Modern Algebra

近世代数

王栓宏　编著

科学出版社

近世代数

王栓宏　编著

科学出版社

北京

内 容 简 介

本书主要介绍了群胚(groupoid)、群(group)、环(ring)和模(module)的基本概念和理论，并特别介绍了与这些概念相关的国际前沿研究课题和应用. 本书内容由浅入深，结合双语课程的特点，在编写方法上对如何组织双语教材进行了有益的探索.

本书可供高等学校数学及相关专业高年级本科生和高校教师从事双语课程教学时阅读和参考.

图书在版编目(CIP)数据

近世代数/王栓宏编著. —北京：科学出版社, 2013
ISBN 978-7-03-036867-6

Ⅰ. ①近… Ⅱ. ①王… Ⅲ. ①抽象代数—双语教学—教材 Ⅳ. ①O153

中国版本图书馆 CIP 数据核字(2013) 第 040560 号

责任编辑：顾 艳 尚 雁 / 责任校对：张怡君
责任印制：赵德静 / 封面设计：许 瑞

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

源海印刷有限责任公司印刷
科学出版社发行 各地新华书店经销
*
2013 年 3 月第 一 版 开本：B5(720×1000)
2013 年 3 月第一次印刷 印张：5 3/4
字数：120 000
定价：29.00 元
(如有印装质量问题，我社负责调换)

前　言

目前, 国内许多大学已经意识到本科教学国际化的重要性, 教学计划中也设置了双语课程, 于是, 如何开展与评估双语教学, 尤其是如何编写双语教材, 学生手上应该有什么样的教材就成为一个很大的问题, 有待探索与研究.

本科教学的国际化最终的落脚点是本科生的国际化, 包括出国交换学习、参加国际会议、在国内听外国专家的各种讲座与学术报告. 不论是研究生还是老师, 与外国同行交流专业知识时, 概念和性质的叙述非常重要, 必须用英语完成; 至于性质的证明则是一种深入的研究过程. 根据作者多年来与国外同行专家合作研究以及参加各种国际会议的经验和体会, 本科生双语教材编写的主要目的是使学生学会应用英语来描述和掌握概念、性质、例子和应用, 而淡化应用英语来证明性质、定理等的研究过程, 也就是说, 我们可用中文给出所有证明过程, 让学生真正领会抽象的概念并会用严密的数学推导来证明相应的性质、定理等, 避免由于对英语语言的误解而没有理解代数专业知识的探究.

正是基于这样的考虑, 本教材在内容与写作上有如下三个特点: 第一, 内容处理上兼顾了与所讲概念相关的国际前沿研究性问题; 第二, 增加了理论的应用内容; 第三, 用英语描述概念、性质、定理、例子、应用与习题等, 所有性质、定理等的证明用中文叙述. 我们相信, 通过这样的双语教材的学习, 本科生与国际同行专家交流本方向的专业知识时就会得心应手.

在完成这本书稿的过程中, 博士生王伟、郭双建、王圣祥和张晓辉做了大量校稿和打印工作; 本书的出版得到了东南大学双语教材项目的资助, 在此一并致谢.

书中难免有不足之处, 恳请读者批评指正.

作　者

2012 年 12 月于南京

目　　录

第 1 章　群胚 (Groupoids)

本章主要介绍群胚 (groupoid) 的概念. 这一概念是由 Heinrich Brandt 在 1926 年最先引进的, 它的深层次研究会涉及弱 Hopf 代数 (weak Hopf algebra) 与弱乘子 Hopf 代数 (weak multiplier Hopf algebra) 理论的建立. 为了构造群胚, 我们首先介绍等价关系与集合分类.

1.1　等价关系 (Equivalence Relations)

本节介绍关系 (relation) 且给出例子, 进一步研究等价关系 (equivalence relation).

Definition 1.1.1　A **relation**(关系) on a nonempty set A is a collection of ordered pairs of elements of A. In other words, it is a subset of the Cartesian product $A^2 = A \times A$.

If S is a set, we will use the symbol "$\sim$" to denote either an abstract relation or a specific relation for which there is no standard notation. For $a, b \in S$, we will write $a \sim b$, not $(a, b) \in \sim$, to indicate that a and b are related.

