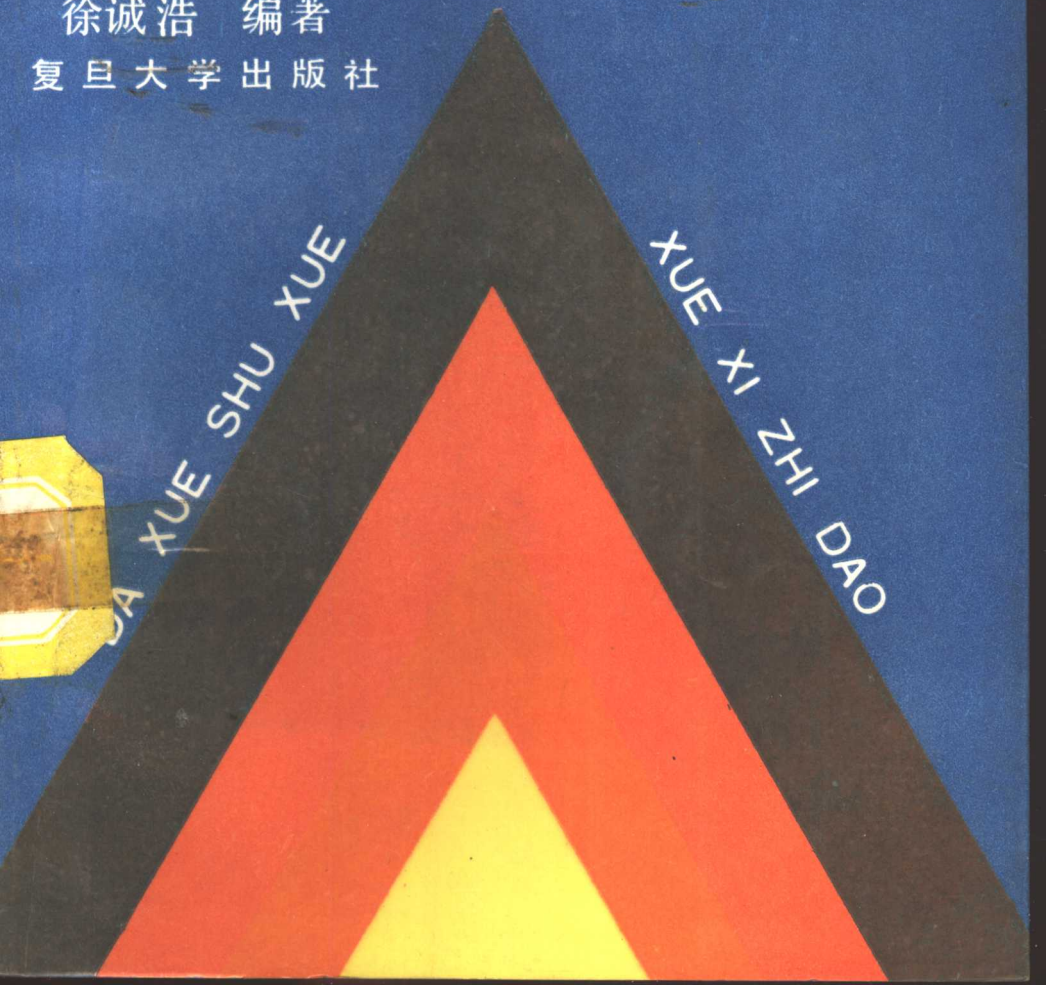
大学数学学习指导

抽象代数

—方法导引

徐诚浩 编著

复旦大学出版社



大学数学学习指导

抽 象 代 数

—方法导引

徐诚浩 编著

复旦大学出版社

内 容 简 介

本书着重介绍抽象代数基础理论（群、环、体、格与扩域）中的各种解题方法与技巧，并配有近200个例题和300多道习题（基本上有提示或答案），所列出的约90个比较重要的定理是读者必须掌握和运用的。本书可供理工科的教师讲授和学生学习抽象代数课程时参考，也可作为报考研究生者的复习资料。

抽 象 代 数

——方法导引

徐诚浩 编著

复旦大学出版社出版

（上海国权路579号）

新华书店上海发行所发行 复旦大学印刷厂印刷

开本 850×1168 1/32 印张 6 字数 173,000

1989年12月第1版 1989年12月第1次印刷

印数 1—3,000

ISBN 7-309-00402-7/O·67

定价：1.70元

前　言

这是一本介绍抽象代数基础知识和解题技巧的学习方法辅导书。在编者多次讲授这门课程的基础上，并根据历经三次修改的自编讲义，本书系统地整理了一些基本概念、重要定理与解题方法，特别还收集并改正了学生在初学阶段易犯的各类错误。

