HEADSPRING 源泉

高等学校经典教材配套辅导丛书

近世代数
辅导及习题精解

许　宁 编著

★ 知识精要归纳　★ 重点难点剖析
★ 典型例题精解　★ 自测习题强化

新版

陕西师范大学出版社
SHAANXI NORMAL UNIVERSITY PRESS

高等学校经典教材配套辅导丛书

近世代数
辅导及习题精解

许　宁　编著

本书同时适用于：
高教版·刘绍学·《近世代数基础》
高教二版·杨子胥·《近世代数》
人教修订版·张禾瑞·《近世代数基础》

陕西师范大学出版社
SHAANXI NORMAL UNIVERSITY PRESS

图书代号:JF6N0828

图书在版编目(CIP)数据

近世代数辅导及习题精解/许宁主编. —西安:陕西师范大学出版社,2006.8
(高等学校经典教材配套辅导丛书)
ISBN 7-5613-3537-7/O·99
Ⅰ.近… Ⅱ.许… Ⅲ.抽象代数-高等学校-教学参考资料 Ⅳ.0153
中国版本图书馆 CIP 数据核字(2006)第 073092 号

责任编辑 陈光明 彭 青
装帧设计 王静婧
出版发行 陕西师范大学出版社
社　　址 西安市陕西师大 120#(邮政编码:710062)
网　　址 http://www.snuph.com
经　　销 新华书店
印　　刷 南京金阳彩色印刷有限公司
开　　本 787×960 1/16
印　　张 11.25
字　　数 198 千
版　　次 2006 年 9 月第 1 版
印　　次 2006 年 9 月第 1 次印刷
定　　价 15.80 元

开户行:光大银行西安电子城支行 账号:0303080-00304001602
读者购书、书店添货或发现印装问题,请与本社营销中心联系、调换。
电 话:(029)85307864 85233753 85251046(传真)
E-mail:if-centre@snuph.com

前言

近世代数又称为抽象代数，它的研究对象是代数系，所谓代数系，就是由一个集合和定义在这个集合中的一种运算或若干种运算所构成的一个系统。近世代数在近代物理、近代化学、计算机科学、数字通信、系统工程等许多领域都有广泛而重要的应用价值。它已经成为现代科学技术的数学基础之一。目前，高等院校相关学科都开设了近世代数这门课程。

为了帮助在校的大学生学好近世代数，扩大学科知识面，提高思维能力和应试能力，我们根据这门课程的教学要求，依照应用和抽象相结合、学习指导和应试训练相结合的原则编写了此书。

本书按预备知识、群、环、域的顺序，分为四章，每章均设计了三个版块，即：

知识点精要：介绍基本概念、重要定理和主要内容，突出必须掌握的核心知识。

典型例题精解：精选了具有代表性的例题进行详尽的解析。这些例题涉及内容广、类型多、技巧性强，旨在提高学习者的分析能力，帮助他们掌握基本概念和理论，开拓解题思路，熟练掌握解题技巧。

自测题及解答：自测题可以帮助学习者进一步强化解题训练，深入理解课程内容的重点、难点，提升综合能力和应变能力，巩固和提高复习效果。

众所周知，学习数学，做练习题是一个非常重要的手段。通过做练习题，可以深入掌握基本概念、基础理论和常用方法。希望读者遇到问题一定要认真思考，努力作出自己的解答，不要轻易查抄本书的解答。

在本书的编写过程中，我们参考了国内外的一些近世代数教科书并在许多方面得到了启发，谨对原书的作者表示感谢。陕西师范大学出版社陈光明、彭青同志对本书的出版给予了有力的支持，编者在此表示衷心的感谢。由于编者水平有限，错误和缺点在所难免，恳请读者批评指正。

编　者

2006年7月于南京大学蒙民伟楼

目 录

第1章　预备知识

一、知识点精要

1　集合

1.1　集合的记号

·集合：具有某种属性的事物的全体，或一些确定对象的汇总称为集合，构成集合的事物或对象，称为元素.

·集合的表示：一种是直接列出所有的元素，另一种是规定元素所具有的性质.

·有限集，无限集：一个集合 A 的元素个数用 $|A|$ 表示. 当 A 中有有限个元素时，称为有限集，否则称为无限集.

1.2　子集与幂集

·属于与不属于："元素 a 属于 A" 记作 $a \in A$，"a 不属于 A" 记作 $a \notin A$.

·子集：设有两个集合 A 和 B，若对 A 中的任意一个元素 a（记作 $\forall a \in A$）皆有 $a \in B$，则称 A 是 B 的子集，记作 $A \subseteq B$，若 $A \subseteq B$ 且 $B \subseteq A$，即 A 和 B 有完全相同的元素，则称 A 与 B 相等，记作 $A = B$，若 $A \subseteq B$，且 $A \neq B$，则称 A 是 B 的真子集，记作 $A \subset B$.

·空集：不含任何元素的集合称为空集，记作 $\varnothing$，空集是任何一个集合的子集.

·幂集：设 A 是一个集合，由 A 的所有子集构成的集合称为 A 的幂集，记作 2^A，当 $|A| < \infty$ 时，2^A 的元素的个数正好是 $|2^A| = 2^{|A|}$.

