

极简数学·中学篇

第四册

大青花鱼

目录

第一章 四边形	5
1.1 平行四边形	5
1.2 特殊平行四边形	7
1.3 梯形	9
1.4 筝形	10
第二章 数的分解	13
2.1 初识素数	13
2.2 算数基本定理	16
第三章 因式分解	21
3.1 一元整式	21
3.2 试根法	22
3.3 一般整式的分解	24
第四章 二次方根和二次根式	27

4.1	二次方根的化简	27
4.2	二次域	29
第五章	一元二次方程	31
5.1	解一元二次方程	32
5.2	根和系数的关系	32
第六章	多变量的问题	33
6.1	二元一次方程组	34
6.2	消元法	34
6.3	多元一次不等式组举例	37
6.4	二元一次不等式组	38
第七章	函数初步 (下)	39
7.1	反比例函数	39
7.2	二次函数	39
7.3	反函数	39

第一章 四边形

四边形是生活中常见的形状。下面来看几种常见的四边形。

1.1 平行四边形

平行四边形是一种重要的四边形。它由两组平行线确定。

设直线 $l_1 \parallel l_2$, $m_1 \parallel m_2$, 且 l_1 和 m_1 有交点 A , 那么 l_2 和 m_1 、 l_2 和 m_2 、 l_1 和 m_2 各有交点 B 、 C 、 D , 四边形 $ABCD$ 叫做平行四边形, 记作 $\square ABCD$ 。

设有四边形 $ABCD$, 我们说 AB 、 CD 互为对边, BC 、 DA 互为对边; $\angle ABC$ 和 $\angle CDA$ 互为对角, $\angle BCD$ 和 $\angle DAB$ 互为对角。线段 AC 和 BD 称为四边形的对角线。

定理 1.1.1. 平行四边形对边平行且等长, 对角相等。

证明: 给定 $\square ABCD$, 按定义可知对边平行。

接着证明 $\square ABCD$ 的对角相等。

$\angle ABC$ 和 $\angle DAB$ 是同旁内角, 所以和为平角。类似地, $\angle ABC$ 和 $\angle BCD$ 是同旁内角, 所以和为平角。于是, $\angle DAB = \angle BCD$ 。同理, $\angle ABC$ 和



$\angle DAB$ 是同旁内角，所以和为平角。类似地， $\angle CDA$ 和 $\angle DAB$ 是同旁内角，所以和为平角。于是， $\angle ABC = \angle CDA$ 。

最后证明 $\square ABCD$ 的对边等长。

连接对角线 AC 。 $AB \parallel CD$ ，所以内错角 $\angle CAB = \angle ACD$ ；同理， $BC \parallel DA$ ，所以内错角 $\angle BCA = \angle DAC$ 。另外 $|AC| = |AC|$ 。所以，根据“角边角”， $\triangle ABC \simeq \triangle CDA$ 。因此， $|AB| = |CD|$ ， $|BC| = |DA|$ 。□

从证明中可以看出，平行四边形和三角形有密切的关系。把平行四边形沿对角线“裁开”，就得到一对同角全等的三角形。一般来说，任何四边形沿对角线裁开，都会得到两个三角形。因此，**四边形的内角和是三角形内角和的两倍**，即两个平角或一个周角（ 360° ）。

除了对边分别平行，还有什么办法，判断一个四边形是不是平行四边形呢？我们可以从这对全等三角形入手。以上证明中用到了“角边角”，是否可以换成“边角边”或“边边边”呢？

定理 1.1.2. 对边等长的四边形是平行四边形。

证明： 设四边形 $ABCD$ 中 $|AB| = |CD|$ ， $|BC| = |DA|$ 。连接 AC ，根据“边边边”， $\triangle ABC \simeq \triangle CDA$ ，因此， $\angle CAB = \angle ACD$ ，于是 $AB \parallel CD$ 。同理，由于 $\angle BCA = \angle DAC$ ， $BC \parallel DA$ 。于是四边形 $ABCD$ 是平行四边形。□

定理 1.1.3. 一对边平行且等长的四边形是平行四边形。

证明： 设四边形 $ABCD$ 中 $AB \parallel CD$ 且 $|AB| = |CD|$ 。连接 AC 。 $|AC| = |AC|$ 。由于 $AB \parallel CD$ ，内错角 $\angle CAB = \angle ACD$ 。根据“边角边”， $\triangle ABC \simeq \triangle CDA$ ，因此，由于 $\angle BCA = \angle DAC$ ， $BC \parallel DA$ 。于是四边形 $ABCD$ 是平行四边形。□

定理 1.1.4. 对角相等的四边形是平行四边形。

证明： 设四边形 $ABCD$ 中 $\angle ABC = \angle CDA$, $\angle BCD = \angle DAB$ 。四边形的内角和是两个平角，所以同旁内角 $\angle ABC$ 和 $\angle BCD$ 满足 $\angle ABC + \angle BCD = 180^\circ$ ，这说明 $AB \parallel CD$ 。同理，同旁内角 $\angle ABC$ 和 $\angle DAB$ 满足 $\angle ABC + \angle DAB = 180^\circ$ ，因此 $BC \parallel DA$ 。 \square

思考 1.1.1. 一对边等长，一对角相等的四边形，是否是平行四边形？

给定 $\square ABCD$ ，设对角线 AC 和 BD 的交点为 G ，我们把 G 叫做平行四边形的**中心**。可以用“角边角”证明： $\triangle ABG \simeq \triangle CDG$, $\triangle BCG \simeq \triangle DAG$ 。因此， $|AG| = |CG|$ 、 $|BG| = |DG|$ 。 G 同时是两条对角线的中点。换句话说，**平行四边形的两条对角线相互平分**。用对称的说法， A 和 C 关于 G 对称， B 和 D 关于 G 对称。

