Untitled

Septsea

First released on the Internet, in June 2021

Abstract

This is an untitled article.

Table of Contents

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。

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

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。不必细品。本节有很多定义。不要害怕: 就当是认识一下词语好了。本文主要讨论多项式, 所以并不会过多涉及到本节内容。说白了, 本节是工具节。

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, $\cdots$ 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

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

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。

[†] 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*.

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

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

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

$$f\colon \quad A \to B, \quad a \mapsto b = f(a)。$$

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

例 可以把 $\mathbb{R}^2$ 看作平面上的点集。所以

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

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。

† 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”。

法则

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

不是 A 到 B 的函数, 因为它给 A 的元 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

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

所以, 复合是 $T(A)$ 的二元运算:

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

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, $1\le i,j\le n$, 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:

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

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

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 举例子。

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 $x\circ y\circ z$。

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

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。

[†] 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 $x + (y \cdot z) = (x + y) \cdot (x + z)$。但有意思的是, 如果把 $+$ 理解为并, $\cdot$ 理解为交, x, y, z 理解为集, 那这个式子是对的。当然, $x \cdot (y + z) = x \cdot y + x \cdot z$ 也是对的。

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

$$\text{(LC)}\qquad x\circ y=x\circ z \implies y=z,$$

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

$$\text{(RC)}\qquad x\circ z=y\circ z \implies x=y,$$

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†。

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:

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

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

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

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

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。

† 后面提到整环时, 我们会稍微修改一下消去律的描述。

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:

$$\begin{aligned} \iota: \quad & A \to A, \\ & a \mapsto a。 \end{aligned}$$

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 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,

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

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。

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 $x \circ y^{-1} \in H$。

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,

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

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。

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

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

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

$$x + y = x + z \implies y = z。$$

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 $x - y \in H$。”

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:

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

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 $q \ge p$, $n \ge m$。$\sum_{i=m}^{n} f(i,j)$ 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:

$$\begin{array}{cccc|c}
f(m,p) & f(m,p+1) & \cdots & f(m,q) & R_m \\
f(m+1,p) & f(m+1,p+1) & \cdots & f(m+1,q) & R_{m+1} \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
f(n,p) & f(n,p+1) & \cdots & f(n,q) & R_n \\
\hline
C_p & C_{p+1} & \cdots & C_q &
\end{array}$$

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 上面的例子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*) 例子。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"。在上个例子里, 取 $k=0$ 就是 N。

例　这里举一个 "不平凡的" (*nontrivial*) 例子。设 $R = \{0, a, b, c\}$。加法和乘法由以下两个表给定:

$+$	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。

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子。设 V ($Vierergruppe$‡) 是 4 元集:

$$V = \{\, 0, 1, \tau, \tau^2 \,\}。$$

† 一般地, 这也可称为消去律。
‡ A German word which means *four-group*.

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子。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。

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 $x-y\in S$, $xy\in S$。”

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, ···, 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,

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

† 这样的元称为常元 (*constant*)。

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 个正偶数的乘积是 $2n$ 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:

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