离散数学导论

无限集合·近世代数·图论部分

黄和之　编著

$$(A \Rightarrow B) \Leftrightarrow (B=0 \Rightarrow A=0)$$

$$R=t(R) \Leftrightarrow R^2 \subset R$$

离散数学导论

无限集合·近世代数·图论部分

黄和之编著

北京经济学院出版社

1993·北京

（京）新登字 211 号

D139/16

离散数学导论
Li san shu xue Dao lun
黄和之 编著
北京经济学院出版社出版
（北京市朝阳区红庙）
北京通县永乐印刷厂印刷
新华书店北京发行所发行
787×1092 毫米 32 开本 14.25 印张 317 千字
1993 年 11 月第 1 版 1993 年 11 月第 1 版第 1 次印刷
印数：00 001—3000
ISBN7-5638-0356-4/O・10
定价：9.15 元

内 容 简 介

本书紧接《离散数学导论(数理逻辑·集合·关系部分)》之后，介绍函数、无限集合、近世代数和图论。

无限集合中有关于枚举函数的定理，使康托尔的对角线法的论证更为严谨；有限域阶数的证明比较简明；求子群的规范化方法，骨架树棵数的求法简便适用。

用移位、取模、比较求出 Z_p 域上全部 n 次本原多项式具有创新性质。

本书适用于经济类信息专业，有关专业本科、专科，电大、成人教育等；也可作计算机工作者自学资料。

序

这本《离散数学导论》是北京经济学院黄和之副教授根据自己在教学中使用多年的讲义经整理补充写成付印的。

此书的最大特点是对一些复杂繁难的问题，力图用简便的办法或初等工具处理，使同学易于掌握，并受到不必墨守成规的启发。逻辑蕴涵式的快速证明和用除法求本原多项式是两个典型的例子。

数理逻辑中，逻辑蕴涵式的证明比较繁难。作者提出的快速证明法对前件多而后件少的逻辑蕴涵式来说，确实是简捷明快。运用此一方法，在逻辑推理中即刻自行构造推理规则有其独到之处。在谓词演算中运用此一方法也是值得探索的。

在有限域 Z_p 上求所有 m 次不可约多项式和 n 次本原多项式，在理论研究和实际应用方面都是有意义的。Church，R. 1935 年发表 Z_2, Z_3, Z_5, Z_7 上的低次不可约多项式及其周期后，几十年来，很多学者作了大量工作。Rudolf Lidl 和 Harald Niedeareiter 1983 年在伦敦出版了带有总结性的 Finite Fields，其中列举了各个时期所得到的多项式数据。理论上推出下列两个公式：

$$I(q,m;x) = \prod_{d|m} (x^{q^d} - x)^{\mu(m/d)}$$

$$Q_{p^n-1}(x) = \prod_{d|p^n-1} (x^d - 1)^{\mu((p^n-1)/d)}$$

前者是所有 m 次不可约多项式的乘积，后者是所有 n 次本原多项式的乘积。求具体的不可约多项式，文献中用筛法或因式分解法，手续繁杂，计算量很大。本书作者不用 Moebius 函数及其反演，只用初等工具证明了几个定理，得出公式或计算格

式。教学中同学反映容易掌握，有的同学还受到敢于创新的启发，发挥了自己的创造性。

此外，书中二元关系的传递性的判别法，利用闭包定义的第三条件简化了几个定理的证明，求子群的规范化方法，有限域阶数的证明，以及求生成树（骨架树）棵数的方法，也都有可取之处。虽然有的方法还需要总结提高。

本书的第二个特点是在章节安排上采取积木式编法。文理跨学科的专业，只愿花较少时间讲授数理逻辑的专业以及专科学校，可只用 1～4 章作教材；学时少的计算机专业可用 1～8 章作教材；学时较多的计算机专业或愿开设离散数学课程的专业则可用全书作教材或教学参考书。编写时采用了较多的例子说明概念，以增强其易读性，有利于教学时采用由浅入深的启发式教学方法。本书作为自学离散数学的参考书也是合适的。与本书配套的《离散数学导论习题选解》业已出版。

