



# 近世代数引论

冯克勤

仅供学习使用，严禁商业使用

# 修订版前言

这本讲义《近世代数引论》在中国科学技术大学使用了十余年.学生的反映尚好,主要问题是习题较难.所以我们在书末对于较难的习题增加了提示,同时也补充了一些新的习题.在内容上去掉“幂零群与可解群”和“ $n \geq 5$ 次一般方程的根式不可解性”两节,把它们改成两个附录.如果学时不够,正文中某些部分也可略去不讲或者只做简要介绍.例如伽罗瓦理论可以只介绍基本定理的内容和它的应用,而不讲证明.对于希洛夫定理、有限生成阿贝耳群的结构、唯一因子分解整环等内容也可以类似地处理.

# 前言

近世代数是讲述群、环、域(以及模)等代数对象基本性质的一门大学课程.它是今后学习和研究代数学的基础,也是研究其他数学、物理学和计算机科学等不可缺少的工具.

本书是我们于1982年在中国科技大学授课讲义基础上,经过五年教学实践改写而成.原讲义共五章,为了在一学期(周四学时)内讲完,这次删去了模论和线性代数两章.

近世代数从它产生的年代起就明显有别于古典代数学.它的主要研究对象不是代数结构中的元素特性,而是各种代数结构本身和不同代数结构之间的相互联系(同态).掌握近世代数中所体现的丰富的数学思想和方法,比背诵一些代数学定义和名词字典要重要得多.我们在教学中几乎用半个学期讲述第一章群论,这是因为在群论中体现了近世代数的基本研究思想和方法,而这些思想和方法在学生过去学习中是不熟悉的.群论中的定理基本上可分为定量和定性两类:前者的典型例子是拉格朗日定理,后者的典型例子是同态基本定理.我们着重讲授定性内容,特别是同态基本定理和群在集合上的作用,这是群论的关键所在.

第二章讲述环论和域论初步,正文中的内容是标准的.但是在几个附录中,我们介绍了在数学发展中有历史意义的几个课题(高斯二平方和问题,代数基本定理,尺规作图,三等分角等),最后一章向学生展示关于域的有限伽罗瓦扩张的优美理论.

最后,我们向过去几年里对此书的前身提供意见的许多学者、教师和学生表示深深的谢意,我们也欢迎大家今后对此书给予更多的批评和指正.

# 目录

修订版前言	i
前言	ii
第一章 群	2
1.1 集合论预备知识 . . . . .	2
1.2 什么是群 . . . . .	6

# 第一章 群

## 1.1 集合论预备知识

群是集合上赋予某种二元运算的一种代数结构.所以在讲述什么是群之前,先要介绍集合论中我们需要的一些预备知识.

一些特定的对象放在一起就叫做一个**集合**.例如全体正整数构成一个集合,表示成  $\mathbb{N}$ .全体整数构成整数集合,表示成  $\mathbb{Z}$ .类似地有复数集合  $\mathbb{C}$ ,实数集合  $\mathbb{R}$ ,有理数集合  $\mathbb{Q}$  等等.集合  $A$  中每个对象  $a$  叫做  $A$  中的**元素**,表示成  $a \in A$ ,说成  $a$  属于  $A$ .否则,如果某个对象  $b$  不属于  $A$ ,则表示成  $b \notin A$ .

设  $A$  和  $B$  是两个集合,如果  $A$  中每个元素均是  $B$  中元素,即

$$a \in A \Rightarrow a \in B.$$

则  $A$  叫做  $B$  的一个**子集**,表示成  $A \subseteq B$  或者  $B \supseteq A$ .如果  $A \subseteq B$  并且  $B \subseteq A$ ,即

$$a \in A \Leftrightarrow a \in B,$$

这也相当于说集合  $A$  与  $B$  包含同样的元素,这时叫做集合  $A$  与  $B$  相等,表示成  $A = B$ .如果  $A$  是  $B$  的子集并且不等于  $B$ ,则  $A$  叫  $B$  的**真子集**,表示成  $A \subset B$  或者  $B \supset A$ .不包含任何元素的集合叫做**空集**,表示成  $\emptyset$ .空集显然是每个集合的子集.

