

清华大学研究生公共课教材——数学系列

应用近世代数(第3版) 学习指导和习题详解

胡冠章 编著

清华大学出版社

清华大学研究生公共课教材——数学系列

应用近世代数(第3版) 学习指导和习题详解

胡冠章 编著

清华大学出版社
北京

内 容 简 介

本书把《应用近世代数(第3版)》(胡冠章,王殿军.清华大学出版社,2006,教育部优秀教材二等奖,普通高等教育“十一五”国家级规划教材)一书的习题全部做了详细解答,并收集了一些补充题.每节开始有内容提要,便于学习.每道题解答之前有分析,启发读者进行思考;每道题解完后有点评,指出该题的意义和是否还有其他解法等;使读者加深对近世代数内容的理解,掌握问题的分析方法和计算技巧,培养举一反三的能力.本书可作为教学参考书,也适合自学之用.适合数学和应用数学、计算机科学、信息科学、物理和化学等专业需要学习抽象代数知识的本科生、研究生和工程技术人员使用.

版权所有,侵权必究.侵权举报电话:010-62782989 13701121933

图书在版编目(CIP)数据

应用近世代数(第3版)学习指导和习题详解/胡冠章编著. —北京:清华大学出版社, 2012.10

(清华大学研究生公共课教材·数学系列)

ISBN 978-7-302-29573-0

I. ①应… II. ①胡… III. ①抽象代数—研究生—教学参考资料 IV. ①O153

中国版本图书馆CIP数据核字(2012)第179293号

责任编辑:佟丽霞

封面设计:常雪影

责任校对:王淑云

责任印制:李红英

出版发行:清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址:北京清华大学学研大厦A座 邮 编:100084

社 总 机:010-62770175 邮 购:010-62786544

投稿与读者服务:010-62776969, c-service@tup.tsinghua.edu.cn

质量反馈:010-62772015, zhiliang@tup.tsinghua.edu.cn

印 刷 者:三河市君旺印装厂

装 订 者:三河市新茂装订有限公司

经 销:全国新华书店

开 本:170mm×230mm 印 张:11.75 字 数:209千字

版 次:2012年10月第1版 印 次:2012年10月第1次印刷

印 数:1~4000

定 价:22.00元

产品编号:027288-01

前 言

本书的目的不是简单地给出习题的解答,而是使读者加深对近世代数内容的理解,掌握问题的分析方法和计算技巧,培养举一反三的能力.因此采取了下面一些新的写法.

1. 每节开始有内容提要,便于复习有关内容.这些内容提要并非简单重复书上的内容,而是经过简化、提炼与组织.对一些概念与定理用简洁的语言表达,便于记忆;或用式子表达,比较确切.例如,群的概念不再重复书上的详细表述,而是简化为:集合对运算满足封闭性、结合律、有单位元和逆元四个条件就构成群.另外,每节内容的顺序也有些改变以适合复习的特点.

2. 每道题开始有分析,主要是指出该题的困难在哪里,可能用什么方法解决等.读者在解题之前先看一下分析,然后先自己去解.当解不下去时再去看解答部分,有思路了再自己做.做完后再详细对照一下解答,看每题后的点评.

3. 每道题解完后有点评,指出该题的意义和是否还有其他解法等.有些题的点评还扩展了有关内容,例如,在第4章的4.3-6的点评中给出了一些有限域上的不可约与本原多项式的表,不仅可作为参考资料查阅,而且读者可自己进一步扩充知识点.

4. 第1~3章是基本部分,都增加了一些补充题,作为综合练习和提高之用.

编者

2012年7月

目 录

第 1 章 引言和预备知识	1
1.1 几类实际问题	1
一、内容提要	1
二、习题 1.1 详细解答	1
1.2 集合与映射	3
一、内容提要	3
二、习题 1.2 详细解答	3
1.3 二元关系	8
一、内容提要	8
二、习题 1.3 详细解答	9
1.4 整数与同余方程	12
一、内容提要	12
二、习题 1.4 详细解答	15
第 1 章补充题	18
第 2 章 群论	24
2.1 群的基本概念	24
一、内容提要	24
二、习题 2.1 详细解答	26
2.2 子群	31
一、内容提要	31
二、习题 2.2 详细解答	32
2.3 循环群和生成群,群的同构	37
一、内容提要	37
二、习题 2.3 详细解答	38
2.4 变换群和置换群, Caylay 定理	45
一、内容提要	45
二、习题 2.4 详细解答	47
2.5 子群的陪集和 Lagrange 定理	52

