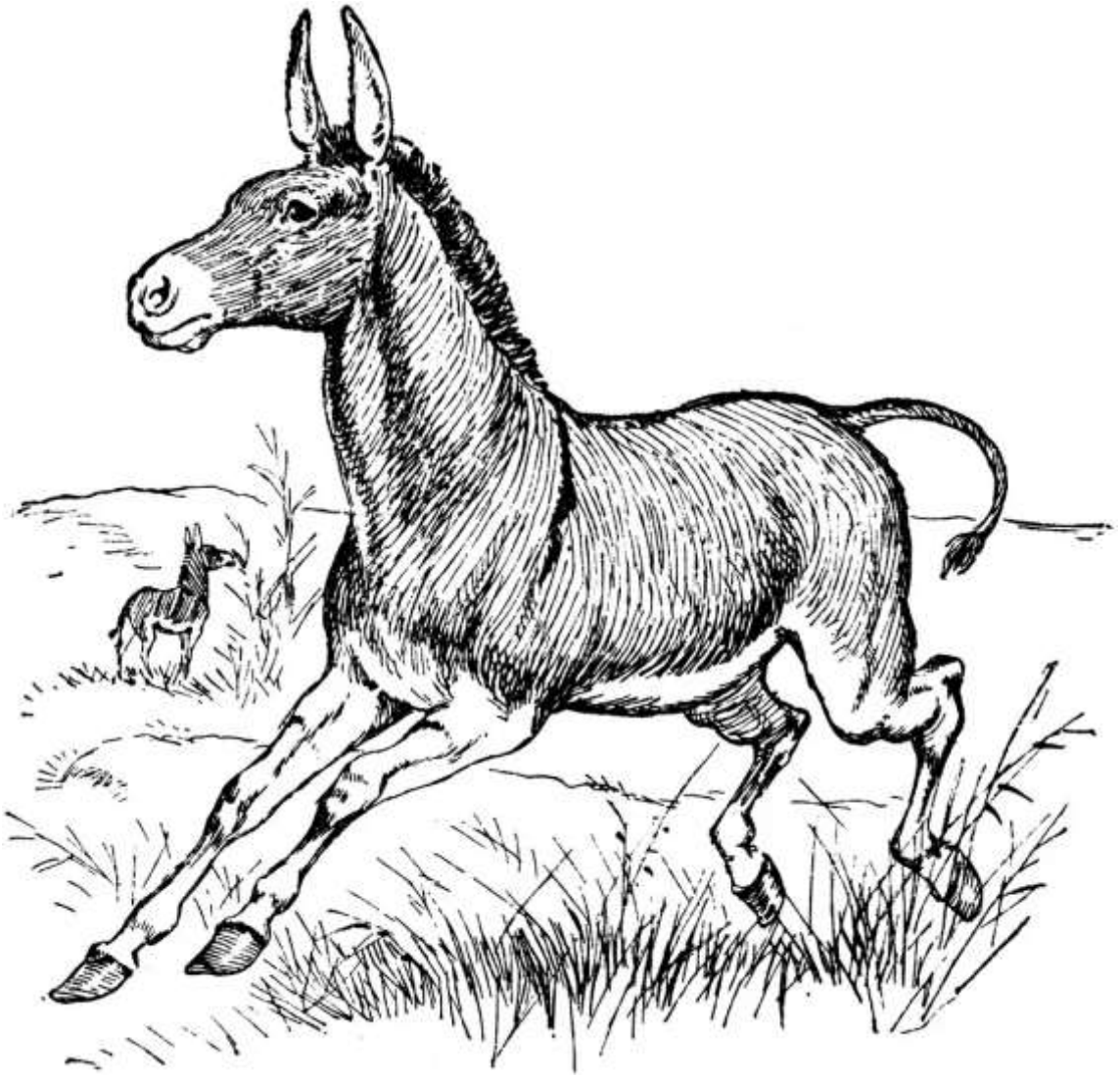
Learn some basic stuffs of polynomials



Delving into Polynomials

An unpractical guide

Rhodes Island

Amiya

Table of Contents

Preface

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。

这是写给中学生看的。

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`

就先说到这里。

评注 总算写完 Prerequisites 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

Delving into Polynomials

Out of boredom, I wrote the article.