可以有多种方式来表达一个确定的集合.例如若集合  $A$  只有限多(不同)元素  $a_1, \dots, a_n (n \in \mathbb{N})$ ,则这个集合可表成

$$A = \{a_1, \dots, a_n\}.$$

只有有限多个元素的集合叫**有限集**,否则叫**无限集**.具有  $n$  个元素的集合叫  $n$  **元集**,元素个数表示成  $|A| = n$ .在一般情形下,集合  $S$  中具有某种性质  $P$  的全体元素构成的集合通常表成

$$\{x \in S \mid x \text{ 有性质 } P\}.$$

例如:偶数集合  $\{0, \pm 2, \pm 4, \dots\}$  可以表成

$$\{n \in \mathbb{Z} \mid n \equiv 0 \pmod{2}\}.$$

由一些已知集合构造新的集合通常用集合上的运算来实现.下面是集合的一些最基本运算.设  $A$  和  $B$  是两个集合,它们的公共元素组成的集合叫做  $A$  和  $B$  的**交**,表示成  $A \cap B$ ,即

$$A \cap B = \{x \mid x \in A \text{ 并且 } x \in B\}.$$

类似地,  $n$  个集合  $A_1, \dots, A_n$  的交为

$$\bigcap_{i=1}^n A_i = A_1 \cap A_2 \cap \dots \cap A_n = \{x \mid x \in A_i, 1 \leq i \leq n\}.$$

更一般地,对于任意多个集合形成的集族  $\{A_i \mid i \in I\}$  (其中  $I$  是一个集合,叫该集族的下标集合,对于每个  $i \in I$ ,  $A_i$  是该集族中的一个集合),它们的交为

$$\bigcap_{i \in I} A_i = \{x \mid x \in A_i, \text{对每个 } i \in I\}.$$

第二个集合运算是集合的并,集合  $A$  与  $B$  的并表示成  $A \cup B$ , 定义为

$$A \cup B = \{x \mid x \in A \text{ 或者 } x \in B\}.$$

类似地:

$$\bigcup_{i=1}^n A_i = A_1 \cup A_2 \cup \cdots \cup A_n = \{x \mid x \in A_i, \text{对某个 } i \in I\}.$$

设  $A$  是  $B$  的子集,则  $B - A = \{x \mid x \in B, x \notin A\}$  叫做子集  $A$  (关于  $B$ ) 的补集.如果在讨论问题中所涉及的集合均是某个固定集合  $\Omega$  的子集,则  $\Omega - A$  也常常简称作  $A$  的补集,表示成  $\bar{A}$ .

设  $A$  和  $B$  是两个集合,我们把集合

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

叫做  $A$  和  $B$  的直积.在  $A \times B$  中,  $(a, b) = (a', b')$  当且仅当  $a = a'$  并且  $b = b'$ .类似可定义多个集合的直积

$$A_1 \times \cdots \times A_n = \prod_{i=1}^n A_i = \{(a_1, \cdots, a_n) \mid a_i \in A_i, 1 \leq i \leq n\}.$$

$$\prod_{i \in I} A_i = \{(a_i)_{i \in I} \mid a_i \in A_i, \text{对每个 } i \in I\}$$

为了比较不同的集合,需要将不同集合发生联系,这就是集合之间的映射.  $f$  叫做从集合  $A$  到集合  $B$  的映射,是指对每个  $a \in A$  均有确定办法给出集合  $B$  中唯一的对应元素,这个对应元素叫做  $a$  在映射  $f$  之下的象,表示成  $f(a)$ .而“ $f$  把  $a$  映成  $f(a)$ ”这件事表示成  $a \rightarrow f(a)$ .从  $A$  到  $B$  的映射  $f$  表示成  $f: A \rightarrow B$  或者  $A \xrightarrow{f} B$ . 设  $f: A \rightarrow B$  和  $g: B \rightarrow C$  都是集合之间的映射.则可经过连续作用,得到一个从  $A$  到  $C$  的映射

$$g \circ f: A \rightarrow C, \quad (g \circ f)(a) = g(f(a)).$$

映射  $g \circ f$  叫做  $f$  与  $g$  的合成映射.

