高等师范学校教材

高观点下的中学数学

代数学

Algebra

王仁发 编著

- 代数运算与自然数
- 不等式
- 多项式与环
- 数论初步
- 排列组合与几何难题
- 伽罗华理论*

高等教育出版社

高等师范学校教材

《分析学》…… 高　夯

《代数学》…… 王仁发

《几何学》…… 于祖焕

ISBN 7-04-010298-6

9 787040 102987 >

定价:11.80元

高观点下的中学数学

代　数　学

王仁发　编著

高等教育出版社

图书在版编目(CIP)数据

代数学／王仁发编.—北京：高等教育出版社；2001
(高观点下的中学数学)
ISBN 7-04-010298-6

Ⅰ.代… Ⅱ.王… Ⅲ.代数－中学－师资培训－自学参考资料 Ⅳ.015

中国版本图书馆 CIP 数据核字 (2001) 第 048596 号

责任编辑 钱正英　**特约编辑** 陈亚
封面设计 吴　昊　**版式设计** 杨歆颖
责任印制 潘文瑞

出版发行	高等教育出版社	**购书热线**	010-58581118
社　　址	北京市西城区德外大街 4 号		021-56964871
邮政编码	100011	**免费咨询**	800-810-0598
总　　机	010-58581000	**网　　址**	http://www.hep.edu.cn
传　　真	021-56965341		http://www.hep.com.cn
			http://www.hepsh.com
经　　销	蓝色畅想图书发行有限公司	**网上订购：**	http://www.landraco.com
			http://www.landraco.com.cn
印　　刷	上海三印时报印刷有限公司	**畅想教育：**	http://www.widedu.com
开　　本	850 × 1168　1/32	**版　　次**	2001 年 7 月第 1 版
印　　张	6.375	**印　　次**	2006 年 4 月第 3 次
字　　数	163 000	**定　　价**	11.80 元

凡购买高等教育出版社图书，如有缺页、倒页、脱页等质量问题，请在所购图书销售部门联系调换。

物料号　10298-00

《高观点下的中学数学》丛书
编 委 会

前 言

代数、分析、几何是数学的核心内容.无论是远古时期，还是近现代，数学这棵根深叶茂的大树就是以分析、代数、几何为其主干.一方面，随着时间的推移，现代数学的内容在不断地发展，另一方面，现代数学的思想又在不断地渗透到经典数学的研究中.如何用现代数学的知识来充实自己，用高等数学的观点去理解初等数学的内容，从而提高自己的数学素养，并进一步指导中学数学的教学工作，这是每一位高等师范院校数学系学生与中学数学教师面临的问题.只有很好地解决了这个问题，才能在现在或将来的中学数学教学中，真正做到居高临下，游刃有余.

1997 年，东北师范大学数学系承担了教育部的“高等师范教育面向 21 世纪教学内容和课程体系改革”项目.与此同时，东北师范大学推出了“优师工程”.在此项目与工程的推动下，我们重新修订了我系的课程设置方案.在新的培养方案中，确定了“两个阶段，1＋3 个模块”的课程结构体系，即将学生四年的学习过程分为必修课学习阶段与选修课学习阶段.课程设置方案分为一个必修课的大模块，三个选修课的小模块.三个选修课的小模块之一是中学数学教育系列课程模块.这套丛书中的“分析学”、“代数学”、“几何学”就是为这个模块准备的系列教材.

2000 年，教育部又推出了“园丁工程”.这一工程旨在对本科毕业后的中学教师进行继续教育.东北师大数学系先后举办过中学数学教师继续教育培训班.在培训班上，我

们开设了“分析专题研究”、“代数专题研究”、“几何专题研究”等课程.

这本代数学,是在几年来相应课程的讲稿基础上整理而成的.在讲义的整理过程中,我们认真听取了我系张永正教授、南基洙教授以及一些中学教师的意见.他们的宝贵意见,使本书增色不少.同时,东北师范大学数学系对本书给予了大力的支持.高等教育出版社的郭立伟编审也为本书的出版付出了辛勤的劳动.在这里,对于给予本书支持与帮助的各位同志一并表示感谢.

我们不能说这是一套完美的教材,但我们相信大多数读者对这套丛书会有新鲜的感觉.阅读这套丛书,不需要高深的现代数学知识,但需要有一定的数学修养.

应该说,这套丛书是在没有成型的教材可模仿,在摸索的过程中编写而成的.由于编者水平所限,不妥之处在所难免,希望读者批评指正.

