教育科学“十五”国家规划课题研究成果

离 散 数 学

杜忠复　陈兆均　主　编

高等教育出版社

内容提要

本书是教育科学“十五”国家规划课题“21世纪中国高等学校应用型人才培养体系的创新与实践”数学类子课题项目成果之一。

全书内容包括：集合论、关系、代数系统、图论和数理逻辑。本书避免先从数理逻辑开始，用逻辑联结词来处理各段内容，并简介了图论的实际应用问题，使学生易于接受。叙述上力求简单、直观易懂，选择大量且较为典型的例题、习题，以便于学生理解、消化。

本书可作为应用型院校计算机专业及相关专业的学生使用，也可供科技人员参考。

图书在版编目（CIP）数据

离散数学/杜忠复，陈兆均主编. —北京：高等教育出版社，2004.4

ISBN 7-04-014000-4

Ⅰ. 离… Ⅱ. ①杜… ②陈… Ⅲ. 离散数学-高等学校-教材 Ⅳ. O158

中国版本图书馆CIP数据核字（2004）第012770号

策划编辑 马 丽 责任编辑 丁鹤龄 封面设计 王凌波 责任绘图 朱 静
版式设计 王艳红 责任校对 俞声佳 责任印制

出版发行	高等教育出版社	购书热线	010-64054588
社 址	北京市西城区德外大街4号	免费咨询	800-810-0598
邮政编码	100011	网 址	http://www.hep.edu.cn
总 机	010-82028899		http://www.hep.com.cn
经 销	新华书店北京发行所		
印 刷			
开 本	787×960 1/16	版 次	年 月第1版
印 张	13.25	印 次	年 月 第 次印刷
字 数	240 000	定 价	15.70元

总　　序

为了更好地适应当前我国高等教育跨越式发展需要，满足我国高校从精英教育向大众化教育的重大转移阶段中社会对高校应用型人才培养的各类要求，探索和建立我国高等学校应用型人才培养体系，全国高等学校教学研究中心（以下简称“教研中心”）在承担全国教育科学“十五”国家规划课题——“21世纪中国高等教育人才培养体系的创新与实践”研究工作的基础上，组织全国100余所以培养应用型人才为主的高等院校，进行其子项目课题——“21世纪中国高等学校应用型人才培养体系的创新与实践”的研究与探索，在高等院校应用型人才培养的教学内容、课程体系研究等方面取得了标志性成果，并在高等教育出版社的支持和配合下，推出了一批适应应用型人才培养需要的立体化教材，冠以“教育科学‘十五’国家规划课题研究成果”。

2002年11月，教研中心在南京工程学院组织召开了“21世纪中国高等学校应用型人才培养体系的创新与实践”课题立项研讨会。会议确定由教研中心组织国家级课题立项，为参加立项研究的高等院校搭建高起点的研究平台，整体设计立项研究计划，明确目标。课题立项采用整体规划、分步实施、滚动立项的方式，分期分批启动立项研究计划。为了确保课题立项目标的实现，组建了“21世纪中国高等学校应用型人才培养体系的创新与实践”课题领导小组（亦为高校应用型人才立体化教材建设领导小组）。会后，教研中心组织了首批课题立项申报，有63所高校申报了近450项课题。2003年1月，在黑龙江工程学院进行了项目评审，经过课题领导小组严格的把关，确定了首批9项子课题的牵头学校、主持学校和参加学校。2003年3月至4月，各子课题相继召开了工作会议，交流了各校教学改革的情况和面临的具体问题，确定了项目分工，并全面开始研究工作。计划先集中力量，用两年时间形成一批有关人才培养模式、培养目标、教学内容和课程体系等理论研究成果报告和在研究报告基础上同步组织建设的反映应用型人才培养特色的立体化系列教材。

与过去立项研究不同的是，“21世纪中国高等学校应用型人才培养体系的创新与实践”课题研究在审视、选择、消化与吸收多年来已有应用型人才培养探索与实践成果基础上，紧密结合经济全球化时代高校应用型人才培养工作的实际需要，努力实践，大胆创新，采取边研究、边探索、边实践的方式，推进高校应用型人才培养工作，突出重点目标，并不断取得标志性的阶段成果。

教材建设作为保证和提高教学质量的重要支柱和基础，作为体现教学内容和教学方法的知识载体，在当前培养应用型人才中的作用是显而易见的。探索、建设适应新世纪我国高校应用型人才培养体系需要的教材体系已成为当前我国高校教学改革和教材建设工作面临的十分重要的任务。因此，在课题研究过程中，各课题组充分吸收已有的优秀教学改革成果，并和教学实际结合起来，认真讨论和研究教学内容和课程体系的改革，组织一批学术水平较高、教学经验较丰富、实践能力较强的教师，编写出一批以公共基础课和专业、技术基础课为主的有特色、适用性强的教材及相应的教学辅导书、电子教案，以满足高等学校应用型人才培养的需要。

我们相信，随着我国高等教育的发展和高校教学改革的不断深入，特别是随着教育部“高等学校教学质量和教学改革工程”的启动和实施，具有示范性和适应应用型人才培养的精品课程教材必将进一步促进我国高校教学质量的提高。

全国高等学校教学研究中心

2003 年 4 月

前　　言

离散数学是描绘一些离散量与量之间的相互逻辑结构及关系的学科。它的思想方法及内容已渗透到计算机科学的各个领域中。因此它成为计算机及相关专业的一门重要专业基础课。

本书是针对大学本科应用型人才培养目标及要求，适用于应用型本科计算机及相关专业的教材。在编写过程中，考虑到这一层次学生的特点及其培养要求，我们在内容上本着必需够用、突出思想方法的原则，选取了离散数学的主要内容：集合论、关系、代数系统、图论和数理逻辑五个部分。在教学实践中我们体会到：结构上，先从集合论入手，后介绍数理逻辑。这样做比先介绍数理逻辑，而只通过逻辑联结词，贯穿全书这种体系更便于学生学习。文字处理上力求简洁、通俗、直观易懂。为使学生能很好的消化理解书中内容，书中列举了大量的较为典型、易于接受、说明问题的例题，配备了相当数量的习题，也列举了部分实际应用问题。

本书由杜忠复、陈兆均主编，其中杜忠复编写第一~第四章，陈兆均编写第五章。全书最后由杜忠复统一定稿。全国高等教育研究会数学学科专业委员会副主任委员、吉林大学数学科学院博士生导师李辉来教授，详细的审阅了本书，提出了一些中肯的意见，作者向他表示衷心的感谢。

高等教育出版社数学策划编辑李艳馥同志，多年来在工作中从各方面给予作者大力的支持和帮助；我校的冯莹女士、赵宏伟老师在本书的编排工作中，也做了许多的工作。作者在这里也一并向她们表示真诚的谢意。

本书是作者在多年从事离散数学教学、总结教学经验的基础上编写而成，由于学识有限，不妥之处必定难免，敬请同行指正。

作者

2003 年 10 月于北华大学

目　　录

第一章　集 合 论

集合论简称集论. 这一数学分支是在 19 世纪初开始发展起来的. 德国数学家康托尔(G·Cantor)是集合论的奠基人. 现在，集合论的概念和方法已经渗透到所有的数学分支，并且改变了它们的面貌，因而各数学分支的完整体系，都是在所取集合上，设定其元素及子集的性质和运算的公理而构成. 所以，不熟悉集合论的原理就不可能对近代数学获得正确的理解. 本章就是先对集合论做一下简单介绍.

第一节　集合的概念

一、集合的概念

数学中的概念有两种定义形式. 其中，一种概念可以用严格的数学逻辑形式来定义，叫做可定义概念. 另一种则不能用严格形式来定义，而只能用语言对它进行大致的描述，叫做不可定义概念. 集合便属于后一种概念. 虽然我们不能给集合以确切的定义，但是一提到一个集合，我们便都清楚所指的是什么；这是因为所提集合中的事物都具有某种共同的性质. 为此我们有：

定义 1　把具有某种共同属性的事物的全体称为一个集合.

通常用大写字母 A、B、C、…、M 等表示集合. 集合中的每一事物叫做集合的元素. 常用小写字母 a、b、c 等表示集合中的元素.

以上只是对集合进行了一些描述，在研究具体问题时，还需把它具体表示出来. 集合的常用表示法有三种：

i）列举法：把集合中的元素一一列举出来，两端用花括号括之.

例 1　小于 5 的所有自然数集合.

$$A=\{0,1,2,3,4\}.$$

全体正奇数集合.

$$B=\{1,3,5,7,9,\cdots\}.$$

ii）描述法：若集合中元素 x 具有某种性质 $P(x)$，可在花括号内用语言叙述之，或可表成 $\{x \mid x$ 具有性质 $P(x)\}$，简记 $\{x \mid P(x)\}$.

例 2 ①全体有理数的集合.

$$A = \{x \mid x \text{ 是有理数}\}.$$

② 方程 $x^2-1=0$ 的解的集合.

$$B = \{x \mid x \text{ 是 } x^2-1=0 \text{ 的解}\}.$$

iii）图示法：用图形表示集合的方法. 例子略.

注意

1. 所谓给出一个集合，就是规定了这个集合是由哪些元素组成的. 并且，对于任意一个元素都能判定它是否是这个集合的元素，是这个集合的元素，或者不是这个集合的元素，二者必居其一.

2. 集合里若干个相同的元素，只能算作一个，也只用一个符号表示出来. 比如，$M=\{1,1,1,2\}$，元素 1 在集合 M 中虽出现三次，但元素 1 只能算作集合 M 的一个元素，通常写成 $M=\{1,2\}$，即集合里的元素是不重复出现的.

3. 集合里不考虑元素的顺序. 如 $\{a,b,c\}$，$\{b,c,a\}$，$\{a,c,b\}$ 似不相同，但从元素看来都认为是同一个集合.

一个元素 a，或者是集合 A 的元素，或者不是集合 A 的元素，二者必居其一. 元素与集合的这种关系叫做从属关系.

若 a 是集合 A 中的元素，就说 a 属于 A，记为 $a \in A$. “$\in$”读作“属于”. 若 a 不是集合 A 的元素，就说 a 不属于 A，记为 $a \notin A$ 或 $a \,\overline{\in}\, A$. “$\notin$”或“$\overline{\in}$”读作“不属于”.

例 3 $A=\{x \mid x$ 是自然数$\}$，则

$$3 \in A，10 \in A，0 \in A，\text{而} -5 \notin A.$$

二、集合间的关系

一个集合，如果它能包括我们所考虑的对象之内的全体元素. 则称此集合为全集合，简称全集，记为 E（或 X）.

例 4 在有理数集合内，讨论它的一些元素所成的集合. 像自然数集合，整数集合，奇数集合，方程 $x^2-1=0$ 的解集等等，都是一些有理数组成的集合. 而全体有理数构成的集合，包含了我们所考虑对象的全体元素，故在这里全体有理数集合便是一个全集合.

与全集相对应的，不包含任何元素的集合，则称为空集，记作$\varnothing$或 $\{\ \}$.

例 5 方程 $x^2+1=0$ 的实数解的集合便是空集.

定义 2 如果集合 A 与 B 之元素相同，则称这两个集合是相等的. 记为 $A=B$，否则称这两个集合为不相等，记为 $A \neq B$.

定义3　设有集合 A、B，如果对于任一 $a\in A$，都有 $a\in B$，则称集合 A 是集合 B 的子集合，或者说 B 包含 A. 记为 $B\supseteq A$ 或 $A\subseteq B$，“$\supseteq$”读作“包含”，“$\subseteq$”读作“包含于”. 若 $B\supseteq A$ 且有 $b\in B$ 但 $b\notin A$，则称 A 是 B 的真子集，或者说 B 真包含 A，记为 $B\supsetneqq A$ 或 $A\subsetneqq B$，“$\supsetneqq$”读作“真包含”，“$\subsetneqq$”读作“真包含于”.

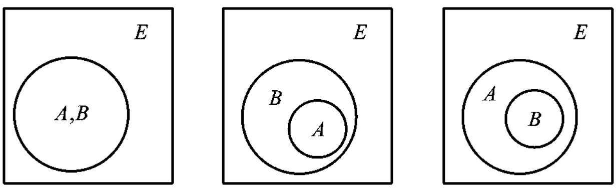
A 不被 B 包含或 B 不包含 A，记作 $A\nsubseteq B$ 或 $B\nsupseteq A$.

例6　① 设 $A=\{a,b,b,c\}$，$B=\{a,b,c\}$，则 $A=B$.

② 设 $A=\{1,2,3,\cdots,100\}$，$\mathbf{N}=\{0,1,2,3,\cdots\}$，则 $A\subseteq\mathbf{N}$ 且有 $A\subsetneqq\mathbf{N}$.

③ 设 $A=\{x\mid x\geqslant 5\}$，$B=\{x\mid x\geqslant 0\}$，则 $A\subseteq B$ 且有 $A\subsetneqq B$.

关于集合的一些属性，直观上可用图示法，即所谓的文氏（Venn）图来描述. 用矩形表示全集合，用圆表示集合. 子集合的概念，可用图1－1直观表示出来.



$A=B$　　$B\supseteq A$ 或 $B\supsetneqq A$　　$A\supseteq B$ 或 $A\supsetneqq B$

图1－1

关于集合还有：

定理1　任意集合 A，必有 $\varnothing\subseteq A$.

证　假设 A 不包含 $\varnothing$，则至少存在一个元素 x，$x\in\varnothing$；但 $\varnothing$ 中无有元素，故 $x\notin\varnothing$，与假设矛盾. 这个矛盾说明必有 $\varnothing\subseteq A$. 证毕.

定理2　对任意集合 A，都有 $E\supseteq A$.

定理3　对任意集合 A，必有 $\varnothing\subseteq A\subseteq E$.

定理4　设有集合 A、B，则 $A=B$ 充要条件是 $A\supseteq B$ 且 $B\supseteq A$.

证　**充分性**　设 $A\supseteq B$ 且 $B\supseteq A$. 假设 $A\neq B$，由定义2至少有一元素属于其中之一，而不属于另一集合. 令其为 x，且令 $x\in A$，而 $x\notin B$；但由于 $A\subseteq B$，故当 $x\in A$ 时必有 $x\in B$，与 $x\notin B$ 矛盾；同理对于 $x\in B$ 且 $x\notin A$ 亦可产生矛盾. 这表明必有 $A=B$.

必要性　设 $A=B$ 且假设 $A\supseteq B$，$B\supseteq A$ 至少有一个不成立；不妨设 $B\supseteq A$ 不成立，则必至少存在一个 $x\in A$ 且 $x\notin B$ 这与 $A=B$ 是矛盾的. 故 $A\supseteq B$ 且 $B\supseteq A$ 成立. 证毕.

练习题 1－1

1. 下列所述是否能组成集合？为什么？

（1）某本书所有的插图；

（2）所有小于 9 的自然数；

（3）太阳系所有的行星；

（4）平面上所有的圆；

（5）某次考试平均 80 分以上的人；

（6）所有高个人的全体；

（7）数学中的所有难题.

2. 令 $S=\{2,a,\{3\},b\}$，$M=\{\{a\},3,\{b\},1\}$，指出下列关系正确否？

（1）$\{a\}\in S$，（2）$3\notin S$，（3）$\{a\}\in M$，（4）$3\in M$，（5）$b\in M$.

3. 举出两个集合：

（1）一个集合是另一个集合的子集合；

（2）一个集合是另一个集合的真子集合；

（3）两个集合相等.

4. 集合 A、B、C 有 $A\subseteq B$ 且 $B\subseteq C$，证明：

$$A\subseteq C,$$

并举例说明.

5. 试问：集合 A 与集合 B 在什么条件下有 $B\subsetneqq A$ 和 $B\subseteq A$，同时成立？

6. * 证明：空集是惟一的.

第二节 集合的运算

一、集合的基本运算

定义 1 由集合 A、B 之所有元素合并组成之集合，叫做集合 A 与 B 的并集，记作 $A\cup B$. 即

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

例 1 若 $A=\{a,b,c,d\}$，$B=\{c,d,e,f\}$，则

$$A\cup B=\{a,b,c,d,e,f\}.$$

例 2 $A=\{x\mid x \text{ 是有理数}\}$，$B=\{x\mid x \text{ 是无理数}\}$，则 $A\cup B=\{x\mid x \text{ 是实数}\}$.

注意 两个集合的公共元素在并集中只能出现一次.

定义 2 由集合 A、B 所有的公共元素所组成的集合，叫做集合 A 与 B 的交集，记作 $A\cap B$. 即

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

例 3　若 $A = \{1,2,3,4\}$，$B = \{2,4,6,8\}$，则 $A \cap B = \{2,4\}$.

例 4　若 $A = \{x \mid x \geqslant 3\}$，$B = \{x \mid x \leqslant 7\}$，则 $A \cap B = \{x \mid 3 \leqslant x \leqslant 7\}$.

定义 3　集合 A、B 若满足 $A \cap B = \varnothing$，则称 A，B 是分离的.

例 5　$A = \{1,2,3\}$，$B = \{a,b,c\}$，则 $A \cap B = \varnothing$，即 A 与 B 是分离的.

定义 4　由集合 A、B 中所有属于 A，而不属于 B 的元素所组成之集合，叫做 A 与 B 的差集合，记作 $A - B$. 即

$$A - B = \{x \mid x \in A \text{ 但 } x \notin B\}.$$

例 6　$A = \{a,b,c,d\}$ 和 $B = \{b,c,e\}$，则 $A - B = \{a,b\}$，$B - A = \{e\}$.

定义 5　集合 A 之补集，记作 $\complement A$. 定义为 $\complement A = E - A$.

例 7　设 $E = \{0,1,2,3,\cdots\}$，$A = \{0,2,4,6,\cdots\}$，则

$$\complement A = E - A = \{1,3,5,7,\cdots\}.$$

定义 6　集合 A、B 之对称差，记作 $A \oplus B$. 定义为

$$\begin{aligned} A \oplus B &= (A - B) \cup (B - A) \\ &= \{x \mid (x \in A \text{ 且 } x \notin B) \text{ 或 } (x \in B \text{ 且 } x \notin A)\}. \end{aligned}$$

例 8　$A = \{1,2,3,4\}$，$B = \{3,4,5,6\}$，则 $A \oplus B = \{1,2,5,6\}$.

前面，我们定义了交集合，那里集合中的元素是定义中两个集合中公共元素，交集合是由这些公共元素作成的集合，而对称差与之正好相反，它恰是去掉二集合的所有公共元素，由剩下的所有元素组成的集合. 以上我们定义了集合中的六种基本运算均可通过文氏图，清楚地表示出来. 如图 1－2.

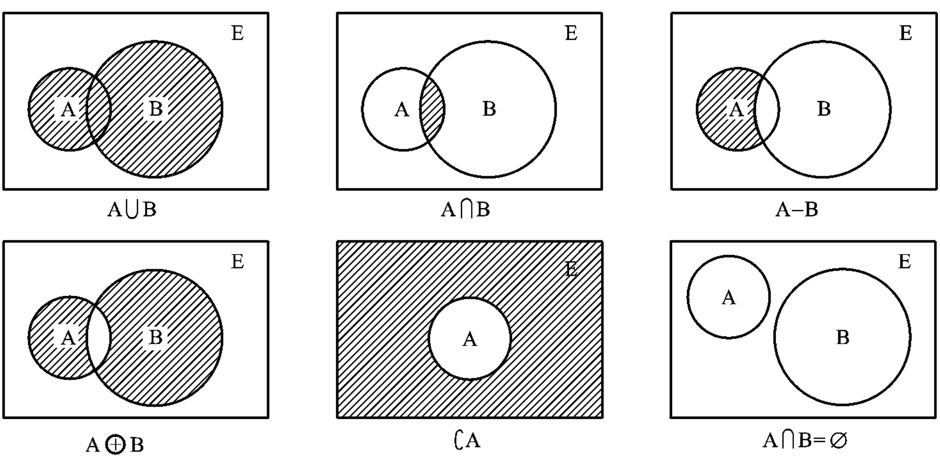


图 1－2

下面介绍几个集合运算的重要公式.

定理 1 对于任意的集合 A、B，有

$$A\cap B\subseteq A,\ A\cap B\subseteq B,$$
$$A\subseteq A\cup B,\ B\subseteq A\cup B.$$

证 $A\subseteq A\cup B$，$B\subseteq A\cup B$ 显然成立．其次，如果 $x\in A\cap B$，则 $x\in A$ 且 $x\in B$，故 $A\cap B\subseteq A$ 且 $A\cap B\subseteq B$．证毕．

定理 2 若 $A\subsetneqq B$，则 $A\cup B=B$，$A\cap B=A$.

证 设 $x\in A\cup B$，则 $x\in A$ 或 $x\in B$．若 $x\in A$，则由 $A\subsetneqq B$，可知 $x\in B$，总之有 $A\cup B\subseteq B$．由定理 1，有 $B\subseteq A\cup B$，故 $A\cup B=B$．同理 $A\cap B=A$．证毕．

定理 3 设 A、B 为任意集合，则有

a）$A-B=A\cap \complement B$.

b）$A-B=A-A\cap B$.

证 a）从略．

b）设 $x\in A-B$，即 $x\in A$ 且 $x\notin B$．故必有 $x\notin A\cap B$，因此 $x\in[A-(A\cap B)]$，即

$$A-B\subseteq[A-(A\cap B)].$$

又设 $x\in[A-(A\cap B)]$，则 $x\in A$ 且 $x\notin(A\cap B)$，即 $x\in A$ 且 $x\in\complement(A\cap B)$；$x\in A$ 且 $[x\in\complement A$ 或 $x\in\complement B]$．（注 $\complement(A\cap B)=\complement A\cup\complement B$ 后面将介绍．）但 $x\in A$ 且 $x\in\complement A$ 是不可能的，故只能有 $x\in A$ 且 $x\in\complement B$．由 a）即 $x\in A-B$，从而得到 $A-(A\cap B)\subseteq A-B$．因此

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

定理 4 设 A、B 为两个集合，若 $A\subseteq B$，则

a）$\complement B\subseteq\complement A$；

b）$(B-A)\cup A=B$.

证 a）若 $x\in A$，则 $x\in B$，因此 $x\notin B$ 必有 $x\notin A$，故 $x\in\complement B$，必有 $x\in\complement A$，即 $\complement B\subseteq\complement A$.

b）设 $x\in(B-A)\cup A$，则 $x\in B-A$ 或 $x\in A$．若 $x\in B-A$，则 $x\in B$；若 $x\in A$，由已知 $A\subseteq B$，应有 $x\in B$．因此，$(B-A)\cup A\subseteq B$.

反之，设 $x\in B$，由 $A\subseteq B$ 有，或者是 $x\in A$，或者是 $x\in B-A$，总之有 $x\in(B-A)\cup A$，即 $B\subseteq(B-A)\cup A$．因此

$$(B-A)\cup A=B.$$ 证毕．

二、集合的运算律

集合上的运算是用给定去指定一新的集合．如上我们所定义的六种运算便是如此．它们之间各种运算还可以混合进行，且运算遵循一定的规律，其一些

运算律如下：

（1）幂等律　$A\cup A=A.$

$A\cap A=A.$

（2）结合律　$(A\cup B)\cup C=A\cup(B\cup C).$

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

（3）交换律　$A\cup B=B\cup A.$

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

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

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

（5）　$A\cup\varnothing=A.$

$A\cap\varnothing=\varnothing.$

（6）　$A\cup E=E.$

$A\cap E=A.$

（7）　$A\cup\complement A=E.$

$A\cap\complement A=\varnothing.$

（8）吸收律　$A\cup(A\cap B)=A.$

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

（9）德·摩根律　$\complement(A\cup B)=\complement A\cap\complement B.$

$\complement(A\cap B)=\complement A\cup\complement B.$

（10）　$\complement\varnothing=E.$

$\complement E=\varnothing.$

（11）　$\complement\complement A=A.$

以上共介绍了二十一个恒等式，除最后一个外，其他的都是成对出现的. 我们现在来证其中的公式(9)德·摩根律，其他从略.

往证$\complement(A\cup B)=\complement A\cap\complement B$($\complement(A\cap B)=\complement A\cup\complement B$同理). 设$x\in\complement(A\cup B)$，则$x\in\!\!\!/\, A\cup B$，因此$x\notin A$且$x\notin B$，从而$x\in\complement A$且$x\in\complement B$，即$x\in\complement A\cap\complement B$，从而$\complement(A\cup B)\subseteq\complement A\cap\complement B$.

反之，设$x\in\complement A\cap\complement B$，则$x\in\complement A$且$x\in\complement B$，从而$x\notin A$且$x\notin B$，还有$x\notin A\cup B$，于是必有$x\in\complement(A\cup B)$，即$\complement A\cap\complement B\subseteq\complement(A\cup B)$. 故$\complement(A\cup B)=\complement A\cap\complement B$. 证毕.

三、例题

上面两段，我们介绍了集合的运算及运算律，现在通过几个例子，我们来观察一下，集合的运算律在运算过程及实际中的应用.

例 1　化简$(A\cup B)\cap(A\cup\complement B)$.

解 $(A\cup B)\cap(A\cup\complement B)\xlongequal{\text{分配律}}A\cup(B\cap\complement B)$

$$\xlongequal{\text{公式(7)}}A\cup\varnothing$$

$$\xlongequal{\text{公式(5)}}A.$$

例 2 **化简**$(A\cup B)\cup(\complement A\cap B)$.

解 $(A\cup B)\cup(\complement A\cap B)$

$$\xlongequal{\text{分配律}}[(A\cup B)\cup\complement A]\cap[(A\cup B)\cup B]$$

$$\xlongequal{\text{结合律}}[A\cup B\cup\complement A]\cap[A\cup B\cup B]$$

$$\xlongequal{\text{交换律、(7)、幂等律}}(E\cup B)\cap(A\cup B)$$

$$\xlongequal{(6)}E\cap(A\cup B)$$

$$\xlongequal{(6)}A\cup B.$$

例 3 **证明若** $A\cup B=A\cap B$，**则** $A=B$.

证 $A\xlongequal{\text{吸收律}}A\cup(A\cap B)\xlongequal{\text{已知条件}}A\cup(A\cup B)\xlongequal{(2)}(A\cup A)\cup B\xlongequal{(1)}A\cup B.$

而 $B\xlongequal{\text{吸收律}}B\cup(B\cap A)\xlongequal{\text{已知条件}}B\cup(B\cup A)\xlongequal{(2)}(B\cup B)\cup A\xlongequal{(1)}A\cup B.$

故得 $A=B$. **证毕.**

例 4 **某图书馆有藏书 100 万册，有一读者前往查阅，他希望了解 19 世纪法国的以描写农民生活为题材的长篇小说，以及 1979 年出版的，我国的，不是描写“文化大革命”的长篇小说之书名. 请将此读者所要了解之书名用集合论的方法描述之.**

解 令 E 表示该图书馆全体藏书之集合；

A：所有法国图书之集合；

B：所有 19 世纪的书组成的书名集合；

C：所有描写农民生活题材长篇小说的书组成的书名集合；

D：所有长篇小说所组成的书名集合；

F：所有 1979 年出版的书的书名集合；

G：所有中国的书之书名集合；

H：所有描写“文化大革命”长篇小说的书之书名集合，

则此读者所要了解之书可用集合方式描述为

$$D\cap[(B\cap A\cap C)\cup(F\cap G\cap\complement H)].$$

此例只是集合论在实际中的一个简单应用，它的应用绝不只于此，这里我们不再一一赘述.

练习题 1 – 2

1. 设 $A=\{x\mid x<5, x\in \mathbf{N}\}$，$B=\{x\mid x<7, x$ 是正偶数$\}$，(N 是自然数集合) 求：
 $A\cup B$，$A\cap B$，$A-B$，$B-A$，$A\oplus B$.
2. 设 $A=\{x\mid x$ 是 book 中的字母$\}$，$B=\{x\mid x$ 是 black 中的字母$\}$ 求：
 $A\cup B$，$A\cap B$，$A-B$，$B-A$，$A\oplus B$.
3. 证明：a) $\complement\varnothing=E$.　　　　b) $\complement E=\varnothing$.
4. 简化下列集合运算：

(1) $(A\cup B)\cap(A\cup B)$.

(2) $(A\cup B)\cup(A\cup B)$.

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

(4) $(A\cap\complement B)\cup(B\cap\complement A)\cup(A\cap B)$.

(5) $(A\cup B\cup\complement C)\cap(\complement A\cap\complement B\cap C)$.

5. 设 A、B、C 为三个集合，则
$A\cap(B-C)=(A\cap B)-(A\cap C)$.
6. 应用集合的运算证明：

(1) $A-(B\cup C)=(A-B)-C$.

(2) $A-(B-C)=(A-B)\cup(A\cap C)$.

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

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

(5) $(A\cup B)\cup(B-A)=A\cup B$.

7. 设 A、B 为任一集合，证明 $A\subseteq B$ 的充要条件为 $A\cap\complement B=\varnothing$.
8. 设全集 $E=\{x\mid x$ 是自然数$\}$，如下是它的子集：
 $A=\{1,2,7,8\}$，$B=\{x\mid x^2<50\}$，
 $C=\{x\mid x$ 可被 3 整除$, 0\leqslant x\leqslant 30\}$，
 $D=\{x\mid x=2^k, k$ 是正整数 $0\leqslant k\leqslant 6\}$.

求下列集合：

(a) $A\cup[B\cup(C\cup D)]$.　　　　(b) $A\cap[B\cap(C\cap D)]$.

(c) $B-(A\cup C)$.　　　　(d) $(\complement A\cap B)\cup D$.

9. (a) 已知 $A\cup B=A\cup C$ 是否必须 $B=C$？

(b) 已知 $A\cap B=A\cap C$ 是否必须 $B=C$？

(c) 已知 $A\oplus B=A\oplus C$ 是否必须 $B=C$？

第三节　幂集合与笛卡儿乘积

一、幂集合

定义 1 设 A 是一集合，A 的幂集合 $\rho(A)$，是 A 的所有子集作元素所组成的集合(其中包括空集 $\varnothing$ 及 A 自身).

例 1 设 $A=\{a,b,c\}$，则 A 有子集：

$A_1=\varnothing$，$A_2=\{a\}$，$A_3=\{b\}$，$A_4=\{c\}$，$A_5=\{a,b\}$，$A_6=\{a,c\}$，

$A_7=\{b,c\}$，$A_8=\{a,b,c\}$.

因此 A 的幂集合为

$$\rho(A)=\{\varnothing,\{a\},\{b\},\{c\},\{a,b\},\{a,c\},\{b,c\},\{a,b,c\}\}.$$

一个给定集合的幂集合是惟一的，因此求一个集合的幂集合是以集合为运算对象的一元运算.

从上面例子我们看到，求一个集合的幂集，关键是把它的所有子集全部找到，然而一个集合究竟有多少个子集呢？下面的定理便回答了这一问题.

定理 1 若集合 A 为由 n 个元素所组成之有限集合，则 $\rho(A)$ 为有限且由 2^n 个元素组成. 即 A 有 2^n 个子集.

证 我们将 $\rho(A)$ 中之每个元素(即 A 之子集)与一个二进制数建立一一对应关系. 设 $A=\{a_1,a_2,a_3,\cdots,a_n\}$，我们建立一个 n 位二进制数；b_1，b_2，$\cdots$，b_n，当 A 的某一子集出现有 a_i 时，则对应之 b_i 为 1，当不出现 a_i 时，则对应之 b_i 为 0. 这样，任一个 A 的子集就与一个二进制数建立一一对应关系：给一个二进制数可得到一个 A 的子集，反之，给一个 A 的子集可得到一个二进制数，而 n 位二进制数共有 2^n 个数，因此可知 $\rho(A)$ 之元素共为 2^n 个. 证毕.

例 2 设集合 $A=\{a,b,c\}$，则 $\rho(A)$ 共有 $2^3=8$ 个元素. 若 $A=\varnothing$，则 $\rho(A)$ 共有 $2^0=1$ 个元素，即 $\rho(A)=\{\varnothing\}$.

显见，即使 A 为空集，$\rho(A)$ 与 A 也是不同.

例 3 $A=\{a\}$，则 $\rho(A)=\{\varnothing,\{a\}\}$.

以上我们只介绍了有限个元素的集合情形，对集合为无限个元素时，仍有幂集之说，若 A 是无限元素之集，则 $\rho(A)$ 也含有无限元素，细节从略.

二、笛卡儿乘积

在实际生活中，有许多事物是成对出现的，而这种成对出现的事物. 具有一定的顺序. 例如，上、下；左、右；$2<7$；平面上点的坐标. 一般地有：

定义 2 两个按一定顺序排列之客体；a，b 组成一个有序列，我们叫做序偶，并记作 (a,b).

加上面我们所说的便可记为(上、下)；(左,右)；$(2,7)$；(x,y). 序偶反映了两个客体之间的顺序，当顺序不同时，序偶也是不同的. 如：$(x,y)\neq$

(y,x)，$(2,7)\neq(7,2)$.

定义 3　两个序偶相等：$(a,b)=(c,d)$，如果 $a=c$，$b=d$.

注意　序偶中的二元素(客体)不一定来自同一个集合，它们可以来自不同的集合. 如 a 代表自然数，b 代表人的身高，则 a，b 也可作成序偶(a,b)或(b,a)；但上述两种约定，一经确定，序偶的顺序就不能再变化了. 在序偶(a,b)中，a 称为第一客体，b 称为第二客体.

以上序偶的概念，可以推广到任意 n 元组上去，即所谓的 n 重有序组. 一般地有：

定义 4　n 个$(n>1)$按一定顺序排列之客体 a_1，a_2，…，a_n 组成一个有序序列，叫做 n 重有序组，并记为$(a_1,a_2,\cdots,a_n)$.

同样还有：

定义 5　两个 n 重有序组相等：

$(a_1,a_2,\cdots,a_n)=(b_1,b_2,\cdots,b_n)$，如果 $a_i=b_i$，$i=1$，2，…，n.

例 4　某校某系某专业某班之学生可以用四重有序组(a,b,c,d)表示.

有了上面序偶的概念，利用它我们引入笛卡儿乘积的概念.

定义 6　集合 A，B 之笛卡儿乘积可表为

$$A\times B=\{(a,b)\mid a\in A,b\in B\}.$$

例 5　平面上直角坐标中之所有点可用一笛卡儿乘积表示.

$$\mathbf{R}\times\mathbf{R}=\{(x,y)\mid x\in\mathbf{R},y\in\mathbf{R}\}.$$

例 6　若 $A=\{a,b\}$，$B=\{1,2,3\}$. 求 $A\times B$，$B\times A$，$A\times A$，$B\times B$ 以及$(A\times B)\cap(B\times A)$.

解

$A\times B=\{(a,1),(a,2),(a,3),(b,1),(b,2),(b,3)\}$.

$B\times A=\{(1,a),(1,b),(2,a),(2,b),(3,a),(3,b)\}$.

$A\times A=\{(a,a),(a,b),(b,a),(b,b)\}$.

$B\times B=\{(1,1),(1,2),(1,3),(2,1),(2,2),(2,3),(3,1),(3,2),(3,3)\}$.

$(A\times B)\cap(B\times A)=\varnothing$.

笛卡儿乘积仍为一集合，这时集合中的每一个元素为序偶. 它还可以推广到 n 个集合 A_1，A_2，…，A_n 上去.

定义 7　集合 A_1，A_2，…，A_n 之笛卡儿乘积可表为

$$A_1\times A_2\times\cdots\times A_n=\{(a_1,a_2,\cdots,a_n)\mid a_i\in A_i,i=1,2,\cdots,n\}.$$

例 7　若 $A=\{a\}$，$B=\{c,d\}$，$C=\{\alpha,\beta\}$，则

$A\times B=\{(a,c),(a,d)\}$.

$A\times B\times C=\{(a,c,\alpha),(a,c,\beta),(a,d,\alpha),(a,d,\beta)\}$.

关于笛卡儿乘积有：

定理2　设 A，B，C 为任意三个集合，则有

a) $A\times(B\cup C)=(A\times B)\cup(A\times C)$.

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

c) $(A\cup B)\times C=(A\times C)\cup(B\times C)$.

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

证　略.

关于笛卡儿乘积显然有 $A\times B\neq B\times A$. 当 $A_1=A_2=\cdots=A_n=A$ 时，记

$$A^n=A_1\times A_2\times\cdots\times A_n.$$

下面我们再从图形上说明一下笛卡儿乘积. 如，$A=\{a,b,c\}$，$B=\{\alpha,\beta\}$，则 $A\times B$ 可由图 1－3 表示.

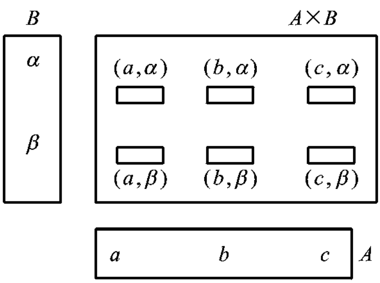


图 1－3

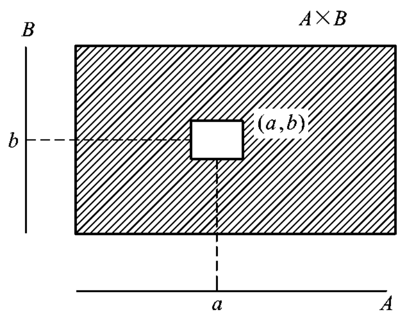


图 1－4

一般地，两集合 A 与 B 的笛卡儿乘积，可以通过图 1－4 表示.

练习题 1－3

1. 设 $A=\{a,b\}$，求出 $\rho(A)\times A$ 及 $A\times\rho(A)$，$\rho(A)\times\rho(A)$.
2. 设 $A=\{0,1\}$，$B=\{1,2\}$ 确定下面集合.

(a) $A\times\{1\}\times B$；(b) $A^2\times B$；(c) $(B\times A)^2$.

3. 证明：若 $A\times A=B\times B$，则 $A=B$.
4. 证明：若 $A\times B=A\times C$，且 $A\neq\varnothing$，则 $B=C$.
5. 设 $A=\varnothing$，求 $\rho(A)$，$\rho(\rho(A))$，$\rho(\rho(\rho(A)))$.
6. 指出下列各式是否成立.

(a) $(A\cup B)\times(C\cup D)=(A\times C)\cup(B\times D)$.

(b) $(A-B)\times(C-D)=(A\times C)-(B\times D)$.

(c) $(A\oplus B)\times(C\oplus D)=(A\times C)\oplus(B\times D)$.

(d) $(A-B)\times C=(A\times C)-(B\times C)$.

(e) $(A \oplus B) \times C=(A \times C) \oplus(B \times C)$.

7. 对任意集合 A，B 证明

$\rho(A) \cup \rho(B) \subseteq \rho(A \cup B)$.

$\rho(A) \cap \rho(B) \subseteq \rho(A \cap B)$.

举例说明：$\rho(A) \cup \rho(B) \neq \rho(A \cup B)$.

第四节　集合概念的扩展

一、无限集

本段我们介绍一下无限集里的一些简单的概念. 为此我们先给出如下定义：

定义 1　设 A，B 为集合，若有一个规则 f，对于每一个 $x \in A$，惟一确定一个 $y \in B$，那么，就说 f 是 A 到 B 的一个映射（变换）.

若 f 是 A 到 B 的一个映射，当 $x \neq y$ 时，有 $f(x) \neq f(y)$，$\forall x$，$y \in A$，就说 f 是 A 到 B 的一个单射. 若对于任意 $y \in B$ 均存在 $x \in A$，使 $f(x)=y$，那么，就说 f 是 A 到 B 的一个满射. 若一个映射 f，既是单射，又是满射，则称 f 是 A 到 B 的一一映射（或称双射、或称 A 与 B 是 1—1 对应）.

例 1　设 $A=\{a_1, a_2, a_3\}$，$B=\{1,2,3\}$，令 $\varphi(a_i)=i$，$i=1$，2，3，则 A 与 B 是 1—1 对应的. 设 $A_1=\{a_2, a_3\}$，则 A_1 是 A 的真子集，显然 A 与 A_1 不存在 1—1 对应.

例 2　设 $\mathbf{N}=\{0,1,2,3,4,5,6, \cdots\}$，$\mathbf{Z}=\{\cdots,-3,-2,-1,0,1,2,3, \cdots\}$.

令 φ 使

$$
\begin{array}{rcccccccc}
\mathbf{N}: & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\
 & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \cdots\cdots, \\
\mathbf{Z}: & 0 & 1 & -1 & 2 & -2 & 3 & -3 & 4
\end{array}
$$

则可见上述对应关系 φ 使 $\mathbf{N}$ 与 $\mathbf{Z}$ 是 1—1 对应的. 设 $N_0=\{2,4,6,8,10, \cdots\}$，令 $\varphi(i)=2i$，$i=1$，2，3，4，…，则 $\mathbf{N}$ 与 N_0 便是 1—1 对应的. 显然 N_0 还是 $\mathbf{N}$ 的真子集.

例 1 中，A_1 是 A 的真子集，而 A_1 不能与 A 之间 1—1 对应. 例 2 中 N_0 是 $\mathbf{N}$ 的真子集，而 N_0 与 $\mathbf{N}$ 却是 1—1 对应的. A_1 与 N_0 所处地位相同，都是某集之真子集，为什么谈到对应时，所得的结果却不一样呢？我们仔细观察一下就会发现，这是由于它们（A_1 与 N_0）的母体（A 与 $\mathbf{N}$）的不同所导致的. A 中的元素为有限个，而 $\mathbf{N}$ 中的元素显然是无限个. 那么，有限集与无限集究竟有何

差别呢？从上面的例子我们便可看到二者各自的属性，同时也清楚了二者的差别. 对于 N 它能与 N_0（其真子集）有 1—1 对应，对于其他无限集合也易证明，它们也具有与某个真子集 1—1 对应的性质. 由此我们便可从数学角度给出无限集合之定义.

定义 2 设 A 为一集合，若存在 A 的真子集 A_1，使 A 与 A_1 之间存在1—1 对应，则称 A 为无限集.

如，$A=\{x \mid -\infty<x<+\infty\}$，$B=\{y \mid y$ 为有理数$\}$ 二者均为无限集.

由无限集之定义及上面的例子可见有限集是不具有与真子集 1—1 对应的性质.

二、并集、交集的推广

两个集合的并、交的概念，可以推广到有限个集合或无限个集合的情况.

定义 3 由 n 个集合 A_1，A_2，…，A_n 的元素的全体（重复的元素只算一次）组成的集合，称为这 n 个集合的并集. 记为

$$\bigcup_{i=1}^{n} A_i=A_1 \cup A_2 \cup A_3 \cup \cdots \cup A_n.$$

定义 4 由一列集合 A_1，A_2，…，A_n，…的元素的全体（重复元素只算一次）组成的集合，称为这一列集合的并集. 记为

$$\bigcup_{n=1}^{\infty} A_i=A_1 \cup A_2 \cup A_3 \cup \cdots \cup A_n \cup \cdots.$$

例 3 设 $A_i=\{i\}\ (i=1,2,3,\cdots)$，则

$$\bigcup_{i=1}^{n} A_i=\{1\} \cup\{2\} \cup \cdots \cup\{n\}=\{1,2,\cdots,n\}.$$

$$\bigcup_{i=1}^{\infty} A_i=\{1\} \cup\{2\} \cup \cdots \cup\{n\} \cup \cdots=\{1,2,\cdots,n,\cdots\}.$$

例 4 设 A_i 为区间 $[i-1,i]\ (i=1,2,\cdots)$，则

$$\bigcup_{i=1}^{n} A_i=[0,1] \cup[1,2] \cup \cdots \cup[n-1,n]=[0,n].$$

$$\bigcup_{i=1}^{\infty} A_i=[0,1] \cup[1,2] \cup \cdots \cup[n-1,n] \cup \cdots=[0. tif,+\infty).$$

定义 5 同时属于 n 个集合 A_1，A_2，…，A_n 的元素的全体组成的集合，称为这个 n 个集合的交集. 记为

$$\bigcap_{i=1}^{n} A_i=A_1 \cap A_2 \cap A_3 \cap \cdots \cap A_n.$$

定义 6 同时属于一列集合 A_1，A_2，…，A_n，…的元素的全体组成的集合，称为这一列集合的交集. 记为

$$\bigcap_{i=1}^{\infty} A_i = A_1 \cap A_2 \cap A_3 \cap \cdots \cap A_n \cap \cdots.$$

例 5　设 $A_i = \{i\}$　$(i = 1,2,\cdots)$，则

$$\bigcap_{i=1}^{n} A_i = \varnothing，\bigcap_{i=1}^{\infty} A_i = \varnothing.$$

设 $A_i = \{x \mid -i \leqslant x \leqslant i\}, i = 1,2,3,\cdots$，则

$$\bigcap_{i=1}^{n} A_i = \{x \mid -1 \leqslant x \leqslant 1\}，$$

$$\bigcap_{i=1}^{\infty} A_i = \{x \mid -1 \leqslant x \leqslant 1\}.$$

在上述的有限集或无限集的情形，集合 A_i 的下标 i 也是一个集合，这个集合或是不包含 0 的自然数集合 $\mathbf{N}^*$（无限情形），或是 $\mathbf{N}^*$ 的前 n 个元素组成的 $\mathbf{N}^*$ 的子集（有限情形）. 近代数学中还要用到更为广泛的标的集合. 设 Γ 是任一集合（Γ 可以是自然数集合，也可以是其他任意的集合），α 是 Γ 的一个元素，对于每一个 $\alpha \in \Gamma$，相应地有一个以 α 为下标的集合 A_α. 这时，所有的集合 A_α 组成一个集系：

$$D = \{A_\alpha \mid \alpha \in \Gamma\}.$$

于是有如下并集，交集的定义：

定义 7　由所有 $A_\alpha(\alpha \in \Gamma)$ 的元素的全体（重复的只算一次）组成的集合，称为所有 $A_\alpha(\alpha \in \Gamma)$ 的并集. 记为

$$\bigcup_{\alpha \in \Gamma} A_\alpha \quad \left(\text{或} \bigcup_{\alpha} A_\alpha\right).$$

定义 8　同时属于所有 $A_\alpha(\alpha \in \Gamma)$ 的元素的全体组成的集合，称为所有 $A_\alpha(\alpha \in \Gamma)$ 的交集. 记为

$$\bigcap_{\alpha \in \Gamma} A_\alpha \quad \left(\text{或} \bigcap_{\alpha} A_\alpha\right).$$

注意　在这里 $\cup$ 或 $\cap$ 的下部标明 $\alpha \in \Gamma$ 或 α 的意义都是指要求遍历 Γ（即取遍 Γ 中的所有元素）. 本段前面关于并集、交集的定义，都是为自然数集合或其子集的情况，这里说明不一定全是自然数集或其子集.

如，设 Γ 为区间 $[0.\ tif, +\infty)$，A_α 是区间 $(-\alpha, \alpha)$，B_α 是区间 $(0, \alpha)$，则

$$\bigcup_{\alpha \in \Gamma} A_\alpha = (-\infty.\ tif, +\infty)， \qquad \bigcap_{\alpha \in \Gamma} A_\alpha = \{0\}$$

$$\bigcup_{\alpha \in \Gamma} B_\alpha = (0.\ tif, +\infty)， \qquad \bigcap_{\alpha \in \Gamma} B_\alpha = \varnothing.$$

三、基数与可数集

在抽象地研究集合时（即对于集合中的元素的性质不加考虑时），一个集

合中元素的多少应该是最基本的概念．对于由有限多个元素作成的集合，表示元素的多少自然就是元素的个数．空集的元素的个数是零，而任意一个不空的有限集合的元素的个数则一定是一个正整数．为了求得一个有限集合 M 的元素的个数，我们只要一个个地去数它的元素就可以了，数到最后的那个数是多少，元素的个数就是多少．但是我们一个个地数集合 M 中的元素，事实上也就是给 M 中每一个元素都编上一个号，比如数到了 5，那就是说从集 M 中挑出了一个元素 a，把它叫做第五号，因此一个集合 M 如果含有 n 个元素，则经过这个数的过程以后，就排成了下述形状：

$$M=\{a_1,a_2,a_3,\cdots,a_n\}.$$

现在我们假设 $M=\{a'\}$ 是另外一个也是由 n 个元素组成的集合，则它自然也可以排成

$$M'=\{a'_1,a'_2,a'_3,\cdots,a'_n\}.$$

因为两个集合 M 和 M' 的元素个数是相同的，因此两个地方的 n 是同一个，如果我们叫 M 中的元素 a_i 与 M' 中的元素 a'_i 对应起来（$i=1,2,3,\cdots,n$），则这个对应关系是一对一的，反之如果另有一个集合 $M''=\{a''\}$，它的元素 a'' 能与 M 的元素 a 之间 1—1 对应起来，则 M 的元素的个数也自然就应该是 n.

以上我们说明了一个极为重要的事实，即要说明两个有限集合 M 和 M' 具有同样多的元素，我们并不需要真正知道它们的元素的个数，比如都是由 1 000 个元素组成，而只要能在它们的元素之间能建立起一个 1—1 对应的关系来就可以了．这个事实启示我们，如何去研究无穷集合中元素的多少，因为对于无穷集合来说，“元素的个数”这个概念是完全没有意义的.

定义 9 设有集合 A 和 B，如果存在对应关系 φ，使 A 与 B 成为 1—1 对应，则称 A 和 B 是等势的（或对等的），记作 $A\sim B$（注意 $A\sim B$ 与 $A=B$ 不一样）.

定义 10

（1）对于有限集合 A，称与 A 等势的那个惟一的自然数为 A 的基数，记作 $\overline{\overline{A}}$.

（2）自然数集合 $\mathbf{N}$ 的基数记作 $\aleph_0$（读作阿列夫零），即 $\overline{\overline{\mathbf{N}}}=\aleph_0$.

（3）实数集 $\mathbf{R}$ 的基数记作 $\aleph$（读作阿列夫），即

$$\overline{\overline{\mathbf{R}}}=\aleph$$

显然，两个集合“具有相同的基数”是有限集合的“具有同样多的元素”这概念的推广，因为对于有限的集合来说，A 和 B 具有相同的基数的充要条件是它们的元素的个数相同.

例 6 设 A 是全体正整数所作成的集合，B 是全体负整数所作成的集合，则 $A\sim B$．事实上只要令 A 中的每一 n 对应 B 中的 $-n$ 即可.

例 7　设 A 是开区间 $(0,1)$ 上所有的点作成的集合，B 是半轴 $(0.\,tif，+\infty)$ 上所有的点作成的集合，则 $A \sim B$.

证　设 C 是图 1－5 所划线段上的点作成的集合（不算端点）．通过从 P 点的中心投影，我们自然可以将 C 中的 z 和 B 中元素 y 之间 1—1 对应起来，而另一方面通过将线段往 Ox 轴上的垂直投影又可以将 A 中的点 x 与 C 中的点 z 之间 1—1 对应起来，于是 A 中的点 x 与 B 中的点 y 通过 z 就 1—1 对应起来了．证毕.

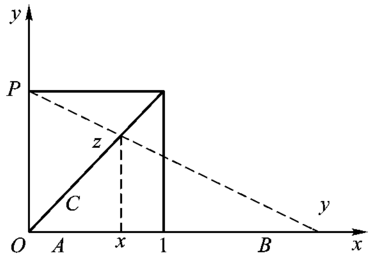


图 1－5

定义 11　设 A、B 是二集合，假如 A 与 B 的某子集 1—1 对应，而 A 不能与 B 本身 1—1 对应，则我们说 A 的基数 $\overline{\overline{A}}$ 小于 B 的基数 $\overline{\overline{B}}$，即 $\overline{\overline{A}} < \overline{\overline{B}}$，或 $\overline{\overline{B}} > \overline{\overline{A}}$.

显然，此定义是有限集合 A 的元素个数小于有限集合 B 的元素的个数这个概念的推广，因为若 A 的元素的个数是 n，B 的元素的个数是 m，$n<m$，则 A 必然可以和一个由 n 个属于 B 的元素所作成的一个 B 的子集 B^* 之间 1—1 对应．关于基数我们有

定理 1（Zermelo）　设 A 与 B 为二集合，则下述情况恰有一个成立.

a）$\overline{\overline{A}} < \overline{\overline{B}}$，　b）$\overline{\overline{B}} < \overline{\overline{A}}$，　c）$\overline{\overline{A}} = \overline{\overline{B}}$.

此定理又称作三岐性定律.

定理 2（Cantor-Schroder-Bernstein）　设 A 与 B 为二集合，如果 $\overline{\overline{A}} \leqslant \overline{\overline{B}}$ 且 $\overline{\overline{B}} \leqslant \overline{\overline{A}}$，则 $\overline{\overline{A}} = \overline{\overline{B}}$.

以上两个定理的证明从略．下面我们介绍可数集合.

定义 12　凡与自然数集 **N** 有相同基数之集叫做可数集.

因为自然数所作成的集合 **N** 是可以排成一个无穷序列形式的，即

$$0，1，2，3，4，5，\cdots，n，\cdots.$$

因此任何可数集合 M 也一定可以将其排成无穷序列形式

$$a_0，a_1，a_2，a_3，a_4，a_5，\cdots，a_n，\cdots.$$

反之，若一集合 M，它的元素可排成上述序列形式，则 M 一定是可数的．关于可数集有：

定理 3　任意无穷集合 A，必含有一可数集.

证　从 A 中取出一个元素 a_1，因 A 是无穷的，故可以在 A 中取出另一元素 a_2，依此可得一无穷集合 $A' = \{a_1, a_2, \cdots\}$，集合 A' 为可数集且 $A \supseteq A'$.

定理 4　可数集之无穷子集仍为一可数集.

证　设有一可数集 $A = \{a_1, a_2, a_3, a_4, \cdots\}$，若 A^* 是 A 的一个无穷子集，则

所有属于 A^* 的 a 的下标的全体作成的集合 $\mathbf{N}^*$ 是自然数集合 $\mathbf{N}$ 的一个子集，而 $\mathbf{N}$ 的任一子集中的元素都可按其元素的大小排成一列，故 $\mathbf{N}^*$ 是一可数集，从而 A^* 是一可数集. 证毕.

定理 5 有理数集 $\mathbf{Q}$ 为可数集.

此定理的证明留给读者自己证. 可数集合之基数记为$\aleph_0$（念作 Aplph 零），则自然数集合 $\mathbf{N}$ 的基数为$\aleph_0$，记为 $\overline{\overline{\mathbf{N}}}=\aleph_0$. 也许有人会问是不是所有无穷集合均是可数的呢？不然.

定理 6 实数集 $\mathbf{R}$ 是不可数的.

证 令 $t=\tan\frac{\pi}{2}x$，$x\in(-1,1)$，则可见集合$(-1,1)$与实数集 $\mathbf{R}$ 有相同基数，要证 $\mathbf{R}$ 不可数只须证$(-1,1)$不可数，同样只须证$(0,1)$不可数即可. 采用反证法：

假设$(0,1)$内之点（无一遗漏的）可排成 x_1，x_2，…，x_n，…，即$(0,1)$可数. 把每个 x_i 写成无穷小数之形式：

$$x_1=0.a_{11}a_{12}\cdots a_{1n}\cdots,$$
$$x_2=0.a_{21}a_{22}\cdots a_{2n}\cdots$$
$$\cdots\cdots\cdots\cdots$$
$$x_n=0.a_{n1}a_{n2}\cdots a_{nn}\cdots.$$

令 $x=0.a_1a_2a_3\cdots a_n\cdots$，则 $x\in(0,1)$，取 $a_n=1$ 或 2，但 $a_n\neq a_{nn}$（若 $a_{nn}=1$，则取 $a_n=2$；若 $a_{nn}=2$，则取 $a_n=1$），$n=1$，2，…，可见 $x\neq x_n$，$n=1$，2，…. 这与上面的说法矛盾. 此矛盾说明$(0,1)$是不可数的，由对应关系 $\mathbf{R}$ 是不可数的. 证毕.

由这个定理可知实数集的基数不是$\aleph_0$，它比$\aleph_0$要大，我们记为$\aleph$，或以 C 表示之，称做连续统的势.

但是，在无限集中除了$\aleph_0$与$\aleph$以外是否还有其他更大基数之集合存在呢？德国数学家康托尔（Cantor）证明了，对任何一个集合 A，它的幂集 $\rho(A)$ 之基数一定比 A 的基数大. 康托尔还认为，$\aleph_0$与$\aleph$之间没有其他基数存在，也就是说$\aleph$是$\aleph_0$后第一个比$\aleph_0$大的基数，这就是有名的连续统假设.

由上面所述，我们知道了：

（1）无限集也有大小，最小的无限集是可数集，其次是实数集，等等；

（2）对任一个无限集，总存在一个基数大于这个集合之集合；即无限集的“大小”是无限的.

练习题 1－4

1. 若 A 与 B 是无限集合，C 是有限集合，回答下述问题，并说明理由.

(a) $A\cap B$ 是无限集合吗？

(b) $A-B$ 是无限集合吗？

(c) $A\cup C$ 是无限集合吗？

2. 证明：(a) 集合 $[0,1]$ 是无限集合；

(b) 自然数集合 $\mathbf{N}$ 是无限集合.

3. 设 $A_K=\left[-1+\dfrac{1}{K},1-\dfrac{1}{K}\right]$ $(K=1,2,\cdots)$，求

(1) $\bigcup\limits_{K=1}^{n}A_K$， $\bigcup\limits_{K=1}^{\infty}A_K$，

(2) $\bigcap\limits_{K=1}^{n}A_K$， $\bigcap\limits_{K=1}^{\infty}A_K$.

4. 设 $A=\left\{x \mid x\text{ 为有理数}, |x|<\dfrac{1}{n}\right\}$ $(n=1,2,\cdots)$，求

$\bigcup\limits_{n=1}^{\infty}A_n$， $\bigcap\limits_{n=1}^{\infty}A_n$

5. 证明下列每组集合 A 与 B 有相同的基数.

