邓胜兰　编著

抽象代数基础

机械工业出版社
CHINA MACHINE PRESS

配电子教案

抽象代数基础

邓胜兰　编著

机械工业出版社

抽象代数是研究计算机科学理论和技术的重要数学工具，在软件工程、数据库理论、数据挖掘、信息安全与保密等诸多领域中具有广泛而重要的应用。本书从一般的代数结构出发，依次讨论了群、环、域、格和布尔代数的基本概念和性质，同时介绍了抽象代数在计算机科学中的应用实例。

本书既可作为计算机专业本科生的教材或参考书，也可供通信、自动化等领域的工程技术人员自学使用。

图书在版编目（CIP）数据

抽象代数基础 / 邓胜兰编著. —北京：机械工业出版社，2011.1
ISBN 978-7-111-32982-4

Ⅰ. ①抽… Ⅱ. ①邓… Ⅲ. ①抽象代数 Ⅳ. ①0153

中国版本图书馆 CIP 数据核字（2011）第 000378 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
责任编辑：陈 皓 李 宁
责任印制：乔 宇

三河市宏达印刷有限公司印刷

2011 年 1 月第 1 版 • 第 1 次印刷
184mm×260mm • 15 印张 • 370 千字
0001－3000 册
标准书号：ISBN 978-7-111-32982-4
定价：32.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务
社服务中心：（010）88361066
销 售 一 部：（010）68326294
销 售 二 部：（010）88379649
读者服务部：（010）68993821

网络服务
门户网：http://www.cmpbook.com
教材网：http://www.cmpedu.com

封面无防伪标均为盗版

前　言

任何一门学科在其研究过程中都需要借助于数学方法和数学工具，计算机科学也不例外。作为信息科学和计算机科学的数学基础，离散数学和抽象代数在建立计算机的应用计算模型中发挥着越来越重要的作用。1936 年，图灵（A. M. Turing）在研究“可计算性”理论的过程中建立了著名的图灵机理论，为计算机的诞生从理论上奠定了基础。在计算机发展初期，利用命题逻辑、布尔代数理论研究开关电路，从而建立起一门完整的数字逻辑理论，对计算机的逻辑设计起了很大作用。之后，人们不断利用离散数学和抽象代数的方法和工具来解决计算机发展中遇到的各种问题。例如，利用代数结构研究编码理论，利用谓词逻辑研究程序正确性问题，利用图论研究操作系统的资源死锁问题，利用关系代数研究数据库，利用群和域的理论研究密码学，等等。

抽象代数是以代数结构作为研究对象的一门学科，是近代数学的一个重要分支。抽象代数的产生源于人们对高次方程根式求解问题的研究。抽象代数主要研究代数结构本身的特性以及代数结构之间的相互关系，它从结构的角度和整体的层次上揭示离散对象的特性及其关系，是描述和解决离散结构问题的重要工具。

抽象代数是一门具有挑战性的课程，因为它的研究内容和研究方法均具有高度的抽象性。读者不仅要学习它的基本概念、定义和定理，还应该学会一种新的思维方法，即基于公理的、严谨的推理方法。

本书是根据国防科技大学计算机软件专业的十多年教学实践经验，参考国内外相关教材，精心编著而成的。以计算机专业本科生为主要读者对象，力求深入浅出地、系统而完整地讲授抽象代数的基本概念和基础理论。精心安排章节内容，使其具有连贯性和条理性，避免定义和定理的杂乱堆砌。书中既有对定义、定理的严格描述和证明，也有通俗易懂的解释和说明，还包含丰富的例题、习题和部分习题参考答案。另外，书中专门有一章介绍抽象代数在计算机领域中的应用实例，以便读者了解抽象代数在研究计算机科学理论和技术中的重要性。本书使用的特殊符号参见附录 A。

本书的主要内容如下：

第 1 章介绍集合与映射的基本概念和主要性质，它们在抽象代数中用于研究代数结构之间的相互关系。

第 2 章介绍初等数论，它们是与抽象代数相关的数论基础知识，包括整除性、同余式与同余方程、欧拉定理和费马小定理等。

第 3 章介绍代数结构的基本概念，包括代数运算及其性质、代数结构与子代数结构、代数结构的同态与同构、代数结构的同余关系与同态定理、商代数与积代数等。后续章节的内容即是围绕这些基本概念展开的。