设  $f$  和  $g$  均是从集合  $A$  到集合  $B$  的映射,我们称  $f$  和  $g$  相等(表示成  $f = g$ ),是指对于每个  $a \in A$ ,均有  $f(a) = g(a)$ .

**引理 1** (合成运算满足结合律) 设  $f: A \rightarrow B$ ,  $g: B \rightarrow C$ ,  $h: C \rightarrow D$  均是集合的映射,则

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

**证明** 对于  $a \in A$ , 令  $f(a) = b$ ,  $g(b) = c$ ,  $h(c) = d$ . 则

$$(g \circ f)(a) = c, \quad (h \circ g)(b) = d. \text{ 于是}$$

$$(h \circ (g \circ f))(a) = h(c) = d, \quad ((h \circ g) \circ f)(a) = (h \circ g)(b) = d. \quad \square$$

设  $f: A \rightarrow B$  是集合的映射.对于  $A$  的每个子集  $A'$ , 令

$$f(A') = \{f(x) \mid x \in A'\},$$

这是  $B$  的子集,叫做  $A$  在  $f$  之下的象.另一方面,对于  $B$  的子集  $B'$ ,令  $f^{-1}(B') = \{x \in A \mid f(x) \in B'\}$ ,这是  $A$  的子集,叫做  $B'$  的原象.如果  $f(A) = B$ ,即  $B$  中每个元素均是  $A$  中某个元素(在  $f$  之下)的象,则  $f$  叫做满射.另一方面,如果  $A$  中不同元素被  $f$  映成  $B$  中不同元素,即:  $a, a' \in A, a \neq a' \Rightarrow f(a) \neq f(a')$ ,则  $f$  叫做单射.最后,若  $f: A \rightarrow B$  同时是单射和满射,则  $f$  叫做一一映射或一一对应.例如:将集合  $A$  中每个元素均映成其自身的映射

$$1_A: A \rightarrow A, 1_A(a) = a.$$

就是  $A$  到  $A$  的一一对应.映射  $1_A$  叫做集合  $A$  的恒等映射.通常采用下面引理来判断一个映射是否为一一对应.

**引理 2** 映射  $f: A \rightarrow B$  是一一对应的充分必要条件是存在映射  $g: B \rightarrow A$ ,使得  $f \circ g = 1_B, g \circ f = 1_A$ .

**证明** 如果  $f$  是一一对应,由定义知这意味着对每个  $b \in B$ ,均存在唯一的  $a \in A$  使得  $f^{-1}(b) = a$  (存在性由于  $f$  是满射,唯一性由于  $f$  是单射)于是可定义映射

$$g: B \rightarrow A, g(b) = f^{-1}(b).$$

直接验证  $g \circ f = 1_A$  和  $f \circ g = 1_B$  成立.

另一方面,如果  $f$  不是满射,则存在  $b \in B$ ,使得  $f^{-1}(b) = \emptyset$ .所以对每个映射  $g: B \rightarrow A$ ,均有  $(f \circ g)(b) = f(g(b)) \neq b$ .于是  $f \circ g \neq 1_B$ .如果  $f$  不是单射,则存在  $a, a' \in A, a \neq a'$ ,使得  $f(a) = f(a') = b$ .那么对于每个映射  $g: B \rightarrow A, (g \circ f)(a) = g(b) = (g \circ f)(a')$ ,于是  $g \circ f \neq 1_A$ .所以若存在  $g: B \rightarrow A$  使得  $f \circ g = 1_B$  并且  $g \circ f = 1_A$ .则必然  $f$  是一一对应.  $\square$

当  $f: A \rightarrow B$  是一一对应时,满足  $f \circ g = 1_B$  和  $g \circ f = 1_A$  的映射  $g: B \rightarrow A$  是唯一的.这是因为:若  $g: B \rightarrow A$  也有性质  $f \circ g' = 1_B, g' \circ f = 1_A$ ,则  $g' = g' \circ 1_B = g' \circ (f \circ g) = (g' \circ f) \circ g = 1_A \circ g = g$ .我们将这个唯一存在的映射  $g$  叫做  $f$  的逆映射,表示成  $f^{-1}$ .

