BCI-代数与半群

杨闻起 著

科学出版社

内 容 简 介

本书是一本研究 BCI-代数与群、半群、环和半环的关系的著作，共有 5 章. 第 1 章是预备知识，包括研究 BCI-代数必备的代数基础知识；第 2 章是 BCI-代数的一般理论，主要介绍该代数系统的基础理论；第 3 章是 BCI-代数与半群，从不同的角度研究了 BCI-代数与群和半群的关系，包括作者多年从事 BCI-代数研究的系列成果；第 4 章是 BCI-半群(IS-代数)，介绍了 BCI-半群(IS-代数)的基础理论，包括韩国田英培教授、西北大学辛小龙教授和作者的研究成果；第 5 章是 IS-代数与半环，讨论了 IS-代数与环和半环的关系，主要是作者的研究成果.

本书适合大学教师和研究生阅读，也可作为数学与计算机专业本科高年级学生的选修课教材.

图书在版编目(CIP)数据

BCI-代数与半群/杨闻起著. —北京：科学出版社，2011

ISBN 978-7-03-033027-7

Ⅰ. ①B… Ⅱ. ①杨… Ⅲ. ①BCI 代数-研究②半群-研究 Ⅳ. O15

中国版本图书馆 CIP 数据核字 (2011) 第 260037 号

责任编辑：王 静 房 阳 / 责任校对：陈玉凤
责任印制：张克忠 / 封面设计：陈 敬

科 学 出 版 社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

骏 杰 印 刷 厂 印刷

科学出版社发行 各地新华书店经销

*

2011 年 12 月第 一 版 开本：720×1000 1/16
2011 年 12 月第一次印刷 印张：10 1/4
字数：208 000

定价：35.00 元

(如有印装质量问题，我社负责调换)

前　言

逻辑代数是信息科学、计算机科学、控制论和人工智能等许多领域的推理机制的代数基础. 随着模糊控制的广泛应用, 作为其理论基础的模糊逻辑和相关的逻辑代数也成为人们研究的热点.

1966 年, 由日本数学家 Y. Imai 和 K. Iséki 以逻辑运算为基础, 根据组合逻辑中组合子的代数表述, 提出了 BCK–代数和 BCI–代数. 1993 年, 韩国数学家田英培 (Young Bae Jun) 教授在 BCI–代数的基础上通过添加半群结构又引入了 BCI–半群 (简称 IS–代数). 与这些逻辑代数相比较, 传统的代数系统 (群、环) 最大的特点就是运算具有结合性, 即传统的代数系统都是结合代数. 而逻辑代数是基于逻辑运算引入的代数系统, 并不要求代数运算具有结合性, 所以逻辑代数都是非结合代数. 尽管逻辑代数与结合代数有明显的区别, 但现有的研究结果已经表明, 逻辑代数与结合代数有着紧密的联系.

从 BCI–代数的发展来看, 主要有以下几种方法研究 BCI–代数与结合代数的关系: 第一, 在 BCI–代数中寻找一些特殊类, 如 1980 年由胡庆平和 K.Iséki 引入的结合 BCI–代数、1983 年由雷天德引入的广义结合 BCI–代数和 1990 年由惠昌常引入的拟结合 BCI–代数. 由这些特殊的 BCI–代数类可直接得到群和半群. 第二, 作者从一般 BCI–代数的运算出发导出了另一种适合结合律的新运算, 从而由一般 BCI–代数得到半群. 第三, 1995 年, 黄文平借助于变换群的思想, 在一般 BCI–代数上寻找一些变换, 将这些变换关于变换的合成运算作成半群. 第四, 1993 年, 由田英培等通过在 BCI–代数上再添加一个半群结构而形成 BCI–半群, 并说明它是环概念的一般化.

本书的主线就是研究 BCI–代数与群和半群的关系问题, 特点如下:

第一, 在论述 BCI–代数理论时, 以作者的研究成果为基础, 通过引入一般 BCI–代数的加法序半群, 建立了一般 BCI–代数与序半群的关系, 以便读者体会逻辑代数与结合代数的紧密联系.