Gohan ni suru? Ofuro ni suru? Sore tomo… wa ta shi?
(Would you like dinner? Would you like a bath? Or… would you like me?)

Prerequisites

您将在本节熟悉一些记号与术语。建议您熟悉本节的内容后学习下一节的内容。

在进入小节 Sets 前, 让我们先回顾复数与数学归纳法吧!

定义 复数 (*complex number*) 是形如 $x+y\mathrm{i}$ (x, y 是实数) 的数。

评注 可将 $x+y\mathrm{i}$ 写为 $x+\mathrm{i}y$。

定义 设 a, b, c, d 是实数。则

$$a+b\mathrm{i}=c+d\mathrm{i} \iff a=c \text{ and } b=d。$$

评注 我们把形如 $a+0\mathrm{i}$ 的复数写为 a, 并认为 $a+0\mathrm{i}$ 是实数。反过来, a 也可以认为是复数 $a+0\mathrm{i}$。

形如 $0+b\mathrm{i}$ 的复数可写为 $b\mathrm{i}$。按照习惯, $1\mathrm{i}$ 可写为 i, 且 $-1\mathrm{i}$ 可写为 $-\mathrm{i}$。

定义 复数的加、乘法定义为

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

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:

$$\mathrm{i}\cdot\mathrm{i}=(0+1\mathrm{i})(0+1\mathrm{i})=(0\cdot 0-1\cdot 1)+(0\cdot 1+1\cdot 0)\mathrm{i}=-1。$$

简单地说, 就是

$$\mathrm{i}\cdot\mathrm{i}=\mathrm{i}^2=-1。$$

设 z_1, z_2, z_3 是任意三个复数 (不必不同)。设 $z_1=a+b\mathrm{i}$。

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 $w=(-a)+(-b)\mathrm{i}$ 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 $(-a)+(-b)\mathrm{i}$ 可写为 $-a-b\mathrm{i}$。

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) 若 $z_1 \neq 0$, 则存在复数 $v = \frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}\mathrm{i}$ 使 $v z_1 = 1$。
通常把适合 (viii) 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:

$$z_1(z_2 + z_3) = z_1 z_2 + z_1 z_3,$$
$$(z_2 + z_3) z_1 = z_2 z_1 + z_3 z_1。$$

评注 a, $b\mathrm{i}$, c, $d\mathrm{i}$ 都可以看成是复数。这样

$$\begin{aligned}(a + b\mathrm{i})(c + d\mathrm{i}) &= (a + b\mathrm{i})c + (a + b\mathrm{i})(d\mathrm{i}) \\ &= ac + bc\mathrm{i} + ad\mathrm{i} + bd\mathrm{i}\mathrm{i} \\ &= ac + bc\mathrm{i} + ad\mathrm{i} + bd\mathrm{i}^2 \\ &= (ac + bd\mathrm{i}^2) + (ad + bc)\mathrm{i} \\ &= (ac - bd) + (ad + bc)\mathrm{i}。\end{aligned}$$

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

定义 $a + b\mathrm{i}$ 的共轭 (*conjugate*) 是复数 $a - b\mathrm{i}$ 。复数 z_1 的共轭可写为 $\overline{z_1}$。

命题 共轭适合如下性质:
(ix) $\overline{z_1} + z_1$ 与 $\mathrm{i} \cdot (\overline{z_1} - z_1)$ 都是实数;
(x) $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$, $\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$;
(xi) $\overline{z_1} z_1$ 是正数, 除非 $z_1 = 0$。

定义 $|z_1| = \sqrt{\overline{z_1} z_1}$ 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?† 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,

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

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

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

† 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。

因为

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

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,

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

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

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

由于

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

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[†]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 $n = 1$ 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 ℓ $(\ell \geq 1)$ 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, ⋯, ℓ 有着相同的发色, 且老婆 2, ⋯, ℓ, $\ell+1$ 有着相同的发色。这二组中都有 2, ⋯, ℓ 这 $\ell - 1$ 个老婆, 所以老婆 1, 2, ⋯, ℓ, $\ell+1$ 有着相同的发色!