Definition 1.1.2　Let $\sim$ be a relation of a set S.

(1) We say that $\sim$ is **reflexive**(自反性) provided for all $a \in S$, it implies $a \sim a$.

(2) We say that $\sim$ is **symmetric**(对称性) provided for all $a, b \in S$, $a \sim b$ implies $b \sim a$.

(3) We say that $\sim$ is **transitive** (传递性) provided for all $a, b, c \in S$, if $a \sim b$ and $b \sim c$, then $a \sim c$.

Example 1.1.3　(1) Consider the relation "$<$" on $\mathbb{R}$. It is easy to check that "$<$" is transitive but not reflexive and symmetric.

(2) Consider the relation "$\leqslant$" on $\mathbb{R}$. It is easy to check that "$\leqslant$" is transitive and reflexive but not symmetric.

(3) Define the relation $\sim$ as follows: $a, b \in \mathbb{Q}$, if $|a - b| < 1$, then $a \sim b$. It is easy to show that $\sim$ is symmetric and reflexive but not transitive.

Definition 1.1.4　A relation $\sim$ on a set S is called an **equivalence relation** provided $\sim$ is reflexive, symmetric, and transitive.

Example 1.1.5　(1) For $x, y \in \mathbb{R}$, define $x \sim y$ to mean that $x - y \in \mathbb{Z}$. It can be showed that $\sim$ is an equivalence relation on $\mathbb{R}$.

(2) Define the "square" relation $\mathbb{R}$ to mean that $x^2 = y^2$. Then the square relation is an equivalence relation.

(3) For $a, b \in \mathbb{Z}$, define $a \sim b$ to mean that a divides b. Since 0 does not divide 0, $\sim$ is not an equivalence relation.

Definition 1.1.6　Let n be a positive integer. For integers a and b, we say that a is **congruent to** b **modulo** n(a 与 b 同余模 n), and write $a \equiv b \pmod{n}$, provided $a - b$ is divisible by n.

The following statements are various ways to say $a \equiv b \pmod{n}$, that is, the statements are equivalent:

(i) $a \equiv b \pmod{n}$;

(ii) $a - b = kn$ for some integer k;

(iii) $a = kn + b$ for some integer k.

Theorem 1.1.7　Congruence modulo n is an equivalence relation on $\mathbb{Z}$.

证明　首先来验证反身性. 设 a 为任一整数. 由 $a - a = 0$ 和 0 可被 n 整除, 知 $a \equiv a \pmod{n}$ 成立.

下证对称性. 设 a 和 b 为整数, 则知必存在整数 k 使得 $a - b = kn$, 此时有 $b - a = -(a - b) = -(kn) = (-k)n$. 故 n 整除 $b - a$, 即 $b \equiv a \pmod{n}$.

再证传递性. 设 $a \equiv b \pmod{n}$, $b \equiv c \pmod{n}$, 则必存在整数 k, k' 使得 $a - b = kn$, $b - c = k'n$. 于是 $a - c = (k + k')n$. 故 n 整除 $a - c$, 即 $a \equiv c \pmod{n}$.

□

1.2　等价类 (Equivalence Classes)

本节利用等价关系对非空集合进行分类, 同时讨论这两个概念的等价性.

Definition 1.2.1　Let $\sim$ be an equivalence relation on a set S. For each $a \in S$, we define the **equivalence class** (等价类) of a, denoted by $\overline{a}$, to be the set

$$\overline{a} = \{b \in S \mid b \sim a\}.$$

Example 1.2.2 For $x, y \in \mathbb{R}$, define $x \sim y$ to mean that $|x| = |y|$. Then for every $a \in \mathbb{R}$, we have

$$\overline{a} = \{a, -a\}.$$

Theorem 1.2.3 Let $\sim$ be an equivalence relation on the set S. For $a, b \in S$, the following statements are equivalent:

(i) $\overline{a} = \overline{b}$;

(ii) $a \sim b$;

(iii) $a \in \overline{b}$;

(iv) $\overline{a} \cap \overline{b} \neq \varnothing$.

证明 (i)⇒(ii): 易知 $b \in \overline{b} = \overline{a}$, 即 $a \sim b$.