第二, 建立了 BCI–代数中元素的阶与群中元素的阶的对应关系, 得到了用元素的阶刻画 BCI–代数的许多结论.

第三, 本书的重点是系统地论述BCI–半群理论, 这在国内外同类著作中尚不多见.

第四, 本书最突出的特点是根据作者的研究成果, 论述 BCI–代数与群和半群的关系、BCI–半群与环和半环的关系.

本书共有 5 章, 其中许多内容是作者多年从事 BCI–代数和 BCI–半群研究的成果. 第 1 章是代数基础知识, 包括序与偏序、群与半群、序半群、环及半环等内容; 第 2

章是 BCI–代数的基本理论, 主要介绍该代数系统的基础理论, 主要包括 BCI–代数和 BCK–代数的概念和基本性质、理想、滤子、商代数及同态等内容; 第 3 章论述 BCI–代数与群和半群的关系, 主要有三种 BCI–代数与群和半群的关系, 一般 BCI–代数的加法序半群和伴随半群, 其中包括了作者多年从事 BCI–代数研究的系列成果. 第 4 章论述 BCI–半群的基础理论, 包括韩国田英培教授、西北大学辛小龙教授和作者的研究成果. 第 5 章论述 BCI–半群与环和半环的关系问题, 主要是作者的研究成果.

本书是陕西省自然科学基金项目 (2010JM1016) 的研究成果汇总. 在本书编写过程中, 西北大学数学系辛小龙教授给予了极大的鼓励, 并为作者提供了许多有价值的资料; 宝鸡文理学院数学系赵天绪主任和宝鸡文理学院学科建设与研究生教育管理处给予了大力支持. 另外, 本书的出版得到了宝鸡文理学院陕西省重点学科基础数学专项经费的资助. 此外, 书中还引用了许多数学工作者的结论, 在此一并致谢!

由于作者水平有限, 书中的错误和疏漏之处在所难免, 恳请有关专家和读者不吝赐教.

作　者

2011 年 10 月于宝鸡

目　录

第 1 章　预备知识

数学中有三个母结构: 代数结构、序结构和拓扑结构. 这三个母结构相互交融, 形成了数学中的多个分支. 本书主要涉及代数结构和序结构. 本章主要介绍与 BCI–代数紧密联系的代数结构和序结构的基础理论, 包括偏序集、格、群、半群、序半群、环和半环等, 为本书后面的论述作好准备.

1.1　偏序集与格

本节介绍偏序集和全序集及其理想和滤子的基本概念和性质, 给出理想和滤子的分解定理, 并介绍格的有关概念和性质.

1.1.1　偏序集与全序集

定义 1.1.1　设 X 是非空集合, 把 $X \times X$ 的子集 R 叫做 X 上的二元关系. 如果 $(x,y) \in R$, 则记为 xRy.

例 1.1.1　(1) 设 X 为实数集合, 规定 $(x,y) \in R \Leftrightarrow x \leqslant y$, 则 R 为 X 上的二元关系.

(2) 设 X 为任意的非空数集, $f(x)$ 为 X 上的一元函数, 则 $f(x)$ 的图像

$$R = \{(x, f(x)) | x \in X\}$$

是 X 上的二元关系, 但是 X 上的二元关系未必全是 X 上的一元函数的图像. 例如, (1) 是二元关系, 但却不是 X 上的一元函数的图像.

定义 1.1.2　设 X 是非空集合, “$\leqslant$” 是 X 上的二元关系, 如果

(1) 自反性: $\forall x \in X$, 必有 $x \leqslant x$;

(2) 传递性: $\forall x \leqslant y, y \leqslant z$, 必有 $x \leqslant z$;

(3) 反对称性: $\forall x \leqslant y, y \leqslant x$, 必有 $x = y$,

则称关系 “$\leqslant$” 为 X 上的偏序, 带偏序的集合 $(X, \leqslant)$ 称为偏序集. 在不致混淆的情况下, 偏序集也简写为 X. 在偏序集 X 中, 也可把 $x \leqslant y$ 写成 $y \geqslant x$.