第 4 章介绍半群和群的基本概念和主要性质，包括子半群和半群同态、子群和群同态、陪集与 Lagrange 定理、正规子群与商群、置换群、循环群等。

第 5 章介绍环和域的基本概念和主要性质，包括子环与环同态、理想与商环、整环和域、多项式环、域的扩张、有限域、Galois 理论及其应用等。

第 6 章介绍格与布尔代数的基本概念和主要性质，包括格的公理体系和格的代数性质、模格和分配格、有界格和有补格、有限布尔代数、布尔表达式及布尔函数等。

第 7 章介绍抽象代数在计算机科学中的应用，以便读者了解抽象代数在研究计算机科学理论和技术中的重要性。

附录 A 列出了书中使用的特殊符号及其说明，以方便读者阅读。

附录 B 给出了部分习题的参考答案，以帮助读者学习。

由于作者水平有限，书中可能存在不妥之处，恳请同行、专家及读者批评指正。

作　者

目　录

第1章　集合与映射

集合和映射是数学中的基本概念，被应用于数学的各个分支，包括抽象代数。抽象代数以代数结构作为研究对象，需要利用集合和映射的许多性质来研究代数结构之间的相互关系。本章将介绍集合和映射的基本概念和主要性质，目的是为后面关于代数结构的讨论做准备。

1.1　集合

1.1.1　集合及其运算

集合是一些对象的总体，总体中的对象称为集合的**元素**或**成员**。如果 x 是集合 S 中的一个元素，则称 x 属于 S，记作 $x\in S$；如果 x 不是集合 S 中的元素，则称 x 不属于 S，记作 $x\notin S$。显然，任何一个元素要么属于某个集合，要么不属于某个集合，二者必居其一。

定义或表述一个集合的方法通常有两种：

（1）列举集合中的元素。例如，$A=\{1, 3, 5, 8\}$，$B=\{2, 4, 6, 8, \cdots\}$，$X=\{x_1, x_2, \cdots, x_k\}$。

（2）描述集合元素的性质。用谓词 $P(x)$表示 x 具有性质 P，用$\{x \mid P(x)\}$表示具有性质 P 的全体元素组成的集合。例如，$A=\{x \mid x$ 是英文字母$\}$，$B=\{x \mid x=2n+1, n\in \mathbf{Z}\}$，$X=\{x \mid x=y^2$ 且 y 是偶数$\}$。

定义 1-1　设 A 和 B 是两个集合，如果 A 中的每个元素都是 B 中的元素，则称 A 是 B 的**子集**，记作 $A\subseteq B$。也称 A 被 B **包含**，或 B 包含 A。

如果 A 不是 B 的子集，则 A 中至少有一个元素不属于 B，记作 $A\nsubseteq B$。

定义 1-2　设 A 和 B 是两个集合，如果 A 中的每个元素都是 B 中的元素，且 B 中的每个元素又都是 A 中的元素，则称 A 和 B **相等**，记作 $A=B$。

如果 A 中至少有一个元素不属于 B，或者 B 中至少有一个元素不属于 A，则称 A 和 B **不等**，记作 $A\neq B$。

集合之间的包含和相等是两个非常重要的概念，根据定义 1-2，显然有：$A=B$ 当且仅当 $A\subseteq B$ 且 $B\subseteq A$。

这个等价条件提供了证明两个集合相等的有效并且经常使用的方法。

定义 1-3　设 A 和 B 是两个集合，如果 $A\subseteq B$ 并且 $A\neq B$，则称 A 是 B 的**真子集**，或 B **真包含** A，记作 $A\subset B$。

【例 1-1】 整数集合 $\mathbf{Z}$ 是有理数集合 $\mathbf{Q}$ 的真子集，有理数集合 $\mathbf{Q}$ 是实数集合 $\mathbf{R}$ 的真子集，而实数集合是复数集合 $\mathbf{C}$ 的真子集，即有 $\mathbf{Z}\subset\mathbf{Q}\subset\mathbf{R}\subset\mathbf{C}$。

如果限定所讨论的集合都是某一集合 E 的子集，则称 E 为**全集**。不含任何对象的集合

称为**空集**，记作∅。显然，对任意集合 A，有$\varnothing \subseteq A$ 和 $A \subseteq E$。

定义 1-4 设 A 为一个集合，称由 A 的所有子集组成的集合为 A 的**幂集**，记作$\mathcal{P}(A)$，即有$\mathcal{P}(A)=\{x \mid x \subseteq A\}$。

用 $|A|$ 表示集合 A 中元素的数目。如果一个集合的元素数目是有限的，则称之为**有限集合**，反之称为**无限集合**。

定理 1-1 设 A 为一个有 n 个元素的集合，则有$|\mathcal{P}(A)|=2^n$。

证明 有两种方法计算$\mathcal{P}(A)$的大小。

第一种方法，考虑 A 的恰好包含 k 个元素的不同子集的数目，该数目是从 n 个元素中选取 k 个元素的组合计数$\binom{n}{k}$，所以有$|\mathcal{P}(A)|=\sum_{k=0}^{n}\binom{n}{k}=2^n$。

第二种方法，考虑为 A 的子集 X 选取元素的过程，对 A 的每个元素 x，都有选取 x 和不选取 x 两种选择，根据组合数学的乘法原理，X 共有 2^n 种不同选取方法。

定义 1-5 设 A 和 B 是两个集合，

（1）称由 A 和 B 的全体元素组成的集合为 A 和 B 的**并集**，记作 $A \cup B$，即 $A \cup B = \{x \mid x \in A \vee x \in B\}$；