作 者

目　　录

* 为选学内容.

第一章　代数运算与自然数

§1　集合与映射

一、集合

集合是数学中最基本的概念，它已深入到各种科学与技术领域中，特别是应用于数学的各个分支中.

“集合”严格地说是没有定义的词，而通常所说的“具有某些性质的物体的总体称之为**集合**”，仅仅是对集合的一种描述. 集合中的每一个个体我们称之为集合中的**元素**. 一般地，我们用大写拉丁字母 $A,B,C,\cdots$ 表示集合，小写拉丁字母 $a,b,c,\cdots$ 表示集合中的元素.

若元素 a 属于集合 A，则记为 $a\in A$；若元素 a 不属于集合 A，则记为 $a\notin A$. 如果集合 B 中每一个元素均属于集合 A，则称**集合 B 属于集合 A**，或者称集合 B 是集合 A 的**子集合**，记为 $B\subseteq A$；如果 $B\subseteq A$，且 A 中至少存在一个元素 a，使得 $a\notin B$，则称 B 是 A 的**真子集合**，记为 $B\subset A$.

定义 1.1　如果集合 B 中每一个元素都属于集合 A，而集合 A 中每一个元素又都属于集合 B，即 $B\subseteq A$，$A\subseteq B$，则称**集合 A 等于集合 B**，记为 $A=B$.

显然集合的相等是等价关系，即

1. 自反性　$A=A$.

2. 对称性　若 $A=B$，则 $B=A$.

3. 传递性　若 $A=B$，$B=C$，则 $A=C$.

下面给出一些集合的例子.

(1) 所有自然数的集合，一般地用 **N** 表示.

(2) 所有有理数的集合，一般地用 **Q** 表示.

(3) $A=\{a,b,c\}$，a,b,c 是集合 A 中元素.

(4) 所有整数的集合，一般地用 **Z** 表示.

(5) 所有偶数的集合可表示为 $B=\{2r \mid r\in \mathbf{Z}\}$.

这里要特别指出的是，不含有任何元素的集合也是集合，称之为**空集合**，用 $\varnothing$ 表示. 空集合 $\varnothing$ 是任何集合的子集合.

集合 A 所含有的元素个数我们用 $|A|$ 表示. 例如，若 $A=\{a,b,c\}$，则 $|A|=3$.

若 $A,B,\cdots$ 是一些集合，把它们放在一起构成一个新的集合 $\{A,B,\cdots\}$，这种集合是以集合作为元素，称之为**集族**.

一个集合的全部子集所构成的集族称为该集合的**幂集**. 例如，$A=\{a,b,c\}$，则 A 的幂集合是由 8 个元素所构成：$\{\varnothing,\{a\},\{b\},\{c\},\{a,b\},\{a,c\},\{b,c\},\{a,b,c\}\}$.

定理 1.1　如果 A 是有限集合，$P(A)$ 是集合 A 的幂集，则 $|P(A)|=2^{|A|}$.

证明　若集合 A 有 n 个元素，则由 A 中 k 个元素所构成的子集合共有 C_n^k 个，这里 k 可从 0 取到 n，所以 A 的所有子集的个数为

$$C_n^0+C_n^1+\cdots+C_n^n=2^n,$$

即
$$|P(A)|=2^{|A|}.$$

若 A 与 B 是两个非空集合，则所有的有序对 (a,b)，$a\in A$，$b\in B$ 所构成的集合称为 A 与 B 的**积集**，记为 $A\times B$.

两个集合的积集显然可以推广为 3 个，$\cdots$，n 个集合的积集，$A_1\times A_2\times\cdots\times A_n$ 是由有序元素组 $(x_1,x_2,\cdots,x_n)$ 所构成，这里 $x_1\in A_1$，$x_2\in A_2,\cdots,x_n\in A_n$.

显然积集 $A_1\times A_2\times\cdots\times A_n$ 中两个元素 $(x_1,x_2,\cdots,x_n)$，$(y_1,y_2,\cdots,y_n)$ 相等的充分必要条件是 $x_1=y_1,x_2=y_2,\cdots,x_n=y_n$.

如果集合 A 与 B 都是有限集合，即 $|A|=n$，$|B|=m$，则

$$|A\times B|=|A|\times|B|=n\times m.$$

二、集合的运算

定义 1.2 集合 A 与 B 的并集 $A\cup B$、交集 $A\cap B$、差集 $A-B$ 分别定义为

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

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

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

在研究一个特定问题时，所有的集合 A 往往都属于一个足够大的集合 V，我们称它为**万有集合**，这时称 $V-A$ 为集合 A 的**补集**，用 $\overline{A}$ 表示，即 $\overline{A}=V-A$.

