

高等院校素质教育通选课教材

# 数学的思维方式与创新

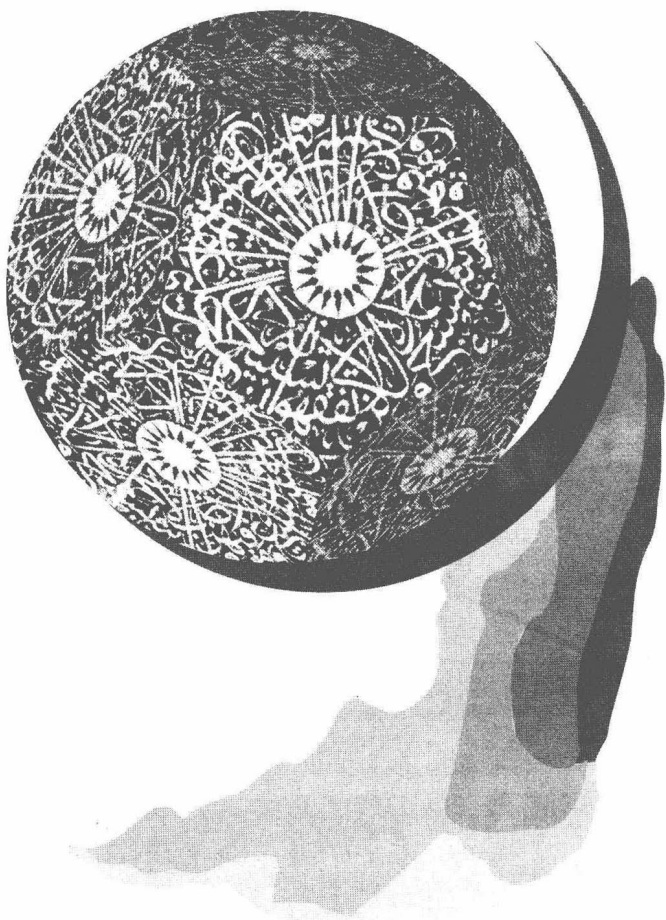
丘维声 著



高等院校素质教育通选课教材

# 数学的思维方式与创新

丘维声 著



北京大学出版社  
PEKING UNIVERSITY PRESS

## 图书在版编目(CIP)数据

数学的思维方式与创新/丘维声著. —北京: 北京大学出版社, 2011. 3  
(高等院校素质教育通选课教材)

ISBN 978-7-301-18391-5

I. ①数… II. ①丘… III. ①数学-思维方法-高等学校-教材 IV. 01-0

中国版本图书馆 CIP 数据核字(2011)第 001786 号

## 书 名: 数学的思维方式与创新

著作责任者: 丘维声 著

责任编辑: 刘 勇 潘丽娜

封面设计: 林胜利

标准书号: ISBN 978-7-301-18391-5/O · 0840

出版发行: 北京大学出版社

地 址: 北京市海淀区成府路 205 号 100871

网 址: <http://www.pup.cn> 电子邮箱: [zpup@pup.pku.edu.cn](mailto:zpup@pup.pku.edu.cn)

电 话: 邮购部 62752015 发行部 62750672 理科编辑部 62752021 出版部 62754962

印 刷 者: 北京鑫海金澳胶印有限公司

经 销 者: 新华书店

787mm×960mm 16 开本 14.5 印张 800千字

2011 年 3 月第 1 版 2011 年 3 月第一次印刷

印 数: 0001—4000 册

定 价: 29.00 元

---

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容  
版权所有,侵权必究

举报电话:010-62752024 电子邮箱: [fd@pup.pup.edu.cn](mailto:fd@pup.pup.edu.cn)

## 内 容 简 介

本书是作者在北京大学多次给本科生讲授“数学的思维方式与创新”素质教育通选课的教材。什么是数学的思维方式？如何培养学生的数学思维能力？数学的思维方式包括哪几个环节？作者用通俗易懂的语言论述了数学思维方式的五个重要环节：观察—抽象—探索—猜测—论证。讲述了数学上的创新是如何推动数学的发展，而数学的思维方式在创新中是怎样起着重要作用的，使学生领略数学创新的风采，受到数学思维方式与创新的熏陶和训练，提高数学素质。

本书以现代数学和信息时代有重要应用的数学知识和数学发展史上若干重要创新为载体，从同学们熟悉的整数、多项式出发，讲述整数环、一元多项式环的结构；从“星期”这一司空见惯的现象引出集合的划分、等价关系和模  $m$  剩余类的概念，进而研究模  $m$  剩余类环的结构；从信息时代为了确保信息安全引出序列密码和公开密钥密码，以及数字签名；从数学发展史上选出三个重大创新进行阐述，它们是：从对运动的研究到微积分的创立和严密化，从平行公设到非欧几里得几何的诞生与实现；从方程的根式可解问题到伽罗瓦理论的创立和代数学的变革。全书共分四章，第一、二、三章每节配置了习题，书末给出了习题解答，供教师和学生参考。

本书的特点是运用数学的思维方式讲授数学知识，通过观察客观现象引出数学概念，提出要研究的问题，着重启发学生进行探索、猜测可能有的规律，然后进行严密论证，在论证中强调创新思想。对数学发展史上三个重大创新，不仅介绍了创新的历史进程，而且着重讲述这些创新的内容及给我们的启迪。

本书可作为高等院校本科生素质教育通选课的教材或教学参考书，也可作为数学工作者、中学数学教师、高中生和大学生课外阅读书。

## 作者简介

丘维声 1966年毕业于北京大学数学力学系. 现为北京大学数学科学学院教授、博士生导师, 全国高等学校首届国家级教学名师, 美国数学会 *Mathematical Reviews* 评论员, 中国数学会组合数学与图论专业委员会首届常务理事, 《数学通报》副主编, 曾任“国家教委高等学校数学与力学教学指导委员会”(第一、二届)委员.

