

交换代数

第 1 讲讲义

郭宁

2026 年 9 月

1.1 第 1 讲 环、单位与素理想

1.1.1 半群：从计数开始

古希腊数学家丢番图(Διόφαντος ὁ Ἀλεξανδρεὺς)的《代数学》中,直接将两数并列或用文字叙述来代表加法;而在中国古代,商周时期的筹算就能熟练施行多位数的加减运算. 在目前的时代,我们记

$$\mathbb{N} := \{1, 2, 3, 4, \dots, \}$$

为自然数的集合. 自然数集合 $\mathbb{N}$ 在加法运算(记作“+”)下构成半群. 回忆这个概念.

定义 1.1. 集合 S 是半群(semigroup)是指 S 在某个结合性二元运算“*”之下封闭,即

$$*: S \times S \rightarrow S, \quad (a, b) \mapsto a * b$$

且 $(a * b) * c = a * (b * c)$. 若 S 有么元(identity element), 即元素 $e \in S$ 使得 $e * a = a * e = a$ 对任意 $a \in S$ 成立(这推得么元唯一), 则 S 是么半群(monoid). 一旦 $*$ 是交换的, 即任意 $a, b \in S$ 满足 $a * b = b * a$, 则称 $*$ 是加法运算, 无歧义时记作“+”.

本讲义统一把 identity element 译为“么元”. “单位元”是它的另一种中文译名, 后文不再采用. 若么半群中有元素 a, b 满足 $ab = ba = e$, 则称 b 为 a 的逆元(inverse), 并称 a 是可逆的(invertible). 这样的元素在英文中称为 unit, 本书译作单位; 这一名词主要用于环的乘法. 因此么元本身是一个单位, 但单位不必等于么元.

为使自然数半群 $\mathbb{N}$ 成为么半群, 我们引入加法的么元“0”. 数字“0”起源于古印度, 最初作为一个占位符和小圆点符号来表示空位. 公元 628 年, 印度数学家婆羅摩笈多(Brahmagupta)在著作《婆罗摩历算书》中, 首次系统化地给出了零的数学运算规则, 把 0 当作一个真正的数字来计算. 我们模仿古印度人的构造, 把半群变成么半群:

$$S^1 := S \sqcup \{e\}, \quad \text{扩展结合二元运算 } *^1 \text{ 使得 } a *^1 e = e *^1 a = a \quad \forall a \in S.$$

即, 任何半群均可嵌入么半群作为子半群. 特别地, 自然数加法半群的么半群化记为

$$\mathbb{N}_0 := \mathbb{N} \cup \{0\}.$$

若 M, N 是交换么半群, 则映射 $f: M \rightarrow N$ 称为么半群同态, 若 $f(a + b) = f(a) + f(b)$ 对所有 $a, b \in M$ 成立, 并且 $f(0_M) = 0_N$.

1.1.2 群:可逆运算与对称性

加法幺半群 $\mathbb{N}_0$ 已有幺元, 却仍不能施行所有减法: 例如方程 $1 + x = 0$ 在 $\mathbb{N}_0$ 中无解. 从幺半群到群, 还需要每个元素都有“逆元”.

定义 1.2. 设 G 是幺半群, 运算记作“ $*$ ”, 幺元记作 e . 若对每个 $g \in G$, 都存在 $h \in G$ 使

$$g * h = h * g = e,$$

则称 G 为群, 并称 h 为 g 的逆元, 记作 g^{-1} . 若进一步有 $g * h = h * g$ 对任意 $g, h \in G$ 成立, 则称 G 为交换群或阿贝尔群.

逆元由 g 唯一决定. 事实上, 若 h 与 k 都是 g 的逆元, 则 $h = h * e = h * (g * k) = (h * g) * k = e * k = k$. 还应注意乘积求逆时次序反转: $(g * h)^{-1} = h^{-1} * g^{-1}$.

交换群通常采用加法记号: 幺元写成 0 , 元素 g 的逆元写成 $-g$, 运算写成 $g + h$. 于是群公理中的可逆性成为 $g + (-g) = 0$. 乘法记号则更适合置换、矩阵与算子的复合.

例 1.3 (平凡群). 若 $G = \{e\}$ 为仅由幺元组成的群, 则称其为平凡群.

例 1.4 (整数加法群). 记全体整数的集合为¹

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

它在加法下构成交换群: 幺元是 0 , 整数 n 的逆元是 $-n$. 自然数幺半群 $\mathbb{N}_0$ 含在 $\mathbb{Z}$ 中. 从 $\mathbb{N}_0$ 得到 $\mathbb{Z}$, 正是对于加法运算补入所有逆元.

定义 1.5. 设 G, H 是群, 幺元分别记作 e_G, e_H , 运算采用乘法记号.