(a) $A=(0,1)$，$B=(0,2)$；

(b) $A=\mathbf{N}$，$B=\mathbf{N}\times\mathbf{N}$，$\mathbf{N}$ 为自然数集合；

(c) $A=\mathbf{R}$，$B=(0,\infty)$，$\mathbf{R}$ 为实数集合；

(d) $A=[0,1)$，$B=\left(\dfrac{1}{4},\dfrac{1}{2}\right]$.

6. 证明，所有整数集是可数集合.

7. 证明，有理数集是可数集合.

8. 设 $A=\{x \mid x\text{ 是有理数 }0<x<1\}$，$B=\{x \mid x\text{ 是无理数 }0<x<1\}$，证明 $\overline{\overline{A}}<\overline{\overline{B}}$.

复 习 题 一

1. 判定下列各题是否成立？说明理由.

(1) $a\in\{\{a\}\}$，(2) $\{a\}\in\{\{a\}\}$，(3) $\{a\}\subseteq\{\{a\}\}$，(4) $\{a\}\in\{\{a\},a\}$，

(5) $\{a\}\subseteq\{\{a\},a\}$，(6) $\varnothing\subseteq\varnothing$，(7) $\varnothing\subseteq\{\varnothing\}$，(8) $\varnothing\in\{\varnothing\}$.

2. 设 A、B、C 是任意集合，问

(1) 如果 $A\in B$，$B\in C$，则 $A\in C$ 吗？

(2) 如果 $A\in B$，$B\subseteq C$，则 $A\in C$ 吗？

(3) 如果 $A\in B$，$B\subseteq C$，则 $A\subseteq C$ 吗？

(4) 如果 $A\subseteq B$，$B\subseteq C$，则 $A\in C$ 吗？

(5) 若 $A\cap B=A\cap C$，$\complement A\cap B=\complement A\cap C$，证明 $B=C$.

(6) 若 $A\cap B\subseteq A\cap C$，$\complement A\cap B=\complement A\cap C$，证明 $A\subseteq B$.

(7) $A\subseteq B$ 和 $A\in B$ 是否会同时成立？

3. 设 A、B 为任意集合，则 $A\cup B=\varnothing$ 的充要条件为 $A=B=\varnothing$.

4. 设 A、B 为任意集合，则 $A\cap B=E$ 的充要条件为 $A=B=E$.

5. 设 A、B、C 为任意集合，且 $A\subseteq C$，证明

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

6. 证明 $A\times B=B\times A$ 充要条件是 $A=\varnothing$ 或 $B=\varnothing$ 或 $A=B$.

7. 证明 $A\oplus A=\varnothing$，$A\oplus\varnothing=A$.

8. 证明 $(A-B)-C=(A-C)-(B-C)$.

9. 证明 $(A\cap B)\times(C\cap D)=(A\times C)\cap(B\times D)$.

10. 列出下列集合的全部子集合

(a) $\{\varnothing\}$.

(b) $\{\varnothing,\{\varnothing\}\}$.

(c) $\{\{\varnothing,a\},\{a\}\}$.

(d) $\{\{a,b\},\{a,a,b\},\{b,a,b\}\}$.

11. 设 A、B、C 是集合，证明或否定以下断言：

(a) $A\notin B$ 且 $B\notin C$，则 $A\notin C$；

(b) $A\in B$ 且 $B\notin C$ 则 $A\notin C$；

(c) $A\subsetneqq B$ 且 $B\notin C$ 则 $A\notin C$.

12. 确定以下各式：

$\varnothing\cap\{\varnothing\}$，$\{\varnothing\}\cap\{\varnothing\}$，$\{\varnothing,\{\varnothing\}\}-\varnothing$，$\{\varnothing,\{\varnothing\}\}-\{\varnothing\}$，$\{\varnothing,\{\varnothing\}\}-\{\{\varnothing\}\}$

13. 求下列集合：

(1) $A\cup(B\cup(\complement A\cup\complement B))$；

(2) $A\cap(B\cap(\complement A\cap\complement B))$；

(3) $(A\cup B)\cap(A\cup B)\cup(A\cup B)$；

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

14. 设 $A_1=\{0,1\}$，$A_2=\left\{0,\frac{1}{2},1\right\}$，$A_3=\left\{0,\frac{1}{4},\frac{1}{2},\frac{3}{4},1\right\}$，

$$A_4=\left\{0,\frac{1}{8},\frac{1}{4},\frac{3}{8},\frac{1}{2},\frac{5}{8},\frac{3}{4},\frac{7}{8},1\right\},$$

…………

$$A_n=\left\{0,\frac{1}{2^{n-1}},\frac{2}{2^{n-1}},\frac{3}{2^{n-1}},\cdots,\frac{2^{n-1}-1}{2^{n-1}},1\right\}.$$

求：(1) $\bigcup\limits_{k=1}^{n}A_k$；(2) $\bigcap\limits_{k=1}^{n}A_k$；(3) $\bigcup\limits_{k=1}^{\infty}A_k$；(4) $\bigcap\limits_{k=1}^{\infty}A_k$.

15. 确定下列集合的幂集

(1) $\{a,b,c\}$； (2) $\{\{a,b\},\{c\}\}$；

(3) $\{a,\{b\}\}$； (4) $\{1,\varnothing,\{\varnothing\}\}$.

16. $S_n=\{a_0,a_1,\cdots,a_n\}$ 和 $S_{n+1}=\{a_0,a_1,\cdots,a_n,a_{n+1}\}$，试用 $\rho(S_n)$ 和 a_{n+1} 表达出 $\rho(S_{n+1})$.

17. 已给 $S=\{2,a,\{3\},4\}$ 和 $R=\{\{a\},3,4,1\}$，指出下列哪些是正确的，哪些是错误的：

(1) $\{a\} \in S$；　(2) $\{a\} \in R$；

(3) $\{a, 4, \{3\}\} \subseteq S$；　(4) $\{\{a\}, 1, 3, 4\} \subsetneqq R$；

(5) $R = S$；　(6) $\{a\} \subseteq S$；

(7) $\{a\} \in R$；　(8) $\varnothing \subseteq R$；

(9) $\varnothing \subseteq \{\{a\}\} \subseteq R \subseteq E$；　(10) $\{\varnothing\} \subseteq \{\{3\}, 4\}$.

18. **如果两集合** A_1 **和** A_2 **是可数的，则** $A_1 \times A_2$ **也是可数的**.

19. **有限集** A **和可数集** B **的笛卡尔乘积** $A \times B$ **是可数的**.

20. **若** A**、**B **是可数集，且** $A \cap B = \varnothing$**，则** $A \cup B$ **可数**. **由此可推出当不考虑** $A \cap B = \varnothing$**时，** $A \cup B$ **仍可数**.

21. **如果** A **是不可数无穷集，**B **是** A **的可数子集，则** $A - B \sim A$.

第二章　关　系

关系是一个基本概念，日常生活中我们经常碰到关系这一概念. 如：兄弟关系；同志关系；位置关系等. 在数学中关系可表示集合中元素间的联系. 如"5小于7"；"a大于b"等. 而"5小于7"；"a大于b"均可用序偶$(5,7)$；(a,b)表出. 本章我们就来从数学角度介绍一下关系，它的重要性及作用通过进一步的学习我们会慢慢看到.

第一节　关系的基本概念

一、关系的定义

定义1　$A\times B$的子集R叫做A到B的一个二元关系，简称A到B的一个关系.

从定义可见A到B的一个关系是一个集合，其中的元素是由序偶组成.

关系R中序偶的第一个客体所允许的选取对象集合叫做关系R的定义域. 记作$D(R)$；第二个客体所允许选取对象的集合叫做关系R的值域，记作$C(R)$.

特别，当$D(R)=C(R)$时，并且设$D(R)=C(R)=M$；M为一集合，此时称关系R为集合M上的关系.

通常用R表示一个二元关系，对于具体的关系，R有确定的符号.

例1　实数集$\mathbf{R}$上的"大于"关系，用"$>$"表示，定义如下：

$$> \ = \{(x,y)\mid x\in\mathbf{R}, y\in\mathbf{R}\text{ 且 } x>y\}.$$

由此可见$(7,3)\in\ >$，但$(3,7)\notin\ >$,此关系中序偶的第一,第二客体均取相同之集合$\mathbf{R}$,故此关系是集合$\mathbf{R}$上的关系.

与集合论中类似,如果从A到B不存在某种关系R,则称关系为空关系. 如果A的每个元素到B的每个元素间均具有某种关系,则称这个关系为全关系. 从A到B的全关系即为$A\times B$.

定义 2　$A_1 \times A_2 \times A_3$ 的子集叫做 A_1, A_2, A_3 间的三元关系；$A_1 \times A_2 \times A_3 \times \cdots \times A_n$ 的子集叫做 $A_1, A_2, A_3, \cdots, A_n$ 间的 n 元关系；$A^n = \underbrace{A \times A \times \cdots \times A}_{n\text{个}}$ 的子集叫做 A 上的 n 元关系.

本章中我们主要讨论二元关系，如无特别声明，所讲关系均指二元关系.

如果 x 与 y 有关系 R，即 $(x,y) \in R$，则记成 xRy；如果 x 与 y 没有关系 R，即 $(x,y) \notin R$，则记成 $x\not{R}y$.

关系是序偶的集合，因此集合的各种运算在这里均适用，运算结果为一个新关系. 设 R 与 S 是给定集合上的两个二元关系，则 $R \cup S, R \cap S, R - S, \complement R$ 可分别定义如下：

1) $x(R \cup S)y$ 当且仅当 xRy 或 xSy；

2) $x(R \cap S)y$ 当且仅当 xRy 且 xSy；

3) $x(R - S)y$ 当且仅当 xRy 且 $x\not{S}y$；

4) $x \complement Ry$ 当且仅当 $x\not{R}y$.

例 2　设 $A = \{1, 2, 3, 4\}$，若 $R = \left\{(x,y) \,\middle|\, \frac{x-y}{2}\text{是正整数}\right\}$，$S = \left\{(x,y) \,\middle|\, \frac{x-y}{3}\text{是正整数}\right\}$，求 $R \cup S$，$R \cap S$，$R - S$，$\complement R$.

解　$R = \{(1,1),(1,3),(2,2),(2,4),(3,3),(3,1),(4,4),(4,2)\}$；

$S = \{(4,1)\}$；

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

$R \cap S = \varnothing$；

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

$\complement R = \{(1,2),(2,1),(2,3),(3,2),(3,4),(4,3),(1,4),(4,1)\}$.

二、关系的矩阵及图的表示法

表达有限集合到有限集合的二元关系时，矩阵及图（详细见第四章）是有力的工具.

设有集合 $A = \{a_1, a_2, \cdots, a_m\}$ 和 $B = \{b_1, b_2, \cdots, b_n\}$，及一个 A 到 B 的二元关系 R. 则对应于关系 R 有一个关系矩阵 $\boldsymbol{M}_R = (r_{ij})_{m \times n}$，其中

$$r_{ij} = \begin{cases} 1, \text{如果 } a_i R b_j, \\ 0, \text{如果 } a_i \not{R} b_j. \end{cases}$$

例 3　设 $A = \{a_1, a_2, a_3\}$，$B = \{b_1, b_2, b_3, b_4\}$，

$R = \{(a_1,b_1),(a_2,b_3),(a_3,b_2),(a_1,b_4),(a_2,b_4)\}$，则其矩阵为：

$$M_R=\begin{pmatrix}1&0&0&1\\0&0&1&1\\0&1&0&0\end{pmatrix}.$$

反之，利用关系矩阵 M_R，也可写出关系 R.

用图表示关系的方法如下：设 R 为集合 A 上的二元关系，用小圆圈标上 a_i 表示元素 a_i，小圆圈叫做结点，如果 a_iRa_j，则从结点 a_i 画一带箭头的弧到 a_j（次序不能变）；如果 a_iRa_i，则通过结点 a_i 画一个叫做环的带箭头的圆弧. 称带箭头的弧为边. 这样由结点及边组成的图叫做关系 R 的图示，又称关系图. 这个图是有向图，其中边的方向不能变.

若 R 是集合 $A=\{x_1,x_2,\cdots,x_m\}$ 到 $B=\{y_1,y_2,\cdots,y_n\}$ 上的二元关系，首先在平面上作出 m 个结点分别记为 x_1，x_2，…，x_m，然后另外作 n 个结点分别记为 y_1，y_2，…，y_n. 如果 x_iRy_j，则可自结点 x_i 到结点 y_j 处作一有向弧，其箭头指向 y_j，这样画出的图为集合 A 到 B 上的二元关系 R 的关系图.

例 4　（1）设 $X=\{x_1,x_2,x_3,x_4\}$，$Y=\{y_1,y_2,y_3\}$.

$R=\{(x_1,y_1),(x_1,y_3),(x_2,y_2),(x_2,y_3),(x_3,y_1),(x_4,y_1),(x_4,y_2)\}$.

（2）设 $A=\{1,2,3,4,5\}$，

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

它们的关系图分别如图 2－1，图 2－2 所示：

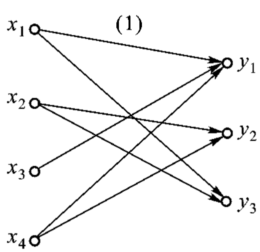


图 2－1

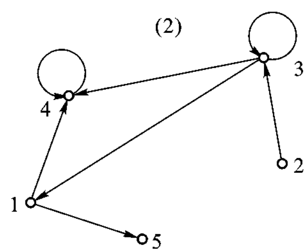


图 2－2

由于关系图主要表示结点与结点之间的邻接关系，故关系图中对结点位置和线段（弧）的长短无关.

三、关系的复合

定义 3　设 R 是一个从 X 到 Y 的关系，S 是一个从 Y 到 Z 的关系，则 R 与 S 的复合关系：$R\circ S$ 定义为

$R\circ S=\{(x,z)\mid x\in X,z\in Z$，至少存在一个 $y\in Y$ 有 $(x,y)\in R$ 且 $(y,z)\in S\}$.

这个复合关系是从 X 到 Z 的关系. 例如，如果 R_1 是关系“是……的

兄弟”，R_2 是关系“是……的父亲”，则 $R_1\circ R_2$ 是关系“是……的叔伯”.

例 5　设 $R=\{(1,2),(3,4),(2,2)\}$，

$S=\{(4,2),(2,5),(3,1)\}$，

则 $R\circ S=\{(1,5),(3,2),(2,5)\}$.

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

$S\circ S=\{(4,5)\}$.

$R\circ R=\{(1,2),(2,2)\}$.

两个关系的复合也通过矩阵及图表示出来. 我们设 $X=\{x_1,x_2,\cdots,x_n\}$，$Y=\{y_1,y_2,\cdots,y_m\}$，$Z=\{z_1,z_2,\cdots,z_p\}$，R 是从 X 到 Y 的关系，S 是从 Y 到 Z 的关系. 这样，关系 R 所表示的矩阵是一个 $m\times n$ 矩阵 $\boldsymbol{M}_R$，关系 S 所表示的矩阵是一个 $n\times p$ 矩阵 $\boldsymbol{M}_S$，于是关系 $R\circ S$ 所表示的矩阵 $\boldsymbol{M}'_{R\circ S}$ 可表示为

$$\boldsymbol{M}'_{R\circ S}=\boldsymbol{M}_R\times\boldsymbol{M}_S,$$

即为一 $m\times p$ 矩阵. 这里矩阵的运算是布尔运算.

例 6　设关系 R，S 的关系矩阵分别为

$$\boldsymbol{M}_R=\begin{pmatrix}1&1&0\\0&1&0\\0&0&0\end{pmatrix},\quad \boldsymbol{M}_S=\begin{pmatrix}0&1&0\\0&0&1\\0&0&1\end{pmatrix},$$

则复合关系 $R\circ S$ 的关系矩阵为

$$\boldsymbol{M}'_{R\circ S}=\boldsymbol{M}_R\times\boldsymbol{M}_S=\begin{pmatrix}1&1&0\\0&1&0\\0&0&0\end{pmatrix}\begin{pmatrix}0&1&0\\0&0&1\\0&0&1\end{pmatrix}=\begin{pmatrix}0&1&1\\0&0&1\\0&0&0\end{pmatrix}.$$

复合关系的关系图如图 2－3 所示.

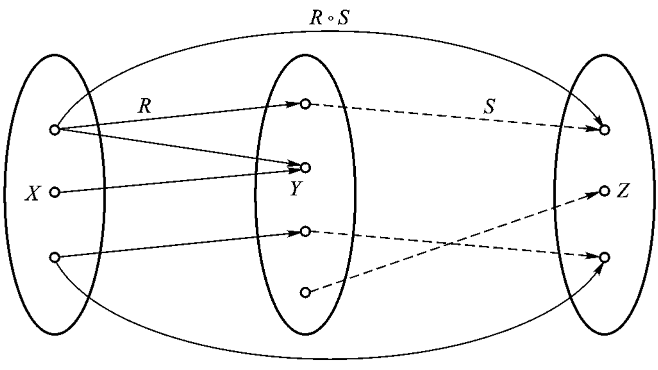


图 2－3

定理 1 设 R、S、T 分别表示从 X 到 Y，Y 到 Z，Z 到 W 的关系，则有

$$(R\circ S)\circ T=R\circ(S\circ T).$$

证 先证 $(R\circ S)\circ T\subseteq R\circ(S\circ T)$.

设 $(x,v)\in(R\circ S)\circ T$，则必存在 $z\in Z$ 有 $(x,z)\in R\circ S$，$(z,v)\in T$；进一步，必存在 $y\in Y$ 有 $(x,y)\in R$，$(y,z)\in S$；因为 $(y,z)\in S$，$(z,v)\in T$，故必有 $(y,v)\in S\circ T$，进一步由 $(x,y)\in R$，$(y,v)\in S\circ T$，故必有 $(x,v)\in R\circ(S\circ T)$.

反之同理可证 $R\circ(S\circ T)\subseteq(R\circ S)\circ T$，也即 $(R\circ S)\circ T=R\circ(S\circ T)$.

证毕

由复合关系的结合律可以知道关系 R 自身所组成的复合关系可以写成：$R\circ R$，$R\circ R\circ R$，$\overbrace{R\circ R\circ\cdots\circ R}^{n}$，分别记作 R^2，R^3，…，R^n，一般地有 $\overbrace{R\circ R\circ\cdots\circ R}^{n-1}\circ R=R^{n-1}\circ R=R^n$. 显然还有

$$R^m\circ R^n=R^{m+n}.$$

$$(R^m)^n=R^{mn}.$$

四、逆关系

定义 4 设 R 是一个从 A 到 B 的关系，则从 B 到 A 的关系 R^{-1}：

$$R^{-1}=\{(y,x)\mid(x,y)\in R\},$$

称之为 R 的逆关系.

一个关系的逆关系亦可用矩阵及图表示出来. 其具体方法是：一关系 R 之逆关系 R^{-1} 之矩阵 $\boldsymbol{M}_{R^{-1}}$ 是 $\boldsymbol{M}_R$ 之转置矩阵；一关系 R 的逆关系 R^{-1} 的图形是将 R 的图形中之有向边之方向改变后即得.

例 7 设 $A=\{1,2,3\}$，$B=\{a,b,c\}$，且设 R 是从 A 到 B 的关系

$$R=\{(1,a),(2,b),(3,c)\},$$

则从 B 到 A 的 R 逆关系 R^{-1} 为

$$R^{-1}=\{(a,1),(b,2),(c,3)\}.$$

其关系矩阵如

$$\boldsymbol{M}_R=\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix},\quad \boldsymbol{M}_{R^{-1}}=\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}.$$

（这里假设 a,b,c 排号 $c_{(1)},a_{(2)},b_{(3)}$）

其关系图如

对于逆关系容易证得：

定理 2 设 R、S 分别是从 X 到 Y 及 Y 到 Z 的关系，则我们有

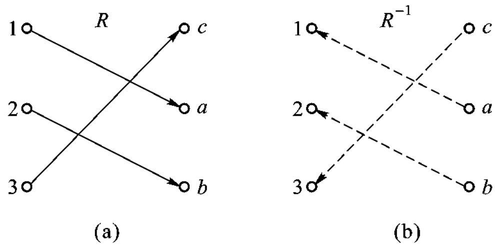


图 2 - 4

(1) $(R^{-1})^{-1}=R$.

(2) $(R\circ S)^{-1}=S^{-1}\circ R^{-1}$.

证　略.

练习题■2 -1

1. **用列举法表出下列** $A\times B$ **上的关系** S.

(a) $A=\{0,1,2\}$，$B=\{0,2,4\}$，

$S=\{(x,y)\mid x,y\in A\cap B\}$.

(b) $A=\{1,2,3,4,5\}$，$B=\{1,2,3\}$，

$S=\{(x,y)\mid x=y^2\}$.

2. **设** $R=\{(1,2),(2,4),(3,3)\}$ **和** $S=\{(1,3),(2,4),(4,2)\}$，**求** $R\cup S$，$R\cap S$，$R-S$，$D(R)$，$D(S)$，$D(R\cup S)$，$C(R)$，$C(S)$ **和** $C(R\cap S)$，**且证明**

$$D(R\cup S)=D(R)\cup D(S).$$

$$C(R\cap S)\subseteq C(R)\cap C(S).$$

3. **对下列关系** R，**求出关系矩阵** S_R

(a) $A=\{1,2,3\}$，$R=\{(2,2),(1,2),(3,1)\}$.

(b) $A=(0,1,2,3)$，$R=\{(x,y)\mid x\leqslant 2$ **且** $y\geqslant 1\}$.

(c) $A=\{5,6,7,8\}$，$B=\{1,2,3\}$，

$R=\{(x,y)\mid x\in A$ **且** $y\in B$ **且** $3\leqslant x-y\leqslant 7\}$

(d) $A=\{0,1,2,3,4,5,6\}$

$R=\{(x,y)\mid x<y$ **或** x **是质数**$\}$

4. **作出上题中的关系图.**

5. **证明定理** 2.

6. **设** R_1 **和** R_2 **是集合** $A=\{a,b,c,d\}$ **上的关系，这里**

$R_1=\{(b,b),(b,c),(c,a)\}$，

$R_2=\{(b,a),(c,d),(c,a),(d,c)\}$.

找出 $R_1\circ R_2$，$R_2\circ R_1$，R_1^{-1}，R_2^{-1}，R_1^2，R_2^3.

7. **证明如果** R **是集合** A **上的空关系或全关系，则** $R^2=R$.

8. 设 $A=\{1,2,\cdots,5\}$，$R=\{(1,2),(3,4),(2,2)\}$，$S=\{(4,2),(2,5),(3,1),(1,3)\}$ 求出 $M_{R\circ S}$，M_R，M_S.

第二节　关系的某些性质

在研究关系时，关系的某些特性有着特殊的作用.

定义 1　在集合 A 上的关系 R，如果对任意 $x\in A$，有 $(x,x)\in R(xRx)$，则称 R 是自反的.

例 1　设 $A=\{a,b,c\}$，$R=\{(a,a),(b,b),(c,c),(a,b),(b,c)\}$，则关系 R 是自反的. 其矩阵 M_R 及关系图如图 2－5 所示.

$$M_R=\begin{pmatrix}1&1&0\\0&1&1\\0&0&1\end{pmatrix}$$

主对角线上元素均为 1

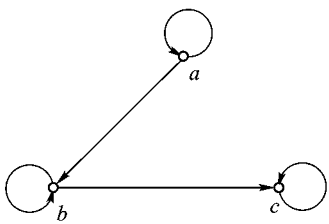


图 2－5

定义 2　在集合 A 上的关系 R，如果对任意 $x\in A$，有 $(x,x)\notin R(x\not R x)$，则称 R 是非自反的.

例 2　设 $A=\{a,b,c\}$，$R=\{(a,b),(a,c),(b,a),(c,b)\}$. 则关系 R 是非自反的，其矩阵 M_R 及关系图如图 2－6 所示：

$$M_R=\begin{pmatrix}0&1&1\\1&0&0\\0&1&0\end{pmatrix}$$

主对角线上元素均为 0

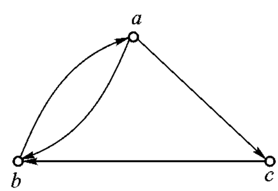


图 2－6

例如，在整数集 Z 上的关系"$\leqslant$"是自反的，不是非自反的. 在 Z 上的关系"$<$"是非自反的，但不是自反的.

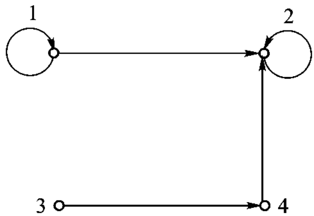
例 3　在集合 $X=\{1,2,3,4\}$ 上的关系 R，

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

此关系既不是自反的也不是非自反的，其矩阵 M_R 及关系图如图 2－7 所示.

$$M_R=\begin{pmatrix}1&1&0&0\\0&1&0&0\\0&0&0&1\\0&1&0&0\end{pmatrix}$$

主对角线上既有 0 又有 1



有的结点有环，有的结点无环

图 2－7

定义 3　在集合 A 上的关系 R，如果有 $(x,y)\in R(xRy)$，必有 $(y,x)\in R(yRx)$，则称 R 是对称的.

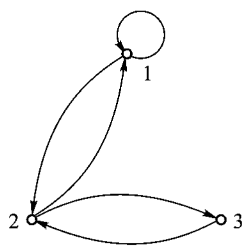
例 4　在集合 $A=\{1,2,3\}$ 上的关系

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

则关系 R 是对称的，其矩阵及关系图如图 2－8 所示.

$$M_R=\begin{pmatrix}1&1&0\\1&0&1\\0&1&0\end{pmatrix}$$

关于主对角线对称



二结点间的弧是双向的

图 2－8

定义 4　在集合 A 上的关系 R，如果有 $(x,y)\in R(xRy)$ 且 $x\neq y$ 必有 $(y,x)\notin R(yRx)$，则称 R 是非对称的.

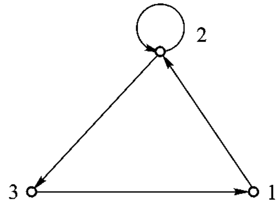
例 5　在集合 $A=\{1,2,3\}$ 上的关系

$R=\{(1,2),(2,3),(3,1),(2,2)\}$，

则关系 R 是非对称的，其矩阵及关系图如图 2－9 所示.

$$M_R=\begin{pmatrix}0&1&0\\0&1&1\\1&0&0\end{pmatrix}$$

如果 $a_{ij}=1$，则 $a_{ji}=0$，$i\neq j$



二结点间的弧是单向的

图 2－9

例如，在一些人的集合中，“同志”关系是对称的，但“父子”关系则是非对称的.

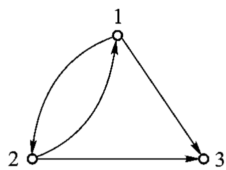
再如，在整数集 Z 上的关系“$<$”及“$\leqslant$”均是非对称的.

例 6 在集合 $A=\{1,2,3\}$ 上的关系 $R=\{(1,2),(2,1),(1,3),(2,3)\}$，此关系既不是对称的亦不是非对称的. 其矩阵及关系图如图 2－10 所示.

$$M_R=\begin{pmatrix}0&1&1\\1&0&1\\0&0&0\end{pmatrix}$$

既有 $a_{ij}=a_{ji}=1$，

又有 $a_{ij}=1$，$a_{ji}=0$，$i\neq j$



既有双向弧
又有单向弧

图 2－10

定义 5 在集合 A 上的关系 R，如果有 $(x,y)\in R\,(xRy)$ 且 $(y,z)\in R\,(yRz)$，则必有 $(x,z)\in R$，则称 R 是传递的.

例 7 设 $A=\{1,2,3,4\}$，$R=\{(4,1),(4,3),(4,2),(3,2),(3,1),(2,1)\}$，则 R 是传递的. 其关系矩阵及关系图如图 2－11 所示.

$$M_R=\begin{pmatrix}0&0&0&0\\1&0&0&0\\1&1&0&0\\1&1&1&0\end{pmatrix}$$

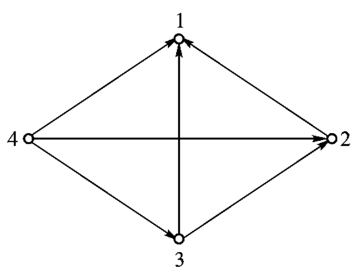


图 2－11

传递关系从关系矩阵上看是不显然的（需仔细推断），关系图的特点隐含在矩阵中. 其特点是：如果 A 到 B 有经过结点 A_0，A_1，…，A_n 等的弧将 A 与

B 连结起来，则 A 到 B（不经过这些点）也存在一条弧．下面再举两个关于传递性的例子．

例如，在一些人的集合上“同志”关系是传递的，但“父子”关系并不是传递的．

又如整数集 Z 上的“$<$”，“$\leqslant$”关系均是传递的．

以上我们介绍了关系的三种特性，在具体讨论关系时，对三种特性可同时进行讨论．从上述我们还看到，关系的特性与关系矩阵及关系图有着密切的联系．只要知道关系矩阵及关系图之一，即可看出关系的特性．

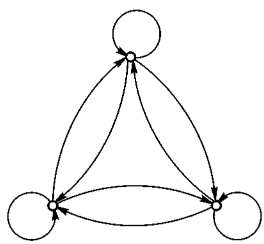
例如，整数集 Z 上的“$<$”关系是非自反的，非对称的，然而是传递的．

再如，整数集 Z 上的“相等”关系是自反的，对称的，同时又是传递的．

例 8　非空集合上全关系 R 是自反的，对称的，又是传递的；非空集合上的空关系 R 是非自反的，对称的，非对称，又是传递的（空集合上的空关系，则五者都具备）．我们以集合 $A=\{1,2,3\}$ 为例，设 R_1，R_2 分别是 A 上的全关系及空关系，其矩阵及关系图分别如图 2－12，图 2－13 所示．

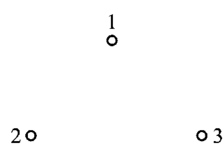
$$\boldsymbol{M}_{R_1}=\begin{pmatrix}1 & 1 & 1\\ 1 & 1 & 1\\ 1 & 1 & 1\end{pmatrix}$$

元素全是 1



每个结点均有环，每两个结点间均有双向弧

图 2－12



$$\boldsymbol{M}_{R_2}=\begin{pmatrix}0 & 0 & 0\\ 0 & 0 & 0\\ 0 & 0 & 0\end{pmatrix}$$

元素全是 0

每个结点均无环，每两个结点间均无弧联结

图 2－13

练习题■2－2

1.（1）举出一个既不是自反的也不是非自反的关系 R；

（2）举出一个既是对称的又是非对称的关系 R．

2. 下列论断是否正确

(1) 若关系 R 是对称的. 则 R^{-1} 也是对称的.

(2) 若关系 R 是非对称的，则 R^{-1} 也是非对称的.

(3) 若关系 R 是非对称的，则 $R\cap R^{-1}\neq\varnothing$.

(4) 若关系 R 是对称的，则 $R\cap R^{-1}\neq\varnothing$.

(5) 若关系 R，S 是传递的，则 $R\cup S$，$R\cap S$ 也是传递的.

3. 设集合 $A=\{1,2,3\}$ 上有三个关系：

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

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

$T=\{(1,1),(2,2),(1,2),(1,3),(3,2)\}$.

判断上述关系是否 A) 自反的；B) 对称的；C) 传递的；D) 非对称的.

4. 已给 $A=\{1,2,3,4\}$ 和定义在 A 上的关系 R：

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

说明 R 不是传递的. 求一个关系 $R_1\supseteq R$ 使得 R_1 是传递的. 还能找出另一个关系 $R_2\supseteq R$ 也是传递的吗？

5. 设 $A=\{1,2,3,4,5,6,7,8,9,10\}$ 和在 A 上的关系 R：

$R=\{(x,y)\mid x+y=10\}$,

关系 R 有什么性质？

6. 下列图 2 – 14 中所表示的关系具有哪些特性. 写出这些关系及关系矩阵.

7. 设 R 是集合 A 上的一个自反关系. 求证：R 是对称和传递的充分必要条件是 (A,B) 和 (A,C) 在 R 中，则有 (B,C) 在 R 之中.

第三节 关系的闭包运算

这一节我们介绍关系的闭包运算，这是关系的一种新运算，对于任给的一个关系我们可以通过这种运算得到一个新关系且这个新关系具有一定的性质.

定义 设 R 是 A 上的一个关系，如果另有一个关系 R' 满足：

a) R' 是自反的(对称的,传递的)；

b) $R'\supseteq R$；

c) 设 R'' 是自反的(对称的,传递的)，如果有 $R''\supseteq R$，就有 $R''\supseteq R'$，则称关系 R' 为 R 的自反(对称,传递)闭包. 记作

$$r(R),(s(R),t(R)).$$

从定义可见闭包也是一个关系，自反(对称,传递)闭包应是包含 R 的最小自反(对称,传递)关系.

定理 1 设 R 是 A 上的一个关系，则

a) R 是自反的，当且仅当 $r(R)=R$；

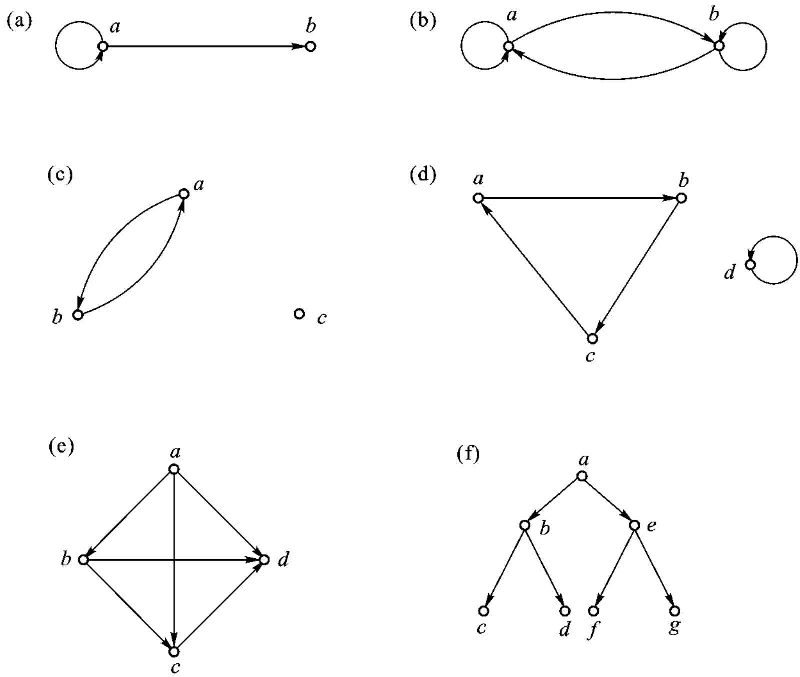


图 2－14

b）R 是对称的，而且仅当 $s(R)=R$；

c）R 是传递的，当且仅当 $t(R)=R$.

证　a）如果 R 是自反的，因 $R\supseteq R$，且对任何包含 R 的自反关系 R''，有 $R''\supseteq R$，故 R 满足自反闭包定义，即 $r(R)=R$.

反之，若 $r(R)=R$，由定义中的 a)，R 是自反的. b) 与 c) 同理可证. 证毕.

例 1　设 R 为集合 $A=\{a,b,c,d,e\}$ 上的关系，其关系图如图 2－15 所示.

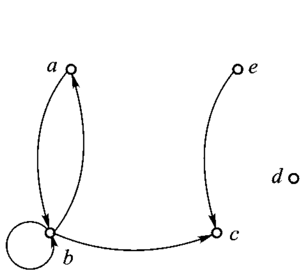


图 2－15

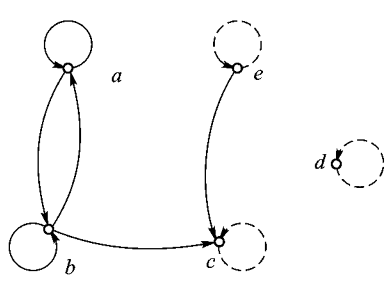


图 2－16

R 的自反闭包 $r(R)$ 的关系图如图 2－16 所示. 它是由 R 的关系图在每个

无环的结点上都增加一个环后得到的.

R 的对称闭包 $s(R)$ 的关系图如图 2－17 所示. 它是把 R 的关系图中的单向边都变为双向变后而得到的.

R 的传递闭包 $t(R)$ 的关系图如图 2－18 所示. 它是这样得到的，若结点 A 到 B 间有边连接(不止一条边)，则在 A 与 B 间添加上“捷径”(一条边)，使 A 与 B 直接连接即可.

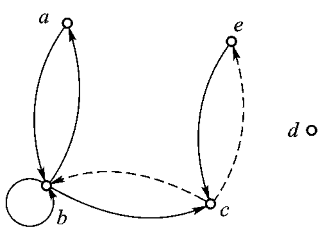


图 2－17

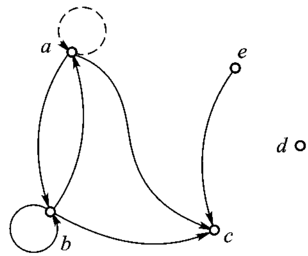


图 2－18

例 2　说明了利用所给关系 R 关系图求 $r(R)$、$s(R)$、$t(R)$ 的方法，对于具体问题也可不经过关系图而直接去求 $r(R)$、$s(R)$、$t(R)$.

定理 2　设 R 是集合 A 上的一关系，则 $r(R)=R\cup Q$，其中 $Q=\{(x,x)\mid x\in A\}$.

证　令 $R'=R\cup Q$，对任意 $x\in A$，因为 $(x,x)\in Q$，故 $(x,x)\in R'$，即 R' 是自反的.

又 $R\subseteq R\cup Q$，即 $R\subseteq R'$. 若有自反关系 R 且 $R''\supseteq R$，显然有 $R''\supseteq Q$，于是

$$R''\supseteq R\cup Q=R'$$

故 $r(R)=R\cup Q$. 证毕.

定理 3　设 R 是集合 A 上的关系，则 $s(R)=R\cup R^{-1}$.

证　令 $R'=R\cup R^{-1}$，显然 $R'\supseteq R$ 且 R' 是对称的. 如果 R'' 是一个在 A 上具有对称性的关系且 $R''\supseteq R$，往证 $R''\supseteq R'$.

设 $(a,b)\in R'$，又 $R'=R\cup R^{-1}$，如果 $(a,b)\in R$，则有 $(a,b)\in R''$，因为 $R''\supseteq R$. 如果 $(a,b)\in R^{-1}$，则 $(b,a)\in R$，于是 $(b,a)\in R''$，而 R 是对称的，故有 $(a,b)\in R''$. 总之，对于 $(a,b)\in R'$，总有 $(a,b)\in R''$，即 $R''\supseteq R'$. 也就是 $s(R)=R\cup R^{-1}$. 证毕.

定理 4　设 R 是集合 A 上的关系，则

$$t(R)=\bigcup_{i=1}^{\infty}R^i=R\cup R^2\cup R^3\cup\cdots.$$

证　先证 $R\cup R^2\cup R^3\cdots\subseteq t(R)$，只须证明对任意的正整数 n 有 $R^n\subseteq t(R)$ 即

可. 用归纳法：由传递闭包定义有 $R\subseteq t(R)$. 假设当 $i=n(n\geqslant 1)$ 时，有 $R^n\subseteq t(R)$，令 $(a,b)\in R^{n+1}$，因 $R^{n+1}=R^n\circ R$，故存在某个 $c\in A$，使 $(a,c)\in R^n$ 及 $(c,b)\in R$，即存在 c 使 $(a,c)\in t(R)$ 且 $(c,b)\in t(R)$，也即 $(a,b)\in t(R)$，故 $R^{n+1}\subseteq t(R)$，由归纳法有

$$\bigcup_{i=1}^{\infty}R^i=R\cup R^2\cup R^3\cup\cdots\subseteq t(R).$$

再证 $t(R)\subseteq R\cup R^2\cup R^3\cup\cdots$

只须证明 $R\cup R^2\cup R^3\cup\cdots$ 是传递的即可.

对任一 (a,c)，(c,b) 由 $(a,c)\in\bigcup\limits_{i=1}^{\infty}R^i$，$(c,b)\in\bigcup\limits_{i=1}^{\infty}R^i$ 存在 t，s，使 $(a,c)\in R^t,(c,b)\in R^s$，于是有 $(a,c)\in R^t\circ R^s=R^{t+s}$，故 $(a,b)\in\bigcup\limits_{i=1}^{\infty}R^i$，即 $\bigcup\limits_{i=1}^{\infty}R^i$ 是传递的. 可见 $t(R)\subseteq\bigcup\limits_{i=1}^{\infty}R^i$.

因此，$t(R)=R\cup R^2\cup R^3\cup\cdots$. 证毕.

当 A 为有限集合时，有下面的

定理5　设 R 是有限集合 A 上的关系，并设 A 有 n 个元素，则 $t(R)\subseteq\bigcup\limits_{i=1}^{n}R^i$.

证　令 $(x,y)\in t(R)$，则必存在最小正整数 k，使 $(x,y)\in R^k$. 现证明 $k\leqslant n$. 若不然，存在 A 的元素序列 $x=a_0$，a_1，a_2，…，a_{k-1}，$a_k=y$，使 xRa_1，a_1Ra_2，…，$a_{k-1}Ry$. 因 $k>n$，a_0，a_1，…，a_k 中必有相同者，不妨设 $a_i=a_j$，$0\leqslant i<j\leqslant k$. 于是 xRa_1，a_1Ra_2，…，$a_{i-1}Ra_i$，a_jRa_{j+1}，…，$a_{k-1}Ry$ 成立. 即 $(x,y)\in R^S$，$s=k-(j-i)$.

（注 这里去掉了 $a_iRa_{i+1},a_{i+1}Ra_{i+2},\cdots,a_{j-2}Ra_{j-1},a_{j-1}Ra_j$）这与 k 是最小的假设矛盾，于是 $k\leqslant n$，又 (x,y) 是任意的，故必有 $t(R)\subseteq\bigcup\limits_{i=1}^{n}R^i$. 证毕.

例3　(1) 整数集 Z 上的关系 $<$ 的自反闭包是 $\leqslant$，对称闭包是关系 $\neq$，传递闭包是关系 $<$ 自身.

(2) 整数集 Z 上的关系 $\leqslant$ 的自反闭包是自身，对称闭包是全关系，传递闭包是自身.

(3) $\neq$ 的自反闭包是全关系，对称闭包是 $\neq$，传递闭包是全关系.

(4) 空关系的自反闭包是 $R=\{(x,x)\mid x\in A\}$，对称闭包与传递闭包是自身.

例4　设 $A=\{a,b,c\}$，R 是 A 上的关系，且 $R=\{(a,b),(b,c),(c,a)\}$，求 r

(R)，$s(R)$，$t(R)$.

解 $r(R)=R\cup Q=\{(a,b),(b,c),(c,a),(a,a),(b,b),(c,c)\}$.

$s(R)=R\cup R^{-1}=\{(a,b),(b,c),(c,a),(b,a),(c,b),(a,c)\}$.

$R^2=\{(a,c),(b,a),(c,b)\}$.

故 $R^3=\{(a,a),(b,b),(c,c)\}$.

$t(R)=R\cup R^2\cup R^3=\{(a,a),(b,b),(c,c),(a,c),(b,a),(c,b),(a,b),(b,c),(c,a)\}$.

练习题■2－3

1.（1）设 $A=\{a_1,a_2,a_3,a_4\}$，

$R=\{(a_1,a_2),(a_1,a_3),(a_2,a_3),(a_3,a_4)\}$；

（2）设 $X=\{x_1,x_2,x_3,x_4,x_5\}$，

$R=\{(x_1,x_2),(x_1,x_4),(x_2,x_4),(x_3,x_5)\}$.

试求 $r(R)$，$s(R)$，$t(R)$.

2. 找出图 2－19 中每个关系的自反，对称与传递闭包.

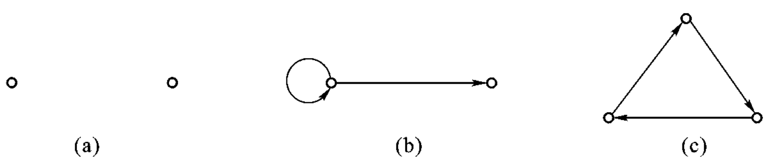


图 2－19

3. 设 R_1 和 R_2 是集合 A 上的关系，且 $R_1\supseteq R_2$，证明下列各式：

（1）$r(R_1)\supseteq r(R_2)$；

（2）$s(R_1)\supseteq s(R_2)$；

（3）$t(R_1)\supseteq t(R_2)$.

4. 设 R_1 和 R_2 是 A 上的关系，证明下列各式：

（1）$r(R_1\cup R_2)=r(R_1)\cup r(R_2)$.

（2）$s(R_1\cup R_2)=s(R_1)\cup s(R_2)$.

（3）$t(R_1\cup R_2)\supseteq t(R_1)\cup t(R_2)$.

5. 设 $A=\{a,b,c,d,e\}$，R 是 A 上的二元关系如图 2－20.

（1）画出 $r(R)$，$s(R)$，$t(R)$，（2）画出 $tsr(R)$.

6.（1）用反例说明“如果 R 是传递的，那么 $s(R)$ 也是传递的”这句话是错的.（2）举例.说明即使 R 是一有限集，$st(R)$ 与 $ts(R)$ 也可以不相等.

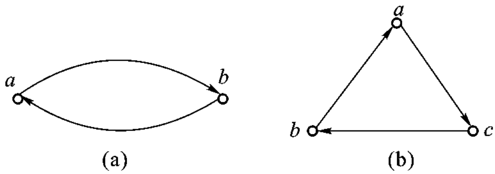


图 2－20

第四节　次序关系

这一节，我们介绍集合上元素之间的次序关系.

定义 1　如果集合 A 上的关系 R 是自反的，非对称的和传递的，则称 R 为 A 上的偏序或称 R 是 A 上的偏序关系，而称序偶 (A,R) 是偏序集合.

一般，我们用符号“ $\leqslant$ ”表示偏序(注意 $a\leqslant b$ 读作 a 在 b 前,它与“小于或等于”的含义是不同的,但也可读成“小于或等于”).

如果 R 是 A 上的偏序，则 R^{-1} 也是 A 上的一个偏序；若用 $\leqslant$ 表示 R，则 R^{-1} 用 $\geqslant$ 表示，即 $(A,\geqslant)$ 也是偏序集，$(A,\leqslant)$ 叫做 $(A,\geqslant)$ 的对偶.

例 1　集合 A 所组成之幂集 $\rho(A)$ 上的关系“ $\subseteq$ ”是自反的，非对称的又是传递的，故它是偏序的，$(\rho(A),\subseteq)$ 是偏序集合.

例 2　实数集 **R** 上的关系“ $\leqslant$ ”(不是偏序符号)是偏序的，$(\mathbf{R},\leqslant)$ 是偏序集合.

例 3　$A=\{2,4,6,8\}$，D 代表整除关系，M 代表整倍数关系，于是

$D=\{(2,2),(4,4),(6,6),(8,8),(2,4),(2,6),(2,8),(4,8)\}$，

$M=\{(2,2),(4,4),(6,6),(8,8),(4,2),(6,2),(8,2),(8,4)\}$，

则 D，M 都是 A 上的偏序关系. (A,D)，(A,M) 为偏序集合，且互为对偶.

定义 2　如果集合 A 上的关系 R 是非自反的，传递的，则称 R 在 A 上是拟序的，(A,R) 称为拟序集合. 常用符号“ $<$ ”表示拟序.

例 4　实数集中的“ $<$ ”关系是拟序的.

例 5　由集合 A 所组成之幂集 $\rho(A)$ 上的关系“ $\subsetneq$ ”是拟序的.

关于拟序有：

定理 1　若 R 是集合 A 上的拟序关系，则它是非对称的.

证　采用反证法，假设 R 不是非对称的，则至少有两个元素 x，$y\in A$，使当 $(x,y)\in R$ 时，必有 $(y,x)\in R$. 由于 R 是拟序，故它是传递的，因此有 $(x,x)\in R$，这与 R 是非自反的矛盾，故 R 是非对称的. 证毕.

拟序与偏序间有如下的联系.

定理 2　设 R 是集合 A 上的关系，则

（1）若 R 是一个拟序关系，则 $r(R)=R\cup Q$ 是一个偏序关系；

（2）若 R 是一个偏序关系，则 $R-Q$ 是一个拟序关系.

证　（1）设 R 是 A 上的拟序关系，则它是非自反的，非对称的和传递的，于是可知 $r(R)=R\cup Q$ 是自反的，非对称的和传递的，即 $r(R)$ 是偏序的.

（2）设 R 是 A 上的偏序关系，则 R 是自反的，非对称的和传递的，因此 $R-Q$ 便是非自反的，非对称的和传递的，即 $R-Q$ 是拟序的.　证毕.

从这个定理可见偏序是拟序的扩充，拟序是偏序的缩减.　二者之间差一个 $Q=\{(x,x)\mid x\in A\}$.

例 6　实数集 **R** 上的“ $<$ ”关系是拟序的，它的自反闭包是“ $\leqslant$ ”，故“ $\leqslant$ ”是偏序的；集合 $\rho(A)$ 上的“ $\subsetneqq$ ”关系是拟序的，它的自反闭包是“ $\subseteq$ ”，故“ $\subseteq$ ”是偏序的.

在例 6 中，“ $\leqslant$ ”及“ $\subseteq$ ”分别是某集合上的偏序，细心的读者会发现实数集 **R** 上的任意两个元素 x，y 都有关系“ $\leqslant$ ”，或者是 $x\leqslant y$ 或者是 $y\leqslant x$，我们说 x 与 y 是可比较的.　而集合 $\rho(A)$ 上的任意两个元素却不一定存在“ $\subseteq$ ”.如，我们设 $A=\{a,b\}$，则 $\rho(A)=\{\varnothing,\{a\},\{b\},\{a,b\}\}$.　则 $\rho(A)$ 中的 $\{a\}$ 与 $\{b\}$ 既不存在 $\{a\}\subseteq\{b\}$，又不存在 $\{b\}\subseteq\{a\}$，这时说 $\{a\}$ 与 $\{b\}$ 是不可比较的.　针对这两种情况我们有：

定义 3　设 R 是集合 A 上的偏序，如果对每个 x，$y\in A$ 必有 $x\leqslant y$ 或 $y\geqslant x$，则称 R 是线序的(或全序的)。称 (A,R) 为全序集合。

例 7　$A=\{\varnothing,\{a\},\{a,b\},\{a,b,c\}\}$ 上的“ $\subseteq$ ”关系是线序的.　$B=\{a,b,c\}$ 而 $\rho(B)$ 上的“ $\subseteq$ ”关系不是线序的.

定义 4　设 $(A,\leqslant)$ 是一个偏序集合，且 $B\subseteq A$.

（1）若存在惟一一个元素 $b\in B$，使对一切 $x\in B$ 均有 $x\leqslant b$，则称 b 是 B 的最大元素.

（2）若存在惟一一个元素 $b\in B$，使对 $x\in B$ 均有 $b\leqslant x$，则称 b 是 B 的最小元素.

（3）如果 $b\in B$，且 B 中不存在元素 x，使 $b\neq x$ 且 $b\leqslant x$，则称 b 为 B 的极大元素.

（4）如果 $b\in B$，且 B 中不存在元素 x，使 $b\neq x$ 且 $x\leqslant b$，则称 b 为 B 的极小元素.

例 8　设 $A=\{a,b\}$，“ $\subseteq$ ”是 $\rho(A)$ 上的偏序.　设 $B=\rho(A)$，则 $\varnothing$ 为 B 的最小元素也是极小元素；$\{a,b\}$ 为 B 的最大元素也是极大元素.　设 $B=\{\{a\},\{b\}\}$，则 B 既无最大元素又无最小元素；但 $\{a\}$ 与 $\{b\}$ 均是 B 的极大元素，又

同时都是 B 的极小元素.

例 9　设 $A=\{x \mid x \in \mathbf{N}$（自然数集）且 $2 \leqslant x \leqslant 18\}$，$R$ 为 A 上的整除关系. $B=\{3,4,7,9\}$，则 B 无最大元素也无最小元素；B 有极大元素 4，7 和 9，B 还有极小元素 3，4 和 7. 设 $C=\{3,6,9,18\}$，则 C 有最大元素及极大元素 18；C 还有最小元素及极小元素 3. 设 $D=\{3,6,9,12,15,18\}$，则 D 无最大元素，但 D 中有极大元素 12，15 和 18；D 有最小元素及极小元素 3.

定义 5　设 $(A,\leqslant)$ 是一偏序集合，且 $B \subseteq A$.

（1）如果对每一 $b \in B$，有 $b \leqslant a$，$a \in A$，则元素 a 叫做 B 的上界；如果对每一 $b \in B$，有 $a \leqslant b$，$a \in A$，则元素 a 叫做 B 的下界.

（2）如果 a 是 B 的一个上界且对 B 的每一上界 a' 有 $a \leqslant a'$，则 a 叫做 B 的上确界，记作 $a=\sup B$；如果 a 是 B 的一个下界且对 B 的每一下界 a' 有 $a' \leqslant a$，则 a 叫做 B 的下确界，记作 $a=\inf B$.

例 10　设 $A=\{1,2,3\}$，"$\subseteq$"是 $\rho(A)$ 上的一个偏序. 令

$B=\{\varnothing,\{1\},\{2,3\},\{1,3\}\}$，则 $\varnothing$ 是 B 的下界，也是下确界，$\varnothing$ 也是 B 的最小及极小元素；$\{1,2,3\}$（$\notin B$）是 B 的上界，也是上确界，B 无最大元素，但有极大元素 $\{2,3\}$ 及 $\{1,3\}$. 令 $C=\{\{1\},\{2\}\}$，则 $\varnothing$ 是 C 的下界，下确界；$\{1,2\}$，$\{1,2,3\}$ 是 C 的上界，$\{1,2\}$ 是 C 的上确界，C 中既无最大元素也无最小元素，C 中有极大元素 $\{1\}$ 与 $\{2\}$，也有极小元素 $\{1\}$ 与 $\{2\}$.

从上面的定义及例题我们可以看出 B 的最大（小）元素和极大（小）元素必须在 B 中，而 B 的上界，上确界与下界，下确界可以在 B 中也可以不在 B 中. B 的最大（小）元素与上，下确界如果存在则必是惟一的，对于有限集合 B，极大（小）元素一定存在，但不一定是惟一的. 它们有如下之联系：

定理 3　设 $(A,\leqslant)$ 是一偏序集合，且 $B \subseteq A$.

（1）如果 b 是 B 的最大元素，则 b 是 B 的极大元素.

（2）如果 b 是 B 的最大元素，则 b 是 B 的上确界.

（3）如果 b 是 B 的一个上界且 $b \in B$，则 b 是 B 的最大元素.

证　留作练习.

以上我们介绍了一些次序关系，它们可用特殊的关系图表示，即所谓哈塞（Hasse）图. 具体方法如下：

设 $\leqslant$ 是集合 A 上的偏序关系，A 中的每个元素用结点表示之. 如 x，$y \in A$ 且 $x \leqslant y$，则在图中将结点 x 画于结点 y 之下面；如 x 与 y 间不存在另一个元素 z 使 $x \leqslant z$，$z \leqslant y$，则在 x 与 y 间用一条线联结之，由此所得到的图即为哈塞图.

例 11　整数集 $\mathbf{Z}$ 上的"$\leqslant$"关系是偏序的，它可用哈塞图描述之，如图 2－21.

例 12　$A=\{2,3,6,12,24,36\}$（A 整除），的哈塞图如图 2－22.

例 13 设 $A=\{a,b,c\}$，$\rho(A)$ 上的偏序关系 $\subseteq$，其哈塞图如图 2－23.

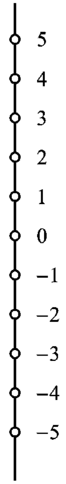


图 2－21 **Z** 上 $\leqslant$ 关系

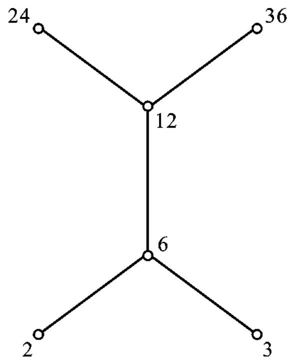


图 2－22

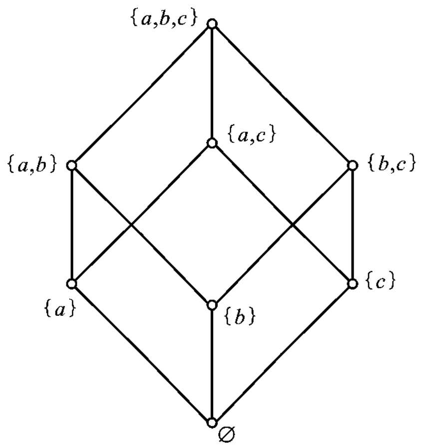


图 2－23

例 11 中的 $\leqslant$ 的关系又是线序的，由图 2－21 我们便可看出线序的含义.

在计算机科学中经常要碰到字典次序，字典次序说的是一些元素的排列的方法. 下面我们介绍字典次序.

定义 6 符号的任一不空有限集合 K，称其为字母表，符号亦称为字母.

例 14 $K=\{a,b\}$，其中 a，b 是两个符号.

例 15 所有小写英文字母可以组成一个字母表，当然每一个小写英文字

母都是它的一个符号. 亦即

$$K=\{a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z\}.$$

一般地，可假定 $K=\{\sigma_1,\sigma_2,\cdots,\sigma_m\}$.

对于给定的字母表 K，K 中任意的符号，例如符号 σ_1，σ_2，可以经过连接产生一些符号串，如 $\sigma_1\sigma_2$，$\sigma_2\sigma_1$，$\sigma_1\sigma_1$，$\sigma_2\sigma_2$，$\sigma_1\sigma_1\sigma_1$，$\sigma_1\sigma_1\sigma_2$，$\sigma_1\sigma_2\sigma_1$ 等等，这些符号串都叫做字. 注意 $\sigma_1\sigma_2\neq\sigma_2\sigma_1$.