设 $(X, \leqslant)$ 是偏序集, 如果 X 中的任意两个元素都可比较, 即 $\forall x, y \in X$ 都有 $x \leqslant y$ 或 $y \leqslant x$, 则称 $(X, \leqslant)$ 为全序集, “$\leqslant$” 叫做全序 (线性序), 把偏序集 X 中的全序子集叫做 X 的链.

例 1.1.2　(1) 设 X 为实数集, "$\leqslant$" 为通常的大小关系, 则 $(X,\leqslant)$ 显然是偏序集, 也是全序集.

(2) 设 $X = C[0,1], \forall f, g \in X$, 规定

$$f \leqslant g \Leftrightarrow f(x) \leqslant g(x), \quad \forall x \in [0,1],$$

则 $(x,\leqslant)$ 是偏序集, 但不是全序集.

定义 1.1.3　设 $(X,\leqslant)$ 是偏序集, m, b 是 X 中的固定元.

(1) $\forall x \in X$, 如果由 $m \leqslant x$ 可以推出 $x = m$, 则称 m 为 X 中的极大元. 如果 $\forall x \in X$ 都有 $x \leqslant b$, 则称 b 为 X 的最大元.

(2) $\forall x \in X$, 如果由 $x \leqslant m$ 可以推出 $x = m$, 则称 m 为 X 的极小元. 如果 $\forall x \in X$ 都有 $b \leqslant x$, 则称 b 为 X 的最小元.

显然, 最大 (小) 元必是极大 (小) 元, 但反之不成立.

例 1.1.3　设 $A = \{1,2,3\}, X$ 是 A 的全体真子集. 规定

$$X_1 \leqslant X_2 \Leftrightarrow X_1 \subseteq X_2,$$

则 $(X,\leqslant)$ 是偏序集, $\{1,2\}, \{1,3\}, \{2,3\}$ 都是 X 的极大元, 但是 X 没有最大元. $\varnothing$ 是 X 的最小元, $\{\{1\}, \{1,2\}, \{1,2,3\}\}$ 是 X 中的一个链.

一般地, 偏序集中的极大元未必存在, 即使存在也未必唯一, 但有如下公认的引理:

Zorn 引理　如果偏序集 X 中的每个链都有上界, 则 X 必有极大元.

定义 1.1.4　设 $(X,\leqslant)$ 是偏序集, $\varnothing \neq Y \subseteq X$, 如果 $\exists a \in X$, 使得 $\forall y \in Y$ 都有 $y \leqslant a (y \geqslant a)$, 则称 a 为 Y 的上界 (下界). 如果 b 是 Y 的上界 (下界), 并且对 Y 的任一上界 (下界)a 都有 $b \leqslant a (b \geqslant a)$, 则称 b 为 Y 的上确界 (下确界), 记为 $b = \sup Y (b = \inf Y)$ 或 $b = \vee Y (b = \wedge Y)$.

1.1.2　理想与滤子

在偏序集中, 理想与滤子是相互对偶的概念.

定义 1.1.5　设 I 是偏序集 X 的非空子集, $\forall x \in X, \forall y \in I$, 如果由 $x \leqslant y$ 可以推出 $x \in I$, 则称 I 为 X 的理想. 如果理想 $I \neq X$, 则称 I 为 X 的真理想. 令

$$(y] = \{x \in X \,|x \leqslant y\},$$

则 $(y]$ 显然是包含 y 的最小理想, 称之为关于 y 的主理想.

一般地, 设 A 是 X 的非空子集, 令

$$(A] = \{x \in X \,|\exists a \in A, x \leqslant a\},$$

显然, $(A]$ 必是包含 A 的最小理想, 称之为由 A 生成的理想.

设 J 是偏序集 X 的非空子集, $\forall x \in X, \forall z \in J$, 如果由 $z \leqslant x$ 可以推出 $x \in J$, 则称 J 为 X 的滤子. 令

$$[z) = \{x \in X \,|z \leqslant x\},$$

则 $[z)$ 显然是包含 z 的最小滤子, 称之为关于 z 的主滤子.