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。这也叫数学归纳法。

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 $P(n_0)$, $P(n_0 + 1)$, ⋯, $P(\ell)$ 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。

知识就回顾到这里。开始进入集的世界吧!

Sets

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, ⋯ 作成, 我们写

$$A = \{\, a, b, c, \cdots \}。$$

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

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

[†] 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。

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 $a \notin A$, 说 a 不属于 A。[†]

例 全体整数作成的集用 $\mathbb{Z}$ (*Zahl*)[‡] 表示。它可以写为

$$\mathbb{Z} = \{\, 0, 1, -1, 2, -2, \cdots, n, -n, \cdots \,\}。$$

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

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

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 $x - y$, $\frac{x}{y} \in F$。
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

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

[†] 有点尴尬, 我太菜了, 那个 "不包含" 符号打不出来。

[‡] A German word which means *number*.

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。

Functions

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

$$\begin{aligned} f\colon \quad & A \to B, \\ & a \mapsto b = f(a)。 \end{aligned}$$

称 A 是定义域 (*domain*), B 是陪域[†] (*codomain*)。

[†] 不要混淆陪域与象集 (*image, range*)。f 的象集是

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

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。

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

是函数: 它表示点 (x,y) 到点 $(0,0)$ 的距离。

例 设

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

法则

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

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

法则

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

不是 A 到 B 的函数, 因为它给 A 的元 me 规定的象不唯一。

法则

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

不是 A 到 B 的函数, 因为它给 A 的元 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。

Binary Functions

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

$$\begin{aligned} g \circ f\colon \quad & A \to A, \\ & a \mapsto g(f(a))。 \end{aligned}$$

所以, 复合是 $T(A)$ 的二元运算:

$$\begin{aligned} \circ\colon \quad & T(A) \times T(A) \to T(A), \\ & (g, f) \mapsto g \circ f。 \end{aligned}$$

评注 设 A 有有限多个元。此时, 可排出 A 的元:

$$A = \{\, a_1, a_2, \cdots, a_n \,\}。$$

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 $\mathbb{F}_{\mathrm{nu}}$ 是将 $\mathbb{F}$ 去掉 0, 1 后得到的集[†]。看下列 6 个法则:

f_0: $x \mapsto x$;

f_1: $x \mapsto 1 - x$;

f_2: $x \mapsto \dfrac{1}{x}$;

f_3: $x \mapsto 1 - \dfrac{1}{1-x}$;

f_4: $x \mapsto 1 - \dfrac{1}{x}$;

f_5: $x \mapsto \dfrac{1}{1-x}$。

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

[†] 这个 $\mathbb{F}_{\mathrm{nu}}$ 只是临时记号: nu 表示 *nil*, *unity*。

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。

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

$$(h \circ (g \circ f))(a) = h((g \circ f)(a)) = h(g(f(a))),$$
$$((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h(g(f(a)))。$$

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

$$x \cdot (y + z) = x \cdot y + x \cdot z, \tag{LD}$$

则说 $+$ 与 $\cdot$ 适合左 $(\cdot)$ 分配律[†] (*left distributivity*)。类似地, 若

$$(y + z) \cdot x = y \cdot x + z \cdot x, \tag{RD}$$

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

$$x \circ y = x \circ z \implies y = z, \tag{LC}$$

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

$$x \circ z = y \circ z \implies x = y, \tag{RC}$$

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[‡]。

[†] 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。

[‡] 后面提到整环时, 我们会稍微修改一下消去律的描述。

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: $a \mapsto a, \quad b \mapsto b, \quad x \mapsto x$ where $x \neq a, b$;