1.3　集的运算

·运算：设 I 是一个集合，A, B, C 皆为 I 的子集，两个子集的并、交、差和一个子集的余定义如下：

并：$A \cup B = \{x \in I \mid x \in A \text{ 或 } x \in B\}$.

交：$A \cap B = \{x \in I \mid x \in A \text{ 且 } x \in B\}$.

差：$A - B = \{x \in I \mid x \in A \text{ 且 } x \notin B\}$.

余：$A' = I - A$.

对称差：$A\triangle B=(A-B)\cup(B-A)$.

· 运算律：

(1) $A\cup B=A$，$A\cap A=A$.　（幂等律）

(2) $A\cup B=B\cup A$，$A\cap B=B\cap A$.　（交换律）

(3) $A\cup(B\cup C)=(A\cup B)\cup C$，

$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$.　（结合律）

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

$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$.　（分配律）

(5) $A\cap(A\cup B)=A\cup(A\cap B)=A$.　（吸收律）

(6) 若 $A\subseteq C$，则 $A\cup(B\cap C)=(A\cup B)\cap C$.　（模律）

(7) $(A\cup B)'=A'\cap B'$，$(A\cap B)'=A'\cup B'$.　（De Morgan 律）

(8) $(A')'=A$.

1.4　包含与排斥原理

· 设 I 是一个集合，A,B,C 是 I 的有限子集，则有

$$|A\cup B|=|A|+|B|-|A\cap B|,$$

$$|A\cap B|=|A|+|B|-|A\cup B|,$$

$$|A\cap B\cap C|=|A|+|B|+|C|-|A\cup B|-|A\cup C|$$
$$-|B\cup C|+|A\cup B\cup C|.$$

· 设 $A_1,A_2,\cdots,A_n$ 是 I 的有限子集，则

$$\left|\bigcap_{i=1}^{n}A_i\right|=\sum_{i=1}^{n}|A_i|-\sum_{1\leqslant i<j\leqslant n}|A_i\cup A_j|+\cdots+(-1)^{n-1}\left|\bigcup_{i=1}^{n}A_i\right|,$$

$$\left|\bigcup_{i=1}^{n}A_i\right|=\sum_{i=1}^{n}|A_i|-\sum_{1\leqslant i<j\leqslant n}|A_i\cap A_j|+\cdots+(-1)^{n-1}\left|\bigcap_{i=1}^{n}A_i\right|.$$

2　映射

2.1　映射的概念

· 映射：设 A、B 为两个非空集合，若存一个 A 到 B 的对应规则 f，使得对 A 中的每一个元素 x，都有 B 中唯一确定的一个元素 y 与之对应，则称 f 是 A 到 B 的一个映射，记作 $y=f(x)$.

y 称为 x 的象，x 称为 y 的原象，常用 $f:A\to B$ 或 $A\xrightarrow{f}B$ 表示 f 是 A 到 B 的一个映射，用记号 $f:x\to f(x)$ 表示映射 f 所规定元素之间的具体对应关系.

2.2　映射的分类

· 单射，满射，双射：设 f 是 A 到 B 的一个映射.

(1) 若 $\forall x_1, x_2 \in A$，且 $x_1 \neq x_2$ 皆有 $f(x_1) \neq f(x_2)$，则称 f 是一个单射.

(2) 若 $\forall y \in B$ 皆有 $x \in A$ 使 $f(x) = y$，则称 f 是满射.

(3) 若 f 既是单射又是满射，则称 f 是双射.

· 象：设 f 是 A 到 B 的一个映射，$S \subseteq A$，记 $f(S) = \{f(x) \mid x \in S\}$，它是 B 的一个子集，称为子集 S 在 f 作用下的象，$f(A)$ 称为 f 的象，记作 $I_m f$.

· 结论：$f: A \to B$ 是满射 $\Leftrightarrow I_m f = f(A) = B$.

· 原象：设 f 是 A 到 B 的一个映射，$T \subseteq B$，记 $f^{-1}(T) = \{x \in A \mid f(x) \in T\}$，它是 A 的一个子集，称为子集 T 在 f 下的完全原象，元素 $b \in B$ 的全原象记作 $f^{-1}(b)$，它可能是空集.

· 结论：$f: A \to B$ 是单射 $\Leftrightarrow \forall b \in f(A)$ 有 $|f^{-1}(b)| = 1$.

2.3　映射的复合

· 复合：设 A, B, C 为三个集合，有两两个映射：$f_1: A \to B$，$f_2: B \to C$，则由 f_1, f_2 可确定一个 A 到 C 的映射 g：

$$g(x) = f_2(f_1(x)), \qquad \forall x \in A,$$

称 g 是 f_1 与 f_2 的复合，记作 $g = f_2 f_1$.

· 变换：当 f 是 A 到 A 自身的映射，则称 f 是 A 上的一个变换. 当 A 是有限集时，A 上的变换通常用“列表法”表示. 一般地，$A = \{1, 2, \cdots, n\}$ 上的一个变换 f 可表示为

$$f = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ f(1) & f(2) & f(3) & \cdots & f(n) \end{pmatrix}.$$

· 恒等变换：设 I_A 是 A 上的一个变换，若 $\forall x \in A$ 有 $I_A(x) = x$，称 I_A 是 A 上的一个单位变换或恒等变换.