一、内容提要	52
二、习题 2.5 详细解答	53
2.6 正规子群和商群	57
一、内容提要	57
二、习题 2.6 详细解答	59
2.7 共轭元和共轭子群	63
一、内容提要	63
二、习题 2.7 详细解答	66
2.8 群的同态	74
一、内容提要	74
二、习题 2.8 详细解答	76
2.9 群对集合的作用, Burnside 引理	81
一、内容提要	81
二、习题 2.9 详细解答	83
2.10 应用举例	85
一、内容提要	85
二、习题 2.10 详细解答	86
2.11 群的直积与有限可换群	90
一、内容提要	90
二、习题 2.11 详细解答	91
2.12 有限群的结构, Sylow 定理	94
一、内容提要	94
二、习题 2.12 详细解答	95
第 2 章补充题	97
第 3 章 环论	105
3.1 环的基本概念	105
一、内容提要	105
二、习题 3.1 详细解答	106
3.2 子环、理想和商环	113
一、内容提要	113
二、习题 3.2 详细解答	115
3.3 环的同构与同态	121
一、内容提要	121

二、习题 3.3 详细解答	122
3.4 整环中的因子分解	130
一、内容提要	130
二、习题 3.4 详细解答	131
3.5 惟一分解整环	133
一、内容提要	133
二、习题 3.5 详细解答	135
3.6 多项式分解问题	139
一、内容提要	139
二、习题 3.6 详细解答	141
3.7 应用举例	145
一、内容提要	145
二、习题 3.7 详细解答	145
第 3 章 补充题	146
第 4 章 域论	149
4.1 域和域的扩张,几何作图问题	149
一、内容提要	149
二、习题 4.1 详细解答	151
4.2 分裂域,代数基本定理	156
一、内容提要	156
二、习题 4.2 详细解答	157
4.3 有限域,有限几何	160
一、内容提要	160
二、习题 4.3 详细解答	162
4.4 单位根,分圆问题	168
一、内容提要	168
二、习题 4.4 详细解答	170
第 5 章 方程根式可解问题简介	172
5.1 多项式的伽罗瓦群	172
一、内容提要	172
二、习题 5.1 详细解答	172

5.2 群的可解性和代数方程的根式求解问题	176
一、内容提要	176
二、习题 5.2 详细解答	177
参考文献	179

第 1 章 引言和预备知识

这一章的内容虽是准备部分,但非常重要,如果不熟悉,以后会处处受阻.考虑到各人原有的基础不同,这一章的内容和习题适宜自学.但不管是谁都应把内容和习题通读一遍,有重点地在某些内容上多加注意,例如关于整数的同余运算一定要熟悉起来.

1.1 几类实际问题

一、内容提要

本节的目的是提出一些可用近世代数解决的实际问题,以期引起读者的兴趣.由于读者现在还未学习到有关内容,所以我们只能用初等的方法来做这些题,从中体会到问题的困难.

二、习题 1.1 详细解答

1.1-1 用两种颜色的珠子做成有 5 颗珠子的项链,问可做出多少种不同的项链?

分析 在学群论前我们没有一般的方法,只能用枚举法.

解 用笔在纸上画一下,用黑白两种珠子,分类进行计算:全白只 1 种,四白一黑 1 种,三白二黑 2 种,二白三黑 2 种,一白四黑 1 种,全黑只 1 种.因此可得总共 8 种.

点评 读者不妨增加颜色数或珠子数再做做看,可以发现越来越难做,从而体会到必须寻找更高明的方法.

1.1-2 对正四面体的顶点用 2 种颜色着色,有多少种本质上不同的着色方法?

分析 我们可以用硬一点的纸做一个正四面体,也可在纸上画一个正四面体.看看有多少种着色方法.这里所说的本质上不同的着色方法,是指对两种着色不论怎样转动此正四面体它们都不能重合.

解 类似第 1 题,用枚举法可得 5 种.

点评 读者不妨增加颜色数再做做看,比项链问题更复杂,如没有更好的

方法是很难走远的.

1.1-3 有 4 个顶点的图共有多少个? 其中互不同构的有多少个?

