

# 查考多项式

*Septsea*



# 目录

版权声明	iii
前言	v
查考多项式	1
预备知识	2
多项式的定义	36
带余除法	47
多项式的相等	53
微商	60
多项式的根	72
$\mathbb{F}$ 上的多项式	80
插值	92
广义二项系数	114
求和公式	123
再探微商	141
多项式的微分学初步	156
同人作	169
整数的一些性质	170
多项式的一些性质	197
综合除法	221
重因子	232
整系数多项式与有理系数多项式	242
整数的因子分解	260
有理系数多项式的有理根	269
有理系数多项式的因子分解	270



# 版权声明

源代码采用 **the Unlicense**:

This is free and unencumbered software released into the public domain.

Anyone is free to copy, modify, publish, use, compile, sell, or distribute this software, either in source code form or as a compiled binary, for any purpose, commercial or non-commercial, and by any means.

In jurisdictions that recognize copyright laws, the author or authors of this software dedicate any and all copyright interest in the software to the public domain. We make this dedication for the benefit of the public at large and to the detriment of our heirs and successors. We intend this dedication to be an overt act of relinquishment in perpetuity of all present and future rights to this software under copyright law.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

For more information, please refer to

[<https://unlicense.org>](https://unlicense.org)

正文采用 **CC0**:

## **No Copyright**

The person who associated a work with this deed has **dedicated** the work to the public domain by waiving all of his or her rights to the

work worldwide under copyright law, including all related and neighboring rights, to the extent allowed by law.

You can copy, modify, distribute and perform the work, even for commercial purposes, all without asking permission. See **Other Information** below.

## **Other Information**

- In no way are the patent or trademark rights of any person affected by CC0, nor are the rights that other persons may have in the work or in how the work is used, such as publicity or privacy rights.
- Unless expressly stated otherwise, the person who associated a work with this deed makes no warranties about the work, and disclaims liability for all uses of the work, to the fullest extent permitted by applicable law.
- When using or citing the work, you should not imply endorsement<sup>†</sup> by the author or the affirmer.

---

<sup>†</sup> In some jurisdictions, wrongfully implying that an author, publisher or anyone else endorses your use of a work may be unlawful.

## 前言

本文是瞎写的. 我给本文的另一个名字是 “Re: ゼロから始めるポリノミアルのイントロダクション”. 不过想了想, 算了算了. 龙鸣日语, 不好意思直接说出来.

本文用尽可能朴素的语言讨论了多项式及其部分应用.

总是可以去这儿得到本文的最新版本:

<https://gitee.com/septsea/strange-book-zero>

<https://github.com/septsea/strange-book-zero>

您可以自由地阅读、修改、再分发本文.

如果您发现本文有什么地方不对, 那么您就毫不犹豫地告诉我. 当然, 任何意见与建议也是可以的.

(记得先看看最新版本改过来没有哟. 不过就算没看最新版本也没关系啦. 我一定会处理您的消息的! 嘿嘿.)

就先说到这里.

**评注** 总算写完“预备知识”了. 我写这玩意儿花了好久好久啊. 先发布再说吧.

*June 3, 2021*

**评注** 忘记介绍域是什么东西了. 我真是笨蛋啊.

*June 3, 2021*

**评注** 前几日意识到, 我不能又写得严谨, 又指望着中学生都能读懂. 不过本文业已成形, “改”不如“重写”. 不过本文是开源的 (主要是无版权), 您可以随意重写.

*June 17, 2021*

**评注** 6月6日, 我在这里发了贴, 目的是让更多的人看到我写的 © 文. 我得到了很多意见与建议. 今日, 我写完了我想写的东西. 我维护本文就好. 我觉得超理太棒了!

*June 20, 2021*

**评注** 我总算在改错了. 感谢超理读者“没啥好叫的”指出本文的一个错误! 然后我自己发现了一堆印刷错误. 啊啦啊啦. 看多了视觉小说, 我的大脑生锈了呢. 顺便一提, 看本文看累了的时候, 不妨看看小说哦! 这里! 这里! I am sharing my copies of visual novels with my readers!

*July 29, 2021*



## 查考多项式

出于无聊, Septsea 撰写本文.

## 预备知识

读者将在本节熟悉一些记号与术语. 建议读者熟悉本节的内容后学习下节的内容.

在进入小节“集”前, 让我们先回顾命题、复数与数学归纳法吧!

**定义** 能判断真假的话是命题 (*proposition*). 正确的命题称为真命题; 错误的命题称为假命题. 当然, 命题也可以用“对”“错”形容.

**例** 根据常识, “日东升西落”是真命题. 类似地, “月自身可发光”是假命题.

“这是什么?” 不是命题, 因为它没有作出判断. 类似地, “请保持安静”也不是命题, 因为它只是一个祈使句 (*imperative sentence*). 不过, “难道中国不强?” 不但是命题, 它还是正确的, 因为这个反问 (*rhetorical question*) 作出了正确的判断.

“ $x > 3$ ”不是命题, 因为它不可判断真假. 像这种话里有未知元, 且揭秘未知元前不可知此话之真伪的话是开句 (*open sentence*).

我们会经常遇到“若  $p$ , 则  $q$ ”的命题.

**定义** 设“若  $p$ , 则  $q$ ”是真命题. 我们说,  $p$  是  $q$  的充分条件 (*sufficient condition*),  $q$  是  $p$  的必要条件 (*necessary condition*). 用符号写出来, 就是

$$p \Rightarrow q \quad \text{or} \quad q \Leftarrow p.$$

**例** “若刚下过雨, 则地面潮湿”是对的. “刚下过雨”是“充分的”: 根据常识可以知道这一点. “地面潮湿”是“必要的”: 地面不潮湿, 那么不可能刚下过雨.

**评注** 我们会遇到形如“ $\ell$  的一个必要与充分条件是  $r$ ”的命题. 换个说法, 就是“ $r$  是  $\ell$  的一个必要与充分条件”. 再分解一下, 就是“ $r$  是  $\ell$  的一个必要条件”与“ $r$  是  $\ell$  的一个充分条件”这二个命题. 根据定义, 这相当于“若  $\ell$ , 则  $r$ ”与“若  $r$ , 则  $\ell$ ”都是真命题. 也就是说,  $\ell$  跟  $r$  是等价的 (*equivalent*). 用符号写出来, 就是

$$p \Leftrightarrow q.$$

证明“ $\ell$  的一个必要与充分条件是  $r$ ”时, 我们会把它分为必要性 (*necessity*) 与充分性 (*sufficiency*) 二个部分. 证明必要性, 就是证明“ $r$  是  $\ell$  的一个必要条件”, 也就是证明“若  $\ell$ , 则  $r$ ”是对的; 换句话说, 证明左边可以推出右边. 证明充分性, 就是证明“ $r$  是  $\ell$  的一个充分条件”, 也就是证明“若  $r$ , 则  $\ell$ ”是对的; 换句话说, 证明右边可以推出左边.

命题就介绍到这里. 下面回顾复数基础.

**定义** 复数 (*complex number*) 是形如  $x + yi$  ( $x, y$  是实数) 的数.

**评注** 可将  $x + yi$  写为  $x + iy$ .

**定义** 设  $a, b, c, d$  是实数. 则

$$a + bi = c + di \iff a = c \text{ and } b = d.$$

**评注** 我们把形如  $a + 0i$  的复数写为  $a$ , 并认为  $a + 0i$  是实数. 反过来,  $a$  也可以认为是复数  $a + 0i$ .

形如  $0 + bi$  的复数可写为  $bi$ . 按照习惯,  $1i$  可写为  $i$ , 且  $-1i$  可写为  $-i$ .

**定义** 复数的加、乘法定义为

$$\begin{aligned}(a + bi) + (c + di) &= (a + c) + (b + d)i, \\ (a + bi)(c + di) &= (ac - bd) + (ad + bc)i.\end{aligned}$$

由此可见, 二个复数的和 (或积) 还是复数.

**例** 我们计算  $i$  与自己的积:

$$i \cdot i = (0 + 1i)(0 + 1i) = (0 \cdot 0 - 1 \cdot 1) + (0 \cdot 1 + 1 \cdot 0)i = -1.$$

简单地说, 就是

$$i \cdot i = i^2 = -1.$$

设  $z_1, z_2, z_3$  是任意三个复数 (不必不同). 设  $z_1 = a + bi$ .

**命题** 复数的加法适合如下运算律:

- (i) 交换律:  $z_1 + z_2 = z_2 + z_1$ ;
- (ii) 结合律:  $(z_1 + z_2) + z_3 = z_1 + (z_2 + z_3)$ ;
- (iii)  $0 + z_1 = z_1$ ;
- (iv) 存在复数  $w = (-a) + (-b)i$  使  $w + z_1 = 0$ .  
通常把适合 (iv) 的  $w$  记为  $-z_1$ , 且称之为  $z_1$  的相反数.

**评注**  $(-a) + (-b)i$  可写为  $-a - bi$ .

**定义** 复数的减法定义为

$$z_2 - z_1 = z_2 + (-z_1).$$

**命题** 复数的乘法适合如下运算律:

- (v) 交换律:  $z_1 z_2 = z_2 z_1$ ;
- (vi) 结合律:  $(z_1 z_2) z_3 = z_1 (z_2 z_3)$ ;
- (vii)  $1 z_1 = z_1$ ;
- (viii)  $(-1) z_1 = -z_1$ ;
- (ix) 若  $z_1 \neq 0$ , 则存在复数  $v = \frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i$  使  $v z_1 = 1$ .  
通常把适合 (ix) 的  $v$  记为  $z_1^{-1}$ , 且称之为  $z_1$  的倒数.

**定义** 复数的除法定义为

$$\frac{z_2}{z_1} = z_2 z_1^{-1}.$$

**命题** 复数的加法与乘法还适合分配律:

$$\begin{aligned} z_1(z_2 + z_3) &= z_1 z_2 + z_1 z_3, \\ (z_2 + z_3)z_1 &= z_2 z_1 + z_3 z_1. \end{aligned}$$

**评注**  $a, bi, c, di$  都可以看成是复数. 这样

$$\begin{aligned} (a + bi)(c + di) &= (a + bi)c + (a + bi)(di) \\ &= ac + bic + adi + bidi \\ &= ac + bci + adi + bdi^2 \\ &= (ac + bdi^2) + (ad + bc)i \\ &= (ac - bd) + (ad + bc)i. \end{aligned}$$

也就是说, 我们不必死记复数的乘法规则: 只要用运算律与  $i^2 = -1$  即可召唤它.

**定义** 设  $a, b$  是实数.  $a + bi$  的共轭 (*conjugate*) 是复数  $a - bi$ . 复数  $z_1$  的共轭可写为  $\bar{z}_1$ .

**命题** 共轭适合如下性质:

(x)  $\bar{z}_1 + z_1$  与  $i \cdot (\bar{z}_1 - z_1)$  都是实数;

(xi)  $\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$ ,  $\overline{z_1 z_2} = \bar{z}_1 \cdot \bar{z}_2$ ;

(xii)  $\overline{\bar{z}_1} = z_1$ ;

(xiii)  $\bar{z}_1 z_1$  是正数, 除非  $z_1 = 0$ .

**定义**  $|z_1| = \sqrt{\bar{z}_1 z_1}$  称为  $z_1$  的绝对值 (*absolute value*).

**命题** 绝对值适合如下性质:

$$|z_1 z_2| = |z_1| |z_2|.$$

**定义** 设  $n$  是整数. 若  $n = 0$ , 则说  $z_1^n = 1$ . 若  $n \geq 1$ , 则说  $z_1^n$  是  $n$  个  $z_1$  的积. 若  $z_1 \neq 0$ , 且  $n \leq -1$ , 则说  $z_1^n$  是  $\frac{1}{z_1^{-n}}$ .  $z_1^n$  的一个名字是  $z_1$  的  $n$  次幂 (*power*).

**命题** 设  $m, n$  是非负整数. 幂适合如下性质:

$$z_1^m z_1^n = z_1^{m+n}, \quad (z_1^m)^n = z_1^{mn}, \quad (z_1 z_2)^m = z_1^m z_2^m.$$

若  $z_1$  与  $z_2$  都不是 0, 则  $m, n$  允许取全体整数.

复数就先回顾到这里. 下面回顾数学归纳法.

**评注** 数学归纳法 (*mathematical induction*) 是一种演绎推理.

**命题** 设  $P(n)$  是跟整数  $n$  相关的命题. 设  $P(n)$  适合:

(i)  $P(n_0)$  是正确的;

(ii) 任取  $\ell \geq n_0$ , 必有“若  $P(\ell)$  是正确的, 则  $P(\ell + 1)$  是正确的”成立. 则任取不低于  $n_0$  的整数  $n$ , 必有  $P(n)$  是正确的.

**评注** 可以这么理解数学归纳法. 假设有一排竖立的砖. 如果 (i) 第一块砖倒下, 且 (ii) 前一块砖倒下可引起后一块砖倒下, 那么所有的砖都可以倒下, 是吧? 由此也可以看出, (i) (ii) 缺一不可. 第一块砖不倒, 后面的砖怎么倒下呢?<sup>†</sup> 如果前一块砖倒下时后一块砖不一定能倒下, 那么会在某块砖后开始倒不下去.

**例** 我们试着用数学归纳法证明, 对任意正整数  $n$ ,

$$P(n): \quad 0 + 1 + \cdots + (n-1) = \frac{n(n-1)}{2}.$$

既然想证明对任意正整数  $n$ ,  $P(n)$  都成立, 我们取  $n_0 = 1$ . 然后验证 (i): 左边只有 0 这一项, 右边是  $\frac{1 \cdot (1-1)}{2} = 0$ . 所以 (i) 适合.

再验证 (ii). (ii) 是说, 要由  $P(\ell)$  推出  $P(\ell+1)$ . 所以, 假设

$$0 + 1 + \cdots + (\ell-1) = \frac{\ell(\ell-1)}{2}, \quad \ell \geq n_0.$$

因为

$$\begin{aligned} 0 + 1 + \cdots + (\ell-1) + \ell &= (0 + 1 + \cdots + (\ell-1)) + \ell \\ \text{(IH)} \quad &= \frac{\ell(\ell-1)}{2} + \ell \\ &= \frac{\ell(\ell-1)}{2} + \frac{\ell \cdot 2}{2} \\ &= \frac{\ell(\ell+1)}{2} \\ &= \frac{(\ell+1)((\ell+1)-1)}{2}, \end{aligned}$$

故我们由  $P(\ell)$  推出了  $P(\ell+1)$ . 我们在哪儿用到了  $P(\ell)$  呢? 我们在标了 (IH) 的那一行用了  $P(\ell)$ . 这样的假设称为归纳假设 (*induction hypothesis*).

既然 (i) (ii) 都适合, 那么任取不低于  $n_0 = 1$  的整数  $n$ ,  $P(n)$  都对.

我们用二个具体的例说明, (i) (ii) 缺一不可.

**例** 我们“证明”, 对任意正整数  $n$ ,

$$P'(n): \quad 0 + 1 + \cdots + (n-1) = \frac{n(n-1)}{2} + 1.$$

---

<sup>†</sup>当然, 也可以从第  $n$  块砖开始倒下 ( $n > 1$ ), 但这就照顾不到第一块了.

这里,  $n_0$  自然取 1.

(i) 不适合: 显然  $n = 1$  时, 左侧是 0 而右侧是 1. 再看 (ii). 假设

$$0 + 1 + \cdots + (\ell - 1) = \frac{\ell(\ell - 1)}{2} + 1, \quad \ell \geq n_0.$$

由于

$$\begin{aligned} 0 + 1 + \cdots + (\ell - 1) + \ell &= (0 + 1 + \cdots + (\ell - 1)) + \ell \\ \text{("IH")} \quad &= \frac{\ell(\ell - 1)}{2} + 1 + \ell \\ &= \frac{\ell(\ell - 1)}{2} + \frac{\ell \cdot 2}{2} + 1 \\ &= \frac{\ell(\ell + 1)}{2} + 1 \\ &= \frac{(\ell + 1)((\ell + 1) - 1)}{2} + 1, \end{aligned}$$

故我们由  $P'(\ell)$  “推出”了  $P'(\ell + 1)$ . 我们也在 (“IH”) 处用到了 “归纳假设”. 那么  $P'(n)$  就是正确的吗? 当然不是! 前面我们知道,

$$0 + 1 + \cdots + (n - 1) = \frac{n(n - 1)}{2},$$

也就是说,  $P'(n)$  的右侧的 “+ 1” 使其错误. 当然, 一般我们很少会犯这样的错误: 毕竟, 一开始就不对的东西就不用看下去了.

**例** 不同的老婆<sup>†</sup>有着不同的发色. 但是, 我们用数学归纳法却可以 “证明”, 任意的  $n$  ( $n \geq 1$ ) 个老婆有着相同的发色! 称这个命题为  $Q(n)$ . 这里,  $n_0$  自然取 1.

(i) 当  $n = n_0 = 1$  时, 一个老婆自然只有一种发色. 这个时候, 命题是正确的!

(ii) 假设任意的  $\ell$  ( $\ell \geq n_0$ ) 个老婆有着相同的发色! 随意取  $\ell + 1$  个老婆. 根据假设, 老婆 1, 2,  $\dots$ ,  $\ell$  有着相同的发色, 且老婆 2,  $\dots$ ,  $\ell$ ,  $\ell + 1$  有着相同的发色. 这二组中都有 2,  $\dots$ ,  $\ell$  这  $\ell - 1$  个老婆, 所以老婆 1, 2,  $\dots$ ,  $\ell$ ,  $\ell + 1$  有着相同的发色!

---

<sup>†</sup>一般地, 二次元人会称动画、漫画、游戏、小说中自己喜爱的女性角色为老婆 (*waifu*). 一个二次元人可以有不止一个老婆.

根据 (i) (ii), 命题成立.

可是这对吗? 不对. 问题出在 (ii). 如果说, 任意二个老婆有着相同的发色, 那任意三个老婆也有着相同的发色. 这没问题. 可是, 由  $Q(1)$  推不出  $Q(2)$ : 老婆 1 与老婆 2 根本就不重叠呀! (ii) 要求任取  $\ell \geq n_0$ , 必有  $Q(\ell)$  推出  $Q(\ell+1)$ . 而  $\ell=1$  时, (ii) 不对, 因此不能推出  $Q(n)$  对任意正整数都对.

下面是数学归纳法的一个变体.

**命题** 设  $P(n)$  是跟整数  $n$  相关的命题. 设  $P(n)$  适合:

(i)  $P(n_0)$  是正确的;

(ii)' 任取  $\ell \geq n_0$ , 必有“若  $\ell - n_0 + 1$  个命题  $P(n_0), P(n_0+1), \dots, P(\ell)$  都是正确的, 则  $P(\ell+1)$  是正确的”成立.

则任取不低于  $n_0$  的整数  $n$ , 必有  $P(n)$  是正确的.

**评注** 可以由下面的推理看出, 上面的数学归纳法变体是正确的.

作命题  $Q(n)$  ( $n \geq n_0$ ) 为“ $n - n_0 + 1$  个命题  $P(n_0), P(n_0+1), \dots, P(n)$  都是正确的”.

(i)  $P(n_0)$  是正确的, 所以  $n_0 - n_0 + 1$  个命题  $P(n_0)$  是正确的, 也就是  $Q(n_0)$  是正确的.

(ii) 任取  $\ell \geq n_0$ . 假设  $Q(\ell)$  是正确的, 也就是假设  $\ell - n_0 + 1$  个命题  $P(n_0), P(n_0+1), \dots, P(\ell)$  都是正确的. 由 (ii)',  $P(\ell+1)$  是正确的. 所以,  $\ell+1 - n_0 + 1$  个命题  $P(n_0), P(n_0+1), \dots, P(\ell), P(\ell+1)$  都是正确的. 换句话说,  $Q(\ell+1)$  是正确的.

由数学归纳法可知, 任取不低于  $n_0$  的整数  $n$ , 必有  $Q(n)$  是正确的. 所以,  $P(n)$  是正确的.

另一方面, 若命题  $P(n)$  适合数学归纳法的条件 (ii), 则它当然适合变体的条件 (ii)'. (读者可思考: 既然  $P(\ell)$  推出  $P(\ell+1)$ , 那么给  $P(\ell)$  “加条件”  $P(n_0), P(n_0+1), \dots, P(\ell-1)$  是不是也能推出  $P(\ell+1)$ ? 如果读者仍未理解, 作者举个形象的例: 若  $a=b$ , 则  $b=a$ .  $a=b$  已经能推出  $b=a$ . “若  $a=b$  且  $a^2=b^2, a^3=b^3$ , 则  $b=a$ ” 是不是也是对的? 当然. 为什么? 因为我们知道, 就算没有  $a^2=b^2, a^3=b^3, b=a$  也是对的——这是由  $a=b$  推出的, 跟其他的条件无关.) 所以, 若数学归纳法的变体是正确的, 则数学归纳法也是正确的. 换句话说, 数学归纳法与其变体是等价的.



以后,“数学归纳法”既可以指老的数学归纳法 (由  $P(\ell)$  推  $P(\ell + 1)$ ), 也可以指变体 (由  $P(n_0), P(n_0 + 1), \dots, P(\ell)$  推  $P(\ell + 1)$ ).

知识就回顾到这里. 开始进入集的世界吧!

## 集

**定义** 集 (*set*) 是具有某种特定性质的对象汇集而成的一个整体, 其对象称为元 (*element*).

**定义** 无元的集是空集 (*empty set*).

**评注** 一般用小写字母表示元, 大写字母表示集.

**定义** 一般地, 若集  $A$  由元  $a, b, c, \dots$  作成, 我们写

$$A = \{a, b, c, \dots\}.$$

还有一种记号. 设集  $A$  是由具有某种性质  $p$  的对象汇集而成, 则记

$$A = \{x \mid x \text{ possesses the property } p\}.$$

**定义** 若  $a$  是集  $A$  的元, 则写  $a \in A$  或  $A \ni a$ , 说  $a$  属于 (*to belong to*)  $A$  或  $A$  包含 (*to contain*)  $a$ . 若  $a$  不是集  $A$  的元, 则写  $a \notin A$  或  $A \not\ni a$ , 说  $a$  不属于  $A$  或  $A$  不包含  $a$ .

**例** 全体整数作成的集用  $\mathbb{Z}$  (*Zahl*)<sup>†</sup> 表示. 它可以写为

$$\mathbb{Z} = \{0, 1, -1, 2, -2, \dots, n, -n, \dots\}.$$

**例** 全体非负整数作成的集用  $\mathbb{N}$  (*natural*) 表示. 它可以写为

$$\mathbb{N} = \{x \mid x \in \mathbb{Z} \text{ and } x \geq 0\}.$$

为了方便, 也可以写为

$$\mathbb{N} = \{x \in \mathbb{Z} \mid x \geq 0\}.$$

---

<sup>†</sup>A German word which means *number*.

**定义** 若任取  $a \in A$ , 都有  $a \in B$ , 则写  $A \subset B$  或  $B \supset A$ , 说  $A$  是  $B$  的子集 (*subset*) 或  $B$  是  $A$  的超集 (*superset*). 假如有一个  $b \in B$  不是  $A$  的元, 可以用“真” (*proper*) 形容之.

**例** 空集是任意集的子集. 空集是任意不空的集的真子集.

**例** 全体有理数作成的集用  $\mathbb{Q}$  (*quotient*) 表示. 因为整数是有理数, 所以  $\mathbb{Z} \subset \mathbb{Q}$ . 因为有理数  $\frac{1}{2}$  不是整数, 我们说  $\mathbb{Z}$  是  $\mathbb{Q}$  的真子集.

**定义** 全体实数作成的集用  $\mathbb{R}$  (*real*) 表示.

**定义** 全体复数作成的集用  $\mathbb{C}$  (*complex*) 表示. 不难看出,

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

**定义**  $\mathbb{F}$  (*field*) 可表示  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$  的任意一个. 不难看出,  $\mathbb{F}$  适合这几条:

- (i)  $0 \in \mathbb{F}, 1 \in \mathbb{F}, 0 \neq 1$ ;
- (ii) 任取  $x, y \in \mathbb{F} (y \neq 0)$ , 必有  $x - y, \frac{x}{y} \in \mathbb{F}$ .

后面会见到稍详细的论述.

**定义** 设  $\mathbb{L}$  是  $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{N}, \mathbb{F}$  的任意一个.  $\mathbb{L}^*$  表示  $\mathbb{L}$  去掉 0 后得到的集. 不难看出,  $\mathbb{L}$  是  $\mathbb{L}^*$  的真超集.

**定义** 若集  $A$  与  $B$  包含的元完全一样, 则  $A$  与  $B$  是同一集. 我们说  $A$  等于  $B$ , 写  $A = B$ . 显然

$$A = B \iff A \subset B \text{ and } B \subset A.$$

**定义** 集  $A$  与  $B$  的交 (*intersection*) 是集

$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}.$$

也就是说,  $A \cap B$  恰由  $A$  与  $B$  的公共元作成.

集  $A$  与  $B$  的并 (*union*) 是集

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\}.$$

也就是说,  $A \cup B$  恰包含  $A$  与  $B$  的全部元.

类似地, 可定义多个集的交与并.

**定义** 设  $A, B$  是集. 定义

$$A \times B = \{ (a, b) \mid a \in A, b \in B \}.$$

$A \times A$  可简写为  $A^2$ . 类似地,

$$A \times B \times C = \{ (a, b, c) \mid a \in A, b \in B, c \in C \}, \quad A^3 = A \times A \times A.$$

**例** 设  $A = \{1, 2\}, B = \{3, 4, 5\}$ . 则

$$A \times B = \{ (1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5) \}.$$

而

$$B \times A = \{ (3, 1), (3, 2), (4, 1), (4, 2), (5, 1), (5, 2) \}.$$

**评注** 一般地,  $A \times B \neq B \times A$ . 假如  $A, B$  各自有  $m, n$  个元, 利用一点计数知识可以看出,  $A \times B$  有  $mn$  个元.

## 函数

**定义** 假如通过一个法则  $f$ , 使任取  $a \in A$ , 都能得到唯一的  $b \in B$ , 则说这个法则  $f$  是集  $A$  到集  $B$  的一个函数 (*function*). 元  $b$  是元  $a$  在函数  $f$  下的象 (*image*). 元  $a$  是元  $b$  在  $f$  下的一个原象 (*inverse image*). 这个关系可以写为

$$\begin{aligned} f: \quad & A \rightarrow B, \\ & a \mapsto b = f(a). \end{aligned}$$

称  $A$  是定义域 (*domain*),  $B$  是陪域<sup>†</sup> (*codomain*).

---

<sup>†</sup>不要混淆陪域与象集 (*image, range*).  $f$  的象集是

$$\text{Im } f = \{ b \in B \mid b = f(a), a \in A \}.$$

这就是中学数学里的“值域”.

**例** 可以把  $\mathbb{R}^2$  看作平面上的点集.

$$f: \begin{aligned} &\mathbb{R}^2 \rightarrow \mathbb{R}, \\ &(x, y) \mapsto \sqrt{x^2 + y^2} \end{aligned}$$

是函数: 它表示点  $(x, y)$  到点  $(0, 0)$  的距离.

**例** 设

$$A = \{\text{dinner, bath, me}\}, \quad B = \{0, 1\}.$$

法则

$$f_1: \quad \text{dinner} \mapsto 0, \quad \text{bath} \mapsto 1$$

不是  $A$  到  $B$  的函数, 因为它没有为  $A$  的元  $\text{me}$  规定象. 但是, 如果记  $A_1 = \{\text{dinner, bath}\}$ , 这个  $f_1$  可以是  $A_1$  到  $B$  的函数.

法则

$$f_2: \quad \begin{aligned} &\text{dinner} \mapsto 0, \\ &\text{bath} \mapsto 1, \\ &\text{me} \mapsto b \quad \text{where } b^2 = b \end{aligned}$$

不是  $A$  到  $B$  的函数, 因为它给  $A$  的元  $\text{me}$  规定的象不唯一.

法则

$$f_3: \quad \text{dinner} \mapsto 0, \quad \text{bath} \mapsto 1, \quad \text{me} \mapsto -1$$

不是  $A$  到  $B$  的函数, 因为它给  $A$  的元  $\text{me}$  规定的象不是  $B$  的元. 但是, 如果记  $B_1 = \{-1, 0, 1\}$ , 这个  $f_3$  可以是  $A$  到  $B_1$  的函数.

**定义** 设  $f_1$  与  $f_2$  都是  $A$  到  $B$  的函数. 若任取  $a \in A$ , 必有  $f_1(a) = f_2(a)$ , 则说这二个函数相等, 写为  $f_1 = f_2$ .

**例** 设  $A \subset \mathbb{C}$ , 且  $A$  非空. 定义二个  $A$  到  $\mathbb{C}$  的函数:  $f_1(x) = x^2$ ,  $f_2(x) = |x|^2$ . 如果  $A = \mathbb{R}$ , 那么  $f_1 = f_2$ . 可是, 若  $A = \mathbb{C}$ ,  $f_1$  与  $f_2$  不相等.

**例** 设  $A$  是全体正实数作成的集. 定义二个  $A$  到  $\mathbb{R}$  的函数:  $f_1(x) = \frac{1}{6} \log_2 x^3$ ,  $f_2(x) = \log_4 x$ . 知道对数的读者可以看出,  $f_1$  与  $f_2$  有着相同的对应法则, 故  $f_1 = f_2$ . 因为  $f_2$  是对数函数 (*logarithmic function*), 所以  $f_1$  也是.

**评注** 在上下文清楚的情况下, 可以单说函数的对应法则. 比如, 中学数学课说 “二次函数  $f(x) = x^2 + x - 1$ ” 时, 定义域与陪域默认都是  $\mathbb{R}$ . 中学的函数一般都是实数的子集到实数的子集的函数. 所谓 “自然定义域” 是指 (在一定范围内) 一切使对应法则有意义的元构成的集. 比如, 在中学, 我们说  $\frac{1}{x}$  的自然定义域是  $\mathbb{R}^*$ ,  $\sqrt{x}$  的自然定义域是一切非负实数. 在研究复变函数时, 我们说  $\frac{1}{z}$  的自然定义域是  $\mathbb{C}^*$ . 如果不明确函数的定义域, 我们会根据上下文作出自然定义域作为它的定义域.

**定义**  $A$  到  $A$  的函数是  $A$  的变换 (*transform*). 换句话说, 变换是定义域跟陪域一样的函数.

## 二元运算

**定义**  $A^2$  到  $A$  的函数称为  $A$  的二元运算 (*binary functions*).

**例** 设  $f(x, y) = x - y$ . 这个  $f$  是  $\mathbb{Z}$  的二元运算; 但是, 它不是  $\mathbb{N}$  的二元运算.

**评注** 设  $\circ$  是  $A$  的二元运算. 代替  $\circ(x, y)$ , 我们写  $x \circ y$ . 一般地, 若表示这个二元运算的符号不是字母, 我们就把这个符号写在二个元的中间.

**定义** 设  $T(A)$  是全部  $A$  的变换作成的集. 设  $f, g$  是  $A$  的变换. 任取  $a \in A$ , 当然有  $b = f(a) \in A$ . 所以,  $g(b) = g(f(a))$  也是  $A$  的元. 当然, 这个  $g(f(a))$  也是唯一确定的. 这样, 我们说,  $f$  与  $g$  的复合 (*composition*)  $g \circ f$  是

$$\begin{aligned} g \circ f: & & A &\rightarrow A, \\ & & a &\mapsto g(f(a)). \end{aligned}$$

所以, 复合是  $T(A)$  的二元运算:

$$\begin{aligned} \circ: & & T(A) \times T(A) &\rightarrow T(A), \\ & & (g, f) &\mapsto g \circ f. \end{aligned}$$

**评注** 设  $A$  有有限多个元. 此时, 可排出  $A$  的元:

$$A = \{a_1, a_2, \dots, a_n\}.$$

设  $f$  是  $A^2$  到  $B$  的函数. 则任给整数  $i, j, 1 \leq i, j \leq n$ , 记

$$f(a_i, a_j) = b_{i,j} \in B.$$

可以用这样的表描述此函数:

	$a_1$	$a_2$	$\cdots$	$a_n$
$a_1$	$b_{1,1}$	$b_{1,2}$	$\cdots$	$b_{1,n}$
$a_2$	$b_{2,1}$	$b_{2,2}$	$\cdots$	$b_{2,n}$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$a_n$	$b_{n,1}$	$b_{n,2}$	$\cdots$	$b_{n,n}$

有的时候, 为了强调函数名, 可在左上角书其名:

$f$	$a_1$	$a_2$	$\cdots$	$a_n$
$a_1$	$b_{1,1}$	$b_{1,2}$	$\cdots$	$b_{1,n}$
$a_2$	$b_{2,1}$	$b_{2,2}$	$\cdots$	$b_{2,n}$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$a_n$	$b_{n,1}$	$b_{n,2}$	$\cdots$	$b_{n,n}$

这种表示函数的方式是方便的. 如果这些  $b_{i,j}$  都是  $A$  的元, 就说这张表是  $A$  的运算表.

**例** 设  $T = \{0, 1, -1\}$ ,  $\circ(x, y) = xy$ . 不难看出,  $\circ$  确实是  $T$  的二元运算. 它的运算表如下:

	0	1	-1
0	0	0	0
1	0	1	-1
-1	0	-1	1

**例** 设  $\mathbb{F}_{\text{nu}}$  是将  $\mathbb{F}$  去掉 0, 1 后得到的集<sup>†</sup>. 看下列 6 个法则:

$$\begin{aligned} f_0: & x \mapsto x; \\ f_1: & x \mapsto 1 - x; \\ f_2: & x \mapsto \frac{1}{x}; \\ f_3: & x \mapsto 1 - \frac{1}{1 - x}; \\ f_4: & x \mapsto 1 - \frac{1}{x}; \\ f_5: & x \mapsto \frac{1}{1 - x}. \end{aligned}$$

记  $S_6 = \{f_0, f_1, f_2, f_3, f_4, f_5\}$ . 可以验证,  $S_6 \subset T(\mathbb{F}_{\text{nu}})$ .

进一步地, 36 次复合告诉我们, 任取  $f, g \in S_6$ , 必有  $g \circ f \in S_6$ . 可以验证, 这是  $S_6$  的 (复合) 运算表:

	$f_0$	$f_1$	$f_2$	$f_3$	$f_4$	$f_5$
$f_0$	$f_0$	$f_1$	$f_2$	$f_3$	$f_4$	$f_5$
$f_1$	$f_1$	$f_0$	$f_4$	$f_5$	$f_2$	$f_3$
$f_2$	$f_2$	$f_5$	$f_0$	$f_4$	$f_3$	$f_1$
$f_3$	$f_3$	$f_4$	$f_5$	$f_0$	$f_1$	$f_2$
$f_4$	$f_4$	$f_3$	$f_1$	$f_2$	$f_5$	$f_0$
$f_5$	$f_5$	$f_2$	$f_3$	$f_1$	$f_0$	$f_4$

我们在本节会经常用  $S_6$  举例.

**定义** 设  $\circ$  是  $A$  的二元运算. 若任取  $x, y, z \in A$ , 必有

$$(x \circ y) \circ z = x \circ (y \circ z),$$

则说  $f$  适合结合律 (*associativity*). 此时,  $(x \circ y) \circ z$  或  $x \circ (y \circ z)$  可简写为  $x \circ y \circ z$ .

**例**  $\mathbb{Z}$  的加法当然适合结合律. 可是, 它的减法不适合结合律.

---

<sup>†</sup>这个  $\mathbb{F}_{\text{nu}}$  只是临时记号: nu 表示 *nil, unity*.

**评注** 变换的复合适合结合律. 确切地, 设  $f, g, h$  都是  $A$  的变换. 任取  $a \in A$ , 则

$$\begin{aligned}(h \circ (g \circ f))(a) &= h((g \circ f)(a)) = h(g(f(a))), \\ ((h \circ g) \circ f)(a) &= (h \circ g)(f(a)) = h(g(f(a))).\end{aligned}$$

也就是说,

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

**例**  $S_6$  的复合当然适合结合律.

**定义** 设  $\circ$  是  $A$  的二元运算. 若任取  $x, y \in A$ , 必有

$$x \circ y = y \circ x,$$

则说  $\circ$  适合交换律 (*commutativity*).

**例**  $\mathbb{F}^*$  的乘法当然适合交换律. 可是, 它的除法不适合交换律.

**例**  $S_6$  的复合不适合交换律, 因为  $f_1 \circ f_2 = f_4$ , 而  $f_2 \circ f_1 = f_5$ , 二者不相等.

**评注** 在本文里,  $\cdot$  运算的优先级高于  $+$  运算. 所以,  $a \cdot b + c$  的意思就是

$$(a \cdot b) + c,$$

而不是

$$a \cdot (b + c).$$

**定义** 设  $+, \cdot$  是  $A$  的二个二元运算. 若任取  $x, y, z \in A$ , 必有

$$(LD) \quad x \cdot (y + z) = x \cdot y + x \cdot z,$$

则说  $+$  与  $\cdot$  适合左 ( $\cdot$ ) 分配律<sup>†</sup> (*left distributivity*). 类似地, 若

$$(RD) \quad (y + z) \cdot x = y \cdot x + z \cdot x,$$

<sup>†</sup>在不引起歧义时, 括号里的内容可省略. 或者这么说: 当我们说  $+, \cdot$  适合分配律时, 我们不会理解为  $x + (y \cdot z) = (x + y) \cdot (x + z)$ . 但有意思的事儿是, 如果把  $+$  理解为并,  $\cdot$  理解为交,  $x, y, z$  理解为集, 那这个式是对的. 当然,  $x \cdot (y + z) = x \cdot y + x \cdot z$  也是对的.



则说  $+$  与  $\cdot$  适合右  $(\cdot)$  分配律 (*right distributivity*). 说既适合 LD 也适合 RD 的  $+$  与  $\cdot$  适合  $(\cdot)$  分配律 (*distributivity*). 显然, 若  $\cdot$  适合交换律, 则 LD 与 RD 等价.

**例**  $\mathbb{F}$  的加法与乘法适合分配律. 当然, 减法与乘法也适合分配律:

$$x(y - z) = xy - xz = yx - zx = (y - z)x.$$

甚至, 在正实数里, 加法与除法适合右分配律:

$$\frac{y + z}{x} = \frac{y}{x} + \frac{z}{x}.$$

**定义** 设  $\circ$  是  $A$  的二元运算. 若任取  $x, y, z \in A$ , 必有

$$(LC) \quad x \circ y = x \circ z \implies y = z,$$

则说  $\circ$  适合左消去律 (*left cancellation property*). 类似地, 若

$$(RC) \quad x \circ z = y \circ z \implies x = y,$$

则说  $\circ$  适合右消去律 (*right cancellation property*). 说既适合 LC 也适合 RC 的  $\circ$  适合消去律 (*cancellation property*). 显然, 若  $\circ$  适合交换律, 则 LC 与 RC 等价.

**例** 显然,  $\mathbb{N}$  的乘法不适合消去律, 但  $\mathbb{N}^*$  的乘法适合消去律<sup>†</sup>.

**例** 考虑  $x \circ y = x^3 + y^2$ . 若把  $\circ$  视为  $\mathbb{N}$  的二元运算, 那么它适合消去律. 若把  $\circ$  视为  $\mathbb{Q}$  的二元运算, 那么它适合右消去律. 若把  $\circ$  视为  $\mathbb{C}$  的二元运算, 那么它不适合任意一个消去律.

**例** 一般地, 当  $A$  至少有二个元时,  $\circ$  (在  $T(A)$  里) 不适合消去律. 设  $a, b \in A, a \neq b$ . 考虑下面 4 个变换:

$$g_0: \quad a \mapsto a, \quad b \mapsto b, \quad x \mapsto x \text{ where } x \neq a, b;$$

$$g_1: \quad a \mapsto a, \quad b \mapsto a, \quad x \mapsto x \text{ where } x \neq a, b;$$

$$g_2: \quad a \mapsto b, \quad b \mapsto b, \quad x \mapsto x \text{ where } x \neq a, b;$$

$$g_3: \quad a \mapsto b, \quad b \mapsto a, \quad x \mapsto x \text{ where } x \neq a, b.$$

---

<sup>†</sup>后面提到整环时, 我们会稍微修改一下消去律的描述.

可以验证,

$$g_3 \circ g_1 = g_2 \circ g_1 = g_2 \circ g_3 = g_2.$$

由此可以看出,  $\circ$  不适合任意一个消去律.

**例** 我们看  $\circ$  在  $S_6$  里是否适合消去律. 取  $f, g, h \in S_6$ . 由表易知, 当  $g \neq h$  时,  $f \circ g \neq f \circ h$  (横着看运算表), 且  $g \circ f \neq h \circ f$  (竖着看运算表). 这说明,  $\circ$  在  $T(\mathbb{F}_{\text{nu}})$  的子集  $S_6$  里适合消去律.

**定义** 设  $\circ$  是  $A$  的二元运算. 若存在  $e \in A$ , 使若任取  $x \in A$ , 必有

$$e \circ x = x \circ e = x,$$

则说  $e$  是  $A$  的 (关于运算  $\circ$  的) 么元 (*identity*). 如果  $e'$  也是么元, 则

$$e = e \circ e' = e'.$$

**例**  $\mathbb{F}$  的加法的么元是 0, 且其乘法的么元是 1.

**例** 不难看出, 这个变换是  $T(A)$  的么元:

$$\begin{aligned} \iota: \quad & A \rightarrow A, \\ & a \mapsto a. \end{aligned}$$

它也有个一般点的名字: 恒等变换 (*identity transform*).

在  $S_6$  里,  $f_0$  就是这里的  $\iota$ .

**定义** 设  $\circ$  是  $A$  的二元运算. 设  $e$  是  $A$  的么元. 设  $x \in A$ . 若存在  $y \in A$ , 使

$$y \circ x = x \circ y = e,$$

则说  $y$  是  $x$  的 (关于运算  $\circ$  的) 逆元 (*inverse*).

**例**  $\mathbb{F}$  的每个元都有加法逆元, 即其相反数.

**评注** 设  $\circ$  适合结合律. 如果  $y, y'$  都是  $x$  的逆元, 则

$$y = y \circ e = y \circ (x \circ y') = (y \circ x) \circ y' = e \circ y' = y'.$$

此时, 一般用  $x^{-1}$  表示  $x$  的逆元. 因为

$$x^{-1} \circ x = x \circ x^{-1} = e,$$

由上可知,  $x^{-1}$  也有逆元, 且  $(x^{-1})^{-1} = x$ .

**例** 一般地, 当  $A$  至少有二个元时,  $T(A)$  既有有逆元的变换, 也有无逆元的变换. 还是看前面的  $g_0, g_1, g_2, g_3$ . 首先,  $g_0$  是么元  $\iota$ . 不难看出,  $g_0$  与  $g_3$  都有逆元:

$$g_0 \circ g_0 = g_3 \circ g_3 = g_0.$$

不过,  $g_1$  不可能有逆元. 假设  $g_1$  有逆元  $h$ , 则应有

$$(h \circ g_1)(a) = \iota(a) = a, \quad (h \circ g_1)(b) = \iota(b) = b.$$

可是,  $g_1(a) = g_1(b) = a$ , 故  $(h \circ g_1)(a) = (h \circ g_1)(b) = h(a)$ , 它不能既等于  $a$  也等于  $b$ , 矛盾!

**例** 再看  $S_6$ . 由表可看出,  $f_0, f_1, f_2, f_3, f_4, f_5$  的逆元分别是  $f_0, f_1, f_2, f_3, f_5, f_4$ .

**评注** 设  $\circ$  适合结合律. 如果  $x, y$  都有逆元, 那么  $x \circ y$  也有逆元, 且

$$(x \circ y)^{-1} = y^{-1} \circ x^{-1}.$$

为了说明这一点, 只要按定义验证即可:

$$(y^{-1} \circ x^{-1}) \circ (x \circ y) = y^{-1} \circ (x^{-1} \circ x) \circ y = y^{-1} \circ e \circ y = y^{-1} \circ y = e,$$

$$(x \circ y) \circ (y^{-1} \circ x^{-1}) = x \circ (y \circ y^{-1}) \circ x^{-1} = x \circ e \circ x^{-1} = x \circ x^{-1} = e.$$

这个规则往往称为袜靴规则 (*socks and shoes rule*): 设  $y$  是穿袜,  $x$  是穿靴,  $x \circ y$  表示动作的复合: 先穿袜后穿靴. 那么这个规则告诉我们,  $x \circ y$  的逆元就是先脱靴再脱袜.

**评注** 由此可见, 结合律是一条很重要的规则. 我们算  $63 \cdot 8 \cdot 125$  时也会想着先算  $8 \cdot 125$ .

## 半群与群

**定义** 设  $S$  是非空集. 设  $\circ$  是  $S$  的二元运算. 若  $\circ$  适合结合律, 则称  $S$  (关于  $\circ$ ) 是半群 (*semi-group*).

**例**  $\mathbb{N}$  关于加法 (或乘法) 作成半群.

**例**  $T(A)$  关于  $\circ$  作成半群.

**评注** 事实上, 这里要求  $S$  非空是有必要的.

首先, 空集没什么意思. 其次, 前面所述的结合律、交换律、分配律等自动成立, 这是因为对形如 “若  $p$ , 则  $q$ ” 的命题而言,  $p$  为假推出整个命题为真. 这是相当 “危险” 的!

**定义** 设  $m$  是正整数. 设  $x$  是半群  $S$  的元. 令

$$x^1 = x, \quad x^m = x \circ x^{m-1}.$$

$x^m$  称为  $x$  的  $m$  次幂. 不难看出, 当  $m, n$  都是正整数时,

$$x^{m+n} = x^m \circ x^n, \quad (x^m)^n = x^{mn}.$$

假如  $S$  有二个元  $x, y$  适合  $x \circ y = y \circ x$ , 那么还有

$$(x \circ y)^m = x^m \circ y^m.$$

**例** 还是看熟悉的  $\mathbb{N}$ . 对于乘法而言, 这里的幂就是普通的幂——一个数自乘多次的结果. 对于加法而言, 这里的幂相当于乘法——一个数自加多次的结果.

**定义** 设  $G$  关于  $\circ$  是半群. 若  $G$  的关于  $\circ$  的么元存在, 且  $G$  的任意元都有关于  $\circ$  的逆元, 则  $G$  是群 (*group*).

**例**  $\mathbb{N}$  关于加法 (或乘法) 不能作成群.  $\mathbb{Z}$  关于加法作成群, 但关于乘法不能作成群.  $\mathbb{F}$  关于乘法不能作成群, 但  $\mathbb{F}^*$  关于乘法作成群. 不过,  $\mathbb{F}^*$  关于加法不能作成群.

**例**  $T(A)$  一般不是群. 不过,  $S_6$  是群.

**评注** 群有唯一的幺元. 群的每个元都有唯一的逆元.

**评注** 设  $G$  关于  $\circ$  是群. 我们说,  $\circ$  适合消去律.

假如  $x \circ y = x \circ z$ . 二侧左边乘  $x$  的逆元  $x^{-1}$ , 就有

$$x^{-1} \circ (x \circ y) = x^{-1} \circ (x \circ z).$$

由于  $\circ$  适合结合律,

$$(x^{-1} \circ x) \circ y = (x^{-1} \circ x) \circ z.$$

也就是

$$e \circ y = e \circ z.$$

这样,  $y = z$ . 类似地, 用同样的方法可以知道, 右消去律也对.

**定义** 已经知道, 群的每个元  $x$  都有逆元  $x^{-1}$ . 由此, 当  $m$  是正整数时, 定义  $x^{-m} = (x^{-1})^m$ . 再定义  $x^0 = e$ . 利用半群的结果, 可以看出, 当  $m, n$  都是整数时,

$$x^{m+n} = x^m \circ x^n, \quad (x^m)^n = x^{mn}.$$

假如  $G$  有二个元  $x, y$  适合  $x \circ y = y \circ x$ , 那么还有

$$(x \circ y)^m = x^m \circ y^m.$$

**例** 对于  $\mathbb{F}^*$  的乘法而言, 这里的任意整数幂跟普通的整数幂没有任何区别. 我们学习数的负整数幂的时候, 也是借助倒数定义的.

## 子群

**定义** 设  $G$  关于  $\circ$  是群. 设  $H \subset G$ ,  $H$  非空. 若  $H$  关于  $\circ$  也作成群, 则  $H$  是  $G$  的子群 (*subgroup*).

**例** 对加法来说,  $\mathbb{Z}$  是  $\mathbb{F}$  的子群. 对乘法来说,  $\mathbb{Z}^*$  不是  $\mathbb{F}^*$  的子群.

**评注** 设  $H \subset G$ ,  $H$  非空.  $H$  是  $G$  的子群的一个必要与充分条件是: 任取  $x, y \in H$ , 必有  $x \circ y^{-1} \in H$ .

怎么说明这一点呢? 先看充分性. 任取  $x \in H$ , 则  $e = x \circ x^{-1} \in H$ . 任取  $y \in H$ , 则  $y^{-1} = e \circ y^{-1} \in H$ . 所以

$$x \circ y = x \circ (y^{-1})^{-1} \in H.$$

$\circ$  在  $G$  适合结合律,  $H \subset G$ , 所以  $\circ$  作为  $H$  的二元运算也适合结合律. 至此,  $H$  是半群.

前面已经说明,  $e \in H$ , 所以  $H$  的关于  $\circ$  的么元存在. 进一步地,  $x \in H$  在  $G$  里的逆元也是  $H$  的元, 所以  $H$  的任意元都有关于  $\circ$  的逆元. 这样,  $H$  是群. 顺便一提, 我们刚才也说明了,  $G$  的么元也是  $H$  的么元, 且  $H$  的元在  $G$  里的逆元也是在  $H$  里的逆元.

再看必要性. 假设  $H$  是一个群. 任取  $x, y \in H$ , 我们要说明  $x \circ y^{-1} \in H$ . 看上去有点显然呀!  $H$  是群, 所以  $y$  有逆元  $y^{-1}$ , 又因为  $\circ$  是  $H$  的二元运算,  $x \circ y^{-1} \in H$ . 不过要注意一个细节. 我们说明充分性时,  $y^{-1}$  被认为是  $y$  在  $G$  里的逆元; 可是, 刚才的论证里  $y^{-1}$  实则是  $y$  在  $H$  里的逆元. 大问题! 怎么解决呢? 如果我们说明  $y$  在  $H$  里的逆元也是  $y$  在  $G$  里的逆元, 那这个漏洞就被修复了.

我们知道,  $H$  有么元  $e_H$ , 所以  $e_H \circ e_H = e_H$ .  $e_H$  是  $G$  的元, 所以  $e_H$  在  $G$  里有逆元  $(e_H)^{-1}$ . 这样,

$$\begin{aligned} e_H &= e \circ e_H \\ &= ((e_H)^{-1} \circ e_H) \circ e_H \\ &= (e_H)^{-1} \circ (e_H \circ e_H) \\ &= (e_H)^{-1} \circ e_H \\ &= e. \end{aligned}$$

取  $y \in H$ .  $y$  在  $H$  里有逆元  $z$ , 即

$$z \circ y = y \circ z = e_H = e.$$

$y, z$  都是  $G$  的元. 这样, 根据逆元的唯一性,  $z$  自然是  $y$  在  $G$  里的逆元.

## 加群

**定义** 若  $G$  关于名为  $+$  的二元运算作成群, 么元  $e$  读作“零元”写作  $0$ ,  $x \in G$  的逆元  $x^{-1}$  读作“ $x$  的相反元”写作  $-x$ , 且  $+$  适合交换律, 则说  $G$  是加群 (*additive group*). 相应地, “元的幂”也应该改为“元的倍”:  $x^m$  写为  $mx$ . 用加法的语言改写前面的幂的规则, 就得到了倍的规则: 对任意  $x, y \in G, m, n \in \mathbb{Z}$ , 有

$$(m+n)x = mx + nx,$$

$$m(nx) = (mn)x,$$

$$m(x+y) = mx + my.$$

顺便一提, 在这种记号下,  $x-y$  是  $x+(-y)$  的简写. 并且

$$x+y = x+z \implies y = z.$$

由于这里的加法适合交换律, 直接换位就是右消去律. 前面说, 若运算适合结合律, 则  $x$  的逆元的逆元还是  $x$ . 这句话用加法的语言写, 就是

$$-(-x) = x.$$

前面的“袜靴规则”就是

$$-(x+y) = (-y) + (-x) = (-x) + (-y) = -x - y.$$

这就是熟悉的去括号法则. 这里体现了交换律的作用.

**评注** 初见此定义可能会觉得有些混乱: 怎么“倒数”又变为“相反数”了? 其实这都是借鉴已有写法. 前面,  $\circ$  虽然不是  $\cdot$ , 但这个形状暗示着乘法, 因此有  $x^{-1}$  这样的记号; 现在, 运算的名字是  $+$ , 自然要根据形状作出相应的改变. 其实, 这里“名为  $+$ ”“零元”“相反元”都不是本质——换句话说, 还是可以用老记号. 不过, 我们主要接触至少与二种运算相关联的结构——整环与域, 所以用二套记号、名字是有必要的.

**评注** 前面的  $x^0 = e$  在加群里变为  $0x = 0$ . 看上去“很普通”, 不过左边的  $0$  是整数, 右边的  $0$  是加群的零元, 二者一般不一样!

**例** 显而易见,  $\mathbb{Z}$ ,  $\mathbb{F}$  都是加群.

**例**  $S_6$  不是加群, 因为它的二元运算不适合交换律.

**评注** 类似地, 可以定义子加群 (*sub-additive group*). 这里, 就直接用等价刻画来描述它: “ $G$  的非空子集  $H$  是加群  $G$  的子加群的一个必要与充分条件是: 任取  $x, y \in H$ , 必有  $x - y \in H$ .”

## 和

**定义** 设  $f$  是  $\mathbb{Z}$  的非空子集  $S$  到加群  $G$  的函数. 设  $p, q$  是二个整数. 如果  $p \leq q$ , 则记

$$\sum_{j=p}^q f(j) = f(p) + f(p+1) + \cdots + f(q).$$

也就是说,  $\sum_{j=p}^q f(j)$  就是  $q - (p - 1)$  个元的和的一种简洁的表示法. 如果  $p > q$ , 约定  $\sum_{j=p}^q f(j) = 0$ .

**例** 我们已经知道,  $n \geq 0$  时

$$0 + 1 + \cdots + (n-1) = \frac{n(n-1)}{2}.$$

用  $\sum$  写出来, 就是

$$\sum_{k=0}^{n-1} k = \frac{n(n-1)}{2}.$$

这里的  $k$  是所谓的 “dummy variable”. 所以

$$\sum_{j=0}^{n-1} j = \sum_{k=0}^{n-1} k = \sum_{\ell=0}^{n-1} \ell = \frac{n(n-1)}{2}.$$

**例**  $f$  可以是常函数:

$$\sum_{t=p}^q 1 = \begin{cases} q - p + 1, & q \geq p; \\ 0, & q < p. \end{cases}$$



**例** 设  $f$  与  $g$  是  $\mathbb{Z}$  的非空子集  $S$  到加群  $G$  的函数. 因为加群的加法适合结合律与交换律, 所以

$$\sum_{j=p}^q (f(j) + g(j)) = \sum_{j=p}^q f(j) + \sum_{j=p}^q g(j).$$

**评注** 设  $f(i, j)$  是  $\mathbb{Z}^2$  的非空子集到加群  $G$  的函数. 记

$$S_C = \sum_{j=p}^q \sum_{i=m}^n f(i, j), \quad S_R = \sum_{i=m}^n \sum_{j=p}^q f(i, j),$$

其中  $q \geq p, n \geq m$ .  $\sum_{i=m}^n f(i, j)$  是何物? 暂时视  $i$  之外的变元为常元, 则

$$\sum_{i=m}^n f(i, j) = f(m, j) + f(m+1, j) + \cdots + f(n, j).$$

$\sum_{j=p}^q \sum_{i=m}^n f(i, j)$  是  $\sum_{j=p}^q (\sum_{i=m}^n f(i, j))$  的简写:

$$\sum_{j=p}^q \sum_{i=m}^n f(i, j) = \sum_{i=m}^n f(i, p) + \sum_{i=m}^n f(i, p+1) + \cdots + \sum_{i=m}^n f(i, q).$$

$\sum_{i=m}^n \sum_{j=p}^q f(i, j)$  有着类似的解释. 我们说,  $S_C$  一定与  $S_R$  相等.

记

$$C_j = \sum_{i=m}^n f(i, j), \quad R_i = \sum_{j=p}^q f(i, j).$$

考虑下面的表:

$f(m, p)$	$f(m, p+1)$	$\cdots$	$f(m, q)$	$R_m$
$f(m+1, p)$	$f(m+1, p+1)$	$\cdots$	$f(m+1, q)$	$R_{m+1}$
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
$f(n, p)$	$f(n, p+1)$	$\cdots$	$f(n, q)$	$R_n$
$C_p$	$C_{p+1}$	$\cdots$	$C_q$	

由此, 不难看出,  $S_C$  与  $S_R$  只是用不同的方法将  $(n-m+1)(q-p+1)$  个元相加罢了.

**评注** 上面的例其实就是一个特殊情形 ( $n-m+1=2$ ).

## 环

**定义** 设  $R$  是加群. 设  $\cdot$  (读作“乘法”) 也是  $R$  的二元运算. 假设

(i)  $\cdot$  适合结合律;

(ii)  $+$  与  $\cdot$  适合分配律.

我们说  $R$  (关于  $+$  与  $\cdot$ ) 是环 (*ring*).

**评注** 在不引起歧义的情况下, 可省去  $\cdot$ . 例如,  $a \cdot b$  可写为  $ab$ .

**例**  $\mathbb{Z}, \mathbb{F}$  (关于普通加法与乘法) 都是环.

**例** 全体偶数作成的集也是环. 一般地, 设  $k$  是整数, 则全体  $nk$  ( $n \in \mathbb{Z}$ ) 作成的集是环.

**例** 这里举一个“平凡的” (*trivial*) 例.  $N$  只有一个元  $0$ . 可以验证,  $N$  关于普通加法与乘法作成群. 这也是“最小的环”. 在上个例里, 取  $k = 0$  就是  $N$ .

**例** 这里举一个“不平凡的” (*nontrivial*) 例. 设  $R = \{0, a, b, c\}$ . 加法和乘法由以下二个表给定:

$+$	$0$	$a$	$b$	$c$
$0$	$0$	$a$	$b$	$c$
$a$	$a$	$0$	$c$	$b$
$b$	$b$	$c$	$0$	$a$
$c$	$c$	$b$	$a$	$0$

$\cdot$	$0$	$a$	$b$	$c$
$0$	$0$	$0$	$0$	$0$
$a$	$0$	$0$	$0$	$0$
$b$	$0$	$a$	$b$	$c$
$c$	$0$	$a$	$b$	$c$

可以验证, 这是一个环.

**评注** 我们看一下环的简单性质.

已经知道,  $R$  的任意元的“整数  $0$  倍”是  $R$  的零元. 不禁好奇, 零元乘任意元会是什么结果. 首先, 回想起,  $R$  的零元适合  $0 + 0 = 0$ . 利用分配律, 当  $x \in R$  时,

$$0x = (0 + 0)x = 0x + 0x.$$

我们知道, 加法适合消去律. 所以

$$0 = 0x.$$

类似地,  $x0 = 0$ . 也许有点眼熟? 但是这里左右二侧的 0 都是  $R$  的元, 不一定是数!

因为

$$xy + (-x)y = (x - x)y = 0,$$

$$xy + x(-y) = x(y - y) = 0,$$

所以

$$(-x)y = x(-y) = -xy.$$

从而

$$(-x)(-y) = -(x(-y)) = -(-xy) = xy.$$

根据分配律,

$$x(y_1 + \cdots y_n) = xy_1 + \cdots + xy_n,$$

$$(x_1 + \cdots + x_m)y = x_1y + \cdots + x_my.$$

二式联合, 就是

$$(x_1 + \cdots + x_m)(y_1 + \cdots y_n) = x_1y_1 + \cdots + x_1y_n + \cdots + x_my_1 + \cdots + x_my_n.$$

利用  $\sum$  符号, 此式可以写为

$$\left(\sum_{i=1}^m x_i\right) \left(\sum_{j=1}^n y_j\right) = \sum_{i=1}^m \sum_{j=1}^n x_i y_j.$$

所以, 若  $n$  是整数,  $x, y \in R$ , 则

$$(nx)y = n(xy) = x(ny).$$

对于正整数  $m, n$  与  $R$  的元  $x$ , 有

$$x^{m+n} = x^m x^n, \quad (x^m)^n = x^{mn}.$$

假如  $R$  有二个元  $x, y$  适合  $xy = yx$ , 那么还有

$$(xy)^m = x^m y^m.$$

**例** 在  $\mathbb{Z}, \mathbb{F}$  里, 这些就是我们熟悉的 (部分的) 数的运算律.

**评注** 类似地, 可以定义子环 (*subring*). 这里, 就直接用等价刻画来描述它: “ $R$  的非空子集  $S$  是环  $R$  的子环的一个必要与充分条件是: 任取  $x, y \in S$ , 必有  $x - y \in S, xy \in S$ .”

**定义** 设  $R$  是环. 假设任取  $x, y \in R$ , 必有  $xy = yx$ , 就说  $R$  是交换环 (*commutative ring*).

**评注** 以后接触的环都是交换环.

## 整环

**定义** 设  $D$  是环. 假设

- (i) 任取  $x, y \in D$ , 必有  $xy = yx$ ;
  - (ii) 存在  $1 \in D, 1 \neq 0$ , 使任取  $x \in D$ , 必有  $1x = x1 = x$ ;
  - (iii)  $\cdot$  适合“消去律变体”<sup>†</sup>: 若  $xy = xz, x \neq 0$ , 则  $y = z$ .
- 我们说  $D$  (关于  $+$  与  $\cdot$ ) 是整环 (*domain, integral domain*).

**例**  $\mathbb{Z}, \mathbb{F}$  都是整环. 当然, 也有介于  $\mathbb{Z}$  与  $\mathbb{F}$  之间的整环. 假如  $s \in \mathbb{C}$  的平方是整数, 那么全体形如  $x + sy$  ( $x, y \in \mathbb{Z}$ ) 的数作成一個整环.

**例** 看一个有限整环的例. 设  $V$  (*Vierergruppe*)<sup>‡</sup> 是 4 元集:

$$V = \{0, 1, \tau, \tau^2\}.$$

加法与乘法由下面的运算表决定:

$+$	0	1	$\tau$	$\tau^2$
0	0	1	$\tau$	$\tau^2$
1	1	0	$\tau^2$	$\tau$
$\tau$	$\tau$	$\tau^2$	0	1
$\tau^2$	$\tau^2$	$\tau$	1	0

$\cdot$	0	1	$\tau$	$\tau^2$
0	0	0	0	0
1	0	1	$\tau$	$\tau^2$
$\tau$	0	$\tau$	$\tau^2$	1
$\tau^2$	0	$\tau^2$	1	$\tau$

<sup>†</sup>一般地, 这也可称为消去律.

<sup>‡</sup>A German word which means *four-group*.

可以验证,  $V$  不但是一个环, 它还适合整环定义的条件 (i) (ii) (iii). 因此,  $V$  是整环.

在  $V$  里,  $1 + 1 = 0$ , 这跟平常的加法有点不一样. 换句话说, 这里的  $0$  跟  $1$  已经不是我们熟悉的数了.

**评注** 整环  $D$  有乘法幺元  $1$ . 因为  $D$  是加群,  $1$  当然有相反元  $-1$ . 任取  $a \in D$ . 根据分配律,

$$0 = 0a = (1 + (-1))a = 1a + (-1)a = a + (-1)a.$$

又因为  $a$  的相反元  $-a$  适合

$$0 = a + (-a),$$

故由 (加法) 消去律知  $-a = (-1)a$ .

**例** 全体偶数作成的集是交换环, 却不是整环.

**例** 再来看一个非整环例. 考虑  $\mathbb{Z}^2$ . 设  $a, b, c, d \in \mathbb{Z}$ . 规定

$$(a, b) = (c, d) \iff a = b \text{ and } c = d,$$

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

$$(a, b)(c, d) = (ac, bd).$$

可以验证, 在这二种运算下,  $\mathbb{Z}^2$  作成交换环, 其加法、乘法幺元分别是  $(0, 0)$ ,  $(1, 1)$ . 可是

$$(1, 0) \neq (0, 0), \quad (0, 1) \neq (0, -1), \quad (1, 0)(0, 1) = (1, 0)(0, -1).$$

也就是说, 乘法不适合消去律.

**评注** 可是, 如果这么定义乘法, 那么  $\mathbb{Z}^2$  可作为一个整环:

$$(a, b)(c, d) = (ac - bd, ad + bc).$$

事实上, 这就是复数乘法, 因为

$$(a + ib)(c + id) = (ac - bd) + i(ad + bc).$$

**评注** 整环  $D$  有乘法幺元 1. 任取  $a \in D$ . 我们定义

$$a^0 = 1.$$

我们已经知道, 当  $m, n$  是正整数,  $x \in D$  时,

$$x^m x^n = x^{m+n}, \quad (x^m)^n = x^{mn}.$$

现在, 当  $m, n$  是非负整数时, 上面的关系仍成立. 并且, 既然  $D$  的乘法适合交换律, 那么任取  $x, y \in D$ , 必有

$$(xy)^m = x^m y^m,$$

$m$  可以是非负整数.

**评注** 类似地, 可以定义子整环 (*subdomain*). 这里, 就直接用前面的等价刻画来描述它: “ $D$  的非空子集  $S$  是整环  $D$  的子整环的一个必要与充分条件是: (i)  $1 \in S$ ; (ii) 任取  $x, y \in S$ , 必有  $x - y \in S, xy \in S$ .”

**例** 设  $D \subset \mathbb{C}$ , 且  $D$  是整环. 不难看出,  $\mathbb{Z} \subset D$ .

## 积

**定义** 设  $f$  是  $\mathbb{Z}$  的非空子集  $S$  到整环  $D$  的函数. 设  $p, q$  是二个整数. 如果  $p \leq q$ , 则记

$$\prod_{j=p}^q f(j) = f(p) \cdot f(p+1) \cdot \cdots \cdot f(q).$$

也就是说,  $\prod_{j=p}^q f(j)$  就是  $q - (p - 1)$  个元的积的一种简洁的表示法. 如果  $p > q$ , 约定  $\prod_{j=p}^q f(j) = 1$ .

**定义** 设  $n$  是正整数. 那么  $1, 2, \dots, n$  的积是  $n$  的阶乘 (*factorial*):

$$n! = \prod_{j=1}^n j.$$

顺便约定  $0! = 1$ .

**评注** 不难看出, 当  $n$  是正整数时,

$$n! = n \cdot (n-1)!$$

**例** 不难验证, 下面是 0 至 9 的阶乘:

$$\begin{array}{ll} 0! = 1, & 1! = 1, \\ 2! = 2, & 3! = 6, \\ 4! = 24, & 5! = 120, \\ 6! = 720, & 7! = 5\,040, \\ 8! = 40\,320, & 9! = 362\,880. \end{array}$$

**评注** 因为整环的乘法也适合结合律与交换律, 所以

$$\begin{aligned} \prod_{j=p}^q (f(j) \cdot g(j)) &= \prod_{j=p}^q f(j) \cdot \prod_{j=p}^q g(j), \\ \prod_{j=p}^q \prod_{i=m}^n f(i, j) &= \prod_{i=m}^n \prod_{j=p}^q f(i, j), \end{aligned}$$

其中,  $\prod_{j=p}^q \prod_{i=m}^n f(i, j)$  当然是  $\prod_{j=p}^q (\prod_{i=m}^n f(i, j))$  的简写.

**评注** 回顾一下  $\sum$  符号. 我们已经知道

$$\sum_{j=p}^q (f(j) + g(j)) = \sum_{j=p}^q f(j) + \sum_{j=p}^q g(j).$$

因为整环有分配律, 故当  $c \in D$  与变元  $j$  无关时<sup>†</sup>

$$\sum_{j=p}^q cf(j) = c \sum_{j=p}^q f(j).$$

进而, 当  $c, d$  都是常元时,

$$\sum_{j=p}^q (cf(j) + dg(j)) = c \sum_{j=p}^q f(j) + d \sum_{j=p}^q g(j).$$

类似地, 当  $q \geq p$ ,  $c$  是常元时,

$$\prod_{j=p}^q cf(j) = c^{q-p+1} \prod_{j=p}^q f(j).$$

---

<sup>†</sup>这样的元称为常元 (constant).

**定义** 最后介绍一下双阶乘 (*double factorial*). 前  $n$  个正偶数的积是  $2n$  的双阶乘:

$$(2n)!! = \prod_{j=1}^n 2j.$$

前  $n$  个正奇数是  $2n-1$  的双阶乘:

$$(2n-1)!! = \prod_{j=1}^n (2j-1).$$

顺便约定  $0!! = (-1)!! = 1$ .

**评注** 不难看出, 对任意正整数  $m$ , 都有

$$m!! = m \cdot (m-2)!!.$$

双阶乘可以用阶乘表示:

$$\begin{aligned} (2n)!! &= 2^n n!, \\ (2n-1)!! &= \frac{(2n)!}{(2n)!!} = \frac{(2n)!}{2^n n!}. \end{aligned}$$

由此可得

$$n!! \cdot (n-1)!! = n!.$$

**例** 不难验证, 下面是 1 至 10 的双阶乘:

$$\begin{array}{ll} 1!! = 1, & 2!! = 2, \\ 3!! = 3, & 4!! = 8, \\ 5!! = 15, & 6!! = 48, \\ 7!! = 105, & 8!! = 384, \\ 9!! = 945, & 10!! = 3\,840. \end{array}$$

## 单位与域

**定义** 设  $D$  是整环. 设  $x \in D$ . 若存在  $y \in D$  使  $xy = 1$ , 则说  $x$  是  $D$  的单位 (*unit*).



**评注** 不难看出,  $D$  至少有一个单位 1, 因为  $1 \cdot 1 = 1$ . 定义里的  $y$  自然就是  $x$  的 (乘法) 逆元, 其一般记为  $x^{-1}$ .  $x^{-1}$  当然也是单位. 二个单位  $x, y$  的积  $xy$  也是单位:  $(xy)(y^{-1}x^{-1}) = 1$ . 单位的乘法当然适合结合律. 这样,  $D$  的单位作成是一个 (乘法) 群. 姑且叫  $D$  的所有单位作成的集为单位群 (*unit group*) 吧!

**评注** 不难看出, 0 一定不是单位.

**例** 看全体整数作成的整环  $\mathbb{Z}$ . 它恰有二个单位: 1 与  $-1$ .

**例**  $\mathbb{F}$  也是整环. 它有无限多个单位: 任意  $\mathbb{F}^*$  的元都是单位.

**例** 前面的 4 元集  $V$  的非零元都是单位.

**例** 现在看一个不那么平凡的例. 设

$$D = \{x + y\sqrt{3} \mid x, y \in \mathbb{Z}\}.$$

这个  $D$  (关于数的运算) 作成整环.

首先, 我们说, 不存在有理数  $q$  使  $q^2 = 3$ . 用反证法. 设  $q = \frac{m}{n}$ ,  $m, n$  是非零整数. 我们知道, 分数可以约分, 故可以假设 3 不是  $m$  与  $n$  的公因子. 这样

$$m^2 = 3n^2.$$

所以 3 一定是  $m^2$  的因子. 因为

$$\begin{aligned}(3\ell)^2 &= 3 \cdot 3\ell^2, \\ (3\ell \pm 1)^2 &= 3(3\ell^2 \pm 2\ell) + 1,\end{aligned}$$

故由此可看出, 3 也是  $m$  的因子. 记  $m = 3u$ . 这样

$$3u^2 = n^2.$$

所以 3 也是  $n$  的因子. 这跟假设矛盾!