(ii)⇒(iii): 显然.

(iii)⇒(iv): 由 $a \in \overline{b}$ 和 $a \in \overline{a}$, 即可知 $\overline{a} \cap \overline{b} \neq \varnothing$.

(iv)⇒(i): 设 $c \in \overline{a} \cap \overline{b}$, 则 $c \sim a$ 且 $c \sim b$. 再任取 $d \in \overline{a}$, 知 $d \sim a$. 于是由 $\sim$ 为等价关系, 满足传递性, 且 $c \sim a$ 和 $d \sim a$ 可知, $d \sim c$. 又由 $c \sim b$, 故 $d \in \overline{b}$, 即 $\overline{a} \subseteq \overline{b}$.

同理可知 $\overline{a} \supseteq \overline{b}$. 于是 $\overline{a} = \overline{b}$. □

Equivalence classes for congruence mod n are also called **congruence classes**(同余类). Let a be an integer. By the definition of an equivalence class we have

$$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a \bmod(n)\} = \{x \in \mathbb{Z} \mid x - a = kn \text{ for some integer } k\}.$$

For the given n, we denote by $\mathbb{Z}_n$ the set of all congruence classes of $\mathbb{Z}$ for the relation congruence mod n. Thus, $\mathbb{Z}_n = \{\overline{a} \mid a \in \mathbb{Z}\}$.

Theorem 1.2.4 For every positive integer n, $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$.

证明 设 $a \in \mathbb{Z}$, 则由带余除法公理知必存在整数 q, r, 使得 $a = qn + r$ 且 $0 \leqslant r < n$. 故 $a - r = qn$, 即 $a \in \overline{r}$. 由定理 1.2.3 可知,$\overline{a} = \overline{r}$. 从而每个小于 0 或大于 $n-1$ 的数都可以被 $0, 1, \cdots, n-1$ 之中的某数表达出来. 故命题成立. □

Corollary 1.2.5 Let n be a positive integer. For every $a, b \in \mathbb{Z}$, the following statements are equivalent:

(i) In $\mathbb{Z}_n$, $\overline{a} = \overline{b}$;

(ii) $a \equiv b \pmod{n}$, that is, n divides $a - b$;

(iii) $a \in \overline{b}$;

(iv) $\overline{a} \cap \overline{b} \neq \varnothing$.

证明 结合定理 1.2.3 和定理 1.2.4 即可得. □

We know that the set of all equivalence classes of S under $\sim$ is defined to be the set of all subsets of S which are equivalence classes of S under $\sim$, and is denoted by $S/\sim$. The map $x \mapsto \overline{x}$ is sometimes referred to as the **canonical projection**(标准投射).

Definition 1.2.6 Let S be a nonempty set. If S can be represented as a union of some subsets and these subsets are disjoint sets with each other, i.e. $S = \bigcup_{i=1}^{n} S_i$, where $S_i \subseteq S$, $n = 1, 2, \cdots, \infty$, $S_i \cap S_j = \varnothing$ for $i \neq j$, then every S_i is called a **class** of S, and $\{S_i \mid i = 1, 2, \cdots, n\}$ is called a **partition** (划分) of S.

Let S be a set with an equivalence relation $\sim$. We will see that for every equivalence relation $\sim$, the set of all equivalence classes of S under $\sim$ is a partition of S, and this correspondence is a bijection between the set of equivalence relations on S and the set of partitions of S (consisting of nonempty sets).

Theorem 1.2.7 A partition of a nonempty set S decided an equivalence relation $\sim$ in S.

证明　设 $S=\bigcup_{i=1}^{n} S_i$, 其中 $S_i \subseteq S$, $n=1,2,\cdots,\infty$, 且若 $i \neq j, S_i$ 与 S_j 非交.

定义 S 中的关系 $\sim$ 如下:

$$a \sim b \Longleftrightarrow a\text{与}b\text{同在一类, 即}a, b\text{同属于某个}S_i.$$

下证 $\sim$ 为一个等价关系.

对称性: 若 $a \sim b$, 则存在 i, 使得 $a, b \in S_i$. 显然有 $b \sim a$.

反身性: 若 $a \in S$, 则必存在 i, 使得 $a \in S_i$. 即 $a \sim a$.