对于一个字来讲，其中符号出现的次数叫做这个字的长度(简称字长)，如 σ_1 的长度为 1，任一字母 σ_i 的长度都是 1；$\sigma_1\sigma_1$ 的字长为 2；$\sigma_1\sigma_2$，$\sigma_2\sigma_1$，$\sigma_2\sigma_2$，$\sigma_1\sigma_3$ 等的字长均为 2；而 $\sigma_1\sigma_1\sigma_1$，$\sigma_1\sigma_1\sigma_2$，$\sigma_1\sigma_2\sigma_1$ 等的字长均为 3. 空字是长度为零的符号串，即没有任何符号出现的字，空字一般记为⊙. 空字⊙不属于字母表，亦即它不是任一字母.

我们用 K^* 表示字母表 K 中字母所构成的所有字(包括空字)组成的集合. 对任意的 $x\in K^*$，都有一自然数 n 和 K 中的符号 σ_{i_1}，σ_{i_2}，…，σ_{i_n}($1\leqslant i_j\leqslant m$，$1\leqslant j\leqslant n$)使得

$$x=\sigma_{i_1}\cdots\sigma_{i_n}.$$

这时 x 是长度为 n 的字，通常记为 $n=|x|$.

对于 K^* 中的两个字母 x 及 y，在字典里常会出现 x 与 y 谁在前谁在后的问题. 如 above 及 abroad 这两个英文单词，在编字典时，就得一个在前一个在后. 英文字典上 above 是在 abroad 前面的，字典次序就是处理如这样问题的一个有利工具. 它在计算机的专业知识中会经常出现.

字典次序可按下面规定定义：

(1) 对字母表上的所有字母规定一个线序关系(可按需要来规定).

(2) 对 K^* 中的任二字 $x=x_1x_2\cdots x_n$ 和 $y=y_1y_2\cdots y_n$，它们是按如下规定处理的.

A) 若 $x_1\neq y_1$，$x_1\leqslant y_1$，则 $x\leqslant y$；

$y_1\leqslant x_1$，则 $y\leqslant x$.

B) 若 $x_1=y_1$，$x_2=y_2$，…，$x_i=y_i$，$x_{i+1}\neq y_{i+1}$：

$x_{i+1}\leqslant y_{i+1}$，则 $x\leqslant y$；

$y_{i+1}\leqslant x_{i+1}$，则 $y\leqslant x$.

C) 若 $x_j=y_j(j=1,\cdots,i)$，$i=\min(m,n)$：

$m\leqslant n$，则 $x\leqslant y$；

$n\leqslant m$，则 $y\leqslant x$.

例如上面说的 above 与 abroad，因为 $a=a$，$b=b$，而在英文字母 o 排在字母 r 之前，所以按字典次序 above 排在 abroad 之前.

练习题■2－4

1. 证明定理3. 并给出最小元素，极小元素及下确界间的关系且与定理3相应的结论.

2. 图2－24中给出了偏序集合(A,R)的哈塞图，这里$A=\{a,b,c,d,e\}$.

(1) 下列关系式哪个是真？

aRb，dRa，cRe，bRe，aRa，bRc，dRe.

(2) 把哈塞图改为有向图.

(3) 求出A的最大元素及最小元素，如果不存在，则指出不存在.

(4) 求出A的极大元素及极小元素.

(5) 求出子集$\{b,c,d\}$，$\{c,d,e\}$和$\{a,b,c\}$的上界和下界，上确界及下确界.

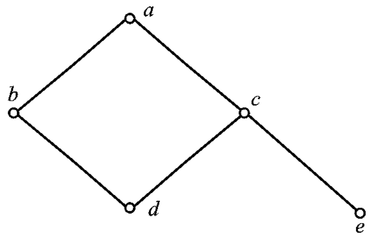


图2－24

3. 设$A=\{1,2,3,4\}$，求出$\rho(A)$，“$\subseteq$”是$\rho(A)$上的关系. 设

$B=\{\varnothing,\{1,2\},\{2,3\},\{2,3,4\},\{1,2,4\}\}$.

$C=\{\{1\},\{2\},\{2,3\},\{3,4\},\{1,3,4\},\{1,2,3,4\}\}$.

试求B及C的最大(小)元素，极大(小)元素，上(下)界，上(下)确界.

4. 说明下列图2－25中的有向图哪些代表偏序集合，拟序集合，线序集合.

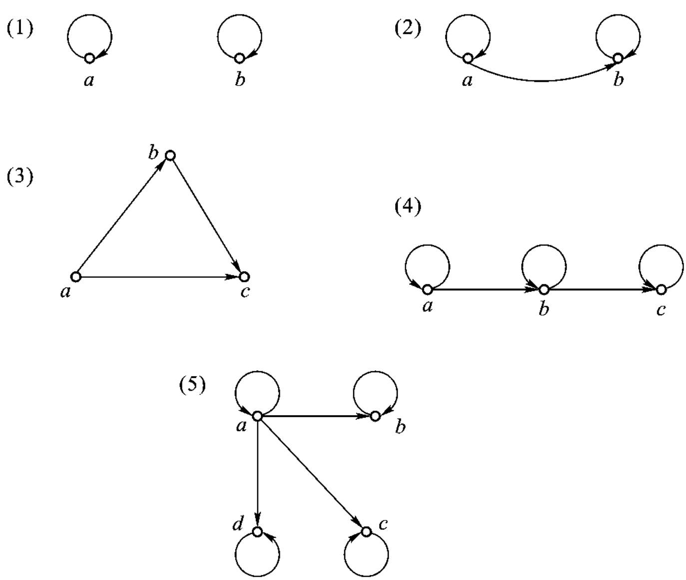


图2－25

5. 证明

(1) 如果R是拟序，则R^{-1}也是拟序.

（2）如果 R 是偏序，则 R^{-1} 也是偏序.

（3）如果 R 是线序，则 R^{-1} 也是线序.

6. 证明

（1）对任意线序集合，每一子集的极小元素是最小元素，每一极大元素是最大元素.

（2）一线序集合的每一非空有限子集有一最小和最大元素.

第五节　等■价■关■系

在讨论集合时，有时需要把一个集合分成一些互不相交的子集，而每个子集中的元素，都具有某些共有特性.

如，我们把非负整数集(或自然数集)N 分为以下 6 部分：

$$A_1 = \{0, 6, 12, 18, \cdots\};$$

$$A_2 = \{1, 7, 13, 19, \cdots\};$$

…………

$$A_6 = \{5, 11, 17, 23, \cdots\}.$$

这时我们不再把 A_1，A_2，…，A_6 看作一些元素作成之集. 而把 A_1，A_2，…，A_6 看作一个新元素，由这些元素再作成一新集合 B. 显见，新集合 B 与原集合 N 相差很远，N 为无限集，而 B 却是仅含 6 个元素的有限集.

用子集作为元素构成的新集合，在第一章中我们已讨论过. 但是只要你细心观察就会发现，我们这里所说的与第一章中介绍的还有所不同，这里的子集，其内的元素都具有某些共有特性，元素之间有特殊的联系(关系).

如，A_1 中任意两个元素之差都是 6 的整倍数；每个元素是 6 的倍数，余数 0；

A_2 中任意两个元素之差都是 6 的整倍数；每个元素是 6 的倍数，余数 1；

…………

A_6 中任意两个元素之差都是 6 的整倍数；每个元素是 6 的倍数，余数 5.

而且像我们这种做法(规定了特性及联系)，B 中就能且只能有 A_1，A_2，A_3，A_4，A_5，A_6 这 6 个元素. 集合的这种划分不是偶然出现的，它是由集合上元素之间的一种特殊关系决定的. 下面我们就讨论这个问题.

定义 1　设 R 是集合 A 上的关系，如果它是自反的，对称的，传递的，则称 R 为等价关系. 常用“ ~ ”表示等价关系. 若集合 A 中的元素 x，y 具有等价关系，则记为 $x \sim y$，说 x 等价 y.

例 1　所有平面图形组成之集合上的“相似”关系是等价关系.

例 2　一些人组成的集合中的“同志”关系是等价关系.

例 3 设 $X=\{1,2,\cdots,7\}$ 和 $R=\{(x,y)\mid x-y$ 被 3 整除$\}$. 关系 R 是一等价关系.

事实上，因为：

1. 对任意 $a\in X$，$a-a$ 可以被 3 整除；因而 aRa，即 R 是自反的.

2. 对任何 a、$b\in X$，如果 $a-b$ 可被 3 整除；则 $b-a$ 也可被 3 整除，即若 aRb，则 bRa，故 R 是对称的.

3. 对于 a、b、$c\in X$，若 aRb 和 bRc，则 $a-b$ 和 $b-c$ 都可被 3 整除，因而 $a-c=(a-b)+(b-c)$ 也可被 3 整除，所以 aRc，即 R 是传递的.

此例是模数系统中的更一般的相等关系的特例. 设 $\mathbf{Z}$ 表示全体整数集合，m 是一正整数. 对于 x，$y\in\mathbf{Z}$，定义 R 为

$$R=\{(x,y)\mid x-y \text{ 可被 } m \text{ 整除}\}.$$

注意 "$x-y$ 可被 m 整除" 等价于 x 和 y 各除以 m 而有相同的余数. 这里一般用 $\equiv$ 表示 R，把 xRy 定义成 $x\equiv y(\bmod\ m)$，叫做 x 与 y 对模 m 是同余的，此式叫做同余式，关系 $\equiv$ 也叫做同余关系. 同例 3 一样易证同余关系是等价关系.

定义 2 设 R 是集合 A 上的等价关系. 对任意 $x\in A$，由

$$[x]_R=\{y\mid y\in A \text{ 且 } xRy\}$$

给出的集合 $[x]_R(\subseteq A)$ 称为 x 对于 R 的等价类.

从定义可见，集合 $[x]_R$ 由集合 A 中所有与 x 有关系 R 的元素组成. 这个集合（等价类集合）有下面一些性质.

1. 对任何元素 $x\in A$，因为 R 是自反的，故有 xRx，所以 $x\in[x]_R$.

2. 设 $y\in A$ 是任意异于 x 使得 xRy 的元素，则 $y\in[x]_R$. 由 R 的对称性，有 yRx 和 $x\in[y]_R$. 现在，若存在元素 $z\in[y]_R$，则 z 必在 $[x]_R$ 中；事实上，因 R_1 $-R_2$ 及 xRy，由传递有 xRz，即 $z\in[x]_R$，从而 $[y]_R\subseteq[x]_R$. 由对称性同样可得 $[x]_R\subseteq[y]_R$. 亦即 $[x]_R=[y]_R$.

3. 第二步说明了，如果 xRy，则 $[x]_R=[y]_R$. 现在来说明，如果 $x\not R\,y$，则 $[x]_R$ 与 $[y]_R$ 必不相交. 假定至少存在一个元素 $z\in[x]_R$ 且 $z\in[y]_R$，就是 xRz 和 yRz，于是有 zRy，从而有 xRy，这与 $x\not R\,y$ 矛盾.

上面的结论说明，只要 $y\in[x]_R$，则由任一元素 $y\in A$ 对于 R 的等价类等于 $x\in A$ 对于 R 的等价类. 否则，由 x 和 y 对于 R 的等价类是相交的. 而且，A 的每一个元素对于 R 的等价类非空. 因此，A 的所有元素对于 R 的等价类盖住 A，即这些等价类的并是集合 A. 因为任意两个元素对于 R 的等价类或相等或不相交，我们可以说 A 的元素对于 R 的等价类（一族）定义了 A 的一个划分；这样的划分是惟一的，因为 A 的任何元素对于 R 的等价类是惟一的.

例 4 本节开头时对集合 $\mathbf{N}$ 的处理，便是通过 $\mathbf{N}$ 上的等价关系 R（同余关

系）对 N 进行了划分，A_1，A_2，A_3，A_4，A_5，A_6 是 N 的元素对等价关系 R（同余关系）所确定出的 6 个等价类. $A_i \cap A_i = \varnothing$，$(i \neq j)$ 且

$$A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5 \cup A_6 = \mathbf{N}\text{，而可记}$$

$$A_1 = [0]_R = [6]_R = [12]_R = [18]_R = \cdots\cdots;$$

$$A_2 = [1]_R = [7]_R = [13]_R = [19]_R = \cdots\cdots;$$

$$A_3 = [2]_R = [8]_R = [14]_R = [20]_R = \cdots\cdots;$$

$$A_4 = [3]_R = [9]_R = [15]_R = [21]_R = \cdots\cdots;$$

$$A_5 = [4]_R = [10]_R = [16]_R = [22]_R = \cdots\cdots;$$

$$A_6 = [5]_R = [11]_R = [17]_R = [23]_R = \cdots\cdots.$$

A_1，A_2，A_3，A_4，A_5，A_6 看作 6 个元素构成集合，则 B 的每一元素便是 N 的一个子集，而这个子集是 N 中的元素对于等价关系 R 所确定的一个等价类.

定理 1　集合 A 上的等价关系所构成的等价类产生集合 A 的一个划分，此划分叫做 A 关于 R 的商集. 记作 A/R.

由定理 1 知商集 A/R 是一个集合，它的元素是 A 上的元素所构成的等价类.

如，例 4 中的 $B = \mathbf{N}/R = \{A_1, A_2, A_3, A_4, A_5, A_6\}$.

例 5　设 $\mathbf{Z}$ 是整数集，$R = \{(x, y) \mid x, y \in \mathbf{Z}, x - y \text{ 被 } m \text{ 整除}\}$，$m$ 为正整数. 由上述知 R 是等价关系，在 $\mathbf{Z}$ 上 R 所构成的等价类分别为

$$[0]_R = \{\cdots, -2m, -m, 0, m, 2m, \cdots\};$$

$$[1]_R = \{\cdots, -2m+1, -m+1, m+1, 2m+1, \cdots\};$$

$$[2]_R = \{\cdots, -2m+2, -m+2, 2, m+2, 2m+2, \cdots\};$$

$$\cdots\cdots\cdots\cdots$$

$$[m-1]_R = \{\cdots, -m-1, -1, m-1, 2m-1, 3m-1, \cdots\}.$$

这些类称为模 m 的剩余类，商集 $\mathbf{Z}/R = \{[0]_R, [1]_R, [2]_R, \cdots, [m-1]_R\}$.

以上我们讨论了用等价关系确定集合的一个划分，然而若知道了集合的一个划分，能否知道这个划分是由什么样的等价关系确定的呢？回答是肯定的.

定理 2　集合 A 上的一个划分 C 可产生 A 的元素间的一个等价关系.

证　设 $C = \{C_1, C_2, \cdots, C_m\}$，$C_i \subsetneqq A$ 且 $\bigcup_{i=1}^{m} C_i = A$，$C_i \cap C_j = \varnothing$，$i \neq j$，由 C 可建立一个关系 $R = (C_1 \times C_1) \cup (C_2 \times C_2) \cup \cdots \cup (C_m \times C_m)$，易证 R 为等价关系. 证毕.

例 6　设 $A = \{1, 2, 3, 4, 5\}$ 的一个划分 $C = \{(1), (2, 3), (4, 5)\}$，试由划分 C 确定 A 上的一个等价关系 R.

解 $C_1 \times C_1 = \{1\} \times \{1\} = \{(1,1)\}$.

$C_2 \times C_2 = \{2,3\} \times \{2,3\} = \{(2,2),(3,3),(2,3),(3,2)\}$.

$C_3 \times C_3 = \{4,5\} \times \{4,5\} = \{(4,4),(5,5),(4,5),(5,4)\}$.

于是所求等价关系 R 为

$$\begin{aligned} R &= (C_1 \times C_1) \cup (C_2 \times C_2) \cup (C_3 \times C_3) \\ &= \{(1,1),(2,2),(3,3),(4,4),(5,5),(2,3),(3,2),(4,5),(5,4)\}. \end{aligned}$$

对于等价关系我们仍可用图及矩阵去研究它. 其关系图的特点为：每个结点均有环；二结点间若有边相联，则必有方向彼此相反之两条有向边；而且任何两结点间若有边相联，则必有边直接相联. 其关系矩阵的特点为：1）M_R 的对角线上的元素全为 1；2）M_R 是对称矩阵；3）M_R 可以经过有限次地把行与行及相应的列与列对调化为主对角型分块矩阵，且对角线上每个子块都是全 1 方阵.

例 7 设 $A = \{1,2,3,4,5,6\}$，R 为 A 上的关系. 取

$$R = \{(1,1),(2,2),(3,3),(4,4),(5,5),(6,6),(1,3),(3,1),(1,5),(5,1),(2,4),(4,2),(3,5),(5,3)\},$$

证明 R 是等价关系.

证 关系 R 的关系图 2－26 及关系矩阵如下

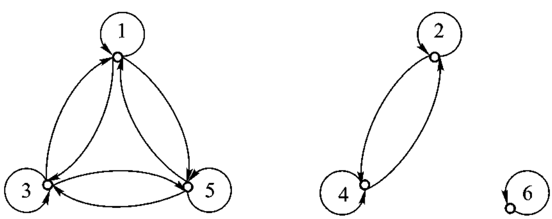


图 2－26

$$M_R = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

只要把 M_R 的第 2 行与第 5 行对调，并把第 2 列与第 5 列对调，就得到如下的矩阵：

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

这是一个主对角型分块矩阵，其对角线上的三个子块分别为：

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad (1)$$

都是全 1 方阵，由关系图或由关系矩阵都可看出 R 是等价关系. 证毕.

在例 7 中从关系图及关系矩阵中均可看出关系 R 在 A 上确立了 3 个等类，它们分别是

$$[1]_R = [3]_R = [5]_R = \{1,3,5\};$$
$$[2]_R = [4]_R = \{2,4\};$$
$$[6]_R = \{6\}.$$

练习题 2－5

1. 设 $\mathbf{Z}$ 为整数集，$R = \{(x,y) \mid x,y \in \mathbf{Z}, x-y$ 被 5 整除$\}$，证明 R 是等价关系且求$\mathbf{Z}/R$.

2. 给定集合 $A = \{1,2,3,4,5\}$，找出 A 上的等价关系 R，此关系 R 能产生划分 $\{\{1,2\},\{3\},\{4,5\}\}$，并画出关系图，写出关系矩阵.

3. 设 R_1，R_2 是 A 上的两个等价关系.

（1）证明 $R_1 \cap R_2$ 是 A 上的等价关系.

（2）用例子说明 $R_1 \cup R_2$ 不一定是等价关系.

4. 证明集合 A 上的全关系 $R = A \times A$ 是等价关系.

5. 设 R_1 和 R_2 是非空集合 A 上的等价关系，下式中哪些是 A 上的等价关系，不是的提供反例说明.

（1）$(A \times A) - R_1$； （2）$R_1 - R_2$； （3）R_1^2；

（4）$r(R_1 - R_2)$； （5）$R_1 \circ R_2$.

复 习 题 二

1. 设 $A = \{a,b,c,d,e,f,g\}$，R 是如图 2－27 所示 A 上的关系，试找出最小的整数 m 和 n，使 $m < n$ 和 $R^m = R^n$.

2. 设 $A\{6:00, 6:30, 7:00, \cdots, 9:30, 10:00\}$ 表示在晚上每隔半小时的 9 个时刻的集合，设 $B = \{1,8,10,12\}$ 表示本地 4 个电视频道的集合，设 R_1 和 R_2 是从 A 到 B 的两个二元关

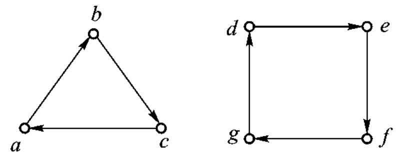


图 2－27

系. 对于二元关系 R_1，R_2，$R_1\cup R_2$，$R_1\cap R_2$，$R_1\oplus R_2$ 和 R_1-R_2 分别可以得出怎样的解释.

3. 设 R_1 和 R_2 是 A 上的任意关系，证明或否定下列断言.

（1）若 R_1 和 R_2 都是自反的，则 $R_1\circ R_2$ 也是自反的；

（2）若 R_1 和 R_2 都是非自反的，则 $R_1\circ R_2$ 也是非自反的；

（3）若 R_1 和 R_2 都是对称的，则 $R_1\circ R_2$ 也是对称的；

（4）若 R_1 和 R_2 都是非对称的，则 $R_1\circ R_2$ 也是非对称的；

（5）若 R_1 和 R_2 都是传递的，则 $R_1\circ R_2$ 也是传递的；

4. 在 $\mathbf{R}^2$ 平面上画出下述关系图，说明其性质.

（1） $\{(x,y)\mid x=y\}$；

（2） $\{(x,y)\mid x^2-1=0$ 且 $y>0\}$；

（3） $\{(x,y)\mid |x|\leqslant 1$ 且 $|y|\geqslant 1\}$.

5. 设 R，S，T 为集合 A 上关系，证明

$$R\circ(S\cup T)=R\circ S\cup R\circ T.$$

6. 设 A 为恰有 n 个元素的有限集.

（1）共有多少个 A 上的不相同的自反关系？

（2）共有多少个 A 上不相同的非自反关系？

（3）共有多少个 A 上的不相同的对称关系？

（4）共有多少个 A 上的不相同的非对称关系？

（5）共有多少个 A 上的不相同的既是对称又是非对称的关系？

7. 设 $Q=\{(x,x)\mid x\in A\}$ 是 A 上的关系，则对 A 上的任意二元关系 R，A 上的关系 $Q\cup R\cup R^{-1}$ 必是自反的和对称的.

8. 设 R 为 A 上关系. 证明

（1）$D(R^{-1})=C(R)$；

（2）$C(R^{-1})=D(R)$.

9. 设 $A=\{1,2,3,4\}$

$$M_R=\begin{pmatrix}0&0&0&1\\0&0&0&0\\1&1&0&0\\0&0&1&0\end{pmatrix}$$

求 M_{R^n}，$n\in N$.

10. 设 R 为非空有限集合 A 上的关系，则 $R\cap R^{-1}$ 的关系矩阵 $M_{R\cap R^{-1}}$ 中最多能有多少

个元素 1.

11. 设 $A=\{a,b,c\}$，R，S 是 A 上的关系，其关系矩阵是

$$\boldsymbol{M}_R=\begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix},\quad \boldsymbol{M}_S=\begin{pmatrix}1&1&0\\0&1&0\\0&1&1\end{pmatrix}.$$

试求 $\boldsymbol{M}_{R^{-1}}$，$\boldsymbol{M}_{s^{-1}}$，$\boldsymbol{M}_{(R\circ S)^{-1}}$，$\boldsymbol{M}_{(R\circ R)^{-1}}$.

12. 设 R 是 $A=\{1,2,3,4\}$ 上的关系，其关系矩阵为

$$\boldsymbol{M}_R=\begin{pmatrix}1&0&1&0\\0&0&1&1\\1&0&1&0\\1&0&1&0\end{pmatrix}$$

求 $\boldsymbol{M}_{r(R)}$，$\boldsymbol{M}_{s(R)}$，$\boldsymbol{M}_{R^2}$，$\boldsymbol{M}_{R^3}$，$\boldsymbol{M}_{R^4}$，及 $\boldsymbol{M}_{t(R)}$.

13. 设 A 是 n 个元素的集合，证明 A 上有 2^{n^2} 个二元关系.

14. R_1，R_2，R_3 是集合 A 上的关系，试证明如果 $R_1\subseteq R_2$，则

（1）$R_1\circ R_3\subseteq R_2\circ R_3$，

（2）$R_3\circ R_1\subseteq R_3\circ R_2$.

15. 设 R 是集合 S 上的关系，S'是 S 的子集，定义 S'上的关系 R'如下：

$$R'=R\cap(S'\times S').$$

确定下述命题是真还是假.

（1）如果 R 在 S 上是传递的，那么 R'在 S'上传递的.

（2）如果 R 在 S 上偏序，那么 R'在 S'是偏序.

（3）如果 R 在 S 上拟序，那么 R'在 S'上是拟序.

（4）如果 R 在 S 上线序，那么 R'在 S'上是线序.

16. 设 $K=\{a,b,c\}$，规定 $a\leqslant b\leqslant c$. 求出下列符号串的字典排序.

（1）$x=abc$；（2）$y=abaa$；（3）$z=bb$.

17. 画出下列集合上的整除关系的哈塞图.

（1）$\{1,2,3,4,6,8,12,24\}$；

（2）$\{i\mid i\in\mathbf{N}$ 且 $1\leqslant i\leqslant 14\}$；

（3）$\{i\mid i\in\mathbf{N}$ 且 $5\leqslant i\leqslant 20\}$.

18. 图 2－28 给出了集合 $\{1,2,3,4\}$ 上的四个偏序关系图，画出它们的哈塞图，并说明哪一个是全序关系.

19. 对下述每一条件，构造有限集和无限集的例子各一个.

（1）非空偏序集合，其中某些子集没有最大元素.

（2）非空偏序集合，其中有一子集存在最大下界，但没有最小元素.

（3）非空偏序集合，其中有一子集存在上界但没有最小上界.

20. 有人说，假设集合 A 上的一个关系 R 满足对称性和传递性，则 R 也满足自反性. 他的论证方法是：因为 R 是对称的，所以

$$aRb\Rightarrow bRa.$$

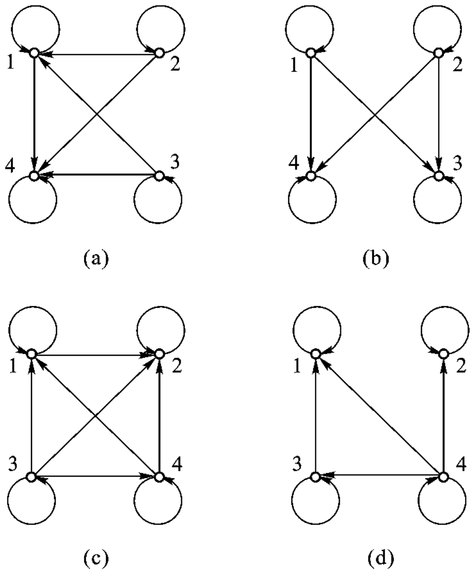


图 2 - 28

又 R 是传递的，所以

$$aRb \text{ 且 } bRa \Rightarrow aRa.$$

问：这个推理方法有什么错误？

21. 对集合 $\mathbf{Z}\times\mathbf{Z}$ 构造一拟序.

22. 找出在集合 $\{0,1,2,3\}$ 上包含序偶 $(0,3)$ 和 $(2,1)$ 的线序关系.

23. 已知集合 $\{a,b,c\}$ 上的关系 R 的关系矩阵 $\boldsymbol{M}_R$，求 R^{-1}，R^2，R^3，$R\circ R^{-1}$ 的关系矩阵.

$$\boldsymbol{M}_R=\begin{pmatrix}1&0&1\\1&1&0\\1&1&1\end{pmatrix}$$

24. 两个关系 R 和 S 由它们的关系矩阵 $\boldsymbol{M}_R$ 和 $\boldsymbol{M}_S$ 给出，证明 $R\circ S$ 不是一个等价关系.

$$\boldsymbol{M}_R=\begin{pmatrix}1&1&0\\1&1&0\\0&0&1\end{pmatrix},\qquad \boldsymbol{M}_S=\begin{pmatrix}1&1&0\\1&1&1\\0&1&1\end{pmatrix}$$

给出 $\{1,2,3\}$ 上的等价关系 R_1 和 R_2，使得 $R_1\circ R_2$ 也是一个等价关系.

25. 给出一个关系使它既是某一集合上的偏序关系又是等价关系.

26. 设 R 是一个二元关系，设

$$S=\{(a,b)\mid \text{对于某一 } c\text{，有}(a,c)\in R \text{ 且}(c,b)\in R\},$$

证明若 R 是一个等价关系，则 S 也是一个等价关系.

27. **设正整数的序偶集合 A，在 A 上定义的二元关系 R 如下：**

$((x,y),(u,v)) \in R$，当且仅当 $xv = yu$，证明 R 是一个等价关系.

28. **设 R 是集合 A 上的对称和传递关系，证明如果对于 A 中的每一个元素 a，在 A 中同时也存在一个 b，使 $(a,b) \in R$，则 R 是一个等价关系.**

第三章　代数系统

代数的概念及方法是研究计算机工程和科学的主要工具之一. 代数又叫代数系统，即具有一些 n 元运算的集合. 代数系统中最简单的而且相当重要的运算就是二元运算. 本章将介绍代数系统中群的有关概念，除此以外，我们还将简单的介绍一下环与域的基本概念.

第一节　运算与半群

一、代数运算及系统

定义 1　设 S 是一个非空集合，如果对于 S 中的任意两个元素 a，b，通过运算“$\circ$”都惟一确定一个 $c\in S$：$a\circ b=c$，则称“$\circ$”为 S 上的一个二元运算.

S 上的一个二元运算也叫 S 的一个结合法，二元运算又称代数运算.

例 1　取定非空集合 A，令 $\rho(A)=S$，对任意 a，$b\in S$，$a\cup b$，$a\cap b$ 均属于 S，故集合的并与交是 S 的两个二元运算.

注意　一般说来，$a\circ b$ 未必等于 $b\circ a$.

例 2　设 S 是所有二阶方阵构成之集合. “$\circ$”为定义在 S 上的矩阵的乘法，则“$\circ$”是 S 的一个二元运算，令

$$\boldsymbol{A}=\begin{pmatrix}2&1\\0&-1\end{pmatrix},\ \boldsymbol{B}=\begin{pmatrix}0&0\\1&1\end{pmatrix}.$$

则 $\boldsymbol{A}\in S$ 且 $\boldsymbol{B}\in S$，但

$$\boldsymbol{A}\circ\boldsymbol{B}=\begin{pmatrix}2&1\\0&-1\end{pmatrix}\begin{pmatrix}0&0\\1&1\end{pmatrix}=\begin{pmatrix}1&1\\-1&-1\end{pmatrix}.$$

$$\boldsymbol{B}\circ\boldsymbol{A}=\begin{pmatrix}0&0\\1&1\end{pmatrix}\begin{pmatrix}2&1\\0&-1\end{pmatrix}=\begin{pmatrix}0&0\\2&0\end{pmatrix}.$$

可见 $\boldsymbol{A}\circ\boldsymbol{B}\neq\boldsymbol{B}\circ\boldsymbol{A}$.

以上我们定义了集合 S 上的二元运算，从定义可以看出，对任意两个属于 S 的元素，通过二元运算产生的新元素仍在 S 中，二元运算的这种性质我们称为运算的封闭性.

例 3　正整数集 $\mathbf{Z}^+$ 上的除法运算“ $\div$ ”，它不是二元运算，因为在 $\mathbf{Z}^+$ 的除法不具有封闭性，但正有理数集 $\mathbf{Q}^+$ 上的除法运算“ $\div$ ”，是二元运算，此时运算在 $\mathbf{Q}^+$ 上是封闭的.

例 4　设 $A=\{x \mid x=2^n, n\in \mathbf{N}\}$，问乘法运算是否封闭？对加法运算呢？

解　对于任意 2^r，$2^s\in A$；r，$s\in N$，因为 $2^r\cdot 2^s=2^{r+s}\in A$，所以乘法运算是封闭的，而加法运算是不封闭的，因为至少有 $2+2^2=6\notin A$.

定义 2　设“ $\circ$ ”是定义在集合 A 上的二元运算，如果对于任意的 a，$b\in A$，都有 $a\circ b=b\circ a$，则称该二元运算“ $\circ$ ”是可交换的.

例 5　$\rho(A)$ 上的运算交与并是可交换的，因为对任意的 a，$b\in\rho(A)$，有 $a\cap b=b\cap a$，且有 $a\cup b=b\cup a$，而 $\rho(A)$ 上的差运算是不可交换的，如，$a=\{x,y\}\in\rho(A)$，$b=\{s,t,x\}\in\rho(A)$，则 $a-b=\{y\}\neq\{s,t\}=b-a$.

定义 3　设“ $\circ$ ”是定义在集合 A 上的二元运算，若对于任意的 a，b，$c\in A$ 都有 $(a\circ b)\circ c=a\circ(b\circ c)$，则称该二元是可结合的.

例 6　设 A 是一个非空集合，则 $\rho(A)$ 上的运算 $\cap$ 与 $\cup$ 是可结合的. 而 $\rho(A)$ 的差运算是不可结合的. 设 A_1，A_2，$A_3\in\rho(A)$ 且令 $A_1=\{x,y\}$，$A_2=\{x\}$，$A_3=\{x,z\}$，则

$$(A_1-A_2)-A_3=\{y\}-\{x,z\}=\{y\},$$
$$A_1-(A_2-A_3)=\{x,y\}-\varnothing=\{x,y\},$$

显见 $$(A_1-A_2)-A_3\neq A_1-(A_2-A_3).$$

定义 4　设“ $\circ$ ”，“ $*$ ”是定义在集合 A 上的两个二元运算，若对于任意的 a，b，$c\in A$，都有

$$a\circ(b*c)=(a\circ b)*(a\circ c),$$
$$(b*c)\circ a=(b\circ a)*(c\circ a),$$

则称二元运算“ $\circ$ ”对于运算“ $*$ ”是可分配的.

例 7　设 S 是所有二阶方阵构成的集合，“ $\circ$ ”是定义在 S 上的矩阵的乘法，“ $*$ ”是定义在 S 上的矩阵的加法，则“ $\circ$ ”对于“ $*$ ”是可分配的，但是，“ $*$ ”对于“ $\circ$ ”是不可分配的.

例 8　设 $S=\rho(A)$，A 非空. “ $\cap$ ”与“ $\cup$ ”是 S 上的两个二元运算，由

$$A_1\cup(A_2\cap A_3)=(A_1\cup A_2)\cap(A_1\cup A_3),$$
$$A_1\cap(A_2\cup A_3)=(A_1\cap A_2)\cup(A_1\cap A_3),$$

可知“ $\cap$ ”对于“ $\cup$ ”是可分配的，而“ $\cup$ ”对于“ $\cap$ ”也是可分配的.

例 9　设 R 是实数集，“ $\circ$ ”与“ $*$ ”分别是定义在 R 上的加法与减法.

此时“$\circ$”对“$*$”是不可分配的，而“$*$”对“$\circ$”也是不可分配的.

事实上，$1, 2, 3 \in \mathbf{R}$，$1+(2-3)=0$，而$(1+2)-(1+3)=-1$，$1+(2-3) \neq (1+2)-(1+3)$；又$1-(2+3)=-4$，$(1-2)+(1-3)=-3$，故还有$1-(2+3) \neq (1-2)+(1-3)$.

以上3例说明了定义在集合上的两个二元运算，既可以是相互分配的，又可以是相互都不可分配的，还可以是单向可分配的.

定义5 设“$\circ$”是定义在集合A上的二元运算，若对于任意的$a \in A$，$a \circ a = a$，则称运算“$\circ$”是等幂的. 若A中某些元素x满足$x \circ x = x$，则称x为运算$\circ$的幂等元.

定义6 设“$\circ$”与“$*$”是定义在集合A上的两个可交换的二元运算，若对于任意的$a, b \in A$，都有$a \circ (a * b) = a$且$a * (a \circ b) = a$，则称运算“$\circ$”与运算“$*$”满足吸收律.

例10 设A是非空集合，$S=\rho(A)$，则S上的运算“$\cap$”及运算“$\cup$”分别是等幂的. 事实上，对任意的$a \in S$，有$a \cap a = a$，$a \cup a = a$. 再由$A_1 \cap (A_1 \cup A_2) = A_1$及$A_1 \cup (A_1 \cap A_2) = A_1$，知运算“$\cap$”与运算“$\cup$”满足吸收律(注意‘$\cap$’与‘$\cup$’是可交换的这个条件).

定义7 一个非空集合S连同若干个定义在集合上的运算$f_1, f_2, \cdots, f_k$所组成的系统就称为一个代数系统，记作$(S, f_1, f_2, \cdots, f_k)$.

如，整数集Z以及其上数的加法运算“$+$”组成一个代数系统$(\mathbf{Z}, +)$. 又如，$S=\rho(A)$(A非空)及S上的运算“$\cup$”,“$\cap$”,“$-$”组成一个代数系统$(\rho(A), \cup, \cap, -)$.

一个代数系统未必非得是集合S同S上的全部运算所构成，给定集合S，S上的任意一个运算“$\circ$”与S都可构成代数系统；S上的任意若干个运算与S也构成代数系统. 我们主要介绍由一个运算“$\circ$”与集合S构成的代数系统.

二、半群

定义8 设$(S, \circ)$是一个代数系统，其中“$\circ$”是二元运算，若“$\circ$”是可结合的，则称$(S, \circ)$为半群；即对任意的$a, b, c \in S$有

$$(a \circ b) \circ c = a \circ (b \circ c).$$

若半群$(S, \circ)$中的“$\circ$”还是可交换的，则半群$(S, \circ)$叫做可换半群.

例11 设$S=\rho(A)$(A非空)，则$(S, \cap)$与$(S, \cup)$为两个半群，且都是可换半群. 事实上，对于任意的$A_1, A_2, A_3 \in S$，有

$$(A_1 \cap A_2) \cap A_3 = A_1 \cap (A_2 \cap A_3),$$
$$(A_1 \cup A_2) \cup A_3 = A_1 \cup (A_2 \cup A_3),$$

且

$$A_1 \cap A_2 = A_2 \cap A_1,$$
$$A_1 \cup A_2 = A_2 \cup A_1.$$

但是$(S,-)$不是半群，设$A_1=\{a,b\}$，$A_2=\{c\}$，$A_3=\{b,c\}$，则

$$(A_1-A_2)-A_3=\{a,b\}-\{b,c\}=\{a\},$$
$$A_1-(A_2-A_3)=\{a,b\}-\varnothing=\{a,b\},$$

而
$$(A_1-A_2)-A_3 \neq A_1-(A_2-A_3).$$

例 12　设 S 是所有二阶方阵的集合. 则$(S,\times)$与$(S,+)$是两个半群. “$\times$”与“$+$”是矩阵的乘法与加法. $(S,+)$是可换半群，而$(S,\times)$不是可换半群.

例 13　设 $S=\{a,b,c\}$，S 的一个二元运算“$\circ$”定义如下表，则$(S,\circ)$是半群.

表 3－1

$\circ$	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

解　由表 3－1 知运算“$\circ$”是封闭的，又对任意 x，y，$z\in S$，都有

$$(x\circ y)\circ z = y\circ z = x\circ(y\circ z).$$

因此，$(S,\circ)$是半群.

定义 9　设有代数系统$(S,\circ)$，M 是 S 的一个子集，如果 M 与运算“$\circ$”构成一代数系统，则称代数系统$(M,\circ)$为代数系统$(S,\circ)$的一个子代数系统. 简称子代数.

定义 10　如果半群$(S,\circ)$的子代数$(M,\circ)$仍是半群，则说$(M,\circ)$是半群$(S,\circ)$的子半群.

例 14　设 S 是所有二阶方阵的集合，M 是所有二阶非奇异矩阵之集合，由例 12 知$(S,\times)$是半群. 下面说明$(M,\times)$是$(S,\times)$的子半群，显然 $M\subset S$，又任取 $\boldsymbol{A}$，$\boldsymbol{B}$，$\boldsymbol{C}\in M$，则有 $\boldsymbol{AB}\in M$，且$(\boldsymbol{AB})\boldsymbol{C}=\boldsymbol{A}(\boldsymbol{BC})$，即$(M,\times)$是$(S,\times)$的子半群.

由例 12 还知$(S,+)$是(可换)半群，但$(M,+)$却不是$(S,+)$的子半群。

事实上，取

$$\boldsymbol{A}_1=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\ \boldsymbol{A}_2=\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix},$$

则 $\boldsymbol{A}_1$，$\boldsymbol{A}_2\in M$，但 $\boldsymbol{A}_1+\boldsymbol{A}_2\notin M$($\boldsymbol{A}_1+\boldsymbol{A}_2$ 是奇异矩阵)，即 M 对于运算“$+$”不

是封闭的. 因此$(M,+)$不是$(S,+)$的子半群.

由上所述，半群的符号中标出二元运算是必要的. 因为一个集合 S 可能有许多个二元运算，从而作成多种不同的半群. 标出运算，就可将它们区别开来，如例 12 中的半群$(S,\times)$或半群$(S,+)$.

定义 11 设$(S,\circ)$是一个半群. 如果存在元素 $e\in S$，对任意的 $a\in S$ 有 $e\circ a=a$，则说 e 是半群$(S,\circ)$的一个左单位元素；

如果存在元素 $f\in S$，对任意的 $a\in S$ 有 $a\circ f=a$，则说 f 是半群$(S,\circ)$的一个右单位元素.

如果半群$(S,\circ)$的一个元素既是左单位元素，又是右单位元素，则称该元素为半群$(S,\circ)$的单位元素.

含有单位元素的半群称为独异点.

一个半群，可以既没有左单位元素，也没有右单位元素；也可以有左单位元素而没有右单位元素；也可以有右单位元素而没有左单位元素. 但是，若半群既有左单位元素，又有右单位元素，则必有单位元素，而且只能有一个单位元素. 即有下述定理 1.

定理 1 设半群$(S,\circ)$有左单位元素 e，又有右单位元素 f，则 $e=f$ 是$(S,\circ)$的惟一的单位元素.

证 因 e 是左单位元素，故 $e\circ f=f$. 又 f 是右单位元素，故 $e\circ f=e$，因为两式左端相等，则 $e=f$ 是$(S,\circ)$的单位元素. 假若$(S,\circ)$有两个单位元素 e_1 和 e_2，则 $e_1\circ e_2=e_1=e_2$，故$(S,\circ)$只能有一个单位元素. 证毕.

例 15 在例 13 中半群$(S,\circ)$没有单位元素，而 a，b，c 为其左单位元素.

例 16 设$(S,*)$是半群，其中 $S=\{a,b,c\}$，“ $*$ ”的运算表如表 3－2.

表 3－2

$*$	a	b	c
a	a	b	c
b	b	c	c
c	c	a	b

则$(S,*)$有单位元素 a.

例 17 设 $S=\rho(A)$，A 非空，则半群$(S,\cup)$有单位元素$\varnothing$，半群$(S,\cap)$有单位元素 A. 令 $A=\{a,b,c\}$，设 $M=\{\{a\},\{b\},\{a,b\},\varnothing\}$，再设 $N=\{\{a\},\{a,b\}\ \{a,c\},\{a,b,c\}\}$，则 $M\subsetneqq S$ 且 $N\subsetneqq S$，易证$(M,\cap)$与$(N,\cup)$均是半群. $(M,\cap)$是$(S,\cap)$的子半群，$(N,\cup)$是$(S,\cup)$的子半群. $(M,\cap)$的单位元素是 $\{a,b\}$，$(S,\cap)$的单位元素是 S，$(N,\cup)$的单位元素是 $\{S\}$，$(S,\cup)$的单位元素是$\varnothing$.

例 18　设 Z 是整数集合，Z^+ 是正整数集合.（Z，+）与（Z^+，+）均是半群，（Z^+，+）是（Z，+）的子半群，这里“ + ”即为数的加法. 半群（Z，+）有单位元素 0，而其子半群（Z^+，+）却没有单位元素.

从以上几例可以看出，半群（S，∘）有单位元素 e，其子半群未必有单位元素；而且，即使有的话，也未必等于 e.

对于有单位元素的半群，我们可以讨论关于逆元的问题.

定义 12　设（S，∘）是有单位元素 S 的半群. S 中元素 a 叫做右可逆的，若存在 $a'\in S$，使 $a\circ a'=e$，a'叫做 S 的一个右逆元素.

S 中元素 a 叫做左可逆的，若存在 $a''\in S$，使 $a''\circ a=e$，a''叫做 a 的一个左逆元素.

若 a 既是右可逆的，又是左可逆的，则说 a 是可逆元素.

当 a 有右逆元素 a'又有左逆元素 a''时，$a'=a''$. 这时称 $a'(=a'')$为 a 的逆元素，简称 a 的逆，记作 a^{-1}. 关于可逆元素有：

定理 2　设（S，∘）是有单位元素 e 的半群，$a\in S$，a 有右逆元素 a'，又有左逆元素 a''，则 a 有惟一的逆元素 a^{-1}，并且还有

$$(a^{-1})^{-1}=a.$$

若 $a,b\in S$，a,b，都可逆，则 $a\circ b$ 也是可逆的，且$(a\circ b)^{-1}=b^{-1}\circ a^{-1}$.

证　因 $a\circ a'=e$，$a''\circ a=e$，故有 $a'=e\circ a'=(a''\circ a)\circ a'=a''\circ(a\circ a')=a''\circ e=a''$.

假定 a 有两个逆元素 b，c，则 $a\circ b=e$，$c\circ a=e$，同上面一样可知 $b=c$. 故可逆元素 a 有惟一的逆元素 a^{-1}，且适合

$$a^{-1}\circ a=a\circ a^{-1}=e.$$

又由 $a^{-1}\circ(a^{-1})^{-1}=(a^{-1})^{-1}\circ a^{-1}=e$，可知$(a^{-1})^{-1}=a$. 再由

$$(a\circ b)\circ(b^{-1}\circ a^{-1})=a\circ(b\circ b^{-1})\circ a^{-1}=a\circ e\circ a^{-1}=a\circ a^{-1}=e.$$

及$(b^{-1}\circ a^{-1})\circ(a\circ b)=b^{-1}\circ(a^{-1}\circ a)\circ b=b^{-1}\circ e\circ b=b^{-1}\circ b=e$.

可知　$(a\circ b)^{-1}=b^{-1}\circ a^{-1}$. 证毕.

例 19　设 S 是所有二阶方阵的集合，（S，×）是含有单位元素的半群. 对于 $\boldsymbol{A}\in S$，若它是奇异阵，则 $\boldsymbol{A}$ 不是可逆元素，即它没有逆元素；对于 $\boldsymbol{B}\in S$，若它是非奇异矩阵，则 $\boldsymbol{B}$ 是可逆元素，且 $\boldsymbol{B}\boldsymbol{B}^{-1}=\boldsymbol{B}^{-1}\boldsymbol{B}=\boldsymbol{E}$，这里 $\boldsymbol{E}=\begin{pmatrix}1&0\\0&1\end{pmatrix}$.

三、循环半群

定义 13　在半群（S，∘）中符号 a^n（n 是自然数）表示 S 中 n 个 a 的运算结

果，即

$$a^n = a \circ a \circ \cdots \circ a. \quad (\text{共 } n \text{ 个})$$

这样，在 S 中指数算律成立，即

$$a^m \circ a^n = a^n \circ a^m = a^{m+n}.$$

$$(a^n)^m = (a^m)^n = a^{mn} \quad (m, n \text{ 为自然数}).$$

定义 14 设$(S, \circ)$是一个半群，a 是 S 内一元素，如果对任意的 $b \in S$，都存在自然数 n，使得 $b = a^n$，则称$(S, \circ)$是由 a 生成的循环半群，而 a 叫做此循环半群的生成元素.

例 20 半群$(\mathbf{Z}^+, +)$是一个循环半群，它的生成元素是 1，因为它的任何元素均可由 1 生成，如 $2 = 1 + 1$，$3 = 2 + 1$，…，$n = (n-1) + 1$….

例 21 设 $S = \{a, b, c, d\}$，S 上的运算“$\circ$”定义如下表 3－3.

表 3－3

$\circ$	a	b	c	d
a	a	b	d	d
b	b	d	a	a
c	d	a	b	b
d	d	a	b	b

则可以验证$(S, \circ)$是半群（逐一验证要验 64 次）. $(S, \circ)$是一个循环半群，其生成元素是 c，因为

$$c^1 = c,$$
$$c^2 = c \circ c = b,$$
$$c^3 = c^2 \circ c = b \circ c = a,$$
$$c^4 = c^3 \circ c = a \circ c = d,$$
$$c^5 = c^4 \circ c = d \circ c = b = c^2.$$

定理 3 一个循环半群一定是可换半群.

证 设有循环半群$(S, \circ)$，它的生成元素是 a，则对任意两个元素 b，$c \in S$ 均有

$$b \circ c = a^m \circ a^n = a^{m+n} = a^{n+m} = a^n \circ a^m = c \circ b.$$

m，n 是自然数. 证毕.

定理 4 一个半群内的任一元素 a 及它所有的幂组成一个由 a 生成的循环子半群.

证 设$(S, \circ)$是一个半群，它的任一元素 a 以及它的幂所组成的集合是：$M = \{a, a^2, a^3, \cdots\}$. 而$(M, \circ)$便是$(S, \circ)$的一个由 a 生成的循环子半群.

例 22 设 $\mathbf{R}^+$ 表示正实数集合，则$(\mathbf{R}^+, \times)$是一个半群. 令

$$A=\{2,4,8,16,32,64,\cdots\}，及 B=\{4,16,64,\cdots\}，$$

则$(A,\times)$与$(B,\times)$便是$(\mathbf{R}^+,\times)$的两个循环子半群. $(A,\times)$的生成元素为 2，$(B,\times)$的生成元素为 4.

练习题 3－1

1. 下列运算在给定的集合上是否封闭：

(1) $A=\{0,1,2,3,4\}$，运算“$+$”为普通加法.

(2) $A=\{0,1,2,3,4\}$，运算“$\vee$”满足 $a\vee b=\max\{a,b\}$.

(3) $A=\{0,1,2,3,4\}$，运算“$\wedge$”满足 $a\wedge b=\min\{a,b\}$.

(4) 自然数集合 $\mathbf{N}$ 上运算“$\times$”,“$\times$”为普通乘法.

2. 设$(A,\circ)$是一代数系统，“$\circ$”为 A 上的二元运算，对任意的 a，$b\in A$ 有 $a\circ b=a$.

(1) 试证“$\circ$”是可结合的.

(2)“$\circ$”是可交换的吗？

3. 在自然数集合 $\mathbf{N}$ 上，下列各运算是否是可结合的.

(1) $a\circ b=\max\{a,b\}$.

(2) $a\circ b=\min\{a,b\}$.

(3) $a\circ b=a+b+3$.

(4) $a\circ b=a+2b$.

4. 定义 $\mathbf{Z}^+$（正整数集合）上的两个元素运算为

$$a\circ b=a^b.$$

$$a*b=a\times b，a，b\in\mathbf{Z}^+，“\times”普通乘法$$

试证“$\circ$”对“$*$”是不可分配的，反过来，“$*$”对“$\circ$”如何呢？

5. 设$(S,\circ)$是一个半群，证明，$S\times S$ 对于下面规定的结合法“$\circ$”作成一个半群：

$$(a_1,a_2)\circ(b_1,b_2)=(a_1\circ b_1,a_2\circ b_2).$$

当 S 有单位元素时，证明 $S\times S$ 也有单位元素.

6. 设$(S,\circ)$是一个半群，$a\in S$，在 S 上定义一个二元运算“Δ”，使得对 S 中的任意元素 x 和 y，都有

$$x\Delta y=x\circ a\circ y.$$

证明二元运算是可结合的.

7. 设$(\mathbf{R},\circ)$是一个代数系统，$\mathbf{R}$ 是实数集合，“$\circ$”是 $\mathbf{R}$ 上的一个二元运算，使得对于任意的 a，b 都有

$$a\circ b=a+b+a\cdot b\quad “\cdot”表通常乘法.$$

证明$(\mathbf{R},\circ)$是独异点，且单位元素是 0.

8. 设$(S,\circ)$为可换半群，证明，若 S 中有元素 a，b，使得 $a\circ a=a$ 及 $b\circ b=b$，则

$$((a\circ b)\circ(a\circ b))=a\circ b.$$

9. 设$(S,\circ)$由表 3－4 给出：

(1) 证明$(S,\circ)$是循环独异点，并求出生成元素.

(2) 把每一元素表示成生成元素的幂.

（3） 列出所有幂等元素

表 3－4

$\circ$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	b

10. $(S,\circ)$由下表 3－5 给出

（1） 它是半群吗？

（2） 它是独异点吗？

（3） 它是循环独异点吗？

表 3－5

$\circ$	a	b	c	d
a	c	b	a	d
b	b	b	b	b
c	a	b	c	d
d	d	b	d	b

11. 设$(S,\circ)$是半群，证明对于 S 中的 a，b，c，如果 $a\circ b=c\circ a$ 和 $a\circ b=b\circ a$ 和 $b\circ c=c\circ b$，那么，$((a\circ b)\circ c=c\circ(a\circ b)$.

12. 设$(\{a,b\},\circ)$是半群，这里 $a\circ a=b$，证明

（1） $a\circ b=b\circ a$.

（2） $b\circ b=b$.

13. 设 $A=\{a,b,c\}$，A 上的运算如下列各表，讨论它们的结合性，交换性，等幂性以及在 A 中对于“$\circ$”是否有单位元素. 每个元素是否可逆，找出逆元素.

表 3－6

$\circ$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

表 3－7

$\circ$	a	b	c
a	a	b	c
b	b	a	c
c	c	c	c

表 3－8

$\circ$	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

表 3－9

$\circ$	a	b	c
a	a	b	c
b	b	b	c
c	c	c	b

第二节　群

一、群的概念及性质

定义 1　一个代数系统$(S,\circ)$，如果满足下列条件：

(1) 结合律成立，即对任意的 a，b，$c\in S$ 有

$$(a\circ b)\circ c=a\circ(b\circ c);$$

(2) 存在单位元素 e：即对任意的 $a\in S$，有

$$e\circ a=a\circ e=a;$$

(3) 对 S 中任意元素 a，存在 $a^{-1}\in S$，使

$$a\circ a^{-1}=a^{-1}\circ a=e,$$

则称此代数系统$(S,\circ)$为群.

若群$(S,\circ)$满足交换律，则称$(S,\circ)$为交换群，或 Abel 群.

例 1　由单位元素自身构成之代数系统是一个群. 因为运算满足结合律，且其本身即是单位元素，它的逆元素即是它自己，故构成一个群.

例 2　设 $\mathbf{Z}$ 是整数集合，则$(\mathbf{Z},+)$是一个群.

单位元素是 0，每个元素 a 的逆元素为 $-a$.

例 3　设 S 是所有 n 阶非奇异矩阵的集合，“$\times$”是矩阵的乘法，则$(S,\times)$是一个群，因矩阵的乘法满足结合律，n 阶单位阵 $\boldsymbol{E}$，即为群$(S,\times)$的单位元素，每个元素 $\boldsymbol{A}$ 的逆元素 $\boldsymbol{A}^{-1}$为 $\boldsymbol{A}$ 的逆阵.

例 4　设 $\mathbf{Z}$ 是整数集，R 是 $\mathbf{Z}$ 上的同余关系，

$$S=\mathbf{Z}/R=\{[0]_R,[1]_R,[2]_R,\cdots,[n-1]_R\}.$$

这里的等价类又称为模 n 的剩余类. 我们在 S 上规定一个二元运算叫做加法，并用普通加法的符号来表示，规定

$$[a]+[b]=[a+b],$$

(这里因不致混淆,把$[a]_R$ 中 R 省略了)

则$(S,+)$作成一个群，这个群叫做模 n 的剩余类加群. 下面证明这个事实.

首先，要说明$(S,+)$是代数系统，即运算“$+$”具有封闭性，这只须证 aRa_1，bRb_1，应有$(a+b)R(a_1+b_1)$；即$[a]=[a_1]$，$[b]=[b_1]$，应有

$$[a+b]=[a]+[b]=[a_1]+[b_1]=[a_1+b_1].$$

这是正确的，因若 aRa_1 及 bRb_1，则 $n\mid a-a_1$，$n\mid b-b_1$，由于

$$(a-a_1)+(b-b_1)=(a+b)-(a_1+b_1),$$

故有 $n\mid[(a+b)-(a_1+b_1)]$，从而$(a+b)R(a_1+b_1)$.