再说一下  $D$  的二个元相等意味着什么. 设  $a, b, c, d$  都是整数. 那么

$$a + b\sqrt{3} = c + d\sqrt{3} \implies (a - c)^2 = 3(d - b)^2.$$

若  $d - b \neq 0$ , 则  $\frac{a-c}{d-b}$  是有理数, 且

$$\left(\frac{a-c}{d-b}\right)^2 = 3,$$

而这是荒谬的. 所以  $d - b = 0$ . 这样  $a - c = 0$ .

现在再来看单位问题. 若  $k$  是高于 1 的整数, 则  $k$  不是  $D$  的单位. 反证法. 若  $k$  是单位, 则有  $c, d \in \mathbb{Z}$  使

$$1 = k(c + d\sqrt{3}) = kc + kd\sqrt{3} \implies 1 = kc,$$

矛盾!

$D$  有无限多个单位. 因为

$$(2 + \sqrt{3})(2 - \sqrt{3}) = 1,$$

故对任意正整数  $n$ , 有

$$(2 + \sqrt{3})^n(2 - \sqrt{3})^n = 1.$$

所以,  $(2 \pm \sqrt{3})^n$  是单位.

**定义** 设  $F$  是整环. 若每个  $F$  的  $\neq 0$  的元都是  $F$  的单位, 则说  $F$  是域 (*field*).

**例** 不难看出,  $\mathbb{F}$  是域. 这也解释了为什么我们用  $\mathbb{F}$  表示  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$  之一.

**评注** 在域  $F$  里, 只要  $a \neq 0$ , 则  $a^{-1}$  有意义. 那么, 我们说  $\frac{b}{a}$  就是  $ba^{-1} = a^{-1}b$  的简写. 不难验证, 当  $a, c \neq 0$  时,

$$\begin{aligned}\frac{b}{a} &= \frac{d}{c} \iff bc = da, \\ \frac{b}{a} \pm \frac{d}{c} &= \frac{bc \pm da}{ac}, \\ \frac{b}{a} \cdot \frac{d}{c} &= \frac{bd}{ac}.\end{aligned}$$

若  $d \neq 0$ , 则

$$\frac{\frac{b}{a}}{\frac{d}{c}} = \frac{bc}{da}.$$

这就是我们熟知的分数运算法则.

**评注** 类似地, 可以定义子域 (*subfield*). 这里, 就直接用前面的等价刻画来描述它: “ $F$  的非空子集  $K$  是域  $F$  的子域的一个必要与充分条件是: (i)  $1 \in K$ ; (ii) 任取  $x, y \in K, y \neq 0$ , 必有  $x - y \in K, \frac{x}{y} \in K$ .”

**例** 设  $F \subset \mathbb{C}$ , 且  $F$  是域. 不难看出,  $\mathbb{Q} \subset F$ .

## 多项式的定义

现在开始介绍多项式.

**定义** 设  $D$  是整环. 设  $x$  是不在  $D$  里的任意一个文字. 形如

$$f(x) = a_0x^0 + a_1x^1 + \cdots + a_nx^n \quad (n \in \mathbb{N}, a_0, a_1, \cdots, a_n \in D, a_n \neq 0)$$

的表达式称为  $D$  上  $x$  的一个多项式 (*polynomial in  $x$  over  $D$* ).  $n$  称为其次 (*degree*),  $a_i$  称为其  $i$  次系数 (*the  $i^{\text{th}}$  coefficient*),  $a_ix^i$  称为其  $i$  次项 (*the  $i^{\text{th}}$  term*).  $f(x)$  的次可写为  $\deg f(x)$ .

若二个多项式的次与各同次系数均相等, 则二者相等.

多项式的系数为 0 的项可以不写.

约定  $0 \in D$  也是多项式, 称为零多项式. 零多项式的次是  $-\infty$ . 任取整数  $m$ , 约定

$$\begin{aligned} -\infty &= -\infty, & -\infty &< m, \\ -\infty + m &= m + (-\infty) = -\infty + (-\infty) = -\infty. \end{aligned}$$

当然, 还约定, 零多项式只跟自己相等. 换句话说,

$$a_0x^0 + a_1x^1 + \cdots + a_nx^n = 0$$

的一个必要与充分条件是

$$a_0 = a_1 = \cdots = a_n = 0.$$

$D$  上  $x$  的所有多项式作成的集是  $D[x]$ :

$$D[x] = \{ a_0x^0 + a_1x^1 + \cdots + a_nx^n \mid n \in \mathbb{N}, a_0, a_1, \cdots, a_n \in D \}.$$

文字  $x$  只是一个符号, 它与  $D$  的元的和与积都是形式的. 我们说,  $x$  是不定元 (*indeterminate*).

**例**  $0y^0 + 1y^1 + (-1)y^2 + 0y^3 + (-7)y^4 \in \mathbb{Z}[y]$  是一个 4 次多项式. 顺便一提, 一般把  $y^1$  写为  $y$ . 这个多项式的一个更普通的写法是

$$y - y^2 - 7y^4.$$

也许  $y^0$  看起来有些奇怪. 如上所言, 这只是一个形式上的表达式. 我们之后再处理这个小细节.

**例**  $z^0 + z + z^{\frac{3}{2}}$  不是  $z$  的多项式.

**例** 考虑  $\mathbb{Z}$  与  $\mathbb{Z}[x]$ . 设

$$f(x) = ax^0 + x + 2x^2 - x^4 - bx^5, \quad g(x) = cx + dx^2 - x^4 - 3x^5,$$

其中  $a, b, c, d$  都是整数. 那么,  $f(x) = g(x)$  相当于

$$a = 0, \quad 1 = c, \quad 2 = d, \quad 0 = 0, \quad -1 = -1, \quad -b = -3,$$

也就是

$$a = 0, \quad b = 3, \quad c = 1, \quad d = 2.$$

**评注** 文字  $x$  的意义在数学中是不断进化的 (*evolving*). 在中小学里,  $x$  是未知元 (*unknown*): 虽然它是待求的, 但是它是一个具体的数. 后来在函数里,  $x$  表示变元 (*variable*), 不过它的取值范围是确定的. 在上面的定义里,  $x$  仅仅是一个文字, 成为不定元.

下面考虑多项式的运算. 先从加法开始.

**定义** 设

$$f(x) = a_0x^0 + a_1x + \cdots + a_nx^n, \quad g(x) = b_0x^0 + b_1x + \cdots + b_nx^n$$

是  $D[x]$  的元. 规定加法如下:

$$f(x) + g(x) = (a_0 + b_0)x^0 + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n.$$

**例** 取  $\mathbb{Z}[x]$  的二个元  $f(x) = x^0 + 2x^2$ ,  $g(x) = -3x^0 + 4x - x^3$ . 先改写一下:

$$f(x) = 1x^0 + 0x + 2x^2 + 0x^3, \quad g(x) = -3x^0 + 4x + 0x^2 + (-1)x^3.$$

所以

$$f(x) + g(x) = -2x^0 + 4x + 2x^2 - x^3.$$

**命题**  $D[x]$  作成加群.

证 设

$$\begin{aligned}f(x) &= a_0x^0 + a_1x + \cdots + a_nx^n, \\g(x) &= b_0x^0 + b_1x + \cdots + b_nx^n, \\h(x) &= c_0x^0 + c_1x + \cdots + c_nx^n\end{aligned}$$

是  $D[x]$  的元. 根据加法的定义,  $+$  显然是  $D[x]$  的二元运算. 因为  $D$  的加法适合交换律, 故

$$\begin{aligned}g(x) + f(x) &= (b_0 + a_0)x^0 + (b_1 + a_1)x + \cdots + (b_n + a_n)x^n \\&= (a_0 + b_0)x^0 + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n \\&= f(x) + g(x).\end{aligned}$$

也就是说,  $D[x]$  的加法适合交换律.

注意到

$$\begin{aligned}&(f(x) + g(x)) + h(x) \\&= ((a_0 + b_0)x^0 + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n) \\&\quad + (c_0x^0 + c_1x + \cdots + c_nx^n) \\&= ((a_0 + b_0) + c_0)x^0 + ((a_1 + b_1) + c_1)x + \cdots + ((a_n + b_n) + c_n)x^n \\&= (a_0 + b_0 + c_0)x^0 + (a_1 + b_1 + c_1)x + \cdots + (a_n + b_n + c_n)x^n.\end{aligned}$$

类似地, 计算  $f(x) + (g(x) + h(x))$  也可以得到一样的结果. 也就是说,  $D[x]$  的加法适合结合律.

零多项式可以写为

$$0 = 0x^0 + 0x + \cdots + 0x^n.$$

这样

$$\begin{aligned}0 + f(x) &= (0 + a_0)x^0 + (0 + a_1)x + \cdots + (0 + a_n)x^n \\&= a_0x^0 + a_1x + \cdots + a_nx^n \\&= f(x).\end{aligned}$$

类似地,  $f(x) + 0 = f(x)$ .

记

$$\underline{f}(x) = (-a_0)x^0 + (-a_1)x + \cdots + (-a_n)x^n.$$

这样

$$\begin{aligned}\underline{f}(x) + f(x) &= (-a_0 + a_0)x^0 + (-a_1 + a_1)x + \cdots + (-a_n + a_n)x^n \\ &= 0x^0 + 0x + \cdots + 0x^n \\ &= 0.\end{aligned}$$

类似地,  $f(x) + \underline{f}(x) = 0$ . 以后, 我们把这个  $\underline{f}(x)$  用普通的符号写为

$$-f(x) = -a_0x^0 - a_1x - \cdots - a_nx^n.$$

综上,  $D[x]$  是加群.



**定义** 设  $f(x), g(x) \in D[x]$ . 规定减法如下:

$$f(x) - g(x) = f(x) + (-g(x)).$$

**评注** 可以看出,  $f(x) \pm g(x)$  的次既不会超出  $f(x)$  的次, 也不会超出  $g(x)$  的次. 用符号写出来, 就是

$$\deg(f(x) \pm g(x)) \leq \max\{\deg f(x), \deg g(x)\}.$$

若  $\deg f(x) > \deg g(x)$ , 则

$$\deg(f(x) \pm g(x)) = \deg f(x).$$

类似地, 若  $\deg f(x) < \deg g(x)$ , 则

$$\deg(f(x) \pm g(x)) = \deg g(x).$$

**评注** 既然  $D[x]$  是加群, 且每个  $a_i x^i$  ( $i = 0, 1, \dots, n$ ) 都可以看成是多项式, 那么多项式的项的次序是不重要的. 前面的写法称为升次排列 (*ascending order*). 下面的写法称为降次排列 (*descending order*):

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 x^0.$$

这跟中学里接触的多项式是一样的.

(非零) 多项式的最高次非零项是首项 (*leading term*). 它的系数是此多项式的首项系数 (*the coefficient of the leading term*).

**例**  $y - y^2 - 7y^4 \in \mathbb{Z}[x]$  可以写为  $-7y^4 - y^2 + y$ , 其首项是  $-7y^4$ , 且其首项系数是  $-7$ .

现在考虑乘法.

**定义** 设

$$f(x) = a_0x^0 + a_1x + \cdots + a_mx^m, \quad g(x) = b_0x^0 + b_1x + \cdots + b_nx^n$$

是  $D[x]$  的元. 规定乘法如下:

$$f(x)g(x) = c_0x^0 + c_1x + \cdots + c_{m+n}x^{m+n},$$

其中

$$c_k = a_0b_k + a_1b_{k-1} + \cdots + a_kb_0.$$

且约定  $i > m$  时  $a_i = 0$ ,  $j > n$  时  $b_j = 0$ . 在这个约定下, 不难看出,  $\ell > m + n$  时,  $c_\ell = 0$ . 所以, 我们至少有

$$\deg f(x)g(x) \leq \deg f(x) + \deg g(x).$$

**例** 取  $\mathbb{Z}[x]$  的二个元  $f(x) = x^0 + 2x^2$ ,  $g(x) = -3x^0 + 4x - x^3$ . 先改写一下:

$$f(x) = 1x^0 + 0x + 2x^2, \quad g(x) = -3x^0 + 4x + 0x^2 + (-1)x^3.$$

所以

$$c_0 = 1 \cdot (-3) = -3,$$

$$c_1 = 1 \cdot 4 + 0 \cdot (-3) = 4,$$

$$c_2 = 1 \cdot 0 + 0 \cdot 4 + 2 \cdot (-3) = -6,$$

$$c_3 = 1 \cdot (-1) + 0 \cdot 0 + 2 \cdot 4 = 7,$$

$$c_4 = 0 \cdot (-1) + 2 \cdot 0 = 0,$$

$$c_5 = 2 \cdot (-1) = -2.$$



所以

$$f(x)g(x) = -3x^0 + 4x - 6x^2 + 7x^3 - 2x^5.$$

**例 设**

$$f(x) = a_0x^0 + a_1x + \cdots + a_mx^m.$$

是  $D[x]$  的元. 零多项式可以写为

$$0 = 0x^0,$$

由此易知

$$0f(x) = f(x)0 = 0.$$

**评注 设**

$$f(x) = a_0x^0 + a_1x + \cdots + a_mx^m, \quad g(x) = b_0x^0 + b_1x + \cdots + b_nx^n$$

是  $D[x]$  的元, 且  $a_m \neq 0, b_n \neq 0$ . 这样,  $f(x)g(x)$  的  $m+n$  次项就是  $cx^{m+n}$ , 其中

$$\begin{aligned} c &= a_0b_{m+n} + \cdots + a_{m-1}b_{n+1} + a_mb_n + a_{m+1}b_{n-1} + \cdots + a_{m+n}b_n \\ &= 0 + \cdots + 0 + a_mb_n + 0 + \cdots + 0 \\ &= a_mb_n. \end{aligned}$$

因为  $a_m \neq 0, b_n \neq 0$ , 所以  $a_mb_n \neq 0$  (反证法: 若  $a_mb_n = 0 = a_m0$ , 因为  $a_m \neq 0$ , 根据  $D$  的消去律, 得  $b_n = 0$ , 矛盾!). 所以

$$\deg f(x)g(x) = \deg f(x) + \deg g(x).$$

可以验证, 若  $f$  或  $g$  的任意一个是 0, 这个关系也对.

**评注 设**

$$\begin{aligned} f(x) &= px^m = a_0 + a_1x + \cdots + a_mx^m, \\ g(x) &= qx^n = b_0 + b_1x + \cdots + b_nx^n. \end{aligned}$$

当  $i \neq m$  时,  $a_i = 0$ ; 当  $i = m$  时,  $a_i = p \neq 0$ . 当  $j \neq n$  时,  $b_j = 0$ ; 当  $j = n$  时,  $b_j = q \neq 0$ . 现在考虑这二个多项式的积

$$f(x)g(x) = c_0 + c_1x + \cdots + c_{m+n}x^{m+n},$$

其中

$$c_k = a_0b_k + a_1b_{k-1} + \cdots + a_kb_0.$$

我们来看什么时候  $a_\ell b_{k-\ell}$  不是 0. 这相当于要求  $a_\ell$  跟  $b_{k-\ell}$  都不是 0, 所以

$$\ell = m, \quad k - \ell = n,$$

也就是

$$\ell = m, \quad k = m + n.$$

所以, 当  $k \neq m + n$  时,  $c_k = 0$ ; 当  $k = m + n$  时,

$$c_{m+n} = a_mb_n = pq \neq 0.$$

所以, 任取  $m, n \in \mathbb{N}$ , 必有

$$(px^m)(qx^n) = (pq)x^{m+n}.$$

特别地, 取  $p = q = 1$ , 有

$$x^m x^n = x^{m+n}.$$

这里提醒读者: 这个式是形式上的表达式, 其内涵与中学的“同底数幂相乘, 底数不变, 指数相加”的内涵是不一样的!

顺便一提, 若  $p$  跟  $q$  的一个是 0, 则每个  $c_k$  全为 0, 故此时积是零多项式, 此式仍成立.

**命题**  $D[x]$  作成整环. 所以,  $D[x]$  的一个名字就是 (整环)  $D$  上  $(x)$  的多项式 (整) 环.

**证** 已经知道,  $D[x]$  是加群. 下面先说明  $D[x]$  是交换环.

根据定义, 多项式的乘法还是多项式, 也就是说, 乘法是二元运算.

设

$$f(x) = a_0x^0 + a_1x + \cdots + a_mx^m,$$

$$g(x) = b_0x^0 + b_1x + \cdots + b_nx^n,$$

$$h(x) = u_0x^0 + u_1x + \cdots + u_sx^s$$

是  $D[x]$  的元. 则

$$f(x)g(x) = c_0x^0 + c_1x + \cdots + c_{m+n}x^{m+n},$$

$$g(x)f(x) = d_0x^0 + d_1x + \cdots + d_{n+m}x^{n+m},$$

其中

$$c_k = a_0b_k + a_1b_{k-1} + \cdots + a_kb_0,$$

$$d_k = b_0a_k + b_1a_{k-1} + \cdots + b_ka_0.$$

因为  $D$  的乘法适合交换律, 加法适合交换律与结合律, 故  $c_k = d_k$ . 这样,  $D[x]$  的乘法适合交换律.

不难算出

$$\begin{aligned} & (f(x)g(x))h(x) \\ &= (c_0x^0 + c_1x + \cdots + c_{m+n}x^{m+n})(u_0x^0 + u_1x + \cdots + u_sx^s) \\ &= v_0x^0 + v_1x + \cdots + v_{m+n+s}x^{m+n+s}, \end{aligned}$$

其中

$$\begin{aligned} v_t &= (\text{the sum of all } a_ib_ju_r \text{'s with } i+j+r=t) \\ &= a_0b_0u_t + a_0b_1u_{t-1} + \cdots + a_0b_tu_0 + a_1b_0u_{t-1} + \cdots. \end{aligned}$$

类似地, 计算  $f(x)(g(x)h(x))$  也可以得到一样的结果. 也就是说,  $D[x]$  的乘法适合结合律.

现在验证分配律. 前面已经看到, 多项式的乘法是交换的, 所以只要验证一个分配律即可. 不失一般性, 设  $s = n$ . 这样

$$g(x) + h(x) = (b_0 + u_0)x^0 + (b_1 + u_1)x + \cdots + (b_n + u_n)x^n.$$

所以

$$f(x)(g(x) + h(x)) = p_0x^0 + p_1x^1 + \cdots + p_{m+n}x^{m+n},$$

其中

$$\begin{aligned} p_k &= a_0(b_k + c_k) + a_1(b_{k-1} + c_{k-1}) + \cdots + a_k(b_0 + c_0) \\ &= (a_0b_k + a_0c_k) + (a_1b_{k-1} + a_1c_{k-1}) + \cdots + (a_kb_0 + a_kc_0) \\ &= (a_0b_k + a_1b_{k-1} + \cdots + a_kb_0) + (a_0c_k + a_1c_{k-1} + \cdots + a_kc_0). \end{aligned}$$

不难看出, 这就是  $f(x)g(x)$  的  $k$  次系数与  $f(x)h(x)$  的  $k$  次系数的和. 这样,  $D[x]$  的加法与乘法适合分配律. 至此, 我们知道,  $D[x]$  是交换环.

交换环离整环还差二步: 一是乘法么元, 二是消去律. 先看消去律. 若  $f(x)g(x) = f(x)h(x)$ ,  $f(x) \neq 0$ , 根据分配律,

$$0 = f(x)g(x) - f(x)h(x) = f(x)(g(x) - h(x)).$$

如果  $g(x) - h(x) \neq 0$ , 则  $g(x) - h(x)$  的次不是  $-\infty$ .  $f(x)$  的次不是  $-\infty$ , 故  $f(x)(g(x) - h(x))$  的次不是  $-\infty$ . 换句话说,  $f(x)(g(x) - h(x)) \neq 0$ , 矛盾!

再看乘法么元. 设

$$e(x) = x^0.$$

不难算出

$$e(x)f(x) = f(x)e(x) = f(x).$$

综上,  $D[x]$  是整环.

✎

**例** 在前面, 我们直接用定义计算了下面二个多项式的积:

$$f(x) = x^0 + 2x^2, \quad g(x) = -3x^0 + 4x - x^3.$$

现在, 我们利用

$$(px^m)(qx^n) = (pq)x^{m+n} \quad (p, q \in D, m, n \in \mathbb{N})$$

与运算律再算一次:

$$\begin{aligned}
 f(x)g(x) &= (x^0 + 2x^2)(-3x^0 + 4x - x^3) \\
 &= x^0(-3x^0 + 4x - x^3) + 2x^2(-3x^0 + 4x - x^3) \\
 &= -3x^{0+0} + 4x^{0+1} - x^{0+3} - 6x^{2+0} + 8x^{2+1} - 2x^{2+3} \\
 &= -3x^0 + 4x - x^3 - 6x^2 + 8x^3 - 2x^5 \\
 &= -3x^0 + 4x - 6x^2 + 7x^3 - 2x^5.
 \end{aligned}$$

这跟之前的结果是一致的.

**定义** 设  $m \in \mathbb{N}$ . 多项式  $f(x)$  的  $m$  次幂就是  $m$  个  $f(x)$  的积:

$$(f(x))^m = \underbrace{f(x) \cdot f(x) \cdot \cdots \cdot f(x)}_{m \text{ } f(x)\text{'s}}.$$

既然  $D[x]$  是整环, 那么前面的幂规则都适用. 具体地说, 设  $m, n \in \mathbb{N}$ ,  $f(x), g(x) \in D[x]$ , 则

$$\begin{aligned}
 (f(x))^m (f(x))^n &= (f(x))^{m+n}, \\
 ((f(x))^m)^n &= (f(x))^{mn}, \\
 (f(x)g(x))^m &= (f(x))^m (g(x))^m.
 \end{aligned}$$

前面, 我们知道

$$x^m x^n = x^{m+n}.$$

当时, 我们还说, 这跟中学的“同底数幂相乘, 底数不变, 指数相加”有着不一样的内涵. 有了“幂”这个概念后, 我们发现,  $x^m$  的确可以视为  $m$  个  $x$  的积.

**评注** 以后, 我们把  $x^0$  写为 1. 换句话说, 代替

$$a_0 x^0 + a_1 x + \cdots + a_n x^n,$$

我们写

$$a_0 + a_1 x + \cdots + a_n x^n.$$

这儿还有一件事儿值得一提. 考虑

$$D_0 = \{ ax^0 \mid a \in D \} \subset D[x].$$

任取  $D_0$  的二元  $ax^0, bx^0$ . 首先,  $ax^0 = bx^0$  的一个必要与充分条件是  $a = b$ . 然后, 不难看出,

$$ax^0 + bx^0 = (a + b)x^0, \quad (ax^0)(bx^0) = (ab)x^0.$$

由此可以看出,  $D_0$  与  $D$  “几乎完全一样”. 用摩登 (*modern*) 数学的话来说, “ $D_0$  与  $D$  是天然同构的 (*naturally isomorphic*)”.

我们不打算深究这一点. 上面, 我们把  $x^0$  写为 1; 反过来,  $D$  的元  $a$  也可以理解为是多项式  $ax^0$ . 这跟中学的习惯是一致的.

最后, 我们指出: 既然非零的  $c \in D$  可视为 0 次多项式, 那么  $cf(x)$  也是多项式. 如果

$$f(x) = a_0 + a_1x + \cdots + a_nx^n,$$

那么

$$cf(x) = ca_0 + ca_1x + \cdots + ca_nx^n,$$

且

$$\deg cf(x) = \deg f(x).$$

## 带余除法

我们知道, 非负整数有这样的性质:

**命题** 设  $f$  是正整数,  $g$  是非负整数. 则必有一对非负整数  $q, r$  使

$$g = qf + r, \quad 0 \leq r < f.$$

例如, 取  $f = 5, g = 23$ . 不难看出,

$$23 = 4 \cdot 5 + 3.$$

多项式也有类似的性质哟.

**命题** 设

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in D[x],$$

且  $a_n$  是  $D$  的单位. 对任意  $g(x) \in D[x]$ , 存在  $q(x), r(x) \in D[x]$  使

$$g(x) = q(x)f(x) + r(x), \quad \deg r(x) < n.$$

一般称其为带余除法:  $q(x)$  就是商 (*quotient*);  $r(x)$  就是余式 (*remainder*).

**证** 用数学归纳法. 记  $\deg g(x) = m$ . 若  $m < n$ , 则  $q(x) = 0, r(x) = g(x)$  适合要求. 所以, 命题对不高于  $n-1$  的  $m$  都成立.

设  $m \leq \ell$  ( $\ell \geq n-1$ ) 时, 命题成立. 考虑  $m = \ell + 1$  的情形. 此时, 设

$$g(x) = b_{\ell+1} x^{\ell} + b_{\ell} x^{\ell} + \cdots + b_0 \in D[x].$$

作一个跟  $g(x)$  有着共同首项的多项式:

$$\begin{aligned} s(x) &= b_{\ell+1} a_n^{-1} x^{\ell+1-n} f(x) \\ &= b_{\ell+1} a_n^{-1} x^{\ell+1-n} (a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0) \\ &= b_{\ell+1} a_n^{-1} (a_n x^{\ell+1} + a_{n-1} x^{\ell} + \cdots + a_0 x^{\ell+1-n}) \\ &= b_{\ell+1} (x^{\ell+1} + a_n^{-1} a_{n-1} x^{\ell} + \cdots + a_n^{-1} a_0 x^{\ell+1-n}) \\ &= b_{\ell+1} x^{\ell+1} + b_{\ell+1} a_n^{-1} a_{n-1} x^{\ell} + \cdots + b_{\ell+1} a_n^{-1} a_0 x^{\ell+1-n}. \end{aligned}$$

因为  $a_n$  是单位, 故  $s(x) \in D[x]$ . 设  $r_1(x) = g(x) - s(x) \in D[x]$ . 这样,  $r_1(x)$  的次不高于  $\ell$ . 根据归纳假设, 有  $q_2(x), r_2(x) \in D[x]$  使

$$r_1(x) = q_2(x)f(x) + r_2(x), \quad \deg r_2(x) < n.$$

所以

$$\begin{aligned} g(x) &= b_{\ell+1}a_n^{-1}x^{\ell+1-n}f(x) + r_1(x) \\ &= b_{\ell+1}a_n^{-1}x^{\ell+1-n}f(x) + q_2(x)f(x) + r_2(x) \\ &= (b_{\ell+1}a_n^{-1}x^{\ell+1-n} + q_2(x))f(x) + r_2(x). \end{aligned}$$

记  $q(x) = b_{\ell+1}a_n^{-1}x^{\ell+1-n} + q_2(x)$ ,  $r(x) = r_2(x)$ , 则  $q(x), r(x)$  符合要求. 所以,  $m \leq \ell + 1$  时, 命题成立. 根据数学归纳法, 命题成立.  $\clubsuit$

**例** 取  $\mathbb{F}[x]$  的二元  $f(x) = 2(x-1)^2(x+2)$ ,  $g(x) = 8x^6 + 1$ . 我们来找一对多项式  $q(x), r(x) \in \mathbb{F}[x]$  使

$$g(x) = q(x)f(x) + r(x), \quad \deg r(x) < \deg f(x).$$

不难看出,  $f(x)$  的次是 3, 且

$$f(x) = 2(x^2 - 2x + 1)(x + 2) = 2x^3 - 6x + 4.$$

我们按上面证明的方法寻找  $q(x)$  与  $r(x)$ .  $a_3 = 2$  是  $\mathbb{F}$  的单位, 且  $a_3^{-1} = \frac{1}{2}$ . 取

$$q_1(x) = 8 \cdot \frac{1}{2} \cdot x^{6-3} = 4x^3.$$

则

$$\begin{aligned} r_1(x) &= g(x) - q_1(x)f(x) \\ &= (8x^6 + 1) - 4x^3(2x^3 - 6x + 4) \\ &= (8x^6 + 1) - (8x^6 - 24x^4 + 16x^3) \\ &= 24x^4 - 16x^3 + 1. \end{aligned}$$

$r_1(x)$  的次仍不低于 3. 因此, 再来一次. 取

$$q_2(x) = 24 \cdot \frac{1}{2} \cdot x^{4-3} = 12x.$$



则

$$\begin{aligned}
 r_2(x) &= r_1(x) - q_2(x)f(x) \\
 &= (24x^4 - 16x^3 + 1) - 12x(2x^3 - 6x + 4) \\
 &= (24x^4 - 16x^3 + 1) - (24x^4 - 72x + 48x) \\
 &= -16x^3 + 72x^2 - 48x + 1.
 \end{aligned}$$

$r_2(x)$  的次仍不低于 3. 因此, 再来一次. 取

$$q_3(x) = -16 \cdot \frac{1}{2} \cdot x^{3-3} = -8.$$

则

$$\begin{aligned}
 r_3(x) &= r_2(x) - q_3(x)f(x) \\
 &= (-16x^3 + 72x^2 - 48x + 1) - (-8)(2x^3 - 6x + 4) \\
 &= (-16x^3 + 72x^2 - 48x + 1) - (-16x^3 + 48x - 32) \\
 &= 72x^2 - 96x + 33.
 \end{aligned}$$

$r_3(x)$  的次低于 3. 这样

$$\begin{aligned}
 g(x) &= q_1(x)f(x) + r_1(x) \\
 &= q_1(x)f(x) + q_2(x)f(x) + r_2(x) \\
 &= q_1(x)f(x) + q_2(x)f(x) + q_3(x)f(x) + r_3(x) \\
 &= (q_1(x) + q_2(x) + q_3(x))f(x) + r_3(x) \\
 &= (4x^3 + 12x - 8)f(x) + (72x^2 - 96x + 33).
 \end{aligned}$$

也就是说,

$$q(x) = 4x^3 + 12x - 8, \quad r(x) = 72x^2 - 96x + 33.$$

**评注** 带余除法要求  $f(x)$  的首项系数是单位是有必要的.

在上面的例里,  $f(x)$  与  $g(x)$  可以看成  $\mathbb{Z}[x]$  的元, 但 2 不是  $\mathbb{Z}$  的单位. 虽然最终所得  $q(x)$ ,  $r(x)$  也是  $\mathbb{Z}[x]$  的元, 但这并不是一定会出现的. 我们看下面的简单例.

考虑  $\mathbb{Z}[x]$  的多项式  $f(x) = 2x$ . 设

$$\begin{aligned} r(x) &= r_0, \\ q(x) &= q_0 + q_1x + \cdots + q_px^p, \\ g(x) &= g_0 + g_1x + \cdots + g_sx^s, \end{aligned}$$

且  $r_0, q_0, \dots, q_p, g_0, \dots, g_s \in \mathbb{Z}$ ,  $q_p, g_s \neq 0$ . 若  $g(x) = q(x)f(x) + r(x)$ , 则

$$g_0 + g_1x + \cdots + g_sx^s = r_0 + 2q_0x + 2q_1x^2 + \cdots + 2q_px^{p+1}.$$

所以

$$\begin{aligned} p &= s - 1, \\ r_0 &= g_0, \\ 2q_{i-1} &= g_i, \quad i = 1, \dots, s. \end{aligned}$$

这说明,  $g(x)$  的  $i$  项系数 ( $i = 1, \dots, s$ ) 必须是偶数. 所以, 不存在  $q(x), r(x) \in \mathbb{Z}[x]$  使

$$1 + 3x + x^2 = q(x) \cdot 2x + r(x), \quad \deg r(x) < 1.$$

我们知道, 用一个正整数除<sup>†</sup>非负整数, 所得的余数与商是唯一的. 比方说, 5 除 23 的余数只能是 3.

多项式也有类似的性质哟. 不过, 我们需要借助另一个命题的帮助.

**命题** 设  $f(x) \in D[x]$ , 且  $f(x) \neq 0$ . 若  $D$  上  $x$  的 2 个多项式  $q(x), r(x)$  适合

$$q(x)f(x) + r(x) = 0, \quad \deg r(x) < \deg f(x),$$

则必有

$$q(x) = r(x) = 0.$$

通俗地说, 二个非零多项式的积的次不可能变低.

---

<sup>†</sup>  $f$  除  $g$  意味着  $g$  除以  $f$ , 也就是  $g \div f$ .

**证** 题设条件即

$$-q(x)f(x) = r(x).$$

反证法. 若  $-q(x) \neq 0$ , 则  $\deg(-q(x)) \geq 0$ . 从而

$$\deg r(x) = \deg(-q(x)) + \deg f(x) \geq \deg f(x).$$

可是,

$$\deg r(x) < \deg f(x),$$

矛盾! 故  $-q(x) = 0$ . 这样,  $r(x) = 0$ . ✎

**命题** 设  $f(x) \in D[x]$ , 且  $f(x) \neq 0$ . 若  $D$  上  $x$  的 4 个多项式  $q_1(x)$ ,  $r_1(x)$ ,  $q_2(x)$ ,  $r_2(x)$  适合

$$q_1(x)f(x) + r_1(x) = q_2(x)f(x) + r_2(x),$$

$$\deg r_1(x) < \deg f(x), \quad \deg r_2(x) < \deg f(x),$$

则必有

$$q_1(x) = q_2(x), \quad r_1(x) = r_2(x).$$

**证** 记

$$Q(x) = q_1(x) - q_2(x), \quad R(x) = r_1(x) - r_2(x).$$

题设条件即

$$(q_1(x) - q_2(x))f(x) + (r_1(x) - r_2(x)) = 0,$$

也就是

$$Q(x)f(x) + R(x) = 0.$$

注意到

$$\begin{aligned} \deg R(x) &= \deg(r_1(x) - r_2(x)) \\ &\leq \max\{\deg r_1(x), \deg r_2(x)\} \\ &< \deg f(x). \end{aligned}$$

根据上个命题,  $Q(x) = R(x) = 0$ . 所以

$$q_1(x) = q_2(x), \quad r_1(x) = r_2(x). \quad \text{✎}$$

这样, 我们得到了这个命题:

**命题** 设

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in D[x],$$

且  $a_n$  是  $D$  的单位. 对任意  $g(x) \in D[x]$ , 存在唯一的  $q(x), r(x) \in D[x]$  使

$$g(x) = q(x)f(x) + r(x), \quad \deg r(x) < n.$$

一般称其为带余除法:  $q(x)$  就是商;  $r(x)$  就是余式. 并且, 当  $f(x)$  的次不高于  $g(x)$  的次时,  $f(x), g(x), q(x)$  间还有如下的次关系:

$$\deg g(x) = \deg(g(x) - r(x)) = \deg q(x) + \deg f(x).$$

## 多项式的相等

本节讨论二个多项式的相等.

设  $a_0, b_0, a_1, b_1, \dots, a_n, b_n$  都是整环  $D$  的元. 根据定义, 我们已经知道,

$$a_0 + a_1x + \dots + a_nx^n = b_0 + b_1x + \dots + b_nx^n$$

的一个必要与充分条件是

$$a_0 = b_0, \quad a_1 = b_1, \quad \dots, \quad a_n = b_n.$$

之后, 我们会遇到形如

$$f(x) = a_0 + a_1(x-c) + a_2(x-c)^2 + \dots + a_n(x-c)^n$$

的式, 这里  $c \in D$ . 因为

$$1, \quad x-c, \quad (x-c)^2, \quad \dots, \quad (x-c)^n$$

是首项系数为 1 的 0, 1, 2,  $\dots$ ,  $n$  次多项式, 所以这个  $f(x)$  也是多项式, 且  $\deg f(x) \leq n$ . 当  $a_n \neq 0$  时,  $\deg f(x) = n$ , 且  $f(x)$  的首项系数为  $a_n$ .

再作一个多项式

$$g(x) = b_0 + b_1(x-c) + b_2(x-c)^2 + \dots + b_n(x-c)^n.$$

$f(x)$  与  $g(x)$  都是多项式, 自然可以讨论是否相等. 若  $c = 0$ ,  $(x-c)^\ell$  就变为普通的  $x^\ell$ . 所以,  $c = 0$  时,  $f(x) = g(x)$  的一个必要与充分条件是

$$a_0 = b_0, \quad a_1 = b_1, \quad \dots, \quad a_n = b_n.$$

可是, 如果  $c \neq 0$  呢? 这个时候, 还是一样的条件吗?

先看一个例.

**例** 我们试研究

$$(\star) \quad a_0 + a_1(x-c) + a_2(x-c)^2 = b_0 + b_1(x-c) + b_2(x-c)^2.$$

在中学, 我们已经知道

$$(x-c)^2 = c^2 - 2cx + x^2.$$

这样, (★) 的左侧变为

$$\begin{aligned}
 & a_0 + a_1(x - c) + a_2(x - c)^2 \\
 &= a_0 + a_1(-c + x) + a_2(c^2 - 2cx + x^2) \\
 &= a_0 + (-a_1c + a_1x) + (a_2c^2 + (-2a_2c)x + a_2x^2) \\
 &= (a_0 - a_1c + a_2c^2) + (a_1 - 2a_2c)x + a_2x^2.
 \end{aligned}$$

同理, (★) 的右侧变为

$$(b_0 - b_1c + b_2c^2) + (b_1 - 2b_2c)x + b_2x^2.$$

所以, (★) 成立等价于

$$\begin{aligned}
 a_0 - a_1c + a_2c^2 &= b_0 - b_1c + b_2c^2, \\
 a_1 - 2a_2c &= b_1 - 2b_2c, \\
 a_2 &= b_2,
 \end{aligned}$$

即

$$\begin{aligned}
 (a_0 - b_0) - c(a_1 - b_1) + c^2(a_2 - b_2) &= 0, \\
 (a_1 - b_1) - 2c(a_2 - b_2) &= 0, \\
 (a_2 - b_2) &= 0.
 \end{aligned}$$

由这个方程组, 可解出

$$a_0 - b_0 = a_1 - b_1 = a_2 - b_2 = 0.$$

这跟  $c = 0$  时的

$$a_0 = b_0, \quad a_1 = b_1, \quad a_2 = b_2$$

是完全一致的.

**定义** 设  $p_0(x), p_1(x), \dots, p_n(x) \in D[x]$ . 设  $c_0, c_1, \dots, c_n \in D$ . 我们说

$$c_0p_0(x) + c_1p_1(x) + \dots + c_np_n(x)$$

是多项式  $p_0(x), p_1(x), \dots, p_n(x)$  的一个线性组合 (*linear combination*).  $c_0, c_1, \dots, c_n$  就是此线性组合的系数.

若不存在一组不全为 0 的  $D$  中元  $d_0, d_1, \dots, d_n$  使

$$d_0 p_0(x) + d_1 p_1(x) + \dots + d_n p_n(x) = 0,$$

则说  $p_0(x), p_1(x), \dots, p_n(x)$  是线性无关的 (*linearly independent*). 换句话说, “ $p_0(x), p_1(x), \dots, p_n(x)$  是线性无关的” 意味着: 若  $D$  中元  $r_0, r_1, \dots, r_n$  使

$$r_0 p_0(x) + r_1 p_1(x) + \dots + r_n p_n(x) = 0,$$

则  $r_0 = r_1 = \dots = r_n = 0$ .

**例** 显然,  $1, x, \dots, x^n$  是线性无关的. 当然, 前面的例告诉我们,  $1, x-c, (x-c)^2$  也是线性无关的.

**例** 单独一个非零多项式是线性无关的.

**评注** 设  $p_0(x), p_1(x), \dots, p_n(x)$  是线性无关的.

(i) 显然, 因为多项式的加法可交换, 随意打乱这  $n+1$  个多项式的次序后得到的多项式仍线性无关.

(ii) 对任意  $\ell$  ( $0 \leq \ell \leq n$ ),  $p_0(x), p_1(x), \dots, p_\ell(x)$  这  $\ell+1$  个多项式也是线性无关的. 设  $c_0, c_1, \dots, c_\ell \in D$ , 且

$$c_0 p_0(x) + c_1 p_1(x) + \dots + c_\ell p_\ell(x) = 0.$$

这个相当于

$$c_0 p_0(x) + c_1 p_1(x) + \dots + c_\ell p_\ell(x) + 0 p_{\ell+1}(x) + \dots + 0 p_n(x) = 0.$$

所以

$$c_0 = c_1 = \dots = c_\ell = \underbrace{0 = \dots = 0}_{(n-\ell) \text{ 0's}} = 0.$$

(iii) 根据 (i) (ii) 可知, 线性无关的多项式的片段也是线性无关的.

**评注** 设  $p_0(x), p_1(x), \dots, p_n(x)$  是线性无关的. 设  $a_0, b_0, a_1, b_1, \dots, a_n, b_n$  都是  $D$  的元. 那么

$$a_0 p_0(x) + a_1 p_1(x) + \dots + a_n p_n(x) = b_0 p_0(x) + b_1 p_1(x) + \dots + b_n p_n(x)$$

相当于

$$(a_0 - b_0)p_0(x) + (a_1 - b_1)p_1(x) + \dots + (a_n - b_n)p_n(x) = 0,$$

也就是

$$a_0 - b_0 = a_1 - b_1 = \dots = a_n - b_n = 0,$$

亦即

$$a_0 = b_0, \quad a_1 = b_1, \quad \dots, \quad a_n = b_n.$$

由此可见, 线性无关的多项式有着优良的性质: 二个线性组合相等的一个必要与充分条件是对应的系数相等.

我们知道,  $1, x, \dots, x^n$  是线性无关的. 在这串多项式里, 后一个的次比前一个的次多 1. 不仅如此, 由多项式的定义可见, 每一个次不高于  $n$  的多项式都可以写为它们的线性组合. 下面的命题就是这二件事实的推广.

**命题** 设  $p_0(x), p_1(x), \dots, p_n(x) \in D[x]$  分别是  $0, 1, \dots, n$  次多项式. 则:

- (i)  $p_0(x), p_1(x), \dots, p_n(x)$  是线性无关的;
- (ii) 若  $p_0(x), p_1(x), \dots, p_n(x)$  的首项系数都是  $D$  的单位, 则任意次不高于  $n$  的多项式都可写为  $p_0(x), p_1(x), \dots, p_n(x)$  的线性组合. 由 (i) 知, 这个组合的系数一定是唯一的.

**证** (i) 用数学归纳法. 当  $n = 0$  时, 只有一个 0 次多项式  $p_0(x) = c \neq 0$  那么, 由  $dc = 0$  可推出  $d = 0$ . 这样, 命题对  $n = 0$  成立. 假定命题对  $n = \ell \geq 0$  成立. 设  $c_0, c_1, \dots, c_{\ell+1} \in D$  使

$$c_0 p_0(x) + c_1 p_1(x) + \dots + c_\ell p_\ell(x) + c_{\ell+1} p_{\ell+1}(x) = 0.$$



记

$$r(x) = c_0 p_0(x) + c_1 p_1(x) + \cdots + c_\ell p_\ell(x),$$

则  $r(x)$  的次不高于  $\ell$ . 所以

$$c_{\ell+1} p_{\ell+1}(x) + r(x) = 0, \quad \deg r(x) \leq \ell < \deg p_{\ell+1}(x).$$

由上节命题知

$$c_{\ell+1} = 0, \quad r(x) = 0.$$

根据归纳假设,

$$r(x) = c_0 p_0(x) + c_1 p_1(x) + \cdots + c_\ell p_\ell(x) = 0 \implies c_0 = c_1 = \cdots = c_\ell = 0.$$

这样,

$$c_0 = c_1 = \cdots = c_\ell = c_{\ell+1} = 0.$$

也就是说,  $n = \ell + 1$  时, 命题成立.

(ii) 用数学归纳法. 当  $n = 0$  时, 只有一个 0 次多项式  $p_0(x) = c \neq 0$ , 且  $c$  是单位. 任取次不高于 0 的多项式  $d$ . 因为  $d = (dc^{-1})c$ , 这样, 命题对  $n = 0$  成立. 这样, 命题对  $n = 0$  成立. 假定命题对  $n = \ell \geq 0$  成立. 任取次不高于  $\ell + 1$  的多项式  $f(x)$ . 由于  $p_{\ell+1}(x)$  的首项系数是单位, 所以, 由带余除法知道, 存在多项式  $q(x), r(x) \in D[x]$  使

$$f(x) = q(x)p_{\ell+1}(x) + r(x), \quad \deg r(x) \leq \ell.$$

如果  $f(x)$  的次不高于  $\ell$ , 则  $q(x) = 0$ ; 如果  $f(x)$  的次是  $\ell + 1$ , 则

$$\deg q(x) = \deg f(x) - \deg p_{\ell+1}(x) = 0.$$

也就是说, 存在  $c_{\ell+1} \in D$  使  $q(x) = c_{\ell+1}$ . 所以

$$f(x) = r(x) + c_{\ell+1} p_{\ell+1}(x), \quad \deg r(x) \leq \ell.$$

根据归纳假设, 存在  $c_0, c_1, \dots, c_\ell \in D$  使

$$r(x) = c_0 p_0(x) + c_1 p_1(x) + \cdots + c_\ell p_\ell(x),$$

即

$$f(x) = c_0 p_0(x) + c_1 p_1(x) + \cdots + c_\ell p_\ell(x) + c_{\ell+1} p_{\ell+1}(x).$$

所以,  $n = \ell + 1$  时, 命题成立. ✎

**评注** 这里, (ii) 要求每个多项式的首项系数为单位是有必要的. 考虑  $\mathbb{Z}$  与  $\mathbb{Z}[x]$ . 取  $n = 2$ , 及

$$p_0(x) = -1, \quad p_1(x) = 2x, \quad p_2(x) = 3x^2.$$

根据上面的命题, 这三个多项式是线性无关的. 考虑  $f(x) = 3 + x - 2x^2$ . 设  $c_0, c_1, c_2 \in \mathbb{Z}$  使

$$3 + x - 2x^2 = c_0 \cdot (-1) + c_1 \cdot 2x + c_2 \cdot 3x^2.$$

这相当于

$$3 = -c_0, \quad 1 = 2c_1, \quad -2 = 3c_2.$$

容易看出, 这个方程组无整数解, 所以  $p_0(x), p_1(x), p_2(x)$  的 (系数为  $\mathbb{Z}$  的元的) 线性组合不能表示每一个次不高于 2 的多项式.

**评注** 不难看出,  $1, x^2, x^3$  线性无关. 可是, 它们不能表示每一个次不高于 3 的多项式, 因为其线性组合

$$c_0 + c_1 x^2 + c_2 x^3, \quad c_0, c_1, c_2 \in D$$

的 1 次系数总是 0. 所以, 最简单的 1 次式  $x$  无法用  $1, x^2, x^3$  的线性组合表出.

设  $p_0(x), p_1(x), \cdots, p_n(x)$  线性无关. 设这些多项式的次的最大值为  $d$ :

$$d = \max\{\deg p_0(x), \deg p_1(x), \cdots, \deg p_n(x)\}.$$

在什么条件下, 其线性组合能表示每一个次不高于  $d$  的多项式? 上面的命题给出了部分的解答. 为什么说它是“部分的解答”呢? 考虑  $\mathbb{Z}[x]$  的二个 1 次多项式

$$p_0(x) = 3 - 7x, \quad p_1(x) = -2 + 5x.$$

读者可验证, 这二个多项式线性无关. 由于

$$1 = 5p_0(x) + 7p_1(x), \quad x = 2p_0(x) + 3p_1(x),$$

故每一个次不高于 1 的多项式都可写为  $p_0(x)$  与  $p_1(x)$  的线性组合.

这个问题的详细讨论将超出本文的范围. 读者也许可在线性代数中找到破解此问题的方法.

本节开头的问题总算得到了解答. 不仅如此, 我们得到了更深的结论:

**命题** 设  $a_0, b_0, a_1, b_1, \dots, a_n, b_n$  都是  $D$  的元. 设  $c \in D$ . 再设

$$\begin{aligned} f(x) &= a_0 + a_1(x-c) + a_2(x-c)^2 + \dots + a_n(x-c)^n, \\ g(x) &= b_0 + b_1(x-c) + b_2(x-c)^2 + \dots + b_n(x-c)^n. \end{aligned}$$

则  $f(x) = g(x)$  的一个必要与充分条件是

$$a_0 = b_0, \quad a_1 = b_1, \quad \dots, \quad a_n = b_n.$$

并且, 任取

$$f(x) = u_0 + u_1x + u_2x^2 + \dots + u_nx^n \in D[x],$$

必存在  $v_0, v_1, \dots, v_n \in D$  使

$$f(x) = v_0 + v_1(x-c) + v_2(x-c)^2 + \dots + v_n(x-c)^n.$$

## 微商

本节讨论多项式的微商.

在本节, 我们会将一些容易证明的命题留给读者练习. 读者可乘此机会让自己熟悉证明命题的过程与数学归纳法.

**定义** 设

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + a_nx^n \in D[x].$$

$f(x)$  的微商 (*derivative*) 是多项式

$$f'(x) = 0 + 1a_1 + 2a_2x + \cdots + (n-1)a_{n-1}x^{n-2} + na_nx^{n-1} \in D[x].$$

$f'(x)$  也可写为  $(f(x))'$ .

**评注** 整环  $D$  里不一定有名为  $\pm 2, \pm 3, \dots$  的元. 回忆一下, 若  $a \in D$ ,  $n \in \mathbb{N}$ , 则

$$na = n \cdot a = \underbrace{a + a + \cdots + a}_{n \text{ a's}}.$$

若  $-n \in \mathbb{N}$ , 则

$$na = -((-n)a).$$

当然, 在  $\mathbb{Z}$  (或  $\mathbb{F}$ ) 里,  $na$  可以认为是  $\mathbb{Z}$  (或  $\mathbb{F}$ ) 的二个元  $n$  与  $a$  的积.

**例** 取  $f(x) = x^6 - x^3 + 1 \in D[x]$ . 若  $D = \mathbb{F}$ , 则

$$f'(x) = 6x^5 - 3x^2 + 0 = 6x^5 - 3x^2.$$

若  $D$  是 4 元集  $V$ , 则

$$f'(x) = (6 \cdot 1)x^5 + (3 \cdot (-1))x^2 + 0 = x^2.$$

这里,  $V = \{0, 1, \tau, \tau^2\}$ . 它的加法与乘法如下:

+	0	1	$\tau$	$\tau^2$	$\cdot$	0	1	$\tau$	$\tau^2$
0	0	1	$\tau$	$\tau^2$	0	0	0	0	0
1	1	0	$\tau^2$	$\tau$	1	0	1	$\tau$	$\tau^2$
$\tau$	$\tau$	$\tau^2$	0	1	$\tau$	0	$\tau$	$\tau^2$	1
$\tau^2$	$\tau^2$	$\tau$	1	0	$\tau^2$	0	$\tau^2$	1	$\tau$

在前面 (“预备知识” 节的 “整环” 小节), 我们知道,  $V$  是整环. 任取  $a \in V$ , 都有

$$2 \cdot a = a + a = 0.$$

所以  $a = -a$ . 这样,

$$6 \cdot 1 = 2 \cdot (3 \cdot 1) = (3 \cdot 1) + (3 \cdot 1) = 0,$$

$$3 \cdot (-1) = (-1) + (-1) + (-1) = 1 + 1 + 1 = 0 + 1 = 1.$$

所以, 当我们把  $f(x)$  视为  $V[x]$  中元时, 它的微商 “有点奇怪”. 同样的道理, 在  $V$  与  $V[x]$  中,

$$(x^{2k})' = (2k \cdot 1)x^{2k-1} = 0x^{2k-1} = 0.$$

**评注** 微商就是  $D[x]$  到  $D[x]$  的函数 (也就是  $D[x]$  的变换):

$$': D[x] \rightarrow D[x],$$

$$a_0 + a_1x + \cdots + a_nx^n \mapsto a_1 + 2a_2x + \cdots + na_nx^{n-1}.$$

**定义** 设

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

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

为  $D[x]$  中的二个元. 我们称

$$(g \circ f)(x) = g(f(x)) = b_0 + b_1f(x) + \cdots + b_n(f(x))^n$$

为  $f(x)$  与  $g(x)$  的复合 (*composition*).

**评注** 可以看到,  $f(x)$  与  $g(x)$  的复合仍为多项式. 设

$$h(x) = d_0 + d_1x + \cdots + d_sx^s \in D[x].$$

记

$$\begin{aligned} \ell(x) &= (h \circ g)(x) \\ &= d_0 + d_1(b_0 + b_1x + \cdots + b_nx^n) + \cdots \\ &\quad + d_s(b_0 + b_1x + \cdots + b_nx^n)^s, \end{aligned}$$

则

$$\begin{aligned}
 ((h \circ g) \circ f)(x) &= (\ell \circ f)(x) \\
 &= d_0 + d_1(b_0 + b_1f(x) + \cdots + b_n(f(x))^n) + \cdots \\
 &\quad + d_s(b_0 + b_1f(x) + \cdots + b_n(f(x))^n)^s \\
 &= d_0 + d_1(g \circ f)(x) + \cdots + d_s((g \circ f)(x))^s \\
 &= (h \circ (g \circ f))(x).
 \end{aligned}$$

换句话说, 多项式的复合适合结合律.

**例 取**

$$g(x) = b_0 + b_1x + \cdots + b_nx^n, \quad f(x) = x - c \in D[x].$$

那么

$$\begin{aligned}
 (g \circ f)(x) &= g(f(x)) = b_0 + b_1(x - c) + \cdots + b_n(x - c)^n, \\
 (f \circ g)(x) &= f(g(x)) = -c + b_0 + b_1x + \cdots + b_nx^n.
 \end{aligned}$$

这表明: 多项式的复合一般不交换.

下面的命题相当显然了.

**命题** 设  $f(x), g(x), h(x) \in D[x]$ .

(i) 设  $p(x) = f(x) + g(x)$ . 则

$$p(h(x)) = f(h(x)) + g(h(x)).$$

(ii) 设  $q(x) = f(x)g(x)$ . 则

$$q(h(x)) = f(h(x))g(h(x)).$$

**证 设**

$$\begin{aligned}
 f(x) &= a_0 + a_1x + \cdots + a_nx^n, \\
 g(x) &= b_0 + b_1x + \cdots + b_nx^n
 \end{aligned}$$

是  $D[x]$  中二个元. 这样,

$$\begin{aligned} f(h(x)) &= a_0 + a_1 h(x) + \cdots + a_n (h(x))^n, \\ g(h(x)) &= b_0 + b_1 h(x) + \cdots + b_n (h(x))^n. \end{aligned}$$

(i) 根据加法的定义, 有

$$p(x) = f(x) + g(x) = c_0 + c_1 x + \cdots + c_n x^n,$$

其中

$$c_i = a_i + b_i, \quad i = 0, 1, \cdots, n.$$

所以

$$p(h(x)) = c_0 + c_1 h(x) + \cdots + c_n (h(x))^n.$$

根据多项式的运算律, 有

$$\begin{aligned} & f(h(x)) + g(h(x)) \\ &= (a_0 + a_1 h(x) + \cdots + a_n (h(x))^n) + (b_0 + b_1 h(x) + \cdots + b_n (h(x))^n) \\ &= (a_0 + b_0) + (a_1 + b_1) h(x) + \cdots + (a_n + b_n) (h(x))^n \\ &= c_0 + c_1 h(x) + \cdots + c_n (h(x))^n \\ &= p(h(x)). \end{aligned}$$

(ii) 根据乘法的定义, 有

$$q(x) = f(x)g(x) = d_0 + d_1 x + \cdots + d_{2n} x^{2n},$$

其中

$$d_i = a_0 b_i + a_1 b_{i-1} + \cdots + a_i b_0, \quad i = 0, 1, \cdots, 2n.$$

所以

$$q(h(x)) = d_0 + d_1 h(x) + \cdots + d_{2n} (h(x))^{2n}.$$

根据多项式的运算律, 有

$$\begin{aligned}
 & f(h(x))g(h(x)) \\
 &= (a_0 + a_1h(x) + \cdots + a_n(h(x))^n)(b_0 + b_1h(x) + \cdots + b_n(h(x))^n) \\
 &= (a_0b_0) + (a_0b_1 + a_1b_0)h(x) + \cdots + (a_nb_n)(h(x))^{2n} \\
 &= (a_0b_0) + (a_0b_1 + a_1b_0)h(x) + \cdots + (a_0b_{2n} + a_1b_{2n-1} + \cdots + a_nb_n \\
 &\quad + a_{n+1}b_{n-1} + \cdots + a_{2n}b_0)(h(x))^{2n} \\
 &= c_0 + c_1h(x) + \cdots + c_{2n}(h(x))^{2n} \\
 &= q(h(x)).
 \end{aligned}$$

☺

**例** 考虑  $\mathbb{Z}$  与  $\mathbb{Z}[x]$ . 取

$$f(x) = x^3 + 2, \quad g(x) = x^2 + x - 1.$$

不难得到

$$f'(x) = 3x^2, \quad g'(x) = 2x + 1.$$

(i)  $4g(x)$  也是多项式, 当然可以有微商. 因为

$$4g(x) = 4x^2 + 4x - 4,$$

故

$$(4g(x))' = 8x + 4,$$

这刚好是  $4g'(x)$ :

$$4g'(x) = 4(2x + 1) = 8x + 4.$$

(ii)  $f(x) + g(x)$  也是多项式. 因为

$$f(x) + g(x) = x^3 + 2 + x^2 + x - 1 = x^3 + x^2 + x + 1,$$

故

$$(f(x) + g(x))' = 3x^2 + 2x + 1,$$

而这刚好是  $f'(x) + g'(x)$ :

$$f'(x) + g'(x) = 3x^2 + 2x + 1.$$



一般地, 我们有

**命题** 设  $f(x), g(x) \in D[x], c \in D$ . 则

$$(i) (cf(x))' = cf'(x);$$

$$(ii) (f(x) \pm g(x))' = f'(x) \pm g'(x).$$

由 (i) (ii) 与数学归纳法可知: 当  $c_0, c_1, \dots, c_{k-1} \in D$ , 且  $f_0(x), f_1(x), \dots, f_{k-1}(x) \in D[x]$  时,

$$\begin{aligned} & (c_0f_0(x) + c_1f_1(x) + \dots + c_{k-1}f_{k-1}(x))' \\ &= c_0f'_0(x) + c_1f'_1(x) + \dots + c_{k-1}f'_{k-1}(x). \end{aligned}$$

**证** 我们证明 (i) (ii), 将剩下的推论留给读者作练习. 设

$$\begin{aligned} f(x) &= a_0 + a_1x + a_2x^2 + \dots + a_{n-1}x^{n-1} + a_nx^n, \\ g(x) &= b_0 + b_1x + b_2x^2 + \dots + b_{n-1}x^{n-1} + b_nx^n \end{aligned}$$

是  $D[x]$  中二个元.

(i)  $cf(x)$  就是多项式

$$ca_0 + ca_1x + ca_2x^2 + \dots + ca_{n-1}x^{n-1} + ca_nx^n,$$

故

$$\begin{aligned} (cf(x))' &= (ca_0 + ca_1x + ca_2x^2 + \dots + ca_{n-1}x^{n-1} + ca_nx^n)' \\ &= ca_1 + 2ca_2x + \dots + (n-1)ca_{n-1}x^{n-2} + nca_nx^{n-1} \\ &= ca_1 + c2a_2x + \dots + c(n-1)a_{n-1}x^{n-2} + cna_nx^{n-1} \\ &= c(a_1 + 2a_2x + \dots + (n-1)a_{n-1}x^{n-2} + na_nx^{n-1}) \\ &= cf'(x). \end{aligned}$$

(ii)  $f(x) \pm g(x)$  就是多项式

$$\begin{aligned} & (a_0 \pm b_0) + (a_1 \pm b_1)x + (a_2 \pm b_2)x^2 + \dots \\ &+ (a_{n-1} \pm b_{n-1})x^{n-1} + (a_n \pm b_n)x^n, \end{aligned}$$

故

$$\begin{aligned}
 & (f(x) \pm g(x))' \\
 &= ((a_0 \pm b_0) + (a_1 \pm b_1)x + (a_2 \pm b_2)x^2 + \cdots \\
 &\quad + (a_{n-1} \pm b_{n-1})x^{n-1} + (a_n \pm b_n)x^n)' \\
 &= (a_1 \pm b_1) + 2(a_2 \pm b_2)x + \cdots + (n-1)(a_{n-1} \pm b_{n-1})x^{n-2} \\
 &\quad + n(a_n \pm b_n)x^{n-1} \\
 &= (a_1 \pm b_1) + (2a_2x \pm 2b_2x) + \cdots + ((n-1)a_{n-1}x^{n-2} \\
 &\quad \pm (n-1)b_{n-1}x^{n-2}) + (na_nx^{n-1} \pm nb_nx^{n-1}) \\
 &= (a_1 + 2a_2x + \cdots + (n-1)a_{n-1}x^{n-2} + na_nx^{n-1}) \\
 &\quad \pm (b_1 + 2b_2x + \cdots + (n-1)b_{n-1}x^{n-2} + nb_nx^{n-1}) \\
 &= f'(x) \pm g'(x). \quad \heartsuit
 \end{aligned}$$

**命题** 设  $f(x), g(x) \in D[x]$ . 则

$$(\star) \quad (f(x)g(x))' = f'(x)g(x) + f(x)g'(x).$$

由  $(\star)$  与数学归纳法可知: 当  $f_0(x), f_1(x), \cdots, f_{k-1}(x) \in D[x]$  时,

$$\begin{aligned}
 & (f_0(x)f_1(x) \cdots f_{k-1}(x))' \\
 &= f_0'(x)f_1(x) \cdots f_{k-1}(x) + f_0(x)f_1'(x) \cdots f_{k-1}(x) + \cdots \\
 &\quad + f_0(x)f_1(x) \cdots f_{k-1}'(x).
 \end{aligned}$$

取  $f_0(x) = f_1(x) = \cdots = f_{k-1}(x) = f(x)$  知

$$((f(x))^k)' = k(f(x))^{k-1}f'(x).$$

**证** 我们证明  $(\star)$ , 将剩下的二个式留给读者作练习. 首先, 任取  $i, j \in \mathbb{N}, p, q \in D$ , 有

$$px^i \cdot qx^j = pqx^{i+j}.$$

这样,

$$\begin{aligned}
 (px^i \cdot qx^j)' &= (pqx^{i+j})' \\
 &= (i+j)pqx^{i+j-1} \\
 &= ipqx^{(i-1)+j} + jpqx^{i+(j-1)} \\
 &= ipqx^{i-1}x^j + jpqx^ix^{j-1} \\
 &= (ipx^{i-1})(qx^j) + (px^i)(jqx^{j-1}) \\
 &= (px^i)'(qx^j) + (px^i)(qx^j)'.
 \end{aligned}$$

设

$$\begin{aligned}
 f(x) &= a_0 + a_1x + \cdots + a_mx^m, \\
 g(x) &= b_0 + b_1x + \cdots + b_nx^n
 \end{aligned}$$

为  $D[x]$  中的二个元. 取  $px^i$  为  $a_0, a_1x, \cdots, a_mx^m$ , 有

$$\begin{aligned}
 (a_0 \cdot qx^j)' &= (a_0)'(qx^j) + (a_0)(qx^j)', \\
 (a_1x \cdot qx^j)' &= (a_1x)'(qx^j) + (a_1x)(qx^j)', \\
 &\dots\dots\dots, \\
 (a_mx^m \cdot qx^j)' &= (a_mx^m)'(qx^j) + (a_mx^m)(qx^j)'.
 \end{aligned}$$

所以

$$\begin{aligned}
 &(f(x) \cdot qx^j)' \\
 &= (a_0 \cdot qx^j + a_1x \cdot qx^j + \cdots + a_mx^m \cdot qx^j)' \\
 &= (a_0 \cdot qx^j)' + (a_1x \cdot qx^j)' + \cdots + (a_mx^m \cdot qx^j)' \\
 &= ((a_0)'(qx^j) + (a_0)(qx^j)') + ((a_1x)'(qx^j) + (a_1x)(qx^j)') \\
 &\quad + \cdots + ((a_mx^m)'(qx^j) + (a_mx^m)(qx^j)') \\
 &= ((a_0)'(qx^j) + (a_1x)'(qx^j) + \cdots + (a_mx^m)'(qx^j)) \\
 &\quad + ((a_0)(qx^j)' + (a_1x)(qx^j)' + \cdots + (a_mx^m)(qx^j)') \\
 &= ((a_0)' + (a_1x)' + \cdots + (a_mx^m)')(qx^j) \\
 &\quad + (a_0 + a_1x + \cdots + a_mx^m)(qx^j)'
 \end{aligned}$$

$$\begin{aligned}
&= (a_0 + a_1x + \cdots + a_mx^m)'(qx^j) + f(x)(qx^j)' \\
&= f'(x)(qx^j) + f(x)(qx^j)'.
\end{aligned}$$

再取  $qx^j$  为  $b_0, b_1x, \dots, b_nx^n$ , 有

$$\begin{aligned}
(f(x) \cdot b_0)' &= f'(x)(b_0) + f(x)(b_0)', \\
(f(x) \cdot b_1x)' &= f'(x)(b_1x) + f(x)(b_1x)', \\
&\dots\dots\dots, \\
(f(x) \cdot b_nx^n)' &= f'(x)(b_nx^n) + f(x)(b_nx^n)'.
\end{aligned}$$

所以

$$\begin{aligned}
&(f(x)g(x))' \\
&= (f(x) \cdot b_0 + f(x) \cdot b_1x + \cdots + f(x) \cdot b_nx^n)' \\
&= (f(x) \cdot b_0)' + (f(x) \cdot b_1x)' + \cdots + (f(x) \cdot b_nx^n)' \\
&= (f'(x)(b_0) + f(x)(b_0)') + (f'(x)(b_1x) + f(x)(b_1x)') \\
&\quad + \cdots + (f'(x)(b_nx^n) + f(x)(b_nx^n)') \\
&= (f'(x)(b_0) + (f'(x)(b_1x) + \cdots + f'(x)(b_nx^n)) \\
&\quad + (f(x)(b_0)' + f(x)(b_1x)' + \cdots + f(x)(b_nx^n)')) \\
&= f'(x)(b_0 + b_1x + \cdots + b_nx^n) \\
&\quad + f(x)((b_0)' + (b_1x)' + \cdots + (b_nx^n)') \\
&= f'(x)g(x) + f(x)(b_0 + b_1x + \cdots + b_nx^n)' \\
&= f'(x)g(x) + f(x)g'(x).
\end{aligned}$$

☞

**例** 考虑  $\mathbb{Z}$  与  $\mathbb{Z}[x]$ . 取

$$f(x) = x^3 + 2, \quad g(x) = x^2 + x - 1.$$

不难得到

$$f'(x) = 3x^2, \quad g'(x) = 2x + 1.$$

$f(x)$  与  $g(x)$  的积

$$f(x)g(x) = x^5 + x^4 - x^3 + 2x^2 + 2x - 2$$

的微商是

$$(f(x)g(x))' = 5x^4 + 4x^3 - 3x^2 + 4x + 2.$$

如果用上面的 (★) 计算, 就是

$$\begin{aligned} & f'(x)g(x) + f(x)g'(x) \\ &= 3x^2(x^2 + x - 1) + (x^3 + 2)(2x + 1) \\ &= 3x^4 + 3x^3 - 3x^2 + 2x^4 + x^3 + 4x + 2 \\ &= 5x^4 + 4x^3 - 3x^2 + 4x + 2. \end{aligned}$$

也许这不太能体现 (★) 的作用: 算二个多项式积的微商时, 先拆再算好像没什么不方便的. 的确如此. 可是 (★) 的推论

$$((f(x))^k)' = k(f(x))^{k-1}f'(x)$$

很有用. 看下面的例.

**例** 还是考虑  $\mathbb{Z}$  与  $\mathbb{Z}[x]$ . 计算

$$\begin{aligned} p(x) &= (g \circ f)(x) = g(f(x)) = (x^3 + 2)^2 + (x^3 + 2) - 1, \\ q(x) &= (f \circ g)(x) = f(g(x)) = (x^2 + x - 1)^3 + 2 \end{aligned}$$

的微商.

用定义写出  $p(x)$  的微商并不是很难. 因为

$$p(x) = (x^6 + 4x^3 + 4) + x^3 + 2 - 1 = x^6 + 5x^3 + 5,$$

故

$$p'(x) = 6x^5 + 15x^2.$$

不过用定义写出  $q(x)$  就有点麻烦了: 三项的立方不是那么好算. 但是, 我们利用这个推论, 可直接写出

$$q'(x) = 3(x^2 + x - 1)^2(2x + 1).$$

记  $g(x) = x^k$ . 取  $f(x) \in D[x]$ . 不难看出,

$$(f(x))^k = (g \circ f)(x).$$

所以

$$(g \circ f)'(x) = ((f(x))^k)' = k(f(x))^{k-1}f'(x) = (g' \circ f)(x)f'(x).$$

这告诉我们什么呢? 如果我们把  $f(x)$  看成文字  $y$ , 那么  $y^k \in D[y]$  的微商是  $ky^{k-1}$ . 将此结果乘  $y = f(x) \in D[x]$  的微商  $f'(x)$ , 就是  $(g \circ f)(x) \in D[x]$  的微商.

取  $h(x) = x \in D[x]$ . 那么  $(f \circ h)(x)$  就是  $f(x)$ . 因为  $(x)' = 1$ , 所以

$$(f \circ h)'(x) = f'(x) = (f' \circ h)(x)h'(x).$$

我们作出猜想: 任取  $f(x), g(x) \in D[x]$ , 必有

$$(g \circ f)'(x) = (g' \circ f)(x)f'(x).$$

幸运的事儿是, 这个猜想是正确的.

**命题** 设  $f(x), g(x) \in D[x]$ . 则  $f(x)$  与  $g(x)$  的复合的微商适合链规则 (*the chain rule*):

$$(g \circ f)'(x) = (g' \circ f)(x)f'(x).$$

链规则也可写为

$$(g(f(x)))' = g'(f(x))f'(x).$$

**证** 设

$$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_{n-1}x^{n-1} + b_nx^n \in D[x],$$

则

$$(g \circ f)(x) = b_0 + b_1f(x) + b_2(f(x))^2 + \cdots + b_{n-1}(f(x))^{n-1} + b_n(f(x))^n.$$

所以

$$\begin{aligned}
 & (g \circ f)'(x) \\
 &= b_1 f'(x) + b_2 ((f(x))^2)' + \cdots + b_{n-1} ((f(x))^{n-1})' + b_n ((f(x))^n)' \\
 &= b_1 f'(x) + b_2 \cdot 2f(x)f'(x) + \cdots + b_{n-1} \cdot (n-1)(f(x))^{n-2} f'(x) \\
 &\quad + b_n \cdot n(f(x))^{n-1} f'(x) \\
 &= b_1 f'(x) + 2b_2 f(x)f'(x) + \cdots + (n-1)b_{n-1} (f(x))^{n-2} f'(x) \\
 &\quad + nb_n (f(x))^{n-1} f'(x) \\
 &= (b_1 + 2b_2 f(x) + \cdots + (n-1)b_{n-1} (f(x))^{n-2} + nb_n (f(x))^{n-1}) f'(x) \\
 &= (g' \circ f)(x) f'(x). \quad \heartsuit
 \end{aligned}$$

**例** 我们用链规则计算  $p(x)$  的微商:

$$p'(x) = (g' \circ f)(x) f'(x) = (2(x^3 + 2) + 1)(3x^2) = 3x^2(2x^3 + 5).$$

这跟前面算出的  $6x^5 + 15x^2$  是一致的.

## 多项式的根

我们回顾一下熟悉的多项式函数.

**定义** 设  $a_0, a_1, \dots, a_n \in D$ . 称

$$\begin{aligned} f: D &\rightarrow D, \\ t &\mapsto a_0 + a_1 t + \dots + a_n t^n \end{aligned}$$

为  $D$  的多项式函数 (*polynomial function*). 我们也说, 这个  $f$  是由  $D$  上  $x$  的多项式

$$f(x) = a_0 + a_1 x + \dots + a_n x^n$$

诱导的多项式函数 (*the polynomial function induced by  $f$* ). 不难看出, 若二个多项式相等, 则其诱导的多项式函数也相等.