传递性: 若 $a \sim b$, $b \sim c$, 则存在 i, j, 使得 $a, b \in S_i$, $b, c \in S_j$, 即 $b \in S_i \cap S_j$. 从而必有 $i = j$. 即 $a, b, c \in S_i$. 于是 $a \sim c$.

综上可知, $\sim$ 为等价关系. □

Theorem 1.2.8 An equivalence relation $\sim$ in a nonempty set S decided a partition of S.

证明　设 $\sim$ 为 S 中的一个等价关系, 则易知 $S = \bigcup_{a \in S} \overline{a}$, 其中 $\overline{a}$ 为 a 的等价类. 由定理 1.2.3, 可知若 a 与 b 不等价, 则 $\overline{a}$ 与 $\overline{b}$ 无交. 从而可得 $S = \bigcup_{a_i \in S} \overline{a_i}$, 其中 a_i 取遍 S 中关于 $\sim$ 的等价类的代表元. □

Then we can get the following

Corollary 1.2.9 For a given set S, $\sim$ is an equivalence relation if and only if it produces a partition.

Definition 1.2.10 Let $\sim$ be an equivalence relation on nonempty set S. The set of all equivalence classes in S is called the **quotient set** (商集) of S relative to $\sim$, and is denoted by $S/\sim$ or $\overline{S}$, that is,

$$S/\sim = \{\overline{a} \mid a \in A\} \subseteq P(S),$$

where $P(S)$ is the power set of S.

Define a canonical projection by

$$v : S \to S/\sim \text{ via } a \mapsto \overline{a},$$

which is a surjection.

1.3 群胚 (Groupoids)

本节主要介绍群胚 (groupoid) 的概念, 并给出构造群胚的方法, 同时指出与之相关的国际前沿研究的问题. 见文献 [4]、[5]、[9]、[10] 和 [12].

Definition 1.3.1 A **groupoid** (群胚) is a set G with a unary operation $^{-1}$: $G \to G$ and a partial function $* : G \times G \to G$ (here $*$ is **not** necessarily defined for all possible pairs of G-elements) such that the following axiomatic properties hold: for every $a, b, c \in G$

(i) **Associativity**(结合性): If $a * b$ and $b * c$ are defined, then $(a * b) * c$ and $a * (b * c)$ are defined and equal. Conversely, if either of these last two expressions is defined, then so is the other (and again they are equal);

(ii) **Inverse**(可逆性): $a^{-1} * a$ and $a * a^{-1}$ are always defined;

(iii) **Identity**(单位性): If $a * b$ is defined, then $a * b * b^{-1} = a$, and $a^{-1} * a * b = b$.

From these axioms, it is easy to get $(a^{-1})^{-1} = a$ and that if $a * b$ is defined, then $(a * b)^{-1} = b^{-1} * a^{-1}$.

Remark 1.3.2 Let G be a groupoid. When G is a finite set, we say that G is a **finite groupoid** (有限群胚). When G is an infinite set, we call G an **infinite groupoid** (无限群胚).

Let G be a groupoid. It is a set with a distinguished subset of pairs (p, q) in $G \times G$ for which the product pq in G is defined. This product is associative, in the

appropriate sense. The product pq is only defined when the so-called source $s(p)$ of the element p is equal to the target $t(q)$ of the element q. The source and target maps are defined from G to the set of units and this set can (and will) be considered as a subset of G.

Examples 1.3.3 The simplest example of a groupoid is obtained from an equivalence relation $\sim$ on a set X. The elements of the groupoid G are pairs (y, x) with $x, y \in X$ and $x \sim y$. The set of units is X and the source and target maps are seperately given by

$$s(y, x) = x \quad \text{and} \quad t(y, x) = y,$$

for (y, x) in G. The set of units is considered as a subset of G via the map $x \to (x, x)$. The product of (z, y) with (y, x) is (z, x) when $x, y, x \in X$, $x \sim y$ and $y \sim z$.

国际前沿研究动态

(1) 当 G 是一个有限群胚时, 由此可以定义一个弱 Hopf 代数 (weak Hopf algebra), 研究见文献 [2]、[3]、[6]~[8].

