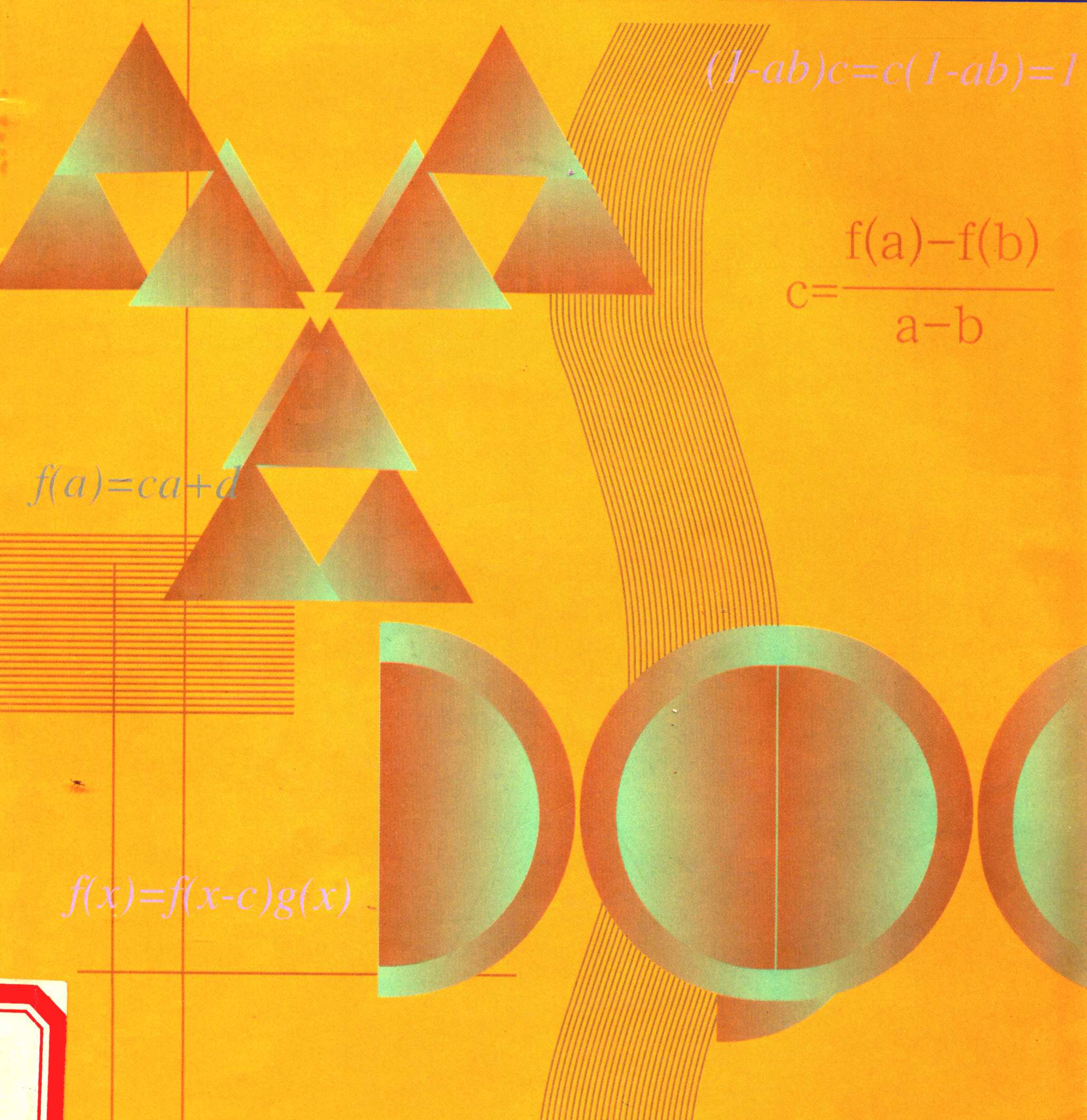
高等代数专题研究

学习指导书

冯　泰　周永胜　张清利



中央广播电视大学出版社

高等代数专题研究学习指导书

冯 泰 周永胜 张清利

中央广播电视大学出版社

图书在版编目（CIP）数据

高等代数专题研究学习指导书/冯泰，周永胜，张清利编.—北京：中央广播电视大学出版社，2002.1

ISBN 7-304-02204-3

Ⅰ.高…　Ⅱ.①冯…②周…③张…　Ⅲ.高等代数-电视大学-教学参考资料　Ⅳ.015

中国版本图书馆 CIP 数据核字(2002)第 000739 号

高等代数专题研究学习指导书

冯　泰　周永胜　张清利

出版·发行/中央广播电视大学出版社

经销/新华书店北京发行所

印刷/北京集惠印刷有限公司

开本/787×1092　1/16　**印张**/7　**字数**/170 千字

版本/2001 年 12 月第 1 版　2002 年 1 月第 1 次印刷

印数/0001—2000

社址/北京市复兴门内大街 160 号　　**邮编**/100031

电话/66419791　68519502　**(本书如有缺页或倒装，本社负责退换)**

书号：ISBN 7-304-02204-3/O·113

定价：12.00 元

前　　言

《高等代数专题研究学习指导书》是王仁发教授编著的《高观点下的中学数学——代数学》(高等教育出版社出版)的辅导书,供广播电视大学本科开放教育理科数学与应用数学专业的学生使用.

