

近世代数学习辅导与习题选解

杨子胥 编



高等教育出版社

内容提要

本书是与《近世代数(第二版)》(杨子胥编著)配套的学习辅导书。本书与主教材平行,按节编写,分为三部分:内容提要、释疑解难、习题解答。最后一章给出关于群、环、域的数学史简介。

本书可作为高等学校数学系学生学习近世代数的参考书。

图书在版编目(CIP)数据

近世代数学习辅导与习题选解/ 杨子胥编. —北京:
高等教育出版社, 2004. 7
ISBN 7 - 04 - 014370 - 4

近 ... 杨 ... 抽象代数-高等学校-
教学参考资料 .O153

中国版本图书馆 CIP 数据核字(2004)第 044944 号

策划编辑 李蕊 责任编辑 蒋青 封面设计 于涛
责任绘图 宗小梅 版式设计 张岚 责任校对 杨雪莲
责任印制

出版发行	高等教育出版社	购书热线	010 - 64054588
社 址	北京市西城区德外大街 4 号	免费咨询	800 - 810 - 0598
邮政编码	100011	网 址	http://www.hep.edu.cn
总 机	010 - 82028899		http://www.hep.com.cn

经 销 新华书店北京发行所
印 刷

开 本	850 × 1168 1/32	版 次	年 月第 1 版
印 张	8.625	印 次	年 月第 次印刷
字 数	220 000	定 价	11.20 元

本书如有缺页、倒页、脱页等质量问题, 请到所购图书销售部门联系调换。

版权所有 侵权必究

前 言

本书是针对作者编著的《近世代数》(第二版)所编写的一本学习指导书。内容以节为单位,每节分三个部分:主要内容、释疑解难、习题解答。可供学习《近世代数》的自学青年和在读大学生参考使用,更可作为教师教学参考之用。

其中“释疑解难”部分,主要是对该节的内容,特别是概念和定理可能产生的误解和疑问作出说明或解释,或举出正反两方面例子,以加深理解。“习题解答”部分,主要是对本节的习题给出解答。不过,很简单的习题多数略去解答,而有的题则只给出证明要领,属于详细提示性的。但一般的习题都给出了详细解答。

为了使读者能对近世代数中某些讨论对象的背景有深入了解,我们在本书中新增加了第七章“有关历史资料”,主要是介绍与近世代数相关的一些历史资料和著名数学家。这也可以增加学习近世代数的兴趣。

今后本书中凡提到“教材”或“本教材”时,均指作者所编著的第二版《近世代数》(2003年12月出版)。

又 $H \leq G$ 均指 H 是群 G 的子群; $H \mid G$ 均指 H 是群 G 的正规子群。对子环、理想也作类似规定。

前 言

由于水平所限,书中错误和不足之处恳请读者批评指正。

杨子胥

2004 年元月于济南

目 录

第一章 基本概念	1
§ 1 集合	1
一、主要内容(1) 二、释疑解难(1) 三、习题 1.1 解答(2)	
§ 2 映射与变换	4
一、主要内容(4) 二、释疑解难(4) 三、习题 1.2 解答(7)	
§ 3 代数运算	8
一、主要内容(8) 二、释疑解难(8) 三、习题 1.3 解答(8)	
§ 4 运算律	9
一、主要内容(9) 二、释疑解难(9) 三、习题 1.4 解答(11)	
§ 5 同态与同构	12
一、主要内容(12) 二、释疑解难(13) 三、习题 1.5 解答(14)	
§ 6 等价关系与集合的分类	15
一、主要内容(15) 二、释疑解难(15) 三、习题 1.6 解答(16)	
第二章 群	23
§ 1 群的定义和初步性质	23
一、主要内容(23) 二、释疑解难(23) 三、习题 2.1 解答(27)	
§ 2 群中元素的阶	30
一、主要内容(30) 二、释疑解难(30) 三、习题 2.2 解答(32)	
§ 3 子群	35
一、主要内容(35) 二、释疑解难(35) 三、习题 2.3 解答(36)	

