高等代数 — 引言

张彪

天津师范大学

数学科学学院

zhang@tjnu.edu.cn

提纲

提纲

宇宙之大，粒子之微，

火箭之速，化工之巧，

地球之变，生物之谜，

日用之繁，无处不用数学。

图: 华罗庚 (1910–1985)

中国解析数论创始人和开拓者

数学是科学的皇后

图: 高斯

高斯 (Johann Carl Friedrich Gauss，1777 年 4 月 30 日-1855 年 2 月 23 日)，德国著名数学家、天文学家、大地测量学家、物理学家。

被认为是最重要的数学家，并有数学王子的美誉。

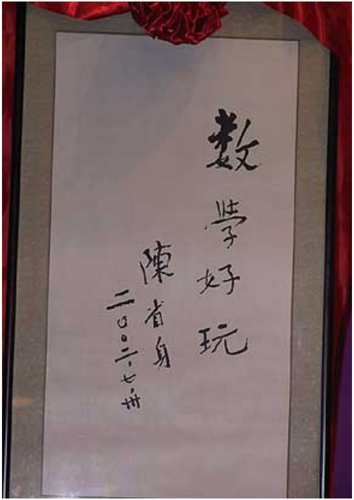


图: 陈省身 (1911-2004)

2002 年 8 月在北京举行国际数学家大会期间，91 岁高龄的数学大师陈省身先生为少年儿童题词。

20 世纪世界最重要的微分几何学家之一、美国国家数学科学研究所首任所长、南开数学研究所首任所长

自然科学的发展往往是在推翻或修正旧的理论基础上建立新理论的大厦。

- 哥白尼 (1473—1543) 的 “日心说” 推翻了托勒密 (约 90-168) 的 “地心说”
- 伽利略（1564-1642）的比萨斜塔落体实验否定了亚里士多德 (前 384-前 322) 的错误想象
- 爱因斯坦 (1879-1955) 的相对论则是对牛顿 (1643 − 1727) 运动定律的修正。

- 然而，作为自然科学的共同语言，数学的独特之处在于它不需要被订正，新的数学理论只是为旧的建筑添砖加瓦，而无须连根拔起。
- 在数学里，已经证明为真的的命题永远为真。比如勾股定理（毕达哥拉斯定理）。
- 欧氏几何源于公元前 3 世纪。古希腊数学家欧几里德把人们公认的一些几何知识作为定义和公理 (公设)，在此基础上研究图形的性质，推导出一系列定理，组成演绎体系，写出《几何原本》，形成了欧氏几何。
- 美国卓越的科普作家阿西莫夫所说: “托勒密也许对天体系统给出了错误的描绘，但他为了计算而发展出的三角学系统永远是正确的。”

代数学起源于人类对于数的理解

代数学习的几个阶段

- 算　术：自然数、正分数的四则运算（小学）
- 初等代数：有理数、无理数、复数、解方程（中学）
- 高等代数：多项式、线性代数（大一）
- 近世代数：群、环、域（大二）
- . . . .

教材

教材

- 北京大学数学系几何与代数教研室代数小组, 高等代数 (第 5 版), 高等教育出版社, 2019.

参考书目

- 王萼芳, 石生明, 高等代数辅导与习题解答 （北大·第 5 版), 高等教育出版社, 2019.
- 徐仲等, 高等代数 (北大第四版) 导教导学导考, 西安: 西北工业大学出版社, 2014.

Outline

第一学期

1 多项式

2 行列式

3 线性方程组

第二学期

4 矩阵

5 二次型

6 线性空间

7 线性变换

9 欧几里得空间

图: 课程网页

提纲

充分条件和必要条件

设 A 与 B 为两命题，

- A 的充分条件是 B

  如果 B 成立，那么 A 成立，即 $A \Leftarrow B$（箭头表示能够推导出）
- A 的必要条件是 B

  如果 A 成立，那么 B 成立，即 $A \Rightarrow B$.
- A 的充分必要条件是 B
  - 充分性 $A \Leftarrow B$
  - 必要性 $A \Rightarrow B$

当且仅当

当且仅当 (英文：If and only if, 或者：iff)，在数学、哲学、逻辑学以及其他一些技术性领域中广泛使用，在英语中的对应标记为 iff。

设 A 与 B 为两命题，在证明

A 当且仅当 B

时，这相当于去同时证明陈述

- 如果 A 成立，那么 B 成立
- 如果 B 成立，把么 A 成立

公认的其他同样说法还有

B 是 A 的充分必要条件 (或称为充要条件).