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

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

g_3: $a \mapsto b, \quad b \mapsto a, \quad x \mapsto x$ where $x \neq a, b$。

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 $T(\mathbb{F}_{\mathrm{nu}})$ 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) 幺元 (*identity*)。如果 e' 也是幺元, 则

$$e = e \circ e' = e'。$$

例 $\mathbb{F}$ 的加法的幺元是 0, 且其乘法的幺元是 1。

例 不难看出, 这个变换是 $T(A)$ 的幺元:

ι: $$A \to A,$$
$$a \mapsto a。$$

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 ι。

定义 设 $\circ$ 是 A 的二元运算。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 是幺元 ι。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 $8 \cdot 125$。

Semi-groups and Groups

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 (*proposition*) 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 $\circ$ 的幺元存在, 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

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

由于 $\circ$ 适合结合律,

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

也就是

$$e\circ y = e\circ z_{\circ}$$

这样, $y = z_{\circ}$ 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,

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

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

$$(x\circ y)^m = x^m \circ y^m_{\circ}$$

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。

Subgroups

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 $x\circ y^{-1} \in H_{\circ}$

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

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

$\circ$ 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 $\circ$ 的幺元存在。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 的幺元也是 H 的幺元, 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 有幺元 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,

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

取 $y \in H$。y 在 H 里有逆元 z, 即

$$z \circ y = y \circ z = e_H = e_\circ$$

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。

Additive Groups

定义 若 G 关于名为 $+$ 的二元运算作成群, 幺元 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

$$\begin{aligned} &(m+n)x = mx + nx, \\ &m(nx) = (mn)x, \\ &m(x+y) = mx + my_\circ \end{aligned}$$

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

$$x + y = x + z \implies y = z_\circ$$

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

$$-(-x) = x_\circ$$

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 $x-y\in H$。”

Sums

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 $p\le q$, 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, $n\ge 0$ 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 $\sum_{j=p}^{q}\left(\sum_{i=m}^{n} f(i,j)\right)$ 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 $(n-m=1)$。

Rings

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 $\cdot$ 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 k 的倍作成的集是环。

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

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

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

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

假如 R 有二个元 x, y 适合 $xy = yx$, 那么还有

$$(xy)^m = x^my^m。$$

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。

Domains

定义 设 D 是环。假设

(i) 任取 $x, y \in D$, 必有 $xy = yx$;

(i) 存在 $1 \in D$, $1 \neq 0$, 使任取 $x \in D$, 必有 $1x = x1 = x$;

(ii) $\cdot$ 适合 "消去律变体"[†]: 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 $x + sy$ $(x, y \in \mathbb{Z})$ 的数作成一个整环。

例 看一个有限整环的例。设 V (*Vierergruppe*)[‡] 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	τ	τ^2
0	0	1	τ	τ^2
1	1	0	τ^2	τ
τ	τ	τ^2	0	1
τ^2	τ^2	τ	1	0

$\cdot$	0	1	τ	τ^2
0	0	0	0	0
1	0	1	τ	τ^2
τ	0	τ	τ^2	1
τ^2	0	τ^2	1	τ

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。

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

$$\begin{aligned}
&(a, b) = (c, d) \iff a = b \text{ and } c = d,\\
&(a, b) + (c, d) = (a + b, c + d),\\
&(a, b)(c, d) = (ac, bd)。
\end{aligned}$$

可以验证, 在这二种运算下, $\mathbb{Z}^2$ 作成一个交换环, 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。

[†] 一般地, 这也可称为消去律。

[‡] A German word which means *four-group*.