按照高等代数专题研究多种媒体教材一体化设计方案的要求,本指导书每章分重难点解析、典型例题、自测题、自测题解答和教材习题解答五部分.高等代数专题研究是初等数学的理论基础,本课程涉及:什么是数,数的运算与映射的关系,不等式理论,多项式理论、因式分解,多项式根的求法与根的估计,初等排列组合的原理与应用,容斥原理和抽屉原理方面的知识等,知识面较广,内容较多.为了使学生能够顺利地学习相关的内容,在重难点解析部分对某些概念或定理、公式等作了较多的解释,并列举了大量例题印证或说明;自测题包括单项选择题、填空题、解答计算题和证明题,学生自己学完各章后,进行一次自我认识;教材中的部分习题有一定难度,在教材习题解答中给出稍细解答,一般题目只给答案.本课程的总体要求以该课程教学大纲为准,为此将《广播电视大学"本科开放教育"高等代数专题研究教学大纲》附上,供参考.教材中第六章"伽罗华理论",教材和教学大纲中均加了" * "号,因时间关系,本书略去.教材中第四章"数论初步",超出本课程的教学大纲,不做教学要求.

参加本书编写的有周永胜(第二章)、张清利(第一、三章)、冯泰(第四章),由冯泰统稿.在编写出版过程中得到了中央电大教务处处长李林曙教授、基础部副主任顾静相副教授的大力支持,首都师范大学王培根副教授在百忙中,抽时间审阅了部分稿件,在此一并致谢.由于时间仓促,水平有限,错误在所难免,欢迎批评指正.

编　者

2001 年 12 月于北京

目　录

广播电视大学本科开放教育
《高等代数专题研究》教学大纲

第一部分 大纲说明

一、课程的作用与任务

《高等代数专题研究》是中央电大理科数学与应用数学(本科)的一门必修课程.本课程从更高的观点看待初等数学,把初等数学中的数和形统一起来.主要内容有数的本质认识、数的发展历史、不等式和多项式的严格定义、因式分解、初等排列组合与多项式的求根方法等.这些问题来自初等数学,但它却含有数学中极深刻的内容,对深化初等数学的学习具有一定意义.

二、课程的目的与要求

《高等代数专题研究》是初等数学的理论基础,所以要求学员了解什么是数,数的运算与映射的关系,掌握因式分解的理论基础,能够证明角为什么不能用尺规三等分,知道5次以上代数方程为什么没有根式解.同时要求学员掌握方程根的解法与方程根的估计,最后还应了解一般排列组合的原理与应用,特别是在古典概率理论中的应用.了解容斥原理和抽屉原理方面的知识和应用.

三、课程的教学要求层次

教学要求中,有关定义、定理、性质、特征等概念内容按"知道、了解和理解"三个层次要求,有关计算、解法、公式和法则等方法的内容按"会、掌握和熟练掌握"三个层次要求.

第二部分 学时、教学安排、教材与教学环节

一、学时和学分

1.本课程共54个学时,学时分配为:

章号	内　　容	课内学时	电视学时	IP学时	备注
1	代数运算与自然数	10			
2	不等式	8			
3	多项式与环	18			
4	排列与组合	14			
5	伽罗华理论简介	4			
合　　计		54	18	27	

2. 学分

本课程共 3 学分.

二、教学安排

本课程安排在第 2 学期，一个学期完成全部教学任务.

三、教　材

1. 根据远距离教育的要求和电大学生入学时水平参差不齐的实际情况，文字教材由主教材和辅导教材两部分组成.

主教材和辅导教材是学生学习的主要用书，主教材是课程的基本内容，是教和学的主要依据. 辅导教材对主教材的内容进行归纳、总结，帮助学生进一步理解基本概念，掌握基本方法，并通过典型例题介绍解题规律和技巧，提高学生解题能力.

文字教材是学生获得知识和提高能力的重要媒体之一，教材的内容要具科学性，叙述和论证要直观和清楚，突出重点，讲透实质内容，以便适合成人业余学习为主的特点，便于自学.

2. 电视录像教材是学生获得本课程知识的主要媒体之一.

本课程的电视课以重点内容系统讲授和非重点内容精讲相结合的方式进行. 精讲是讲重点、讲方法，或解答疑难问题.

在电大多年录像教材的基础上，进行多种媒体的一体化设计，适当地多引入一些现代化教学手段，如计算机虚拟教室环境、动画、字幕、实景等，强化教学效果.