注: 在定义中，“如果…那么…” 的意思就是当且仅当。

比如书上两个多项式相等的定义。

提纲

如果你有一排很长的直立着的多米诺骨牌那么如果你可以确定:

第一张骨牌将要倒下.

只要某一个骨牌倒了, 与他相临的下一个骨牌也要倒.

那么你就可以推断所有的的骨牌都将要倒.

第一数学归纳法

第一数学归纳法可以概括为以下三步:

1. 归纳奠基：证明 $n = 1$ 时命题成立.
2. 归纳假设：假设 $n = k$ 时命题成立.
3. 归纳递推：由归纳假设推出 $n = k + 1$ 时命题也成立.

例 1

证明对于任意正整数 n，下面的公式都成立

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

例 1

证明对于任意正整数 n，下面的公式都成立

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

证明

- 这个公式在 $n=1$ 时成立. 左边 $=1$，右边 $=\frac{1\times 2}{2}=1$.
  所以这个公式在 $n=1$ 时成立.
- 我们假设 $n=k$ 时公式成立，即
  $$1+2+\cdots+k=\frac{k(k+1)}{2}.$$
- 在上式等号两边分别加上 $k+1$ 得到
  $$1+2+\cdots+k+(k+1)=\frac{k(k+1)}{2}+(k+1)=\frac{(k+1)(k+2)}{2}.$$
  这就是 $n=k+1$ 时的等式.
  因此，对于任意正整数等式都成立. ∎

例 2

证明对于任意正整数 n，下面的公式都成立

$$1^2+2^2+3^2+\cdots+n^2=\frac{n(n+1)(2n+1)}{6}.$$

例 2

证明对于任意正整数 n，下面的公式都成立

$$1^2+2^2+3^2+\cdots+n^2=\frac{n(n+1)(2n+1)}{6}.$$

证明

- 这个公式在 $n=1$ 时成立. 左边 $=1$，右边 $=\frac{1\times2\times3}{6}=1$.
  所以这个公式在 $n=1$ 时成立.
- 我们假设 $n=k$ 时公式成立，即
  $$1^2+2^2+3^2+\cdots+k^2=\frac{k(k+1)(2k+1)}{6}.$$
- 在上式等号两边分别加上 $k+1$ 得到
  $$\begin{aligned}1^2+2^2+\cdots+k^2+(k+1)^2&=\frac{k(k+1)(2k+1)}{6}+(k+1)^2\\&=\frac{(k+1)(k+2)(2k+3)}{6}.\end{aligned}$$

  这就是 $n=k+1$ 时的等式.

例 3

对于任意自然数 n 证明 3^n-1 是 2 的倍数.

例 3

对于任意自然数 n 证明 3^n-1 是 2 的倍数.

证明

- $3^0-1=1-1=0$ 是 2 的倍数. 所以, 当 $n=0$ 时命题成立.
- 我们假设 $n=k$ 时命题成立, 即 3^k-1 是 2 的倍数.
- 接下来证明 $n=k+1$ 时命题也成立.

$$3^{k+1}-1=2\cdot 3^k+(3^k-1)$$

$2\cdot 3^k$ 是 2 的倍数. 由归纳假设，3^k-1 是 2 的倍数. 又因为 $2\cdot 3^k$ 也是 2 的倍数, 所以 $3^{k+1}-1$ 是 2 的倍数.