在直角坐标系中，如果 A 的坐标是 (x_A, y_A) ， B 的坐标是 (x_B, y_B) ， C 的坐标是 (x_C, y_C) ， D 的坐标是 (x_D, y_D) ，那么 G 的坐标 (x_G, y_G) 满足：

$$x_A + x_C = 2x_G = x_B + x_D, \quad y_A + y_C = 2y_G = y_B + y_D.$$

平行四边形还可以用来定义**平移**。平移是对平面上点和更复杂图形的操作。平移可以用两个点 A, B 定义。我们把 A 叫做起点，把 B 叫做终点。对平面上任一点 D ，作平行四边形 $ABCD$ ，那么 C 就是 D 平移后得到的点。用坐标来表示的话，平移可以定义为这样的函数：

$$(x_D, y_D) \mapsto (x_A + x_B - x_D, y_A + y_B - y_D)$$

习题 1.1.1. 证明：

1. 对角线相互平分的四边形是平行四边形。

1.2 特殊平行四边形

平行四边形是对边平行、对角相等的四边形。下面我们来看几种特殊的平行四边形。

如果四边形四边等长，就说它是**菱形**。菱形肯定是平行四边形。由于平行四边形对边等长，所以也可以这样判定菱形：

定理 1.2.1. 邻边等长的平行四边形是菱形。

把菱形沿对角线“裁开”，得到的一对三角形都是等腰三角形。由于对角线平分，菱形的中心是等腰三角形底边中点，对角线也是中线。而等腰三角形三线合一，中线就是高线。所以菱形的对角线不仅相互平分，而且相互垂直。

反过来，如果四边形的对角线相互平分，而且相互垂直，那么它是菱形。菱形的两条对角线把它分为四个全等的直角三角形。

如果四边形四角相等，就说它是**矩形或长方形**。由于四边形内角和是周角，平行四边形对角相等，所以也可以这样判定矩形：

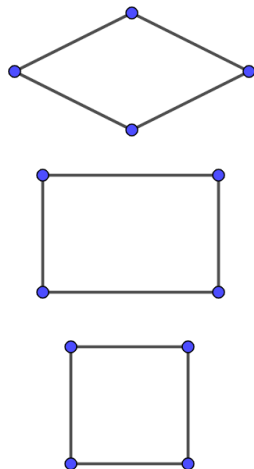
定理 1.2.2. 有一个角是直角的平行四边形是矩形。

把矩形 $ABCD$ 沿对角线 AC “裁开”，得到 $\triangle ABC$ 和 $\triangle CDA$ ，由于 $\angle ABC$ 和 $\angle CDA$ 都是直角， $\triangle ABC$ 和 $\triangle CDA$ 是直角三角形。根据勾股定理。 $|AC|^2 = |AB|^2 + |BC|^2$ 。另一方面，把矩形 $ABCD$ 沿对角线 BD “裁开”，通过类似推理可以得到： $|BD|^2 = |AB|^2 + |AD|^2$ 。而 $|BC| = |AD|$ ，所以 $|AC| = |BD|$ 。即：

定理 1.2.3. 矩形的对角线相互平分，而且等长。

反过来，如果四边形的对角线相互平分而且等长，那么它是矩形。矩形的两条把它分为两对全等的等腰三角形。

如果一个四边形既是菱形，又是矩形，就称它为**正方形**。正方形是我们很熟悉的图形。正方形的四边等长，四个内角都是直角。它的对角线长度是



边长的 $\sqrt{2}$ 倍。把正方形沿对角线“裁开”，得到一对等腰直角三角形。正方形的两条对角线把它分为四个更小而全等的等腰直角三角形。

1.3 梯形

除了平行四边形，还有其他类型的四边形。

如果四边形有一对边平行，就说它是**梯形**。如果梯形另一对边也平行，就是平行四边形。我们已经研究过平行四边形了，所以，一般说梯形时，都指非平行四边形的梯形。

研究相似三角形的时候，我们已经接触过梯形。如右图，大的三角形里去掉小的三角形，就是梯形。把梯形补全为一对相似三角形，是常见的思考方式。



按照这个说法，梯形平行的一对边长度不等。我们称它们为**上底**和**下底**。一般会把较短的一边称为上底，较长的称为下底。另外两条边一般称为梯形的**腰**。两腰等长的梯形，称为**等腰梯形**。等腰梯形对应一对相似的等腰三角形。

设梯形 $ABCD$ 中 $BC \parallel AD$ ，那么同旁内角 $\angle ABC + \angle DAB = 180^\circ$ ， $\angle BCD + \angle CDA = 180^\circ$ 。如果其中一个角是直角，这样的梯形叫作**直角梯形**。直角梯形对应一对相似的直角三角形。

梯形两腰的中点连线，称为梯形的**中位线**。

定理 1.3.1. 梯形中位线长度是两底长度之和的一半。

证明： 设梯形 $ABCD$ 中 $BC \parallel AD$, M 是边 AB 的中点, N 是边 CD 的中点, 直线 AB 、 CD 交于点 O 。由于 $BC \parallel AD$, $\triangle OBC \sim \triangle OAD$ 。因此:

$$\frac{|OB|}{|OA|} = \frac{|OC|}{|OD|} = \frac{|BC|}{|AD|} = k.$$

其中 k 是比例系数, 即:

$$|OB| = k|OA|, \quad |OC| = k|OD|.$$

于是

$$|OM| = |OB| + \frac{|AB|}{2} = \frac{|OA| + |OB|}{2} = \frac{k+1}{2} \cdot |OA|.$$