例如，若集合 $A=\{1,2,3\}$，$B=\{2,3,4\}$，则

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

如果万有集合 $V=\{1,2,3,4,5\}$，则

$$\overline{A}=\{4,5\},\overline{B}=\{1,5\}.$$

对于集合的运算显然有如下性质：

(1) $A\cup B=B\cup A$，

$A\cap B=B\cap A$.

(2) $(A\cup B)\cup C=A\cup(B\cup C)$，

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

(3) $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$.

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

(5) $A\cup\overline{A}=V$，$A\cap\overline{A}=\varnothing$.

(6) 若 $A\subseteq B$，则 $A\cup B=B$.

若 $A\subseteq B$，则 $A\cap B=A$.

上述性质我们仅证明(3)：

若 $a\in(A\cup B)\cap(A\cup C)$，则

$$a\in A\cup B\text{ 且 }a\in A\cup C.$$

如果 $a \in A$,则 $a \in A \cup (B \cap C)$.

如果 $a \notin A$,则必有 $a \in B$ 且 $a \in C$,即 $a \in B \cap C$,$a \in A \cup (B \cap C)$.

所以无论怎样均有 $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.

另一方面,若 $a \in A \cup (B \cap C)$,则

或者 $a \in A \Rightarrow a \in (A \cup B) \cap (A \cup C)$,

或者 $a \in B \cap C \Rightarrow a \in (A \cup B) \cap (A \cup C)$,

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

由此 $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

三、映射

定义 1.3 设 A 和 B 是任意两个集合. 如果有一个确定的规则(或法则)σ,使集合 A 中每一个元素 a 都对应到集合 B 中一个唯一确定的元素 b,则称这个规则 σ 为从集合 A 到集合 B 的一个**映射**,表示为 $\sigma: A \longrightarrow B$ 或 $A \xrightarrow{\sigma} B$.

定义 1.4 如果元素 $a \in A$ 经过映射 σ 变成元素 $b \in B$,则记为 $\sigma(a) = b$,这时我们称 b 为 a 在映射 σ 下的**象**,称 a 为 b 的**原象**.

从映射的定义可知,A 中每一个元素都有象,且象是唯一的,但 B 中并不是每一个元素都有原象. 如果 A 和 B 是通常数的集合,那么从集合 A 到 B 的映射就是通常的函数,所以映射的概念是函数概念的推广.

定义 1.5 $\sigma: A \longrightarrow B$,集合 A 的全部元素在映射 σ 下的全体象所构成的集合称为 σ 的**值域**,记为 $Im(\sigma)$,显然

$$Im(\sigma) = \{\sigma(a) \mid a \in A\}.$$

定义 1.6 若 $\sigma: A \longrightarrow B$, $\tau: A \longrightarrow B$,如果对集合 A 中任意元素 a,均有 $\sigma(a) = \tau(a)$,则称映射 σ 与 τ **相等**,记为 $\sigma = \tau$.

例 1 设 $A = \{a_1, a_2, a_3, a_4\}$,$B = \{b_1, b_2, b_3\}$,若 $\sigma(a_1) = b_2$,$\sigma(a_2) = b_2$,$\sigma(a_3) = b_1$,$\sigma(a_4) = b_1$,则 σ 是 A 到 B 的映射,$Im(\sigma) =$

$\{b_1, b_2\}$.

若 $\sigma(a_1)=b_1, \sigma(a_1)=b_2, \sigma(a_2)=b_2, \sigma(a_3)=b_3, \sigma(a_4)=b_3$，则 σ 不是 A 到 B 的映射，因为 $\sigma(a_1)$ 的象不是唯一的.

若 $\sigma(a_1)=b_1, \sigma(a_2)=b_2, \sigma(a_3)=b_3$，则 σ 也不是 A 到 B 的映射，因为元素 a_4 没有象.

从定义 1.6 我们知道，从集合 A 到集合 B 的映射，在怎样的情况下才是相等的. 那么从集合 A 到集合 B 可以定义多少个不同的映射？请看下面的定理.

定理 1.2 从有限集合 A 到有限集合 B 的映射共有 $|B|^{|A|}$ 个.