因此，对于任意自然数 n，都有 3^n-1 是 2 的倍数. ∎

第二数学归纳法

有些命题用第一归纳法证明不大方便，可以用第二归纳法证明.

第二数学归纳法的证明步骤是：

1. 证明当 $n = 1$ 时命题成立.
2. 假设 $n \leq k$ 时命题都成立.
3. 由归纳假设推出 $n = k + 1$ 时命题也成立.

提纲

在数学中经常碰到若干个数连加的情况

$$a_1 + a_2 + \cdots + a_n. \tag{1}$$

为了简便起见，我们通常记成

$$\sum_{i=1}^{n} a_i. \tag{2}$$

称 $\sum$ 为连加号，而连加号上下的写法表示 i 的取值由 1 到 n.
例如

$$1^2 + 2^2 + \cdots + n^2 = \sum_{i=1}^{n} i^2.,$$

这里的 i 称为求和指标, 它只起一个辅助的作用.
把 (2) 还原成 (1) 时，它是不出现的. 譬如说, (1)也可以记成

$$\sum_{j=1}^{n} a_j.$$

因之, 只要不与连加号中出现的其它指标相混, 用什么字母作为求和指标是任意的.

提纲

整数的可除性理论

用 $\mathbb{Z}$ 表示全体整数组成的数集.

整数有加法, 减法和乘法等运算, 减法是加法的逆运算.

- 带余除法
- 整除
- 最大公因数
- 辗转相除法
- 互素
- 素数
- 因数分解定理
- 最小公倍数

带余除法

在 $\mathbb{Z}$ 中不能作除法, 但是有以下的带余除法.

定理 1

对于任意两个整数 a, b, 其中 $b \neq 0$, 存在一对整数 q, r 满足

$$a = q \cdot b + r, \quad 0 \leqslant r < |b|$$

而且满足这个条件的整数 q, r 是唯一的.

定义

- q 称为 b 除 a 的商,
- r 称为 b 除 a 的余数.

定义

对于整数 a, b, 如果存在一个整数 c 使得 $a = bc$, 则称

- b 是 a 的因数,
- a 是 b 的倍数.

注

在定义中我们并不要求 $b \neq 0$.

性质

当 $b \neq 0$ 时， b 是 a 的因数的充分必要条件是 b 除 a 所得的余数为 0.

因此 b 是 a 的因数, 也称 b 整除 a, 记作 $b|a$.

关于整除，有以下一些性质：

性质

1. 如果 $a|b, b|a$, 则 $a=\pm b$
2. 如果 $a|b, b|c$, 则 $a|c$
3. 如果 $a|b, a|c$, 则对任意整数 k, l 都有 $a|kb+lc$

注

- 如果 $a|b$, 则有 $-a|b$ 及 $a|(-b)$, 因此以后我们只讨论非负整数的非负因数和非负倍数，不再加以说明.
- 根据定义，每个整数都是 *0* 的因数，但是 *0* 不是任何非零整数的因数.

定义

如果 a 既是 b 的因数, 又是 c 的因数, 则称 a 是 b 和 c 的一个公因数.

公因数中最重要的是最大公因数.

定义

设 d 是 a 和 b 的一个公因数. 如果 a, b 的任一个共因数都是 d 的因数, 则称 d 是 a, b 的一个最大公因数.

注

- 根据定义，如果 d_1, d_2 都是 a, b 的最大公因数, 那么 $d_1 \mid d_2, d_2 \mid d_1$. 从而 $d_1 = \pm d_2$. 按规定 d_1, d_2 皆非负, 故 $d_1 = d_2$.
- 当 $b|a$ 时, b 是 a 与 b 的最大公因数.
- 特别地当 $b = 0$ 时, a 是 a 与 b 的一个最大公因数.
- 当 a, b 不全为零时, a, b 的最大公因数不为 0, 这时我们规定: 以 (a, b) 表示 a, b 的正的最大公因数. 在这个规定下，(a, b) 是唯一的.