§ 4 循环群	39
一、主要内容(39) 二、释疑解难(39) 三、习题 2.4 解答(40)	
§ 5 变换群	44
一、主要内容(44) 二、释疑解难(44) 三、习题 2.5 解答(45)	
§ 6 置换群	46
一、主要内容(46) 二、释疑解难(47) 三、习题 2.6 解答(48)	
§ 7 陪集、指数和 Lagrange 定理	50
一、主要内容(50) 二、释疑解难(50) 三、习题 2.7 解答(52)	
第三章 正规子群和群的同态与同构	69
§ 1 群同态与同构的简单性质	69
一、主要内容(69) 二、释疑解难(69) 三、习题 3.1 解答(70)	
§ 2 正规子群和商群	73
一、主要内容(73) 二、释疑解难(73) 三、习题 3.2 解答(75)	
§ 3 群同态基本定理	77
一、主要内容(77) 二、释疑解难(77) 三、习题 3.3 解答(78)	
§ 4 群的同构定理	81
一、主要内容(81) 二、释疑解难(81) 三、习题 3.4 解答(83)	
§ 5 群的自同构群	86
一、主要内容(86) 二、释疑解难(86) 三、习题 3.5 解答(88)	
§ 6 共轭关系与正规化子	90
一、主要内容(90) 二、释疑解难(90) 三、习题 3.6 解答(92)	
* § 7 群的直积	94
一、主要内容(94) 二、释疑解难(95) 三、习题 3.7 解答(98)	
* § 8 Sylow 定理	101
一、主要内容(101) 二、释疑解难(101) 三、习题 3.8 解答(103)	
* § 9 有限交换群	106
一、主要内容(106) 二、释疑解难(107) 三、习题 3.9 解答(109)	
第四章 环与域	127
§ 1 环的定义	127

目 录

一、主要内容(127)	二、释疑解难(127)	三、习题 4.1 解答(130)
§ 2 环的零因子和特征		133
一、主要内容(133)	二、释疑解难(133)	三、习题 4.2 解答(135)
§ 3 除环和域		138
一、主要内容(138)	二、释疑解难(139)	三、习题 4.3 解答(140)
§ 4 环的同态与同构		142
一、主要内容(142)	二、释疑解难(142)	三、习题 4.4 解答(143)
§ 5 模 n 剩余类环		146
一、主要内容(146)	二、释疑解难(147)	三、习题 4.5 解答(148)
§ 6 理想		151
一、主要内容(151)	二、释疑解难(151)	三、习题 4.6 解答(153)
§ 7 商环与环同态基本定理		156
一、主要内容(156)	二、释疑解难(157)	三、习题 4.7 解答(157)
§ 8 素理想和极大理想		160
一、主要内容(160)	二、释疑解难(160)	三、习题 4.8 解答(161)
§ 9 环与域上的多项式环		164
一、主要内容(164)	二、释疑解难(164)	三、习题 4.9 解答(164)
* § 10 分式域		166
一、主要内容(166)	二、释疑解难(166)	三、习题 4.10 解答(168)
* § 11 环的直和		169
一、主要内容(169)	二、释疑解难(170)	三、习题 4.11 解答(171)
* § 12 非交换环		176
一、主要内容(176)	二、释疑解难(176)	三、习题 4.12 解答(176)
第五章 唯一分解整环		195
§ 1 相伴元和不可约元		195
一、主要内容(195)	二、释疑解难(195)	三、习题 5.1 解答(196)
§ 2 唯一分解整环定义和性质		198
一、主要内容(198)	二、释疑解难(198)	三、习题 5.2 解答(199)
§ 3 主理想整环		201