(2) 当 G 是一个无限群胚时, 由此可以定义一个弱乘子 Hopf 代数 (weak multiplier Hopf algebra), 研究见文献 [1]、[11]、[13]~[18].

参 考 文 献

[1] Abe E. Hopf Algebras. New York: Cambridge University Press, 1977.

[2] Böhm G, Nill F, Szlachányi K. Weak Hopf algebras I: integral theory and C^*-structure. Journal of Algebra, 1999, 221(2): 385-438.

[3] Böhm G, Szlachányi K. Weak Hopf algebras II: representation theory, dimensions and the Markov trace. Journal of Algebra, 2000, 233(1): 156-212.

[4] Brown R. From groups to groupoids: a brief survey. Bull. London Math. Soc., 1987, 19: 113-134.

[5] Higgins P J. Notes on Categories and Groupoids// Halmos P R, et al., ed. Van Nostrand Reinhold Mathematical Studies. Vol.32. London: Van Nostrand Reinhold, 1971.

[6] Nikshych D. On the structure of weak Hopf algebras. Adv. Math., 2002, 170: 257-286.

[7] Nikshych D, Vainerman L. Algebraic versions of a finite dimensional quantum groupoid. Lecture Notes in Pure and Applied Mathematics, 2000, 209: 189-221.

[8] Nikshych D, Vainerman L. Finite quantum groupiods and their applications. New Directions in Hopf Algebras, 2002, 43: 211-262.

[9] Paterson A. Groupoids, Inverse Semigroups and Their Operator Algebras. Boston: Birkhauser, 1999.

[10] Renault J. A Groupoid Approach to C^*-algebras//Morel, et al. Lecture Notes in Mathematics. Vol.793. Berlin: Springer Verlag, 1980.

[11] Sweedler M. Hopf Algebras. New York: Benjamin, 1969.

[12] Vainerman L. Locally compact quantum groups and groupoids. IRMA Lectures in Mathematics and Theoretical Physics 2. Proceedings of a meeting in Strasbourg, de Gruyter, 2002.

[13] Van Daele A. Multiplier Hopf algebras. Trans. Am. Math. Soc., 1994, 342(2): 917-932.

[14] Van Daele A. An algebraic framework for group duality. Adv. in Math., 1998, 140: 323-366.

[15] Van Daele A, Wang S H. Weak multiplier Hopf algebras. Preliminaries, motivation and basic examples. Preprint University of Leuven and Southeast University of Nanjing (2012). Arxiv:1210.3954v1 [math.RA]. To appear in the proceedings of the conference .Operator Algebras and Quantum Groups (Warsaw, September 2011), series .Banach Center Publications..

[16] Van Daele A, Wang S H. Weak multiplier Hopf algebras I: The main theory. Preprint University of Leuven and Southeast University of Nanjing (2012). Arxiv: 1210.4395v1[math.RA].

[17] Van Daele A, Wang S H. Weak multiplier Hopf algebras II: The source and target algebras. University of Leuven and Southeast University of Nanjing (in preparation).

[18] Van Daele A, Wang S H. Weak multiplier Hopf algebras III: Integrals and duality. University of Leuven and Southeast University of Nanjing (in preparation).

习　题

1. For $A, B \in P(Z)$, define $A \sim B$ to mean that $A \cap B = \varnothing$ (Recall that $P(Z)$ is the power set of Z),

(i) Prove or disprove that $\sim$ is reflexive;

(ii) Prove or disprove that $\sim$ is symmetric;

(iii) Prove or disprove that $\sim$ is transitive.

2. For $(a,b),(c,d) \in \mathbb{R}^2$, define $(a,b) \sim (c,d)$ to mean that $2a - b = 2c - d$. Prove that $\sim$ is an equivalence relation on $\mathbb{R}^2$.

3. Define a function $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = x^2 + 1$. For $a, b \in \mathbb{R}$, define $a \sim b$ to mean that $f(a) = f(b)$.

(i) Prove that $\sim$ is an equivalence relation on $\mathbb{R}$;

(ii) List all elements in the set $\{x \in \mathbb{R} | x \sim 3\}$.