设  $A$  是集合,集合  $A \times A$  的每个子集  $R$  叫做集合  $A$  上的一个关系.如果  $(a, b) \in R$ ,便称  $a$  和  $b$  有关系  $R$ ,写成  $aRb$ .例如  $\mathbf{R} \times \mathbf{R}$  中子集

$$R = \{(a, b) \in \mathbf{R} \times \mathbf{R} \mid a \text{ 比 } b \text{ 大}\}$$

则实数  $a$  和  $b$  有关系  $R$  即指  $a$  比  $b$  大,这就是“大于”关系.通常将这个关系记成  $a > b$ .同样还有  $\mathbf{R}$  上的关系  $\geq$  (大于或等于),  $<$  (小于),  $\leq$  (小于或等于),  $=$  (等于).集合  $A$  上的关系  $\sim$  叫做等价关系,是指它满足如下三个条件:

- (1)自反性:  $a \sim a$  (对于每个  $a \in A$ )
- (2)对称性:若  $a \sim b$ ,则  $b \sim a$ .
- (3)传递性:若  $a \sim b, b \sim c$ ,则  $a \sim c$ .

设  $\sim$  是集合  $A$  上的等价关系.如果  $a \sim b$ ,由对称性知  $b \sim a$ .这时称元素  $a$  和  $b$  等价.对于每个  $a \in A$ ,以  $[a]$  表示  $A$  中与  $a$  等价的全部元素构成的集合,即

$$[a] = \{b \in A \mid b \sim a\}.$$

由自反性知  $a \in [a]$ ,称  $[a]$  为  $a$  所在的等价类,由传递性可知同一等价类中任意二元素彼此等价(设  $b, c \in [a]$ ,则  $b \sim a, a \sim c$ ,于是  $b \sim c$ ).不同等价类之间没有公共元素(为什么?)因此集合  $S$  是一些等价类  $\{[a_i] \mid i \in I\}$  的并,而这些等价类是两两不相交的.我们从每个等价类  $[a_i]$  中取出一个元素  $b_i$ ; (即  $b_i \in [a_i]$ )

),则  $R = \{b_i | i \in I\}$  具有如下性质:  $A$  中每个元素均等价于某个  $b$ , 而不同的  $b$  彼此不等价. 我们把具有这样性质的  $R$  叫做  $S$  对于等价关系  $\sim$  的完全代表系. 于是

$$A = \bigcup_{a \in R} [a] \text{ (两两不相交之并)}. \quad (*)$$

一般地, 若集合  $A$  是它的某些子集  $\{A_i | i \in I\}$  之并, 并且  $A_i$  两两不相交, 便称  $\{A_i | i \in I\}$  是集合  $S$  的一个分拆. 如上所述,  $S$  上的每个等价关系给出集合  $A$  的一个分拆(\*). 反过来, 如果  $\{A_i | i \in I\}$  是集合  $A$  的一个分拆, 可如下定义  $A$  上一个关系: 对于  $a, b \in A$ ,

$$a \sim b \Leftrightarrow a \text{ 和 } b \text{ 在同一 } A_i \text{ 之中},$$

请读者证明这是等价关系. 以  $E$  表示  $A$  的全部等价关系, 以  $P$  表示  $A$  的全部分拆, 则上面由等价关系到分拆的映射  $f: E \rightarrow P$  和从分拆到等价关系的映射  $g: P \rightarrow E$  满足  $f \circ g = 1_P$ ,  $g \circ f = 1_E$ , 从而  $f$  是一一对应. 引理 2. 换句话说, 集合  $A$  上的等价关系和  $A$  的分拆是一一对应的.