3. IP 课程是基于网络的新型教学媒体之一.

本课程要积极探索基于网络环境的远程开放教育的教学模式、学习模式，充分利用 IP 课程的卫星、网络传播的优势，充分发挥 IP 课程的教学内容可选和交互性，为学生自主学习本课程提供更方便的教学资源.

四、教学环节

1. 本课程配有电视课和 IP 课程，是重要的教学形式.

2. 自学

自学是电大学生获得知识的重要方式，自学能力的培养也是远程开放高等教育的目的之一，本课程的教学要注意对学生自学能力的培养. 学生可以通过自学、收看电视、IP 课程、直播课堂和网上教学辅导等形式进行学习，各地可以采用灵活多样的助学方式，帮助学生学习.

3. 面授助学

面授助学要服务于教学大纲、文字教材、音像教材或 IP 课程，采用讲解、讨论、答疑等方式，通过解题思路分析，基本方法训练，培养学生基本运算的能力和分析、解决问题的能力.

4. 作业

独立完成作业是学生学好本课程的必经之路.

通过做作业，加深对所学内容的理解，熟悉各种解题方法，达到消化、掌握所学知识的目的.

5. 期末考试

考试题目要全面，符合教学大纲要求，同时要做到体现重点，题量适度，难度适中，难度和题量梯度应按照要求的三个不同的层次安排. 不出难题、怪题.

第三部分　教学内容与教学要求

一、代数运算与自然数(10 学时)

(一)教学内容

集合的概念及其运算,映射的定义及其运算、映射与函数的关系,映射的合成,复合函数表示方法.

自然数的定义及其运算,归纳法原理.

重点:映射性质,自然数的定义,归纳法原理.

难点:自然数的定义和归纳法原理.

(二)教学基本要求

1.了解自然数的定义及其运算.

2.了解映射的定义、映射与数的运算关系、映射与函数之间的关系.

3.掌握各种归纳法及其应用.

二、不等式(8 学时)

(一)教学内容

不等式的定义和性质,柯西不等式,赫勒德尔不等式,明可夫斯基不等式,凸函数及其应用,若干个分析上常用不等式.

重点:柯西不等式、凸函数的定义与应用.

难点:不等式的几种变通证明.

(二)教学要求

1.掌握柯西不等式的两种证明.

2.了解赫勒德尔与明可夫斯基不等式及其证明方法.

3.了解凸函数性质,掌握它的某些应用.

三、多项式与环(18 学时)

(一)教学内容

环的定义及其分类,整环的定义和性质.

素元素与不可约元素的定义与区别.

多项式的代数定义与分析定义.

代数学基本定理与多项式根的求法,因式分解,多项式的根的估计,重因式判别法,施斗姆定理.

重点:素元素与不可约元素定义,整系数多项式的因式分解.

难点:代数基本定理证明与施斗姆定理.

(二)教学基本要求

1.掌握整环的性质,掌握素元素与不可约元素的定义及其区别.

2.了解环的定义、分类,了解代数基本定理的证明.

3. 了解整系数多项式因式分解的方法、多项式根的求法与估计，了解重因式判别法，知道施斗姆定理.

四、排列与组合(14 学时)

(一)教学内容

初等排列组合原理，可重复的排列与组合，容斥原理，分部与递推公式，抽屉原理.

重点：重复排列与组合，容斥原理及其应用.

难点：重复组合与容斥原理的两种证明.

(二)教学要求

1. 了解排列组合原理，可重复排列与组合的应用.

2. 理解容斥原理，掌握应用容斥原理解决简单数学问题的方法，知道递推公式原理.

五、伽罗华理论简介(4 学时)

(一)教学内容

伽罗华群定义，伽罗华群基本定理，可解群.

重点：伽罗华基本定理

难点：伽罗华群基本定理的证明

(二)教学要求

1. 知道伽罗华群的定义.

2. 了解为什么 5 次以上代数方程没有根式解.

第一章　代数运算与自然数

【重难点解析】

（一）集合与映射

1. 集合

(1)集合的概念

假设有一系列数学概念：甲、乙、丙、…….定义甲要用到乙，定义乙要用到丙，…….这样追溯下去，就必须有原始的、不定义的概念.集合就是这样一个不加定义的基本概念.我们把一些事物的总体就称为一个**集合**，集合中的事物称为**元素**.常用大写字母 A、B、C 等表示集合，小写字母 a、b、c 等表示元素.

一个集合中的元素是确定的，即任一元素或者是这个集合的元素，或者不是这个集合的元素，二者必居其一，且仅居其一.例如，某班所有年龄较大的同学，就不能构成一个集合，因为这里没有"年龄较大"的标准，我们无法判断一个同学是否年龄较大.另外，集合中的元素是彼此不同的，即相同的事物归入一个集合时，只能算作一个元素.例如，我们不能说一个集合中有三个元素都是数1，只能说数1是这个集合的一个元素.