学习抽象代数的困难，主要在于对抽象概念的理解，其次才是解题技巧！解题的技巧主要来源于对概念的透彻理解。忽视概念而企求漂亮的解题技巧，是一种最忌讳的学习方法。因为它最多只能学会机械地生搬硬套，而不会举一反三。这实际上等于没有掌握解题的方法。所以读者的学习重点应放在对概念的正确理解上，善于对各概念举出正例和反例。当然，也经常出现这样一种情形：同一道题有多种解法，其繁复与简洁相差悬殊！这不仅仅取决于对概念是否理解，而且还反映了读者对有关基本定理是否掌握，对各种基本技巧是否能运用自如。因此，本书在讲清各种概念的前提下，介绍了一些常用解题方法和技巧。在书中列出的定理是相当基本的，所给出的证明（包括定理和例题）是相当简洁的，并同时尽可能举一些反例作辅助说明。每看完一个证明，应找出关键步骤和所用技巧，然后归纳整理成便于记忆的几条，这无疑是收效甚大的学习方法。

在现有的各种抽象代数书籍中，所用术语极不统一！为此在本书中不得不花一些篇幅来叙述概念。并在每个概念之后配备若干例子和习题，作为对一些概念的补充说明或应用，并指出各相关概念之间的区别与联系。这一部分习题是比较容易的，也是基本的。本书在每章末所配的习题大都是一些较难的和综合性的习题，用以让读者作对概念理解程度的自我鉴定。打＊号的内容可略去不看。

本书主要供教师或学生在讲授或学习抽象代数时作参考，也可作为报考研究生者的复习资料。

限于本人水平，书中难免有处理不当，甚至错误之处，恳请同行和读者批评指正，本书中部分习题的解题方法是由姚慕生、黄昌令、徐崇业、严民和陈毓卿等同志提供的，我在此向他们表示衷心的感谢。

目　录

第一章 集合与映射

集合与映射是现代数学中两个重要的基本概念。

§1 集 合

集合的专用记号 在本书中，N 表示**自然数集**，Z 表示**整数集**，E 表示**偶数集**，Q 表示**有理数集**，R 表示**实数集**，C 表示**复数集**。设 F 是某个数域，$M_n(F)$ 表示 F 上 n **阶方阵全体**，$M_{m\times n}(F)$ 表示 F 上 $m\times n$ **矩阵全体**，$F[x]$ 表示 F 上**一元多项式全体**，$GL_n(F)$ 表示 F 上 n **阶可逆阵全体**，$SL_n(F)$ 表示 F 上**行列式为 1 的 n 阶阵全体**。对 C 的任一子集 P，常用 P^* 表示在 P 中去掉 0 以后所得的集合。例如 R^* 表示非零实数全体。

集合 S 中元素个数用 $|S|$ 表示。由集合 S 的所有子集（包括空集 ϕ 和 S 本身）构成的集合称为 S 的**幂集**，记为 $P(S)$。若 $|S|=n$，则 $|P(S)|=2^n$，$|P(P(S))|=2^{2^n}$。

集合的运算 设 A 和 B 是集合 S 的子集，则可定义如下四个运算：

并集 $A\cup B=\{x\mid x\in A$ 或 $x\in B\}$，

交集 $A\cap B=\{x\mid x\in A$ 且 $x\in B\}$，

差集 $A\setminus B=\{x\mid x\in A$ 但 $x\notin B\}$，

余集 $\bar{A}=S\setminus A$。

A 是 B 的子集用 $A\subseteq B$ 表示，$A\subset B$ 表示 A 是 B 的真子集。在证明两个集合 A 与 B 相等时，最常用的方法是分别证明 $A\subseteq B$ 和 $B\subseteq A$。当然，也可用其它简易的证法。

例 1 设 A,B 是 S 的子集，证明

$$\overline{A\cup B}=\bar{A}\cap\bar{B},\quad \overline{A\cap B}=\bar{A}\cup\bar{B}。$$

