow \mathbb{R}$ 是非减的, 证明: γ 是有界变差函数, 且 $V(\gamma) = \gamma(b) - \gamma(a)$.
2. 证明命题34.1.
3. 证明命题34.3.
4. 证明命题34.4 (利用归纳法).
5. 设 $\gamma(t) = \exp((-1+i)t^{-1})$, $0 < t < 1$, 且 $\gamma(0) = 0$, 证明: γ 是可求长路径, 并求出 $V(\gamma)$, 作出 γ 的迹的略图.
6. 证明: 如果 $\gamma: [a, b] \rightarrow \mathbb{C}$ 是 Lipschitz 函数, 则 γ 是有界变差函数.
7. 设 $\gamma: [a, b] \rightarrow \mathbb{C}$ 定义为 $\gamma(t) = t + it \sin \frac{1}{t}$, 当 $t \neq 0$ 时. $\gamma(0) = 0$. 证明 γ 是一条路径, 但不是可求长的, 作出这一条路径.
8. 设 γ 和 σ 是两条折线 $[1, i]$ 和 $[1, 1+i, i]$. 试将 γ 和 σ 表示为路径, 并计算 $\int_{\gamma} f$ 和 $\int_{\sigma} f$, 其中 $f(z) = |z|^2$.
9. 定义

34.2 解析函数的幂级数表示

命题 34.7

设 φ



第 三十五 章 Runge 定理

35.1 Runge 定理

35.2 单连通性

35.3 Mittag-Leffler 定理

第 三 十 六 章 调 和 函 数

第九部分

数学分析

《数学分析》的作者是克莱鲍尔 (G.Klambauer)。参考：[8]。

第三十七章 实数系

在这一章,我们考察实数系的一些性质,它们对于真正地理解微积分的基本概念(如收敛性,连续性,微分和积分)是必不可少的。不过,对于初学者来说,本章前两节中命题的证明细节可以略去不看。

37.1 整数,有理数与无理数

全体正整数(自然数)之集 \mathbb{N} 有两个重要性质。我们将叙述这两个性质并建立其等价性。

良序原理 任何非空正整数集有最小元素。

数学归纳原理 若 P 是具有下列性质的正整数集。

(i) P 含有数 1;

(ii) 只要 P 含有正整数 n , 它也含有正整数 $n+1$;

则 P 含有所有正整数, 即 $P = \mathbb{N}$ 。

命题 37.1

数 1 是最小正整数。



证法 1 (根据数学归纳原理) 设 S 是所有 ≥ 1 的正整数集。显然, 1 属于 S 。若整数 n 属于 S , 则 $n \geq 1$ 。因此 $n+1 > n \geq 1$, $n+1$ 属于 S 。由数学归纳原理, $S = \mathbb{N}$, 故所有正整数大于或等于 1。

证法 2 (根据良序原理) 从良序原理知道存在最小正整数, 比如说是 s , 设 $s < 1$ 。以 s 乘不等式 $0 < s < 1$ 得 $0 < s^2 < s$, 这说明 s 不是最小正整数。由于设 $s < 1$ 导致矛盾, 故这个假设不正确。因而 1 是最小正整数。

推论 37.1

若 n 是整数, 则 n 与 $n+1$ 之间不存在整数。



证明 设存在整数 k 满足 $n < k < n+1$, 则 $0 < k-n < 1$, 与 1 是最小正整数矛盾。

注 断言“存在最大正整数 n ”是错误的。因为由此将有 $n^2 = n$, 而这就是说 n 应该等于 1。

命题 37.2

数学归纳原理与良序原理等价, 即, 只要以整数的通常的算术性质为前提, 就能从其中之一推出另一个。



证明 (第一部分) 设良序原理成立, S 是具有性质

(i) 1 属于 S ;

(ii) 若 n 属于 S , 则 $n+1$ 也属于 S

的正整数集。我们应该证明 S 是所有正整数之集 \mathbb{N} 。

设 T 是所有不属于 S 的正整数之集. 若 T 非空, 则由良序原理知有最小元素, 设为 t . 因为 1 属于 S , 且 1 是最小正整数 (见用良序原理建立的命题 1), 故 $t > 1$. 这样 $t-1$ 必定是属于 S 的正整数, 因为 $t-1 < t$. 由于 $t = (t-1) + 1$, S 的第二个性质保证 t 也属于 S . 但 S 与 T 不相交, 故矛盾. 由于我们假设 T 非空导致矛盾, 故 T 是空集, 即 $S = \mathbb{N}$.

(第二部分) 假定数学归纳原理成立, 其次, 设存在非空正整数集 S 没有最小元素. 因为 1 是最小正整数 (见用数学归纳原理建立的命题 1), 故 1 不属于 S 且小于 S 的所有元素.


设 T 是比 S 的所有元素小的全体正整数之集. 我们已经知道 1 属于 T . 设 n 属于 T . 若 $n+1$ 属于 S , 则由于 n 与 $n+1$ 之间不存在整数 (由命题 1 推论), $n+1$ 将是 S 的最小元素; 但这与我们对 S 的假设矛盾. 因而, n 属于 T 时 $n+1$ 必属于 T . 由数学归纳原理, T 含有全体正整数, 从而 S 是空集. 但这又与原来假设 S 非空矛盾. 故若 S 是非空正整数集, 则 S 有最小元素. 证毕.