本书在同行中必将引起争论的是数理逻辑部分选用了过多的文学、数学、先秦典籍中事例的例子。赞成者会认为可以扩大知识面，提高学习兴趣；反对者会认为这些旁征博引是喧宾夺主。再有，某些用词也可能引起争议，如从 A 集到 B 集的所有函数的集合不叫超幂而叫配置集；Bijective 不译双射而译作单满射；Contingency 译作偶真式等。这些词是否妥当，有待于专家指教和大多数读者认可。另外，对于某些史实，作者在查阅了有关书籍后，再三考虑，没有袭用别人的说法。

据作者称，他的这些作法以及他提出的一些简化方法，意在抛砖引玉。他希望在批评或否定他的“立异”时，他的愿望能得到理解。我想，学术研究，贵在百家争鸣，作者的愿望是会被理解的。

不久前，我通读了本书原稿，并与作者讨论过几次。在这里写下我的一些印象和看法，供读者参考。

邹德林

1991.10.3

前　言

在北京经济学院信息管理专业几年教学实践的基础上编成了这本《离散数学导论(无限集合·近世代数·图论部分)》作为《离散数学导论(数理逻辑·集合·关系部分)》(已出版)的续篇。编写时作者追求一种风格,这种风格要求理论上由浅入深、由粗到细,方法上则力求简便,并且多用例子阐述概念。

原讲义使用过程中,同学反映较好。有的同学还补充或改进了一些定理的证明,有的同学提出了一些简化方法。

这次编辑成书,作了较大的修改和补充。主要有以下四个方面。

一、数理逻辑部分[读者可参看《离散数学导论(数理逻辑·集合·关系部分)》一书]。为适应同学在工作中、生活中应用逻辑知识的需要,我们附带介绍一些形式逻辑和逻辑史方面的知识;为提高学习逻辑的自觉性,选用了数学、文学的例子,也举了先秦著作中的事例来说明逻辑概念。这种讲法,在多轮教学中都是受欢迎的。一些同学认为他们第一次接触抽象的逻辑符号和公式时,对这些材料是有兴趣的。命题蕴涵式的快速证明法的论文已于1985年发表,这次写成一章列入第一篇。大多数永真式在论证中作推理规则使用,在这一章中专用一节讨论构造永真式。

二、集合论部分[读者可参看《离散数学导论(数理逻辑·集合·关系部分)》一书]。讨论了悖论,介绍了一些资料,对罗素悖论的来源作了考证。这也是尝试性的。读者对此不感兴趣的话,可以不看,对后面阅读不会有影响。求传递闭包的加弧法是谓词理论的应用,对1962年发表的Warshall法,可用它作出简易而轻巧的证明。

三、近世代数部分增写了九、十、十一等三章。对求子群，提出一种规范化的方法。对有限域，用初等工具探索出构造不可约多项式的简便方法，证明了并不需要从不可约多项式中筛选出本原多项式的定理。据此编制了两个软件，在计算机上计算并打印出比 1983 年伦敦出版的 Finite Fields 中一些表的数据更全面的多项式表。例如，按键 P,D,19,2,2,打印出 Z_{19} 上二次不可约多项式 171 个及其周期。按键 P,R,2,11,13,打印出 Z_2 上 11 次本原多项式 176 个，12 次 144 个及 13 次 630 个。按键 P,R,43,1,2,打印出 Z_{43} 上一次本原多项式 12 个，二次 240 个。

四、图论部分。给出计算骨架树(生成树)棵数的简易方法。

离散数学著作近几年已出版多种，本书在内容取舍和章节安排上是否合适，希望得到专家们指教。限于作者水平，书中会出现缺点和错误，敬请读者指正。对于作者提出的一些方法，作者的动机是抛砖引玉，希望同行们提出更好的方法。至于能否为初学者提供一些方便，就只能在使用过程中由读者评价了。