（2）称由 A 和 B 的共同元素组成的集合为 A 和 B 的**交集**，记作 $A \cap B$，即 $A \cap B = \{x \mid x \in A \wedge x \in B\}$；

（3）称属于 A 但不属于 B 的元素组成的集合为 A 对 B 的**差集**，记作 $A-B$，即 $A-B=\{x \mid x \in A \wedge x \notin B\}$；

（4）称由 A 和 B 的非共同元素组成的集合为 A 和 B 的**对称差集**，记作 $A \oplus B$，即 $A \oplus B = \{x \mid x \in A-B \vee x \in B-A\}$；

（5）设 E 为全集，$A \subseteq E$，称 $E-A$ 为 A 的**补集**，记作$\sim A$ 或$\overline{A}$，即$\sim A=\{x \mid x \notin A\}$。

【例 1-2】 设 $A=\{a, b, c, d, e\}$，$B=\{a, b, e, g\}$，全集 $E=\{a, b, c, d, e, f, g, h\}$，则有

$$A \cup B=\{a, b, c, d, e, g\}$$
$$A \cap B=\{a, b, e\}$$
$$A-B=\{c, d\}$$
$$B-A=\{g\}$$
$$A \oplus B=\{c, d, g\}$$
$$\sim A=\{f, g, h\}$$
$$\sim B=\{c, d, f, h\}$$

如果集合 A 和集合 B 的交集为非空集，则称 A 与 B **相交**；否则，称 A 与 B **不相交**。

定理 1-2 设 A 和 B 是两个集合，则下面的命题是相互等价的。

（1）$A \subseteq B$；

（2）$A \cup B=B$；

（3）$A \cap B=A$。

证明 先证（1）⇔（2）。

若 $A \subseteq B$，即 A 中每个元素都属于 B，由并集的定义，有

$$A \cup B=\{x \mid x \in A \ \vee \ x \in B\}=\{x \mid x \in B\}=B$$

若 $A\cup B=B$，则对任意 $x\in A$，有 $x\in A\cup B$，从而有 $x\in B$，故 $A\subseteq B$。

再证（1）⇔（3）。

若 $A\subseteq B$，即 A 中每个元素都属于 B，由交集的定义，有

$$A\cap B=\{x\mid x\in A\ \wedge\ x\in B\}=\{x\mid x\in A\}=A$$

若 $A\cap B=A$，则对任意 $x\in A$，有 $x\in A\cap B$，从而有 $x\in B$，故 $A\subseteq B$。

定理 1-3 设 E 为全集，则对任意集合 A，B，C，下面的等式成立。

（1）$A\cup A=A$，$A\cap A=A$；

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

（3）$A\cup(B\cup C)=(A\cup B)\cup C$，$A\cap(B\cap A)=(B\cap A)\cap A$；

（4）$A\cup\varnothing=A$，$A\cap E=A$，$A\cap\varnothing=\varnothing$，$A\cup E=E$；

（5）$A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$，$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$；

（6）$A\cup\overline{A}=E$，$A\cap\overline{A}=\varnothing$；

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

（8）$\overline{A\cup B}=\overline{A}\cap\overline{B}$，$\overline{A\cap B}=\overline{A}\cup\overline{B}$。

证明 上述等式都可以由定义 1-5 直接推导得到，（1）～（4）留给读者证明。

（5）$$\begin{aligned}A\cup(B\cap C)&=\{x\mid x\in A\vee x\in(B\cap C)\}\\&=\{x\mid x\in A\vee(x\in B\wedge x\in C)\}\\&=\{x\mid(x\in A\vee x\in B)\wedge(x\in A\vee x\in C)\}\\&=\{x\mid x\in(A\cup B)\wedge x\in(A\cup C)\}\\&=(A\cup B)\cap(A\cup C)\end{aligned}$$

类似地可证明 $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$。

（6）由交集和并集的定义可知：

$$A\cup\overline{A}=\{x\mid x\in A\vee x\in\overline{A}\}=\{x\mid x\in A\vee x\notin A\}=E$$

$$A\cap\overline{A}=\{x\mid x\in A\wedge x\in\overline{A}\}=\{x\mid x\in A\wedge x\notin A\}=\varnothing$$

（7）利用（4）和（5）中的等式，有

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

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

（8）由（6）可知，对任意 $x\in E$，如果 $x\notin A$，则 $x\in\overline{A}$；反之，如果 $x\notin\overline{A}$，则 $x\in A$。所以有

$$\overline{A\cup B}=\{x\mid x\notin(A\cup B)\}=\{x\mid x\notin A\wedge x\notin B\}=\{x\mid x\in\overline{A}\wedge x\in\overline{B}\}=\overline{A}\cap\overline{B}$$