证明 设 A 有 n 个元素，$A=\{a_1, a_2, \cdots, a_n\}$，$B$ 有 m 个元素，$B=\{b_1, b_2, \cdots, b_m\}$，$\sigma$ 是从 A 到 B 的映射，则 $(\sigma(a_1), \sigma(a_2), \cdots, \sigma(a_n))$ 就是映射 σ 的表示，这里 $\sigma(a_1)$ 有 m 种选择，$\sigma(a_2)$ 也有 m 种选择，$\cdots$，$\sigma(a_n)$ 还有 m 种选择，显然一共有 m^n 种选择，即从 A 到 B 的不同映射共有 $m^n=|B|^{|A|}$ 个.

例 2 令 $A=\{a_1, a_2\}$，$B=\{b_1, b_2, b_3\}$，从集合 A 到集合 B 的所有不同映射共有 $|B|^{|A|}=3^2=9$ 个，它们是：

	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8	σ_9
a_1	b_1	b_1	b_1	b_2	b_2	b_2	b_3	b_3	b_3
a_2	b_1	b_2	b_3	b_1	b_2	b_3	b_1	b_2	b_3.

而从集合 B 到集合 A 的所有不同映射共有 $|A|^{|B|}=2^3=8$ 个，它们是：

	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6	τ_7	τ_8
b_1	a_1	a_2	a_1	a_2	a_1	a_2	a_1	a_2
b_2	a_1	a_1	a_2	a_2	a_1	a_1	a_2	a_2
b_3	a_1	a_1	a_1	a_1	a_2	a_2	a_2	a_2.

定义 1.7 设 $\sigma: A \longrightarrow A$，若对 A 中任意元素 a，均有 $\sigma(a)=a$，则称 σ 为集合 A 上的**恒等映射**，记为 $\sigma=I_A$.

定义 1.8 设 $\sigma: A \longrightarrow B$，若 $Im(\sigma)=B$，则称 σ 为**满射**. 若由 a_1

$\neq a_2 \Rightarrow f(a_1) \neq f(a_2)$，则称 σ 为**单射**. 如果 $\sigma: A \longrightarrow B$ 即是单射，又是满射，则称 σ 为**双射**（或一一映射）

映射的合成　如果 $\sigma: A \longrightarrow B$，$\tau: B \longrightarrow C$，那么连续执行两次 σ 与 τ 的映射，它的总效果就是把集合 A 中元素 a 映到集合 C 的元素 c. 这就构成了一个从 A 到 C 的映射，记为 $\tau \circ \sigma$，（或者称 τ 与 σ 的乘积简记为 $\tau\sigma$）. 具体规定如下：

$$\tau \circ \sigma(a) = \tau(\sigma(a)).$$

如果 A, B, C 都是通常的数的集合，σ 与 τ 就都是函数，$\tau \circ \sigma$ 就是复合函数.

例如，若 $A = B = C$ 为实数集合，$\sigma(x) = x^2$，$\tau(x) = e^x$，则 $\varpi(x) = e^{x^2}$.

如果 $\sigma: A \longrightarrow B$，若存在一个 $\tau: B \longrightarrow A$，使得 $\varpi = I_A$，$\sigma\tau = I_B$，则称 σ 是**可逆映射**，τ 为 σ 的**逆映射**，记为 $\tau = \sigma^{-1}$.

显然 σ 是可逆映射的充要条件为 σ 是从 A 到 B 的双射.

四、置换

下面简单介绍一下置换知识，它在伽罗华理论中起重要作用，有关定理不加严格证明.

如果 A 是有限集合，则由 A 到 A 的双射称为 A 上的**置换**. 特别是当 $A = \{1, 2, \cdots, n\}$ 时，则 A 中的置换 σ 可表示成

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

例如，若 $A = \{1, 2, 3\}$，则 A 中所有置换为

$$\sigma_1 = \begin{pmatrix} 1\ 2\ 3 \\ 1\ 2\ 3 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1\ 2\ 3 \\ 1\ 3\ 2 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1\ 2\ 3 \\ 2\ 1\ 3 \end{pmatrix},$$

$$\sigma_4 = \begin{pmatrix} 1\ 2\ 3 \\ 2\ 3\ 1 \end{pmatrix}, \quad \sigma_5 = \begin{pmatrix} 1\ 2\ 3 \\ 3\ 1\ 2 \end{pmatrix}, \quad \sigma_6 = \begin{pmatrix} 1\ 2\ 3 \\ 3\ 2\ 1 \end{pmatrix}.$$

置换 $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & & \sigma(n) \end{pmatrix}$ 的逆置换为

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

例如，$\sigma=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$，则 $\sigma^{-1}=\begin{pmatrix}3 & 1 & 2\\ 1 & 2 & 3\end{pmatrix}=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$.