- (1) 映射 $\varphi: G \rightarrow H$ 称为群同态, 若 $\varphi(gh) = \varphi(g)\varphi(h)$ 对任意 $g, h \in G$ 成立.
- (2) 若 φ 为群同态, 称 $\varphi^{-1}(e_H)$ 为 φ 的核(它是 G 的子群), 记作 $\ker(\varphi)$.
- (3) 若群同态 φ 是双射, 则称之为群同构, 记为 $G \cong H$.

同态只需保持乘法, 就自动保持幺元和逆元.

例 1.6 (有理数乘法群). 非零有理数的集合记为 $\mathbb{Q}^\times$. 它在乘法下构成交换群: 幺元是 1 , 而 a/b 的逆元是 b/a . 不同分式可能表示同一有理数; 对 $a, b, c, d \in \mathbb{Z}$ 且 $b, d \neq 0$, 有

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

例如 $2/3 = 4/6$. 集合 $\mathbb{Q}$ 还含有 0 ; 因为 0 没有乘法逆元, $\mathbb{Q}$ 本身在乘法下不是群.

¹记号 $\mathbb{Z}$ 源自德语单词 Zahlen,

从 $\mathbb{N}_0$ 发展到 $\mathbb{Z}$ 再到 $\mathbb{Q}$ 的次序与历史发展并不相同. 分数的使用远早于负数成为普遍接受的数. 约公元前 1650 年, 书吏阿赫莫斯(Ahmosé)抄写的莱因德数学纸草书已经系统处理除法与分数, 并列出把 $2/n$ 写成单位分数之和的表. 这些计算来自配给、面积和容积等问题, 其中“一个量被另一个量除”先于有理数的抽象构造出现.



莱因德数学纸草书第一部分左侧残片, 约公元前 1650 年, 由书吏阿赫莫斯抄写. 全卷包含除法表、单位分数计算及几何问题.²

例 1.7 (有理数、实数与复数的加法群). $\mathbb{Q}, \mathbb{R}$ 与 $\mathbb{C}$ 在加法下都是交换群, 么元均为 0, 元素 x 的逆元均为 $-x$. 它们依次包含 $(\mathbb{Z}, +) \subseteq (\mathbb{Q}, +) \subseteq (\mathbb{R}, +) \subseteq (\mathbb{C}, +)$. 这三个数系在乘法下不构成群: 0 没有乘法逆元, 删去 0 后才得到 $\mathbb{Q}^\times, \mathbb{R}^\times$ 与 $\mathbb{C}^\times$.

例 1.8 (圆群 S^1). 在复平面 $\mathbb{C}$ 中, 令 $S^1 := \{e^{i\phi} : \phi \in \mathbb{R}\}$. 复数乘法给出 $e^{i\alpha}e^{i\beta} = e^{i(\alpha+\beta)}$; 么元为 $1 = e^{0i}$, 而 $e^{i\alpha}$ 的逆元是 $e^{-i\alpha}$. 因而 S^1 是交换群. 指数映射

$$(\mathbb{R}, +) \longrightarrow S^1, \quad x \longmapsto e^{ix}$$

是满群同态, 并且 $e^{ix} = e^{iy}$ 当且仅当 $x - y \in 2\pi\mathbb{Z}$. 因此圆群把实数加法按周期 2π 卷到单位圆周上; 实数直线上的平移在这里成为绕原点的旋转.

例 1.9 ($\mathbb{N}_0$ 的作用). 设 $m \geq 2$, 集合 $B_m := \{x_0, \dots, x_{m-1}\}$ 由 m 个元素构成. 考虑映射

$$\mathbb{N}_0 \times B_m \rightarrow B_m, \quad (n, x_r) \mapsto x_{(r+n) \bmod m}.$$

这里 0 保持每个元素不变, 并且 $(n + n') \cdot x_r = n \cdot (n' \cdot x_r)$, 故这确实是么半群作用. 该

²图源: Wikimedia Commons, Rhind Mathematical Papyrus; 藏品为大英博物馆 EA10057.

作用由 1 的作用生成; 相对于有序排列 $(x_0, \dots, x_{m-1})$, 生成元 1 的置换矩阵是

$$P_m = \begin{pmatrix} & & 1 \\ 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}.$$

因此 n 的作用由 P_m^n 给出. 由于 $P_m^m = I_m$, 该作用只依赖于 n 模 m 的剩余类, 从而经由 $\mathbb{Z}/m\mathbb{Z}$ 分解. 把 P_m 视为复向量空间 $\mathbb{C}^m$ 上的算子, 它是酉算子³, 且 $P_m^{-1} = P_m^{m-1}$. 因而这个 $\mathbb{N}_0$ 作用还可延伸为 $\mathbb{Z}$ 作用, 其中负整数 $-n$ 由 P_m^{-n} 作用.