一般地, 设 A 是 X 的非空子集, 记

$$[A) = \{x \in X \,|\exists a \in A, a \leqslant x\},$$

显然, $[A)$ 是 X 的滤子, 称之为 A 生成的滤子.

例 1.1.4 在实数偏序集 $(R, \leqslant)$ 中, $\forall a \in R$, 则 $(-\infty, a), (-\infty, a]$ 都是 R 的理想, $(-\infty, a]$ 是关于 a 的主理想, $(a, +\infty), [a, +\infty)$ 都是 R 的滤子, $[a, +\infty)$ 是关于 a 的主滤子.

定义 1.1.6 设 X_1, X_2 都是偏序集, f 是 X_1 到 X_2 的映射, $\forall x_1, y_1 \in X$, 如果由 $x_1 \leqslant y_1$ 可以推出 $f(x_1) \leqslant f(y_1)$, 则称 f 为保序的. 如果存在一个 $X_1 \to X_2$ 的双射 f, 使得 f, f^{-1} 都是保序的, 则称 X_1, X_2 为序同构.

定理 1.1.1 设 X_1, X_2 都是偏序集, f 是 $X_1 \to X_2$ 的映射, 则以下命题等价:

(1) f 是保序的;

(2) X_2 的每个主理想的原象要么为空, 要么为 X_1 的理想;

(3) X_2 的每个主滤子的原象要么为空, 要么为 X_1 的滤子.

证明 (1)⇒(2) $\forall x_2 \in X_2$, 设 $f^{-1}((x_2]) = A_1 \neq \varnothing, \forall y_1 \in A_1$, 则 $f(y_1) \in (x_2]$, 即

$$f(y_1) \leqslant x_2, \quad \forall x_1 \leqslant y_1,$$

则 $f(x_1) \leqslant f(y_1) \leqslant x_2$, 从而 $f(x_1) \in (x_2]$, 即 $x_1 \in A_1$, 故 A_1 是 X_1 的理想.

(2)⇒(1) $\forall x_1, y_1 \in X_1$ 且 $x_1 \leqslant y_1$, 令

$$(f(y_1)] = \{y_2 \in X_2 \,|y_2 \leqslant f(y_1)\} = A_2,$$

则

$$f^{-1}(A_2) = \{z_1 \in X_1 \,|f(z_1) \in A_2\} = \{z_1 \in X_1 \,|f(z_1) \leqslant f(y_1)\}.$$

显然, $y_1 \in f^{-1}(A_2)$, 即 $f^{-1}(A_2) \neq \varnothing$, 故 $f^{-1}(A_2)$ 必为 X_1 的理想. 由于 $x_1 \leqslant y_1$, 从而 $x_1 \in f^{-1}(A_2)$, 即得 $f(x_1) \leqslant f(y_1)$.

(1) 与 (3) 的等价性同理可证. 证毕

定理 1.1.2 设 X 是偏序集, $\{I_k \,|k \in K\}$ 是一族理想 (滤子), 则

(1) $\bigcup\limits_{k \in K} I_k$ 是 X 的理想 (滤子);

(2) 如果 $\bigcap\limits_{k\in K} I_k \neq \varnothing$, 那么 $\bigcap\limits_{k\in K} I_k$ 也是 X 的理想 (滤子).

证明　(1) 设 $I = \bigcup\limits_{k\in K} I_k$, 对 $\forall y \in I, \exists k_0 \in K$, 使得 $y \in I_{k_0}$. 设 $x \in X, x \leqslant y$, 由于 I_{k_0} 是 X 的理想, 故 $x \in I_{k_0} \subseteq I$, 即得 $x \in I$, 从而 I 是 X 的理想.

(2) 设 $I = \bigcap\limits_{k\in K} I_k \neq \varnothing, \forall z \in I$, 则 $\forall k \in K$ 有 $z \in I_k$. 设 $x \in X, x \leqslant z$, 由于 I_k 是 X 的理想, 故 $x \in I_k$. 由 k 的任意性知 $x \in I$, 从而 I 是 X 的理想.