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

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

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, $\mathbb{Z}\subset D$。

Sums and Products

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 $p\le q$, 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, $\cdots$, 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:

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

评注 因为整环的乘法也适合结合律与交换律, 所以

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

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

例 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[†]

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

进而, 当 c, d 都是常元时,

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

评注 类似地, 当 $q\geq p$, c 是常元时,

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

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

$$m!!=m\cdot(m-2)!!。$$

[†] 这样的元称为常元 (*constant*)。

双阶乘可以用阶乘表示:

$$(2n)!! = 2^n n!,$$
$$(2n-1)!! = \frac{(2n)!}{(2n)!!} = \frac{(2n)!}{2^n n!}。$$

由此可得

$$n!! \cdot (n-1)!! = n!。$$

例 不难验证, 下面是 1 至 10 的双阶乘:

$$1!! = 1, \qquad 2!! = 2,$$
$$3!! = 3, \qquad 4!! = 8,$$
$$5!! = 15, \qquad 6!! = 48,$$
$$7!! = 105, \qquad 8!! = 384,$$
$$9!! = 945, \qquad 10!! = 3\,840。$$

Units and Fields

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。它有无数个单位: 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 m, n 不全为 3 的倍。这样

$$m^2 = 3n^2。$$

所以 m^2 一定是 3 的倍。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, m 也是 3 的倍。记 $m = 3u$。这样

$$3u^2 = n^2。$$

所以 n 也是 3 的倍。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 是大于 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 有无数多个单位。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 的不是 0 的元都是 F 的单位, 则说 F 是域 (*field*)。

例 上面的 $\mathbb{F}$ 跟 V 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 $F \subset C$, 且 F 是域。不难看出, $\mathbb{Q} \subset F$。

Definition of Polynomials

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^{th} coefficient*), a_ix^i 称为其 i 次项 (*the i^{th} coefficient*)。$f(x)$ 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

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

当然, 还约定, 零多项式只跟自己相等。换句话说,

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

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。

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。

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

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

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。 ✌

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

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

评注 既然 $D[x]$ 是加群, 且每个 a_ix^i $(i=0,1,\cdots,n)$ 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*):

$$a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0x^0。$$

这跟中学里接触的多项式是一样的。当然, 也可以用 $\sum$ 符号书写:

$$\sum_{i=0}^{n}a_ix^i\quad\text{or}\quad\sum_{i=0}^{n}a_{n-i}x^{n-i}。$$

(非零) 多项式的最高次非零项是首项 (*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 $-7y^4$。

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

$$\begin{aligned}
c_0&=1\cdot(-3)=-3,\\
c_1&=1\cdot 4+0\cdot(-3)=4,\\
c_2&=1\cdot 0+0\cdot 4+2\cdot(-3)=-6,\\
c_3&=1\cdot(-1)+0\cdot 0+2\cdot 4=7,\\
c_4&=0\cdot(-1)+2\cdot 0=0,\\
c_5&=2\cdot(-1)=-2。
\end{aligned}$$

所以

$$f(x)g(x)=-3x^0+4x-6x^2+7x^3-2x^5。$$

例 再看一个例。设

$$f(x)=x,\quad g(x)=x^\ell。$$

a_i 在 $i=1$ 时为 1, $i\neq 1$ 时为 0; b_j 在 $j=\ell$ 时为 1, $j\neq\ell$ 时为 0。

$\ell=0$ 时, 不难算出, $f(x)g(x)=x$。现在设 $\ell\geq 1$。$k\leq\ell$ 时,

$$c_k=0b_k+1\cdot 0+\cdots+0\cdot 0=0。$$

$k=\ell+1$ 时,

$$c_{\ell+1}=0\cdot 0+1\cdot 1+0\cdot 0+\cdots+0\cdot 0=1。$$

所以

$$x\cdot x^\ell=x^{\ell+1}。$$

这样, x^ℓ 可以视为 x 的 ℓ 次幂。

评注 由上面二个例可以看到, 这跟中学的多项式乘法运算没有什么本质区别。

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。

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

$$\begin{aligned} f(x) &= a_0x^0 + a_1x + \cdots + a_mx^m, \\ g(x) &= b_0x^0 + b_1x + \cdots + b_nx^n, \\ h(x) &= u_0x^0 + u_1x + \cdots + u_sx^s \end{aligned}$$