同理,

$$|ON| = |OC| + \frac{|CD|}{2} = \frac{k+1}{2} \cdot |OD|.$$

这说明

$$\frac{|OM|}{|OA|} = \frac{|ON|}{|OD|} = \frac{k+1}{2}.$$

而 $\angle MON = \angle AOD$, 所以 $\triangle OAD \sim \triangle OMN$ 。于是中位线 MN 的长度为

$$|MN| = |AD| \cdot \frac{|OM|}{|OA|} = \frac{k+1}{2} \cdot |AD|.$$

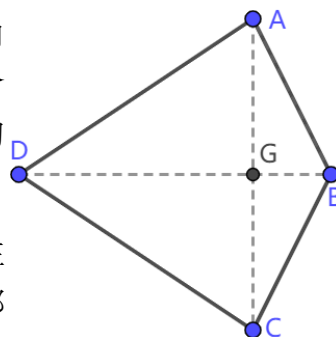
将 $k = \frac{|BC|}{|AD|}$ 代入, 就得到

$$|MN| = \frac{|BC| + |AD|}{2}.$$

□

1.4 筝形

平行四边形可以“裁成”两个同角全等的三角形。或者说，一对同角全等的三角形可以拼出一个平行四边形。那么，一对反角全等的三角形拼出的图形是什么呢？



这个图形叫作**筝形**。我们对筝形并不陌生，在证明“角边角”的时候已经见过。四边形的两对邻边分别等长，就叫作筝形。

如果筝形的对边也等长，就成了菱形。所以，一般说筝形时，都指非菱形的筝形。

筝形的最大特点，就是一条对角线是另一条的垂直平分线。我们把它叫作**脊线**，把另一条（被它平分的）对角线叫作**肩线**。我们已经证明过，脊线和肩线相互垂直。它们把筝形分为两对全等直角三角形。

直角坐标系中，把 $(0,0)$ 、 $(0,a)$ 、 (a,a) 、 $(a,0)$ 四点依次连起来，就得到一个边长为 a 的正方形。如果把 $(0,0)$ 、 $(0,b)$ 、 (a,b) 、 $(a,0)$ 四点依次连起来，就得到一个长宽为 a 和 b 的矩形。如果把 $(-a,0)$ 、 $(0,b)$ 、 $(a,0)$ 、 $(0,-b)$ 四点依次连起来，就得到一个菱形。如果把 $(0,0)$ 、 (a,b) 、 $(a+u,b+v)$ 、 (u,v) 四点依次连起来，就得到一个平行四边形。

把原点 $(0,0)$ 作为起点，选 $(0,a)$ 作为终点，把 $(0,0)$ 、 $(0,a)$ 、 (a,a) 、 $(a,0)$ 连成的正方形平移，可以得到一个新的正方形，它是 $(0,a)$ 、 $(0,2a)$ 、 $(a,2a)$ 、 (a,a) 连成的正方形。

从一个正方形出发，通过平移，能否填满整个平面，不留空隙也不互相重叠？从一个矩形、菱形、平行四边形出发，通过平移，能否填满整个平面，不留空隙也不互相重叠？

如果从一个图形出发，用和它全等的图形可以填满整个平面，不留空隙也不互相重叠，就说它是**密铺图形**，可以密铺平面。正方形、矩形、菱形、平行四边形、等腰梯形、直角梯形、筝形，哪些是密铺图形？

如果一个图形关于某条直线的轴对称图形是它自己，就说它是**轴对称图形**，该直线是它的对称轴。同样，如果一个图形关于某点的中心对称图形是它自己，就说它是**中心对称图形**，该点是它的对称中心。正方形、矩形、菱形、平行四边形、等腰梯形、直角梯形、筝形，哪些是轴对称图形，哪些是中心对称图形？它们分别有哪些对称轴和对称中心？

第二章 数的分解

自然数是我们最早认识的数。我们已经熟悉了自然数的四则运算，并且学习了因数和倍数。了解一个数的因数，无论对于理论研究，还是在实际生活中，都很有用处。

2.1 初识素数

我们已经学习过因数的概念。我们把因数只有自己和 1 的正整数叫做**素数**，除了 1 和自己还有别的因数的正整数叫做**合数**。约定 1 既不是素数也不是合数。

举例来说，2、3、5、7 是素数，而 4、6、8 是合数。偶素数只有一个：2，其余素数都是奇数。

定理 2.1.1. 设 p 是素数。任何正整数要么是 p 的倍数，要么与 p 互素。

证明： 设 n 是正整数。记 n 和 p 的最大公因数为 d 。 d 是 p 的因数。因此按 p 的定义，要么 $d = p$ ，要么 $d = 1$ 。如果 $d = p$ ，那么 n 是 p 的倍数。如果 $d = 1$ ，那么 n 与 p 互素。 \square

素数与合数有什么关系呢？

定理 2.1.2. 合数总有素因数。

证明： 按照定义，合数总有真因数。给定合数 n ，它的真因数大于 1、小于 n ，至少有一个，至多有 $n-2$ 个。其中总有一个最小的真因数，我们把它记为 p 。

p 的因数也是 n 的因数，所以要么是 1，要么大于等于 p 。也就是说， p 没有真因数。所以 p 是素数。 \square

定理 2.1.3. 每个大于 1 的整数都可以表示成素数或其乘积。

证明： 使用归纳法。命题 $P(n)$ ：整数 n 可以表示成素数或其乘积。下面证明 P 对每个大于 1 的整数成立。

$n = 2$ 时，由于 $2 = 2$ ， $P(2)$ 成立。

假设对某个大于 1 的整数 n ， $P(2), \dots, P(n)$ 都成立，下面证明 $P(n+1)$ 也成立。

如果 $n+1$ 是素数，那么 $n+1 = n+1$ 就是素数，于是 $P(n+1)$ 成立。

如果 $n+1$ 是合数，那么它至少有一个素因数 p 。设 $n+1 = mp$ ， $m \in \mathbb{Z}^+$ ，由于 $1 < p < n+1$ ，所以 $1 < m < n+1$ 。根据假设， $P(m)$ 成立，也就是说， m 可以表示成素数或其乘积：