· 映射的复合的性质：设有映射 $f: A \to B$，$g: B \to C$，$h: C \to D$，则有：

(1) $h(gf) = (hg)f$，　　(结合律)

(2) $I_B f = f I_A = f$.

2.4　映射的逆

· 左逆，右逆，可逆：设 $f: A \to B$，

(1) 若存在映射 $g: B \to A$ 使 $gf = I_A$，则称 g 是 f 的左逆.

(2) 若存在映射 $h: B \to A$ 使 $fh = I_B$，则称 h 是 f 的右逆.

(3) 若 f 同时有左逆和右逆，则左、右逆相等，称为 f 的逆，记作 f^{-1}，于是说 f 可逆.

· 注：若 f 只有左逆或只有右逆，则 f 未必可逆.

· 映射有左逆，右逆，可逆的判别：设 $f: A \to B$，则

(1) f 有左逆的充分必要条件为 f 是单射.

(2) f 有右逆的充分必要条件为 f 是满射.

(3) f 可逆的充分必要条件为 f 是双射.

· 逆映射性质：

(1) $(f^{-1})^{-1}=f$.

(2) 若 g 是 $A\to B$ 的可逆映射，f 是 $B\to C$ 的可逆映射，则 fg 是 $A\to C$ 可逆映射，且有 $(fg)^{-1}=g^{-1}f^{-1}$.

· 注：记号 $f^{-1}(b)$ 的意义：前面我们用 $f^{-1}(b)$ 表示 b 在 f 下的完全原象，不管 f 是否可逆. 当 f 是可逆时，$f^{-1}(b)$ 既表示 b 在 f 下在完全原象，也表示 b 在 f^{-1} 作用下的象，二者是一致的.

· 注：当 A 是有限集时，A 上的一个变换 f 可逆的充分必要条件是 f 是单射.

3 二元关系

3.1 集合的笛卡尔积

· 笛卡尔积：设 A,B 是两个非空集合，作一个新的集合

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

称该集合是 A 与 B 的笛卡尔积，记作 $A\times B$.

· 注：当 $|A|<\infty$，$|B|<\infty$，有 $|A\times B|=|A|\cdot|B|$.

· 注：一个 A 到 B 的映射 f 可以用 $A\times B$ 的一个子集 $\{(a,f(a))\mid a\in A\}$ 来表示.

3.2 二元运算

· 二元运算：设 S 是一个非空集合，若有一个对应规则 f，对 S 中每一对元素 a 和 b 都规定了一个唯一的元素 $c\in S$ 与之对应，即 f 是 $S\times S\to S$ 的一个映射，则称 f 为 S 中的一个二元运算，并表示为 $a\cdot b=c$，其中 $\cdot$ 表示运算符.

· 注：一个二元运算必须满足封闭性：$a\cdot b\in S$，唯一性：$a\cdot b$ 是唯一确定的.

· 代数系统：设 S 是一个非空集合，若在 S 中定义了一种运算 $\cdot$（或若干种运算 $+,\cdot,\times$ 等）则称 S 是一个代数系统，记作 $(S,\cdot)$ 或 $(S,+,\cdot)$ 等.

· 二元关系：设 A,B 是两个集合，则 $A\times B$ 的子集 R 称为 A,B 间的一个二元关系. 当 $(a,b)\in R$ 时，称 a 与 b 具有关系 R，记作 aRb；当 $(a,b)\notin R$ 时，称 a 与 b 不具有关系 R，记作 $aR'b$，A,A 间的二元关系，简称为 A 上的关系.

· 等价关系：设 $\sim$ 是集合 A 上的一个二元关系，并满足以下条件：

(1) 自反性：$\forall a\in A$，有 $a\sim a$，

(2) 对称性：$\forall a,b\in A$，有 $a\sim b\Rightarrow b\sim a$，

(3) 传递性：$\forall a,b,c\in A$，有 $a\sim b,b\sim c\Rightarrow a\sim c$，

则称 $\sim$ 是 A 上的一个等价关系. 子集 $\bar{a}=\{x\mid x\in A,x\sim a\}$，即所有与 a 等价的元素的集合，称为 a 所在的一个等价类，a 称为这个等价类的代表元.

· 等价关系的性质：

(1) $a \sim b \Leftrightarrow \bar{a} = \bar{b}$,即等价类中每一个元素都可作为代表元.

(2) 对任何两个元素 a 和 b,或有 $\bar{a} = \bar{b}$,或有 $\bar{a} \cap \bar{b} = \varnothing$.

· 集合的划分:设 A 为非空集合,$A_\alpha(\alpha \in I)$ 为 A 的一些非空子集,其中 I 为子集 A_α 的脚标 α 构成的集合,若有

(1) $\bigcup\limits_{\alpha \in I} A_\alpha = A$,

(2) 当 $\alpha, \beta \in I$ 且 $\alpha \neq \beta$ 有 $A_\alpha \cap A_\beta = \varnothing$,

则称 $\{A_\alpha \mid \alpha \in I\}$ 为 A 的一个划分或分类.

· 注:设 $\sim$ 为非空集合 A 中的一个等价关系,则等价类集合 $\{\bar{a} \mid a \in A\}$ 是 A 的一个划分,反之,A 的任何一个划分 $\{A_\alpha \mid \alpha \in I\}$ 决定了 A 中的一个等价关系:$a \sim b \Leftrightarrow$ 有 $\alpha \in I$,使 $a, b \in A_\alpha$.