若考虑无限可数集合 $B_\infty := \{x_1, x_2, \dots, x_m, \dots\}$, 则 $\mathbb{N}_0$ 仍可作用于 $B_\infty: n \cdot x_r = x_{r+n}$. 生成元 1 把 $(x_1, x_2, \dots)$ 送到 $(x_2, x_3, \dots)$, 其矩阵是

$$S = \begin{pmatrix} 1 & & \\ & 1 & \\ & & \ddots \end{pmatrix}.$$

这里右上角不再有使末端返回起点的 1, 所以 S 的像不含 x_1 . 将 x_r 视为 $\ell^2(\mathbb{N})$ 的标准正交基, S 是左平移算子; 它不是酉算子. 相应的 $\mathbb{N}_0$ 作用不能延伸为同一集合上的 $\mathbb{Z}$ 作用, 这正是无限情形与有限循环作用的区别.

例 1.10 (循环与置换). 集合 X 的所有双射 $X \rightarrow X$ 在映射复合下构成对称群 $\text{Sym}(X)$. 恒等映射是幺元, 每个双射的逆映射就是其群论逆元. 前例中的 P_m 对应循环置换 $(x_0 \ x_1 \ \cdots \ x_{m-1})$ (我们用括弧来简记循环置换: 括弧里每个元素被送到它紧邻右侧的元素, 最右的元素被送到最左的元素), 而 P_m 的次幂构成的集合

$$\langle P_m \rangle := \{I_m, P_m, P_m^2, \dots, P_m^{m-1}\}$$

是一个有 m 个元素的交换群, 并与 $\mathbb{Z}/m\mathbb{Z}$ 同构. 原来的 $\mathbb{N}_0$ 作用之所以能够延伸为 $\mathbb{Z}$ 作用, 正因为它实际上只看见这个有限群.

对称群一般并不交换. 例如在 $\{1, 2, 3\}$ 上, 令 σ 交换 1, 2, 令 τ 交换 2, 3, 并约定复合从右向左施行. 我们采用上例中的括弧记号来表示循环置换. 则 $\sigma\tau = (1 \ 2 \ 3)$, 而 $\tau\sigma = (1 \ 3 \ 2)$, 两者不同. 这里 $(1 \ 2 \ 3)$ 表示 $1 \mapsto 2 \mapsto 3 \mapsto 1$.

例 1.11 (线性群). 有限维实向量空间 $V = \mathbb{R}^n$ 到自身的全体线性变换在复合运算下构成幺半群 $M_n(\mathbb{R})$, 其中每个元素都是 $n \times n$ 的实矩阵. 其中, 可逆线性变换构成一个群 $\text{GL}_n(\mathbb{R})$, 称为 n 维实向量空间的一般线性群, 其中每个元素 $A \in M_n(\mathbb{R})$ 满足

³设 H 为复 Hilbert 空间. 线性算子 $U: H \rightarrow H$ 称为有界的 (即存在 $C \geq 0$, 使 $\|Ux\| \leq C\|x\|$ 对所有 $x \in H$ 成立). 若 U 有界且 $U^*U = UU^* = I_H$, 则称 U 为酉算子 (unitary operator); 其中 U^* 是 U 的伴随算子 (由 $\langle Ux, y \rangle = \langle x, U^*y \rangle$ 对所有 $x, y \in H$ 确定). 等价地, U 是满射等距同构; 此时 $U^{-1} = U^*$.

$\det(A) \neq 0$. 进一步地, 行列式为 1 的矩阵全体构成一个群 $SL_n(\mathbb{R})$, 称为特殊线性群.

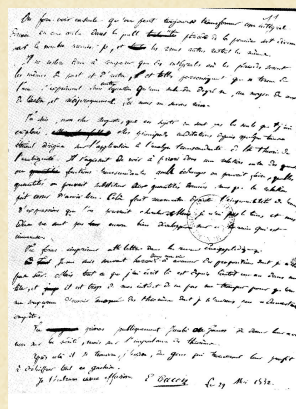
例 1.12 (算子群). 设 E 是 Banach 空间. 全体有界线性算子 $\mathcal{B}(E)$ 在复合下只是么半群; 其中可逆的算子组成一般线性群 $GL(E)$. 对 Hilbert 空间 H , 全体酉算子组成群 $\mathcal{U}(H)$, 因为 $U^{-1} = U^*$, 且酉算子的复合仍是酉算子. 前例的有限循环算子 P_m 属于 $\mathcal{U}(C^m)$, 左平移算子 $S \notin GL(\ell^2(\mathbb{N}))$: 它不是满射, 故没有定义在整个空间的逆算子.