辗转相除法

设 $b \neq 0$, 即 $b > 0$. 反复应用带余除法.

$$\begin{aligned} a &= q_1 b + r_1, & 0 < r_1 < b \\ b &= q_2 r_1 + r_2, & 0 < r_2 < r_1 \\ &\cdots & \cdots \\ r_{k-2} &= q_k r_{k-1} + r_k, & 0 < r_k < r_{k-1} \\ r_{k-1} &= q_{k+1} r_k + 0 \end{aligned}$$

直到出现余数为零而终止. 则有

$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{k-1}, r_k) = r_k$$

从上面的算法中还可以找到整数 u, v 使得

$$(a, b) = ua + vb$$

这是最大公因数的重要性质.

定义

如果整数 a, b 的最大公因数等于 1, 则称 a, b 互素 (也称互质).

例如，3 与 5 互素, 21 与 40 互素.

互素有以下一些重要性质:

1. a, b 互素的充分必要条件是存在整数 u, v 使
$$u\,a + v\,b = 1$$
2. 如果 $a|bc$, 且 $(a, b) = 1$, 则 $a|c$.
3. 如果 $a|c, b|c$ 而且 $(a, b) = 1$, 则 $ab|c$
4. 如果 $(a, c) = 1, (b, c) = 1$, 则 $(ab, c) = 1$

这些性质说明了互素的重要性.

注

对于整数 $c \neq 1$, 如果存在整数 u, v 使 $u\,a + v\,b = c$, 这不意味着 c 是 a 和 b 的最大公因数。试试自己举出反例。

定义

设 a 是一个大于 *1* 的整数. 如果除去 *1* 和本身外, a 没有其它因数, 那么称 a 是一个素数(也称质数).

例如 2, 3, 5, 23 等都是素数.

从定义可知, 如果 p 表示成 $p = a \cdot b$, 则必有 $a = 1, b = p$ 或 $a = p, b = 1$

性质

1. 一个素数 p 和任一个整数 a 都有 或者 $p|a$, 或者 $(p, a) = 1$.
2. 如果素数 $p|ab$, 那么 $p|a$ 或 $p|b$.
3. 如果一个大于 *1* 的整数 p 和任何整数 a 都有 $p|a$ 或$(p, a) = 1$, 则 p 是一个素数.
4. 如果大于 *1* 的整数 p 具有下述性质: 对任何整数 a, b 从 $p|ab$ 可推出 $p|a$ 或 $p|b$, 则 p 是一个素数.

如果一个素数 p 是整数 a 的一个因数, 则 p 称为 a 的一个素因数.

根据互素及素数的性质, 应用数学归纳法可以证明整数的一个基本定理.

定理 2 (因数分解及唯一性定理)

任一个大于 *1* 的整数 *a* 可以分解成有限多个素因数的乘积:

$$a = p_1 p_2 \cdots p_s$$

而且分解法是唯一的，即如果有两种分解法:

$$a = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$$

其中 $p_1, \cdots, p_s; q_1, \cdots, q_t$ 都是素数, 那么有 $s = t$, 并且重新将 $q_1, \cdots, q_t$ 适当排序后，可得 $p_i = q_i, \quad i = 1, 2, \cdots, s.$

在 a 的分解式中, 将同一个素因数合并写成方幂, 并且将素因数按大小排列, 得到

$$a = p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}, \quad p_1 < p_2 < \cdots < p_r, l_i > 0, i = 1, \cdots, r.$$

这种表示法称为 a 的标准分解式.

可以应用整数的分解式来判断整除性及计算最大公因数.