例如, 设  $F$  是由某些集合构成的集族. 在  $F$  上定义如下的关系: 对于  $A, B \in F$ ,

$$A \sim B \Leftrightarrow \text{存在从 } A \text{ 到 } B \text{ 的一一对应}.$$

这是  $F$  上的等价关系(自反性:  $1_A: A \rightarrow A$  是一一对应, 从而  $A \sim A$ . 对称性: 若  $f: A \rightarrow B$  是一一对应, 则  $f^{-1}: B \rightarrow A$  是一一对应, 从而  $A \sim B \Rightarrow B \sim A$ . 传递性基于习题 3.) 对于这种等价关系, 彼此等价的集合叫做是等势的. 比如说, 两个有限集合等势(即存在一一对应)的充要条件是它们有同样多元素, 即  $|A| = |B|$ . 与正整数集合  $N$  等势的集合叫做可数无限集合, 其他无限集合叫做不可数集合. 熟知实数集合  $R$  是不可数集合. 而正偶整数的全体  $E$  是可数(无穷)集合, 因为存在着  $N \rightarrow E, n \rightarrow 2n$ . 这个例子也表明, 无限集合  $A$  的一个真子集可以与  $A$  等势!

设  $A$  是集合. 从  $A \times A$  到  $A$  的映射

$$f: A \times A \rightarrow A$$

叫做集合  $A$  上的一个(二元)运算. 例如: 通常复数加法就是运算

$$f: C \times C \rightarrow C, f(\alpha, \beta) = \alpha + \beta.$$

我们经常把集合  $A$  上的运算表示成  $\cdot$ , 即对于  $a, b \in A$ ,  $f(a, b)$  写成  $a \cdot b$  ( $\in A$ ) 或者更简单写成  $ab$ .

运算  $\cdot$  叫做满足结合律, 是指

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \text{ (对任意 } a, b, c \in A \text{)}.$$

运算  $\cdot$  叫做满足交换律, 是指

$$a \cdot b = b \cdot a \text{ (对任意 } a, b \in A \text{)}.$$

一个集合赋予满足某些特定性质的(一个或多个)二元运算, 便得到各种代数结构. 本书讲述群、环和域三种代数结构.

## 习 题

1. 设  $B, A_i (i \in I)$  试证:

$$(a) B \cap (\bigcup_{i \in I} A_i) = \bigcup_{i \in I} (B \cap A_i),$$



$$(b) B \cup (\bigcap_{i \in I} A_i) = \bigcap_{i \in I} (B \cup A_i),$$

$$(c) \overline{\bigcup_{i \in I} A_i} = \bigcap_{i \in I} \overline{A_i}, \quad \overline{\bigcap_{i \in I} A_i} = \bigcup_{i \in I} \overline{A_i}.$$

2. 设  $f: A \rightarrow B$  是集合的映射,  $A$  是非空集合. 试证:

(a)  $f$  为单射  $\Leftrightarrow$  存在  $g: B \rightarrow A$ , 使得  $g \circ f = 1_A$ .

(b)  $f$  为满射  $\Leftrightarrow$  存在  $h: B \rightarrow A$ , 使得  $f \circ h = 1_B$ .

3. 如果  $f: A \rightarrow B, g: B \rightarrow C$  均是一一对应, 则  $g \circ f: A \rightarrow C$  也是一一对应, 且  $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ .

4. 设  $A$  是有限集,  $P(A)$  是  $A$  的全部子集(包括空集)所构成的集族, 试证  $|P(A)| = 2^{|A|}$ . 换句话说,  $n$  元集合共有  $2^n$  个不同的子集.

5. 设  $f: A \rightarrow B$  是集合的映射. 在集合  $A$  上如下定义一个关系: 对任意  $a, a' \in A, a \sim a'$  当且仅当  $f(a) = f(a')$ . 试证, 这样定义的关系是一个等价关系.