出版著作 38 部, 发表教学研究论文 22 篇, 译著(合译)6 部. 他编写的具有代表性的优秀教材有: 《高等代数(上、下册)——大学高等代数课程创新教材》(清华大学出版社, 2010), 《高等代数(第二版)(上、下册)》(高等教育出版社, 2003), 《简明线性代数》(北京大学出版社, 2002), 《解析几何(第二版)》(北京大学出版社, 1996), 《抽象代数基础》(高等教育出版社, 2003), 《有限群和紧群的表示论》(北京大学出版社, 1997)等.

作者的研究方向: 代数组合论、群表示论、密码学, 发表科学论文 46 篇. 承担国家自然科学基金重点项目 2 项, 主持国家自然科学基金面上项目 3 项.

丘维声教授获全国高等学校首届国家级教学名师奖, 三次被评为北京大学最受学生爱戴的十佳教师, 获宝钢教育奖优秀教师特等奖, 北京市高等教育教学成果一等奖, 被评为全国电视大学优秀主讲教师、北京市科学技术先进工作者, 获北京大学杨芙清-王阳元院士教学科研特等奖, 三次获北京大学教学优秀奖、北京大学科研成果奖等.

## 序 言

从2007年春季学期开始,每个学期我都在北京大学给全校本科生开设素质教育通选课:“数学的思维方式与创新”.到这学期已经讲了八遍.每讲一遍我都要对2007年写的讲义进行修改.现在把经过多次修改后的讲义整理成本书出版.

每一个人都按照一定的思维方式处理工作和生活中遇到的事情.具有科学的思维方式是一个人素质高的体现.科学的思维方式是需要经过熏陶和训练才能具备的.数学的思维方式是一种科学的思维方式,它是一个全过程:观察客观现象,提出要研究的问题,抓住主要特征,抽象出概念,或者建立模型;运用解剖麻雀、直觉、归纳、类比、联想、逻辑推理等进行探索,猜测可能有的规律;采用公理化的方法,即只使用公理、定义和已经证明了的定理进行逻辑推理来严密论证,揭示出事物的内在规律,从而使纷繁复杂的现象变得井然有序.“观察—抽象—探索—猜测—论证”是数学思维方式全过程的五个重要环节.按照数学的思维方式学习数学是学好数学的正确途径,在学习数学过程中受到数学思维方式的熏陶和训练,对于学生今后从事任何工作都有帮助,终身受益.

不管做什么工作,进行创新都需要科学的思维方式.从数学的发展历史可以看到:数学的思维方式在创新中起着重要作用.一个重要的数学概念的提出,往往是数学创新迈出的第一步.进行艰辛的探索是数学创新的必经之路.在探索的基础上产生的想法(通常称之为猜想)是在创新旅程中迈上的一个新台阶.寻求对于猜想的论证吸引着众多数学家呕心沥血.最终取得的突破性进展是数学创新的一个标志.在其他工作岗位上进行创新可以从数学的创新中受到启迪.

2006年4月,北京大学数学科学学院的领导委托王长平副院长交给我一项教学任务:新开设一门全校素质教育通选课,课程的内容和名称由我自己确定.我经过较长时间的酝酿和构思,决定开设“数学的思维方式与创新”这门通选课.我觉得无论对于理科学学生还是文科学生,受到数学思维方式的熏陶和训练,领略数学创新的风采,对于他们在大学的学习以及今后的工作都是有帮助的.鉴于选这门课的学生来自全校各个院系,因此我在讲课中,作为载体的数学知识经过了精心挑选,以现代数学和信息时代有重要应用的数学知识,以及数学发展史上若干重大创新为载体.从同学们熟悉的整数、多项式出发,讲述整数环的结构,一元多项式环的结构;从“星期”这一司空见惯的现象引出集合的划分、等价关系和模 $m$ 剩余类的概念,进而研究模 $m$ 剩余类环的结构.从信息时代为了确保信息安全,引出序列密码和公开密钥密码,以及数字签名.从数学发展史上挑选出三

个重大创新进行阐述,它们分别属于分析学、几何学、代数学三个领域.它们是:从对运动的研究到微积分的创立和严密化;从平行公设到非欧几里得几何的诞生与实现;从方程的根式可解问题到伽罗瓦理论的创立和代数学的变革.我们不仅介绍了这些创新的历史进程,详细讲解了这些创新的内容,而且讲述了这些创新给我们的启迪.这门课的特点是运用数学的思维方式讲授数学知识,通过观察客观现象或熟悉的数学例子自然而然地引出概念,提出要研究的问题,着重启发学生进行探索,猜测可能有的规律,然后进行严密论证,在论证中突出想法,尤其是要指出其中的创新想法.