设 G 是么元为 e_G 的群. G 在集合 X 上的作用是映射 $G \times X \rightarrow X, (g, x) \mapsto g \cdot x$, 满足 $e_G \cdot x = x$ 与 $(gh) \cdot x = g \cdot (h \cdot x)$. 对固定的 g , 变换 $x \mapsto g \cdot x$ 自动是双射, 其逆变换由 g^{-1} 给出. 等价地, 群作用就是群同态 $G \rightarrow \text{Sym}(X)$. 反过来, 群也可作用在自身: 每个 $g \in G$ 给出左平移 $L_g(x) = gx$, 并且 $L_g L_h = L_{gh}$. 因而任何群都可视为对称群.

从根的置换到抽象群. 十九世纪初, 代数学家研究多项式方程的根在某些置换下如何影响这些根的多项式组合, 尤其是方程的系数. 例如二次方程 $x^2 + c_1 x + c_0 = 0$ 的两个根为 α, β , 则交换 α 与 β 不改变 $\alpha + \beta = -c_1$ 和 $\alpha\beta = c_0$, 却把 $\alpha - \beta$ 变为 $-(\alpha - \beta)$. 对高次方程同理, 保持某些根的关系的置换可以继续复合, 也可以反向施行, 因此构成群.



Évariste Galois (1811–1832) 肖像, 约 1826 年绘, 后由 Paul Dupuy 于 1896 年刊布.



Galois 于 1832 年 5 月 29 日致 Auguste Chevalier 信札的末页; 信中讨论在保持关系成立时可以施行的量与函数的置换.⁴

Galois 在 1830 年代用法语 *groupe* 称呼这样的置换族. 他的关键思想不是显式地求解根式解, 而是研究哪些根可以互相置换而不破坏方程已有的代数关系, 并由这族置换的结构判断方程能否用根式求解. 群的元素由此不再是普通的“数”, 而是对数学对象的变换. 后来的抽象定义进一步舍去根的具体来源, 只保留复合、么元与逆元; 之前所列举的置换、矩阵、几何对称和可逆算子等被纳入到“群”这个统一的代数框架去研究.

群只涉及一种可逆运算, 而上面的数系例子分别使用整数的加法与非零有理数的乘法. 我们介绍“环”, 它把加法和乘法置于同一结构中; 下面从环的定义开始.

⁴图源: Wikimedia Commons, Galois 肖像与 1832 年 5 月 29 日信札.

1.1.3 环的定义

环论起源于十九世纪, 其两个主要来源是多项式的算术与代数整数的算术. Dedekind 在 1871 年研究代数整数, 并在这一背景下引入理想与模; 他所处理的数系已经是今天所说的环, 却还没有使用“环”这个名称, 也没有把环定义为任意的抽象结构.



David Hilbert
(1862–1943) 肖像.⁵

Hilbert 于 1892 年提出 *Zahlring* 一词, 并使用于在 1897 年发表的《代数数域理论》. *Zahl* 意为“数”, *Zahlring* 即“数环”, 后来简称 *Ring*, 中文译作“环”. 这个名称与代数整数的乘法结构相联系. 例如若 $a^3 - 4a + 1 = 0$, 则 $a^3 = 4a - 1$, $a^4 = 4a^2 - a$, 继续相乘并约去 a^3 后, 每个高次幂 a^n 都是 $1, a, a^2$ 的整数线性组合. 高次幂不断回到有限个低次幂张成的系统中, 这正是早期“数环”的典型情形.

1915 年, Fraenkel 首次给出环的公理化定义, 但条件比今日定义更强. 1921 年, Noether 以现代方式处理含么元与不含么元的交换环, 并奠定抽象交换环论的基础.

定义 1.13. 一个环是一个集合 A , 配备加法与乘法两种运算, 使得 A 对加法构成交换群, 对乘法构成么半群, 并且乘法对加法满足左右分配律:

$$a(b + c) = ab + ac, \quad (a + b)c = ac + bc \quad (a, b, c \in A).$$

若还满足 $ab = ba$ 对所有 $a, b \in A$ 成立, 则称 A 为交换环.

除非另行说明, 以下的环均为交换环. 只含一个元素的环满足 $0 = 1$, 称为零环. 在非零环中 $0 \neq 1$. 对正整数 n , 记 $a^n = a \cdots a$, 其中右端有 n 个因子, 并约定 $a^0 = 1$. 环中的乘法么元相加 n 次所得的元素 $1 + \cdots + 1$ 也记为 $n \in A$.