目 录

一、主要内容(201)	二、释疑解难(202)	三、习题 5.3 解答(202)
§ 4 欧氏环		204
一、主要内容(204)	二、释疑解难(204)	三、习题 5.4 解答(205)
* § 5 唯一分解整环的多项式扩张		208
一、主要内容(208)	二、释疑解难(208)	三、习题 5.5 解答(209)
第六章 域的扩张		218
§ 1 扩域和素域		218
一、主要内容(218)	二、释疑解难(218)	三、习题 6.1 解答(219)
§ 2 单扩域		222
一、主要内容(222)	二、释疑解难(222)	三、习题 6.2 解答(224)
§ 3 代数扩域		227
一、主要内容(227)	二、释疑解难(228)	三、习题 6.3 解答(229)
§ 4 多项式的分裂域		231
一、主要内容(231)	二、释疑解难(232)	三、习题 6.4 解答(233)
§ 5 有限域		236
一、主要内容(236)	二、释疑解难(236)	三、习题 6.5 解答(237)
§ 6 可离扩域		238
一、主要内容(238)	二、释疑解难(239)	三、习题 6.6 解答(240)
第七章 有关历史资料		249
§ 1 群、环、域发展史简介		249
§ 2 代数方程的根式解		253
§ 3 几位数学家简介		257
阿贝尔、伽罗瓦、弗罗贝尼乌斯、哈密顿、诺特、阿廷、雅各布森		
参考文献		266

第一章 基本概念

§ 1 集 合

一、主要内容

1. 集合的表示法,子集、真子集以及集合相等的概念.
2. 集合的交集与并集的定义及其简单性质:幂等性、交换性、结合性和分配性,等.

二、释疑解难

1. 集合的概念是德国数学家康托尔(G.Cantor, 1845—1918)于 1894 年所首先建立的.到现在,集合论不仅已成为数学中一个专门理论和独立学科,而且广泛地应用到数学的各个分支中.

在近世代数中,不仅每章每节甚至几乎处处离不开集合,由此可见集合在近世代数中的重要性.但这只是问题的一方面.另一方面,我们在这里讲集合主要是为在近世代数中讲最基本的概念群、环、域作准备,而并不是要对集合本身的理论作太多和深入的阐述.这是因为,在近世代数中只用到集合的一些初步概念,诸如子集、真子集、集合的相等、幂集、交集、并集以及集合的差、余集和它们的简单性质,而并不用到其他.

2. 读者可能会发现,不同的书对“集合”的定义总稍有差异.这是因为“集合”是数学中最原始的一个基本概念,要真正准确地定义它则比较困难,所以一般的书中多采用先举实例后用归纳和描述性的方法来定义“集合”.

3. 关于集合,要首先注意其元素的确定性.就是说,一个元素是或不是属于这个集合,是完全确定而不能模棱两可的.例如,若说某年级“全体高个子同学作成的集合”就不合适.除非事先定一个“高个子”的严格标准,否则无法判断一个同学是不是“高个子”,也就是是不是属于这个集合.

4. 关于集合的相等.应注意集合相等的概念,例如,集合

$$A = \{1, 2\}, \quad B = \{2, 1\}, \quad C = \{1, 1, 2\}$$

被认为是相等的集合,即 $A = B = C$.亦即集合中的元素既不讲次序也不讲重复.教材中所说两个集合相等就是这个意思.也就是说:

$$A = B \iff A \subseteq B \text{ 且 } B \subseteq A.$$

因此,条件“ $A \subseteq B$ 且 $B \subseteq A$ ”实际上可作为集合 A 与 B 相等的定义.

教材中所说的集合一般均指非空集合.但有时也可以是空集合,对此应稍加留意即可.

三、习题 1.1 解答

1. 证明本节的等式 4).

证 任取 $x \in A \cap (B \cup C)$, 则

$$x \in A \text{ 且 } x \in B \cup C. \text{ 从而 } x \in B \text{ 或 } x \in C.$$

若 $x \in B$, 则 $x \in A \cap B$. 从而 $x \in (A \cap B) \cup (A \cap C)$. 因此

$$A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C).$$

反之,任取 $x \in (A \cap B) \cup (A \cap C)$, 类似可得 $x \in A \cap (B \cup C)$.

故

$$(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C).$$

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

同理可得 4) 中另一等式.

2. 若 $A \cap B = A \cap C$, 问: 是否 $B = C$? 把 $\cap$ 改成 $\cup$ 时又如何?

解 不一定有 $B = C$. 例如

$$A = \{1\}, \quad B = \{1, 2\}, \quad C = \{1, 3\}.$$

把 $\cap$ 改成 $\cup$ 后也不一定有 $B = C$. 例如

$$A = \{1\}, \quad B = \{2\}, \quad C = \{1, 2\}.$$

3. 设 A 是有限集合, 且 $|A| = n$. 证明: $|P(A)| = 2^n$.