分析 复习一下图的概念, 图一般指有标号的图, n 个点的图有 $2^{\binom{n}{2}} = 2^{\frac{n(n-1)}{2}}$ 个. 但其中有很多是互相同构的, 即不考虑点号, 两个图可以重合就称为它们同构. 互不同构的图又叫无标号图. 求互不同构的图的个数是很难的问题, 需要用群论方法.

解 由本节内容, 有 4 个顶点的图共有 64 个图. 用分类计数的方法可得共有 11 个互不同构的图: 无边的空图 1 个, 一条边的图 1 个, 有 2 条边的图有 2 个, 有 3 条边的图有 3 个, 有 4 条边的图有 2 个, 有 5 条边的图有 1 个, 有 6 条边的图有 1 个.

点评 读者不妨算一下有 5 个顶点的图共有多少个有标号图, 有多少个互不同构的图. 虽只增加一个点, 但难度有很大的提高.

1.1-4 如何用圆规 5 等分一个圆周?

分析 可先作一个单位圆, 设其半径长度为 1, 问题变成如何求出五边形的边长.

解 用初等数学的方法求五边形的边长: 作一个顶角为 36° 、腰长为 1 的等腰三角形, 设底边长为 a , 则 a 就是十边形的边长, 以 a 为半径以单位圆周上任意一点为圆心在圆周上交出两点, 则这两点之间的距离就是五边形的边长. 那么 a 怎么求呢? 只要在那个等腰三角形上作一条辅助线: 底角的角平分线, 再利用相似三角形边长成比例的关系, 可得 $a = \frac{\sqrt{5}-1}{2}$, 分别以 1 和 2 作直角边, 斜边就是 $\sqrt{5}$, 所以 a 就可作出了.

点评 由于一个数的开平方可以在圆上作出 (见图 1.1, 即主教材图 4.2), 所以, 如果正 n 边形的边长, 可由某个有理数经过有限次开平方与四则运算求得, 则就可 n 等分一个圆. 但这是否是可 n 等分一个圆周的必要条件呢? 我们将在第 4 章中详细讨论此问题.

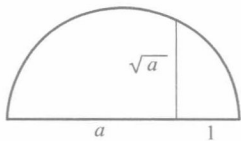


图 1.1

1.1-5 如何用根式表示 3 次和 4 次代数方程的根?

查看数学手册. 因公式较复杂, 不在这里列出了.

点评 从手册可见, 对 3 次和 4 次代数方程可通过几步表示它的根, 每一步都是根式表示式. 而对于 5 次以上的某些代数方程, 伽罗瓦证明了对某些 5 次方程不能用根式表示它的根. 我们将在第 5 章中讨论此问题.

1.2 集合与映射

一、内容提要

由于集合的概念太基本了,没有必要从头复习,我们只是强调和补充一些东西.

1. 集合

- 集合的记号: 本书用大写字母表示集合. $|A|$ 表示集合 A 的元素的个数,称为基数. 用 $|A| < \infty$ 表示有限集.

整数集合记作: \mathbb{Z} . 正整数(即自然数)集合记作: \mathbb{Z}^+ (自然数是否包含 0, 有不同的说法, 高等教育出版社出版的《数学手册》把自然数定义为正整数). 非负整数的集合无专门的记号. 非零整数的集合记作: \mathbb{Z}^* . 类似的, 对有理数有记号: $\mathbb{Q}, \mathbb{Q}^+, \mathbb{Q}^*$; 对实数有记号: $\mathbb{R}, \mathbb{R}^+, \mathbb{R}^*$; 对复数有记号: \mathbb{C}, \mathbb{C}^* .

- 集合 A 的幂集记作: $\mathcal{P}(A) = 2^A = \{A \text{ 的所有子集的集合}\}$. 当 $|A| < \infty$ 时有 $|2^A| = 2^{|A|}$.
- 包含与排斥原理: 设 A_1, A_2, \dots, A_n 是集合 S 的有限子集, 则

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

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

当并集的基数比交集的基数容易求时, 用第一个公式. 反之, 用第二个公式.

2. 映射

集合 A 到集合 B 的映射记作: $f: x \mapsto f(x) (A \rightarrow B)$.

- f 是单射 $\Leftrightarrow f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.
- f 是满射 $\Leftrightarrow f(A) = B$.
- f 是双射 $\Leftrightarrow f$ 既是单射又是满射.
- f 可逆 $\Leftrightarrow f$ 是双射.