$$m = p_1 p_2 \cdots p_k, \quad l \in \mathbb{Z}^+$$

于是， $n+1 = mp = p p_1 p_2 \cdots p_k$ 也是素数的乘积。于是 $P(n+1)$ 成立。

综上所述， $P(n)$ 对每个大于 1 的整数成立。 \square

我们把这种表示正整数的方式称为**素因数分解**。如果把自然数比作一座座房屋，那么素数就是砖瓦，构建起一个个合数。

素数与合数，谁比较多呢？一位数中，有 4 个素数，4 个合数；二位数中，有 21 个素数，69 个合数；三位数中，有 143 个素数，757 个合数；四位数中有 1061 个素数，7939 个合数。

越大的素数，越是罕见。

会不会从某个数开始，所有比它大的都是合数？也许，素数只有有限个？我们有这样一个定理：

定理 2.1.4. 素数的个数是无穷的。

证明： 使用反证法证明。反设素数的个数不是无穷的，即只有有限多个素数。把素数的个数记为 N ，把它们从小到大分别记为 p_1, p_2, \dots, p_N 。

考察这样的正整数：

$$m = p_1 p_2 \cdots p_N + 1.$$

m 与所有素数互素。所以， m 的因数要么是 1，要么是它自己，要么是某个与 p_1, p_2, \dots, p_N 都不一样的数。这就说明，要么 m 自己是素数，要么它的因数中有和 p_1, p_2, \dots, p_N 都不一样的素数。这就和“素数一共有 N 个”矛盾了。

因此，原命题的否定“素数的个数不是无穷的”是假的，原命题成立。 \square

素数作为“砖瓦”的性质，还体现在以下定理中：

定理 2.1.5. 存因定理 如果素数 p 整除两个自然数 a 和 b 的乘积： $p|ab$ ，那么 p 整除 a 或 p 整除 b 。

证明： 给定符合条件的素数 p 和自然数 a, b 。如果 p 整除 a ，那么命题得证。

如果 p 不整除 a ，那么由于两者的最大公因数是 p 的因数，因此只能是 1。两者互素。根据倍和析因定理，存在整数 m, n 使得

$$mp + na = 1.$$

两边乘以 b ，就得到：

$$mp + nab = b.$$

根据已知条件，存在整数 k 使得 $ab = kp$ ，于是

$$b = mp + nkp = (m + nk)p,$$

即 p 整除 b 。 □

存因定理告诉我们，如果某个正整数 n 有素因数 p ，把 n “拆成” 两个数的乘积，那么总有一个有素因数 p 。反复运用存因定理，我们可以把这个结论加强：无论把 n “拆成” 几个数的乘积，总有一个有素因数 p 。这反映了素数作为自然数中的“砖瓦”的性质。

习题 2.1.1. 证明：

1. 两个素数要么相等，要么互素。
2. 如果素数 p 整除完全平方数 n ，那么 p^2 也整除 n 。
3. 设 p, q 是素数， i, j 是正整数，那么要么 p^i 和 q^j 互素，要么 p^i 整除 q^j ，要么 q^j 整除 p^i 。
4. 对任何正整数 n ，都存在 n 个连续合数 $a, a+1, \dots, a+n-1$ 。

2.2 算数基本定理

从存因定理出发，可以得到一个很重要的结论：

定理 2.2.1. 算术基本定理 如果不考虑素因数的排列顺序，素因数分解的方式是唯一的。

证明： 如果某个大于 1 的整数 n 有两种素因数分解。把每种分解的素因数从小到大排列：

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l, \quad k, l \in \mathbb{Z}^+.$$

我们要证明这两种分解是一样的。

考虑 p_1 ， p_1 整除 $n = q_1 q_2 \cdots q_l$ 。根据存因定理，存在某个 j 使得 p_1 整除 q_j 。 q_j 也是素数，所以 p_1 不可能是它的真因数。于是 $p_1 = q_j \geq q_1$ 。

考虑 q_1 ，按照相同的推理，存在某个 i 使得 q_1 整除 p_i 。于是 $q_1 = p_i \geq p_1$ 。

因此, $p_1 = q_1$ 。

我们把 n 除以 p_1 , 得到正整数 n_1 。如果 $n_1 = 1$, 那么我们有 $n_1 = p_1$, 分解方式是唯一的。如果 $n_1 = p_2 \cdots p_k = q_2 \cdots q_l > 1$, 我们可以再次运用以上的推理, 得到: $p_2 = q_2$ 。

以此类推, 经过有限步后, 我们可以得到: $k = l$, 且

$$p_1 = q_1, p_2 = q_2, \cdots, p_k = q_k.$$

也就是说, n 的素因数分解只有一种方式。 \square

这个结论非常重要, 我们把它称为算术基本定理。算术基本定理告诉我们, 不考虑排列顺序的话, 每个大于 1 的正整数都可以用唯一的方式写成素数或其乘积。这种唯一的方式可以看作每个正整数的“身份证”。为了方便讨论, 素因数分解中, 一般素因数从小到大排列, 并用乘方的形式合并相同的素因数。比如, 252 的素因数分解写成;

$$252 = 2^2 \cdot 3^2 \cdot 7^1.$$

这种写法称为数的**标准分解**。以上就是 252 的标准分解。有时候, 为了便于讨论, 我们会把不是 n 的因数的素数也写进分解表达式里, 用它的 0 次方“占位”。比如 210 就可以写成:

$$252 = 2^2 \cdot 3^2 \cdot 5^0 \cdot 7^1.$$

这样的写法, 在规定了涉及的素数集合后, 仍然是唯一的。

习题 2.2.1. 写出以下数的标准分解:

1. 256, 243, 125.
2. 60, 780, 1296.
3. 1001, 5929, 8801.