· 商集:集合 A 对某个等价关系 $\sim$ 的所有等价类构成的集合,称为 A 关于 $\sim$ 的商集,记作 $A/\sim$,即 $A/\sim = \{\bar{a} \mid a \in A\}$,它是 2^A 的一个子集.

二、典型例题精解

例 1　证明下列命题成立:

设 $A \subseteq C$,则 $A \cup (B \cap C) = (A \cup B) \cap C$.

【证】　$\forall x \in A \cup (B \cap C)$,有 $x \in A$ 或 $x \in B \cap C$,当 $x \in A$ 时,有 $x \in A \cup B$,又因为 $A \subseteq C$ 时,所以 $x \in C$,从而 $x \in (A \cup B) \cap C$;当 $x \in B \cap C$ 时,有 $x \in B$ 且 $x \in C$,于是 $x \in A \cup B$ 且 $x \in C$,从而 $x \in (A \cup B) \cap C$,由此推出,$A \cup (B \cap C) \subseteq (A \cup B) \cap C$.

反之,$\forall x \in (A \cup B) \cap C$,有 $x \in A \cup B$ 且 $x \in C$,于是"$x \in A$ 或 $x \in B$" 且 $x \in C$,所以 $x \in A$,或"$x \in B$ 且 $x \in C$",从而 $x \in A \cup (B \cap C)$,于是 $(A \cup B) \cap C \subseteq A \cup (B \cap C)$,因此,$A \cup (B \cap C) = (A \cup B) \cap C$.

例 2　设 A, B 是全集 U 的两个子集,证明:若 $A \cup B = U$,$A \cap B = \varnothing$,则 $B = A'$.

【证】　因为

$$A' = A' \cap U = A' \cap (A \cup B) = (A' \cap A) \cup (A' \cap B)$$
$$= \varnothing \cup (A' \cap B) = A' \cap B,$$

所以 $A' \subseteq B$,又因为

$$A' = A' \cup \varnothing = A' \cup (A \cap B) = (A' \cup A) \cap (A' \cup B)$$
$$= U \cap (A' \cup B) = A' \cup B,$$

所以 $B \subseteq A'$,因此 $A' = B$.

例 3　证明:

(1) $A - B = \varnothing \Leftrightarrow A \subseteq B$;

(2) $A - B = A \Leftrightarrow A \cap B = \varnothing$.

【证】 (1) 设 I 为全集,若 $A-B=\varnothing$,则

$$A=A\cap I=A\cap(B\cup B')=(A\cap B)\cup(A\cap B')$$
$$=(A\cap B)\cup(A-B)=(A\cap B)\cup\varnothing=A\cap B\subseteq B.$$

反之,若 $A\subseteq B$,则

$$A-B=A\cap B'=(A\cap B)\cap B'$$
$$=A\cap(B\cap B')=A\cap\varnothing=\varnothing.$$

因此 $A-B=\varnothing\Leftrightarrow A\subseteq B$.

(2) 设 I 为全集,若 $A-B=A$,则

$$A\cap B=(A-B)\cap B=(A\cap B')\cap B$$
$$=A\cap(B'\cap B)=A\cap\varnothing=\varnothing.$$

反之,若 $A\cap B=\varnothing$,则

$$A=A\cap I=A\cap(B\cup B')=(A\cap B)\cup(A\cap B')$$
$$=\varnothing\cup(A\cap B')=A\cap B'=A-B,$$

因此 $A-B=A\Leftrightarrow A\cap B=\varnothing$.

例 4 求不大于 500 可被 5,7,9 中某一个数整除的正整数的个数.

【解】 设不大于 500 可被 5 整除的正整数集合为 A_1,不大于 500 可被 7 整除的正整数集合为 A_2,不大于 500 可被 9 整除的正整数集合为 A_3,则

$$|A_1|=100,\ |A_2|=\left[\frac{500}{7}\right]=71,\ |A_3|=\left[\frac{500}{9}\right]=55,$$

$$|A_1\cap A_2|=\left[\frac{500}{35}\right]=14,\ |A_1\cap A_3|=\left[\frac{500}{45}\right]=11,$$

$$|A_2\cap A_3|=\left[\frac{500}{63}\right]=7,\ |A_1\cap A_2\cap A_3|=\left[\frac{500}{315}\right]=1,$$

故有

$$|A_1\cup A_2\cup A_3|=\sum_{i=1}^{3}=|A_i|-\sum_{i<j}|A_i\cap A_j|+|A_1\cap A_2\cap A_3|$$
$$=100+71+55-14-11-7+1=195.$$

例 5 证明下列命题:

设 $f:A\to B,g:B\to C,h:C\to D$,则

(1) $h\circ(g\circ f)=(h\circ g)\circ f$, (2) $I_B\circ f=f,f\circ I_A=f$.