是 $D[x]$ 的元。则

$$\begin{aligned} f(x)g(x) &= c_0x^0 + c_1x + \cdots + c_{m+n}x^{m+n}, \\ g(x)f(x) &= d_0x^0 + d_1x + \cdots + d_{n+m}x^{n+m}, \end{aligned}$$

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

$$v_t = (\text{the sum of all } a_ib_ju_r\text{'s with } i + j + r = t)。$$

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: 一是乘法幺元, 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!

再看乘法幺元。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。 ✌

评注 以后, 我们把 x^0 写为 1。换句话说, 代替

$$a_0x^0+a_1x+\cdots+a_nx^n,$$

我们写

$$a_0+a_1x+\cdots+a_nx^n。$$

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。

Division Algorithm

我们知道, 非负整数有这样的性质:

命题 设 n 是正整数, m 是非负整数。则必有一对非负整数 q,r 使

$$m=qn+r,\quad 0\leq r<n。$$

例如, 取 $n=5$, $m=23$。不难看出,

$$18=4\cdot 5+3。$$

多项式也有类似的性质哟。

命题 设

$$f(x)=\sum_{i=0}^{n}a_ix^i\in D[x],$$

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 $m\le\ell$ $(\ell\ge n-1)$ 时, 命题成立。考虑 $m=\ell+1$ 的情形。此时, 设

$$g(x)=\sum_{i=0}^{\ell+1}b_ix^i。$$

则

$$\begin{aligned}
&g(x)-b_{\ell+1}a_n^{-1}x^{\ell+1-n}f(x)\\
=&\sum_{i=0}^{\ell+1}b_ix^i-b_{\ell+1}a_n^{-1}x^{\ell+1-n}\sum_{i=0}^{n}a_ix^i\\
=&\sum_{i=0}^{\ell}b_ix^i+b_{\ell+1}x^{\ell+1}-\sum_{i=0}^{n-1}b_{\ell+1}a_n^{-1}a_ix^{\ell+1-n+i}-b_{\ell+1}a_n^{-1}a_nx^{\ell+1}\\
=&\sum_{i=0}^{\ell}b_ix^i-\sum_{i=0}^{n-1}b_{\ell+1}a_n^{-1}a_ix^{\ell+1-n+i}+b_{\ell+1}x^{\ell+1}-b_{\ell+1}x^{\ell+1}\\
=&\sum_{i=0}^{\ell}b_ix^i-\sum_{i=0}^{n-1}b_{\ell+1}a_n^{-1}a_ix^{\ell+1-n+i}。
\end{aligned}$$

设 $r_1(x)=g(x)-b_{\ell+1}a_n^{-1}x^{\ell+1-n}f(x)$。这样, $r_1(x)$ 的次不高于 ℓ。根据归纳假设, 有 $q_1(x),r(x)\in D[x]$ 使

$$r_1(x)=q_1(x)f(x)+r(x),\quad \deg r(x)<n。$$

所以

$$\begin{aligned}
g(x)&=b_{\ell+1}a_n^{-1}x^{\ell+1-n}f(x)+r_1(x)\\
&=b_{\ell+1}a_n^{-1}x^{\ell+1-n}f(x)+q_1(x)f(x)+r(x)\\
&=(b_{\ell+1}a_n^{-1}+q_1(x))f(x)+r(x)。
\end{aligned}$$

记 $q(x)=b_{\ell+1}a_n^{-1}+q_1(x)$, 则 $q(x),r(x)$ 适合要求。所以, $m\le\ell+1$ 时, 命题成立。根据数学归纳法, 命题成立。 ✌