置换 $\sigma=\begin{pmatrix}1 & 2 & 3 & \cdots & n\\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n)\end{pmatrix}$，

若排列 $\sigma(1),\sigma(2),\cdots,\sigma(n)$ 为奇排列，则称 σ 为**奇置换**；若 $\sigma(1),\sigma(2),\cdots,\sigma(n)$ 为偶排列，则称 σ 为**偶置换**.

关于置换的合成可见下例：

$$\sigma_6\circ\sigma_2=\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}=\sigma_5$$

即 $1\to1\to3$，　$2\to3\to1$，　$3\to2\to2$.

定义 1.9　设 $a_1,a_2,\cdots,a_r$ 是集合 $A=\{a_1,a_2,\cdots,a_n\}$ 的 $r(r\leqslant n)$ 个不同元素，σ 是 A 上的置换，它使 $\sigma(a_1)=a_2,\sigma(a_2)=a_3,\cdots\sigma(a_{r-1})=a_r,\sigma(a_r)=a_1$，对于 A 中其他元素 a 均有 $\sigma(a)=a$，这时我们称 σ 为长是 r 的**轮换**，记为

$$\sigma=\begin{pmatrix}a_1 & a_2 & \cdots & a_r\\ a_2 & a_3 & \cdots & a_1\end{pmatrix}=(a_1\quad a_2\quad\cdots\quad a_r).$$

不难看出，$(a_1\ a_2\cdots a_r)=(a_2\ a_3\cdots a_r\ a_1)=\cdots=(a_r\ a_1\ a_2\cdots a_{r-1})$，且称 $a_1,a_2,\cdots,a_r$ 为轮换 σ 的**可搬动的元素**.

如果两个轮换 σ 与 τ 没有共同可搬动的元素，则称这样的两个轮换是**不相交的轮换**.

定理 1.3　每一个轮换可写成若干个不相交的轮换的乘积.

例如，$\sigma=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 3 & 1 & 5 & 4\end{pmatrix}=(1\ 2\ 3)(4\ 5)$.

只含有两个数码的轮换 $(i\ j)$ 称为**对换**.

如果　$\sigma=\begin{pmatrix}1 & 2 & i & \cdots & j & \cdots & n\\ a_1 & a_2 & a_i & \cdots & a_j & \cdots & a_n\end{pmatrix}$，$\tau=(i\ j)$，则

$$\sigma\tau = \begin{pmatrix} 1 & 2 & i & \cdots j & \cdots & n \\ a_1 & a_2 & a_i & \cdots a_j & \cdots & a_n \end{pmatrix} \cdot (i\ j)$$

$$= \begin{pmatrix} 1 & 2 & i & \cdots & j & \cdots & n \\ a_1 & a_2 & a_j & \cdots & a_i & \cdots & a_n \end{pmatrix}.$$

显然 σ、τ 把置换 σ 的第二行数码 a_i 与 a_j 交换，而其余字码不动，所以我们有如下定理.

定理 1.4　任何一个置换乘一个对换后所得新的置换与原置换奇偶性相反.

任何一个轮换可以表示成若干个对换的乘积.

实际上，

$$(a_1 a_2 \cdots a_r) = (a_1 a_r)(a_1 a_{r-1})(a_1 a_{r-2})\cdots(a_1 a_2)$$

所以，我们有：

定理 1.5　任何一个置换都能分解成若干个对换的乘积.

奇置换只能分解成奇数个对换的乘积.

偶置换只能分解成偶数个对换的乘积.

n 个数码的所有 $n!$ 个置换构成一个乘法群，而所有偶置换则构成置换群的子群.

§2*　有限集合与无限集合

一般地说，一个集合的元素个数如果是有限的则称它为有限集合，否则称为无限集合. 但什么是“有限”，什么又是“无限”呢. 下面我们给出它的严格定义.

定义 2.1　如果两个集合 A 与 B 之间存在一个一一映射 σ：$A \longrightarrow B$，则称这两个集合是**等价**的，并称它们具有相同的**势**.

对于自然数 **N** 的一部分集合 $\{1,2,\cdots,n\}$，我们称它为自然数集合的一个**片断**，并用 $|1,n|$ 表示.

定义 2.2　与自然数的一个片断 $|1,n|$ 等价的集合 A，称为**有限**