初编讲义时，李斯奇同志曾协助收集资料，改写成书时，邹德林同志提过很多好的建议，编者向他们致谢。

本书出版过程中，曾得到台湾台中县昭武公司陈德荣先生的关心和支持，编者深表谢忱。希望今后两岸学术著作的交流会有进一步的发展。

编　者

1991 年

目　　录[①]

① 第1～5章内容参看《离散数学导论(数理逻辑·集合·关系部分)》一书。本书自第6章开始，共计8章。

第二篇　集合论

第六章　函数

函数是数学的基本概念之一。

17 世纪 Galileo 等由对运动的研究引出函数概念，如把落体的距离叙述为 $s=kt^2$，这样就把理论科学归结到数学，也使数学得到巨大的推动力量。1714 年 Leibniz 用函数(Function)一词表示依赖于一个变量的量。1734 年 Euler 引进 f(x) 符号。19 世纪 Dirichlet 给出单值函数的定义："如果对于给定区间上每一个 x 的值，有唯一的一个 y 值和它对应，则 y 就是 x 的一个函数。"现在一般数学分析中的函数定义常写为："非空点集 A 与实数集 R，若任 $x\in A$，按对应关系 f 有唯一的一个数 $y\in R$ 与 x 对应，则 f 是定义在 A 上的函数。"为了简便，常笼统地说"f(x)是 x 的函数。"(严格说来，这样会混淆函数和函数值，这只算是一种约定。)

数学发展以后，自变量已不限于数的笛卡尔积中的元素，如变分法中，把一类函数 $\{y(x)\}$ 作为空间中的点集，在某一"点"，可使积分 $J=\int_a^b F(x,y,y')dx$ 取最大值或最小值，这是从函数集合到实数的函数。以日常的经济活动来看，建设宾馆，资金多，可建高档的，资金少，可建中档的、低档的；上街买菜，货款依赖于蔬菜品种、单价和数量，这些函数关系都不是从数集到数集的。

有必要把函数概念严密化，既能表示数学分析中的概念，也适用于抽象的数学学科和日常生活。这就是本章所要讨论的问题。

计算机科学中充分地运用数学分析对函数研究的成果（如程序语言中 SIN(x)、SQR(x)、LOG(x)等就是按 Taylor 公式展开而编成的标准程序，在使用时只要调用即可），也把函数当作输入输出关系，有一输入通过某一规则，可产生唯一的输出，这规则就是函数。这一领域的很多知识，可通过对某些类型的函数的性质的描述而得到条理化。

离散数学中常把几种特殊类型的函数作为有效的数学工具（见第七、八章）。

§6.1 函数的基本性质

一、函数概念

从集合 A 到 B 的函数是一个规则，它对 A 的每一个元素都指定 B 的一个元素。而所谓规则，可用关系概念来描述。常用字母 f、g、h 表示函数，函数也叫映射或变换。

定义6.1.1 A 和 B 是集合，从 A 到 B 的函数 f，记为 $f:A\to B$，是从 A 到 B 的一个关系；且对任一 $a\in A$，总存在唯一的 $b\in B$，使 $<a,b>\in f$。当 $<a,b>\in f$ 时，记为 $f(a)=b$。

由定义，从 A 到 B 的函数 f 是具有特殊性质的从 A 到 B 的二元关系，这些性质是：

（Ⅰ）A 的每一元素都作为 f 的一个序偶的第一分量。

（Ⅱ）若 $f(a)=b, f(a)=c$，则 $b=c$。

函数既是特殊的二元关系，则可把用于关系的术语稍作改变，作为用于函数的术语。$f:A\to B$，A 叫 f 的定义域，B 叫 f 的值域，在表达式 $f(a)=b$ 中，a 叫自变量，b 叫关于自变量 a

的函数值。

要定义一个函数，必须指出定义域、值域和每个自变量 x 的函数值 f(x)。符号 f:A→B 表示定义域为 A，值域为 B 的函数，对 f(x)的值，常用一组取遍所有 x 值的规则来确定。例如：

$$f:N\to N \quad f(x)=\begin{cases}1 & \text{当 x 是奇数}\\ x/2 & \text{当 x 是偶数}\end{cases}$$