在阅读第四章 § 4.3 的第 4.3.4, 4.3.5 和 4.3.6 小节之前,请先阅读附录 1 和附录 2. 附录 1 是“研究群的结构途径”,附录 2 是“域扩张的途径及其性质”.这两个附录也是按照数学的思维方式来写的,因此阅读这两个附录也可受到数学思维方式的熏陶和训练.

本书可作为大学本科生通选课教材.如果周学时为 3 学时,可以在课堂上讲授第一、二、三章,用楷体字排印的内容可不必讲;把第四章留给有兴趣的学生自己阅读.第一章讲授 20 学时,第二章讲授 13 学时,第三章讲授 7 学时.如果周学时为 2 学时,可以在课堂上讲授第一、三章,以及第四章的第 1 节(这一节讲授 4 学时);把第二章和第四章的第 2, 3 节留给有兴趣的学生自己阅读.如果没有固定的周学时,而是开设讲座,那么可以从下述内容根据具体情况挑选一些来讲授:第一章的第 1 节(2 学时),第 2 节(2 学时);第 8 节(2~4 学时);第三章的第 1 节(3 学时);第四章的第 1 节(2~4 学时);第四章的第 2 节(4~8 学时);第四章的第 3 节(4~12 学时).

本书的第一、二、三章的每一节都配备了习题.在书末附有习题解答.

本书可供大学本科生(包括理工科和文科)阅读(可阅读第一、二、三章和第四章的第 4.1 节),也可供高中生阅读(可阅读第一、二、三章).全书(包括附录 1 和附录 2)可供大学数学系和物理系的学生阅读.

本门课程的教材于 2007 年获得北京大学教材建设立项,特此向北京大学教材建设委员会表示感谢.作者感谢本书的责任编辑刘勇和潘丽娜,他们为本书的编辑和出版付出了辛勤劳动.

作者欢迎广大读者对本书提出宝贵意见.

丘维声

2010 年 10 月于北京大学  
数学科学学院



# 目 录

引 言 .....	(1)	第二章 从解方程到一元	
习题 .....	(5)	多项式环 .....	(55)
第一章 从星期到模 $m$ 剩余类环 .....	(6)	§ 2.1 一元多项式环的概念 .....	(55)
§ 1.1 集合的划分与等价关系 .....	(6)	习题 2.1 .....	(58)
习题 1.1 .....	(10)	§ 2.2 带余除法, 整除关系 .....	(59)
§ 1.2 模 $m$ 剩余类环 $\mathbf{Z}_m$ , 环和域		习题 2.2 .....	(61)
的概念 .....	(11)	§ 2.3 最大公因式 .....	(62)
习题 1.2 .....	(15)	2.3.1 最大公因式 .....	(62)
§ 1.3 整数环的结构 .....	(15)	2.3.2 互素的多项式 .....	(64)
习题 1.3 .....	(20)	习题 2.3 .....	(65)
§ 1.4 $\mathbf{Z}_m$ 的可逆元的判定, 模 $p$ 剩余类		§ 2.4 不可约多项式, 唯一因式分解	
域, 域的特征, 费马小定理 .....	(21)	定理 .....	(66)
习题 1.4 .....	(25)	习题 2.4 .....	(68)
§ 1.5 中国剩余定理 .....	(25)	§ 2.5 多项式的根, 多项式函数, 复数域	
习题 1.5 .....	(28)	上的不可约多项式 .....	(69)
§ 1.6 $\mathbf{Z}_m$ 的可逆元的个数,		2.5.1 多项式的根 .....	(69)
欧拉函数 .....	(28)	2.5.2 多项式函数 .....	(70)
习题 1.6 .....	(34)	2.5.3 复数域上的不可约多项式 .....	(71)
§ 1.7 $\mathbf{Z}_m$ 的单位群 $\mathbf{Z}_m^*$ , 欧拉		习题 2.5 .....	(74)
定理, 循环群及其判定 .....	(34)	§ 2.6 实数域上的不可约	
1.7.1 $\mathbf{Z}_m^*$ 的结构, 群 .....	(34)	多项式 .....	(75)
1.7.2 欧拉定理 .....	(36)	习题 2.6 .....	(78)
1.7.3 群的元素阶 .....	(37)	§ 2.7 有理数域上的不可约	
1.7.4 循环群及其判定 .....	(39)	多项式 .....	(78)
习题 1.7 .....	(43)	习题 2.7 .....	(86)
§ 1.8 筛法, 威尔逊定理, 素数的		第三章 从通信安全到密码学 .....	(87)
分布 .....	(44)	§ 3.1 序列密码 .....	(87)
1.8.1 筛法, 威尔逊定理 .....	(44)	习题 3.1 .....	(96)
1.8.2 素数的分布 .....	(45)	§ 3.2 线性反馈移位寄存器,	
1.8.3 素数的计数 .....	(47)	$m$ 序列 .....	(97)
习题 1.8 .....	(53)	习题 3.2 .....	(107)



