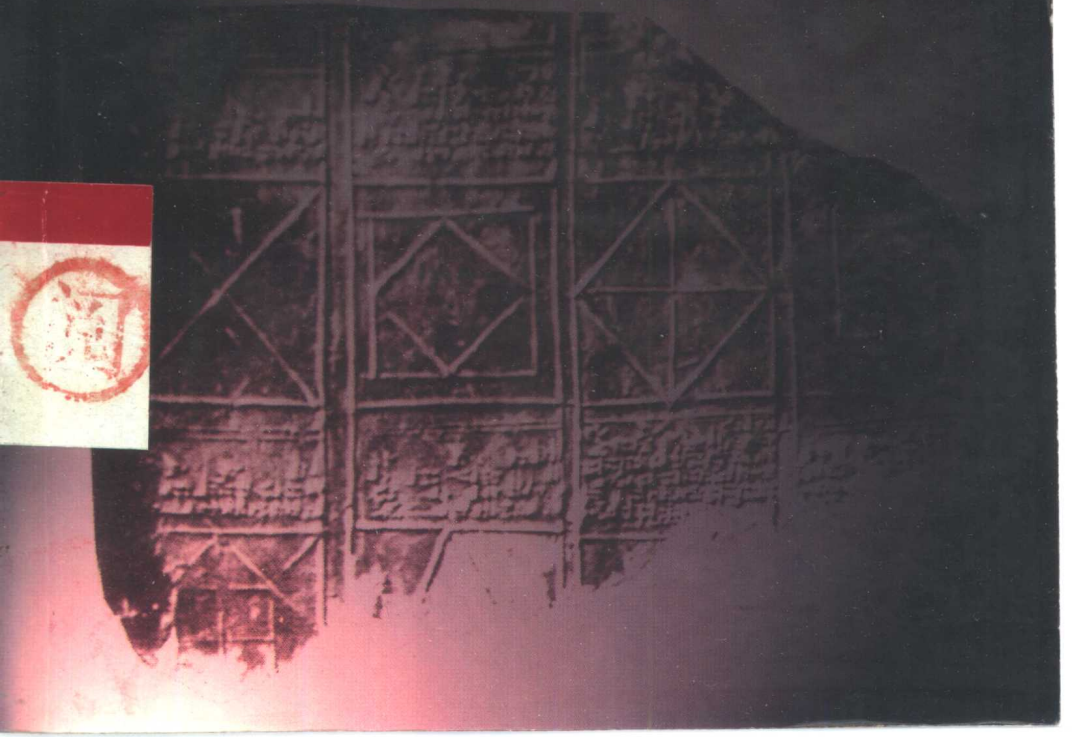
第2版

应用近世代数

胡冠章 编著

清华大学出版社



应用近世代数

（第2版）

胡冠章 编著

清华大学出版社

(京)新登字 158 号

内 容 提 要

近世代数(又名抽象代数)是现代数学的重要基础,在计算机科学、信息科学、近代物理与近代化学等方面有广泛的应用,是从事现代科学技术人员所必需的数学基础。本书介绍群、环、域的基本理论与应用。适用于数学与应用数学、计算机科学、无线电、物理、化学、生物医学等专业的学生、研究生以及专业人员。

图书在版编目(CIP)数据

应用近世代数/胡冠章编著. —2 版. —北京:清华大学出版社,1999

ISBN 7-302-03264-5

Ⅰ. 应… Ⅱ. 胡… Ⅲ. 抽象代数 Ⅳ. 0153

中国版本图书馆 CIP 数据核字(98)第 37310 号

出版者:清华大学出版社(北京清华大学校内,邮编 100084)

http://www.tup.tsinghua.edu.cn

印刷者:北京市密云胶印厂

发行者:新华书店总店北京发行所

开 本:850×1168 1/32 印张:8.125 字数:211 千字

版 次:1999 年 2 月第 2 版 1999 年 2 月第 2 次印刷

书 号:ISBN 7-302-03264-5/O・206

印 数:0001～4000

定 价:10.00 元

前　言

为了满足数学与应用数学以及理工科专业学生和科技人员学习近世代数的需要，本书尽力做到联系实际，多举例子，使读者感到有趣想学。在叙述方法上尽力做到连贯、前后呼应、合乎中文习惯。对部分定理的证明采用提示式、部分论证式等方式给出，留有思考余地，读者若能边学边动手按提示完成证明或计算，会收到满意效果。每节后的习题均附有提示或答案，便于自学。