4. Describe the set of all integers x such that $x \equiv 4 \pmod 9$ and use the description to list all integers x such that $-36 \leqslant x \leqslant 36$ and $x \equiv 4 \pmod 9$.

5. Let m and n be positive integers such that m divides n. Prove that for all integers a and b, if $a \equiv b \pmod n$, then $a \equiv b \pmod m$.

6. Let $\mathbb{R}^*$ denote the set of all nonzero real numbers and let $\mathbb{Q}^*$ denote the set of all nonzero rational numbers. For $a, b \in \mathbb{R}^*$, define $a \sim b$ to mean that $a/b \in \mathbb{Q}^*$. Prove that $\sim$ is an equivalence relation, and prove each of the following:

(i) $\overline{\sqrt{3}} = \overline{\sqrt{12}}$;

(ii) $\overline{\sqrt{3}} \cap \overline{\sqrt{6}} = \varnothing$;

(iii) $\overline{\sqrt{8}} \neq \overline{\sqrt{12}}$;

(iv) $x = 3$ is the solution to the equation $\overline{x\sqrt{2}} = \overline{2\sqrt{2}}$.

7. In $\mathbb{Z}_9$, prove or disprove

(i) $\overline{32} = \overline{50}$;

(ii) $\overline{-33} = \overline{75}$;

(iii) $\overline{-16} = \overline{-37}$.

8. For a positive integer n, set

$$\mathbb{Z}_{(n)} = \{\overline{a} \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}.$$

Thus, for example, $\mathbb{Z}_{(10)} = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$.

(i) Prove that the set $\mathbb{Z}_{(n)}$ is well-defined, that is, prove that for all integers a_1 and a_2, if $\overline{a_1} = \overline{a_2}$ in $\mathbb{Z}_{(n)}$ and $\overline{a_1} \in \mathbb{Z}_{(n)}$, then $\overline{a_2} \in \mathbb{Z}_{(n)}$;

(ii) Prove that for all integers a and b, if $\overline{a}, \overline{b} \in \mathbb{Z}_{(n)}$, then $\overline{ab} \in \mathbb{Z}_{(n)}$.

第 2 章　群 (Groups)

本章主要介绍群 (group) 的概念 (最先由 E.Galois 引进) 及其结构性质, 涉及子群 (subgroup)、正规子群 (normal subgroup)、对称群 (symmetric group)、群同态 (homomorphism) 和商群 (quotient group). 它的深层次研究会涉及量子群 (quantum group) 与乘子 Hopf 代数 (multiplier Hopf algebra) 理论的建立.

2.1　群　概　念

本节主要介绍群的定义并给出群的简单例子.

Definition 2.1.1　A **binary operation**(二元运算) on a set G is a function $*: G \times G \to G$.

In more details, an operation assigns an element $*(x, y)$ in G to each ordered pair (x, y) of elements in G. It is more natural to write $x * y$ instead of $*(x, y)$; thus, composition of functions is the function $(f, g) \mapsto g \circ f$, while multiplication, addition, and subtraction are respectively the functions $(x, y) \mapsto xy$, $(x, y) \mapsto x + y$, and $(x, y) \mapsto x - y$. The examples of composition and subtraction show why we want ordered pairs, for $x*y$ and $y*x$ may be distinct. As function,each operation is single-valued; when one says this explicitly, it is usually called the **law of substitution**:

$$\text{if } x = x' \text{ and } y = y', \text{ then } x * y = x' * y'.$$

Definition 2.1.2　A **group**(群) $(G, *, e)$ is a nonempty set G equipped with a binary operation $*$ and a special element $e \in G$ called the **identity**(单位元), such that

(1) **Associativity**(结合性) holds: for every $a, b, c \in G$,

$$a * (b * c) = (a * b) * c;$$

(2) **Left Identity**(左单位性) holds: $e * a = a$ for all $a \in G$, i.e., e is a left identity;

(3) **Left inverse** (左逆性) holds: for every $a \in G$, there is $a' \in G$ with $a' * a = e$, i.e., a' is a left inverse of a.

Remark 2.1.3 We can refer to G in place of a group $(G, *, e)$, provided that no confusion will result.

Example 2.1.4 (1) The set of integers under addition forms an infinite additive group, $(\mathbb{Z}, +, 0)$.