只含有限个元素的集合称为**有限集**.含无限多个元素的集合称为**无限集**.不含任何元素的集合称为**空集**，记作 Φ.把空集看作集合是必要的，正像数零也是数一样.空集也算作有限集.一个有限集 A 所含元素的个数记作 $|A|$.

a 是集合 A 的一个元素，称为 **a 属于 A**，记作 $a\in A$. a 不是 A 的元素，称为 **a 不属于 A**，记作 $a\notin A$.若集合 A 的每个元素都是集合 B 的元素，则称 A 是 B 的一个**子集**，记作 $A\subseteq B$，读作 A 包含于 B.若 $A\subseteq B$，且至少有一个元素 a 使 $a\in B$ 而 $a\notin A$，则称 A 是 B 的一个**真子集**，记作 $A\subset B$，读作 A 真包含于 B.若 $A\subseteq B$ 且 $B\subseteq A$，则 A 与 B 包含的元素完全相同，这时称 A 与 B **相等**，记作 $A=B$.规定空集是任意集合 A 的子集，即 $\Phi\subseteq A$.

集合的表示法：一些常见的集合，用专门的符号表示.我们用 $\mathbf{N}$,$\mathbf{Z}$,$\mathbf{Q}$,$\mathbf{R}$ 与 $\mathbf{C}$ 分别表示自然数集、整数集、有理数集、实数集与复数集.由元素 $a_1, a_2, \cdots, a_n$ 组成的集合记作 $\{a_1, a_2, \cdots, a_n\}$.这种表示集合的方法称为列举法.具有性质 P 的所有元素的集合记作 $\{x\mid P\}$.这种表示集合的方法称为描述法.

例1　6的全体正因数的集合，用列举法表示为 $\{1,2,3,6\}$.用描述法表示为：

$$\{x\mid x\text{ 是 6 的正因数}\}$$

例2　方程 $x^3-x+1=0$ 的全体实根的集合为：

$$\{x\mid x\in\mathbf{R}, x^3-x+1=0\}$$

例3　形如 $a+b\sqrt{2}$(a,b 是有理数)的全体实数的集合为：

$$\{a+b\sqrt{2}\mid a,b\in\mathbf{Q}\}$$

集合 A 的所有子集的集合称为 A 的**幂集**，记作 $P(A)$.

例4　设 $A=\{a,b,c\}$，求 $P(A)$.

解 A 的不含任何元素的子集为 Φ. 只含一个元素的子集有 3 个,它们是:

$$\{a\},\{b\},\{c\}$$

只含两个元素的子集有 3 个,它们是:

$$\{a,b\},\{a,c\},\{b,c\}$$

含有三个元素的子集就是 A 本身. 故:

$$P(A)=\{\Phi,\{a\},\{b\},\{c\},\{a,b\},\{a,c\},\{b,c\},A\}$$

由于 $P(A)$ 一共有 8 个元素,所以 $|P(A)|=8$.

一般地,若 $|A|=n$,则 $|P(A)|=2^n$.

设 A,B 是两个集合,所有有序元素对

$$(a,b)\quad a\in A, b\in B$$

的集合称为 A 与 B 的**积集**,记作 $A\times B$,即:

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

注意:在 $A\times B$ 中,$(a,b)=(c,d)\Leftrightarrow a=c, b=d$.

例 5 设 $A=\{a,b,c\}$, $B=\{1,2\}$,则:

$$A\times B=\{(a,1),(a,2),(b,1),(b,2),(c,1),(c,2)\}$$

其元素个数为 6,故 $|A\times B|=6$.

一般地,若 $|A|=m$, $|B|=n$,则 $|A\times B|=mn$.

例 6 实数集与本身的积集

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

即为全体有序实数对的集合.

两个集合的积集可以推广到多个集合的积集(见教材 p.2).

(2)集合的运算

设 A,B 是两个集合,由属于 A 或属于 B 的所有元素作成的集合称为 A 与 B 的**并**,记作 $A\cup B$,即:

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

由属于 A 且属于 B 的所有元素作成的集合称为 A 与 B 的**交**,记作 $A\cap B$,即:

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

由属于 A 而不属于 B 的所有元素作成的集合称为 A 与 B 的**差**,记作 $A-B$,即:

$$A-B=\{x\mid x\in A \text{ 且 } x\notin B\}$$

任意两个集合 A,B 都可以作并、交、差三种运算,$A\cup B$、$A\cap B$、$A-B$ 仍然是集合. 特别地,若 $A\subseteq B$,则 $A\cup B=B$, $A\cap B=A$, $A-B=\Phi$.

例 1 设 A 为全体有理数的集合,即 $A=\mathbf{Q}$, B 为全体无理数的集合,则 $A\cup B=\mathbf{R}$, $A\cap B=\Phi$.