本书出版后受到读者的欢迎，并得到同行的好评和支持，荣获国家教委第三届高校优秀教材二等奖。本次再版时，根据读者和同行的意见与建议做了修改与补充。在此，作者向所有给予本书关心、支持与提供宝贵意见的读者、同行和编辑表示衷心的感谢。

目　录

第 1 章　引言和预备知识

1.1　几类实际问题

初等代数、高等代数和线性代数都称为**经典代数**(classical algebra)，它的研究对象主要是代数方程和线性方程组。**近世代数**(modern algebra)又称为**抽象代数**(abstract algebra)，它的研究对象是代数系，所谓代数系，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。例如，整数集合 $\mathbf{Z}$，和普通的整数加法“+”构成一个代数系，记作$(\mathbf{Z},+)$。$\mathbf{Z}$ 和普通加法“+”以及普通乘法“·”两种运算也构成一个代数系，记作$(\mathbf{Z},+,\cdot)$。

由于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重要应用，因而它是现代科学技术的数学基础之一，许多科技人员都希望掌握它的基本内容与方法。本书将以一些实际问题为背景，在初等代数和线性代数的基础上，由浅入深地介绍它的基本内容，使读者感到通俗易懂，饶有兴趣。下面介绍几类与近世代数的应用有关的实际问题。

1. 项链问题

这个问题的提法是：用 n 种颜色的珠子做成有 m 颗珠子的项链，问可做成多少种不同类型的项链？

首先需要对此问题作数学上的确切描述。设由 m 颗珠子做成一个项链，可用一个正 m 边形来代表它，每个顶点代表一颗珠子。从任意一个顶点开始，沿逆时针方向，依次给每个顶点标以号码：$1,2,\cdots,m$。这样的一个项链称之为有标号的项链。由于每一颗珠子的颜色有 n 种选择，因而由乘法原理，这些有标号的项链共有 n^m 种。但是其中有一些项链可通过旋转一个角度或翻转 180°使它们完全重合。对于这些项链，称它们本质上是相同的。对那些无论怎样旋转或翻转都不能使它们重合的项链，称之为本质上不同的项链，即为问题所提的不同类型的项链。当 n 与 m 较小时，不难用枚举法求得问题的解答，读者不妨自行解决以下例子。

例 1 用黑、白 2 种颜色的珠子做成有 5 颗珠子的项链，问可以做成多少种不同类型的项链？

随着 n 与 m 的增加，用枚举法越来越困难，因而必须寻找更加有效的可解决一般的任意正整数 n 与 m 的方法。采用群论方法可完全解决此问题，且至今尚未发现其它更为简单和有效的方法。

2. 分子结构的计数问题

在化学中研究由某几种元素可合成多少种不同物质的问题，由此可以指导人们在大自然中寻找或人工合成这些物质。

例 2 在一个苯环上结合 H 原子或 CH_3 原子团，问可能形成多少种不同的化合物（见图 1.1(a)）？

如果假定苯环上相邻 C 原子之间的键都是互相等价的，则此问题就是两种颜色 6 颗珠子的项链问题。

3. 正多面体着色问题

对一个正多面体的顶点或面用 n 种颜色进行着色，问有多少种不同的着色方法？

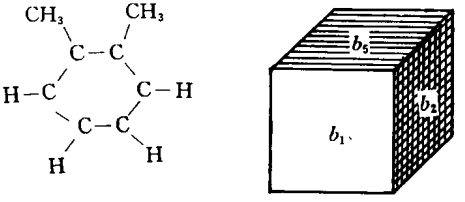


图 1.1

下面以正六面体为例说明此问题的数学描述。

例 3 用 n 种颜色对正六面体的面着色，问有多少种不同的着色方法(图 1.1(b))？

首先建立此问题的数学模型，将问题中的一些概念给以量化。

设 n 种颜色的集合为

$$A = \{a_1, a_2, \cdots, a_n\},$$

正六面体的面集合为

$$B = \{b_1, b_2, b_3, b_4, b_5, b_6\},$$

则每一种着色法对应一个映射：

$$f: B \to A,$$

反之，每一个映射 $f: B \to A$ 对应一种着色法。由于每一个面的颜色有 n 种选择，所以全部着色法的总数为 n^6，但这样的着色法与面的编号有关，其中有些着色法可适当旋转正六面体使它们完全重合，对这些着色法，称它们为本质上是相同的。我们的问题是求本质上不同的着色法的数目。