任取 $x\in\overline{A\cap B}$，由补集的定义可知 $x\notin(A\cap B)$，即 $x\in A$ 和 $x\in B$ 不能同时成立，由此得到 $x\notin A$ 或 $x\notin B$，所以有

$$\overline{A\cap B}=\{x\mid x\notin(A\cap B)\}=\{x\mid x\notin A\vee x\notin B\}=\{x\mid x\in\overline{A}\vee x\in\overline{B}\}=\overline{A}\cup\overline{B}$$

【例 1-3】 证明 $A\cap(B\oplus C)=(A\cap B)\oplus(A\cap C)$。

证明 由差集、对称差集和补集的定义可知：

$$A-B=\{x\mid x\in A\wedge x\notin B\}=\{x\mid x\in A\wedge x\in\overline{B}\}=A\cap\overline{B}$$

$$A\oplus B=\{x\mid x\in(A-B)\vee x\in(B-A)\}=(A-B)\cup(B-A)=(A\cap\overline{B})\cup(B\cap\overline{A})$$

所以有

$$
\begin{aligned}
(A\cap B)\oplus(A\cap C) &= ((A\cap B)\cap \overline{A\cap C})\cup((A\cap C)\cap \overline{A\cap B})\\
&= ((A\cap B)\cap(\overline{A}\cup\overline{C}))\cup((A\cap C)\cap(\overline{A}\cup\overline{B}))\\
&= ((A\cap B\cap \overline{A})\cup(A\cap B\cap \overline{C}))\cup((A\cap C\cap \overline{A})\cup(A\cap C\cap \overline{B}))\\
&= (A\cap B\cap \overline{C})\cup(A\cap C\cap \overline{B})\\
&= A\cap((B\cap \overline{C})\cup(C\cap \overline{B}))\\
&= A\cap(B\oplus C)
\end{aligned}
$$

定义 1-6 n 个集合 A_1，A_2，…，A_n 的**直积** $A_1\times A_2\times\cdots\times A_n$ 是由全体有序 n 元组$(a_1$，a_2，…，$a_n)$构成的集合，其中 $a_i\in A_i$，$1\leqslant i\leqslant n$。

两个有序 n 元组 $a=(a_1$，a_2，…，$a_n)$和 $b=(b_1$，b_2，…，$b_n)$是相等的，当且仅当它们的每个分量都相等，即 $a_i=b_i$，$1\leqslant i\leqslant n$。由此可以得到

$$|A_1\times A_2\times\cdots\times A_n|=|A_1|\cdot|A_2|\cdot\cdots\cdot|A_n|$$

如果 $A_1=A_2=\cdots=A_n$，记 $A_1\times A_2\times\cdots\times A_n$ 为 A^n。

【例 1-4】 设 $A=\{1,2\}$，$B=\{m,n\}$，$C=\{0\}$，$D=\varnothing$，则有

$$A\times B=\{(1,m),(1,n),(2,m),(2,n)\}$$
$$A\times C=\{(1,0),(2,0)\}$$
$$C\times A=\{(0,1),(0,2)\}$$
$$A\times D=\varnothing$$

注意 一般情况下，$A\times C\neq C\times A$。这说明集合的直积运算不满足交换律。

1.1.2 集合上的关系

在现实世界中，许多对象之间存在某种关联或联系。例如，学生与课程的关联，课程与教师的关联，教师与课题研究组的关联，等等。这些关联或联系用数学语言描述时就是集合上的关系。用两个元素 x 和 y 的有序对(x,y)可以表达 x 与 y 的关联，这是一种最直接的表达方式，其中元素 x 和 y 可以属于同一集合，也可以属于不同集合。有序对(x,y)的集合构成了集合上的关系。

定义 1-7 设 A 和 B 是集合，$A\times B$ 的子集称为 A 到 B 的一个**二元关系**，简称**关系**，通常用大写英文字母 R 表示。

如果有序对$(x,y)\in R$，表示 x **关联于** y，记作 xRy。如果$(x,y)\notin R$，表示 x **不关联于** y，记作 $x\not R y$。如果 R 是集合 A 到自身的关系，则称 R 是集合 A 上的关系。用 I_A 表示集合 A 上的**恒等关系**：

$$I_A=\{(a,a)\mid a\in A\}$$

【例 1-5】 令 D 是整数集合 $\mathbf{Z}$ 上的“整除”关系：对任意 a，$b\in\mathbf{Z}$，aDb 当且仅当 $a\mid b$，则$(3,12)\in D$，$(4,8)\in D$，$(5,12)\notin D$。

定义 1-8 设 R 是集合 A 上的关系。

（1）如果对任意 $x\in A$，均有 xRx，则称 R 是**自反的**。

（2）如果对任意 $x\in A$，均有 $x\not R x$，则称 R 是**反自反的**。

（3）如果对任意 x，$y\in A$，$xRy\Rightarrow yRx$，则称 R 是**对称的**。

（4）如果对任意 x，$y\in A$，$xRy\Rightarrow y\not R x$，则称 R 是**反对称的**。

（5）如果对任意 x，y，$z\in A$，xRy 且 $yRz \Rightarrow xRz$，则称 R 是**传递的**。

应该注意到，若一个关系 R 不具有“自反”性质，并不一定就具有“反自反”性质。因为在集合 A 中可能有部分元素使 xRx 成立，而另一部分元素使得 $x \not R x$ 成立。这说明“自反”性质与“反自反”性质不是互补的。同样，“对称”性质与“反对称”性质也不是互补的。