其次，说明$(S,+)$满足群定义中的三条：

$$[a]+([b]+[c])=[a]+[b+c]=[a+b+c].$$

$$([a]+[b])+[c]=[a+b]+[c]=[a+b+c].$$

即
$$([a]+[b])+[c]=[a]+([b]+[c]).$$

$$[0]+[a]=[0+a]=[a]=[a+0]=[a]+[0].$$

$$[-a]+[a]=[-a+a]=[0]=[a+(-a)]=[a]+[-a].$$

故$(S,+)$作成一个群，且易证它是 Abel 群，其单位元素$[0]$，每个元素$[a]$的逆元素为$[-a]$．其具体运算可由表 3－10 给出

表 3－10

$+$	$[0]$	$[1]$	……	$[n-2]$	$[n-1]$
$[0]$	$[0]$	$[1]$	……	$[n-2]$	$[n-1]$
$[1]$	$[1]$	$[2]$	……	$[n-1]$	$[0]$
$[n-1]$	$[n-1]$	$[0]$	……	$[n-3]$	$[n-2]$

定理 1 （1）设半群$(S,\circ)$有一个左单位元素 e，$e\circ a=a$，$a\in S$，且对每一 $a\in S$，a 有左逆元素 a^{-1}：$a^{-1}\circ a=e$，则$(S,\circ)$是群．

（2）设$(S,\circ)$是一半群，若对于 S 中任意 a，b，方程 $a\circ x=b$，$y\circ a=b$ 在 S 中都有解，则$(S,\circ)$是群．

证 略．

例 5 设 S 为所有二阶非奇异矩阵的集合，“$\times$”是矩阵的乘法，$\boldsymbol{E}=\begin{pmatrix}1&0\\0&1\end{pmatrix}$，$\boldsymbol{A}=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in S$，有 $\boldsymbol{E}\times\boldsymbol{A}=\begin{pmatrix}1&0\\0&1\end{pmatrix}\times\begin{pmatrix}a&b\\c&d\end{pmatrix}=\begin{pmatrix}a&b\\c&d\end{pmatrix}=\boldsymbol{A}$，且有

$\boldsymbol{A}^{-1}=\dfrac{1}{\det\boldsymbol{A}}\begin{pmatrix}d&-b\\-c&a\end{pmatrix}\in S$，使 $\boldsymbol{A}^{-1}\times\boldsymbol{A}=\boldsymbol{E}$，于是由定理 1 中的(1)便知$(S,\times)$是群．还可以这样考虑，设 $\boldsymbol{A}$，$\boldsymbol{B}\in S$，则有 $\boldsymbol{A}^{-1}$，$\boldsymbol{B}^{-1}$使 $\boldsymbol{A}^{-1}\times\boldsymbol{A}=\boldsymbol{A}\times\boldsymbol{A}^{-1}=\boldsymbol{E}$ 及 $\boldsymbol{B}^{-1}\times\boldsymbol{B}=\boldsymbol{B}\times\boldsymbol{B}^{-1}=\boldsymbol{E}$，对于方程 $\boldsymbol{A}\times\boldsymbol{X}=\boldsymbol{B}$ 及 $\boldsymbol{Y}\times\boldsymbol{A}=\boldsymbol{B}$ 有

$$\boldsymbol{X}=\boldsymbol{E}\times\boldsymbol{X}=\boldsymbol{A}^{-1}\times\boldsymbol{A}\times\boldsymbol{X}=\boldsymbol{A}^{-1}\times\boldsymbol{B},\quad \boldsymbol{Y}=\boldsymbol{Y}\times\boldsymbol{E}=\boldsymbol{Y}\times\boldsymbol{A}\times\boldsymbol{A}^{-1}=\boldsymbol{B}\times\boldsymbol{A}^{-1},$$

而 $\boldsymbol{A}^{-1}\times\boldsymbol{B}$ 与 $\boldsymbol{B}\times\boldsymbol{A}^{-1}$均属于 S，故由定理 1 中的(2)知$(S,\times)$是群．

例 6 设 H 是所有 2 阶方阵的集合，则$(H,\times)$不作成群．因为对某一元素 $\boldsymbol{A}\in H$，$\boldsymbol{A}$ 不一定有左逆元素 $\boldsymbol{A}^{-1}$；另外从方程 $\boldsymbol{A}\times\boldsymbol{X}=\boldsymbol{B}$ 及 $\boldsymbol{Y}\times\boldsymbol{A}=\boldsymbol{B}$ 在 H 内不一定有解也可得知$(H,\times)$不是群．

定义 2 设$(S,\circ)$为一个群，H 是 S 的一个子集，若$(H,\circ)$仍是群；则群$(H,\circ)$叫做群$(S,\circ)$的一个子群．

例 7 已知$(\mathbf{Z},+)$是一个群，设 $\mathbf{Z}_E=\{x\mid x=2n,n\in\mathbf{Z}\}$，证明$(\mathbf{Z}_E,+)$是

$(\mathbf{Z},+)$的一个子群.

证　对任意的 x，$y\in\mathbf{Z}_E$，设 $x=2n_1$，$y=2n_2$，n_1，$n_2\in\mathbf{Z}$，则

$$x+y=2n_1+2n_2=2(n_1+n_2).$$

而 $n_1+n_2\in\mathbf{Z}$，所以 $x+y\in\mathbf{Z}_E$，即$(\mathbf{Z}_E,+)$为一个代数系统. 又

(1) 运算"$+$"在 $\mathbf{Z}_E$ 上结合律成立.

(2) $(\mathbf{Z},+)$中的单位元素也在$(\mathbf{Z}_E,+)$中.

(3) 对于任意的 $x\in\mathbf{Z}_E$，必有 n 使得 $x=2n$，而 $-x=-2n=2(-n)$，$-n\in\mathbf{Z}$，所以 $-x\in\mathbf{Z}_E$，且有 $x+(-x)=0$.

因此，$(\mathbf{Z}_E,+)$是$(\mathbf{Z},+)$的一个子群. 证毕.

例 8　设 $\boldsymbol{E}$ 是 n 阶单位矩阵，$\boldsymbol{A}_k$ 为 n 阶矩阵，且

$$\boldsymbol{A}_1=\begin{pmatrix}0&1&0&\cdots&0&0\\0&0&1&\cdots&0&0\\ & & & & & \\0&0&0&\cdots&0&1\\1&0&0&\cdots&0&0\end{pmatrix},\ \boldsymbol{A}_k=\begin{pmatrix}0&\boldsymbol{E}_{n-k}\\\boldsymbol{E}_k&0\end{pmatrix},\ k=1,2,\cdots,n-1.$$

$\boldsymbol{E}_k$ 为 k 阶单位矩阵，S 是所有 n 阶非奇异矩阵之集合，由例子知$(S,\times)$为一个群. 令 $L_n=\{\boldsymbol{E},\boldsymbol{A}_1,\boldsymbol{A}_2,\boldsymbol{A}_3,\cdots,\boldsymbol{A}_{n-2},\boldsymbol{A}_{n-1}\}$，则易证 $L_n\subseteq S$，又对任意的 A_s，$\boldsymbol{A}_t\in L_n$，有 $\boldsymbol{A}_s\times\boldsymbol{A}_t=\boldsymbol{A}_{s+t}$，

$$\boldsymbol{A}_{s+t}=\begin{pmatrix}0&\boldsymbol{E}_{n-(s+t)}\\\boldsymbol{E}_{s+t}&0\end{pmatrix}，当 s+t<n 时，$$

有 $\boldsymbol{A}_{s+t}=\boldsymbol{A}_{s+t-n}=\begin{pmatrix}0&\boldsymbol{E}_{n-(s+t-n)}\\\boldsymbol{E}_{s+t-n}&0\end{pmatrix}=\begin{pmatrix}0&\boldsymbol{E}_{2n-(s+t)}\\\boldsymbol{E}_{s+t-n}&0\end{pmatrix}$，当 $s+t>n$ 时.

而 $2n-(s+t)<n$，$s+t-n<n$，故有 $A_{s+t}\in L_n$，即$(L_n,\times)$为代数系统. 又运算"$\times$"在 L_n 上结合律成立，对每一 $A_k\in L_n$，存在 $A_{n-k}\in L_n$，使 $\boldsymbol{A}_k\times\boldsymbol{A}_{n-k}=\boldsymbol{A}_{n-k}\times\boldsymbol{A}_k=\boldsymbol{E}$，而 $E\in L_n$，故知$(L_n,\times)$是群$(S,\times)$的一个子群.

对于半群来说，它与其子半群可能有不同的单位元素，而对于群来说，就不存在这种现象，群与其任一子群的单位元素都是一致的.

定理 2　设$(S,\circ)$为一群，则在$(S,\circ)$中消去律成立. 即对任意的 a，b，$c\in S$，有

(左消去律) $a\circ b=a\circ c\Rightarrow b=c$.

(右消去律) $b\circ a=c\circ a\Rightarrow b=c$.

证　只证左消去律

$b=e\circ b=(a^{-1}\circ a)\circ b=a^{-1}\circ(a\circ b)=a^{-1}\circ(a\circ c)=(a^{-1}\circ a)\circ c=e\circ c=c$. 证毕.

定理 3　设$(H,\circ)$是群$(S,\circ)$的一个子群，则$(H,\circ)$的单位元素e_1就是$(S,\circ)$中的单位元素；$a\in H$，则a在$(S,\circ)$中的逆元素就是a在$(H,\circ)$中的逆元素.

证　设e_1是$(H,\circ)$的单位元素，e是$(S,\circ)$的单位元素，则$e_1=e_1\circ e_1$，$e_1=e_1\circ e$，由消去律得出$e_1=e$.

设$a\in H$，a在$(S,\circ)$的逆为a^{-1}，a在$(H,\circ)$中的逆为b，则$a\circ a^{-1}=e=a\circ b$，由消去律得出$a^{-1}=b$.　证毕.

从例 7、例 8 中很容易验证定理 3 的结论，下面的定理 4 是子群的判定方法.

定理 4　设H是S的一个非空子集，则$(H,\circ)$作为群$(S,\circ)$的子群的充要条件是

(1)　$(H,\circ)$是一个代数系统

(2)　对每一$a\in H$，有$a^{-1}\in H$.

证　设$(H,\circ)$是群$(S,\circ)$的子群，(1) 是显然的，由定理 3，$a\in H$，a在$(H,\circ)$中的逆就是a在$(S,\circ)$中的逆a^{-1}，故$a^{-1}\in H$.

反之，设$(H,\circ)$适合 (1)，(2)．由 (1) 知$(H,\circ)$是$(S,\circ)$的子半群．由于H非空，故存在$a\in H$，由 (2)，$a^{-1}\in H$．又由 (1)，$a\circ a^{-1}=e\in H$，即$(H,\circ)$有单位元素，且每一元素均有逆元素．故$(H,\circ)$是群$(S,\circ)$的一个子群．证毕.

任意群都有子群，自身及仅含单位元素的子集是两个子群．除此之外，若还存在其他子群，则称这些子群为真子群.

例 9　设$(H_1,\circ)$与$(H_2,\circ)$都是群$(S,\circ)$的子群，则$(H_1\cap H_2,\circ)$是$(S,\circ)$的子群.

证　设$a，b\in H_1\cap H_2$，则$a，b\in H_1$且$a，b\in H_2$，故由题知$a\circ b\in H_1$，$a\circ b\in H_2$，从而$a\circ b\in H_1\cap H_2$，即知$(H_1\cap H_2,\circ)$是一个代数系统.

又设$a\in H_1\cap H_2$，则$a\in H_1$，$a\in H_2$，由于$(H_1,\circ)$ $(H_2,\circ)$是$(S,\circ)$的子群，再由定理 3 知a在$(H_1,\circ)$及$(H_2,\circ)$中的逆元素就是a在$(S,\circ)$中的逆元素a^{-1}，故$a^{-1}\in H_1\cap H_2$，由定理 4 知$(H_1\cap H_2,\circ)$是$(S,\circ)$的子群．证毕.

例 10　设$(S,\circ)$是一个群，S是n阶非奇异矩阵集合，“$\circ$”是矩阵的乘．令

$$H=\{\boldsymbol{A}\mid \boldsymbol{A}\in S\ 且\ \det \boldsymbol{A}=1\},$$

则$(H,\circ)$是$(S,\circ)$的一个子群.

证　设$\boldsymbol{A}，\boldsymbol{B}\in H$，则$\det\boldsymbol{A}=1$且$\det\boldsymbol{B}=1$．由$\det(\boldsymbol{A}\circ\boldsymbol{B})=\det\boldsymbol{A}\cdot\det\boldsymbol{B}=1$，知$\boldsymbol{A}\circ\boldsymbol{B}\in H$.

又设$\boldsymbol{A}\in H$，$\det\boldsymbol{A}=1$，由矩阵知识可知$\boldsymbol{A}$的逆阵为

$$\boldsymbol{A}^{-1}=\frac{1}{\det\boldsymbol{A}}\operatorname{adj}\boldsymbol{A}，于是$$

$\det A^{-1}=\frac{1}{(\det A)^n}\cdot\det(\mathrm{adj}\,A)=\frac{\det A}{(\det A)^{n+1}}\cdot\det(\mathrm{adj}\,A)=\frac{1}{(\det A)^{n+1}}\cdot\det(A\circ\mathrm{adj}\,A)=\frac{1}{(\det A)^{n+1}}\cdot\det(\det A\cdot E_n)=\frac{(\det A)^n}{(\det A)^{n+1}}=\frac{1}{\det A}=1.$

及 $A^{-1}\in H$. 由定理 4 知$(H,\circ)$是$(S,\circ)$的子群.

（注 $\det A$ 表示 A 的行列式,$\mathrm{adj}\,A$ 表示 A 的伴随阵,$\det(A\circ B)=\det A\cdot\det B$ 为行列式的乘法规则,E_n 为 n 阶单位阵）. 证毕.

在群$(S,\circ)$中，每一个元素 a 可能有正整数 n 存在，使 $a^n=e$，也可能 a，a^2，…，a^n，…均不等于 e，即对任意正整数 n，$a^n\neq e$. 关于这两种情形我们有

定义 3 设$(S,\circ)$是一个群，$a\in S$. 使 $a^n=e$ 的最小自然数 n，叫做 a 的周期(或 a 的阶). 如果这样的 n 不存在，则说 a 的周期是无限的.

例 11 S 是 n 阶非奇异矩阵的集合，$(S,\times)$为一群. 设 A_1 如例 8 中所示，则 $A_1^n=E$，即 A_1 的周期为 n. 设 A 为对合矩阵，即 $A^2=E$，则 A 的周期为 2. A_k 亦如例 8 中所示，可以推得每个 A_k 的周期是有限数，当 n 给定后，便可求出 A_k 的周期.

例 12 $(\mathbf{Z},+)$中，除 0 以外，每一元素的周期均是无限的.

定义 4 如果群$(S,\circ)$只含有限个元素，则说$(S,\circ)$是有限群；否则，$(S,\circ)$叫做无限群. 有限群的元素个数叫做群$(S,\circ)$的阶，记作 $|S|$.

定理 5 (1) 设 a 的周期为 m，当且仅当 $m\mid n$ 时，$a^n=e$；

(2) 设$(S,\circ)$是有限群，则$(S,\circ)$的每一元素的周期均为有限.

证 (1) 请读者自证.

(2) $\forall a\in S$，则 a，a^2，a^2，$\cdots\in S$，由于 S 为有限集合，故 a，a^2，a^2，…不能全部不相同. 设 $a^i=a^j$，$i>j$，则 $a^{i-j}=e$，$i-j=k$ 是自然数. 命 $A=\{k\mid a^k=e\}$，则 A 不空，而自然数的非空集合有最小元，设 A 的最小元为 n，则 $a^n=e$，即 n 是 a 的周期. 证毕.

例 13 在例 8 中的群$(L_n,\times)$，$|L_n|=n$，每个元素的周期为有限.

例 14 在例 4 的群$(S,+)$中，每个元素的周期也都是有限的，当 n 具体给定时，便能求出每个元素的周期. $|S|=n$.

例 15 设 a，b 为群$(S,\circ)$中的任意二元素，则 $a\circ b$ 与 $b\circ a$ 具有相同的周期.

证 设 $a\circ b$ 的周期为 n，即$(a\circ b)^n=e$，而

$$\begin{aligned}(b\circ a)^n&=(b\circ a)\circ(b\circ a)\circ(b\circ a)\circ\cdots\cdots\circ(b\circ a)\circ(b\circ a)\\&=b\circ(a\circ b)\circ(a\circ b)\circ\cdots\cdots\circ(a\circ b)\circ a\\&=b\circ(a\circ b)^{n-1}\circ a\\&=b\circ(a\circ b)^{n-1}\circ a\circ b\circ b^{-1}\end{aligned}$$

$$=b\circ(a\circ b)^n\circ b^{-1}$$
$$=b\circ e\circ b^{-1}$$
$$=e.$$

又当 $k<n$ 时，$(b\circ a)^k\neq e$，否则，可推出 $(a\circ b)^k=e$，与 n 是 $a\circ b$ 的周期矛盾，故 n 也是 $b\circ a$ 的周期. 证毕.

二、循环群

定义 5 若一个群 $(S,\circ)$ 的每一元素 b 均是它的某一固定元素 a 的某次方幂，即存在 n 使 $b=a^n$，$n\in\mathbf{Z}$，则称 $(S,\circ)$ 是由 a 生成之循环群，而 a 叫做 $(S,\circ)$ 的生成元素.

例 16 设 $G=\{1,-1,\mathrm{i},-\mathrm{i}\}$，则 $(G,\times)$ 是一个循环群，生成元素为 i，因为 $\mathrm{i}^0=1$，$\mathrm{i}^1=\mathrm{i}$，$\mathrm{i}^2=-1$，$\mathrm{i}^3=-\mathrm{i}$，$\mathrm{i}^4=1$，$\mathrm{i}^5=\mathrm{i}$，…. 群的阶是 4，单位元素是 1，生成元素 i 的周期为 4.

例 17 例 4 所说的群 $(S,+)$ 与例 8 所说的群 $(L_n,\times)$ 均是循环群. $(S,+)$ 的生成元为 $[1]$，$(L_n,\times)$ 的生成元为 A_1.

例 18 设 $G=\{x\mid x=2^k,k\in\mathbf{Z}\}$，则 $(G,\times)$ 是一循环群. 生成元素为 2 或 2^{-1}，单位元素 $1=2^0$，生成元素 2 或 2^{-1} 的周期为无限.

定理 6 循环群 $(S,\circ)$ 必是可换(Abel)群.

证 设循环群 $(S,\circ)$ 生成元为 a，且 b，$c\in S$，则存在 m 及 n 使 $b=a^m$，$c=a^n$. 于是

$$b\circ c=a^m\circ a^n=a^{m+n}=a^{n+m}=a^n\circ a^m=c\circ b,$$

即 $(S,\circ)$ 为可换(Abel)群. 证毕.

一个群 $(S,\circ)$ 不一定是循环群，但它的子群却可能是循环群. 见下面的定理.

定理 7 若 b 是群 $(S,\circ)$ 中的一个元素，b 的周期为 m，令 $H=\{b^n\mid n\in\mathbf{Z}\}$，则 $(H,\circ)$ 是 $(S,\circ)$ 的一个 m 阶子群. 它是由 b 生成的循环群.

证 首先 $(H,\circ)$ 是 $(S,\circ)$ 的一个子群. 因为对所有 s，$t\in\mathbf{Z}$. 有

(1) 对每个 b^s，$b^t\in H$，$b^s\circ b^t=b^{s+t}\in H$.

(2) 设 $b^s\in H$，有 $(b^s)^{-1}=b^{-s}\in H$.

其次，$(H,\circ)$ 是循环子群.

若 m 为无限数，往证 b^s 是互不相同的，假定 $b^s=b^t$，不妨设 $s>t$，于是 $b^{s-t}=e$，于是 b 的周期是 $s-t$ 的因数，这与 b 的周期 m 为无限矛盾. b 的周期为无限，则 $|H|$ 也是无限的.

若 m 为有限数，我们证明 $H=\{b^0=e,b^1,b^2,\cdots,b^{m-1}\}$. 假定 $b^s=b^t$，其中 $0\leqslant t<s\leqslant m-1$，于是 $b^{s-t}=e$，其中 $0<s-t<m$，这与 b 的周期是 m 矛盾，因

此当 $0\leqslant t<s<m-1$ 时，$b^t\neq b^s$. 而当 $u\geqslant m$ 时，总有 $u=km+t$，$0\leqslant t<m$，于是

$$b^u=b^{km+t}=b^{km}\circ b^t=(b^m)^k\circ b^t=e^k\circ b^t=b^t.$$

故必有 $H=\{b^0,b^1,b^2,\cdots,b^{m-1}\}$，即 $|H|=m$. 证毕.

例 19　设 $\mathbf{Q}^*$ 是非零有理数集合，则在乘法运算下 $(\mathbf{Q}^*,\times)$ 是一个群，但它不是循环群，因为没有一个有理数 r 使得其他每个非零有理数用 r^n 表示. 令 H 如例 18，则 H 是 $\mathbf{Q}^*$ 的子集，而 $(H,\times)$ 也是群. 它是 $(\mathbf{Q}^*,\times)$ 的子群，且是其循环子群.

例 20　n 阶非奇异矩阵集合 S 在矩阵乘法下作成一群 $(S,\times)$，它不是循环群. 由例 8 及例 17 知 $(L_n,\times)$ 是 $(S,\times)$ 的循环子群.

定理 8　循环群的子群也是循环群.

证　设 $(S,\circ)$ 是循环群，$(H,\circ)$ 是其子群，a 是 $(S,\circ)$ 的生成元素，对任一 $b\in S$，存在 $n\in\mathbf{Z}$，使 $b=a^n$.

若 $H=\{e\}$，则 $(H,\circ)$ 是循环子群，生成元素为 e.

若 $(H,\circ)$ 是 $(S,\circ)$ 真子群，则有 $a^t\in H$，$t\neq 0$，$t\in\mathbf{Z}$. 由于子群 $(H,\circ)$ 对求逆是封闭的，故可让 $t>0$，令

$$m=\min\{t\mid a^t\in H,t>0,t\in\mathbf{Z}\}$$

让 $b=a^m$，往证 b 生成 $(H,\circ)$.

设 $x\in H$，$x\neq b$，因 $x\in S$，故有 $n\in\mathbf{Z}$ 使 $x=a^n$. 而 n 可表为

$$n=mk+r\text{，这里 }0\leqslant r<m\text{，}k\text{，}r\in\mathbf{Z}\text{，于是有}$$

$$a^n=a^{mk+r}=a^{mk}\circ a^r=(a^m)^k\circ a^r=b^k\circ a^r.$$

故 $a^r=b^{-k}\circ a^n$，由于 a^n，$b^k\in H$，$(H,\circ)$ 是子群，因此 $b^{-k}\circ a^n\in H$，从而 $a^r\in H$. 由上面 m 的选取及 $0\leqslant r<m(n=mk+r)$ 知必有 $r=0$. 从而可知 $a^n=b^k\circ a^r=b^k\circ e=b^k$，即 $x=b^k$. 由循环群定义及 x 的任意性知 $(H,\circ)$ 是循环群. 证毕.

下面再举两个循环群的例子

例 21　设 $G=\{\alpha,\beta,\gamma,\delta\}$，在 G 上定义二元运算“$\circ$”如表 3－11

表 3－11

$\circ$	α	β	γ	δ
α	α	β	γ	δ
β	β	α	δ	γ
γ	γ	δ	β	α
δ	δ	γ	α	β

则 $(G,\circ)$ 是一个循环群.

证　由运算表可知运算“$\circ$”是封闭的，α 是单位元素，β，γ 和 δ 的逆

元素分别是 β，δ 和 γ。（G，$\circ$）是一个群.

由于

$$\gamma^1=\gamma^2，\gamma^2=\gamma\circ\gamma=\beta，\gamma^3=\beta\circ\gamma=\delta，\gamma^4=\delta\circ\gamma=\alpha.$$

$$\delta^1=\delta，\delta^2=\delta\circ\delta=\beta，\delta^3=\beta\circ\delta=\gamma，\delta^4=\gamma\circ\delta=\alpha.$$

故群（G，$\circ$）是一循环群，生成元素是 γ 或 δ.

例 22　如果 6 个元素的交换（Abel）群包含了一个周期为 3 的元素，则这个群是循环群.

证　设（S，$\circ$）是由题所给的群，a 是一个周期为 3 的元素，则 S 中含有 e，a，a^2. 令 S 中的另外三个元素分别为 b，c，d，则由于（S，$\circ$）是群及逆元素的惟一性可知 b，c，d 三个元素中至少有一个周期为 2. 事实上 a 与 a^2 互逆，若 b，c，d 中有两个元素互为逆元素，则剩下的一个元素必与自身互逆，这个剩下的元素，周期便是 2. 不妨设 b 的周期为 2，于是可证 $a\circ b$ 生成（G，$\circ$）.

$(a\circ b)=a\circ b.$

$(a\circ b)^2=(a\circ b)\circ(a\circ b)=a^2\circ b^2=a^2\circ e=a^2.$

$(a\circ b)^3=a^3\circ b^3=e\circ b^2\circ b=b.$

$(a\circ b)^4=a^4\circ b^4=a^3\circ a\circ b^2\circ b^2=a.$

$(a\circ b)^5=a^5\circ b^5=a^3\circ a^2\circ b^2\circ b^2\circ b=a^2\circ b.$

$(a\circ b)^6=a^6\circ b^6=e.$

$(a\circ b)^7=a^7\circ b^7=a^6\circ a\circ b\circ b^6=a\circ b.$

$(a\circ b)^8=a^6\circ a^2\circ b^8=a^2.$

… … … …

（注意 $(a\circ b)^i=a^i\circ b^i$ 是由可交换性得到）

可见 $G=\{e,a\circ b,a^2,b,a,a^2\circ b\}$，因此，（$G$，$\circ$）是循环群，生成元素为 $a\circ b$. 证毕.

由上述介绍中可以看出，一个循环群中，任意由生成元生成的两个元素是不相同的.

从例 18 及例 21 可见循环群的生成元素不一定惟一.

从上面的内容还可看出要说明群（S，$\circ$）是循环群，找出其生成元素即可.

练习题 3－2

1. 确定下列集合中的每一个，关于所指出的元素运算是否组成群：

（1）整数，关于加法；

（2）偶数，关于加法；

（3）非负整数，关于加法；

（4）奇整数，关于加法；

（5）整数，关于减法；

（6）有理数，关于加法；

（7）有理数，关于乘法；

（8）非零有理数，关于乘法；

（9）正有理数，关于乘法；

（10）正有理数，关于除法.

2. 试证下面四个矩阵对于乘法成群

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\ \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix},\ \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},\ \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}.$$

3. 有单位元素且适合消去律的有限半群一定是群.

4. 令 $G=\{km \mid k\in \mathbf{Z}, m$ 是取定的自然数$\}$，证明$(G,+)$是一个群.

5. $G=\{a+b\mathrm{i} \mid a,b\in \mathbf{Z}, \mathrm{i}$ 是虚数单位$\}$，证明$(G,+)$是一个群.

6. $G=\{2^m 3^n \mid m,n\in \mathbf{Z}\}$，证明，$G$ 对于数字乘法作成群.

7.（1）如果 H 是群$(G,\circ)$的有限子集，并且对任意的 a，$b\in H$，有 $a\circ b\in H$，则$(H,\circ)$是$(G,\circ)$的子群.

（2）设 H 是群$(G,\circ)$有子集，且 H 中的元素在乘法“$\circ$”下周期均为有限，还有“$\circ$”在 H 上封闭，则$(H,\circ)$是$(G,\circ)$的子群.

8. 设 a，b 是群$(S,\circ)$中的两个元素，如果$(a\circ b)^2=a^2\circ b^2$，试证 $a\circ b=b\circ a$.

9. 设$(G,\circ)$是群，若对任意的 $a\in G$ 有 $a=a^{-1}$，则$(G,\circ)$是可换(Abel)群.

10. 设 $a\in G$，则 a 与 a^{-1}有相同周期.

11. 设$(G,\circ)$是 6 阶循环群，找出$(G,\circ)$的一切生成元，再找出$(G,\circ)$的所有子群.

12. 设 a，b 是群$(G,\circ)$元素，a 的周期为 2，b 的周期为 3，且 $ab=ba$，则 ab 的周期为 6.

13. 列出例 16 中群$(G,\times)$的运算(群)表.

14. 设集合 $G=\mathbf{Q}-\{1\}$，其中 $\mathbf{Q}$ 是有理数集，定义 G 上的二元运算 $*$ 为 $\forall a$，$b\in G$，$a*b=a+b-ab$，试证$(G,*)$是群.

15. 设 $S=\{0,1,2,3\}$，$\otimes$为模 4 乘法，即 $\forall x$，$y\in S$，$x\otimes y=(xy)\bmod 4$. 问$(S,\otimes)$构成什么代数系统(半群,独异点,群)？为什么？

16. 设$(G,\circ)$是 24 阶循环群，求出它的所有子群.

第三节　变　换　群

本节我们介绍变换群，它在群论中是具有代表性的群. 我们先介绍变换的一些概念，之后通过变换的合成及群的定义就可得到变换群.

定义 1　设 A，B 是给定的两个集合，如果有一个规则 f，通过它对于每一 $x\in A$，惟一确定一个 $y\in B$，则称 f 是 A 到 B 的一个变换(映射). 记为

$$f: A\to B.$$

A 叫做变换 f 的定义域，B 叫做 f 的值域，y 叫做 x 的像，记为 $y=f(x)$，且用符号 $f: x\mapsto y$ 表示，而 x 叫做 y 的原像.

设 f、g 是 A 到 B 的两个变换，若对于任意的 $x\in A$ 有 $f(x)=g(x)$，则称 f 等于 g，记为 $f=g$.

例 1 设 $A=\{x_1,x_2,\cdots,x_n\}$，定义 f 为 $f(x_i)=x_j$，i，$j=1$，2，$\cdots$，n，则 f 是 A 到 A 上的一个变换，将 $f(x_i)=x_j$ 可记为 $f: x_i\mapsto x_j$. 例如 $A=\{a,b,c\}$ $f(a)=a$，$f(b)=b$，$f(c)=c$，显然 f 是 A 到 A 上的一个变换.

例 2 设 $A=\{a,b,c,d\}$，$B=\{1,2,3,4,5\}$.

令 $f: a\mapsto 3$，$b\mapsto 4$，$c\mapsto 2$，$d\mapsto 1$，

$g: a\mapsto 1$，$b\mapsto 5$，$c\mapsto 5$，$d\mapsto 1$，

$h: a\mapsto 2$，$c\mapsto 5$，

则 f、g 是 A 到 B 的变换，而 h 不是 A 到 B 的变换，因 b、d 在 h 的作用下没有像.

定义 2 从 A 到 A 的变换 $I_x: x\mapsto x$，$x\in A$，称为 A 上的单位变换（或恒等变换）.

在例 1 中如 $A=\{a,b,c\}$，$f: x\mapsto x$，$x\in A$，则 f 为 A 上的单位变换.

定义 3 设 f 是 A 到 B 的一个变换.

（1）若对任意的 a，$b\in A$，当 $a\neq b$ 时，有 $f(a)\neq f(b)$，称 f 是 A 到 B 的一个单一变换.

（2）若对任意 $b\in B$，均存在 $a\in A$，使得 $f(a)=b$，则称 f 是 A 到 B 上的一个变换.

（3）若 f 既是 A 到 B 的单一变换，又是 A 到 B 上的变换，则称 f 是 A 到 B 上的一一变换.

例 3 设 $f(x)=2x$，则 f 是 $A=[0,1]$ 到 $B=[0,2]$ 上的一个一一变换. 设 $g(x)=2x^2$，则 g 也是 $A=[0,1]$ 到 $B=[0,2]$ 上的一个一一变换. 再设 $h(x)=2x^k$，k 是自然数，则 h 是 $A=[0,1]$ 到 $B=[0,2]$ 上的一个一一变换. 由此可见，A 到 B 上一一变换可以有无限个.

例 4 设 $A=\{a,b,c,d\}$，$B=\{1,2,3,4,5\}$，$C=\{x,y,z\}$，令 $f: a\mapsto 1$，$b\mapsto 2$，$c\mapsto 3$，$d\mapsto 4$，$g: a\mapsto y$，$b\mapsto y$，$c\mapsto x$，$d\mapsto z$. 则 f 是 A 到 B 的单一变换，但不是 A 到 B 上的变换. 而 g 是 A 到 C 上的变换，但不是单一变换，f 与 g 都不是 A 到 B 上与 A 到 C 上的一一变换.

若 $A=\{x_1,x_2,\cdots,x_n\}$，f 是 A 到 A 上的一一变换，则称 f 是 A 上的一个 n 阶置换. 一般将 n 阶置换 f 记为

$$f=\begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ f(x_1) & f(x_2) & \cdots & f(x_n) \end{pmatrix}.$$

易见 A 上 n 阶置换共有 $n!$ 个. 如，设 $A=\{a,b,c\}$，则 A 上的 3 阶置换为

$$f_1=\begin{pmatrix}a & b & c\\ a & b & c\end{pmatrix},\ f_2=\begin{pmatrix}a & b & c\\ a & c & b\end{pmatrix},\ f_3=\begin{pmatrix}a & b & c\\ b & a & c\end{pmatrix},$$

$$f_4=\begin{pmatrix}a & b & c\\ b & c & a\end{pmatrix},\ f_5=\begin{pmatrix}a & b & c\\ c & a & b\end{pmatrix},\ f_6=\begin{pmatrix}a & b & c\\ c & b & a\end{pmatrix}.$$

共有 $3!=6$ 个.

定义 4　设有三个集合 A、B、C，及变换 $\varphi: A\to B$. $f: B\to C$，对任意 $a\in A$，由 φ、f 确定的 A 到 C 的变换 $g: a\mapsto f[\varphi(a)]$ 叫做变换 φ、f 的合成，记为 $g=f\circ\varphi$，也即 $g(a)=f[\varphi(a)]=f\circ\varphi(a)$. g 可用图 3－1 表示.

$$\begin{tikzcd} A \arrow[rr, "g=f\circ\varphi"] \arrow[dr, "\varphi"'] & & C \\ & B \arrow[ur, "f"'] & \end{tikzcd}$$

图 3－1

例 5　设

$$f_1=\begin{pmatrix}a & b & c & d\\ b & c & d & a\end{pmatrix},\ f_2=\begin{pmatrix}a & b & c & d\\ c & d & a & b\end{pmatrix}$$

，

则
$$f_1\circ f_2=\begin{pmatrix}a & b & c & d\\ b & c & d & a\end{pmatrix}\circ\begin{pmatrix}a & b & c & d\\ c & d & a & b\end{pmatrix}=\begin{pmatrix}a & b & c & d\\ d & a & b & c\end{pmatrix}.$$

即把 f_1 的上排及 f_2 的下排作为中间量；而取 f_1 的下排及 f_2 的上排作一个新置换，即为 $f_1\circ f_2$. 具体做法是 f_2 中 $a\mapsto c$，而 f_1 中 $c\mapsto d$，故在 $f_1\circ f_2$ 中有 $a\mapsto d$，其他同理. 置换的合成也叫做置换的乘法. 易见

$$f_1\circ f_2=\begin{pmatrix}a & b & c & d\\ d & a & b & c\end{pmatrix}.$$

可见 $f_1\circ f_2=f_2\circ f_1$，这种性质叫做变换合成的可交换性.

值得注意的是变换的合成不一定都具备例 5 中说到的可交换性. 如

$$\varphi_1=\begin{pmatrix}a & b & c & d\\ d & c & a & b\end{pmatrix},\ \varphi_2=\begin{pmatrix}a & b & c & d\\ c & a & b & d\end{pmatrix},$$

则
$$\varphi_1\circ\varphi_2=\begin{pmatrix}a & b & c & d\\ a & d & c & b\end{pmatrix},\ \varphi_2\circ\varphi_1=\begin{pmatrix}a & b & c & d\\ d & b & c & a\end{pmatrix},$$

而
$$\varphi_1\circ\varphi_2\neq\varphi_2\circ\varphi_1.$$

例 6　设 $f(y)=\arcsin y$，则 $f=\arcsin$ 是从 $A=[-1,1]$ 到 $B=\left[-\frac{\pi}{2},\frac{\pi}{2}\right]$ 上的一一变换，再设 $y=\varphi(x)=2x$，$x\in\left[-\frac{1}{2},\frac{1}{2}\right]$，则 φ 是从 $C=\left[-\frac{1}{2},\frac{1}{2}\right]$ 到 $A=[-1,1]$ 上的一一变换. 于是 $f\circ\varphi$ 是从 C 到 B 上的一一变换，且 $f\circ\varphi(x)=\arcsin(2x)$.

关于变换的合成及单位变换有

定理 1 设 $f: A\to B$，$g: B\to C$，$\varphi: C\to D$，则有

(1) $\varphi\circ(g\circ f)=(\varphi\circ g)\circ f$.

(2) $I_B\circ f=f$，$f\circ I_A=f\circ$ (I_A、I_B 分别表示 A 上与 B 上的单位变换).

证 (1) 显然 $\varphi\circ(g\circ f)$ 与 $(\varphi\circ g)\circ f$ 的定义域及值域都相同，定义域为 A，值域为 D. 又由于

$$[\varphi\circ(g\circ f)](x)=\varphi[(g\circ f)(x)]=\varphi\{g[f(x)]\}$$
$$=(\varphi\circ g)[f(x)]=[(\varphi\circ g)\circ f](x),x\in A.$$

故有
$$\varphi\circ(g\circ f)=(\varphi\circ g)\circ f.$$

(2) $I_B\circ f=f$ 与 f 的定义域均为 A，值域均为 B. 并且对于任意的 $x\in A$，有

$$(I_B\circ f)(x)=I_B[f(x)]=f(x)，即 I_B\circ f=f. 同理 f\circ I_A=f. 证毕.$$

例 7 设 $A=B=[0,+\infty)$，$f: x\mapsto x^2$，$g: x\mapsto x$，$x\in A$，则有 $f\circ g: x\mapsto x^2$，$g\circ f: x\mapsto x^2$，故知 $f\circ g=g\circ f$.

例 8 设 $A=\{a,b,c\}$，$B=\{1,2,3,4\}$，令 $f: A\to B$，且 $f: a\mapsto 1$，$b\mapsto 2$，$c\mapsto 3$；$g: B\to A$，且 $g: 1\mapsto a$，$2\mapsto b$，$3\mapsto c$，$4\mapsto a$，则 $g\circ f=I_A$，而 $f\circ g\neq I_B$.

为此我们引入定义 5.

定义 5 设 $f: A\to B$. 若存在 $g: B\to A$，使 $g\circ f=I_A$，则说 f 是左可逆变换，g 叫做 f 的一个左逆变换. 同样若 $f\circ\varphi=I_B$，则说 f 是右可逆变换，φ 叫做 f 的一个右逆变换. 当 f 是双侧可逆变换时，称 f 是可逆变换.

如：例 7 中的 f 是可逆变换，而且它的左逆变换与右逆变换相等. 例 8 中的 f 是左可逆变换，但不是右可逆变换，其左逆变换为 g. 若令 $g: 1\mapsto a$，$2\mapsto b$，$3\mapsto c$，$4\mapsto b$，则 φ 是不同于 g 的 f 的另一个左逆变换. 可见，左逆变换不一定惟一；当然，右逆变换也不一定惟一.

定理 2 $f: A\to B$. f 是左可逆变换的充要条件是，f 为单一变换；f 是右可逆变换的充要条件是，f 是 A 到 B 上的变换.

推论 $f: A\to B$，则 f 是可逆变换的充要条件是. f 是 A 到 B 上的一一变换.

证 略.

上面我们看到，左(右)可逆变换的左(右)逆变换不一定惟一，但却有

定理 3 设 $f: A\to B$，且 $g\circ f=I_A$，$f\circ\varphi=I_B$，则 $g=\varphi$，即可逆变换的左逆变换与右逆变换相等，这时逆变换还是惟一的，称 g 为 f 的逆变换. 记为 $g=f^{-1}$.

证 由定理 1，$g=g\circ I_B=g\circ(f\circ\varphi)=(g\circ f)\circ\varphi=I_A\circ\varphi=\varphi$，若 g_1 是 f 的另一个左逆变换，则由上面证明知 $g_1=\varphi=g$，即左逆变换的惟一，同样知右

逆变换惟一，也即逆变换惟一．证毕．

关于 f 的逆变换有 $(f^{-1})^{-1}=f$.

有了上面关于变换的概念及前述对群的讨论便会得出

定理 4　设 S 是一个集合，$G=\{f \mid f: S\to S, f$ 是 S 到 S 上的一一变换$\}$，"$\circ$"是关于变换的合成，则 $(G,\circ)$ 是一个群，这个群称为变换群.

证　对任意的 f，$\varphi\in G$，$f\circ\varphi$ 及 $\varphi\circ f$ 是 S 到 S 上的一一变换，故 $f\circ\varphi\in G$，$\varphi\circ f\in G$，又 $I_S\circ f=f\circ I_S=f$，I_S 是单位变换，$I_S\in G$；若 f 在 G 中，由定理 2 的推论知 f 存在逆变换 f^{-1}，且 f^{-1} 也是一一变换，即 $f^{-1}\in G$，由定理 1 的(1)及群的定义可知 $(G,\circ)$ 为一个群．证毕．

例 9　设 $A=\{a,b,c\}$，则 A 上的所有三阶置换为

$$f_1=\begin{pmatrix}a&b&c\\a&b&c\end{pmatrix},\ f_2=\begin{pmatrix}a&b&c\\b&a&c\end{pmatrix},\ f_3=\begin{pmatrix}a&b&c\\c&b&a\end{pmatrix},$$

$$f_4=\begin{pmatrix}a&b&c\\a&c&b\end{pmatrix},\ f_5=\begin{pmatrix}a&b&c\\b&c&a\end{pmatrix},\ f_6=\begin{pmatrix}a&b&c\\c&a&b\end{pmatrix}.$$

$S=\{f_1,f_2,f_3,f_4,f_5,f_6\}$，"$\circ$"是置换的合成，则 $(S,\circ)$ 构成一个群，称其为 3 次对称群。f_1 是单一元素，f_2，f_3，f_4 分别以自身为逆元素，f_5 及 f_6 互为逆元素，其运算如表 3－12：

表 3－12

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_6	f_5	f_4	f_3
f_3	f_2	f_5	f_1	f_6	f_3	f_4
f_4	f_4	f_6	f_5	f_1	f_3	f_2
f_5	f_5	f_3	f_4	f_2	f_6	f_1
f_6	f_6	f_4	f_3	f_2	f_1	f_5

当 $A=\{a_1,a_2,\cdots,a_n\}$ 时，A 上的所有 n 阶置换在置换的合成下也是一个群，叫做 n 次对称群，3 次对称群的阶为 $3!=6$，n 次对称群的阶为 $n!$.

例 10　设 $G=\{f \mid f:\mathbf{R}\to\mathbf{R}, f(x)=ax+b$；$a$，$b\in\mathbf{Q}$，$a\neq 0\}$，$\mathbf{R}$ 是实数集合，$\mathbf{Q}$ 是有理数集合，"$\circ$"为变换的合成，则 $(G,\circ)$ 为变换群.

证　运算"$\circ$"满足结合律是显然的，对任意的 f，$g\in G$，有 a，b，a_1，$b_1\in\mathbf{Q}$，使 $f(x)=ax+b$ 及 $g(x)=a_1x+b_1$，$a\neq 0$，$a_1\neq 0$，于是有 $f\circ g(x)=ag(x)+b=a(a_1x+b_1)+b=aa_1x+(ab_1+b)$，而 aa_1，$ab_1+b\in\mathbf{Q}$，$aa_1\neq 0$，故 $f\circ g\in G$，同样 $g\circ f\in G$，$I_{\mathbf{R}}$ 为 $I_{\mathbf{R}}(x)=x$，则 $I_{\mathbf{R}}\in G$ 且易证 $I_{\mathbf{R}}$ 为单位元素，对 $f\in G$，其逆 f^{-1} 为 $f^{-1}(x)=\dfrac{1}{a}x+\left(-\dfrac{b}{a}\right)$. 由群的定义可知 $(G,\circ)$

为变换群. 证毕.

练习题 3-3

1. 设 $S=\mathbf{R}-\{0,1\}$，$\mathbf{R}$ 是实数集，在 S 上定义 6 个变换如下：

$f_1(x)=x$；$f_2(x)=x^{-1}$；$f_3(x)=1-x$；$f_4(x)=(1-x)^{-1}$；$f_5(x)=(x-1)x^{-1}$；$f_6(x)=x(x-1)^{-1}$，$x\in S$.

证明 $(G,\circ)$ 是一变换群. $G=\{f_1,f_2,f_3,f_4,f_5,f_6\}$，“$\circ$”是变换的合成.

2. 设在实数集 $\mathbf{R}$ 上定义变换 $f:\mathbf{R}\to\mathbf{R}$ 且 $f(x)=ax+b$. 在下列各种情况中，以所指定类型的 a 和 b 为系数的所有可能变换 f 组合的集合，哪些是变换群，并给出证明：

(1) $a=1$，b 是奇数；

(2) $a=1$，b 是正整数或零；

(3) $a=1$，b 是偶数；

(4) a 是整数，$b=0$；

(5) $a\neq 0$，a 和 b 是实数；

(6) $a\neq 0$，a 是整数，b 是实数；

(7) $a\neq 0$，a 是实数，b 是整数；

(8) $a\neq 0$，a 是整数，b 是无理数；

(9) $a\neq 0$，a 是有理数，b 是实数；

在这些变换群中，哪些满足交换律？

3. 证明：所有正整数 $\mathbf{Z}^+$ 的集合上的变换 $f:n\mapsto n^2$，没有左逆变换. 并列出两个明显的右逆变换.

4. 设 σ，τ 是 5 阶置换，且

$$\sigma=\begin{pmatrix}1&2&3&4&5\\2&1&4&5&3\end{pmatrix},\quad \tau=\begin{pmatrix}1&2&3&4&5\\3&4&5&1&2\end{pmatrix}$$

求 $\sigma\tau$，$\tau\sigma$，σ^{-1}，τ^{-1}，$\sigma^{-1}\tau\sigma$.

5. 写出例 9 中群 $(S,\circ)$ 的所有子群.

第四节 同构与同态

本节我们介绍两个群之间的联系，主要研究两个群的同构与同态.

一、同构

设 $G=(\mathbf{R}^+,\times)$，即一切正实数对数的乘法作成的群，$S=(\mathbf{R},+)$ 为实数加群. 令 $f:x\to\ln x$，$x\in\mathbf{R}^+$，则 f 是 G 到 S 上的一个一一变换，并且

$$f(xy)=\ln xy=\ln x+\ln y=f(x)+f(y),\quad \forall x,\ y\in G.$$

$$f(1)=\ln 1=0,\ f\left(\frac{1}{x}\right)=\ln\frac{1}{x}=-\ln x.$$

我们看到这个变换具有良好的性质，$(\mathbf{R}^+,\times)$中任意二元素，按运算“$\times$”所得的结果在f作用下的像，恰好是这两个元素的像在$(\mathbf{R},+)$中运算所得结果，$(\mathbf{R}^+,\times)$的单位元素的像恰是$(\mathbf{R},+)$中的单位元素，群$(\mathbf{R}^+,\times)$中任意元素x的逆元素$1/x$的像$-\ln x$恰是x的像在$(\mathbf{R},+)$中的逆元素，从本质上看这两个群没什么区别，它们的内在结构是相同的，我们将这样的代数系统称为同构.

定义1　设$(S,\circ)$，$(G,*)$是两个群，若存在S到G上的一一变换f，且保持运算，即

$$f(a\circ b)=f(a)*f(b),\ a,\ b\in S,$$

则称f是$(S,\circ)$到$(G,*)$上的一个同构变换. 若两个群$(S,\circ)$，$(G,*)$之间存在同构变换，则称这两个群同构，记为$(S,\circ)\cong(G,*)$.

从定义1可以得出剩余类加群$(S,+)$与群$(L_n,\times)$是同构的.

例1　设$S=\{\alpha,\beta,\delta,\gamma\}$，$G=\{1,2,3,4\}$在$S$及$G$上定义运算如表3－13，3－14：

表3－13

$\circ$	α	β	δ	γ
α	α	β	δ	γ
β	β	α	γ	δ
δ	δ	γ	β	α
γ	γ	δ	α	β

表3－14

$*$	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	2	1
4	4	3	1	2

易证$(S,\circ)$与$(G,*)$作成群. 设f是$(S,\circ)$到$(G,*)$的一个变换，且让

$$f：\alpha\mapsto 1,\ \beta\mapsto 2,\ \delta\mapsto 3,\ \gamma\mapsto 4,$$

则f是$(S,\circ)$到$(G,*)$上的一一变换，又

$$f(\alpha\circ x)=f(x)=1*f(x)=f(\alpha)*f(x),\quad x=\beta,\ \delta,\ \gamma,\ \alpha.$$

$$f(\beta\circ x)=\begin{cases}f(\beta\circ\alpha)=f(\beta)=2=2*1=f(\beta)*f(\alpha),\\ f(\beta\circ\beta)=f(\alpha)=1=2*2=f(\beta)*f(\beta),\\ f(\beta\circ\delta)=f(\gamma)=4=2*3=f(\beta)*f(\delta),\\ f(\beta\circ\gamma)=f(\delta)=3=2*4=f(\beta)*f(\gamma).\end{cases}$$

$$f(\delta\circ x)=\begin{cases}f(\delta\circ\alpha)=f(\delta)=3=3*1=f(\delta)*f(\alpha),\\ f(\delta\circ\beta)=f(\gamma)=4=3*2=f(\delta)*f(\beta),\\ f(\delta\circ\delta)=f(\beta)=2=3*3=f(\delta)*f(\delta),\\ f(\delta\circ\gamma)=f(\alpha)=1=3*4=f(\delta)*f(\gamma).\end{cases}$$

$$f(\gamma\circ x)=\begin{cases}f(\gamma\circ\alpha)=f(\gamma)=4=4*1=f(\gamma)*f(\alpha),\\ f(\gamma\circ\beta)=f(\delta)=3=4*2=f(\gamma)*f(\beta),\\ f(\gamma\circ\delta)=f(\alpha)=1=4*3=f(\gamma)*f(\delta),\\ f(\gamma\circ\gamma)=f(\beta)=2=4*4=f(\gamma)*f(\gamma).\end{cases}$$

故知对任意的 x，$y\in(S,\circ)$，都有

$$f(x\circ y)=f(x)*f(y).$$

由定义 1 知 f 是同构变换，即 $(S,\circ)\cong(G,*)$.

例 2 设有两个群 $(\mathbf{R}^+,\times)$ 与 $(\mathbf{R},+)$，其中 $\mathbf{R}^+$ 与 $\mathbf{R}$ 分别表示正实数集合与实数集合.

令
$$\varphi: x\mapsto \ln x,\ x\in\mathbf{R}^+,$$
则 φ 是 $\mathbf{R}^+$ 至 $\mathbf{R}$ 上的一个一一变换，且

$$\varphi(x\times y)=\ln(x\times y)=\ln x+\ln y=\varphi(x)+\varphi(y),\ x,\ y\in\mathbf{R}^+,$$

故 φ 是 $(\mathbf{R}^+,\times)$ 到 $(\mathbf{R},+)$ 的一个同构变换，即有 $(\mathbf{R}^+,\times)\cong(\mathbf{R},+)$.

若令
$$\varphi: x\mapsto \log_a x,\ a,\ x\in\mathbf{R}^+,$$
则 φ 仍是 $(\mathbf{R}^+,\times)$ 到 $(\mathbf{R},+)$ 的同构变换，而若令

$$\varphi: x\mapsto 2^{x-1},\ x\in\mathbf{R},$$

则 φ 是 $\mathbf{R}$ 到 $\mathbf{R}^+$ 上的一一变换，但不是 $(\mathbf{R},+)$ 到 $(\mathbf{R}^+,\times)$ 的同构变换.

由以上两例可见，两个有限群同构，首先要阶数相同；两个群之间若存在同构变换，则两个群同构；两个同构的群，它们之间的一一变换，不一定都是同构变换. 关于同构变换，我们有

定理 1 设 f 是群 $(S,\circ)$ 到群 $(G,*)$ 的同构变换，e_1 和 e_2 分别为 $(S,\circ)$ 和 $(G,*)$ 的单位元素，则

(1) $f(e_1)=e_2$；

(2) $(f(a))^{-1}=f(a^{-1})$, $\forall a\in S$.

证 (1) 对于任意的 $a\in S$，有 $e_1\circ a=a\circ e_1=a$，于是 $f(e_1\circ a)=f(a\circ e_1)=f(a)$，

即 $f(e_1)*f(a)=f(a)*f(e_1)=f(a)$，因为 $f(e_1)$，$f(a)\in G$. 所以 $f(e_1)$ 为

群$(G,*)$的单位元素，故$f(e_1)=e_2$.

（2）$\forall a\in S$，有$a\circ a^{-1}=a^{-1}\circ a=e_1$，则$f(a\circ a^{-1})=f(a^{-1}\circ a)=f(e_1)=e_2$，即

$$f(a)*f(a^{-1})=f(a^{-1})*f(a)=e_2,$$

故　$(f(a))^{-1}=f(a^{-1})$.　证毕.

有了同构的概念，我们可以更好的了解循环群与变换群，这两种群在同构的意义下有着特殊的性质.

定理 2　设$(S,\circ)$是循环群，生成元为a.

（1）若a的周期为无限，则$(S,\circ)\cong(\mathbf{Z},+)$.

（2）若a的周期为n，则$(S,\circ)\cong(\mathbf{Z}_n,+)$.

这里$(\mathbf{Z},+)$表示整数加群，$(\mathbf{Z}_n,+)$表示模为n的剩余类加群.

证　（1）设a的周期为无限，则对任意$m\in\mathbf{Z}$，只要$m\neq0$，就有$a^m\neq e$. 这时，若$m_1\neq m_2$便有$a^{m_1}\neq a^{m_2}$；因若$a^{m_1}=a^{m_2}=e$，于是有$m_1-m_2=0$，即$m_1=m_2$.　令$f:a^k\mapsto k$，可证f是S到$\mathbf{Z}$上的一一变换且保持运算.

任取$x\in S$，$x=a^k$，$f(x)=k\in\mathbf{Z}$，即f是S到$\mathbf{Z}$上的一个变换.

对任意的$x,y\in S$，$x\neq y$，$x=a^{m_1}$，$y=a^{m_2}$，则$m_1\neq m_2$，故$f(x)\neq f(y)$，即f是S到$\mathbf{Z}$上的单一变换.

任取$k\in\mathbf{Z}$，则$x=a^k\in S$，且$f(x)=k$，即f是S到$\mathbf{Z}$上的变换.

再设$x,y\in S$，$x=a^{m_1}$，$y=a^{m_2}$，则$x\circ y=a^{m_1}\cdot a^{m_2}=a^{m_1+m_2}$，$f(x\circ y)=f(x)+f(y)$.

由上述可知$(S,\circ)\cong(\mathbf{Z},+)$

（2）设a的周期为n，则$a^0=e$，a，a^2，…，a^{n-1}是$(S,\circ)$中n个不同的元素；因为，若$a^i=a^j$，$0\leqslant i<j<n$，则$a^{j-i}=e$，此处$0<j-i<n$，与a的周期为n矛盾.　而$(S,\circ)$中有且仅有这n个元素，因为对任意整数m，均有整数q，r，使$m=nq+r$，$0\leqslant r<n$，而$a^m=a^{nq+r}=(a^n)^q\circ a^r=e\circ a^r=a^r$.　令$f:a^k\mapsto[k]$，$k=0,1,2,\cdots,n-1$，则$f$是$S$到$\mathbf{Z}_n$上的一一变换.　又$f(a^k\circ a^l)=f(a^{k+l})=[k+l]=[k]+[l]=f(a^k)+f(a^l)$，故知$(S,\circ)\cong(\mathbf{Z},+)$.　证毕.

这定理告诉我们循环群仅有两类，一类为有限，一类为无限.　分别称作有限循环群和无限循环群.　当需要讨论循环群的某个性质时，我们只须讨论群$(\mathbf{Z},+)$或$(\mathbf{Z}_n,+)$即可.

定理 3（凯莱（Cayley）定理）　任意群都与一个变换群同构.

证　任取$a\in S$，作变换如下

$$f_a:x\mapsto a\cdot x,\ x\in S,$$

则f_a是S上的一一变换，事实上，因$a\cdot x=b$在S中有解，故对任意的$b\in S$，存在$x\in S$使$f_a(x)=b$，即f_a是S到S上的变换. 又$x_1\neq x_2$知$a\cdot x_1\neq a\cdot x_2$，故$f_a$是$S$到$S$的单一变换. 令$G=\{f_a\mid a\in S\}$，则易证$(G,\circ)$为一个群，“$\circ$”为变换的合成. 令$\varphi: a\mapsto f_a$，当$a\neq b$时，存在$x\in S$，使$f_a(x)=a\cdot x\neq b\cdot x=f_b(x)$；即$f_a\neq f_b$，故$\varphi$是$S$到$G$上的一一变换. 又

$$\varphi(a\cdot b)=f_{a\cdot b}=f_a\circ f_b=\varphi(a)\circ\varphi(b),$$

于是知$(S,\cdot)$同构于变换群$(G,\circ)$.

(注：$f_{a\cdot b}=f_a\circ f_b$，$f_a\circ f_b(x)=f_a(f_b(x))=f_a(b\cdot x)=a\cdot(b\cdot x)=(a\cdot b)\cdot x=f_{a\cdot b}(x)$，即$f_a\circ f_b=f_{a\cdot b}$) 证毕.

二、同态

上一段，我们介绍了群的同构的概念，这是为了抽象研究不同的群是否有相同的结构引入的. 同态则是同构概念的扩张，也是研究群的重要工具.

定义2 设$(S,\circ)$和$(G,*)$是两个群，变换$f: S\to G$称为从$(S,\circ)$到$(G,*)$的一个同态变换. 如果对任意的$a, b\in S$.

$$f(a\circ b)=f(a)*f(b).$$

若此时f是S到G上的单一变换，则称f是$(S,\circ)$到$(G,*)$的单一同态；若f是S到G上的变换，则称f是$(S,\circ)$到$(G,*)$的满同态.

例3 设$(S,\circ)$，$(G,*)$是两个群，对任意$a\in S$令

$$f: a\mapsto e.$$

e是$(G,*)$的单位元素，f是S到G上的一个变换，且对任意的$a, b\in S$，有

$$f(a\circ b)=e=e*e=f(a)*f(b),$$

即f是$(S,\circ)$到$(G,*)$的同态变换，这时$f(S)=\{e\}$.

例4 设$\mathbf{R}$是实数集，$\mathbf{R}-\{0\}$为非零实数集，则$(\mathbf{R},+)$与$(\mathbf{R}-\{0\},\cdot)$均为群. 令

$$f: x\mapsto 2^x,\quad x\in\mathbf{R},$$

则f是$(\mathbf{R},+)$到$(\mathbf{R}-\{0\},\cdot)$的单一同态.

在例3中，如果$(G,*)$只有一个元素e，则f是$(S,\circ)$到$(G,*)$的满同态.

例5 设$\mathbf{R}^+$表示正实数集，$(\mathbf{R}^+,\cdot)$是一个群. 若令$f: x\mapsto 2^x$，$x\in R$，则f是$(\mathbf{R},+)$到$(\mathbf{R}-\{0\},\cdot)$的满同态，这时f也是同构变换. 若令

$$\varphi: x\mapsto 2x,\qquad x\in\mathbf{R}-\{0\},$$
$$g: x\mapsto -x,\qquad x\in\mathbf{R}-\{0\},$$

则φ与g均是$\mathbf{R}-\{0\}$到$R-\{0\}$的变换，但均不是$(R-\{0\},\cdot)$到$(R-\{0\},\cdot)$的同态变换. 事实上

$$\varphi(x_1 \cdot x_2) = 2(x_1 \cdot x_2) \neq \varphi(x_1) \cdot \varphi(x_2),$$
$$g(x_1 \cdot x_2) = -(x_1 \cdot x_2) \neq g(x_1) \cdot g(x_2).$$

由同态的定义及同构的概念可以看出，若一个变换既是单一同态，又是满同态，则它是同构变换.