当 n 很小时不难用枚举法求得结果，例如，当 $n=2$ 时，读者可以自己算出本质上不同的着色法数为 10，对于一般的情况则必须用群论方法才能解决。

4. 图的构造与计数问题

首先让我们介绍一下**图论**(graph theory)的一些基本概念。

设 $V=\{v_1,v_2,\cdots,v_n\}$,称为**顶点**集合(vertex set),E 是由 V 的一些 2 元子集构成的集合,称为**边集**(edge set),则有序对:(V,E)称为一个**图**(graph),记作 $G=(V,E)$。

例如,设 $V=\{1,2,\cdots,10\}$,$E=\{e_1,e_2,\cdots,e_{15}\}$,其中 $e_1=\{1,2\}$,$e_2=\{2,3\}$,$e_3=\{3,4\}$,$e_4=\{4,5\}$,$e_5=\{1,5\}$,$e_6=\{1,6\}$,$e_7=\{2,7\}$,$e_8=\{3,8\}$,$e_9=\{4,9\}$,$e_{10}=\{5,10\}$,$e_{11}=\{6,8\}$,$e_{12}=\{7,9\}$,$e_{13}=\{8,10\}$,$e_{14}=\{6,9\}$,$e_{15}=\{7,10\}$。图 $G=(V,E)$可用图 1.2 来表示。此图是图论中有名的彼得松(Petersen)图。每一个顶点用圆圈表示,对边集 E 中的每一个元素$\{i,j\}\in E$,用一条直线或曲线连接顶点 i 与 j。顶点的位置及边的长短,形状均无关紧要。

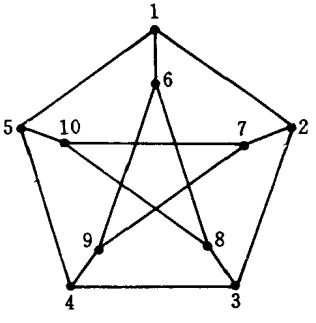


图 1.2

一个图可以代表一个电路,水网络,通信网络,交通网络,地图等有形的结构,也可以代表一些抽象关系。例如可用一个图表示一群人之间的关系:点代表人,凡有边相连的两个点表示他们互相认识,否则表示不认识,则这个图就表示出了这群人之间的关系。图论中有许多有趣的问题,有兴趣的读者可阅读有关参考书。

图论中自然会提出某类图有多少个的问题。

例 4 画出所有点数为 3 的图。

此问题可以这样来解决:首先画出 3 个顶点:1,2,3.在每两个点之间有"无边"和"有边"两种情况,因而全部有 $2\times2\times2=2^3=8$ 种情况,每一种情况对应一个图(图 1.3)。

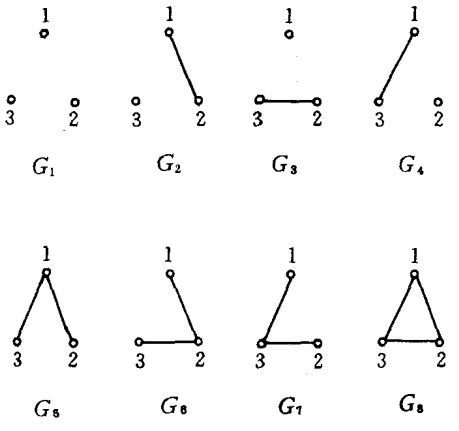


图 1.3

当点数为 n 时，共可形成 $\binom{n}{2}$ 个 2 元子集，每一个 2 元子集可以对应图中的边或不对应边两种情况，故可形成 $2^{\binom{n}{2}}$ 个图。但是，我们观察一下图 1.3 中的 8 个图，可以发现有些图的构造是完全相同的，如果不考虑它们的点号，可以完全重合，这样的图称它们是同构的。例如图 1.3 中的 G_2，G_3 与 G_4。可以看出图 1.3 中的图，共有 4 个互不同构的图。那么，对一般情况，n 个点的图中互不同构的图有多少个呢？这个问题也不能用初等方法来解决。