【例 1-6】 Σ^*是由字母表$\Sigma=\{a, b, \cdots, z\}$上定义的所有字符串组成的集合，在$\Sigma^*$上分别定义关系 R_1，R_2，R_3：对任意 x，$y\in \Sigma^*$，

$xR_1y \Leftrightarrow$ x 与 y 的长度相等；

$xR_2y \Leftrightarrow$ x 的长度大于 y 的长度；

$xR_3y \Leftrightarrow$ x 的某个前缀是 y 的一个真后缀，

则 R_1 是自反的、对称的和传递的；R_2 是反自反的、反对称的和传递的；R_3 既不是自反的也不是反自反的，因为 aaR_3aa 而 $ab \not R_3 ab$。实事上，R_3 不具有定义 1-8 中的任何性质。

定义 1-9 设 R 是集合 A 到集合 B 的关系，S 是集合 B 到集合 C 的关系，$R\circ S$ 是集合 A 到集合 C 的关系：对任意 $a\in A$，$c\in C$，

$$a(R\circ S)c \text{ 当且仅当存在 } b\in B \text{ 使得 } aRb \text{ 且 } bSc$$

称 $R\circ S$ 为 R 与 S 的**合成关系**。

【例 1-7】 R，S 都是集合 $A=\{1, 2, 3, 4, 5\}$上的关系，其中

$$R=\{(1, 2), (2, 2), (3, 4)\}$$
$$S=\{(1, 3), (2, 5), (3, 1), (4, 2)\}$$

则有

$$R\circ S=\{(1, 5), (2, 5), (3, 2)\}$$
$$S\circ R=\{(1, 4), (3, 2), (4, 2)\}$$

$R\circ S$ 和 $S\circ R$ 都是 A 上的合成关系，但是 $R\circ S\neq S\circ R$。由此可见，关系的合成运算不满足交换律。

定义 1-10 设 R 是集合 A 到集合 B 的关系，则有从集合 B 到集合 A 的关系：对任意 $a\in A$，$b\in B$，

$$bR^{-1}a \text{ 当且仅当 } aRb$$

称为 R 的**逆关系**，记作 R^{-1}。

不难验证，$R^{-1}\circ R=I_B$，$R\circ R^{-1}=I_A$。

定理 1-4 关系的合成运算满足结合律。

证明 设 R_1 是集合 A 到集合 B 的关系，R_2 是集合 B 到集合 C 的关系，R_3 是集合 C 到集合 D 的关系。需要证明 $R_1\circ(R_2\circ R_3)=(R_1\circ R_2)\circ R_3$。

由合成关系的定义可知：

$$R_1\circ R_2=\{(a, c)\mid (a, b)\in R_1 \text{ 且 } (b, c)\in R_2\}$$
$$R_2\circ R_3=\{(b, d)\mid (b, c)\in R_2 \text{ 且 } (c, d)\in R_3\}$$

所以有

$$\begin{aligned}R_1\circ(R_2\circ R_3)&=\{(a, d)\mid (a, b)\in R_1 \text{ 且 } (b, d)\in (R_2\circ R_3)\}\\&=\{(a, d)\mid (a, b)\in R_1 \text{ 且 } (b, c)\in R_2 \text{ 且 } (c, d)\in R_3\}\end{aligned}$$
$$(R_1\circ R_2)\circ R_3=\{(a, d)\mid (a, c)\in (R_1\circ R_2) \text{ 且 } (c, d)\in R_3\}$$

$$=\{(a,\ d)\mid (a,\ b)\in R_1 \text{ 且 } (b,\ c)\in R_2 \text{ 且 } (c,\ d)\in R_3\}$$

故 $R_1\circ(R_2\circ R_3)=(R_1\circ R_2)\circ R_3$。

令 R 是集合 A 上的关系，记 $R^0=I_A$，$R^1=R$，则有 $R^n=R^{n-1}\circ R$，称 R^n 为关系 R 的**幂**。

定理 1-5 集合 A 的关系 R 是传递的当且仅当 $R^2\subseteq R$。

证明 必要性。对任意 $(a,\ b)\in R^2$，则存在 $x\in A$，使得 $(a,\ x)\in R$，$(x,\ b)\in R$。因为 R 是传递关系，所以有 $(a,\ b)\in R$，故 $R^2\subseteq R$。

充分性。对任意 a，b，$c\in A$，如果 $(a,\ b)\in R$，$(b,\ c)\in R$，则有 $(a,\ c)\in R^2$。因为 $R^2\subseteq R$，故 $(a,\ c)\in R$，即 R 是传递的。