例 2 设 $A=\{1,2,3,4\}$, $B=\{0,1,2\}$,则:

$$A\cup B=\{0,1,2,3,4\}$$
$$A\cap B=\{1,2\}$$
$$A-B=\{3,4\}$$
$$B-A=\{0\}$$

注意:$\{0\}$ 与 Φ 是两个不同的集合. $\{0\}$ 是单独一个数 0 作成的集合,0 是这个集合的元素.

而 Φ 是不含任何元素的集合.

在研究一个特定的问题时,所有的集合往往都是一个足够大的集合 V 的子集.我们称 V 为**万有集合**(即通常所说的**全集**,记作 I).V 与集合 A 的差集 $V-A$ 称为 A 的**补集**,记作 $\bar{A}$,即 $\bar{A}=V-A$.

集合的运算有以下**性质**(算律):

幂等律	$A\cup A=A,A\cap A=A$
交换律	$A\cup B=B\cup A,A\cap B=B\cap A$
结合律	$(A\cup B)\cup C=A\cup(B\cup C)$
	$(A\cap B)\cap C=A\cap(B\cap C)$
分配律	$A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$
	$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$
基元律	$A\cup\Phi=A,A\cap V=A$
补元律	$A\cup\bar{A}=V,A\cap\bar{A}=\Phi$

根据集合相等的定义,要证集合 A 与 B 相等,只要证 $A\subseteq B$ 与 $B\subseteq A$.这就是所谓用"双包含"的方法来证明集合相等.教材 p.3 中用这种方法证明了并对交的分配律,请读者务必认真阅读.以上所列集合运算的性质均已得到验证,我们可以直接应用它们,推得集合运算的一些其它结果.

例 3 证明集合的运算有**吸收律**:

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

证明 只证前一个等式:

$$\begin{aligned}
&A\cup(A\cap B)\\
&=(A\cap V)\cup(A\cap B) && \text{(基元律)}\\
&=A\cap(V\cup B) && \text{(分配律)}\\
&=A\cap(B\cup V) && \text{(交换律)}\\
&=A\cap[(B\cup V)\cap V] && \text{(基元律)}\\
&=A\cap[(B\cup V)\cap(B\cup\bar{B})] && \text{(补元律)}\\
&=A\cap[B\cup(V\cap\bar{B})] && \text{(分配律)}\\
&=A\cap[B\cup(\bar{B}\cap V)] && \text{(交换律)}\\
&=A\cap(B\cup\bar{B}) && \text{(基元律)}\\
&=A\cap V && \text{(补元律)}\\
&=A && \text{(基元律)}
\end{aligned}$$

(3)用集合论的观点来看中学数学的几个问题

①设 $f(x)=0$ 是一个代数方程,则它的所有解的集合称为它的解集合.解方程 $f(x)=0$ 通常要求它的全部解,实际上就是求出它的解集合.方程 $f(x)=0$ 无解,就是说它的解集合是空集.两个代数方程 $f(x)=0$ 与 $g(x)=0$ 同解的意义是:$f(x)=0$ 的每个解都是 $g(x)=0$ 的解,$g(x)=0$ 的每个解也是 $f(x)=0$ 的解.也就是说,这两个方程的解集合相等.

②在平面上取定直角坐标系.设曲线 l 上所有点的集合为 A,坐标满足方程 $f(x,y)=0$ 的所有点的集合为 B.证明曲线 l 的方程为 $f(x,y)=0$ 须证:曲线 l 上点的坐标都满足方程 $f(x,y)=0$,即 $A\subseteq B$;坐标满足方程 $f(x,y)=0$ 的点都在曲线 l 上,即 $B\subseteq A$.上述两个条件

恰好说明 $A=B$.

③数轴上的区间表示一些实数作成的集合,例如:

$$[0,1]=\{x \mid x\in\mathbf{R}, 0\leqslant x\leqslant 1\}$$

$$(-\infty,2)=\{x \mid x\in\mathbf{R}, x<2\}$$

由于实数与数轴上的点一一对应,每个区间也可以看作数轴上一些点的集合.例如$[0,1]$表示数轴上0,1之间,包括0,1的所有点的集合. $x\in[0,1]$, $[0,1]\cap(-\infty,2)$, $(-2,1)\cup[2,+\infty)$等符号有意义.用区间表示函数的定义域或不等式(组)的解往往很方便.

2.映射

集合的产生源于人们试图从整体上把握数学对象的需要,映射则提供了研究对象之间联系的手段.有关的主要概念如下:

映射 设 A,B 是两个集合.如果有一个规则 σ,使得 A 中每个元素 a 都对应着 B 中一个惟一确定的元素 b,则称 σ 是 A 到 B 的一个**映射**,记作 $\sigma: A\to B$.元素 a 对应着元素 b,记作 $a\mapsto b$或 $\sigma(a)=b$. b 称为 a 在 σ 下的**象**, a 称为 b 的**原象**.

例1 设 $A=B=\mathbf{Z}$, $\sigma: n\mapsto 2n$,则 σ 是 A 到 B 的映射.