## 目录

§ 3.3 公开密钥密码体制, RSA 密码系统 .....	(107)	伽罗瓦理论的创立与 代数学的变革 .....	(144)
习题 3.3 .....	(111)	4.3.1 三次、四次方程的解法 .....	(144)
§ 3.4 数字签名 .....	(112)	4.3.2 拉格朗日等人对于五次及更高次一般 方程不能用根式解的研究 .....	(146)
习题 3.4 .....	(113)	4.3.3 伽罗瓦研究可用根式求解的 方程的特性的思想 .....	(147)
<b>第四章 数学发展史上若干重大 创新 .....</b>	<b>(114)</b>	4.3.4 伽罗瓦理论的基本定理 .....	(152)
§ 4.1 从对运动的研究到微积分 的创立和严密化 .....	(114)	4.3.5 方程根式可解的判别准则 .....	(154)
4.1.1 17 世纪对天体运动的研究 .....	(114)	4.3.6 高于四次的一般方程不是 根式可解的证明 .....	(159)
4.1.2 牛顿和莱布尼茨创立 微积分 .....	(115)	4.3.7 伽罗瓦理论的创立给我们 的启迪 .....	(162)
4.1.3 微积分的严密化 .....	(118)	<b>附录 1 研究群的结构的途径 .....</b>	<b>(164)</b>
4.1.4 实数系的连续性与完备性 .....	(119)	§ 1.1 子群, 正规子群, 商群 .....	(164)
§ 4.2 从平行公设到非欧几里得 几何的诞生与实现 .....	(124)	§ 1.2 群的同态, 可解群 .....	(171)
4.2.1 欧几里得几何 .....	(124)	<b>附录 2 域扩张的途径及其性质 .....</b>	<b>(181)</b>
4.2.2 对平行公设的质疑 .....	(125)	§ 2.1 理想, 商环, 环同态, 极大理想, 域扩张的途径 .....	(181)
4.2.3 非欧几里得几何的诞生 .....	(126)	§ 2.2 域扩张的性质, 分裂域, 伽罗瓦扩张 .....	(191)
4.2.4 非欧几何在现实物质世界中 的实现 .....	(128)	<b>习题解答 .....</b>	<b>(204)</b>
4.2.5 非欧几何的诞生与实现给 我们的启迪 .....	(143)	<b>参考文献 .....</b>	<b>(223)</b>
§ 4.3 从方程根式可解问题到			



# 引言

数学以公式之优美、理论之奇妙、论证之严密、应用之广泛令人惊叹不已！究其原因，数学的思维方式发挥着巨大的威力，数学的创新赋予数学旺盛的生命力。

数学的思维方式是一个全过程：观察客观现象，提出要研究的问题，抓住主要特征，抽象出概念，或者建立模型；运用解剖麻雀、直觉、归纳、类比、联想、逻辑推理等进行探索，猜测可能有的规律；采用公理化的方法，即只使用公理、定义和已经证明了的定理进行逻辑推理来严密论证，揭示出事物的内在规律，从而使纷繁复杂的现象变得井然有序。

按照“观察—抽象—探索—猜测—论证”这一数学的思维方式去学习数学，就使数学变得比较容易学，而且可以享受到学习数学的乐趣。

按照数学的思维方式讲授数学，不仅传授了数学知识，而且可以使同学们受到科学思维方式的训练，陶冶人文精神：客观、公正、讲理、严谨、勇于创新、坚韧不拔、灵活机动、谦虚谨慎，从而使同学们终身受益。

下面我们通过几个例子来感受数学的思维方式，领略数学的风采。

听这门课的同学走进教室都要找一个椅子坐下。用  $A$  表示听这门课的所有同学组成的集合，用  $B$  表示这个教室的所有椅子组成的集合，同学找一个椅子坐下就是集合  $A$  到  $B$  的一个对应法则，使得集合  $A$  中的每一个同学，有集合  $B$  中唯一确定的一个椅子与他（她）对应。

当今信息时代，信息的传送实行数字化。作为数字化的第一步，需要把 26 个英文字母分别对应于数。自然可以把  $a$  对应到 0,  $b$  对应到 1,  $c$  对应到 2,  $\dots$ ,  $z$  对应到 25。于是由 26 个英文字母组成的集合，到前 26 个自然数组成的集合有一个对应法则，使得每个英文字母有唯一的一个自然数与它对应。

上述两个例子的主要特征是：一个集合到另一个集合有一个对应法则，使得第一个集合的每一个元素，有第二个集合的唯一确定的一个元素与它对应。我们抓住这个主要特征，抽象出下述概念：

**定义 1** 设  $A$  和  $B$  是两个集合，如果集合  $A$  到集合  $B$  有一个对应法则  $f$ ，使得  $A$  中每一个元素  $a$ ，都有  $B$  中唯一确定的一个元素  $b$  与它对应，那么称  $f$  是集合  $A$  到  $B$  的一个映射，记做

$$\begin{aligned} f: A &\rightarrow B \\ a &\mapsto b, \end{aligned}$$

其中  $b$  称为  $a$  在  $f$  下的像， $a$  称为  $b$  在  $f$  下的一个原像。 $a$  在  $f$  下的像用符号  $f(a)$  表示，于是映射  $f$  也可以记成

$$f(a) = b, \quad a \in A.$$

事先给了两个集合  $A$  和  $B$ , 才能谈论  $A$  到  $B$  的映射. 设  $f$  是集合  $A$  到集合  $B$  的一个映射, 则把  $A$  叫做  $f$  的定义域, 把  $B$  叫做  $f$  的陪域. 一个映射  $f: A \rightarrow B$  由定义域、陪域和对应法则组成. 因此, 如果映射  $f$  与映射  $g$  的定义域相等、陪域也相等、并且对应法则相同, 那么称  $f$  与  $g$  相等, 记做  $f=g$ . 所谓  $f$  与  $g$  的对应法则相同, 是指对于定义域中的每一个元素  $a$ , 有  $f(a)=g(a)$ .