对滤子同理可证.　证毕

1.1.3　理想 (滤子) 分解定理

在偏序集的理想 (滤子) 中, 希望找出一些特殊理想 (滤子), 把所有理想 (滤子) 表示出来.

首先, 给出用主理想表示任意理想 (滤子) 的一个结论.

定理 1.1.3　设 I 是偏序集 X 的任意理想 (滤子), 则

$$I = \bigcup_{a\in I} (a] \left(I = \bigcup_{a\in I} [a) \right).$$

证明　由于 I 是偏序集 X 的理想, $a \in I$, 故 $(a] \subseteq I$, 从而

$$\bigcup_{a\in I} (a] \subseteq I.$$

又由于 $\forall a \in I, a \in (a]$, 所以 $I \subseteq \bigcup\limits_{a\in I} (a]$, 从而 $I = \bigcup\limits_{a\in I} (a]$.

对滤子同理可证.　证毕

下面通过引入次极大理想的概念, 给出另一个理想分解定理.

定义 1.1.7　设 M 是偏序集 X 的真理想, 如果对 X 的任意理想 I, 只要 $M \subseteq I$ 就有 $I = M$ 或者 $I = X$, 则称 M 为 X 的极大理想. 如果存在 $x \in X - M$, 使得对 X 的任意理想 I, 只要 $x \notin I \supseteq M$ 就有 $I = M$, 则称 M 为关于 x 的次极大理想, 记为 M_x.

定理 1.1.4　对偏序集 X 中的任意真理想 I 及任意 $x \in X - I$, 必存在关于 x 的次极大理想 M_x, 使得 $x \notin M_x \supseteq I$.

证明　设 $\alpha = \{A | A$ 是 X 的理想, 并且 $x \notin A \supseteq I\}$, 由于 $I \in \alpha$, 所以 α 非空. 设 β 为 α 中的任意链 (关于包含关系的全序子集), 令 B_0 是 β 中所有理想的并, 于是由定理 1.1.2 知, B_0 是 X 的理想, 且 $x \notin B_0 \supseteq I$, 即 $B_0 \in \alpha$, 所以 β 在 α 中有上界. 根据 Zorn 引理, α 中必有极大元, 不妨设为 M_x, 则显然, M_x 是关于 x 的次极大理想, 并且 $x \notin M_x \supseteq I$.　证毕

定理 1.1.5　偏序集 X 的每个真理想均可表示为一些 (有限或无限) 次极大理想的交.

证明 设 I 是 X 的真理想, 由定理 1.1.4 知, $\forall x \in X - I$, 存在次极大理想 M_x, 使得 $x \notin M_x \supseteq I$. 令 $J = \bigcap\limits_{x \in X - I} M_x$, 下证 $I = J$. 对任意 $x_0 \in X - I$, 有

$$x_0 \in X - M_{x_0} \subseteq \bigcup_{x \in X - I} (X - M_x) = X - J,$$

所以 $X - I \subseteq X - J$, 即 $J \subseteq I$. 又显然 $J \supseteq I$, 所以

$$I = J = \bigcap_{x \in X - I} M_x.$$

证毕

定义 1.1.8 偏序集 X 满足理想的降链条件 (DCC), 是指对 X 的每个无限理想链

$$I_1 \supset I_2 \supset \cdots$$

均存在正整数 n, 使得当 $i \geqslant n$ 时都有 $I_i = I_n$.

定理 1.1.6 设偏序集 X 满足理想的降链条件, 则 X 的每个真理想均可表示为有限个次极大理想的交.