命题 1.14. 对任意环 A 及 $a, b \in A$, 有

$$0a = a0 = 0, \quad (-a)b = -(ab) = a(-b) \quad \text{以及} \quad (-a)(-b) = ab.$$

证明. 由分配律, $0a = (0 + 0)a = 0a + 0a$. 在加法群中消去 $0a$, 得到 $0a = 0$; 同理 $a0 = 0$. 再由 $ab + (-a)b = (a - a)b = 0$, 可知 $(-a)b$ 是 ab 的加法逆元, 故 $(-a)b = -(ab)$. 其余等式同理. $\square$

例 1.15. 整数集合 $\mathbb{Z}$ 对通常的加法和乘法构成交换环. 有理数 $\mathbb{Q}$ 与实数 $\mathbb{R}$ 也构成交换环. 但是在 $\mathbb{Z}$ 中, 方程 $2x = 1$ 没有整数解; 在 $\mathbb{Q}$ 和 $\mathbb{R}$ 中, 该方程的解都是 $x = 1/2$.

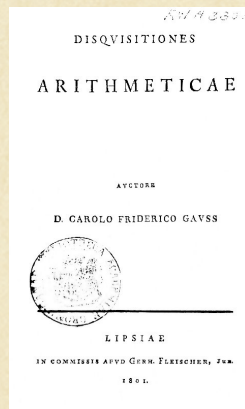
⁵图源: MacTutor, David Hilbert. 历史脉络参考 Wikipedia “环”的历史.

例 1.16 (剩余类环). 固定正整数 n . 把两个整数 a, b 视为相同的剩余类, 当且仅当 n 整除 $a - b$ (我们以 $n \mid a - b$ 记此性质). 剩余类的集合记为 $\mathbb{Z}/n\mathbb{Z}$, 其中元素可以写成 $[m] := m + n\mathbb{Z}$, 其中 m 也称为剩余类 $[m]$ 的一个代表元. 同一个剩余类的可以取不同的代表元, 但是它们总相差 n 的整数倍. 我们定义 $[a] + [b] = [a + b]$ 、 $[a][b] = [ab]$. 这些运算与代表元的选择无关, 并使 $\mathbb{Z}/n\mathbb{Z}$ 成为交换环. 例如在 $\mathbb{Z}/5\mathbb{Z}$ 中, $[2][3] = [1]$; 在 $\mathbb{Z}/6\mathbb{Z}$ 中, $[2][3] = [0]$, 尽管 $[2]$ 与 $[3]$ 都不是零.

〔史略〕 Gauß 的同余算术



Gauß 肖像

Gauß《算术研究》(*Disquisitiones Arithmeticae*)1801 年初版扉页.⁶

1801 年, Gauß 在《算术研究》中以 $a \equiv b \pmod{n}$ 表示 $n \mid (a - b)$. 若 $a \equiv a' \pmod{n}$ 且 $b \equiv b' \pmod{n}$, 则 $a + b \equiv a' + b' \pmod{n}$; 又因 $ab - a'b' = a(b - b') + b'(a - a')$, 也有 $ab \equiv a'b' \pmod{n}$. 现代的剩余类环 $\mathbb{Z}/n\mathbb{Z}$ 正是把 Gauß 的同余运算组织成一个代数对象 [1]^{第 2 条}、[2].

例 1.17 (乘积环). 若 A, B 是交换环, 则笛卡儿积 $A \times B$ 按坐标运算成为交换环: $(a, b) + (a', b') = (a + a', b + b')$, $(a, b)(a', b') = (aa', bb')$. 它的零元是 $(0, 0)$, 乘法幺元是 $(1, 1)$. 若 A, B 都非零, 则 $(1, 0)(0, 1) = (0, 0)$.

例 1.18 (函数环). 设 X 是非空集合, A 是交换环. 所有函数 $f: X \rightarrow A$ 构成交换环 A^X , 其运算逐点定义, 即 $(f + g)(x) = f(x) + g(x)$ 与 $(fg)(x) = f(x)g(x)$. 零元和乘法幺元分别是常值函数 0 与 1.

例 1.19 (连续函数环). 设 X 是紧空间, $\mathbb{F} = \mathbb{R}$ 或 $\mathbb{C}$. 连续函数组成函数环 $\mathbb{F}^X$ 的子环 $C(X, \mathbb{F})$: 两个连续函数之和与乘积仍连续, 常值函数 0, 1 也连续.

例 1.20 (非交换环). 对任意 $n \geq 2$, 实 $n \times n$ 矩阵在通常的加法和乘法下构成含幺元的环 $M_n(\mathbb{R})$. 矩阵乘法一般不交换, 故它是非交换环的基本例子.

⁶两图来源: Wikimedia Commons, Carl Friedrich Gauss.jpg; Disquisitiones-800.jpg.