在上述第一个例子中, 听课的每一个同学找一个椅子坐下, 就是集合  $A$  到集合  $B$  的一个映射. 有同学坐着的椅子组成的集合称为这个映射的值域(或像集).

一般地, 设  $f$  是集合  $A$  到集合  $B$  的一个映射,  $A$  的所有元素在  $f$  下的像组成的集合称为  $f$  的值域(或像集), 记做  $f(A)$ , 即

$$f(A) := \{f(a) \mid a \in A\}.$$

容易看出,  $f(A) \subseteq B$ , 即  $f$  的值域是  $f$  的陪域的子集.

在上述第一个例子中, 如果教室里的每一个椅子都有同学坐着, 那么自然可以说这个映射是满射, 此时, 这个映射的值域等于陪域.

一般地, 设  $f$  是集合  $A$  到集合  $B$  的一个映射, 如果  $f$  的值域  $f(A)$  与  $f$  的陪域  $B$  相等, 那么称  $f$  是满射.

在上述第一个例子中, 显然, 不同的同学坐在不同的椅子上, 自然可以把这个映射称为单射.

一般地, 设  $f$  是集合  $A$  到集合  $B$  的一个映射, 如果  $A$  中不同的元素在  $f$  下的像不同, 那么称  $f$  是单射.

在上述第二个例子中, 26 个英文字母组成的集合到前 26 个自然数组成的集合有一个映射  $f$ :

$$a \mapsto 0, \quad b \mapsto 1, \quad c \mapsto 2, \quad \dots, \quad z \mapsto 25,$$

显然,  $f$  既是满射, 又是单射.

一般地, 设  $f$  是集合  $A$  到集合  $B$  的一个映射, 如果  $f$  既是满射, 又是单射, 那么称  $f$  是双射(或者称  $f$  是  $A$  与  $B$  之间的一个一一对应).

上面我们通过观察具体例子, 抓住其主要特征, 抽象出了映射、满射、单射、双射的概念. 现在我们来探索双射的性质.

在上述第一个例子中, 如果教室里的椅子都坐满了, 并且不同的同学坐在不同的椅子上, 那么同学坐在椅子上这个映射就是双射. 此时听课同学的数目等于教室里椅子的数目. 由此猜测有下述命题, 并且进行论证.

**命题 1** 设  $A$  和  $B$  都是有限集, 如果存在  $A$  到  $B$  的一个双射  $f$ , 那么  $A$  与  $B$  的元素个数相等, 即  $|A| = |B|$ .

**证明** 设  $A = \{a_1, a_2, \dots, a_n\}$ , 由于  $f$  是单射, 因此  $f(a_1), f(a_2), \dots, f(a_n)$  两两不等, 从

而值域为

$$f(A) = \{f(a_1), f(a_2), \dots, f(a_n)\}.$$

于是  $|f(A)| = n = |A|$ . 又由于  $f$  是满射, 因此  $f(A) = B$ . 从而  $|f(A)| = |B|$ . 所以  $|A| = |B|$ .  $\square$

命题 1 给出了判别两个有限集的元素个数是否相等的一种方法.

在上述第一个例子中, 设已经知道听课同学的数目等于教室里椅子的数目. 如果椅子都坐满了 (即坐在椅子上这个映射是满射), 那么不同的同学一定是坐在不同的椅子上 (即这个映射一定是单射), 如果不同的同学坐在不同的椅子上 (即单射), 那么椅子一定都坐满了 (即满射). 由此猜测有下述命题, 并且进行论证.

**命题 2** 设  $A$  和  $B$  都是有限集, 且  $|A| = |B|$ ,  $f$  是  $A$  到  $B$  的一个映射.

(1) 若  $f$  是满射, 则  $f$  必为单射.

(2) 若  $f$  是单射, 则  $f$  必为满射.

**证明** 设  $A = \{a_1, a_2, \dots, a_n\}$ .

(1) 由于  $f$  是满射, 因此  $f(A) = B$ . 从而

$$|f(A)| = |B| = |A| = n.$$

于是  $f(a_1), f(a_2), \dots, f(a_n)$  一定两两不同 (否则这些元素不够  $n$  个). 因此  $f$  是单射.

(2) 由于  $f$  是单射, 因此  $f(a_1), f(a_2), \dots, f(a_n)$  两两不同. 从而  $|f(A)| = n = |A| = |B|$ . 又由于  $f(A) \subseteq B$ , 因此  $f(A) = B$ . 于是  $f$  为满射.  $\square$

命题 2 使我们对于元素个数相等的两个有限集  $A, B$ , 如果有  $A$  到  $B$  的一个映射  $f$  可证它是满射, 那么  $f$  也是单射, 从而  $f$  是双射. 类似地, 如果已证  $f$  是单射, 那么  $f$  一定也是满射, 从而  $f$  是双射. 这样起到了事半功倍的效果.