如果定义域是有限集合，也可用列出所有自变量的函数值的显式确定函数，例如：

g:{1,2,3}→{A,B,C}

g(1)=A

g(2)=C

g(3)=C

或用图表示。

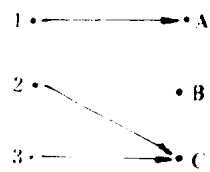

图 6.1.1

【例 1】 (a)A={a,b}，B={1,2,3}，图 6.1.2 表示从 A 到 B 的三个函数。

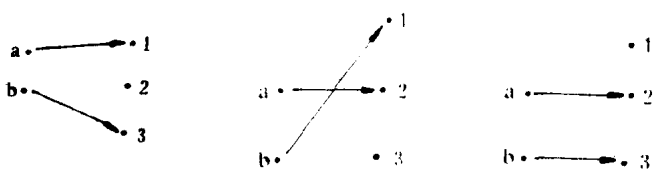

图 6.1.2

(b)图 6.1.3 表示的只是关系，不是函数。

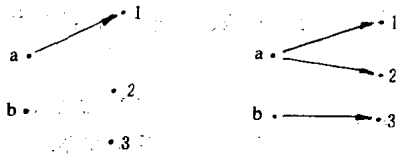

图 6.1.3

(c)若 $A=\phi$，B 为任一集合，则空关系 ϕ 是从 A 到 B 的空函数。若 $A\neq\phi$，$B=\phi$，则从 A 到 B 的关系是无效关系，不是函数。

对 $f:A\to B$，常看作 A 的元素映射到 B 的元素，$f(a)=b$，b 叫在映射 f 下 a 的象，a 叫 f 下 b 的象源。有时把 f 看作将 A 的子集映射到 B 的子集，下面的定义给出方便的记号。

定义 6.1.2　f 是从 A 到 B 的函数，$A'\subset A$，则 $f(A')$ 表示 B 的一个子集，叫 A' 在 f 下的象

$$f(A')=\{f(x)\mid x\in A'\}。$$

整个定义域 A 的象 f(A)叫函数 f 的象。

对任一函数 $f:A\to B$，定义 6.1.2 隐含地规定了另一函数 $F:P(A)\to P(B)$，即把定义域 A 的各子集映射到值域 B 的一些子集。对 $A'\subset A$，集合 $F(A')$ 用 $f(A')$ 表示，但要注意 f 和 F 并不是同一函数，f 的定义域是 A，值域是 B，F 的定义域是幂集 P(A)，值域是幂集 P(B)。如图 6.1.4 所示。

尽管 f 和 F 有区别，但仍按习惯只用 f，即 f 既表示原来的函数 f，也表示派生函数 F，根据所使用的自变量，就能说明是哪一种函数，这种符号的用法，不会产生混乱。

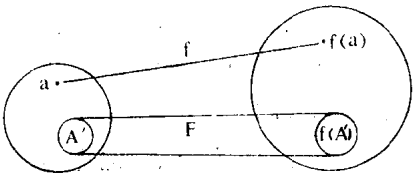

图 6.1.4

【例 2】 (a)$f:\{0,1,2,3\}\to\{a,b,c\}$由图 6.1.5 给出定义，

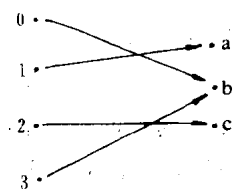

图 6.1.5

则 $f(\{0,1,2,3\})=\{a,b,c\}$

$f(\{2,3\})=\{b,c\}$

$f(\{0\})=\{b\}$

$f(\{0,3\})=\{b\}$。

(b)$f:N\to N, f(x)=\begin{cases}1 & \text{当 } x \text{ 是奇数}\\ x/2 & \text{当 } x \text{ 是偶数}\end{cases}$

$f(0)=0$ $\quad f(\{0\})=\{0\}$

$f(1)=1$ $\quad f(\{1\})=\{1\}$