【证】 (1) 显然,$h\circ(g\circ f)$ 与 $(h\circ g)\circ f$ 有相同的定义域 A,相同的值域 D,又 $\forall x\in A$,有

$$(h\circ(g\circ f))(x)=h((g\circ f)(x))=h(g(f(x))),$$
$$((h\circ g)\circ f)(x)=(h\circ g)(f(x))=h(g(f(x))),$$

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

(2) 显然,$I_B\circ f$ 与 f 有相同的定义域 A,相同的值域 B,又 $\forall x\in A$,有

$$(I_B\circ f)(x)=I_B(f(x))=f(x),$$

因此，$I_B \circ f = f$，另一式同理可证.

例 6　若两个集合 A 和 B 之间存在一个双射，则称 A 和 B 等势. 证明实数区间 $(0,1)$ 与闭区间 $[0,1]$ 等势.

【证】　设

$$A_1 = \left\{\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \cdots\right\}, A_2 = \left\{0, 1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \cdots\right\},$$

作 $(0,1)$ 到 $[0,1]$ 的对应关系 φ：

$$\varphi\left(\frac{1}{2}\right) = 0, \varphi\left(\frac{1}{n}\right) = \frac{1}{n-2}, n \geqslant 3, \varphi(x) = x, \forall x \in (0,1) \backslash A_1,$$

显然 φ 是 $(0,1)$ 到 $[0,1]$ 的双射，故它们等势.

例 7　设 $f: A \to B$，证明：

(1) f 有左逆的充分必要条件为 f 是单射；

(2) f 有右逆的充分必要条件为 f 是满射；

(3) f 可逆的充分必要条件为 f 是双射.

【证】　(1) 必要性：设 f 有左逆 g，若 $f(x_1) = f(x_2)$，两边作用 g，有

$$gf(x_1) = gf(x_2),$$

即 $I_A(x_1) = I_A(x_2)$，从而有 $x_1 = x_2$，故 f 是单射.

充分性：设 f 是单射，定义 B 到 A 对应关系 g 为

$$g(b) = \begin{cases} a, & \text{若 } b \in f(A) \text{ 且 } f(a) = b, \\ a_1, & \text{若 } b \in B - f(A), \end{cases}$$

其中 a 是 A 中任意取定的一个元素，因 f 是单射，$g(b)$ 唯一确定，故 g 是映射，又 $\forall a \in A$ 有 $gf(a) = g(b) = a$，所以，$gf = I_A$，g 是 f 的左逆.

(2) 必要性：设 f 有右逆 h，则 $\forall b \in B$ 有 $fh(b) = b$，即 $f(h(b)) = b$，于是 $\forall b \in B$，存在 $x = h(b)$ 使 $f(x) = b$，所以 f 是满射.

充分性：设 f 是满射，我们定义一个 B 到 A 的对应关系 h：$\forall b \in B$，因为 f 是满射，存在一个 a，使 $f(a) = b$，于是，令 $h(b) = a$，则 h 是 B 到 A 的一个映射，且有

$$fh(b) = f(h(b)) = f(a) = b,$$

所以 $fh = I_B$，即 h 是 f 的右逆.

(3) 由 (1)(2) 可得.

例 8　设 $A = \{1,2,3,4,5\}$，在 2^A 中定义的元关系 $\sim$：$S \sim T \Leftrightarrow |S| = |T|$，证明 $\sim$ 是等价关系，并写出等价和商集 $2^A / \sim$.

【证】　$\forall T \in 2^A$，有 $|T| = |T|$，于是 $T \sim T$，从而 $\sim$ 有反身性，又 $\forall S, T \in 2^A$，$|S| = |T|$，由定义 $S \sim T$，又 $|T| = |S|$，从而 $T \sim S$，于是我们有 $S \sim T \Rightarrow T \sim S$，故 $\sim$ 有对称性. 对任何 $S, T, V \in 2^A$，且设 $S \sim T$，$T \sim V$，从而 $|S| = |T|$，$|T| = |V|$，即 $|S| = |V|$，故 $S \sim V$，于是 $\sim$ 有传递性，故 $\sim$ 是等价关系，商集 $2^A / \sim$ 为

$$2^A / \sim = \{\overline{\varnothing}, \overline{\{1\}}, \overline{\{1,2\}}, \overline{\{1,2,3\}}, \overline{\{1,2,3,4\}}, \overline{A}\}.$$

例 9 设 A 是一个非空集合，2^A 是 A 的幂集，证明：2^A 与 A 间不存在双射.

【证】 反证法，假设存在双射 $\varphi: x \to S_x (A \to 2^A)$，令 $T = \{a \in A \mid a \notin S_a\}$，显然 $T \in 2^A$，由于 φ 是双射，必有 $b \in A$ 使 $\varphi(b) = S_b = T$，若 $b \in S_b$，有 $b \in T$，由 T 的定义知 $b \notin S_b$，矛盾，若 $b \notin S_b$，知 $b \in T$，又由 $S_b = T$ 有 $b \in S_b$，矛盾，因此，2^A 与 A 之间不存在双射.

例 10 设给出三个$\mathbb{Z}$到$\mathbb{Z}$的映射：

$$f: x \to 2x, g: x \to 2x+1,$$

$$h: x \to \begin{cases} \dfrac{x}{2}, & \text{当 } 2 \mid x \text{ 时}, \\ \dfrac{x-1}{2}, & \text{当 } 2 \nmid x \text{ 时}. \end{cases}$$

(1) 计算：$f \circ g, g \circ f, h \circ f, h \circ g, f \circ h, g \circ h$；

(2) 证明：f, g 是单射，并分别求出 f, g 的一个左逆映射；

(3) 证明：h 是满射，并求出 h 的一个右逆映射.