在上述第二个例子中,  $f$  是 26 个英文字母组成的集合  $C$  到前 26 个自然数组成的集合  $D$  的一个双射. 考虑  $D$  到  $C$  的一个对应法则  $g$ :

$$0 \mapsto a, \quad 1 \mapsto b, \quad 2 \mapsto c, \quad \dots, \quad 25 \mapsto z,$$

显然  $g$  是  $D$  到  $C$  的一个映射. 观察:

$$g(0) = a, \quad g(1) = b, \quad g(2) = c, \quad \dots, \quad g(25) = z;$$

$$f(a) = 0, \quad f(b) = 1, \quad f(c) = 2, \quad \dots, \quad f(z) = 25.$$

$g$  与  $f$  的对应法则正好相反, 自然可以把  $g$  叫做  $f$  的逆映射. 由此受到启发, 引出下述概念:

**定义 2** 设  $f$  是集合  $A$  到集合  $B$  的一个映射, 如果对于  $B$  中每一个元素  $b$ , 都有  $A$  中唯一的元素  $a$ , 使得  $f(a) = b$ , 那么把  $b$  对应到  $a$  的映射  $g$  称为  $f$  的逆映射, 把  $g$  记做  $f^{-1}$ , 此时称  $f$  是可逆的.

从定义 2 看出: 如果映射  $f: A \rightarrow B$  有逆映射  $g: B \rightarrow A$ , 那么  $f$  的值域等于  $B$ , 并且  $A$  中不同的元素在  $f$  下的像不同. 从而  $f$  既是满射, 又是单射, 因此  $f$  是双射. 反之, 如果  $f$  是  $A$  到  $B$  的双射, 那么显然满足定义 2 中的条件, 从而  $f$  有逆映射, 因此  $f$  是可逆的. 这样我们证

明了下述结论：

**定理 1** 映射  $f: A \rightarrow B$  是可逆的充分必要条件为  $f$  是双射。  $\square$

定理 1 给出了判别映射  $f: A \rightarrow B$  是否为双射的一个方法：去探究  $f$  有没有逆映射，这比起去探究  $f$  是否既为满射又为单射可能简捷一些。

两个无限集之间是否存在双射？下面我们来看一个例子。

指数函数  $y=2^x$  的定义域是实数集  $\mathbf{R}$ ，值域是正实数集  $\mathbf{R}^+$ 。于是指数函数  $y=2^x$  是  $\mathbf{R}$  到  $\mathbf{R}^+$  的满射。由于指数函数  $y=2^x$  是增函数，因此不同的实数在这个映射下的像不同，从而指数函数  $y=2^x$  是单射。于是指数函数  $y=2^x$  是  $\mathbf{R}$  到  $\mathbf{R}^+$  的一个双射。即实数集  $\mathbf{R}$  与正实数集  $\mathbf{R}^+$  之间有一个一一对应： $x$  对应到  $2^x$ 。注意到  $\mathbf{R}^+$  是  $\mathbf{R}$  的真子集，可是它们的元素竟然可以一一对应，这是多么地奇妙！

1905 年，爱因斯坦(A. Einstein)发表了狭义相对论，他揭示了质点的总能量  $E$  与质量  $m$  之间的关系：

$$E = mc^2, \quad (1)$$

其中  $c$  是真空中光速，这就是著名的质能关系，这是一个多么优美的公式！这个公式为原子弹的制造和核动力的应用奠定了理论基础。按照这个公式，如果使粒子系统的质量减少  $\Delta m$ ，那么这个系统就会释放出  $(\Delta m)c^2$  的巨大能量，这就是原子弹爆炸时碎片动能的来源。

数学不仅在物理学中有大量的重要应用，而且在化学、生物、地理等自然科学，计算机科学，社会科学，人文学，经济学，医学，以及工程技术中都有应用。

数学的发展史上有许多重要的创新。1637 年，笛卡儿(R. Descartes)创建了解析几何；1666 年，牛顿(I. Newton)和莱布尼茨(G. W. Leibniz)创立了微积分。1776 年，瓦特(J. Watt)发明了蒸汽机。正是有了解析几何和微积分作为理论基础，才有以蒸汽机的发明为标志的工业革命的兴起与成功。

1829 年，罗巴切夫斯基(N. I. Lobatchevsky)创立了非欧几里得几何。他放弃了欧几里得几何的平行公设，而采用“过已知直线外一点可以至少作两条直线与已知直线平行”的假设。

1829~1831 年间，伽罗瓦(E. Galois)为了解决方程根式可解的判别准则问题创立了崭新的理论，后来被人们称为伽罗瓦理论，这引起了代数学发生革命性的变化，从以研究方程的根为中心转变为以研究各种代数系统的结构及其态射(保持运算的映射)为中心。

1847 年，布尔(G. Boole)创立了布尔代数。1946 年，J. W. Mauchly 与 J. P. Eckert 制造出了数字计算机。数字计算机的理论基础是布尔代数。计算机的普及和互联网的出现，使得世界进入了信息时代。

1936 年，柯尔莫哥洛夫(A. H. Колмогоров)提出了概率论的公理系统。概率论及以它为理论基础的数理统计在现代医学、经济学、信息安全与密码学等领域都有重要的应用。

数学的思维方式在数学创新中起着重要作用。一个重要的新的数学概念的提出，往往是

数学创新迈出的第一步. 而数学的思维方式告诉我们, 应当怎样通过观察客观现象, 抓住主要特征, 抽象出概念. 数学的定理不是数学家脑子里蹦出来的, 而是经过艰辛的探索, 猜测可能有什么结论, 然后进行严密的证明才得到的. 在探索过程中, 要运用解剖麻雀、直觉、归纳、类比、联想、逻辑推理等手段, 其中联想是至关重要的.