(2) The set of nonzero real numbers under multiplication forms an infinite multiplicative group, $(\mathbb{R} \setminus \{0\}, \times, 1)$.

(3) The complex numbers under the operation of addition, forms a group, $(\mathbb{C}, +, 0)$.

(4) The set

$$S = \{x + y\sqrt{2} | x, y \in \mathbb{Z}, \text{ where } (x, y) \neq (0, 0)\}$$

under multiplication forms a group, $(S, \times, 1)$.

Let G be a group. If for all $x, y \in G$, $xy = yx$, we call the group **Abelian or commutative** (阿贝尔或交换的).

Lemma 2.1.5 If $*$ is an associative operation on a set G, then

$$(a * b) * (c * d) = [a * (b * c)] * d,$$

for all $a, b, c, d \in G$.

证明　如果设 $g = a * b$, 那么就有 $(a * b) * (c * d) = g * (c * d) = (g * c) * d = [(a * b) * c] * d = [a * (b * c)] * d$. □

Lemma 2.1.6 If G is a group and $a \in G$ satisfies $a * a = a$, then $a = e$.

证明　由群定义知, 存在 $a' \in G$ 使得 $a' * a = e$. 在 $a * a = a$ 左右两边同时乘以 a', 则等式右边为 e, 而左边为 $a' * (a * a) = (a' * a) * a = e * a = a$, 所以 $a = e$. □

Proposition 2.1.7 Let G be a group with operation $*$ and identity e, then we have

(1) $a * a' = e$ for all $a \in G$;

(2) $a * e = a$ for all $a \in G$;

(3) if $e_0 \in G$ satisfies $e_0 * a = a$ for all $a \in G$, then $e_0 = e$;

(4) if $a \in G$. If $b \in G$ satisfies $b * a = e$, then $b = a'$.

证明 (1) 我们已知 $a' * a = e$, 接下来证明 $a * a' = e$. 由引理 2.1.5,

$$\begin{aligned}(a * a') * (a * a') &= [a * (a' * a)] * a' \\ &= (a * e) * a' \\ &= a * (e * a') \\ &= a * a'.\end{aligned}$$

再根据引理 2.1.6, $a * a' = e$.

(2) 应用 (1)

$$a * e = a * (a' * a) = (a * a') * a = e * a = a.$$

因此, $a * e = a$.

(3) 我们现在证明一个群只含有唯一的单位元. 如果 $e_0 * a = a$, 对所有的 $a \in G$, 那么特别地 $e_0 * e_0 = e_0$. 再由引理 2.1.6, $e_0 = e$.

(4) 在 (1) 中, 我们证得如果 $a' * a = e$, 则 $a * a' = e$. 那么

$$b = b * e = b * (a * a') = (b * a) * a' = e * a' = a'. \qquad \square$$

From this proposition, we know that a **left inverse** is also a **right inverse**. Thus, we use a^{-1} to denote the inverse of a. The identity element of a group can also be denoted by 1.

We now present a very important group. In high school mathematics, the words of permutation and arrangement are used interchangeably, if the word arrangement is used at all. We draw a distinction between them.

Definition 2.1.8 If X is a set, then a **list** in X is a function $f : \{1, 2, \cdots, n\} \to X$. If a list f in X is a bijection (so that X is now a finite set with $|X| = n$), then f is called an **arrangement** of X.

If f is a list, denote its values $f(i)$ by x_i, where $1 \leqslant i \leqslant n$. Thus, a list in X is merely an n-tuple $(x_1, x_2, \cdots, x_n)$. To say that a list f is injective is to say that there are no repeated coordinates [if $i \neq j$, then $x_i = f(i) \neq f(j) = x_j$]; to say that f is surjective is to say that every $x \in X$ occurs as some coordinate. Thus, an arrangement of X is an n-tuple $(x_1, x_2, \cdots, x_n)$ of all the elements of X with no repetitions. We often omit parentheses and write a list as $x_1, x_2, \cdots, x_n$. For example, there are 27 lists in $X = \{a, b, c\}$ and 6 arrangements:

$$abc; \quad acb; \quad bac; \quad bca; \quad cab; \quad cba.$$