首先，第一式可证明如下：

$$x\in\overline{A\cup B}\Longleftrightarrow x\notin A\cup B\Longleftrightarrow x\notin A\text{ 且 }x\notin B$$
$$\Longleftrightarrow x\in\bar{A}\text{ 且 }x\in\bar{B}\Longleftrightarrow x\in\bar{A}\cap\bar{B}。$$

这实际上是证明了$\overline{A\cup B}\subseteq\bar{A}\cap\bar{B}$和$\bar{A}\cap\bar{B}\subseteq\overline{A\cup B}$。

其次，对第一式两边求余得$A\cup B=\overline{(\bar{A}\cap\bar{B})}$。因为这对$S$的任意子集都成立，利用$\bar{\bar{A}}=A$，$\bar{\bar{B}}=B$即得第二式。　　证毕

题1　设A,B,C是S的子集，证明

$$\overline{(A\cup B)\cap C}=(\bar{A}\cap\bar{B})\cup\bar{C}。$$

题2　先分别证明

$$(A\cup B)\cap C=(A\cap C)\cup(B\cap C),\ (A\cap B)\cup C=(A\cup C)\cap(B\cup C)。$$

然后，再分别从其中一式推出另一式。

§2　映射与变换

单值映射　所谓集合A到集合D的一个**单值映射**指的是满足如下条件的某个对应法则φ：对任一$a\in A$都能唯一确定$d\in D$与之对应。注意，对于单值映射来说，以下三个条件缺一不可。每个$a\in A$都有像d，d必须在D中，d必须是唯一的。本书中所涉及的映射都是单值映射。对于一个定义在集合A上的映射，当A中的元素的表示方法不唯一时，必须验证这个映射的单值性。

例1　设$\langle a\rangle$和$\langle b\rangle$分别为m和n阶循环群，证明自然数k使得映射

$$\eta:a^i\to b^{ik},\ i=1,2,\cdots,m$$

是$\langle a\rangle$到$\langle b\rangle$内的同态映射$\Longleftrightarrow n\mid mk$。

证　如果η是同态映射，则由$a^m=e$知必有$b^{mk}=e$，所以由b的阶为n知$n\mid mk$。反之，设$n\mid mk$。显然η保持运算。由于$\langle a\rangle$是m阶循环群，有

$$a^t=a^{t+ms},\ \forall s\in Z。$$

这说明$\langle a\rangle$中元素的表示法不唯一，因此必须验证η的单值性。若

$a^i = a^j$，则 $m|(i-j)$。由条件 $n|mk$ 知 $n|(ik-jk)$，故由 b 的阶为 n 知 $b^{ik} = b^{jk}$，这说明 η 是单值的。 证毕

题 1 设$\langle a\rangle$和$\langle b\rangle$分别为 m 和 n 阶循环群，证明此两群是同态的$\langle a\rangle \sim \langle b\rangle$当且仅当 $n|m$。（提示：同态满射必把生成元变为生成元。）

映射的种类 我们把A到D的一般映射记为$A \xrightarrow{\varphi} D$。如果像集

$$\varphi(A) = \{d \mid d \in D, \text{存在 } a \in A \text{ 使 } \varphi(a) = d\} = D,$$

则称 φ 为**满射**。如果 $\varphi(a) = \varphi(b)$当且仅当 $a = b$，则称 φ 为**单射**。如果 φ 既是满射，又是单射，则称 φ 为**双射**或**一一对应**，记为 $A \xleftrightarrow{\varphi} D$。要注意单射与单值映射是两个不同的概念，单射是不同元素有不同的像的单值映射。集合 A 到 A 的映射称为**变换**。相应地可定义**满变换**、**单变换**和**一一变换(可逆变换)**。A 中的恒等变换用 1_A 表示。

映射的乘积 关于两个映射的乘积，有两种常用的表示方法。要弄清楚它们之间的区别和联系，初学者往往感到比较困难。考虑以下两个映射

$$S \xrightarrow{\alpha} T, \quad T \xrightarrow{\beta} U。$$

所谓 α 与 β 的**乘积**(或**合成**)指的是映射 $S \xrightarrow{\gamma} U$。对任一 $s \in S$，先求 s 在 α 之下的像 $t \in T$，再求 t 在 β 之下的像 $u \in U$。但如何书写 γ 与 α，β 之间的关系式呢？是 $\gamma = \alpha\beta$ 还是 $\gamma = \beta\alpha$？事实上，这两种写法都是经常被采用的。