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

$$r(x) = r_0, \quad q(x) = \sum_{i=0}^{p} q_i x^i, \quad g(x) = \sum_{i=0}^{s} g_i x^i,$$

且 $r_0, q_0, \cdots, q_p, g_0, \cdots, g_s \in \mathbb{Z}$。由 $g(x) = q(x)f(x) + r(x)$ 知

$$\sum_{i=0}^{s} g_i x^i = r_0 + \sum_{i=1}^{p+1} 2q_{i-1} x^i。$$

所以

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

这说明, $g(x)$ 的 i 项系数 $(i = 1, \cdots, s)$ 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。

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

$$\begin{aligned} &q_1(x)f(x) + r_1(x) = q_2(x)f(x) + r_2(x), \\ &\deg r_1(x) < \deg f(x), \quad \deg r_2(x) < \deg f(x), \end{aligned}$$

则必有

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

证 记

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

题设条件即

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

也就是

$$-Q(x)f(x) = R(x)。$$

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

$$\deg R(x) = \deg(r_2(x) - r_1(x)) \leq \deg r_1(x) < \deg f(x),$$

矛盾! 故 $-Q(x) = 0$。这样, $R(x) = 0$。 ✌

这样, 我们得到了这个命题:

命题 设

$$f(x) = \sum_{i=0}^{n} a_i x^i \in D[x],$$

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:

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

Roots of Polynomials

我们回顾一下熟悉的多项式函数。

定义 设 $a_0, a_1, \cdots, a_n \in D$ 称

$$\begin{aligned} f\colon \quad & D \to D, \\ & t \mapsto a_0 + a_1 t + \cdots + a_n t^n \end{aligned}$$

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

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

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

$$\begin{aligned} f+g\colon \quad & D \to D, \\ & t \mapsto f(t) + g(t)。 \end{aligned}$$

二者的积 fg 定义为

$$\begin{aligned} fg\colon \quad & D \to D, \\ & t \mapsto f(t)g(t)。 \end{aligned}$$

例 设 f, g 是 D 的二个多项式函数:

$$\begin{aligned} f\colon \quad & D \to D, \\ & t \mapsto a_0 + a_1 t + \cdots + a_n t^n, \\ g\colon \quad & D \to D, \\ & t \mapsto b_0 + b_1 t + \cdots + b_n t^n。 \end{aligned}$$

利用 D 的运算律, 可以得到

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

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, 就是: 若多项式 $f_1(x)$, $f_2(x)$, $\cdots$, $f_n(x)$ 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, 有这样的问题: 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 $V = \{0, 1, \tau, \tau^2\}$。它的加法与乘法如下:

$+$	0	1	τ	τ^2
0	0	1	τ	τ^2
1	1	0	τ^2	τ
τ	τ	τ^2	0	1
τ^2	τ^2	τ	1	0

$\cdot$	0	1	τ	τ^2
0	0	0	0	0
1	0	1	τ	τ^2
τ	0	τ	τ^2	1
τ^2	0	τ^2	1	τ

在前面, 我们已经知道, V 是整环。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

$$f(t)=a_0+a_1t+\cdots+a_nt^n。$$

至少, 一方通行 (*one-way traffic*) 是没问题的。

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

$$f(x)=q(x)(x-a)+f(a)。$$

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 $r=0$)。

那么, 这有什么用呢? 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。之后我们还会提到这一点。

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, $\frac{1}{2}$, $\pm\sqrt{3}$, $\pm\mathrm{i}$, $\pm 2\mathrm{i}$。

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 τ, τ^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

$$f(x) = q(x)(x-a)。$$

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

$$f(x) = q(a)(x-a) + f(a) = q(a)(x-a)。$$ 🐰

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 ℓ 次多项式至多有 ℓ 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 ℓ 次多项式 $q(x)$ 使

$$f(x) = q(x)(x - a)。$$

根据归纳假设, $q(x)$ 至多有 ℓ 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。 ✌