1.1.4 单位

定义 1.21. 设 A 是环. 若 $a \in A$ 存在 $b \in A$ 使 $ab = ba = 1$, 则称 a 为 单位(unit). 此时 a 是可逆的, b 是它的逆元, 并记为 a^{-1} . 全体单位组成的集合记为 $A^\times$.

一个单位的逆元唯一. 事实上, 若 $ab = ac = 1$, 则 $b = b(ac) = (ba)c = c$. 两个单位的乘积仍是单位, 且 $(ab)^{-1} = b^{-1}a^{-1}$.

〔思路〕 乘法映射的可逆性

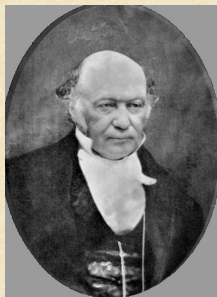
在 $\mathbb{Z}/12\mathbb{Z}$ 上, 乘法映射 $m_{[5]}([x]) = [5x]$ 是双射, 且连续施行两次得到恒等映射, 因为 $[5]^2 = [1]$. 相反, $m_{[3]}([0]) = m_{[3]}([4]) = [0]$, 故 $m_{[3]}$ 不是单射. 这分别对应 $[5]$ 可逆, 而 $[3]$ 不可逆.

例 1.22 (四元数). 四元数集合记为 $\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$. 在通常的四元数乘法下, 它是含幺元的结合环; 虚单位满足

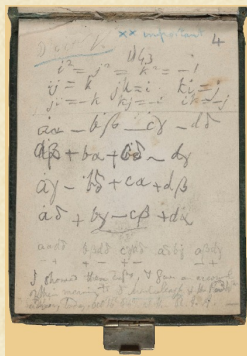
$$i^2 = j^2 = k^2 = -1, \quad ij = k = -ji, \quad jk = i = -kj, \quad ki = j = -ik.$$

因此 $ij \neq ji$. 若 $q = a + bi + cj + dk$, 令 $\bar{q} = a - bi - cj - dk$. 则 $q\bar{q} = \bar{q}q = a^2 + b^2 + c^2 + d^2$. 对 $q \neq 0$, 于是 $q^{-1} = \bar{q}/(a^2 + b^2 + c^2 + d^2)$. 因而 $\mathbb{H}$ 是一个乘法不交换, 但每个非零元素都是单位的环.

〔史略〕 Hamilton 与四元数的发现



William Rowan
Hamilton (1805–1865)
肖像.



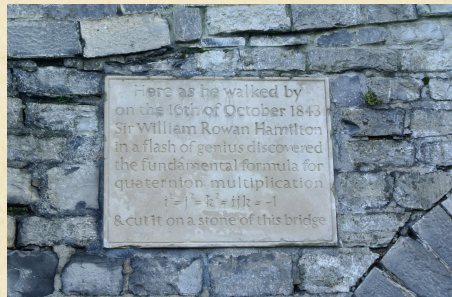
Hamilton 于 1843 年 10 月 16 日写下第一份四元数公式的随身笔记本(TCD 1492/59.6).⁷

四元数来自 Hamilton 对复数乘法的推广. 他多年试图以三元数组构造类似复数的数系; 若 i, j 表示两个独立的虚方向, 乘法封闭性便引出新的方向 $k = ij$, 而 $ji = -k$ 迫使乘法不再交换. 放弃交换律并补入第四个坐标, 才使这套乘法同时保留结合律与范数的乘法性.

1843 年 10 月 16 日, Hamilton 行至都柏林皇家运河上的 Brougham Bridge 时得到四元数的基本关系; 当晚, 他又在随身笔记本中写下公式.



Brougham Bridge(今称 Broom Bridge). Hamilton 于 1843 年 10 月 16 日经过此处时发现四元数乘法.



Broom Bridge 现存纪念铭牌,记录发现日期及关系 $i^2 = j^2 = k^2 = ijk = -1$.

例 1.23 (Banach 空间的有界算子环). 实或复 Banach 空间 E 上的全体有界线性算子组成环 $\mathcal{B}(E)$: 加法逐点定义, 乘法是算子复合, 幺元是恒等算子 I_E . 这个环通常不交换. 它的单位恰是可逆的有界算子; 由有界逆定理, 这也等价于算子是双射的线性映射.

若 $E = E_1 \oplus E_2$ 是两个非零闭子空间的拓扑直和, 令 P 为到 E_1 的坐标投影. 则 $P^2 = P$ 且 $P(I_E - P) = 0$. 这个等式说明投影算子不是单位, 符合几何直观.