例2 设 $A=\mathbf{R}$, B 是全体非负实数的集合, $\sigma: x\mapsto x^2$,则 σ 是 A 到 B 的映射.

例3 设 $A=B=\{1,2,3,4\}$, $\sigma: 1\mapsto 2, 2\mapsto 3, 3\mapsto 4, 4\mapsto 1$,则 σ 是 A 到 B 的映射.

例4 设 $A=\{a,b,c\}$, $B=\{1,2\}$.写出 A 到 B 的一切映射.

解 a 的象有两种选择.当 a 的象取定后, b 的象也有两种选择.当 a,b 的象都取定后, c 的象仍然有两种选择.根据排列组合的乘法原理 a,b,c 的象共有 $2\times2\times2=8$(种)选择,即 A 到 B 的映射一共有8个,它们是:

$$\sigma_1: a\mapsto 1, b\mapsto 1, c\mapsto 1$$

$$\sigma_2: a\mapsto 1, b\mapsto 1, c\mapsto 2$$

$$\sigma_3: a\mapsto 1, b\mapsto 2, c\mapsto 1$$

$$\sigma_4: a\mapsto 1, b\mapsto 2, c\mapsto 2$$

$$\sigma_5: a\mapsto 2, b\mapsto 1, c\mapsto 1$$

$$\sigma_6: a\mapsto 2, b\mapsto 1, c\mapsto 2$$

$$\sigma_7: a\mapsto 2, b\mapsto 2, c\mapsto 1$$

$$\sigma_8: a\mapsto 2, b\mapsto 2, c\mapsto 2$$

一般地,设 A,B 是两个集合, $|A|=n$, $|B|=m$,则 A 到 B 的映射一共有 m^n 个.

例5 设 A 是一个集合,规定 A 中任一元素的象是其本身,就得到了一个 A 到 A 的映射,将其记作 I_A,称 I_A 是集合 A 的**恒等映射**.

映射的相等 设 σ,τ 都是 A 到 B 的映射,若对任意 $a\in A$ 有 $\sigma(a)=\tau(a)$,则称 σ 与 τ **相等**,记作 $\sigma=\tau$.

映射的合成 设 σ 是 A 到 B 的映射, τ 是 B 到 C 的映射,规定 A 中任意元素 a 对应着 C 中的元素 $\tau(\sigma(a))$,就得到了一个 A 到 C 的映射.这个映射称为 τ 与 σ 的**乘积**,记作 $\tau\sigma$ 或 $\tau\cdot\sigma$.即:

$$\tau\sigma: A \to C,\ a \mapsto \tau(\sigma(a))$$

映射的合成具有以下**性质**：

(1)设 f 是 A 到 B 的映射，则：

$$fI_A = f,\ I_B f = f$$

(2)设 f 是 A 到 B 的映射，g 是 B 到 C 的映射，h 是 C 到 D 的映射，则

$$h(gf) = (hg)f$$

设 f,g 是两个映射，若 fg 有意义，未必 gf 有意义，即使二者都有意义也未必 $fg = gf$.

例 6 已知映射 $\sigma: \mathbf{R} \to \mathbf{R},\ x \mapsto x^2$，$\tau: \mathbf{R} \to \mathbf{R},\ x \mapsto \sin x$，则

$$\sigma\tau: \mathbf{R} \to \mathbf{R},\ x \mapsto \sin^2 x$$

$$\tau\sigma: \mathbf{R} \to \mathbf{R},\ x \mapsto \sin x^2$$

这里 $\sigma\tau \neq \tau\sigma$.

单射 设 σ 是 A 到 B 的映射，若 A 中不同的元素在 B 中有不同的象，则称 σ 为**单射**.

满射 设 σ 是 A 到 B 的映射，若 B 中每个元素都在 A 中有原象，则称 σ 为**满射**.

双射 既单又满的映射称为双射或一一映射.

可逆映射 设 σ 是 A 到 B 的映射，若存在 B 到 A 的映射 τ 使得

$$\tau\sigma = I_A,\ \sigma\tau = I_B$$

则称 σ 是一个**可逆映射**. 若 σ 可逆，则 σ 的逆映射是惟一的，记作 σ^{-1}.

映射 σ 可逆的充分必要条件是它为一一的.

任意两个集合之间未必可以建立一一映射，如果能够建立一一映射，则称这两个集合有相同的势(对于有限集来说，就是元素个数). 这方面的讨论参见教材第一章§2，这里不再详细叙述.

3. 置换

作为一种特殊的映射，置换在抽象代数的理论中起着重要作用. 本课程要求大家掌握与之相关的基本概念与运算.