**定义** 设  $f$  与  $g$  是  $D$  的二个多项式函数. 二者的和  $f + g$  定义为

$$\begin{aligned} f + g: D &\rightarrow D, \\ t &\mapsto f(t) + g(t). \end{aligned}$$

二者的积  $fg$  定义为

$$\begin{aligned} fg: D &\rightarrow D, \\ t &\mapsto f(t)g(t). \end{aligned}$$

设  $f, g$  是  $D$  的二个多项式函数:

$$\begin{aligned} f: D &\rightarrow D, \\ t &\mapsto a_0 + a_1 t + \dots + a_n t^n, \\ g: D &\rightarrow D, \\ t &\mapsto b_0 + b_1 t + \dots + b_n t^n. \end{aligned}$$

利用  $D$  的运算律, 可以得到

$$\begin{aligned} f + g: D &\rightarrow D, \\ t &\mapsto (a_0 + b_0) + (a_1 + b_1)t + \dots + (a_n + b_n)t^n, \\ fg: D &\rightarrow D, \\ t &\mapsto c_0 + c_1 t + \dots + c_{2n} t^{2n}, \end{aligned}$$



其中

$$c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0.$$

由此可得下面的命题:

**命题** 设  $f(x), g(x) \in D[x]$ ,  $f, g$  分别是  $f(x), g(x)$  诱导的多项式函数. 那么  $f + g$  是  $f(x) + g(x)$  诱导的多项式函数, 且  $fg$  是  $f(x)g(x)$  诱导的多项式函数.

通俗地说, 若多项式  $f_0(x), f_1(x), \dots, f_{n-1}(x)$  之间有一个由加法与乘法计算得到的关系, 那么将  $x$  换为  $D$  的元  $t$ , 这样的关系仍成立.

**例** 考虑  $\mathbb{F}$  与  $\mathbb{F}[x]$ . 前面, 利用带余除法, 得到关系

$$8x^6 + 1 = (4x^3 + 12x - 8) \cdot 2(x - 1)^2(x + 2) + (72x^2 - 96x + 33).$$

这里  $x$  只是一个文字, 不是数! 但是, 上面的命题告诉我们, 可以把  $x$  看成一个数. 比如, 由上面的式可以立即看出,  $8t^6 + 1$  与  $72t^2 - 96t + 33$  在  $t = 1$  或  $t = -2$  时值是一样的.

可是, 对于这样的式, 我们不能将  $x$  改写为  $\mathbb{F}$  的元  $t$ :

$$\deg 3x^2 < \deg 2x^3.$$

可以看到, 若  $t = 0$ , 则  $3t^2 = 2t^3 = 0$ , 而  $0$  的次是  $-\infty$ ; 若  $t \neq 0$ , 则  $3t^2$  与  $2t^3$  都是非零数, 次都是  $0$ .

**评注** 我们已经知道, 多项式确定多项式函数. 自然地, 有这样的问題: 多项式函数能否确定多项式? 一般情况下, 这个问题的答案是 no.

考虑 4 元集  $V$ . 作  $V$  上  $x$  的二个多项式:

$$f(x) = x^4 - x, \quad g(x) = 0.$$

显然, 这是二个不相等的多项式. 但是, 任取  $t \in V$ , 都有

$$t^4 - t = 0.$$

因此,  $f(x)$  与  $g(x)$  诱导的多项式函数是同一函数!

不过, 在某些场合下, 多项式函数可以确定多项式. 之后我们还会提到这一点.

**评注** 设  $f(x) = a_0 + a_1x + \cdots + a_nx^n \in D[x]$ . 设  $t$  是  $D$  的元. 以后, 我们直接写

$$f(t) = a_0 + a_1t + \cdots + a_nt^n.$$

并称  $f(t)$  是多项式  $f(x)$  在点 (*point*)  $t$  的值. 至少, 一方通行 (*one-way traffic*) 是没问题的.

顺便一提,  $f(x)$  的微商也是多项式:

$$f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}.$$

我们把

$$a_1 + 2a_2t + \cdots + na_nt^{n-1} \in D$$

简单地写为  $f'(t)$ .

了解了多项式与多项式函数的关系后, 下面的这个命题就不会太凸兀了.

**命题** 设  $f(x) \in D[x]$  是  $n$  次多项式 ( $n \geq 1$ ),  $a \in D$ . 则存在  $n-1$  次多项式  $q(x)$  ( $\in D[x]$ ) 使

$$f(x) = q(x)(x-a) + f(a).$$

根据带余除法, 这样的  $q(x)$  一定是唯一的.

**证** 因为  $x-a$  的首项系数 1 是单位, 故存在  $D[x]$  的二元  $q(x), r(x)$  使

$$f(x) = q(x)(x-a) + r(x), \quad \deg r(x) < \deg(x-a) = 1.$$

所以,  $r(x) = c, c \in D$ . 用  $D$  的元  $a$  替换  $x$ , 有

$$f(a) = q(a)(a-a) + c = c.$$

所以

$$f(x) = q(x)(x-a) + f(a).$$

再看这个  $q(x)$  的次. 因为  $f(x)$  的次不低于  $x-a$  的次, 故

$$\deg q(x) = \deg f(x) - \deg(x-a) = n-1.$$

**评注** 如果用  $D$  的元  $b$  替换  $x$ , 则

$$f(b) = (b-a)q(b) + f(a),$$

也就是说, 存在  $r \in D$  使

$$f(b) - f(a) = (b-a)r.$$

所以, 若  $f(x) \in D[x]$  是  $n$  次多项式 ( $n \geq 1$ ),  $a, b \in D$ , 则存在  $r \in D$  使  $f(b) - f(a) = (b-a)r$ . 当  $f(x)$  的次低于 1 时, 这个命题也对 (取  $r = 0$ ).

举个简单的例. 我们说, 不存在系数为整数的多项式  $f(x)$  使  $f(1) = f(-1) + 1$ . 假如说这样的  $f$  存在, 那么应存在整数  $r$  使

$$1 = f(1) - f(-1) = (1 - (-1))r = 2r,$$

而 1 不是偶数, 矛盾.

现在, 我们讨论多项式的根的基本性质.

**定义** 设  $f(x)$  是  $D$  上  $x$  的多项式. 若有  $a \in D$  使  $f(a) = 0$ , 则说  $a$  是 (多项式)  $f(x)$  的根 (*root*).

**例** 设  $D \subset \mathbb{C}$ , 且  $\mathbb{Z} \subset D$ . 看  $D$  上  $x$  的多项式

$$f(x) = (2x-1)(x+1)(x^2-3)(x^2+1)(x^2+4).$$

如果  $D = \mathbb{Z}$ , 则  $f(x)$  有一个在  $D$  里的根:  $-1$ . 如果  $D = \mathbb{Q}$ , 则  $f(x)$  有二个在  $D$  里的根:  $-1, \frac{1}{2}$ . 如果  $D = \mathbb{R}$ , 则  $f(x)$  有四个在  $D$  里的根:  $-1, \frac{1}{2}, \pm\sqrt{3}$ . 如果  $D = \mathbb{C}$ , 则  $f(x)$  有八个在  $D$  里的根:  $-1, \frac{1}{2}, \pm\sqrt{3}, \pm i, \pm 2i$ .

**例** 再来一个例. 看  $D$  上  $x$  的多项式

$$f(x) = x^2 + x - 1.$$

若  $D = \mathbb{R}$ , 则  $f(x)$  的二个根是  $\frac{-1 \pm \sqrt{5}}{2}$ . 若  $D = V$ , 则  $f(x)$  的二个根是  $\tau, \tau^2$ . 当然, 若  $D \subset \mathbb{Q}$ , 则  $f(x)$  无 ( $D$  的) 根.

**评注** 设  $a, b \in D$ , 且  $a \neq 0$ .

若  $f(x) = a$ , 则  $f(x)$  无根. 换句话说, 零次多项式至多有零个根.

再设  $f(x) = ax + b$  是一次多项式. 若存在  $c \in D$  使  $b = ac$ , 则  $f(x)$  有一个根  $-c$ . 并且,  $f(x)$  也不会有另一个根 (若  $at_1 + b = at_2 + b$ , 则  $at_1 = at_2$ , 故  $t_1 = t_2$ ). 若这样的  $c$  不存在, 则  $f(x)$  无根 (反设  $f(x)$  有根  $d$ , 则由  $ad + b = 0$  知  $b = a(-d)$ , 矛盾). 换句话说, 一次多项式至多有一个根.

结合上面的二个例, 我们猜想:  $n$  次多项式 ( $n \in \mathbb{N}$ ) 至多有  $n$  个 (不同的) 根. 幸运的事儿是, 这个猜想是正确的.

**命题** 设  $f(x) \in D[x]$  是  $n$  次多项式 ( $n \geq 1$ ).  $a$  是  $f(x)$  的根的一个必要与充分条件是: 存在  $n-1$  次多项式  $q(x) (\in D[x])$  使

$$f(x) = q(x)(x - a).$$

根据带余除法, 这样的  $q(x)$  一定是唯一的.

**证** 先看充分性. 若这样的  $q(x)$  存在, 则

$$f(a) = q(a)(a - a) = 0.$$

再看必要性. 设  $f(a) = 0$ . 根据上面的命题, 存在  $n-1$  次多项式  $q(x) \in D[x]$  使

$$f(x) = q(x)(x - a) + f(a) = q(x)(x - a). \quad \text{☞}$$

**命题** 设  $f(x) \in D[x]$  是  $n$  次多项式 ( $n \in \mathbb{N}$ ). 则  $f(x)$  至多有  $n$  个不同的根.

**证**  $n = 0$  或  $n = 1$  时, 我们已经知道这是对的. 用数学归纳法. 假设  $\ell$  次多项式至多有  $\ell$  个不同的根. 看  $\ell+1$  次多项式  $f(x)$ . 如果它没有根, 当然至多有  $\ell+1$  个不同的根. 如果它有一个根  $a$ , 则存在  $\ell$  次多项式  $q(x)$  使

$$f(x) = q(x)(x - a).$$

根据归纳假设,  $q(x)$  至多有  $\ell$  个不同的根. 而且, 若  $b \neq a$ , 且  $b$  不是  $q(x)$  的根, 利用消去律可知  $f(b) \neq 0$ . 这样,  $f(x)$  至多有  $\ell+1$  个不同的根. ☞

由此可推出一个很有用的事实:

**命题** 设  $a_0, a_1, \dots, a_n$  是  $D$  的元. 设  $n$  是非负整数. 设

$$f(x) = a_0 + a_1x + \dots + a_nx^n.$$

若  $t_0, t_1, \dots, t_n$  是  $n+1$  个互不相同的  $D$  的元, 且

$$f(t_0) = f(t_1) = \dots = f(t_n) = 0,$$

则  $f(x)$  必为零多项式. 通俗地说, 次不高于  $n$  (且系数为整环的元) 的多项式不可能有  $n$  个以上的互不相同的根, 除非这个多项式是零.

**证** 反证法. 设  $f(x)$  不是零多项式. 设  $f(x)$  的次为  $m$ , 则  $0 \leq m \leq n$ . 根据上个命题,  $f(x)$  至多有  $m$  个不同的根, 这与题设矛盾! 故  $f(x) = 0$ .  $\clubsuit$

**评注** 再看前面提到的 4 元集  $V$ . 可以看出, 因为  $V$  的元 “不够多”, 所以出现了取零值的非零多项式.

此事实的一个推论是:

**命题** 设  $a_0, b_0, a_1, b_1, \dots, a_n, b_n$  是  $D$  的元. 设  $n$  是非负整数. 设

$$f(x) = a_0 + a_1x + \dots + a_nx^n,$$

$$g(x) = b_0 + b_1x + \dots + b_nx^n.$$

若  $t_0, t_1, \dots, t_n$  是  $n+1$  个互不相同的  $D$  的元, 且

$$f(t_0) = g(t_0), \quad f(t_1) = g(t_1), \quad \dots, \quad f(t_n) = g(t_n),$$

则  $f(x)$  必等于  $g(x)$ . 通俗地说, 若次不高于  $n$  (且系数为整环的元) 的二个多项式若在多于  $n$  处取一样的值, 则这二个多项式相等.

**证** 考虑  $h(x) = f(x) - g(x)$ . 则  $\deg h(x) \leq n$ .  $h(x)$  有  $n+1$  个不同的根. 根据上个命题,  $h(x)$  是零多项式. 这样,  $f(x) = g(x)$ .  $\clubsuit$

在中学, 我们学过解一元二次方程  $at^2 + bt + c = 0$  ( $a, b, c$  为实数, 且  $a \neq 0$ ) 的一种方法: 直接套用公式

$$t = \frac{-b \pm \sqrt{\Delta}}{2a},$$

其中

$$\Delta = b^2 - 4ac$$

是判别式: 当  $\Delta > 0$  时, 方程有二个不等的实数解; 当  $\Delta = 0$  时, 方程有二个相等的实数解; 当  $\Delta < 0$  时, 方程无实数解.

当  $\Delta = 0$  时,  $c = \frac{b^2}{4a}$ , 则

$$at^2 + bt + c = a \left( t^2 + 2\frac{b}{2a}t + \left( \frac{b}{2a} \right)^2 \right) = a \left( t + \frac{b}{2a} \right)^2.$$

记

$$f(x) = a \left( x + \frac{b}{2a} \right)^2 \in \mathbb{R}[x].$$

根据根的定义,  $-\frac{b}{2a} \in \mathbb{R}$  是  $f(x)$  的根. 我们发现, 这个根“出现了”2次, 是重复的. 我们给这样的根一个特殊点的称呼.

**定义** 设  $a \in D$  是多项式  $f(x) \in D[x]$  的根. 那么, 存在唯一的多项式  $q(x) \in D[x]$  使

$$f(x) = (x - a)q(x).$$

若  $q(a) = 0$ , 则说  $a$  是  $f(x)$  的一个重根 (*multiple root*). 若  $q(a) \neq 0$ , 则说  $a$  是  $f(x)$  的一个单根 (*simple root*).

**例** 看  $\mathbb{Z}$  上  $x$  的多项式

$$f(x) = (x^2 - 3)(x^2 + 2)(x - 1)^2(x + 2).$$

显然,  $f(x)$  的根是 1 与 -2. 因为

$$f(x) = (x + 2) \underbrace{(x^2 - 3)(x^2 + 2)(x - 1)^2}_{q_1(x)},$$

且  $q_1(x) \neq 0$ , 故  $-2$  是  $f(x)$  的单根. 类似地, 由于

$$f(x) = (x-1) \underbrace{(x^2-3)(x^2+2)(x-1)(x+2)}_{q_2(x)},$$

且  $q_2(x) = 0$ , 故  $1$  是  $f(x)$  的重根.

**命题** 设  $a \in D$  是多项式  $f(x) \in D[x]$  的根. 则:

(i) 若  $a$  是  $f(x)$  的重根, 则  $a$  是  $f'(x)$  的根;

(ii) 若  $a$  是  $f(x)$  的单根, 则  $a$  不是  $f'(x)$  的根.

所以,  $f(x)$  有重根的一个必要与充分条件是:  $f(x)$  与  $f'(x)$  有公共根.

**证** 因为  $a$  是  $f(x)$  的根, 故存在唯一的  $q(x)$  使

$$f(x) = (x-a)q(x).$$

从而

$$f'(x) = (x-a)'q(x) + (x-a)q'(x) = q(x) + (x-a)q'(x).$$

这样

$$f'(a) = q(a) + (a-a)q'(a) = q(a).$$

(i) 若  $a$  是  $f(x)$  的重根, 则  $q(a) = 0$ , 故  $f'(a) = 0$ .

(ii) 若  $a$  是  $f(x)$  的单根, 则  $q(a) \neq 0$ , 故  $f'(a) \neq 0$ . ✎

**例** 我们看

$$f(x) = ax^2 + bx + c \in \mathbb{R}[x], \quad a \neq 0.$$

它的微商  $f'(x) = 2ax + b$  恰有一个根  $t_0 = -\frac{b}{2a}$ . 由上个命题,  $f(x)$  有重根相当于  $f(t_0) = 0$ , 即

$$0 = f(t_0) = a \cdot \frac{b^2}{4a^2} - \frac{b^2}{2a} + c = \frac{4ac - b^2}{4a} = -\frac{\Delta}{4a}.$$

## $\mathbb{F}$ 上的多项式

我们在前几节讨论的都是整环  $D$  上的多项式, 所以它们看上去是有些抽象的. 从现在开始, 我们不讨论抽象的  $D$  与  $D[x]$ , 而是讨论  $\mathbb{F}$  与  $\mathbb{F}[x]$ , 其中  $\mathbb{F}$  可代指  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$  的任意一个. 细心的读者会注意到我们在前几节未使用  $\sum$  符号: 这是为了让读者没那么困难地适应多项式理论. 从本节起, 我们会较多地使用这个  $\sum$ . 读者也可以乘此机会让自己熟悉它. 当然, 我们偶尔也会使用  $\prod$  符号.

本节并没有什么新的知识. 读者可以乘此机会温习一下所学内容. 我们将重述一些定义与命题. 我们在学校学数学的时候, 也会有复习课. 就当本节就是“复习节”吧!

先从多项式的定义与运算开始.

**定义** 设  $x$  是不在  $\mathbb{F}$  里的任意一个文字. 形如

$$\begin{aligned} f(x) &= \sum_{i=0}^n a_i x^i \\ &= a_0 + a_1 x + \cdots + a_n x^n \quad (n \in \mathbb{N}, a_0, a_1, \dots, a_n \in \mathbb{F}, a_n \neq 0) \end{aligned}$$

的表达式称为  $\mathbb{F}$  上  $x$  的一个多项式.  $n$  称为其次,  $a_i$  称为其  $i$  次系数,  $a_i x^i$  称为其  $i$  次项.  $f(x)$  的次可写为  $\deg f(x)$ .

若二个多项式的次与各同次系数均相等, 则二者相等.

多项式的系数为 0 的项可以不写.

约定  $0 \in \mathbb{F}$  也是多项式, 称为零多项式. 零多项式的次是  $-\infty$ . 任取整数  $m$ , 约定

$$\begin{aligned} -\infty &= -\infty, \quad -\infty < m, \\ -\infty + m &= m + (-\infty) = -\infty + (-\infty) = -\infty. \end{aligned}$$

当然, 还约定, 零多项式只跟自己相等. 换句话说,

$$\sum_{i=0}^n a_i x^i = 0$$

的一个必要与充分条件是

$$a_0 = a_1 = \cdots = a_n = 0.$$



$\mathbb{F}$  上  $x$  的所有多项式作成的集是  $\mathbb{F}[x]$ :

$$\mathbb{F}[x] = \left\{ \sum_{i=0}^n a_i x^i \mid n \in \mathbb{N}, a_0, a_1, \dots, a_n \in \mathbb{F} \right\}.$$

文字  $x$  只是一个符号, 它与  $\mathbb{F}$  的元的和与积都是形式的. 我们说,  $x$  是不定元.

**定义** 设

$$f(x) = \sum_{i=0}^n a_i x^i, \quad g(x) = \sum_{i=0}^n b_i x^i \in \mathbb{F}[x].$$

规定加法如下:

$$f(x) + g(x) = \sum_{i=0}^n (a_i + b_i) x^i.$$

**命题** 设  $f(x), g(x), h(x) \in \mathbb{F}[x]$ .  $\mathbb{F}[x]$  的加法适合如下性质:

- (i)  $f(x) + g(x) \in \mathbb{F}[x]$ ;
- (ii)  $(f(x) + g(x)) + h(x) = f(x) + (g(x) + h(x))$ ;
- (iii) 存在多项式  $0$  使  $0 + f(x) = f(x) + 0 = f(x)$ ;
- (iv) 存在多项式  $-f(x)$  使  $-f(x) + f(x) = f(x) + (-f(x)) = 0$ ;
- (v)  $f(x) + g(x) = g(x) + f(x)$ .

**定义** 设

$$f(x) = \sum_{i=0}^n a_i x^i, \quad g(x) = \sum_{i=0}^n b_i x^i \in \mathbb{F}[x].$$

则

$$-g(x) = \sum_{i=0}^n (-b_i) x^i.$$

规定减法如下:

$$f(x) - g(x) = f(x) + (-g(x)).$$

**命题** 设  $f(x), g(x) \in \mathbb{F}[x]$ . 则

$$\deg(f(x) \pm g(x)) \leq \max\{\deg f(x), \deg g(x)\}.$$

若  $\deg f(x) > \deg g(x)$ , 则

$$\deg(f(x) \pm g(x)) = \deg f(x).$$

类似地, 若  $\deg f(x) < \deg g(x)$ , 则

$$\deg(f(x) \pm g(x)) = \deg g(x).$$

**定义** 设

$$f(x) = \sum_{i=0}^n a_i x^i = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{F}[x].$$

这称为  $f(x)$  的升次排列. 下面的写法称为  $f(x)$  的降次排列:

$$\sum_{j=0}^n a_{n-j} x^{n-j} = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0.$$

(非零) 多项式的最高次非零项是首项. 它的系数是此多项式的首项系数.

**定义** 设

$$f(x) = \sum_{i=0}^m a_i x^i, \quad g(x) = \sum_{j=0}^n b_j x^j \in \mathbb{F}[x].$$

规定乘法如下:

$$f(x)g(x) = \sum_{k=0}^{m+n} \left( \sum_{i=0}^k a_i b_{k-i} \right) x^k.$$

**命题** 设  $m, n \in \mathbb{N}, p, q \in \mathbb{F}$ . 则

$$px^i \cdot qx^j = (px^i)(qx^j) = (pq)x^{i+j}.$$

**命题** 设  $f(x), g(x) \in \mathbb{F}[x]$ . 则

$$\deg f(x)g(x) = \deg f(x) + \deg g(x).$$

**命题** 设  $f(x), g(x), h(x) \in \mathbb{F}[x]$ .  $\mathbb{F}[x]$  的加法与乘法适合 (i) 至 (v) 及如下性质:

- (vi)  $f(x)g(x) \in \mathbb{F}[x]$ ;
- (vii)  $(f(x)g(x))h(x) = f(x)(g(x)h(x))$ ;
- (viii) 存在多项式  $1$  使  $1f(x) = f(x)1 = f(x)$ ;
- (ix)  $(-1)f(x) = -f(x)$ ;
- (x)  $f(x)g(x) = g(x)f(x)$ ;
- (xi) 若  $f(x) \neq 0$ , 则

$$\begin{aligned} f(x)g(x) &= f(x)h(x) \implies g(x) = h(x), \\ g(x)f(x) &= h(x)f(x) \implies g(x) = h(x); \end{aligned}$$

(xii) 二个分配律都对:

$$\begin{aligned} f(x)(g(x) + h(x)) &= f(x)g(x) + f(x)h(x), \\ (g(x) + h(x))f(x) &= g(x)f(x) + h(x)f(x). \end{aligned}$$

**评注**  $\mathbb{F}[x]$  的一个名字就是 (域)  $\mathbb{F}$  上  $(x)$  的多项式环.

**定义** 设  $m \in \mathbb{N}$ . 多项式  $f(x)$  的  $m$  次幂就是  $m$  个  $f(x)$  的积:

$$(f(x))^m = \underbrace{f(x) \cdot f(x) \cdots f(x)}_{m \text{ } f(x)\text{'s}} = \prod_{\ell=0}^{m-1} f(x).$$

设  $m, n \in \mathbb{N}$ ,  $f(x), g(x) \in \mathbb{F}[x]$ , 则多项式的幂适合如下规则:

$$\begin{aligned} (f(x))^m (f(x))^n &= (f(x))^{m+n}, \\ ((f(x))^m)^n &= (f(x))^{mn}, \\ (f(x)g(x))^m &= (f(x))^m (g(x))^m. \end{aligned}$$

**命题** 设  $f(x) \in \mathbb{F}[x]$ . 非零的  $c \in \mathbb{F}$  是 0 次多项式, 那么

$$\deg cf(x) = \deg f(x).$$

再来看多项式的带余除法. 因为  $\mathbb{F}$  的每个非零元都是  $\mathbb{F}$  的单位, 所以有

**命题** 设  $f(x) \in \mathbb{F}[x]$  是非零多项式. 对任意  $g(x) \in \mathbb{F}[x]$ , 存在唯一的  $q(x), r(x) \in \mathbb{F}[x]$  使

$$g(x) = q(x)f(x) + r(x), \quad \deg r(x) < \deg f(x).$$

一般称其为带余除法:  $q(x)$  就是商;  $r(x)$  就是余式. 并且, 当  $f(x)$  的次不高于  $g(x)$  的次时,  $f(x), g(x), q(x)$  间还有如下的次关系:

$$\deg g(x) = \deg(g(x) - r(x)) = \deg q(x) + \deg f(x).$$

可以看到, 在  $\mathbb{F}[x]$  里, 带余除法的适用范围更广了.

下面回顾多项式的相等. 我们借助“线性无关”讨论相等问题.

**定义** 设  $p_0(x), p_1(x), \dots, p_n(x) \in \mathbb{F}[x]$ . 设  $c_0, c_1, \dots, c_n \in \mathbb{F}$ . 我们说

$$\sum_{i=0}^n c_i p_i(x)$$

是多项式  $p_0(x), p_1(x), \dots, p_n(x)$  的一个线性组合.  $c_0, c_1, \dots, c_n$  就是此线性组合的系数.

若不存在一组不全为 0 的  $\mathbb{F}$  中元  $d_0, d_1, \dots, d_n$  使

$$\sum_{i=0}^n d_i p_i(x) = 0,$$

则说  $p_0(x), p_1(x), \dots, p_n(x)$  是线性无关的. 换句话说, “ $p_0(x), p_1(x), \dots, p_n(x)$  是线性无关的”意味着: 若  $\mathbb{F}$  中元  $r_0, r_1, \dots, r_n$  使

$$\sum_{i=0}^n r_i p_i(x) = 0,$$

则  $r_0 = r_1 = \dots = r_n = 0$ .

**命题** 设  $p_0(x), p_1(x), \dots, p_n(x) \in \mathbb{F}[x]$  分别是 0, 1,  $\dots$ ,  $n$  次多项式. 则:

- (i)  $p_0(x), p_1(x), \dots, p_n(x)$  是线性无关的;
- (ii) 任意次不高于  $n$  的多项式都可唯一地写为  $p_0(x), p_1(x), \dots, p_n(x)$  的线性组合.

由于  $\mathbb{F}$  的每个非零元都是单位, 上面的命题的结论变强了. 下面的例体现了这一点.

**例** 考虑  $\mathbb{F}$  与  $\mathbb{F}[x]$ . 取  $n = 2$ , 及

$$p_0(x) = -1, \quad p_1(x) = 2x, \quad p_2(x) = 3x^2.$$

这三个多项式是线性无关的. 考虑  $f(x) = 3 + x - 2x^2$ . 设  $c_0, c_1, c_2 \in \mathbb{F}$  使

$$3 + x - 2x^2 = c_0 \cdot (-1) + c_1 \cdot 2x + c_2 \cdot 3x^2.$$

这相当于

$$3 = -c_0, \quad 1 = 2c_1, \quad -2 = 3c_2.$$

由此可得

$$c_0 = -3, \quad c_1 = \frac{1}{2}, \quad c_2 = -\frac{2}{3}.$$

可以看到, 在  $\mathbb{Z}$  与  $\mathbb{Z}[x]$  里  $p_0(x), p_1(x), p_2(x)$  的线性组合还不能表示这个  $f(x)$ , 但当我们在“大环境”  $\mathbb{F}$  与  $\mathbb{F}[x]$  下讨论问题时就可以了.

**评注** 我们常常把  $D$  的元分为三类: 零、单位、非零且不是单位的元. 但是在  $\mathbb{F}$ , 只要分为二类即可: 零与非零.

**命题** 设  $a_0, b_0, a_1, b_1, \dots, a_n, b_n \in \mathbb{F}$ . 设  $c \in \mathbb{F}$ . 再设

$$f(x) = \sum_{i=0}^n a_i(x-c)^i, \quad g(x) = \sum_{i=0}^n b_i(x-c)^i.$$

则  $f(x) = g(x)$  的一个必要与充分条件是

$$a_0 = b_0, \quad a_1 = b_1, \quad \dots, \quad a_n = b_n.$$

并且, 任取

$$f(x) = \sum_{i=0}^n u_i x^i \in \mathbb{F}[x],$$

必存在  $v_0, v_1, \dots, v_n \in \mathbb{F}$  使

$$f(x) = \sum_{i=0}^n v_i(x-c)^i.$$

我们看看多项式的微商.

**定义** 设

$$f(x) = \sum_{i=0}^n a_i x^i \in \mathbb{F}[x].$$

$f(x)$  的微商是多项式

$$f'(x) = \sum_{i=1}^n i a_i x^{i-1} \in \mathbb{F}[x].$$

$f'(x)$  也可写为  $(f(x))'$ .

**评注** 若  $f(x) = c$ ,  $c \in \mathbb{F}$ , 则  $f'(x)$  为零多项式.

**定义** 设

$$f(x) = \sum_{i=0}^m a_i x^i, \quad g(x) = \sum_{j=0}^n b_j x^j$$

为  $\mathbb{F}[x]$  中的二个元. 我们称

$$(g \circ f)(x) = g(f(x)) = \sum_{j=0}^n b_j (f(x))^j$$

为  $f(x)$  与  $g(x)$  的复合.

**命题** 多项式的复合适合结合律. 具体地说, 设  $f(x)$ ,  $g(x)$ ,  $h(x) \in \mathbb{F}[x]$ , 则

$$((h \circ g) \circ f)(x) = (h \circ (g \circ f))(x).$$

**命题** 设  $f(x)$ ,  $g(x)$ ,  $h(x) \in \mathbb{F}[x]$ .

(i) 设  $p(x) = f(x) + g(x)$ . 则

$$p(h(x)) = f(h(x)) + g(h(x)).$$

(ii) 设  $q(x) = f(x)g(x)$ . 则

$$q(h(x)) = f(h(x))g(h(x)).$$

**命题** 设  $f(x), g(x) \in \mathbb{F}[x]$ ,  $c \in \mathbb{F}$ . 则

(i)  $(cf(x))' = cf'(x)$ ;

(ii)  $(f(x) \pm g(x))' = f'(x) \pm g'(x)$ .

由 (i) (ii) 与数学归纳法可知: 当  $c_0, c_1, \dots, c_{k-1} \in \mathbb{F}$ , 且  $f_0(x), f_1(x), \dots, f_{k-1}(x) \in \mathbb{F}[x]$  时,

$$\left( \sum_{\ell=0}^{k-1} c_\ell f_\ell(x) \right)' = \sum_{\ell=0}^{k-1} c_\ell f'_\ell(x).$$

**命题** 设  $f(x), g(x) \in \mathbb{F}[x]$ . 则

(★)  $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$ .

由 (★) 与数学归纳法可知: 当  $f_0(x), f_1(x), \dots, f_{k-1}(x) \in \mathbb{F}[x]$  时,

$$\begin{aligned} & (f_0(x)f_1(x) \cdots f_{k-1}(x))' \\ &= f'_0(x)f_1(x) \cdots f_{k-1}(x) + f_0(x)f'_1(x) \cdots f_{k-1}(x) + \cdots \\ & \quad + f_0(x)f_1(x) \cdots f'_{k-1}(x). \end{aligned}$$

取  $f_0(x) = f_1(x) = \cdots = f_{k-1}(x) = f(x)$  知

$$((f(x))^k)' = k(f(x))^{k-1}f'(x).$$

**命题** 设  $f(x), g(x) \in \mathbb{F}[x]$ . 则  $f(x)$  与  $g(x)$  的复合的微商适合链规则:

$$(g \circ f)'(x) = (g' \circ f)(x)f'(x).$$

链规则也可写为

$$(g(f(x)))' = g'(f(x))f'(x).$$

最后, 我们回顾多项式函数与多项式的根.

**定义** 设  $a_0, a_1, \dots, a_n \in \mathbb{F}$ . 称

$$\begin{aligned} f: & \quad \mathbb{F} \rightarrow \mathbb{F}, \\ & \quad t \mapsto \sum_{i=0}^n a_i t^i \end{aligned}$$

为  $\mathbb{F}$  的多项式函数. 我们也说, 这个  $f$  是由  $\mathbb{F}$  上  $x$  的多项式

$$f(x) = \sum_{i=0}^n a_i x^i$$

诱导的多项式函数. 不难看出, 若二个多项式相等, 则其诱导的多项式函数也相等.

**定义** 设  $f$  与  $g$  是  $\mathbb{F}$  的二个多项式函数. 二者的和  $f + g$  定义为

$$\begin{aligned} f + g: & \quad \mathbb{F} \rightarrow \mathbb{F}, \\ t & \mapsto f(t) + g(t). \end{aligned}$$

二者的积  $fg$  定义为

$$\begin{aligned} fg: & \quad \mathbb{F} \rightarrow \mathbb{F}, \\ t & \mapsto f(t)g(t). \end{aligned}$$

设  $f, g$  是  $\mathbb{F}$  的二个多项式函数:

$$\begin{aligned} f: & \quad \mathbb{F} \rightarrow \mathbb{F}, \\ t & \mapsto \sum_{i=0}^n a_i t^i, \\ g: & \quad \mathbb{F} \rightarrow \mathbb{F}, \\ t & \mapsto \sum_{i=0}^n b_i t^i. \end{aligned}$$

利用  $\mathbb{F}$  的运算律, 可以得到

$$\begin{aligned} f + g: & \quad \mathbb{F} \rightarrow \mathbb{F}, \\ t & \mapsto \sum_{i=0}^n (a_i + b_i) t^i, \\ fg: & \quad \mathbb{F} \rightarrow \mathbb{F}, \\ t & \mapsto \sum_{i=0}^{2n} \left( \sum_{\ell=0}^i a_\ell b_{i-\ell} \right) t^i. \end{aligned}$$

由此可得下面的命题:



**命题** 设  $f(x), g(x) \in \mathbb{F}[x]$ ,  $f, g$  分别是  $f(x), g(x)$  诱导的多项式函数. 那么  $f + g$  是  $f(x) + g(x)$  诱导的多项式函数, 且  $fg$  是  $f(x)g(x)$  诱导的多项式函数.

通俗地说, 若多项式  $f_0(x), f_1(x), \dots, f_{n-1}(x)$  之间有一个由加法与乘法计算得到的关系, 那么将  $x$  换为  $\mathbb{F}$  的元  $t$ , 这样的关系仍成立.

**定义** 设

$$f(x) = \sum_{i=0}^n a_i x^i \in \mathbb{F}[x].$$

设  $t \in \mathbb{F}$ . 我们把  $\mathbb{F}$  的元

$$\sum_{i=0}^n a_i t^i$$

简单地写为  $f(t)$ , 并称其为多项式  $f(x)$  在点  $t$  的值.

顺便一提,  $f(x)$  的微商也是多项式:

$$f'(x) = \sum_{i=1}^n i a_i x^{i-1}.$$

我们把

$$\sum_{i=1}^n i a_i t^{i-1} \in \mathbb{F}$$

简单地写为  $f'(t)$ .

下面是带余除法的推论. 它在根的讨论里起了重要的作用.

**命题** 设  $f(x) \in \mathbb{F}[x]$  是  $n$  次多项式 ( $n \geq 1$ ),  $a \in \mathbb{F}$ . 则存在  $n-1$  次多项式  $q(x) (\in \mathbb{F}[x])$  使

$$f(x) = q(x)(x - a) + f(a).$$

根据带余除法, 这样的  $q(x)$  一定是唯一的.

**定义** 设  $f(x)$  是  $\mathbb{F}$  上  $x$  的多项式. 若有  $a \in \mathbb{F}$  使  $f(a) = 0$ , 则说  $a$  是 (多项式)  $f(x)$  的根.

**命题** 设  $f(x) \in \mathbb{F}[x]$  是  $n$  次多项式 ( $n \geq 1$ ).  $a$  是  $f(x)$  的根的一个必要与充分条件是: 存在  $n-1$  次多项式  $q(x) (\in \mathbb{F}[x])$  使

$$f(x) = q(x)(x - a).$$

根据带余除法, 这样的  $q(x)$  一定是唯一的.

**命题** 设  $f(x) \in \mathbb{F}[x]$  是  $n$  次多项式 ( $n \in \mathbb{N}$ ). 则  $f(x)$  至多有  $n$  个不同的根.

**评注** 在上节, 我们知道, 整环  $D$  上的多项式  $f(x) = ax + b$  ( $a \neq 0$ ) 不一定有根. 可是, 在域  $\mathbb{F}$  里,  $f(x)$  就有根  $-\frac{b}{a}$ .

**命题** 设  $a_0, a_1, \dots, a_n$  是  $\mathbb{F}$  的元. 设  $n$  是非负整数. 设

$$f(x) = \sum_{i=0}^n a_i x^i.$$

若  $t_0, t_1, \dots, t_n$  是  $n+1$  个互不相同的  $\mathbb{F}$  的元, 且

$$f(t_0) = f(t_1) = \dots = f(t_n) = 0,$$

则  $f(x)$  必为零多项式. 通俗地说, 次不高于  $n$  (且系数为  $\mathbb{F}$  的元) 的多项式不可能有  $n$  个以上的互不相同的根, 除非这个多项式是零.

**命题** 设  $a_0, b_0, a_1, b_1, \dots, a_n, b_n$  是  $\mathbb{F}$  的元. 设  $n$  是非负整数. 设

$$f(x) = \sum_{i=0}^n a_i x^i, \quad g(x) = \sum_{i=0}^n b_i x^i.$$

若  $t_0, t_1, \dots, t_n$  是  $n+1$  个互不相同的  $\mathbb{F}$  的元, 且

$$f(t_0) = g(t_0), \quad f(t_1) = g(t_1), \quad \dots, \quad f(t_n) = g(t_n),$$

则  $f(x)$  必等于  $g(x)$ . 通俗地说, 若次不高于  $n$  (且系数为  $\mathbb{F}$  的元) 的二个多项式若在多于  $n$  处取一样的值, 则这二个多项式相等.

**定义** 设  $a \in \mathbb{F}$  是多项式  $f(x) \in \mathbb{F}[x]$  的根. 那么, 存在唯一的多项式  $q(x) \in \mathbb{F}[x]$  使

$$f(x) = (x - a)q(x).$$

若  $q(a) = 0$ , 则说  $a$  是  $f(x)$  的一个重根. 若  $q(a) \neq 0$ , 则说  $a$  是  $f(x)$  的一个单根.

**命题** 设  $a \in \mathbb{F}$  是多项式  $f(x) \in \mathbb{F}[x]$  的根. 则:

- (i) 若  $a$  是  $f(x)$  的重根, 则  $a$  是  $f'(x)$  的根;
- (ii) 若  $a$  是  $f(x)$  的单根, 则  $a$  不是  $f'(x)$  的根.

所以,  $f(x)$  有重根的一个必要与充分条件是:  $f(x)$  与  $f'(x)$  有公共根.

下面是一些新命题. 由于  $\mathbb{F}$  里有无限多个元, 所以

**命题** 设  $f(x) \in \mathbb{F}[x]$ . 设  $S \subset \mathbb{F}$ , 且  $S$  有无限多个元. 若任取  $t \in S$ , 必有  $f(t) = 0$ , 则  $f(x)$  必为零多项式. 通俗地说, 系数为  $\mathbb{F}$  的元的多项式不可能有无限多个根, 除非这个多项式是零.

**证**  $f(x)$  的次不可能是非负整数. 所以  $f(x)$  只能是 0. ✎

由此立得

**命题** 设  $f(x), g(x) \in \mathbb{F}[x]$ . 设  $S \subset \mathbb{F}$ , 且  $S$  有无限多个元. 若任取  $t \in S$ , 必有  $f(t) = g(t)$ , 则  $f(x)$  与  $g(x)$  是二个相同的多项式. 通俗地说, 若系数为  $\mathbb{F}$  的元的二个多项式在无限多个地方有相同的取值, 则这二个多项式必相等.

**证** 考虑  $h(x) = f(x) - g(x)$ , 并利用上个命题. ✎

前面已经知道, 多项式确定多项式函数. 利用上面的命题, 我们有

**命题**  $\mathbb{F}$  上的多项式与  $\mathbb{F}$  的多项式函数是一一对应的: 不但二个不同的  $\mathbb{F}$  上的多项式给出二个不同的  $\mathbb{F}$  的多项式函数, 而且二个不同的  $\mathbb{F}$  的多项式函数给出二个不同的  $\mathbb{F}$  上的多项式.

**评注** 以后, 我们不再区分“多项式”与“多项式函数”. 从现在开始, 读者可以认为本文接下来讨论的“多项式”跟中学里的多项式是同一事物.

## 插值

本节讨论多项式插值问题.

“插值”听上去可能比较陌生. 不过, 读者在初中一定见过这样的问题:

**例** 已知一次函数的图像经过点  $(-1, 2)$  与  $(1, 3)$ , 求其解析式.

**例** 已知二次函数的图像经过点  $(-1, -1)$ ,  $(1, 1)$  与  $(2, 5)$ , 求其解析式.

在初中, 我们是用“待定系数法” (*the method of undetermined coefficients*) 求解的. 它的基本思想是“求什么, 设什么”. 设此一次函数的解析式为

$$y = ax + b, \quad a \neq 0.$$

代入已知条件, 得到二元一次方程组

$$\begin{cases} 2 = -a + b, \\ 3 = a + b. \end{cases}$$

由此可解出

$$a = \frac{1}{2}, \quad b = \frac{5}{2}.$$

所以此一次函数的解析式为

$$y = \frac{1}{2}x + \frac{5}{2}.$$

完全类似地, 设此二次函数的解析式为

$$y = ax^2 + bx + c, \quad a \neq 0.$$

代入已知条件, 得到三元一次方程组

$$\begin{cases} -1 = a - b + c, \\ 1 = a + b + c, \\ 5 = 4a + 2b + c. \end{cases}$$

由此可解出

$$a = 1, \quad b = 1, \quad c = -1.$$

所以此二次函数的解析式为

$$y = x^2 + x - 1.$$

在初中, 一般用左  $y$  右  $x$  的等式表示函数 (的解析式). 这种表示法强调因变元 (*dependent variable*)  $y$  与自变元 (*independent variable*)  $x$  的关系. 不过, 既然我们有  $f(x)$  这样的记号, 那么因变元就不必写出了. 并且, 我们在前节提到, 我们不再区分多项式与多项式函数. 所以, 为方便, 我们用另一种方式叙述这二个问題:

**例** 求次为 1 的多项式  $f(x)$ , 使  $f(-1) = 2, f(1) = 3$ .

**例** 求次为 2 的多项式  $f(x)$ , 使  $f(-1) = -1, f(1) = 1, f(2) = 5$ .

设  $x_0, x_1, \dots, x_n$  是  $\mathbb{F}$  的  $n+1$  个互不相同的元. 这  $n+1$  个不同的元称为  $n+1$  个节点 (*node*). 设  $y_0, y_1, \dots, y_n \in \mathbb{F}$ . 通俗地说, 多项式插值 (*polynomial interpolation*) 的任务是: 找一个多项式  $f(x) \in \mathbb{F}[x]$  使

$$f(x_i) = y_i \quad (i = 0, 1, \dots, n),$$

且适合“附加条件”.

这里, “附加条件”是有必要的: 如果太松, 可能找出的  $f(x)$  不止一个; 如果太紧, 则可能找不到  $f(x)$ .

**例** 找一个多项式  $f(x)$  使  $f(-1) = -1, f(0) = 0, f(1) = 1$ .

如果不作任何别的约束, 那么  $n$  是奇数时,  $f(x) = x^n$  适合这些条件. 不仅如此, 下面的多项式也适合条件:

$$\frac{1}{6}x + \frac{1}{3}x^3 + \frac{1}{2}x^5, \quad -x + 2x^7, \quad \frac{x + x^3 + \dots + x^{2k-1}}{k}.$$

在初中, 我们知道, 若平面直角坐标系的三点  $A, B, C$  不在同一直线上, 且任意二点的连线既不与  $y$  轴平行也不与  $y$  轴重合, 则存在 (唯一的) 二

次函数  $y = ax^2 + bx + c$  ( $a \neq 0$ ) 使其图像过此三点. 假如“附加条件”是“ $f(x)$  是次为 2 的多项式”呢? 设

$$f(x) = ax^2 + bx + c, \quad a \neq 0.$$

代入已知条件, 得到三元一次方程组

$$\begin{cases} -1 = a - b + c, \\ 0 = c, \\ 1 = a + b + c. \end{cases}$$

由此可解出

$$a = 0, \quad b = 1, \quad c = 0.$$

这与假定  $a \neq 0$  不符. 所以, 这个条件太紧了.

有没有什么“松紧得当的”“附加条件”呢? 回想一下这个命题:

**命题** 设  $a_0, b_0, a_1, b_1, \dots, a_n, b_n$  是  $\mathbb{F}$  的元. 设  $n$  是非负整数. 设

$$f(x) = \sum_{i=0}^n a_i x^i, \quad g(x) = \sum_{i=0}^n b_i x^i.$$

若  $t_0, t_1, \dots, t_n$  是  $n+1$  个互不相同的  $\mathbb{F}$  的元, 且

$$f(t_0) = g(t_0), \quad f(t_1) = g(t_1), \quad \dots, \quad f(t_n) = g(t_n),$$

则  $f(x)$  必等于  $g(x)$ . 通俗地说, 若次不高于  $n$  (且系数为  $\mathbb{F}$  的元) 的二个多项式若在多于  $n$  处取一样的值, 则这二个多项式相等.

由此, 我们可以试着作出这样的“附加条件”: 多项式的次低于节点数. 至少, 这个条件不是太松: 因为上面的命题说, 这样的多项式若存在, 必唯一.

这个“附加条件”一定能让我们求出这个多项式吗? 不好说.



**证** 先看充分性. 既然  $f(x)$  能写为这种形式, 将  $x$  换为  $t_i$  ( $i = 0, 1, \dots, s-1$ ), 则有  $f(t_i) = 0$ .

再看必要性. 因为  $t_0$  是  $f(x)$  的根, 故存在  $n-1$  次多项式  $q_1(x) \in \mathbb{F}[x]$  使

$$f(x) = (x - t_0)q_1(x).$$

设  $t_j$  是  $t_1, t_2, \dots, t_{s-1}$  的一个. 则  $t_j \neq t_0$ . 因为  $t_j$  也是  $f(x)$  的根, 故

$$(t_j - t_0)q_1(t_j) = f(t_j) = 0 = (t_j - t_0)0.$$

根据消去律,  $q_1(t_j) = 0$ . 这样,  $t_1, \dots, t_{s-1}$  这  $s-1$  个  $\mathbb{F}$  中元是  $q_1(x)$  的根. 所以, 对  $q_1(x)$  来说, 存在  $n-1-1 = n-2$  次多项式  $q_2(x) \in \mathbb{F}[x]$  使

$$q_1(x) = (x - t_1)q_2(x) \implies f(x) = (x - t_0)(x - t_1)q_2(x),$$

且  $t_2, \dots, t_{s-1}$  这  $s-2$  个  $\mathbb{F}$  中元是  $q_2(x)$  的根. 再将这个过程进行  $s-2$  次, 可得到  $n-s$  次多项式  $q_s(x) \in \mathbb{F}[x]$  使

$$f(x) = (x - t_0)(x - t_1) \cdots (x - t_{s-1})q_s(x).$$

取  $q(x) = q_s(x)$  即可. ✎

**例** 我们考虑非常特殊的情形. 如果  $y_0, y_1, \dots, y_n$  中恰有一个是 1, 而剩下的全是 0, 那这样的多项式应该长什么样呢?

以  $y_0 = 1, y_1 = y_2 = \dots = y_n = 0$  为例. 这样, 多项式  $f(x)$  有根  $x_1, x_2, \dots, x_n$ . 根据上个命题, 存在多项式  $q(x)$  使

$$f(x) = q(x)(x - x_1)(x - x_2) \cdots (x - x_n).$$

因为  $f(x)$  的次低于  $n+1$ , 而  $(x - x_1)(x - x_2) \cdots (x - x_n)$  的次为  $n$ , 故  $q(x)$  一定是非零数  $c$ , 即

$$f(x) = c(x - x_1)(x - x_2) \cdots (x - x_n).$$

因为  $f(x_0) = y_0 = 1$ , 故

$$1 = c(x_0 - x_1)(x_0 - x_2) \cdots (x_0 - x_n),$$



也就是

$$c = \frac{1}{(x_0 - x_1)(x_0 - x_2) \cdots (x_0 - x_n)}.$$

故

$$f(x) = \frac{(x - x_1)(x - x_2) \cdots (x - x_n)}{(x_0 - x_1)(x_0 - x_2) \cdots (x_0 - x_n)}.$$

类似地, 适合条件  $y_1 = 1, y_0 = y_2 = y_3 = \cdots = y_n = 0$  的多项式是

$$\frac{(x - x_0)(x - x_2)(x - x_3) \cdots (x - x_n)}{(x_1 - x_0)(x_1 - x_2)(x_1 - x_3) \cdots (x_1 - x_n)}.$$

可以将这个多项式简单地写为

$$\prod_{\substack{0 \leq \ell \leq n \\ \ell \neq 1}} \frac{x - x_\ell}{x_1 - x_\ell}.$$

上面的  $f(x)$  也可以写为

$$\prod_{\substack{0 \leq \ell \leq n \\ \ell \neq 0}} \frac{x - x_\ell}{x_0 - x_\ell}.$$

回到一般的设定 (也就是说,  $y_0, y_1, \dots, y_n$  是  $\mathbb{F}$  的任意元). 作  $n+1$  个多项式

$$L_i(x) = \prod_{\substack{0 \leq \ell \leq n \\ \ell \neq i}} \frac{x - x_\ell}{x_i - x_\ell} \quad (i = 0, 1, \dots, n).$$

不难看出, 任取  $i, j = 0, 1, \dots, n$ ,

$$L_i(x_j) = \begin{cases} 1, & i = j; \\ 0, & i \neq j. \end{cases}$$

所以

$$f(x) = \sum_{i=0}^n y_i L_i(x) = y_0 L_0(x) + y_1 L_1(x) + \cdots + y_n L_n(x)$$

适合条件

$$f(x_i) = y_i \quad (i = 0, 1, \dots, n),$$

且

$$\deg f(x) \leq n < n + 1.$$

综合上面的事实, 我们已经证明了

**命题** 设  $x_0, x_1, \dots, x_n$  是  $\mathbb{F}$  的  $n + 1$  个互不相同的元. 设  $y_0, y_1, \dots, y_n \in \mathbb{F}$ . 存在唯一的多项式

$$f(x) = \sum_{i=0}^n y_i \prod_{\substack{0 \leq \ell \leq n \\ \ell \neq i}} \frac{x - x_\ell}{x_i - x_\ell}$$

适合条件

$$f(x_i) = y_i \quad (i = 0, 1, \dots, n),$$

且

$$\deg f(x) < n + 1.$$

这个公式的一个名字是 “Lagrange 插值公式” (*Lagrange's interpolation formula*).

**评注** 我们在前面接触的线性无关的多项式组 (几乎都) 是次不等的多项式. Lagrange 插值公式告诉我们,  $L_0(x), L_1(x), \dots, L_n(x)$  适合:

- (i)  $L_0(x), L_1(x), \dots, L_n(x)$  是线性无关的;
- (ii) 任意次不高于  $n$  的多项式都可唯一地写为  $L_0(x), L_1(x), \dots, L_n(x)$  的线性组合;
- (iii)  $L_0(x), L_1(x), \dots, L_n(x)$  全为  $n$  次多项式.

**评注** 由上面的公式, 可以看出,  $f(x)$  的  $n$  次系数是

$$\sum_{i=0}^n y_i \prod_{\substack{0 \leq \ell \leq n \\ \ell \neq i}} \frac{1}{x_i - x_\ell}.$$

看上去有点复杂. 我们想个办法简单地写出  $\prod$  符号代表的内容. 作  $n+1$  次多项式

$$N_{n+1}(x) = (x - x_0)(x - x_1) \cdots (x - x_n).$$

从  $0, 1, \dots, n$  里任取一个整数  $i$ . 那么

$$N_{n+1}(x) = (x - x_i) \prod_{\substack{0 \leq \ell \leq n \\ \ell \neq i}} (x - x_\ell).$$

二边求微商, 有

$$N'_{n+1}(x) = \prod_{\substack{0 \leq \ell \leq n \\ \ell \neq i}} (x - x_\ell) + (x - x_i) \left( \prod_{\substack{0 \leq \ell \leq n \\ \ell \neq i}} (x - x_\ell) \right)'.$$

用  $x_i$  代替  $x$ , 有

$$N'_{n+1}(x) = \prod_{\substack{0 \leq \ell \leq n \\ \ell \neq i}} (x_i - x_\ell) + 0,$$

即

$$\prod_{\substack{0 \leq \ell \leq n \\ \ell \neq i}} \frac{1}{x_i - x_\ell} = \frac{1}{N'_{n+1}(x_i)}.$$

这样,  $f(x)$  的  $n$  次系数可简单地写为

$$\sum_{i=0}^n \frac{y_i}{N'_{n+1}(x_i)}.$$

**例** 取  $n = 2$ . 取

$$\begin{aligned} x_0 &= -1, & x_1 &= 1, & x_2 &= 2, \\ y_0 &= -1, & y_1 &= 1, & y_2 &= 5. \end{aligned}$$

计算  $L_0(x)$ ,  $L_1(x)$ ,  $L_2(x)$ :

$$L_0(x) = \prod_{\substack{0 \leq \ell \leq 2 \\ \ell \neq 0}} \frac{x - x_\ell}{x_0 - x_\ell} = \frac{(x-1)(x-2)}{(-1-1)(-1-2)} = \frac{1}{6}x^2 - \frac{1}{2}x + \frac{1}{3},$$

$$L_1(x) = \prod_{\substack{0 \leq \ell \leq 2 \\ \ell \neq 1}} \frac{x - x_\ell}{x_1 - x_\ell} = \frac{(x+1)(x-2)}{(1+1)(1-2)} = -\frac{1}{2}x^2 + \frac{1}{2}x + 1,$$

$$L_2(x) = \prod_{\substack{0 \leq \ell \leq 2 \\ \ell \neq 2}} \frac{x - x_\ell}{x_2 - x_\ell} = \frac{(x+1)(x-1)}{(2+1)(2-1)} = \frac{1}{3}x^2 - \frac{1}{3}.$$

所以, 适合条件

$$f(-1) = -1, \quad f(1) = 1, \quad f(2) = 5,$$

$$\deg f(x) < n+1 = 3$$

的多项式  $f(x)$  就是

$$\begin{aligned} & (-1)L_0(x) + 1L_1(x) + 5L_2(x) \\ &= -L_0(x) + L_1(x) + 5L_2(x) \\ &= -\frac{1}{6}x^2 + \frac{1}{2}x - \frac{1}{3} - \frac{1}{2}x^2 + \frac{1}{2}x + 1 + \frac{5}{3}x^2 - \frac{5}{3} \\ &= x^2 + x - 1. \end{aligned}$$

这跟前面用三元一次方程组算出的答案完全一致.

**例** 取  $n = 3$ . 在上例的基础上, 追加

$$x_3 = -2, \quad y_3 = -11.$$

我们的目标是: 找多项式  $f(x)$  适合条件

$$f(-1) = -1, \quad f(1) = 1, \quad f(2) = 5, \quad f(-2) = -11,$$

$$\deg f(x) < n+1 = 4.$$

在原理上, 并没有什么复杂的地方. 求出  $L_0(x)$ ,  $L_1(x)$ ,  $L_2(x)$ ,  $L_3(x)$  后, 答案就出来了:

$$\begin{aligned} f(x) = & -\frac{(x-1)(x-2)(x+2)}{(-1-1)(-1-2)(-1+2)} + \frac{(x+1)(x-2)(x+2)}{(1+1)(1-2)(1+2)} \\ & + 5 \cdot \frac{(x+1)(x-1)(x+2)}{(2+1)(2-1)(2+2)} - 11 \cdot \frac{(x+1)(x-1)(x-2)}{(-2+1)(-2-1)(-2-2)}. \end{aligned}$$

不过, 实践告诉我们, 拆开 4 个 3 次多项式后再相加可不是什么轻松的事儿——至少比前一个例复杂一些. 而且, 加一个节点后,  $L_0(x)$ ,  $L_1(x)$ ,  $L_2(x)$  (跟之前相比) 都要多乘一个一次多项式. 有无稍微容易一些算法呢?

**定义** 设  $x_0, x_1, \dots, x_n$  是  $\mathbb{F}$  的  $n+1$  个互不相同的元. 设  $y_0, y_1, \dots, y_n \in \mathbb{F}$ . 定义

$$[x_i, x_j] = \frac{y_i - y_j}{x_i - x_j} \quad (i \neq j).$$

这称为 1 级差商 (*first-order divided difference*). 类似地, 当  $i, j, k$  互不相同, 2 级差商是

$$[x_i, x_j, x_k] = \frac{[x_i, x_j] - [x_j, x_k]}{x_i - x_k}.$$

一般地, 当  $i_0, i_1, \dots, i_{\ell-1}$  互不相同,  $\ell-1$  级差商定义为

$$[x_{i_0}, x_{i_1}, \dots, x_{i_{\ell-1}}] = \frac{[x_{i_0}, x_{i_1}, \dots, x_{i_{\ell-2}}] - [x_{i_1}, x_{i_2}, \dots, x_{i_{\ell-1}}]}{x_{i_0} - x_{i_{\ell-1}}}.$$

“差商”可指代任意级差商. 高级差商可任意指代  $\ell$  级差商, 此处  $\ell > 1$ .

**例** 取  $n = 2$ . 取

$$\begin{aligned} x_0 &= -1, & x_1 &= 1, & x_2 &= 2, \\ y_0 &= -1, & y_1 &= 1, & y_2 &= 5. \end{aligned}$$

我们随意地计算三个 1 级差商:

$$\begin{aligned} [x_0, x_1] &= \frac{y_0 - y_1}{x_0 - x_1} = 1, \\ [x_0, x_2] &= \frac{y_0 - y_2}{x_0 - x_2} = 2, \\ [x_1, x_2] &= \frac{y_1 - y_2}{x_1 - x_2} = 4. \end{aligned}$$

由此可知

$$[x_0, x_1, x_2] = \frac{[x_0, x_1] - [x_1, x_2]}{x_0 - x_2} = \frac{1 - 4}{-1 - 2} = 1.$$

根据 1 级差商的定义,

$$[x_j, x_i] = \frac{y_j - y_i}{x_j - x_i} = \frac{y_i - y_j}{x_i - x_j} = [x_i, x_j],$$

故

$$[x_2, x_1] = [x_1, x_2] = 4.$$

所以

$$[x_0, x_2, x_1] = \frac{[x_0, x_2] - [x_2, x_1]}{x_0 - x_1} = \frac{2 - 4}{-1 - 1} = 1.$$

同样的道理,

$$[x_1, x_0] = [x_0, x_1] = 1.$$

所以

$$[x_1, x_0, x_2] = \frac{[x_1, x_0] - [x_0, x_2]}{x_1 - x_2} = \frac{1 - 2}{1 - 2} = 1.$$

我们发现, 在这些特殊的  $x_i$  与  $y_j$  ( $i, j = 0, 1, 2$ ) 下

$$[x_0, x_1, x_2] = [x_0, x_2, x_1] = [x_1, x_0, x_2].$$

类似地, 读者还可以计算  $[x_1, x_2, x_0]$ ,  $[x_2, x_0, x_1]$ ,  $[x_2, x_1, x_0]$ , 它们跟上面三个 2 级差商有着同样的值. 换句话说, 我们猜想, 2 级差商  $[x_i, x_j, x_k]$  的三个文字  $x_i, x_j, x_k$  的次序可以任意交换, 且值不变 (当然,  $y_i, y_j, y_k$  的次序也要交换).

幸运的事儿是, 我们没猜错:

**命题** 设  $m$  是高于 1 的整数.  $m - 1$  级差商  $[x_0, x_1, \dots, x_{m-1}]$  可表示为

$$[x_0, x_1, \dots, x_{m-1}] = \sum_{k=0}^{m-1} \frac{y_k}{N'_m(x_k)},$$

这里

$$N_m(x) = (x - x_0)(x - x_1) \cdots (x - x_{m-1}) = \prod_{k=0}^{m-1} (x - x_k).$$

由此立得: 随意交换  $x_0, x_1, \dots, x_{m-1}$  的次序, 若  $y_0, y_1, \dots, y_{m-1}$  的次序也跟着改变, 得到的新  $m - 1$  级差商的值不变.

**证** 回想一下,  $\ell$  级差商 ( $\ell > 1$ ) 是用  $\ell - 1$  级差商定义的. 所以, 我们用数学归纳法证明这个结论.

当  $m = 2$  时,

$$N_2(x) = (x - x_0)(x - x_1) = x^2 - (x_0 + x_1)x + x_0x_1,$$

故

$$N_2'(x) = 2x - (x_0 + x_1).$$

从而

$$N_2'(x_0) = x_0 - x_1, \quad N_2'(x_1) = x_1 - x_0.$$

根据定义,

$$\begin{aligned} [x_0, x_1] &= \frac{y_0 - y_1}{x_0 - x_1} \\ &= \frac{y_0}{x_0 - x_1} - \frac{y_1}{x_0 - x_1} \\ &= \frac{y_0}{x_0 - x_1} + \frac{y_1}{x_1 - x_0} \\ &= \frac{y_0}{N_2'(x_0)} + \frac{y_1}{N_2'(x_1)} \\ &= \sum_{k=0}^{2-1} \frac{y_k}{N_2'(x_k)}. \end{aligned}$$

所以, 结论对  $m = 2$  成立.

假设结论对  $m = \ell \geq 2$  成立. 我们要由此推出: 结论对  $m = \ell + 1$  也成立.  $x_0, x_1, \dots, x_\ell$  这  $\ell + 1$  个元的  $\ell$  级差商, 按定义, 是

$$[x_0, x_1, \dots, x_\ell] = \frac{[x_0, x_1, \dots, x_{\ell-1}] - [x_1, x_2, \dots, x_\ell]}{x_0 - x_\ell}.$$

这里,  $[x_0, x_1, \dots, x_{\ell-1}]$  与  $[x_1, x_2, \dots, x_\ell]$  都是  $\ell - 1$  级差商. 按归纳假设,

$$\begin{aligned} [x_0, x_1, \dots, x_{\ell-1}] &= \sum_{k=0}^{\ell-1} \frac{y_k}{P'(x_k)}, \\ [x_1, x_2, \dots, x_\ell] &= \sum_{k=1}^{\ell} \frac{y_k}{Q'(x_k)}, \end{aligned}$$

其中

$$\begin{aligned} P(x) &= (x - x_0)(x - x_1) \cdots (x - x_{\ell-1}), \\ Q(x) &= (x - x_1)(x - x_2) \cdots (x - x_\ell). \end{aligned}$$

作

$$N_{\ell+1}(x) = (x - x_0)(x - x_1) \cdots (x - x_{\ell-1})(x - x_\ell),$$

我们观察  $N_{\ell+1}(x)$  与  $P(x)$  (或  $Q(x)$ ) 的关系. 显然,

$$N_{\ell+1}(x) = P(x)(x - x_\ell).$$

二边求微商, 有

$$N'_{\ell+1}(x) = P'(x)(x - x_\ell) + P(x).$$

用  $x_u$  ( $u \neq \ell$ ) 代替  $x$ , 有

$$\begin{aligned} N'_{\ell+1}(x_u) &= P'(x_u)(x_u - x_\ell) + P(x_u) = P'(x_u)(x_u - x_\ell) \\ \implies \frac{1}{P'(x_u)} &= \frac{x_u - x_\ell}{N'_{\ell+1}(x_u)}. \end{aligned}$$

同理, 若  $v \neq 0$ , 则

$$\frac{1}{Q'(x_v)} = \frac{x_v - x_0}{N'_{\ell+1}(x_v)}.$$

所以

$$\begin{aligned} & [x_0, x_1, \cdots, x_{\ell-1}] - [x_1, x_2, \cdots, x_\ell] \\ &= \sum_{k=0}^{\ell-1} \frac{y_k}{P'(x_k)} - \sum_{k=1}^{\ell} \frac{y_k}{Q'(x_k)} \\ &= \sum_{k=0}^{\ell-1} \frac{y_k(x_k - x_\ell)}{N'_{\ell+1}(x_k)} + \sum_{k=1}^{\ell} \frac{-y_k(x_k - x_0)}{N'_{\ell+1}(x_k)} \\ &= \sum_{k=0}^{\ell} \frac{y_k(x_k - x_\ell)}{N'_{\ell+1}(x_k)} + \sum_{k=0}^{\ell} \frac{y_k(x_0 - x_k)}{N'_{\ell+1}(x_k)} \end{aligned}$$



$$\begin{aligned}
&= \sum_{k=0}^{\ell} \frac{y_k(x_k - x_{\ell}) + y_k(x_0 - x_k)}{N'_{\ell+1}(x_k)} \\
&= \sum_{k=0}^{\ell} \frac{y_k(x_0 - x_{\ell})}{N'_{\ell+1}(x_k)} \\
&= (x_0 - x_{\ell}) \sum_{k=0}^{\ell} \frac{y_k}{N'_{\ell+1}(x_k)}.
\end{aligned}$$

这样

$$\begin{aligned}
[x_0, x_1, \dots, x_{\ell}] &= \frac{[x_0, x_1, \dots, x_{\ell-1}] - [x_1, x_2, \dots, x_{\ell}]}{x_0 - x_{\ell}} \\
&= \frac{1}{x_0 - x_{\ell}} \cdot (x_0 - x_{\ell}) \sum_{k=0}^{\ell} \frac{y_k}{N'_{\ell+1}(x_k)} \\
&= \sum_{k=0}^{(\ell+1)-1} \frac{y_k}{N'_{\ell+1}(x_k)}. \quad \text{☺}
\end{aligned}$$

**评注** 前面, 我们知道, 用 Lagrange 插值公式算出的次不高于  $n$  的多项式的  $n$  次系数是

$$\sum_{i=0}^n \frac{y_i}{N'_{n+1}(x_i)},$$

其中

$$N_{n+1}(x) = (x - x_0)(x - x_1) \cdots (x - x_n).$$

用差商的语言, 有:  $f(x)$  的  $n$  次系数可用  $n$  级差商

$$[x_0, x_1, \dots, x_n]$$

表示.

现在, 我们来看看差商在多项式插值里的用处. 设  $x_0, x_1, \dots, x_n$  是  $\mathbb{F}$

的  $n+1$  个互不相同的元. 设  $y_0, y_1, \dots, y_n \in \mathbb{F}$ . 作  $n+1$  个多项式:

$$\begin{aligned} N_0(x) &= 1, \\ N_1(x) &= x - x_0, \\ N_2(x) &= (x - x_0)(x - x_1), \\ &\dots\dots\dots, \\ N_n(x) &= (x - x_0)(x - x_1) \cdots (x - x_{n-1}). \end{aligned}$$

因为  $N_0(x), N_1(x), \dots, N_n(x)$  的次分别是  $0, 1, \dots, n$ , 所以:

- (i)  $N_0(x), N_1(x), \dots, N_n(x)$  是线性无关的;
- (ii) 任意次不高于  $n$  的多项式都可唯一地写为  $N_0(x), N_1(x), \dots, N_n(x)$

的线性组合.

由前面的 Lagrange 插值公式可知, 存在一个次不高于  $n$  的多项式  $f(x)$  使

$$f(x_i) = y_i \quad (i = 0, 1, \dots, n).$$

对这个  $f(x)$  而言, 存在 (唯一的)  $c_0, c_1, \dots, c_n \in \mathbb{F}$  使

$$f(x) = \sum_{i=0}^n c_i N_i(x).$$

我们的任务就是找出  $c_0, c_1, \dots, c_n$ . 先从  $c_n$  看起. 显然, 左侧的  $n$  次系数是  $[x_0, x_1, \dots, x_n]$ , 而右侧的  $n$  次系数是  $c_n$ , 故

$$c_n = [x_0, x_1, \dots, x_n].$$

找出  $c_n$ , 还有  $n$  个系数要找呢! 接下来的系数该怎么找呢?

**命题** 设  $x_0, x_1, \dots, x_n$  是  $\mathbb{F}$  的  $n+1$  个互不相同的元 ( $n \geq 1$ ). 设  $y_0, y_1, \dots, y_n \in \mathbb{F}$ . 作  $n+1$  个多项式:

$$\begin{aligned} N_0(x) &= 1, \\ N_1(x) &= x - x_0, \\ N_2(x) &= (x - x_0)(x - x_1), \\ &\dots\dots\dots, \\ N_n(x) &= (x - x_0)(x - x_1) \cdots (x - x_{n-1}). \end{aligned}$$

由 Lagrange 插值公式可知, 存在一个次不高于  $n$  的多项式  $f(x)$  使

$$f(x_i) = y_i \quad (i = 0, 1, \dots, n).$$

对这个  $f(x)$  而言, 存在 (唯一的)  $c_0, c_1, \dots, c_n \in \mathbb{F}$  使

$$f(x) = \sum_{i=0}^n c_i N_n(x).$$

这些系数有着简单的形式:

$$c_0 = y_0,$$

$$c_i = [x_0, x_1, \dots, x_i] \quad (i = 1, 2, \dots, n).$$

**证** 用数学归纳法. 当  $n = 1$  时,

$$\begin{aligned} f(x) &= y_0 \frac{x - x_1}{x_0 - x_1} + y_1 \frac{x - x_0}{x_1 - x_0} \\ &= y_0 \frac{(x - x_0) + (x_0 - x_1)}{x_0 - x_1} - y_1 \frac{x - x_0}{x_0 - x_1} \\ &= y_0 + y_0 \frac{x - x_0}{x_0 - x_1} - y_1 \frac{x - x_0}{x_0 - x_1} \\ &= y_0 + \frac{y_0 - y_1}{x_0 - x_1} (x - x_0) \\ &= y_0 N_0(x) + [x_0, x_1] N_1(x). \end{aligned}$$

这样, 结论对  $n = 1$  成立.

设结论对  $n = \ell \geq 1$  成立. 我们看  $n = \ell + 1$  的情形.

由 Lagrange 插值公式可知, 存在一个次不高于  $\ell + 1$  的多项式  $f(x)$  使

$$f(x_i) = y_i \quad (i = 0, 1, \dots, \ell + 1).$$

对这个  $f(x)$  而言, 存在 (唯一的)  $c_0, c_1, \dots, c_\ell, c_{\ell+1} \in \mathbb{F}$  使

$$f(x) = \sum_{i=0}^{\ell} c_i N_i(x) + c_{\ell+1} N_{\ell+1}(x).$$

左侧的  $\ell + 1$  次系数是  $[x_0, x_1, \dots, x_\ell, x_{\ell+1}]$ , 右侧的  $\ell + 1$  次系数是  $c_{\ell+1}$ , 故

$$c_{\ell+1} = [x_0, x_1, \dots, x_\ell, x_{\ell+1}].$$

作

$$g(x) = f(x) - [x_0, x_1, \dots, x_\ell, x_{\ell+1}]N_{\ell+1}(x).$$

则

$$g(x) = \sum_{i=0}^{\ell} c_i N_i(x),$$

且  $i \neq \ell + 1$  时,

$$g(x_i) = f(x_i) - [x_0, x_1, \dots, x_\ell, x_{\ell+1}]0 = y_i.$$

这个  $g(x)$  的次不会高于  $\ell$ . 并且,  $i = 0, 1, \dots, \ell$  时,  $g(x_i) = y_i$ .