例 1.24 (函数环中的单位). 设 A 是非零交换环, X 是非空集合. 函数 $f \in A^X$ 是单位, 当且仅当每个 $f(x)$ 都是 A 中的单位; 此时逆元逐点给出, 即 $f^{-1}(x) = f(x)^{-1}$.

特别地, 若 $\mathbb{F} = \mathbb{R}$ 或 $\mathbb{C}$, 则 $f \in C(X, \mathbb{F})$ 是单位, 当且仅当 $f(x) \neq 0$ 对每个 $x \in X$ 成立. 此时 $f^{-1}(x) = f(x)^{-1}$, 而 $\mathbb{F} \setminus \{0\}$ 上的求逆映射连续, 故 f^{-1} 仍属于 $C(X, \mathbb{F})$.

1.1.5 理想与素理想

定义 1.25. 设 A 是交换环. 加法子群 $I \subseteq A$ 称为 A 的理想, 若对每个 $a \in A$ 与 $x \in I$, 都有 $ax \in I$. 若 $I \neq A$, 则称 I 为真理想. 零理想 $(0) = \{0\}$ 与全环理想 $A = (1)$ 总是理想. 对 $a \in A$, 集合 $(a) = aA = \{ax : x \in A\}$ 是理想, 称为由 a 生成的主理想.

定义 1.26. 设 A 是交换环, $\mathfrak{p} \subsetneq A$ 是真理想. 若对任意 $a, b \in A$, 条件 $ab \in \mathfrak{p}$ 总能推出 $a \in \mathfrak{p}$ 或 $b \in \mathfrak{p}$, 则称 $\mathfrak{p}$ 为 A 的素理想.

这个定义把素数的整除性质移植到一般的环中. 真理想的要求不可省略: 全环理想包含所有乘积, 却不应被称为素理想.

例 1.27 (整数环的素理想). 首先, 每个 $\mathbb{Z}$ 的理想都形如 $(n) = n\mathbb{Z}$, 其中 $n \geq 0$. 若理想 $I \neq (0)$, 取 I 中最小的正整数 n . 对任意 $a \in I$, 作带余除法 $a = qn + r$, 其中 $0 \leq r < n$. 因为 $r = a - qn \in I$, 最小性迫使 $r = 0$, 故 $I \subseteq (n)$; 反向包含由 $n \in I$ 得到.

零理想是素理想: 若整数 a, b 满足 $ab = 0$, 则 $a = 0$ 或 $b = 0$. 若 p 是素数且 $ab \in (p)$, 则 $p \mid ab$. 当 $p \nmid a$ 时, $\gcd(a, p) = 1$, 故存在 $u, v \in \mathbb{Z}$ 使 $ua + vp = 1$. 两

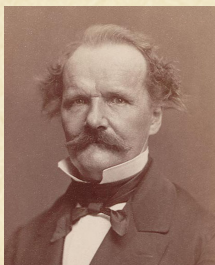
⁷四图来源: MacTutor, William Rowan Hamilton; 都柏林三一学院图书馆, Notebook containing the first written record of quaternions(TCD 1492/59.6); Wikimedia Commons, Johnflan, Broom Bridge.jpg; Wikimedia Commons, Cone83, Broom Bridge inscription. 乘法关系见 Hamilton, On Quaternions.

边乘以 b 可知 $p \mid b$. 因而 (p) 是素理想. 反之, 若 $n > 1$ 是合数, 写成 $n = rs$, 其中 $1 < r, s < n$, 则 $rs \in (n)$, 但 $r, s \notin (n)$, 所以 (n) 不是素理想. 全环理想 $(1) = \mathbb{Z}$ 不是真理想. 综上, $\mathbb{Z}$ 的全部素理想为

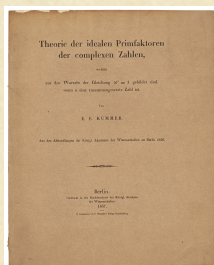
$$\{(0)\} \cup \{(p) : p \text{ 是素数}\}.$$

〔史略〕 “理想”一词的来历

十九世纪中叶, 数学家发现素因子唯一分解在某些代数整数环中会失效. 例如 $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ 在 $\mathbb{Z}[\sqrt{-5}]$ 中给出 6 的两种素因子分解: 考虑范数 $N(a + b\sqrt{-5}) = a^2 + 5b^2$, 方程 $N(x) = 2$ 或 $N(x) = 3$ 均无解; 结合范数的乘法性可知, 上述四个因子都不能继续分解为两个非单位的乘积.