如果把 x 在映射 φ 之下的像记为 $\varphi(x)$，则 $\gamma = \beta\alpha$，即

$$\gamma(s) = (\beta\alpha)(s) = \beta(\alpha(s)), \forall s \in S。$$

有时把 x 在 φ 之下的像记为 x^φ，甚至记为 $(x)\varphi$，则 $\gamma = \alpha\beta$，即

$$s^\gamma = s^{\alpha\beta} = (s^\alpha)^\beta \text{ 或 } (s)\gamma = (s)(\alpha\beta) = ((s)\alpha)\beta, \forall s \in S。$$

前者是先写的 β 后作用，后写的 α 先作用，是逆序的；后者是先写的 α 先作用，后写的 β 后作用，是顺序的。在第二章 §7 中我们将对此作进一步的讨论。

不论用何种方式表示乘积，结合律总是满足的。在一般情况下，我们总是采用第一种表示方法，即 α 与 β 的乘积是 $\beta\alpha$。对于置换的乘积，则采用第二种表示方法。

各类映射的判别法

定理 1 $S\xrightarrow{\alpha}T$ 是双射$\Longleftrightarrow$存在 $T\xrightarrow{\beta}S$ 使得

$$\beta\alpha=1_S \text{ 且 } \alpha\beta=1_T。$$

易证，对双射 α 来说，满足上述条件的 β 是唯一的，称为 α 的逆映射，记为 α^{-1}。故双射又称为可逆映射。两个可逆映射之积仍为可逆映射，且满足**穿脱原理**：

$$(\alpha\beta)^{-1}=\beta^{-1}\alpha^{-1}。$$

这好比穿时先穿袜子后穿鞋子，脱时必须先脱鞋子后脱袜子。

例 2 取 N 中如下两个变换：

$$\alpha:\ \begin{array}{ccccccccc} 1 & 2 & 3 & \cdots & n & \cdots \\ \downarrow & \downarrow & \downarrow & & \downarrow & \\ 1 & 1 & 2 & \cdots & n-1 & \cdots \end{array},\quad \beta:\ \begin{array}{ccccccccc} 1 & 2 & 3 & \cdots & n & \cdots \\ \downarrow & \downarrow & \downarrow & & \downarrow & \\ 2 & 3 & 4 & \cdots & n+1 & \cdots \end{array}$$

易见 $\alpha\beta=1_N$ 而 $\beta\alpha\neq 1_N$。原因是 α 与 β 都不是双射。

题 2 (1) 设 $|S|\geqslant 2$。证明 $S\xrightarrow{\alpha}T$ 是单射$\Longleftrightarrow$存在 $T\xrightarrow{\beta}S$ 使 $\beta\alpha=1_S$。且当这种 β 唯一时，α 必是双射。

(2) 证明 $S\xrightarrow{\alpha}T$ 是满射$\Longleftrightarrow$存在 $T\xrightarrow{\beta}S$ 使 $\alpha\beta=1_T$。且当这种 β 唯一时，α 必是双射。(**提示**：构造 β。)

例 3* (1) 证明 $S\xrightarrow{\alpha}T$ 是单射$\Longleftrightarrow$不存在某集合 U 到 S 内的两个不同的映射 β_1,β_2 使 $\alpha\beta_1=\alpha\beta_2$。

(2) 证明 $S\xrightarrow{\alpha}T$ 是满射$\Longleftrightarrow$不存在 T 到某集合 U 内的两个不同的映射 β_1,β_2 使 $\beta_1\alpha=\beta_2\alpha$。

证 (1) 设 α 是单射。如果存在 $U\xrightarrow{\beta_i}S$，$i=1,2$，使 $\alpha\beta_1=\alpha\beta_2$。任取 $u\in U$，记 $s_1=\beta_1(u)$，$s_2=\beta_2(u)$。则 $\alpha(s_1)=\alpha(s_2)$。再据 α 是单射知 $s_1=s_2$，即 $\beta_1=\beta_2$。

设 α 不是单射，则存在互异的 $s_1,s_2\in S$ 使

$$\alpha(s_1)=\alpha(s_2)=t_0\in T。$$

取 $U=\alpha(S)\subseteq T$。则可构造 U 到 S 的如下两个互异映射

$$\beta_i(u)=\begin{cases}s_i, & \text{若 } u=t_0;\\ s, & \text{若 } u\neq t_0。\end{cases}\quad (i=1,2)$$