同定理 1 一样有

定理 4 设 f 是群 $(S,\circ)$ 到群 $(G,*)$ 的同态变换，则 $(S,\circ)$ 的单位元素 e 的像 $f(e)$ 是 $(G,*)$ 的单位元素；$(S,\circ)$ 的元素 a 的逆 a^{-1} 的像 $f(a^{-1})$ 是 $f(a)$ 的逆，即 $[f(a)]^{-1} = f(a^{-1})$；设 $(H,\circ)$ 是 $(S,\circ)$ 的子群，$f(H) = \{f(a) \mid a \in H\}$，则 $(f(H),*)$ 是 $(G,*)$ 的子群.

此证明留作习题.

定义 3 设 f 是群 $(S,\circ)$ 到群 $(G,*)$ 的同态变换，e_1 是 $(G,*)$ 单位元素，记 $\mathrm{Ker}\, f = \{a \mid a \in S$ 且 $f(a) = e_1\}$，称 $\mathrm{Ker}\, f$ 为同态变换 f 的核，简称同态核.

定理 5 设 f 是群 $(S,\circ)$ 到群 $(G,*)$ 的同态变换，$\mathrm{Ker}\, f$ 是 f 的同态核，则 $(\mathrm{Ker}\, f,\circ)$ 是 $(S,\circ)$ 的子群.

证 由定理 4 知 $f(e) = e_1$，$e \in S$，$e_1 \in G$，设 a，$b \in \mathrm{Ker}\, f$，则

$$f(a \circ b) = f(a) * f(b) = e_1 * e_1 = e_1,$$

故

$$a \circ b \in \mathrm{Ker}\, f.$$

对任意 $a \in K$，由定理 4 知 $f(a^{-1}) = [f(a)]^{-1} = e_1^{-1} = e_1$，即 $a^{-1} \in \mathrm{Ker}\, f$. 由子群判定法知 $(\mathrm{Ker}\, f,\circ)$ 是 $(S,\circ)$ 的子群. 证毕.

下面再举两例.

例 6 设有群 $(\mathbf{Z},+)$，$(\mathbf{R}-\{0\},\cdot)$，令

$$f: n \mapsto \begin{cases} 1, & 2 \mid n, \\ -1, & 2 \nmid n, \quad n \in \mathbf{Z}, \end{cases}$$

则 f 是 $\mathbf{Z}$ 到 $\mathbf{R}-\{0\}$ 的一个变换，且对于 m，$n \in \mathbf{Z}$ 有 $f(m+n) = f(m) \cdot f(n)$，即 f 是 $(\mathbf{Z},+)$ 到 $(\mathbf{R}-\{0\},\cdot)$ 的一个同态变换. $f(\mathbf{Z}) = \{1,-1\}$，而 $(f(\mathbf{Z}),\cdot)$ 是 $(\mathbf{R}-\{0\},\cdot)$ 的子群. $\mathrm{Ker}\, f = \{x \mid x = 2n, n \in \mathbf{Z}\}$，而易证 $(\mathrm{Ker}\, f, +)$ 是 $(\mathbf{Z},+)$ 的子群.

例 7 设 $\mathbf{Q}$ 是有理数集，群 $(\mathbf{Q},+)$ 与群 $(\mathbf{Q}-\{0\},\cdot)$ 间是否存在同构变换.

解 假设有同构变换 $f: \mathbf{Q} \to \mathbf{Q}-\{0\}$；设 $0 \in \mathbf{Q}$ 在 f 作用下的像为 $\bar{a}_0$，即

$$f: 0 \mapsto \bar{a}_0.$$

对任意 $a \in \mathbf{Q}$，令 $f: a \mapsto \bar{a}$，则由假设应有

$$f(a+0) = f(a) \cdot f(0) = \bar{a} \cdot \bar{a}_0.$$

又

$$f(a+0) = f(a) = \bar{a}.$$

故

$$\bar{a}\cdot\bar{a}_0=\bar{a}.$$

这表明$\bar{a}_0$是$(\mathbf{Q}-\{0\},\cdot)$的单位元素，即$\bar{a}_0=1$，$f(0)=1$；另外，对$-1\in\mathbf{Q}-\{0\}$，设$f(b)=-1$，$b\in\mathbf{Q}$，且$b\neq0$；由于f是同构变换，所以

$$f(b+b)=f(2b)=f(b)\cdot f(b)=(-1)\cdot(-1)=1.$$

这表明$2b=0$，即$b=0$，这与$b\neq0$矛盾．故从$(\mathbf{Q},+)$到$(\mathbf{Q}-\{0\},\cdot)$无同构变换.

练习题 3－4

1. 证明群$(\mathbf{Z},+)$与群$(\mathbf{Z}_{2n},+)$同构；$\mathbf{Z}_{2n}$为偶数集.

2. 设$(G,\circ)$是一个群，而$a\in G$，对任意$x\in G$，

令

$$f(x)=a_0x\circ a^{-1}.$$

证明f是$(G,\circ)$到$(G,\circ)$上的同构变换(自身到自身的同构变换称为自同构).

3. 证明：如果f是由$(A,\circ)$到$(B,*)$的同态变换，g是由$(B,*)$到(C,Δ)的同态变换，则$g\circ f$是$(A,\circ)$到(C,Δ)的同态变换.

4. f_1，f_2是从$(A,\circ)$到$(B,*)$的同态变换，设g是从A到B的一个变换且

$$g(a)=f_1(a)*f_2(a),\ a\in A.$$

证明：如果$(B,*)$是一可换半群，则g是一个由$(A,\circ)$到$(B,*)$的同态变换.

5. 证明：循环群的同态像必是循环群.

6. $(\mathbf{R},+)$与$(\mathbf{R}-\{0\},\cdot)$是否同构.

7. 证明：同构关系是等价关系.

8. 证明群的同构像是群.

9. 证明定理 4.

第五节　陪集与商群

一、陪集

定义 1　设$(H,\circ)$是群$(S,\circ)$的子群，我们称集合

$$aH=\{a\circ h\mid h\in H\}$$

为由元素$a\in S$所确定的子群$(H,\circ)$的左陪集．元素a称为左陪集aH的代表元素．我们称集合

$$Ha=\{h\circ a\mid h\in H\}$$

为由元素$a\in S$所确定的子群$(H,\circ)$的右陪集．元素a称为右陪集Ha的代表元

素.

例 1　$(\mathbf{Q},+)$为一群($\mathbf{Q}$ 为有理数集)，$(\mathbf{Z},+)$为它的一个子群，任取有理数 a，则有 a 所确定左陪集为 $a\mathbf{Z}=\{a+k\mid k\in\mathbf{Z}\}$. 如

$$a=\frac{1}{2},\ \frac{1}{2}\mathbf{Z}=\left\{\cdots,\ \frac{1}{2}+(-n),\ \cdots,\ \frac{1}{2}+(-1),\ \frac{1}{2}+0,\ \frac{1}{2}+1,\ \cdots,\ \frac{1}{2}+n,\ \cdots\right\},$$

$$a=\frac{1}{3},\ \frac{1}{3}\mathbf{Z}=\left\{\cdots,\ \frac{1}{3}+(-n),\ \cdots,\ \frac{1}{3}+(-1),\ \frac{1}{3}+0,\ \frac{1}{3}+1,\ \cdots,\ \frac{1}{3}+n,\ \cdots\right\},$$

$$a=\frac{p}{q},\ \frac{p}{q}\mathbf{Z}=\left\{\cdots,\ \frac{p}{q}+(-n),\ \cdots,\ \frac{p}{q}+(-1),\ \frac{p}{q}+0,\ \frac{p}{q}+1,\ \cdots,\ \frac{p}{q}+n,\ \cdots\right\}.$$

(p/q 为 0 与 1 之间的既约分数). 显见若 $a_1,\ a_2\in\mathbf{Z}$，$a_2\neq a_1$，则有 $a_1\mathbf{Z}\neq a_2\mathbf{Z}$. 对于右陪集有相同的结论.

例 2　设 S 是所有二阶非奇异方阵集合，则$(S,\times)$是一个群. 令

$H=\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}-1&0\\0&-1\end{pmatrix},\begin{pmatrix}1&0\\0&-1\end{pmatrix},\begin{pmatrix}-1&0\\0&1\end{pmatrix}\right\}$，则$(H,\times)$作成$(S,\times)$的子群.

设 $A=\begin{pmatrix}2&5\\1&3\end{pmatrix}$，则 $A\in S$，于是由 A 所确定的左、右陪集分别为

$$\begin{aligned}\begin{pmatrix}2&5\\1&3\end{pmatrix}H&=\left\{\begin{pmatrix}2&5\\1&3\end{pmatrix}\times\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}2&5\\1&3\end{pmatrix}\times\begin{pmatrix}-1&0\\0&-1\end{pmatrix},\begin{pmatrix}2&5\\1&3\end{pmatrix}\times\begin{pmatrix}1&0\\0&-1\end{pmatrix},\begin{pmatrix}2&5\\1&3\end{pmatrix}\times\begin{pmatrix}-1&0\\0&1\end{pmatrix}\right\}\\&=\left\{\begin{pmatrix}2&5\\1&3\end{pmatrix},\begin{pmatrix}-2&-4\\-1&-3\end{pmatrix},\begin{pmatrix}2&-5\\1&-3\end{pmatrix},\begin{pmatrix}-2&5\\-1&3\end{pmatrix}\right\},\end{aligned}$$

$$\begin{aligned}H\begin{pmatrix}2&5\\1&3\end{pmatrix}&=\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}\times\begin{pmatrix}2&5\\1&3\end{pmatrix},\begin{pmatrix}-1&0\\0&-1\end{pmatrix}\times\begin{pmatrix}2&5\\1&3\end{pmatrix},\begin{pmatrix}1&0\\0&-1\end{pmatrix}\times\begin{pmatrix}2&5\\1&3\end{pmatrix},\begin{pmatrix}-1&0\\0&1\end{pmatrix}\times\begin{pmatrix}2&5\\1&3\end{pmatrix}\right\}\\&=\left\{\begin{pmatrix}2&5\\1&3\end{pmatrix},\begin{pmatrix}-2&-5\\-1&-3\end{pmatrix},\begin{pmatrix}2&5\\-1&-3\end{pmatrix},\begin{pmatrix}-2&-5\\1&3\end{pmatrix}\right\}.\end{aligned}$$

显见，$\begin{pmatrix}2&5\\1&3\end{pmatrix}H\neq H\begin{pmatrix}2&5\\1&3\end{pmatrix}$，在 S 中再取一个二阶方阵，同样可确定它关于子群$(H,\times)$的左、右陪集.

定理 1　**设$(H,\circ)$是群$(S,\circ)$的子群，aH 和 bH 是任意两个左陪集，则**

或 $aH=bH$ 或 $aH\cap bH=\varnothing$.

证　假设 aH 与 bH 相交，则必有一个公共元素 f，$f\in aH$ 且 $f\in bH$，于是存在 $h_1,\ h_2\in H$，使 $f=a\circ h_1=b\circ h_2$. 因此，$a=b\circ h_2\circ h_1^{-1}$，设 $x\in aH$，则存在 $h_3\in H$ 使 $x=a\circ h_3$，因而有 $x=b\circ h_2\circ h_1^{-1}\circ h_3$，又 $h_2\circ h_1^{-1}\circ h_3\in H$，故 $x\in bH$，即 $aH\subseteq bH$. 同理可有 $bH\subseteq aH$，即有 $aH=bH$，因为 aH 与 bH 都是非空集合，$aH=bH$ 与 $aH\cap bH=\varnothing$ 只能成立一个. 证毕.

定理 2 设$(H, \circ)$是群$(S, \circ)$的子群，则$(H, \circ)$的所有左陪集均具有相同的基数.

证 设$a \in S$，h_1，$h_2 \in H$. 若$h_1 \neq h_2$，则$a \circ h_1 \neq a \circ h_2$. 故$aH$中没有相同元素，而$aH$与$H$有相同基数，因此，$(H, \circ)$的所有左陪集具有相同的基数. 证毕.

由于$(H, \circ)$是$(S, \circ)$的子群，单位元素$e \in H$，故$a \in aH$，由以上两个定理可知，子群$(H, \circ)$的所有左陪集的并为集合S. 即$(H, \circ)$的左陪集集合构成S的一个划分，且这种划分中的块的大小是一样的. 如例 2 中的每块都是四个元素.

定义 2 群$(S, \circ)$关于其子群$(H, \circ)$的左(右)陪集个数，叫做$(H, \circ)$在$(S, \circ)$中的指数，用符号$[S: H]$表示.

如：在例 1 及例 2 中均有$[S: H]$为无限.

例 3 设$(S_3, \circ)$是 3 次对称群.

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

$S_3 = \{f_1, f_2, f_3, f_4, f_5, f_6\}$. 取$H = \{f_1, f_4\}$，则$(H, \circ)$是$(S, \circ)$的子群. 左陪集是：

$$f_1H = f_4H = \{f_1, f_4\},$$
$$f_2H = f_6H = \{f_2, f_6\},$$
$$f_3H = f_5H = \{f_3, f_5\},$$

$[S_3: H] = 3$，$f_1H \cup f_2H \cup f_3H = S_3$.

右陪集是：

$$Hf_1 = Hf_4 = \{f_1, f_4\},$$
$$Hf_2 = Hf_6 = \{f_2, f_6\},$$
$$Hf_3 = Hf_5 = \{f_3, f_5\}.$$

$[S_3: H] = 3$，$Hf_1 \cup Hf_2 \cup Hf_3 = S_3$.

取$H = \{f_1, f_5, f_6\}$，$(H, \circ)$为$(S_3, \circ)$的子群. 其左陪集是：

$$f_1H = f_5H = f_6H = \{f_1, f_5, f_6\},$$
$$f_2H = f_3H = f_4H = \{f_2, f_3, f_4\}.$$

其右陪集是

$$Hf_1 = Hf_5 = Hf_6 = \{f_1, f_5, f_6\},$$
$$Hf_2 = Hf_3 = Hf_4 = \{f_2, f_3, f_4\}.$$

这里$[S_3: H] = 2$，$\cup f_iH = \cup Hf_i = S_3$，且$f_iH = Hf_i$.

关于有限群$(S, \circ)$的阶数与其子群$(H, \circ)$的阶数及陪集的个数，有下面的

重要定理.

定理 3（Lagrange）　设$(S,\circ)$是有限群，$(H,\circ)$是$(S,\circ)$的子群，则

$$|S| = [S:H]\cdot|H|.$$

证　由于每一个左陪集与 H 含有相同个数的元素，而 S 共有$[S:H]$个左陪集，故 S 有$[S:H]\cdot|H|$个元素，即

$$|S| = [S:H]\cdot|H|.$$　证毕.

由定理 3 可得以下重要推论.

推论 1　有限群$(S,\circ)$中每一元素的周期都是$|S|$的因数.

证　设 $a\in S$，a 的周期为 m，令 $H=\{e,a,\cdots,a^{m-1}\}$，则$(H,\circ)$是$(S,\circ)$的(循环)子群. 由定理 3 有

$$|S| = [S:H]\cdot|H| = [S:H]m,$$

即 m 是$|S|$的因数. 证毕.

推论 2　每一个阶数为素数 P 的群$(S,\circ)$是循环群.

证明留作习题.

注意　定理 3 之逆定理并不成立，即如果$|S|=n$，m 是 n 的因数，则阶数为 m 的子群未必存在. 但对循环群来说，却是成立的.

上面的定理证明了 H 的左陪集集合是 S 的一个划分，由此划分必然可导出一个相应的等价关系，我们称它为 H 的左陪集等价关系，它使每一等价类就 H 的一个左陪集，为了定义 H 的左陪集等价关系，我们先证下面的定理.

定理 4　设$(H,\circ)$是群$(S,\circ)$的子群，于是 $b\in aH$ 的充要条件是 $a^{-1}\circ b\in H$.

证　$b\in aH$ 充要条件是存在某一 $h\in H$，使 $b=a\circ h$，即 $a^{-1}\circ b=h$. 因而 $b\in aH$ 充要条件是 $a^{-1}\circ b=h\in H$. 证毕.

由此定理可知，H 的左陪集等价关系 ~ 可定义如下：

$$a\sim b\quad \text{充要条件是}\ a^{-1}\circ b\in H.$$

即是说同在一个左陪集中的元素必然有 ~ 关系；反之，具有 ~ 关系的元素，必在同一个左陪集中. 另外，也可直接验证 ~ 具有自反性、对称性和传递性，因此 ~ 是一等价关系. 事实上

(1) $a^{-1}\circ a\in H$，所以 $a\sim a$，$a\in S$；

(2) $a\sim b$，则 $a^{-1}\circ b\in H$，$b^{-1}\circ a=(a^{-1}\circ b)^{-1}\in H$，故 $b\sim a$.

(3) $a\sim b$，$b\sim c$，则 $a^{-1}\circ b\in H$，$b^{-1}\circ c\in H$，

$$a^{-1}\circ c=a^{-1}\circ(b\circ b^{-1})\circ c=(a^{-1}\circ b)\circ(b^{-1}\circ c)\in H，\text{故 } a\sim c.$$

本段的中心意思是说：子群$(H,\circ)$可以诱导出 b 由 H 的左陪集构成 S 的一个划分和由这个划分可以诱导出 S 的一个左陪集等价关系. 以上关于左陪集的一些理论都可推广到右陪集上去，也容易得知左陪集集合与右陪集集合是一一对应的.

二、商群

上一段我们介绍了陪集的一般理论，对于群$(S,\circ)$的任意子群$(H,\circ)$，由例2及例3可知，左陪集aH未必等于右陪集Ha，对于特殊的子群，有可能其左陪集等于其右陪集，即$aH=Ha$，$a\in S$.

定义3 设$(H,\circ)$是群$(S,\circ)$的一个子群，如果对任意的$a\in S$都有

$$aH=Ha,$$

则称$(H,\circ)$是$(S,\circ)$的一个正规子群.

如例1中的$(\mathbf{Z},+)$是$(\mathbf{Q},+)$的正规子群. 例3中的$(\{f_1,f_5,f_6\},\circ)$是$(S_2,\circ)$的正规子群；而$(\{f_1,f_4\},\circ)$是$(S_3,\circ)$的子群，但不是正规子群，例2中的$(H,\times)$不是$(S,\times)$的正规子群.

例4 设$(S,\circ)$是可换群，则$(S,\circ)$的任意子群都是正规子群. 因

$$aH=\{a\circ h\mid h\in H\}=\{h\circ a\mid h\in H\}=Ha.$$

如，$(\mathbf{Q}-\{0\},\times)$非零有理数关于数目乘法组成的群，取$H=\{1,-1\}$，则$(H,\times)$是$(\mathbf{Q}-\{0\},\times)$的正规子群.

设$(S,\circ)$是一个群，$(H,\circ)$是$(S,\circ)$的正规子群. 我们对$(H,\circ)$的全体陪集所成集合规定一个结合法. 为此，先介绍S的两个非空子集的乘积.

设A，B是S的两个非空子集，我们把集合$\{a\circ b\mid a\in A,b\in B\}$叫做$A$，$B$的积，记为$A\cdot B$. 于是可证$(A\cdot B)\cdot C=A\cdot(B\cdot C)$，即集合的积适合结合律. 这样一来可知，$\rho(S)-\{\varnothing\}$关于集合的积是一个半群，且有单位元素$\{e\}$，$e$是$(S,\circ)$的单位元素. 需要指出的是我们可令$A^{-1}=\{a^{-1}\mid a\in A\}$，但一般来说，$A\cdot A^{-1}\neq\{e\}$，因此当$A$不止含有一个元素时，$A\cdot A^{-1}=\{a\circ b^{-1}\mid a,b\in A\}$，除了含有$e$以外，还有其他元素.

定理5 设$(H,\circ)$是群$(S,\circ)$的一个正规子群，S/H表示$(H,\circ)$的所有陪集作成的集合，则S/H关于上面规定的集合乘积“·”组成一个群.

证 设aH，$bH\in S/H$，若$aH=xH$，$bH=yH$则有$aH\cdot bH=xH\cdot yH$，任取a，b，x，$y\in S$，则有$aH=xH$且$bH=yH$，那么存在n_1，n_2

$$(a=x\circ n_1\text{ 且 }b=y\circ n_2)\Rightarrow(a\circ b)H=(x\circ n_1)\circ(y\circ n_2)H$$
$$=(n_1\circ n_2'\circ x\circ y)H\Rightarrow(a\circ b)H=(x\circ y)H\Rightarrow aH\cdot bH=xH\cdot yH.$$

显然S/H关于·运算是封闭的.

$\forall a,b,c\in S.\quad ((aH)(bH))\cdot cH$

$$=(a\circ b)H\cdot cH=((a\circ b)\cdot c)H=(a\circ b\circ c)H$$
$$aH\cdot(bH\cdot cH)=aH\cdot(b\circ c)H=a\circ(b\circ c)H=(a\circ b\circ c)H$$

所以有$(aH\cdot bH)\cdot cH=aH\cdot(bH\cdot cH)$.

故·运算是可结合的.

$aH\cdot eH=(a\circ e)H=aH$，故 eH 是 $(S/H,\cdot)$ 的单位元素. aH 的逆元素为 $a^{-1}H$，从而 $(S/H,\cdot)$ 作成一个群. 证毕.

定义 4 群 $(S,\circ)$ 关于其正规子群 $(H,\circ)$ 的陪集作成的群 $(S/H,\cdot)$ 叫做 $(S,\circ)$ 关于 $(H,\circ)$ 的商群.

如，在例 1 中 $(\mathbf{Z},+)$ 是 $(\mathbf{Q},+)$ 的一个正规子群，$\mathbf{Q}/\mathbf{Z}=\{a\mathbf{Z}\mid a\in\mathbf{Q}\}$，$(\mathbf{Q}/\mathbf{Z},\cdot)$ 为商群，结合法为：$a\mathbf{Z}\cdot b\mathbf{Z}=(a+b)\mathbf{Z}$，$\mathbf{Z}$ 是单位元素，$a\mathbf{Z}$ 的逆元素为 $(-a)\mathbf{Z}$. 在例 4 中 $(H,\times)$ 是 $(\mathbf{Q}-\{0\},\times)$ 的正规子群. 由于 $aH=-aH$；故 $[\mathbf{Q}-\{0\}]/H=\{aH\mid a>0\}$，其上的结合法为：$aH\cdot bH=(a\circ b)\cdot H$，单位元素为 H，aH 的逆元素为 $a^{-1}H$.

判断正规子群，除定义外还有如下的方法.

定理 6 设 $(H,\circ)$ 是 $(S,\circ)$ 的子群，则下面四个条件是等价的：

(1) $(H,\circ)$ 是 $(S,\circ)$ 的正规子群；

(2) $aHa^{-1}=H$，$a\in H$；

(3) $aHa^{-1}\subseteq H$，$a\in S$；

(4) $aha^{-1}\in H$，$a\in S$，$h\in H$.

证 按下面途径 (1)(2)(3)(4)(1) 从而四个条件等价.

(1) $\Rightarrow$(2)，因 $(H,\circ)$ 是正规子群，故对任意的 $a\in S$，有 $aH=Ha$，于是 $aHa^{-1}=(aH)a^{-1}=(Ha)a^{-1}=H(a\circ a^{-1})=He=H$，即 (2) 成立.

(2) $\Rightarrow$(3)，对任意的 $a\in S$，$aHa^{-1}=H$，故 $aHa^{-1}\subseteq H$.

(3) $\Rightarrow$(4)，由于 $aHa^{-1}\subseteq H$，故对任意的 $a\in S$，$h\in H$，有 $aha^{-1}\in H$.

(4) $\Rightarrow$(1)，设 $aha^{-1}\in H$，则对任意的 h，存在 $h_1\in H$，使 $aha^{-1}=h_1$，即 $ah=h_1a$，也就是 $aH\subseteq Ha$. 另一方面，任取 $ha\in Ha$，则 $a^{-1}ha\in H$，存在 $h_2\in H$，使 $a^{-1}ha=h_2$，即 $h\circ a=a\circ h_2$，也即 $ah\in aH$，$Ha\subseteq aH$. 所以，对任意 $a\in S$，有

$$aH=Ha,$$

从而 $(H,\circ)$ 是群 $(S,\circ)$ 的正规子群. 证毕.

例 5 设 $(H,\circ)$ 是群 $(S,\circ)$ 的一个子群，且 $(H,\circ)$ 的任意两个左陪集的乘积仍是一个左陪集，则 $(H,\circ)$ 是 $(S,\circ)$ 的一个正规子群.

证 先证 $aH\cdot bH=(a\circ b)H$. 由已知，$aH\cdot bH$ 是一个左陪集，设为 cH，但 $a\circ b=a\circ e\circ b\circ e\in aH\cdot bH$，故 $a\circ b\in cH$，即 $cH=(a\circ b)H$.

任取 $h\in H$，则 $a\circ h\circ a^{-1}\circ b\in aH\cdot a^{-1}H=(a\circ a^{-1})H=H$，于是 $a\circ h\circ a^{-1}\in H$，对任意的 $a\in S$，即 $(H,\circ)$ 是群 $(S,\circ)$ 的正规子群.

练习题 3－5

1. 设 $(H,\circ)$ 是群 $(S,\circ)$ 的子群，a，$b\in S$. 证明以下 6 个条件是等价的.

(1) $b^{-1}\circ a\in H$; (2) $a^{-1}\circ b\in H$;

(3) $b\in aH$; (4) $a\in bH$;

(5) $aH=bH$; (6) $aH\cap bH\neq\varnothing$.

2. $G=(\mathbf{Z},+)$为整数加群，$H=\{3k\mid k\in\mathbf{Z}\}$，商群$(G/H,\cdot)$中含有哪些元素？单位元素是什么？“·”是怎么样.

3. 设S含有8个元素：

$$\pm\begin{pmatrix}1&0\\0&1\end{pmatrix},\ \pm\begin{pmatrix}\mathrm{i}&0\\0&-\mathrm{i}\end{pmatrix},\ \pm\begin{pmatrix}0&1\\-1&0\end{pmatrix},\ \pm\begin{pmatrix}0&\mathrm{i}\\\mathrm{i}&0\end{pmatrix},\ (\mathrm{i}^2=-1).$$

证明，S关于矩阵乘法作成一个群，且它的每一子群都是正规子群.

4. 举例说明定理3的逆定理不真，证明对于循环群，定理3的逆定理成立.

5. 证明定理3的推论2.

6. 设$(H,\circ)$是群$(K,\circ)$的子群，$(K,\circ)$是群$(S,\circ)$的子群，证明

$$[S:H]=[S:K]\cdot[K:H].$$

第六节 环与域简介

以上几节我们研究了关于群的一般理论. 群是具有一个二元运算的代数系统. 对于两个代数系统$(T,+)$和$(T,*)$，可以将它们组合成一个具有两个二元运算的代数系统$(T.tif,+,*)$，我们关心的是两个二元运算“+”和“$*$”之间有联系的代数系统$(T.tif,+,*)$.

常称“+”为“加法”；称“$*$”为“乘法”.

例如：具有乘法和加法这两个二元运算的实数系统$(\mathbf{R}.tif,+,\times)$是我们所熟知的代数系统. 对任意的$a,b,c\in\mathbf{R}$，都有

$$a\times(b+c)=(a\times b)+(a\times c),\ \text{以及}\ (b+c)\times a=(b\times a)+(c\times a).$$

这种联系就是乘法运算对于加法运算是可分配的，为此我们有定义1.

定义1 一个代数系统$(T.tif,+,*)$，如果它的两个二元运算满足下列条件：

(1) $(T,+)$是一个可换群；

(2) $(T,*)$是一个半群；

(3) 运算“$*$”对“+”满足分配律：

$$a*(b+c)=(a*b)+(a*c);$$
$$(b+c)*a=(b*a)+(c*a).$$

其中$a,b,c\in\mathbf{R}$，则称$(T.tif,+,*)$为环.

注意：环中之运算“+”及“$*$”仅仅表示某二种运算，它的含义不限于初等数学中的数的“加”与“乘”运算.

例 1 设 $K=\{e,a,b,c\}$，在 K 上定义两个二元运算，如表 3－15 和表 3－16：

表 3－15

+	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

表 3－16

*	e	a	b	c
e	e	e	e	e
a	e	a	e	a
b	e	b	e	b
c	e	c	e	c

则 $(K.\ tif,+,*)$ 是一个环.

证 易证 $(K,+)$ 是一个可换群.

接下来我们首先证 $(K,*)$ 是半群.

由表 3－16 知，对于任意的 $x\in K$，都有 $x*e=e*x=e$；a 和 c 都是关于运算"$*$"的右单位元素；对于任意的 $x\in K$ 都有 $x*b=e$.

对于 x，y，$z\in K$，可以证明必有 $(x*y)*z=x*(y*z)$，这是因为

如果 $z=e$ 或 $z=b$，则 $(x*y)*z=e=x*(y*z)$.

如果 $z=a$ 或 $z=c$，则 $(x*y)*z=x*y=x*(y*z)$，即 $(K,*)$ 是半群.

下面证明"$*$"关于"$+$"是可分配的.

先看等式 $(y+z)*x=(y*x)+(z*x)$.

如果 $x=e$ 或 $x=b$，则 $(y+z)*x=e=e+e=(y*x)+(z*x)$.

如果 $x=a$ 或 $x=c$，则 $(y+z)*x=y+z=(y*x)+(z*x)$.

其次看等式 $x*(y+z)=(x*y)+(x*z)$.

如果 $y=z$，则 $y+z=e$，于是

$$x*(y+z)=x*e=e=(x*y)+(x*y)=(x*y)+(x*z).$$

如果 y 与 z 中有一个等于 e，则等式 $x*(y+z)=(x*y)+(x*z)$.

如果 y 与 z 均不等于 e，且 $y\neq z$，则有以下三种情况.

(1) $x*(a+b)=x$ 且 $(x*a)+(x*b)=x+e=x$；

(2) $x*(a+c)=x*b=e$ 且 $(x*a)+(x*c)=x+x=e$；

(3) $x*(b+c)=x*a=x$ 且$(x*b)+(x*c)=e+x=x$.

所以，在代数系统$(K. tif, +, *)$中运算“ $*$ ”对于运算“ $+$ ”是可分配的，因此$(K. tif, +, *)$是一个环.　证毕.

定义 2　设$(T. tif, +, *)$是一个环，如果$(T, *)$中无零因子，即对任意的 a，$b\in T$，$a\neq 0$，$b\neq 0$，必有 $a*b\neq 0$，则称$(T. tif, +, *)$为无零因子环.

如果$(T, *)$是可交换的，称$(T. tif, +, *)$是可交换环.

如果$(T, *)$是有单位元素，称$(T. tif, +, *)$是含单位元环.

如果$(T. tif, +, *)$是可交换的，含单位元素而无零因子环，则称它是整环.

例如：$(\mathbf{Z}. tif, +, \cdot)$是整环.　因“ $\cdot$ ”可交换，1 是乘法单位元素，且无零因子.

定义 3　设$(T. tif, +, *)$是一个代数系统，如果它满足：

(1) $(T, +)$是可换群；

(2) $(T-\{0\}, *)$是可换群；

(3) 运算“ $*$ ”对于运算“ $+$ ”是可分配的，则称$(T. tif, +, *)$是域.

例如　$(\mathbf{Q}. tif, +, \cdot)$，$(\mathbf{R}. tif, +, \cdot)$，$(\mathbf{C}. tif, +, \cdot)$都是域，这是 **Q** 为有理数集，**R** 为实数集，**C** 为复数集；上面的域分别称为有理数域，实数域，复数域.

注意　$(\mathbf{Z}. tif, +, \cdot)$是整环，但不是域，因为$(\mathbf{Z}-\{0\}, *)$不是群，即整环不一定是域.

这一点也说明了有理数域是最小数域.

关于环，整环，域的例子很多，且还有子环，理想等概念，这里我们就不一一介绍了.

练习题 3－6

1. 环$(T. tif, +, *)$是无零的，当且仅当$(T. tif, +, *)$满足消去律.

2. 设$(T. tif, +, *)$是一个代数系统，其中“ $+$ ”，“ $*$ ”为普通的数的加法与乘法，T 为下列集合：

(1) $T=\{x\mid x=2n, n\in \mathbf{Z}\}$；

(2) $T=\{x\mid x=2n+1, n\in \mathbf{Z}\}$；

(3) $T=\{x\mid x\geqslant 0$, 且 $x\in \mathbf{Z}\}$；

(4) $T=\{x\mid x=a+45b, a, b\in \mathbf{R}\}$；

(5) $T=\{x\mid x=a+3b, a, b\in \mathbf{R}\}$.

问$(T. tif, +, *)$是整环吗？为什么？

3. 设$(T. tif, +, *)$为一个代数系统，其中“ $+$ ”，“ $*$ ”为普通的数的加法与乘法，且

(1) $T=\{x \mid x\geqslant 0, x\in \mathbf{Z}\}$；

(2) $T=\{x \mid x=a+3b, a, b\in \mathbf{Q}\}$；

(3) $T=\{x \mid x=a+3\sqrt{5}b, a, b\in \mathbf{Q}\}$，$\mathbf{Q}$ 为有理数集；

(4) $T=\{x \mid x=a+\sqrt{5}b, a, b\in \mathbf{Q}\}$，$\mathbf{Z}^{+}$ 为正整数集合；

(5) $T=\left\{x \mid x=\frac{a}{b}, a, b\in \mathbf{Z}^{+}, \text{且 } a\neq k*b\right\}$.

问$(T.\ tif, +, *)$是域否？为什么？

复 习 题 三

1. 设$(G,\circ)$是一个群，$u\in G$，在 G 中规定结合法“ $*$ ”

$$a*b=a\circ u^{-1}\circ b \quad a, b\in G.$$

证明$(G,*)$是一个群.

2. 证明任何阶数分别为 1，2，3，4 的群都是可换群，并举一个 6 阶群它不是可换群.

3. 设$(S,\circ)$是一个群，证明：如果对任意的 a，$b\in S$ 都有

$a^3\circ b^3=(a\circ b)^3$，$a^4\circ b^4=(a\circ b)^4$ 和 $a^5\circ b^5=(a\circ b)^5$，则$(S,\circ)$是一个交换群.

4. 设$(S,\circ)$是一个半群，对于 x，$y\in S$，如果 $a\circ x=b\circ y$，便有 $x=y$，则称元素 S 是左可约的，试证，如果 a 和 b 是左可约的，则 $a\circ b$ 也是左可约的.

5. 具有关系 $i^2=j^2=k^2=-1$，$(-1)^2=1$，$i\circ j=k=-j\circ i$，$i\circ k=i=-k\circ j$，$k\circ i=j-i\circ k$ 的 8 元素集合，$G=\{1, -1, i, -i, j, -j, k, -k\}$ 可构成群$(G,\circ)$.

(1) 列出群的运算表.

(2) 证明$(H,\circ)$是不变子群，这里 $H=\{1, -1, j, -j\}$.

(3) 写出关于$(H,\circ)$的陪集划分.

(4) 写出 G/H.

6. 证明群中只有单位元素是幂等的.

7. 证明，在由群$(S,\circ)$的一个子群$(H,\circ)$所确定的陪集中，只有一个陪集是一子群.

8. 设$(G,\circ)$是一个任一群，定义 $R\subseteq G\times G$ 为

$$R=\{(x,y) \mid \text{存在 } a\in G \text{ 使 } y=a\circ x\circ a^{-1}\}.$$

验证 R 是 G 上的等价关系.

9. 设$(H,\circ)$是$(S,\circ)$的子群，证明 $H=Ha$ 当且仅当 $a\in H$.

10. 证明：有限群的任意分群的右陪集个数等于左陪集个数(提示 利用对应 $x\longmapsto x^{-1}$).

11. 设 f_1，f_2 都是从代数系统$(A,\circ)$到代数系统$(B,*)$的同态，设 g 是从 A 到 B 的一个变换，使得对任意的 $a\in A$，都有

$$g(a)=f_1(a)*f_2(a).$$

证明：如果$(B,*)$是一个可换半群，则 g 是由$(A,\circ)$到$(B,\circ)$的同态.

12. 设 φ 是由群$(S,\circ)$到群$(G,*)$的同态，e 是$(S,\circ)$的单位元素，证明 $\varphi(e)$是$(G,*)$的单位元素；$[\varphi(a)]^{-1}=\varphi(a^{-1})$ $a\in S$.

13. $(S_4,\circ)$为 4 次对称群，设

$$\alpha=\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix},\quad \beta=\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}$$

求：(1) $\alpha\circ\beta$，$\beta\circ\alpha$，α^2 及 α^{-1}.

(2) α，β 及 $\alpha\circ\beta$ 的阶.

14. 已知一个环($\{a,b,c,d\}$. tif，+，*)，它的运算由表 3－17，3－18 给出：

表 3－17

+	a	b	c	d
a	a	b	b	d
b	b	c	d	a
c	c	d	a	d
d	d	a	b	c

表 3－18

*	a	b	c	d
a	a	a	a	a
b	a	c	a	a
c	a	a	a	a
d	a	c	a	c

它是一个交换环吗？它有乘法单位元素吗？这个环中的零元素是什么？并求出每个元素的加法逆元.

15. 证明($\{0,1\}$. tif，+，*)是一个整环，其中运算“+”和 * 由表 3－19，3－20 定义.

表 3－19

+	0	1
0	1	1
1	1	0

表 3－20

*	0	1
0	0	0
1	0	1

第四章　图　论

图论是数学的一个重要分支. 起源于 18 世纪,它在近代科学,尤其是在计算机科学的研究中起着重要的作用. 而且这门学科自成体系,研究的问题相当广泛,如著名的四色猜想(地图着色)问题便是其中之一. 由于篇幅所限，这里我们只能介绍一些基本内容.

第一节　图的基本概念

我们这里要介绍的图与高等数学中所讨论的图是完全不一样的，那里研究的是点与点之间构成的图形的形状和位置性质，诸如：连续、间断、极值、可导等等. 而我们这里研究的是点与点之间的联系(能否联结)与形是无关的. 如：以点表示一些工厂，以联结两点的连线表示两工厂间有业务往来. 对于这种图形，我们感兴趣的是有多少点和哪些点之间有线连接，至于连线的长短，曲直和点的位置却是无关紧要的.

定义 1　图 G 是由非空点集 $V=\{v_1,v_2,\cdots,v_n\}$(结点集)，以及非空线集 $E=\{l_1,l_2,\cdots,l_m\}$(边集)所组成. 其中每条边可用一个结点对表示之. 亦即

$l_i=(v_{i_1},v_{i_2})\quad(i=1,2,\cdots,m)$.

图 G 可用 $G=\langle V,E\rangle$ 表示.

一个图可以用一个图形表示.

例 1　设 $G=\langle V,E\rangle$，其中 $V=\{a,b,c,d\}$，$E=\{l_1,l_2,l_3,l_4,l_5,l_6,l_7\}$，$l_1=(a,b)$，$l_2=(a,c)$，$l_3=(b,d)$，$l_4=(b,c)$，$l_5=(d,c)$，$l_6=(a,d)$，$l_7=(b,b)$，则图 G 可用图 4－1(a)或(b)表示

定义中的结点对可以是有序的，也可以是无序的. 若边所对应的结点对(a,b)是有序的，则称 l 是有向边. a 称为 l 的起点，b 成为 l 的终点. 若边 l 所对应的结点对(a,b)是无序的，则称 l 是无向边. 图中所有边均是有向边的图称为有向图，如图 4－2；图中所有边均是无向边的图称为无向图，如图 4－1；既不是有向图也不是无向图，则称为混合图. 我们仅讨论有向图和无向图，

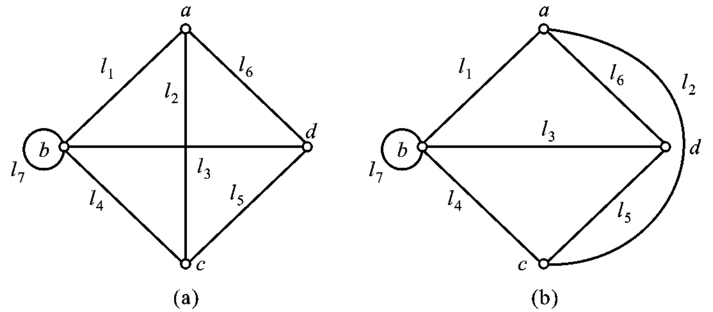


图 4－1

且 V 和 E 限于有限集合.

对于图中的边 $l=(a,b)$ 不管 l 如何(有向或无向)，称边 l 与结点 a 与 b 相关联，而 a 与 b 称为邻接的. 若干条边关联于同一结点，则这些边称为邻接的，如图 4－3. 一条边若与两个相同的 a 结点相关联，则称其为环，即环具有 (a,a) 状之边，如图 4－1 中的边 l_7，图 4－2 中的边 (e,e) 即为环. 不与任何结点相邻之结点称为孤立点，如图 4－2 中的点 f.

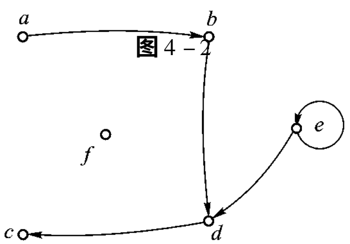


图 4－2

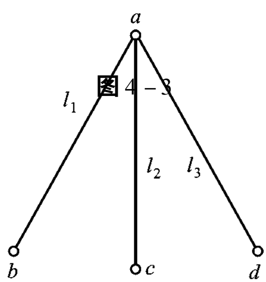


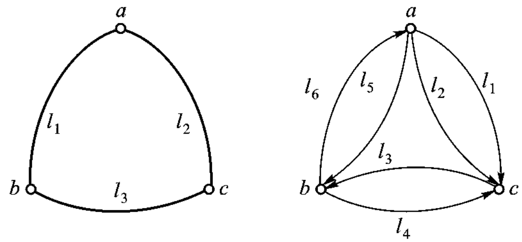
图 4－3

图 4－3 中 l_1，l_2，l_3 关联于结点 a，即 l_1，l_2，l_3 为邻接的.

在无向图中，一般一个无序结点对只对应一条边；在有向图中，一般一个有序结点对也只对应一条边. (注:方向相反之两条边可看成是由两个不同的结点对应之,如 (a,b) 与 (b,a) 不同).

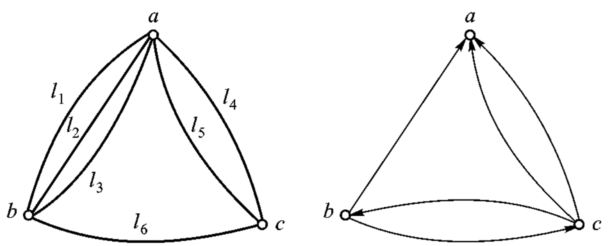
有时一个结点对对应若干条边，这种边称为多重边；包括多重边的图称为多重图；既不含多重边，也不含环的图称为简单图. 图 4－4(a) 是简单图，图 4－5 是多重图.

有时在一个图中边的旁侧加一些数字以刻画某些特征，叫做边的权. 这样的边叫有权边；每边都是有权边的图叫做有权图，亦称赋权图如图 4－6. 而



(a)　　(b)

图 4 – 4



(a)　　(b)

图 4 – 5

无有权边的图叫无权图.

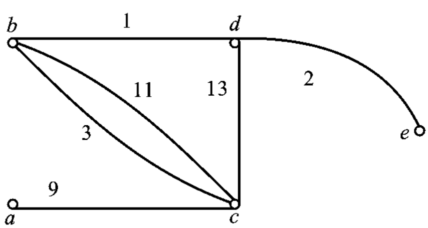


图 4 – 6

定义 2　在有向图中的结点 v，**以** v **为起点的边的条数称为结点** v **的引出次数，记为** $\overleftarrow{\deg}(v)$；**以** v **为终点的边的条数称为** v **的引入次数，记为** $\overrightarrow{\deg}(v)$；v **的引出次数与引入次数之和称为结点** v **的次数，记为** $\deg(v)$.

在无向图中以 v **作为边的端点次数之和称为** v **的次数**. **也记为** $\deg(v)$. **孤立结点的次数为零**.

显见，任一图的所有结点的次数之和必为偶数，且必为图中边数的两倍. **因每条边必与两个结点相关联**. **为了方便，以后把具有** n **个结点和** m **条边的**

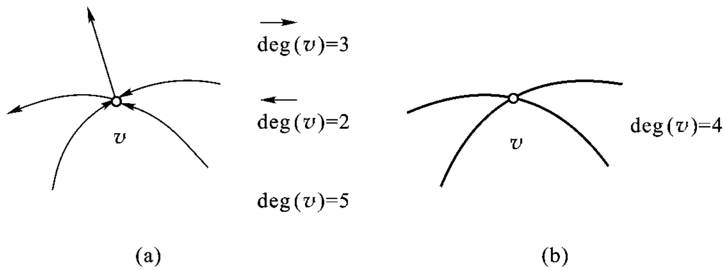


图 4－7

图称为(n,m)图.

定理 1　设 $G=\langle V,E\rangle$是一个(n,m)图，其中，$V=\{v_1,v_2,\cdots,v_n\}$，则

$$\sum_{i=1}^{n}\deg(v_i)=2m.$$

证　因为每条边有两个次数，故 m 条边就有 $2m$ 个次数，即上式成立. 证毕. 在有向图中，上式也可以写成

$$\sum_{i=1}^{n}\overleftarrow{\deg}(v_i)+\sum_{i=1}^{n}\overrightarrow{\deg}(v_i)=2m.$$

定理 2　在一个图中，次数为奇数的结点必为偶数个.

证　设次数为偶数的结点有 n_1 个，记为 $v_{E_i}(i=1,2,\cdots,n_1)$. 次数为奇数的结点有 n_2 个，记为 $v_{F_i}(i=1,2,\cdots,n_2)$，由定理 1 得

$$2m=\sum_{i=1}^{n}\deg(v_i)=\sum_{i=1}^{n}\deg(v_{E_i})+\sum_{i=1}^{n}\deg(v_{F_i})$$

因为次数为偶数的各结点次数之和为偶数，故$\sum\limits_{i=1}^{n}\deg(v_{E_i})$是偶数.若 n_2 是奇数，则$\sum\limits_{i=1}^{n}\deg(v_{F_i})$为奇数，于是$\sum\limits_{i=1}^{n}\deg(v_i)$是奇数，这是矛盾的，故 n_2 必为偶数. 证毕.

在 n 阶无向简单图 G 中，如果每个结点的次数都是 d，称图 G 为 d 次正则图.

定义 3　设有图 $G=\langle V,E\rangle$，$G'=\langle V',E'\rangle$，若有 $V\supseteq V'$及 $E\supseteq E'$；则称 G' 是 G 的子图. 若在图 G，G'中有 $V=V'$，$E\supseteq E'$，则称 G'是 G 的生成子图.

如图 4－9 中，(b)，(c)是(a)的子图，也是真子图，且(c)是(a)的生成子图.

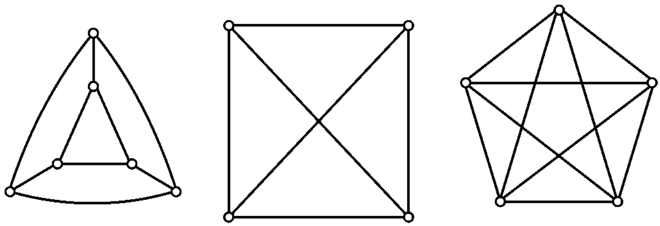


图 4－8

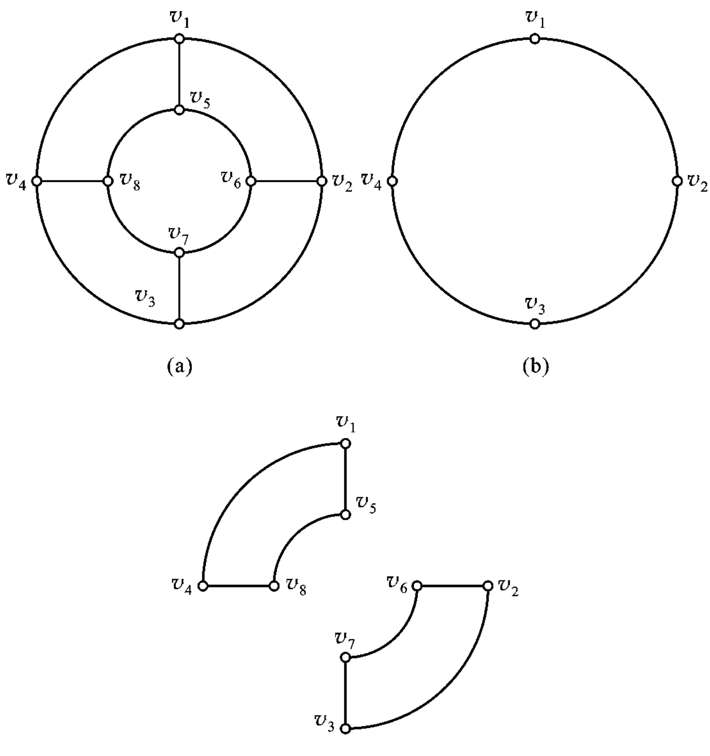
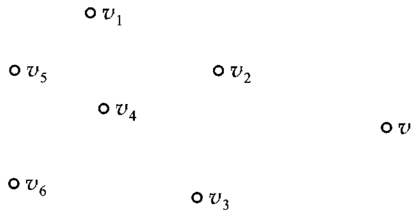


图 4－9

如果图 G 是一个(n,0)图，则称此图为零图，即零图是由一些孤立点所组成. 如果图 G 是一个(1,0)图，则称此零图为平凡图.

图 4－10



(a) 零图　　　　(b) 平凡图

对于无向简单图 $G=(n,m)$，如果 G 中每个结点均与其余 $n-1$ 个结点邻接，这样的图称为完全图，记为 $K_n(n\geqslant 1)$. 此时 $m=\dfrac{n(n-1)}{2}$，如图 4-11 所示.

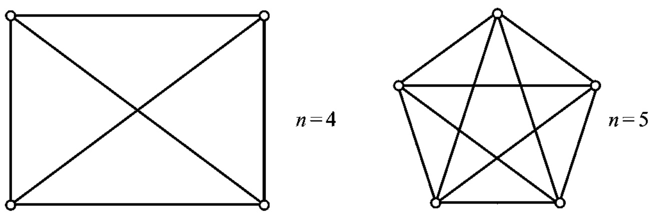


图 4-11　完全图

定义 4　设有两个无向简单图 $G'=\langle V,E'\rangle$ 与 $G=\langle V,E\rangle$，若图 $\overline{G}=\langle V,E\cup E'\rangle$ 是完全图，且 $E\cap E'=\varnothing$，则称 G' 是 G 的补图.

由定义 4 可见 G 也是 G' 的补图. 即二者互为补图. 一个图的补图的补图是其本身.

图 4-12 的(a)与(b)是互为补图. (c)与(d)是互为补图.

一个图的图形，比较形象的反映了图中结点与边间的相互关系. 对于图形，我们只注重结点与边的相互关系而不注重它的几何外观. 一个图可以有多个图形. 图 4-13 表示一个图的四个图形.

定义 5　设有图 $G=\langle V,E\rangle$ 与 $G'=\langle V',E'\rangle$，如果存在一一对应映射 $g: v_i\to v_i'$ 且 $l=(v_i,v_j)$（或 $\langle v_i,v_j\rangle$）是 G 的一条边，当且仅当 $l'=(g(v_i),g(v_j))$（或 $\langle g(v_i),g(v_j)\rangle$）是 G' 的一条边，则称 G 与 G' 同构.

应当注意：定义 5 中的 $\langle v_i,v_j\rangle$ 是以结点 v_i 为起点，v_j 为终点的一条有向边；$\langle g(v_i),g(v_j)\rangle$ 是以 $g(v_i)$ 为起点，$g(v_j)$ 为终点的一条有向边.

如图 4-12，(a)与(b)同构，图 4-13 中的四个图是同构的.

图 4-14 所示的两个图是同构的. 因为 $v_i\leftrightarrow a_i(i=1,2,3,4,5,6)$ 可使 $(v_i,v_j)\leftrightarrow(a_i,a_j)$.

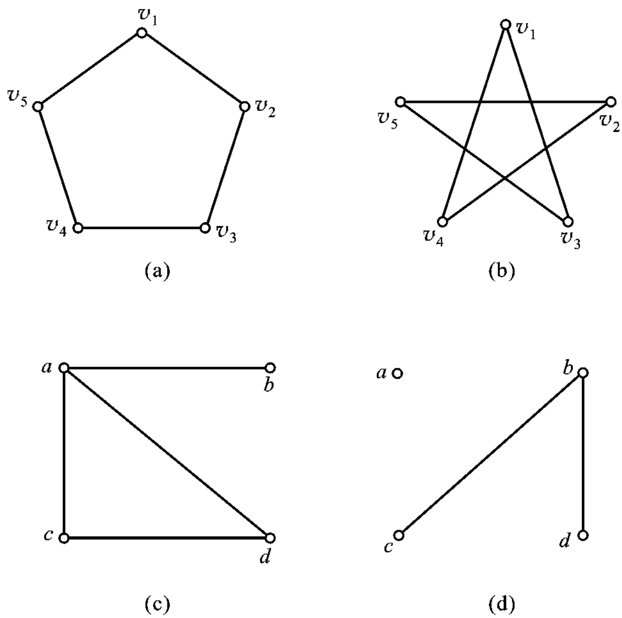


图 4－12

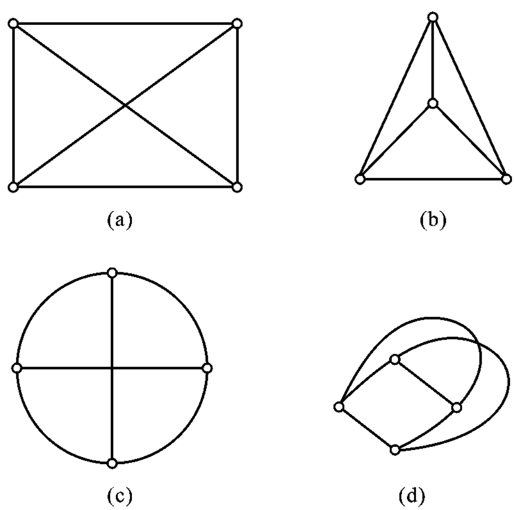


图 4－13

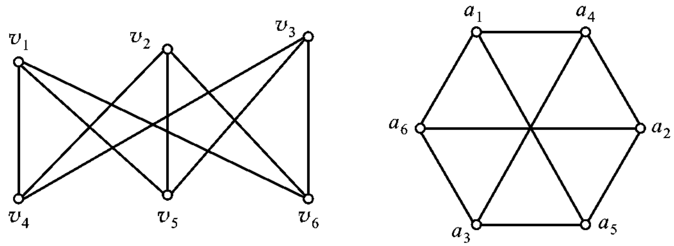


图 4－14

两个图同构的必要条件是

1. **结点数相同；**
2. **边数相等；**
3. **次数相同的结点数相等.**

但它不是充分条件.

例 2　图 4－15 **的两个图，虽然满足以上三个条件，但不同构.**（a）**中的** x **应与**（b）**中的** y **对应，因为次数都是** 3，**但**（a）**中的** x **与两个次数为** 1 **的结点** u，v **邻接，而**（b）**中的** y **仅与一个次数为** 1 **的结点** w **相邻接.**

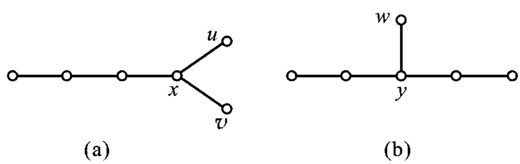


图 4－15

练习题 4－1

1. **证明在任何有向图中，所有结点引入次数之和等于所有结点的引出次数之和.**

图 4－16

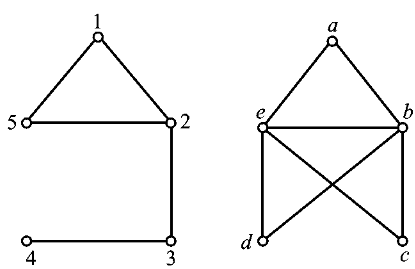
2. **证明在任何有向完全图中，所有结点引入次数平方之和，等于所有结点引出次数平方之和.**

3. **证明，在** n **个结点的无向完全图中共有** $n(n-1)/2$ **条边.**

4. **画出无向完全图** K_4 **的所有非同构的子图，指出哪些是生成子图，哪些是自补图.**

5. **画六个结点的完全图，并举出其中互补的图.**

6. **下列各对图**（图 4－16，图 4－17，图 4－18）**同构吗？找出对应关系.**



7. 一个图如果同构于它的补图，则这个图称为自互补图.

（1）画出具有四个结点的自互补图.

（2）存在三个结点和六个结点的自互补图吗？

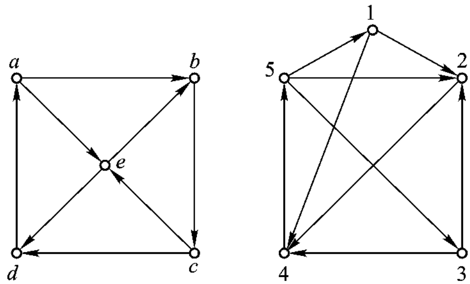


图 4－17

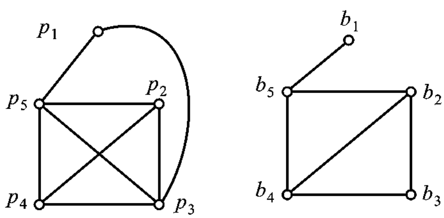


图 4－18

（3）证明一个自互补图必有 $4k$ 或 $4k+1$ 个结点.