5. 开关线路的构造与计数问题

一个有两种状态的电子元件称为一个开关，例如普通的电灯开关，二极管等。由一些开关组成的二端网络称为开关线路。一个开关线路的两端也只有两种状态：通与不通。我们的问题是：用 n 个开关可以构造出多少种不同的开关线路？

首先必须对此问题建立一个数学模型，然后用适当的数学工具来解决它。

我们用 n 个变量 $x_1,x_2,\cdots,x_n$ 代表 n 个开关，每一个变量 x_i 的取值只能是 0 或 1，代表开关的两个状态。开关线路的状态也用一个变量 f 来表示，f 的取值也是 0 或 1，代表开关线路的两个状态。f 是 $x_1,x_2,\cdots,x_n$ 的函数，称 f 为开关函数，记作

$$f(x_1,x_2,\cdots,x_n)。$$

令 $A=\{0,1\}$，则 f 是 $\underbrace{A\times A\times\cdots\times A}_{n个}$ 到 A 的一个映射（函数），反之，每一个函数

$$f:A\times A\times\cdots\times A\to A$$

对应一个开关线路。因此，开关线路的数目就是开关函数的数目。下面来计算这个数目。

由于 f 的定义域的点数为 $|A|^n=2^n$，f 在定义域的每一个点上的取值有两种可能，所以全部开关函数的数目为 2^{2^n}，这也就是 n 个开关的开关线路的数目。

但是上面考虑的开关线路中的开关是有标号的，有一些开关线路结构完全相同，只是标号不同，我们称这些开关线路本质上是相同的。参见 2.10 节图 2.8 中的(a)与(b)。要进一步解决本质上不同的开关线路的数目问题，必须用群论方法。

6. 数字通信的可靠性问题

现代通信中用数字代表信息，用电子设备进行发送、传递和接收，并用计算机加以处理。由于信息量大，在通信过程中难免出现错误。为了减少错误，除了改进设备外，还可以从信息的表示方法上想办法。用数字表示信息的方法称为编码。编码学就是一门研究高效编码方法的学科。下面用两个简单的例子来说明检错码与纠错码的概念。

例 5 简单检错码——奇偶性检错码

设用 6 位二进制码来表示 26 个英文字母，其中前 5 位顺序表

示字母，第 6 位作检错用，当前 5 位的数码中 1 的个数为奇数时，第 6 位取 1，否则第 6 位是 0。这样编出的码中 1 的个数始终是偶数个。例如，

A:000011　　B:000101　　C:000110

D:001001　　……

用这种码传递信息时可检查错误。当接收一方收到的码中含有奇数个 1 时，则可断定该信息是错的，可要求发送者重发。因而，同样的设备，用这种编码方法可提高通信的准确度。

但是，人们并不满足仅仅发现错误，能否不通过重发的办法，仅从信息本身来纠正其错误呢？这在一定的程度上也可用编码方法解决。

例 6　简单纠错码——重复码

设用 3 位二进制重复码表示 A，B 两个字母如下：

A:000　　B:111

则接收的一方对收到的信息码不管其中是否有错，均可译码如下：

接收信息：000 001 010 011 100 101 110 111

译　　码：A　A　A　B　A　B　B　B

这就意味着，对其中的错误信息做了纠正。

利用近世代数方法可得到更高效的检错码与纠错码。

7. 几何作图问题

古代数学家们曾提出一个有趣的作图问题：用圆规和直尺可做出哪些图形？而且规定所用的直尺不能有刻度和不能在其上作记号。为什么会提出这样的问题呢？一方面是由于生产发展的需要，圆规、直尺是丈量土地的基本工具，且最初的直尺是无刻度的；另一方面，从几何学观点看，古人认为直线与圆弧是构成一切平面图形的要素。据说，古人还认为只有使用圆规与直尺作图才能确保其严密性。且整个平面几何学是以圆规与直尺作为基本工具。