下面讨论两类重要的二元关系：等价关系和偏序关系。

定义 1-11 设 R 是集合 A 上的关系，如果 R 是自反的、对称的和传递的，则称 R 为集合 A 上的**等价关系**。

【例 1-8】 整数集合 $\mathbf{Z}$ 上的模 m 同余关系是一种重要的等价关系，这个关系将在第 2 章中进行详细讨论。对任意 a，$b\in\mathbf{Z}$，

$$a\equiv b\ (\mathrm{mod}\ m) \quad \text{当且仅当 } a \text{ 与 } b \text{ 除以 } m \text{ 的余数相等}$$

根据定理 2-19 可以证明：

$$a\equiv a\ (\mathrm{mod}\ m)$$

$$a\equiv b\ (\mathrm{mod}\ m)\Longrightarrow b\ (\mathrm{mod}\ m)\equiv a\ (\mathrm{mod}\ m)$$

$$a\equiv b\ (\mathrm{mod}\ m),\ b\equiv c\ (\mathrm{mod}\ m)\Longrightarrow a\equiv c\ (\mathrm{mod}\ m)$$

所以，同余关系是等价关系。

设 R 是集合 A 上的等价关系，对 A 中的任意元素 x，y，如果 xRy，则称 x 与 y **等价**，记作 $x\sim y$。令 $[a]_R$ 或 $[a]$ 表示所有与 a 等价的元素的集合，即

$$[a]_R=\{x\mid x\in A,\ xRa\}$$

称 $[a]_R$ 为 R 产生的元素 a 的**等价类**。

定理 1-6 设 R 是集合 A 上的等价关系，则由 R 产生的所有等价类是 A 的一个划分，即

（1）对 A 中的任意元素 a，b，或者 $[a]_R=[b]_R$，或者 $[a]_R\cap[b]_R=\varnothing$；

（2）$\bigcup\limits_{a\in A}[a]_R=A$。

证明 所谓集合的划分是并集等于全集但又互不相交的一组非空子集，如图 1-1 所示。

（1）对 A 中的任意元素 a，b，或者 aRb，或者 $a\not R b$。

当 aRb 时，如果 $x\in[a]_R$，则有 xRa，由 R 的传递性可知 xRb，所以 $[a]_R\subseteq[b]_R$；反之，如果 $x\in[b]_R$，则有 bRx，由 R 的传递性可知 aRx。所以，$[b]_R\subseteq[a]_R$。故 $[a]_R=[b]_R$。

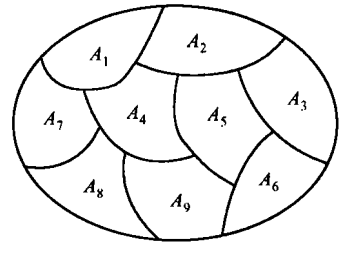

图 1-1 集合的划分

当 $a\not R b$ 时，假设 $[a]_R\cap[b]_R\neq\varnothing$，则存在 $x\in A$，使得

$$x\in[a]_R \text{ 且 } x\in[b]_R$$

则有 aRx，xRb，由 R 的传递性可知 aRb，此为矛盾。故 $[a]_R\cap[b]_R=\varnothing$。

（2）因为 A 中的每个元素 a 都唯一地属于一个等价类 $[a]_R$，所以有

$$\bigcup_{a\in A}[a]_R = A$$

从上面的讨论中不难得到，如果 R 是集合 A 上的等价关系，则有

$$a\,R\,b \Leftrightarrow [a]_R = [b]_R$$

$$a\,\not R\,b \Leftrightarrow [a]_R \cap [b]_R = \varnothing$$

因此，称集合 $\{[a]_R \mid a\in A\}$ 为 A 关于 R 的**商集**。

【例 1-9】 例 1-8 中的同余关系产生了整数集合 $\mathbf{Z}$ 的一个划分，即划分成 m 个等价类：

$$[0]，[1]，[2]，\cdots，[m-1]$$

它们称为模 m 的**同余类**。其中

$$[i] = \{mk + i \mid k\in\mathbf{Z}\}，\ 0\leqslant i\leqslant m-1$$

由定理 1-6 可知，由集合 A 上的等价关系 R 可以得到 A 的一个划分；反过来，由集合 A 的一个划分 $\{A_1，A_2，\cdots，A_n\}$ 也可以得到 A 上的等价关系 R。定义 R 为：

$$R = \{(a，b) \mid a \text{ 和 } b \text{ 在同一个子集 } A_i \text{ 中}\}$$

即对 A 中的任意元素 a，b：

$$a\,R\,b \Leftrightarrow \text{存在 } 1\leqslant i\leqslant n \text{ 使得 } a\in A_i \text{ 且 } b\in A_i$$

不难证明 R 是自反的、对称的和传递的。

定义 1-12 设 R 是集合 A 上的关系，如果 R 是自反的、反对称的和传递的，则称 R 为集合 A 上的**偏序关系**。通常用 $\leqslant$ 表示。