由 Lagrange 插值公式, 存在一个次不高于  $\ell$  的多项式  $h(x)$  使

$$h(x_i) = y_i \quad (i = 0, 1, \dots, \ell).$$

对这个  $h(x)$  而言, 存在 (唯一的)  $d_0, d_1, \dots, d_\ell \in \mathbb{F}$  使

$$h(x) = \sum_{i=0}^{\ell} d_i N_i(x).$$

根据归纳假设,

$$d_0 = y_0,$$

$$d_i = [x_0, x_1, \dots, x_i] \quad (i = 1, 2, \dots, \ell).$$

由插值的唯一性,  $g(x) = h(x)$ . 所以

$$c_0 = d_0 = y_0,$$

$$c_i = d_i = [x_0, x_1, \dots, x_i] \quad (i = 1, 2, \dots, \ell).$$

所以,  $n = \ell + 1$  时, 结论是正确的.

✎

为方便, 记  $[x_i] = y_i$ , 称其为  $x_i$  的 0 级差商. 我们证明了

**命题** 设  $x_0, x_1, \dots, x_n$  是  $\mathbb{F}$  的  $n+1$  个互不相同的元. 设  $y_0, y_1, \dots, y_n \in \mathbb{F}$ . 存在唯一的多项式

$$\begin{aligned} f(x) &= \sum_{i=0}^n [x_0, x_1, \dots, x_i] \prod_{j=0}^{i-1} (x - x_j) \\ &= [x_0] + [x_0, x_1](x - x_0) + \dots + [x_0, x_1, \dots, x_n](x - x_0) \\ &\quad \cdot (x - x_1) \cdots (x - x_{n-1}) \end{aligned}$$

适合条件

$$f(x_i) = y_i \quad (i = 0, 1, \dots, n),$$

且

$$\deg f(x) < n + 1.$$

这个公式的一个名字是 “Newton 插值公式” (*Newton's interpolation formula*).

我们举三个具体的例帮读者消化这个 Newton 插值公式.

**例** 求次不高于 1 的多项式  $f(x)$ , 使  $f(-1) = 2, f(1) = 3$ .

这里,  $n = 1$ , 且

$$x_0 = -1, \quad x_1 = 1,$$

$$y_0 = 2, \quad y_1 = 3.$$

不难算出

$$[x_0] = y_0 = 2,$$

$$[x_0, x_1] = \frac{y_0 - y_1}{x_0 - x_1} = \frac{1}{2}.$$

所以

$$f(x) = 2 + \frac{1}{2}(x - (-1)) = \frac{1}{2}x + \frac{5}{2}.$$

**例** 求次不高于 2 的多项式  $f(x)$ , 使  $f(-1) = -1$ ,  $f(1) = 1$ ,  $f(2) = 5$ .  
这里,  $n = 2$ , 且

$$\begin{aligned}x_0 &= -1, & x_1 &= 1, & x_2 &= 2, \\y_0 &= -1, & y_1 &= 1, & y_2 &= 5.\end{aligned}$$

不难算出

$$\begin{aligned}[x_0] &= y_0 = -1, \\[x_0, x_1] &= \frac{y_0 - y_1}{x_0 - x_1} = 1, \\[x_1, x_2] &= \frac{y_1 - y_2}{x_1 - x_2} = 4, \\[x_0, x_1, x_2] &= \frac{[x_0, x_1] - [x_1, x_2]}{x_0 - x_2} = 1.\end{aligned}$$

所以

$$f(x) = -1 + (x + 1) + (x + 1)(x - 1) = x^2 + x - 1.$$

前面, 我们用 Lagrange 插值公式, 得到了一样的结果, 不过计算过程稍繁.

实操时, 往往用名为“差商表”的表进行计算. 当  $n = 2$  时, 它长这样:

$$\begin{array}{c|ccc}x_2 & [x_2] & & \\x_1 & [x_1] & [x_1, x_2] & \\x_0 & [x_0] & [x_0, x_1] & [x_0, x_1, x_2]\end{array}$$

在这个问题里, 差商表如下:

$$\begin{array}{c|ccc}2 & 5 & & \\1 & 1 & 4 & \\-1 & -1 & 1 & 1\end{array}$$

**例** 求次不高于 3 的多项式  $f(x)$ , 使  $f(-1) = -1$ ,  $f(1) = 1$ ,  $f(2) = 5$ ,  $f(-2) = -11$ .

这里,  $n = 3$ , 且

$$\begin{aligned}x_0 &= -1, & x_1 &= 1, & x_2 &= 2, & x_3 &= -2 \\y_0 &= -1, & y_1 &= 1, & y_2 &= 5, & y_3 &= -11.\end{aligned}$$

画出  $n = 3$  时的差商表:

$x_3$	$[x_3]$			
$x_2$	$[x_2]$	$[x_2, x_3]$		
$x_1$	$[x_1]$	$[x_1, x_2]$	$[x_1, x_2, x_3]$	
$x_0$	$[x_0]$	$[x_0, x_1]$	$[x_0, x_1, x_2]$	$[x_0, x_1, x_2, x_3]$

我们已经在上个例里算出了  $[x_0, x_1]$ ,  $[x_1, x_2]$ ,  $[x_0, x_1, x_2]$ :

$x_3$	$[x_3]$			
2	1	$[x_2, x_3]$		
1	1	4	$[x_1, x_2, x_3]$	
-1	-1	1	1	$[x_0, x_1, x_2, x_3]$

我们的目标是算出  $[x_0, x_1, x_2, x_3]$ . 所以, 我们要算出  $[x_1, x_2, x_3]$ ; 所以, 我们要算出  $[x_2, x_3]$ ; 所以, 我们要算出  $[x_3]$ . 不过,  $[x_3]$  是已知的, 它就是  $y_3$ , 也就是  $-11$ .

列出算式:

$$\begin{aligned}
 x_3 &= -2, \\
 [x_3] &= y_3 = -11, \\
 [x_2, x_3] &= \frac{y_2 - y_3}{x_2 - x_3} = 4, \\
 [x_1, x_2, x_3] &= \frac{[x_1, x_2] - [x_2, x_3]}{x_1 - x_3} = 0, \\
 [x_0, x_1, x_2, x_3] &= \frac{[x_0, x_1, x_2] - [x_1, x_2, x_3]}{x_0 - x_3} = 1.
 \end{aligned}$$

此时, 差商表如下:

$-2$	$-11$			
2	1	4		
1	1	4	0	
-1	-1	1	1	1

所以

$$\begin{aligned} f(x) &= -1 + (x+1) + (x+1)(x-1) + (x+1)(x-1)(x-2) \\ &= (x^2 + x - 1) + (x^3 - 2x^2 - x + 2) \\ &= x^3 - x^2 + 1. \end{aligned}$$

用 Lagrange 插值公式, 有

$$\begin{aligned} f(x) &= -\frac{(x-1)(x-2)(x+2)}{(-1-1)(-1-2)(-1+2)} + \frac{(x+1)(x-2)(x+2)}{(1+1)(1-2)(1+2)} \\ &\quad + 5 \cdot \frac{(x+1)(x-1)(x+2)}{(2+1)(2-1)(2+2)} - 11 \cdot \frac{(x+1)(x-1)(x-2)}{(-2+1)(-2-1)(-2-2)}. \end{aligned}$$

有兴趣的读者可展开上式, 以验证我们的计算是否正确. 由此可见, Newton 插值公式在实操上优于 Lagrange 插值公式.

我们以带余除法与插值的关系结束本节.

**命题** 设  $x_0, x_1, \dots, x_n$  是  $\mathbb{F}$  的  $n+1$  个互不相同的元. 设

$$d(x) = (x-x_0)(x-x_1)\cdots(x-x_n) \in \mathbb{F}[x]$$

是  $n+1$  次多项式. 由带余除法知, 任取  $f(x) \in \mathbb{F}[x]$ , 存在唯一的  $q(x)$ ,  $r(x) \in \mathbb{F}[x]$  使

$$f(x) = q(x)d(x) + r(x), \quad \deg r(x) < n+1.$$

余式  $r(x)$  可具体地写出:

$$r(x) = \sum_{i=0}^n f(x_i) \prod_{\substack{0 \leq \ell \leq n \\ \ell \neq i}} \frac{x - x_\ell}{x_i - x_\ell}$$

或

$$r(x) = \sum_{i=0}^n [x_0, x_1, \dots, x_i] \prod_{j=0}^{i-1} (x - x_j),$$

其中差商的  $y_i$  取  $f(x_i)$ ,  $i = 0, 1, \dots, n$ .



**证** 由带余除法知, 任取  $f(x) \in \mathbb{F}[x]$ , 存在唯一的  $q(x), r(x) \in \mathbb{F}[x]$  使

$$f(x) = q(x)d(x) + r(x), \quad \deg r(x) < n + 1.$$

用  $x_i$  代替  $x$ , 有

$$f(x_i) = q(x_i)d(x_i) + r(x_i) = r(x_i).$$

因为  $\deg r(x) < n + 1$ , 故由插值公式即得待证命题.

✎

## 广义二项系数

本节讨论广义二项系数.

回忆一下: 正整数  $n$  的阶乘  $n!$  是前  $n$  个正整数的积; 0 的阶乘  $0!$  是 1.

**定义** 设  $n$  是整数. 设  $r \in \mathbb{F}[x]$ . 定义广义二项系数 (*generalized binomial coefficient*) 如下:

$$\binom{r}{n} = \begin{cases} \frac{1}{n!}(r-0)(r-1)\cdots(r-(n-1)), & n > 0; \\ 1, & n = 0; \\ 0, & n < 0. \end{cases}$$

广义二项系数在计数上是有用的.

从  $m$  人里选出  $n$  人 ( $1 \leq n \leq m$ , 且任意二个人都不同), 并按一定的顺序让他们坐在  $n$  个座位上. 一个座位上至多坐一人, 且每一个选出的人都要坐在座位上. 共有多少种不同的安排座位的方法?

不难看出, 我们可以分步安排座位. 可以从  $m$  人里选 1 人坐第 1 个座位, 再从剩下的  $m-1$  人里选 1 人坐第 2 个座位……最后从剩下的  $m-(n-1)$  人里选 1 人坐第  $n$  个座位. 所以, 共有

$$m \cdot (m-1) \cdot \cdots \cdot (m-(n-1))$$

种不同的安排座位的方法.

前面, 我们是直接按座位数选人坐座位; 现在我们先选  $n$  人, 再让他们坐在这  $n$  个座位上. 设从  $m$  人里选  $n$  人有  $C$  种选法. 给这  $n$  人安排座位, 有多少种不同的方法呢? 跟上面的推理完全一致: 从这  $n$  人里选 1 人坐第 1 个座位, 再从剩下的  $n-1$  人里选 1 人坐第 2 个座位……最后剩下的 1 人坐第  $n$  个座位. 所以, 有

$$n \cdot (n-1) \cdot \cdots \cdot 1 = n!$$

种不同的为这  $n$  人安排座位的方法. 进而共有

$$C \cdot n!$$

种不同的安排座位的方法.

综上, 我们有

$$m \cdot (m-1) \cdots (m-(n-1)) = C \cdot n!.$$

由此可得, 从  $m$  人里选  $n$  人有

$$C = \frac{m \cdot (m-1) \cdots (m-(n-1))}{n!} = \binom{m}{n}$$

种选法.

一般地, 我们有

**命题** 从  $m$  个不同的文字里选  $n$  个的选法数为广义二项系数

$$\binom{m}{n} = \frac{m(m-1) \cdots (m-(n-1))}{n!} = \frac{m!}{n!(m-n)!}.$$

**证** 把上面的“人”换为“文字”, 再拟人化文字, 使其“坐在座位上”, 即可套用上面的推理, 从而得到第一个等号. 至于第二个等号, 直接计算即可:

$$\begin{aligned} & \frac{m(m-1) \cdots (m-(n-1))}{n!} \\ &= \frac{m(m-1) \cdots (m-(n-1))(m-n)(m-n-1) \cdots 1}{n!(m-n)!} \\ &= \frac{m!}{n!(m-n)!}. \end{aligned}$$

**命题** 广义二项系数适合如下性质:

(i)  $n \geq 0$  时,  $\binom{x}{n}$  是首项系数为  $\frac{1}{n!}$  的  $n$  次多项式, 前  $n$  个非负整数恰为其根, 且

$$\binom{n}{n} = 1;$$

(ii) 任取  $n \in \mathbb{Z}$ , 必有

$$\binom{x+1}{n} = \binom{x}{n} + \binom{x}{n-1};$$

(iii) 若  $m, n$  是非负整数, 则

$$\sum_{\ell=0}^{m-1} \binom{\ell}{n} = \binom{m}{n+1};$$

(iv) 任取  $n \in \mathbb{Z}$ , 必有

$$\binom{-x}{n} = (-1)^n \binom{x+n-1}{n};$$

(v) 若  $t, n$  是整数, 则

$$\binom{t}{n} \in \mathbb{Z}.$$

**证** (i)  $\binom{x}{0} = 1$  是 0 次多项式, 无根, 首项系数为 1, 且  $\binom{0}{0} = 1$ .  $n > 0$  时,

$$\binom{x}{n} = \frac{1}{n!} (x-0)(x-1)\cdots(x-(n-1)),$$

故  $\binom{x}{n}$  是首项系数为  $\frac{1}{n!}$  的  $n$  次多项式, 且  $0, 1, \dots, n-1$  恰为  $\binom{x}{n}$  的根. 最后, 不难验证

$$\binom{n}{n} = \frac{(n-0)(n-1)\cdots(n-(n-1))}{n!} = 1.$$

(ii) 若  $n < 0$ , 则  $\binom{x+1}{n}, \binom{x}{n}, \binom{x}{n-1}$  都是 0, 显然. 若  $n = 0$ , 则  $\binom{x+1}{n}, \binom{x}{n}$  都是 1, 而  $\binom{x}{n-1}$  都是 0, 显然. 若  $n = 1$ , 则  $\binom{x+1}{n}, \binom{x}{n}, \binom{x}{n-1}$  分别是  $x+1, x, 1$ , 显然. 若  $n \geq 2$ , 则

$$\begin{aligned} & \binom{x}{n} + \binom{x}{n-1} \\ &= \frac{x(x-1)\cdots(x-(n-2))(x-(n-1))}{n!} + \frac{x(x-1)\cdots(x-(n-2))}{(n-1)!} \\ &= \frac{x(x-1)\cdots(x-(n-2))(x-(n-1))}{n!} + \frac{x(x-1)\cdots(x-(n-2))(n)}{n!} \\ &= \frac{x(x-1)\cdots(x-(n-2))(x-(n-1)+n)}{n!} \\ &= \frac{(x+1)x(x-1)\cdots(x-(n-2))}{n!} \\ &= \frac{(x+1)(x+1-1)(x+1-2)\cdots(x+1-(n-1))}{n!} \\ &= \binom{x+1}{n}. \end{aligned}$$

(iii) 由 (ii) 知

$$\binom{\ell}{n} = \binom{\ell+1}{n+1} - \binom{\ell}{n+1}.$$

所以

$$\begin{aligned} \sum_{\ell=0}^{m-1} \binom{\ell}{n} &= \sum_{\ell=0}^{m-1} \left( -\binom{\ell}{n+1} + \binom{\ell+1}{n+1} \right) \\ &= -\binom{0}{n+1} + \binom{1}{n+1} - \binom{1}{n+1} + \binom{2}{n+1} \\ &\quad + \cdots - \binom{m-1}{n+1} + \binom{m}{n+1} \\ &= -\binom{0}{n+1} + \binom{m}{n+1} \\ &= \binom{m}{n+1}. \end{aligned}$$

(iv) 当  $n < 0$  时,  $\binom{-x}{n}$  与  $\binom{x+n-1}{n}$  都是 0. 当  $n = 0$  时,  $\binom{-x}{n}$  与  $\binom{x+n-1}{n}$  都是 1, 且  $(-1)^n = 1$ . 当  $n > 0$  时,

$$\begin{aligned} \binom{-x}{n} &= \frac{(-x)(-x-1)\cdots(-x-(n-1))}{n!} \\ &= (-1)^n \frac{x(x+1)\cdots(x+(n-1))}{n!} \\ &= (-1)^n \frac{(x+n-1)(x+n-1-1)\cdots(x+n-1-(n-1))}{n!} \\ &= (-1)^n \binom{x+n-1}{n}. \end{aligned}$$

(v) 若  $n < 0$ , 则  $\binom{t}{n} = 0 \in \mathbb{Z}$ . 若  $n = 0$ , 则  $\binom{t}{n} = 1 \in \mathbb{Z}$ . 下面考虑  $n \geq 1$  的情形.

我们先说明, 当  $t$  是非负整数时,  $\binom{t}{n} \in \mathbb{Z}$ .

对  $n$  用数学归纳法. 当  $n = 1$  时,  $\binom{t}{n} = t \in \mathbb{Z}$ .

设  $n = s \geq 1$  时,  $\binom{t}{n} \in \mathbb{Z}$ . 考虑  $n = s + 1$  的情形. 由 (iii) 可知

$$\binom{t}{s+1} = \sum_{\ell=0}^{t-1} \binom{\ell}{s}.$$

根据归纳假设,  $\binom{\ell}{s}$  ( $\ell = 0, 1, \dots, t-1$ ) 都是整数, 故它们的和  $\binom{t}{s+1}$  也是整数. 所以,  $n = s+1$  时,  $\binom{t}{n} \in \mathbb{Z}$ .

现在考虑  $t$  为负整数的情形. 由 (iv) 可知

$$\binom{t}{n} = (-1)^n \binom{-t+n-1}{n} \in \mathbb{Z}.$$

综上, 若  $t, n$  是整数, 则  $\binom{t}{n} \in \mathbb{Z}$ . ✎

性质 (i) (ii) 有计数相关的解释. 下面我们为读者提供二例.

**例** (i) 表明, 从  $n$  个不同的文字里选  $n$  个的选法数是 1. 这是显然的, 因为所有的文字都被选中了, 也没得选.

**例** 此例有“生活的气息”. 由 (ii) 可知,

$$\binom{7}{3} = \binom{6}{2} + \binom{6}{3}.$$

据说在中华人民共和国东部的浙江省, 参加“普通高等学校招生全国统一考试” (*Nationwide Unified Examination for Admissions to General Universities and Colleges*) 的人, 除了有必考的语文、数学、外语, 还要从物理、化学、生物、技术、政治、历史、地理这 7 个科目里选择 3 个作为选考科目. 由于物理是“很有挑战性的科目”, 故有不少人不选物理. 上式右侧的  $\binom{6}{2}$  表示选择物理的选法数, 而  $\binom{6}{3}$  表示不选物理的选法数. 因为人要么选物理, 要么不选, 故它们的和就是 7 选 3 的选法数.

**命题** 设  $n$  是非负整数. 广义二项系数适合如下性质:

(vi) 任意次不高于  $n$  的多项式都可唯一地写为  $\binom{x}{0}, \binom{x}{1}, \dots, \binom{x}{n}$  的线性组合;

(vii) 设  $c_0, c_1, \dots, c_n \in \mathbb{F}$ . 设

$$f(x) = c_0 \binom{x}{0} + c_1 \binom{x}{1} + \dots + c_n \binom{x}{n}.$$

若  $c_0, c_1, \dots, c_n \in \mathbb{Z}$ , 则任取  $t \in \mathbb{Z}$ , 必有  $f(t) \in \mathbb{Z}$ ; 若  $c_0, c_1, \dots, c_n$  不全是整数, 则存在整数  $u$  使  $f(u)$  不是整数. 换句话说, 任取  $t \in \mathbb{Z}$ , 必有  $f(t) \in \mathbb{Z}$  的一个必要与充分条件是:  $c_0, c_1, \dots, c_n$  全是整数.

**证** (vi) 注意到  $\binom{x}{0}, \binom{x}{1}, \dots, \binom{x}{n}$  的次分别是  $0, 1, \dots, n$ .

(vii) 设  $c_0, c_1, \dots, c_n \in \mathbb{Z}$ . 设  $t \in \mathbb{Z}$ . 由 (v),  $\binom{t}{0}, \binom{t}{1}, \dots, \binom{t}{n}$  都是整数, 故  $f(t)$  也是整数.

设  $c_0, c_1, \dots, c_n$  不全是整数. 这样, 存在  $\ell$  使  $c_0, c_1, \dots, c_{\ell-1}$  这  $\ell$  个数全为整数, 而  $c_\ell$  不是整数 (从左往右, 一个一个地看). 那么

$$\begin{aligned} f(\ell) &= \underbrace{c_0 \binom{\ell}{0} + c_1 \binom{\ell}{1} + \dots + c_{\ell-1} \binom{\ell}{\ell-1}}_{\ell \text{ terms}} + c_\ell \binom{\ell}{\ell} \\ &\quad + \underbrace{c_{\ell+1} \binom{\ell}{\ell+1} + \dots + c_n \binom{\ell}{n}}_{(n-\ell) \text{ terms}} \\ &= (\text{an integer } q) + c_\ell + 0 \\ &= q + c_\ell. \end{aligned}$$

我们说,  $f(\ell)$  不是整数. 用反证法. 若  $f(\ell)$  是整数, 因为  $q$  也是整数, 故  $c_\ell = f(\ell) - q$  是整数, 矛盾!  $\clubsuit$

**例** 我们知道, 若多项式  $f(x)$  的系数全为整数, 则  $t \in \mathbb{Z}$  时  $f(t) \in \mathbb{Z}$ . 不过, 反过来就不对了. 在中学, 读者也许知道  $n$  是整数时  $\frac{n(n+1)}{2}$  也是整数:  $n$  与  $n+1$  必一奇一偶, 故积是偶数, 从而被 2 除后仍为整数. 现在可以这么看:

$$\frac{n(n+1)}{2} = \frac{(n+1)(n+1-1)}{2} = \binom{n+1}{2}.$$

下面我们介绍二个与广义二项系数有关的和. 不过, 我们先介绍一个用完就丢的工具.

**定义** 固定某  $h \in \mathbb{F}[x]$ . 设  $n$  是非负整数,  $r \in \mathbb{F}[x]$ . 定义

$$r^{[n]} = \begin{cases} (r-0)(r-h) \cdots (r-(n-1)h), & n > 0; \\ 1, & n = 0. \end{cases}$$

不难看出,

$$r^{[n+1]} = r^{[n]}(r-nh).$$

若  $h = 0$ ,  $r^{[n]}$  就变为  $r$  的  $n$  次幂. 若  $h = 1$ ,  $r^{[n]}$  就变为  $n! \binom{x}{n}$ .

**命题** 设  $r, s \in \mathbb{F}[x]$ . 设  $n$  是非负整数. 则

$$(\star) \quad (r+s)^{[n]} = \sum_{k=0}^n \binom{n}{k} r^{[n-k]} s^{[k]}.$$

取  $h=0$ , 得到二项展开 (*binomial expansion*):

$$(BE) \quad (r+s)^n = \sum_{k=0}^n \binom{n}{k} r^{n-k} s^k.$$

取  $h=1$ , 得

$$n! \binom{r+s}{n} = \sum_{k=0}^n \binom{n}{k} (n-k)! k! \binom{r}{n-k} \binom{s}{k}.$$

二边同乘  $\frac{1}{n!}$ , 再利用

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

可得 Vandermonde 恒等式 (*Vandermonde's identity*):

$$(VI) \quad \binom{r+s}{n} = \sum_{k=0}^n \binom{r}{n-k} \binom{s}{k}.$$

**证** 用数学归纳法. 当  $n=0$  时,  $(\star)$  的左侧是 1, 右侧是  $1 \cdot 1 \cdot 1$ . 当  $n=1$  时,  $(\star)$  的左侧是  $r+s$ , 右侧是  $1 \cdot r \cdot 1 + 1 \cdot 1 \cdot s$ .

设  $n=\ell \geq 1$  时,  $(\star)$  正确, 即

$$(\star) \quad (r+s)^{[\ell]} = \sum_{k=0}^{\ell} \binom{\ell}{k} r^{[\ell-k]} s^{[k]}.$$

现在, 考虑  $n=\ell+1$  的情形:

$$\begin{aligned} & (r+s)^{[\ell+1]} \\ &= (r+s)^{[\ell]}(r+s-\ell h) \\ &= \sum_{k=0}^{\ell} \binom{\ell}{k} r^{[\ell-k]} s^{[k]} (r+s-\ell h) \\ &= \sum_{k=0}^{\ell} \binom{\ell}{k} r^{[\ell-k]} s^{[k]} (r+s-(\ell-k+k)h) \end{aligned}$$



$$\begin{aligned}
 &= \sum_{k=0}^{\ell} \binom{\ell}{k} r^{[\ell-k]} s^{[k]} ((r - (\ell - k)h) + (s - kh)) \\
 &= \sum_{k=0}^{\ell} \binom{\ell}{k} (r^{[\ell-k]} (r - (\ell - k)h) s^{[k]} + r^{[\ell-k]} s^{[k]} (s - kh)) \\
 &= \sum_{k=0}^{\ell} \binom{\ell}{k} (r^{[\ell-k+1]} s^{[k]} + r^{[\ell-k]} s^{[k+1]}) \\
 &= \sum_{k=0}^{\ell} \binom{\ell}{k} r^{[\ell+1-k]} s^{[k]} + \sum_{k=0}^{\ell} \binom{\ell}{k} r^{[\ell-k]} s^{[k+1]} \\
 &= \sum_{k=0}^{\ell} \binom{\ell}{k} r^{[\ell+1-k]} s^{[k]} + \sum_{k=0}^{\ell} \binom{\ell}{k+1-1} r^{[\ell+1-(k+1)]} s^{[k+1]} \\
 &= \sum_{k=0}^{\ell} \binom{\ell}{k} r^{[\ell+1-k]} s^{[k]} + \sum_{k=1}^{\ell+1} \binom{\ell}{k-1} r^{[\ell+1-k]} s^{[k]} \\
 &= \sum_{k=0}^{\ell+1} \binom{\ell}{k} r^{[\ell+1-k]} s^{[k]} + \sum_{k=0}^{\ell+1} \binom{\ell}{k-1} r^{[\ell+1-k]} s^{[k]} \\
 &= \sum_{k=0}^{\ell+1} \left( \binom{\ell}{k} + \binom{\ell}{k-1} \right) r^{[\ell+1-k]} s^{[k]} \\
 &= \sum_{k=0}^{\ell+1} \binom{\ell+1}{k} r^{[\ell+1-k]} s^{[k]}. \quad \text{☺}
 \end{aligned}$$

**评注** Too cruel though it is, let's say *farewell* to  $r^{[n]}$ . We will not use  $r^{[n]}$  any longer from this moment forward. It is born to be a good old tool for us. May  $r^{[n]}$  and its soul rest in peace!

**例** (VI) 也有计数相关的解释. 老规矩, 先写下算式:

$$\binom{7}{3} = \binom{3}{3} \binom{4}{0} + \binom{3}{2} \binom{4}{1} + \binom{3}{1} \binom{4}{2} + \binom{3}{0} \binom{4}{3}.$$

回到中华人民共和国东部的浙江省. 回到“普通高等学校招生全国统一考试”. 前面提到, 在那儿, 参加考试的人从 7 科目里选 3 个. 政治、历史、地理是偏“阿先生”(arts)的; 物理、化学、生物、技术是偏“赛先生”(science)的.

7 选 3 可以这么选:

- (i) 选 3 个阿先生与 0 个赛先生:  $\binom{3}{3}\binom{4}{0}$ ;
  - (ii) 或者, 选 2 个阿先生与 1 个赛先生:  $\binom{3}{2}\binom{4}{1}$ ;
  - (iii) 或者, 选 1 个阿先生与 2 个赛先生:  $\binom{3}{1}\binom{4}{2}$ ;
  - (iv) 或者, 选 0 个阿先生与 3 个赛先生:  $\binom{3}{0}\binom{4}{3}$ .
- 把这 4 种情形下的选法数相加, 就是  $\binom{7}{3}$ .

## 求和公式

本节讨论求和公式 (*summation formula*) 问题: 设  $f(x) \in \mathbb{F}[x]$ , 求

$$S(n) = \sum_{\ell=0}^{n-1} f(\ell) = f(0) + f(1) + \cdots + f(n-1).$$

**例** 相信大家应该听说过德意志数学家 Carl Friedrich Gauß. 1787 年, Gauß 还只是一个 10 岁的孩子. 据说, 当时他的数学教师给全班同学出了这样的算术题:

$$1 + 2 + 3 + \cdots + 100 = ?$$

这里, 后一个数比前一个数多 1, 且共有 100 个数. 教师刚写完问题, Gauß 就算出, 答案是 5 050. 他的同学还在一个一个地加, 算了很久, 还没算对.

Gauß 是怎么快速算出答案的呢? 设

$$S = 1 + 2 + 3 + \cdots + 100.$$

因为加法适合交换律, 故

$$S = 100 + 99 + 98 + \cdots + 1.$$

所以

$$\begin{aligned} 2S &= (1 + 100) + (2 + 99) + (3 + 98) + \cdots + (100 + 1) \\ &= \underbrace{101 + 101 + 101 + \cdots + 101}_{\text{a hundred 101's}} \\ &= 100 \cdot 101 \\ &= 10\,100. \end{aligned}$$

由此可得

$$S = \frac{10\,100}{2} = 5\,050.$$

如果记  $f(x) = x + 1$ , 则

$$\begin{aligned} S &= 1 + 2 + 3 + \cdots + 100 \\ &= f(0) + f(1) + f(2) + \cdots + f(100-1) \\ &= \sum_{\ell=0}^{100-1} f(\ell). \end{aligned}$$

考虑更一般的情形. 设  $f(x) = a + bx$ . 记

$$S(n) = f(0) + f(1) + \cdots + f(n-1).$$

类似地, 把右侧倒着写:

$$S(n) = f(n-1) + f(n-1) + \cdots + f(0).$$

因为

$$f(k) + f(n-1-k) = a + bk + a + b(n-1-k) = 2a + b(n-1),$$

故

$$\begin{aligned} 2S(n) &= (f(0) + f(n-1)) + (f(1) + f(n-2)) + \cdots + (f(n-1) + f(0)) \\ &= n(2a + b(n-1)), \end{aligned}$$

即

$$S(n) = \frac{n(2a + b(n-1))}{2} = \left(a - \frac{b}{2}\right)n + \frac{b}{2}n^2.$$

我们还可以看出:  $S(n)$  是多项式, 且

$$\deg S(n) = \deg f(n) + 1.$$

上面讨论了当  $f(x)$  的次不高于 1 时如何求  $S(n)$ . 那么, 当  $f(x)$  的次高于 1 时, 怎么找  $S(n)$ ? 它还是多项式吗?

在求和前, 我们看  $S(n)$  适合什么性质.  $S(n)$  是  $f(0), f(1), \cdots, f(n-1)$  这  $n$  个数的和. 因为 0 个数的和是 0, 故  $S(0) = 0$ . 同时, 不难看出,  $S(n+1)$  比  $S(n)$  多出  $f(n)$ , 也即

$$S(n+1) - S(n) = f(n).$$

反过来, 设  $\mathbb{N}$  到  $\mathbb{F}$  的函数  $W(n)$  适合  $W(0) = 0$  与  $W(n+1) - W(n) = f(n)$ , 则

$$\begin{aligned}\sum_{\ell=0}^{n-1} f(\ell) &= \sum_{\ell=0}^{n-1} (W(\ell+1) - W(\ell)) \\ &= \sum_{\ell=0}^{n-1} W(\ell+1) - \sum_{\ell=0}^{n-1} W(\ell) \\ &= \sum_{\ell=1}^n W(\ell) - \sum_{\ell=0}^{n-1} W(\ell) \\ &= W(n) - W(0) \\ &= W(n).\end{aligned}$$

这样, 任给  $f(x) \in \mathbb{F}[x]$ , 若我们能找到适合条件  $S(0) = 0$  与  $S(x+1) - S(x) = f(x)$  的多项式, 则

$$\sum_{\ell=0}^{n-1} f(\ell) = S(n).$$

**命题** 设  $f(x) \in \mathbb{F}[x]$  是  $m$  次多项式. 存在唯一的  $m+1$  次多项式  $F(x) \in \mathbb{F}[x]$  适合条件:

- (i)  $F(0) = 0$ ;
- (ii)  $F(x+1) - F(x) = f(x)$ .

**证** 先看存在性. 若  $f(x) = 0$ , 则  $F(x) = 0$  显然适合 (i) (ii), 且

$$\deg F(x) = -\infty = -\infty + 1 = \deg f(x) + 1.$$

设  $m \geq 0$ . 根据广义二项系数的性质, 存在  $m+1$  个  $\mathbb{F}$  中元  $c_0, \dots, c_m$  使

$$f(x) = \sum_{\ell=0}^m c_{\ell} \binom{x}{\ell}, \quad c_m \neq 0.$$

(读者可思考: 若  $c_m = 0$ ,  $f(x)$  还能是  $m$  次多项式吗?) 作多项式

$$F(x) = \sum_{\ell=0}^m c_{\ell} \binom{x}{\ell+1} \in \mathbb{F}[x].$$

显然  $\deg F(x) = m + 1$ . 验证 (i):

$$F(0) = \sum_{\ell=0}^m c_{\ell} \binom{0}{\ell+1} = \sum_{\ell=0}^m 0 = 0.$$

验证 (ii):

$$\begin{aligned} F(x+1) - F(x) &= \sum_{\ell=0}^m c_{\ell} \binom{x+1}{\ell+1} - \sum_{\ell=0}^m c_{\ell} \binom{x}{\ell+1} \\ &= \sum_{\ell=0}^m c_{\ell} \left( \binom{x+1}{\ell+1} - \binom{x}{\ell+1} \right) \\ &= \sum_{\ell=0}^m c_{\ell} \binom{x}{\ell} \\ &= f(x). \end{aligned}$$

再看唯一性. 设  $G(x) \in \mathbb{F}[x]$  是  $m+1$  次多项式, 并适合条件  $G(0) = 0$  与  $G(x+1) - G(x) = f(x)$ . 作

$$H(x) = F(x) - G(x).$$

则  $H(0) = 0$ ,  $H(x+1) - H(x) = 0$ . 所以,  $r$  为非负整数时,  $H(r) = 0$ . 从而  $H(x)$  一定是零多项式, 即  $F(x) = G(x)$ . ✎

**例** 记  $f(x) = x^2$ . 我们求

$$S(n) = f(0) + f(1) + \cdots + f(n-1) = \sum_{\ell=0}^{n-1} f(\ell).$$

由上个命题可知, 存在唯一的次为 3 的多项式  $F(x)$  使  $F(0) = 0$ ,  $F(x+1) - F(x) = f(x)$ , 且  $S(n) = F(n)$ .

可以用插值的思想求  $F(x)$ . 取  $x_0, x_1, x_2, x_3$  为 0, 1, -1, 2. 不难算出:

$$\begin{aligned} y_0 &= F(0) = 0, \\ y_1 &= F(1) = F(0) + f(0) = 0, \\ y_2 &= F(-1) = F(0) - f(-1) = -1, \\ y_3 &= F(2) = F(1) + f(1) = 1. \end{aligned}$$

注意到  $y_0 = y_1 = 0$ , 故可以考虑 Lagrange 插值 (只要算  $L_2(x)$  与  $L_3(x)$ ):

$$\begin{aligned} L_2(x) &= \frac{(x-0)(x-1)(x-2)}{(-1-0)(-1-1)(-1-2)} = -\frac{x(x-1)(x-2)}{6}, \\ L_3(x) &= \frac{(x-0)(x-1)(x+1)}{(2-0)(2-1)(2+1)} = \frac{x(x-1)(x+1)}{6}, \\ F(x) &= y_2 L_2(x) + y_3 L_3(x) = \frac{x(x-1)(2x-1)}{6}. \end{aligned}$$

当然, 也可利用 Newton 插值. 作出差商表:

$$\begin{array}{c|ccc} 2 & 1 & & & \\ -1 & -1 & \frac{2}{3} & & \\ 1 & 0 & \frac{1}{2} & \frac{1}{6} & \\ 0 & 0 & 0 & -\frac{1}{2} & \frac{1}{3} \end{array}$$

故

$$\begin{aligned} F(x) &= [0] + [0, 1](x-0) + [0, 1, -1](x-0)(x-1) \\ &\quad + [0, 1, -1, 2](x-0)(x-1)(x+1) \\ &= -\frac{1}{2}x(x-1) + \frac{1}{3}x(x-1)(x+1) \\ &= \frac{x(x-1)(2x-1)}{6}. \end{aligned}$$

综上, 我们有

$$\sum_{\ell=0}^{n-1} \ell^2 = 0^2 + 1^2 + \cdots + (n-1)^2 = \frac{n(n-1)(2n-1)}{6}.$$

其实, 我们可以在此处结束本节. 设  $f(x)$  是  $n$  次多项式. 上面的命题告诉我们, 存在唯一的  $n+1$  次多项式  $F(x)$  使  $F(0) = 0$ ,  $F(x+1) - F(x) = f(x)$ , 且  $S(n) = F(n)$ . 利用这些条件, 可以确定  $F(x)$  在  $n+2$  个整数点处的值, 从而可用插值公式求出  $F(x)$ . 不过, 为了使实操容易一些, 我们还得再研究一点.

由上个命题的证明过程, 有

**命题** 若

$$f(x) = c_0 \binom{x}{0} + c_1 \binom{x}{1} + \cdots + c_m \binom{x}{m},$$

则

$$S(n) = \sum_{\ell=0}^{n-1} f(\ell) = c_0 \binom{n}{1} + c_1 \binom{n}{2} + \cdots + c_m \binom{n}{m+1}.$$

由此可见, 若我们能把  $f(x)$  写为广义二项系数的线性组合, 则寻找  $S(n)$  的过程将十分简单. 接下来, 我们讨论怎么方便地把多项式写为广义二项系数的线性组合.

**定义** 设  $f(x) \in \mathbb{F}[x]$ . 定义  $f(x)$  的差分 (*difference*) 为

$$\Delta f(x) = f(x+1) - f(x) \in \mathbb{F}[x].$$

设  $t \in \mathbb{F}$ . 我们把

$$f(t+1) - f(t) \in \mathbb{F}$$

也写为  $\Delta f(t)$ .

**例** 取  $f(x) = x^2 + x - 1$ . 则

$$f(x+1) = (x+1)^2 + (x+1) - 1 = x^2 + 3x + 1,$$

故

$$\Delta f(x) = 2x + 2.$$

所以

$$\Delta f(332) = 2 \cdot 332 + 2 = 666.$$

**命题** 设  $k$  是整数. 则

$$\Delta \binom{x}{k} = \binom{x}{k-1}.$$

**证** 也许, 这就是所谓的“新瓶装旧酒”吧! 不过, 为了方便, 我们还是单独列出来. ✎



回忆一下, 微商适合如下二条性质:

- (i)  $(cf(x))' = cf'(x)$ ;
- (ii)  $(f(x) \pm g(x))' = f'(x) \pm g'(x)$ .

差分也有类似的性质.

**命题** 设  $f(x), g(x) \in \mathbb{F}[x]$ ,  $c \in \mathbb{F}$ . 则

- (i)  $\Delta(cf(x)) = c\Delta f(x)$ ;
- (ii)  $\Delta(f(x) \pm g(x)) = \Delta f(x) \pm \Delta g(x)$ .

由 (i) (ii) 与数学归纳法可知: 当  $c_0, c_1, \dots, c_{k-1} \in \mathbb{F}$ , 且  $f_0(x), f_1(x), \dots, f_{k-1}(x) \in \mathbb{F}[x]$  时,

$$\Delta \left( \sum_{\ell=0}^{k-1} c_{\ell} f_{\ell}(x) \right) = \sum_{\ell=0}^{k-1} c_{\ell} \Delta f_{\ell}(x).$$

**证** 老样子, 我们证明 (i) (ii), 将剩下的推论留给读者作练习. 设

(i) 设  $p(x) = cf(x)$ . 则

$$\begin{aligned} \Delta(cf(x)) &= \Delta p(x) \\ &= p(x+1) - p(x) \\ &= cf(x+1) - cf(x) \\ &= c(f(x+1) - f(x)) \\ &= c\Delta f(x). \end{aligned}$$

(ii) 设  $q(x) = f(x) \pm g(x)$ . 则

$$\begin{aligned} \Delta(f(x) \pm g(x)) &= \Delta q(x) \\ &= q(x+1) - q(x) \\ &= (f(x+1) \pm g(x+1)) - (f(x) \pm g(x)) \\ &= (f(x+1) - f(x)) \pm (g(x+1) - g(x)) \\ &= \Delta f(x) \pm \Delta g(x). \end{aligned}$$

☺

**定义** 设  $f(x) \in \mathbb{F}[x]$ . 记

$$\Delta^0 f(x) = f(x) \in \mathbb{F}[x],$$

并称其为  $f(x)$  的 0 级差分 (*zeroth-order difference*). 1 级差分就是差分:

$$\Delta^1 f(x) = \Delta f(x) = \Delta(\Delta^0 f(x)) \in \mathbb{F}[x].$$

1 级差分的差分是 2 级差分:

$$\Delta^2 f(x) = \Delta(\Delta^1 f(x)) \in \mathbb{F}[x].$$

2 级差分的差分是 3 级差分:

$$\Delta^3 f(x) = \Delta(\Delta^2 f(x)) \in \mathbb{F}[x].$$

一般地,  $e$  级差分就是  $e - 1$  级差分的差分:

$$\Delta^e f(x) = \Delta(\Delta^{e-1} f(x)) \in \mathbb{F}[x].$$

高级差分可指代任意  $e$  级差分, 此处  $e > 1$ .

设  $t \in \mathbb{F}$ . 既然  $\Delta^e f(x)$  是某个多项式

$$v_0 + v_1 x + \cdots + v_s x^s \in \mathbb{F}[x],$$

我们将

$$v_0 + v_1 t + \cdots + v_s t^s \in \mathbb{F}$$

简单地写为  $\Delta^e f(t)$ .

**例 设**

$$f(x) = 2x^3 + 3x^2 + 5x + 7.$$

根据定义,  $f(x)$  的 0 级差分就是自己:

$$\Delta^0 f(x) = 2x^3 + 3x^2 + 5x + 7.$$

因为

$$\begin{aligned} (1+x)^3 &= (1+x)^2(1+x) \\ &= (1+2x+x^2)(1+x) \\ &= 1+2x+x^2+x+2x^2+x^3 \\ &= 1+3x+3x^2+x^3, \end{aligned}$$

故

$$\begin{aligned}f(x+1) &= 2(x+1)^3 + 3(x+1)^2 + 5(x+1) + 7 \\&= 2x^3 + 9x^2 + 17x + 17.\end{aligned}$$

从而  $f(x)$  的 1 级差分是

$$\Delta^1 f(x) = \Delta f(x) = f(x+1) - f(x) = 6x^2 + 12x + 10.$$

因为

$$\Delta^1 f(x+1) = 6(x+1)^2 + 12(x+1) + 10 = 6x^2 + 24x + 28,$$

故  $f(x)$  的 2 级差分是

$$\Delta^2 f(x) = \Delta(\Delta^1 f(x)) = \Delta^1 f(x+1) - \Delta^1 f(x) = 12x + 18.$$

因为

$$\Delta^2 f(x+1) = 12(x+1) + 18 = 12x + 30,$$

故  $f(x)$  的 3 级差分是

$$\Delta^3 f(x) = \Delta(\Delta^2 f(x)) = \Delta^2 f(x+1) - \Delta^2 f(x) = 12.$$

因为

$$\Delta^3 f(x+1) = 12,$$

故  $f(x)$  的 4 级差分是

$$\Delta^4 f(x) = \Delta(\Delta^3 f(x)) = \Delta^3 f(x+1) - \Delta^3 f(x) = 0.$$

读者不难验证: 对任意超出 3 的整数  $e$ , 必有

$$\Delta^e f(x) = 0.$$

由上面的计算, 可知

$$\Delta^0 f(1) = 2 \cdot 1^3 + 3 \cdot 1^2 + 5 \cdot 1 + 7 = 17,$$

$$\Delta^1 f(1) = 6 \cdot 1^2 + 12 \cdot 1 + 10 = 28,$$

$$\Delta^2 f(1) = 12 \cdot 1 + 18 = 30,$$

$$\Delta^3 f(1) = 12,$$

$$\Delta^e f(1) = 0 \quad (e > 3).$$

高级差分适合如下性质:

**命题** 设  $e$  是非负整数. 当  $c_0, c_1, \dots, c_{k-1} \in \mathbb{F}$ , 且  $f_0(x), f_1(x), \dots, f_{k-1}(x) \in \mathbb{F}[x]$  时,

$$\Delta^e \left( \sum_{\ell=0}^{k-1} c_\ell f_\ell(x) \right) = \sum_{\ell=0}^{k-1} c_\ell \Delta^e f_\ell(x).$$

**证** 用数学归纳法. 我们把具体过程留给读者当练习. ✎

**命题** 设  $e$  是非负整数. 设  $k$  是整数. 则

$$\Delta^e \binom{x}{k} = \binom{x}{k-e}.$$

**证** 用数学归纳法. 我们把具体过程留给读者当练习. ✎

**命题** 设  $e$  是非负整数. 设  $f(x) \in \mathbb{F}[x]$ . 则

$$\Delta^e f(x) = \sum_{k=0}^e (-1)^{e-k} \binom{e}{k} f(x+k).$$

**证** 当  $e = 0$  时, 左侧是  $f(x)$ , 右侧是

$$(-1)^0 \binom{0}{0} f(x+0) = f(x).$$

当  $e = 1$  时, 左侧是  $f(x+1) - f(x)$ , 右侧是

$$(-1)^1 \binom{1}{0} f(x+0) + (-1)^0 \binom{1}{1} f(x+1) = -f(x) + f(x+1).$$

所以, 命题对  $e = 0$  或  $e = 1$  成立.

设命题对  $e = \ell \geq 1$  成立, 即

$$\Delta^\ell f(x) = \sum_{k=0}^{\ell} (-1)^{\ell-k} \binom{\ell}{k} f(x+k).$$

则  $e = \ell + 1$  时,

$$\begin{aligned}
 & \Delta^{\ell+1} f(x) \\
 &= \Delta(\Delta^{\ell} f(x)) \\
 &= \Delta^{\ell} f(x+1) - \Delta^{\ell} f(x) \\
 &= \sum_{k=0}^{\ell} (-1)^{\ell-k} \binom{\ell}{k} f(x+1+k) - \sum_{k=0}^{\ell} (-1)^{\ell-k} \binom{\ell}{k} f(x+k) \\
 &= \sum_{k=0}^{\ell} (-1)^{(\ell+1)-(k+1)} \binom{\ell}{k+1-1} f(x+k+1) \\
 &\quad + \sum_{k=0}^{\ell} (-1)^{\ell+1-k} \binom{\ell}{k} f(x+k) \\
 &= \sum_{k=1}^{\ell+1} (-1)^{\ell+1-k} \binom{\ell}{k-1} f(x+k) + \sum_{k=0}^{\ell} (-1)^{\ell+1-k} \binom{\ell}{k} f(x+k) \\
 &= \sum_{k=0}^{\ell+1} (-1)^{\ell+1-k} \binom{\ell}{k-1} f(x+k) + \sum_{k=0}^{\ell+1} (-1)^{\ell+1-k} \binom{\ell}{k} f(x+k) \\
 &= \sum_{k=0}^{\ell+1} \left( (-1)^{\ell+1-k} \binom{\ell}{k-1} f(x+k) + (-1)^{\ell+1-k} \binom{\ell}{k} f(x+k) \right) \\
 &= \sum_{k=0}^{\ell+1} (-1)^{\ell+1-k} \left( \binom{\ell}{k-1} + \binom{\ell}{k} \right) f(x+k) \\
 &= \sum_{k=0}^{\ell+1} (-1)^{\ell+1-k} \binom{\ell+1}{k} f(x+k). \quad \text{☞}
 \end{aligned}$$

我们再补充一个跟广义二项系数有关的性质:

**命题** 设  $k$  是整数. 则

$$\binom{0}{k} = \begin{cases} 1, & k = 0; \\ 0, & k \neq 0. \end{cases}$$

**证** 显然. ☞

设  $f(x) \in \mathbb{F}[x]$  是次不高于  $m$  的多项式. 我们知道,  $f(x)$  一定可以写

为广义二项系数的线性组合:

$$f(x) = \sum_{k=0}^m c_k \binom{x}{k}.$$

对左右二侧求  $e$  级差分 ( $e \leq m$ ), 有

$$\Delta^e f(x) = \sum_{k=0}^m c_k \binom{x}{k-e}.$$

用 0 替换  $x$ , 有

$$\Delta^e f(0) = \sum_{k=0}^m c_k \binom{0}{k-e} = c_e.$$

所以

$$\begin{aligned} f(x) &= \sum_{k=0}^m \Delta^k f(0) \binom{x}{k} \\ &= \Delta^0 f(0) \binom{x}{0} + \Delta^1 f(0) \binom{x}{1} + \cdots + \Delta^m f(0) \binom{x}{m} \\ &= f(0) + \Delta f(0) \binom{x}{1} + \cdots + \Delta^m f(0) \binom{x}{m}. \end{aligned}$$

我们已经证明了

**命题** 设  $f(x) \in \mathbb{F}[x]$  是次不高于  $m$  的多项式. 则

$$\begin{aligned} f(x) &= \sum_{k=0}^m \Delta^k f(0) \binom{x}{k} \\ &= \Delta^0 f(0) \binom{x}{0} + \Delta^1 f(0) \binom{x}{1} + \cdots + \Delta^m f(0) \binom{x}{m} \\ &= f(0) + \Delta f(0) \binom{x}{1} + \cdots + \Delta^m f(0) \binom{x}{m}, \end{aligned}$$

所以

$$S(n) = \sum_{\ell=0}^{n-1} f(\ell) = f(0) \binom{n}{1} + \Delta f(0) \binom{n}{2} + \cdots + \Delta^m f(0) \binom{n}{m+1}.$$

注意到

$$\Delta^k f(0) = \sum_{u=0}^k (-1)^{k-u} \binom{k}{u} f(u),$$

故计算  $\Delta^k f(0)$  需要用到  $f(0), f(1), \dots, f(k)$  这  $k+1$  个数. 也就是说, 计算  $\Delta^0 f(0), \Delta^1 f(0), \dots, \Delta^m f(0)$  需要用到  $f(0), f(1), \dots, f(m)$  这  $m+1$  个数.

下面我们举几个具体的例, 帮助读者消化这种求和方法.

**例** 设  $f(x) = x^2 + x - 1$ . 求

$$S(n) = \sum_{\ell=0}^{n-1} f(\ell) = f(0) + f(1) + \dots + f(n-1).$$

这里,  $m = 2$ . 所以, 我们计算  $f(0), f(1), f(2)$ :

$$f(0) = -1, \quad f(1) = 1, \quad f(2) = 5.$$

由此, 不难算出:

$$\Delta^0 f(0) = f(0) = -1,$$

$$\Delta^1 f(0) = f(1) - f(0) = 2,$$

$$\Delta^1 f(1) = f(2) - f(1) = 4,$$

$$\Delta^2 f(0) = \Delta^1 f(1) - \Delta^1 f(0) = 2.$$

所以

$$\begin{aligned} f(x) &= f(0) + \Delta f(0) \binom{x}{1} + \Delta^2 f(0) \binom{x}{2} \\ &= -1 + 2 \binom{x}{1} + 2 \binom{x}{2}. \end{aligned}$$

从而

$$\begin{aligned} S(n) &= \sum_{\ell=0}^{n-1} f(\ell) \\ &= -1 \binom{n}{1} + 2 \binom{n}{2} + 2 \binom{n}{3} \\ &= -n + n(n-1) + \frac{n(n-1)(n-2)}{3} \\ &= \frac{n(n+2)(n-2)}{3}. \end{aligned}$$

实操时, 往往用名为“差分表”的表进行计算. 当  $m = 2$  时, 它长这样:

$$\begin{array}{rcl} \Delta^0 f(2) & & \\ \Delta^0 f(1) & \Delta^1 f(1) & \\ \Delta^0 f(0) & \Delta^1 f(0) & \Delta^2 f(0) \end{array}$$

在这个问题里, 差分表如下:

$$\begin{array}{rcl} 5 & & \\ 1 & 4 & \\ -1 & 2 & 2 \end{array}$$

**例** 求前  $n$  个非负整数的立方和

$$S(n) = 0^3 + 1^3 + \cdots + (n-1)^3 = \sum_{\ell=0}^{n-1} \ell^3.$$

取  $f(x) = x^3$ . 这里,  $m = 3$ . 画出  $m = 3$  时的差分表:

$$\begin{array}{rclcl} \Delta^0 f(3) & & & & \\ \Delta^0 f(2) & \Delta^1 f(2) & & & \\ \Delta^0 f(1) & \Delta^1 f(1) & \Delta^2 f(1) & & \\ \Delta^0 f(0) & \Delta^1 f(0) & \Delta^2 f(0) & \Delta^3 f(0) & \end{array}$$

$\Delta^0 f(t)$  就是  $f(t)$ :

$$f(0) = 0, \quad f(1) = 1, \quad f(2) = 8, \quad f(3) = 27.$$

写在表上, 就是

$$\begin{array}{rclcl} 27 & & & & \\ 8 & \Delta^1 f(2) & & & \\ 1 & \Delta^1 f(1) & \Delta^2 f(1) & & \\ 0 & \Delta^1 f(0) & \Delta^2 f(0) & \Delta^3 f(0) & \end{array}$$

由此可确定 1 级差分:

$$\begin{aligned} \Delta^1 f(2) &= f(3) - f(2) = 19, \\ \Delta^1 f(1) &= f(2) - f(1) = 7, \\ \Delta^1 f(0) &= f(1) - f(0) = 1. \end{aligned}$$



写在表上, 就是

$$\begin{array}{cccc}
 & & & 27 \\
 & & 8 & 19 \\
 & 1 & 7 & \Delta^2 f(1) \\
 0 & 1 & \Delta^2 f(0) & \Delta^3 f(0)
 \end{array}$$

类似地, 可确定 2 级差分:

$$\begin{aligned}
 \Delta^2 f(1) &= \Delta^1 f(2) - \Delta^1 f(1) = 12, \\
 \Delta^2 f(0) &= \Delta^1 f(1) - \Delta^1 f(0) = 6.
 \end{aligned}$$

写在表上, 就是

$$\begin{array}{cccc}
 & & & 27 \\
 & & 8 & 19 \\
 & 1 & 7 & 12 \\
 0 & 1 & 6 & \Delta^3 f(0)
 \end{array}$$

最后, 可确定 3 级差分:

$$\Delta^3 f(0) = \Delta^2 f(1) - \Delta^2 f(0) = 6.$$

写在表上, 就是

$$\begin{array}{cccc}
 & & & 27 \\
 & & 8 & 19 \\
 & 1 & 7 & 12 \\
 0 & 1 & 6 & 6
 \end{array}$$

所以

$$\begin{aligned}
 f(x) &= f(0) + \Delta f(0) \binom{x}{1} + \Delta^2 f(0) \binom{x}{2} + \Delta^3 f(0) \binom{x}{3} \\
 &= \binom{x}{1} + 6 \binom{x}{2} + 6 \binom{x}{3}.
 \end{aligned}$$

从而

$$\begin{aligned}
 S(n) &= \sum_{\ell=0}^{n-1} f(\ell) \\
 &= \binom{n}{2} + 6\binom{n}{3} + 6\binom{n}{4} \\
 &= \frac{n(n-1)}{2} + n(n-1)(n-2) + \frac{n(n-1)(n-2)(n-3)}{4} \\
 &= \frac{n(n-1)}{4}(2 + 4(n-2) + (n-2)(n-3)) \\
 &= \frac{n(n-1)}{4}n(n-1) \\
 &= \left(\frac{n(n-1)}{2}\right)^2.
 \end{aligned}$$

**评注** 回忆一下, 前  $n$  个非负整数的和

$$0 + 1 + \cdots + (n-1) = \frac{n(n-1)}{2}.$$

上面的例告诉我们,

$$0^3 + 1^3 + \cdots + (n-1)^3 = (0 + 1 + \cdots + (n-1))^2.$$

所以, 前  $n$  个非负整数的立方和等于前  $n$  个非负整数的和的平方.

**例** 求前  $n$  个非负整数的 4 次幂和

$$S(n) = 0^4 + 1^4 + \cdots + (n-1)^4 = \sum_{\ell=0}^{n-1} \ell^4.$$

取  $f(x) = x^4$ . 这里,  $m = 4$ . 画出  $m = 4$  时的差分表:

$$\begin{array}{cccccc}
 \Delta^0 f(4) & & & & & \\
 \Delta^0 f(3) & \Delta^1 f(3) & & & & \\
 \Delta^0 f(2) & \Delta^1 f(2) & \Delta^2 f(2) & & & \\
 \Delta^0 f(1) & \Delta^1 f(1) & \Delta^2 f(1) & \Delta^3 f(1) & & \\
 \Delta^0 f(0) & \Delta^1 f(0) & \Delta^2 f(0) & \Delta^3 f(0) & \Delta^4 f(0) & 
 \end{array}$$

我们直接填差分表:

256				
81	$\Delta^1 f(3)$			
16	$\Delta^1 f(2)$	$\Delta^2 f(2)$		
1	$\Delta^1 f(1)$	$\Delta^2 f(1)$	$\Delta^3 f(1)$	
0	$\Delta^1 f(0)$	$\Delta^2 f(0)$	$\Delta^3 f(0)$	$\Delta^4 f(0)$

256				
81	175			
16	65	$\Delta^2 f(2)$		
1	15	$\Delta^2 f(1)$	$\Delta^3 f(1)$	
0	1	$\Delta^2 f(0)$	$\Delta^3 f(0)$	$\Delta^4 f(0)$

256				
81	175			
16	65	110		
1	15	50	$\Delta^3 f(1)$	
0	1	14	$\Delta^3 f(0)$	$\Delta^4 f(0)$

256				
81	175			
16	65	110		
1	15	50	60	
0	1	14	36	$\Delta^4 f(0)$

256				
81	175			
16	65	110		
1	15	50	60	
0	1	14	36	24

所以

$$\begin{aligned}
 f(x) &= f(0) + \Delta f(0) \binom{x}{1} + \Delta^2 f(0) \binom{x}{2} + \Delta^3 f(0) \binom{x}{3} + \Delta^4 f(0) \binom{x}{4} \\
 &= \binom{x}{1} + 14 \binom{x}{2} + 36 \binom{x}{3} + 24 \binom{x}{4}.
 \end{aligned}$$

从而

$$\begin{aligned}
 S(n) &= \sum_{\ell=0}^{n-1} f(\ell) \\
 &= \binom{n}{2} + 14\binom{n}{3} + 36\binom{n}{4} + 24\binom{n}{5} \\
 &= \frac{n(n-1)}{2} + \frac{7n(n-1)(n-2)}{3} + \frac{3n(n-1)(n-2)(n-3)}{2} \\
 &\quad + \frac{n(n-1)(n-2)(n-3)}{5} \\
 &= \frac{n(n-1)}{30} (15 + 70(n-2) + 45(n-3)(n-2) \\
 &\quad + 6(n-4)(n-3)(n-2)) \\
 &= \frac{n(n-1)}{30} (6n^3 - 9n^2 + n + 1) \\
 &= \frac{n(n-1)}{120} (24n^3 - 36n^2 + 4n + 4) \\
 &= \frac{n(n-1)}{120} (3(2n)^3 - 9(2n)^2 + 2(2n) + 4) \\
 &= \frac{n(n-1)}{120} (3(2n)^3 - 3 - 9(2n)^2 + 9 + 2(2n) - 2) \\
 &= \frac{n(n-1)}{120} (3((2n)^3 - 1) - 9((2n)^2 - 1) + 2((2n) - 1)) \\
 &= \frac{n(n-1)}{120} (2n-1)(3((2n)^2 + 2n + 1) - 9(2n+1) + 2) \\
 &= \frac{n(n-1)(2n-1)}{120} (12n^2 - 12n - 4) \\
 &= \frac{n(n-1)(2n-1)}{30} (3n^2 - 3n - 1) \\
 &= \frac{n(n-1)(2n-1)(3n^2 - 3n - 1)}{30}.
 \end{aligned}$$

## 再探微商

本节将再讨论多项式的微商.

在讨论微商前, 让我们捡起在“广义二项系数”节里没用过的二项展开:

**命题** 设  $r, s \in \mathbb{F}[x]$ . 设  $n$  是非负整数. 则

$$(r + s)^n = \sum_{k=0}^n \binom{n}{k} r^{n-k} s^k.$$

此式称为二项展开.

**评注** 等式右侧的  $\binom{n}{k}$  称为二项系数 (*binomial coefficient*). 事实上,  $\binom{n}{k}$  一开始就是为讨论  $(r + s)^n$  的展开而生的.

**例** 在中学, 我们学过完全平方和公式:

$$(r + s)^2 = r^2 + 2rs + s^2.$$

在二项展开里, 取  $n = 2$ , 就可以得到这个公式:

$$\begin{aligned} \binom{2}{0} &= 1, \quad \binom{2}{1} = 2, \quad \binom{2}{2} = 1, \\ (r + s)^2 &= 1r^2s^0 + 2r^1s^1 + 1r^0s^2 \\ &= r^2 + 2rs + s^2. \end{aligned}$$

在上节, 我们用分配律拆开了  $(1 + x)^3$ :

$$\begin{aligned} (1 + x)^3 &= (1 + x)^2(1 + x) \\ &= (1 + 2x + x^2)(1 + x) \\ &= 1 + 2x + x^2 + x + 2x^2 + x^3 \\ &= 1 + 3x + 3x^2 + x^3. \end{aligned}$$

在二项展开里, 取  $n = 3$ :

$$\begin{aligned} \binom{3}{0} &= 1 = \binom{3}{3}, \quad \binom{3}{1} = 3 = \binom{3}{2}, \\ (r + s)^3 &= 1r^3s^0 + 3r^2s^1 + 3r^1s^2 + 1r^0s^3 \\ &= r^3 + 3r^2s + 3rs^2 + s^3. \end{aligned}$$

用  $1, x$  替换  $r, s$ , 有

$$\begin{aligned}(1+x)^3 &= 1^3 + 3 \cdot 1^2x + 3 \cdot 1x^2 + x^3 \\ &= 1 + 3x + 3x^2 + x^3.\end{aligned}$$

设  $c \in \mathbb{F}$ . 在“多项式的相等”节, 我们用  $1, x-c, (x-c)^2, \dots, (x-c)^n$  引出线性无关, 并证明了

**命题** 设  $a_0, b_0, a_1, b_1, \dots, a_n, b_n \in \mathbb{F}$ . 设  $c \in \mathbb{F}$ . 再设

$$f(x) = \sum_{i=0}^n a_i(x-c)^i, \quad g(x) = \sum_{i=0}^n b_i(x-c)^i.$$

则  $f(x) = g(x)$  的一个必要与充分条件是

$$a_0 = b_0, \quad a_1 = b_1, \quad \dots, \quad a_n = b_n.$$

并且, 任取

$$f(x) = \sum_{i=0}^n u_i x^i \in \mathbb{F}[x],$$

必存在  $v_0, v_1, \dots, v_n \in \mathbb{F}$  使

$$f(x) = \sum_{i=0}^n v_i(x-c)^i.$$

利用二项展开, 有

$$\begin{aligned}x^i &= (c + (x-c))^i \\ &= \sum_{j=0}^i \binom{i}{j} c^{i-j} (x-c)^j.\end{aligned}$$

由此, 我们可以把任意多项式

$$f(x) = \sum_{i=0}^n u_i x^i \in \mathbb{F}[x]$$

写为

$$f(x) = \sum_{i=0}^n v_i(x-c)^i \in \mathbb{F}[x].$$

**例 设**

$$f(x) = x^3 - 6x^2 + 15x - 12.$$

取  $c = 2$ . 利用二项展开, 有

$$\begin{aligned} x^3 &= (2 + (x - 2))^3 \\ &= 1 \cdot 2^3 + 3 \cdot 2^2(x - 2) + 3 \cdot 2^1(x - 2)^2 + 1 \cdot 2^0(x - 2)^3 \\ &= 8 + 12(x - 2) + 6(x - 2)^2 + (x - 2)^3, \\ x^2 &= (2 + (x - 2))^2 \\ &= 1 \cdot 2^2 + 2 \cdot 2^1(x - 2) + 1 \cdot 2^0(x - 2)^2 \\ &= 4 + 4(x - 2) + (x - 2)^2, \\ x &= 2 + (x - 2). \end{aligned}$$

所以

$$\begin{aligned} f(x) &= x^3 - 6x^2 + 15x - 12 \\ &= 8 + 12(x - 2) + 6(x - 2)^2 + (x - 2)^3 \\ &\quad - 6(4 + 4(x - 2) + (x - 2)^2) \\ &\quad + 15(2 + (x - 2)) - 12 \\ &= (x - 2)^3 + 3(x - 2) + 2. \end{aligned}$$

现在, 读者可能不再那么不熟悉二项展开了. 我们正式重述微商. 不过, 我们并不会完全照搬“微商”节.

**定义 设**

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + a_nx^n \in \mathbb{F}[x].$$

$f(x)$  的微商是多项式

$$Df(x) = 0 + 1a_1 + 2a_2x + \cdots + (n-1)a_{n-1}x^{n-2} + na_nx^{n-1} \in \mathbb{F}[x].$$

设  $t \in \mathbb{F}$ . 我们把

$$0 + 1a_1 + 2a_2t + \cdots + (n-1)a_{n-1}t^{n-2} + na_nt^{n-1} \in \mathbb{F}$$

简单地写为  $Df(t)$ .

**评注** 若  $f(x) = c, c \in \mathbb{F}$ , 则  $Df(x)$  为零多项式.

**评注** 读者可能会注意到我们在这里换了个记号. 之前, 我们用  $f'(x)$  或  $(f(x))'$  表示多项式  $f(x)$  的微商——那个时候, 我们还是在抽象的整环  $D$  上讨论问题. 现在, 我们在熟悉的  $\mathbb{F}$  里讨论问题. 读者已经很久都没见到  $D$  了吧? 从此节开始, 我们用  $D$  记号表示微商. 所以,  $D$  将不表示整环.

**例** 取  $f(x) = x^6 - x^3 + 1 \in \mathbb{F}[x]$ . 则

$$Df(x) = 6x^5 - 3x^2.$$

下面的命题也是老朋友了.

**命题** 设  $f(x), g(x) \in \mathbb{F}[x], c \in \mathbb{F}$ . 则

- (i)  $D(cf(x)) = cDf(x)$ ;
- (ii)  $D(f(x) \pm g(x)) = Df(x) \pm Dg(x)$ .

由 (i) (ii) 与数学归纳法可知: 当  $c_0, c_1, \dots, c_{k-1} \in \mathbb{F}$ , 且  $f_0(x), f_1(x), \dots, f_{k-1}(x) \in \mathbb{F}[x]$  时,

$$D\left(\sum_{\ell=0}^{k-1} c_\ell f_\ell(x)\right) = \sum_{\ell=0}^{k-1} c_\ell Df_\ell(x).$$

**证** 本来我们不必重复证明这些命题. 不过, 为了让读者更好地熟悉  $D$  记号, 我们还是在此处证明 (i) (ii), 并将剩下的推论留给读者作练习. 设

$$\begin{aligned} f(x) &= a_0 + a_1x + a_2x^2 + \dots + a_{n-1}x^{n-1} + a_nx^n, \\ g(x) &= b_0 + b_1x + b_2x^2 + \dots + b_{n-1}x^{n-1} + b_nx^n \end{aligned}$$

是  $\mathbb{F}[x]$  中二个元.

(i)  $cf(x)$  就是多项式

$$ca_0 + ca_1x + ca_2x^2 + \dots + ca_{n-1}x^{n-1} + ca_nx^n,$$



故

$$\begin{aligned}
 D(cf(x)) &= D(ca_0 + ca_1x + ca_2x^2 + \cdots + ca_{n-1}x^{n-1} + ca_nx^n) \\
 &= ca_1 + 2ca_2x + \cdots + (n-1)ca_{n-1}x^{n-2} + nca_nx^{n-1} \\
 &= ca_1 + c2a_2x + \cdots + c(n-1)a_{n-1}x^{n-2} + cna_nx^{n-1} \\
 &= c(a_1 + 2a_2x + \cdots + (n-1)a_{n-1}x^{n-2} + na_nx^{n-1}) \\
 &= cDf(x).
 \end{aligned}$$

(ii)  $f(x) \pm g(x)$  就是多项式

$$\begin{aligned}
 &(a_0 \pm b_0) + (a_1 \pm b_1)x + (a_2 \pm b_2)x^2 + \cdots \\
 &\quad + (a_{n-1} \pm b_{n-1})x^{n-1} + (a_n \pm b_n)x^n,
 \end{aligned}$$

故

$$\begin{aligned}
 &D(f(x) \pm g(x)) \\
 &= D((a_0 \pm b_0) + (a_1 \pm b_1)x + (a_2 \pm b_2)x^2 + \cdots \\
 &\quad + (a_{n-1} \pm b_{n-1})x^{n-1} + (a_n \pm b_n)x^n) \\
 &= (a_1 \pm b_1) + 2(a_2 \pm b_2)x + \cdots + (n-1)(a_{n-1} \pm b_{n-1})x^{n-2} \\
 &\quad + n(a_n \pm b_n)x^{n-1} \\
 &= (a_1 \pm b_1) + (2a_2x \pm 2b_2x) + \cdots + ((n-1)a_{n-1}x^{n-2} \\
 &\quad \pm (n-1)b_{n-1}x^{n-2}) + (na_nx^{n-1} \pm nb_nx^{n-1}) \\
 &= (a_1 + 2a_2x + \cdots + (n-1)a_{n-1}x^{n-2} + na_nx^{n-1}) \\
 &\quad \pm (b_1 + 2b_2x + \cdots + (n-1)b_{n-1}x^{n-2} + nb_nx^{n-1}) \\
 &= Df(x) \pm Dg(x).
 \end{aligned}$$

☞

**例 取**

$$f(x) = x^3 + 2, \quad g(x) = x^2 + x - 1.$$

不难得到

$$Df(x) = 3x^2, \quad Dg(x) = 2x + 1.$$

(i)  $4g(x)$  也是多项式, 当然可以有微商. 因为

$$4g(x) = 4x^2 + 4x - 4,$$

故

$$D(4g(x)) = 8x + 4,$$

这刚好是  $4Dg(x)$ :

$$4Dg(x) = 4(2x + 1) = 8x + 4.$$

(ii)  $f(x) + g(x)$  也是多项式. 因为

$$f(x) + g(x) = x^3 + 2 + x^2 + x - 1 = x^3 + x^2 + x + 1,$$

故

$$D(f(x) + g(x)) = 3x^2 + 2x + 1,$$

而这刚好是  $Df(x) + Dg(x)$ :

$$Df(x) + Dg(x) = 3x^2 + 2x + 1.$$

前面讲差商与差分时, 我们引入了高级差商与高级差分. 类似地, 我们引入高级微商.

**定义** 设  $f(x) \in \mathbb{F}[x]$ . 记

$$D^0 f(x) = f(x) \in \mathbb{F}[x],$$

并称其为  $f(x)$  的 0 级微商 (*zeroth-order derivative*). 1 级微商就是微商:

$$D^1 f(x) = Df(x) = D(D^0 f(x)) \in \mathbb{F}[x].$$

1 级微商的微商是 2 级微商:

$$D^2 f(x) = D(D^1 f(x)) \in \mathbb{F}[x].$$

2 级微商的微商是 3 级微商:

$$D^3 f(x) = D(D^2 f(x)) \in \mathbb{F}[x].$$

一般地,  $e$  级微商就是  $e - 1$  级微商的微商:

$$D^e f(x) = D(D^{e-1} f(x)) \in \mathbb{F}[x].$$

高级微商可指代任意  $e$  级微商, 此处  $e > 1$ .