证明 假设存在一个真理想 I 不能表示为有限个次极大理想的交, 取 $x_1 \in X - I$, 于是由定理 1.1.4, 必存在关于 x_1 的次极大理想 M_{x_1}, 使得 $x_1 \notin M_{x_1} \supseteq I$. 令 $N_1 = M_{x_1}$, 则由假设知, N_1 真包含 I. 取 $x_2 \in N_1 - I$, 又由定理 1.1.4 知, 存在关于 x_2 的次极大理想 M_{x_2}, 使得 $x_2 \notin M_{x_2} \supseteq I$. 令 $N_2 = N_1 \cap M_{x_2}$, 则由于 $x_2 \in N_1, x_2 \notin N_2$, 故 N_1 真包含 N_2. 重复以上过程, 由于 I 不能表示为有限个次极大理想的交, 便得到一个无限严格降链

$$N_1 \supset N_2 \supset \cdots \supset N_k \supset \cdots,$$

这与 X 满足理想的降链条件矛盾. 证毕

1.1.4 格及其基本性质

定义 1.1.9 设 $(L, \leqslant)$ 是偏序集, 如果 $\forall a, b \in L, \sup\{a, b\}$ 恒存在, 则称 $(L, \leqslant)$ 为上半格; 如果 $\forall a, b \in L, \inf\{a, b\}$ 恒存在, 则称 $(L, \leqslant)$ 为下半格, 常记

$$a \vee b = \sup\{a, b\}, \quad a \wedge b = \inf\{a, b\}.$$

既是上半格又是下半格的偏序集称为格. 显然, 全序集必是格.

容易证明以下结论成立:

定理 1.1.7 设 $(L, \leqslant)$ 是上半格 (下半格), 则 L 中的任意非空有限子集都有上确界 (下确界), 并且有以下公式:

(1) $a \vee b = b \vee a (a \wedge b = b \wedge a)$;

(2) $(a \vee b) \vee c = a \vee (b \vee c)((a \wedge b) \wedge c = (a \wedge b) \wedge c)$;

(3) $a \leqslant b \Leftrightarrow a \vee b = b(a \wedge b = a)$.

定义 1.1.10　设 $(L, \leqslant)$ 是偏序集, 如果 $\forall A \subseteq L, \sup A, \inf A$ 恒存在, 则称 $(L, \leqslant)$ 为完备格. 在完备格中, 把 $\sup L$ 叫做最大元, 记为 1; 把 $\inf \varnothing$ 叫做最小元, 记为 0.

例 1.1.5　R 是实数集合, $\leqslant$ 为实数的大小关系, 则 $(\mathbf{R}, \leqslant)$ 是格, 但不是完备格. 然而 $([0,1], \leqslant)$ 是完备格.

定理 1.1.8　设 $(L, \leqslant)$ 是格, 则以下两个公式等价:

(1) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$;

(2) $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

证明　设 (1) 成立, 由于 $a \leqslant a \vee b, a \wedge c \leqslant a$, 由定理 1.1.7 得

$$(a \vee b) \wedge a = a, \quad a \vee (a \wedge c) = a,$$

于是

$$\begin{aligned}(a \vee b) \wedge (a \vee c) &= ((a \vee b) \wedge a) \vee ((a \vee b) \wedge c) \\ &= a \vee ((a \vee b) \wedge c) = a \vee ((a \wedge c) \vee (b \wedge c)) \\ &= (a \vee (a \wedge c)) \vee (b \wedge c) = a \vee (b \wedge c),\end{aligned}$$

从而 (2) 成立.

反过来, 同理可证.　　证毕

1.2　群 与 半 群

群和半群是最基本的结合代数, 本节介绍有关的概念和基本性质.

1.2.1　群

设 X 为非空集, 把 $X \times X \to X$ 的映射 "$\circ$" 叫做 X 上的二元运算. 设 $(a, b) \in X \times X$, 如果 (a, b) 在该映射下的像为 c, 则记为 $c = a \circ b$.

定义 1.2.1　设 G 是非空集合, "$\circ$" 是 G 上的二元运算, 如果

(1) 结合律成立, 即 $\forall a, b, c \in G$ 有 $(a \circ b) \circ c = a \circ (b \circ c)$;

(2) G 中存在左单位元 e, 即 $\exists e \in G$, 使得 $\forall a \in G$ 有 $e \circ a = a$;

(3) G 中任意元素都有左逆元, 即 $\forall a \in G$, $\exists a^{-1} \in G$, 使得 $a^{-1} \circ a = e$,

则称 G 关于这个二元运算作成一个群, 记为 $(G, \circ)$. 在不致混淆时, 简记为 G.