二、习题 1.2 详细解答

1.2-1 设 $|A| < \infty$, 用二项式定理证明: $|2^A| = 2^{|A|}$.

分析 二项式定理为: $(a+b)^n = a^n + \binom{n}{1} a^{n-1} b + \binom{n}{2} a^{n-2} b^2 + \dots + b^n$. 求

幂集的元素个数如何与二项式定理联系起来呢? 我们从二项式系数 $\binom{n}{k}$ 入手, 它是从 n 个元素中取 k 个元素的取法, 正好是 k 元子集的个数, 而全部子集的个数正好就是这些二项式系数之和.

证 设 $A = \{a_1, a_2, \dots, a_n\}$, 由于 A 中 k 元子集的个数等于二项式系数 $\binom{n}{k}$, 于是把它们从 $k=1$ 到 $k=n$ 加起来, 再加一个空集, 所以

$$|2^A| = 1 + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{n} = (1+1)^n = 2^n = 2^{|A|}.$$

点评 证明该公式方法至少有以下几种:

证法 1 如主教材 1.2.2(指主教材的节号, 下同. 例子号, 定理号等均指主教材中的.) 中所说: 每一个元素有在子集中与不在子集中 2 种可能, 因而共有 2^n 种可能, 每一种可能对应一个子集, 所以共有 2^n 个子集.

证法 2 用二项式定理.

证法 3 利用主教材 1.2.6 节中公式: $|B^A| = |B|^{|A|}$. 令 $A = \{a_1, a_2, \dots, a_n\}$, $B = \{0, 1\}$, 则每一个 A 到 B 的映射对应一个子集, 所以全部子集的个数为 $|B^A| = |B|^{|A|} = 2^n$.

1.2-2 一个班有 93% 的人是团员, 80% 的人担任过社会工作, 70% 的人受过奖励, 问:

- (1) 受过奖励的团员至少占百分之几?
- (2) 三者兼而有之的人至少占百分之几?

分析 该题是求几个集合的交集的基数, 可用包含与排斥原理得到比较精确的结果.

解 设 A 为团员的集合, B 为担任过社会工作的人的集合, C 为受过奖励的人的集合, 则由包含与排斥原理, 可得

$$(1) |A \cap C| = |A| + |C| - |A \cup C| \geq 93 + 70 - 100 = 63,$$

所以受过奖励的团员至少占 63%.

(2) $|A \cap B \cap C| = |A| + |B| + |C| - |A \cup B| - |B \cup C| - |A \cup C| + |A \cup B \cup C|$, 由于 $|A \cup B \cup C| - |A \cup B| \geq 0$, 所以

$$\begin{aligned} |A \cap B \cap C| &\geq |A| + |B| + |C| - |B \cup C| - |A \cup C| \\ &\geq 93 + 80 + 70 - 100 - 100 = 43. \end{aligned}$$

故三者兼而有之的人至少占 43%.

点评 该题主要是复习集合运算的包含与排斥原理. 对于集合个数较少时, 可用画图的方法来确定.

1.2-3 在不大于 1000 的正整数中,求:

- (1) 不能被 5, 6, 8 中任何一个整数整除的个数.
 (2) 既非平方数也非立方数的个数.

分析 利用包含与排斥原理,参考主教材例 1.2.1.

解 (1) 设 $X = [1, 1000]$ 表示 1 到 1000 的所有整数, $A = \{x | x \in X \& 5 | x\}$, 即为 X 中能被 5 整除的所有整数的集合, $B = \{x | x \in X \& 6 | x\}$, $C = \{x | x \in X \& 8 | x\}$. 则

$$|A| = \frac{1000}{5}, \quad |B| = \left\lfloor \frac{1000}{6} \right\rfloor, \quad |C| = \left\lfloor \frac{1000}{8} \right\rfloor,$$

并可求出

$$|A \cap B| = \left\lfloor \frac{1000}{5 \times 6} \right\rfloor = 33, \quad |B \cap C| = \left\lfloor \frac{1000}{[6, 8]} \right\rfloor = 41,$$

$$|A \cap C| = \left\lfloor \frac{1000}{5 \times 8} \right\rfloor = 25, \quad |A \cap B \cap C| = \left\lfloor \frac{1000}{[5, 6, 8]} \right\rfloor = 8,$$