把正整数 n 分解, 得到: $n = p_1^{u_1} p_2^{u_2} \cdots p_k^{u_k}$ 。我们把 u_i 称为 p_i 在 n 中的重数。它是让 p_i^i 整除 n 的最大自然数 i 。

定理 2.2.2. 如果 n 整除 m , 那么任何素数在 n 中的重数小于等于它在 m 中的重数。

证明： 设素数 p 在 n 和 m 中的重数分别是 u 和 v 。于是 p^u 整除 n ，因而整除 m 。另一方面， v 是让 p^i 整除 m 的最大自然数 i 。所以， $u \leq v$ 。 \square

上面的结论也可以换个方式说成：如果 n 是 m 的因数，那么任何素数在 n 中的重数小于等于它在 m 中的重数；如果 n 是 m 的倍数，那么任何素数在 n 中的重数大于等于它在 m 中的重数。

定理 2.2.3. 正整数 n, m 的乘积，等于它们的最大公因数和最小公倍数的乘积。

证明： 设 n, m 的最大公因数是 d ，最小公倍数是 q ，下面证明 $nm = dq$ 。把 n, m, d, q 分解，设涉及的素数为 p_1, p_2, \dots, p_k 。把四个数分别记为：

$$\begin{aligned} n &= p_1^{u_1} p_2^{u_2} \cdots p_k^{u_k}, & m &= p_1^{v_1} p_2^{v_2} \cdots p_k^{v_k}, \\ d &= p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}, & q &= p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}. \end{aligned}$$

d 既是 n 的因数也是 m 的因数，所以对每个素因数 p_i ，它在 d 中的重数 s_i 都小于等于 u_i 和 v_i 。同时，由于 d 是最大公因数，所以 s_i 是 u_i 和 v_i 中较小的数。

q 既是 n 的倍数也是 m 的倍数，所以对每个素因数 p_i ，它在 q 中的重数 t_i 都大于等于 u_i 和 v_i 。同时，由于 q 是最小公倍数，所以 t_i 是 u_i 和 v_i 中较大的数。

因此，对每个素因数 p_i ， $s_i + t_i = u_i + v_i$ 。于是，

$$\begin{aligned} nm &= (p_1^{u_1} p_2^{u_2} \cdots p_k^{u_k}) \cdot (p_1^{v_1} p_2^{v_2} \cdots p_k^{v_k}) \\ &= p_1^{u_1+v_1} p_2^{u_2+v_2} \cdots p_k^{u_k+v_k} \\ &= p_1^{s_1+t_1} p_2^{s_2+t_2} \cdots p_k^{s_k+t_k} \\ &= (p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}) \cdot (p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}) \\ &= dq \end{aligned}$$

\square

习题 2.2.2.

1. 设 i 是素数 p 在正整数 n 中的重数。
 1. 1. 如果 p 不整除 n , 证明 $i = 0$ 。
 1. 2. 如果自然数 $j < i$, 证明: p^j 整除 n 。
 1. 3. 如果自然数 $j > i$, 证明: p^j 不整除 n 。
2. 设正整数 n, m 的最大公因数是 d , 素数 p 在 d, n, m 中的重数分别是 s, u, v 。
 2. 1. 设 v 是 u, v 中较小的数, 证明: $s \leq v$ 。
 2. 2. 假设 $s < v$, 考虑 pd , 证明 pd 是 n, m 的公因数。
 2. 3. 证明 s 等于 u, v 中较小的数。
 2. 4. 设正整数 n, m 的最小公倍数是 q , 素数 p 在 q, n, m 中的重数分别是 t, u, v , 证明: t 等于 u, v 中较大的数。

给定一个正整数, 如何将它分解呢? 这个问题一直困扰着人类。将非常大的整数分解, 是一项非常困难的任务。即便在现代, 电子计算机计算能力有极大发展, 可以轻易做到每秒百亿乃至万亿次运算, 分解大整数仍然需要非常多的时间。一些常用的密码技术, 就依赖于分解大整数非常困难这个事实。

如今, 量子计算理论不断发展。人们将希望寄于量子计算机, 认为将来使用量子计算机及相应的算法, 可以在合理时间内分解大整数。

第三章 因式分解

整式是变量和数量作加减法和乘法得到的代数式。它的性质和整数很相似。整数可以分解成因数的乘积，整式也可以分解为整式的乘积。把整式的乘积写成若干项的和，叫做整式的展开；反过来，把一个整式写成多个整式的乘积，称为整式的**因式分解**。乘积中每个整式称为原整式的**因式**。

整式的因式分解是一个非常庞大的问题。我们只从最简单的情况出发，归纳一些特殊情况下的简单方法。

3.1 一元整式

一种简单的情况是一元整式的因式分解。给定变量为 x 的一元整式 p ，合并同类项后按照次数从高到低排列，可以写成：

$$p = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0.$$

其中 a_0, a_1, \dots, a_n 都是有理数，称为 p 的系数。其中 a_n 不等于 0，而其它数可能等于 0。 $a_n x^n$ 称为 p 的**最高次项**， a_n 就是最高次项的系数， n 称为 p 的次数。比如 $n = 1$ 时， p 就是我们见过的一元一次式。 $n = 0$ 时， p 只有常数项，称为常式。为了强调 p 是关于 x 的一元式，我们也将 p 记为 $p(x)$ 。