设  $t \in \mathbb{F}$ . 既然  $D^e f(x)$  是某个多项式

$$v_0 + v_1 x + \cdots + v_s x^s \in \mathbb{F}[x],$$

我们将

$$v_0 + v_1 t + \cdots + v_s t^s \in \mathbb{F}$$

简单地写为  $D^e f(t)$ .

**例 设**

$$f(x) = 2x^3 + 3x^2 + 5x + 7.$$

根据定义,  $f(x)$  的 0 级微商就是自己:

$$D^0 f(x) = 2x^3 + 3x^2 + 5x + 7.$$

$f(x)$  的 1 级微商是

$$D^1 f(x) = Df(x) = 6x^2 + 6x + 5.$$

$f(x)$  的 2 级微商是

$$D^2 f(x) = D(D^1 f(x)) = 12x + 6.$$

$f(x)$  的 3 级微商是

$$D^3 f(x) = D(D^2 f(x)) = 12.$$

$f(x)$  的 4 级微商是

$$D^4 f(x) = D(D^3 f(x)) = 0.$$

读者不难验证: 对任意超出 3 的整数  $e$ , 必有

$$D^e f(x) = 0.$$

类似地, 高级微商适合如下性质:

**命题** 设  $e$  是非负整数. 当  $c_0, c_1, \dots, c_{k-1} \in \mathbb{F}$ , 且  $f_0(x), f_1(x), \dots, f_{k-1}(x) \in \mathbb{F}[x]$  时,

$$D^e \left( \sum_{\ell=0}^{k-1} c_\ell f_\ell(x) \right) = \sum_{\ell=0}^{k-1} c_\ell D^e f_\ell(x).$$

**证** 用数学归纳法. 我们把具体过程留给读者当练习. ✎

当初我们为得到 Vandermonde 恒等式与二项展开, 我们引入了临时工具  $r^{[k]}$ . 现在, 类似地, 为了方便地讨论多项式的高级微商, 我们引入

**定义** 设  $m$  为整数. 设  $r \in \mathbb{F}[x]$ . 定义

$$q_m(r) = \begin{cases} \frac{1}{m!} r^m, & m > 0; \\ 1, & m = 0; \\ 0, & m < 0. \end{cases}$$

设  $k$  是整数. 我们知道

$$\Delta \binom{x}{k} = \binom{x}{k-1}.$$

类似地, 我们有

**命题** 设  $m$  为整数. 则

$$Dq_m(x) = q_{m-1}(x).$$

**证**  $m > 0$  时,

$$Dq_m(x) = m \cdot \frac{x^{m-1}}{m!} = \frac{x^{m-1}}{(m-1)!} = q_{m-1}(x).$$

$m \leq 0$  时,  $q_m(x) = a$ , 这里  $a \in \mathbb{F}$ . 故

$$Dq_m(x) = 0 = q_{m-1}(x). ✎$$

由此可得

**命题** 设  $e$  是非负整数. 设  $m$  为整数. 则

$$D^e q_m(x) = q_{m-e}(x).$$

**证** 用数学归纳法. 我们把具体过程留给读者当练习. ✎

现在, 我们看高级微商与二项展开的关系.

固定某  $c \in \mathbb{F}$ . 固定某非负整数  $n$ . 任取不高于  $n$  的非负整数  $i$ . 则

$$\begin{aligned} q_i(x) &= \frac{1}{i!} \sum_{j=0}^i \binom{i}{j} c^{i-j} (x-c)^j \\ &= \frac{1}{i!} \sum_{j=0}^i \frac{i!}{(i-j)!j!} c^{i-j} (x-c)^j \\ &= \frac{1}{i!} \sum_{j=0}^i i! q_{i-j}(c) q_j(x-c) \\ &= \sum_{j=0}^i q_{i-j}(c) q_j(x-c) \\ &= \sum_{j=0}^n q_{i-j}(c) q_j(x-c). \end{aligned}$$

任取次不高于  $n$  的多项式

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{F}[x].$$

设

$$b_\ell = \ell! a_\ell \quad (\ell = 0, 1, \cdots, n).$$

则

$$f(x) = b_0 q_0(x) + b_1 q_1(x) + \cdots + b_n q_n(x).$$

不难看出, 当  $j$  是非负整数时,

$$D^j f(x) = b_0 q_{0-j}(x) + b_1 q_{1-j}(x) + \cdots + b_n q_{n-j}(x).$$

所以

$$\begin{aligned}
 f(x) &= \sum_{i=0}^n b_i q_i(x) \\
 &= \sum_{i=0}^n b_i \sum_{j=0}^n q_{i-j}(c) q_j(x-c) \\
 &= \sum_{i=0}^n \sum_{j=0}^n b_i q_{i-j}(c) q_j(x-c) \\
 &= \sum_{j=0}^n \sum_{i=0}^n b_i q_{i-j}(c) q_j(x-c) \\
 &= \sum_{j=0}^n \left( \sum_{i=0}^n b_i q_{i-j}(c) \right) q_j(x-c) \\
 &= \sum_{j=0}^n D^j f(c) q_j(x-c) \\
 &= \sum_{j=0}^n \frac{D^j f(c)}{j!} (x-c)^j.
 \end{aligned}$$

我们已经证明了

**命题** 设  $n$  是非负整数. 设  $f(x)$  是次不高于  $n$  的多项式. 设  $c \in \mathbb{F}$ . 则 Taylor 公式 (*Taylor's formula*) 成立:

$$f(x) = \sum_{j=0}^n \frac{D^j f(c)}{j!} (x-c)^j.$$

**评注** 我们可以说, Taylor 公式是二项展开的推广. 也可以说, 二项展开是 Taylor 公式的特例.

**评注** 取  $c = 0$ , 有

$$f(x) = \sum_{j=0}^n \frac{D^j f(0)}{j!} x^j.$$

读者可能会注意到, 上式的形式与

$$f(x) = \sum_{k=0}^n \Delta^k f(0) \binom{x}{k}$$

的形式十分相似.

**评注** 以后我们不用  $q_m(r)$  记号了.

**评注** 我们提一个读者可能已经注意到的事实. 设  $n$  是非负整数. 则  $n$  次多项式的  $n$  级微商不是 0, 但  $n+1$  级微商是 0. 这也解释了为什么在 Taylor 公式里, 我们只要求  $n$  不低于  $f(x)$  的次.

**例** 取  $n=3$ . 设

$$f(x) = x^3 - 6x^2 + 15x - 12.$$

则  $f(x)$  的次不高于  $n$ , 且

$$D^0 f(x) = f(x) = x^3 - 6x^2 + 15x - 12,$$

$$D^1 f(x) = Df(x) = 3x^2 - 12x + 15,$$

$$D^2 f(x) = D(Df(x)) = 6x - 12,$$

$$D^3 f(x) = D(D^2 f(x)) = 6.$$

取  $c=2$ . 则

$$D^0 f(2) = 2^3 - 6 \cdot 2^2 + 15 \cdot 2 - 12 = 2,$$

$$D^1 f(2) = 3 \cdot 2^2 - 12 \cdot 2 + 15 = 3,$$

$$D^2 f(2) = 6 \cdot 2 - 12 = 0,$$

$$D^3 f(2) = 6.$$

根据 Taylor 公式,

$$\begin{aligned} f(x) &= 2 + \frac{3}{1!}(x-2) + \frac{0}{2!}(x-2)^2 + \frac{6}{3!}(x-2)^3 \\ &= 2 + 3(x-2) + (x-2)^3. \end{aligned}$$

Taylor 公式一个用途是证明

**命题** 设  $f(x), g(x) \in \mathbb{F}[x]$ . 则

$$(\star) \quad D(f(x)g(x)) = Df(x) \cdot g(x) + f(x) \cdot Dg(x).$$

**证** 设  $h(x) = f(x)g(x)$ . 取整数  $n$  使  $\deg f(x) \leq n, \deg g(x) \leq n, \deg h(x) \leq n$ , 且  $1 \leq n$ . 任取  $c \in \mathbb{F}$ . 则

$$\begin{aligned} f(x) &= \sum_{i=0}^n \frac{D^i f(c)}{i!} (x-c)^i, \\ g(x) &= \sum_{j=0}^n \frac{D^j g(c)}{j!} (x-c)^j, \\ h(x) &= \sum_{k=0}^n \frac{D^k h(c)}{k!} (x-c)^k. \end{aligned}$$

不过, 既然  $h(x)$  是  $f(x)$  与  $g(x)$  的积, 也应有

$$h(x) = \sum_{k=0}^{n+n} s_k (x-c)^k = \sum_{k=0}^n s_k (x-c)^k,$$

其中

$$\begin{aligned} s_k &= \sum_{i=0}^k \frac{D^i f(c)}{i!} \cdot \frac{D^{k-i} g(c)}{(k-i)!} \\ &= \frac{1}{k!} \sum_{i=0}^k \binom{k}{i} D^i f(c) D^{k-i} g(c). \end{aligned}$$

所以, 任取不超过  $n$  的非负整数  $k$ , 必有

$$\begin{aligned} s_k &= \frac{D^k h(c)}{k!} \\ \Rightarrow D^k h(c) &= \sum_{i=0}^k \binom{k}{i} D^i f(c) D^{k-i} g(c). \end{aligned}$$

作多项式

$$E(x) = D^k h(x) - \sum_{i=0}^k \binom{k}{i} D^i f(x) D^{k-i} g(x).$$

上面的推理告诉我们, 任取  $c \in \mathbb{F}$ , 必有  $E(c) = 0$ . 所以  $E(x)$  一定是零多项式, 即

$$D^k h(x) = \sum_{i=0}^k \binom{k}{i} D^i f(x) D^{k-i} g(x).$$



取  $k = 1$ , 有

$$\begin{aligned}
 & D(f(x)g(x)) \\
 &= D^1 h(x) \\
 &= \sum_{i=0}^1 \binom{1}{i} D^i f(x) D^{1-i} g(x) \\
 &= 1 \cdot D^0 f(x) D^1 g(x) + 1 \cdot D^1 f(x) D^0 g(x) \\
 &= Df(x) \cdot g(x) + f(x) \cdot Dg(x). \quad \text{☞}
 \end{aligned}$$

**评注** 事实上, 我们得到了高级微商的 Leibniz 公式 (*Leibniz's formula*): 若  $k$  是非负整数, 且  $f(x), g(x) \in \mathbb{F}[x]$ , 则

$$D^k(f(x)g(x)) = \sum_{i=0}^k \binom{k}{i} D^i f(x) D^{k-i} g(x).$$

不过, 在本文里, 我们用不到这个公式.

**例 取**

$$f(x) = x^3 + 2, \quad g(x) = x^2 + x - 1.$$

不难得到

$$Df(x) = 3x^2, \quad Dg(x) = 2x + 1.$$

$f(x)$  与  $g(x)$  的积

$$f(x)g(x) = x^5 + x^4 - x^3 + 2x^2 + 2x - 2$$

的微商是

$$D(f(x)g(x)) = 5x^4 + 4x^3 - 3x^2 + 4x + 2.$$

如果用上面的 (★) 计算, 就是

$$\begin{aligned}
 & Df(x)g(x) + f(x)Dg(x) \\
 &= 3x^2(x^2 + x - 1) + (x^3 + 2)(2x + 1) \\
 &= 3x^4 + 3x^3 - 3x^2 + 2x^4 + x^3 + 4x + 2 \\
 &= 5x^4 + 4x^3 - 3x^2 + 4x + 2.
 \end{aligned}$$

下面的二个命题是正确的:

**命题** 当  $f_0(x), f_1(x), \dots, f_{k-1}(x) \in \mathbb{F}[x]$  时,

$$\begin{aligned} & D(f_0(x)f_1(x)\cdots f_{k-1}(x)) \\ &= Df_0(x)f_1(x)\cdots f_{k-1}(x) + f_0(x)Df_1(x)\cdots f_{k-1}(x) + \cdots \\ & \quad + f_0(x)f_1(x)\cdots Df_{k-1}(x). \end{aligned}$$

取  $f_0(x) = f_1(x) = \cdots = f_{k-1}(x) = f(x)$  知

$$D((f(x))^k) = k(f(x))^{k-1}Df(x).$$

**证** 用数学归纳法. 我们把具体过程留给读者当练习. ✎

**例** 设  $f(x) = (x^2 + x - 1)^{666}$ . 求  $Df(x)$ .

取  $g(x) = x^2 + x - 1$ . 显然,  $f(x) = (g(x))^{666}$ . 所以

$$\begin{aligned} Df(x) &= D((g(x))^{666}) \\ &= 666(g(x))^{666-1}Dg(x) \\ &= 666(x^2 + x - 1)^{665}(2x + 1) \\ &= 666(2x + 1)(x^2 + x - 1)^{665}. \end{aligned}$$

**命题** 设  $f(x), g(x) \in \mathbb{F}[x]$ . 则  $f(x)$  与  $g(x)$  的复合的微商适合链规则:

$$D(g \circ f)(x) = (Dg \circ f)(x)Df(x).$$

**证** 可看“微商”节的相应内容. ✎

**例** 设  $f(x) = (x^2 + x - 1)^5 + 3(x^2 + x - 1)^4 - 1$ . 求  $Df(x)$ .

取  $g(x) = x^5 + 3x^4 - 1$  与  $h(x) = x^2 + x - 1$ . 则

$$\begin{aligned} Dg(x) &= 5x^4 + 12x^3 = x^3(5x + 12), \\ Dh(x) &= 2x + 1. \end{aligned}$$

显然,

$$f(x) = g(h(x)) = (g \circ h)(x).$$

所以

$$\begin{aligned}Df(x) &= (Dg \circ h)(x)Dh(x) \\&= (x^2 + x - 1)^3(5(x^2 + x - 1) + 12)(2x + 1) \\&= (2x + 1)(5x^2 + 5x + 7)(x^2 + x - 1)^3.\end{aligned}$$

## 多项式的微分学初步

本节讨论多项式的微分学 (*differential calculus*) 初步<sup>†</sup>. 这也是本文的最终节.

How time flies! 一开始, 我们在“预备知识”给读者介绍预备知识. 然后, 我们给读者介绍了系数为整环的元的多项式. 当初, 多项式还是有点抽象的. 我们利用带余除法推出了几个很重要的命题, 并指出: 当多项式的系数为  $F$  的元时, 多项式与中学学的多项式 (函数) 没有根本上的区别. 我们在“插值”节开始介绍多项式的应用. 后面的“求和公式”节告诉读者一种方便的求和法. 在上节, 我们捡起很久未出场的微商, 并把它重讲了一遍. 我们利用高级微商推广了二项展开, 得到了 Taylor 公式, 并用它重证多项式的积的微商规则.

之前, 微商都是形式的——有点“空降”的味道. 现在, 我们要用 Taylor 公式给微商一种含义. 如果您知道一点微积分 (*calculus*), 您将不会对本节感到特别陌生; 如果您没有学过微积分, 无妨将本节作为“入微作”.

我们在“ $F$  上的多项式”节说过, 我们不再讨论抽象的整环或系数为整环的元的多项式, 而是讨论  $F$  与  $F[x]$ . 现在, 我们再具体一点——讨论老朋友  $\mathbb{R}$  与  $\mathbb{R}[x]$ ——再准确点, 其实是  $\mathbb{R}$  到  $\mathbb{R}$  的多项式函数.

不过, 我们需要承认一个事实是对的. 为什么说“承认”呢? 因为它的证明需要超出本文的知识很多很多的工具. 但是, 它并不是什么“牵强附会”的命题. 是什么命题呢? 我们不必现在就说; 我们在用到它的时候再说.

我们先带读者熟悉实数.

读者也许还记得实数  $a$  的绝对值:

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

请读者尝试自行证明下面四个命题. 当然, 熟悉这四个命题的读者可以不证. 我们把它们写在这里供读者参考.

**命题** 设  $a \in \mathbb{R}$ . 则  $|a| \geq 0$ .

<sup>†</sup> 学过一元函数微分学的读者可能会觉得本节废话连篇. 不过, 为照顾不熟悉三角不等式及相关知识的读者, 作者也没什么更好的写作思路了.

**命题** 设  $a \in \mathbb{R}$ . 则

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

**命题** 设  $a \in \mathbb{R}$ . 则  $-|a| \leq a \leq |a|$ .

**命题** 设  $a \in \mathbb{R}$ , 且  $b > 0$ . 则

$$|a| \leq b \iff -b \leq a \leq b;$$

$$|a| < b \iff -b < a < b.$$

读者也许还记得平方的性质:

$$a^2 = (-a)^2.$$

并且, 若  $a, b$  都是非负数, 则

$$a = b \iff a^2 = b^2.$$

利用这些性质, 我们有

**命题** 设  $a_0, a_1, \dots, a_{n-1} \in \mathbb{R}$ . 则

$$|a_0 a_1 \cdots a_{n-1}| = |a_0| \cdot |a_1| \cdots |a_{n-1}|.$$

特别地, 若  $a_0 = a_1 = \cdots = a_{n-1} = a$ , 则

$$|a^n| = |a|^n.$$

**证** 请读者尝试自行证明此命题. 不过, 我们愿意提示读者: (i) 等式的左右二侧都是非负的; (ii) 等式的左右二侧的平方是一样的.  $\clubsuit$

下面是一个十分重要的不等式:

**命题** 设  $a_0, a_1, \dots, a_{n-1} \in \mathbb{R}$ . 则

$$|a_0 + a_1 + \cdots + a_{n-1}| \leq |a_0| + |a_1| + \cdots + |a_{n-1}|.$$

这个不等式的一个名字是三角不等式 (*triangle inequality*).

证 易知

$$\begin{aligned} -|a_0| &\leq a_0 \leq |a_0|, \\ -|a_1| &\leq a_1 \leq |a_1|, \\ &\dots\dots\dots, \\ -|a_{n-1}| &\leq a_{n-1} \leq |a_{n-1}|. \end{aligned}$$

记

$$b = |a_0| + |a_1| + \cdots + |a_{n-1}|.$$

易知  $b \geq 0$ , 且

$$-b \leq a_0 + a_1 + \cdots + a_{n-1} \leq b.$$

所以

$$|a_0 + a_1 + \cdots + a_{n-1}| \leq b = |a_0| + |a_1| + \cdots + |a_{n-1}|. \quad \text{☺}$$

**定义** 设  $a, b$  是实数, 且  $a < b$ . 称

$$[a, b] = \{t \in \mathbb{R} \mid a \leq t \leq b\}$$

为闭区间 (*closed interval*); 称

$$(a, b) = \{t \in \mathbb{R} \mid a < t < b\}$$

为开区间 (*open interval*). 类似地, 有半闭区间 (*half-closed interval*):

$$[a, b) = \{t \in \mathbb{R} \mid a \leq t < b\},$$

$$(a, b] = \{t \in \mathbb{R} \mid a < t \leq b\}.$$

$[a, b], (a, b), [a, b), (a, b]$  都是有限区间 (*finite interval*). 此名暗示着, 还有无限区间 (*infinite interval*):

$$(-\infty, a) = \{t \in \mathbb{R} \mid t < a\},$$

$$(-\infty, a] = \{t \in \mathbb{R} \mid t \leq a\},$$

$$(b, +\infty) = \{t \in \mathbb{R} \mid t > b\},$$

$$[b, +\infty) = \{t \in \mathbb{R} \mid t \geq b\},$$

$$(-\infty, +\infty) = \mathbb{R}.$$

有限区间与无限区间都是区间 (*interval*).

**命题** 设  $a, b$  是实数, 且  $a < b$ . 若  $r > |a|$  且  $r > |b|$ , 则  $[a, b], (a, b), [a, b), (a, b]$  都是  $[-r, r]$  的真子集.

**证** 请读者尝试自行证明此命题. ✎

下面建立一些关于多项式的不等式.

**命题** 设  $n$  是非负整数. 设  $a_0, a_1, \dots, a_n \in \mathbb{R}$ . 任取正数  $r$ , 必存在正数  $M$  使

$$|u| \leq r \implies |a_0 + a_1 u + \dots + a_n u^n| \leq M.$$

**证** 设正数  $C$  不低于  $|a_0|, |a_1|, \dots, |a_n|$  的任意一个. 则  $|u| \leq r$  时,

$$\begin{aligned} & |a_0 + a_1 u + \dots + a_n u^n| \\ & \leq |a_0| + |a_1 u| + \dots + |a_n u^n| \\ & = |a_0| + |a_1| |u| + \dots + |a_n| |u|^n \\ & \leq C(1 + |u| + \dots + |u|^n) \\ & \leq C(1 + r + \dots + r^n). \end{aligned}$$

记

$$M = C(1 + r + \dots + r^n) > 0.$$

由此,

$$|u| \leq r \implies |a_0 + a_1 u + \dots + a_n u^n| \leq M. \quad \text{✎}$$

**命题** 设  $I$  是有限区间. 设  $f(x) \in \mathbb{R}[x]$ . 存在正数  $M$  使

$$u \in I \implies |f(u)| \leq M.$$

用文字描述这句话, 就是: 多项式函数在任意有限区间上都是有界的 (*to be bounded*).

**证** 取  $r > 0$  使  $I \subset [-r, r]$ . 设

$$f(x) = a_0 + a_1 x + \dots + a_n x^n \in \mathbb{R}[x].$$

根据上个命题, 存在正数  $M$  使

$$|u| \leq r \implies |f(u)| \leq M.$$

所以

$$u \in I \implies |f(u)| \leq M.$$

✎

我们有时称  $\mathbb{R}$  的元为点.

**命题** 设  $f(x) \in \mathbb{R}[x]$ . 设  $t_0 \in \mathbb{R}$ . 任取  $\varepsilon > 0$ , 必有  $\delta > 0$ , 使

$$|t - t_0| < \delta \implies |f(t) - f(t_0)| < \varepsilon.$$

通俗地说, 当点  $t$  与点  $t_0$  足够近时, 多项式在二点的值可任意接近.

**证** 若  $f(x) = c$ ,  $c \in \mathbb{R}$ , 则

$$|f(t) - f(t_0)| = |c - c| = 0 < \varepsilon$$

总是成立的. 下设  $f(x)$  的次高于 0.

根据“多项式的根”节的结论, 存在多项式  $q(x)$  使

$$f(x) = (x - t_0)q(x) + f(t_0).$$

所以

$$|f(t) - f(t_0)| = |q(t)||t - t_0|.$$

设  $I = [t_0 - 1, t_0 + 1]$ . 不难看出,

$$\begin{aligned} I &= \{t \in \mathbb{R} \mid t_0 - 1 \leq t \leq t_0 + 1\} \\ &= \{t \in \mathbb{R} \mid -1 \leq t - t_0 \leq 1\} \\ &= \{t \in \mathbb{R} \mid |t - t_0| \leq 1\}. \end{aligned}$$

利用上个命题, 存在  $M > 0$  使

$$|t - t_0| \leq 1 \implies |q(t)| \leq M.$$



这样,

$$|t - t_0| \leq 1 \implies |f(t) - f(t_0)| \leq M|t - t_0|.$$

任取  $\varepsilon > 0$ . 取一个既低于 1 也低于  $\frac{\varepsilon}{M}$  的正数  $\delta$ . 这样,  $|t - t_0| < \delta$  时, 必有

$$|f(t) - f(t_0)| \leq M|t - t_0| < M \cdot \frac{\varepsilon}{M} = \varepsilon. \quad \clubsuit$$

**命题** 设  $t_0 \in \mathbb{R}$ . 设  $\ell$  是非负整数. 设

$$\begin{aligned} f(x) &= a_\ell(x - t_0)^\ell + a_{\ell+1}(x - t_0)^{\ell+1} + \cdots + a_n(x - t_0)^n, \\ g(x) &= a_\ell(x - t_0)^\ell, \end{aligned}$$

且  $a_\ell \neq 0$ . 则存在  $\delta > 0$ , 使  $0 < |t - t_0| < \delta$  时, 必有  $f(t)$  与  $g(t)$  同号.

**证** 我们说, 二个不为 0 的数  $a, b$  同号, 相当于  $ab > 0$ . 记

$$p(x) = \frac{1}{a_\ell} \sum_{j=\ell+1}^n a_j(x - t_0)^{j-(\ell+1)}.$$

则

$$\begin{aligned} f(x) &= a_\ell(x - t_0)^\ell + a_\ell(x - t_0)^\ell(x - t_0)p(x) \\ &= a_\ell(x - t_0)^\ell(1 + (x - t_0)p(x)) \\ &= g(x)(1 + (x - t_0)p(x)). \end{aligned}$$

所以

$$f(x)g(x) = (g(x))^2(1 + (x - t_0)p(x)).$$

记  $q(x) = 1 + (x - t_0)p(x)$ . 取  $\varepsilon = \frac{1}{2}$ . 由上个命题, 存在  $\delta > 0$  使

$$|t - t_0| < \delta \implies |q(t) - 1| = |q(t) - q(t_0)| < \varepsilon = \frac{1}{2}.$$

所以

$$|t - t_0| < \delta \implies q(t) - 1 > -\frac{1}{2}.$$

所以

$$0 < |t - t_0| < \delta \implies q(t) > \frac{1}{2}.$$

因为

$$0 < |t - t_0| \implies (g(t))^2 > 0,$$

故

$$0 < |t - t_0| < \delta \implies f(t)g(t) > \frac{1}{2}(g(t))^2 > 0. \quad \text{♣}$$

下面讨论微商与变率的关系.

**定义** 设  $a, b$  是实数, 且  $a < b$ . 设  $f(x) \in \mathbb{R}[x]$ . 我们说多项式  $f(x)$  在区间  $[a, b]$  的平均变率 (*average rate of change*) 是

$$\frac{f(b) - f(a)}{b - a}.$$

**例** 设  $f(x) = a_0 + a_1x$ . 则

$$\frac{f(b) - f(a)}{b - a} = \frac{(a_0 + a_1b) - (a_0 + a_1a)}{b - a} = a_1.$$

可以看到,  $f(x)$  在  $[a, b]$  的平均变率与具体区间无关. 反过来, 若多项式  $f(x)$  适合: 任取  $c, d \in \mathbb{R}, c < d$ , 都有

$$\frac{f(d) - f(c)}{d - c}$$

为常数  $A$ , 则

$$d > 0 \implies f(d) = f(0) + Ad.$$

作多项式

$$E(x) = f(0) + Ax - f(x),$$

则任取  $d > 0$ , 都有  $E(d) = 0$ . 这样,  $E(x)$  是零多项式, 即

$$f(x) = f(0) + Ax.$$

从上面的例可知: 次低于 2 的多项式  $f(x) = a_0 + a_1x$  在任意闭区间  $[a, b]$  的平均变率都是常数. 我们说, 任取  $t \in \mathbb{R}$ ,  $f(x)$  在点  $t$  的变率 (rate of change) 是  $a_1$ .

不过, 次高于 1 的多项式有着不一样的平均变率.

**例** 设  $f(x) = x^2 + x - 1$ . 取  $a = 0, b = 1, c = 2$ . 易知

$$f(a) = -1, \quad f(b) = 1, \quad f(c) = 5.$$

所以,  $f(x)$  在  $[a, b]$  的平均变率是

$$\frac{f(b) - f(a)}{b - a} = \frac{1 - (-1)}{1 - 0} = 2.$$

而  $f(x)$  在  $[b, c]$  的平均变率是

$$\frac{f(c) - f(b)}{c - b} = \frac{5 - 1}{2 - 1} = 4.$$

顺便一提,  $f(x)$  在  $[a, c]$  的平均变率是

$$\frac{f(c) - f(a)}{c - a} = \frac{5 - (-1)}{2 - 0} = 3.$$

虽然我们现在还不知道任意多项式  $f(x)$  在点  $t$  的变率, 但我们还是能作出一些定性判断的.

**例** 设  $f_1(x), f_2(x)$  是多项式. 设想  $P_1, P_2$  二人同时同地在一条笔直的路上骑车单向前进. 设  $f_1(t), f_2(t)$  分别表示  $t$  s 后  $P_1, P_2$  距始点的距离. 所以,  $f_1(x)$  (或  $f_2(x)$ ) 在  $[a, b]$  的平均变率代表  $a$  s 至  $b$  s 这一段的平均速率. 如果  $f_1(x)$  (或  $f_2(x)$ ) 的次为 1, 则平均变率  $A$  不变, 也就是我们常说的“匀速直线运动”. 我们也说, 任取  $a > 0$ ,  $P_1$  (或  $P_2$ ) 在  $a$  s 的速率都是  $A$ .

设  $t_0$  s 后,  $P_1$  从后赶上  $P_2$  并超越之. 这相当于, 存在  $\delta > 0$  使

$$t_0 - \delta < t < t_0 \implies f_1(t) < f_2(t),$$

$$t = t_0 \implies f_1(t) = f_2(t),$$

$$t_0 < t < t_0 + \delta \implies f_1(t) > f_2(t).$$

经验告诉我们,  $P_1$  在  $t_0$  s 的速率一定不低于  $P_2$  在  $t_0$  s 的速率. 若不然,  $P_1$  是不可能赶上  $P_2$  后并超越之, 是不是?

抽象上面的例, 我们可得到

**命题** 虽然我们还不能准确地定义变率, 但生活经验告诉我们, 变率应适合如下特性:

设  $f(x), g(x) \in \mathbb{R}[x]$ . 若  $f(t_0) = g(t_0)$ , 且存在  $\delta > 0$  使

$$t_0 - \delta < t < t_0 \implies f(t) < g(t),$$

$$t_0 < t < t_0 + \delta \implies f(t) > g(t).$$

我们说,  $f(x)$  在点  $t_0$  的变率不低于  $g(x)$  在点  $t_0$  的变率.

为充分利用此特性, 我们特化之.

设  $A \in \mathbb{R}$ . 取  $g(x) = f(t_0) + A(x - t_0)$ , 则  $f(t_0) = g(t_0)$ . 因为  $g(x)$  在  $t_0$  的变率是  $A$ , 故

**命题** 变率应适合如下特性:

设  $f(x) \in \mathbb{R}[x]$ . 若存在  $\delta_0 > 0$  使

$$t_0 - \delta_0 < t < t_0 \implies f(t) < f(t_0) + A(t - t_0),$$

$$t_0 < t < t_0 + \delta_0 \implies f(t) > f(t_0) + A(t - t_0).$$

我们说,  $f(x)$  在点  $t_0$  的变率不低于  $A$ .

若存在  $\delta_1 > 0$  使

$$t_0 - \delta_1 < t < t_0 \implies f(t) > f(t_0) + A(t - t_0),$$

$$t_0 < t < t_0 + \delta_1 \implies f(t) < f(t_0) + A(t - t_0).$$

我们说,  $f(x)$  在点  $t_0$  的变率不高于  $A$ .

若  $t_0 - \delta < t < t_0$ , 则  $t_0 - t > 0$ . 所以

$$\begin{aligned} f(t) < f(t_0) + A(t - t_0) &\iff f(t) < f(t_0) - A(t_0 - t) \\ &\iff A(t_0 - t) < f(t_0) - f(t) \\ &\iff A < \frac{f(t_0) - f(t)}{t_0 - t} \\ &\iff \frac{f(t) - f(t_0)}{t - t_0} > A. \end{aligned}$$

若  $t_0 < t < t_0 + \delta$ , 则  $t - t_0 > 0$ . 所以

$$\begin{aligned} f(t) > f(t_0) + A(t - t_0) &\iff f(t) - f(t_0) > A(t - t_0) \\ &\iff \frac{f(t) - f(t_0)}{t - t_0} > A. \end{aligned}$$

$t_0 - \delta < t < t_0$  与  $t_0 < t < t_0 + \delta$  相当于

$$0 < |t - t_0| < \delta.$$

这样, 我们有

**命题** 变率应适合如下特性:

设  $f(x) \in \mathbb{R}[x]$ . 若存在  $\delta > 0$  使

$$0 < |t - t_0| < \delta \implies \frac{f(t) - f(t_0)}{t - t_0} > A,$$

我们说,  $f(x)$  在点  $t_0$  的变率不低于  $A$ .

同理可得

**命题** 变率应适合如下特性:

设  $f(x) \in \mathbb{R}[x]$ . 若存在  $\delta > 0$  使

$$0 < |t - t_0| < \delta \implies \frac{f(t) - f(t_0)}{t - t_0} < A,$$

我们说,  $f(x)$  在点  $t_0$  的变率不高于  $A$ .

现在, 让我们揭秘变率.

设  $t_0 \in \mathbb{R}$ . 设  $f(x)$  的次不高于  $n$ . 根据 Taylor 公式,

$$f(x) = f(t_0) + Df(t_0)(x - t_0) + \sum_{j=2}^n \frac{D^j f(t_0)}{j!} (x - t_0)^j.$$

所以,  $t \neq t_0$  时,

$$\frac{f(t) - f(t_0)}{t - t_0} = Df(t_0) + \sum_{j=2}^n \frac{D^j f(t_0)}{j!} (t - t_0)^{j-1}.$$

设  $A \in \mathbb{R}$ . 则

$$\frac{f(t) - f(t_0)}{t - t_0} - A = (Df(t_0) - A) + \sum_{j=2}^n \frac{D^j f(t_0)}{j!} (t - t_0)^{j-1}.$$

记

$$q(x) = (Df(t_0) - A) + \sum_{j=2}^n \frac{D^j f(t_0)}{j!} (x - t_0)^{j-1}.$$

若  $Df(t_0) - A \neq 0$ , 则存在  $\delta > 0$ , 使  $0 < |t - t_0| < \delta$  时,  $q(t)$  与  $Df(t_0) - A$  同号.

设  $f(x)$  在点  $t_0$  的变率为  $r$ . 任取  $A < Df(t_0)$ , 必有

$$0 < |t - t_0| < \delta \implies \frac{f(t) - f(t_0)}{t - t_0} > A \implies r \geq A.$$

任取  $A > Df(t_0)$ , 必有

$$0 < |t - t_0| < \delta \implies \frac{f(t) - f(t_0)}{t - t_0} < A \implies r \leq A.$$

我们证明:  $r = Df(t_0)$ . 反证法. 若  $r < Df(t_0)$ , 作

$$A_0 = \frac{Df(t_0) + r}{2}.$$

不难看出

$$A_0 < \frac{Df(t_0) + Df(t_0)}{2} = Df(t_0),$$

故

$$r \geq A_0 = \frac{Df(t_0) + r}{2} \implies r \geq Df(t_0),$$

矛盾! 若  $r > Df(t_0)$ , 作

$$A_1 = \frac{Df(t_0) + r}{2}.$$

不难看出

$$A_1 > \frac{Df(t_0) + Df(t_0)}{2} = Df(t_0),$$

故

$$r \leq A_1 = \frac{Df(t_0) + r}{2} \implies r \leq Df(t_0),$$

矛盾! 所以,  $r$  必为  $Df(t_0)$ .

我们得到了本节最重要的命题:

**命题** 设  $f(x) \in \mathbb{R}[x]$ . 设  $t_0 \in \mathbb{R}$ . 则  $Df(t_0)$  是  $f(x)$  在点  $t_0$  的变率.

至此, 我们找到了微商的一种含义, 本节的任务终了. 我们就讨论到这里吧. 再见, 读者朋友!





## 同人作

“啊, 这. ‘查考多项式’ 都能出同人作?”

“还真有人写呢. 不过, 挺烂的. Still better than nothing, though.”

“Fine. I get it.”

## 整数的一些性质

本文的目标是补充一点整数的性质; 我们后面会用到这些东西.

为尽可能多地照顾读者, 本文被加了一点细节.

在正式进入讨论前, 作者希望读者能回想起二件事:

(i) 整数  $f$  的绝对值是

$$|f| = \begin{cases} f, & f \geq 0; \\ -f, & f < 0. \end{cases}$$

若整数  $g, h$  适合  $f = gh$ , 则  $|f| = |g| \cdot |h|$ .

(ii) 整数的乘法适合消去律. 设  $f, g, h$  是整数. 若  $f \neq 0$ , 且  $fg = fh$ , 则  $g = h$ .

我们先从整数的单位开始.

**定义** 设  $f$  是整数. 若存在整数  $g$  使  $fg = 1$ , 则说  $f$  是单位 (*unit*).  $g$  称为  $f$  的逆 (*inverse*).

**命题** 1 是单位.

**证** 因为  $1 \cdot 1 = 1$ . ☞

**命题** 0 一定不是单位.

**证** 0 与任何整数的积都是 0, 不等于 1. ☞

**命题** 设  $f$  是单位. 若整数  $g, h$  适合  $fg = fh = 1$ , 则  $g = h$ .

**证** 因为整数的乘法是交换的、结合的, 故

$$g = g1 = g(fh) = (gf)h = (fg)h = 1h = h. \quad \text{☞}$$

**定义** 设  $f$  是单位. 上个命题指出,  $f$  的逆一定是唯一的 (根据单位的定义,  $f$  的逆当然存在). 我们用  $f^{-1}$  表示  $f$  的逆.

**命题** 设  $f$  是单位.  $f$  的逆  $f^{-1}$  也是单位, 且  $(f^{-1})^{-1} = f$ .

**证** 因为  $f$  是单位, 故存在整数  $f^{-1}$  使  $ff^{-1} = 1$ . 因为乘法可交换, 故  $f^{-1}f = 1$ . 所以对整数  $f^{-1}$  而言, 存在整数  $f$  使  $f^{-1}f = 1$ . 由单位的定义,  $f^{-1}$  是单位. 因为单位的逆唯一, 故  $f$  是  $f^{-1}$  的逆.  $\clubsuit$

**命题** 设  $f_1, f_2, \dots, f_n$  是单位. 则  $f_1f_2 \cdots f_n$  也是单位, 且

$$(f_1f_2 \cdots f_n)^{-1} = f_n^{-1} \cdots f_2^{-1}f_1^{-1}.$$

**证** 既然  $f_1, f_2, \dots, f_n$  是单位, 那么它们都有逆, 分别为  $f_1^{-1}, f_2^{-1}, \dots, f_n^{-1}$ . 所以

$$\begin{aligned} & (f_1f_2 \cdots f_{n-1}f_n)(f_n^{-1}f_{n-1}^{-1} \cdots f_2^{-1}f_1^{-1}) \\ &= (f_1f_2 \cdots f_{n-1})(f_nf_n^{-1})(f_{n-1}^{-1} \cdots f_2^{-1}f_1^{-1}) \\ &= (f_1f_2 \cdots f_{n-1})(1)(f_{n-1}^{-1} \cdots f_2^{-1}f_1^{-1}) \\ &= (f_1f_2 \cdots f_{n-1})(f_{n-1}^{-1} \cdots f_2^{-1}f_1^{-1}) \\ &= \dots\dots\dots \\ &= f_1f_1^{-1} \\ &= 1. \end{aligned}$$

所以,  $f_1f_2 \cdots f_n$  是单位. 因为单位的逆唯一, 故

$$(f_1f_2 \cdots f_n)^{-1} = f_n^{-1} \cdots f_2^{-1}f_1^{-1}. \quad \clubsuit$$

**定义** 整数的全体单位称为整数的单位群.

**命题** 整数的单位群恰由 1 与  $-1$  作成.

**证** 1 当然是单位. 因为  $(-1) \cdot (-1) = 1$ , 故  $-1$  也是单位.

设  $f$  是单位. 所以, 存在整数  $g$  使  $fg = 1$ . 我们证明:  $|f| = 1$ .

反证法. 若  $|f| > 1$ , 则  $|g| = \frac{1}{|f|} < 1$ . 因为  $g$  是整数, 故  $|g|$  是非负整数, 且  $|g| = 0$ . 所以,  $g = 0$ . 但  $f0 = 0 \neq 1$ , 矛盾! 若  $|f| < 1$ , 类似地, 有  $f = 0$ . 但  $0g = 0 \neq 1$ , 矛盾! 所以  $|f|$  一定是 1.

综上, 整数的单位恰有二个: 1 与  $-1$ .  $\clubsuit$

**定义** 设  $t$  是实数. 称最大的且不超过  $t$  的整数  $[t]$  为  $t$  的整数部分 (integer part);  $t - [t]$  为  $t$  的小数部分 (fractional part).

**例** 读者可能已经知道数学里有一个叫  $2\pi$  的数. 如果圆的半径为  $r$ , 则圆的周长是  $2\pi r$ , 圆的面积是  $\frac{1}{2} \cdot 2\pi r \cdot r$ . 由定义, 知

$$\lfloor 2\pi \rfloor = 6.$$

不过,

$$\lfloor -2\pi \rfloor = -7;$$

不仔细的读者很容易犯错哟.

**命题** 对任意实数  $t$ ,

$$0 \leq t - \lfloor t \rfloor < 1.$$

**证**  $0 \leq t - \lfloor t \rfloor$  是显然的:  $\lfloor t \rfloor$  被定义为最大的且“不超过” $t$  的整数. 另一半  $t - \lfloor t \rfloor < 1$  可以这么看: 既然  $\lfloor t \rfloor$  被定义为“最大的”且不超过  $t$  的整数, 那么

$$\lfloor t \rfloor + 1 > t.$$

这就是我们所需要的关系.



我们知道, 非负整数有这样的性质:

**命题** 设  $f$  是正整数,  $g$  是非负整数. 则必有一对非负整数  $q, r$  使

$$g = qf + r, \quad 0 \leq r < f.$$

例如, 取  $f = 5, g = 23$ . 不难看出,

$$23 = 4 \cdot 5 + 3.$$

现在, 我们看一看为什么上面的命题是正确的. 顺便一提, 我们可以抛弃一个假定:  $g \geq 0$ .

还是假定  $f$  是正整数.  $\frac{g}{f}$  是一个有理数, 当然也是实数. 所以

$$\frac{g}{f} = \underbrace{\left\lfloor \frac{g}{f} \right\rfloor}_q + \left( \frac{g}{f} - \left\lfloor \frac{g}{f} \right\rfloor \right).$$

二边同乘  $f$ , 有

$$g = f \cdot q + \underbrace{\left(g - f \left\lfloor \frac{g}{f} \right\rfloor\right)}_r.$$

显然  $q$  与  $r$  是整数. 注意到  $0 \leq \frac{r}{f} < 1$ , 所以  $0 \leq r < f$ .

换句话说, 我们证明了

**命题** 设  $f$  是正整数,  $g$  是整数. 则必有一对整数  $q, r$  使

$$g = qf + r, \quad 0 \leq r < f.$$

设  $f$  是负整数. 那么  $-f$  是正整数. 所以, 有一对整数  $q, r$  使

$$g = q(-f) + r, \quad 0 \leq r < -f.$$

也就是

$$g = (-q)f + r, \quad 0 \leq r < |f|,$$

综上, 我们证明了“整数的带余除法”:

**命题** 设  $f$  是非零整数,  $g$  是整数. 则必有一对整数  $q, r$  使

$$g = qf + r, \quad 0 \leq r < |f|.$$

还有一个小惊喜: 上述命题的  $q$  与  $r$  必定唯一. 设

$$\begin{aligned} q_1 f + r_1 &= q_2 f + r_2, \\ 0 \leq r_1 < |f|, \quad 0 \leq r_2 < |f|. \end{aligned}$$

这样

$$(q_1 - q_2)|f| = r_1 - r_2.$$

不难看出

$$0 - |f| < r_1 - r_2 < |f| + 0,$$

即

$$|r_1 - r_2| < |f|.$$

从而

$$|q_1 - q_2| = \frac{|r_1 - r_2|}{|f|} < \frac{|f|}{|f|} = 1.$$

因为  $|q_1 - q_2|$  是整数, 故

$$|q_1 - q_2| = 0 \implies q_1 = q_2.$$

进而

$$|r_1 - r_2| = |q_1 - q_2||f| = 0 \implies r_1 = r_2.$$

请读者休息一会儿.

读者或许还记得“因子”与“公因子”的概念.

**定义** 设  $f, g$  是整数. 若存在整数  $h$  使  $f = gh$ , 则说  $g$  是  $f$  的因子 (factor).

**评注** 或许, 读者更熟悉“因数”, 而不是“因子”. 毕竟, 在小学, 我们就已经接触了“因数”. 之后我们还会利用多项式的带余除法作类似的讨论, 所以作者特地选用了更一般的词.

**例** (i) 单位是任意整数的因子; 单位的因子一定是单位.

(ii) 任意整数都是 0 的因子; 非零整数的因子一定不是 0.

**命题** 设  $f, g, h$  是整数. 因子适合如下性质:

(i)  $f$  是  $f$  的因子;

(ii) 若  $h$  是  $g$  的因子, 且  $g$  是  $f$  的因子, 则  $h$  是  $f$  的因子;

(iii) 若  $f$  是  $g$  的因子, 且  $g$  是  $f$  的因子, 则存在单位  $q$  使  $f = qg$ ;

(iv) 设  $k, \ell$  是整数. 若  $h$  是  $f$  的因子, 且  $h$  是  $g$  的因子, 则  $h$  是  $kf \pm \ell g$  的因子;

(v) 若  $\varepsilon_1, \varepsilon_2$  是单位, 且  $g$  是  $f$  的因子, 则  $\varepsilon_2 g$  是  $\varepsilon_1 f$  的因子.

**证** (i) 注意到  $f = 1f$ , 其中 1 是单位.

(ii) 因为  $h$  是  $g$  的因子, 故存在整数  $p$  使  $g = ph$ . 因为  $g$  是  $f$  的因子, 故存在整数  $q$  使  $f = qg$ . 所以

$$f = qg = q(ph) = (qp)h.$$

因为  $qp$  也是整数, 故  $h$  是  $f$  的因子.

(iii) 若  $f = 0$ , 则  $g = 0$ , 当然有  $f = 1g = 0$ , 其中 1 是单位. 下设  $f \neq 0$ .

因为  $f$  是  $g$  的因子, 故存在整数  $p$  使  $g = pf$ ; 因为  $g$  是  $f$  的因子, 故存在整数  $q$  使  $f = qg$ . 所以

$$f = qg = q(pf) = (qp)f.$$

因为  $f \neq 0$ , 故可从等式二边消去  $f$ , 即

$$1 = qp.$$

由此可知  $q$  是单位.

(iv) 因为  $h$  是  $f$  的因子, 且  $h$  是  $g$  的因子, 故存在整数  $p, q$  使  $f = ph$  且  $g = qh$ . 所以

$$kf \pm \ell g = k(ph) \pm \ell(qh) = (kp)h \pm (\ell q)h = (kp \pm \ell q)h.$$

(v) 若存在整数  $q$  使  $f = gq$ , 则

$$\varepsilon_1 f = g(\varepsilon_1 q) = g(\varepsilon_2 \varepsilon_2^{-1})(\varepsilon_1 q) = (g\varepsilon_2)(\varepsilon_2^{-1} \varepsilon_1 q).$$

因为单位的逆是整数, 且 (有限多个) 整数的积是整数, 故  $\varepsilon_2^{-1} \varepsilon_1 q$  是整数. 从而  $\varepsilon_2 g$  是  $\varepsilon_1 f$  的因子. ✎

为方便, 我们定义一个新词.

**定义** 设  $f, g$  是整数. 若存在单位  $\varepsilon$  使  $f = \varepsilon g$ , 则说  $f$  是  $g$  的相伴 (*associate*). 因为

$$g = 1g = (\varepsilon^{-1}\varepsilon)g = \varepsilon^{-1}(\varepsilon g) = \varepsilon^{-1}f,$$

故  $g$  当然也是  $f$  的相伴. 所以, 我们说  $f$  与  $g$  相伴 (*to be associate*).

显然, 因为  $f = 1f$ , 故  $f$  与  $f$  相伴. 上面的文字已经说明  $f$  与  $g$  相伴相当于  $g$  与  $f$  相伴. 我们还有下面的

**命题** 设  $f, g, h$  是整数. 若  $f$  与  $g$  相伴, 且  $g$  与  $h$  相伴, 则  $f$  与  $h$  相伴.

**证** 因为  $f$  与  $g$  相伴, 故存在单位  $\varepsilon_1$  使  $f = \varepsilon_1 g$ . 因为  $g$  与  $h$  相伴, 故存在单位  $\varepsilon_2$  使  $g = \varepsilon_2 h$ . 所以

$$f = \varepsilon_1 g = \varepsilon_1(\varepsilon_2 h) = (\varepsilon_1 \varepsilon_2)h.$$

因为  $\varepsilon_1 \varepsilon_2$  是单位, 故  $f$  与  $h$  相伴. ✎

根据 (iii), 我们有

**命题** 设  $f, g$  是整数.  $f$  与  $g$  相伴的一个必要与充分条件是  $f$  是  $g$  的因子, 且  $g$  是  $f$  的因子.

**定义** 设  $f, g$  是整数. 若  $d$  是  $f$  的因子, 且  $d$  是  $g$  的因子, 则  $d$  是  $f$  与  $g$  的公因子 (*common factor*).

**评注** 若  $d$  是  $f$  与  $g$  的公因子, 则  $d$  当然也是  $g$  与  $f$  的公因子. 换句话说, 公因子与次序无关.

**例** 单位是任意二个整数的公因子.

现在我们引出“最大公因子”的概念.

**定义** 设  $f, g$  是整数. 适合下述二性质的整数  $d$  是  $f$  与  $g$  的最大公因子 (*greatest common factor*):

- (i)  $d$  是  $f$  与  $g$  的公因子;
- (ii) 若  $e$  是  $f$  与  $g$  的公因子, 则  $e$  是  $d$  的因子.

**评注** 若  $d$  是  $f$  与  $g$  的最大公因子, 则  $d$  当然也是  $g$  与  $f$  的最大公因子. 换句话说, 最大公因子与次序无关. 这是因为公因子与次序无关.

**评注** 或许, 读者更熟悉这句话 (小学里学到的定义): “设  $f, g$  是二个整数.  $f$  与  $g$  的公因数的最大者是  $f$  与  $g$  的最大公因数.”



由定义立即可得

**命题** 设  $f, g$  是整数. 若  $d_1$  与  $d_2$  都是  $f$  与  $g$  的最大公因子, 则  $d_1$  与  $d_2$  相伴.

**证** 因为  $d_1$  是  $d_2$  的因子, 且  $d_2$  也是  $d_1$  的因子. ✎

**评注** 由此可见, 最大公因子不一定是唯一的. 但这不是很重要.

**例** 不难看出,  $d = f$  是 0 与  $f$  的最大公因子: (i)  $d$  是 0 的因子, 且  $d$  是  $f$  的因子; (ii) 若  $e$  是 0 与  $f$  的公因子, 则  $e$  当然是  $d$  (即  $f$ ) 的因子.

**例** 设  $\varepsilon$  是单位. 不难看出,  $d = \varepsilon$  是  $\varepsilon$  与  $f$  的最大公因子: (i)  $d$  是  $\varepsilon$  的因子, 且  $d$  是  $f$  的因子; (ii) 若  $e$  是  $\varepsilon$  与  $f$  的公因子, 则  $e$  当然是  $d$  (即  $\varepsilon$ ) 的因子.

**命题** 设  $f, g, q$  是整数. 设  $f$  与  $g$  的最大公因子是  $d_1$ ; 设  $f - gq$  与  $g$  的最大公因子是  $d_2$ . 则  $d_1$  与  $d_2$  相伴.

**证** 因为  $d_1$  是  $f$  与  $g$  的公因子, 故  $d_1$  是  $1 \cdot f - q \cdot g$  的因子. 这说明,  $d_1$  是  $f - gq$  与  $g$  的公因子. 因为  $d_2$  是  $f - gq$  与  $g$  的最大公因子, 故  $d_1$  是  $d_2$  的因子.

因为  $d_2$  是  $f - gq$  与  $g$  的公因子, 故  $d_2$  是  $1 \cdot (f - gq) + q \cdot g$  的因子. 这说明,  $d_2$  是  $f$  与  $g$  的公因子. 因为  $d_1$  是  $f$  与  $g$  的最大公因子, 故  $d_2$  是  $d_1$  的因子.

综上,  $d_1$  与  $d_2$  相伴. ✎

我们现在可以证明

**命题** 设  $f, g$  是整数.  $f$  与  $g$  的最大公因子一定存在.

**证** 不妨假定  $g$  不是 0. 所以, 根据带余除法, 有

$$f = gq_0 + r_0, \quad 0 \leq r_0 < |g|.$$

根据上一个命题,  $r_0$  与  $g$  的最大公因子是  $f$  与  $g$  的最大公因子. 若  $r_0 = 0$ , 则  $g$  就是 0 与  $g$  (从而也是  $f$  与  $g$ ) 的最大公因子. 若  $r_0 \neq 0$ , 则

$$g = r_0q_1 + r_1, \quad 0 \leq r_1 < r_0.$$

根据上一个命题,  $r_1$  与  $r_0$  的最大公因子是  $r_0$  与  $g$  的最大公因子, 所以也是  $f$  与  $g$  的最大公因子. 若  $r_1 = 0$ , 则  $r_0$  就是 0 与  $r_0$  (从而也是  $f$  与  $g$ ) 的最大公因子. 若  $r_1 \neq 0$ , 则

$$r_0 = r_1 q_2 + r_2, \quad 0 \leq r_2 < r_1.$$

这个过程必定会在有限多步后停止. 反证法. 如果此过程可一直进行下去, 则我们可得到无限多个正整数  $r_0, r_1, \dots$  使

$$|g| > r_0 > r_1 > \dots > r_k > r_{k+1} > \dots.$$

可是, 不存在无限递降的正整数列 (低于  $|g|$  的正整数至多有  $|g| - 1$  个), 矛盾!

为方便, 分别称  $f$  与  $g$  为  $r_{-2}$  与  $r_{-1}$ . 根据上面的讨论, 一定存在整数  $n$  使

$$r_{\ell-2} = r_{\ell-1} q_\ell + r_\ell, \quad 0 < r_\ell < |r_{\ell-1}|, \quad \ell = 0, 1, \dots, n-2;$$

$$r_{n-3} = r_{n-2} q_{n-1}.$$

$r_{n-2}$  是 0 与  $r_{n-2}$  的最大公因子, 也是  $r_{n-2}$  与  $r_{n-3}$  的最大公因子, 也是  $r_{n-3}$  与  $r_{n-4}$  的最大公因子……也是  $r_{-2}$  与  $r_{-1}$  的最大公因子. 所以,  $r_{n-2}$  是  $f$  与  $g$  的最大公因子. ✎

这个命题的证明过程事实上也给出了一个计算二个整数的最大公因子的算法 (“辗转相除法”).

**例** 设  $f = 2116, g = 667$ . 我们来找一个  $f$  与  $g$  的最大公因子. 不难作出如下计算:

$$2116 = 667 \cdot 3 + 115,$$

$$667 = 115 \cdot 5 + 92,$$

$$115 = 92 \cdot 1 + 23,$$

$$92 = 23 \cdot 4.$$

所以, 23 是 92 与 115 的最大公因子, 是 115 与 667 的最大公因子, 是 667 与 2116 的最大公因子.

当然, 读者不难说明,  $-23$  是另一个最大公因子.  $\pm 23$  是  $f$  与  $g$  唯一的最大公因子.

根据上面的计算, 我们有

$$1 \cdot 115 + (-1) \cdot 92 = 23.$$

又因为

$$92 = 1 \cdot 667 + (-5) \cdot 115,$$

故

$$1 \cdot 115 + (-1 \cdot 1) \cdot 667 + (-1 \cdot (-5)) \cdot 115 = 23,$$

即

$$6 \cdot 115 + (-1) \cdot 667 = 23.$$

又因为

$$115 = 1 \cdot 2116 + (-3) \cdot 667,$$

故

$$(6 \cdot 1) \cdot 2116 + (6 \cdot (-3)) \cdot 667 + (-1) \cdot 667 = 23,$$

即

$$6 \cdot 2116 + (-19) \cdot 667 = 23.$$

一般地, 我们有

**命题** 设  $f, g$  是整数. 设  $d$  是  $f$  与  $g$  的最大公因子. 存在整数  $s$  与  $t$  使

$$sf + tg = d.$$

这个等式的一个名字是 Bézout 等式 (*Bézout's identity*).

**证** 若  $f = g = 0$ , 则可取  $s = t = 0$ . 下设  $g \neq 0$ .

为方便, 分别称  $f$  与  $g$  为  $r_{-2}$  与  $r_{-1}$ . 设存在整数  $n$  使

$$r_{\ell-2} = r_{\ell-1}q_{\ell} + r_{\ell}, \quad 0 < r_{\ell} < |r_{\ell-1}|, \quad \ell = 0, 1, \dots, n-2;$$

$$r_{n-3} = r_{n-2}q_{n-1}.$$

为方便, 记

$$r_{\ell} = 0, \quad \ell \geq n-1.$$

我们用数学归纳法证明辅助命题  $P(\ell)$ : 任取非负整数  $\ell$ , 必有二整数  $s, t$  使

$$r_{\ell} = sf + tg.$$

$r_0$  可写为

$$r_0 = 1r_{\ell-2} + (-q_0)r_{\ell} = 1f + (-q_0)g.$$

$r_1$  可写为

$$r_1 = 1r_{-1} + (-q_1)r_0 = (-q_1)f + (1 + q_0q_1)g.$$

所以  $P(0)$  与  $P(1)$  正确. 假定  $P(0), P(1), \dots, P(k-1)$  正确. 我们的目标是: 推出  $P(k)$  正确. 若  $k \geq n-1$ , 则

$$r_k = 0 = 0f + 0g.$$

若  $k \leq n-2$ , 则根据归纳假设, 存在整数  $u, v, z, w$  使

$$r_{k-2} = uf + vg, \quad r_{k-1} = zf + wg.$$

所以

$$r_k = r_{k-2} - r_{k-1}q_k = (u - zq_k)f + (v - wq_k)g.$$

因为  $u - zq_k$  与  $v - wq_k$  均为整数, 故  $P(k)$  正确.

所以, 存在整数  $s, t$  使

$$sf + tg = r_{n-2}.$$

因为  $r_{n-2}$  与  $d$  都是  $f$  与  $g$  的最大公因子, 故  $d = \varepsilon r_{n-2}$ , 其中  $\varepsilon$  是单位. 所以

$$(\varepsilon s)f + (\varepsilon t)g = d. \quad \text{☞}$$

有了最大公因子的概念, 我们可以引出“互素”:

**定义** 设  $f, g$  是整数. 若单位是  $f$  与  $g$  的最大公因子, 则称  $f$  与  $g$  互素 (*to be relatively prime*).

**评注** 因为最大公因子与次序无关, 故互素也与次序无关. 换句话说, “ $f$  与  $g$  互素” 相当于 “ $g$  与  $f$  互素”.

**例** 显然, 单位与任意整数都互素.

下面给出一个极重要的命题:

**命题** 设  $f, g$  是整数.  $f$  与  $g$  互素的一个必要与充分条件是: 存在整数  $s, t$  使

$$sf + tg = 1.$$

**证** 先看必要性. 显然; 这是 Bézout 等式的结果.

再看充分性. 设  $d$  是  $f$  与  $g$  的最大公因子. 因为  $sf + tg = 1$ , 故  $d$  是 1 的因子. 这样,  $d$  一定是单位. ☞

下面是几个关于互素的性质.

**命题** 设  $f, g, h$  是整数. 互素有如下性质:

- (i) 若  $h$  是  $fg$  的因子, 且  $h$  与  $f$  互素, 则  $h$  是  $g$  的因子;
- (ii) 若  $f$  与  $g$  互素, 且  $f$  与  $h$  互素, 则  $f$  与  $gh$  互素;
- (iii) 若  $f$  是  $h$  的因子,  $g$  是  $h$  的因子, 且  $f$  与  $g$  互素, 则  $fg$  是  $h$  的因子.

证 (i) 因为  $h$  与  $f$  互素, 故存在整数  $s$  与  $t$  使

$$sh + tf = 1.$$

所以

$$(gs)h + t(fg) = g.$$

因为  $h$  是  $h$  的因子, 且  $h$  是  $fg$  的因子, 故  $h$  是  $g = (gs)h + t(fg)$  的因子.

(ii) 因为  $f$  与  $g$  互素, 故存在整数  $u, v$  使

$$uf + vg = 1.$$

因为  $f$  与  $h$  互素, 故存在整数  $s, t$  使

$$sf + th = 1.$$

从而

$$1 = (uf + vg)(sf + th) = (ufs + uth + vgs)f + (vt)(gh).$$

所以  $f$  与  $gh$  互素.

(iii) 因为  $f$  是  $h$  的因子, 故存在整数  $p$  使  $h = fp$ . 因为  $g$  是  $h = fp$  的因子, 且  $f$  与  $g$  互素, 故由 (i) 知  $g$  是  $p$  的因子. 设  $p = gq$ . 这样

$$h = fp = f(gq) = (fg)q,$$

故  $fg$  是  $h$  的因子. ✎

感谢您的阅读. 请休息一会儿.

现在我们推广公因子、最大公因子、互素的概念.

前面, 我们讨论了二个整数的公因子、最大公因子、互素; 现在, 我们从量的角度推广.

**定义** 设  $f_1, f_2, \dots, f_n$  是整数. 若  $d$  是  $f_1$  的因子,  $d$  是  $f_2$  的因子……  
 $d$  是  $f_n$  的因子, 则  $d$  是  $f_1, f_2, \dots, f_n$  的公因子.

**评注** 我们并没有禁止  $n$  取 1: 一个整数的“公因子”当然是它的因子. 同理, 一个整数也可以有“最大公因子”; 一个整数也可以“互素”.

作为练习, 请读者证明

**命题** 设  $k_1, k_2, \dots, k_n, f_1, f_2, \dots, f_n$  是整数. 若  $d$  是  $f_1, f_2, \dots, f_n$  的公因子, 则  $d$  是  $k_1 f_1 + k_2 f_2 + \dots + k_n f_n$  的因子.

**定义** 设  $f_1, f_2, \dots, f_n$  是整数. 适合下述二性质的整数  $d$  是  $f_1, f_2, \dots, f_n$  的最大公因子:

- (i)  $d$  是  $f_1, f_2, \dots, f_n$  的公因子;
- (ii) 若  $e$  是  $d$  是  $f_1, f_2, \dots, f_n$  的公因子, 则  $e$  是  $d$  的因子.

由定义立即可得

**命题** 设  $f_1, f_2, \dots, f_n$  是整数. 若  $d_1$  与  $d_2$  都是  $f_1, f_2, \dots, f_n$  的最大公因子, 则  $d_1$  与  $d_2$  相伴.

**证** 因为  $d_1$  是  $d_2$  的因子, 且  $d_2$  也是  $d_1$  的因子. ✎

**命题** 设  $f_1, f_2, \dots, f_n$  是整数.

- (i)  $f_1, f_2, \dots, f_n$  的最大公因子存在;
- (ii) 若  $d$  是  $f_1, f_2, \dots, f_n$  的最大公因子, 则存在整数  $u_1, u_2, \dots, u_n$  使

$$u_1 f_1 + u_2 f_2 + \dots + u_n f_n = d.$$

**证** (i) 对  $n$  用数学归纳法. 显然,  $n = 1$  或  $n = 2$  时, 命题成立. 设  $n = k$  ( $k \geq 2$ ) 时命题成立, 即:  $f_1, f_2, \dots, f_k$  的最大公因子存在.

今看  $n = k + 1$  时的情形. 令  $d_k$  为  $f_1, f_2, \dots, f_k$  的最大公因子. 令  $d$  为  $d_k$  与  $f_{k+1}$  的最大公因子. 我们证明:  $d$  是  $f_1, f_2, \dots, f_k, f_{k+1}$  的最大公因子.

首先,  $d$  是  $f_1, f_2, \dots, f_k, f_{k+1}$  的公因子.  $d$  当然是  $f_{k+1}$  的因子. 任取某个 1 至  $k$  间的  $\ell$ . 因为  $d$  是  $d_k$  的因子, 而  $d_k$  是  $f_\ell$  的因子, 故  $d$  是  $f_\ell$  的因子. 这样,  $d$  确为  $f_1, f_2, \dots, f_k, f_{k+1}$  的公因子.

其次, 若  $e$  是  $f_1, f_2, \dots, f_k, f_{k+1}$  的公因子, 则  $e$  当然是  $f_1, f_2, \dots, f_k$  的公因子, 故  $e$  是  $d_k$  的因子. 又因为  $e$  是  $f_{k+1}$  的因子, 则  $e$  是  $d_k$  与  $f_{k+1}$  的公因子. 这样,  $e$  是  $d$  的因子.

根据最大公因子的定义,  $d$  一定是  $f_1, f_2, \dots, f_k, f_{k+1}$  的最大公因子. 所以,  $n = k + 1$  时, (i) 正确.

(ii) 对  $n$  用数学归纳法. 显然,  $n = 1$  或  $n = 2$  时, 命题成立. 设  $n = k$  ( $k \geq 2$ ) 时命题成立, 即: 若  $d_k$  是  $f_1, f_2, \dots, f_k$  的最大公因子, 则存在整数  $u_1, u_2, \dots, u_k$  使

$$u_1 f_1 + u_2 f_2 + \dots + u_k f_k = d_k.$$

今看  $n = k + 1$  时的情形. 令  $d$  为  $d_k$  与  $f_{k+1}$  的最大公因子. 由 (i) 知,  $d$  是  $f_1, f_2, \dots, f_k, f_{k+1}$  的最大公因子. 由 Bézout 等式知, 存在整数  $u, u_{k+1}$  使

$$u d_k + u_{k+1} f_{k+1} = d.$$

根据归纳假设, 存在整数  $v_1, v_2, \dots, v_k$  使

$$v_1 f_1 + v_2 f_2 + \dots + v_k f_k = d_k.$$

这样

$$(uv_1)f_1 + (uv_2)f_2 + \dots + (uv_k)f_k + u_{k+1}f_{k+1} = d.$$

所以,  $n = k + 1$  时, (ii) 正确. ✎

跟之前一样, 有了最大公因子的概念, 我们可以引出“互素”:

**定义** 设  $f_1, f_2, \dots, f_n$  是整数. 若单位是  $f_1, f_2, \dots, f_n$  的最大公因子, 则称  $f_1, f_2, \dots, f_n$  互素.

下面的命题也是十分自然的.

**命题** 设  $f_1, f_2, \dots, f_n$  是整数.  $f_1, f_2, \dots, f_n$  互素的一个必要与充分条件是: 存在整数  $u_1, u_2, \dots, u_n$  使

$$u_1 f_1 + u_2 f_2 + \dots + u_n f_n = 1.$$

**证** 先看必要性. 显然; 这是上个命题的结果.

再看充分性. 设  $d$  是  $f_1, f_2, \dots, f_n$  的最大公因子. 因为  $u_1 f_1 + u_2 f_2 + \dots + u_n f_n = 1$ , 故  $d$  是 1 的因子. 这样,  $d$  一定是单位. ✎



**命题** 设  $f_1, f_2, \dots, f_n, f$  是整数. 若  $f_1$  与  $f$  互素,  $f_2$  与  $f$  互素…… $f_n$  与  $f$  互素, 则  $f_1 f_2 \cdots f_n$  与  $f$  互素.

**证** 用数学归纳法.  $n = 1$  时, 显然. 设  $f_1 f_2 \cdots f_{n-1}$  与  $f$  互素. 因为  $f_n$  与  $f$  互素, 故  $f_1 f_2 \cdots f_{n-1} \cdot f_n$  与  $f$  互素.  $\clubsuit$

**命题** 设整数  $f_1, f_2, \dots, f_n$  不全是零.

- (i)  $f_1, f_2, \dots, f_n$  的最大公因子  $d$  不是零;
- (ii) 任取 1 至  $n$  间的整数  $\ell$ , 必有 (唯一的) 整数  $g_\ell$  使  $f_\ell = dg_\ell$ ;
- (iii) 单位是  $g_1, g_2, \dots, g_n$  的最大公因子; 换句话说,  $g_1, g_2, \dots, g_n$  互素;
- (iv) 反过来, 若整数  $u_1, u_2, \dots, u_n$  互素, 则  $w$  是  $wu_1, wu_2, \dots, wu_n$  的最大公因子.

**证** (i) 零一定不是非零整数的因子, 故零不是  $f_1, f_2, \dots, f_n$  的公因子, 当然也不是最大公因子.

(ii) 既然  $d$  是最大公因子, 当然也是公因子. 对  $f_\ell$  而言, 由因子的定义, 知: 存在整数  $g_\ell$  使  $f_\ell = dg_\ell$ . 现在看唯一性. 假定  $f_\ell = dg_\ell = dg'_\ell$ . 因为  $d \neq 0$ , 故可从等式二边消去  $d$ , 即  $g_\ell = g'_\ell$ .

(iii) 设  $g_1, g_2, \dots, g_n$  的最大公因子是  $\delta$ . 这样, 由 (ii), 知: 对任意  $g_\ell$ , 有整数  $h_\ell$  使  $g_\ell = \delta h_\ell$ . 所以

$$f_\ell = dg_\ell = d(\delta h_\ell) = (d\delta)h_\ell.$$

所以  $d\delta$  是  $f_1, f_2, \dots, f_n$  的公因子. 所以  $d\delta$  是  $d$  的因子.  $d$  显然是  $d\delta$  的因子, 故  $d\delta = \varepsilon d$ , 其中  $\varepsilon$  是单位. 因为  $d \neq 0$ , 故可从等式二边消去  $d$ , 即  $\delta = \varepsilon$ .

(iv) 若  $w = 0$ , 命题显然成立:  $0, 0, \dots, 0$  的最大公因子当然是  $0$ . 下设  $w \neq 0$ .

$w$  显然是  $wu_1, wu_2, \dots, wu_n$  的公因子. 设  $ws$  是  $wu_1, wu_2, \dots, wu_n$  的最大公因子, 这里  $s$  是某个整数. 由 (ii), 对每个  $wu_\ell$ , 都有整数  $q_\ell$  使  $wu_\ell = wsq_\ell$ . 因为  $w \neq 0$ , 故可从等式二边消去  $w$ , 即  $u_\ell = sq_\ell$ . 这样,  $s$  是  $u_1, u_2, \dots, u_n$  的公因子, 故  $s$  是单位的因子, 即  $s$  是单位. 所以  $w$  是  $wu_1, wu_2, \dots, wu_n$  的最大公因子.  $\clubsuit$

**例** 读者可能还记得, 有理数是全体形如  $\frac{p}{q}$  的数, 其中  $p, q$  为整数, 且  $q \neq 0$ . 我们说, 每一个有理数都可以写为  $\frac{m}{n}$ , 其中  $m$  为整数,  $n$  为正整数, 且  $m$  与  $n$  互素. 通俗地说, 就是“每个分数<sup>†</sup>都可以约分为最简分数”. 有了上面的整数知识, 我们可以解释为什么.

任取有理数  $\frac{P}{Q}$ . 若  $Q < 0$ , 则令  $q = -Q, p = -P$ ; 若  $Q > 0$ , 则令  $q = Q, p = P$ . 所以

$$\frac{P}{Q} = \frac{p}{q}, \quad q > 0.$$

既然  $q \neq 0$ , 那么  $p$  与  $q$  的最大公因子不是零. 令  $d$  是正的最大公因子. 这样, 必有 (唯一的) 整数  $m, n$  使  $p = dm, q = dn$ . 所以

$$\frac{p}{q} = \frac{dm}{dn} = \frac{m}{n}.$$

因为  $q > 0, d > 0$ , 故  $n > 0$ . 根据上个命题,  $m$  与  $n$  互素.

这是一个相当常见的事实.

互素的一个特殊情形是 PRP.

**定义** 设  $f_1, f_2, \dots, f_n$  是整数 ( $n \geq 2$ ). 若任取 1 至  $n$  间的二个不同的整数  $i, j$ , 都有  $f_i$  与  $f_j$  互素, 则  $f_1, f_2, \dots, f_n$  PRP<sup>‡</sup> (*to be pairwise relatively prime*).

为方便, 若  $f$  是单位, 我们也说 “ $f$  PRP” (这相当于定义了  $n = 1$  时 PRP 的意义).