其中 $[6, 8]$ 和 $[5, 6, 8]$ 是最小公倍数的记号. 记号 $\lfloor x \rfloor$ 表示 x 的下整数, $\lceil x \rceil$ 表示 x 的上整数. 所以所求的个数为

$$\begin{aligned} |X| - |A \cup B \cup C| &= 1000 - |A| - |B| - |C| + |A \cap B| \\ &\quad + |B \cap C| + |A \cap C| - |A \cap B \cap C| \\ &= 1000 - 200 - 166 - 125 + 33 + 41 + 25 - 8 \\ &= 600. \end{aligned}$$

(2) 设 A 为 X 中平方数的个数, B 为 X 中立方数的个数, 则

$$|A| = \lfloor \sqrt{1000} \rfloor = 31, \quad |B| = \lfloor \sqrt[3]{1000} \rfloor = 10,$$

$$|A \cap B| = \lfloor \sqrt[6]{1000} \rfloor = 3.$$

所以所求的个数为

$$\begin{aligned} |X| - |A \cup B| &= 1000 - |A| - |B| + |A \cap B| \\ &= 1000 - 31 - 10 + 3 \\ &= 962. \end{aligned}$$

点评 根据题意, 首先确定是求集合的交还是并, 然后利用包含与排斥原理.

1.2-4 设 $|A| = m, |B| = n$, 求:

- (1) A 到 B 的单射有多少个?
 (2) 当 $m=3, n=2$ 时, 求 A 到 B 的满射有多少个?

分析 $f: A \rightarrow B$ 是单射 $\Leftrightarrow |f(A)| = |A|$, 因而 $|A| \leq |B|$.

$f: A \rightarrow B$ 是满射 $\Leftrightarrow |f(A)| = |B|$, 因而 $|A| \geq |B|$.

解 (1) 当 $m > n$ 时, 显然不存在 A 到 B 的单射.

当 $m \leq n$ 时, 由于单射的像必是 B 中的某个 m -子集, 且和子集元素的次序有关, 由此可得 A 到 B 的单射个数为以下从 m 个元素中选取 n 个元素的选排列数:

$$P(m, n) = m(m-1)\cdots(m-n+1).$$

(2) 当 $m < n$ 时, 显然不存在 A 到 B 满射.

当 $m \geq n$ 时, 存在 A 到 B 满射. 对于 $m=3, n=2$, 设 $A = \{a_1, a_2, a_3\}$, $B = \{0, 1\}$, 我们知道 A 到 B 全部映射数为 8, 非满射只有 2 个, 所以 A 到 B 的满射有 6 个.

点评 对一般情形, 求满射数的问题可参看 [4]p. 52-53. (参考文献的页码是本书后所附的参考文献, 下同.)

1.2-5 证明实数区间 $(0, 1)$ 与 $(-\infty, +\infty)$ 等势.

分析 关键是在这两个集合之间找一个双射.

证 作映射 $f: x \mapsto \ln \frac{x}{1-x}$. 可证 f 是单射: 任取 $x_1, x_2 \in (0, 1)$, 有

$$\begin{aligned} \ln \frac{x_1}{1-x_1} = \ln \frac{x_2}{1-x_2} &\Rightarrow \frac{x_1}{1-x_1} = \frac{x_2}{1-x_2} \Rightarrow x_1 - x_1x_2 \\ &= x_2 - x_1x_2 \Rightarrow x_1 = x_2. \end{aligned}$$

所以 f 是单射.

再证 f 是满射: 任取 $y \in (-\infty, +\infty)$, 令 $y = \ln \frac{x}{1-x}$, 可解出 $x = \frac{e^y}{1+e^y} \in (0, 1)$ 使 $f(x) = y$, 所以 f 是满射.

综上, f 是双射, 因此 $(0, 1)$ 与 $(-\infty, +\infty)$ 等势.

点评 可以找到很多满足要求的映射, 读者试另找一个双射.

1.2-6 设 f 是 A 到 B 的一个映射, $S \subseteq A$, 举例说明 $f^{-1}[f(S)] = S$ 是否成立?

注意 这里的记号 f^{-1} 并非指 f 的逆, f 不一定可逆. $f^{-1}[T]$ 表示 T 的全原像.

解 不一定成立.