置换 有限集$\{1,2,\cdots,n\}$到自身的双射 σ 称为 ***n* 元置换**，简称**置换**. 设 σ 把 1 变为 i_1，2 变为 i_2，…，n 变为 i_n，即：

$$\sigma(1) = i_1,\ \sigma(2) = i_2,\ \cdots,\ \sigma(n) = i_n$$

则 σ 可以表示为：

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$$

这里 $i_1\, i_2 \cdots\, i_n$ 是 $1,2,\cdots,n$ 的一个排列. 当 $i_1\, i_2 \cdots\, i_n$ 为奇排列时，σ 称为**奇置换**. 当 $i_1\, i_2 \cdots\, i_n$ 为偶排列时，σ 称为**偶置换**. 由于 n 个元素全排列的总数为 $n!$，故 n 元置换共 $n!$ 个. 其中一半是奇排列，一半是偶排列.

例 1 设5元置换 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$，在排列 2 3 1 5 4 中有 21，31，54 三个反序，故 2 3 1 5 4 是奇排列，从而 σ 是奇置换.

例 2 3元排列共 3! $=6$ 个，它们是：

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},$$

$$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}.$$

请读者自己判断一下这6个置换的奇偶性.

设 σ,τ 是两个 n 元置换,则:

$$\sigma\tau=\begin{pmatrix}1&2&\cdots&n\\\sigma\tau(1)&\sigma\tau(2)&\cdots&\sigma\tau(n)\end{pmatrix}$$

我们只要知道 $1,2,\cdots,n$ 中任一数字 k 先经过 τ,再经过 σ 变成什么数字,就可以把 $\sigma\tau$ 具体写出来.

例3 设 $\sigma=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\tau=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$,则:

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

从这个例子看出,置换的乘法没有交换律.

因为置换是双射,所以是可逆的.将置换 $\sigma=\begin{pmatrix}1&2&\cdots&n\\i_1&i_2&\cdots&i_n\end{pmatrix}$ 上、下两行数字对调,就得到了它的逆置换 $\sigma^{-1}=\begin{pmatrix}i_1&i_2&\cdots&i_n\\1&2&&n\end{pmatrix}$.

例4 设 $\sigma=\begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix}$,则:

$$\sigma^{-1}=\begin{pmatrix}3&2&4&1\\1&2&3&4\end{pmatrix}=\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}$$

σ^{-1}的上述两种表示方法都是对的,后者更符合我们的习惯.

不难得知,置换的逆有下列性质:

$$(\sigma^{-1})^{-1}=\sigma,(\sigma\tau)^{-1}=\tau^{-1}\sigma^{-1}$$

轮换 $A=\{1,2,\cdots,n\}$的一个把 i_1 变为 i_2, i_2 变为 $i_3,\cdots,i_{k-1}$ 变为 i_k, i_k 变为 i_1.而使 A 中其余数字不动的置换称为一个**轮换**,记作

$$(i_1\quad i_2\quad\cdots\quad i_k)$$

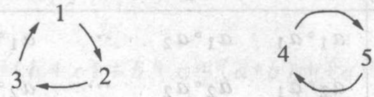
并称此轮换的长为 k.

定理1 每个置换都可以表示为若干个不相交(无共同数字)的轮换的乘积.

例5 设 $\sigma=\begin{pmatrix}1&2&3&4&5\\1&5&2&4&3\end{pmatrix}$,则 σ 把2变5,5变3,3变2,而使1,4不变,故 $\sigma=(2\quad 5\quad 3)$是长为3的轮换.

注意 σ 又可写成$(5\quad 3\quad 2)$或$(3\quad 2\quad 5)$.

例6 设 $\sigma=\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix}$.我们发现 σ 把1变2,2变3,3变1,并且4变5,5变4.图示如下:



σ 可表为两个不相交的轮换的乘积：$\sigma=(1\ 2\ 3)(4\ 5)$.

注意恒等置换 $I_A=\begin{pmatrix}1 & 2 & \cdots & n\\ 1 & 2 & \cdots & n\end{pmatrix}$，它可表示为 $I_A=(1)=(2)=\cdots=(n)$，它是长为 1 的轮换，通常将它记为(1).

对换 长为 2 的轮换 (ij) 称为**对换**.

例 7 设 $\sigma=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 4 & 3 & 2 & 5\end{pmatrix}$，则 $\sigma=(2\quad 4)$ 是一个对换.

定理 2 每个轮换都可以表示为若干个对换的乘积：

$$(i_1\ i_2\cdots\ i_k)=(i_1\ i_2)(i_2\ i_3)\cdots(i_{k-1}\ i_k)$$

从而每个置换都可以表示为若干个对换的乘积．并且奇(偶)置换只能表示为奇(偶)数个对换的乘积.

由此我们得知：

(1)轮换的奇偶性与它的长的奇偶性相反；

(2)两个奇(偶)置换的乘积是一个偶置换；

(3)一个奇(偶)置换与一个偶(奇)置换的乘积是一个奇置换.

轮换的奇偶性容易判断，求逆也比较容易，我们有公式：

$$(i_1\ i_2\cdots\ i_k)^{-1}=(i_k\cdots\ i_2\ i_1)$$

例 8 设 $\sigma=(1\ 3\ 4\ 5)(2\ 6\ 7)$，判断 σ 的奇偶性并求 σ^{-1}.