**例** 设  $f_1 = 2, f_2 = 3, f_3 = 5$ . 因为  $f_1$  与  $f_2$  互素,  $f_2$  与  $f_3$  互素,  $f_3$  与  $f_1$  互素, 故  $f_1, f_2, f_3$  PRP. 读者不难发现:  $f_1, f_2, f_3$  互素.

一般地, 我们有

**命题** 设整数  $f_1, f_2, \dots, f_n$  PRP. 则  $f_1, f_2, \dots, f_n$  互素.

<sup>†</sup>有理数也叫分数.

<sup>‡</sup>因为作者的汉语不是很好, 所以作者用英语缩写表示这个概念. 作为参考, 作者用英语定义 PRP: A list of integers  $p_1, p_2, \dots, p_n$  is said to be *pairwise relatively prime* if  $p_i$  and  $p_j$  are relatively prime for any two distinct integers  $i, j$  in  $\{1, 2, \dots, n\}$ .

**证** 用数学归纳法.  $n = 1$  时,  $f_1$  是单位, 故  $f_1$  “互素”.  $n = 2$  时,  $f_1$  与  $f_2$  PRP 相当于  $f_1$  与  $f_2$  互素.

设  $n = s$  时命题成立. 考虑  $n = s + 1$  的情形.

既然  $f_1, f_2, \dots, f_s, f_{s+1}$  PRP, 那么 “暂时地不考虑  $f_{s+1}$ ”, 可知  $f_1, f_2, \dots, f_s$  PRP. 所以, 单位  $\varepsilon$  是  $f_1, f_2, \dots, f_s$  的最大公因子 (归纳假设). 设  $d$  是  $f_1, f_2, \dots, f_s, f_{s+1}$  的最大公因子.  $d$  当然是  $f_1, f_2, \dots, f_s$  的公因子. 所以  $d$  是  $\varepsilon$  的因子. 故  $d$  也是单位.

所以,  $n = s + 1$  时, 命题也成立. ✎

不过反过来就不一定了.

**例** 设  $g_1 = 1, g_2 = 2, g_3 = 4$ . 显然,  $g_1, g_2, g_3$  互素. 可是, 2 是  $g_2$  与  $g_3$  的最大公因子. 所以,  $g_1, g_2, g_3$  不 PRP.

**命题** 设整数  $f_1, f_2, \dots, f_n$  PRP. 设  $m_1, m_2, \dots, m_n$  是非负整数. 记  $F_i = f_i^{m_i}, i$  是 1 至  $n$  间的整数. 则  $F_1, F_2, \dots, F_n$  也 PRP.

**证** 根据 PRP 的定义, 我们只需证: 若  $f$  与  $g$  互素, 且  $s, t$  是非负整数, 则  $f^s$  与  $g^t$  互素.

若  $s = 0$  或  $t = 0$ , 因为 1 与任意整数都互素, 故此时显然. 下设  $s \geq 1$  且  $t \geq 1$ .

我们先证:  $f^s$  与  $g$  互素. 因为  $f$  与  $g$  互素,  $f$  与  $g$  互素…… $f$  与  $g$  互素 ( $s$  个 “ $f$  与  $g$  互素”), 故  $f^s = \underbrace{f \cdot f \cdots f}_{s \text{ 个 } f}$  与  $g$  互素.

暂时记  $F = f^s$ . 因为  $F$  与  $g$  互素, 故 (照搬上段的推理)  $F$  与  $g^t$  互素. ✎

**命题** 设整数  $f_1, f_2, \dots, f_n$  PRP. 则  $f_1 f_2 \cdots f_{i-1}$  与  $f_i$  互素 ( $i$  是 1, 2,  $\dots, n$  中的数). 我们约定: 0 个整数的和为 0, 而 0 个整数的积为 1. 所以,  $i = 1$  时, 1 当然与  $f_1$  互素.

**证**  $i = 1$  时, 显然. 设  $i \geq 2$ . 因为  $f_1$  与  $f_i$  互素,  $f_2$  与  $f_i$  互素…… $f_{i-1}$  与  $f_i$  互素, 故  $f_1 \cdot f_2 \cdots f_{i-1}$  与  $f_i$  互素. ✎

**评注** 设六整数  $f_1, f_2, \dots, f_6$  PRP. 作者问:  $f_1 f_4 f_6$  与  $f_3$  互素吗? 当然了. 为什么呢?

既然  $f_1, f_2, \dots, f_6$  PRP, 那么  $f_1, f_4, f_6, f_3, f_2, f_5$  也 PRP, 对不对? 令  $g_1 = f_1, g_2 = f_4, g_3 = f_6, g_4 = f_3, g_5 = f_2, g_6 = f_5$ , 则  $g_1, g_2, \dots, g_6$  PRP. 所以, 根据刚证过的命题,  $g_1 g_2 g_3$  与  $g_4$  互素. 因为  $g_1 g_2 g_3 = f_1 f_4 f_6, g_4 = f_3$ , 故  $f_1 f_4 f_6$  与  $f_3$  互素.

本评注的目的是告诉读者, 不要死学作者所讲述的知识. 读者要灵活运用所学的知识, 并逐渐适应“显然”“当然”等词语. 的确, 作者可以写得更详细, 但这没有必要. “学而不思则罔, 思而不学则殆.” 读者一定要边学边想! 还有, 如果读者真地想学作者讲述的知识, 作者建议读者不要狼吞虎咽. 相信作者; 作者不会害读者的!

**命题** 设整数  $f_1, f_2, \dots, f_n$  PRP. 若  $f_1, f_2, \dots, f_i$  都是  $f$  的因子, 则  $f_1 f_2 \dots f_i$  也是  $f$  的因子 ( $i$  是  $1, 2, \dots, n$  中的数). 特别地,  $i = n$  时,  $f_1 f_2 \dots f_n$  是  $f$  的因子.

**证** 用数学归纳法.  $i = 1$  时, 显然. 设  $f_1 f_2 \dots f_{i-1}$  是  $f$  的因子 (归纳假设). 因为  $f_i$  也是  $f$  的因子, 且  $f_1 f_2 \dots f_{i-1}$  与  $f_i$  互素, 故  $f_1 f_2 \dots f_{i-1} \cdot f_i$  也是  $f$  的因子. ✎

**评注** 其实读者在小学或中学一定见过 (甚至用过) 本文的很多命题, 所以这些命题是自然的 (不凸兀的). 本文的目的有:

- (i) 总结与“查考多项式” (原作) 相关的整数性质. 同人作还会讨论原作未讨论的多项式理论, 而部分内容要求读者了解整数的稍深的知识.
- (ii) 相对系统地为读者展示初等数论初步 (的初步) 理论. 本文相对独立; 或者说, 读者就算没读原作, 也可以只读“整数的一些性质”.
- (iii) 杀作者的时间. 这是最重要的点; 或者说, 上面二点都是胡扯. 请读者休息一下. 等会儿还有一点东西呢.

现在, 我们讨论不可约的整数.

**定义** 设整数  $f$  既不是 0, 也不是单位.

- (i) 若存在二个不全为单位的整数  $f_1, f_2$  使  $f = f_1 f_2$ , 则  $f$  是可约的 (reducible).

(ii) 若  $f$  不是可约的, 则说  $f$  是不可约的 (*irreducible*). 换言之, 若  $f$  是不可约的, 则“整数  $f_1, f_2$  使  $f = f_1 f_2$ ”可推出“ $f_1$  是单位或  $f_2$  是单位”.

**评注** 或许, 读者还能记起素数<sup>†</sup> (*prime number*) 的定义:

设整数  $f > 1$ . 若“正整数  $f_1, f_2$  使  $f = f_1 f_2$ ”可推出“ $f_1 = 1$  或  $f_2 = 1$ ”, 则  $f$  是素数.

作者当然可以不用“不可约的整数”; 但是, 为了让读者更好地体会到整数与多项式的相似的地方, 作者还是使用了一般的词.

**评注** 0 或单位既不是可约的, 也不是不可约的.

**例** 2 是不可约的.

设整数  $f_1, f_2$  适合  $f_1 f_2 = 2$ . 所以,  $|f_1| |f_2| = 2$ .

设  $|f_1| \leq |f_2|$ . 这样, 由  $|f_1|^2 \leq |f_1| |f_2| = 2$  知  $|f_1| \leq 1$ ; 由  $|f_2|^2 \geq |f_1| |f_2| = 2$  知  $|f_2| \geq 2$ .  $f_1$  当然不为零, 故  $|f_1|$  一定是 1. 所以  $f_1 = \pm 1$ .


若设  $|f_1| > |f_2|$ , 可得  $|f_1|^2 > 2$ , 且  $|f_2|^2 < 2$ . 这样, 因为  $f_2$  不为零, 有  $|f_2| = 1$ . 所以  $f_2 = \pm 1$ .

不管怎么样, 我们已经证明了“整数  $f_1, f_2$  使  $2 = f_1 f_2$ ”可推出“ $f_1$  是单位或  $f_2$  是单位”. 这样, 2 是不可约的.

类似地, 读者可 (几乎完全一样地) 证明: 3 是不可约的.

**例** 6 是可约的:  $6 = 2 \cdot 3$ , 而 2 不是单位, 3 也不是单位.

**命题** 设整数  $p$  既不是 0, 也不是单位. 设  $\varepsilon$  是单位. 若  $p$  是不可约的, 则  $\varepsilon p$  也是不可约的.

**证** 设二整数  $f_1, f_2$  使  $\varepsilon p = f_1 f_2$ . 所以,  $p = (\varepsilon^{-1} f_1)(f_2)$ . 因为  $p$  是不可约的, 故  $\varepsilon^{-1} f_1$  是单位或  $f_2$  是单位. 这也就是说,  $f_1$  是单位或  $f_2$  是单位. 所以,  $\varepsilon p$  是不可约的. 

**命题** 设整数  $p$  既不是 0, 也不是单位. 下述四命题等价:

- (i) 若整数  $f_1, f_2$  使  $f = f_1 f_2$ , 则  $f_1$  是单位或  $f_2$  是单位;
- (ii) 对任意整数  $f$ , 要么  $p$  是  $f$  的因子, 要么  $p$  与  $f$  互素 (二者不会同时发生);

---

<sup>†</sup>“素数”的一个同义词是“质数”.

(iii) 若  $f, g$  是整数, 且  $p$  是  $fg$  的因子, 则  $p$  是  $f$  的因子, 或  $p$  是  $g$  的因子;

(iv) 不存在整数  $f_1, f_2$  使  $p = f_1 f_2$ , 且  $|f_1| < |p|, |f_2| < |p|$ .

**证** (i)  $\Rightarrow$  (ii): 任取整数  $f$ . 设  $d$  是  $p$  与  $f$  的最大公因子. 所以, 存在整数  $g$  使  $p = dg$ . 所以,  $d$  是单位或  $g$  是单位. 若  $d$  是单位, 则单位是  $p$  与  $f$  的最大公因子, 即  $p$  与  $f$  互素; 若  $g$  是单位, 则  $d = pg^{-1}$ , 故  $p$  是  $f$  的因子.

若二者同时发生, 则  $d$  是单位且  $g$  是单位, 故  $p$  也是单位. 这与  $p$  不是单位矛盾.

(ii)  $\Rightarrow$  (iii): 若  $p$  是  $f$  的因子, 则不必证了. 今假设  $p$  不是  $f$  的因子. 所以,  $p$  与  $f$  互素. 因为  $p$  是  $fg$  的因子, 故  $p$  一定是  $g$  的因子.

(iii)  $\Rightarrow$  (iv): 反证法. 设  $p = f_1 f_2$ , 且  $|f_1| < |p|, |f_2| < |p|$ . 因为  $p \neq 0$ , 故  $f_1 \neq 0$ , 且  $f_2 \neq 0$ . 所以,  $|f_1| \geq 1$ , 且  $|f_2| \geq 1$ . 既然  $p = f_1 f_2$ ,  $p$  当然是  $f_1 f_2$  的因子. 所以,  $p$  是  $f_1$  的因子, 或  $p$  是  $f_2$  的因子. 若  $p$  是  $f_1$  的因子, 则存在整数  $g_1$  使  $f_1 = pg_1$ . 因为  $f_1 \neq 0$ , 故  $g_1 \neq 0$ . 这样,  $|g_1| \geq 1$ . 所以  $|f_1| = |p||g_1| \geq |p|$ . 这与假定  $|f_1| < |p|$  矛盾! 类似地, 若  $p$  是  $f_2$  的因子, 也有  $|f_2| \geq |p|$ , 矛盾! 综上, 这样的  $f_1$  与  $f_2$  不存在.

(iv)  $\Rightarrow$  (i): 这说明: 若整数  $f_1, f_2$  使  $p = f_1 f_2$ , 则  $|f_1| \geq |p|$  或  $|f_2| \geq |p|$ . 若  $|f_1| \geq |p|$ , 则  $|p| = |f_1||f_2| \geq |p||f_2|$ , 故  $|f_2| \leq 1$  (因为  $p \neq 0$ , 故  $|p| \neq 0$ , 从而可从不等式二边消去正因子), 即  $f_2 = \pm 1$  (因为  $f_2$  不能为 0), 即  $f_2$  是单位. 类似地, 若  $|f_2| \geq |p|$ , 则  $f_1$  是单位.  $\clubsuit$

**评注** 利用 (iii) 与数学归纳法, 读者可得如下结论 (作为练习):

设  $f_1, f_2, \dots, f_n$  是整数. 设整数  $p$  是不可约的. 若  $p$  是  $f_1 f_2 \cdots f_n$  的因子, 则存在 1 至  $n$  间的整数  $\ell$ , 使  $p$  是  $f_\ell$  的因子.

**评注** 设整数  $f$  既不是 0, 也不是单位. (iv) 表明, “ $f$  是可约的” 的一个必要与充分条件是 “存在二个整数  $f_1, f_2$ , 使  $f = f_1 f_2$ , 且  $|f_1| < |f|, |f_2| < |f|$ ”.

事实上,  $|f_1| \geq 2$ , 且  $|f_2| \geq 2$ . 反证法. 设  $|f_1| < 2$ . 因为  $f \neq 0$ , 故  $f_1 \neq 0$ , 即  $|f_1| \geq 1$ . 所以  $|f_1| = 1$ . 所以  $|f_2| = 1 \cdot |f_2| = |f_1||f_2| = |f| > |f_2|$ . 这是矛盾! 类似地, 若  $|f_2| < 2$ , 则  $|f_1| = |f| > |f_1|$ . 这也是矛盾.

综上, 我们得到了一个更好用的命题: “ $f$  是可约的” 的一个必要与充分条件是 “存在二个整数  $f_1, f_2$ , 使  $f = f_1 f_2$ , 且  $2 \leq |f_1| < |f|, 2 \leq |f_2| < |f|$ ”.

**评注** 设  $p, q$  是不可约的整数. 要么  $p$  是  $q$  的相伴, 要么  $p$  与  $q$  互素 (二者不会同时发生).

为什么呢? 若  $p$  与  $q$  互素, 则不必论证了. 所以, 我们假定  $p$  与  $q$  不互素. 所以  $p$  一定是  $q$  的因子 (因为  $p$  是不可约的), 且  $q$  一定是  $p$  的因子 (因为  $q$  是不可约的). 所以,  $p$  与  $q$  相伴.

若  $p$  与  $q$  相伴, 且  $p$  与  $q$  互素, 则有单位  $\varepsilon$  使  $q = p\varepsilon$ . 故  $p$  是  $p$  与  $q$  的公因子. 从而  $p$  是单位的因子. 所以  $p$  是单位. 这跟  $p$  是不可约的矛盾!

下面是关于不可约的整数的积的命题.

**命题** 设整数  $p_1, p_2, \dots, p_m, q_1, q_2, \dots, q_n$  都是不可约的. 设

$$p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n.$$

(i)  $m = n$ ;

(ii) 可以适当地调换  $q_1, q_2, \dots, q_m$  (注意,  $n = m$ ) 的顺序, 使任取 1 至  $m$  间的整数  $\ell, p_\ell$  与  $q_\ell$  相伴 (注意: 调换顺序后的  $q_\ell$  不一定跟原来的  $q_\ell$  相等!).

**证** 对等式左侧的不可约的整数的数目  $m$  用数学归纳法. 当  $m = 1$  时, 有

$$p_1 = q_1 q_2 \cdots q_n.$$

先证明:  $n = 1$ . 反证法. 设  $n > 1$ . 因为  $p_1 = q_1 q_2 \cdots q_n$ , 故  $p_1$  是某个  $q_i$  的因子 ( $i$  是某个 1 至  $n$  间的整数). 因为乘法可交换, 不失一般性, 设  $p_1$  是  $q_1$  的因子. 因为  $q_1$  是不可约的, 且  $q_1$  与  $p_1$  不是互素的, 故  $q_1$  也是  $p_1$  的因子. 所以, 存在单位  $\varepsilon$  使  $q_1 = \varepsilon p_1$ . 进而

$$p_1 = (\varepsilon p_1) q_2 \cdots q_n = p_1 (\varepsilon q_2) \cdots q_n.$$

因为  $p_1 \neq 0$ , 故可从等式二边消去  $p_1$ , 即

$$1 = (\varepsilon q_2) \cdots q_n.$$

因为  $q_2$  是不可约的, 故  $\varepsilon q_2$  也是不可约的. 上式表明,  $\varepsilon q_2$  是 1 的因子, 故  $\varepsilon q_2$  是单位. 这与假定矛盾! 所以,  $n$  不可高于 1. 这样,  $n = 1$ .

既然  $n = 1$ , 那么  $p_1 = q_1$ . 所以, 不必调换顺序即可知  $p_1$  与  $q_1$  相伴.

所以,  $m = 1$  时, 命题成立.

假定  $m = k$  时, 命题成立. 现在看  $m = k + 1$  时的情形. 设  $p_1, p_2, \dots, p_k, p_{k+1}, q_1, q_2, \dots, q_n$  是不可约的. 设

$$p_1 p_2 \cdots p_k p_{k+1} = q_1 q_2 \cdots q_n.$$

因为  $p_1$  是  $q_1 q_2 \cdots q_n$  的因子, 故  $p_1$  是某个  $q_j$  的因子 ( $j$  是某个 1 至  $n$  间的整数). 因为乘法可交换, 不失一般性, 设  $p_1$  是  $q_1$  的因子. 因为  $q_1$  是不可约的, 且  $q_1$  与  $p_1$  不是互素的, 故  $q_1$  也是  $p_1$  的因子. 所以, 存在单位  $\varepsilon'$  使  $q_1 = \varepsilon' p_1$ . 进而

$$p_1 p_2 \cdots p_k p_{k+1} = (\varepsilon' p_1) q_2 \cdots q_n = p_1 (\varepsilon' q_2) \cdots q_n.$$

因为  $p_1 \neq 0$ , 故可从等式二边消去  $p_1$ , 即

$$p_2 \cdots p_k p_{k+1} = (\varepsilon' q_2) \cdots q_n.$$

因为  $q_2$  是不可约的, 故  $\varepsilon' q_2$  也是不可约的. 上式左侧的不可约的整数的数目是  $k$ . 根据归纳假设,  $n - 1 = k$ , 即  $n = k + 1$ . 这证明了  $m = k + 1$  时 (i) 成立.

前面已证得, 适当地调换  $q_1, q_2, \dots, q_n$  的顺序, 可使  $p_1$  与  $q_1$  相伴. 根据归纳假设, 可以适当地调换  $\varepsilon' q_2, \dots, q_{k+1}$  (注意,  $n = k + 1$ ) 的顺序, 使任取 3 至  $k + 1$  间的整数  $u$ ,  $p_u$  与  $q_u$  相伴. 当然  $p_2$  与  $\varepsilon' q_2$  也相伴. 因为  $\varepsilon' q_2$  与  $q_2$  相伴, 所以  $p_2$  与  $q_2$  相伴. 把这些事实放在一块儿, 就是: 可以适当地调换  $q_1, q_2, \dots, q_{k+1}$  的顺序, 使任取 1 至  $k + 1$  间的整数  $\ell$ ,  $p_\ell$  与  $q_\ell$  相伴. 这样,  $m = k + 1$  时, (ii) 成立.  $\clubsuit$

**命题** 设整数  $f$  既不是 0, 也不是单位. 存在不可约的整数  $p_1, p_2, \dots, p_m$  使

$$f = p_1 p_2 \cdots p_m.$$



**证** 对  $f$  的绝对值  $N$  用数学归纳法. 因为  $f$  既不是 0, 也不是单位, 故  $N \geq 2$ .  $N = 2$  时,  $f = \pm 2$ . 我们已经知道, 2 是不可约的; 所以,  $-2$  也是不可约的. 这样,  $f$  是不可约的, 故存在不可约的整数  $p_1 = f$  使  $f = p_1$ . 这样,  $N = 2$  时, 命题成立.

设  $N \leq k$  ( $k \geq 2$ ) 时, 命题成立. 考虑  $N = k + 1$ . 若  $f$  是不可约的, 则存在不可约的整数  $p_1 = f$  使  $f = p_1$ . 若  $f$  是可约的, 则存在二整数  $f_1, f_2$ , 使  $f = f_1 f_2$ , 且  $2 \leq |f_1| < |f|$ ,  $2 \leq |f_2| < |f|$ . 所以  $|f_1| \leq |f| - 1 = k$ ,  $|f_2| \leq |f| - 1 = k$ . 根据归纳假设, 存在不可约的整数  $p_1, p_2, \dots, p_i, p_{i+1}, p_{i+2}, \dots, p_m$  使

$$f_1 = p_1 p_2 \cdots p_i, \quad f_2 = p_{i+1} p_{i+2} \cdots p_m.$$

所以

$$f = f_1 f_2 = p_1 p_2 \cdots p_i p_{i+1} p_{i+2} \cdots p_m.$$

故  $N = k + 1$  时, 命题也成立. ✎

合并上二个命题, 可得“算术基本定理” (*the fundamental theorem of arithmetic*):

**命题** 设整数  $f$  既不是 0, 也不是单位.

(i) 存在不可约的整数  $p_1, p_2, \dots, p_m$  使

$$f = p_1 p_2 \cdots p_m;$$

(ii) 若  $q_1, q_2, \dots, q_m, s_1, s_2, \dots, s_n$  是不可约的整数, 且

$$f = q_1 q_2 \cdots q_m = s_1 s_2 \cdots s_n,$$

则  $m = n$ , 且可以适当地调换  $s_1, s_2, \dots, s_m$  的顺序, 使任取 1 至  $m$  间的整数  $\ell$ ,  $q_\ell$  与  $s_\ell$  相伴 (注意: 调换顺序后的  $s_\ell$  不一定跟原来的  $s_\ell$  相等!).

设整数  $f$  既不是 0, 也不是单位. 利用上个命题, 我们可以方便地定出  $f$  的因子.

**命题** 设整数  $f$  既不是 0, 也不是单位. 设  $p_1, p_2, \dots, p_m$  是不可约的整数, 且

$$f = p_1 p_2 \cdots p_m.$$

$f$  的因子必为

$$(\star) \quad \varepsilon p_{j_1} p_{j_2} \cdots p_{j_s},$$

其中  $\varepsilon$  是单位,  $j_1, j_2, \dots, j_s$  是  $1, 2, \dots, m$  中  $s$  个不同的数 ( $s$  可取 0; 此时, 这就是单位).

**证** 从  $1, 2, \dots, m$  中选出  $s$  个不同的数  $j_1, j_2, \dots, j_s$ , 那么还剩  $m - s$  个数未被挑选. 记这  $m - s$  个数为  $j_{s+1}, \dots, j_m$ . 由于

$$\begin{aligned} f &= p_1 p_2 \cdots p_m \\ &= (p_{j_1} p_{j_2} \cdots p_{j_s}) (p_{j_{s+1}} \cdots p_{j_m}) \\ &= (\varepsilon p_{j_1} p_{j_2} \cdots p_{j_s}) (\varepsilon^{-1} p_{j_{s+1}} \cdots p_{j_m}), \end{aligned}$$

且  $\varepsilon^{-1} p_{j_{s+1}} \cdots p_{j_m}$  是整数, 故  $\varepsilon p_{j_1} p_{j_2} \cdots p_{j_s}$  是  $f$  的因子.

设  $g$  是  $f$  的因子. 我们证明:  $g$  一定能写为  $(\star)$  的形式.

首先,  $g$  一定不是 0. 若  $g$  是单位, 取  $s = 0$ ,  $g$  即可写为  $(\star)$  的形式. 现在设  $g$  既不是 0, 也不是单位.

设整数  $h$  使  $f = gh$ .  $h$  当然不是 0. 若  $h$  是单位, 则

$$g = h^{-1} f = h^{-1} p_1 p_2 \cdots p_m.$$

$h^{-1}$  也是单位, 且  $1, 2, \dots, m$  当然是  $1, 2, \dots, m$  中  $m$  个不同的数.

若  $h$  不是单位, 则存在不可约的整数  $q_1, q_2, \dots, q_s, q_{s+1}, \dots, q_n$  使

$$g = q_1 q_2 \cdots q_s, \quad h = q_{s+1} \cdots q_n.$$

所以

$$f = gh = q_1 q_2 \cdots q_s q_{s+1} \cdots q_n.$$

从而  $n = m$ , 且可以适当地调换  $p_1, p_2, \dots, p_m$  的顺序, 使任取  $1, 2, \dots, m$  中的数  $\ell$ ,  $q_\ell$  与  $p_\ell$  相伴. 但是, 我们注意到, 调换后的  $p_\ell$  跟题设的  $p_\ell$  不一定是相等的, 所以我们稍微变通一下.

我们把  $s$  个不可约的整数  $q_1, q_2, \dots, q_s$  写在左边, 把  $m$  个不可约的整数  $p_1, p_2, \dots, p_m$  写在右边:

$$q_1, q_2, \dots, q_s; \quad p_1, p_2, \dots, p_m.$$

对  $q_1$  而言, 肯定有整数  $j_1$  使  $q_1$  不与  $p_i$  ( $i < j_1$ ) 相伴 (从左向右看诸  $p_\ell$  即可), 但  $q_1$  与  $p_{j_1}$  相伴. 也就是说, 存在单位  $\varepsilon_1$  使  $q_1 = \varepsilon_1 p_{j_1}$ . 去掉左边的  $q_1$  与右边的  $p_{j_1}$ , 有

$$q_2, \dots, q_s; \quad p_1, \dots, p_{j_1-1}, p_{j_1+1}, \dots, p_m.$$

类似地, 对  $q_2$  而言, 肯定有整数  $j_2$  使  $q_2$  不与  $p_i$  ( $i < j_2, i \neq j_1$ ) 相伴, 但  $q_2$  与  $p_{j_2}$  相伴. 也就是说, 存在单位  $\varepsilon_2$  使  $q_2 = \varepsilon_2 p_{j_2}$ .

反复地执行此事, 可知: 存在  $1, 2, \dots, m$  中  $s$  个不同的数  $j_1, j_2, \dots, j_s$ , 存在  $s$  个单位  $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_s$  使  $q_\ell = \varepsilon_\ell p_{j_\ell}$ . 所以


$$\begin{aligned} f &= q_1 q_2 \cdots q_s \\ &= (\varepsilon_1 p_{j_1})(\varepsilon_2 p_{j_2}) \cdots (\varepsilon_s p_{j_s}) \\ &= (\varepsilon_1 \varepsilon_2 \cdots \varepsilon_s) p_{j_1} p_{j_2} \cdots p_{j_s} \\ &= \varepsilon p_{j_1} p_{j_2} \cdots p_{j_s}. \end{aligned} \quad \text{☺}$$

我们以一个简单的命题结束本文.

**命题** 设  $f_1, f_2, \dots, f_n$  是整数.  $f_1, f_2, \dots, f_n$  互素的一个必要与充分条件是: 任取不可约的整数  $p$ , 存在某个  $f_i$ , 使  $p$  不是  $f_i$  的因子.

**证** 先看必要性. 反证法. 假定结论不成立, 即: 存在不可约的整数  $p$ , 使任取  $f_i$ ,  $p$  是  $f_i$  的因子. 这样,  $p$  就是  $f_1, f_2, \dots, f_n$  的公因子. 所以,  $p$  是单位的因子. 矛盾!

再看充分性. 还是反证法. 假定结论不成立, 即: 设  $d$  是  $f_1, f_2, \dots, f_n$  的最大公因子, 且  $d$  不是单位. 若  $d$  是 0, 则  $f_1, f_2, \dots, f_n$  全是 0, 故任意的不可约的整数都是  $f_1, f_2, \dots, f_n$  的公因子, 矛盾! 若  $d$  不是 0, 也不是单位,

那么一定存在不可约的整数  $p_0$ , 使  $p_0$  是  $d$  的因子. 所以, 存在不可约的整数  $p_0$ , 使任取  $f_i$ ,  $p_0$  是  $f_i$  的因子. 矛盾! 

本文就到这里. 再见, 亲爱的读者朋友!

## 多项式的一些性质

本文的目标是补充一点多项式的性质; 我们后面会用到这些东西.

为尽可能多地照顾读者, 本文被加了一点细节.

$\mathbb{F}$  表示全体有理数 (或实数、复数) 作成的集.  $\mathbb{F}[x]$  是全体系数为  $\mathbb{F}$  的元的多项式作成的集. 在本文 “多项式的一些性质” 里, 我们约定: “多项式” 都是  $\mathbb{F}[x]$  的元, 而 “数” 都是  $\mathbb{F}$  的元 (当然也是多项式). “整数” 还是读者熟悉的整数; 当然, 这也是多项式.

读者可能还记得, 我们写多项式时, 一般都会带 “ $(x)$ ” 记号:

$$f(x) = a_0 + a_1x + \cdots + a_nx^n.$$

这个记号的优点有: (i) 清楚地表示出多项式的不定元为  $x$ ; (ii) 若  $t$  是数, 可用  $f(t)$  表示数

$$a_0 + a_1t + \cdots + a_nt^n;$$

(iii) 若  $g(x)$  是多项式, 可用  $f(g(x))$  表示多项式

$$a_0 + a_1g(x) + \cdots + a_ng(x)^n.$$

不过, 在本文里, 我们一般不干 (ii) (iii) 这二件事. 所以, 为了方便, 我们也写

$$f = a_0 + a_1x + \cdots + a_nx^n.$$

为方便, 我们定义一些词.

**定义** 设  $f$  是多项式. 若  $f$  的系数都是复数, 则  $f$  是复系数多项式 (*polynomial with complex coefficients*); 若  $f$  的系数都是实数, 则  $f$  是实系数多项式 (*polynomial with real coefficients*); 若  $f$  的系数都是有理数, 则  $f$  是有理系数多项式 (*polynomial with rational coefficients*); 若  $f$  的系数都是整数, 则  $f$  是整系数多项式 (*polynomial with integral coefficients*).

**评注** 我们提醒读者: 因为实数是复数, 故实系数多项式当然是复系数多项式; 因为有理数是实数, 故有理系数多项式当然是实系数多项式; 因为整数是有理数, 故整系数多项式当然是有理系数多项式.

以  $x^2 + 3$  为例. 当我们讨论复系数多项式  $x^2 + 3$  时, 我们允许不是实数的复数出现, 所以 “ $x^2 + 3$  可写为二个 1 次多项式的积” 是对的<sup>†</sup> 但是, 当我们讨论有理系数多项式  $x^2 + 3$  时, 我们不允许不是有理数的复数出现, 所以 “ $x^2 + 3$  可写为二个 1 次多项式的积” 是错的.

所以, 明确多项式的系数范围是有必要的. 不过, 正如前面所说, 我们讨论系数为  $F$  的多项式, 而  $F$  可以是  $\mathbb{Q}$ , 可以是  $\mathbb{R}$ , 也可以是  $\mathbb{C}$ . 所以, 读者不必 (在本文) 过于关注这件小事. 不同的系数的范围引起的差别主要体现在可约的与不可约的多项式上.

在正式进入讨论前, 作者希望读者能回想起二件事:

(i) 多项式  $f$  的次用  $\deg f$  表示. 零多项式的次是  $-\infty$ . 若多项式  $g, h$  适合  $f = gh$ , 则

$$\deg f = \deg g + \deg h.$$

(ii) 多项式的乘法适合消去律. 设  $f, g, h$  是多项式. 若  $f \neq 0$ , 且  $fg = fh$ , 则  $g = h$ .

我们先从多项式的单位开始.

**定义** 设  $f$  是多项式. 若存在多项式  $g$  使  $fg = 1$ , 则说  $f$  是单位 (*unit*).  $g$  称为  $f$  的逆 (*inverse*).

**命题** 1 是单位.

**证** 因为  $1 \cdot 1 = 1$ . ☞

**命题** 0 一定不是单位.

**证** 0 与任何多项式的积都是 0, 不等于 1. ☞

**命题** 设  $f$  是单位. 若多项式  $g, h$  适合  $fg = fh = 1$ , 则  $g = h$ .

**证** 因为多项式的乘法是交换的、结合的, 故

$$g = g1 = g(fh) = (gf)h = (fg)h = 1h = h. \quad \text{☞}$$

---

<sup>†</sup> 因为  $x^2 + 3 = x^2 - (\sqrt{3}i)^2 = (x + \sqrt{3}i)(x - \sqrt{3}i)$ .

**定义** 设  $f$  是单位. 上个命题指出,  $f$  的逆一定是唯一的 (根据单位的定义,  $f$  的逆当然存在). 我们用  $f^{-1}$  表示  $f$  的逆.

**命题** 设  $f$  是单位.  $f$  的逆  $f^{-1}$  也是单位, 且  $(f^{-1})^{-1} = f$ .

**证** 因为  $f$  是单位, 故存在多项式  $f^{-1}$  使  $ff^{-1} = 1$ . 因为乘法可交换, 故  $f^{-1}f = 1$ . 所以对多项式  $f^{-1}$  而言, 存在多项式  $f$  使  $f^{-1}f = 1$ . 由单位的定义,  $f^{-1}$  是单位. 因为单位的逆唯一, 故  $f$  是  $f^{-1}$  的逆.  $\clubsuit$

**命题** 设  $f_1, f_2, \dots, f_n$  是单位. 则  $f_1f_2 \cdots f_n$  也是单位, 且

$$(f_1f_2 \cdots f_n)^{-1} = f_n^{-1} \cdots f_2^{-1}f_1^{-1}.$$

**证** 既然  $f_1, f_2, \dots, f_n$  是单位, 那么它们都有逆, 分别为  $f_1^{-1}, f_2^{-1}, \dots, f_n^{-1}$ . 所以

$$\begin{aligned} & (f_1f_2 \cdots f_{n-1}f_n)(f_n^{-1}f_{n-1}^{-1} \cdots f_2^{-1}f_1^{-1}) \\ &= (f_1f_2 \cdots f_{n-1})(f_nf_n^{-1})(f_{n-1}^{-1} \cdots f_2^{-1}f_1^{-1}) \\ &= (f_1f_2 \cdots f_{n-1})(1)(f_{n-1}^{-1} \cdots f_2^{-1}f_1^{-1}) \\ &= (f_1f_2 \cdots f_{n-1})(f_{n-1}^{-1} \cdots f_2^{-1}f_1^{-1}) \\ &= \dots\dots\dots \\ &= f_1f_1^{-1} \\ &= 1. \end{aligned}$$

所以,  $f_1f_2 \cdots f_n$  是单位. 因为单位的逆唯一, 故

$$(f_1f_2 \cdots f_n)^{-1} = f_n^{-1} \cdots f_2^{-1}f_1^{-1}. \quad \clubsuit$$

**定义** 多项式的全体单位称为多项式的单位群.

**命题** 多项式的单位群恰由全体非零数作成.

**证** 每个非零数  $c$  都有倒数  $\frac{1}{c}$ .  $\frac{1}{c}$  也是非零数, 故由  $c \cdot \frac{1}{c} = 1$  可知  $c$  是单位.

设  $f$  是单位. 所以, 存在多项式  $g$  使  $fg = 1$ . 我们证明:  $\deg f = 0$ .

这很容易. 因为  $fg = 1$ , 故  $\deg f + \deg g = \deg 1 = 0$ . 显然  $\deg f$  与  $\deg g$  都是非负整数. 这样,  $\deg f = 0$ . 零次多项式就是非零数.

综上, 多项式的单位群恰由全体非零数作成.  $\clubsuit$

读者可能还记得, 多项式也有带余除法:

**命题** 设  $f$  是非零多项式. 对任意多项式  $g$ , 存在唯一的一对多项式  $q, r$  使

$$g = qf + r, \quad \deg r < \deg f.$$

一般称其为带余除法:  $q$  就是商;  $r$  就是余式. 并且, 当  $f$  的次不高于  $g$  的次时,  $f, g, q$  间还有如下的次关系:

$$\deg g = \deg(g - r) = \deg q + \deg f.$$

我们已经在前面证明过这个关系, 所以我们就不赘述了.  
请读者休息一会儿.

**定义** 设  $f, g$  是多项式. 若存在多项式  $h$  使  $f = gh$ , 则说  $g$  是  $f$  的因子 (*factor*).

**例** (i) 单位是任意多项式的因子; 单位的因子一定是单位.

(ii) 任意多项式都是 0 的因子; 非零多项式的因子一定不是 0.

**命题** 设  $f, g, h$  是多项式. 因子适合如下性质:

- (i)  $f$  是  $f$  的因子;
- (ii) 若  $h$  是  $g$  的因子, 且  $g$  是  $f$  的因子, 则  $h$  是  $f$  的因子;
- (iii) 若  $f$  是  $g$  的因子, 且  $g$  是  $f$  的因子, 则存在单位  $q$  使  $f = qg$ ;
- (iv) 设  $k, \ell$  是多项式. 若  $h$  是  $f$  的因子, 且  $h$  是  $g$  的因子, 则  $h$  是  $kf \pm \ell g$  的因子;
- (v) 若  $\varepsilon_1, \varepsilon_2$  是单位, 且  $g$  是  $f$  的因子, 则  $\varepsilon_2 g$  是  $\varepsilon_1 f$  的因子.

**证** (i) 注意到  $f = 1f$ , 其中 1 是单位.

(ii) 因为  $h$  是  $g$  的因子, 故存在多项式  $p$  使  $g = ph$ . 因为  $g$  是  $f$  的因子, 故存在多项式  $q$  使  $f = qg$ . 所以

$$f = qg = q(ph) = (qp)h.$$



因为  $qp$  也是多项式, 故  $h$  是  $f$  的因子.

(iii) 若  $f = 0$ , 则  $g = 0$ , 当然有  $f = 1g = 0$ , 其中  $1$  是单位. 下设  $f \neq 0$ .

因为  $f$  是  $g$  的因子, 故存在多项式  $p$  使  $g = pf$ ; 因为  $g$  是  $f$  的因子, 故存在多项式  $q$  使  $f = qg$ . 所以

$$f = qg = q(pf) = (qp)f.$$

因为  $f \neq 0$ , 故可从等式二边消去  $f$ , 即

$$1 = qp.$$

由此可知  $q$  是单位.

(iv) 因为  $h$  是  $f$  的因子, 且  $h$  是  $g$  的因子, 故存在多项式  $p, q$  使  $f = ph$  且  $g = qh$ . 所以

$$kf \pm \ell g = k(ph) \pm \ell(qh) = (kp)h \pm (\ell q)h = (kp \pm \ell q)h.$$

(v) 若存在多项式  $q$  使  $f = gq$ , 则

$$\varepsilon_1 f = g(\varepsilon_1 q) = g(\varepsilon_2 \varepsilon_2^{-1})(\varepsilon_1 q) = (g\varepsilon_2)(\varepsilon_2^{-1} \varepsilon_1 q).$$

因为单位的逆是多项式, 且 (有限多个) 多项式的积是多项式, 故  $\varepsilon_2^{-1} \varepsilon_1 q$  是多项式. 从而  $\varepsilon_2 g$  是  $\varepsilon_1 f$  的因子. ✎

为方便, 我们定义一个新词.

**定义** 设  $f, g$  是多项式. 若存在单位  $\varepsilon$  使  $f = \varepsilon g$ , 则说  $f$  是  $g$  的相伴 (*associate*). 因为

$$g = 1g = (\varepsilon^{-1}\varepsilon)g = \varepsilon^{-1}(\varepsilon g) = \varepsilon^{-1}f,$$

故  $g$  当然也是  $f$  的相伴. 所以, 我们说  $f$  与  $g$  相伴 (*to be associate*).

显然, 因为  $f = 1f$ , 故  $f$  与  $f$  相伴. 上面的文字已经说明  $f$  与  $g$  相伴相当于  $g$  与  $f$  相伴. 我们还有下面的

**命题** 设  $f, g, h$  是多项式. 若  $f$  与  $g$  相伴, 且  $g$  与  $h$  相伴, 则  $f$  与  $h$  相伴.

**证** 因为  $f$  与  $g$  相伴, 故存在单位  $\varepsilon_1$  使  $f = \varepsilon_1 g$ . 因为  $g$  与  $h$  相伴, 故存在单位  $\varepsilon_2$  使  $g = \varepsilon_2 h$ . 所以

$$f = \varepsilon_1 g = \varepsilon_1 (\varepsilon_2 h) = (\varepsilon_1 \varepsilon_2) h.$$

因为  $\varepsilon_1 \varepsilon_2$  是单位, 故  $f$  与  $g$  相伴. ✎

根据 (iii), 我们有

**命题** 设  $f, g$  是多项式.  $f$  与  $g$  相伴的一个必要与充分条件是  $f$  是  $g$  的因子, 且  $g$  是  $f$  的因子.

**定义** 设  $f, g$  是多项式. 若  $d$  是  $f$  的因子, 且  $d$  是  $g$  的因子, 则  $d$  是  $f$  与  $g$  的公因子 (*common factor*).

**评注** 若  $d$  是  $f$  与  $g$  的公因子, 则  $d$  当然也是  $g$  与  $f$  的公因子. 换句话说, 公因子与次序无关.

**例** 单位是任意二个多项式的公因子.

现在我们引出“最大公因子”的概念.

**定义** 设  $f, g$  是多项式. 适合下述二性质的多项式  $d$  是  $f$  与  $g$  的最大公因子 (*greatest common factor*):

- (i)  $d$  是  $f$  与  $g$  的公因子;
- (ii) 若  $e$  是  $f$  与  $g$  的公因子, 则  $e$  是  $d$  的因子.

**评注** 若  $d$  是  $f$  与  $g$  的最大公因子, 则  $d$  当然也是  $g$  与  $f$  的最大公因子. 换句话说, 最大公因子与次序无关. 这是因为公因子与次序无关.

由定义立即可得

**命题** 设  $f, g$  是多项式. 若  $d_1$  与  $d_2$  都是  $f$  与  $g$  的最大公因子, 则  $d_1$  与  $d_2$  相伴.

**证** 因为  $d_1$  是  $d_2$  的因子, 且  $d_2$  也是  $d_1$  的因子. ✎

**评注** 由此可见, 最大公因子不一定是唯一的. 但这不是很重要.

**例** 不难看出,  $d = f$  是 0 与  $f$  的最大公因子: (i)  $d$  是 0 的因子, 且  $d$  是  $f$  的因子; (ii) 若  $e$  是 0 与  $f$  的公因子, 则  $e$  当然是  $d$  (即  $f$ ) 的因子.

**例** 设  $\varepsilon$  是单位. 不难看出,  $d = \varepsilon$  是  $\varepsilon$  与  $f$  的最大公因子: (i)  $d$  是  $\varepsilon$  的因子, 且  $d$  是  $f$  的因子; (ii) 若  $e$  是  $\varepsilon$  与  $f$  的公因子, 则  $e$  当然是  $d$  (即  $\varepsilon$ ) 的因子.

**命题** 设  $f, g, q$  是多项式. 设  $f$  与  $g$  的最大公因子是  $d_1$ ; 设  $f - gq$  与  $g$  的最大公因子是  $d_2$ . 则  $d_1$  与  $d_2$  相伴.

**证** 因为  $d_1$  是  $f$  与  $g$  的公因子, 故  $d_1$  是  $1 \cdot f - q \cdot g$  的因子. 这说明,  $d_1$  是  $f - gq$  与  $g$  的公因子. 因为  $d_2$  是  $f - gq$  与  $g$  的最大公因子, 故  $d_1$  是  $d_2$  的因子.

因为  $d_2$  是  $f - gq$  与  $g$  的公因子, 故  $d_2$  是  $1 \cdot (f - gq) + q \cdot g$  的因子. 这说明,  $d_2$  是  $f$  与  $g$  的公因子. 因为  $d_1$  是  $f$  与  $g$  的最大公因子, 故  $d_2$  是  $d_1$  的因子.

综上,  $d_1$  与  $d_2$  相伴. ✎

我们现在可以证明

**命题** 设  $f, g$  是多项式.  $f$  与  $g$  的最大公因子一定存在.

**证** 不妨假定  $g$  不是 0. 所以, 根据带余除法, 有

$$f = gq_0 + r_0, \quad \deg r_0 < \deg g.$$

根据上一个命题,  $r_0$  与  $g$  的最大公因子是  $f$  与  $g$  的最大公因子. 若  $r_0 = 0$ , 则  $g$  就是 0 与  $g$  (从而也是  $f$  与  $g$ ) 的最大公因子. 若  $r_0 \neq 0$ , 则

$$g = r_0q_1 + r_1, \quad \deg r_1 < \deg r_0.$$

根据上一个命题,  $r_1$  与  $r_0$  的最大公因子是  $r_0$  与  $g$  的最大公因子, 所以也是  $f$  与  $g$  的最大公因子. 若  $r_1 = 0$ , 则  $r_0$  就是 0 与  $r_0$  (从而也是  $f$  与  $g$ ) 的最大公因子. 若  $r_1 \neq 0$ , 则

$$r_0 = r_1q_2 + r_2, \quad \deg r_2 < \deg r_1.$$

这个过程必定会在有限多步后停止. 反证法. 如果此过程可一直进行下去, 则我们可得到无限多个非负整数  $\deg r_0, \deg r_1, \dots$  使

$$\deg g > \deg r_0 > \deg r_1 > \dots > \deg r_k > \deg r_{k+1} > \dots.$$

可是, 不存在无限递降的非负整数列 (低于  $\deg g$  的非负整数至多有  $\deg g$  个), 矛盾!

为方便, 分别称  $f$  与  $g$  为  $r_{-2}$  与  $r_{-1}$ . 根据上面的讨论, 一定存在整数  $n$  使

$$r_{\ell-2} = r_{\ell-1}q_{\ell} + r_{\ell}, \quad 0 \leq \deg r_{\ell} < \deg r_{\ell-1}, \quad \ell = 0, 1, \dots, n-2;$$

$$r_{n-3} = r_{n-2}q_{n-1}.$$

$r_{n-2}$  是 0 与  $r_{n-2}$  的最大公因子, 也是  $r_{n-2}$  与  $r_{n-3}$  的最大公因子, 也是  $r_{n-3}$  与  $r_{n-4}$  的最大公因子……也是  $r_{-2}$  与  $r_{-1}$  的最大公因子. 所以,  $r_{n-2}$  是  $f$  与  $g$  的最大公因子. ✎

这个命题的证明过程事实上也给出了一个计算二个多项式的最大公因子的算法 (“辗转相除法”).

**例** 设  $f = x^5 + 3x + 1, g = x^2 - x - 1$ . 我们来找一个  $f$  与  $g$  的最大公因子.

不难作出如下计算:

$$x^5 + 3x + 1 = (x^2 - x - 1) \cdot (x^3 + x^2 + 2x + 3) + (8x + 4),$$

$$x^2 - x - 1 = (8x + 4) \cdot \frac{2x - 3}{16} - \frac{1}{4}.$$

所以,  $-\frac{1}{4}$  是  $8x + 4$  与  $x^2 - x - 1$  的最大公因子, 是  $x^2 - x - 1$  与  $x^5 + 3x + 1$  的最大公因子.

当然, 读者不难说明, 每个单位都是  $f$  与  $g$  的最大公因子.

根据上面的计算, 我们有

$$1 \cdot (x^2 - x - 1) + \frac{-2x + 3}{16} \cdot (8x + 4) = -\frac{1}{4}.$$

又因为

$$8x + 4 = 1 \cdot (x^5 + 3x + 1) + (-x^3 - x^2 - 2x - 3) \cdot (x^2 - x - 1),$$

故

$$\begin{aligned} & \frac{-2x+3}{16}(x^5+3x+1) \\ & + \left(1 + \frac{-2x+3}{16}(-x^3-x^2-2x-3)\right)(x^2-x-1) = -\frac{1}{4}. \end{aligned}$$

即

$$\frac{-2x+3}{16}(x^5+3x+1) + \frac{2x^4-x^3+x^2+7}{16}(x^2-x-1) = -\frac{1}{4}.$$

一般地, 我们有

**命题** 设  $f, g$  是多项式. 设  $d$  是  $f$  与  $g$  的最大公因子. 存在多项式  $s$  与  $t$  使

$$sf + tg = d.$$

这个等式的一个名字是 Bézout 等式 (*Bézout's identity*).

**证** 若  $f = g = 0$ , 则可取  $s = t = 0$ . 下设  $g \neq 0$ .

为方便, 分别称  $f$  与  $g$  为  $r_{-2}$  与  $r_{-1}$ . 设存在整数  $n$  使

$$r_{\ell-2} = r_{\ell-1}q_{\ell} + r_{\ell}, \quad 0 \leq \deg r_{\ell} < \deg r_{\ell-1}, \quad \ell = 0, 1, \dots, n-2;$$

$$r_{n-3} = r_{n-2}q_{n-1}.$$

为方便, 记

$$r_{\ell} = 0, \quad \ell \geq n-1.$$

我们用数学归纳法证明辅助命题  $P(\ell)$ : 任取非负整数  $\ell$ , 必有二多项式  $s, t$  使

$$r_{\ell} = sf + tg.$$

$r_0$  可写为

$$r_0 = 1r_{\ell-2} + (-q_0)r_\ell = 1f + (-q_0)g.$$

$r_1$  可写为

$$r_1 = 1r_{-1} + (-q_1)r_0 = (-q_1)f + (1 + q_0q_1)g.$$

所以  $P(0)$  与  $P(1)$  正确. 假定  $P(0), P(1), \dots, P(k-1)$  正确. 我们的目标是: 推出  $P(k)$  正确. 若  $k \geq n-1$ , 则

$$r_k = 0 = 0f + 0g.$$

若  $k \leq n-2$ , 则根据归纳假设, 存在多项式  $u, v, z, w$  使

$$r_{k-2} = uf + vg, \quad r_{k-1} = zf + wg.$$

所以

$$r_k = r_{k-2} - r_{k-1}q_k = (u - zq_k)f + (v - wq_k)g.$$

因为  $u - zq_k$  与  $v - wq_k$  均为多项式, 故  $P(k)$  正确.

所以, 存在多项式  $s, t$  使

$$sf + tg = r_{n-2}.$$

因为  $r_{n-2}$  与  $d$  都是  $f$  与  $g$  的最大公因子, 故  $d = \varepsilon r_{n-2}$ , 其中  $\varepsilon$  是单位. 所以

$$(\varepsilon s)f + (\varepsilon t)g = d. \quad \heartsuit$$

有了最大公因子的概念, 我们可以引出“互素”:

**定义** 设  $f, g$  是多项式. 若单位是  $f$  与  $g$  的最大公因子, 则称  $f$  与  $g$  互素 (*to be relatively prime*).

**评注** 因为最大公因子与次序无关, 故互素也与次序无关. 换句话说, “ $f$  与  $g$  互素” 相当于 “ $g$  与  $f$  互素”.

**例** 显然, 单位与任意多项式都互素.

下面给出一个极重要的命题:

**命题** 设  $f, g$  是多项式.  $f$  与  $g$  互素的一个必要与充分条件是: 存在多项式  $s, t$  使

$$sf + tg = 1.$$

**证** 先看必要性. 显然; 这是 Bézout 等式的结果.

再看充分性. 设  $d$  是  $f$  与  $g$  的最大公因子. 因为  $sf + tg = 1$ , 故  $d$  是 1 的因子. 这样,  $d$  一定是单位. ✎

下面是几个关于互素的性质.

**命题** 设  $f, g, h$  是多项式. 互素有如下性质:

- (i) 若  $h$  是  $fg$  的因子, 且  $h$  与  $f$  互素, 则  $h$  是  $g$  的因子;
- (ii) 若  $f$  与  $g$  互素, 且  $f$  与  $h$  互素, 则  $f$  与  $gh$  互素;
- (iii) 若  $f$  是  $h$  的因子,  $g$  是  $h$  的因子, 且  $f$  与  $g$  互素, 则  $fg$  是  $h$  的因子.

**证** (i) 因为  $h$  与  $f$  互素, 故存在多项式  $s$  与  $t$  使

$$sh + tf = 1.$$

所以

$$(gs)h + t(fg) = g.$$

因为  $h$  是  $h$  的因子, 且  $h$  是  $fg$  的因子, 故  $h$  是  $g = (gs)h + t(fg)$  的因子.

(ii) 因为  $f$  与  $g$  互素, 故存在多项式  $u, v$  使

$$uf + vg = 1.$$

因为  $f$  与  $h$  互素, 故存在多项式  $s, t$  使

$$sf + th = 1.$$

从而

$$1 = (uf + vg)(sf + th) = (ufs + uth + vgs)f + (vt)(gh).$$

所以  $f$  与  $gh$  互素.

(iii) 因为  $f$  是  $h$  的因子, 故存在多项式  $p$  使  $h = fp$ . 因为  $g$  是  $h = fp$  的因子, 且  $f$  与  $g$  互素, 故由 (i) 知  $g$  是  $p$  的因子. 设  $p = gq$ . 这样

$$h = fp = f(gq) = (fg)q,$$

故  $fg$  是  $h$  的因子.

☞

感谢您的阅读. 请休息一会儿.

现在我们推广公因子、最大公因子、互素的概念.

前面, 我们讨论了二个多项式的公因子、最大公因子、互素; 现在, 我们从量的角度推广.

**定义** 设  $f_1, f_2, \dots, f_n$  是多项式. 若  $d$  是  $f_1$  的因子,  $d$  是  $f_2$  的因子  $\dots d$  是  $f_n$  的因子, 则  $d$  是  $f_1, f_2, \dots, f_n$  的公因子.

**评注** 我们并没有禁止  $n$  取 1: 一个多项式的“公因子”当然是它的因子. 同理, 一个多项式也可以有“最大公因子”; 一个多项式也可以“互素”.

作为练习, 请读者证明

**命题** 设  $k_1, k_2, \dots, k_n, f_1, f_2, \dots, f_n$  是多项式. 若  $d$  是  $f_1, f_2, \dots, f_n$  的公因子, 则  $d$  是  $k_1f_1 + k_2f_2 + \dots + k_nf_n$  的因子.

**定义** 设  $f_1, f_2, \dots, f_n$  是多项式. 适合下述二性质的多项式  $d$  是  $f_1, f_2, \dots, f_n$  的最大公因子:

- (i)  $d$  是  $f_1, f_2, \dots, f_n$  的公因子;
- (ii) 若  $e$  是  $d$  是  $f_1, f_2, \dots, f_n$  的公因子, 则  $e$  是  $d$  的因子.

由定义立即可得



**命题** 设  $f_1, f_2, \dots, f_n$  是多项式. 若  $d_1$  与  $d_2$  都是  $f_1, f_2, \dots, f_n$  的最大公因子, 则  $d_1$  与  $d_2$  相伴.

**证** 因为  $d_1$  是  $d_2$  的因子, 且  $d_2$  也是  $d_1$  的因子. ✎

**命题** 设  $f_1, f_2, \dots, f_n$  是多项式.

(i)  $f_1, f_2, \dots, f_n$  的最大公因子存在;

(ii) 若  $d$  是  $f_1, f_2, \dots, f_n$  的最大公因子, 则存在多项式  $u_1, u_2, \dots, u_n$  使

$$u_1 f_1 + u_2 f_2 + \dots + u_n f_n = d.$$

**证** (i) 对  $n$  用数学归纳法. 显然,  $n = 1$  或  $n = 2$  时, 命题成立. 设  $n = k$  ( $k \geq 2$ ) 时命题成立, 即:  $f_1, f_2, \dots, f_k$  的最大公因子存在.

今看  $n = k + 1$  时的情形. 令  $d_k$  为  $f_1, f_2, \dots, f_k$  的最大公因子. 令  $d$  为  $d_k$  与  $f_{k+1}$  的最大公因子. 我们证明:  $d$  是  $f_1, f_2, \dots, f_k, f_{k+1}$  的最大公因子.

首先,  $d$  是  $f_1, f_2, \dots, f_k, f_{k+1}$  的公因子.  $d$  当然是  $f_{k+1}$  的因子. 任取某个 1 至  $k$  间的  $\ell$ . 因为  $d$  是  $d_k$  的因子, 而  $d_k$  是  $f_\ell$  的因子, 故  $d$  是  $f_\ell$  的因子. 这样,  $d$  确为  $f_1, f_2, \dots, f_k, f_{k+1}$  的公因子.

其次, 若  $e$  是  $f_1, f_2, \dots, f_k, f_{k+1}$  的公因子, 则  $e$  当然是  $f_1, f_2, \dots, f_k$  的公因子, 故  $e$  是  $d_k$  的因子. 又因为  $e$  是  $f_{k+1}$  的因子, 则  $e$  是  $d_k$  与  $f_{k+1}$  的公因子. 这样,  $e$  是  $d$  的因子.

根据最大公因子的定义,  $d$  一定是  $f_1, f_2, \dots, f_k, f_{k+1}$  的最大公因子. 所以,  $n = k + 1$  时, (i) 正确.

(ii) 对  $n$  用数学归纳法. 显然,  $n = 1$  或  $n = 2$  时, 命题成立. 设  $n = k$  ( $k \geq 2$ ) 时命题成立, 即: 若  $d_k$  是  $f_1, f_2, \dots, f_k$  的最大公因子, 则存在多项式  $u_1, u_2, \dots, u_k$  使

$$u_1 f_1 + u_2 f_2 + \dots + u_k f_k = d_k.$$

今看  $n = k + 1$  时的情形. 令  $d$  为  $d_k$  与  $f_{k+1}$  的最大公因子. 由 (i) 知,  $d$  是  $f_1, f_2, \dots, f_k, f_{k+1}$  的最大公因子. 由 Bézout 等式知, 存在多项式  $u, u_{k+1}$  使

$$u d_k + u_{k+1} f_{k+1} = d.$$

根据归纳假设, 存在多项式  $v_1, v_2, \dots, v_k$  使

$$v_1 f_1 + v_2 f_2 + \dots + v_k f_k = d_k.$$

这样

$$(uv_1)f_1 + (uv_2)f_2 + \dots + (uv_k)f_k + u_{k+1}f_{k+1} = d.$$

所以,  $n = k + 1$  时, (ii) 正确. ✎

跟之前一样, 有了最大公因子的概念, 我们可以引出“互素”:

**定义** 设  $f_1, f_2, \dots, f_n$  是多项式. 若单位是  $f_1, f_2, \dots, f_n$  的最大公因子, 则称  $f_1, f_2, \dots, f_n$  互素.

下面的命题也是十分自然的.

**命题** 设  $f_1, f_2, \dots, f_n$  是多项式.  $f_1, f_2, \dots, f_n$  互素的一个必要与充分条件是: 存在多项式  $u_1, u_2, \dots, u_n$  使

$$u_1 f_1 + u_2 f_2 + \dots + u_n f_n = 1.$$

**证** 先看必要性. 显然; 这是上个命题的结果.

再看充分性. 设  $d$  是  $f_1, f_2, \dots, f_n$  的最大公因子. 因为  $u_1 f_1 + u_2 f_2 + \dots + u_n f_n = 1$ , 故  $d$  是 1 的因子. 这样,  $d$  一定是单位. ✎

**命题** 设  $f_1, f_2, \dots, f_n, f$  是多项式. 若  $f_1$  与  $f$  互素,  $f_2$  与  $f$  互素…… $f_n$  与  $f$  互素, 则  $f_1 f_2 \dots f_n$  与  $f$  互素.

**证** 用数学归纳法.  $n = 1$  时, 显然. 设  $f_1 f_2 \dots f_{n-1}$  与  $f$  互素. 因为  $f_n$  与  $f$  互素, 故  $f_1 f_2 \dots f_{n-1} \cdot f_n$  与  $f$  互素. ✎

**命题** 设多项式  $f_1, f_2, \dots, f_n$  不全是零.

(i)  $f_1, f_2, \dots, f_n$  的最大公因子  $d$  不是零;

(ii) 任取 1 至  $n$  间的整数  $\ell$ , 必有 (唯一的) 多项式  $g_\ell$  使  $f_\ell = dg_\ell$ ;

(iii) 单位是  $g_1, g_2, \dots, g_n$  的最大公因子; 换句话说,  $g_1, g_2, \dots, g_n$  互素;

(iv) 反过来, 若多项式  $u_1, u_2, \dots, u_n$  互素, 则  $w$  是  $wu_1, wu_2, \dots, wu_n$  的最大公因子.

**证** (i) 零一定不是非零多项式的因子, 故零不是  $f_1, f_2, \dots, f_n$  的公因子, 当然也不是最大公因子.

(ii) 既然  $d$  是最大公因子, 当然也是公因子. 对  $f_\ell$  而言, 由因子的定义, 知: 存在多项式  $g_\ell$  使  $f_\ell = dg_\ell$ . 现在看唯一性. 假定  $f_\ell = dg_\ell = dg'_\ell$ . 因为  $d \neq 0$ , 故可从等式二边消去  $d$ , 即  $g_\ell = g'_\ell$ .

(iii) 设  $g_1, g_2, \dots, g_n$  的最大公因子是  $\delta$ . 这样, 由 (ii), 知: 对任意  $g_\ell$ , 有多项式  $h_\ell$  使  $g_\ell = \delta h_\ell$ . 所以

$$f_\ell = dg_\ell = d(\delta h_\ell) = (d\delta)h_\ell.$$

所以  $d\delta$  是  $f_1, f_2, \dots, f_n$  的公因子. 所以  $d\delta$  是  $d$  的因子.  $d$  显然是  $d\delta$  的因子, 故  $d\delta = \varepsilon d$ , 其中  $\varepsilon$  是单位. 因为  $d \neq 0$ , 故可从等式二边消去  $d$ , 即  $\delta = \varepsilon$ .

(iv) 若  $w = 0$ , 命题显然成立:  $0, 0, \dots, 0$  的最大公因子当然是  $0$ . 下设  $w \neq 0$ .

$w$  显然是  $wu_1, wu_2, \dots, wu_n$  的公因子. 设  $ws$  是  $wu_1, wu_2, \dots, wu_n$  的最大公因子, 这里  $s$  是某个多项式. 由 (ii), 对每个  $wu_\ell$ , 都有多项式  $q_\ell$  使  $wu_\ell = wsq_\ell$ . 因为  $w \neq 0$ , 故可从等式二边消去  $w$ , 即  $u_\ell = sq_\ell$ . 这样,  $s$  是  $u_1, u_2, \dots, u_n$  的公因子, 故  $s$  是单位的因子, 即  $s$  是单位. 所以  $w$  是  $wu_1, wu_2, \dots, wu_n$  的最大公因子.  $\text{☞}$

互素的一个特殊情形是 PRP.

**定义** 设  $f_1, f_2, \dots, f_n$  是多项式 ( $n \geq 2$ ). 若任取  $1$  至  $n$  间的二个不同的整数  $i, j$ , 都有  $f_i$  与  $f_j$  互素, 则  $f_1, f_2, \dots, f_n$  PRP<sup>†</sup> (*to be pairwise relatively prime*).

为方便, 若  $f$  是单位, 我们也说 “ $f$  PRP” (这相当于定义了  $n = 1$  时 PRP 的意义).

**例** 设  $f_1 = x, f_2 = x + 3, f_3 = x - 1$ . 因为  $f_1$  与  $f_2$  互素,  $f_2$  与  $f_3$  互素,  $f_3$  与  $f_1$  互素, 故  $f_1, f_2, f_3$  PRP. 读者不难发现:  $f_1, f_2, f_3$  互素.

<sup>†</sup>因为作者的汉语不是很好, 所以作者用英语缩写表示这个概念. 作为参考, 作者用英语定义 PRP: A list of polynomials  $p_1, p_2, \dots, p_n$  is said to be *pairwise relatively prime* if  $p_i$  and  $p_j$  are relatively prime for any two distinct integers  $i, j$  in  $\{1, 2, \dots, n\}$ .

一般地, 我们有

**命题** 设多项式  $f_1, f_2, \dots, f_n$  PRP. 则  $f_1, f_2, \dots, f_n$  互素.

**证** 用数学归纳法.  $n = 1$  时,  $f_1$  是单位, 故  $f_1$  “互素”.  $n = 2$  时,  $f_1$  与  $f_2$  PRP 相当于  $f_1$  与  $f_2$  互素.

设  $n = s$  时命题成立. 考虑  $n = s + 1$  的情形.

既然  $f_1, f_2, \dots, f_s, f_{s+1}$  PRP, 那么 “暂时地不考虑  $f_{s+1}$ ”, 可知  $f_1, f_2, \dots, f_s$  PRP. 所以, 单位  $\varepsilon$  是  $f_1, f_2, \dots, f_s$  的最大公因子 (归纳假设). 设  $d$  是  $f_1, f_2, \dots, f_s, f_{s+1}$  的最大公因子.  $d$  当然是  $f_1, f_2, \dots, f_s$  的公因子. 所以  $d$  是  $\varepsilon$  的因子. 故  $d$  也是单位.

所以,  $n = s + 1$  时, 命题也成立. ✎

不过反过来就不一定了.

**例** 设  $g_1 = 1, g_2 = x, g_3 = x^2$ . 显然,  $g_1, g_2, g_3$  互素. 可是,  $x$  是  $g_2$  与  $g_3$  的最大公因子. 所以,  $g_1, g_2, g_3$  不 PRP.

**命题** 设多项式  $f_1, f_2, \dots, f_n$  PRP. 设  $m_1, m_2, \dots, m_n$  是非负整数. 记  $F_i = f_i^{m_i}$ ,  $i$  是 1 至  $n$  间的整数. 则  $F_1, F_2, \dots, F_n$  也 PRP.

**证** 根据 PRP 的定义, 我们只需证: 若  $f$  与  $g$  互素, 且  $s, t$  是非负整数, 则  $f^s$  与  $g^t$  互素.

若  $s = 0$  或  $t = 0$ , 因为 1 与任意多项式都互素, 故此时显然. 下设  $s \geq 1$  且  $t \geq 1$ .

我们先证:  $f^s$  与  $g$  互素. 因为  $f$  与  $g$  互素,  $f$  与  $g$  互素…… $f$  与  $g$  互素 ( $s$  个 “ $f$  与  $g$  互素”), 故  $f^s = \underbrace{f \cdot f \cdots f}_{s \text{ 个 } f}$  与  $g$  互素.

暂时记  $F = f^s$ . 因为  $F$  与  $g$  互素, 故 (照搬上段的推理)  $F$  与  $g^t$  互素. ✎

**命题** 设多项式  $f_1, f_2, \dots, f_n$  PRP. 则  $f_1 f_2 \cdots f_{i-1}$  与  $f_i$  互素 ( $i$  是 1, 2,  $\dots, n$  中的数). 我们约定: 0 个多项式的和为 0, 而 0 个多项式的积为 1. 所以,  $i = 1$  时, 1 当然与  $f_1$  互素.

**证**  $i = 1$  时, 显然. 设  $i \geq 2$ . 因为  $f_1$  与  $f_i$  互素,  $f_2$  与  $f_i$  互素…… $f_{i-1}$  与  $f_i$  互素, 故  $f_1 \cdot f_2 \cdots f_{i-1}$  与  $f_i$  互素. ✎

**评注** 设六多项式  $f_1, f_2, \dots, f_6$  PRP. 作者问:  $f_1 f_4 f_6$  与  $f_3$  互素吗? 当然了. 为什么呢?

既然  $f_1, f_2, \dots, f_6$  PRP, 那么  $f_1, f_4, f_6, f_3, f_2, f_5$  也 PRP, 对不对? 令  $g_1 = f_1, g_2 = f_4, g_3 = f_6, g_4 = f_3, g_5 = f_2, g_6 = f_5$ , 则  $g_1, g_2, \dots, g_6$  PRP. 所以, 根据刚证过的命题,  $g_1 g_2 g_3$  与  $g_4$  互素. 因为  $g_1 g_2 g_3 = f_1 f_4 f_6, g_4 = f_3$ , 故  $f_1 f_4 f_6$  与  $f_3$  互素.

本评注的目的是告诉读者, 不要死学作者所讲述的知识. 读者要灵活运用所学的知识, 并逐渐适应“显然”“当然”等词语. 的确, 作者可以写得更详细, 但这没有必要. “学而不思则罔, 思而不学则殆.” 读者一定要边学边想! 还有, 如果读者真地想学作者讲述的知识, 作者建议读者不要狼吞虎咽. 相信作者; 作者不会害读者的!<sup>†</sup>

**命题** 设多项式  $f_1, f_2, \dots, f_n$  PRP. 若  $f_1, f_2, \dots, f_i$  都是  $f$  的因子, 则  $f_1 f_2 \cdots f_i$  也是  $f$  的因子 ( $i$  是  $1, 2, \dots, n$  中的数). 特别地,  $i = n$  时,  $f_1 f_2 \cdots f_n$  是  $f$  的因子.

**证** 用数学归纳法.  $i = 1$  时, 显然. 设  $f_1 f_2 \cdots f_{i-1}$  是  $f$  的因子 (归纳假设). 因为  $f_i$  也是  $f$  的因子, 且  $f_1 f_2 \cdots f_{i-1}$  与  $f_i$  互素, 故  $f_1 f_2 \cdots f_{i-1} \cdot f_i$  也是  $f$  的因子. ✎

---

现在, 我们讨论不可约的多项式.

**定义** 设多项式  $f$  既不是 0, 也不是单位.

(i) 若存在二个不全为单位的多项式  $f_1, f_2$  使  $f = f_1 f_2$ , 则  $f$  是可约的 (*reducible*).

(ii) 若  $f$  不是可约的, 则说  $f$  是不可约的 (*irreducible*). 换言之, 若  $f$  是不可约的, 则“多项式  $f_1, f_2$  使  $f = f_1 f_2$ ”可推出“ $f_1$  是单位或  $f_2$  是单位”.

**评注** 0 或单位既不是可约的, 也不是不可约的.

---

<sup>†</sup>敏锐的读者应该注意到了: 此评注是从“整数的一些性质”复制过来的; “六整数”被替换为“六多项式”; 别的没变.

**例** 设  $t$  是数. 则  $x - t$  是不可约的.

设多项式  $f_1, f_2$  适合  $f_1 f_2 = x - t$ . 所以,  $\deg f_1 + \deg f_2 = \deg(x - t) = 1$ .

$f_1$  与  $f_2$  当然是非零的. 这样,  $\deg f_1$  与  $\deg f_2$  都是非负整数. 所以,  $\deg f_1$  与  $\deg f_2$  必定有一个是 0, 另一个是 1. 不妨假设  $\deg f_1 = 0$ . 所以  $f_1$  是非零数. 所以  $f_1$  是单位. 类似地, 若  $\deg f_2 = 0$ , 则  $f_2$  是单位.

不管怎么样, 我们已经证明了 “多项式  $f_1, f_2$  使  $x - t = f_1 f_2$ ” 可推出 “ $f_1$  是单位或  $f_2$  是单位”. 这样,  $x - t$  是不可约的.