证 因为 $|A| = n$, 故 A 的含 k ($0 \leq k \leq n$) 个元素的子集共有 C_n^k 个, 从而 A 共有

$$2^n = (1 + 1)^n = C_n^0 + C_n^1 + \dots + C_n^n$$

个子集, 即 $|P(A)| = 2^n$.

4. 设 A, B 是两个有限集合. 证明:

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

证 设 $|A| = m$, $|B| = n$, $|A \cap B| = k$, 则显然

$$|A \cup B| = m + n - k,$$

由此即得要证的等式.

5. 设 A, B 是两个集合. 称集合

$$A - B = \{a \mid a \in A, a \notin B\}$$

为 A 与 B 的差集. 特别, 当 $Y \subseteq X$ 时, 用 Y 表示 $X - Y$, 并称为 Y 在 X 中的补集. 证明德·摩根(A. De Morgan, 1806—1871)律: 若 $A, B \subseteq X$, 则

$$(A - B)' = A' \cap B', \quad (A \cap B)' = A' \cup B'.$$

证 设 $x \in (A - B)'$, 即 $x \notin A - B$. 故 $x \notin A$ 且 $x \in B$. 从而

$$x \in A' \text{ 且 } x \in B'. \quad \text{故 } x \in A' \cap B'.$$

从而 $(A - B)' \subseteq A' \cap B'$. 反推上去得 $A' \cap B' \subseteq (A - B)'$. 故得证.

另一等式可类似证明.

§ 2 映射与变换

一、主要内容

1. 映射、单射、满射以及双射的定义和例子 .
2. 变换、单射变换、满射变换以及双射变换的定义和例子 . 含 n 个元素的集合有且仅有 $n!$ 个双射变换 .

有限集合双射变换的特殊符号和名称——置换 .

3. 映射下元素或子集的象和逆象, 映射的相等及逆映射等概念 .

二、释疑解难

1. 若 φ 是集合 X 到 Y 的一个双射, 则 φ 有逆映射 φ^{-1} , 而 φ^{-1} 是集合 Y 到 X 的一个双射, 且根据映射的合成可知:

$$\varphi^{-1} \varphi = \varepsilon_X, \quad \varphi \varphi^{-1} = \varepsilon_Y .$$

其中 $\varepsilon_X, \varepsilon_Y$ 分别为 X 与 Y 的恒等变换 .

应注意, 在这里不能写成 $\varphi^{-1} \varphi = \varphi \varphi^{-1}$: 因为乘积 $\varphi^{-1} \varphi$ 是集合 X 的一个变换, 而 $\varphi \varphi^{-1}$ 是集合 Y 的一个变换, 但 X 与 Y 可能是两个不相干的集合, 那么两个不相干的集合它们的变换怎么能谈得上相等或不相等呢! 因此, 不要说不能写成 $\varphi^{-1} \varphi = \varphi \varphi^{-1}$, 同样也不能写成 $\varphi^{-1} \varphi \neq \varphi \varphi^{-1}$, 因为一般而言, 这是两个不可比较的对象 .

当然, 如果 $X = Y$, 即 φ 是 X 的一个双射变换, 则 φ 与 φ^{-1} 都是 X 的双射变换, 此时当然就有

$$\varphi^{-1} \varphi = \varphi \varphi^{-1} = \varepsilon_X .$$

此外还应注意, 如果 φ 是集合 X 到 Y 的任意一个映射, 又 $B \subseteq Y$, 则 $\varphi^{-1}(B)$ 并不意味着 φ 有逆映射 φ^{-1} (即 φ 不一定是双射). 在这里, 此时 $\varphi^{-1}(B)$ 只是一种符号, 即 B 中所有元素在 φ 之下所有逆象作成的集合, 它是 X 的一个子集, 甚至可能是一个空

集. 又若 $A \subseteq X$, 则有

$$A \subseteq \varphi^{-1}(\varphi(A)), \quad \varphi(\varphi^{-1}(B)) \subseteq B.$$

