高等代数

张彪

天津师范大学

zhang@tjnu.edu.cn

Outline

宇宙之大，粒子之微，
火箭之速，化工之巧，
地球之变，生物之评，
日用之繁，
无处不用数学.
一华罗庚

大约在 1637 年, 法国数学家 Fermat 断言,

猜想

对于大于 2 的整数 n, 三个未知量 x, y, z 的代数方程 $x^n + y^n = z^n$ 没有正整数解.

大约在 1637 年, 法国数学家 Fermat 断言,

猜想

对于大于 2 的整数 n, 三个未知量 x, y, z 的代数方程 $x^n + y^n = z^n$ 没有正整数解.

它历经 350 余年, 无数第一流的数学家为之绞尽脑汁, 才于 1994 年被 Princeton 大学的数学家 Wiles 使用现代最深奥的数学理论得出解答.

- 从生产实践和自然科学理论中，自然地产生了求解代数方程的问题，它就是代数学的经典课题.
- 例如，根据牛顿第二运动定律，物体所受的力 F，它的质量 m 和产生的加速度 a 之间存在关系 $F = \mathrm{ma}$. 如果已知物体的质量 m 和所受的力 F，求加速度 a，这就是一元一次方程的求解问题.
- 又比如，一个以初速 v_0 在水平面上作匀加速运动的物体，它的加速度 a，运动时间 t 和移动的距离 S 满足

$$S = v_0 t + \frac{1}{2}at^2$$

如果已知 S, v_0, a，求运动时间 t，这就是求一元二次方程的根.

- 数学史表明, 早在中世纪人们就已经找到解一元一次、二次代数方程的一般方法.
- 到欧洲的文艺复兴时代，又找到一元三次、四次方程的求根公式.
- 但是随后数学家们就碰到难题了. 在数百年时间内，他们苦苦寻求五次以上代数方程的求根公式, 却总是遭到失败.

- 数学史表明, 早在中世纪人们就已经找到解一元一次、二次代数方程的一般方法.
- 到欧洲的文艺复兴时代，又找到一元三次、四次方程的求根公式.
- 但是随后数学家们就碰到难题了. 在数百年时间内，他们苦苦寻求五次以上代数方程的求根公式, 却总是遭到失败.
- 直到 1832 年，法国数学家 Galois 才找到了一个高次代数方程有根式解 (即用该方程的系数经加、减、乘、除及开方运算表示它的全部根）的判别准则，完满地解决了高次代数方程根的理论课题.

根据 Galois 的理论，五次以上的一般代数方程没有求根公式.

Galois 的工作中最值得注意的是，他不是局限在数的四则运算的范围内考查问题.

他跳出这个圈子, 考查 n 次方程的 n 个根的某些置换所组成的集合 G, 规定 G 内两个置换的“乘积”是对根的集合逐次进行这两个置换.

他在一个并非由数组成的集合 G 内定义了一种新的代数运算：乘法(它完全不同于数的乘法). 他发现这种乘法也具有与数的乘法相类似的某些运算法则 (例如满足结合律等等). 这个新的具有乘法运算的集合我们现在把它称为该高次代数方程的 Galois 群.

Galois 证明：

高次代数方程有没有根式解取决于它的 Galois 群的结构.

这样，人们的认识发生了一个质的飞跃, 那就是为了研讨数及其代数运算中所包含的深刻规律, 我们必须跳出数及其四则运算的框框, 去研究一个更一般的集合及其中应有的代数运算.

这样, 代数学发生了一个革命性的变化：从研究代数方程的求根这一经典课题解脱出来, 变成研究一个一般的集合(其元素可以完全抽象, 没有具体内容)，在其中存在一种或若干种代数运算(这种运算不同于数的四则运算, 甚至可以是抽象定义的)，同时要求这些运算要满足一定的运算法则.

Outline

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，则 B 成立
- 如果 B 成立，则 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).