6. 证明等价关系的三个条件是互相独立的, 也就是说, 已知任意两个条件不能推出第三个条件.

7. 设  $A, B$  是两个有限集合.

(a)  $A$  到  $B$  的不同映射共有多少个?

(b)  $A$  上不同的二元运算共有多少个?

## 1.2 什么是群

让我们先从半群讲起.

**定义** 集合  $S$  和  $S$  上满足结合律的二元运算  $\cdot$  所形成的代数结构叫做**半群**. 这个半群记成  $(S, \cdot)$  或者简记成  $S$ , 运算  $x \cdot y$  也常常简写成  $xy$ .

如果运算又满足交换律, 则  $(S, \cdot)$  叫做**交换半群**. 象通常那样令  $x^2 = x \cdot x, x^{n+1} = x^n \cdot x (= x \cdot x^n, n \geq 1)$

**定义** 设  $S$  是半群, 元素  $e \in S$  叫做半群  $S$  的**么元素**, 是指对每个  $x \in S, xe = ex = x$ .

如果半群  $S$  有么元素  $e$ , 则它是唯一的, 因若  $e'$  也是么元素, 则  $e' = e'e = e$ . 我们将半群  $S$  中这个唯一的么元素(如果存在的话)通常记作  $1_S$  或者  $1$  具有么元素的半群叫**含么半群**.

**定义** 设  $S$  是含么半群, 元素  $y \in S$  叫做元素  $x \in S$  的**逆元素**, 是指  $xy = yx = 1$ .

如果  $x$  有逆元素, 则它一定唯一. 因为若  $y'$  也是  $x$  的逆元素, 则  $xy' = y'x = 1$ . 于是

$$y = y \cdot 1 = y(xy') = (yx)y' = 1 \cdot y' = y'.$$

所以若  $x$  具有逆元素, 我们把这个唯一的逆元素记作  $x^{-1}$ , 则  $xx^{-1} = x^{-1}x = 1$ .

**定义** 定义半群  $G$  如果有么元素, 并且每个元素均可逆, 则  $G$  叫做**群**. 此外, 若运算又满足交换律, 则  $G$  叫做**交换群**或叫**阿贝耳(Abel)群**.

下面给出半群和群的一些例子.

**例 1** 设  $M$  为非负整数全体,  $(M, +)$  是含么交换半群, 么元素是数  $0$ , 但它不是群, 因为只有  $0$  对于加法在  $M$  中才可逆.

$\mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}$  对于加法均是阿贝耳群,叫做整数加法群,有理数加法群等等.

$(N, \cdot)$  是含么交换(乘法)半群,么元素为 1.它不是群.令  $\mathbf{Q}^*$  为非零有理数全体,则  $(\mathbf{Q}^*, \cdot)$  是交换群,么元素为 1,非零有理数  $a$  的乘法逆为  $a^{-1}$ .这叫非零有理数乘法群,同样有  $(\mathbf{R}^*, \cdot)$  和  $(\mathbf{C}^*, \cdot)$ ,这些都是阿贝耳群.

**例 2** 以  $M_{m,n}(\mathbf{C})$  表示全体  $m$  行  $n$  列复矩阵组成的集合,它对矩阵加法形成阿贝耳群.么元素是全零矩阵,而矩阵  $A = (a_{ij})$  的加法逆是  $-A = (-a_{ij})$ .以  $M_n(\mathbf{C})$  表示  $n$  阶复方阵全体,它对乘法形成含么半群,么元素是单位方阵  $I_n$ .由线性代数可知, $n$  阶复方阵  $A$  有乘法逆的充要条件是  $\det A \neq 0$ .从而  $M_n(\mathbf{C})$  不是群,并且当  $n \geq 2$  时,易知半群  $M_n(\mathbf{C})$  不是交换的.类似有加法交换群  $M_{m,n}(\mathbf{R})$ ,含么半群  $M_n(\mathbf{Q})$  等等.