第二节　路径与回路

立陶宛的哥尼斯堡城（Konigsberg）位于普雷格尔（Pregel）河畔，河中有两个岛，城市的各部分由七座桥接通，如图 4－19（a）.

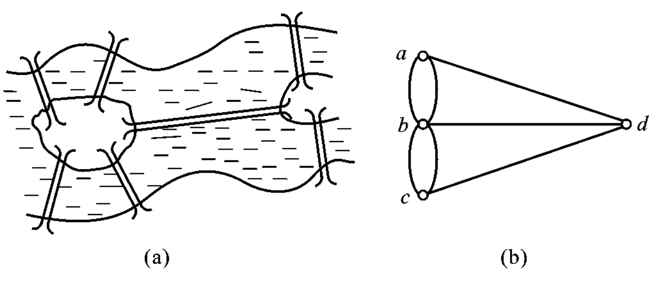


图 4－19　七桥问题

古时城中居民热衷于这样一个问题：游人从任一地点出发，怎样才能做到穿过每座桥一次且仅一次后又返回原出发地．这便是著名的七桥问题．1736 年，欧拉(Euler)研究了这个问题，他用四个点代表四块陆地，联结各地点的边表示桥，这样得到一个抽象的图形，如图 4－19(b)．于是上面问题就转变成为：从图 4－19(b)中任一点出发，通过每条边一次而返回原点之回路是否存在？为说明这个问题我们介绍下面的

一、路径与回路

定义 1 在有向图中，路径是一条边的序列$(l_{i_1},l_{i_2},\cdots,l_{i_k})$，其中 l_{i_j} 的终点与 $l_{i_{j+1}}$ 的起点一致．如果序列中同一条边不出现两次，则称此路径是简单路径．如果同一点不碰到两次，则称此路径是基本路径．如果路径中的边 l_{i_k} 的终点与边 l_{i_1} 的起点相重合，则此路径称为回路；没有相同边的回路称为简单回路；除 l_{i_1} 的起点与 l_{i_k} 的终点重合外，既没有相同的边，又没有相同的结点的回路称为基本回路．

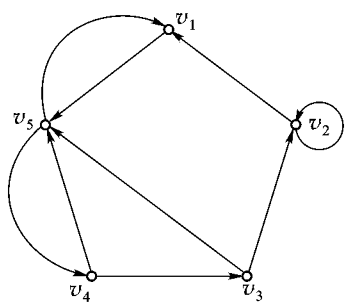


图 4－20

在路径$(l_{i_1},l_{i_2},\cdots,l_{i_k})$中有重复的边出现，则称该路径为复杂路径，又如果 l_{i_1} 的起点与 l_{i_k} 的终点重合，则称该路径为复杂回路．

在图 4－20 中，

(a) $P_1=((v_4,v_5),(v_5,v_1))$是一基本路径，也是简单路径．

(b) $P_2=((v_3,v_2),(v_2,v_2),(v_2,v_1),(v_1,v_5),(v_5,v_1))$是一简单路径但不是基本路径．

(c) $P_3=((v_1,v_5),(v_5,v_4),(v_4,v_3),(v_3,v_2),(v_2,v_2),(v_2,v_1))$是简单回路但不是基本回路．

(d) $P_4=((v_3,v_5),(v_5,v_4),(v_4,v_3))$是基本回路．

在简单图中路径与回路也可以用结点序列表示．如上面的 P_2 与 P_4 可记为：

$$(v_3,v_2,v_2,v_1,v_5,v_1)\text{和}(v_3,v_5,v_4,v_3)$$

且称 P_2 穿程于$(v_3,v_2,v_2,v_1,v_5,v_1)$，$P_4$ 穿程于(v_3,v_5,v_4,v_3)．

在无向图中一条边 l_k 对应于无序结点对(v_i,v_j)，而此无序结点对(v_i,v_j)可以看成是两个有序结点对：(v_i,v_j)及(v_j,v_i)．由此可用方向相反之两条有向边代替一条无向边．这样一个无向图就可转换成有向图了．从而有向图的概念，定理亦可适用于无向图．

定义 2　路径 P 中所含边的条数称为路径 P 的长度.

关于路径的长度有下面的基本路径定理：

定理 1　一个有向(n,m)图中任何基本路径长度均不超过 $n-1$；而任何基本回路长度均不超过 n.

证　在基本路径中各结点均不相同，在长度为 k 的基本回路径中，不同的结点数为 $k+1$，因(n,m)图中仅有 n 个不同的结点，故基本路径之长度不会超过 $n-1$；对于长度为 k 的基本回路，不同结点的数目也为 k，因图中仅有 n 个结点，故基本回路的长度不会超过 n. 证毕.

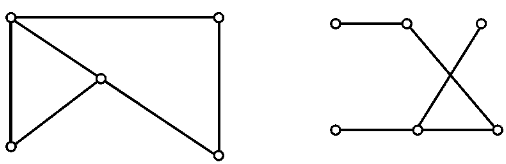
定义 3　在一有向图的结点 v_i 与另一结点 v_j 间，若存在一条路径，则称 v_i 到 v_j 是可达的；v_i 到 v_j 的路径长度的最小者，称为 v_i 到 v_j 的距离. 用 $d(v_i,v_j)$ 表示.

如图 4－20v_3 到 v_1 是可达的，且 $d(v_3,v_1)=2$.

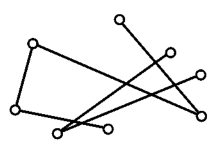
二、连通性

定义 4　设无向图 $G=\langle V,E\rangle$，$\forall v_i$，$v_j\in V$，若 v_i，v_j 之间存在路径，则称 v_i，v_j 是可达的；若图 G 中任何两个结点都是可达的，则称图 G 为连通图；否则称为非连通图. 规定平凡图是连通图.

一个有向图，如果忽略其边的方向后得到的无向图是连通的，则称此有向图为连通图；否则称为非连通图.



连通图



非连通图

图 4－21

关于有向图的连通性还分如下三种情况.

定义 5　一个有向连通图 G，如果其任何两结点间均是互相可达的，则称图 G 是强连通的；

如果其任何两结点间至少存在一向是可达的，则称图 G 是单向连通的；

如果忽略边的方向后其无向图是连通的，则称图 G 是弱连通的.

如图 4－22，(a)是强连通的，(b)是单向连通的，(c)是弱连通的，(d)是非连通的.

显然，强连通图一定是单向连通图；单向连通图一定是弱连通图；反之，

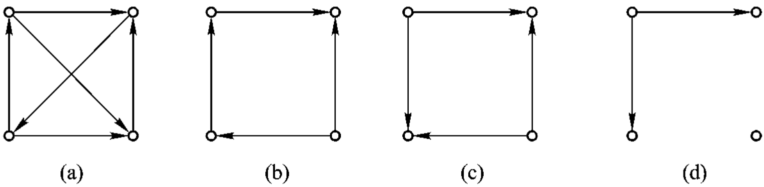


图 4－22

则不真.

三、欧拉(Euler)路径

定义 6 通过图 G 中每条边一次且仅一次的路径称为欧拉路径. 若图 G 中的一个回路通过 G 中每条边一次，这样的回路称为欧拉回路，具有欧拉回路的图称为欧拉图.

从这个定义中我们可以看出，本节开头我们提到的哥尼斯堡七桥问题，欧拉把它抽象成图 4－19(b)，就是要判断它是否是欧拉图？如果是的话，则七桥问题成立；否则不成立. 为此我们有下面的

定理 2 无向连通图具有一条欧拉路径的充要条件是有零个或两个次数为奇数的结点.

证 必要性 设$(v_1, v_2, \cdots, v_k)$是一个欧拉路径，对于每个 v_i $(v_1, v_2, \cdots, v_k)$都通过(v_{i-1}, v_i) (v_i, v_{i+1})两条边，且这两条边以前未出现过. 因此，除 v_1，v_k 外，必有 $\deg(v_i)$为偶数$(i=2, \cdots, k-1)$；若 $v_1 \neq v_k$，则 $\deg(v_1)$及 $\deg(v_k)$均为奇数，即此时有两个次数为奇数的结点. 若 $v_1 = v_k$，则$\deg(v_1)$必为偶数，这时所有结点之次数均是偶数，即有零个次数为奇数的结点.

充分性 若图 G 有零个或两个次数为奇数的结点，我们构造一条欧拉路径. 若有两个奇次数结点，则从其中的一个结点开始构造一条路径. 即从 v_0 出发经关联边 l_1 “进入” v_1，若 $\deg(v_1)$为偶数，则必可由 v_1 再经关联边 l_2 “进入” v_2，如此下去，每边仅取一次，由图 G 的连通性，必可达到另一个奇次数结点停下，得到一条路径 P：$(v_1, v_2, \cdots, v_k)$. 若 G 中没有奇次数结点，则从任一结点 v_0 出发，用上述方法必可回到结点 v_0，得到上述一条回路 P_1.

若 P(或 P_1)通过了 G 的所有边，则 P(或 P_1)便是欧拉路径.

若 G 中去掉 P(或 P_1)后得到子图 G'，则 G'中的每个结点次数为偶数，由连通性 P(或 P_1)与 G'至少有一个结点 v_i 重合，在 G'中由 v_i 出发重复上法，得到路径 P_2.

若当 P(或 P_1)与 P_2 组合在一起恰好是 G，则即得欧拉路径；否则，可再得 P_3，依此类推直到得到欧拉路径为止. 证毕.

推论 1　无向连通图 G 为欧拉图的充要条件是 G 的每个结点的次数均为偶数.

由这个定理我们可以看出哥尼斯堡七桥问题是不成立的，因图中四个结点次数全是奇数. 欧拉正是应用这个理论解决七桥问题的，从而出现了第一篇关于图论的文章.

例 1　邮递员从邮局 v_1 出发，沿邮路投递信件，其邮路如图 4－23，试问是否存在一条投递路线使邮递员从邮局出发通过所有路线而不重复，且最后回到邮局？

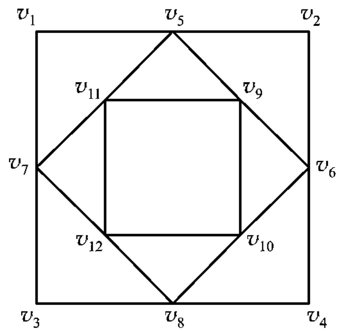


图 4－23

解　此题即为求证图 4－23 是否为欧拉图. 由于图中每个结点次数均为偶数，故由定理 2 可知这样的邮递线路是存在的，且为

$$P:(v_1,v_5,v_{11},v_7,v_{12},v_8,v_{10},v_6,v_9,v_{11},v_{12},v_{10},v_9,v_5,v_2,v_6,v_4,v_8,v_3,v_7,v_1,).$$

四、哈密顿（Hamilton）图

与欧拉图类似的问题是哈密顿图的问题. 1859 年，英国数学家威廉哈密顿提出一个关于十二面体的数学游戏；即在图 4－24 中能否找到一条回路，使它含有这个图的所有结点？他把结点看作城市，边看成交通线，称这个问题为周游世界问题，即从某个城市出发，经每个城市一次，再回到原来的城市，经过验证这个问题是成立的.

定义 7　图 G 的一个回路，若它通过 G 中每个结点一次且仅一次，则称它为哈密顿回路；具有这种回路的图称为哈密顿图.

通过 G 中每个结点一次之路径（非回路）称为哈密顿路径.

关于哈密顿路径与回路，至今尚未找到它的充要条件；对于一个图，要想断定它是否是哈密顿图，只能用尝试法.

例 2　判断下列图 4－25 所示的图是否是哈密顿图？欧拉图？

解　图（a）由回路 $P:(v_1,v_2,v_3,v_4,v_8,v_7,v_6,v_5,v_1)$ 可知它是哈密顿图；由定理 2 的推论知它也是欧拉图.

图（b）显然不存在通过每一结点一次的回路，即它不是哈密顿图；由定理 2 的推论知它是欧拉图.

图（c）是哈密顿图，但不是欧拉图.

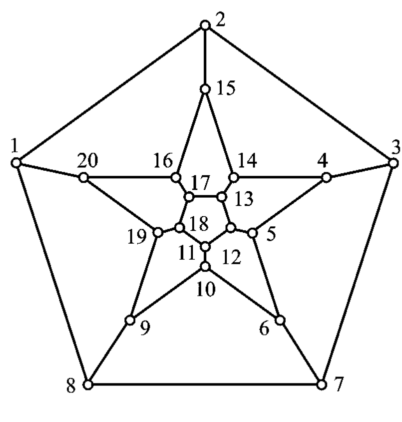


图 4－24

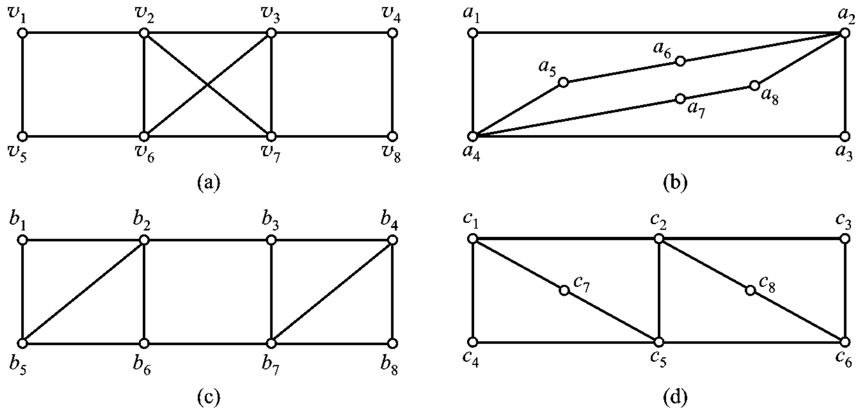


图 4－25

图(d)既不是哈密顿图，也不是欧拉图.

练习题 4－2

1. 若无向图 G 中恰有两个次数为奇数的结点，则这两点间必有一条路径.

2. 分析图 4－26

(1) 从 A 到 F 的所有路径；

(2) 从 A 到 F 的距离；

(3) 它是否是欧拉图、哈密顿图？

3. 找出图 4－25 中 4 个图中的一个基本回路与一个简单回路.

4. 在图 4－27 中给出有向图，试求 $d(v_1,v_4)$，$d(v_2,v_5)$，$d(v_3,v_6)$. 此有向图对应的关系是否可传递的？如果不是可传递的，试求此图的传递闭包.

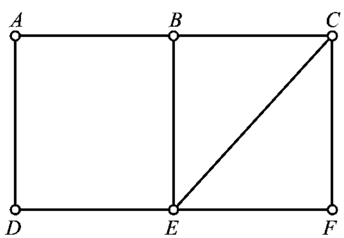


图 4－26

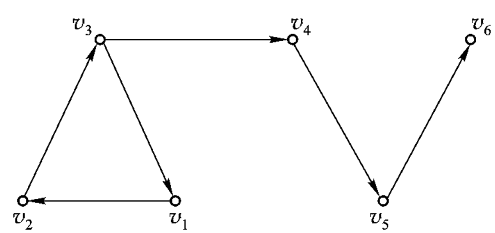


图 4－27

5. 在图 4－28 中，哪一个是(a)连通的，(b)无环图，(c)简单图？

6. 图 4－29 中，哪一个存在欧拉路径？哪一个存在哈密顿路径？哪一个是欧拉图、哈密顿图？

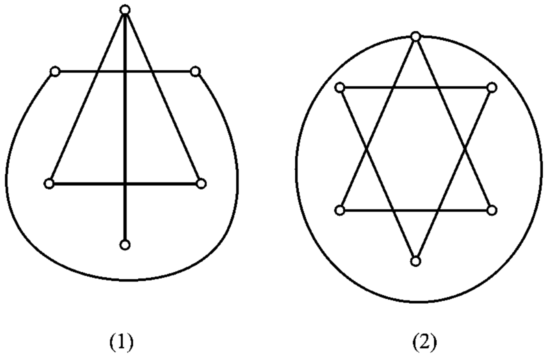


图 4－28

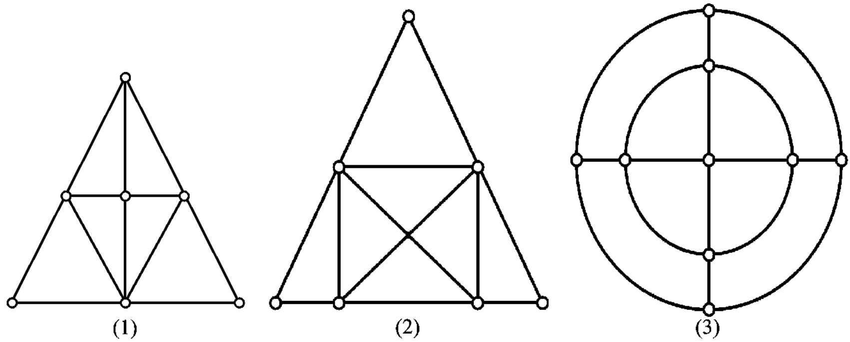


图 4－29

第三节　图的矩阵表示

前面，我们讲述了图的一些概念及欧拉图和哈密顿图．那里为了解决问题我们引进了图形．用图形表示一个图，直观、明了、有一定的优越性，但是我们只是对一些较简单的图用起它来才比较方便．对稍复杂一些的图就有些为难了，因此有必要引进新的手段方法．矩阵就是解决图的问题的有力工具，用矩阵表示一个图的方法，简单且颇具有普遍性．

一、邻接矩阵

定义 1　设一有向图 $G=\langle V,E\rangle$，其中 $V=\{v_1,v_2,\cdots,v_n\}$，$E=\{l_1,l_2,\cdots,l_m\}$．假定各结点从 v_1 到 v_n 排列．定义一个 $n\times n$ 矩阵 A，A 中的元素为

$$a_{ij}=\begin{cases}1，如果(v_i,v_j)\in E,\\0，如果(v_i,v_j)\notin E.\end{cases}$$

此矩阵称为图 G 的邻接矩阵.

零图的邻接矩阵的元素全为 0，完全图的邻接矩阵除主对角线元素全为 0 外，其他元素均为 1.

有向图 G 的各边均取反向所得的图称为 G 的逆图，记作 $\overline{G}$. 图 $\overline{G}$ 的邻接矩阵是 A 的转置矩阵，记为 A^{T}.

对于无向图同样有邻接矩阵的概念，在无向图中将无向边用两条方向相反之有向边代替，使无向图转成有向图，无向图的邻接矩阵是对称的.

邻接矩阵的概念还可推广到多重图和有权图. 对多重图，a_{ij} 代表从 v_i 到 v_j 的边的重数；对有权图，a_{ij} 代表权，当从 v_i 到 v_j 不存在边时，规定 $a_{ij}=0$.

例 1　求下列图 4－30 所示的邻接矩阵.

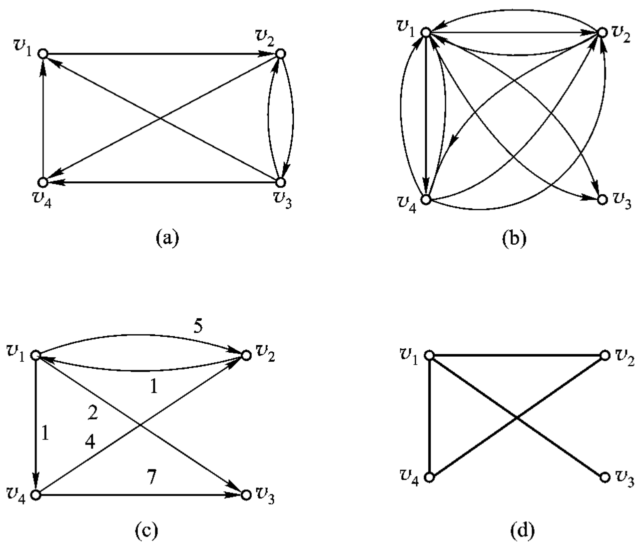


图 4－30

解　(a)

$$A=\begin{pmatrix}0&1&0&0\\0&0&1&1\\1&1&0&1\\1&0&0&0\end{pmatrix};$$

(b)

$$A=\begin{pmatrix}0&1&2&1\\2&0&0&1\\0&0&0&0\\2&2&0&0\end{pmatrix};$$

（c）

$$A=\begin{pmatrix}0&5&2&1\\1&0&0&0\\0&0&0&0\\0&4&7&0\end{pmatrix};$$

（d）

$$A=\begin{pmatrix}0&1&1&1\\1&0&0&1\\1&0&0&0\\1&1&0&0\end{pmatrix}.$$

通过邻接矩阵的运算还可获得对应图的某些特征.

（1）设 A 为有向图 G 的邻接矩阵，则图 G 中结点 v_i 的引出次数为

$$\overleftarrow{\deg}(v_i)=\sum_{k=1}^{n}a_{ik}.$$

v_i 的引入次数为

$$\overrightarrow{\deg}(v_i)=\sum_{k=1}^{n}a_{ki}.$$

v_i 的全次数为

$$\deg(v_i)=\sum_{k=1}^{n}(a_{ki}+a_{ki}),$$

即 v_i 的引出次数为第 i 行的全体元素之和，v_i 的引入次数为第 i 列的全体元素之和.

如图 4－30 中(a)由邻接矩阵 A 可得出 v_1 的引出次数 $\deg(v_1)=1$，v_1 的引入次数为 $\deg(v_1)=2$.

（2）$A^n=\overbrace{A\cdot A\cdot\cdots\cdot A}^{n\text{个}}$的元素的意义

$n=1$ 时，$a_{ij}=1$ 表示存在一条边(v_i,v_j)，或说，从 v_i 到 v_j 存在一条长度为 1 的路径.

$n=2$ 时，A^2 中的元素

$$b_{ij}=\sum_{k=1}^{n}a_{ik}a_{kj}$$

当且仅当 a_{ik}与 a_{kj}都等于 1 时，$b_{ij}\neq0$，a_{ik}和 a_{kj}都等于 1，表明存在边(v_i,v_k)和(v_k,v_j)，即存在一条从 v_i 到 v_j 的长度为 2 的路径，b_{ij}表示从 v_i 到 v_j 长度为 2 的路径的数目. 如 $b_{ij}=0$，则长度为 2 的路径不存在. b_{ii}表示长度为 2 的回路数目.

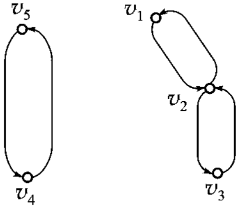


图 4－31

$n=l$ 时，令 $c=A^l$，c_{ij}表示从 v_i 到 v_j 的长度为 l 的路径的数目；如 $c_{ij}=0$，则表示长度为 l 的路径不存在. c_{ii}表示从 v_i 出发的长度为 l 的回路的数目.

例 2　给定一图 $G=\langle V,E\rangle$，如图 4－31

$$\boldsymbol{A}=\begin{pmatrix}0&1&0&0&0\\1&0&1&0&0\\0&1&0&0&0\\0&0&0&0&1\\0&0&0&1&0\end{pmatrix},\quad \boldsymbol{A}^2=\begin{pmatrix}1&0&1&0&0\\0&2&0&0&0\\1&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{pmatrix},$$

$$\boldsymbol{A}^3=\begin{pmatrix}0&2&0&0&0\\2&0&2&0&0\\0&2&0&0&0\\0&0&0&0&1\\0&0&0&1&0\end{pmatrix},\quad \boldsymbol{A}^4=\begin{pmatrix}2&0&2&0&0\\0&4&0&0&0\\2&0&2&0&0\\0&0&0&1&0\\0&0&0&0&1\end{pmatrix}.$$

上述矩阵中我们可以得到一些结论，如 v_1 与 v_2 之间有 2 条长度为 3 的路径，v_1 与 v_3 之间有一条长度为 2 的路径，从 v_1 发出的长度为 2 的回路只有 1 条，从 v_2 发出的长度为 4 的回路有 4 条.

利用邻接矩阵 A，通过计算 A，A^2，…，A^l，…，可以看出 v_i 到 v_j 是否存在路径，且长度，路径数目也可同时得到. 若 $C=\boldsymbol{A}^l$ 中 $c_{ij}\geqslant 1$，则表示 v_i 到 v_j 可达，但 A^l 要算到何时呢？我们知道，如果有向图 G 有 n 个结点，v_i 到 v_j 可达，则必然有一条长度不超过 n 的路径，因此，只须算到 $\boldsymbol{A}^l(1\leqslant l\leqslant n)$ 即可，关于可达性亦可用矩阵表示.

二、可达性矩阵

考虑矩阵 $\boldsymbol{R}_r=(r_{ij})_{n\times n}$

$$\boldsymbol{R}_r=\boldsymbol{A}+\boldsymbol{A}^2+\cdots+\boldsymbol{A}^r.$$

r_{ij}表示从结点 v_i 到 v_j 的所有长度为 1 至 r 的路径的数目之和.

由上节定理 1 知有 n 个结点的有向图中，基本路径及基本回路长度不超过 n；因此要研究是否存在一条从 v_i 到 v_j 的任意长的路径，仅需考虑

$$\boldsymbol{R}_n=\boldsymbol{A}+\boldsymbol{A}^2+\boldsymbol{A}^3+\cdots+\boldsymbol{A}^n$$

时，$r_{ij}\neq 0$，$i\neq j$ 表示 v_i 到 v_j 是可达的，$i=j$ 表示经过 v_j 的回路存在；$r_{ij}=0$，$i\neq j$ 表示 v_i 到 v_j 是不可达的，$i=j$ 表示不存在经过 v_j 的回路. 即 r_{ij}表明了点间的可达性.

由于在讨论可达性时，我们仅需知道结点间是否可达，而不需知道结点间存在多少条路径和怎样的路径，故引入下面的

定义 2 设 $G=\langle V,E\rangle$是有 n 个结点的有向图，定义一个矩阵 $\boldsymbol{P}=(p_{ij})_{n\times n}$，且

$$p_{ij}=\begin{cases}1，当 \boldsymbol{R}_n 中 r_{ij}\neq 0 时，\\0，当 \boldsymbol{R}_n 中 r_{ij}=0 时，\end{cases}$$

称矩阵 P 为图 G 的可达性矩阵.

例 3　求图 $G=\langle V,E\rangle$ 之可达性矩阵，其中：

$V=\{v_1,v_2,v_3,v_4\}$，

$E=\{(v_1,v_2),(v_2,v_3),(v_2,v_4),(v_3,v_2),(v_3,v_4),(v_3,v_1),(v_4,v_1)\}$.

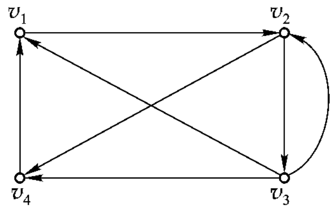


图 4-32

解　图 G 的图形如图 4-32，邻接矩阵为

$$A=\begin{pmatrix}0&1&0&0\\0&0&1&1\\1&1&0&1\\1&0&0&0\end{pmatrix}，于是，A^2=\begin{pmatrix}0&0&1&1\\2&1&0&1\\1&1&1&1\\0&1&0&0\end{pmatrix},$$

$$A^3=\begin{pmatrix}2&1&0&1\\1&2&1&1\\2&2&1&2\\0&0&1&1\end{pmatrix},\qquad A^4=\begin{pmatrix}1&2&1&1\\2&2&2&3\\3&3&2&3\\2&1&0&1\end{pmatrix}.$$

$$R_4=A+A^2+A^3+A^4=\begin{pmatrix}3&4&2&3\\5&5&4&6\\7&7&4&7\\3&2&1&2\end{pmatrix},\qquad P=\begin{pmatrix}1&1&1&1\\1&1&1&1\\1&1&1&1\\1&1&1&1\end{pmatrix}.$$

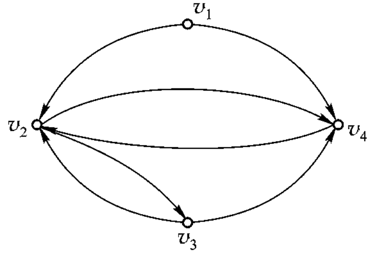
由此可达性矩阵可知，图 G 之任意两结点间均可达，且每个结点均有回路通过.

练习题 4-3

1. 图 4-33 给出了一个有向图

(a) 求出它的邻接矩阵 A.

图 4-33



(b) 求出 A^2，A^3，A^4，说明从 v_1 到长度为 1，2，3 和 4 的路径各有几条？

(c) 求出它的可达性矩阵 P.

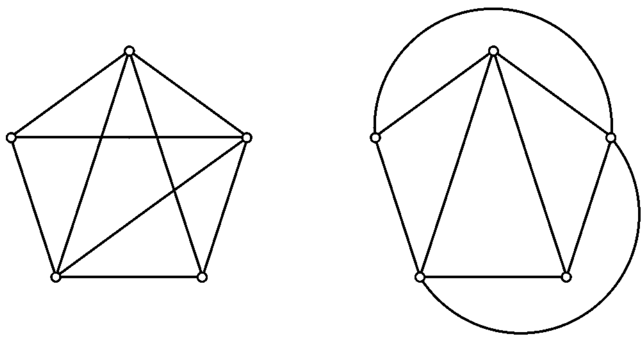
2. 一个图 G 的邻接矩阵为 $A=\begin{pmatrix}1&3&0&0\\3&0&1&1\\0&1&2&2\\0&1&2&0\end{pmatrix}$ 画出它的图

3. **如何从邻接矩阵看出它所表示的图是欧拉图？**

第四节　平面图与二部图

定义 1　设 $G=\langle V,E\rangle$ 是一个无向图，如果能够把 G 的所有结点和边画在平面上，且使得任何两条边除了端点外没有其他的交点，就称 G 是一个平面图.

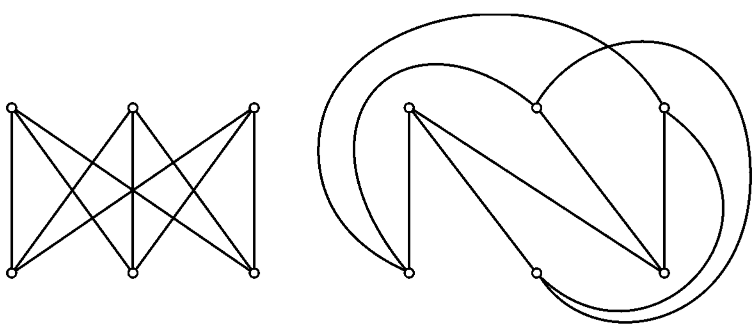
有一些图表面上看有两条或几条边是相交的，但是不能就此肯定它不是平面图，如图 4－34(a) 表面上看有几条边相交，但如把它画成图 4－34(b) 则可看出它是一个平面图.



(a)　(b)

图 4－34

有些图不论怎样改画，除去结点外，总有边相交，这样的图是非平面图. 如图 4－35(a)，这个图不论怎样，改画后至少有一条边与其他边相交，如图 4－35(b)，即它是非平面图.



(a)　(b)

图 4－35

定义 2　设 G 是一个连通平面图，由图中的边所包围的最小平面块，其内部不包含图的结点，也不包含图的边，称为 G 的一个区域，包围该区域的诸边所构成的回路称为这个区域的边界．区域面积为有限者称为有限区域；否则称为无限区域．

如图 4－36 有五个区域，区域 1——其边界是：$(a,b,c,g,e,h,i,h,j,h,e,a)$；

区域 2——其边界是：(e,f,g,e)；

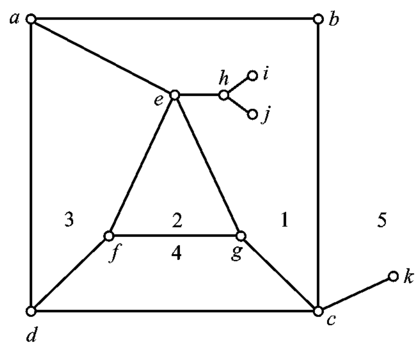
区域 3——其边界是：(a,d,f,e,a)；

区域 4——其边界是：(d,c,g,f,d)；

区域 5——其边界是：(a,b,c,k,c,d,a)

显然，区域 1，2，3，4，是有限区域，

图 4－36



而区域 5 是无限区域．一个平面图有惟一的一个无限区域．一个平面图按区域将整个平面完全划分．一个图的结点，边与区域之间有下面关系：

定理 1（欧拉定理）　设图 G 是一个 (n,m) 连通平面图，它的区域数为 r，则有

$$n-m+r=2.$$

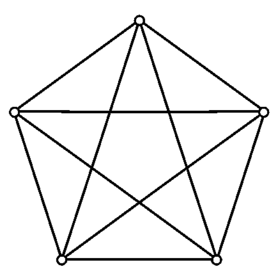
定理 2　设图 G 是一个 n 个结点 m 条边的简单连通平面图，若 $n\geqslant 3$，则有

$$m<3n-6. \tag{*}$$

两个定理证明均略．

一个连通平面图一般均应满足公式（ * ），否则它是非平面图．

图 4－37



例 1　设图 G 如图 4－37 所示．因为有 5 个结点 10 条边，故 $3\times 5-6<10$，即 $3n-6>m$ 对本图不成立，故它是非平面图．

需要注意定理 2 的条件并不充分，如图 4－35，结点数为 6，边数为 9，即满足 $3n-6>m$，但它却不是平面图．

例 2　有三个工厂和三个矿山，要从每一个工厂到每一个矿山各修一条专用铁路，这些铁路能否在同一个平面上并且互不交叉？

解　将三个工厂与三个矿山用六个结点表示，九条铁路用九条边表示就得到图 4－35，这表明在平面上九条专用铁路必相交.

欧拉定理有时可以帮助我们确定一个图是非平面图，但它有许多弱点，它无法使我们断定一个图是否是平面图，还是非平面图. 而库拉拖夫斯基(Kuratowski)定理能使我们解决这个问题. 为此我们先介绍定义 3.

定义 3　在一个图 $G=\langle V,E\rangle$ 中，将一些边 (v_{i_1},v_{j_1})，(v_{i_2},v_{j_2})，…，(v_{i_k},v_{j_k}) 删除，并分别将结点 v_{i_1} 与 v_{j_1}，…，v_{i_k} 与 v_{j_k} 合并而且用新结点 w_1，w_2，…，w_k 代替之，所得的新图 $G=\langle V,E\rangle$ 叫做图 G 的基本减缩.

图 4－38 中(b)是(a)的基本减缩.

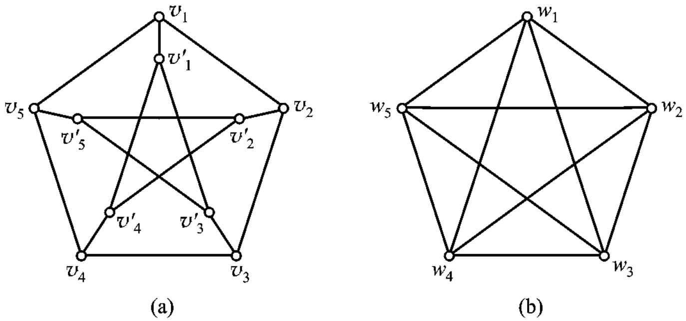


图 4－38

定理 3(Kuratowski 定理)　一个图是平面图的充要条件是它的任何子图都不可能减缩成下面的两个图.

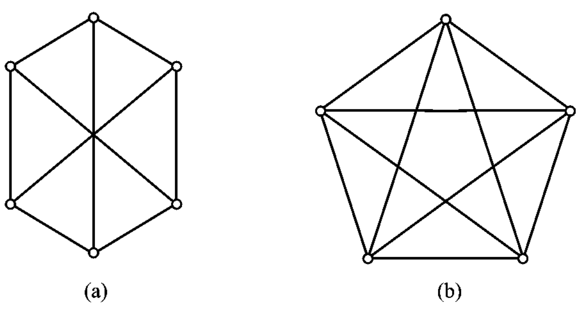
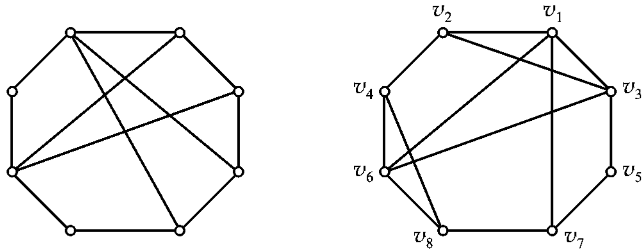


图 4－39

证　略

例 3　图 4－40 中(a)是平面图，(b)是一个非平面图，在(b)中将边 (v_2,v_4)，(v_3,v_5)，(v_7,v_8) 减缩成三个结点 w_1，w_2，w_3 后即成为图 4－39 中



(a) 平面图　　(b) 非平面图

图 4－40

下面介绍一下二部图.

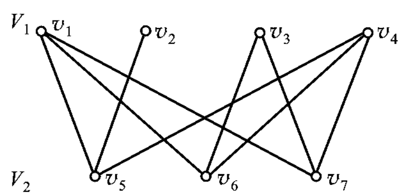
定义 4　设无向图 $G=\langle V,E\rangle$ 有两个 V 的子集 V_1，V_2，它们满足

$$V_1\cup V_2=V,$$

$$V_1\cap V_2=\varnothing.$$

图 G 的每条边 $l=(v_i,v_j)$ 均满足 $v_i\in V_1$，$v_j\in V_2$，此时称图 G 为二部图.

图 4－41



在二部图 G 中，其结点集 V 被划分成两部分，它们是 V_1 与 V_2，在 V_1 与 V_2 各结点间无边相联，V_1 与 V_2 称为 G 的互补结点子集.

下面是一个二部图且

$$V_1=\{v_1,v_2,v_3,v_4\},$$

$$V_2=\{v_5,v_6,v_7\}.$$

关于二部图有下面的

定理 4　无向图 G 是一个二部图充要条件是 G 的所有回路的长度均为偶数.

图 4－41 是一个二部图.

练习题 4－4

1. 在图 4－42 中，如可能，画出每个图的一个平面表示.
2. 图 4－43 是否是二部图？如果是，找出其互补结点子集.
3. 证明：若 G 是每个区域至少由 $k(k>3)$ 条边围成的连通平面图，则 $m<\dfrac{k(n-2)}{k-2}$，这里 n，m 分别是图 G 的结点数和边数.

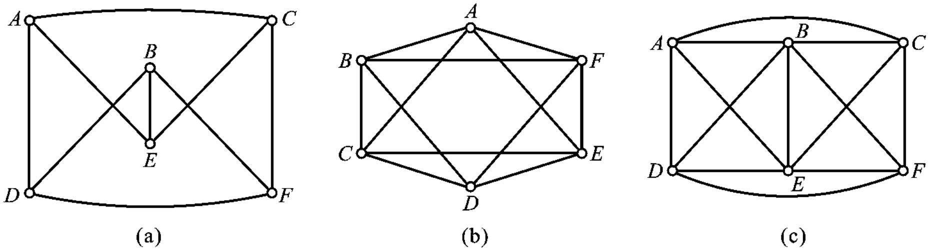


图 4 - 42

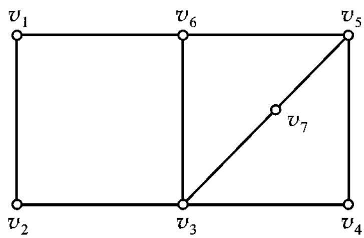


图 4 - 43

第五节 树

一、树及其基本性质

定义 1 不含有回路的连通图称为树；在树中次数为 1 的结点称为叶，次数大于 1 的结点称为分支结点.

如图 4 - 44，(a) 是树，(b)，(c) 均不是树；(b) 中带有回路；(c) 是非连通的；(a) 中 v_1，v_3，v_4 为叶，v_2 为分支结点.

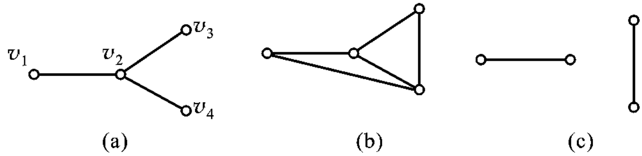


图 4 - 44

关于树有下面几个特性

定理 1 在 (n,m) 树中，必有 $m = n - 1$.

证 采用数学归纳法，对 n 进行归纳.

$n=1$ 时，$m=0$，定理成立.

设对所有 $i(i<n)$ 定理成立，需证在 $i=n$ 时，$m=n-1$. 在 (n,m) 树中，由于其不包含任何回路，故从树中删去一边后就变成两个互不连通的子图，而其每个子图则是连通的，故其每个子图均为树，设它们分别是 (n_1,m_1) 树及 (n_2,m_2) 树，由于 $n_1<n$，$n_2<n$，故由归纳法假设可得

$$m_1=n_1-1,\ m_2=n_2-1.$$

而
$$n=n_1+n_2,\ m=m_1+m_2+1.$$

故有
$$m=n-1.$$ 证毕.

定理 2　具有两个结点以上的树必至少有两片叶.

证　由第一节定理 1 知，任何 (n,m) 图的所有结点次数之和为 $2m$. 对于树而言必为 $2n-2$. 若存在某树其叶少于 2，则此时其分支结点至少为 $n-1$. 此时树的结点次数的和必大于 $2n-2$，矛盾. 此矛盾说明定理成立. 证毕.

定理 3　图 G 是树的充要条件是图 G 的每对结点间只有一条路径.

证　因 G 是树，故对每对结点间均有路径，若 v_i 与 v_j 间有两条路径，则这二条路径必构成一条回路，而这与树的定义矛盾. 必要性得证.

反之，图 G 的每对结点间存在路径，故 G 是连通的，又由于路径是惟一的，故图中不含有回路，即 G 是树. 充分性得证. 证毕.

二、生成树

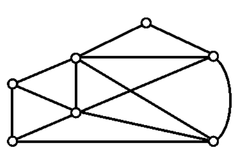
定义 2　一个连通图 $G=\langle V,E\rangle$ 的生成树，$T_G=\langle V',E'\rangle$ 是 G 的一个子图，它是树，且有 $V'=V$，$E'\subseteq E$.

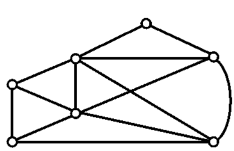
由一个连通图 G 寻找它的生成树的过程是：

在 G 中寻找基本回路，找到后在此回路中删去一边，并继续寻找之，直至 G 中无基本回路出现为止.

例 1　图 4-45 中(i)是(a)的生成树.

图 G 的生成树一般来说是不惟一的. 对于一个 (n,m) 连通图 G，我们知 T_G 是一个 $(n,n-1)$ 图. 故由 G 求得 T_G 必须删除 $m-(n-1)=m-n+1$ 条边，这个数称为图 G 的秩. 图 G 的基本回路的秩是为了打断它的所有基本回路，必须从 G 中删除之最小边数. 每一条被删除的边数叫做 G 的弦.


(a)


(b)

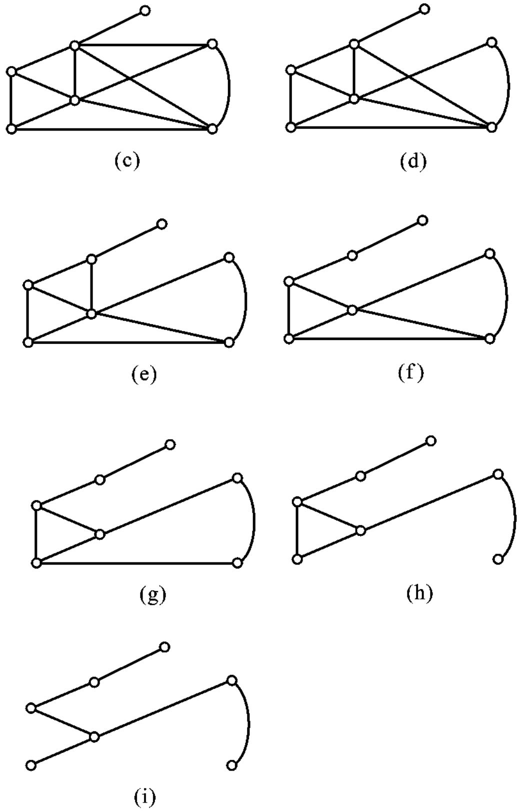


图 4－45

寻找一个连通图的生成树是很有实际价值的.

例 2 设有六个城市 v_1，v_2，v_3，v_4，v_5，v_6 它们间有输油管连通，其布置如图 4－46（a），为了保证油管不受破坏，在每段油管间须派一个连的士兵看守，为了保证正常供应，最少需多少连的士兵看守？他们应驻于哪些油管处.

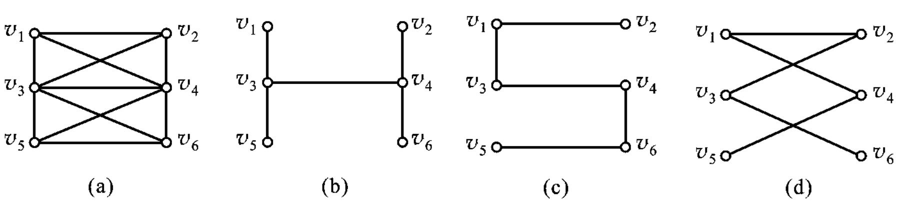


图 4－46

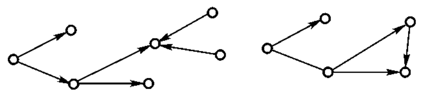
解 此问题即为寻找 4－46（a）之生成树问题. 首先由图我们知道 $n=6$，

$m=11$，故生成树的边数为 5，亦即至少须 5 个连的士兵看守．看守地段，或是图(b)，或是图(c)，或是图(d)所示．它们都是(a)的生成树．

三、有向树

定义 3　在有向图中，如果不考虑边的方向而构成树，则称此有向图为有向树．

例如图 4－47(a)是有向树，(b)不是有向树．



(a)　　(b)

图 4－47

一般常用之有向树为外向树及内向树．我们首先定义外向树：

定义 4　满足下列条件之有向树 T，称为外向树．

(1) T 有一个结点(也仅有一个)它的引入次数为 0，这个结点称为 T 的根；

(2) T 的其他结点的引入次数均为 1；

(3) T 有一些结点，它的引出次数为 0——这些结点称为 T 的叶．

图 4－48 即是一个外向树．在此图 v_1 是根，v_5—v_9 是叶．

在外向树中，非根非叶的结点，称为分支结点．图 4－48 中 v_2，v_3，v_4 为分支结点．分支结点的引入次数与引出次数均不为 0．

定义 5　由外向树的根到结点 v_i 的路径长度称为结点 v_i 的级．

由级的定义可知，根的级为 0．两个结点如从根到结点之路径长度相等，则它们有相同的级或称同级，否则称不同级．

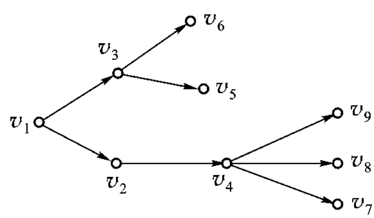


图 4－48

在图 4－48 中，v_1 的级为 0，v_2，v_3 的级为 1，v_4，v_5，v_6 的级为 2，v_7，v_8，v_9 的级为 3．

例 3　可用外向树表示家属关系．

设有某祖宗 a 生有两个儿子：b 及 c．b 与 c 又分别生三个儿子，它们分别是 d，e，f，及 g，h，i．而 d 与 g 又分别生了一个儿子，它们是 j 与 k．这样的家属关系可用图 4－49 所示的外向树表示，称为家属树．

由于可用外向树表示家属关系，故现在一般均用家属关系中之术语来称呼外向树中结点间的关系．外向树中如从结点 a 到 b 有一条边，则称 b 是 a 的儿子，而称 a 是 b 的父亲或双亲(父母)．外向树中从结点 a 到 b 及 a 到 c 均有一条边，则称 b，c 为兄弟．从结点 a 至结点 f 有一条路径，则称 f 是 a 的子孙，而 a 是 f 的祖先．

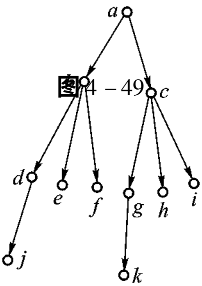
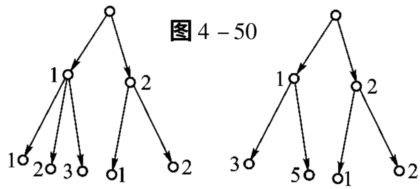


图4－49



(a)　　(b)

图4－50

由家属树所引出的第二个概念是关于有序树的概念．在家属树中，兄弟间是有一定次序的，老大、老二、老三，……等等，它们是不能随意颠倒的．如图4－49中，e 与 d 是不能相互替代的，因为 d 有儿子 j，而 e 无儿子．这给我们一个启示，在一些外向树中需要对每个分支结点（及根）的儿子顺序编号．如一结点有三个儿子，则从左到右可以编以1，2，3，也可以编成1，3，5等等．图4－50（a），（b）便是两个有序树．

我们还可以用类似的方法定义内向树：

（1）T 有一个结点（也仅有一个结点）它的引出次数为0，这个结点称为 T 的根；

（2）T 的其他结点引出次数均为1；

（3）T 有一些结点，它的引入次数为0，这些结点称为 T 的叶．

与外向树类似，内向树也有分支结点，级等概念，它们的含义也与外向树类似，这里不再叙述了．

四、二元树

外向树中除叶外每个结点的引出次数均大于0，结点的引出次数均不超过某一正整数 m，则称此外向树为 m 元树．

定义6　一 n 个结点的外向树如满足：

$$\deg(v_i) \leqslant m \quad (i=1,2,\cdots,n),$$

则称此外向树为 m 元树．

如满足（除叶外）

$$\deg(v_i) = m \quad (i=1,2,\cdots,n),$$

则称此外向树为 m 元完全树．

当 $m=2$ 时，则分别称为二元树及二元完全树．

图4－51中（a），（b），（c），（d）分别给出了四元树，四元完全树；二元

树及二元完全树.

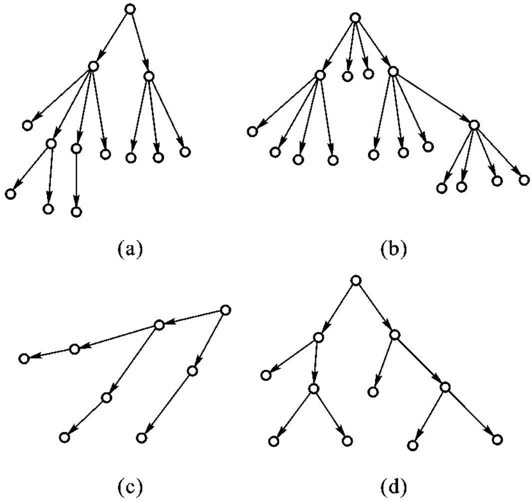


图 4－51

在二元树中，每个结点最多可以有两个儿子，称位于左边的为左儿子，右边的为右儿子.

例 4　可用二元树表示算术表达式，如下列表达式

$(v_1 - v_2)/v_3 + v_4(v_5 - v_6/v_7)$

这个表达式可用图 4－52 所示之有序二元树表示.

当然，二元树的作用远不止于此. 而它的真正作用在于：任一外向树均可用二元树表示.

用二元树表示外向树的方法如下：

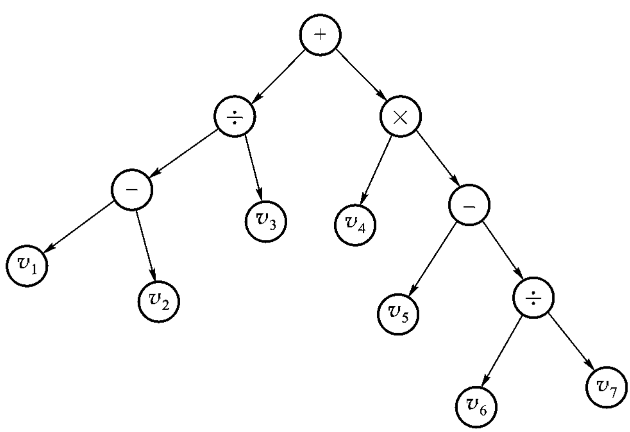
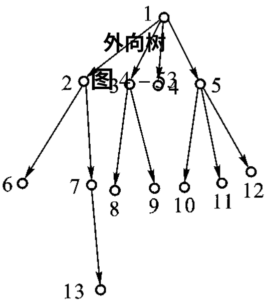


图 4－52

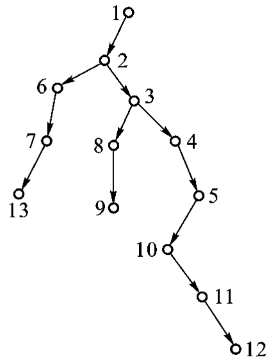
对外向树的结点从根开始逐级讨论，每级从左到右顺序讨论之. 若一结点与前一结点是兄弟则在二元树中作为前一结点的右儿子，若一结点是某一结点最左边儿子，则在二元树中作为某一结点的左儿子.

例 5 图 4－53 是一外向树可用图 4－54 之二元树表示.



外向树

图 4－53



用二元树表示外向树

图 4－54

练习题 4－5

1. 根据有向图的邻接矩阵，如何确定它是否是有向树？如果它是有向树，如何确定它的根和叶？

2. 将图 4－55 外向树表成二元树.

3. 一个树 T 有两个结点次数为 2，一个结点次数为 3，三个结点次数为 4，问它有几个次数为 1 的结点？

4. 求图 4－56 的生成树.

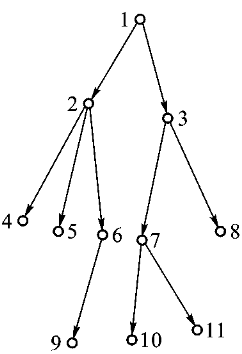


图 4－55

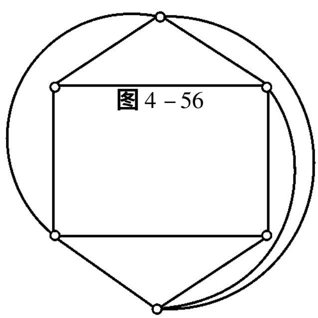


图 4－56

第六节　运输网络问题

交通、运输是人们日常生活中常常遇到的问题. 合理的安排交通线路、运送货物会收到很好的经济效益. 本节作为应用问题我们介绍运输网络的最大流及算法.

一、网络的流

设 $N=(V,U)$ 是一个有向图，满足：

（1）V 中有两个结点子集 X 和 Y，X 中的任一结点的引入次数为零，Y 中任一结点的引出次数为零；

（2）边集 U 上定义一个非负整数值函数 c；则称 N 为一个网络.

X 中的结点称为源，Y 中的结点称为汇，既非源又非汇的结点称为中间结点. 函数 c 称为网络 N 的容量函数，容量函数 c 在边 a 上的值称为 a 的容量.

边　$a=(i,j)$ 的容量记为 $c(a)$ 或 $c(i,j)$. 通常 $c(i,j)\neq c(j,i)$.

图 4－57 是有一源一汇的网络图.

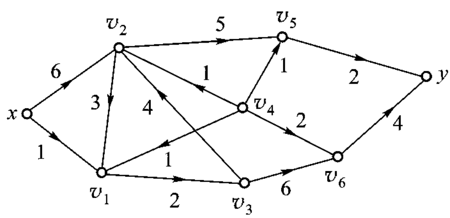


图 4－57

网络 N 中通过每条边 (i,j) 的某事物的多少称为通过该边的流，记为 $f(i,j)$.

显然

$$0\leqslant f(i,j)\leqslant c(i,j). \tag{1}$$

设 V_1 和 V_2 是结点集 V 的子集，用 (V_1,V_2) 表示起点在 V_1 中，终点在 V_2 中的边的集合. 用 $f(V_1,V_2)$ 表示 (V_1,V_2) 中边的流的和. 则

$$f(V_1,V_2)=\sum_{(i,j)\in(V_1,V_2)}f(i,j).$$

$f(i,V)$ 表从 i 流出的流的和，$f(V,i)$ 表流向 i 的流的和. 当 i 为中间结点时 $f(i,V)-f(V,i)=0$.

设从源 x 流出的流为 f_{xy}，从汇 y 流出的流为 $-f_{xy}$（流入 y 的流 f_{xy}），则有

$$f(i,V)-f(V,i)=\begin{cases} f_{xy}, & i=x, \\ 0, & i\neq x\neq y,\ \forall i\in V, \\ -f_{xy}, & i=y. \end{cases} \tag{2}$$

集 $F=\{f(i,j),(i,j)\in U\}$ 称为网络 N 的流；也就是全体流之集. 若 N 满足(1)，(2)，则称 F 是 N 上的可行流. $f_{xy}=8$ 称为流 F 的值.

在网络 N 中每条边旁通常标有两个数，第一个数为 $c(i,j)$，第二个数为 $f(i,j)$，如图 4 - 58. 该图中 $f_{xy}=8$.

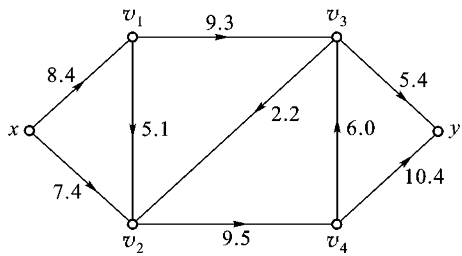


图 4 - 58

对于边 (i,j)，当 $f(i,j)=c(i,j)$ 时，称边 (i,j) 为饱和边，否则为非饱和边.

每个网络 N 至少有一个可行流. 若 $f(i,j)=0$. 则流为零，称为零流. 我们的问题是求满足(1)，(2)式的最大流 f_{xy}.

二、割、最大流最小割定理

设 $N=(V,U)$ 是有单一源 x 和单一汇 y 的运输网络.