本课程以现代数学和信息时代有重要应用的数学知识, 以及数学发展史上若干重大创新为载体, 按照数学的思维方式讲授这些知识, 点评其中的创新点或创新的想法, 使同学们受到数学思维方式的熏陶和训练, 并且领略数学创新的风采. 讲授深入浅出, 通俗易懂, 从同学们生活中熟悉的例子引出数学概念; 引导同学们从具体的数学例子出发, 进行探索, 着重于创新的想法, 猜测可能有的规律; 然后通过深入分析、逻辑推理和计算等进行严密论证, 揭示出事物的内在规律.

### 习 题

1. 在区间  $\left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$  与  $[-1, 1]$  之间是否存在一个双射? 如果存在, 试举出一个例子.
2. 在区间  $[0, \pi]$  与  $[-1, 1]$  之间是否存在一个双射? 如果存在, 试举出一个例子.
3. 在实数集  $\mathbf{R}$  与开区间  $(0, 1)$  之间是否存在一个双射? 如果存在, 试举出一个例子.

从星期到模  $m$  剩余类环

星期一,星期二,……,星期日,周而复始.本章从人们最熟悉的这一现象,引出集合的划分与等价关系,提出模  $m$  剩余类的概念并且规定了它们的加法和乘法运算,进而抽象出模  $m$  剩余类环的概念.模  $m$  剩余类也可以进行加法和乘法,这是数学上的一个创新点,它开拓了人们的视野.从模 7 剩余类环的每个非零元都可逆,引出模 7 剩余类域的概念.当  $m$  为素数时,模  $m$  剩余类环是否一定是域?这需要研究素数的特性,为此研究了整数环的结构.模  $p$  ( $p$  是素数) 剩余类域在当今信息时代有重要应用.模  $m$  剩余类环  $\mathbb{Z}_m$  中可逆元的个数记做  $\varphi(m)$ ,称  $\varphi(m)$  是欧拉函数.我们运用现代数学研究结构和态射(即保持运算的映射)的观点,探索和论证了欧拉函数  $\varphi(m)$  的计算公式,并且简捷地证明了欧拉定理和费马小定理,在探索和论证  $\varphi(m)$  的计算公式时,需要利用中国剩余定理.中国剩余定理和欧拉函数在公开密钥密码学中有重要应用.

在本章中我们介绍了素数分布的研究成果,特别是 2006 年获得菲尔兹奖的陶哲轩关于素数等差数列的出色工作.

我们按照数学的思维方式讲述本章内容,既使同学们容易学习本章的数学知识(它们是学习本书第二、三章的基础),又使同学们从中受到数学思维方式的熏陶和训练.我们强调研究各种数学结构,是因为从求解一类一类的数学问题,到研究各种各样的数学结构,这是数学的创新过程.

## § 1.1 集合的划分与等价关系

下表是 2010 年 3 月份的月历:

日	一	二	三	四	五	六
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

显然,星期一是由无穷多天组成的集合,星期二、……、星期日也是. 如何表示星期一这个集合呢? 用列举法无法把属于星期一的无穷多天一一写出来,于是想到用描述法. 那么属于星期一的那些天的特征性质是什么呢? 为此我们把 2010 年 3 月 1 日对应到 1, 3 月 2 日对应到 2, …… , 3 月 31 日对应到 31, …… ; 把 2010 年 2 月 28 日对应到 0, 2 月 27 日对应到 -1, 2 月 26 日对应到 -2, …… . 这个对应法则就是时间长河中的所有日子组成的集合到整数集  $\mathbf{Z}$  的一个一一对应. 此时星期一、星期二、……、星期六、星期日分别是由什么样的整数组成的子集呢? 观察 2010 年 3 月份的月历可以看出: 星期一是由被 7 除后余数为 1 的整数组成的子集, 星期二是由被 7 除后余数为 2 的整数组成的子集, …… , 星期六是由被 7 除后余数为 6 的整数组成的子集, 星期日是由被 7 除后余数为 0 的整数(即能被 7 整除的整数)组成的子集, 把这些子集依次记成  $H_1, H_2, \dots, H_6, H_0$ . 即

$$\begin{aligned} H_1 &= \{7k + 1 \mid k \in \mathbf{Z}\}, \\ H_2 &= \{7k + 2 \mid k \in \mathbf{Z}\}, \\ &\dots \quad \dots \\ H_6 &= \{7k + 6 \mid k \in \mathbf{Z}\}, \\ H_0 &= \{7k \mid k \in \mathbf{Z}\}. \end{aligned}$$

于是  $\mathbf{Z}$  被分成了 7 个子集, 显然有

$$\mathbf{Z} = H_1 \cup H_2 \cup H_3 \cup H_4 \cup H_5 \cup H_6 \cup H_0, \quad H_i \cap H_j = \emptyset \text{ 当 } i \neq j.$$

从这个例子以及其他许多例子抽象出下述概念:

**定义 1** 如果集合  $S$  是它的一些非空子集的并集, 其中每两个不相等的子集的交为空集(此时称它们不相交), 那么把这些子集组成的集合称为  $S$  的一个划分.

在上述例子中,  $\{H_1, H_2, H_3, H_4, H_5, H_6, H_0\}$  是整数集  $\mathbf{Z}$  的一个划分.