**例 3** 设  $A$  是非空集合,以  $\Sigma(A)$  表示从  $A$  到  $A$  全体映射组成的集合.则  $\Sigma(A)$  对于映射合成运算形成含么半群.么元素为  $A$  上恒等映射  $1_A$ .由 1.1 的引理 2 可知,  $\Sigma(A)$  中映射  $f$  可逆的充要条件是  $f$  为一一对应.所以当  $|A| > 1$  时,  $\Sigma(A)$  不是群,并且半群  $\Sigma(A)$  不是交换的.

**例 4** 欧氏平面  $\mathbf{R}^2$  中保持欧氏距离不变的运动叫做欧氏运动.由于欧氏运动必为  $\mathbf{R}^2$  到自身之上的一一对应,并且它的逆仍是欧氏运动,而两个欧氏运动的合成仍是欧氏运动,从而全体欧氏运动形成群,叫做平面上的欧氏运动群,这也是非阿贝耳群.

**例 5** 设  $n$  为正整数,我们在  $\mathbf{Z}$  上定义如下关系:对于整数  $a$  和  $b$ ,

$$a \sim b \Leftrightarrow n \mid a - b \text{ (即 } a \equiv b \pmod{n} \text{)}$$

易知这是等价关系,于是整数集合  $\mathbf{Z}$  分拆成  $n$  个等价类:  $\bar{0}, \bar{1}, \dots, \overline{n-1}$ , 其中  $\bar{i}$  表示  $i$  所在的等价类,即  $\bar{i} = \{m \in \mathbf{Z} \mid m \equiv i \pmod{n}\}$ .而  $\{0, 1, 2, \dots, n-1\}$  是  $\mathbf{Z}$  对于上述模  $n$  同余关系的一个完全代表系.

以  $Z_n$  表示上述  $n$  个等价类组成的集合.在  $Z_n$  上定义加法:

$$\bar{a} + \bar{b} = \overline{a + b}$$

由同余式基本性质可知这个加法运算是可以定义的,即与等价类(或叫模  $n$  同余类)中代表元的取法无关,并且  $Z_n$  对于这个运算形成交换群,么元素是  $\bar{0}$ ,这叫整数模  $n$  加法群.

如果  $Z_n$  中定义乘法

$$\bar{a}\bar{b} = \overline{ab}$$

则  $Z_n$  对此乘法是含么交换半群,么元素为  $\bar{1}$ .由于等式  $\bar{a}\bar{b} = \bar{1}$  相当于同余式  $ab \equiv 1 \pmod{n}$ .从初等数论知道,对于给定的  $a$ ,存在  $b$  满足  $ab \equiv 1 \pmod{n}$  的充要条件是  $(a, n) = 1$ .从而  $a$  对于上述乘法可逆的充要条件是  $(a, n) = 1$ .

设  $(M, \cdot)$  是含么半群,我们以  $U(M)$  或者  $M^*$  表示半群  $M$  中可逆元素全体.

**定义** 若  $(M, \cdot)$  是含么半群,则  $(U(M), \cdot)$  是群.

**证明** 由  $1_M^{-1} = 1_M$  可知  $1 = 1_M \in U(M)$ .若  $a, b \in U(M)$ ,则  $a, b$  均可逆,易知  $b^{-1}a^{-1}$  是  $ab$  的逆元素,从而  $ab \in U(M)$ .因此  $\cdot$  是  $U(M)$  上的二元运算.这运算在  $U(M)$  中当然也满足结合律,于是  $(U(M), \cdot)$  是含么半群.由于  $U(M)$  中每个元素  $a$  均可逆,从而  $a^{-1} \in M$  也可逆(因为  $a$  是  $a^{-1}$  的逆),因此  $a^{-1} \in U(M)$ .从而  $U(M)$  中每个元素在  $U(M)$  中均可逆.根据定义,  $U(M)$  为群.  $\square$

于是由前面的例子便知:

1. 全体  $n$  阶可逆复方阵形成乘法群,叫做复数上的  $n$  次一般线性群,表示成  $GL(n, \mathbf{C})$ .同样有群  $GL(n, \mathbf{R})$ ,  $GL(n, \mathbf{Q})$  等.