如果对 $\forall a, b \in G$ 均有 $a \circ b = b \circ a$, 即群 G 的二元运算满足交换律, 则称群 G 为交换群 (Abel 群).

例 1.2.1　设 G 为整数集, $a \circ b = a + b + 4$, 则容易验证, G 关于运算 "$\circ$" 是交换群, 并且 -4 是左单位元, $-8 - a$ 是 a 的左逆元.

通常把群中的二元运算 “$\circ$” 写成乘法, 这时群 G 也叫乘群, 但有时在交换群 G 中, 常把 G 中的二元运算写成加法, 这时 G 也叫加群. 在加群中, 单位元叫做零元, 记为 0, a 的逆元叫做负元, 记为 $-a$.

把群 G 中元素的个数叫做 G 的阶, 记为 $|G|$. 如果 $|G|$ 有限, 则称 G 为有限群; 如果 $|G|=\infty$, 则称 G 为无限群.

定理 1.2.1 群 G 中的左单位元也是右单位元, 元素 a 的左逆元也是右逆元.

证明 设 a^{-1} 是元素 a 的左逆元. 由于 G 是群, 故 a^{-1} 在 G 中也有左逆元, 不妨设为 a', 即 $a'a^{-1}=e$. 由于 e 为左单位元, 则

$$\begin{aligned}aa^{-1}&=eaa^{-1}=(a'a^{-1})(aa^{-1})\\&=a'(a^{-1}a)a^{-1}=a'(ea^{-1})=a'a^{-1}=e,\end{aligned}$$

从而

$$aa^{-1}=a^{-1}a=e.$$

由于 e 为左单位元, 即 $ea=a$, 从而

$$ae=a(a^{-1}a)=(aa^{-1})a=ea=a,$$

故 e 也为右单位元, 从而 a^{-1} 也是 a 的右逆元. 证毕

把左 (右) 单位元统称为群 G 的单位元, 记为 e. a 的左、右逆元统称为 G 的逆元, 记为 a^{-1}.

定理 1.2.2 群 G 的单位元唯一, 每个元素 a 的逆元都由 a 唯一确定.

证明 设 e,e' 都是 G 的单位元, 则

$$e=ee'=e'.$$

设 a^{-1},a' 都是 a 的逆元, 于是

$$a'=a'e=a'(aa^{-1})=(a'a)a^{-1}=ea^{-1}=a^{-1}.$$ 证毕

在群 G 中, 如果 $ab=ac$, 则左乘 a^{-1} 便得 $b=c$. 如果 $ba=ca$, 则右乘 a^{-1} 便得 $b=c$. 故群中左右消去律成立.

定义 1.2.2 设 G 是群, 如果 $\forall a\in G$ 有 $a^2=e$, 则称 G 为对合群.

定理 1.2.3 对合群必是交换群.

证明 设 G 是对合群, $\forall a,b\in G$ 有

$$a^2=e,\quad b^2=e,\quad (ab)^2=e,$$

故有

$$ba=(ab)^2ba=ababba=abaea=abe=ab,$$

即 G 是交换群. 证毕

定义 1.2.3　设 H 是群 G 的非空子集, 如果 H 关于 G 的乘法也是群, 则称 H 为 G 的子群, 记为 $H \leqslant G$.

定理 1.2.4　设 H 是群 G 的子群, 则 H 中的单位元必是 G 中的单位元, 元素 a 在 H 中的逆元必是 a 在 G 中的逆元.

证明　设 e' 为 H 的单位元, e 为 G 的单位元, 则

$$e'e' = e', \quad e'e = e',$$

即 $e'e' = e'e$, 由消去律得 $e' = e$.

设 a^{-1}, a' 分别为 a 在 G, H 中的逆元, 则 $a'a = a^{-1}a = e$, 由消去律得 $a' = a^{-1}$. 证毕

定理 1.2.5　设 H 是群 G 的非空子集, 则 $H \leqslant G$ 当且仅当

(1) $\forall a, b \in H$ 有 $ab \in H$;

(2) $\forall a \in H$ 有 $a^{-1} \in H$.