【解】 (1) $(f \circ g)(x) = f(g(x)) = 4x+2$，

$(g \circ f)(x) = g(f(x)) = 4x+1$，

$(h \circ f)(x) = h(f(x)) = x$，

$(h \circ g)(x) = h(g(x)) = x$，

$$(f \circ h)(x) = f(h(x)) = \begin{cases} x, & \text{当 } 2 \mid x \text{ 时}, \\ x-1, & \text{当 } 2 \nmid x \text{ 时}. \end{cases}$$

$$(g \circ h)(x) = g(h(x)) = \begin{cases} x+1, & \text{当 } 2 \mid x \text{ 时}, \\ x, & \text{当 } 2 \nmid x \text{ 时}. \end{cases}$$

(2) 证明：① $\forall x, y \in \mathbb{Z}$，若 $f(x) = f(y)$，即 $2x = 2y$，于是 $x = y$，所以 f 是单射，取定一个整数 n，令

$$k(x) = \begin{cases} \dfrac{x}{2}, & \text{当 } 2 \mid x \text{ 时}, \\ n, & \text{当 } 2 \nmid x \text{ 时}. \end{cases}$$

则 k 是 f 的左逆映射.

② $\forall x, y \in \mathbb{Z}$，若 $g(x) = g(y)$，即 $2x+1 = 2y+1$，于是 $x = y$，所以 g 是单射，取定一个整数 n，令

$$s(x) = \begin{cases} \dfrac{x-1}{2}, & \text{当 } 2 \nmid x \text{ 时}, \\ n, & \text{当 } 2 \mid x \text{ 时}. \end{cases}$$

则 s 是 g 的左逆映射.

(3) 证明：$\forall x \in \mathbb{Z}$，$\exists 2x \in \mathbb{Z}$，使 $h(2x) = x$，所以 h 是满射，且由(1) 知 f, g 都是 h 的右逆映射.

三、自测题与解答

自测题

1. 设 $f(x),g(x)$ 是两个实系数一元多项式,其实根的集合分别记作 A,B 证明:

(1) 多项式 $f(x)g(x)$ 实根的集合为 $A \cup B$,

(2) 多项式 $f(x)^2+g(x)^2$ 实根的集合为 $A \cap B$.

2. 证明:

(1) $A\times(B \cup C)=(A\times B) \cup (A\times C)$,

(2) $A\times(B \cap C)=(A\times B) \cap (A\times C)$.

3. 设 $f:A\to B$ 是映射,$S\subseteq A,T\subseteq B$,证明:

(1) $f(f^{-1}(T))=T \cap f(A)$,

(2) $f(S \cap f^{-1}(T))=f(S) \cap T$,

(3) $S\subseteq f^{-1}(f(S))$,并举例说明"$=$"未必成立.

4. 设 R 与 $R_i,(i\in I)$ 都是 A 上的关系,证明:

(1) $(R^{-1})^{-1}=R$,

(2) 当 $R_1\subseteq R_2$ 时,有 $R_1^{-1}\subseteq R_2^{-1}$,

(3) $(\bigcup\limits_{i\in I}R_i)^{-1}=\bigcup\limits_{i\in I}R_i^{-1}$,

(4) $(\bigcap\limits_{i\in I}R_i)^{-1}=\bigcap\limits_{i\in I}R_i^{-1}$.

这里 $R^{-1}=\{(b,a)\mid(a,b)\in R\}$ 是 B,A 间的关系,是 R 的逆关系.

5. 设 A 是有限集,证明 $|2^A|=2^{|A|}$.

6. 设 $|A|=m,|B|=n$,求

(1) A 到 B 的单射有多少个?

(2) 当 $m=3,n=2$ 时,A 到 B 的满射有多少个?

7. 设 σ 是集合 A 到集合 B 的一个映射,证明:

(1) σ 是单射 $\Leftrightarrow$ 对任意集合 Z 到 A 的任意映意,映射 τ_1,τ_2,若有 $\sigma\tau_1=\sigma\tau_2$,必有 $\tau_1=\tau_2$,

(2) σ 是满射 $\Leftrightarrow$ 对任意,集合 $\overline{Y}$ 与 B 到 $\overline{Y}$ 的任意映射 τ_1,τ_2,若 $\tau_1\sigma=\tau_2\sigma$,必有 $\tau_1=\tau_2$.

解答

1.【证】 (1) a 是 $f(x)g(x)$ 的实根 $\Leftrightarrow f(a)g(a)=0\Leftrightarrow f(a)=0$ 或 $g(a)=0\Leftrightarrow a\in A$ 或 $a\in B\Leftrightarrow a\in A\cup B$,因此,多项式 $f(x)g(x)$ 实根的集合为 $A\cup B$.

(2) a 是 $f(x)^2+g(x)^2$ 的实根 $\Leftrightarrow f(a)^2+g(a)^2=0\Leftrightarrow f(a)=g(a)=0\Leftrightarrow a\in A$ 且 $a\in B\Leftrightarrow a\in A\cap B$,所以,多项式 $f(x)^2+g(x)^2$ 实根的集合为 $A\cap B$.