第一数学归纳法

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

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

证明对于任意自然数 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 $=1(1+1)/2=1$. 所以这个公式在 $n=1$ 时成立.
- 我们假设 $n=m$ 时公式成立，即
$$1+2+\cdots+m=\frac{m(m+1)}{2}.$$
- 在上式等号两边分别加上 $m+1$ 得到
$$1+2+\cdots+m+(m+1)=\frac{m(m+1)}{2}+(m+1)=\frac{(m+1)(m+2)}{2}.$$
这就是 $n=m+1$ 时的等式.
因此，对于任意自然数等式都成立. ∎

例 2

对于任意自然数 n 证明 3^n-1 是 2 的倍数.

证明

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

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

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

高中的时候，定义了

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

然后形如：

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

这样的数就是复数。全体复数的集合记为

$$\mathbb{C} = \{a + bi \,|\, a, b \text{ 取所有实数}\}$$

有了复数之后，开方运算就不再局限于大于 0 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

$$(a+bi)+(c+di):=(a+c)+(b+d)i$$

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

$$(a+bi)-(c+di)=(a-c)+(b-d)i$$

- 定义 $\mathbb{C}$ 内的乘法

$$(a+bi)(c+di)=(ac-bd)+(ad+bc)i$$

- 定义 $a+bi$ 的倒数或逆

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

- $\mathbb{C}$ 内的除法是 (设 $c+di\neq 0$)

$$\frac{a+bi}{c+di}=(a+bi)\frac{1}{c+di}=(a+bi)\frac{c-di}{c^2+d^2}$$

复数的表示：实部、虚部、共轭、模

定义

对于复数 $z = a + bi$, 其中 a, b 是实数.

- a 称为 z 的**实部**, 记为 Rez
- b 称为 z 的**虚部**, 记为 Imz
- 复数 $z = a + bi$ 的**共轭** $\bar{z} := a - bi$
- $|z| = \sqrt{a^2 + b^2}$ 称为 $a + bi$ 的**模**或绝对值。

性质

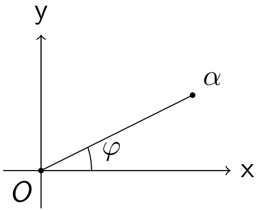
- $z\bar{z} = (a + bi)(a - bi) = a^2 + b^2.$
- $z + \bar{z} = (a + bi) + (a - bi) = 2a.$
- $z - \bar{z} = (a + bi) - (a - bi) = 2bi.$

将 Ox 轴正方向沿反时针方向旋转到直线 OA 的旋转角 φ 称为复数 $\alpha = a + bi$ 的辐角. 辐角的值不是唯一确定的, 可以加上 2π 的任意整数倍.

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

$$\alpha = a + bi = |\alpha|(\cos\varphi + i\sin\varphi)$$

上式称为复数的三角表示.



如果又有复数

$$\beta = c + di = |\beta|(\cos\psi + \mathrm{isin}\,\psi)$$

那么

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

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

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

上式表示的复数模为 1，称为复数的欧拉公式.
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 $e, i, \pi, -1$ 连起来.

给定正整数 n, 考查下列 n 个复数

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

其中 $k = 0, 1, 2, \cdots, n-1$. 这 n 个复数就是以坐标原点 O 为中心的单位圆的内接正 n 边形的 n 个顶点. 于是

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

因此，上面 n 个复数 $e^{\frac{2k\pi}{n}i} = \cos\frac{2k\pi}{n} +$ isin $\frac{2k\pi}{n}$ 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, 它们是很有用的工具，在许多问题中都会用到.

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 $a, b, b \neq 0$, 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 $b \mid a$ 时，b 是 a 与 b 的最大公因数.
- 特别地当 $a = 0$ 时，b 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 (亦称互质).

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
$$ua + vb = 1$$
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.

定义

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**.

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 $p|a \cdot b$ 则 $p|a$ 或 $p|b$.
3. 如果一个 >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

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

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 (1), 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

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