给定一元整式 $n(x)$ 和 $m(x)$ ，如果 $n(x)$ 可以写成 $m(x)$ 和另一个一元整式 $q(x)$ 的乘积，就说 $n(x)$ 是 $m(x)$ 的**倍式**， $m(x)$ 是 $n(x)$ 的**因式**。

和整数一样，一元整式也有带余除法。整式的带余除法可以和整数除法一样，用竖式计算。比如 $8x^5 + 2x^4 - 9x^3 + 4x - 5$ 除以 $2x^2 + x - 1$ ：

$$\begin{array}{r}
 4x^3 - x^2 - 2x + \frac{1}{2} \\
 \hline
 2x^2 + x - 1 8x^5 + 2x^4 - 9x^3 \\
 - 8x^5 - 4x^4 + 4x^3 \\
 \hline
 - 2x^4 - 5x^3 \\
 2x^4 + x^3 - x^2 \\
 \hline
 - 4x^3 - x^2 + 4x \\
 4x^3 + 2x^2 - 2x \\
 \hline
 x^2 + 2x - 5 \\
 - x^2 - \frac{1}{2}x + \frac{1}{2} \\
 \hline
 \frac{3}{2}x - \frac{9}{2}
 \end{array}$$

可以看到，**被除式** $8x^5 + 2x^4 - 9x^3 + 4x - 5$ 除以**除式** $2x^2 + x - 1$ ，得到**商式** $4x^3 - x^2 - 2x + \frac{1}{2}$ 和**余式** $\frac{3}{2}x - \frac{9}{2}$ 。竖式除法中，不同次数的项就好像整数的个十百千等数位。不同的是相减的时候没有借位，而且由于系数可以是分数，所以只要剩下的式子的次数不少于除式，就可以继续相减。最后得到的余式，次数一定严格小于除式。

思考 3.1.1. 整式 $p(x)$ 除以一次式，余式是怎样的？除以常式呢？

习题 3.1.1. 计算带余除法：

1. $x^3 - 3x^2 + 2x - 5$ 除以 $x^2 + x + 2$ 。
2. $x^6 - x^5 - 4x^3 + 11x^2 - 9x + 19$ 除以 $x^3 - 2x^2 + x + 4$ 。

3.2 试根法

怎么样找到一元整式的因式呢？我们来看上面的整式除法。

不过,如果余式是常式,那么它是不是 0,就和 x 的取值无关了。一种特殊情况是:除式是一次式: $x - a$ 。它只在 x 取值为 a 的时候为 0。这时,如果被除式也是 0,那么余式肯定是 0。于是除式是被除式的因式。

定理 3.2.1. 如果 a 是一元整式 $p(x)$ 的根,那么 $x - a$ 是它的因式。

习题 3.2.1.

设有整式 $p = 6x^3 - 3x^2 + 2x - 1$:

1. 试着分解 p 。
2. 如果既约分数 $\frac{a}{b}$ 是 p 的根,证明: $|b|$ 整除 6。

设有整式 $p = x^3 - 4x^2 - x - 20$:

1. 试着分解 p 。
2. 如果既约分数 $\frac{a}{b}$ 是 p 的根,证明: $|a|$ 整除 20。

如果既约分数 $\frac{a}{b}$ 是整式 $p = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ 的根, a 和 b 应该满足什么条件?

3.3 一般整式的分解

对一般的整式来说,也有一些普遍适用的方法。

提公因式法

如果要分解的整式中有显然的公因式,那么可以将它提取出来。比如:

$$x^6 - 2x^4 + 19x^3 - 3x$$

以上这个式子中,每一项显然都有 x 作为因式。因此,可以分解为:

$$x(x^5 - 2x^3 + 19x^2 - 3).$$

提公因式法是分配律的逆应用。

公式法

如果可以注意到要分解的整式是某个公式的展开形式，那么应用公式，就可以把展开的形式还原成因式的成绩形式。比如：

$$x^4 + 4$$

这个式子可以看成两个平方的差：

$$x^4 + 4 = x^4 - 4x^2 + 4 - 4x^2 = (x^2 - 2)^2 - (2x)^2.$$

于是，使用 $a^2 - b^2 = (a + b)(a - b)$ 这个公式，就可以得到：

$$x^4 + 4 = (x^2 - 2 + 2x)(x^2 - 2 - 2x).$$

应用公式法，取决于要分解的整式是否符合某个特定公式的展开形式。

分组分解法

分组分解的思想是从提公因式法出发。如果不能发现显然的公因式，就分组考察整式的项，看看是不是有哪些项可以先提取公因式。比如：

$$ab + abc - a^2 - b^2c$$

可以先把上式的项分为两组：

$$ab + abc - a^2 - b^2c = (ab - a^2) + (abc - b^2c)$$

然后分别对每一组做因式分解：

$$ab + abc - a^2 - b^2c = (ab - a^2) + (abc - b^2c) = a(b - a) + bc(a - b)$$

然后再提取公因式 $a - b$ ：

$$ab + abc - a^2 - b^2c = a(b - a) + bc(a - b) = (a - b)(-a + bc).$$

可以看到，分组分解的关键在于：各组各自分解的结果，应该有共同的因式。比如上式分成两组，每组都分解出了 $a - b$ 这个因式。

待定系数法

如果对因式分解的结果有一定的猜测，可以先用变量代替暂时不知道的系数，写出因式乘积。展开后，通过对比各项，得到系数。比如：

$$3ab + ac - a^2 - bc - 2b^2$$

上式中，让 $a = b$ ，则式子变为：

$$3ab + ac - a^2 - bc - 2b^2 = 3b^2 + bc - b^2 - bc - 2b^2 = 0$$

所以，猜测 $a - b$ 是因式。由于式子最高次项次数是 2，猜测因式分解结果为：

$$3ab + ac - a^2 - bc - 2b^2 = (a - b)(ua + vb + wc).$$

展开后得到：

$$3ab + ac - a^2 - bc - 2b^2 = ua^2 + vb^2 + (v - u)ab + wac - wbc.$$

对比左右各项，得到 $u = -1$ 、 $v = 2$ 、 $w = 1$ 。即：

$$3ab + ac - a^2 - bc - 2b^2 = (a - b)(-a + 2b + c).$$

待定系数法建立在对因式分解结果的合理猜测上。如果猜测出现错误，后面对比各项时就会发现矛盾。

第四章 二次方根和二次根式

分式开平方得到的代数式,叫做**二次根式**。二次根式可以看成用代数式代替二次方根 \sqrt{q} 中的数量 q 得到的结果。 \sqrt{c} 、 $\sqrt{1-a+a^2}$ 、 $\sqrt{x^3-x^2-2}$ 等都是二次根式。通过二次根式,我们可以更好地理解二次方根的性质。

4.1 二次方根的化简

思考 4.1.1. 以下二次方根有什么联系?

1. $\sqrt{2}$ 、 $\sqrt{8}$ 、 $\sqrt{72}$.
2. $\sqrt{3}$ 、 $\sqrt{45}$ 、 $\sqrt{147}$.
3. $\sqrt{5}$ 、 $\sqrt{\frac{5}{4}}$ 、 $\sqrt{\frac{20}{49}}$.

如果正整数 n 有完全平方数 a^2 作为因数: $n = ma^2$, 那么

$$\sqrt{n} = \sqrt{m}\sqrt{a^2} = a\sqrt{m}.$$

用这个方法,可以把正整数 n 的二次方根 \sqrt{n} 写成一个整数 a 和一个无理数 \sqrt{m} 的乘积。其中 m 没有完全平方数作为因数,所以 \sqrt{m} 是无理数。我们把这样的形式称为 \sqrt{n} 的**最简形式**,把找到最简形式的过程称为(整数)二次方根的化简。

要化简整数的二次方根,可以先把整数分解成素因数的乘积。给定(大

于 1 的) 正整数 n , 写出它的标准分解:

$$n = p_1^{u_1} p_2^{u_2} \cdots p_k^{u_k}$$

如果某个素因数 p_i 在 n 中的指数 u_i 是偶数, 那么 $p_i^{u_i}$ 是一个完全平方数; 如果 u_i 是奇数, 那么 $p_i^{u_i-1}$ 是一个完全平方数。于是, 我们可以把 n 的素因数分为两类, 一类是指数为偶数的, 另一类是指数为奇数的。我们可以把前一类中的 $p_i^{u_i}$ 和后一类的 $p_i^{u_i-1}$ 提出来, 相乘得到一个完全平方数。剩下的就是指数为奇数的素因数的乘积。如果我们定义这样的函数:

$$\varsigma : n = p_1^{u_1} p_2^{u_2} \cdots p_k^{u_k} \mapsto p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}.$$

其中的 r_1, r_2, \cdots, r_k 分别是 u_1, u_2, \cdots, u_k 除以 2 的余数。那么 $\varsigma(n)$ 就是剩下的指数为奇数的素因数的乘积。而 $\frac{n}{\varsigma(n)}$ 是一个完全平方数。

$\varsigma(n)$ 已经没有完全平方数的因子了, 我们把它叫做 n 的**二次方余**。 n 可以写成:

$$\sqrt{n} = a\sqrt{\varsigma(n)}.$$

其中正整数 a 是 $\frac{n}{\varsigma(n)}$ 的平方根。

举例来说, 要化简 $\sqrt{2520}$, 可以先把正整数 2520 分解:

$$2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7.$$

然后提出完全平方的部分, 计算方余:

$$2520 = (2^2 \cdot 3^2) \cdot (2 \cdot 5 \cdot 7)$$

因此 $\varsigma(n) = 2 \cdot 5 \cdot 7 = 70$,

$$\sqrt{2520} = 6\sqrt{70}.$$

对一般的正有理数 r , 我们也希望将 \sqrt{r} 表示成 $a\sqrt{m}$ 的形式, 其中 a 是有理数, 而 m 是没有完全平方数因子的正整数。我们把这样的形式称为有理数二次方根的最简形式。

把 r 写成既约分数: $r = \frac{p}{q}$, 不难发现, 可以把 \sqrt{r} 写成:

$$\sqrt{r} = \sqrt{\frac{p}{q}} = \sqrt{\frac{pq}{q^2}} = \frac{\sqrt{pq}}{q}.$$

这样, 只需要把正整数 pq 的二次方根化简, 就能得到 \sqrt{r} 的最简形式。

对整式和分式来说, 它们开平方得到的二次根式也可以用类似的方式化简。

习题 4.1.1. 化简以下的二次方根:

1. $\sqrt{5480}, \sqrt{1240}, \sqrt{5760}.$
2. $\frac{2}{\sqrt{3}}, \sqrt{\frac{1744}{85}}, \sqrt{\frac{576}{132}}, \sqrt{\frac{2240}{6897}}.$
3. $\sqrt{48} - 1.8\sqrt{6} + 5\sqrt{3}, 7\sqrt{18} + 1.5\sqrt{108} + 10\sqrt{242}.$

化简以下的代数式:

1. $\sqrt{(1-a^2)(1+a)}, \sqrt{(b^3-a^3)(a-b)}.$
2. $\sqrt{\frac{1-a^4}{(1+a)^3}}, \sqrt{\frac{1-a^4}{a(a+1)}} + \sqrt{a^2+1}.$

4.2 二次域

考虑这样一个集合: $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ 。有理数集 \mathbb{Q} 是它的子集, 它是实数集 \mathbb{R} 的子集。我们把它记为 $\mathbb{Q}(\sqrt{2})$ 。

举例来说, $\mathbb{Q}(\sqrt{2})$ 的元素有: $1 + \sqrt{2}, 3 - 2\sqrt{2}, 0, 7$ 等等。

$\mathbb{Q}(\sqrt{2})$ 的元素有什么性质呢?