2.【证】 (1) 由于

$$\begin{aligned}&\forall x\in A\times(B\cup C)\\&\Leftrightarrow x=(a,b),a\in A,b\in B\cup C\\&\Leftrightarrow x=(a,b),a\in A,b\in B\text{或}b\in C\\&\Leftrightarrow x=(a,b)\in A\times B\text{或}x=(a,b)\in A\times C\\&\Leftrightarrow x\in(A\times B)\cup(A\times C),\end{aligned}$$

因此,$A\times(B\cup C)=(A\times B)\cup(A\times C)$.

(2) 由于

$$\begin{aligned}&\forall x\in A\times(B\cap C)\\&\Leftrightarrow x=(a,b),a\in A,b\in B\cap C\\&\Leftrightarrow x=(a,b),a\in A,b\in B\text{且}b\in C\\&\Leftrightarrow x=(a,b)\in A\times B\text{且}x=(a,b)\in A\times C\\&\Leftrightarrow x\in(A\times B)\cap(A\times C),\end{aligned}$$

因此,$A\times(B\cap C)=(A\times B)\cap(A\times C)$.

3.【证】 (1) $\forall x\in f(f^{-1}(T))\Leftrightarrow\exists y\in f^{-1}(T)$,满足 $x=f(y)$

$$\begin{aligned}&\Leftrightarrow x=f(y)\in T\text{且}x=f(y)\in f(A)\\&\Leftrightarrow x=f(y)\in T\cap f(A),\end{aligned}$$

于是,$f(f^{-1}(T))=T\cap f(A)$.

(2) $\forall x\in f(S\cap f^{-1}(T))\Leftrightarrow\exists y\in S\cap f^{-1}(T)$,满足 $x=f(y)$

$$\begin{aligned}&\Leftrightarrow\exists y\in S\text{且}y\in f^{-1}(T)\text{,满足}x=f(y)\\&\Leftrightarrow x\in f(S)\text{且}x=f(y)\in T\\&\Leftrightarrow x\in f(S)\cap T\end{aligned}$$

故

$$f(S\cap f^{-1}(T))=f(S)\cap T.$$

(3) 由

$$\forall x\in S\Rightarrow f(x)\in f(S)\Rightarrow x\in f^{-1}(f(S))\text{,有}S\subseteq f^{-1}(f(S)).$$

但"="未必成立,如设 $A=B=\mathbb{Z}$,$\forall a\in A$,令 $f(a)=0$,则 f 是 A 到 B 的映射,现设 $S=\{0\}$,则 $f(S)=\{0\}$,而 $f^{-1}(f(S))=A$,于是 $S\neq f^{-1}(f(S))$.

4.【证】 (1) $\forall(a,b)\in(R^{-1})^{-1}\Leftrightarrow(b,a)\in R^{-1}$

$$\Leftrightarrow(a,b)\in R,$$

于是,$(R^{-1})^{-1}=R$.

(2) $\forall(a,b)\in R_1^{-1}\Rightarrow(b,a)\in R_1\Rightarrow(b,a)\in R_2$

$$\Rightarrow(a,b)\in R_2^{-1},$$

因此,$R_1^{-1}\subseteq R_2^{-1}$.

(3) $\forall (a,b) \in (\bigcup\limits_{i\in I} R_i)^{-1} \Leftrightarrow (b,a) \in \bigcup\limits_{i\in I} R_i$

$\Leftrightarrow \exists i \in I$,使$(b,a) \in R_i$

$\Leftrightarrow \exists i \in I$,使$(a,b) \in R_i^{-1}$

$\Leftrightarrow (a,b) \in \bigcup\limits_{i\in I} R_i^{-1}$,

故,$(\bigcup\limits_{i\in I} R_i)^{-1} = \bigcup\limits_{i\in I} R_i^{-1}$.

(4) $\forall (a,b) \in (\bigcap\limits_{i\in I} R_i)^{-1} \Leftrightarrow (b,a) \in \bigcap\limits_{i\in I} R_i \Leftrightarrow \forall i \in I, (b,a) \in R_i$

$\Leftrightarrow \forall i \in I, (a,b) \in R_i^{-1}$

$\Leftrightarrow (a,b) \in \bigcap\limits_{i\in I} R_i^{-1}$,

于是,$(\bigcap\limits_{i\in I} R_i)^{-1} = \bigcap\limits_{i\in I} R_i^{-1}$.

5.【证】 因为 A 中 k 元子集个数为 $C_{|A|}^k$,于是

$$|2^A| = C_{|A|}^0 + C_{|A|}^1 + C_{|A|}^2 + \cdots + C_{|A|}^k + \cdots + C_{|A|}^{|A|} = 2^{|A|}.$$

6.【解】 (1) 若 $m \leqslant n$ 时,则单射个数为 n 中取 m 个的选排列数. 即 A 到 B 的单射个数为 $n(n-1)\cdots(n-m+1)$.

若 $m > n$,则没有 A 到 B 的单射,即单射个数为 0.

(2) 我们知道 A 到 B 可建立满射的充要条件是 $m \geqslant n$,现知 $m = 3, n = 2$,故 $B = \{b_1, b_2\}$ 中每个元素皆有逆象,于是 b_1 的逆象在 A 中有 3 种取法,b_2 的逆象有 2 种取法,从而共有 $3 \times 2 = 6$ 种取法,因此 A 到 B 的满射有 6 个.