至于 $\varphi^{-1}(\varphi(A))$ 与 $\varphi(\varphi^{-1}(B))$ 之间一般无任何关系: 因为 $\varphi^{-1}(\varphi(A))$ 是 X 的子集, 而 $\varphi(\varphi^{-1}(B))$ 是 Y 的子集; 即使 $X = Y$ 且 φ 是 X 的双射, 也只能

$$\varphi^{-1}(\varphi(A)) = A, \quad \varphi(\varphi^{-1}(B)) = B,$$

此时 $\varphi^{-1}(\varphi(A))$ 与 $\varphi(\varphi^{-1}(B))$ 即 A 与 B 都是 X 的子集, 它们间也不一定有什么包含关系.

2. 关于在映射(变换)下元素的象的表示法.

设 τ 是集合 X 到 Y 的一个映射, $x \in X$. 则 x 在 τ 之下的象教材中用 $\tau(x)$ 表示, 这也是多数书中的表示法. 但也有的书表示成

$$(x)\tau \quad \text{或} \quad x^\tau \quad (1)$$

的. 不同的表示方法虽无实质性差别, 但也会产生一些不同的影响, 主要体现在映射或变换的乘法上. 例如, 若 σ 是集合 Y 到 Z 的一个映射, 则按教材中的规定, 乘积 $\sigma\tau$ 应为:

$$\sigma\tau(x) = \sigma(\tau(x)). \quad (2)$$

现在简称此为“自右向左乘法”.

若用(1)中两个表示法, 则应为:

$$(x)\tau\sigma = ((x)\tau)\sigma, \quad x^{\tau\sigma} = (x^\tau)^\sigma. \quad (3)$$

应注意的是, 当然不能写成 $(x)\sigma\tau = ((x)\sigma)\tau$ 及 $x^{\sigma\tau} = (x^\sigma)^\tau$, 因为这两个式子是毫无意义的(因为 σ 是 Y 到 Z 的映射, 而 $x \in X$, 故 $(x)\sigma$ 与 x^σ 都无意义). 另外易知, (3)中的两种表示法(分别称为“自左向右乘法”及“指数表示法”)实质上是一样的. 即使 σ, τ 是同一个集合的变换, 那么“自右向左乘法”与“自左向右乘法”(及“指数表示法”)也有差异, 其最主要的是表现在置换的乘法上. 例如, 设

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

则按教材中的规定(即“自右向左乘法”, 亦即“先 τ 后 σ ”)应为

$$\sigma\tau = \begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 2 & 3 \\ 2 & 1 & 3 & 2 & 3 & 1 \end{array} = \begin{array}{ccc} 1 & 2 & 3 \\ 1 & 3 & 2 \end{array} \quad (4)$$

(先 τ 后 σ)

然而,若按(1)中的“自左向右乘法”(即先 σ 后 τ)则应为

$$\sigma\tau = \begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 2 & 3 \\ 2 & 1 & 3 & 2 & 3 & 1 \end{array} = \begin{array}{ccc} 1 & 2 & 3 \\ 3 & 2 & 1 \end{array} \quad (5)$$

(先 σ 后 τ)

从而乘积(4)与(5)有很大差异.产生这种差异的原因,就是因为元素在映射下象的表示法不同而引起的.

这两种表示法究竟采用哪一种好,可以说各有利弊.若采用 $\tau(x)$,则符合通常函数的习惯表示法(通常的函数用 $f(x)$ 表示,而不是 $(x)f$),缺点是在做乘法时则需“自右向左乘”,这跟通常行文自左向右的习惯不符合;若采用 $(x)\tau$,则虽然在做乘法时“自左向右”符合行文习惯,但 $(x)\tau$ 表示法本身与函数通常表示法相悖.读者在看参考书时应予留意.

3. 映射与通常函数的关系.

设 $y = f(x)$ 是任意一个(实、单值)函数, D 是其定义域, Y 是其值域.则根据 $y = f(x)$ 我们可以确定一个 D 到 Y 的映射 f ,它对于 D 中每个元素(实数) x 都有 Y 中唯一的元素 $y = f(x)$ 与之对应.这就是说,对任意(实、单值)函数都可确定一个映射,并且其元素对应法则也是一致的.