如果对 A 中的元素 a，b，或者 $a\leqslant b$，或者 $b\leqslant a$，则称 a 与 b **可比**。如果 A 中的任意两个元素 a，b 都是可比的，则 $\leqslant$ 是**全序关系**。

【例 1-10】 整数集合 $\mathbf{Z}$ 上的“大于或等于”关系是偏序关系，并且是全序关系，因为任何两个整数都可以比较大小。正整数集合 $\mathbf{Z}_+$ 上的“整除”关系也是偏序关系，但不是全序关系，因为有的正整数之间不存在整除关系。

定义 1-13 设 R 是集合 A 上的偏序关系，x，$y\in A$，如果 $x\leqslant y$ 且不存在 $z\in A$ 使得 $x\leqslant z\leqslant y$，则称 y **覆盖** x。

集合 A 上的偏序关系 $\leqslant$ 可以用哈斯图表示（见图 1-2），A 中的每个元素是一个结点。如果 A 中的元素 y 覆盖 x，那么 y 的位置在 x 的位置的上方，并且用一条边连接 x 和 y。显然，哈斯图只包含 A 中元素之间的覆盖关系，但利用偏序关系的自反、反对称和传递性，不难从中得到关于偏序关系的全部信息。

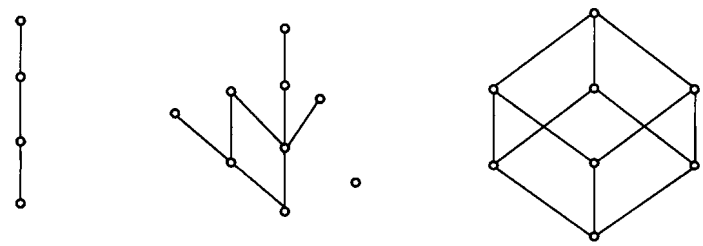

图 1-2 哈斯图

在哈斯图中，元素的位置代表了元素在偏序意义下的排序。如果存在从 x 到 y 的一条向上的链，则意味着 $x\leqslant y$，x 按照偏序排在 y 的前面。显然，如果 $\leqslant$ 是全序关系，则其哈斯图

就是一条链。如果$\leqslant$不是全序关系，则其哈斯图包含多条链。

假设有一个项目包含 n 个任务，某些任务只能在另一些任务结束之后开始进行。如何找到完成这些任务的正确顺序呢？为了对这个问题构造模型，我们建立一个任务集合上的偏序关系：使得 $a \leqslant b$，当且仅当任务 b 必须在任务 a 结束后才能开始，完成这些任务的顺序是任务集合上的一个全序关系。因此，需要解决的问题就是找到与任务偏序关系$\leqslant$相容的一个全序关系。

定义 1-14 设$\leqslant$是集合 A 上的偏序关系，R 是集合 A 上的全序关系，对任意 x，$y \in A$，如果 $x \leqslant y$，则有 xRy，称偏序关系$\leqslant$与全序关系 R 是**相容**的。从一个偏序关系构造全序关系的过程称为**拓扑排序**。

为了讨论拓扑排序算法，需要下面的定义和命题。

定义 1-15 设$\leqslant$是集合 A 上的偏序关系，$x \in A$，

（1）如果对任意 $y \in A$，$x \leqslant y \Rightarrow x = y$，则称 x 是 A 的**极大元**。

（2）如果对任意 $y \in A$，$y \leqslant x \Rightarrow x = y$，则称 x 是 A 的**极小元**。

命题 1-7 设$\leqslant$是非空有限集合 A 上的偏序关系，则 A 中存在极小元和极大元。

证明 任取 A 的一个元素 a_0。如果 a_0 不是极小元，那么存在 $a_1 \in A-\{a_0\}$，满足 $a_0 \leqslant a_1$。如果 a_1 不是极小元，那么存在 $a_2 \in A-\{a_0, a_1\}$，满足 $a_1 \leqslant a_2$。因为 A 是有限集合，所以这个过程一定结束并且得到 A 的极小元 a_k。

类似地，可得到 A 的极大元。

如果$\leqslant$是非空有限集合 A 上的偏序关系，则拓扑排序算法为：

1）$k=1$，$S=A$，$n=|A|$；

2）当 $k=1$，2，…，n 时，执行 3）和 4）；

3）寻找 S 中的极小元 a_k（由命题 1-7 可知 S 中存在极小元）；

4）从 S 中删除元素 a_k（$S \subseteq A$ 且$\leqslant$仍是 S 上的偏序关系）；

5）输出 a_1，a_2，…，a_n，结束。

1.2 映射

1.2.1 映射及其性质

在许多情况下，我们会为一个集合中的每个元素指派另一个集合的某个特定元素。例如，为本课程的每个学生从{A，B，C，D，E}中指定一个字母作为该学生的成绩，每个学生都对应一个唯一的字母，即有唯一的成绩。这种对应关系就是映射。