7.【证】 (1) 设 σ 是单射,$\sigma\tau_1 = \sigma\tau_2$,这里 τ_1, τ_2 皆为集合 Z 到 A 的映射. 于是,$\forall a \in Z$,有$(\sigma\tau_1)(a) = (\sigma\tau_2)(a)$,即 $\sigma(\tau_1(a)) = \sigma(\tau_2(a))$,而 σ 是单射,故 $\tau_1(a) = \tau_2(a)$,从而 $\tau_1 = \tau_2$.

反之,若对任意集合 z 到 A 的任意映射 τ_1, τ_2 由 $\sigma\tau_1 = \sigma\tau_2$ 可得 $\tau_1 = \tau_2$,则 τ 必为单射,反证法,若命题不成立,即 σ 不是单射,则在 A 中 $\exists a_1 \neq a_2$,满足 $\sigma(a_1) = \sigma(a_2)$,现取 $Z = A$,令

$$\tau_1 : x \to a_1, \tau_2 : x \to a_2 \quad (\forall x \in Z),$$

则

$$(\sigma\tau_1)(x) = \sigma(t_1(x)) = \sigma(a_1), (\sigma\tau_2)(x) = \sigma(\tau_2(x)) = \sigma(a_2),$$

由 $\sigma(a_1) = \sigma(a_2)$,知$(\sigma\tau_1)(x) = (\sigma\tau_2)(x)$,从而 $\sigma\tau_1 = \sigma\tau_2$,但 $\tau_1(x) = a_1 \neq a_2 = \tau_2(x)$,于是 $\tau_1 \neq \tau_2$,矛盾,因此,σ 为单射.

(2) 设 σ 为满射,$\tau_1\sigma = \tau_2\sigma$,这里 τ_1, τ_2 是集合 B 到集合 $\overline{Y}$ 的两个映射,则对任意 $b \in B$ 有 $a \in A$ 使得 $\sigma(a) = b$. 于是

$$(\tau_1\sigma)(a) = (\tau_2\sigma)(a), \tau_1(b) = \tau_2(b).$$

故 $\tau_1 = \tau_2$.

反之,若对 B 到任意集合 $\overline{Y}$ 的任意,映射 τ_1, τ_2 有 $\tau_1\sigma = \tau_2\sigma$ 必有 $\tau_1 = \tau_2$,则 σ 必有满射,若不成立,任取一个集合 $\overline{Y}$,使 $|\overline{Y}| \geqslant 2$,则

$C = B - \sigma(A) \neq \varnothing$,于是任意取定 $y_1, y_2, y \in \overline{Y}$,且 $y_1 \neq y_2$,令

$$\tau_1 : b \to y, c \to y_1, \tau_2 : b \to y, c \to y_2,$$

这里 $b \in \sigma(A), c \in C$,则 τ_1, τ_2 是 B 到 $\overline{Y}$ 的两个不同的映射,但对任意 $a \in A$,有

$$(\tau_1\sigma)(a) = \tau_1(\sigma(a)) = y, (\tau_2\sigma)(a) = \tau_2(\sigma(a)) = y.$$

即有 $\tau_1\sigma = \tau_2\sigma$,而 $\tau_1 \neq \tau_2$,矛盾,故 σ 必为满射.

第2章 群 论

一、知识点精要

1 基本概念

1.1 群和半群

· 半群：设 G 是一个非空集合，若在 G 上定义一个二元运算满足结合律：对任何 $a,b,c \in G$，有 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$，则称 G 是一个半群，记作 $(G, \cdot)$.

· 群：设 $(G, \cdot)$ 是一个半群，若满足

(1) 存在单位元 e，使对任何 $a \in G$ 有 $e \cdot a = a \cdot e = a$，

(2) 对任何 $a \in G$，有逆元 a^{-1}，使 $a^{-1} \cdot a = a \cdot a^{-1} = e$，

则称 $(G, \cdot)$ 是一个群.

· 阿贝尔群：设 $(G, \cdot)$ 是一个群，且对任何 $a,b \in G$，有 $a \cdot b = b \cdot a$，则称 G 为可换群或阿贝尔群.

· 注：群的定义概括为四点：封闭性，结合律，单位元，逆元.

· 有限群，无限群，群的阶：若一个群 G 是个有限集，则称 G 是有限群，否则称为无限群，G 的元素个数 $|G|$ 称为群的阶.

· 加群，零元，负元：可换群中的运算称为加法，可换群又叫加群，加群中的单位元叫零元，逆元叫负元.

· 元素 a 的幂：$a^n = \underbrace{a \cdots a}_{n个}$，其中 n 为正整数，并规定 $a^0 = e$.

2 性质

2.1 关于单位元的性质

· 左单位元：设 $(G, \cdot)$ 是一个半群，若有元素 e_L，使对任何 $a \in G$，有 $e_L \cdot a = a$，则 e_L 叫做左单位元.

· 右单位元：设 $(G, \cdot)$ 是一个半群，若有元素 e_R，使对任何 $a \in G$，有 $a \cdot e_R = a$，则 e_R