



# 数学书籍汇总

## 读书笔记

作者：虞朝阳

组织：西北工业大学

更新：February 16, 2020

版本：1.00

$$e^{i\pi} + 1 = 0$$

*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。

# 目录

<b>Preface</b>	<b>1</b>
<b>I 代数</b>	<b>1</b>
1 近世代数概论	2
1.1 整数	2
1.1.1 交换环, 整环	2
1.1.2 交换环的基本性质	3
1.1.3 有序整环的性质	5
1.1.4 良序原则	7
1.1.5 数学归纳法, 指数定律	8
1.1.6 可除性	9
1.1.7 欧几里得算法	10
1.1.8 算术基本定理	13
1.1.9 同余式	13
2 基础代数	15
3 代数	16
<b>II 分析</b>	<b>17</b>
4 数学分析	18
5 高等微积分:微分形式导引	19

# 第 I 部分 I

## 代数

# 第 1 章 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：S.麦克莱恩 (1979)。

## 1.1 整数

### 1.1.1 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:

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

## 1.1.2 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 $a + b \in S, ab \in S$ 。

## 1.1.3 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：

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

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 $1, 2, 3, \dots$ 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德绝对值的定律:

$$|a + b| \leq |a| + |b|; \quad |ab| = |a||b|. \quad (1.1)$$

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。

### 1.1.4 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。

### 1.1.5 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。

$$a(b_1 + b_2 + \cdots + b_n) = ab_1 + ab_2 + \cdots + ab_n. \quad (1.2)$$

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:

$$b_1 + \cdots + b_k + b_{k+1} = (b_1 + \cdots + b_k) + b_{k+1}. \quad (1.3)$$

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1.9, 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:

$$a^1 = a, a^{n+1} = a^n a. \quad (\forall a \in R) \quad (1.4)$$

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：

$$a^m a^n = a^{m+n}, \quad (1.5)$$

$$(a^m)^n = a^{mn}, \quad (ab)^m = a^m b^m. \quad (1.6)$$

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

$$\begin{aligned} (x+y)^n &= x^n + nx^{n-1}y + \cdots + \binom{n}{k}x^{n-k}y^k + \cdots + y^n \\ &= \sum_{k=0}^n \binom{n}{k}x^{n-k}y^k. \end{aligned} \quad (1.7)$$

和

$$k!(n-k)! \binom{n}{k} = n! \quad (1.8)$$

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。

### 1.1.6 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 $\pm 1$

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 $\pm 1$ , 并且 $p$ 只能被 $\pm 1$ 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。

## 1.1.7 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

$$a = bq + r, \quad 0 \leq r < b. \quad (1.9)$$

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1.9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

$$(a, b) = sa + tb. \quad (1.10) \heartsuit$$

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。 \heartsuit

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：

$$a = bq_1 + r_1, \quad 0 \leq r_1 < b, \quad (1.11)$$

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：

$$\begin{aligned} b &= r_1q_2 + r_2, & 0 < r_2 < r_1 \\ r_1 &= r_2q_3 + r_3, & 0 < r_3 < r_2 \\ &\dots & \dots \\ r_{n-2} &= r_{n-1}q_n + r_n, & 0 < r_n < r_{n-1} \\ r_{n-1} &= r_nq_{n+1} \end{aligned} \quad (1.12)$$

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 $ac|m$ 。



## 1.1.8 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 $(\pm 1)$ 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:

$$a = \pm p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \quad (1 < p_1 < p_2 < \cdots < p_k). \quad (1.13)$$

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。

## 1.1.9 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 $m|(a - b)$ 。



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

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



## 第 2 章 基础代数



## 第 3 章 代数



《代数》的作者是M.阿廷。

## 第 II 部分 II

### 分析

## 第 4 章 数学分析



## 第 5 章 高等微积分:微分形式导引



## 参考文献

S.麦克莱恩, G.伯克霍夫, 近世代数概论, 北京: 人民教育出版社, 1979.