解 $\because(1\ 3\ 4\ 5)$ 是奇置换，$(2\ 6\ 7)$ 是偶置换.

$\therefore\sigma$ 是奇置换.

$$\sigma^{-1}=(2\ 6\ 7)^{-1}(1\ 3\ 4\ 5)^{-1}$$
$$=(7\ 6\ 2)(5\ 4\ 3\ 1)$$

(二) 代数体系

1. 代数运算

定义 设 A 是一个非空集合，则 $A\times A$ 到 A 的映射称为 A 的**代数运算**.

设“$\circ$”是 A 的一个代数运算，$A\times A$ 中的元素 (a,b) 在$\circ$下的象为 c，通常记作 $a\circ b=c$．这就和我们作数字运算时的算式 $2\times6=12$，$3+5=8$ 等等在写法上一致起来．由定义看出，若$\circ$是 A 的代数运算，则：

(1)对任意 $a,b\in A$，$a\circ b$ 有意义，即 A 中任意两个元素都可以作运算；

(2)当 a,b 取定后，$a\circ b$ 是 A 中惟一确定的元素，即运算的结果是 A 中惟一确定的元素.

需要指出的是，若 $a,b\in A$，$a\neq b$，则在 $A\times A$ 中 $(a,b)\neq(b,a)$，故一般来说，$a\circ b$ 与 $b\circ a$ 未必相等.

有限集 $A=\{a_1,a_2,\cdots,a_n\}$ 的代数运算$\circ$可以用运算表来表示：

$\circ$	a_1	a_2	$\cdots$	a_n
a_1	$a_1\circ a_1$	$a_1\circ a_2$	$\cdots$	$a_1\circ a_n$
a_2	$a_2\circ a_1$	$a_2\circ a_2$	$\cdots$	$a_2\circ a_n$
$\vdots$	$\vdots$	$\vdots$		$\vdots$
a_n	$a_n\circ a_1$	$a_n\circ a_2$	$\cdots$	$a_n\circ a_n$

在表中 a_i 所在的行与 a_j 所在的列的交叉处填写 $a_i\circ a_j$，它应是 A 中的一个元素.

在具体问题中，往往要对所讨论的代数运算提出一些要求.最常见的是结合律、交换律和分配律.

定义 设$\circ$是集合 A 的一个代数运算.若对任意 $a,b,c\in A$ 有

$$(a\circ b)\circ c=a\circ(b\circ c)$$

则称$\circ$满足**结合律**.

若 A 的代数运算$\circ$满足结合律，则 A 中任意 n 个元素 $a_1,a_2,\cdots,a_n$ 作运算

$$a_1\circ a_2\circ\cdots\circ a_n$$

用各种方法加括号所得结果相同，因而可以不加括号.

定义 设$\circ$是集合 A 的代数运算.若对任意 $a,b\in A$ 有

$$a\circ b=b\circ a$$

则称$\circ$满足**交换律**.

定义 设$\circ$，$\oplus$是集合 A 的两个代数运算.对任意 $a,b,c\in A$

(1)若 $a\circ(b\oplus c)=(a\circ b)\oplus(a\circ c)$，则称$\circ$对$\oplus$满足**左分配律**.

(2)若$(b\oplus c)\circ a=(b\circ a)\oplus(c\circ a)$，则称$\circ$对$\oplus$满足**右分配律**.

当$\circ$适合交换律时，上述两个分配律等价，即可以互推.在算术里，我们只说乘法对加法有分配律，而不提左、右分配律，就是这个道理.

若$\circ$对$\oplus$满足左、右分配律，且$\oplus$适合结合律，则可用数学归纳法证明对任意的 $b_1,b_2,\cdots,b_n\in A$ 有：

$$a\circ(b_1\oplus b_2\oplus\cdots\oplus b_n)=(a\circ b_1)\oplus(a\circ b_2)\oplus\cdots\oplus(a\circ b_n)$$
$$(b_1\oplus b_2\oplus\cdots\oplus b_n)\circ a=(b_1\circ a)\oplus(b_2\circ a)\oplus\cdots\oplus(b_n\circ a)$$

例 1 对整数集 $\mathbf{Z}$ 定义代数运算$\circ$如下：

$$a\circ b=b\quad(\forall\, a,b\in\mathbf{Z})$$

加法为普通的加法，则

(1)$\circ$有结合律

(2)$\circ$没有交换律

(3)$\circ$对$+$有左分配律

(4)$\circ$对$+$没有右分配律

证明 (1)$\forall\, a,b,c\in\mathbf{Z}$，因为

$$(a\circ b)\circ c=c,\ a\circ(b\circ c)=a\circ c=c$$

所以$(a\circ b)\circ c=a\circ(b\circ c)$，即$\circ$有结合律.

(2)$\because 1\circ2=2,2\circ1=1$