如何给出集合  $S$  的一个划分呢?

从上面的例子看到: 两个整数  $a$  与  $b$  属于同一个子集当且仅当它们被 7 除后余数相同, 此时称  $a$  与  $b$  模 7 同余, 记做  $a \equiv b \pmod{7}$ , 读作“ $a$  同余于  $b$  模 7”或“ $a$  模 7 同余于  $b$ ”. 任给两个整数  $a$  与  $b$ , 要么  $a$  与  $b$  模 7 同余, 要么  $a$  与  $b$  模 7 不同余, 二者必居其一且只居其一. 很自然地可以把模 7 同余称为整数集  $\mathbf{Z}$  上的一个二元关系. 数学上如何给出集合  $S$  的二元关系的定义呢? 从  $\mathbf{Z}$  上的模 7 同余关系这个例子看到, 既然要考察任意两个整数有没有这个关系, 自然要考虑所有有序整数对组成的集合:



$$\{(a, b) \mid a, b \in \mathbf{Z}\}.$$

这类似于在平面笛卡儿直角坐标系中, 点的坐标组成的集合, 于是很自然地把上述集合称为  $\mathbf{Z}$  与自身的笛卡儿积, 记做  $\mathbf{Z} \times \mathbf{Z}$ . 一般地, 设  $S$  和  $M$  是两个集合, 下述集合

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

称为  $S$  与  $M$  的笛卡儿积. 记做  $S \times M$ .

由于整数  $a$  与  $b$  模 7 同余当且仅当  $a$  与  $b$  被 7 除后余数或者是 0, 或者是 1,  $\dots$ , 或者是 6, 因此

$$a \equiv b \pmod{7} \iff (a, b) \in \bigcup_{i=0}^6 H_i \times H_i,$$

其中  $\bigcup_{i=0}^6 H_i \times H_i = (H_0 \times H_0) \cup (H_1 \times H_1) \cup \dots \cup (H_6 \times H_6)$ . 由于  $H_i \times H_i$  是  $\mathbf{Z} \times \mathbf{Z}$  的一个子集,  $i=0, 1, \dots, 6$ , 因此  $\bigcup_{i=0}^6 H_i \times H_i$  是  $\mathbf{Z} \times \mathbf{Z}$  的一个子集. 由于  $(a, b)$  属于这个子集就表明  $a$  与  $b$  有模 7 同余关系,  $(a, b)$  不属于这个子集就表明  $a$  与  $b$  没有模 7 同余关系, 因此可以干脆把  $\mathbf{Z} \times \mathbf{Z}$  的这个子集  $\bigcup_{i=0}^6 H_i \times H_i$  就叫做  $\mathbf{Z}$  上的模 7 同余关系. 由此抽象出下述概念:

**定义 2** 设  $S$  是一个非空集合, 我们把  $S \times S$  的一个非空子集  $W$  叫做  $S$  上的一个二元关系. 如果  $(a, b) \in W$ , 那么称  $a$  与  $b$  有  $W$  关系, 记做  $aWb$ , 或记做  $a \sim b$ ; 如果  $(a, b) \notin W$ , 那么称  $a$  与  $b$  没有  $W$  关系.

$\mathbf{Z}$  上的模 7 同余关系具有下列性质:

- 1°  $a \equiv a \pmod{7}$ ,  $\forall a \in \mathbf{Z}^{\text{①}}$ , 称为反身性;
- 2° 若  $a \equiv b \pmod{7}$ , 则  $b \equiv a \pmod{7}$ , 称为对称性;
- 3° 若  $a \equiv b \pmod{7}$  且  $b \equiv c \pmod{7}$ , 则  $a \equiv c \pmod{7}$ , 称为传递性.

由此受到启发, 引出下述概念:

**定义 3** 集合  $S$  上的一个二元关系  $\sim$  如果具有下列性质:

- 1°  $a \sim a$ ,  $\forall a \in S$  (反身性);
- 2° 若  $a \sim b$ , 则  $b \sim a$  (对称性);
- 3° 若  $a \sim b$  且  $b \sim c$ , 则  $a \sim c$  (传递性),

那么称  $\sim$  是  $S$  上的一个等价关系.

$\mathbf{Z}$  上的模 7 同余关系就是  $\mathbf{Z}$  上的一个等价关系. 星期一就是由与 1 模 7 同余的整数组成的子集,  $\dots$ , 星期日是由与 0 模 7 同余的整数组成的子集. 由此受到启发, 引出下述概念.

**定义 4** 设  $\sim$  是集合  $S$  上的一个等价关系, 任给  $a \in S$ ,  $S$  的子集

$$\{x \in S \mid x \sim a\}$$

① 符号“ $\forall$ ”表示“任给”或“对任给的”之意. 下同.