设 K 是形为 $(V_1,\overline{V}_1)$ 的边的集合，$x\in V_1$，$y\in\overline{V}_1$，而 $V_1\subseteq V$，则 K 称为 N 中的割.

如在图 4 - 58 的网络 N 中，取 $V_1=\{x,v_1,v_2\}$，$\overline{V}_1=\{v_3,v_4,y\}$，则 $K=(V_1,\overline{V}_1)=\{(v_1,v_3),(v_2,v_4)\}$.

可见，割 K 是分离源和汇的边的集合.

若记 $c(V_1,\overline{V}_1)$ 或 $c(K)$ 表示割 K 的容量，则

$$c(K)=c(V_1,\overline{V}_1)=\sum_{(i,j)\in(V_1,\overline{V}_1)}c(i,j).$$

与割相近的概念有：

设 S 是图 G 的一个边集，在 G 中去掉 S 的所有边后，G 变成有两个分支的分离图；但是去掉 S 的任一真子集图仍连通，则 S 称为图 G 的一个割集.

注 割与割集是有区别的. 割是有向图，而割集是无向图. 在图 4 - 58 中

$\{(v_1,v_3),(v_3,v_2),(v_2,v_4)\}$是$N$的割集．割不一定是割集，把割删去，$N$未必分离成两部分；但把割集删去后，一定把$N$的全部自$x$到$y$的有向链断开．

关于割和流有：

定理1　设运输网络N的一个自源x到汇y的流是F，其值为f_{xy}，且令$(V_1,\overline{V}_1)$为分离x和y的任何一个割，则

$$f_{xy}=f(V_1,\overline{V}_1)-f(\overline{V}_1,V_1).$$

证　观察(2)式，对任何满足$x\in X$，$y\in\overline{X}$的$X\subseteq V$有

$$\sum_{i\in X}[f(i,V)-f(V,i)]=f_{xy},$$

或

$$f(X,V)-f(V,X)=f_{xy}.$$

把$V=X\cup\overline{X}$代入上式，注意$X\cap\overline{X}=\varnothing$有

$$f(X,V)-f(V,\overline{X})=f(X,X\cup\overline{X})-f(X\cup\overline{X},X),$$

但

$$f(X,X\cup\overline{X})=f(X,X)+f(X,\overline{X})-f(X,X\cap\overline{X})=f(X,X)+f(X,\overline{X}).$$

$$f(X\cup\overline{X},X)=f(X,X)+f(\overline{X},X)-f(X\cap\overline{X},X)=f(X,X)+f(\overline{X},X).$$

故

$$f(X,\overline{X})-f(\overline{X},X)=f_{xy}.$$　证毕

推论1　对任意f_{xy}及$(V_1,\overline{V}_1)$有

$$f_{xy}\leqslant c(V_1,\overline{V}_1).$$

证　对$\forall X\subseteq V$，$f(X,\overline{X})\geqslant 0$，由定理

$$f_{xy}\leqslant f(X,\overline{X})=\sum_{i\in X,j\in\overline{X}}f(i,j)\leqslant\sum_{i\in X,j\in\overline{X}}c(i,j)=c(X,\overline{X}).$$

推论2　最大流值不超过最小割容量，即

$$\max[f_{xy}]\leqslant\min[c(K)].$$

福特和傅克逊在1956年给出

定理2（最大流最小割定理）　在运输网络中，最大流的值等于最小割的容量．

$$\max[f_{xy}]=\min[c(K)].$$

证　略

三、寻求最大流的基本思想

设N是一个网络，N中相异点序列v_{i_1}，v_{i_2}，…，v_{i_N}具有下列性质：对$\forall r$ $(r=1,2,\cdots,n-1)$或者$(v_{i_r},v_{i_{r+1}})$是一条边或者$(v_{i_{r+1}},v_{i_r})$是一条边，二者不能同时出现，由这样一些边组成的序列称为N中由v_{i_1}到v_{i_n}的路．

在路 $v_i \cdots v_p v_q \cdots v_j$ 中，若(v_p, v_q)视为前向边，则(v_q, v_p)便视为后向边.

寻求最大流的基本思想是：先任意假设网络的一个满足条件(1)的流，然后自此出发设法逐渐增大流值(假定 c 为正整数). 若自 x 到 y 的路中存在一条路，其所有前向边未被饱和，其所有后边具有正值的流. 这时总能使这条路的前向边的流增加一个正整数 ε，所有后向边的流减去 ε，而同时保持全部边的流为正值且不超过边的容量. 不破坏(1)不影响其他路. 但 f_{xy} 增加了 ε. 故总有可能逐次增加 f_{xy}. 使 N 的自 x 到 y 的全部路中的任何一条，其中至少有一条前向边被饱和，和一条后向边的流为零. 具有这种条件的路称为不可增广路，否则称为可增广路，当自 x 到 y 的路都不可增广时，f_{xy} 就不能再增大，即 f_{xy} 最大. 否则重复上述增大 f_{xy}.

四、标记法确定最大流

本段我们介绍用标记法确定最大流. 标记法共分为两个过程. 一是标记过程，二是增广过程. 标记过程用来寻找可增广路；同时确定 V_1，这个过程只需对网络中每点检查一次.

通常 V_1 按如下定义：

① $x \in V_1$；

② 若 $i \in V_1$ 且 $f(i,j) < c(i,j)$，则 $j \in V_1$，

若 $i \in V_1$ 且 $f(j,i) > 0$， 则 $j \in V_1$.

在标记过程中，对每个 v_i 给三个不同的记号，第一个记号是下标 i；第二个记号用“ + ”或“ - ”，若

$c(i,j) - f(i,j) > 0$ 则记为“ + ”，若 $f(j,i) > 0$ 则记为“ - ”；第三个记号为增大的流值. 这里是想通过 v_j 来检查 v_i. 增广过程是使沿增广路的流增加.

标记法确定最大流的具体方法步骤如下：

(A) 标记过程

A_1：源 x 标记为$(x.\ tif, +, \varepsilon(x) = \infty)$，这时 x 称为被标记，未检查. 其余结点则称为未标记，未检查.

A_2：任选一个已标记未检查的结点 i，若 j 与 i 关联且尚未标记，则当

Ⅰ. $(i,j) \in U$，$c(i,j) > f(i,j)$时，将 j 标上$(x.\ tif, +, \varepsilon(j))$.

$\varepsilon(j) = \min\ \{\varepsilon(i),\ c(i,j) - f(i,j)\}$，称 j 已标记，未检查.

Ⅱ. $(j,i) \in U$，$f(j,i) > 0$ 时，将 j 标上$(i, -, \varepsilon(j))$.

$\varepsilon(j) = \min\ \{\varepsilon(i),\ f(j,i)\}$，称 j 已标记，未检查.

Ⅲ. 与结点 i 关联的结点都被标记后，将 i 的第二个记号“ + ”或“ - ”用一个小圆圈圈起来，称 i 已被标记且已被检查.

A_3：重复 A_2，如果汇 y 已被标记，转向增广过程，直至不再有结点可以被

标记，算法结束.

（B）增广过程

B_1：令 $z=y$ 转 B_2.

B_2：若 z 的标记为($s.\ tif$，+，ε)，则把 $f(s,z)$ 增加 $\varepsilon(y)$.

若 z 的标记为(s，-，ε)，则把 $f(z,s)$ 减小 $\varepsilon(y)$.

B_3：若 $s=x$，把全部标记去掉，回到标记过程 A，否则令 $z=s$ 回到 B_2.

例　用标记法求下图 4－59(a)所示的网络的最大流.

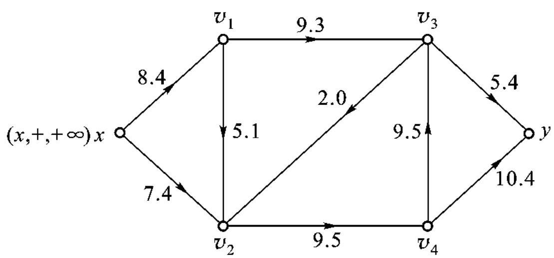


图 4－59(a)

解　用 1，2，3，4 表示 v_1，v_2，v_3，v_4.

x 记成($x.\ tif$，+，∞)，与 x 邻接的 1，2.

对 1，$(x,1)\in U$，$c(x,1)=8$，$f(x,1)=4$，

$\varepsilon(1)=\min\{\infty, c-f\}=4$，于是 2 标成($x.\ tif$，+，4).

对 2，$(x,2)\in U$ 且 $c(x,2)=7$，$f(x,2)=4$，

$\varepsilon(2)=\min\{\infty, c-f\}=3$，于是 2 标成($x.\ tif$，+，3)图 4－59(b).

与 x 关联的结点均被标记，故 x 标记中的记号“＋”用○圈起来，于是 x 被标记且被检查.

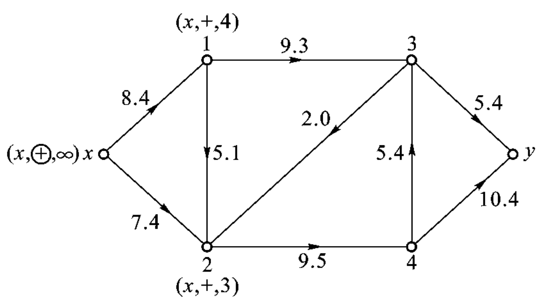


图 4－59(b)

继续上面过程：

与 v_1 邻接的点 v_3，$c(1,3)=9$，$f(1,3)=3$，$\varepsilon(3)=\min\{\varepsilon(1), c-f\}$ ＝

$\min\{4, 9-3\}=4$，结点 3 被标记成(1. tif，+，4).

与 v_2 邻接的点为 v_4，$c(2,4)=9$，$f(2,4)=5$，$\varepsilon(4)=\min\{\varepsilon(2), c-f\}=\min\{3, 9-5\}=3$，结点 4 被标记成(2. tif，+，3).

此时结点 1，2 被标记且被检查.

与 v_4 邻接的点 y，$c(4,y)=10$，$f(4,y)=4$，$\varepsilon(y)=\min\{\varepsilon(4), c-f\}=\min\{3, 10-4\}=3$，$y$ 被标记成(4. tif，+，3)；此时 4 被检查. 上述也可从 v_3 考虑去做.

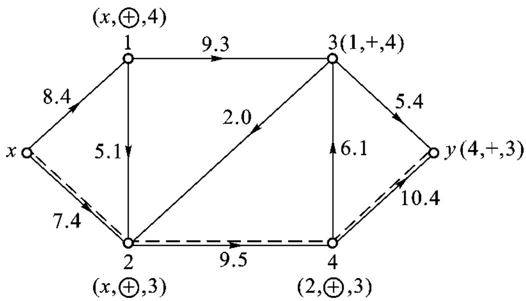


图 4－59(c)

由标记过程得到一条作为可增广路，x，v_2，v_4，y. 上图 4－59(c)虚线.

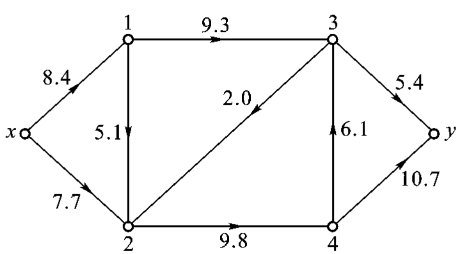
令 $v_4=y$

y 的标记为(4. tif，+，3)，故把$(4,y)$上的流值增加 $\varepsilon(y)=3$. 依次(令 $v_2=y$)把边$(2,4)$，$(x,2)$上的流值增加 3.

去掉全部标记，得一(新)网络图 4－60. 再回到标记过程.

对图 4－60 继续标记过程和增广过程可得图 4－61.

由图 4－64 可见网络不再具有可增广路，且可以看出 $V_1=\{x, v_1, v_2, v_3\}$，$c(V_1, V_2)=14$，故所求最大流为 $\max f_{xy}=14$.



图图 4－6260

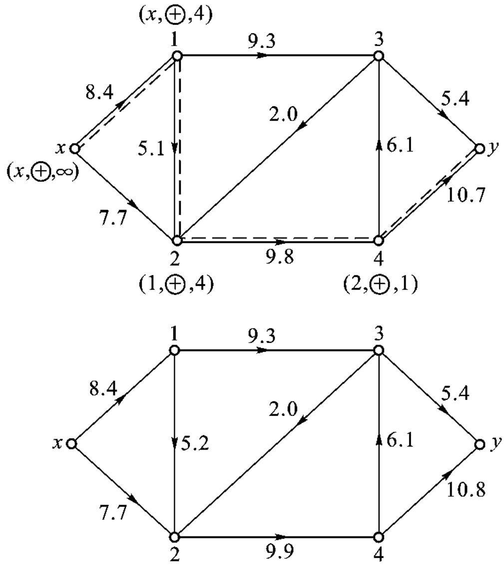


图 4－61

对图 4－61 **标记，增广得图** 4－62.

对图 4－62 **继续标记，增广得图** 4－63.

对图 4－63 **进行标记得图** 4－64.

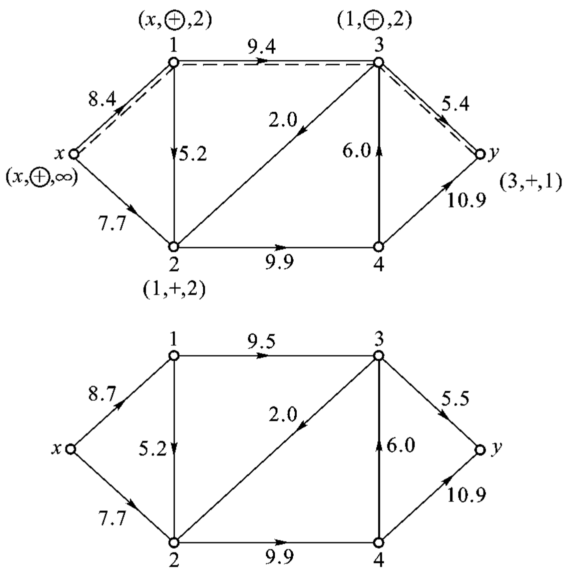


图 4－63

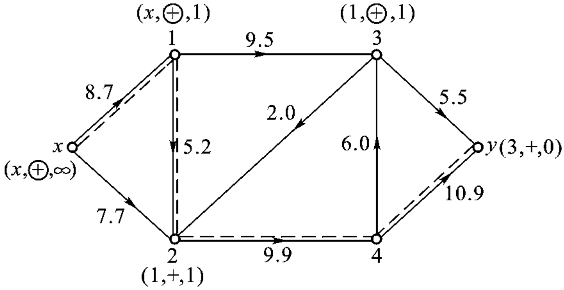


图 4－64

练习题 4－6

1. 求如图 4－65 所示网络由 x 到 y 的最大流 f_{xy}.
2. 求如图 4－66 所示网络由 x 到 y 的最大流 f_{xy}.

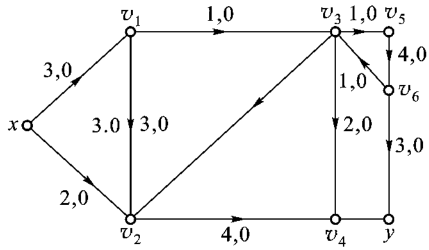


图 4-65

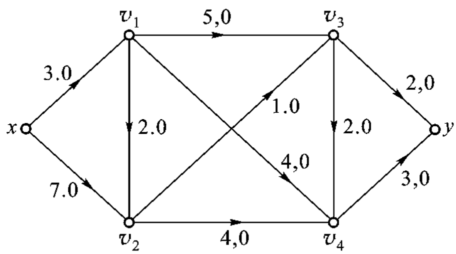


图 4-66

第七节　最短路与最小树问题

本节作为应用问题介绍网络的最短路及最小(生成)树及其求法.

一、最短路问题

设 H 是赋权图 G 的子图，H 的权(或称 H 的长)是它的每条边上的权的和记作 $l(H)$，即

$$l(H)=\sum_{e\in E(H)}l(e).$$

所有(v_i,v_j)通路中权(长)为最小的通路称为由 v_i 到 v_j 的最短路. 从 v_i 到 v_j 的最短路的权记作 $d(v_i,v_j)$.

假定 $l(v_i,v_j)=l_{ij}\geqslant 0$，若 v_i 与 v_j 不邻接，$l(v_i,v_j)=l_{ij}=+\infty$；$l(v_i,v_i)=l_{ii}=0$.

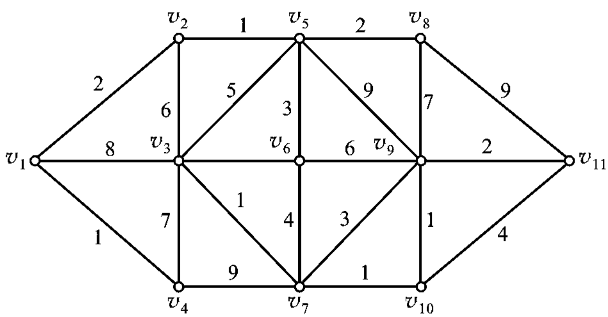
这里我们只介绍从一个始点 v_1 到一个终点 v_n 的最短路问题的求法. 其他情况请参阅有关运筹学方面的著作.

这里介绍的算法是由 Dijkstra 于 1959 提出的，即标号法.

标号法的基本思想是：所有结点都标号. 标号分两类；一类称为 T 标号(临时标号)，即从 v_1 到被标号的结点 v_s 的权的上界，记为 $d_T(v_s)=l_{1s}$，$s=2$， 3，…，n. 另一类称为 P 标号（固定标号）v_1 从到 v_s 的最短路的权（长）. 记 $d_P(v_1)=0$. 开始时 $d_P(v_1)=0$，对 $j\neq 1$ 的 v_j 标上 $d_T(v_j)=l_{1j}$，然后设法将 T 标号变成 P 标号，直到没有 T 标号为止.

标号法求最短路的方法是：

在所有 T 标号中取权（长）最小者，如 $d_T(v_{j_0})=l_{1j_0}$，则 v_{j_0} 的 T 标号改为 P 标号，并重新计算具有 T 标号的其他各结点的 T 标号：选 v_j 的 T 标号 $d_T(v_j)$ 与 $d_T(v_{j_0})+l_{j_0j}$ 中较小者为 v_j 的新 T 标号.



设 $P=\{v_j \mid v_j$ 具有 P 标号$\}$，$T=\{v_j \mid v_j$ 具有 T 标号$\}=V-P=V$

图 4-67

令 $d_P(v_k)=\min\limits_{v_j\in T}\{d_T(v_j)\}$，为结点 v_k 的 P 标号，于是 $v_k\in P$，把 $T\setminus\{v_k\}$ 中的结点

$d_T(v_j)=\min\{d_T(v_j),\ d_P(v_k)+l_{kj}\}$.

重复进行，直到 $v_n\in P$，这时 $d(v_n)$ 便是从 v_1 到 v_n 的最短路长.

通常用标号法寻求最短路要经过几轮甚至更多的反复标号才能完成，对运算

例 1 求如图 4-67 所示网络由 v_1 到 v_{11} 的最短路.

解 第一轮（T）标号：

Z（Z】 $d_P(v_1)=0$.

$d_T(v_2)=l_{12}=2$.

$d_T(v_3)=l_{13}=8$.

$d_T(v_4)=l_{14}=1$.

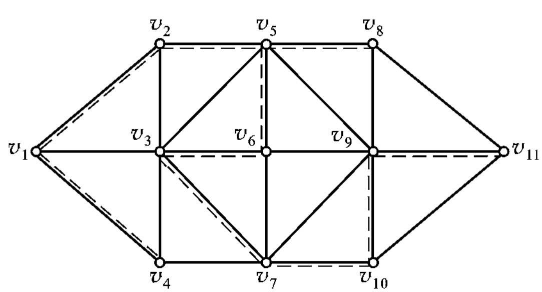
$d_T(v_j)=\infty$，$j=5$，6，…

比较可见：

$d_T(v_4)=\min\limits_{v_j\in T}\{d_T(v_j)\}=d_P(v_4)=1$.

第一轮标号结束，v_4 变成 P 标号，即 $v_4\in P$，再进行下轮（重新）标号.

第二轮（T）标号



$d_T(v_2)=\min\{d_T(v_2),\ d_P(v_4)+l_{42}\}=\min\{2,\infty\}=2.$

$d_T(v_3)=\min\{d_T(v_3),\ d_P(v_4)+l_{43}\}=\min\{8,1+7\}=8.$

$d_T(v_7)=\min\{d_T(v_7),\ d_P(v_4)+l_{47}\}=\min\{\infty,1+9\}=10.$

对其他 $v_j\in T$ **由于不与** v_4 **邻接，故** $d_T(v_j)=\infty$. **比较知：**

$d_T(v_2)=\min\limits_{j\in T}\{d_T(v_j)\}=d_P(v_2)=2.$

v_2 **变成** P **标号，此时** v_1，v_4，$v_2\in P$. **第二轮标号结束.**

第三轮(T)标号

$d_T(v_3)=\min\{d_T(v_3),\ d_P(v_2)+l_{23}\}=\min\{8,2+6\}=8.$

$d_T(v_5)=\min\{d_T(v_5),\ d_P(v_2)+l_{25}\}=\min\{\infty,2+1\}=3.$

$d_T(v_7)=\min\{d_T(v_7),\ d_P(v_2)+l_{27}\}=\min\{10,\infty\}=10.$

对其他 $v_j\in T$**，故** $d_T(v_j)=\infty$. **比较知：**

$d_T(v_5)=\min\limits_{j\in T}\{d_T(v_j)\}=d_P(v_5)=3.$

v_5 **变成** P **标号，此时** v_1，v_4，v_2，$v_5\in P$. **第三轮标号结束.**

第四轮(T)标号

$d_T(v_3)=\min\{d_T(v_3),\ d_P(v_5)+l_{53}\}=\min\{8,3+5\}=8.$

$d_T(v_6)=\min\{d_T(v_6),\ d_P(v_5)+l_{56}\}=\min\{\infty,3+3\}=6.$

$d_T(v_7)=\min\{d_T(v_7),\ d_P(v_5)+l_{57}\}=\min\{10,\infty\}=10.$

$d_T(v_8)=\min\{d_T(v_8),\ d_P(v_5)+l_{58}\}=\min\{\infty,3+2\}=5.$

$d_T(v_9)=\min\{d_T(v_9),\ d_P(v_5)+l_{59}\}=\min\{\infty,3+9\}=12.$

对其他 $v_j\in T$**，故** $d_T(v_j)=\infty$. **比较知：**

$d_T(v_8)=\min\limits_{j\in T}\{d_T(v_j)\}=d_P(v_8)=5.$

v_8 **变成** P **标号，此时** v_1，v_4，v_2，v_5，$v_8\in P$. **第四轮标号结束.**

第五轮(T)标号

$d_T(v_3)=\min\{d_T(v_3),\ d_P(v_8)+l_{83}\}=\min\{8,\infty\}=8.$

$d_T(v_6)=\min\{d_T(v_6),\ d_P(v_8)+l_{86}\}=\min\{6,\infty\}=6.$

$d_T(v_7)=\min\{d_T(v_7),\ d_P(v_8)+l_{87}\}=\min\{10,\infty\}=10.$

$d_T(v_9)=\min\{d_T(v_9),\ d_P(v_8)+l_{89}\}=\min\{\infty,5+7\}=12.$

$d_T(v_{10})=\infty.$

$d_T(v_{11})=\min\{d_T(v_{11}),\ d_P(v_8)+l_{811}\}=\min\{\infty,5+9\}=14.$

对其他 $v_j\in T$**，故** $d_T(v_j)=\infty$. **比较知：**

$d_T(v_6)=\min\limits_{j\in T}\{d_T(v_j)\}=d_P(v_6)=6.$

v_6 **变成** P **标号，此时** v_1，v_4，v_2，v_5，v_8，$v_6\in P$. **第五轮标号结束.**

第六轮(T)标号

$d_T(v_3)=\min\{d_T(v_3),\ d_P(v_6)+l_{63}\}=\min\{8,6+1\}=7$

$d_T(v_5)=\min\{d_T(v_5),\ d_P(v_6)+l_{65}\}=\min\{3,6+3\}=3.$

$d_T(v_7)=\min\{d_T(v_7),\ d_P(v_6)+l_{67}\}=\min\{10,6+4\}=10.$

$d_T(v_9)=\min\{d_T(v_9),\ d_P(v_6)+l_{69}\}=\min\{12,6+6\}=12.$

$d_T(v_{10})=\infty.$

$d_T(v_{11})=\min\{d_T(v_{11}),\ d_P(v_6)+l_{611}\}=\min\{14,\infty\}=14$

v_1 到 v_{11}（按 P 标号顺序）有一条通路 v_1，v_2，v_5，v_6，v_3，v_7，v_{10}，v_9，v_{11}，此即为所求之最短路，且 $d_P(v_{11})$

二、最小（生成）树及求法

定义　T^* 是赋权图 G 的一棵生成树，若对任一 G 的生成树 T 有 $l(T^*)\leqslant l(T)$，则称 T^* 是 G 的最小生成树.

最小生成树的求法：

把 G 的边按权的递增顺序排列

$l(a_1)\leqslant l(a_2)\leqslant\cdots\leqslant l(a_q)$，

取 $e_1=a_1$，$e_2=a_2$，检查 a_3. 若 a_3 与 e_1，e_2 不构成回路，则取 $e_3=a_3$；若 a_3 与 e_1，e_2 构成回路，则放弃 a_3 检查 a_4；若 a_4 与 e_1，e_2 不构成回路，则取 $e_3=a_4$，否则放弃 a_4. 如此下去，直到找出 e_1，e_2，…，e_{p-1} 条边的连通图为止，则 $\{e_1,e_2,\cdots,e_{p-1}\}$ 就是所求.

例 2　求图 4－69 的最小生成树.

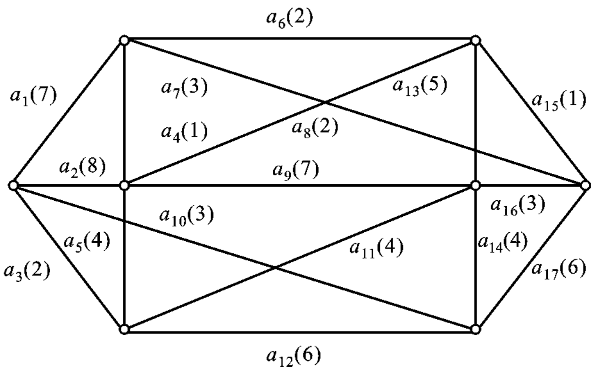


图 4－69

解　按权由小到大，边序也是由小到大排列有

$a_4(1)$，$a_{15}(1)$，$a_3(2)$，$a_6(2)$，$a_8(2)$，$a_7(3)$，$a_{10}(3)$，$a_{16}(3)$，$a_5(4)$，$a_{11}(4)$，$a_{14}(4)$，$a_{13}(5)$，$a_{12}(6)$，$a_{17}(6)$，$a_1(7)$，$a_9(7)$，$a_2(8)$.

取 $e_1=a_4$，$e_2=a_{15}$，$e_3=a_3$，$e_4=a_6$，$e_5=a_{10}$，$e_6=a_{16}$，$e_7=a_5$，则得图 4－69 的一棵最小生成树，且其权为 16.

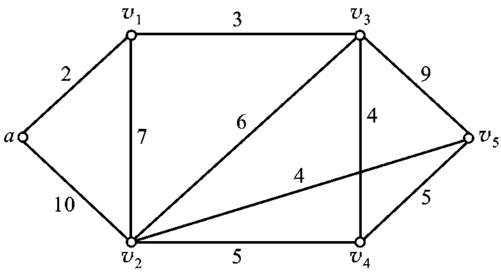
取 $e_1=a_4$，$e_2=a_{15}$，$e_3=a_3$，$e_4=a_8$，$e_5=a_{10}$，$e_6=a_{16}$，$e_7=a_{14}$ 则得图 4－69 的又一棵最小生成树，且权为 16.

可见图 G 的最小生成树不惟一，但他们的权是一致的.

练习题 4－7

1. 用 Dijkstra 算法求图 4－70 中从 a 点到其他各结点的最短路.

图 4－70



2. 求图 4－71 中 3 个图的最小生成树

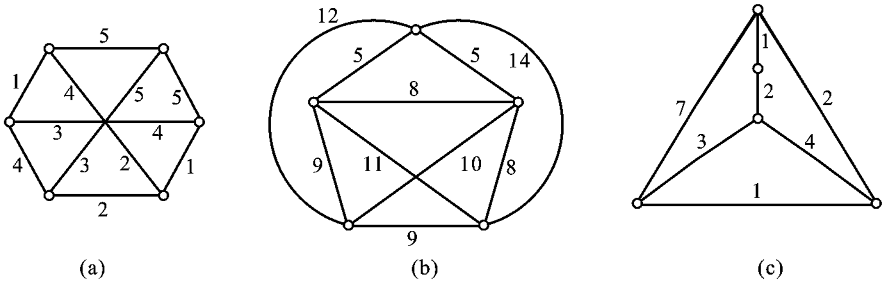


图 4－71

复 习 题 四

1. 画出图 4－72 的相对于完全图的补图.

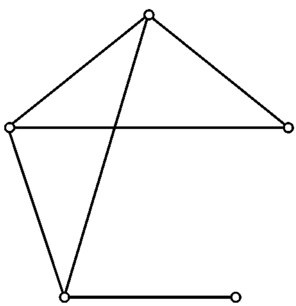


图 4－72

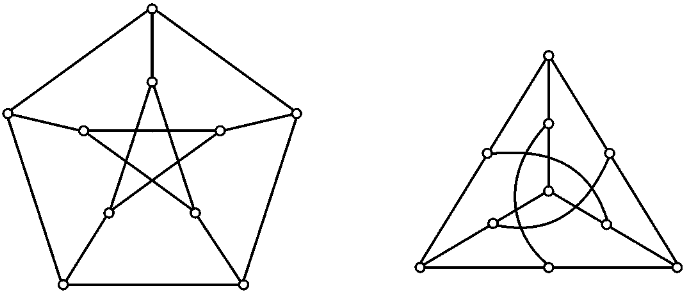
2. 证明图 4－73 中两个图是同构的.

图 4－73

3. 证明在 n 个结点的有向简单图中最多只有 $n(n-1)$ 条边.

4. 证明在 n 个结点的简单无向图中，至少有两个结点次数相同，这里 $n\geqslant 2$.

5. 在无向图 G 中，从结点 u 到结点 v 有一条长度为偶数的路径，从结点 u 到结点 v 又



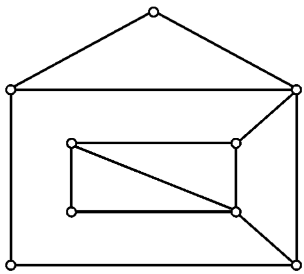
(a) (b)

有一条长度为奇数的路径，则在 G 中必有一条长度为奇数的回路.

6. 若无向图 G 中恰有两个结点次数为奇数，则这两个结点间必有一条路径.

7. 若图 G 是不连通的，则 G 的补图 $\overline{G}$ 是连通的.

图 4－74



8. 构造一个欧拉图，其结点数 n 和边数 m 满足下述条件.

（1） n，m 的奇偶性一样.

（2） n，m 的奇偶性相反.

如果不能，说明原因.

9. 设 G 是一个具有 k 个奇次数结点的图，问最少加几条边到 G 中，而使所得的图有一条欧拉回路，说明对于图 4－74 如何能做到这一点.

10.（1） 画一个有一条欧拉回路和一条哈密顿回路的图.

（2） 画一个有一条欧拉回路，但没有一条哈密顿回路的图.

（3） 画一个没有一条欧拉回路，但有一条哈密顿回路的图.

11. 判断图 4－75 中是否有哈密顿回路.

12. 求出图 4－76 中有向图的邻接矩阵 $\boldsymbol{A}$，找出从结点 v_1 到结点 v_4 长度为 2 和 4 的路径，用计算 $\boldsymbol{A}^2$，$\boldsymbol{A}^3$ 和 $\boldsymbol{A}^4$ 来验证这结论.

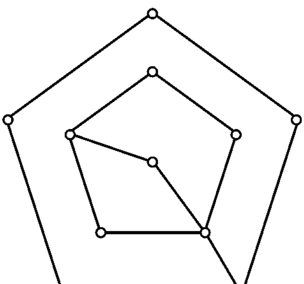


图 4－75

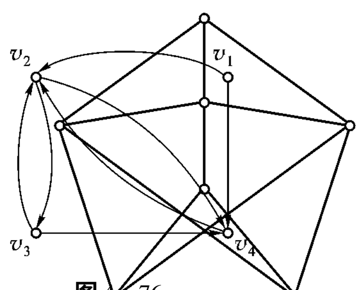


图 4－76

图 4－77

13. 证明在一个(6,12)的连通平面简单图中，每个区

域用三条边围成.

14. 证明图 4－77 是非平面图.

15. 设 G 为 11 个或更多个结点的图，证明 G 或 $\overline{G}$ 是非平面图.

16. 证明在完全二元树中，边的总数等于 $2(n_i-1)$，式中 n_i 是叶数.

17. 证明有 n 个结点的树，其结点次数之和为 $2n-2$.

18. 如何由无向图 G 的邻接矩阵判断 G 是不是二部图.

19. n 个城市用 K 条公路的网络连接（一条公路定义为两个城市间的一条不穿过任何中间城市的道路）. 证明：如果 $k>\dfrac{(n-1)(n-2)}{2}$，则人们总能通过连接的公路，在任何两个城市间旅行.

20. 试用有向图描述下述问题的解决路径：

某人 m 带一条狗 d，一只猫 c 和一只兔子 r 过河，没有船只. 他每次游过河时只能带一只动物，当没人管理时，狗和兔子不能相处，猫和兔子也不能相处. 在这些条件的约束下，他怎样才能将三只动物从左岸带往右岸？（提示：用结点表示状态，例如初始状态可记为 $\langle\{m,d,c,r\},\varnothing\rangle$，人和兔子过河后的状态可记为 $\langle\{d,c\},\{m,r\}\rangle$，若从状态 S_1 可变为状态 S_2，则从结点 S_1 画一条弧到结点 S_2）.

21. 画出求运输网络最大的逻辑框图.

22. 画出计算最短路（Dijkstra）算法的逻辑框图.

第五章　数理逻辑

数理逻辑是研究推理的数学分支. 创始人是 17 世纪的德国数学家、哲学家莱布尼茨. 他是用数学方法研究抽象思维. 数理逻辑与计算机科学有着密切的关系，它已成为计算机科学的基础理论. 在提高计算机的工作效率，研究计算机实现哪些思维过程等方面，数理逻辑起到了重要的作用.

数理逻辑包括证明论、模型论、递归论、公理化集合论、命题逻辑和谓词逻辑.

本章主要介绍数理逻辑的基础：命题逻辑和谓词逻辑.

第一节　命题及联结词

一、命题

数理逻辑又称符号逻辑，它是用数学方法去研究抽象思维的规律的应用学科，研究抽象思维的中心问题是推理，推理必须包含前提和结论，而前提和结论又都是由陈述句组成的. 因此，陈述句是推理的基本要素. 我们把能判断真假的陈述句称为命题. 作为命题的陈述句表达的判断结果称为命题的真值. 真值只能取两个值：真或假. 真值为真的命题称为真命题，真值为假的命题称为假命题. 真和假分别用 1 和 0 表示，或者分别用符号 T 和 F 表示.

怎样判断给定的句子是否为命题呢？首先判断它是否为陈述句，其次判断它是否有惟一的真值. 即有惟一真值的陈述句为命题.

例 1　判断下列句子是否为命题

（1） 请勿吸烟！

（2） 您今天上网了吗？

（3） $x-y>1$.

（4） 火星上有生物.

（5） 人类战胜非典了吗？

（6）雪是黑的.

（7）这束花真好看啊！

（8）本命题是假的.

（9）我正在说假话.

在上面这些例子中，(1)是祈使句，(2)、(5)是疑问句，(7)是感叹句，因而(1)、(2)、(5)、(7)都不是命题. 剩下的5个句子都是陈述句，(3)无法确定真值，根据x，y的不同取值情况它可真可假，即无惟一的真值，因此不是命题. (8)、(9)是悖论，凡是悖论都不是命题. (4)、(6)是命题. (6)是假命题. 虽然今天我们还不知道(4)的真值，但它的真值客观存在，而且是惟一的，随着科学技术发展，不久的将来就会知道(4)的真值.

在数理逻辑中，我们用大写字母P，Q，…，A，B，…，或加下标的大写字母P_1，Q_1，…表示命题. 表示命题的符号称为命题的标识符. 在例1中，用P，Q分别表示(4)，(6)中命题，称为这些命题的符号化，其表示方法为：

P：火星上有生物.

Q：雪是黑的.

其中Q的真值为0，P的真值暂时不知道. 在例1中的命题(4)、(6)都是简单陈述句，它们都不能被分解成更简单的陈述句. 我们把不能再分解成其他命题的命题称为原子命题. 由若干个原子命题经过联结词复合而成的陈述句，称为复合命题. 例如：如果天下大雨，那么他乘班车上班. 天下大雨与他乘班车上班是两个原子命题，经过联结词如果…，那么…，复合构成一个复合命题.

二、联结词

在自然语言中，常用的联结词有："非"、"并且"、"或"、"如果…，那么…"、"当且仅当"等. 但自然语言中出现的联结词有的具有二义性，而在命题逻辑中必须给出联结词的确切定义，并且将它们符号化.

定义1　设P为命题，复合命题"非P"（或"P的否定"）称为P的否定式，记作$\square P$，符号$\square$称为否定联结词，并规定$\square P$为T当且仅当P为F.

例2　P：吉林市在吉林省，则$\square P$：吉林市不在吉林省.

定义2　设P，Q为两个命题，复合命题"P并且Q"（或"P与Q"）称为P与Q的合取式，记作$P \wedge Q$，$\wedge$称为合取联结词，并规定当且仅当P，Q同时为T时，$P \wedge Q$为T，其余情况，$P \wedge Q$为F.

在自然语言中的"虽然…，但是…"，"不仅…，而且…"，"既…，又…"，"一面…，一面…"等联结词都可以符号化为$\wedge$. 但是不要见到"与"或"和"就使用联结词$\wedge$.

例3　将下列命题符号化：

（1） 马华既聪明又用功.

（2） 马华虽然聪明，但不用功.

（3） 赵海与赵波是兄弟.

解 首先将原子命题符号化：

P：马华聪明.

Q：马华用功.

则（1）可符号化为 $P \wedge Q$.

（2） 可符号化为 $P \wedge \square Q$.

在（3）中，虽然使用了联结词“与”，但是它是联结该句主语的，而整个句子仍是简单陈述句，所以（3）是原子命题. 可符号化为 R. 即

R：赵海与赵波是兄弟.

定义 3 设 P，Q 为两个命题，复合命题“P 或 Q”称为 P 与 Q 的析取式，记作 $P \vee Q$，$\vee$ 称为析取联结词. 当且仅当 P，Q 同时为 F 时，$P \vee Q$ 的真值为 F，否则 $P \vee Q$ 的真值为 T.

从上述定义可以看出，析取联结词与自然语言中的“或”有些相似，但是在自然语言中的“或”具有二义性. 用“或”联结的命题有时具有相容性，有时具有排斥性. 所以在使用联结词 $\vee$ 时要注意区分. 析取联结词 $\vee$ 所表示的“或”是具有相容性的，凡是具有排斥性的“或”都不能用析取联结词.

例 4 将下列命题符号化.

（1） 王强爱唱歌或爱跳舞.

（2） 张莉在教室里上课或参加长跑比赛.

（3） 他做了十道或二十道习题.

解 P：王强爱唱歌

Q：王强爱跳舞

显然（1）中“或”为相容（可兼）或，即 P 与 Q 可以同时为真，符号化为 $P \vee Q$.

（2） R：张莉在教室里上课.

S：张莉参加长跑比赛.

显然（2）中“或”具有排斥性，R 和 S 是不可能同时成立. 因此该命题不可符号化为 $R \vee S$，而应为 $(R \wedge \square S) \vee (\square R \wedge S)$.

（3） 中“或”只表示大约的意思，不能用联结词 $\vee$. （3）是一个原子命题，可符号化为 A.

定义 4 设 P，Q 为两个命题，复合命题“如果 P，则 Q”称为 P 与 Q 的蕴含式，记作 $P \to Q$，称 P 是蕴含式的前件，Q 为蕴含式的后件，$\to$ 称作蕴含联结词. 并规定 $P \to Q$ 为 F 当且仅当 P 为 T，Q 为 F，其余情况 $P \to Q$ 的真值为 T. $P \to Q$ 的逻辑关系为 Q 是 P 的必要条件.

在使用联结词→时，叙述为“只要 P 就 Q”，“P 仅当 Q”，“因为 P，所以 Q”，“只有 Q 才 P”，“除非 Q 才 P”，“除非 Q，否则非 P”，等等，都可以符号化为 $P \to Q$. 在自然语言中，“如果 P，则 Q”等叙述中的 P 和 Q 往往有因果关系，否则就没有意义了. 但是在数理逻辑中，P 与 Q 可以无任何内在联系.

例 5　将下列命题符号化，并指出各复合命题的真值.

(1) 如果雪是白色的，则 $1+2=3$.

(2) 如果雪不是白色的，则 $1+2=3$.

(3) 只有 $1+2\neq 3$，雪才不是白色的.

(4) 除非 $1+2=3$，否则雪不是白色的.

(5) 除非 $1+2\neq 3$，雪才是白色的.

解　设 P：雪是白色的，P 的真值为 T.

Q：$1+2=3$，Q 的真值为 T.

(1)到(5)的符号化分别为 $P\to Q$，$\square P\to Q$，$\square P\to \square Q$，$\square P\to Q$，$P\to \square Q$.

这五个复合命题的真值分别为 T，T，T，T，F.

定义 5　设 P，Q 为两个命题，复合命题“P 当且仅当 Q”称为 P 与 Q 的等价式，记作 $P\leftrightarrow Q$，↔称为等价联结词. 当 P 与 Q 的真值相同时，$P\leftrightarrow Q$ 的真值为 T，否则 $P\leftrightarrow Q$ 的真值为 F.

$P\leftrightarrow Q$ 的逻辑关系为 P 与 Q 互为充分必要条件.

例 6　将下列命题符号化.

(1) 美国位于欧洲当且仅当 $1+2=4$.

(2) 小华心情愉快时，她就唱歌. 反之，当她唱歌时，一定心情愉快.

解　(1) 设 P：美国位于欧洲.

Q：$1+2=4$.

则(1)符号化为 $P\leftrightarrow Q$.

(2) 设 R：小华心情愉快.

S：小华唱歌.

则：(2)符号化为 $R\leftrightarrow S$

例 7　设有命题 P，Q，R 分别为：

P：小王是大学生.

Q：小刘是中共党员.

R：小李是三好学生.

写出命题 $P\wedge Q$，$Q\vee R$，$(P\wedge R)\to Q$，$P\leftrightarrow R$.

解　$P\wedge Q$：小王是大学生且小刘是中共党员.

$Q\vee R$：小刘是中共党员或小李是三好学生.

$(P\wedge R)\to Q$：如果小王是大学生且小李是三好学生，则小刘是中共党员.

$P\leftrightarrow R$：小王是大学生当且仅当小李是三好学生.

以上定义了五种最常用、也是最重要的联结词，即□，$\wedge$，$\vee$，$\rightarrow$，$\leftrightarrow$. 其中称□为一元联结词，其余联结词都称作二元联结词. 下面给出由原子命题和联结词组成复合命题的取值情况列于表 5－1.

表 5－1

P　Q	□P	$P\wedge Q$	$P\vee Q$	$P\rightarrow Q$	$P\leftrightarrow Q$
F　F	T	F	F	T	T
F　T	T	F	T	T	F
T　F	F	F	T	F	F
T　T	F	T	T	T	T

练习题 5－1

1. 分析下列句子哪些是命题？哪些不是命题？指出其真值.

（1）$\sqrt{3}$是无理数.

（2）0 不是自然数.

（3）2 是素数或 4 是素数.

（4）请大家不要说话！

（5）$x+y<1$.

（6）这个函数可微当且仅当它可导.

（7）调和级数收敛.

（8）明天你去上网吗？

（9）$1+11=100$.

（10）2006 年元旦下雪.

（11）今天天气多么好啊！

2. 将下列命题符号化.

（1）煤球不是黑的.

（2）因为天气冷，所以我穿了毛衣.

（3）不经一事，不长一智.

（4）“人不犯我，我不犯人；人若犯我，我必犯人”.

（5）除非天下大雨，否则他骑自行车上班.

（6）刘洋与刘海是兄弟.

（7）6 是奇数的充分必要条件是 8 能被 3 整除.

（8）天不刮风，天不下雨，天中有太阳.

（9）他一面吃饭，一面听英语广播.

（10）王老师在 201 室或 202 室上课.

3. 将下列复合命题分成若干原子命题.

（1）张丽是上海人或北京人.

（2）我既不看电视，也不去看电影，我准备去打球.

（3）2 不是素数当且仅当 5 大于 6.

4. 试给出四个语句，符号化后是合取式、析取式、蕴含式和等价式.

第二节　命题公式及公式的等值和蕴含关系

在上节中，我们介绍了 5 种命题联结词. 还把不含任何联结词的命题称作原子命题，至少包含一个联结词的命题称作复合命题. 原子命题的真值是惟一的，所以也称原子命题为命题常项或命题常元. 真值可以变化的陈述句称作命题变项或命题变元. 命题常元和命题变元仍用大写字母或加下标的大写字母表示.

一、命题公式

由命题变元，联结词和圆括号按一定规则组成的符号串称作合式公式.

定义 1　命题公式是由下列规则所产生的符号串：

（1）单一命题变元本身是一个合式公式.

（2）如果 A 是合式公式，则$\square A$ 是合式公式.

（3）如果 A 和 B 是合式公式，则 $A\wedge B$，$A\vee B$，$A\rightarrow B$，$A\leftrightarrow B$ 都是合式公式.

（4）只有有限次地应用(1)，(2)，(3)，所产生的符号串才是合式公式.

合式公式也称命题公式，简称公式.

下列各式都是命题公式：

$$P\rightarrow(P\vee Q)，((P\rightarrow Q)\rightarrow R)，(R\rightarrow Q)\rightarrow R，(\square P\rightarrow(Q\wedge R)\vee S).$$

在合式公式中，规定最外层括号可以省略，联结词运算的优先次序规定为：

$$\square，\wedge，\vee，\rightarrow，\leftrightarrow，$$

则上述公式可以写成：

$$P\rightarrow P\vee Q，(P\rightarrow Q)\rightarrow R，(R\rightarrow Q)\rightarrow R，\square P\rightarrow Q\wedge R\vee S.$$

而　$PQ\wedge R$，$(P\rightarrow(Q\rightarrow R)$，$P\rightarrow Q\rightarrow R$，$\vee P$，$P\rightarrow$都不是命题公式.

命题公式不是命题. 只有在命题公式中，每个命题变元用指定的命题常元代替后，命题公式才能有确定的真值，成为命题.

例 1　设P：3 是奇数

Q：2 是偶数

R：$\sqrt{2}$是无理数

试把下列命题公式翻译成自然语言：

(1) $\neg(P \wedge Q)$

(2) $R \rightarrow (\neg P \wedge \neg Q)$

(3) $\neg P \vee \neg Q \leftrightarrow \neg R$

解　(1) 3 是奇数且 2 是偶数是不对的.

(2) 如果$\sqrt{2}$是无理数，则 3 不是奇数并且 2 不是偶数.

(3) 3 不是奇数或 2 不是偶数当且仅当$\sqrt{2}$不是无理数.

定义 2　设 A 为一命题公式，P_1，P_2，…，P_n 为出现在 A 中的所有命题变元，对 P_1，P_2，…，P_n 指定一组真值，称为对 A 的一种赋值或指派. 若指定一种指派使 A 的真值为 T，则称这组值为 A 的成真指派，若使 A 的真值为 F，则称这组值为 A 的成假指派.

由定义可知，具有 n 个命题变元的公式有 2^n 组不同的真值指派. 我们把命题公式 A 在所有指派下取值情况列成的表，称为命题公式 A 的真值表. 在真值表中，真值 T，F，分别用 1，0 代替.

例 2　试求下列公式的真值表

(1) $(P \rightarrow Q) \leftrightarrow \neg P \vee Q$

(2) $\neg(P \rightarrow Q) \wedge Q$

(3) $(P \wedge \neg Q) \rightarrow R$

解　(1) 表 5－2 $(P \rightarrow Q) \leftrightarrow \neg P \vee Q$ 的真值表：

表 5－2

P　Q	$\neg P$	$P \rightarrow Q$	$\neg P \vee Q$	$(P \rightarrow Q) \leftrightarrow \neg P \vee Q$
0　0	1	1	1	1
0　1	1	1	1	1
1　0	0	0	0	1
1　1	0	1	1	1

(2) 表 5－3 $\neg(P \rightarrow Q) \wedge Q$ 的真值表：

表 5－3

P　Q	$P \rightarrow Q$	$\neg(P \rightarrow Q)$	$\neg(P \rightarrow Q) \wedge Q$
0　0	1	0	0
0　1	1	0	0
1　0	0	1	0
1　1	1	0	0

（3）表 5－4 $(P \wedge \square Q) \rightarrow R$ 的真值表：

表 5－4

$P \quad Q \quad R$	$\square Q$	$P \wedge \square Q$	$(P \wedge \square Q) \rightarrow R$
0　0　0	1	0	1
0　0　1	1	0	1
0　1　0	0	0	1
0　1　1	0	0	1
1　0　0	1	1	0
1　0　1	1	1	1
1　1　0	0	0	1
1　1　1	0	0	1

从表 5－2 中，可见公式（1）的真值在任何指派下都为真；从表 5－3 中，可见公式（2）的真值在任何指派下都为假；而公式（3）的真值有真有假. 真值永为真和永为假的公式在今后的命题演算中极为重要.

定义 3　设 A 为一命题公式：

（1）若 A 在它的各种指派下取值均为真，则称 A 是重言式或永真式.

（2）若 A 在它的各种指派下取值均为假，则称 A 是矛盾式或永假式.

（3）若 A 不是矛盾式，则称 A 是可满足式.

由定义可以看出，重言式是可满足式，但是其逆命题不真，可满足式不一定是重言式，用真值表可以判断公式的类型.

例 3　用真值表判断下列公式的类型

（1）$(\square P \vee \square Q) \leftrightarrow \square(P \wedge Q)$

（2）$\square(P \vee Q) \wedge P$

解　（1）

表 5－5

$P \quad Q$	$\square P$	$\square Q$	$\square P \vee \square Q$	$P \wedge Q$	$\square(P \wedge Q)$	$(\square P \vee \square Q)$ $\leftrightarrow \square(P \wedge Q)$
0　0	1	1	1	0	1	1
0　1	1	0	1	0	1	1
1　0	0	1	1	0	1	1
1　1	0	0	0	1	0	1

从表 5－5 可以看出，不论命题变元的何种指派，命题公式 $(\square P \vee \square Q) \leftrightarrow$

$\neg(P \wedge Q)$的真值均为真，故是永真式.

（2） 表 5 - 6

P Q	$P \vee Q$	$\neg(P \vee Q)$	$\neg(P \vee Q) \wedge P$
0 0	0	1	0
0 1	1	0	0
1 0	1	0	0
1 1	1	0	0

从表 5 - 6 可以看出，不论命题变元的何种指派，命题公式$\neg(P \vee Q) \wedge P$的真值均为假. 故该公式是矛盾式. 从表 5 - 4 可知，公式$(P \wedge \neg Q) \to R$是非重言式的可满足式.

我们常把重言式记为 1，把矛盾式记为 0.

二、命题公式的等值式

对于 n 个命题变元，按合式公式的定义，可以形成无数多个命题公式. 这些公式的真值表是否有无穷多种不同的情况呢？答案是否定的. 例如当 $n=2$ 时，

$$P \to Q，\neg P \vee Q，(\neg P \vee Q) \wedge (\neg P \vee Q)，$$
$$\neg(P \wedge \neg Q)，\neg Q \to \neg P，\cdots$$

它们是不同的命题公式，但是它们在 4 个指派 00，01，10，11 下均有相同的真值. n 个命题变元有 2^n 个指派，每个公式在一种指派下，真值不是 0 就是 1. 所以含 n 个命题变元的公式的真值表只有 2^{n^2} 种不同的情况.

定义 4 设 A、B 是命题公式，若 $A \leftrightarrow B$ 是重言式，则称 A 与 B 为等值的，记作 $A \Leftrightarrow B$，读作 A 与 B 等值.

定义中的符号$\Leftrightarrow$不是联结词，它是用来表示 A 与 B 等值（$A \leftrightarrow B$ 是重言式）的一种记法. 所以 $A \Leftrightarrow B$ 不是公式，不要将$\Leftrightarrow$与$\leftrightarrow$混为一谈.

对于两个含有相同命题变元的公式 A 和 B，当 $A \Leftrightarrow B$ 时，公式 A 和 B 的真值表完全相同，反之也成立. 所以我们可以利用真值表来判断两个公式是否等值.

例 4 判断下列各组公式是否等值

（1）$(P \to Q) \to R$ 与 $P \to (Q \to R)$

（2）$P \vee (Q \wedge R)$ 与 $(P \vee Q) \wedge (P \vee R)$

解 设 A 表示 $(P \to Q) \to R$.

B 表示 $P \to (Q \to R)$.

C 表示 $P \vee (Q \wedge R)$.

D 表示 $(P \vee Q) \wedge (P \vee R)$.

列真值表如表 5－7

表 5－7

$P\ Q\ R$	$Q\wedge R$	$P\vee Q$	$P\vee R$	$P\rightarrow Q$	$Q\rightarrow R$	$A\ B\ C\ D$
0 0 0	0	0	0	1	1	0 1 0 0
0 0 1	0	0	1	1	1	1 1 0 0
0 1 0	0	1	0	1	0	0 1 0 0
0 1 1	1	1	1	1	1	1 1 1 1
1 0 0	0	1	1	0	1	1 1 1 1
1 0 1	0	1	1	0	1	1 1 1 1
1 1 0	0	1	1	1	0	0 0 1 1
1 1 1	1	1	1	1	1	1 1 1 1

从表 5－7 中可以看出 A 与 B 的真值表不同，因而 $(P\rightarrow Q)\rightarrow R$ 与 $P\rightarrow(Q\rightarrow R)$ 不等值，C 与 D 的真值表相同，所以 $P\vee(Q\wedge R)$ 与 $(P\vee Q)\wedge(P\vee R)$ 等值，即 $P\vee(Q\wedge R)\Leftrightarrow(P\vee Q)\wedge(P\vee R)$.

对于命题公式 A，B，C，有下面性质：

（1） 自反性：$A\Leftrightarrow A$.

（2） 对称性：若 $A\Leftrightarrow B$，则 $B\Leftrightarrow A$.

（3） 传递性：若 $A\Leftrightarrow B$，并且 $B\Leftrightarrow C$，则 $A\Leftrightarrow C$.

以上性质请读者给出证明.

我们用真值表法可以判断任何两个公式是否等值，但当命题变元较多时，工作量很大，所以本书列出了非常重要的等值式，希望读者牢记它们.

表 5－8

1. 双重否定律	$\square\square A\Leftrightarrow A$
2. 幂等律	$A\vee A\Leftrightarrow A$，$A\wedge A\Leftrightarrow A$
3. 结合律	$(A\vee B)\vee C\Leftrightarrow A\vee(B\vee C)$，$(A\wedge B)\wedge C\Leftrightarrow A\wedge(B\wedge C)$
4. 交换律	$A\vee B\Leftrightarrow B\vee A$，$A\wedge B\Leftrightarrow B\wedge A$
5. 分配律	$A\vee(B\wedge C)\Leftrightarrow(A\vee B)\wedge(A\vee C)$，$A\wedge(B\vee C)\Leftrightarrow(A\wedge B)\vee(A\wedge C)$
6. 吸收律	$A\vee(A\wedge B)\Leftrightarrow A$，$A\wedge(A\vee B)\Leftrightarrow A$
7. 德·摩根律	$\square(A\vee B)\Leftrightarrow\square A\wedge\square B$，$\square(A\wedge B)\Leftrightarrow\square A\vee\square B$
8. 同一律	$A\vee 0\Leftrightarrow A$，$A\wedge 1\Leftrightarrow A$
9. 零律	$A\vee 1\Leftrightarrow 1$，$A\wedge 0\Leftrightarrow 0$
10. 互否律	$A\vee\square A\Leftrightarrow 1$，$A\wedge\square A\Leftrightarrow 0$
11. 蕴含等值式	$A\rightarrow B\Leftrightarrow\square A\vee B$
12. 等价等值式	$A\leftrightarrow B\Leftrightarrow(A\rightarrow B)\wedge(B\rightarrow A)$
13. 假言易位	$A\rightarrow B\Leftrightarrow\square B\rightarrow\square A$
14. 等价否定等值式	$A\leftrightarrow B\Leftrightarrow\square A\leftrightarrow\square B$

15.	归谬论	$(A\rightarrow B)\wedge(A\rightarrow\Box B)\Leftrightarrow\Box A$

表 5－8 给出了 15 组 24 个重要等值式，也称命题定律. 这些等值式都可以用真值表的方法证明. 其中 A，B，C 可以代表任意的命题公式.

设 A_i 是公式 A 的一部分，且 A_i 也是一个公式，称 A_i 是公式 A 的子公式.

由表 5－8 中的等值式能够推演出更复杂的命题公式，我们称由已知的等值式推出另一些等值式的过程为等值演算. 在演算过程中，还需要使用下面的规则：

置换规则 设 X 是公式 A 的子公式，若有 Y 也是一个公式，且 $X\Leftrightarrow Y$，如果 A 中 X 用 Y 置换，得到公式 B，则 $A\Leftrightarrow B$.