定义 1-16 设 A 和 B 是集合，如果有一个确定的法则 f，它将集合 A 中的每个元素 a 都对应成集合 B 的唯一确定的元素 b，则称 f 为从集合 A 到集合 B 的一个**映射**或**函数**，表示成 f：$A \to B$。

定义 1-17 如果元素 $a \in A$ 经过映射 f 变成元素 $b \in B$，则记作

$$f(a) = b \text{ 或 } f: a \mapsto b$$

称 b 为 a 在映射 f 下的**像**，或者映射 f 在 a 处的**值**，称 a 为 b 的**原像**。

如果 A 是一个积集，$A = A_1 \times A_2 \times \cdots \times A_n$，那么，元素 $a = (a_1, a_2, \cdots, a_n)$（$a_i \in A_i$，

$1 \leqslant i \leqslant n$）在映射 f：$A \to B$ 下的像为 $f(a_1, a_2, \cdots, a_n) = b \in B$，称 f 为**多元函数**。用 I_A 表示集合 A 上的**恒等映射**：

$$I_A: A \to A,\ I_A(a) = a$$

从映射 f：$A \to B$ 的定义看到，集合 A 中的每个元素在映射 f 的作用下均有像，并且有唯一的像，而集合 B 中的元素可能没有原像。集合 A 中的不同元素可能有相同的像，而集合 B 中的不同元素如果有原像，则必有不同的原像。由此可见，映射是一种特殊的二元关系 R：对 A 中的每个元素 a，在 R 中有且仅有一个有序对$(a, f(a))$。

【例 1-11】 下面是映射的例子。

（1）f：$\mathbf{R} \to \mathbf{R}$，$f(x) = x^2 + x - 1$ 是实数集合上的映射。

（2）h：$A \to \mathcal{P}(A)$，$h(x) = \{x\}$ 是从集合 A 到幂集$\mathcal{P}(A)$的映射。

（3）设 $V = \{a_1, a_2, \cdots, a_n\}$是 n 个任务的集合，定义映射 f：$V \to \mathbf{N}$，

$$f(a_i) = t_i,\ 1 \leqslant i \leqslant n$$

其中，t_i 是任务 a_i 的开始时间。映射 f 是对任务集合 V 的一个调度方案。

根据定义 1-16，映射 f：$A \to B$ 必须满足两个条件：

1）A 的每个元素有像，即对任意 $x \in A$，有 $f(x) \in B$；

2）A 的每个元素有唯一的像，即对任意 $x, y \in A$，若 $x = y$，则必有 $f(x) = f(y)$。

如果映射 f 满足上述两个条件，则称 f 是**良定义**的。因此，在定义一个映射时应该说明或证明它满足上面两个条件。

【例 1-12】 下面是非良定义的映射例子。

（1）f：$\mathbf{R} \to \mathbf{R}$，$f(x) = \sqrt{x}$。当 $x < 0$ 时，$f(x) \notin \mathbf{R}$。

（2）h：$\mathbf{Z} \to \mathbf{Z}$，$a \mapsto a$ 的正因子 b。显然 h 不满足像的唯一性。

定义 1-18 设 A 和 B 是集合，f：$A \to B$。集合 A 称为 f 的**定义域**，集合 B 称为 f 的**陪域**。集合 A 的全部元素在映射 f 下的全体像组成的集合称为 f 的**像集**或**值域**，记作 $f[A]$，

$$f[A] = \{b \mid b = f(a), a \in A, b \in B\}$$

如果 $S \subseteq B$ 中的每个元素有原像，则 S 的全部元素的原像组成的集合称为 S 的**原像集**，记作 $f^{-1}[S]$。图 1-3 是一个映射的图形表示，它解释了定义 1-18 提到的概念。

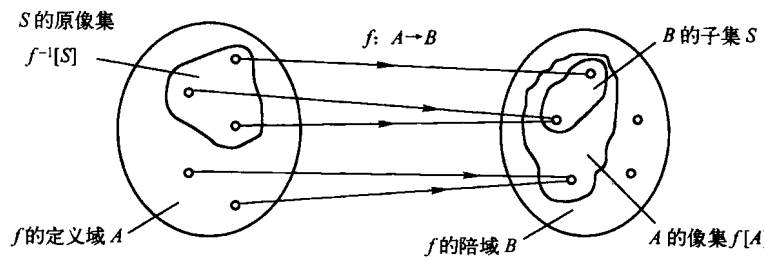

图 1-3　映射图

【例 1-13】 f：$\mathbf{Z} \to \mathbf{Z}$，$f(a) = a \pmod m$ 是整数集合上的映射，f 的像集是 $\mathbf{N}_m$，$\{1\}$的原像集是$\{km + 1 \mid k \in \mathbf{Z}\}$。

定义 1-19 设 f：$A \to B$ 和 g：$A \to B$。如果对任意 $x \in A$ 都有 $f(x) = g(x)$，则称映射 f 与 g **相等**，记为 $f = g$。