这里s是u在α之下的任意取定的一个原像，规定$\beta_1(u)=\beta_2(u)=s$，$\forall u\neq t_0$。则显然$\alpha\beta_1=\alpha\beta_2$。

(2) 设α是满射。如果存在$T\xrightarrow{\beta_i}U$，$i=1,2$，使$\beta_1\alpha=\beta_2\alpha$，则由$\alpha(S)=T$知对任一$t\in T$，必存在$s\in S$使$\alpha(s)=t$，于是由$\beta_1(t)=\beta_2(t)$，$\forall t\in T$知$\beta_1=\beta_2$。

设α不是满射，即$\alpha(S)\subset T$。当$|S|\geqslant 2$时，取$U=S$，则可构造T到S的如下两个互异映射

$$\beta_i(t)=\begin{cases}s, & \text{若 } t=\alpha(s);\\ s_i, & \text{若 } t\notin\alpha(S)。\end{cases}\quad (i=1,2)$$

这里s_1和s_2是S中任意取定的两个互异元，s是t在α之下的任意取定的一个原像，规定$\beta_1(t)=\beta_2(t)=s$，易见有$\beta_1\alpha=\beta_2\alpha$。当$|S|=1$时，由$\alpha$不是满射知$|T|\geqslant 2$。记$\alpha(s)=t_0\in T$，则必存在$t_1\in T$，$t_1\neq t_0$。于是对任意集合$U$，$|U|\geqslant 2$，总可构造两个$T\xrightarrow{\beta_i}U$，$i=1,2$，满足

$$\beta_i(t_0)=u_0,\ i=1,2;\ \beta_1(t)\neq\beta_2(t)。$$

这里u_0为U中取定的一个元素。于是$\beta_1\neq\beta_2$，而

$$\beta_1\alpha(s)=\beta_1(t_0)=\beta_2(t_0)=\beta_2\alpha(s),$$

即$\beta_1\alpha=\beta_2\alpha$。 **证毕**

§3 代数运算与等价关系

代数运算 设A,B和D是任意三个集合，则积集

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

到D的任何一个映射φ都称为$A\times B$到D的一个**代数运算**。特别，$A\times A$到A的代数运算称为A中的**二元运算**。A中的变换称为A中的**一元运算**。

例如，对数域F，代数运算

$$\varphi(k,M)=kM,\forall k\in F,M\in M_n(F)$$

就是通常的数与矩阵的乘法，二元运算

$$\varphi(f(x),g(x))=f(x)g(x),\quad \forall f(x),g(x)\in F[x]$$

就是通常的多项式乘法。$A\cup B$ 和 $A\cap B$ 都是集合 S 的幂集 $P(S)$ 中的二元运算，求余 $\bar{A}$ 是 $P(S)$ 中的一元运算。

如果用小圆圈“$\circ$”代表某个代数运算，则可把运算结果写成习惯的形式 $a\circ b$，或者干脆写成 ab。当然，这未必就是通常的乘法运算。定义了二元运算 $\circ$ 的非空集合 G 就记为 $(G,\circ)$。

要注意，二元运算未必都满足结合律、交换律和左、右分配律。例如，空间矢量的矢积一般有

$$(\vec{a}\times\vec{b})\times\vec{c}\neq\vec{a}\times(\vec{b}\times\vec{c}),$$

矩阵乘积一般不能交换等等。

设 S 是某个带有二元运算 $\circ$ 的集合，$\mathscr{A}$ 是由 S 中变换(自)体所成的集合。若对 $f,g\in\mathscr{A}$ 规定以下两个运算：

$$(f+g)(x)=f(x)\circ g(x),\quad \forall x\in S,$$

$$(f*g)(x)=f(g(x)),\quad \forall x\in S,$$

则易验证右分配律成立：

$$(f+g)*h=f*h+g*h,\quad \forall f,g,h\in\mathscr{A},$$

但左分配律不成立。当 h 是 S 中的自同态时，有

$$h*(f+g)=h*f+h*g。$$

等价关系与集合的划分 设 A 是任一集合，$D=\{0,1\}$ 为二元集合。任意给定 $A\times A$ 到 D 的某个代数运算 φ。对 $a,b\in A$，规定

$$a\sim b \text{ 当且仅当 } \varphi(a,b)=0,$$

则称 φ 在 A 中定义了一个关系 $\sim$。如果如此确定的关系还满足

(1) 反身性：对任意 $a\in A$ 都有 $a\sim a$；

(2) 对称性：当 $a\sim b$ 时必有 $b\sim a$；

(3) 传递性：当 $a\sim b, b\sim c$ 时，必有 $a\sim c$，

则称 $\sim$ 是 A 中的一个等价关系。

例如，$M_n(F)$ 中的相似关系 $B=PAP^{-1}$，相抵关系 $B=PAQ$ 和合同关系 $B=PAP'$ 都是等价关系，这里 P 和 Q 都是可逆方阵。