2. 设  $A$  为非空集合,  $A$  到自身之上的所有一一对应对于合成运算形成群, 叫做集合  $A$  上的对称群或全置换群, 表示成  $S(A)$ , 其中元素(即  $A$  到  $A$  的一一对应)叫做集合  $A$  上的置换.
3. 设  $n$  为正整数,  $\bar{a}$  为整数  $a$  的模  $n$  同余类. 则集合

$$Z_n^* = \{\bar{a} \mid (a, n) = 1\}$$

对于乘法形成阿贝耳群. 这个群有  $\varphi(n)$  个元素, 其中  $\varphi(n)$  是 1 到  $n$  中与  $n$  互素的整数个数( $\varphi(n)$  叫欧拉函数).

设  $G$  是群. 若集合  $G$  有限, 称  $G$  为有限群, 否则叫无限群. 若有限群  $G$  共有  $n$  个元素, 则  $G$  叫  $n$  阶群或叫  $n$  元群,  $n = |G|$  叫有限群  $G$  的阶.

为了考查各种群之间的联系, 我们要研究群之间的映射. 但是群不仅是集合还有运算, 所以我们需要映射与群运算保持协调. 确切地说:

**定义** 设  $(G, \cdot)$  和  $(G', \circ)$  是两个群. 映射  $f: G \rightarrow G'$  叫做群  $G$  到群  $G'$  的同态, 是指对  $a, b \in G$

$f(a \cdot b) = f(a) \circ f(b)$  (简记为  $f(ab) = f(a)f(b)$ ). 此外, 若  $f$  又为单射或满射, 则  $f$  分别叫单同态或满同态. 如果同态  $f$  是一一对应, 则称  $f$  是群  $G$  到群  $G'$  的同构. 这时, 称群  $G$  和  $G'$  是同构的, 表示成  $G = G'$  或者  $f: G \xrightarrow{\sim} G'$ .

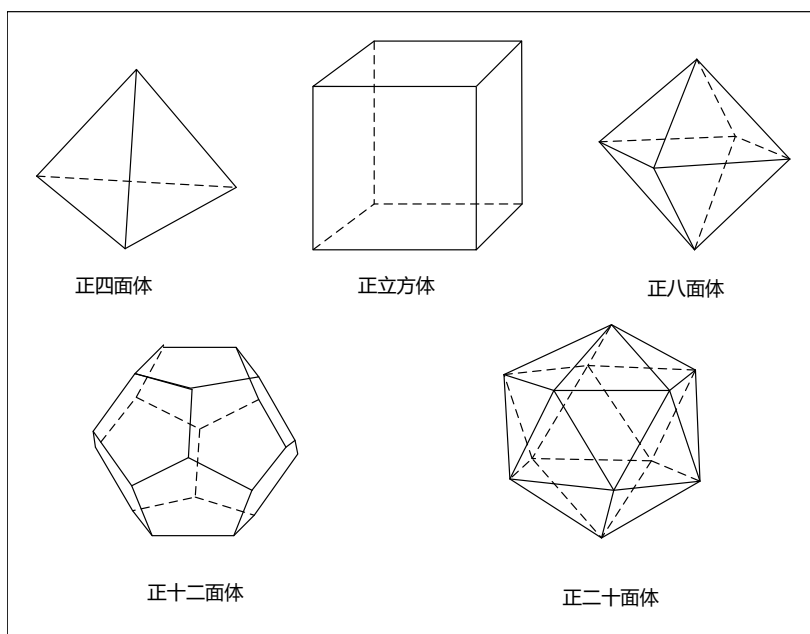


图 1.1:

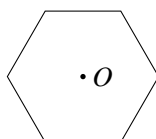


图 1.2: 正六边形