反之,任给一个集合 X 到 Y 的映射 τ ,是否由映射 τ 也能确定一个函数呢?回答是否定的.这是因为 X 与 Y 不一定是(实)数集,从而就不能由 τ 的元素对应关系来确定一个函数.但是,若 X 与 Y 都是数集,则可以根据映射 τ 来确定一个函数:

$$y = \tau(x) \quad (x \in X).$$

这个函数的定义域是 X ,但其值域不一定是 Y ,而只是 Y 的一个子集.教材中已有这样的例子,不再重复.

映射与函数除去以上差异外,还应注意:关于映射必须先明确所涉及的两个集合 X 与 Y 是什么,再明确元素对应法则是什么;

而函数往往是先给出元素的对应法则(即自变量和因变量的对应关系),然后再去找其定义域和值域.

三、习题 1.2 解答

1. 设 $X = \{1, 2, 3, 4, 5\}$, $Y = \{0, 2, 4, 6, 8, 10\}$. 试给出 X 到 Y 的两个单射.

解 略.

2. 设 X 是数域 F 上全体 n ($n > 1$) 阶方阵作成的集合. 问:

$$\varphi: A \mapsto |A|$$

是否为 X 到 F 的一个映射? 其中 $|A|$ 为 A 的行列式. 是否为满射或单射?

解 φ 是映射, 且是满射, 但不是单射.

3. 设 A 与 B 是数域 F 上两个 n 阶相似方阵, $F[A]$ 为系数属于 F 的关于 A 的一切多项式作成的集合. 问: 法则

$$\varphi: f(A) \mapsto f(B)$$

是否为 $F[A]$ 到 $F[B]$ 的映射? 其中 $f(x)$ 是系数属于 F 的任意多项式. 又 φ 是否为单射或满射?

解 设 $B = CAC^{-1}$ (C 为 F 上 n 阶满秩方阵). 若 $f(A) = g(A)$, 则

$$\begin{aligned} f(B) &= f(CAC^{-1}) = Cf(A)C^{-1} \\ &= Cg(A)C^{-1} = g(CAC^{-1}) = g(B). \end{aligned}$$

即 φ 是 $F[A]$ 到 $F[B]$ 的一个映射. 又类似易知, φ 是单射和满射, 从而 φ 是双射.

4. 对本节中给出的 3 次置换, 求出下列各元素:

$$1) \varphi(\varphi(\varphi(1))) = ?$$

$$2) \varphi(\varphi(\varphi(2))) = ?$$

解 略.

5. 给出整数集的两个不同的双射.

解 略.

§3 代数运算

一、主要内容

1. 代数运算定义和例子 .

2. 变换的乘法及恒等变换 .

3. 一个集合 M 的全体变换的集合 $T(M)$ 关于变换的乘法作成代数系统 . 而 M 的全体双射变换的集合 $S(M)$ 也作成代数系统, 它是 $T(M)$ 的一个子系统 .

二、释疑解难

1. 若 $\cdot$ 是集合 M 的一个代数运算, 则对 M 中任二元素 a, b 都有 M 中一个惟一确定的元素 d 与之对应, 写成 $a \cdot b = d$. 这实质上就是加氏积

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

到 M 的一个映射:

$$\cdot : (a, b) \mapsto a \cdot b = d .$$

应注意, 这里 a, b 可以相等也可以不相等, 完全是 M 中任意的元素 . 又 d 必须是由 a 与 b 惟一确定的元素, 而且必须属于 M .

2. 变换是一种特殊的映射, 因此, 变换的乘法是由映射的乘法(合成)所决定的, 即上一节所说的“自右向左的乘法” . 关于这个乘法, 由下一章将知道, $T(M)$ 作成有单位元的半群, 而 $S(M)$ 作成群 . 当 $|M| = n$ 时, $S(M)$ 就是所谓的 n 次对称群 .

3. 群是有一个代数运算的代数系统, 环与域是有两个代数运算的代数系统 . 近世代数最主要的任务就是讨论这两类代数系统 .

三、习题 1.3 解答

1. 设 M 是正整数集 . 下列各法则哪些是 M 的代数运算 ?