成立的情况: 显然当 f 可逆时, $f^{-1}[f(S)] = S$ 成立. 实际上, 只要 f 是单射, 式子就成立: $\forall x \in S$, 设 $f(x) = y$, 由于 f 是单射, y 的原像只有 x , 即 $f^{-1}[f(x)] = x$, 所以 $f^{-1}[f(S)] = S$.

不成立的情况: 只要举一个 f 不是单射的例子. 例如: $f: x \mapsto x^2, \mathbb{R} \rightarrow \mathbb{R}$. 取 $S = \{1\}$, 则 $f(S) = \{1\}$, 但 $f^{-1}[f(S)] = f^{-1}(1) = \{-1, 1\} \neq S$.

点评 可以一般的证明： $f^{-1}[f(S)] = S$ 成立的充分必要条件是 f 是单射。

1.2-7 设 $|A| < \infty, f: A \rightarrow A$, 证明以下三个命题等价：

(1) f 是单射； (2) f 是满射； (3) f 可逆。

分析 这个题的结论很重要，即有限集上的单射、满射与双射都是互为充要条件。证明方法并不复杂。

证 用循环证法：

(1) \Rightarrow (2)：因为 f 是单射，且 A 是有限集，故有 $|f(A)| = |A|$ 。所以 f 是满射。

(2) \Rightarrow (3)：因为 f 是满射，故有 $f(A) = A$ 。下面用反证法证明 f 是单射：假设 f 不是单射，由于 A 是有限集，必故有 $|f(A)| < |A|$ 。与 f 是满射矛盾，所以 f 是单射。因而 f 是双射，即可逆。

(3) \Rightarrow (1)：显然。

点评 我们再强调一下，对有限集这个结论很重要！即有限集上的单变换必是满变换，也必是双变换和可逆变换。通常遇到有限集的问题我们要充分利用有限性使问题简化，甚至可列出所有的元素来进行分析。

1.2-8 设 $A \neq \emptyset$, 证明不存在 A 到它的幂集 $\mathcal{P}(A)$ 的双射。

分析 如果 A 是有限集，这个结论是显然的。因为 $\mathcal{P}(A)$ 的元素个数多于 A 的元素个数，因此不存在 A 到 $\mathcal{P}(A)$ 的双射。但对于无限集，就不能用这种方法证明了。下面的证法有特殊的技巧。

证 用反证法。

假设存在 A 到 $\mathcal{P}(A)$ 的双射 $f: x \mapsto f(x) = S_x \in \mathcal{P}(A)$ 。在 A 中取一个满足以下条件的子集：

$$T = \{x \mid x \in A \& x \notin S_x\}.$$

$T \in \mathcal{P}(A)$ ，由于 f 是满射，存在 $a \in A$ 使 $f(a) = S_a = T$ ，现我们分析 a 是否在 T 中？

若 $a \in T$ ，根据 T 的定义有 $a \notin S_a$ ，即 $a \notin T$ ，矛盾。

若 $a \notin T$ ，即 $a \in S_a$ ，根据 T 的定义有 $a \in T$ ，也矛盾。

所以不可能有这样的双射存在。

点评 是否有其他的证明方法呢？如有更简单的证明方法请发 Email 至 hugz@tsinghua.edu.cn.

1.3 二元关系

一、内容提要

1. 二元运算和代数系

我们从小学开始所做的运算大多是两个数的运算,但不太关心数的范围的变化.例如,两个正整数相减,其结果可能跑出正整数的范围;一个整数开平方,其结果不仅可能跑出整数的范围,而且可能跑出有理数的范围.在近世代数中,不管做什么样的运算,我们始终念念不忘是在什么集合里进行,其结果是否还在这个集合里?而且只有其结果仍在原集合的运算称为二元运算,具体定义如下:

- **二元运算**: 设 S 为非空集合,则映射 $f: S \times S \rightarrow S$ 就称为 S 中的一个二元运算.其最主要之点是满足封闭性和惟一性.
- **代数系**: 定义了一个或几个二元运算的集合就称为一个代数系.对不同的集合定义不同的运算就得到不同的代数系,例如群,环,域等.代数系是近世代数的基本舞台.

2. 二元关系和等价关系

我们从小学开始就知道相等、大于和小于等关系,后来学几何又知道三角形的全等、相似等关系,在线性代数里又有矩阵的相似、相合等关系.这些都是二元关系.其中最重要的是等价关系.