**例**  $x^2 - 1$  是可约的:  $x^2 - 1 = (x + 1)(x - 1)$ , 而  $x + 1$  不是单位,  $x - 1$  也不是单位.

**评注** 作者在此有必要提醒读者: 不可约的多项式与多项式的系数所在范围密切相关.

我们看  $f = x^2 - 2$ . 显然, 读者在中学可能已经知道, “这没法再 (在有理数范围里) ‘分解’ 了”. 的确,  $f$  作为有理系数多项式是不可约的. 不过, 如果视  $f$  为实系数多项式, 则可继续将  $f$  写为  $(x + \sqrt{2})(x - \sqrt{2})$ . 类似地, 若视  $g = x^2 + 1$  为实系数多项式, 则  $g$  “也没办法再 (在实数范围里) ‘分解’ 了”. 可是, 若视  $g$  为复系数多项式, 则  $g = (x + i)(x - i)$ .

所以, 除非语境明确 (或者系数所在范围无关紧要), 我们总是说 “某多项式作为有理 (实、复) 系数多项式是不可约的”.

**命题** 设多项式  $p$  既不是 0, 也不是单位. 设  $\varepsilon$  是单位. 若  $p$  是不可约的, 则  $\varepsilon p$  也是不可约的.

**证** 设二多项式  $f_1, f_2$  使  $\varepsilon p = f_1 f_2$ . 所以,  $p = (\varepsilon^{-1} f_1)(f_2)$ . 因为  $p$  是不可约的, 故  $\varepsilon^{-1} f_1$  是单位或  $f_2$  是单位. 这也就是说,  $f_1$  是单位或  $f_2$  是单位. 所以,  $\varepsilon p$  是不可约的. ✎

**例** 由上个命题可知: 1 次多项式一定是不可约的.

**命题** 设多项式  $p$  既不是 0, 也不是单位. 下述四命题等价:

- (i) 若多项式  $f_1, f_2$  使  $f = f_1 f_2$ , 则  $f_1$  是单位或  $f_2$  是单位;
- (ii) 对任意多项式  $f$ , 要么  $p$  是  $f$  的因子, 要么  $p$  与  $f$  互素 (二者不会同时发生);

(iii) 若  $f, g$  是多项式, 且  $p$  是  $fg$  的因子, 则  $p$  是  $f$  的因子, 或  $p$  是  $g$  的因子;

(iv) 不存在多项式  $f_1, f_2$  使  $p = f_1 f_2$ , 且  $\deg f_1 < \deg p, \deg f_2 < \deg p$ .

**证** (i)  $\Rightarrow$  (ii): 任取多项式  $f$ . 设  $d$  是  $p$  与  $f$  的最大公因子. 所以, 存在多项式  $g$  使  $p = dg$ . 所以,  $d$  是单位或  $g$  是单位. 若  $d$  是单位, 则单位是  $p$  与  $f$  的最大公因子, 即  $p$  与  $f$  互素; 若  $g$  是单位, 则  $d = pg^{-1}$ , 故  $p$  是  $f$  的因子.

若二者同时发生, 则  $d$  是单位且  $g$  是单位, 故  $p$  也是单位. 这与  $p$  不是单位矛盾.

(ii)  $\Rightarrow$  (iii): 若  $p$  是  $f$  的因子, 则不必证了. 今假设  $p$  不是  $f$  的因子. 所以,  $p$  与  $f$  互素. 因为  $p$  是  $fg$  的因子, 故  $p$  一定是  $g$  的因子.

(iii)  $\Rightarrow$  (iv): 反证法. 设  $p = f_1 f_2$ , 且  $\deg f_1 < \deg p, \deg f_2 < \deg p$ . 因为  $p \neq 0$ , 故  $f_1 \neq 0$ , 且  $f_2 \neq 0$ . 所以,  $\deg f_1 \geq 0$ , 且  $\deg f_2 \geq 0$ . 既然  $p = f_1 f_2$ ,  $p$  当然是  $f_1 f_2$  的因子. 所以,  $p$  是  $f_1$  的因子, 或  $p$  是  $f_2$  的因子. 若  $p$  是  $f_1$  的因子, 则存在多项式  $g_1$  使  $f_1 = pg_1$ . 因为  $f_1 \neq 0$ , 故  $g_1 \neq 0$ . 这样,  $\deg g_1 \geq 0$ . 所以  $\deg f_1 = \deg p + \deg g_1 \geq \deg p$ . 这与假定  $\deg f_1 < \deg p$  矛盾! 类似地, 若  $p$  是  $f_2$  的因子, 也有  $\deg f_2 \geq \deg p$ , 矛盾! 综上, 这样的  $f_1$  与  $f_2$  不存在.

(iv)  $\Rightarrow$  (i): 这说明: 若多项式  $f_1, f_2$  使  $p = f_1 f_2$ , 则  $\deg f_1 \geq \deg p$  或  $\deg f_2 \geq \deg p$ . 若  $\deg f_1 \geq \deg p$ , 则  $\deg p = \deg f_1 + \deg f_2 \geq \deg p + \deg f_2$ , 故  $\deg f_2 \leq 0$ , 即  $f_2$  是非零数, 即  $f_2$  是单位. 类似地, 若  $\deg f_2 \geq \deg p$ , 则  $f_1$  是单位. ✎

**评注** 利用 (iii) 与数学归纳法, 读者可得如下结论 (作为练习):

设  $f_1, f_2, \dots, f_n$  是多项式. 设多项式  $p$  是不可约的. 若  $p$  是  $f_1 f_2 \cdots f_n$  的因子, 则存在 1 至  $n$  间的整数  $\ell$ , 使  $p$  是  $f_\ell$  的因子.

**评注** 设多项式  $f$  既不是 0, 也不是单位. (iv) 表明, “ $f$  是可约的” 的一个必要与充分条件是 “存在二个多项式  $f_1, f_2$ , 使  $f = f_1 f_2$ , 且  $\deg f_1 < \deg f, \deg f_2 < \deg f$ ”.

事实上,  $\deg f_1 \geq 1$ , 且  $\deg f_2 \geq 1$ . 反证法. 设  $\deg f_1 < 1$ . 因为  $f \neq 0$ , 故  $f_1 \neq 0$ , 即  $\deg f_1 \geq 0$ . 所以  $\deg f_1 = 0$ . 所以  $\deg f_2 = 0 + \deg f_2 =$

$\deg f_1 + \deg f_2 = \deg f > \deg f_2$ . 这是矛盾! 类似地, 若  $\deg f_2 < 1$ , 则  $\deg f_1 = \deg f > \deg f_1$ . 这也是矛盾.

综上, 我们得到了一个更好用的命题: “ $f$  是可约的” 的一个必要与充分条件是 “存在二个多项式  $f_1, f_2$ , 使  $f = f_1 f_2$ , 且  $1 \leq \deg f_1 < \deg f$ ,  $1 \leq \deg f_2 < \deg f$ ”.

**评注** 设  $p, q$  是不可约的多项式. 要么  $p$  是  $q$  的相伴, 要么  $p$  与  $q$  互素 (二者不会同时发生).

为什么呢? 若  $p$  与  $q$  互素, 则不必论证了. 所以, 我们假定  $p$  与  $q$  不互素. 所以  $p$  一定是  $q$  的因子 (因为  $p$  是不可约的), 且  $q$  一定是  $p$  的因子 (因为  $q$  是不可约的). 所以,  $p$  与  $q$  相伴.

若  $p$  与  $q$  相伴, 且  $p$  与  $q$  互素, 则有单位  $\varepsilon$  使  $q = p\varepsilon$ . 故  $p$  是  $p$  与  $q$  的公因子. 从而  $p$  是单位的因子. 所以  $p$  是单位. 这跟  $p$  是不可约的矛盾!

下面是关于不可约的多项式的积的命题.

**命题** 设多项式  $p_1, p_2, \dots, p_m, q_1, q_2, \dots, q_n$  都是不可约的. 设

$$p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n.$$

(i)  $m = n$ ;

(ii) 可以适当调换  $q_1, q_2, \dots, q_m$  (注意,  $n = m$ ) 的顺序, 使任取 1 至  $m$  间的整数  $\ell$ ,  $p_\ell$  与  $q_\ell$  相伴 (注意: 调换顺序后的  $q_\ell$  不一定跟原来的  $q_\ell$  相等!).

**证** 对等式左侧的不可约的多项式的数目  $m$  用数学归纳法. 当  $m = 1$  时, 有

$$p_1 = q_1 q_2 \cdots q_n.$$

先证明:  $n = 1$ . 反证法. 设  $n > 1$ . 因为  $p_1 = q_1 q_2 \cdots q_n$ , 故  $p_1$  是某个  $q_i$  的因子 ( $i$  是某个 1 至  $n$  间的整数). 因为乘法可交换, 不失一般性, 设  $p_1$  是  $q_1$  的因子. 因为  $q_1$  是不可约的, 且  $q_1$  与  $p_1$  不是互素的, 故  $q_1$  也是  $p_1$  的因子. 所以, 存在单位  $\varepsilon$  使  $q_1 = \varepsilon p_1$ . 进而

$$p_1 = (\varepsilon p_1) q_2 \cdots q_n = p_1 (\varepsilon q_2) \cdots q_n.$$



因为  $p_1 \neq 0$ , 故可从等式二边消去  $p_1$ , 即

$$1 = (\varepsilon q_2) \cdots q_n.$$

因为  $q_2$  是不可约的, 故  $\varepsilon q_2$  也是不可约的. 上式表明,  $\varepsilon q_2$  是 1 的因子, 故  $\varepsilon q_2$  是单位. 这与假定矛盾! 所以,  $n$  不可高于 1. 这样,  $n = 1$ .

既然  $n = 1$ , 那么  $p_1 = q_1$ . 所以, 不必调换顺序即可知  $p_1$  与  $q_1$  相伴.

所以,  $m = 1$  时, 命题成立.

假定  $m = k$  时, 命题成立. 现在看  $m = k + 1$  时的情形. 设  $p_1, p_2, \cdots, p_k, p_{k+1}, q_1, q_2, \cdots, q_n$  是不可约的. 设

$$p_1 p_2 \cdots p_k p_{k+1} = q_1 q_2 \cdots q_n.$$

因为  $p_1$  是  $q_1 q_2 \cdots q_n$  的因子, 故  $p_1$  是某个  $q_j$  的因子 ( $j$  是某个 1 至  $n$  间的整数). 因为乘法可交换, 不失一般性, 设  $p_1$  是  $q_1$  的因子. 因为  $q_1$  是不可约的, 且  $q_1$  与  $p_1$  不是互素的, 故  $q_1$  也是  $p_1$  的因子. 所以, 存在单位  $\varepsilon'$  使  $q_1 = \varepsilon' p_1$ . 进而

$$p_1 p_2 \cdots p_k p_{k+1} = (\varepsilon' p_1) q_2 \cdots q_n = p_1 (\varepsilon' q_2) \cdots q_n.$$

因为  $p_1 \neq 0$ , 故可从等式二边消去  $p_1$ , 即

$$p_2 \cdots p_k p_{k+1} = (\varepsilon' q_2) \cdots q_n.$$

因为  $q_2$  是不可约的, 故  $\varepsilon' q_2$  也是不可约的. 上式左侧的不可约的多项式的数目是  $k$ . 根据归纳假设,  $n - 1 = k$ , 即  $n = k + 1$ . 这证明了  $m = k + 1$  时 (i) 成立.

前面已证得, 适当地调换  $q_1, q_2, \cdots, q_n$  的顺序, 可使  $p_1$  与  $q_1$  相伴. 根据归纳假设, 可以适当地调换  $\varepsilon' q_2, \cdots, q_{k+1}$  (注意,  $n = k + 1$ ) 的顺序, 使任取 3 至  $k + 1$  间的整数  $u$ ,  $p_u$  与  $q_u$  相伴. 当然  $p_2$  与  $\varepsilon' q_2$  也相伴. 因为  $\varepsilon' q_2$  与  $q_2$  相伴, 所以  $p_2$  与  $q_2$  相伴. 把这些事实放在一块儿, 就是: 可以适当地调换  $q_1, q_2, \cdots, q_{k+1}$  的顺序, 使任取 1 至  $k + 1$  间的整数  $\ell$ ,  $p_\ell$  与  $q_\ell$  相伴. 这样,  $m = k + 1$  时, (ii) 成立.  $\clubsuit$

**命题** 设多项式  $f$  既不是 0, 也不是单位. 存在不可约的多项式  $p_1, p_2, \cdots, p_m$  使

$$f = p_1 p_2 \cdots p_m.$$

**证** 对  $f$  的次  $N$  用数学归纳法. 因为  $f$  既不是 0, 也不是单位, 故  $N \geq 1$ .  $N = 1$  时,  $f = ax + b$ , 这里  $a, b$  是数, 且  $a \neq 0$ . 我们已经知道, 1 次多项式是不可约的. 这样,  $f$  是不可约的, 故存在不可约的多项式  $p_1 = f$  使  $f = p_1$ . 这样,  $N = 1$  时, 命题成立.

设  $N \leq k$  ( $k \geq 1$ ) 时, 命题成立. 考虑  $N = k + 1$ . 若  $f$  是不可约的, 则存在不可约的多项式  $p_1 = f$  使  $f = p_1$ . 若  $f$  是可约的, 则存在二多项式  $f_1, f_2$ , 使  $f = f_1 f_2$ , 且  $1 \leq \deg f_1 < \deg f$ ,  $1 \leq \deg f_2 < \deg f$ . 所以  $\deg f_1 \leq \deg f - 1 = k$ ,  $\deg f_2 \leq \deg f - 1 = k$ . 根据归纳假设, 存在不可约的多项式  $p_1, p_2, \dots, p_i, p_{i+1}, p_{i+2}, \dots, p_m$  使

$$f_1 = p_1 p_2 \cdots p_i, \quad f_2 = p_{i+1} p_{i+2} \cdots p_m.$$

所以

$$f = f_1 f_2 = p_1 p_2 \cdots p_i p_{i+1} p_{i+2} \cdots p_m.$$

故  $N = k + 1$  时, 命题也成立. ✎

合并上二个命题, 可得

**命题** 设多项式  $f$  既不是 0, 也不是单位.

(i) 存在不可约的多项式  $p_1, p_2, \dots, p_m$  使

$$f = p_1 p_2 \cdots p_m;$$

(ii) 若  $q_1, q_2, \dots, q_m, s_1, s_2, \dots, s_n$  是不可约的多项式, 且

$$f = q_1 q_2 \cdots q_m = s_1 s_2 \cdots s_n,$$

则  $m = n$ , 且可以适当地调换  $s_1, s_2, \dots, s_m$  的顺序, 使任取 1 至  $m$  间的整数  $\ell$ ,  $q_\ell$  与  $s_\ell$  相伴 (注意: 调换顺序后的  $s_\ell$  不一定跟原来的  $s_\ell$  相等!).

设多项式  $f$  既不是 0, 也不是单位. 利用上个命题, 我们可以方便地定出  $f$  的因子.

**命题** 设多项式  $f$  既不是 0, 也不是单位. 设  $p_1, p_2, \dots, p_m$  是不可约的多项式, 且

$$f = p_1 p_2 \cdots p_m.$$

$f$  的因子必为

$$(\star) \quad \varepsilon p_{j_1} p_{j_2} \cdots p_{j_s},$$

其中  $\varepsilon$  是单位,  $j_1, j_2, \dots, j_s$  是  $1, 2, \dots, m$  中  $s$  个不同的数 ( $s$  可取 0; 此时, 这就是单位).

**证** 从  $1, 2, \dots, m$  中选出  $s$  个不同的数  $j_1, j_2, \dots, j_s$ , 那么还剩  $m - s$  个数未被挑选. 记这  $m - s$  个数为  $j_{s+1}, \dots, j_m$ . 由于

$$\begin{aligned} f &= p_1 p_2 \cdots p_m \\ &= (p_{j_1} p_{j_2} \cdots p_{j_s})(p_{j_{s+1}} \cdots p_{j_m}) \\ &= (\varepsilon p_{j_1} p_{j_2} \cdots p_{j_s})(\varepsilon^{-1} p_{j_{s+1}} \cdots p_{j_m}), \end{aligned}$$

且  $\varepsilon^{-1} p_{j_{s+1}} \cdots p_{j_m}$  是多项式, 故  $\varepsilon p_{j_1} p_{j_2} \cdots p_{j_s}$  是  $f$  的因子.

设  $g$  是  $f$  的因子. 我们证明:  $g$  一定能写为  $(\star)$  的形式.

首先,  $g$  一定不是 0. 若  $g$  是单位, 取  $s = 0$ ,  $g$  即可写为  $(\star)$  的形式. 现在设  $g$  既不是 0, 也不是单位.

设多项式  $h$  使  $f = gh$ .  $h$  当然不是 0. 若  $h$  是单位, 则

$$g = h^{-1}f = h^{-1}p_1 p_2 \cdots p_m.$$

$h^{-1}$  也是单位, 且  $1, 2, \dots, m$  当然是  $1, 2, \dots, m$  中  $m$  个不同的数.

若  $h$  不是单位, 则存在不可约的多项式  $q_1, q_2, \dots, q_s, q_{s+1}, \dots, q_n$  使

$$g = q_1 q_2 \cdots q_s, \quad h = q_{s+1} \cdots q_n.$$

所以

$$f = gh = q_1 q_2 \cdots q_s q_{s+1} \cdots q_n.$$

从而  $n = m$ , 且可以适当地调换  $p_1, p_2, \dots, p_m$  的顺序, 使任取  $1, 2, \dots, m$  中的数  $\ell$ ,  $q_\ell$  与  $p_\ell$  相伴. 但是, 我们注意到, 调换后的  $p_\ell$  跟题设的  $p_\ell$  不一定是相等的, 所以我们稍微变通一下.

我们把  $s$  个不可约的多项式  $q_1, q_2, \dots, q_s$  写在左边, 把  $m$  个不可约的多项式  $p_1, p_2, \dots, p_m$  写在右边:

$$q_1, q_2, \dots, q_s; \quad p_1, p_2, \dots, p_m.$$

对  $q_1$  而言, 肯定有整数  $j_1$  使  $q_1$  不与  $p_i$  ( $i < j_1$ ) 相伴 (从左向右看诸  $p_\ell$  即可), 但  $q_1$  与  $p_{j_1}$  相伴. 也就是说, 存在单位  $\varepsilon_1$  使  $q_1 = \varepsilon_1 p_{j_1}$ . 去掉左边的  $q_1$  与右边的  $p_{j_1}$ , 有

$$q_2, \dots, q_s; \quad p_1, \dots, p_{j_1-1}, p_{j_1+1}, \dots, p_m.$$

类似地, 对  $q_2$  而言, 肯定有整数  $j_2$  使  $q_2$  不与  $p_i$  ( $i < j_2, i \neq j_1$ ) 相伴, 但  $q_2$  与  $p_{j_2}$  相伴. 也就是说, 存在单位  $\varepsilon_2$  使  $q_2 = \varepsilon_2 p_{j_2}$ .

反复地执行此事, 可知: 存在  $1, 2, \dots, m$  中  $s$  个不同的数  $j_1, j_2, \dots, j_s$ , 存在  $s$  个单位  $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_s$  使  $q_\ell = \varepsilon_\ell p_{j_\ell}$ . 所以

$$\begin{aligned} f &= q_1 q_2 \cdots q_s \\ &= (\varepsilon_1 p_{j_1})(\varepsilon_2 p_{j_2}) \cdots (\varepsilon_s p_{j_s}) \\ &= (\varepsilon_1 \varepsilon_2 \cdots \varepsilon_s) p_{j_1} p_{j_2} \cdots p_{j_s} \\ &= \varepsilon p_{j_1} p_{j_2} \cdots p_{j_s}. \end{aligned} \quad \clubsuit$$

我们以一个简单的命题结束本文.

**命题** 设  $f_1, f_2, \dots, f_n$  是多项式.  $f_1, f_2, \dots, f_n$  互素的一个必要与充分条件是: 任取不可约的多项式  $p$ , 存在某个  $f_i$ , 使  $p$  不是  $f_i$  的因子.

**证** 先看必要性. 反证法. 假定结论不成立, 即: 存在不可约的多项式  $p$ , 使任取  $f_i$ ,  $p$  是  $f_i$  的因子. 这样,  $p$  就是  $f_1, f_2, \dots, f_n$  的公因子. 所以,  $p$  是单位的因子. 矛盾!

再看充分性. 还是反证法. 假定结论不成立, 即: 设  $d$  是  $f_1, f_2, \dots, f_n$  的最大公因子, 且  $d$  不是单位. 若  $d$  是 0, 则  $f_1, f_2, \dots, f_n$  全是 0, 故任意的不可约的多项式都是  $f_1, f_2, \dots, f_n$  的公因子, 矛盾! 若  $d$  不是 0, 也不是单位, 那么一定存在不可约的多项式  $p_0$ , 使  $p_0$  是  $d$  的因子. 所以, 存在不可约的多项式  $p_0$ , 使任取  $f_i$ ,  $p_0$  是  $f_i$  的因子. 矛盾!  $\clubsuit$

**评注** 作者说一件不是很重要事. 事实上, 本文改编自“整数的一些性质”. 作者干了这么几件事: (i) 将大量的“整数”替换为“多项式”; (ii) 修改一些细节; (iii) 修改了几个例. (i) 是最容易的, 而 (iii) 是最繁的.

本文就到这里. 再见, 亲爱的读者朋友!

## 综合除法

本文的目标是为读者介绍带余除法的一个特殊情况——综合除法 (*synthetic division*). 当然, 细心的读者一定不会只学到综合除法.

还是老样子: “数”一定是复数 (或实数、有理数); “多项式”的系数一定是数.

前面, 我们讨论了多项式的一些性质. 我们没有在“查考多项式”里讨论那些性质, 是因为当时我们不需要“因子”“公因子”“最大公因子”等概念. 读者应该还记得, 多项式的微商、多项式的根、插值、广义二项系数、求和公式等内容是我们讨论的重点. 现在, 我们的方向变了很多.

在讨论多项式的根时, 我们曾经为读者介绍过这个命题:

**命题** 设  $f(x)$  是  $n$  次多项式 ( $n \geq 1$ ),  $a$  是数. 则存在  $n-1$  次多项式  $q(x)$  使

$$f(x) = q(x)(x - a) + f(a).$$

根据带余除法, 这样的  $q(x)$  一定是唯一的.

这是带余除法的推论. 我们当时并不关心  $q(x)$  是什么; 我们只关心这个  $q(x)$  不但存在, 且唯一. 我们用它建立了多项式与多项式函数的联系: (系数为数的) 多项式与多项式函数没有本质区别. 但现在, 我们不但关心  $q(x)$  到底是什么, 我们还要给出一种方便计算  $q(x)$  的方法——这就是综合除法所干的事情.

综合除法, 原则上, 当然也可以放在“多项式的一些性质”里讨论. 不过, 作者为了让“整数的一些性质”与“多项式的一些性质”的结构一致, 作者决定专门写二篇文讨论多项式独有的东西: 综合除法与重因子. 这么安排, 还有一个好处: 消除了过长的文给读者带来的压力.

**例** 设  $f(x) = x^6 + x^3 + 1$ . 我们计算  $x-2$  除  $f(x)$ .

我们先用普通的带余除法试试看. 显然,  $\deg(x-2) = 1$ . 这里,  $x-2$  的首项系数为 1, 所以我们的计算并不会很复杂. 取

$$q_1(x) = 1 \cdot 1^{-1} \cdot x^{6-1} = x^5.$$

则

$$\begin{aligned}
 r_1(x) &= f(x) - q_1(x)(x-2) \\
 &= (x^6 + x^3 + 1) - x^5(x-2) \\
 &= (x^6 + x^3 + 1) - (x^6 - 2x^5) \\
 &= 2x^5 + x^3 + 1.
 \end{aligned}$$

$r_1(x)$  的次仍不低于 1. 因此, 再来一次. 取

$$q_2(x) = 2 \cdot 1^{-1} \cdot x^{5-1} = 2x^4.$$

则

$$\begin{aligned}
 r_2(x) &= r_1(x) - q_2(x)(x-2) \\
 &= (2x^5 + x^3 + 1) - 2x^4(x-2) \\
 &= (2x^5 + x^3 + 1) - (2x^5 - 4x^4) \\
 &= 4x^4 + x^3 + 1.
 \end{aligned}$$

$r_2(x)$  的次仍不低于 1. 因此, 再来一次. 取

$$q_3(x) = 4 \cdot 1^{-1} \cdot x^{4-1} = 4x^3.$$

则

$$\begin{aligned}
 r_3(x) &= r_2(x) - q_3(x)(x-2) \\
 &= (4x^4 + x^3 + 1) - 4x^3(x-2) \\
 &= (4x^4 + x^3 + 1) - (4x^4 - 8x^3) \\
 &= 9x^3 + 1.
 \end{aligned}$$

$r_3(x)$  的次仍不低于 1. 因此, 再来一次. 取

$$q_4(x) = 9 \cdot 1^{-1} \cdot x^{3-1} = 9x^2.$$

则

$$\begin{aligned}
 r_4(x) &= r_3(x) - q_4(x)(x-2) \\
 &= (9x^3 + 1) - 9x^2(x-2) \\
 &= (9x^3 + 1) - (9x^3 - 18x^2) \\
 &= 18x^2 + 1.
 \end{aligned}$$

$r_4(x)$  的次仍不低于 1. 因此, 再来一次. 取

$$q_5(x) = 18 \cdot 1^{-1} \cdot x^{2-1} = 18x.$$

则

$$\begin{aligned} r_5(x) &= r_4(x) - q_5(x)(x-2) \\ &= (18x^2 + 1) - 18x(x-2) \\ &= (18x^2 + 1) - (18x^2 - 36x) \\ &= 36x + 1. \end{aligned}$$

$r_5(x)$  的次仍不低于 1. 因此, 再来一次. 取

$$q_6(x) = 36 \cdot 1^{-1} \cdot x^{1-1} = 36.$$

则

$$\begin{aligned} r_6(x) &= r_5(x) - q_6(x)(x-2) \\ &= (36x + 1) - 36(x-2) \\ &= (36x + 1) - (36x - 72) \\ &= 73. \end{aligned}$$

$r_6(x)$  的次低于 1. 这样

$$\begin{aligned} f(x) &= q_1(x)(x-2) + r_1(x) \\ &= q_1(x)(x-2) + q_2(x)(x-2) + r_2(x) \\ &= q_1(x)(x-2) + q_2(x)(x-2) + q_3(x)(x-2) + r_3(x) \\ &= q_1(x)(x-2) + q_2(x)(x-2) + q_3(x)(x-2) + q_4(x)(x-2) + r_4(x) \\ &= q_1(x)(x-2) + q_2(x)(x-2) + q_3(x)(x-2) + q_4(x)(x-2) \\ &\quad + q_5(x)(x-2) + r_5(x) \\ &= q_1(x)(x-2) + q_2(x)(x-2) + q_3(x)(x-2) + q_4(x)(x-2) \\ &\quad + q_5(x)(x-2) + q_6(x)(x-2) + r_6(x) \\ &= (q_1(x) + q_2(x) + q_3(x) + q_4(x) + q_5(x) + q_6(x))(x-2) + r_6(x) \\ &= (x^5 + 2x^4 + 4x^3 + 9x^2 + 18x + 36)(x-2) + 73. \end{aligned}$$

也就是说,

$$q(x) = x^5 + 2x^4 + 4x^3 + 9x^2 + 18x + 36, \quad f(2) = r_6(x) = 73.$$

读者可能感到疲劳. 的确, 作者自己都快要睡着了. 这些文字打出来, 作者可再算九遍了吧.

设  $a$  为数. 我们用  $x-a$  除  $f(x)$ . 设  $f(x)$  的次为  $n$ , 且  $n \geq 1$  (若  $n < 1$ , 则  $x-a$  除  $f(x)$  的商与余式分别是  $0$  与  $f(x)$ ). 所以, 商的次是  $n-1$ , 且余式 (可认为) 是数. 这样, 我们可以待定系数. 具体地说, 设

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

且

$$f(x) = (x-a)(b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_0) + b_{-1}.$$

上式可写为

$$\begin{aligned} f(x) &= b_{n-1}x^n + (b_{n-2} - ab_{n-1})x^{n-1} + \cdots + (b_{j-1} - ab_j)x^j \\ &\quad + \cdots + (b_0 - ab_1)x + (b_{-1} - ab_0). \end{aligned}$$

比较系数, 有

$$\begin{aligned} a_n &= b_{n-1}, \\ a_{n-1} &= b_{n-2} - ab_{n-1}, \\ &\dots\dots\dots, \\ a_j &= b_{j-1} - ab_j \quad (0 \leq j < n), \\ &\dots\dots\dots, \\ a_1 &= b_0 - ab_1, \\ a_0 &= b_{-1} - ab_0. \end{aligned}$$

由此解出

$$\begin{aligned} (R) \quad &b_{n-1} = a_n, \\ &b_{j-1} = ab_j + a_j \quad (j = n-1, n-2, \dots, 0). \end{aligned}$$



**评注** 或许, 读者觉得  $b_{j-1} = ab_j + a_j$  的右侧还有“未知的”  $b_j$ , 因此作者“并没有解出  $b_{n-1}, b_{n-2}, \dots, b_0, b_{-1}$ ”. 事实上, 作者在后面也写了,  $j$  取  $n-1, n-2, \dots, 0$ . 因为  $b_{n-1}$  已知 (它就是  $a_n$ ), 故可求出  $b_{n-2} = ab_{n-1} + a_{n-1} = a_n a + a_{n-1}$ . 所以, 读者可接着求出  $b_{n-3} = ab_{n-2} + a_{n-2} = a_n a^2 + a_{n-1} a + a_{n-2}$ . 也就是说,  $b_{n-1}, b_{n-2}, \dots, b_0, b_{-1}$  是按次序被求出的数. 当然, 作者知道, 肯定有读者不服. 作为参考, 作者也给出一个直接的表达式.

一般地,  $b_{n-1}, b_{n-2}, \dots, b_0, b_{-1}$  的具体的表达式如下:

$$\begin{aligned}
 & b_{n-1} = a_n, \\
 & b_{n-2} = a_n a + a_{n-1}, \\
 & b_{n-3} = a_n a^2 + a_{n-1} a + a_{n-2}, \\
 & \dots, \\
 (E) \quad & b_j = a_n a^{n-1-j} + a_{n-1} a^{n-2-j} + \dots + a_{j+1} \quad (-1 \leq j < n), \\
 & \dots, \\
 & b_0 = a_n a^{n-1} + a_{n-1} a^{n-2} + \dots + a_1, \\
 & b_{-1} = a_n a^n + a_{n-1} a^{n-1} + \dots + a_1 a + a_0.
 \end{aligned}$$

**例** 还是取  $f(x) = x^6 + x^3 + 1$ . 我们计算  $x-2$  除  $f(x)$ . 这里,  $a=2$ . 如果利用公式 (R), 则

$$\begin{aligned}
 b_5 &= a_6 = 1, \\
 b_4 &= ab_5 + a_5 = 2, \\
 b_3 &= ab_4 + a_4 = 4, \\
 b_2 &= ab_3 + a_3 = 9, \\
 b_1 &= ab_2 + a_2 = 18, \\
 b_0 &= ab_1 + a_1 = 36, \\
 b_{-1} &= ab_0 + a_0 = 73.
 \end{aligned}$$

故

$$\begin{aligned}
 f(x) &= (x-a)(b_5 x^5 + b_4 x^4 + b_3 x^3 + b_2 x^2 + b_1 x + b_0) + b_{-1} \\
 &= (x^5 + 2x^4 + 4x^3 + 9x^2 + 18x + 36)(x-2) + 73.
 \end{aligned}$$

可是, 如果用公式 (E), 则

$$\begin{aligned}
 b_5 &= a_6 = 1, \\
 b_4 &= a_6 a + a_5 = a = 2, \\
 b_3 &= a_6 a^2 + a_5 a + a_4 = a^2 = 4, \\
 b_2 &= a_6 a^3 + a_5 a^2 + a_4 a + a_3 = a^3 + 1 = 9, \\
 b_1 &= a_6 a^4 + a_5 a^3 + a_4 a^2 + a_3 a + a_2 = a^4 + a = 18, \\
 b_0 &= a_6 a^5 + a_5 a^4 + a_4 a^3 + a_3 a^2 + a_2 a = a^5 + a^2 = 36, \\
 b_{-1} &= a_6 a^6 + a_5 a^5 + a_4 a^4 + a_3 a^3 + a_2 a^2 + a_1 a + a_0 \\
 &= a^6 + a^3 + 1 \\
 &= 73.
 \end{aligned}$$

结果当然是一样的. 不过, 读者是否感觉, 公式 (E) 不如公式 (R) 简单? 公式 (R) 里, 后一个数  $(b_{j-1})$  都是  $f(x)$  的某个系数  $(a_j)$  加前一个数  $(b_j)$  乘  $a$ ; 公式 (E) 里, 越到后面, 表达式越长. 作者挑选的  $f(x)$  的 1, 2, 4, 5 次系数都是 0, 所以还不是那么可怕. 但如果作者挑选的多项式的系数全都不是 0 呢?

这就是作者推荐公式 (R) 的理由.

---

下面我们来看看综合除法的应用.

读者可能已经注意到了,  $b_{-1} = f(a)$ . 这是正确的: 因为商与余式是唯一的. 所以, 如果不关心  $b_{-1}$  之前的数  $b_{n-1}, b_{n-2}, \dots, b_1, b_0$  的意义, 我们可得到计算多项式在点  $a$  的值的 Horner 算法<sup>†</sup> (*Horner's algorithm*):

**命题** 设  $a$  是数. 设  $n$  是正整数. 设

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0.$$

---

<sup>†</sup>在西方, 一般用不列颠数学家 William George Horner 的名字命名此算法; 在中国, 一般用中国数学家秦九韶的名字命名此算法. 换句话说, 在大多数汉语文献里, 此算法叫秦九韶算法.

按如下规则作  $n$  个数  $b_{n-1}, b_{n-2}, \dots, b_0, b_{-1}$ :

$$b_{n-1} = a_n,$$

$$b_{j-1} = ab_j + a_j \quad (j = n-1, n-2, \dots, 0).$$

则  $b_{-1} = f(a)$ .

**例 设**

$$f(x) = 8x^8 - 12x^7 - 2x^6 + 43x^5 - 78x^4 + 77x^3 - 46x^2 + 15x - 2.$$

设  $a = 3$ . 求  $f(a)$ .

读者可以试试直接将  $x$  替换为  $a$ . 不难看出, 计算  $a_j a^j$  需  $j+1$  次乘法 ( $j \geq 1$ ), 故直接将  $x$  替换为  $a$ , 需  $9 + 8 + 7 + \dots + 2 + 0 = 35$  次乘法. 最后, 把 9 个数相加, 需 8 次加法. 挑战有点大; 请有兴趣的读者这么算一算.

再试试上个命题所说的方法:

$$b_7 = a_8 = 8,$$

$$b_6 = ab_7 + a_7 = 12,$$

$$b_5 = ab_6 + a_6 = 34,$$

$$b_4 = ab_5 + a_5 = 145,$$

$$b_3 = ab_4 + a_4 = 357,$$

$$b_2 = ab_3 + a_3 = 1\,148,$$

$$b_1 = ab_2 + a_2 = 3\,398,$$

$$b_0 = ab_1 + a_1 = 10\,209,$$

$$b_{-1} = ab_0 + a_0 = 30\,625.$$

由此可见, 每步

$$b_{j-1} = ab_j + a_j \quad (j = 7, 6, \dots, 0)$$

需 1 次乘法与 1 次加法.  $j$  从 7 降到 0, 故有 8 步. 所以, 用此方法, 需 8 次乘法与 8 次加法.

现在, 读者应该能体会到此法的威力了.

我们还可利用综合除法得到一个很有用的乘法公式.

设  $n$  是正整数. 设

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

则

$$a_n = 1, \quad a_{n-1} = a_{n-2} = \cdots = a_1 = a_0 = 0.$$

设  $a$  是某个非零数. 设

$$f(x) = (x - a)(b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_0) + b_{-1}.$$

根据综合除法, 知

$$\begin{aligned} b_{n-1} &= a_n, \\ (\star) \quad b_{j-1} &= ab_j + a_j \quad (j = n-1, n-2, \cdots, 0). \end{aligned}$$

由于  $0 \leq j < n$  时  $a_j = 0$ , 故  $(\star)$  变为

$$b_{j-1} = ab_j.$$

二侧同乘  $a^{j-1}$ , 得

$$a^j b_j = a^{j-1} b_{j-1}, \quad 0 \leq j < n.$$

由此可知

$$a^{-1} b_{-1} = \cdots = a^{j-1} b_{j-1} = a^j b_j = a^{j+1} b_{j+1} = \cdots = a^{n-1} b_{n-1} = a^{n-1}.$$

所以

$$a^j b_j = a^{n-1}, \quad -1 \leq j < n.$$

所以

$$b_j = a^{n-1-j}, \quad -1 \leq j < n.$$

所以

$$x^n = (x - a)(x^{n-1} + ax^{n-2} + \cdots + a^{n-2}x + a^{n-1}) + a^n.$$

此式也可写为

$$x^n - a^n = (x - a)(x^{n-1} + ax^{n-2} + \cdots + a^{n-2}x + a^{n-1}).$$

我们得到了重要的乘法公式:

**命题** 设  $n$  是正整数. 设  $a$  是数, 且  $a \neq 0$ . 则

$$x^n - a^n = (x - a)(x^{n-1} + ax^{n-2} + \cdots + a^{n-2}x + a^{n-1}).$$

值得一提的是, 这个公式可推广为

**命题** 设  $f, g$  是多项式. 设  $n$  是正整数. 则

$$f^n - g^n = (f - g)(f^{n-1} + f^{n-2}g + \cdots + f^{n-i}g^{i-1} + \cdots + g^{n-1}).$$

**证** 记

$$P = f^{n-1} + f^{n-2}g + \cdots + f^{n-i}g^{i-1} + \cdots + g^{n-1}.$$

则

$$\begin{aligned} fP &= f^n + f^{n-1}g + f^{n-2}g^2 + \cdots + fg^{n-1}, \\ gP &= f^{n-1}g + f^{n-2}g^2 + \cdots + fg^{n-1} + g^n. \end{aligned}$$

从而

$$(f - g)P = fP - gP = f^n - g^n. \quad \text{☺}$$

**例** 设  $n = 2$ . 则

$$f^2 - g^2 = (f - g)(f + g).$$

这就是平方差公式. 类似地, 取  $n = 3$ . 则

$$f^3 - g^3 = (f - g)(f^2 + fg + g^2).$$

这就是立方差公式. 若把  $g$  换为  $-g$ , 则

$$\begin{aligned} f^3 - (-g)^3 &= f^3 + g^3, \\ (f - (-g))(f^2 + f(-g) + (-g)^2) &= (f + g)(f^2 - fg + g^2). \end{aligned}$$

由此可得立方和公式:

$$f^3 + g^3 = (f + g)(f^2 - fg + g^2).$$

最后, 我们以一个稍复杂的 (但有用的) 例结束本文.

**例** 设  $f, g, h$  都是多项式. 则

$$\begin{aligned} & f^3 + g^3 + h^3 - 3fgh \\ &= (f + g)(f^2 - fg + g^2) + h^3 - 3fgh \\ &= (f + g)(f^2 + 2fg + g^2 - 3fg) + h^3 - 3fgh \\ &= (f + g)(f^2 + 2fg + g^2) - (f + g)(3fg) + h^3 - 3fgh \\ &= (f + g)^3 + h^3 - (3fg(f + g) + 3fgh) \\ &= (f + g + h)((f + g)^2 - (f + g)h + h^2) - (f + g + h)(3fg) \\ &= (f + g + h)(f^2 + 2fg + g^2 - fh - gh + h^2 - 3fg) \\ &= (f + g + h) \underbrace{(f^2 + g^2 + h^2 - fg - fh - gh)}_P. \end{aligned}$$

由此, 我们得到了新的公式:

$$f^3 + g^3 + h^3 - 3fgh = (f + g + h)(f^2 + g^2 + h^2 - fg - fh - gh).$$

若假定  $f, g, h$  都是复系数多项式, 我们还可以对  $P$  下手:

$$\begin{aligned} & f^2 + g^2 + h^2 - fg - fh - gh \\ &= f^2 - 2f \cdot \frac{g+h}{2} + (g^2 - gh + h^2) \\ &= f^2 - 2f \cdot \frac{g+h}{2} + \frac{(g+h)^2}{4} + (g^2 - gh + h^2) - \left( \frac{g^2}{4} + \frac{2gh}{4} + \frac{h^2}{4} \right) \\ &= \left( f - \frac{g}{2} - \frac{h}{2} \right)^2 + \frac{3}{4}(g^2 - 2gh + h^2) \end{aligned}$$

$$\begin{aligned}
&= \left(f - \frac{g}{2} - \frac{h}{2}\right)^2 - \left(\frac{\mathrm{i}\sqrt{3}}{2}(g-h)\right)^2 \\
&= \left(f - \frac{g}{2} - \frac{h}{2} + \mathrm{i}\sqrt{3}\frac{g}{2} - \mathrm{i}\sqrt{3}\frac{h}{2}\right) \left(f - \frac{g}{2} - \frac{h}{2} - \mathrm{i}\sqrt{3}\frac{g}{2} + \mathrm{i}\sqrt{3}\frac{h}{2}\right) \\
&= \left(f + \frac{-1 + \mathrm{i}\sqrt{3}}{2}g + \frac{-1 - \mathrm{i}\sqrt{3}}{2}h\right) \left(f + \frac{-1 - \mathrm{i}\sqrt{3}}{2}g + \frac{-1 + \mathrm{i}\sqrt{3}}{2}h\right).
\end{aligned}$$

记

$$\omega = \frac{-1 + \mathrm{i}\sqrt{3}}{2}.$$

则

$$\omega^2 = \frac{(-1)^2 + 2(-1)\mathrm{i}\sqrt{3} + 3\mathrm{i}^2}{4} = \frac{-1 - \mathrm{i}\sqrt{3}}{2}.$$

故

$$\begin{aligned}
&f^2 + g^2 + h^2 - fg - fh - gh \\
&= \left(f + \frac{-1 + \mathrm{i}\sqrt{3}}{2}g + \frac{-1 - \mathrm{i}\sqrt{3}}{2}h\right) \left(f + \frac{-1 - \mathrm{i}\sqrt{3}}{2}g + \frac{-1 + \mathrm{i}\sqrt{3}}{2}h\right) \\
&= (f + \omega g + \omega^2 h)(f + \omega^2 g + \omega h).
\end{aligned}$$

所以

$$f^3 + g^3 + h^3 - 3fgh = (f + g + h)(f + \omega g + \omega^2 h)(f + \omega^2 g + \omega h).$$

感谢您的阅读.

## 重因子

本文将为读者介绍多项式的重因子.

还是老样子: “数” 一定是复数 (或实数、有理数); “多项式” 的系数一定是数.

在正式进入本文的讨论前, 作者带领读者回忆一下微商.

设

$$f = a_0 + a_1x + a_2x^2 + \cdots + a_ix^i + \cdots + a_nx^n$$

是多项式.  $f$  的微商也是多项式:

$$Df = 0 + a_1 + 2a_2x + \cdots + ia_ix^{i-1} + \cdots + na_nx^{n-1}.$$

由此可知: 若  $f$  是数, 则  $Df$  是 0; 若  $f$  的次  $n \geq 1$ , 则  $Df$  的次为  $n-1$ .

设  $a, b$  是数; 设  $f, g$  是多项式; 设  $m$  是正整数. 微商有如下运算规则:

$$D(af + bg) = aDf + bDg,$$

$$D(fg) = Df \cdot g + f \cdot Dg,$$

$$D(f^m) = mf^{m-1}Df.$$

**例** 设  $f = x^8 + x^4 + 1$ ,  $g = 3x^2 - 9x + 1$ . 不难算出

$$Df = 8x^7 + 4x^3, \quad Dg = 6x - 9.$$

(i)  $f$  与  $g$  的和:

$$f + g = x^8 + x^4 + 3x^2 - 9x,$$

故

$$D(f + g) = 8x^7 + 4x^3 + 6x - 9.$$

这恰好与  $Df + Dg$  相等.

(ii)  $f$  与  $g$  的积:

$$\begin{aligned} fg &= x^8g + x^4g + g \\ &= (3x^{10} - 9x^9 + x^8) + (3x^6 - 9x^5 + x^4) + (3x^2 - 9x + 1) \\ &= 3x^{10} - 9x^9 + x^8 + 3x^6 - 9x^5 + x^4 + 3x^2 - 9x + 1. \end{aligned}$$



故

$$D(fg) = 30x^9 - 81x^8 + 8x^7 + 18x^5 - 45x^4 + 4x^3 + 6x - 9.$$

而

$$\begin{aligned} Df \cdot g &= (8x^7 + 4x^3)(3x^2 - 9x + 1) \\ &= 24x^9 - 72x^8 + 8x^7 + 12x^5 - 36x^4 + 4x^3, \\ f \cdot Dg &= (x^8 + x^4 + 1)(6x - 9) \\ &= 6x^9 - 9x^8 + 6x^5 - 9x^4 + 6x - 9, \end{aligned}$$

故

$$Df \cdot g + f \cdot Dg = 30x^9 - 81x^8 + 8x^7 + 18x^5 - 45x^4 + 4x^3 + 6x - 9.$$

这与  $D(fg)$  一致.

(iii) 不难算出

$$\begin{aligned} (x^2 + x + 1)^2 &= x^4 + 2x^3 + 3x^2 + 2x + 1, \\ (x^2 + x + 1)^3 &= x^6 + 3x^5 + 6x^4 + 7x^3 + 6x^2 + 3x + 1, \end{aligned}$$

故

$$\begin{aligned} f^2 &= (x^8 + x^4 + 1)^2 = x^{16} + 2x^{12} + 3x^8 + 2x^4 + 1, \\ f^3 &= (x^8 + x^4 + 1)^3 = x^{24} + 3x^{20} + 6x^{16} + 7x^{12} + 6x^8 + 3x^4 + 1. \end{aligned}$$

所以

$$D(f^3) = 24x^{23} + 60x^{19} + 96x^{15} + 84x^{11} + 48x^7 + 12x^3.$$

因为

$$\begin{aligned} 3f^2Df &= 3(x^8 + x^4 + 1)^2(8x^7 + 4x^3) \\ &= 12x^3(2x^4 + 1)(x^{16} + 2x^{12} + 3x^8 + 2x^4 + 1) \\ &= 12x^3(2x^{20} + 5x^{16} + 8x^{12} + 7x^8 + 4x^4 + 1) \\ &= 24x^{23} + 60x^{19} + 96x^{15} + 84x^{11} + 48x^7 + 12x^3, \end{aligned}$$

故

$$D(f^3) = 3f^2Df.$$

温习微商后, 我们进入本文的正题.

**定义** 设  $p$  是不可约的多项式. 设  $m$  是非负整数. 设多项式  $f \neq 0$ . 若  $p^m$  是  $f$  的因子, 但  $p^{m+1}$  不是  $f$  的因子, 则  $p$  是  $f$  的  $m$  重因子<sup>†</sup>. 若  $m = 0$ ,  $p$  当然不是  $f$  的因子; 若  $m = 1$ , 则  $p$  是  $f$  的单因子 (*simple factor*); 若  $m \geq 2$ , 则  $p$  是  $f$  的重因子 (*multiple factor*).

**命题** 设  $p$  是不可约的多项式. 设  $m$  是非负整数. 设多项式  $f \neq 0$ .  $p$  是  $f$  的  $m$  重因子的一个必要与充分条件是: 存在多项式  $g$  使  $f = p^m g$ , 且  $p$  不是  $g$  的因子.

**证** 先看必要性. 设  $p$  是  $f$  的  $m$  重因子. 所以,  $p^m$  是  $f$  的因子, 也就是说, 存在多项式  $h$  使  $f = p^m h$ . 我们的目标是: 证明  $p$  不是  $h$  的因子. 用反证法. 若存在多项式  $\ell$  使  $h = p\ell$ , 则  $f = p^{m+1}\ell$ . 所以,  $p^{m+1}$  是  $f$  的因子. 不过, 既然  $p$  是  $f$  的  $m$  重因子,  $p^{m+1}$  不是  $f$  的因子. 矛盾!

再看充分性. 设多项式  $g$  使  $f = p^m g$ , 且  $p$  不是  $g$  的因子. 所以,  $p^m$  是  $f$  的因子. 我们的目标是: 证明  $p^{m+1}$  不是  $f$  的因子. 还是用反证法. 若多项式  $k$  使  $f = p^{m+1}k$ , 则  $p^{m+1}k = p^m g$ . 因为  $p \neq 0$ , 故  $p^m \neq 0$ , 从而可从等式二边消去  $p^m$ . 即  $pk = g$ . 所以,  $p$  是  $g$  的因子. 矛盾!  $\clubsuit$

**例 设**

$$f = (x+1)(x^2-3)^2(x^2+4)^3.$$

若视  $f$  为有理系数多项式, 则  $x+1$ ,  $x^2-3$ ,  $x^2+4$  都是不可约的<sup>‡</sup>. 由此易知:  $x+1$  是  $f$  的 1 重因子 (亦即单因子);  $x^2-3$  是  $f$  的 2 重因子;

<sup>†</sup> 此定义是合理的. 因为  $f \neq 0$ , 故次是非负整数  $n$ . 因为  $p$  是不可约的, 故  $p$  的次是正整数  $b$ . 若整数  $k \geq \frac{n+1}{b}$ , 则  $p^k$  的次  $bk \geq n+1 > n$ . 此时,  $p^k$  当然不是  $f$  的因子.  $p^0 = 1$  显然是  $f$  的因子. 所以, 从左向右看  $p^k, p^{k-1}, \dots, p^0$ , 必有某整数  $m$  使  $k-m$  个多项式  $p^k, p^{k-1}, \dots, p^{m+1}$  不是  $f$  的因子, 但  $p^m$  是  $f$  的因子.

<sup>‡</sup>  $x+1$  的次为 1, 故它是不可约的. 若有理系数多项式  $x^2+b$  是可约的, 则存在有理数  $s, t$  使  $x^2+b = (x-s)(x-t)$ . 比较系数, 有  $s+t=0, st=b$ . 所以  $s^2=t^2=-b$ . 当  $b=-3$  时,  $s^2=t^2=3$ . 不过, 有理数的平方一定不是 3, 故  $x^2-3$  是不可约的. 同理,  $b=4$  时,  $s^2=t^2=-4$ . 有理数的平方一定是非负的, 故  $x^2+4$  也是不可约的. 顺便一提, 因为实数的平方也是非负的, 故就算视  $x^2+4$  为实系数多项式, 它也不是可约的.

$x^2 + 4$  是  $f$  的 3 重因子;  $x^2 - 3$  与  $x^2 + 4$  都是  $f$  的重因子; 不跟  $x + 1$ ,  $x^2 - 3$  或  $x^2 + 4$  相伴的不可约的多项式都是  $f$  的 0 重因子.

若视  $f$  为实系数多项式, 则  $x + 1$ ,  $x^2 + 4$  仍是不可约的. 所以,  $x + 1$  仍为  $f$  的单因子,  $x^2 + 4$  仍为  $f$  的 3 重因子. 可是

$$x^2 - 3 = (x + \sqrt{3})(x - \sqrt{3}),$$

从而

$$f = (x + 1)(x + \sqrt{3})^2(x - \sqrt{3})^2(x^2 + 4)^3.$$

也就是说,  $x^2 - 3$  “不配当”  $m$  重因子, 此处  $m$  是任意的非负整数. 不过,  $x + \sqrt{3}$  与  $x - \sqrt{3}$  是可以的, 且它们都是  $f$  的 2 重因子.

若视  $f$  为复系数多项式, 则  $x + 1$  依旧为  $f$  的单因子.  $x + \sqrt{3}$  与  $x - \sqrt{3}$  都是  $f$  的 2 重因子. 不过,  $x^2 + 4$  是可约的:

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

所以

$$f = (x + 1)(x + \sqrt{3})^2(x - \sqrt{3})^2(x + 2i)^3(x - 2i)^3.$$

类似地,  $x^2 + 4$  也不配成为  $m$  重因子;  $x + 2i$  与  $x - 2i$  都是  $f$  的 3 重因子.

作者举本例的目的是使读者明白:  $f$  的重因子 (究竟是什么) 与系数的范围有关. 这跟之前讨论不可约的多项式时是类似的.

下面的命题是有用的.

**命题** 设  $p$  是不可约的多项式. 设多项式  $f \neq 0$ .  $p$  是  $f$  的重因子的一个必要与充分条件是:  $p^2$  是  $f$  的因子.

**证** 先看必要性. 既然  $p$  是  $f$  的重因子, 则  $p^m$  是  $f$  的因子, 这里  $m$  是某个不低于 2 的整数. 因为  $p^2$  是  $p^m$  的因子, 故  $p^2$  是  $f$  的因子.

再看充分性. 设多项式  $g$  使  $f = p^2g$ . 因为  $f \neq 0$ , 故  $g \neq 0$ . 设  $p$  是  $g$  的  $j$  重因子, 这里  $j$  是非负整数. 所以, 存在多项式  $h$  使  $g = p^j h$ , 且  $p$  不是  $h$  的因子. 故  $f = p^{2+j}h$ , 且  $p$  不是  $h$  的因子. 因为  $2 + j$  是不低于 2 的整数, 故  $p$  是  $f$  的重因子. ✎

**命题** 设  $p$  是不可约的多项式.  $p$  一定不是  $Dp$  的因子.

**证** 设  $\deg p = n$ . 因为  $p$  是不可约的, 故  $n \geq 1$ . 所以  $\deg Df = n - 1$ . 用反证法. 若  $p$  是  $Dp$  的因子, 则有 (非零) 多项式  $h$  使  $Dp = ph$ . 从而

$$n - 1 = \deg Dp = \deg p + \deg h \geq \deg p = n.$$

这是矛盾!

✎

下面的命题揭示了微商与重因子的关系.

**命题** 设  $p$  是不可约的多项式. 设  $m$  是正整数. 设多项式  $f \neq 0$ . 若  $p$  是  $f$  的  $m$  重因子, 则  $p$  是  $Df$  的  $m - 1$  重因子. 由此可见:

- (i) 若  $p$  是  $f$  的单因子 ( $m = 1$ ), 则  $p$  不是  $Df$  的因子;
- (ii) 若  $p$  是  $f$  的重因子 ( $m \geq 2$ ), 则  $p$  也是  $Df$  的因子;
- (iii)  $p$  是  $f$  的重因子的一个必要与充分条件是:  $p$  是  $f$  与  $Df$  的公因子.

**证** 设  $f = p^m g$ , 其中  $p$  不是  $g$  的因子. 从而

$$\begin{aligned} Df &= D(p^m) \cdot g + p^m \cdot Dg \\ &= mp^{m-1}Dp \cdot g + p^m \cdot Dg \\ &= p^{m-1} \underbrace{(mgDp + pDg)}_h. \end{aligned}$$

所以,  $p^{m-1}$  是  $Df$  的因子. 我们的目标是: 证明  $p$  不是  $h$  的因子.

我们先证明:  $p$  不是  $mgDp$  的因子. 用反证法. 若  $p$  是  $mgDp$  的因子, 则  $p$  是  $mg$  的因子, 或  $p$  是  $Dp$  的因子. 因为  $p$  不是  $g$  的因子, 故  $p$  也不是  $mg$  的因子 (此判断又可以用反证法来证; 这里, 作者就不赘述了). 这样,  $p$  一定是  $Dp$  的因子. 不过, 根据上个命题,  $p$  一定不是  $Dp$  的因子. 矛盾!

现在我们总算可以证明  $p$  不是  $h$  的因子了. 还是用反证法. 若  $p$  是  $h$  的因子, 则因  $p$  显然是  $pDg$  的因子, 故  $p$  是  $mgDp = h - pDg$  的因子. 这跟上段文字得到的结论矛盾!

在证明这个关系后, (i) 与 (ii) 就相当显然了. 合并 (i) (ii), 即可得 (iii).

✎

下面的命题讨论了  $f$  与  $Df$  的最大公因子. (vii) 是重要的、有用的.

**命题** 设多项式  $f \neq 0$ . 设  $p_1, p_2, \dots, p_k$  是  $f$  的重因子. 设  $p_i$  不与  $p_j$  相伴 ( $i \neq j$ ). (这说明,  $p_1, p_2, \dots, p_k$  是  $f$  的所有的“互不相伴的”重因子.) 设“若不可约的多项式  $u$  是  $f$  的重因子, 则  $u$  必跟某  $p_\ell$  相伴”是真命题 (因为  $p_1, p_2, \dots, p_k$  互不相伴, 故  $u$  只能跟一个  $p_\ell$  相伴). 设  $p_1, p_2, \dots, p_k$  分别是  $f$  的  $m_1, m_2, \dots, m_k$  重因子, 其中  $m_1, m_2, \dots, m_k$  全是不低于 2 的整数.

(i) 设  $\ell$  是 1 至  $k$  间的整数.  $M_\ell = p_\ell^{m_\ell-1}$  是  $f$  与  $Df$  的公因子.

(ii) 设  $s, t$  是 1 至  $k$  间的整数, 且  $s \neq t$ .  $M_s$  与  $M_t$  互素. 也就是说,  $M_1, M_2, \dots, M_k$  PRP.

(iii)  $M_1 M_2 \cdots M_{\ell-1}$  与  $M_\ell$  互素.

(iv)  $M = M_1 M_2 \cdots M_k$  是  $f$  与  $Df$  的公因子.

(v)  $M$  是  $f$  与  $Df$  的最大公因子.

(vi) 存在多项式  $w$  使  $f = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k} w$ , 且  $p_1, p_2, \dots, p_k$  都不是  $w$  的因子.

(vii) 设多项式  $h$  适合  $f = hM$ . 设  $p$  是不可约的多项式. 若  $p$  是  $f$  的因子, 则  $p$  是  $h$  的单因子. 也就是说,  $h$  与  $f$  有相同的不可约的因子, 但  $h$  无重因子. (显然  $h$  的因子都是  $f$  的因子; 本条有意思的地方是:  $f$  的不可约的因子一定是  $h$  的因子.)

**证** (i) 因为  $p_\ell$  是  $f$  的  $m_\ell$  重因子 ( $m_\ell \geq 2$ ), 故  $p_\ell$  是  $Df$  的  $m_\ell - 1$  重因子 ( $m_\ell - 1 \geq 1$ ). 所以  $M_\ell$  是  $f$  与  $Df$  的公因子.

(ii) 因为  $s \neq t$ , 故  $p_s$  不与  $p_t$  相伴, 从而  $p_s$  与  $p_t$  互素. 也就是说,  $p_1, p_2, \dots, p_k$  PRP. 由 PRP 的性质, 知:  $M_1, M_2, \dots, M_k$  亦 PRP.

(iii) 由 PRP 的性质, 立得.

(iv) 设  $d$  是  $f$  与  $Df$  的最大公因子. 从而  $M_1, M_2, \dots, M_k$  都是  $d$  的因子. 由 PRP 的性质, 知:  $M$  是  $d$  的因子. 故  $M$  当然是  $f$  与  $Df$  的公因子.

(v) 设  $d$  是  $f$  与  $Df$  的最大公因子. 由 (iv) 知,  $M$  是  $d$  的因子. 所以, 存在多项式  $g$  使  $d = Mg$ . 因为  $f \neq 0$ , 故  $d \neq 0$ , 从而  $g \neq 0$ . 我们证明:  $g$  一定是单位. 此时,  $d$  与  $M$  相伴, 故  $M$  也是  $f$  与  $Df$  的最大公因子.

用反证法. 若  $g$  不是单位, 则存在某个不可约的多项式  $q'$  使  $q'$  是  $g$  的因子. 当然,  $q'$  是  $d$  的因子, 故  $q'$  是  $f$  与  $Df$  的公因子. 所以,  $q'$  是  $f$  的重因子. 所以,  $q'$  与某个  $p_\ell$  相伴. 从而必有单位  $\varepsilon$  使  $q' = \varepsilon p_\ell$ . 所以,  $p_\ell$  是  $g$

的因子. 因为  $M_\ell$  是  $M$  的因子, 故  $p_\ell^{m_\ell-1}p_\ell = p_\ell^{m_\ell}$  是  $Mg = d$  的因子. 所以  $p_\ell^{m_\ell}$  是  $Df$  的因子. 这跟  $p_\ell$  是  $Df$  的  $m_\ell - 1$  重因子矛盾!

(vi) 因为  $p_1, p_2, \dots, p_k$  PRP, 故  $p_1^{m_1}, p_2^{m_2}, \dots, p_k^{m_k}$  亦 PRP.  $p_1^{m_1}, p_2^{m_2}, \dots, p_k^{m_k}$  都是  $f$  的因子, 故  $p_1^{m_1} \cdot p_2^{m_2} \cdots p_k^{m_k}$  是  $f$  的因子. 所以, 存在多项式  $w$  使  $f = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k} w$ .

现在我们说明, 每个  $p_\ell$  都不是  $w$  的因子. 用反证法. 若存在多项式  $v$  使  $w = p_\ell v$ , 则

$$f = \underbrace{(p_1^{m_1} \cdots p_{\ell-1}^{m_{\ell-1}})}_{(\ell-1) \text{ p's}} p_\ell^{m_\ell+1} \underbrace{(p_{\ell+1}^{m_{\ell+1}} \cdots p_k^{m_k})}_{(k-\ell) \text{ p's}} v.$$

故  $p_\ell^{m_\ell+1}$  是  $f$  的因子. 可是,  $p_\ell$  是  $f$  的  $m_\ell$  重因子, 矛盾!

(vii) 由 (v),  $M = p_1^{m_1-1} p_2^{m_2-1} \cdots p_k^{m_k-1}$  是  $f$  与  $Df$  的最大公因子. 由 (vi), 知

$$\begin{aligned} f &= p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k} w \\ &= (M_1 p_1)(M_2 p_2) \cdots (M_k p_k) w \\ &= (M_1 M_2 \cdots M_k)(p_1 p_2 \cdots p_k) w \\ &= M(p_1 p_2 \cdots p_k w). \end{aligned}$$

所以  $h = p_1 p_2 \cdots p_k w$ , 且  $p_1, p_2, \dots, p_k$  都不是  $w$  的因子.

设不可约的多项式  $p$  是  $f$  的因子. 所以,  $p$  要么是  $f$  的单因子, 要么是  $f$  的重因子.

若  $p$  是  $f$  的重因子, 则  $p$  恰与某一个  $p_\ell$  相伴, 即存在单位  $\varepsilon$  使  $p_\ell = \varepsilon p$ . 故

$$\begin{aligned} h &= p_\ell(p_1 \cdots p_{\ell-1} p_{\ell+1} \cdots p_k w) \\ &= p \underbrace{(\varepsilon p_1 \cdots p_{\ell-1} p_{\ell+1} \cdots p_k w)}_Q. \end{aligned}$$

$p$  不是  $Q$  的因子. 用反证法. 如果  $p$  是  $Q$  的因子, 则因  $p$  是不可约的, 故  $p$  是  $p_1, \dots, p_{\ell-1}, p_{\ell+1}, \dots, p_k$  或  $w$  的因子, 矛盾!

若  $p$  是  $f$  的单因子, 则由 (vi),  $p$  一定是  $p_1^{m_1}, p_2^{m_2}, \dots, p_k^{m_k}$  或  $w$  的因子.  $p$  一定不是  $p_1, p_2, \dots, p_k$  的任意一个的因子, 故  $p$  一定是  $w$  的因子. 所

以  $p$  也是  $h$  的因子.  $p$  能为  $h$  的重因子吗? 不能. 如果  $p$  是  $h$  的重因子, 则  $p^2$  是  $h$  的因子, 故  $p$  是  $f$  的重因子, 矛盾!  $\clubsuit$

为方便, 我们给出

**命题** 设多项式  $f \neq 0$ .  $f$  无重因子的一个必要与充分条件是:  $f$  与  $Df$  互素.

**证** 先看必要性. 反证法. 若  $f$  与  $Df$  不互素, 则存在不可约的多项式  $p$  使  $p$  是  $f$  与  $Df$  的公因子. 所以  $p$  是  $f$  的重因子. 矛盾!

再看充分性. 还是用反证法. 若  $f$  有重因子  $q$ , 则  $q$  是  $f$  与  $Df$  的公因子. 故  $f$  与  $Df$  不互素. 矛盾!  $\clubsuit$

作者举一个例. 此例的运算量比较大; 请读者忍耐一会儿. 有兴趣的读者可自己试试此例的  $f$ ; 无兴趣的读者可试试  $f = x^4 - x^2 + 2x + 2$  (也可“就看看, 不算”; 毕竟, 作者无权也无法强迫读者动手). 不过, 作者还是先给出一个有用的评注.

**评注** 读者或许有这样的经验: 不是整数的有理数的加、乘运算似乎没有整数的加、乘容易. 带余除法时, 我们往往会碰到商或余式不是整系数的情形. 如果只是执行一次带余除法, 读者 (也包括作者) 还是可以接受的. 可是, 我们用辗转相除法找二个多项式的最大公因子时, 要执行多次带余除法. 作者愿意解救读者<sup>†</sup>.

设  $f$  与  $g$  是二个多项式. 无妨设  $g \neq 0$ . 设  $\varepsilon_1$  与  $\varepsilon_2$  是单位. 若  $f = gq + r$ , 则

$$\begin{aligned}\varepsilon_1 f &= \varepsilon_1 gq + \varepsilon_1 r \\ &= \varepsilon_1 (\varepsilon_2^{-1} \varepsilon_2) g + \varepsilon_1 r \\ &= (\varepsilon_2 g) (\varepsilon_1 \varepsilon_2^{-1}) + (\varepsilon_1 r).\end{aligned}$$

也就是说, 商与余式顶多差个单位.

设  $f$  与  $g$  的最大公因子为  $d_1$ ,  $\varepsilon_1 f$  与  $\varepsilon_2 g$  的最大公因子为  $d_2$ . 我们看  $d_1$  与  $d_2$  的关系. 因为  $f$  是  $\varepsilon_1 f$  的因子,  $g$  是  $\varepsilon_2 g$  的因子, 故  $d_1$  是  $\varepsilon_1 f$  与

<sup>†</sup>这是给不用计算机计算的读者的建议; 如果读者用计算机计算, 这些建议就没什么用了.

$\varepsilon_2 g$  的公因子. 这样,  $d_1$  是  $d_2$  的因子. 不过,  $\varepsilon_1 f$  是  $f = \varepsilon_1^{-1} \varepsilon_1 f$  的因子,  $\varepsilon_2 g$  是  $f = \varepsilon_2^{-1} \varepsilon_2 g$  的因子, 故  $d_2$  是  $f$  与  $g$  的公因子. 这样,  $d_2$  是  $d_1$  的因子. 所以  $d_1$  与  $d_2$  相伴.

综上可知: 在辗转相除法里, 将被除式与除式<sup>†</sup>乘单位因子 (不要求一样), 不影响最大公因子的结果.

**例 设**

$$f = x^9 - 2x^6 + 3x^5 - 6x^4 + 12x - 8.$$

我们看看  $f$  是否有重因子.

不难算出

$$Df = 9x^8 - 12x^5 + 15x^4 - 24x^3 + 12.$$

所以

$$f = \frac{x}{9} Df - \frac{2}{3} \underbrace{(x^6 - 2x^5 + 5x^4 - 16x + 12)}_{r_0}.$$

用  $r_0$  (这里的  $r_0$  不是余式!) 除  $Df$ , 有

$$Df = 9(x^2 + 2x - 1)r_0 - 60 \underbrace{(2x^5 - x^4 - 2x^3 - 3x^2 + 6x - 2)}_{r_1}.$$

用  $r_1$  除  $r_0$ , 有

$$r_0 = \frac{1}{4}(2x - 3)r_1 + \frac{21}{4} \underbrace{(x^4 - x^2 - 2x + 2)}_{r_2}.$$

用  $r_2$  除  $r_1$ , 有

$$r_1 = (2x - 1)r_2.$$

所以,  $r_2$  就是  $f$  与  $Df$  的最大公因子. 记  $M = r_2 = x^4 - x^2 - 2x + 2$ . 利用带余除法, 可算出适合  $f = hM$  的  $h$ :

$$f = (x^5 + x^3 + 2x - 4)M \implies h = x^5 + x^3 + 2x - 4.$$

---

<sup>†</sup>在  $f = gq + r$  ( $\deg r < \deg g$ ) 里,  $f$  是“被除式” (dividend),  $g$  是“除式” (divisor).



上面的计算告诉我们,  $f$  有重因子. 虽然我们不知道  $f$  的重因子是什么, 但我们知道  $f$  有重因子! 这很有用, 因为我们还不知道怎么找  $f$  的不可约的因子 (之后作者会告诉读者如何因子分解).

作为一个额外的挑战, 我们看看  $h$  是否有重因子. 按照前面的命题, 这么作出的  $h$  跟  $f$  有相同的不可约的因子, 且  $h$  无重因子. 假如我们“忘记了”这个结论呢? 我们可以求  $h$  与  $Dh$  的最大公因子呀! 不难写出

$$Dh = 5x^4 + 3x^2 + 2.$$

用  $Dh$  除  $h$ :

$$h = \frac{x}{5}Dh + \frac{2}{5}\underbrace{(x^3 + 4x - 10)}_{r_0}.$$

用  $r_0$  除  $Dh$ :

$$Dh = 5xr_0 + \underbrace{(-17x^2 + 50x + 2)}_{r_1}.$$

用  $r_1$  除  $r_0$ :

$$r_0 = -\frac{1}{289}(17x + 50)r_1 + \frac{90}{289}\underbrace{(41x - 31)}_{r_2}.$$

用  $r_2$  除  $r_1$ :

$$r_1 = -\frac{1}{1681}(697x - 1523)r_2 + \frac{50575}{\underbrace{1681}_{r_3}}.$$

到此为止, 咱们不用执行带余除法了 ( $r_3$  是单位; 单位当然是  $r_2$  的因子). 由此可见, 单位就是  $h$  与  $Dh$  的最大公因子, 故  $h$  无重因子.

作者就说这么多吧! 再见, 读者.

## 整系数多项式与有理系数多项式

在“整数的一些性质”与“多项式的一些性质”里, 我们系统地介绍了整数与(系数为  $\mathbb{F}$  的元的)多项式的一些性质. 它们有一个共同点: 都可以作带余除法. 因为带余除法, 我们证明了最大公因子的存在性与 Bézout 等式; 因为最大公因子与 Bézout 等式, 我们考察了互素, 进而考虑了不可约的整数(多项式).

读者可能注意到, 在“多项式的一些性质”里, 我们没有讨论整系数多项式. 为什么没讨论呢? 读者可以想一想, 整系数多项式是否还有带余除法.

**例** 以  $f = x^2 + 1$ ,  $g = 2x$  为例. 设存在整系数多项式  $q, r$  使

$$f = gq + r, \quad \deg r < \deg g = 1.$$

由此可设  $r = c$ ,  $c$  是某个待确定的整数. 设

$$q = a_0 + a_1x + \cdots + a_nx^n,$$

且  $a_0, a_1, \dots, a_n$  都是整数. 所以

$$x^2 + 1 = c + 2a_0x + 2a_1x^2 + \cdots + 2a_nx^{n+1}.$$

由此可知  $n + 1 = 2$ , 且

$$1 = c, \quad 0 = 2a_0, \quad 1 = 2a_1.$$

问题来了: 哪个整数乘 2 等于 1? 所以这样的  $q$  不存在.

当然, 如果读者视  $f, g, q, r$  为有理系数多项式, 立即可得

$$q = \frac{1}{2}x, \quad r = 1.$$

在“多项式的一些性质”里, 我们把“整数的一些性质”的套路几乎原封不动地搬了过来. 不过, 由于整系数多项式不一定有带余除法, 故我们没法“偷懒地”讨论整系数多项式.