证明　设 $H \leqslant G$, 则显然 (1) 成立. $\forall a \in H$, 设 a' 是 a 在 H 中的逆元, 由定理 1.2.4 知 $a' = a^{-1}$, 故 $a^{-1} \in H$, 从而 (2) 成立.

反之, 设 (1), (2) 成立, 则显然, G 中的乘法是 H 上的二元运算, 并且 H 中的乘法结合律成立. 任取 $a \in H$, 由 (2) 知, $a^{-1} \in H$. 又由 (1) 知 $e = aa^{-1} \in H$, 从而 H 是 G 的子群. 证毕

定理 1.2.5 (1), (2) 显然可合并如下:

(3) $\forall a, b \in H$ 有 $ab^{-1} \in H$.

定义 1.2.4　设 H 是 G 的子群, $a \in G$, 将

$$aH = \{ah \,|h \in H\}, \quad Ha = \{ha \,|h \in H\}$$

分别叫做 a 关于子群 H 的左陪集和右陪集. 如果 $\forall a \in G$ 有 $aH = Ha$, 则称 H 为 G 的正规子群.

显然, $aN = bN \Leftrightarrow ab^{-1} \in N$.

定理 1.2.6　设 N 是群 G 的正规子群, 令

$$G/N = \{aN \,|a \in G\},$$

在 G/N 中规定

$$aN \cdot bN = (ab)N,$$

则 G/N 关于以上乘法作成一个群, 称之为 G 关于 N 的商群.

证明 首先, 说明以上陪集的运算是良好的. 设 $aN=uN,bN=vN$, 则 $au^{-1}\in N,bv^{-1}\in N$. 设 $bv^{-1}=n$, 则 $an\in aN=Na$. 再设 $an=n_1a(n_1\in N)$, 则有

$$(ab)(uv)^{-1}=a(bv^{-1})u^{-1}=anu^{-1}=n_1(au^{-1})\in N,$$

故

$$aN\cdot bN=(ab)N=(uv)N=uN\cdot vN,$$

即以上陪集的运算是良好的.

其次, 容易验证, $(G/N,\cdot)$ 是群, 并且 N 是其中的单位元, $a^{-1}N$ 是 aN 的逆元.

证毕

1.2.2 群中元素的阶

在群 G 中, 由于结合律成立, 故 $aa\cdots a$(n 个 a) 有意义. 规定

$$a^n=aa\cdots a,$$
$$a^0=e,$$
$$a^{-n}=(a^{-1})^n.$$

容易验证, 对任意整数 n,m 有

$$a^na^m=a^{n+m},\quad (a^n)^m=a^{nm}.$$

定义 1.2.5 设 a 为群 G 中的元素, 把满足 $a^n=e$ 的最小正整数 n 叫做元素 a 的阶, 记为 $|a|$. 如果这样的 n 不存在, 则称 a 的阶为 ∞.

把每个元素的阶都有限的群叫做周期群.

例 1.2.2 设 $G=\{1,-1,\mathrm{i},-\mathrm{i}\}$, 它关于复数的乘法作成群, 叫做 4 次单位根群, 其中 $|1|=1$, $|-1|=2$, $|\mathrm{i}|=|-\mathrm{i}|=4$, 从而 G 为周期群.

定理 1.2.7 设群 G 中元素 a 的阶为 n, 则 $a^m=e\Leftrightarrow n\,|\,m$.

证明 设 $n\,|\,m$, 可设 $m=nq$, 则

$$a^m=(a^n)^q=e^q=e.$$

反之, 设 $a^m=e$, 并令 $m=qn+r$, 其中 $0\leqslant r<n$, 则

$$a^m=a^{qn+r}=(a^n)^qa^r=a^r=e.$$

由于 $|a|=n$, 故 $r=0$, 从而 $n\,|\,m$. 证毕

定理 1.2.8 设群 G 中元素 a 的阶为 n, k 为任意整数, 则 a^k 的阶为

$$|a^k|=\frac{n}{(k,n)}.$$