要注意的是，等价关系所满足的三个条件是互相独立的，任何一个

都不可能由其他两个推出来。

题 1 指出以下证明的错误所在。因为由 $a\sim b$ 必可推出 $b\sim a$，所以再由传递性推出 $a\sim a$。故反身性可由对称性和传递性推出。(提示：注意对称性的叙述。)

设～是集合 A 中某个等价关系，则 A 必是若干个两两不相交的等价类

$$\bar{a}=\{x\mid x\in A,\ x\sim a\}$$

之并，即～确定了 A 的一个**划分**。反之，易见，A 的任一划分

$$A=\cup A_i,\ A_i\cap A_j=\phi,\ i\neq j,$$

必可确定 A 中某个等价关系：$a\sim b$ 当且仅当 a 与 b 属于同一个 A_i。

广义同态定理 利用等价关系可建立一个最广泛意义下的同态定理。设 α 是集合 S 到集合 T 的一个满射，对 $a,b\in S$ 规定

$$a\sim b\Longleftrightarrow\alpha(a)=\alpha(b)。$$

易见，～是 S 中一个等价关系。任取 $a\in S$，记 $t=\alpha(a)$，则 a 所属的等价类

$$\bar{a}=\{x\mid x\in S,\ \alpha(x)=t\}=\alpha^{-1}(t)$$

是 t 在 α 之下的**完全原像**。称互异等价类集合

$$S/\sim=\{\bar{a}\mid a\in S\}$$

为 S 关于～的**商集**。定义以下两个映射

$$S\xrightarrow{\nu}S/\sim,\ \nu:\ a\to\bar{a},$$

$$S/\sim\xrightarrow{\alpha^*}T,\ \alpha^*:\ \bar{a}\to\alpha(a),$$

容易验证 ν 是满射，α^* 是双射且 $\alpha=\alpha^*\nu$。

后面我们将要给出的群的同态定理（第二章§5）、环的同态定理（第三章§4）和格的同态定理（第四章§2）都是广义同态定理的特例。

习 题 一

1. 设 A 和 B 是集合 S 的子集，如果规定

$$A+B=(A\setminus B)\cup(B\setminus A),$$

证明 $A+B=B+A$，$A+\phi=A$，$A+A=\phi$。

2. 设 φ 是 A 到 B 的双射，$a\in A$，试问

$$\varphi^{-1}(\varphi(a))=?\qquad \varphi(\varphi^{-1}(a))=?$$

若 φ 是 A 中一一变换，则结论如何？

3. 设 $A\xrightarrow{f}B$，$S\subseteq A$，证明 $f^{-1}(f(S))\supseteq S$，并举例说明等式未必成立。

4. 设 V 是欧氏平面，S 是 V 中有向直线段 $\overrightarrow{PQ}$ 全体所成的集合。试确定 S 中某个等价关系～使对应的等价类恰好对应通常的平面向量所成的集合。

（提示：$\overrightarrow{PQ}\sim\overrightarrow{RS}\iff\overrightarrow{PQ}\parallel\overrightarrow{RS}$，$|\overrightarrow{PQ}|=|\overrightarrow{RS}|$且方向相同。）

5. (1) 设 C 是复数全体，R^+ 是非负实数全体，$f:z\to|z|$ 是 C 到 R^+ 的映射，试确定由 f 所确定的 C 中的等价关系，并说明相应等价类的几何意义。

(2) 设 C^* 是非零复数全体，$g:z\to z/|z|$ 是 C^* 中的一个变换，试确定由 g 所确定的 C^* 中的等价关系，并说明相应等价类的几何意义。（提示：(1) $z_1\sim z_2\iff|z_1|=|z_2|$。等价类是以原点为圆心的圆，(2) $z_1\sim z_2\iff z_1$ 和 z_2 的幅角相等，等价类是不包括原点的半射线。）