但情况不是特别糟. 首先, 整数是有理数, 故整系数多项式是有理系数多项式. 其次, 读者知道, 有理数是二个整数的比(分母不为零). 取不为零的有理系数多项式

$$f = \frac{p_0}{q_0} + \frac{p_1}{q_1}x + \cdots + \frac{p_n}{q_n}x^n,$$

这里  $p_0, q_0, p_1, q_1, \dots, p_n, q_n$  都是整数, 且  $q_0, q_1, \dots, q_n$  都不是零. 作整数

$$\begin{aligned} Q &= q_0 q_1 \cdots q_n, \\ Q_0 &= q_1 q_2 \cdots q_n = \frac{Q}{q_0}, \\ Q_1 &= q_0 q_2 \cdots q_n = \frac{Q}{q_1}, \\ &\dots\dots\dots, \\ Q_n &= q_0 q_1 \cdots q_{n-1} = \frac{Q}{q_n} \end{aligned}$$

将  $f$  改写为

$$f = \frac{p_0 Q_0}{Q} + \frac{p_1 Q_1}{Q} x + \cdots + \frac{p_n Q_n}{Q} x^n.$$

设  $d$  是整数 (而不是多项式)  $p_0 Q_0, p_1 Q_1, \dots, p_n Q_n$  的最大公因子. 这样, 存在整数  $m_0, m_1, \dots, m_n$  使

$$p_0 Q_0 = d m_0, \quad p_1 Q_1 = d m_1, \quad \dots, \quad p_n Q_n = d m_n.$$

所以

$$f = \frac{d}{Q} (m_0 + m_1 x + \cdots + m_n x^n).$$

由最大公因子的性质, 知  $m_0, m_1, \dots, m_n$  互素. 最后, 设  $D$  是  $d$  与  $Q$  的最大公因子, 且  $d = D d', Q = D Q'$ . 所以

$$f = \frac{d'}{Q'} (m_0 + m_1 x + \cdots + m_n x^n).$$

上面的叙述看起来有些抽象, 实则很好理解.

**例 取**

$$f = 1 + \frac{2}{3}x + \frac{1}{6}x^2 + \frac{3}{5}x^3.$$

这里

$$q_0 = 1, \quad q_1 = 3, \quad q_2 = 6, \quad q_3 = 5.$$

所以

$$Q = 180, \quad Q_0 = 180, \quad Q_1 = 60, \quad Q_2 = 30, \quad Q_3 = 36.$$

因为

$$p_0 = 1, \quad p_1 = 2, \quad p_2 = 1, \quad p_3 = 3,$$

故

$$p_0 Q_0 = 180, \quad p_1 Q_1 = 120, \quad p_2 Q_2 = 30, \quad p_3 Q_3 = 108.$$

所以  $f$  可被改写为

$$f = \frac{180}{180} + \frac{120}{180}x + \frac{30}{180}x^2 + \frac{108}{180}x^3.$$

读者可能一眼就认出来, 这如果不是通分, 那它什么都不是.

不难算出 6 是 180, 120, 30, 108 的最大公因子是 6. 所以

$$f = \frac{6}{180}(30 + 20x + 5x^2 + 18x^3).$$

不难算出, 1 是 30, 20, 5, 18 的最大公因子. 最后, 因为 6 是 6 与 180 的最大公因子, 故可进一步将  $f$  改写为

$$f = \frac{1}{30}(30 + 20x + 5x^2 + 18x^3).$$

上面假定  $f \neq 0$ ; 现在考虑 0. 显然  $0 = 0 \cdot 1$ , 其中 1 是整系数多项式, 且其系数互素.

上面的文字说明: 有理系数多项式  $f$  总可以写为一个有理数  $c_f$  与一个整系数多项式  $f^*$  的积, 且  $f^*$  的系数互素.

因此, 我们可以借助有理系数多项式讨论整系数多项式.

**定义** 设

$$f = a_0 + a_1x + \cdots + a_nx^n.$$

若系数  $a_0, a_1, \cdots, a_n$  都是整数, 且整数  $a_0, a_1, \cdots, a_n$  互素, 则  $f$  是本原的 (*primitive*).

**命题** 设  $f$  是有理系数多项式, 且  $f$  不是零.

(i)  $f$  一定可以写为有理数  $c_f$  与本原的多项式  $f^*$  的积, 即  $f = c_f f^*$ ;

(ii) 若有理数  $r$  与本原的多项式  $g$  适合  $f = rg$ , 必有  $r = \varepsilon c_f$ ,  $g = \varepsilon^{-1} f^*$ ,

其中  $\varepsilon = \pm 1$ .

$c_f$  称为  $f$  的容量 (content);  $f^*$  称为  $f$  的本原的相伴 (primitive associate).

**证** (i) 显然.

(ii) 设  $c_f f^* = rg$ , 其中  $c_f, r$  是有理数,  $f^*, g$  是本原的多项式. 不难看出,  $f$  的次一定等于  $g$  的次. 设

$$f^* = s_0 + s_1 x + \cdots + s_n x^n,$$

$$g = t_0 + t_1 x + \cdots + t_n x^n.$$

设  $\frac{c_f}{r} = \frac{p}{q}$ ,  $p, q$  为整数,  $q \geq 1$  且  $p$  与  $q$  互素. 所以

$$pf^* = q \frac{c_f f^*}{r} = q \frac{rg}{r} = qg.$$

所以

$$ps_i = qt_i, \quad i = 0, 1, \cdots, n.$$

因为  $p$  与  $q$  互素, 故任取  $g$  的系数  $t_i$ ,  $p$  一定是  $t_i$  的因子. 所以  $p$  是  $t_0, t_1, \cdots, t_n$  的公因子. 因为  $t_0, t_1, \cdots, t_n$  互素, 故  $p$  是 (整数的) 单位  $\varepsilon_1$ . 既然  $p$  与  $q$  互素, 则  $q$  也是 (整数的) 单位  $\varepsilon_2$ . 所以

$$r = c_f \frac{q}{p} = (\varepsilon_1^{-1} \varepsilon_2) c_f.$$

从而

$$g = f^* \frac{c_f}{f} = (\varepsilon_1 \varepsilon_2^{-1}) f^*.$$

记  $\varepsilon = \varepsilon_1^{-1} \varepsilon_2$ , 则  $\varepsilon^{-1} = \varepsilon_1 \varepsilon_2^{-1}$ . 因为  $\varepsilon_1, \varepsilon_2$  都是整数的单位, 故  $\varepsilon$  也是整数的单位. 所以,  $\varepsilon = \pm 1$ . ✎

**评注** 我们可以这么叙述我们刚才证明的命题: 若忽略 (整数的) 单位的区别, 有理系数多项式可唯一地写为有理数与本原的多项式的积.

**命题** 设多项式  $f, g, h$  的系数都是整数. 设  $f = gh$ .

- (i) 若  $f$  是本原的, 则  $g$  与  $h$  也是本原的;  
 (ii) 若  $g$  与  $h$  是本原的, 则  $f$  也是本原的.

**证** (i) 反证法. 因为乘法可交换, 故不失一般性, 设  $g$  不是本原的. 这样, 存在整系数多项式  $\ell$  与不是 (整数的) 单位的整数  $t$ , 使  $g = t\ell$ . 这样,  $f = t \cdot (\ell h)$ . 所以  $t$  是  $f$  的所有系数的公因子, 故  $t$  是 (整数的) 单位的公因子, 即  $t$  也是 (整数的) 单位. 矛盾!

(ii) 任取不可约的整数  $p$ . 我们证明: 存在  $f$  的系数  $c$ , 使  $p$  不是  $c$  的因子. 设

$$\begin{aligned} g &= g_m x^m + g_{m-1} x^{m-1} + \cdots + g_0, \\ h &= h_n x^n + h_{n-1} x^{n-1} + \cdots + h_0 \end{aligned}$$

是二个本原的多项式. 所以, 从次高的项往次低的项看, 一定存在二个整数  $s, t$  使  $p$  是  $g_m, g_{m-1}, \cdots, g_{s+1}, h_n, h_{n-1}, \cdots, h_{t+1}$  的因子, 但  $p$  不是  $g_s$  的因子, 且  $p$  不是  $h_t$  的因子. 我们看  $f$  的  $s+t$  次系数:

$$\begin{aligned} f_{s+t} &= g_s h_t + g_{s+1} h_{t-1} + \cdots + g_{s+t} h_0 \\ &\quad + g_{s-1} h_{t+1} + \cdots + g_0 h_{s+t}. \end{aligned}$$

由此可见,  $p$  是上式右侧除  $g_s h_t$  外的任意一项的因子. 这样,  $p$  不是  $f$  的  $s+t$  次系数  $f_{s+t}$  的因子. 所以  $f$  的全部系数一定互素.  $\clubsuit$

**命题** 设多项式  $f, g$  的系数都是整数.

- (i) 若  $g$  是本原的, 且存在多项式  $h$  使  $f = gh$ , 则  $h$  的系数也都是整数;  
 (ii) 在 (i) 的基础上, 若还假定  $f$  也是本原的, 则  $h$  也是本原的.

**证** (i)  $f$  与  $g$  当然可以视为有理系数多项式. 由带余除法知,  $h$  至少也是有理系数多项式. 将  $h$  写为  $c_h h^*$ , 其中  $c_h$  是某有理数,  $h^*$  是本原的多项式. 所以

$$f = gh = g(c_h h^*) = c_h (gh^*).$$

显然,  $gh^*$  是本原的. 当然,  $f$  也可写为

$$f = c_f f^*,$$

其中  $c_f$  是整数 (因为  $f$  的系数都是整数), 且  $f^*$  是本原的多项式. 所以, 存在 (整数的) 单位  $\varepsilon$ , 使

$$c_h = \varepsilon c_f, \quad gh^* = \varepsilon^{-1} f^*.$$

从而

$$h = c_h h^* = \varepsilon c_f h^*$$

的系数都是整数.

(ii) 若  $f$  也是本原的, 则由 (i) 的证明过程, 知  $h$  是本原的. ✎

**命题** 设多项式  $f$  的系数都是整数. 设  $f$  可写为二个有理系数多项式  $g, h$  的积. 则  $f$  可写为

$$f = c_f g^* h^*.$$

上式应这么理解: 存在  $g$  的某个本原的相伴  $g^*$ , 存在  $h$  的某个本原的相伴  $h^*$ , 存在  $f$  的某个容量  $c_f$ , 使上式成立.

**证** 设  $f = c_f f^*, g = c_g g^*, h = c_h h^*$ , 其中  $f^*, g^*, h^*$  都是本原的多项式,  $c_g$  与  $c_h$  使有理数, 且  $c_f$  (由题设) 是整数. 因为  $f = gh$ , 故

$$c_f f^* = (c_g c_h)(g^* h^*).$$

$g^* h^*$  是本原的. 所以, 存在 (整数的) 单位  $\varepsilon$ , 使

$$c_g c_h = \varepsilon c_f, \quad g^* h^* = \varepsilon^{-1} f^*.$$

所以

$$f = c_g c_h g^* h^* = (\varepsilon c_f) g^* h^* = c'_f g^* h^*. \quad \text{✎}$$

**评注** 设多项式  $f$  的系数都是整数. 上个命题表明: 若  $f$  可写为二个有理系数多项式的积, 则  $f$  可写为二个整系数多项式的积. 反过来, 因为整数是有理数, 故若  $f$  可写为二个整系数多项式的积,  $f$  当然可写为二个有理系数多项式的积. 每个有理系数多项式都可写为有理数与本原的多项式的积. 所以, 我们可以借整数的性质研究有理系数多项式是否是可约的.

作者本想到此结束本文. 不过, 抱着认真、负责的态度, 作者再给几个重要的命题就结束本文吧.

先从几个简单的小命题开始吧. 这里, 为了方便, 称正的不可约的整数为素数.

**命题** 设  $p$  是素数. 若  $j$  是低于  $p$  的正整数, 则  $p$  是 (广义) 二项系数  $\binom{p}{j}$  的因子.

**证** 易知

$$\binom{p}{j} = \frac{p \cdot (p-1) \cdots (p-(j-1))}{j!} = K,$$

其中  $K$  是整数. 所以

$$p \cdot (p-1) \cdots (p-(j-1)) = K \cdot j!.$$

我们的目标是: 证明  $p$  是  $K$  的因子. 这里,  $p$  已经是  $K \cdot j!$  的因子了. 如果我们能证明  $p$  与  $j!$  互素, 那么  $p$  一定是  $K$  的因子. 想法很美好, 是吧? 确实.

继续分解这个目标. 假如我们能说明  $1, 2, \dots, j$  都与  $p$  互素, 那  $1! = 1$  与  $p$  互素,  $2! = 1! \cdot 2$  与  $p$  也互素,  $3! = 2! \cdot 3$  与  $p$  也互素……一直到  $j! = (j-1)! \cdot j$  与  $p$  也互素.

好! 任取低于  $p$  的正整数  $\ell$ . 我们证明:  $p$  与  $\ell$  互素. 反证法. 若  $p$  与  $\ell$  不互素, 则  $p$  一定是  $\ell$  的因子. 所以, 存在整数  $q$  使  $\ell = pq$ . 因为  $\ell \neq 0$ , 故  $q \neq 0$ , 即  $|q| \geq 1$ . 所以

$$\ell = |\ell| = |p||q| \geq |p| \cdot 1 = p.$$

但是, 这与假定  $\ell < p$  矛盾. 矛盾. 完了.

☺

前面, 我们讨论多项式的性质时, 为了简单, 我们把  $f(x), g(x), h(x), \dots$  写为  $f, g, h, \dots$ . 现在, 因为我们需要多项式的复合, 我们需要写出被省略的 “ $(x)$ ”.



**命题** 设

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$

是有理系数多项式, 且  $n \geq 1$ ,  $a_n \neq 0$  (这表明,  $f(x)$  不是 0, 也不是多项式的单位, 且  $f(x)$  的次为  $n$ ). 设  $\alpha, \beta$  是有理数, 且  $\alpha \neq 0$ . 设

$$g(x) = f(\alpha x + \beta) = a_0 + a_1(\alpha x + \beta) + \cdots + a_n(\alpha x + \beta)^n.$$

显然,  $g(x)$  也是有理系数多项式, 且次仍为  $n$  ( $g(x)$  的次不超过  $n$ , 且其  $n$  次系数  $a_n\alpha^n \neq 0$ ). 因为

$$x = \alpha \cdot \left( \frac{1}{\alpha}x + \frac{-\beta}{\alpha} \right) + \beta,$$

故

$$f(x) = f\left(\alpha \cdot \left( \frac{1}{\alpha}x + \frac{-\beta}{\alpha} \right) + \beta\right) = g\left(\frac{1}{\alpha}x + \frac{-\beta}{\alpha}\right).$$

这里,  $\frac{1}{\alpha}, \frac{-\beta}{\alpha}$  当然也是有理数, 且  $\frac{1}{\alpha} \neq 0$ .

- (i) 若  $f(x)$  是可约的<sup>†</sup>, 则  $g(x)$  是可约的;
- (ii) 若  $g(x)$  是可约的, 则  $f(x)$  是可约的.

简单点说, “ $f(x)$  是可约的 (不可约的)” 的一个必要与充分条件是: “ $f(\alpha x + \beta)$  ( $\alpha, \beta$  是有理数, 且  $\alpha \neq 0$ ) 是可约的 (不可约的)”.

---

<sup>†</sup> 这里的“可约的”是指  $f(x)$  作为有理系数多项式是可约的 (也就是说, 这是“多项式的一些性质”里的“可约的”). 作者不打算讨论详细讨论整系数多项式的“可约的”的含义; 相反, 作者决定只在脚注里简单地提一提.

设  $f$  是整系数多项式. 若存在整系数多项式  $g$  使  $fg = 1$ , 则说  $f$  是整系数多项式的单位. 由此, 读者可以证明: 整系数多项式的单位恰为  $1, -1$ ——这跟有理系数多项式的单位很不一样.

设  $f$  是整系数多项式, 且  $f$  既不是 0, 也不是单位.  $f$  作为整系数多项式是可约的, 是指存在二个不是单位的 (整系数) 多项式  $f_1, f_2$ , 使  $f = f_1f_2$ . 所以, 若把  $4x$  视为整系数多项式,  $4x$  是可约的:  $4 = 4 \cdot x$ , 且  $4$  与  $x$  都不是 (整系数多项式的) 单位. 但若视  $4x$  为有理系数多项式, 则  $4x$  当然是不可约的.

作者不希望这些小差异影响读者. 而且, 这不是什么很重要的点.

**证** 事实上, 我们只要证明 (i). (ii) 的证明就是把 (i) 的证明里的  $f$  与  $g$  互换, 且  $\alpha, \beta$  分别换为  $\frac{1}{\alpha}, \frac{-\beta}{\alpha}$ .

设  $f(x)$  是可约的. 所以, 存在二个不是单位的 (次高于 0 的) 多项式  $f_1(x), f_2(x)$  使

$$f(x) = f_1(x)f_2(x).$$

记

$$g_1(x) = f_1(\alpha x + \beta), \quad g_2(x) = f_2(\alpha x + \beta),$$

则

$$g(x) = f(\alpha x + \beta) = f_1(\alpha x + \beta)f_2(\alpha x + \beta) = g_1(x)g_2(x).$$

因为  $\deg g_1(x) = \deg f_1(x), \deg g_2(x) = \deg f_2(x)$ , 故  $g_1(x), g_2(x)$  都不是单位. 从而  $g(x)$  也是可约的. ✎

**评注** 有一点值得读者注意.

设  $f(x) = x + 4$ . 显然,  $f(x)$  是不可约的.

设  $g(x) = f(x^2) = x^2 + 4$ . 我们证明:  $g(x)$  是不可约的.

反证法. 假定存在二个有理系数多项式  $g_1(x), g_2(x)$  使

$$g(x) = g_1(x)g_2(x),$$

且  $g_1(x), g_2(x)$  都不是单位. 根据前面的命题, 可进一步假定  $g_1(x), g_2(x)$  的系数都是整数 (这可以简化讨论). 因为  $\deg g_1(x) + \deg g_2(x) = 2$ , 而  $\deg g_1(x) > 0, \deg g_2(x) > 0$ , 故  $g_1(x)$  与  $g_2(x)$  的次都是 1. 所以, 设

$$g_1(x) = ax + b, \quad g_2(x) = cx + d,$$

其中  $a, b, c, d$  都是整数. 从而

$$x^2 + 4 = (ax + b)(cx + d) = (ac)x^2 + (ad + bc)x + (bd),$$

也就是

$$ac = 1, \quad ad + bc = 0, \quad bd = 4.$$

由  $ac = 1$  知  $a = c = 1$  或  $a = c = -1$ . 所以

$$\begin{aligned} b + d &= \frac{ad + ba}{a} = \frac{ad + bc}{a} = 0, \\ bd &= 4. \end{aligned}$$

消去  $d$ , 有

$$b^2 = -4.$$

看到这里, 读者可能笑了: 整数的平方不可能是  $-4$  呀! 所以,  $g(x)$  一定是不可约的.

设  $h(x) = g(x^2) = x^4 + 4$ . 我们证明:  $h(x)$  是可约的.

这里就没必要反证了. 作者直接点吧. 无非就是添平方嘛! 具体一点, 就是

$$\begin{aligned} x^4 + 4 &= x^4 + 4x^2 + 4 - 4x^2 \\ &= (x^2 + 2)^2 - (2x)^2 \\ &= (x^2 + 2x + 2)(x^2 - 2x + 2). \end{aligned}$$

显然  $x^2 \pm 2x + 2$  不是单位. 所以,  $h(x)$  是可约的.

设  $\ell(x) = h(x^2) = x^8 + 4$ . 显然,

$$\begin{aligned} x^8 + 4 &= (x^2)^4 + 4 \\ &= ((x^2)^2 + 2x^2 + 2)((x^2)^2 - 2x^2 + 2) \\ &= (x^4 + 2x^2 + 2)(x^4 - 2x^2 + 2), \end{aligned}$$

且  $x^4 \pm 2x^2 + 2$  不是单位, 故  $\ell(x)$  是可约的.

作者举这个例的目的是提醒读者: 上个命题的  $\alpha x + \beta$  不能改为较高次的多项式; 否则, 命题不一定成立.

**定义** 设

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$

是多项式,  $a_n \neq 0$ , 且  $a_0 \neq 0$ .  $f(x)$  的反多项式 (*reciprocal polynomial*) 是

$$f^r(x) = a_n + a_{n-1}x + \cdots + a_0x^n.$$

也就是说,  $f^r(x)$  的  $j$  次系数是  $a_{n-j}$  ( $j = 0, 1, \dots, n$ ).

请读者注意: 上面的  $f(x)$  的 0 次系数不是 0. 如果  $a_0 = 0$ , 它的反多项式是未定义的.

**例 设**

$$f(x) = 1 + 3x + 6x^2 + 10x^3 + 15x^4 + 21x^5.$$

所以

$$f^r(x) = 21 + 15x + 10x^2 + 6x^3 + 3x^4 + x^5.$$

**例 设**

$$g(x) = -6 - 5(x-1) + 2(x-1)^2 + (x-1)^3.$$

读者可能会觉得

$$g^r(x) = 1 + 2(x-1) - 5(x-1)^2 - 6(x-1)^3.$$

但这不对. 按照定义, 我们要先展开  $g(x)$ :

$$\begin{aligned} g(x) &= -6 - 5(x-1) + 2(x^2 - 2x + 1) + (x^3 - 3x^2 + 3x - 1) \\ &= -6 + (-5x + 5) + (2x^2 - 4x + 2) + (x^3 - 3x^2 + 3x - 1) \\ &= -6x - x^2 + x^3. \end{aligned}$$

由此可见,  $g(x)$  的 0 次系数为 0. 所以,  $g^r(x)$  是未定义的.

**命题 设**

$$f(x) = a_0 + a_1x + \dots + a_nx^n$$

是多项式,  $a_n \neq 0$ , 且  $a_0 \neq 0$ .

- (i)  $f(x)$  的反多项式  $f^r(x)$  的次仍为  $n$ ;
- (ii)  $f^r(x)$  的反多项式  $(f^r)^r(x)$  是  $f(x)$ ;
- (iii) 若  $t$  是非零数, 则

$$f^r(t) = t^n f\left(\frac{1}{t}\right).$$

证 (i)  $f(x)$  的反多项式是

$$f^r(x) = a_n + a_{n-1}x + \cdots + a_0x^n.$$

因为  $a_0 \neq 0$ , 故  $f^r(x)$  的次仍为  $n$ .

(ii) 设

$$b_j = a_{n-j}, \quad j = 0, 1, \cdots, n.$$

则  $f(x)$  的反多项式可写为

$$f^r(x) = b_0 + b_1x + \cdots + b_nx^n.$$

因为  $b_0 = a_n \neq 0$ , 且  $b_n = a_0 \neq 0$ , 故  $f^r(x)$  的反多项式是

$$\begin{aligned} (f^r)^r(x) &= b_n + b_{n-1}x + \cdots + b_0x^n \\ &= a_0 + a_1x + \cdots + a_nx^n \\ &= f(x). \end{aligned}$$

(iii) 设  $t$  是非零数. 则

$$\begin{aligned} f\left(\frac{1}{t}\right) &= a_0 + a_1\frac{1}{t} + a_2\left(\frac{1}{t}\right)^2 + \cdots + a_n\left(\frac{1}{t}\right)^n \\ &= a_0 + a_1\frac{1}{t} + a_2\frac{1}{t^2} + \cdots + a_n\frac{1}{t^n} \\ &= a_0\frac{t^n}{t^n} + a_1\frac{t^{n-1}}{t^n} + a_2\frac{t^{n-2}}{t^n} + \cdots + a_n\frac{1}{t^n} \\ &= \frac{a_0t^n + a_1t^{n-1} + a_2t^{n-2} + \cdots + a_n}{t^n} \\ &= \frac{a_n + a_{n-1}t + \cdots + a_0t^n}{t^n} \\ &= \frac{f^r(t)}{t^n}. \end{aligned}$$

所以

$$f^r(t) = t^n f\left(\frac{1}{t}\right).$$

✎

**命题** 设

$$f(x) = a_0 + a_1x + \cdots + a_nx^n,$$

$$f_1(x) = p_0 + p_1x + \cdots + p_ux^u,$$

$$f_2(x) = q_0 + q_1x + \cdots + q_vx^v$$

是多项式, 其中  $p_u \neq 0$ ,  $q_v \neq 0$ ,  $a_n \neq 0$  且  $a_0 \neq 0$ . 设

$$f(x) = f_1(x)f_2(x).$$

(i)  $u + v = n$ ;

(ii)  $p_0 \neq 0$ ,  $q_0 \neq 0$ ;

(iii)  $f^r(x) = f_1^r(x)f_2^r(x)$ .

**证** (i) 显然<sup>†</sup>.

(ii) 因为  $f(x) = f_1(x)f_2(x)$ , 故  $p_0q_0 = a_0$ . 因为  $a_0 \neq 0$ , 故  $p_0 \neq 0$ ,  $q_0 \neq 0$ .

(iii) 因为  $a_0 \neq 0$ ,  $p_0 \neq 0$ ,  $q_0 \neq 0$ , 故  $f(x)$ ,  $f_1(x)$ ,  $f_2(x)$  都有反多项式:

$$f^r(x) = a_n + a_{n-1}x + \cdots + a_0x^n,$$

$$f_1^r(x) = p_u + p_{u-1}x + \cdots + p_0x^u,$$

$$f_2^r(x) = q_v + q_{v-1}x + \cdots + q_0x^v.$$

记

$$E(x) = f^r(x) - f_1^r(x)f_2^r(x).$$

任取非零数  $t$ . 则

$$\begin{aligned} E(t) &= f^r(t) - f_1^r(t)f_2^r(t) \\ &= t^n f\left(\frac{1}{t}\right) - t^u f_1\left(\frac{1}{t}\right) t^v f_2\left(\frac{1}{t}\right) \\ &= t^n f\left(\frac{1}{t}\right) - t^u t^v f_1\left(\frac{1}{t}\right) f_2\left(\frac{1}{t}\right) \end{aligned}$$

---

<sup>†</sup>因为  $f(x) = f_1(x)f_2(x)$ , 故  $\deg f(x) = \deg f_1(x) + \deg f_2(x)$ .

$$\begin{aligned}
&= t^n f\left(\frac{1}{t}\right) - t^{u+v} f\left(\frac{1}{t}\right) \\
&= t^n f\left(\frac{1}{t}\right) - t^n f\left(\frac{1}{t}\right) \\
&= 0.
\end{aligned}$$

这说明, 多项式  $E(x)$  有无限多个根. 所以,  $E(x)$  一定是零多项式, 即

$$f^r(x) = f_1^r(x)f_2^r(x). \quad \text{✎}$$

**命题** 设

$$\begin{aligned}
f(x) &= a_0 + a_1x + \cdots + a_nx^n, \\
f_1(x) &= p_0 + p_1x + \cdots + p_u x^u, \\
f_2(x) &= q_0 + q_1x + \cdots + q_v x^v
\end{aligned}$$

是多项式, 其中  $p_u \neq 0, q_v \neq 0, a_n \neq 0$  且  $p_0 \neq 0, q_0 \neq 0, a_0 \neq 0$ . 设

$$f^r(x) = f_1^r(x)f_2^r(x).$$

则

$$f(x) = f_1(x)f_2(x).$$

**证** 因为 (0 次系数不为 0 的) 多项式  $g$  的反多项式的反多项式是  $g$ , 故由上命题知本命题也对. ✎

跟前面的 “ $\alpha x + \beta$ ” 类似, 我们有

**命题** 设多项式  $f(x)$  既不是 0, 也不是单位, 且 0 次系数不为 0. “ $f(x)$  是可约的 (不可约的)” 的一个必要与充分条件是: “反多项式  $f^r(x)$  是可约的 (不可约的)”.

**证** 这是作者留给读者的练习题; 请读者尝试自行补充细节 (可以说, 这跟 “ $\alpha x + \beta$ ” 几乎一致). ✎

抱歉, 读者朋友. 作者一不小心, 又写多了. “喧宾夺主了, 属于是.” 所以, 请读者消化一下.

我们继续吧!

本来, 作者只想用下面的判别法结束本文, 但又觉得只是冷冰冰地丢下一个判别法不是很负责. 所以, 作者决定加几个例. 为尽可能地消除读者的疑惑, 作者再加了一点细节. 加着加着, 又写多了……

下述命题一般被称为 Eisenstein 判别法 (*Eisenstein criterion*). 当然了, 此命题仅仅是“ $f$  是不可约的”的一个充分条件哟.

**命题** 设多项式

$$f = a_0 + a_1x + \cdots + a_nx^n$$

的系数都是整数. 若存在不可约的整数  $p$  适合如下三条件, 则  $f$  是不可约的:

- (i)  $p$  不是  $a_n$  的因子 (这说明  $a_n \neq 0$ );
- (ii)  $p$  是  $a_{n-1}, a_{n-2}, \cdots, a_0$  的因子.
- (iii)  $p^2$  不是  $a_0$  的因子 (这说明  $a_0 \neq 0$ ).

**证** 用反证法. 设二个 (系数都是整数的) 的多项式  $g, h$  使  $f = gh$ , 其中

$$\begin{aligned} g &= g_0 + g_1x + \cdots + g_\ell x^\ell, \\ h &= h_0 + h_1x + \cdots + h_mx^m \end{aligned}$$

都不是单位, 且  $g_\ell \neq 0, h_m \neq 0$ . 所以  $1 \leq \ell < n, 1 \leq m < n$ , 且  $\ell + m = n$ .

因为  $p$  是  $a_0 = g_0h_0$  的因子, 故  $p$  是  $g_0$  的因子, 或  $p$  是  $h_0$  的因子. 因为  $p^2$  不是  $a_0$  的因子, 故  $p$  不可能是  $g_0$  与  $h_0$  的公因子. 不失一般性, 设  $p$  是  $g_0$  的因子, 且  $p$  不是  $h_0$  的因子. 因为  $p$  不是  $a_n = g_\ell h_m$  的因子, 故  $p$  不是  $g_\ell$  的因子. 所以, 从次低的项往次高的项看, 必有整数  $k$  ( $1 \leq k \leq \ell < n$ ) 使  $p$  是  $g_0, g_1, \cdots, g_{k-1}$  的因子, 但  $p$  不是  $g_k$  的因子. 所以

$$a_k = g_k h_0 + g_{k-1} h_1 + \cdots + g_0 h_k.$$

由此可见,  $p$  是上式右侧除  $g_k h_0$  外的任意一项的因子. 这样,  $p$  不是  $a_k$  的因子. 这跟  $k < n$  矛盾!





我们用几个例帮助读者消化此判别法.

**例** 我们可以随手写出任意次的不可约的多项式:  $x^n + p$ , 这里  $p$  是某个不可约的整数, 且  $n$  是正整数.

**例** 设  $h = x^{m+1} + x^n - 2$ , 其中  $m$  是正整数. 所以,  $h$  的次不低于 2. 所以,  $h$  既不是 0, 也不是单位. 这样,  $h$  一定可以写为不可约的多项式的积. 我们试写  $h$  为不可约的多项式的积.

读者可能还记得

$$f^n - g^n = (f - g)(f^{n-1} + f^{n-2}g + \cdots + f^{n-i}g^{i-1} + \cdots + g^{n-1}).$$

由此, 我们可以将  $h$  改写为

$$h = (x^{m+1} - 1) + (x^m - 1).$$

因为

$$\begin{aligned} & x^n - 1 \\ &= x^n - 1^n \\ &= (x - 1)(x^{n-1} + x^{n-2} \cdot 1 + \cdots + x^{n-i} \cdot 1^{i-1} + \cdots + 1^{n-1}) \\ &= (x - 1)(x^{n-1} + x^{n-2} + \cdots + 1), \end{aligned}$$

故

$$\begin{aligned} h &= (x - 1)(x^m + x^{m-1} + x^{m-2} + \cdots + 1) \\ &\quad + (x - 1)(x^{m-1} + x^{m-2} + \cdots + 1) \\ &= (x - 1) \underbrace{(x^m + 2x^{m-1} + 2x^{m-2} + \cdots + 2)}_q. \end{aligned}$$

显然  $x - 1$  是不可约的. 我们再看看  $q$  是不是可约的. 读者不难看出, 取  $p = 2$ , 则  $p$  (与  $q$ ) 适合 Eisenstein 判别法的三条件, 故  $q$  是不可约的. 所以,  $h$  可写为二个不可约的多项式的积:  $(x - 1) \cdot q$ .

**例** 设  $f = -7 + 9x + 3x^6$ . 不难看出, 不存在不可约的整数  $p$  适合 Eisenstein 判别法的三条件.

因为 (不是单位的) 多项式与其反多项式 (若存在) 要么都是可约的, 要么都是不可约的, 所以我们可以试试<sup>†</sup>反多项式.  $f$  的 0 次系数不是 0, 故  $f$  的反多项式存在, 且  $f^r = 3 + 9x^5 - 7x^6$ . 由此可见, 取  $p = 3$ , 则  $p$  (与  $f^r$ ) 适合 Eisenstein 判别法的三条件, 故  $f^r$  是不可约的. 从而  $f$  也是不可约的.

一般地, 下面的 Eisenstein 判别法的变体成立:

**命题** 设多项式

$$f = a_0 + a_1x + \cdots + a_nx^n$$

的系数都是整数. 若存在不可约的整数  $p$  适合如下三条件, 则  $f$  是不可约的:

- (i)  $p$  不是  $a_0$  的因子 (这说明  $a_0 \neq 0$ );
- (ii)  $p$  是  $a_1, a_2, \dots, a_n$  的因子.
- (iii)  $p^2$  不是  $a_n$  的因子 (这说明  $a_n \neq 0$ ).

**证** 考虑  $f$  的反多项式  $f^r$ . 对  $f^r$  施行 Eisenstein 判别法, 可知  $f^r$  是不可约的. 故  $f$  也是不可约的. (作者邀请感兴趣的读者补全细节.)  $\clubsuit$

我们用经典的例结束本文.

**例** 设  $q$  是素数. 设

$$f(x) = 1 + x + \cdots + x^{q-2} + x^{q-1}.$$

我们证明:  $f(x)$  是不可约的.

显然, 不存在不可约的整数  $p$  适合 Eisenstein 判别法的三条件. 反多项式也没有帮助:  $f(x)$  的反多项式刚好是  $f(x)$ . 我们试试 “ $\alpha x + \beta$ ” 吧.

考虑

$$g(x) = f(x+1) = (1+x)^0 + (1+x)^1 + \cdots + (1+x)^{q-2} + (1+x)^{q-1}.$$

我们需要展开  $g(x)$ . 我们知道,  $(1+x)^\ell$  的  $j$  次系数是  $\binom{\ell}{j}$ . 所以,  $g(x)$  的  $j$  次系数是

$$\binom{0}{j} + \binom{1}{j} + \cdots + \binom{q-2}{j} + \binom{q-1}{j} = \binom{q}{j+1}.$$

---

<sup>†</sup>只是“试试”;不一定管用哟.

也就是说,

$$g(x) = \binom{q}{1} + \binom{q}{2}x + \cdots + \binom{q}{q-1}x^{q-2} + x^{q-1}.$$

取  $p = q$ . 因为  $q$  是素数 (正的不可约的整数),  $p$  当然是不可约的整数. 由此可见,  $p$  (与  $g(x)$ ) 适合 Eisenstein 判别法的三条件, 故  $g(x)$  是不可约的. 故  $f(x)$  也是不可约的.

感谢读者的阅读! 再见.

## 整数的因子分解

作者将在本文为读者介绍整数的因子分解, 并告诉读者如何寻找整数的所有因子.

读者可能还能想起这个命题 (算术基本定理):

**命题** 设整数  $f$  既不是 0, 也不是单位.

(i) 存在不可约的整数  $p_1, p_2, \dots, p_m$  使

$$f = p_1 p_2 \cdots p_m;$$

(ii) 若  $q_1, q_2, \dots, q_m, s_1, s_2, \dots, s_n$  是不可约的整数, 且

$$f = q_1 q_2 \cdots q_m = s_1 s_2 \cdots s_n,$$

则  $m = n$ , 且可以适当地调换  $s_1, s_2, \dots, s_m$  的顺序, 使任取 1 至  $m$  间的整数  $\ell$ ,  $q_\ell$  与  $s_\ell$  相伴 (注意: 调换顺序后的  $s_\ell$  不一定跟原来的  $s_\ell$  相等!).

如果读者还能回忆起此命题的证明, 读者就会发现: 我们只要知道  $\pm 2$  是不可约的就够了 (数学归纳法的始条件: 命题对绝对值为 2 的整数成立). 甚至,  $\pm 3$  是不是可约的不影响此命题的证明: 如果  $\pm 3$  是可约的, 根据可约的整数的定义, 我们将它写为二个不是单位的整数的积, 然后再对这二个整数进行讨论; 如果  $\pm 3$  是不可约的, 则不必证了. (当然, 正如读者所想象的那样,  $\pm 3$  是不可约的.) 换句话说, 虽然此命题断言, 我们可写既不是 0, 也不是单位的整数为若干个不可约的整数的积, 但它可没告诉我们怎么写. 本文就是要告诉读者一个具体的写法.

在前面, 我们稍细致地讨论了不可约的多项式<sup>†</sup>, 并知道, 任取非负整数  $N$ , 必有次高于  $N$  的不可约的多项式<sup>‡</sup> (如  $x^{N+1} + 2$ ). 类似地, 我们也有

**命题** 设  $N$  是非负整数. 存在不可约的整数  $p$  使  $|p| > N$ . 通俗地说, 有无限多个不可约的整数.

<sup>†</sup>这里的多项式的系数是有理数.

<sup>‡</sup>但是, 不可约的复系数多项式的次一定是 1; 不可约的实系数多项式的次一定是 1 或 2. 由于作者不假定读者有实分析 (这里的“实分析”是“广义的”: 研究实数的子集到实数的函数的学问) 或复分析 (类似地, “复分析”是研究复数的子集到复数的函数的学问) 的知识, 故作者无法详细地展开这些事实. 读者可参考任意一本讲“高等代数”的教材. 如果您不知道什么是“分析学”, 那么您可以粗略地视分析学为“微积分”.

**证** 设  $N$  是某非负整数. 用反证法. 假定不存在不可约的整数  $p$  使得  $|p| > N$ ; 也就是说, 每个不可约的整数  $p$  都适合  $|p| \leq N$ . 因为适合条件  $|t| \leq N$  的非负整数  $t$  至多有  $2N + 1$  个<sup>†</sup>, 故只有有限多个不可约的整数. 设  $p_1, p_2, \dots, p_s$  是所有的不可约的整数. 考虑整数

$$M = |p_1| \cdot |p_2| \cdots |p_s| + 1.$$

任取一个不可约的整数  $p_\ell$ . 因为不可约的整数的绝对值不低于 1, 故

$$M \geq |p_\ell| + 1 > |p_\ell|.$$

所以,  $M$  不等于  $p_\ell$ . 换句话说,  $M$  不是不可约的整数. 因为  $|p_\ell| \geq 1$ , 故  $M \geq 2$ . 所以,  $M$  既不是 0, 也不是单位. 所以,  $M$  是可约的. 既然  $M$  是可约的, 那必有某个不可约的整数  $p_k$  是  $M$  的因子.  $p_k$  当然也是  $|p_1| \cdot |p_2| \cdots |p_s|$  的因子. 所以  $p_k$  也是

$$1 = M - |p_1| \cdot |p_2| \cdots |p_s|$$

的因子. 1 当然是  $p_k$  的因子, 故  $p_k$  与 1 相伴. 所以  $p_k$  是单位. 矛盾!  $\clubsuit$

前面, 我们知道: 有无限多个不可约的整数. 那么, 不可约的整数有什么特征呢? 作者给一个简单的命题.

**命题** 设  $p$  是整数, 且  $|p| \geq 5$ . 若  $p$  是不可约的, 则存在整数  $\ell$  使  $p = 6\ell + 1$  或  $p = 6\ell + 5$ .

**证** 既然  $p$  是整数, 那么一定存在唯一的一对整数  $q, r$  使

$$p = 6q + r, \quad 0 \leq r \leq 5.$$

假定  $p = 6q$ . 因为  $|p| \geq 5$ , 故  $p \neq 0$ . 所以  $q \neq 0$ . 因为  $p = 2 \cdot 3q$ , 而 2 不是单位,  $3q$  也不是单位 (因为  $|3q| = 3|q| \geq 3$ ), 这与  $p$  是不可约的矛盾!


假定  $p = 6q + 2 = 2(3q + 1)$ . 因为  $|p| \geq 5$ , 故  $|3q + 1| \geq \frac{5}{2}$ . 因为  $3q + 1$  是整数, 故  $|3q + 1| \geq 3$ . 2 不是单位, 且  $3q + 1$  也不是单位. 这与  $p$  是不可约的矛盾.

---

<sup>†</sup>也就是  $0, 1, -1, 2, -2, \dots, N, -N$ .

假定  $p = 6q + 3 = 3(2q + 1)$ . 因为  $|p| \geq 5$ , 故  $|3q + 1| \geq \frac{5}{3}$ . 因为  $3q + 1$  是整数, 故  $|3q + 1| \geq 2$ . 3 不是单位, 且  $2q + 1$  也不是单位. 这与  $p$  是不可约的矛盾.

假定  $p = 6q + 4 = 2(3q + 2)$ . 因为  $|p| \geq 5$ , 故  $|3q + 2| \geq \frac{5}{2}$ . 因为  $3q + 2$  是整数, 故  $|3q + 2| \geq 3$ . 2 不是单位, 且  $3q + 2$  也不是单位. 这与  $p$  是不可约的矛盾.

综上, 若  $|p| \geq 5$ , 且  $p$  是不可约的, 则  $p = 6q + 1$  或  $p = 6q + 5$ . 取  $\ell = q$  即可. 

**评注** 读者可能听说过,  $25 = 5 \cdot 5$ . 5 不是单位, 故 25 是可约的. 不过,  $25 = 6 \cdot 4 + 1$ . 类似地,  $143 = 11 \cdot 13$ . 11 与 13 都不是单位, 故 143 也是可约的. 不过,  $143 = 6 \cdot 23 + 5$ . 此评注的目的是告诉读者, 上个命题反过来不一定对. 换句话说, 不是所有的  $6\ell + 1$  或  $6\ell + 5$  都是不可约的.

设  $f$  既不是 0, 也不是单位. 判断  $f$  是否是不可约的整数的最简单的方法可能是试除法. 设  $N = |f|$ . 若  $f$  是不可约的, 则不存在整数  $f_1, f_2$  使  $f = f_1 f_2$ , 且  $2 \leq |f_1| < N, 2 \leq |f_2| < N$ ; 反之也对. 适合条件  $2 \leq |t| < N$  的整数至多有  $2(N - 2)$  个<sup>†</sup>, 故我们可以用这  $2(N - 2)$  个整数一个一个地除, 以判断这样的  $f_1, f_2$  是否存在. 因为  $g$  是  $f$  的因子的一个必要与充分条件是  $-g$  是  $f$  的因子, 故我们不必用负整数除  $f$ ; 也就是说, 用  $N - 2$  个整数  $2, 3, \dots, N - 1$  除  $f$  就够了. 当然, 如果这  $N - 2$  个整数中有一个是  $f$  的因子, 则  $f$  是可约的; 我们可以停下来了.

**例** 设  $f = 17$ . 则  $N = |f| = 17$ . 我们用  $N - 2 = 15$  个整数  $2, 3, \dots, 16$  除  $f$ . 2 不是  $f$  的因子; 3 不是  $f$  的因子……16 不是  $f$  的因子<sup>‡</sup>. 所以, 17 是不可约的. 当然,  $-17$  也是不可约的.

**例** 设  $f = 35$ . 则  $N = |f| = 35$ . 我们用  $N - 2 = 33$  个整数  $2, 3, \dots, 34$  除  $f$ . 2, 3, 4 都不是  $f$  的因子, 但 5 是  $f$  的因子. 所以,  $f$  是可约的. 我们看看 5. 5 是最小的高于 1 的  $f$  的因子. 读者可能也知道, 5 是不可约的.

<sup>†</sup>也就是  $2, -2, 3, -3, \dots, N - 1, -(N - 1)$ .

<sup>‡</sup>感兴趣的读者可自行完成 15 次带余除法.


再看  $g = 49$ . 则  $N = |g| = 49$ . 我们用  $N - 2 = 47$  个整数  $2, 3, \dots, 48$  除  $g$ .  $2, 3, 4, 5, 6$  都不是  $g$  的因子, 但  $7$  是  $f$  的因子. 所以,  $g$  是可约的. 我们看看  $7$ .  $7$  是最小的高于  $1$  的  $h$  的因子. 读者可能也知道,  $7$  是不可约的.

一般地, 我们有

**命题** 设  $f$  既不是  $0$ , 也不是单位. 若  $p$  是最小的高于  $1$  的  $f$  的因子, 则  $p$  是不可约的.

**证** 用反证法. 若  $p$  是可约的, 存在整数  $f_1, f_2$  使  $p = f_1 f_2$ , 且  $f_1, f_2$  不是单位. 因为  $p$  高于  $1$ , 故可假定  $f_1, f_2$  是正整数. 所以,  $f_1$  与  $f_2$  也都高于  $1$ . 所以

$$p - f_1 = f_1 f_2 - f_1 = f_1 (f_2 - 1) > 0.$$

因为  $f_1$  是  $p$  的因子, 而  $p$  是  $f$  的因子, 故  $f_1$  是  $f$  的因子. 因为  $f_1 > 1$ , 且  $f_1 < p$ , 故  $p$  不是最小的高于  $1$  的  $f$  的因子. 矛盾! 

**评注** 上面的命题表明: 若  $f$  是可约的, 则  $2, 3, \dots, |f| - 1$  的首个  $f$  的因子一定是不可约的. 这也是一种找不可约的整数的办法. 后面, 我们在讨论整数的因子分解时, 此命题将很有用.

或许读者觉得试除法要太长时间了. 的确如此; 作者也这么认为. 若  $f$  是可约的, 则我们不必试全部的  $|f| - 2$  个整数; 可如果  $f$  不是可约的, 那这太糟糕了——试了  $|f| - 2$  次. 所以, 我们有必要简化试除法.

请读者先回忆一下算术平方根. 若  $t$  是非负实数, 则存在唯一的非负实数  $s$  适合  $s^2 = t$ . 我们用  $\sqrt{t}$  表示这个  $s$ ;  $\sqrt{t}$  就是  $t$  的算术平方根<sup>†</sup>. 比方说,  $\sqrt{4} = 2$ ,  $\sqrt{121} = 11$ ,  $\sqrt{0} = 0$ ,  $\sqrt{1} = 1$ .

**命题** 设  $f$  是整数. 设整数  $f_1, f_2$  适合  $f = f_1 f_2$ . 设  $|f_1| \leq |f_2|$ . 则  $|f_1| \leq \sqrt{|f|}$ .

**证** 用反证法. 若  $|f_1| > \sqrt{|f|}$ , 则  $|f_2|$  也高于  $\sqrt{|f|}$ . 所以

$$|f| = |f_1| \cdot |f_2| > \sqrt{|f|} \cdot \sqrt{|f|} = |f|,$$

矛盾! 

<sup>†</sup>很遗憾, 作者无法在这里证明这个命题. 它的严格证明需要本文没介绍的 (分析学) 知识; 这些知识的讨论又可单独成册了.

根据此命题, 我们在试除时, 不必从 2 到  $N-2$  (这里  $N = |f|$ ), 只要用从 2 到  $\sqrt{N}$  的整数即可. 最大的且不超过  $\sqrt{N}$  的整数是  $\lfloor \sqrt{N} \rfloor$ . 所以, 试除法的 “ $N-2$  个整数 2, 3,  $\dots$ ,  $N-1$ ” 可改为 “ $\lfloor \sqrt{N} \rfloor - 1$  个整数 2, 3,  $\dots$ ,  $\lfloor \sqrt{N} \rfloor - 1$ ”.

**例** 设  $f = 233$ . 则  $N = |f| = 233$ . 对人而言, 233 已经不算小了. 如果不进行任何优化, 我们需要用  $N-2 = 231$  个整数除  $f$ . 作者不知道读者怎么想; 作者肯定不愿意用 231 个整数除  $f$ . 所以, 我们用上面的花招简化一下.

如果读者背通过小整数的平方, 就会知道  $15^2 = 225$ ,  $16^2 = 256$ . 所以, 最大的且不超过  $\sqrt{233}$  的整数就是 15. 我们用 14 个整数 2, 3,  $\dots$ , 15 除  $f$ . 从 233 到 14, 这是很大的进步! 现在, 我们可以试除了. 14 次除法后, 可知: 2, 3,  $\dots$ , 15 都不是  $f$  的因子. 所以, 233 是不可约的.

事实上, 试除时, 我们可以只用不可约的整数试除. 这很明显. 若  $g$  是不可约的, 则存在可约的整数  $p$  使  $p$  是  $g$  的因子. 进一步, 我们可假定此  $p$  是正整数. 若  $g$  是  $f$  的因子, 则  $p$  当然也是  $f$  的因子; 所以, 若  $p$  不是  $f$  的因子, 那么  $g$  不可能是  $f$  的因子.

不过, 不可约的整数应该往哪儿找呢?

前面, 我们已看到: 任给不是  $\pm 2$ ,  $\pm 3$  的不可约的整数  $p$  (4 当然是可约的:  $4 = 2 \cdot 2$ ), 必有整数  $\ell$  使  $p = 6\ell + 1$  或  $p = 6\ell + 5$ . 因为

$$6\ell + 5 = 6\ell + 6 - 1 = 6(\ell + 1) - 1,$$

故  $p$  可写为  $6k \pm 1$ , 其中  $k$  是整数. 为方便, 无妨假定  $p$  是正整数<sup>†</sup>. 这样,  $p \geq 5$ . 由此可知  $6k \pm 1 \geq 5$ , 即  $k \geq \frac{5 \pm 1}{6}$ . 因为  $k$  是整数, 故  $k \geq 1$ . 换句话说, 我们证明了

**命题** 设正整数  $p$  是不可约的. 则  $p = 2$ , 或  $p = 3$ , 或存在正整数  $k$  使  $p = 6k \pm 1$ .

综上, 我们有如下的方法判断一个整数  $f$  (既不是单位, 也不是 0) 是否是不可约的:

<sup>†</sup>若整数  $p$  是不可约的, 则  $-p$  也是不可约的. 试除时只需选正的整数, 故作者在此处 (为方便) 也选正的不可约的整数.



- (i) 置  $S = \lfloor \sqrt{|f|} \rfloor$ .
- (ii) 若  $2 > S$ , 则  $f$  是不可约的, 停止. 若  $2 \leq S$ , 用 2 除  $f$ . 若 2 是  $f$  的因子, 则  $f$  是可约的, 停止; 若 2 不是  $f$  的因子, 跳转到 (iii).
- (iii) 若  $3 > S$ , 则  $f$  是不可约的, 停止. 若  $3 \leq S$ , 用 3 除  $f$ . 若 3 是  $f$  的因子, 则  $f$  是可约的, 停止; 若 3 不是  $f$  的因子, 跳转到 (iv).
- (iv) 置  $p = 5$  (这相当于是令  $k = 1, p = 6k - 1$ ).
- (v) 若  $p > S$ , 则  $f$  是不可约的, 停止. 若  $p \leq S$ , 用  $p$  除  $f$ . 若  $p$  是  $f$  的因子, 则  $f$  是可约的, 停止; 若  $p$  不是  $f$  的因子, 跳转到 (vi).
- (vi) 将  $p$  替换为  $p + 2$  (这相当于把  $p = 6k - 1$  变为  $p = 6k + 1$ ).
- (vii) 若  $p > S$  (这里的  $p$  是新  $p$ , 下同), 则  $f$  是不可约的, 停止. 若  $p \leq S$ , 用  $p$  除  $f$ . 若  $p$  是  $f$  的因子, 则  $f$  是可约的, 停止; 若  $p$  不是  $f$  的因子, 跳转到 (viii).
- (viii) 将  $p$  替换为  $p + 4$  (这相当于把  $6k + 1$  变为  $6k + 5 = 6(k + 1) - 1$ ; 换句话说, 先把  $k$  变为  $k + 1$ , 再把  $p$  变为  $6k + 1$ ). 跳转到 (v).

这个方法, 当然, 还是“试除法”. 而且, 上面的叙述相当“死板”: 初见此方法的读者可能不会立即理解此法是正确的. 此法适合丢给计算机, 让计算机判断一个“不太大的”整数<sup>†</sup>是否是不可约的. 如果人在脑中 (或用纸笔) 作运算, 那么作者给个建议: 若 (v) (vii) 里的  $p$  是可约的, 则跳过此步 (也就是所谓的 continue).

“光说不练, 假把式.” 所以, 作者举一个例.

**例** 设  $f = 2333$ . 则  $N = |f| = 2333$ . 如果读者背通过“小”整数的平方, 就会知道  $48^2 = 2304$ ,  $49^2 = 2401$ . 所以,  $S = \lfloor \sqrt{N} \rfloor = 48$ . 利用“ $6k \pm 1$ ”, 我们只要用 17 个整数 2, 3, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47 除  $f$  ( $49 > S$ , 故我们不必考虑 49 及其以后的整数). 事实上, 因为  $25 = 5 \cdot 5$ ,  $35 = 5 \cdot 7$ , 故 25 与 35 都是可约的; 这样, 我们可以划去这两个数——只剩 15 个啦! 一个一个地除, 发现这 15 个整数都不是  $f$  的因子. 所以, 2333 是不可约的.

辛苦了! 请读者休息一会儿.

---

<sup>†</sup> 设  $t$  是整数. 若  $t$  不高于  $2^{31} - 1$  且  $t$  不低于  $-2^{31}$ , 则说  $t$  是“不太大的”. 了解一点计算机知识的读者可看出, 这恰为 int (或 int32) “数据类型”的“取值范围”.

前面, 我们用试除法判断一个 (既不是 0, 也不是单位的) 整数是否是可约的. 现在, 我们考虑不等于非零整数的因子分解.

在正式地给出因子分解的定义前, 我们看一个例.

**例** 设  $f = 12$ . 读者不难验证

$$f = 2 \cdot 2 \cdot 3.$$

这是写  $f$  为不可约的整数的积的一个结果. 为什么只是一个呢? 因为

$$f = (-2) \cdot (-2) \cdot 3,$$

而  $-2$  也是不可约的. 读者不至于认为  $-2$  不是不可约的吧?

当然了, 作者清楚, 读者更习惯正的不可约的整数; 作者知道, 负的不可约的整数看上去有些奇怪. 可是,  $g = -12$  该怎么写呢? 因为  $g = (-1)f$ , 故一个自然的写法是

$$g = (-1) \cdot 2 \cdot 2 \cdot 3.$$

不过,  $-1$  是单位, 故它既不是可约的, 也不是不可约的. 此时, 如果仍要写  $g$  为不可约的整数的积, 读者不得不至少用一个负的不可约的整数:

$$g = 2 \cdot 2 \cdot (-3).$$

此处,  $-3$  自然也是不可约的. 当然, 在这个特殊的例里, 读者也可以写

$$g = (-2) \cdot (-2) \cdot (-3).$$

这里, 可写  $g$  为负的不可约的整数的积. 不过  $-6$  要怎么办? 读者不至于写  $-6 = (-2) \cdot (-3)$  吧? 负负得正呀!

**评注** 读者应该意识到了上例暴露的“问题”. 怎么办呢, 读者朋友? 作者提供三个方案:

(i) “剥夺” 负整数的“因子分解权”. 别笑! 虽然中国人很早 (1 世纪左右) 就开始玩负数了 (见《九章算术》的《方程》), 可是有的西方人 (主要是欧

洲人) 怀疑负数 (据说, 到 19 世纪中期, 西方的数学家才普遍地接受负数). 法兰西数学家 Blaise Pascal 的朋友 Antoine Arnauld 如此质疑负数: 如果允许负数, 那么  $\frac{-1}{1} = \frac{1}{-1}$ ; 可是, 这说明小数 (较小的数, 下同) 与大数的比等于大数与小数的比, 矛盾!<sup>†</sup> 西方人接受 0 的过程也是漫长的 (感兴趣的读者可自行查阅相关资料), 更别提负数了. 所以, 早期西方人研究 “因数” “最大公因数” “素数” 时, 这些数至少都是非负的. 所以 “素数” 一般都是指正的不可约的整数. 在研究不可约的整数的 “高级性质” 时, 为方便, 数学家往往要求它是正的; 这算是历史习惯了. 作者并没有说这个习惯不好; 事实上, 有时, 为方便, 作者自己也用 “素数”.<sup>‡</sup>

(ii) 忽视这个问题, 且不限定不可约的整数的正负. 当然可以; 毕竟, 作者一开始可没说不可约的整数一定是正的. 不过, 有一点小问题. 为方便, 我们往往会把相伴的整数化为同一个. 比方说, 我们往往不写  $-12 = (-2) \cdot 2 \cdot 3$ , 而是写  $-12 = 2 \cdot 2 \cdot (-3)$ . 可是,  $-9$  要怎么办呢? 要么写  $3 \cdot (-3)$ , 要么写  $(-3) \cdot 3$ ; 毕竟, 负负得正. 当然, 我们可以无视这一点: 相伴的整数可以不化为同一个.

(iii) 跳出 “不可约的整数的积” 的 “舒适圈” (*comfort zone*). 假如我们允许单位, 那么每个非零整数都可以写为 (至多) 一个单位与有限多个不可约的整数的积. 这很好理解: 单位自然是 “一个单位与零个不可约的整数的积 (我们约定, 零个数的积是 1; 这跟零个数的和是 0 类似)”; 既不是 0, 也不是单位的整数自然是 “零个单位 (也可以是一个: 1) 与有限多个 (至少有 1 个) 不可约的整数的积”. 而且, 相伴的整数一定可被化为同一个. 若  $q$  与  $p$

<sup>†</sup> 如果这里的数都是正数, 那么小数与大数的比当然不是大数与小数的比; 可这里出现了负数. 如果读者还有印象, 就会记得, 不等式二侧同乘负数, 不等式反向. 或许此事实有助于解释此 “怪事”.

<sup>‡</sup> 既然作者说这么多了, 那么作者解释一下作者为什么讨论 “整数的一些性质” 而不是 “非负整数的一些性质” 吧. 在整数里, 我们可自由地加、减、乘; 类似地, 多项式也可自由地被加、减、乘. 整数与多项式都有带余除法; 整数与多项式都有用来求最大公因子的辗转相除法……作者在此就不重复整数与多项式的大量的共同点了. 我们再看非负整数. 非负整数可加、乘, 但不一定能减 (小数减大数 “不够减”). 在同人文里, 作者先讨论整数, 再讨论多项式. 如果负数还能通过只考虑非整数避开 (毕竟, 因子可正可负), 那多项式呢? 只考虑 0 与首项系数为 1 的多项式吗 (毕竟, 二个非零多项式的首项系数为 1 的最大公因子恰有一个; 这跟二个非零整数的正的最大公因子恰有一个类似)? 当然可以; 不过, 没有必要: 借助 “单位” “相伴” 的概念, 我们克服了这个小问题.

相伴, 则有单位  $\varepsilon$  使  $q = \varepsilon p$ , 则  $pq = \varepsilon(pp)$ . 因为乘法可交换、结合, 故我们可把多个单位都写在最前; 因为有限多个单位的积还是单位, 故多个单位可被写为一个单位. 具体地,  $-9 = 3 \cdot (-3) = 3 \cdot (-1) \cdot 3 = (-1) \cdot 3 \cdot 3$  (当然, 也可以是  $-9 = (-1) \cdot (-3) \cdot (-3)$ ).

在这里, 作者选用方案 (iii). 毕竟, 如果允许单位, 读者可自由地改变不可约的整数的形式, 直到其适合读者的口味为止. 所以, 相应地, 作者给出

**定义** 设整数  $f \neq 0$ . 那么,  $f$  一定可写为 (至多一个) 单位与有限多个 (可以是零个) 不可约的整数的积, 即: 存在单位  $\varepsilon$  与不可约的整数  $p_1, p_2, \dots, p_s$  ( $s$  可为 0; 此时,  $f$  是单位) 使

$$f = \varepsilon p_1 p_2 \cdots p_s.$$

上式右侧即为  $f$  的因子分解 (*factorization of  $f$* ). 动词短语 “写  $f$  为单位与有限多个不可约的整数的积” 的一个简单的称呼是 “因子分解  $f$ ” (*to factorize  $f$* ).

## 有理系数多项式的有理根

To be continued.

## 有理系数多项式的因子分解

To be continued. I will finish this part later.

Well, whatsoever.

本文的主要目的: (i) 为读者介绍因子分解整数的方法; (ii) 为读者介绍一些 (在有理数范围里) 因子分解有理系数多项式的方法.

我们先讨论因子分解整数吧.

现在, 我们讨论因子分解多项式.

本文的多项式的系数都是有理数. 所以, 在本文里, 为了方便, 作者单说“多项式”时, 它一定是有理系数多项式.

作者再约定一次 (其实作者早就在“整系数多项式与有理系数多项式”里说过了): 说多项式  $f$  是可约的, 是指视  $f$  为有理系数多项式时,  $f$  是可约的. 所以, 当读者看到形如“ $4x$  是不可约的”的陈述时, 作者希望读者不要认为这是错的.

**定义** 设  $f, g_1, g_2, \dots, g_n$  是多项式. 根据分配律, 有

$$\underbrace{fg_1 + fg_2 + \dots + fg_n}_{\text{LHS}} = \underbrace{f \cdot (g_1 + g_2 + \dots + g_n)}_{\text{RHS}}.$$

我们唤写 LHS<sup>†</sup> 为 RHS 的行为为提出 LHS 的  $f$  (to extract  $f$  from the LHS). 当然, 若省略“LHS 的”不会造成歧义, 我们也可以只说“提出  $f$ ”.

**例** 设  $f = x^2 - a^2$ ,  $a$  为数. 则

$$\begin{aligned} f &= x^2 - a^2 \\ &= x^2 - xa + ax - a^2 \\ &= (x^2 - xa) + (ax - a^2). \end{aligned}$$

根据分配律,

$$x^2 - xa = x(x - a), \quad ax - a^2 = a(x - a).$$

<sup>†</sup>LHS, left-hand side 也; RHS, right-hand side 也.

所以, 我们提出  $x^2 - xa$  的  $x$ , 并提出  $ax - a^2$  的  $a$ :

$$f = x(x - a) + a(x - a).$$

根据分配律,

$$x(x - a) + a(x - a) = (x + a)(x - a).$$

所以, 提出  $x - a$ , 就有

$$f = (x + a)(x - a).$$

**定义** 设  $f$  是多项式, 且  $f \neq 0$ . 将  $f$  写为 (有理数的) 单位<sup>†</sup>与有限多个<sup>‡</sup>不可约的多项式的幂<sup>§</sup>的积的行为是“因子分解” (*to factorize*); “因子分解”的过程也是“因子分解” (*factorization*); “因子分解”的结果 (单位与有限多个不可约的多项式的幂的积) 也是“因子分解” (*factorization*).

**例** 设  $f = 4x^2 - 64$ . 不难看出,

$$f = (2x)^2 - 8^2 = (2x + 8)(2x - 8).$$

因为  $2x \pm 8$  都是不可约的, 故  $(2x + 8)(2x - 8)$  是  $f$  的 (一个) 因子分解.

可是, 读者可能会觉得“这没分解完”. 如果读者是说  $2x \pm 8 = 2(x \pm 4)$ , 那“的确如此”. 可是, 按照我们的定义,  $2x \pm 8$  已经是可约的.

当然, 读者可以再看看因子分解的定义: 单位与有限多个不可约的多项式的幂的积. 也就是说, 我们可以认为  $4(x + 4)(x - 4)$  也是  $f$  的因子分解, 因为 4 是单位, 且  $x \pm 4$  是不可约的. 不过, 既然这样, 读者也应该接受  $64(\frac{x}{4} + 1)(\frac{x}{4} - 1)$  为  $f$  的因子分解, 因为 64 也是单位, 且  $\frac{x}{4} \pm 1$  也是不可约的.

这或许就跟有理数一样:  $\frac{-1}{2}$  跟  $-\frac{111}{222}$ ,  $\frac{1234}{-2468}$  表示同一个分数. 我们一般都会让分子与分母互素. 类似地, 我们也会对因子分解的结果作一些限定 (当然, 不强行要求唯一). 常用的一个约定是这样的. 假定

$$f = \varepsilon f_1^{k_1} f_2^{k_2} \cdots f_n^{k_n},$$

<sup>†</sup>单位可以是 1; 换句话说, 这个单位可以“不出现”.

<sup>‡</sup>允许 0 个. 此时,  $f$  就是单位.

<sup>§</sup>举一个例. 设  $f = 2x^3 + 4x^2 + 2x$ . 不难看出,  $f = 2x \cdot (x + 1) \cdot (x + 1)$ . 为方便, 我们可以把  $(x + 1) \cdot (x + 1)$  写为  $(x + 1)^2$ , 即  $f = 2x(x + 1)^2$ .

其中  $\varepsilon$  是单位,  $f_1, f_2, \dots, f_n$  都是不可约的多项式, 且  $k_1, k_2, \dots, k_n$  都是正整数. 把每个  $f_i$  写为  $c_i F_i$ , 其中  $F_i$  是  $f_i$  的一个本原的相伴. 这样

$$\begin{aligned} f &= \varepsilon(c_1 F_1)^{k_1} (c_2 F_2)^{k_2} \cdots (c_n F_n)^{k_n} \\ &= \varepsilon(c_1^{k_1} F_1^{k_1}) (c_2^{k_2} F_2^{k_2}) \cdots (c_n^{k_n} F_n^{k_n}) \\ &= (\varepsilon c_1^{k_1} c_2^{k_2} \cdots c_n^{k_n}) F_1^{k_1} F_2^{k_2} \cdots F_n^{k_n} \\ &= \varepsilon' F_1^{k_1} F_2^{k_2} \cdots F_n^{k_n}. \end{aligned}$$

按照此约定,  $4x^2 - 64$  的因子分解如下:

$$\begin{aligned} 4x^2 - 64 &= 4(x+4)(x-4) \\ &= -4(-x-4)(x-4) \\ &= 4(-x-4)(-x+4) \\ &= -4(x+4)(-x+4). \end{aligned}$$

读者可以按需选一个因子分解. 比方说, 喜欢使不可约的因子的首项系数为正数的读者可选  $4(x+4)(x-4)$ ; 当然, 喜欢使不可约的因子的 0 次系数为正数的读者可选  $-4(x+4)(-x+4)$ ; 最后, 不在乎这些细节的读者可随意地选.

这么看来, 要求不可约的因子都是本原的似乎不是很奇怪. 事实上, 它很有用. 读者马上就可以看到这一点.

在前面, 我们讨论了整系数多项式与多项式的关系. 利用本原的多项式, 我们得到了下面的结论.

(i) 每个多项式都是某个有理数与本原的多项式的积. 所以, 遇到  $\frac{1}{2} + \frac{1}{3}x + \frac{1}{5}x^2$  时, 我们可将其写为  $\frac{1}{30}(15 + 10x + 6x^2)$ , 然后考虑  $15 + 10x + 6x^2$  的因子分解.

(ii) 若整系数多项式可写为二个多项式的积, 则其一定可写为二个整系数多项式的积. 所以, 当我们假设整系数多项式是可约的时, 我们可以假定因子的系数都是整数. 这一点, 在证明 Eisenstein 判别法时就用到.

(iii) 设  $f$  是整系数多项式,  $g$  是本原的多项式. 若存在多项式  $h$  使  $f = gh$ , 则  $h$  的系数一定都是整数. 这也暗示了本原的多项的特殊性: 提出



整系数多项式的本原的因子, 剩下的部分仍是整系数的. 我们等会儿就要演示这一点有多么有用.

最简单的不可约的多项式是 1 次的. 所以, 让我们从 1 次因子开始吧!

**命题** 设整数  $u, v$  互素, 且  $u \neq 0$ . 这样,  $g = ux - v$  是本原的 1 次多项式. 设  $f$  是整系数多项式. 若  $g$  是  $f$  的因子, 则  $u$  是  $f$  的首项系数的因子, 且  $v$  是  $f$  的 0 次系数的因子.

**证** 设

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

是整系数多项式, 且  $a_n \neq 0$ . 因为  $g = ux - v$  是本原的,  $g$  是  $f$  的因子, 故存在整系数多项式  $h$  使  $f = gh$ . 因为  $\deg f = \deg g + \deg h$ , 故  $\deg h = n - 1$ . 所以, 可设

$$h = b_{n-1} x^{n-1} + \cdots + b_1 x + b_0,$$

且  $b_{n-1} \neq 0$ . 从而

$$a_n = ub_{n-1}, \quad a_0 = -vb_0.$$

故  $u$  是  $a_n$  的因子, 且  $v$  是  $a_0$  的因子. ✎

既然  $ux - v$  是  $f$  的因子, 那么有多项式  $h$  使

$$f = (ux - v)h.$$

适当地改写一下:

$$f = \left(x - \frac{v}{u}\right)(uh)$$

由此可见,  $\frac{v}{u}$  是  $f$  的根. 所以, 用根的语言描述上个命题, 就是

**命题** 设整数  $u, v$  互素, 且  $v \neq 0$ . 设  $f$  是整系数多项式. 若  $\frac{v}{u}$  是  $f$  的根, 则  $u$  是  $f$  的首项系数的因子, 且  $v$  是  $f$  的 0 次系数的因子.

有二个特殊情形值得一提.

若  $f$  的 0 次系数是 0, 则由于每个整数都是 0 的因子, 这似乎是“听君一席话, 胜听一席话”. 不过, 并不是这样. 既然  $f$  的 0 次系数是 0, 那么

$$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + 0,$$

其中  $a_n \neq 0$ . 从次低的项往次高的项看, 必存在正整数  $\ell$  使  $\ell$  个系数  $a_0, a_1, \cdots, a_{\ell-1}$  为 0, 而  $a_\ell$  不为 0. 所以,

$$\begin{aligned} f &= a_n x^n + a_{n-1} x^{n-1} + \cdots + a_\ell x^\ell \\ &= x^\ell \cdot \underbrace{(a_n x^{n-\ell} + a_{n-1} x^{n-1-\ell} + \cdots + a_\ell)}_g. \end{aligned}$$

不难看出,  $n - \ell$  次多项式  $g$  的 0 次系数  $a_\ell \neq 0$ . 我们已提出  $x^\ell$ , 故我们只要继续寻找  $g$  的 1 次因子 (或有理根) 即可.

若  $f$  的首项系数是  $\pm 1$ , 则  $u$  也一定是  $\pm 1$ . 所以我们有

**命题** 设  $f$  是整系数多项式, 且其首项系数是  $\pm 1$ . 若有理数  $r$  是  $f$  的根, 则  $r$  一定是整数, 且  $r$  是  $f$  的 0 次系数的因子.

**例** 设  $n$  是正整数. 设  $m$  是整数, 且不存在整数  $s$  使  $s^n = m$ . 我们证明: 不存在有理数  $r$  使  $r^n = m$ .

反证法. 若存在有理数  $r$  使  $r^n = m$ , 则有理数  $r$  是整系数多项式  $f = x^n - m$  的根. 因为  $f$  的首项系数是 1, 故  $r$  一定是整数. 可是,  $m$  不是整数的平方, 矛盾!

读者可能听说过,  $\sqrt{2}$  是无理数. 我们可以这么看:  $\sqrt{2}$  是实数; 实数不是有理数就是无理数;  $\sqrt{2}$  的平方是 2; 整数的平方不可能是 2.

类似地, 读者可证明:  $\sqrt[3]{2}$  也是无理数.

呀! 作者跑远了. 回来, 回来!

设  $f$  是整系数多项式, 且其首项系数  $a_n \neq 0$ , 0 次系数为  $a_0$ . 设  $a_0$  的全部因子为