现在将整数 a , b 的因数合在一起, 设为 $p_1, p_2, \cdots, p_t$, 并设

$$\begin{cases} a = p_1^{\ell_1} p_2^{\ell_2} \cdots p_t^{\ell_t}, & \ell_i \geqslant 0, \quad i = 1, 2, \cdots, t \\ b = p_1^{d_1} p_2^{d_2} \cdots p_t^{d_t}, & d_i \geqslant 0, \quad i = 1, 2, \cdots, t \end{cases} \tag{3}$$

则

1. a 能整除 b 的充分必要条件为 $\ell_i \leqslant d_i$, $i = 1, 2, \cdots, t$
2. $(a, b) = p_1^{\min(\ell_1, d_1)} p_2^{\min(\ell_2, d_2)} \cdots p_t^{\min(\ell_t, d_t)}$

定义

设 a, b 是两个非负整数. m 是 a, b 的一个公倍数 (按前面约定, 也是非负的). 如果 a, b 的任一个公倍数都是 m 的倍数, 则 m 称为 a, b 的一个**最小公倍数**.

注

- 由定义可看出 a, b 的最小公倍数是唯一的, 记作 $[a, b]$.
- 当 a, b 是正整数时, 从它们的标准分解式可以求出最小公倍数. 设 a , b 的分解如 (3)，则

$$[a, b] = p_1^{\max(l_1, d_1)} p_2^{\max(l_2, d_2)} \cdots p_t^{\max(p_t, d_t)}$$

- 由此还可看出

$$ab = (a, b) \cdot [a, b]$$

例 4 (思考题)

一个整数能被 3 整除当且仅当这个数的数字和能被 3 整除。

例 5 (思考题)

一个数字能被 7 整除当且仅当其末 3 位与末 3 位之前的数字之差能被 7 整除。

提纲

高中的时候，定义了

$$\mathrm{i} = \sqrt{-1}$$

然后形如：

$$a + b\,\mathrm{i} \quad (a, b \in \mathbb{R})$$

这样的数就是复数。全体复数的集合记为

$$\mathbb{C} = \{a + b\,\mathrm{i} \mid a, b \in \mathbb{R}\}$$

有了复数之后，开方运算就不再局限于大于零的数了，这样一元二次方程

$$ax^2 + bx + c = 0 \quad (a \neq 0)$$

就总是有解了：

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

- 定义 $\mathbb{C}$ 内的加法

$$(a + bi) + (c + d\mathrm{i}) := (a + c) + (b + d)\,\mathrm{i}$$

- 定义 $a + b\,\mathrm{i}$ 的负数 $-(a + b\,\mathrm{i})$ 是 $(-a) + (-b)\,\mathrm{i}$
- 定义 $\mathbb{C}$ 内的减法

$$(a + b\,\mathrm{i}) - (c + d\mathrm{i}) = (a - c) + (b - d)\,\mathrm{i}$$

- 定义 $\mathbb{C}$ 内的乘法

$$(a+b\mathrm{i})(c+d\mathrm{i})=(ac-bd)+(ad+bc)\mathrm{i}$$

- 定义 $a+b\mathrm{i}$ 的倒数或逆

$$\frac{1}{a+b\mathrm{i}}=\frac{1}{a^2+b^2}(a-b\mathrm{i})=\frac{a-b\mathrm{i}}{a^2+b^2}$$

- $\mathbb{C}$ 内的除法是 (设 $c+d\mathrm{i}\neq 0$)

$$\frac{a+b\mathrm{i}}{c+d\mathrm{i}}=(a+b\mathrm{i})\frac{1}{c+d\mathrm{i}}=(a+b\mathrm{i})\frac{c-d\mathrm{i}}{c^2+d^2}$$

复数的表示：实部、虚部、共轭、模

定义

对于复数 $z = a + b\mathrm{i}$, 其中 a, b 是实数.

- a 称为 z 的实部, 记为 $\mathit{Re}z$
- b 称为 z 的虚部, 记为 $\mathit{Im}z$
- 复数 $z = a + b\mathrm{i}$ 的共轭 $\bar{z} := a - b\mathrm{i}$
- $|z| = \sqrt{a^2 + b^2}$ 称为 $a + b\mathrm{i}$ 的模或绝对值。

性质

- $z\bar{z} = (a + b\mathrm{i})(a - b\mathrm{i}) = a^2 + b^2.$
- $z + \bar{z} = (a + b\mathrm{i}) + (a - b\mathrm{i}) = 2a.$
- $z - \bar{z} = (a + b\mathrm{i}) - (a - b\mathrm{i}) = 2b\mathrm{i}.$

定义

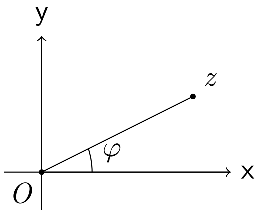
一个复数 $z=a+b\,\mathrm{i}$ 的**辐角**是指将 Ox 轴正方向沿逆时针方向旋转到 Oz 的旋转角 φ .