Kummer(1810–1893)
肖像



Kummer《复数的理想素因子理论》1857 年单行本封面

Ernst Eduard Kummer 在研究分圆整数时, 于 1840 年代引入“理想数”和“理想素因子”, 使得在加入“理想因子”扩大的代数体系中恢复素因子唯一分解. 因为这些因子并不实际存在于原有数环, 而是由整除行为刻画的设想元素, “理想”一词由此而来. 用此概念看, 尽管 $\mathbb{Z}[\sqrt{-5}]$ 中没有同时整除 2 与 $1 + \sqrt{-5}$ 的非单位, 它们可有共同理想因子.

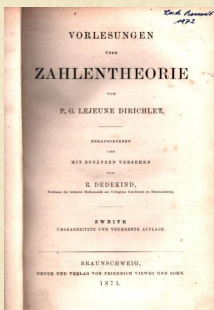
Richard Dedekind 在 1871 年保留“理想”这个名称, 却以实际存在的数集取代 Kummer 的设想因子. 在 $\mathbb{Z}[\sqrt{-5}]$ 中, 取

$$I := \{a + b\sqrt{-5} \mid a \equiv b \pmod{2}\}$$

该集合就是 2 和 $1 + \sqrt{-5}$ 生成的理想 $(2, 1 + \sqrt{-5})$; 易验证任意 $x, y \in \mathbb{Z}[\sqrt{-5}]$, 线性组合 $2x + (1 + \sqrt{-5})y \in I$. 加法封闭性与乘法吸收性由此把“共同的理想因子”落实为环内的具体子集, 正是理想定义所保留的两项性质.



Dedekind(1831–1916)
肖像



Dirichlet《数论讲义》1871 年第二版扉页; 该版由 Dedekind 修订并增补.⁸

⁸图源: MacTutor, Ernst Eduard Kummer; Christie's, Kummer's papers on ideal prime factors; ETH-Bibliothek / Wikimedia Commons, Richard Dedekind portrait; e-rara, Vorlesungen über Zahlentheorie.

习题

- (1) $\star$ 在 $\mathbb{N}_0 \times \mathbb{N}_0$ 上规定 $(a, b) \sim (c, d)$ 当且仅当 $a + d = b + c$. 令 G 为等价类的集合, 并定义 $[a, b] + [c, d] = [a + c, b + d]$. 证明这个运算使 G 成为交换群, 且 $[a, b] \mapsto a - b$ 给出 $G \cong (\mathbb{Z}, +)$. 这个构造称为 $(\mathbb{N}_0, +)$ 的群化.
- (2) 仅用环公理证明 $a(-b) = -(ab)$ 与 $(-a)(-b) = ab$.
- (3) 验证偶数集合在通常的加法下是交换群, 但在通常乘法下没有幺元 1, 因而它不是环.
- (4) 求整数环 $\mathbb{Z}$ 的全部单位, 并证明你的答案没有遗漏.
- (5) 分别研究乘法映射 $[x] \mapsto [2x]$ 在 $\mathbb{Z}/5\mathbb{Z}$ 与 $\mathbb{Z}/6\mathbb{Z}$ 上的单射性和满射性. 由此求 $[2] \in \mathbb{Z}/5\mathbb{Z}$ 的逆元, 并指出 $\mathbb{Z}/6\mathbb{Z}$ 中乘以 $[2]$ 后发生重合的剩余类.
- (6) 设 A, B 是交换环. 证明 $(a, b) \in A \times B$ 是单位, 当且仅当 $a \in A^\times$ 且 $b \in B^\times$, 并写出其逆元.
- (7) 设 A 是非零交换环, X 是非空集合. 证明 $f \in A^X$ 是单位, 当且仅当 $f(x)$ 对每个 $x \in X$ 都是 A 中的单位.
- (8) 设 $n \geq 2$. 仅用素理想的定义证明: $(n) \subseteq \mathbb{Z}$ 是素理想, 当且仅当 n 是素数.
- (9) 设 A 是交换环, $a \in A$. 直接从定义验证 $(a) = aA$ 是理想.
- (10) 设 I, J 是交换环 A 的理想. 证明 $I \cap J$ 与 $I + J = \{x + y : x \in I, y \in J\}$ 都是理想.
- (11) 设 $I \subseteq \mathbb{Z}$ 是非零理想. 取 I 中最小的正整数 n , 证明 $I = (n)$.
- (12) 证明 $(6, 15) = (3)$; 再解释为何这表明一个理想可以由不止一个元素生成.

参考文献与延伸阅读

- [1] GAUSS C F. Disquisitiones Arithmeticae[M/OL]. Leipzig: Gerhard Fleischer, 1801 [2026-08-27]. <https://www.loc.gov/item/36021572/>.
- [2] MacTutor History of Mathematics Archive. Earliest Uses of Symbols of Number Theory[EB/OL]. [2026-08-27]. <https://mathshistory.st-andrews.ac.uk/Miller/mathsym/nth/>.