$1 + \sqrt{2}$ 和 $3 - 2\sqrt{2}$ 是 $\mathbb{Q}(\sqrt{2})$ 的元素, 它们的和是 $4 - \sqrt{2}$, 差是 $-2 + 3\sqrt{2}$, 乘积是 $-1 + \sqrt{2}$, 商是 $7 + 5\sqrt{2}$ 。

一般来说, 如果 x 和 y 是 $\mathbb{Q}(\sqrt{2})$ 的元素, 它们进行四则运算的结果仍然是 $\mathbb{Q}(\sqrt{2})$ 的元素。具有这种性质的数集叫做**数域**。有理数、实数都是数域, 自然数、整数、正数不是数域。 $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$ 这样的数域叫做**二次域**。

如果 n 是正整数, \sqrt{n} 在不在 $\mathbb{Q}(\sqrt{2})$ 里呢?

定理 4.2.1. $\sqrt{3}$ 不属于 $\mathbb{Q}(\sqrt{2})$ 。

证明: 用反证法。反设 $\sqrt{3}$ 属于 $\mathbb{Q}(\sqrt{2})$ 。于是存在有理数 a, b 使得

$$\sqrt{3} = a + b\sqrt{2}.$$

两边平方, 得到:

$$3 = a^2 + 2b^2 + 2ab\sqrt{2}.$$

如果 $ab \neq 0$, 那么 $\sqrt{2} = \frac{3-a^2-2b^2}{2ab}$ 是有理数。矛盾!

如果 $a = 0$, 那么 $2b^2 = 3$, 于是 $b = \frac{\sqrt{6}}{2}$ 是无理数。矛盾!

如果 $b = 0$, 那么 $a^2 = 3$, 于是 $a = \sqrt{3}$ 是无理数。矛盾!

综上所述, 原命题的否定 “ $\sqrt{3}$ 属于 $\mathbb{Q}(\sqrt{2})$ ” 是假的, 因此原命题是真的。

□

用同样的方法, 可以证明 $\sqrt{2}$ 不属于 $\mathbb{Q}(\sqrt{3})$ 。也就是说, $\mathbb{Q}(\sqrt{2})$ 不是 $\mathbb{Q}(\sqrt{3})$ 的子集, $\mathbb{Q}(\sqrt{3})$ 也不是 $\mathbb{Q}(\sqrt{2})$ 的子集。

习题 4.2.1. 想一想:

1. 对哪些正整数 n , \sqrt{n} 在 $\mathbb{Q}(\sqrt{2})$ 里?
2. $\mathbb{Q}(\sqrt{2})$ 和 $\mathbb{Q}(\sqrt{3})$ 的交集是什么集合? 是不是数域?
3. $\mathbb{Q}(\sqrt{2})$ 和 $\mathbb{Q}(\sqrt{3})$ 的并集是什么集合? 是不是数域?

第五章 一元二次方程

我们已经学习过一元一次方程。解一元一次方程可以看作找出一元一次式 $ax + b = 0$ 时变量 x 的取值。找出一元二次式 $ax^2 + bx + c = 0$ 时 x 的取值，叫做解一元二次方程。

例子 5.0.1. 根据以下问题，设未知数并列出方程：

- (1). 一座方城，南北正中有城门。北门出城直走 100 步有树，南门出城直走 100 步转西，走 1200 步后恰能望到。问方城长度是多少？
- (2). 氢气和碘蒸气产生化学反应： $H_2 + I_2 = 2HI$ 。50 摄氏度时，正反应的平衡常数 $k_c = 5.25$ 。现在将 1 摩尔氢气和 2 摩尔碘蒸气放置于 1 升的容器中，将温度调节到 50 摄氏度。反应达到平衡时，有多少摩尔的 HI 产生？

解答.

(1) 解：设方城长 x 步，北门位置为 M 点，外树的位置为 A 点，南门外转向的位置为 B 点，西行恰好望见树的位置为 C 点，城西北角为 N 点。直角三角形 AMN 和 ABC 相似。因此：

$$\frac{|AM|}{|MN|} = \frac{|AB|}{|BC|}$$

根据已知条件， $|AM| = 100$ ， $|MN| = 0.5x$ ， $|AB| = x + 200$ ， $|BC| = 1200$ 。于是可以列出方程：

$$\frac{100}{0.5x} = \frac{x + 200}{1200},$$

即:

$$\begin{aligned}0.5x(x + 200) &= 100 \cdot 1200 \\x^2 + 200x - 240000 &= 0\end{aligned}$$

(2) 解: 设平衡时产生了 x 摩尔的 HI 。根据反应方程式, 这时 H_2 和 I_2 分别消耗了 $0.5x$ 摩尔。因此平衡时三者浓度分别为 $1 - 0.5x$ 摩尔/升、 $2 - 0.5x$ 摩尔/升和 x 摩尔/升。根据条件, 反应平衡常数为 5.25, 即浓度比:

$$\frac{(1 - 0.5x)(2 - 0.5x)}{x^2} = 5.25,$$

也即:

$$\begin{aligned}5.25x^2 &= (1 - 0.5x)(2 - 0.5x) \\10x^2 + 3x - 4 &= 0\end{aligned}$$

5.1 解一元二次方程

5.2 根和系数的关系

第六章 函数初步（下）

6.1 反比例函数

6.2 二次函数

6.3 反函数

第七章 多变量不等式

7.1 二元一次不等式组

7.2 一次方程与不等式组