辐角的值不是唯一确定的，可以加上 2π 的任意整数倍.

因为 $a=|z|\cos\varphi, b=|z|\sin\varphi$, 故有

$$z=a+b\,\mathrm{i}=|\alpha|(\cos\varphi+i\sin\varphi)$$

上式称为复数的**三角表示**.



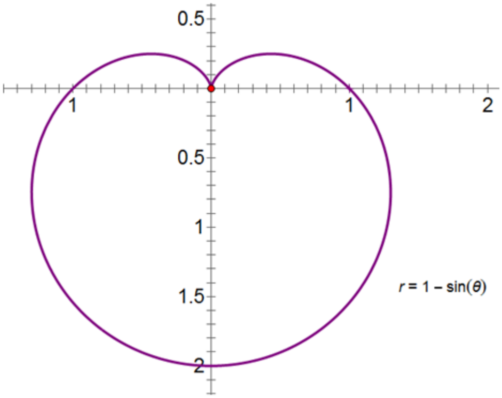


图: 笛卡尔心形线

如果又有复数

$$\beta = c + d\mathrm{i} = |\beta|(\cos\psi + \mathrm{i}\sin\psi)$$

那么

$$\begin{aligned}\alpha\beta &= |\alpha||\beta|(\cos\varphi + \mathrm{i}\sin\varphi)(\cos\psi + i\sin\psi) \\ &= |\alpha||\beta|(\cos\varphi\cos\psi - \sin\varphi\sin\psi) + (\sin\varphi\cos\psi + \cos\varphi\sin\psi)\,\mathrm{i}) \\ &= |\alpha||\beta|(\cos(\varphi + \psi) + \mathrm{i}\sin(\varphi + \psi))\end{aligned}$$

上式表示, 两个复数相乘时，其模为这两个复数的模相乘, 其辐角相加 (因为三角函数以 2 π 为周期, 故把相差 2 π 的整数倍的角认为是相同的).

欧拉公式

令模为 1 的复数

$$e^{i\varphi} = \cos\varphi + i\sin\varphi,$$

上式称为欧拉公式.

因而位于以坐标原点 O 为中心的单位圆上，其辐角为 φ. 于是

$$e^{i\varphi}e^{i\psi} = e^{i(\varphi+\psi)}.$$

当 φ 为 π 时,

$$e^{i\pi} = -1.$$

将数学内 4 个极重要的数 e, i, π, -1 连起来.

方程 $x^n - 1 = 0$ 的解

给定一个正整数 n, 考虑下面 n 个复数

$$\mathrm{e}^{\frac{2k\pi}{n}\mathrm{i}} = \cos\frac{2k\pi}{n} + \mathrm{i}\sin\frac{2k\pi}{n},$$

其中 $k = 0, 1, 2, \cdots, n-1$.

这 n 个复数就是以原点 O 为中心的单位圆的内接正 n 边形的 n 个顶点.

由欧拉公式可知,

$$\left(\mathrm{e}^{\frac{2k\pi}{n}i}\right)^n = \left(\cos\frac{2k\pi}{n} + \mathrm{i}\sin\frac{2k\pi}{n}\right)^n = \cos 2k\pi + \mathrm{i}\sin 2k\pi = 1.$$

因此，这 n 个复数恰为 n 次代数方程

$$x^n - 1 = 0$$

在复数系 $\mathbb{C}$ 内的 n 个根, 称为 n 次单位根。