第二章 群 论

群论是抽象代数的基础，也是抽象代数中应用最广泛的分支之一，因此，要特别重视。

§1 群的各种等价定义

群的定义 对于一个代数系统$(G,\circ)$，可以提出以下诸条件：

（Ⅰ）封闭性。对任何$a,b\in G$都有$ab\in G$。

（Ⅱ）结合律。对任何$a,b,c\in G$都有$(ab)c=a(bc)$。

（Ⅲ）左方程$xa=b$和右方程$ax=b$在G中都有解。即对任何$a,b\in G$，必存在$c,d\in G$使$ca=b$和$ad=b$。此条件等价于对任何$a\in G$必有

$$G\subseteq Ga=\{ga\mid g\in G\},\quad G\subseteq aG=\{ag\mid g\in G\}。$$

特别，当封闭性条件满足时，它等价于

$$Ga=aG=G,\quad \forall a\in G。$$

（Ⅳ）至少存在一个左单位元素$e_l\in G$，使对任何$g\in G$都有$e_lg=g$。

（Ⅳ）′至少存在一个右单位元素$e_r\in G$，使对任何$g\in G$都有$ge_r=g$。

（Ⅴ）任意取定一个左单位元e_l，对任一$a\in G$，至少存在一个a的关于这个e_l的左逆元$a_l^{-1}\in G$，使$a_l^{-1}a=e_l$。

（Ⅴ）′任意取定一个右单位元e_r，对任一$a\in G$，至少存在一个a的关于这个e_r的右逆元$a_r^{-1}\in G$，使$aa_r^{-1}=e_r$。

（Ⅵ）左、右消去律。对任何$a,b,c\in G$，由$ab=ac$必可推出$b=c$；由$ba=ca$必可推出$b=c$。

当然，这些条件不是彼此独立的，用它们可组成若干个等价条件

组。

定义1 称$(G,\circ)$为群，如果它满足(Ⅰ)、(Ⅱ)和(Ⅲ)。

定义2 称$(G,\circ)$为群，如果它满足(Ⅰ)、(Ⅱ)、(Ⅳ)和(Ⅴ)。

定义2′ 称$(G,\circ)$为群，如果它满足(Ⅰ)、(Ⅱ)、(Ⅳ)′和(Ⅴ)′。

这三个定义是等价的。满足定义2(定义2′)的任何一个左(右)单位元必是右(左)单位元，而且是唯一的，我们称之为单位元e。$a\in G$的任一左逆元和右逆元都是同一个元素，记为a^{-1}。由此可得群的常用定义：

定义3 称非空集合G关于其中某运算成群，如果满足

(1) **封闭性**。对任何$a,b\in G$，都有$ab\in G$。

(2) **结合律**。对任何$a,b,c\in G$，都有$(ab)c=a(bc)$。

(3) **单位元**。存在唯一的$e\in G$，使对任何$a\in G$，有

$$ae=ea=a。$$

(4) **逆元**。对任一$a\in G$，必存在唯一的$a^{-1}\in G$，使

$$a^{-1}a=aa^{-1}=e。$$

表面上看起来，定义3的条件要比定义2和定义2′中的条件强得多，然而它们却是等价的。若要验证某个$(G,\circ)$是群，当然仅需验证定义2或定义2′中诸条件就足够了；若已知某个$(G,\circ)$是群，则用定义3可得出较强的结论。由此可见，定义2和定义3各有所用。

为叙述简洁起见，G成群就是指非空集合G关于某个确定的运算成群。

满足条件(1)的G称为**群胚**。满足条件(1)和(2)的G称为**半群**。满足条件(1)、(2)和(3)的G称为**么半群**。满足交换律$ab=ba$的群称为**交换群**。

例1 设G在定义2意义下成群，证明G中任一左单位元e_l必是右单位元，且左、右单位元相等，它们就是G的唯一的单位元。

证 任取$a\in G$，由条件(Ⅴ)知，存在$a_l^{-1}\in G$，使得$a_l^{-1}a=e_l$。仍由条件(Ⅴ)知存在$a'\in G$使$a'a_l^{-1}=e_l$。在$a_l^{-1}a=e_l$两侧左乘a'和右乘a_l^{-1}得

$$(a'a_l^{-1})aa_l^{-1}=a'(e_la_l^{-1})=a'a_l^{-1}=e_l,$$