- **二元关系**: 在两个集合 A 和 B 的元素之间如果有一个规则 R , $\forall a \in A, \forall b \in B$ 可判断 aRb (a 与 b 符合规则 R), 或 $aR'b$ (a 与 b 不符合规则 R). 则规则 R 就称为集合 A 和 B 的元素之间的一个二元关系.
- **等价关系**: 在同一个集合里,一个二元关系如果满足 3 个条件: 反身性,对称性和传递性.则此二元关系称为此集合中的一个等价关系,等价关系记作 \sim 、 $=$ 、 \equiv 等.
- **等价类及其代表元**: 设集合 A 中的一个等价关系为 \sim , 则子集 $\bar{a} = \{x | x \sim a\}$ 称为以 a 为代表的等价类,它的记号有: \bar{a} , $[a]$ 等,以 \bar{a} 最简单,本书主要采用此记号.
- **商集**: A 中等价类的集合,记作 $A/\sim = \{\bar{a} | a \in A\}$, 称为 A 模 \sim 的商集.它是 A 的幂集的一个子集.
- **一个重要的等价关系——同余关系(非常重要!)**: 先在整数集合 \mathbb{Z} 中

定义一个二元关系称为整除关系： $a|b \Leftrightarrow \exists c \in \mathbb{Z}$ 使 $b=ac$. 然后可定义两整数的同余关系.

整数集合 \mathbb{Z} 中模 n 的同余关系记作： $\equiv (\text{mod } n)$, 定义为

$$a \equiv b (\text{mod } n) \Leftrightarrow n | (a - b).$$

这个等价关系的记号有点复杂和特殊, “ a 与 b 模 n 同余” 习惯记作 $a \equiv b (\text{mod } n)$. 整数模 n 的同余类： $\bar{a} = \{a + qn | q \in \mathbb{Z}\}$. a 是 \bar{a} 的代表元, 代表元不是惟一的. 若取代表元满足： $0 \leq a < n$, 则称它是正则代表元, 是惟一确定的.

有的书把同余类记作： $[a] = \{a + qn | q \in \mathbb{Z}\}$.

整数模 n 的商集： $Z_n = \mathbb{Z} / \equiv (\text{mod } n) = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$. 称为整数模 n 的同(剩)余类集合.

二、习题 1.3 详细解答

1.3-1 $A = \{1, 2, 3, 4, 5\}$, 在 2^A 中定义二元关系 \sim : $S \sim T \Leftrightarrow |S| = |T|$. 证明 \sim 是等价关系, 并写出等价类和商集 $2^A / \sim$.

分析 此题虽然简单, 但对还不太熟悉等价类和商集的读者来说, 还是应认真做一下.

证 易证 \sim 满足等价关系的三个条件, 反身性, $|S| = |S| \Rightarrow S \sim S$; 对称性: $S \sim T \Rightarrow |S| = |T| \Rightarrow T \sim S$; 传递性: $S \sim T, T \sim U \Rightarrow |S| = |T| = |U| \Rightarrow S \sim U$.

等价类为： $\overline{\emptyset} = \{\emptyset\}$, $\overline{\{1\}} = \{\{1\}, \{2\}, \{3\}, \{4\}, \{5\}\}$,

$$\overline{\{1, 2\}} = \{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{1, 5\}, \{2, 3\}, \{2, 4\}, \{2, 5\}, \{3, 4\}, \{3, 5\}, \{4, 5\}\},$$

$$\overline{\{1, 2, 3\}} = \{\{1, 2, 3\}, \{1, 2, 4\}, \{1, 2, 5\}, \dots, \{3, 4, 5\}\},$$

$$\overline{\{1, 2, 3, 4\}} = \{\{1, 2, 3, 4\}, \dots, \{2, 3, 4, 5\}\},$$

$$\overline{A} = \{A\}.$$

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

点评 这是概念题, 虽然简单, 但必须仔细写一写, 以加深印象, 并熟悉表示方法.

1.3-2 $S = \{0, 1, \dots, n\}$, $f: A \mapsto r(A) (M_n(\mathbb{R}) \rightarrow S)$. 求由 f 所决定的等价关系, 并决定等价类和商集.

分析 本题是把所有实 n 阶矩阵按秩分类, 注意把等价类的代表元写得简单一些.