数学归纳原理的一种修改过的、但等价的形式说:

满足下列两个性质的关于正整数的陈述对所有正整数成立:

- (i) 此陈述对整数 1 成立;
- (ii) 若这个陈述对正整数 n 成立, 则对正整数 $n+1$ 也必成立.


定义 37.1

设 a, b 是整数, $b \neq 0$. 若存在第三个整数 c 使 $bc = a$, 则称 a 能被 b 整除. 我们也说 b 整除 a 或 a 是 b 的倍数, 记为 $b \mid a$. 若 $b \neq 0$ 且 a 不能被 b 整除, 则写成 $b \nmid a$. 


容易证明下列性质:

- (i) $b \mid a$ 与 $a > 0, b > 0$ 蕴含 $1 \leq b \leq a$;
- (ii) $c \mid b$ 与 $b \mid a$ 蕴含 $c \mid a$;
- (iii) 对所有整数 $m, n, c \mid a$ 与 $c \mid b$ 蕴含 $c \mid ma + nb$.

定义 37.2

设 $p > 1$ 是整数, 若除 1 以外 p 不能被比它小的正整数整除, 则称 p 为素数. 不是素数的大于 1 的正整数叫合数. 

命题 37.3

大于 1 的整数是素数或素数之积. 其次, 如果不计因数的次序, 则分解为素因数之积的方法唯一. 

证明 先证明合数可分解为素数之积.

设这个结论不正确, 则存在不能写成素数之积的合数. 设 n 是这样的数里最小的一个 (由良序原理, 这样的 n 是存在的). 因为 n 是合数, 故可写作

$$n = ab, 1 < a < n, 1 < b < n.$$

当 a 比 n 小时, a 是素数或素数之积; 对 b 也一样. 但这样一来, $n = ab$ 是素数之积, 矛盾. 因此合数都可以分解为素因数之积.

现在证明分解方法唯一。设存在分解方法不唯一的合数。这样的数里最小的一个（这里用到良序原理）设为

$$Q = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_j,$$

这里的 p_1, p_2, \dots, p_k 与 q_1, q_2, \dots, q_j 都是素数。显然，所有的 p 与所有的 q 都不同，否则可约去某个 p 与某个 q 而得到更小有两种不同分解的整数。设

$$p_1 \leq p_2 \leq \cdots \leq p_k, q_1 \leq q_2 \leq \cdots \leq q_j.$$

由于 $p_1 \neq q_1$, 故可设 $p_1 < q_1$ 而不会带来什么不便。考虑

$$P = p_1 q_2 \cdots q_j.$$

显然, $p_1 \mid P, p_1 \mid Q$, 故 $p_1 \mid (Q - P)$. 但

$$Q - P = (q_1 - p_1) q_2 q_3 \cdots q_j,$$

因此 $Q - P$ 是正的。把 $q_1 - p_1$ 写成素数之积, 设为

$$q_1 - p_1 = r_1 \cdots r_s,$$

则

$$Q - P = r_1 \cdots r_s q_2 \cdots q_j.$$

我们已经知道 p_1 与各个 q_i 都不相等。由于 $p_1 \nmid (q_1 - p_1)$, 故对所有 i 有 $p_1 \nmid r_i$. 因此所有的 q 和 r 都与 p_1 不同。另一方面, $Q - P$ 能被 p_1 整除, 因而

$$Q - P = p_1 t_1 \cdots t_h,$$

这里的各个 t 都是素数。这样, 我们得到了 $Q - P$ 的两种不同的因数分解, 其中之一出现 p_1 , 另一种不出现 p_1 . 这与 Q 的最小性矛盾, 因为 $0 < Q - P < Q$. 证毕。

命题 37.4

任意给定的素数的有限集之外存在另一个素数, 即, 不存在最大素数。



证明 设 $q = 2 \cdot 3 \cdot 5 \cdots p$ 是所有 $\leq p$ 的素数之积。数

$$q + 1 = (2 \cdot 3 \cdot 5 \cdots p) + 1$$

不能被这些素数里的任何一个整除。由于 $q + 1 > 1$, 故 $q + 1$ 或者是比 p 大的素数, 或者能被比 p 大的素数整除。所以素数必是无限个。

注 设 p_n 表示第 n 个素数。由上述命题的证明可知, 存在某个 $m > n$, 使

$$p_m \mid (p_1 p_2 \cdots p_n + 1),$$

因此 $p_{n+1} \leq p_m < p_n^n + 1$.

37.2 Dedekind 分割

37.3 不等式

37.4 实数列

37.5 实数级数

37.6 有规则的小数

第 三十八 章 连续性

第 三十九 章 微分与积分

第 四十 章 一致收敛性

第 四 十 一 章 度 量 空 间

参考文献

- [1] S. 麦克莱恩 G. 伯克霍夫. 近世代数概论[M]. 北京: 人民教育出版社, 1979.
- [2] MICHAEL.ARTIN. 代数[M]. 北京: 机械工业出版社, 2015.
- [3] N.JACOBSON. 基础代数[M]. 北京: 高等教育出版社, 1987.
- [4] MICHAEL.SPIVAK. 微积分[M]. 北京: 人民教育出版社, 1981.
- [5] C.GOFFMAN. 多元微积分[M]. 北京: 人民教育出版社, 1978.
- [6] TOM.M.APOSTOL. 数学分析[M]. 北京: 机械工业出版社, 2006.
- [7] J.B. 康威. 单复变函数[M]. 上海: 上海科学技术出版社, 1978.
- [8] TOM.M.APOSTOL. 数学分析[M]. 上海: 上海科学技术出版社, 1981.