证 因为 $X\Leftrightarrow Y$，所以对任一组命题变元的真值指派，X 和 Y 的真值都相同，而 A、B 除 X 和 Y 以外的部分相同，因此 A 和 B 的真值都相同，即有 $A\Leftrightarrow B$.

代入规则 在重言式中，将某一命题变元全用同一命题公式代入后，得到的公式仍是重言式(其正确性请读者思考).

例 5 证明 $P\rightarrow(Q\vee(P\wedge Q))\Leftrightarrow P\rightarrow Q$.

证 设 A：$P\rightarrow(Q\vee(P\wedge Q))$，$B$：$P\rightarrow Q$.

因为 $Q\vee(P\wedge Q)\Leftrightarrow Q\vee(Q\wedge P)\Leftrightarrow Q$.

故 $P\rightarrow(Q\vee(P\wedge Q))\Leftrightarrow P\rightarrow Q$.

即： $A\Leftrightarrow B$.

例 6 证明 $(P\rightarrow R)\wedge(Q\rightarrow R)\Leftrightarrow(P\vee Q)\rightarrow R$.

证

$$
\begin{aligned}
&(P\rightarrow R)\wedge(Q\rightarrow R)\\
\Leftrightarrow&(\Box P\vee R)\wedge(\Box Q\vee R)\\
\Leftrightarrow&(\Box P\wedge\Box Q)\vee R\\
\Leftrightarrow&\Box(P\vee Q)\vee R\\
\Leftrightarrow&(P\vee Q)\rightarrow R.
\end{aligned}
$$

例 7 用等值演算法判断下列公式的类型

(1) $(P\rightarrow(P\vee Q))\vee(P\rightarrow R)$

(2) $\Box(P\wedge Q\rightarrow Q)$

(3) $(P\wedge\Box P)\leftrightarrow Q$

解 (1) $(P\rightarrow(P\vee Q))\vee(P\rightarrow R)$

$$
\begin{aligned}
\Leftrightarrow&(\Box P\vee(P\vee Q))\vee(\Box P\vee R)\\
\Leftrightarrow&(\Box P\vee P)\vee Q\vee\Box P\vee R\\
\Leftrightarrow&1\vee Q\vee\Box P\vee R\\
\Leftrightarrow&1.
\end{aligned}
$$

由此可知(1)为重言式.

(2) $\square(P\wedge Q\rightarrow Q)$

$$\begin{aligned}
&\Leftrightarrow\square(\square(P\wedge Q)\vee Q)\\
&\Leftrightarrow(P\wedge Q)\wedge\square Q\\
&\Leftrightarrow P\wedge(Q\wedge\square Q)\\
&\Leftrightarrow P\wedge 0\\
&\Leftrightarrow 0.
\end{aligned}$$

故(2)是矛盾式.

(3) $(P\wedge\square P)\leftrightarrow Q$

$$\begin{aligned}
&\Leftrightarrow 0\leftrightarrow Q\\
&\Leftrightarrow(0\rightarrow Q)\wedge(Q\rightarrow 0)\\
&\Leftrightarrow 1\wedge(Q\rightarrow 0)\\
&\Leftrightarrow Q\rightarrow 0\\
&\Leftrightarrow\square Q.
\end{aligned}$$

故(3)为可满足式.

三、公式的蕴含关系

定义 5　设 P，Q 是两个命题公式，若 $P\rightarrow Q$ 是重言式，则称 $P\rightarrow Q$ 为蕴含重言式，记作 $P\Rightarrow Q$，读作“P 永真蕴含 Q”.

注意　$\rightarrow$和$\Rightarrow$意义不同. $\Rightarrow$不是联结词，用来表示蕴含式为重言式.

蕴含重言式有下列性质：

(1) 自反性：对于任意公式 A，有 $A\Rightarrow A$；

(2) 反对称性：对于任意公式 A，B，若 $A\Rightarrow B$，$A\not\Leftrightarrow B$，则 $B\not\Rightarrow A$；

(3) 传递性：对于任意公式 A，B，C，若 $A\Rightarrow B$，且 $B\Rightarrow C$，则 $A\Rightarrow C$.

证　(2) 反证法

若 $A\Rightarrow B$，有 $B\Rightarrow A$.

即：命题公式 $A\rightarrow B$ 与 $B\rightarrow A$ 都是重言式，则：

命题公式$(A\rightarrow B)\wedge(B\rightarrow A)$就是重言式，而

$$(A\rightarrow B)\wedge(B\rightarrow A)\Leftrightarrow A\leftrightarrow B,$$

故 $A\leftrightarrow B$ 是重言式，则有 $A\Leftrightarrow B$，这与 $A\not\Leftrightarrow B$ 矛盾. 所以，反对称性成立.

“命题公式中常见的蕴含重言式见表 5－9”，其中 A，B，C，D 可以代表任意的命题公式.

表 5－9

化简律	(1) $A\wedge B\Rightarrow A$ (2) $A\wedge B\Rightarrow B$

附加律	(3) $A \Rightarrow A \vee B$
	(4) $B \Rightarrow A \vee B$

续表

假言推理	(5) $(A \rightarrow B) \wedge A \Rightarrow B$
析取三段论	(6) $(A \vee B) \wedge \square B \Rightarrow A$
假言三段论	(7) $(A \rightarrow B) \wedge (B \rightarrow C) \Rightarrow A \rightarrow C$
拒取式	(8) $(A \rightarrow B) \wedge \square B \Rightarrow \square A$
构造性二难	(9) $(A \rightarrow B) \wedge (C \rightarrow D) \wedge (A \vee C) \Rightarrow (B \vee D)$
	(10) $(A \rightarrow B) \wedge (\square A \rightarrow B) \wedge (A \vee \square A) \Rightarrow B$
变形附加律	(11) $\square A \Rightarrow A \rightarrow B$
	(12) $B \Rightarrow A \rightarrow B$
变形简化律	(13) $\square (A \rightarrow B) \Rightarrow A$
	(14) $\square (A \rightarrow B) \Rightarrow \square B$
前后件附加律	(15) $A \rightarrow B \Rightarrow (A \vee C) \rightarrow (B \vee C)$
	(16) $A \rightarrow B \Rightarrow (A \wedge C) \rightarrow (B \wedge C)$

证明 $A \Rightarrow B$ 的方法

第一种：用真值法或等值演算法证明 $A \rightarrow B$ 是重言式.

第二种：(1) 假设前件 A 为真时，推出后件 B 也为真，则 $A \Rightarrow B$.

(2) 假设后件 B 为假时，推出前件 A 也为假，则 $A \Rightarrow B$.

表 5-9 所列的各蕴含重言式都可用上述方法证明.

定理 1 设 A、B 为任意两个命题，$A \Leftrightarrow B$ 的充分必要条件是 $A \Rightarrow B$ 且 $B \Rightarrow A$.

证 必要性：若 $A \Leftrightarrow B$，则 $A \leftrightarrow B$ 是重言式. 但

$$A \leftrightarrow B \Leftrightarrow (A \rightarrow B) \wedge (B \rightarrow A),$$

故 $A \rightarrow B$，$B \rightarrow A$ 都为真，所以 $A \Rightarrow B$ 且 $B \Rightarrow A$.

充分性：若 $A \Rightarrow B$ 且 $B \Rightarrow A$，则 $A \rightarrow B$，$B \rightarrow A$ 为重言式，所以 $A \leftrightarrow B$ 为重言式，故 $A \Leftrightarrow B$ 成立.

由上述定理知，表 5-8 中的每一个等值式都能派生出两个蕴含重言式.

例 8 证明 $(A \rightarrow B) \wedge (B \rightarrow C) \Rightarrow A \rightarrow C$.

证 $(A \rightarrow B) \wedge (B \rightarrow C) \rightarrow (A \rightarrow C)$

$\Leftrightarrow (\square A \vee B) \wedge (\square B \vee C) \rightarrow \square A \vee C$

$\Leftrightarrow \square ((\square A \vee B) \wedge (\square B \vee C)) \vee (\square A \vee C)$

$\Leftrightarrow (A \wedge \square B) \vee (B \wedge \square C) \vee \square A \vee C$

$\Leftrightarrow ((A \wedge \square B) \vee \square A) \vee ((B \wedge \square C) \vee C)$

$\Leftrightarrow ((A \vee \square A) \wedge (\square B \vee \square A)) \vee ((B \vee C) \wedge (\square C \vee C))$

$\Leftrightarrow (\square A \vee \square B) \vee (B \vee C)$

$\Leftrightarrow \square A \vee \square B \vee B \vee C$

$\Leftrightarrow \square A \vee 1 \vee C$

$\Leftrightarrow 1$

故$(A \to B) \wedge (B \to C) \Rightarrow A \to C$.

练习题 5－2

1. 判别下列符号串哪些是命题公式，哪些不是命题公式？

(1) $P \to Q \wedge S$.

(2) $Q \to R$.

(3) $P \to Q \Leftrightarrow \square P \vee Q$.

(4) $(P \vee Q) \wedge R$.

(5) $(P \to Q) \Rightarrow \square Q \to \square P$.

2. 设 P、Q 的真值为 0，R、S 的真值为 1；求下列各命题公式的真值.

(1) $P \to (Q \vee R)$.

(2) $P \vee (Q \wedge R)$.

(3) $(P \leftrightarrow Q) \wedge (\square R \vee S)$.

(4) $(\square P \to Q) \wedge (R \leftrightarrow S)$.

3. 求下列命题公式的真值表.

(1) $P \wedge (Q \vee R)$.

(2) $(P \to (Q \vee R)) \leftrightarrow ((P \wedge \square Q) \to R)$.

4. 判断下面一段论述是否为真：“π 是无理数，并且，如果 3 是无理数，则$\sqrt{2}$也是无理数. 另外，只有 6 能被 2 整除，6 才能被 4 整除”.

5. 判断下列各式，哪些是重言式，哪些是矛盾式，哪些是可满足式？

(1) $\square(A \wedge B \to B)$.

(2) $(A \to (A \vee B)) \vee (A \to C)$.

(3) $(A \vee B) \to (A \wedge C)$.

(4) $A \to (A \vee B \vee C)$.

(5) $(A \to \square A) \to \square A$.

(6) $(A \leftrightarrow B) \to \square(A \vee B)$.

(7) $(A \wedge \square A) \leftrightarrow B$.

(8) $(\square A \to B) \to (B \to \square A)$.

6. 设 A，B，C 为任意的命题公式.

(1) 已知 $A \vee C \Leftrightarrow B \vee C$，$A \Leftrightarrow B$ 一定成立吗？

(2) 已知 $A \wedge C \Leftrightarrow B \wedge C$，$A \Leftrightarrow B$ 一定成立吗？

(3) 已知$\square A \Leftrightarrow \square B$，$A \Leftrightarrow B$ 一定成立吗？

7. 将语句“居里夫人是波兰人，她是一个伟大的科学家，由于她对科学事业作出了巨大的贡献，因此，她被授予诺贝尔奖金.”写成命题公式的形式.

8. 不用真值表方法，证明下列命题公式是等值的.

(1) $P \Leftrightarrow (P \wedge Q) \vee (P \wedge \square Q)$.

(2) $P\to(Q\to P)\Leftrightarrow\square P\to(P\to Q)$.

(3) $((P\to Q)\wedge(P\to R))\Leftrightarrow(P\to(Q\wedge R))$.

(4) $\square(P\leftrightarrow Q)\Leftrightarrow(P\vee Q)\wedge\square(P\wedge Q)$.

9. 不用真值方法，证明下列蕴含重言式：

(1) $P\wedge(P\to Q)\Rightarrow Q$.

(2) $P\to Q\Rightarrow P\to P\wedge Q$.

(3) $P\Rightarrow\square P\to Q$.

(4) $(P\to Q)\to Q\Rightarrow P\vee Q$.

10. 化简命题公式：

(1) $((P\to Q)\leftrightarrow(\square Q\to\square P))\wedge R$.

(2) $((A\to B)\leftrightarrow(\square B\to\square A))\vee C$.

11. 已知 A 是 B 的充分条件，B 是 C 的必要条件，C 是 D 的必要条件，D 是 B 的必要条件，问：

(1) A 是 D 的什么条件？

(2) B 是 D 的什么条件？

第三节 对偶与范式

一、对偶

在表 5－8 的命题定律中，有些公式是成对出现的，这些成对出现的公式称为对偶式.

定义 1 在仅含有$\square$，$\wedge$，$\vee$ 的命题公式 A 中，将 $\wedge$，$\vee$ 分别换成 $\vee$，$\wedge$，若 A 中有 1 或 0 亦互相取代，所得公式 A^* 称为 A 的对偶.

显然 A 也是 A^* 的对偶.

例 1 试写出下列命题的对偶.

(1) $\square(P\wedge Q)\vee R$.

(2) $((P\to Q)\wedge\square R)\vee 0$.

解 (1) 的对偶为$\square(P\vee Q)\wedge R$.

(2) $((P\to Q)\wedge\square R)\vee 0\Leftrightarrow((\square P\vee Q)\wedge\square R)\vee 0$.

所以(2)的对偶为$((\square P\wedge Q)\vee\square R)\wedge 1$.

定理 1 设 A 与 A^* 是互为对偶的两个公式，所含的命题变元为 P_1，P_2，…，P_n，则

$$\square A(P_1,P_2,\cdots,P_n)\Leftrightarrow A^*(\square P_1,\square P_2,\cdots,\square P_n)$$

或

$$A(\square P_1,\square P_2,\cdots,\square P_n)\Leftrightarrow\square A^*(P_1,P_2,\cdots,P_n)$$

即公式的否定等值于其对偶变元的否定.

该定理的一般性证明要用数学归纳法，我们只以一例说明.

设
$$A(P,Q,R)\Leftrightarrow(P\vee Q)\wedge R,$$
则
$$\square A(P,Q,R)\Leftrightarrow\square((P\vee Q)\wedge R)$$
$$\Leftrightarrow(\square P\wedge\square Q)\vee\square R.$$
而
$$A^*(P,Q,R)\Leftrightarrow(P\wedge Q)\vee R.$$
$$A^*(\square P,\square Q,\square R)\Leftrightarrow(\square P\wedge\square Q)\vee\square R.$$
故
$$\square A(P,Q,R)\Leftrightarrow A^*(\square P,\square Q,\square R).$$

定理 2（对偶原理）　如果
$$A(P_1,P_2,\cdots,P_n)\Leftrightarrow B(P_1,P_2,\cdots,P_n),$$
则
$$A^*(P_1,P_2,\cdots,P_n)\Leftrightarrow B^*(P_1,P_2,\cdots,P_n).$$

证　因为
$$A(P_1,P_2,\cdots,P_n)\Leftrightarrow B(P_1,P_2,\cdots,P_n),$$
所以
$$A(P_1,P_2,\cdots,P_n)\leftrightarrow B(P_1,P_2,\cdots,P_n)$$
为重言式，由定理 1 有：公式
$$A^*(\square P_1,\square P_2,\cdots,\square P_n)\leftrightarrow B^*(\square P_1,\square P_2,\cdots,\square P_n)$$
为重言式. 由代入规则，以$\square P_i$ 代替 $P_i(i=1,2,\cdots,n)$有
$$A^*(P_1,P_2,\cdots,P_n)\leftrightarrow B^*(P_1,P_2,\cdots,P_n)$$
为重言式，故
$$A^*(P_1,P_2,\cdots,P_n)\Leftrightarrow B^*(P_1,P_2,\cdots,P_n).$$

二、范式

利用真值表和等值演算法可以化简或推证一些命题公式，但是当命题的变元的数目较多时，上述方法都显得不方便，所以需要给出把命题公式规范的方法. 即把命题公式化成主合取范式和主析取范式的方法.

定义 2　仅由命题变元或其否定构成的合取式称为质合取式，或简单合取式.

定义 3　仅由命题变元或其否定构成的析取式称为质析取式，或简单析取式.

若 P，Q，R 是命题变元，则 P、Q、R、$\square Q$，$P\wedge Q$，$\square P\wedge\square Q\wedge R$，$P\wedge Q\wedge R$ 等都是质合取式；而 P，Q，R，$\square P$，$P\vee Q$，$\square P\vee Q\vee\square R$，$P\vee Q\vee R$ 等都是质析取式.

应该注意，单个的命题变元或其否定既是质合取式，又是质析取式.

定理 3　（1）一质合取式为矛盾式当且仅当它同时含有某个命题变元 P 及其否定$\square P$.

（2）一质析取式为重言式当且仅当它同时含有某个命题变元 P 及其否定$\square P$.

证明 设命题公式含有 n 个命题变元或其否定.

（1）**必要性**：A 是矛盾式，则 A 中必同时含某个命题变元 P 及其否定 $\square P$. 否则，若将 A 中的不带否定联结词的命题变元都取 1，带否定联结词的命题变元都取 0，则此指派为 A 的成真指派，这与 A 是矛盾式相矛盾的.

充分式：设命题公式 A 中含有命题变元 P 及其否定 $\square P$，则由交换律、互否律和零律可知 A 为矛盾式.

（2）**必要性**：A 是重言式，则它必同时含有某个命题变元 P 及它的否定 $\square P$. 否则，若将不带否定联结词的命题变元都取 0，带否定联结词的命题变元都取 1，此指派为 A 的成假指派，这与 A 是重言式相矛盾.

充分性：若 A 中既含某个命题变元 P，又含它的否定 $\square P$，由交换律、互否律和零律可知，A 为重言式.

定义 4 （1）仅由有限个质合取式构成的析取式称为析取范式.

（2）由有限个质析取式构成的合取式称为合取范式.

（3）析取范式与合取范式统称为范式.

例如：$\square P \vee (P \wedge \square Q) \vee (P \wedge Q \wedge R)$ 为析取范式.

而 $P \wedge (P \vee \square Q) \wedge (P \vee Q \vee R)$ 为合取范式.

注意 $P \wedge Q \wedge \square R$ 既是合取范式（由三个质析取式的合取构成），又是析取范式（由一个质合取式构成）.

定理 4（范式存在定理） 任意一个命题公式都存在与之等值的析取范式和合取范式.

证明 略

下面给出求命题公式范式的步骤：

1. 消去联结词→，↔.

2. 利用双重否定律，德·摩根律，将否定联结词□消去或移到各命题变元之前.

3. 利用分配律：$\wedge$ 对 $\vee$ 分配求析取范式，$\vee$ 对 $\wedge$ 分配求合取范式.

例 2 求命题公式 $P \leftrightarrow (P \wedge Q)$ 的析取范式和合取范式.

解 （1）先求合取范式

$$
\begin{aligned}
P \leftrightarrow (P \wedge Q) &\Leftrightarrow (P \rightarrow (P \wedge Q)) \wedge ((P \wedge Q) \rightarrow P) \\
&\Leftrightarrow (\square P \vee (P \wedge Q)) \wedge (\square (P \wedge Q) \vee P) \\
&\Leftrightarrow ((\square P \vee P) \wedge (\square P \vee Q)) \wedge ((\square P \vee \square Q) \vee P) \\
&\Leftrightarrow (1 \wedge (\square P \vee Q)) \wedge (\square P \vee P \vee \square Q) \\
&\Leftrightarrow (\square P \vee Q) \wedge (1 \vee \square Q) \\
&\Leftrightarrow (\square P \vee Q) \wedge 1 \\
&\Leftrightarrow \square P \vee Q.
\end{aligned}
$$

（2）求析取范式

$P \leftrightarrow (P \wedge Q)$

$\Leftrightarrow (\square P \vee (P \wedge Q)) \wedge (\square (P \wedge Q) \vee P)$

$\Leftrightarrow (\square P \vee (P \wedge Q) \wedge ((\square P \vee \square Q) \vee P)$

$\Leftrightarrow (\square P \vee (P \wedge Q)) \wedge (\square Q \vee 1)$

$\Leftrightarrow (\square P \vee (P \wedge Q)) \wedge 1$

$\Leftrightarrow \square P \vee (P \wedge Q)$.

定理 5　（1）命题公式 A 为重言式当且仅当 A 的合取范式中每个质析取式至少同时含有一个命题变元及其否定.

（2）命题公式 A 为矛盾式当且仅当 A 的析取范式中每个质合取式至少同时含有一个命题变元及其否定.

由上述定理知：公式 A 的析取范式可用于判定 A 是否为矛盾式；而 A 的合取范式可用于判定 A 是否为重言式.

证明从略.

例 3　判断公式 $((P \rightarrow Q) \wedge P) \rightarrow Q$ 是否为重言式或矛盾式.

解

$((P \rightarrow Q) \wedge P) \rightarrow Q$

$\Leftrightarrow ((\square P \vee Q) \wedge P) \rightarrow Q$

$\Leftrightarrow \square ((\square P \vee Q) \wedge P) \vee Q$

$\Leftrightarrow ((P \wedge \square Q) \vee \square P) \vee Q \Leftrightarrow (P \wedge \square Q) \vee (\square P \vee Q)$

$\Leftrightarrow (P \vee \square P \vee Q) \wedge (\square Q \vee P \vee Q)$

$\Leftrightarrow 1 \wedge 1$

$\Leftrightarrow 1$.

故公式 $((P \rightarrow Q) \wedge P) \rightarrow Q$ 是重言式

例 4　判别命题公式 $(P \rightarrow Q) \rightarrow R$ 是否为重言式或矛盾式.

解　$(P \rightarrow Q) \rightarrow R$

$\Leftrightarrow (\square P \vee Q) \rightarrow R$

$\Leftrightarrow \square (\square P \vee Q) \vee R$

$\Leftrightarrow (P \wedge \square Q) \vee R$　　　　（析取范式）

$\Leftrightarrow (P \vee R) \wedge (\square Q \vee R)$　（合取范式）.

由定理 5 知，此公式既不是重言式，又不是矛盾式.

从例 3 可以看出，一个公式的析取范式和合取范式是不惟一的. 为了使任意一个命题公式，化为惟一的等值的标准形式，下面介绍主析取范式和主合取范式的概念.

定义 5　在含有 n 个命题变元的质合取式中，若每个命题变元和它的否定

不同时出现，但是两者必须出现且仅出现一次，且第 i 个命题变元或它的否定式出现在从左算起的第 i 位上(若命题变项无脚标,则按字典顺序排列)，这样的质合取式称为最小项.

例如，两个命题变元 P 和 Q，其最小项为：$P\wedge Q$，$P\wedge\square Q$，$\square P\wedge Q$，$\square P\wedge\square Q$.

三个命题变元 P、Q、R，其最小项为：

$$P\wedge Q\wedge R,\ P\wedge Q\wedge\square R,\ P\wedge\square Q\wedge R,\ P\wedge\square Q\wedge\square R,$$
$$\square P\wedge Q\wedge R,\ \square P\wedge Q\wedge\square R,\ \square P\wedge\square Q\wedge R,\ \square P\wedge\square Q\wedge\square R.$$

一般来说，n 个命题变元共可产生 2^n 个不同的最小项，且每个最小项只有一个成真指派. 若将命题变元看成 1，它的否定看成 0，则每个最小项对应一个二进制数或一个十进制数 i. 我们把所对应最小项记作 m_i.

以三个命题变元为例：

$$m_{000}=\square P\wedge\square Q\wedge\square R,\qquad m_{001}=\square P\wedge\square Q\wedge R,$$
$$m_{010}=\square P\wedge Q\wedge\square R,\qquad m_{011}=\square P\wedge Q\wedge R,$$
$$m_{100}=P\wedge\square Q\wedge\square R,\qquad m_{101}=P\wedge\square Q\wedge R,$$
$$m_{110}=P\wedge Q\wedge\square R,\qquad m_{111}=P\wedge Q\wedge R.$$

为了便于记忆，分别给出 P，Q 与 P，Q，R 形成的最小项的真值表.

表 5－10　P，Q 形成的最小项

P	Q	$m_0=\square P\wedge\square Q$	$m_1=\square P\wedge Q$	$m_2=P\wedge\square Q$	$m_3=P\wedge Q$
0	0	1	0	0	0
0	1	0	1	0	0
1	0	0	0	1	0
1	1	0	0	0	1

表 5－11　P，Q，R 形成的最小项

P	Q	R	$m_0=$ $\square P\wedge\square Q\wedge\square R$	$m_1=$ $\square P\wedge\square Q\wedge R$	$m_2=$ $\square P\wedge Q\wedge\square R$	$m_3=$ $\square P\wedge Q\wedge R$
0	0	0	1	0	0	0
0	0	1	0	1	0	0
0	1	0	0	0	1	0
0	1	1	0	0	0	1
1	0	0	0	0	0	0
1	0	1	0	0	0	0
1	1	0	0	0	0	0

1	1	1	0	0	0	0

续表

P	Q	R	$m_4 =$ $P\wedge\square Q\wedge\square R$	$m_5 =$ $P\wedge\square Q\wedge R$	$m_6 =$ $P\wedge Q\wedge\square R$	$m_7 =$ $P\wedge Q\wedge R$
0	0	0	0	0	0	0
0	0	1	0	0	0	0
0	1	0	0	0	0	0
0	1	1	0	0	0	0
1	0	0	1	0	0	0
1	0	1	0	1	0	0
1	1	0	0	0	1	0
1	1	1	0	0	0	1

从表 5－11 中可以看出最小项有如下性质：

（1）每个最小项具有一个编码，当真值指派与该编码相同时，该最小项的真值为 1，其余 2^n-1 种指派其真值为 0.

例如，最小项 $\square P\wedge Q\wedge\square R$，编码为 m_{010}，当 P 真值为 0，Q 真值为 1，R 真值为 0 时，最小项 $m_2=\square P\wedge Q\wedge\square R$ 的真值为 1，其余的各种指派，该最小项真值都为 0.

（2）任意两个不同最小项的合取式为永假式.

例如，$m_{101}\wedge m_{010}=(P\wedge\square Q\wedge R)\wedge(\square P\wedge Q\wedge\square R)$

$\Leftrightarrow P\wedge\square P\wedge\square Q\wedge Q\wedge R\wedge\square R\Leftrightarrow 0.$

（3）全体最小项的析取式为永真式.

$$m_0\vee m_1\vee\cdots\vee m_{2^n-1}\Leftrightarrow 1.$$

定义 6　对于给定的命题公式 $A(P_1,P_2,\cdots,P_n)$，如果有一个仅由最小项的析取构成的等值式，则该等值式称为原命题公式的主析取范式.

定理 6　任意含 n 个命题变元的非永假式，其主析取范式是惟一的.

证明　（反证法）

假设非永假式 $A(P_1,P_2,\cdots,P_n)$ 有两个不同的主析取范式 A_1 和 A_2，则 $A\Leftrightarrow A_1$，$A\Leftrightarrow A_2$ 故 $A_1\Leftrightarrow A_2$. 由于 A_1 和 A_2 是两个不同的主析取范式，故至少存在一个最小项 m_i，使 m_i 只存在于 A_1 和 A_2 两者之一中，不妨设 m_i 在 A_1 中，而不在 A_2 中. 设 m_i 在 A_1 中有一组成真指派 R，于是在 R 指派下，主析取范式 A_1 为真. 但在 R 指派情况下，主析取范式 A_2 为假，这与 $A_1\Leftrightarrow A_2$ 矛盾.

定义 7　在含有 n 个命题变元的质析取式中，若每个命题变元和它的否定不同时出现，但是两者必须出现且仅出现一次，且第 i 个命题变元或它的否定

式出现在从左算起的第 i 位上（若命题变项无脚标，则按字典顺序排列），这样的质析取式称为最大项.

两个命题变元 P 和 Q，其最大项为：$P \vee Q$，$P \vee \square Q$，$\square P \vee Q$，$\square P \vee \square Q$.

三个命题变元 P、Q、R，其最大项为：

$P \vee Q \vee R$，$P \vee Q \vee \square R$，$P \vee \square Q \vee R$，$P \vee \square Q \vee \square R$，

$\square P \vee Q \vee R$，$\square P \vee Q \vee \square R$，$\square P \vee \square Q \vee R$，$\square P \vee \square Q \vee \square R$.

如果将命题变元对应为 0，它的否定对应为 1，则每个最大项对应一个二进制数和一个十进制数. 二进制数恰好是该最大项的成假指派. 最大项记为 M_i，其下标 i 是由二进制数化为十进制数. 例如由两个命题变元 P，Q 形成 4 个最大项：$P \vee Q$，$P \vee \square Q$，$\square P \vee Q$，$\square P \vee \square Q$，分别记为 M_{00}，M_{01}，M_{10}，M_{11}，也可分别记为 M_0，M_1，M_2，M_3. 最大项 $\square P \vee Q \vee \square R$，$P \vee \square Q \vee \square R \vee S$，分别记为 M_{101}，M_{0110}. 也可记为 M_5，M_6.

定义 8　对于给定的命题公式 $A(P_1, P_2, \cdots, P_n)$，如果有一个仅由最大项的合取构成的等值式，则该等值式称为原命题公式的主合取范式.

定理 7　任意含 n 个命题变元的非重言式，其主合取范式是惟一的.

本定理证明类似于定理 6，证明从略.

定理 8　（1）在真值表中，一个命题公式的真值为 1 的指派所对应的最小项的析取，就是此命题公式的主析取范式.

（2）在真值表中，一个命题公式的真值为 0 的指派所对应的最大项的合取，就是此命题公式的主合取范式.

证明从略.

例 5　公式 A 的真值表如下，求主析取范式和主合取范式.

P	Q	R	A	P	Q	R	A
0	0	0	1	1	0	0	0
0	0	1	0	1	0	1	1
0	1	0	1	1	1	0	0
0	1	1	1	1	1	1	0

解　（1）从真值表中看出其真值为 1 的最小项有 m_{000}，m_{010}，m_{011}，m_{101}，即：

$\square P \wedge \square Q \wedge \square R$，$\square P \wedge Q \wedge \square R$，$\square P \wedge Q \wedge R$，$P \wedge \square Q \wedge R$.

由定理 8 中（1）得：A 的主析取范式为：

$$(\square P \wedge \square Q \wedge \square R) \vee (\square P \wedge Q \wedge \square R) \vee (\square P \wedge Q \wedge R) \vee (P \wedge \square Q \wedge R)$$

$$\Leftrightarrow m_{000} \vee m_{010} \vee m_{011} \vee m_{101}$$

$$\Leftrightarrow m_0 \vee m_2 \vee m_3 \vee m_5.$$

也可表示为：$A \Leftrightarrow \sum(0,2,3,5)$.

（2）从真值表中还能看出其真值为 0 的最大项有 M_{001}，M_{100}，M_{110}，M_{111}. 即：

$$P \vee Q \vee \square R,\ \square P \vee Q \vee R,\ \square P \vee \square Q \vee R,\ \square P \vee \square Q \vee \square R.$$

由定理 8 中(2)得：A 的主合取范式为：

$$(P \vee Q \vee \square R) \wedge (\square P \vee Q \vee R) \wedge (\square P \vee \square Q \vee R) \wedge (\square P \vee \square Q \vee \square R)$$

$$\Leftrightarrow M_{001} \wedge M_{100} \wedge M_{110} \wedge M_{111} \Leftrightarrow M_1 \wedge M_4 \wedge M_6 \wedge M_7.$$

也可表示为：$A \Leftrightarrow \prod(1,4,6,7)$.

例 6　求公式 $P \to (P \to Q) \wedge \square(\square Q \vee \square P)$ 的主合取式和主析取范式.

表 5－12

P	Q	$P \to Q$	$\square P \wedge \square Q$	$\square(\square P \wedge \square Q)$	$(P \to Q) \wedge \square(\square P \wedge \square Q)$	$P \to (P \to Q) \wedge \square(\square P \wedge \square Q)$
0	0	1	1	0	0	1
0	1	1	0	1	1	1
1	0	0	0	1	0	0
1	1	1	0	1	1	1

从表 5－12 看出：$P \to (P \to Q) \wedge \square(\square Q \vee \square P)$

$$\Leftrightarrow m_{00} \vee m_{01} \vee m_{11} \Leftrightarrow m_0 \vee m_1 \vee m_3 \Leftrightarrow \sum(0,1,3).$$

$$P \to (P \to Q) \wedge \square(\square Q \vee \square P)$$

$$\Leftrightarrow M_{10} \Leftrightarrow M_2 \Leftrightarrow \prod(2).$$

定理 9　任意命题公式都存在着与之等值的主析取范式和主合取范式，并且是惟一的.

证明　略.

例 7　用等值演算法求命题公式 $P \wedge Q \vee R$ 的主析取式和主合取范式.

解　$P \wedge Q \vee R \Leftrightarrow (P \vee R) \wedge (Q \vee R)$

$$\Leftrightarrow (P \vee (Q \wedge \square Q) \vee R) \wedge ((P \wedge \square P) \vee Q \vee R)$$

$$\Leftrightarrow (P \vee Q \vee R) \wedge (P \vee \square Q \vee R) \wedge (P \vee Q \vee R) \wedge (\square P \vee Q \vee R)$$

$$\Leftrightarrow (P \vee Q \vee R) \wedge (P \vee \square Q \vee R) \wedge (\square P \vee Q \vee R)$$

$$\Leftrightarrow M_{000} \wedge M_{010} \wedge M_{100}$$

$$\Leftrightarrow M_0 \wedge M_2 \wedge M_4$$

$$\Leftrightarrow \prod(0,2,4).$$

即公式的主合取范式为 $M_0 \wedge M_2 \wedge M_4$.

$$P \wedge Q \vee R \Leftrightarrow ((P \wedge Q) \wedge (R \vee \square R)) \vee ((P \vee \square P) \wedge R)$$

$\Leftrightarrow(P\wedge Q\wedge R)\vee(P\wedge Q\wedge\square R)\vee(P\wedge R)\vee(\square P\wedge R)$

$\Leftrightarrow(P\wedge Q\wedge R)\vee(P\wedge Q\wedge\square R)\vee(P\wedge(Q\vee\square Q)\wedge R)\vee(\square P\wedge(Q\vee\square Q)\wedge R)$

$\Leftrightarrow(P\wedge Q\wedge R)\vee(P\wedge Q\wedge\square R)\vee(P\wedge Q\wedge R)\vee(P\wedge\square Q\wedge R)\vee(\square P\wedge Q\wedge R)\vee(\square P\wedge\square Q\wedge R)$

$\Leftrightarrow(\square P\wedge\square Q\wedge R)\vee(\square P\wedge Q\wedge R)\vee(P\wedge\square Q\wedge R)\vee(P\wedge Q\wedge\square R)\vee(P\wedge Q\wedge R)$

$\Leftrightarrow m_{001}\vee m_{011}\vee m_{101}\vee m_{110}\vee m_{111}$

$\Leftrightarrow m_1\vee m_3\vee m_5\vee m_6\vee m_7$

$\Leftrightarrow\sum(1,3,5,6,7)$.

即公式的主析取范式为 $m_1\vee m_3\vee m_5\vee m_6\vee m_7$.

从例 7 中，我们可以看到：公式 $P\wedge Q\vee R$ 的主析取范式中含有 5 个最小项，而它的主合取范中含有 3 个最大项.

一般地，如果命题公式 A 中含有 n 个命题变元，且 A 的主析取范式中含有 k 个最小元，则 A 的主合取范式中必含有 2^n-k 个最大元. 若公式 A 的主析取范式为：

$$\sum(i_1,i_2,\cdots,i_k),$$

则 A 的主合取范式为：

$$\prod(0,1,\cdots,i_1-1,i_1+1,\cdots,i_k-1,i_k+1,\cdots,2^n-1).$$

例如 $(P\vee Q)\rightarrow R\Leftrightarrow\sum(0,1,3,5,7)$,

则 $(P\vee Q)\rightarrow R\Leftrightarrow\prod(2,4,6)$.

例 8 证明 $(P\rightarrow R)\wedge(Q\rightarrow R)\Leftrightarrow P\vee Q\rightarrow R$.

证 $(P\rightarrow R)\wedge(Q\rightarrow R)$

$\Leftrightarrow(\square P\vee R)\wedge(\square Q\vee R)$

$\Leftrightarrow((\square P\vee(Q\wedge\square Q))\vee R)\wedge((P\wedge\square P)\vee\square Q\vee R)$

$\Leftrightarrow(\square P\vee Q\vee R)\wedge(\square P\vee\square Q\vee R)\wedge(P\vee\square Q\vee R)\wedge(\square P\vee\square Q\vee R)$

$\Leftrightarrow(P\vee\square Q\vee R)\wedge(\square P\vee Q\vee R)\wedge(\square P\vee\square Q\vee R)$

$\Leftrightarrow M_{010}\wedge M_{100}\wedge M_{110}$.

而公式 $(P\vee Q)\rightarrow R$

$\Leftrightarrow\square(P\vee Q)\vee R$

$\Leftrightarrow(\square P\wedge\square Q)\vee R$

$\Leftrightarrow(\square P\vee R)\wedge(\square Q\vee R)$

$\Leftrightarrow\prod(2,4,6)$.

所以 $(P\rightarrow R)\wedge(Q\rightarrow R)\Leftrightarrow P\vee Q\rightarrow R$.

利用公式的主析取范式或主合取范式可以判断公式的类型.

（1）公式 A 为重言式当且仅当 A 的主析取范式含全部 2^n 个最小项.
（2）公式 A 为矛盾式当且仅当 A 的主合取范式含全部 2^n 个最大项.
（3）公式 A 为可满足式当且仅当 A 的主析取范式中至少含一个最小项.

练习题 5 - 3

1. 将下面公式化成与之等值式，并且仅含 $\{\square, \wedge\}$ 中联结词的公式.

（1）$\square(P \vee Q) \leftrightarrow (P \wedge Q)$.

（2）$P \wedge (Q \vee R)$.

2. 求下列各公式的主析取范式、主合取范式，并判断各式的类型.

（1）$((P \to Q) \wedge P) \to Q$.

（2）$\square(P \to Q) \wedge Q \wedge R$.

（3）$P \vee (Q \wedge R) \to (P \wedge Q \wedge R)$.

3. 用主析取范式判断下列公式是否等值.

（1）$(P \to Q) \to R$ 与 $Q \to (P \to R)$.

（2）$P \to (Q \to R)$ 与 $\square(P \wedge Q) \vee R$.

4. 求下列公式的主析取范式，再用主析取范式求主合取范式.

（1）$(P \wedge Q) \vee \square R$.

（2）$(P \leftrightarrow Q) \to R$.

5. 某科研所要从 3 名科研骨干 A，B，C 中挑选 1 ~ 2 名出国进修，由于工作需要，选派时要满足以下条件：

（1）若 A 去，则 C 同去，

（2）若 B 去，则 C 不能去，

（3）若 C 不去，则 A 或 B 可以去.

问该科研所应如何选派他们？

第四节　命题演算的推理规则

数理逻辑的主要任务是用数学方法来研究推理. 是从前提出发，按照推理规则推导出一个结论的思维过程. 前提是已知的命题、公式、集合，结论是从前提出发应用推理规则推出的命题、公式. 在推理过程中，我们关心的是推理的有效性，必须把推理的有效性和结论的真实性区别开来. 推理正确，不能保证结论一定为真，这与数学中的推理是不同的. 另外，结论为真的推理过程不一定有效. 为此，首先需要明确怎样的推理是有效的.

定义 1　设 A_1，A_2，…，A_n，B 是命题公式，如果 $A_1 \wedge A_2 \wedge \cdots \wedge A_n \to B$ 为重言式，则称 B 为前提集合 $\{A_1, A_2, \cdots, A_n\}$ 的有效结论.

关于定义 1 作以下两点说明：

（1）如果公式 $A_1 \wedge A_2 \wedge \cdots \wedge A_n \to B$ 是重言式，则 $A_1 \wedge A_2 \wedge \cdots \wedge A_n \to B$ 可记作：

$$A_1 \wedge A_2 \wedge \cdots \wedge A_n \Rightarrow B.$$

（2）由前提 A_1，A_2，…，A_n 推 B 的推理记为 $\{A_1, A_2, \cdots, A_n\} \vdash B$. 如果推理是有效的，则记为 $\{A_1, A_2, \cdots, A_n\} \models B$；否则记为 $\{A_1, A_2, \cdots, A_n\} \not\models B$.

判断推理是否有效，就是判断命题公式 $A_1 \wedge A_2 \wedge \cdots \wedge A_n \to B$ 是否为重言式. 所以判别推理是否有效的方法有：真值表法、等值演算法、主析取范式法等.

例 1　判断下面推理是否有效.

如果他是理科学生，他必学好数学. 如果他不是文科学生，他必是理科学生. 他没有学好数学. 所以他是文科学生.

解　设 P：他是理科学生，

Q：他学好数学，

R：他是文科学生，

则：前提：$P \to Q$，$(\neg R \to P)$，$\neg Q$.

结论：R.

上述语句可以表述如下：

$$(P \to Q) \wedge (\neg R \to P) \wedge \neg Q \Rightarrow R.$$

列出真值表如表 5－13：

表 5－13

P Q R	$\neg Q$	$P \to Q$	$\neg R \to P$	$(P \to Q) \wedge (\neg R \to P) \wedge \neg Q$
0　0　0	1	1	0	0
0　0　1	1	1	1	1
0　1　0	0	1	1	0
0　1　1	0	1	1	0
1　0　0	1	0	1	0
1　0　1	1	0	1	0
1　1　0	0	1	1	0
1　1　1	0	1	1	0

在表 5－13 中，当 $(P \to Q) \wedge (\neg R \to P) \wedge \neg Q$ 的真值为 1 时，R 的真值也是 1，所以 $(P \to Q) \wedge (\neg R \to P) \wedge \neg Q \to R$ 是重言式.

故该推理是有效的.

例 2　判断下列推理是否正确.

（1）$\{P, P \to Q\} \vdash P$.

（2）　$\{\square P, P\to Q\}\ \vdash Q.$

解　（1）**等值演算法**

$$P\wedge(P\to Q)\to P$$
$$\Leftrightarrow P\wedge(\square P\vee Q)\to P$$
$$\Leftrightarrow \square(P\wedge(\square P\vee Q))\vee P$$
$$\Leftrightarrow \square P\vee(P\wedge\square Q)\vee P$$
$$\Leftrightarrow(\square P\vee P)\vee(P\wedge\square Q)$$
$$\Leftrightarrow 1\vee(P\wedge\square Q)$$
$$\Leftrightarrow 1.$$

由此可知，P 是 P 和 $P\to Q$ 的有效结论. 因而(1)中推理正确，即

$$\{P, P\to Q\}\ \vdash P.$$

（2）**主析取范式法**

$$\square P\wedge(P\to Q)\to Q$$
$$\Leftrightarrow(\square P\wedge(\square P\vee Q))\to Q$$
$$\Leftrightarrow \square P\to Q$$
$$\Leftrightarrow P\vee Q$$
$$\Leftrightarrow(P\wedge(Q\vee\square Q))\vee((P\vee\square P)\wedge Q)$$
$$\Leftrightarrow(P\wedge Q)\vee(P\wedge\square Q)\vee(P\wedge Q)\vee(\square P\wedge Q)$$
$$\Leftrightarrow(\square P\wedge Q)\vee(P\wedge\square Q)\vee(P\wedge Q)$$
$$\Leftrightarrow m_1\vee m_2\vee m_3$$
$$\Leftrightarrow\sum(1,2,3).$$

由此可知公式$\square P\wedge(P\to Q)\to Q$ 不是重言式，所以 Q 不是$\square P$ 和 $P\to Q$ 的有效结论，因而(2)中推理不正确，即 $\{\square P, P\to Q\} \mid\neq Q.$

在推理过程中，经常使用蕴含重言式和等值式，为了引用上的方便将它们加以编号归纳如表 5－14 和表 5－15，其中 A，B，C，D 为任意的命题公式.

表 5－14

E_1	$\square\square A\Leftrightarrow A$	双重否定律
E_2	$A\wedge B\Leftrightarrow B\wedge A$	交换律
E_3	$A\vee B\Leftrightarrow B\vee A$	
E_4	$(A\wedge B)\wedge C\Leftrightarrow A\wedge(B\wedge C)$	结合律
E_5	$(A\vee B)\vee C\Leftrightarrow A\vee(B\vee C)$	
E_6	$(A\wedge(B\vee C))\Leftrightarrow(A\wedge B)\vee(A\wedge C)$	分配律
E_7	$A\vee(B\wedge C)\Leftrightarrow(A\vee B)\wedge(A\vee C)$	
E_8	$\square(A\wedge B)\Leftrightarrow\square A\vee\square B$	德·摩根律

续表

E_9	$\neg(A\vee B)\Leftrightarrow\neg A\wedge\neg B$	
E_{10}	$A\wedge A\Leftrightarrow A$	幂等律
E_{11}	$A\vee A\Leftrightarrow A$	
E_{12}	$A\vee(B\wedge\neg B)\Leftrightarrow A$	同一律
E_{13}	$A\wedge(B\vee\neg B)\Leftrightarrow A$	
E_{14}	$A\vee(B\vee\neg B)\Leftrightarrow 1$	零律
E_{15}	$A\wedge(B\wedge\neg B)\Leftrightarrow 0$	
E_{16}	$A\rightarrow B\Leftrightarrow\neg A\vee B$	蕴含等值式
E_{17}	$\neg(A\rightarrow B)\Leftrightarrow A\wedge\neg B$	蕴含否定等值式
E_{18}	$A\rightarrow B\Leftrightarrow\neg B\rightarrow\neg A$	假言易位律
E_{19}	$A\leftrightarrow B\Leftrightarrow(A\rightarrow B)\wedge(B\rightarrow A)$	等价等值式
E_{20}	$A\leftrightarrow B\Leftrightarrow\neg A\leftrightarrow\neg B$	等价否定等值式
I_1	$A\wedge B\Rightarrow A$	化简律
I_2	$A\wedge B\Rightarrow B$	
I_3	$A\Rightarrow A\vee B$	附加律
I_4	$B\Rightarrow A\vee B$	
I_5	$\neg A\Rightarrow A\rightarrow B$	
I_6	$B\Rightarrow A\rightarrow B$	
I_7	$\neg(A\rightarrow B)\Rightarrow A$	
I_8	$\neg(A\rightarrow B)\Rightarrow\neg B$	
I_9	A，$B\Rightarrow A\wedge B$	合取引入
I_{10}	$\neg A$，$A\vee B\Rightarrow B$	析取三段论
I_{11}	A，$A\rightarrow B\Rightarrow B$	假言推理
I_{12}	$\neg B$，$A\rightarrow B\Rightarrow\neg A$	拒取式
I_{13}	$A\rightarrow B$，$B\rightarrow C\Rightarrow A\rightarrow C$	假言三段论
I_{14}	$A\vee B$，$A\rightarrow C$，$B\rightarrow D\Rightarrow C\vee D$	构造性二难

我们已经介绍了判断推理是否有效的三种方法，即真值表法、等值演算法和主析取范式法. 如果命题变元较多，以上三种方法的演算量太大. 因此，我们需要寻求行之有效的推理方法.

下面给出常用的推理规则：

（1） 前提引入规则（简称 P 规则）：

在证明的任何步骤上都可以引入前提.

（2） 结论引入规则（简称 T 规则）：

在证明的任何步骤上所得到的结论都可以作为后继证明的前提.

（3） 置换规则：

在证明的任何步骤上，命题公式中的子公式都可以用与之等值的公式置换.

在表 5 – 15 中每一个蕴含重言式称为推理定律，而表 5 – 14 中的每一个等值式都能产生两个推理定律.

1. 直接证法：利用表 5 – 14 和表 5 – 15 及其 P、T 规则、置换规则来构造命题序列以证明 A_1，A_2，…，$A_n \Rightarrow B$，这种证明方法称为直接证法.

例 3　试证 $P \wedge Q \rightarrow R$，$\square R \vee S$，$\square S \Rightarrow \square P \vee \square Q$.

证

(1) $\square R \vee S$　　P

(2) $\square S$　　P

(3) $\square R$　　T(1),(2)(析取三段论)

(4) $P \wedge Q \rightarrow R$　　P

(5) $\square(P \wedge Q)$　　T(3),(4)(拒取式)

(6) $\square P \vee \square Q$　　T(5)(德 · 摩根律)

2. 间接证法：

① 在推理中，经常遇到结论是蕴含式的情形，即具有如下形式的推理：

$$A_1 \wedge A_2 \wedge \cdots \wedge A_n \Rightarrow B \rightarrow C$$

因为 $A_1 \wedge A_2 \wedge \cdots \wedge A_n \rightarrow (B \rightarrow C)$

$\Leftrightarrow \square(A_1 \wedge A_2 \wedge \cdots \wedge A_n) \vee (\square B \vee C)$

$\Leftrightarrow \square(A_1 \wedge A_2 \wedge \cdots \wedge A_n \wedge B) \vee C$

$\Leftrightarrow (A_1 \wedge A_2 \wedge \cdots \wedge A_n \wedge B) \rightarrow C$.

所以，如果证明 $A_1 \wedge A_2 \wedge \cdots \wedge A_n \Rightarrow B \rightarrow C$，

只要证明 $A_1 \wedge A_2 \wedge \cdots \wedge A_n \wedge B \Rightarrow C$ 即可.

这种将结论中的蕴含式的前件作为前提的证明方法称为附加前提证明法. 简称 CP 规则.

例 4　证明 $P \rightarrow (Q \rightarrow R)$，$P \vee \square S$，$Q \vdash S \rightarrow R$

证

(1) S　　P(附加前提)

(2) $P \vee \square S$　　P

(3) P　　T(1),(2)析取三段论

(4) $P \rightarrow (Q \rightarrow R)$　　P

(5) $Q \rightarrow R$　　T(3),(4)假言推理

(6) Q　　P

(7) R　　T(5),(6)假言推理

(8) $S \rightarrow R$　　CP

例 5　如果电影已开演，则大门关着. 如果他们八点钟以前到达，则大门开着. 他们八点以前到达. 所以电影没开演. 说明这些语句构成一个正确推

理.

解 先将原子命题符号化.

P：电影开演.

Q：大门开着.

R：他们八点钟前到达.

前提：$P\to\square Q$，$R\to Q$，R

结论：$\square P$

证明

(1) R P

(2) $R\to Q$ P

(3) Q T(1),(2)I_{11}

(4) $P\to\square Q$ P

(5) $\square P$ T(3),(4)I_{12}

② 归谬法(反证法)

因为 $A_1\wedge A_2\wedge\cdots\wedge A_n\to B$

$\Leftrightarrow\square(A_1\wedge A_2\wedge\cdots\wedge A_n)\vee B$

$\Leftrightarrow\square(A_1\wedge A_2\wedge\cdots\wedge A_n\wedge\square B)$.

如果$(A_1\wedge A_2\wedge\cdots\wedge A_n\wedge\square B)$为矛盾式，

则 $A_1\wedge A_2\wedge\cdots\wedge A_n\to B$ 为重言式，

即 $A_1\wedge A_2\wedge\cdots\wedge A_n\Rightarrow B$.

故推理正确.

这种把$\square B$ 作为附加前提推出矛盾的证明方法称为归谬法，又称反证法.

例 6 试证明 $P\to\square Q$，$Q\vee\square R$，$R\wedge\square S\vdash\square P$

证

(1) P P(附加前提)

(2) $P\to\square Q$ P

(3) $\square Q$ T(1),(2)(假言推理)

(4) $Q\vee\square R$ P

(5) $\square R$ T(3),(4)(析取三段论)

(6) $R\wedge\square S$ P

(7) R T(6)(化简)

(8) $\square R\wedge R$ T(5),(8)(合取引入)

由(8)得出矛盾式，所以$\square P$ 为原前提的有效结论.

练习题 5－4

1. 给定下列前提，推出有效结论.

（1）$P \to R$，$Q \to R$，$P \vee Q$.

（2）$\square(P \vee \square Q)$，$\square R \vee S$，$\square S$.

（3）$P \to Q$，$\square Q \vee R$，$\square R \vee S$.

（4）$P \to (Q \to R)$，P，Q.

2. 用三种方法(真值表法,等值演算法,主析取范式法)证明下面推理是正确的：

若我学习，那么我数学不会不及格. 如果我不热衷于上网，那么我将学习. 我数学课不及格，因此我热衷于上网.

3. 用推理规则证明以下各式：

（1）$\square P \vee Q$，$R \to \square Q \vdash P \to \square R$.

（2）$P \to (Q \to R)$，P，$Q \vdash R \vee S$.

（3）$P \to Q \vdash P \to (P \wedge Q)$.

（4）$Q \to P$，$Q \leftrightarrow S$，$S \leftrightarrow t$，$t \wedge R \vdash P \wedge Q$.

（5）$P \to \square Q$，$\square R \vee Q$，$R \wedge \square S \vdash \square P$.

（6）$P \to Q$，$(\square Q \vee R) \wedge \square R$，$\square(\square P \wedge S) \Rightarrow \square R$.

4. 如果 A 曾到过受害者房间并且 11 点以前没离开，A 则能犯谋杀罪. A 曾到过受害者房间. 如果 A 在 11 点以前离开，看门人会看见他. 看门人没有看见他. 所以 A 犯了谋杀罪. 请用推理方法，证明有效结论.

第五节　谓词逻辑简介

逻辑学中的著名三段论：凡人要死，苏格拉底是人，所以苏格拉底要死. 显然，这个推理是正确的，但是在命题逻辑中却无法得到证明. 因为在命题逻辑中只能将推理中三个原子命题依次符号化为 P，Q，R，则$(P \wedge Q) \to R$ 为上述推理，但$(P \wedge Q) \to R$ 不是重言式. 这说明命题逻辑具有局限性. 在命题逻辑中，原子命题是不可分解的基本单位，而且不考虑命题之间的内在联系和数量关系，这就是命题逻辑有局限性的原因. 因此，我们将原子命题再细分出个体词、谓词和量词. 进一步揭示命题的内在联系和命题之间的逻辑关系.

一、个体、谓词和量词

1. **个体词**

我们把研究对象中可以独立存在的具体的或抽象的客体称为个体词. 例如，小刘，小张，中国，5，定义，马克思主义等都可以作为个体词. 表示具体或特定的客体的个体词称为个体常项，一般用小写英文字母 a，b，c…表示，表示抽象或泛指的个体词称为个体变项，常用 x，y，z…表示. 个体变项的取值范围称为个体域. 将宇宙间一切事物组成的个体域称为全总个体域.

2. 谓词

用来刻画个体词性质及个体词之间关系的词称为谓词. 常用大写英文字母表示谓词. 考虑下面三个命题:

(1) 零是自然数.

(2) 小刘与小陈是同学.

(3) x 在 y 与 z 之间.

在上例子中,零,小刘,小陈,x,y,z 都是个体词. 其中零,小刘,小陈是个体常项,而 x,y,z 是个体变项. "…是自然数"是谓词,记为 F,并用 $F(0)$ 表示(1)中命题. "…与…是同学"是谓词,记为 G,则(2)中命题符号化为 $G(a,b)$,其中 a:小刘,b:小陈. "…在…与…之间"是谓词,记为 H,则(3)中命题符号化为 $H(x,y,z)$.

表示具体性质或关系的谓词称为谓词常项,表示抽象的或泛指的性质或关系的谓词称为谓词变项. 例如 $F(0)$,$F(a,b)$,$H(3,4,5)$ 等等都是谓词常项,而 $A(x)$,$B(x,y)$ 等都是谓词变项,其中 x,y 是个体变项. 在一个谓词中,个体变项的数目称作谓词的元数. 如 $F(x)$ 为一元谓词,$G(x,y)$ 为二元谓词,$P(x_1,x_2,\cdots,x_n)$ 为 n 元谓词. 在谓词 $P(a_1,a_2,\cdots,a_k,x_{k+1},\cdots,x_n)$ 中,a_1,…,a_k 是个体常项,x_{k+1},…,x_n 是个体变项,则 $P(a_1,a_2,\cdots,a_k,x_{k+1},\cdots,x_n)$ 是 $(n-k)$ 元谓词. 我们把不带个体变项的谓词称为 0 元谓词. 如 $F(a)$,$P(a_1,a_2,\cdots,a_n)$ 都是 0 元谓词.

注意 0 元谓词是命题.

例 1 用谓词表达下列命题(符号化):

(1) 赵子龙救出阿斗.

(2) 他是跳高或蓝球运动员.

解 (1) 设 $F(x,y)$:x 救出 y. a:赵子龙,b:阿斗,则(1)中命题符号化为 $F(a,b)$.

(2) $G(x)$:x 是跳高运动员.

$H(x)$:x 是蓝球运动员.

a:他,

则(2)中命题符号化为 $G(a)\vee H(a)$.

3. 量词

我们把表示个体常项或个体变项之间数量关系的词称为量词. 量词分两种:

(1) 全称量词 对于日常生活中的"任意的"、"所有的"、"一切"、"凡是"、"每一个"、"都"等词称作全称量词,用符号"$\forall$"表示. $\forall x$ 表示个体域中的所有 x,而 $\forall xF(x)$ 表示个体域里所有个体,都有性质 F.

（2）存在量词　对于日常生活中的“存在”、“有些”、“至少有一个”等词称作存在量词，用符号“$\exists$”表示. $\exists x$ 表示个体域中至少有一个 x，而 $\exists xF(x)$：表示个体域中至少有一个 x 具有性质 F.

例 2　将下列命题符号化

（1）没有不犯错误的人.

（2）有些人既聪明又美丽.

解　首先考虑个体域 D.

（a）D_1：人类的集合.

$F(x)$：x 犯错误，$G(x)$：x 聪明，$H(x)$：x 美丽.

（1）在 D_1 中除人外，无别的东西，所以“没有不犯错误的人”符号化为：

$$\forall xF(x).$$

（2）在 D_1 中“有些人既聪明又美丽”符号化为：

$$\exists x(G(x)\wedge H(x)).$$

（b）D_2：全总个体域.

在 D_2 中除人外，还有万物，因此(1)，(2)符号化时，必须将人先分离出来. 令 $M(x)$：x 是人，在 D_2 中，(1)，(2)可分别重述如下：

（1）对于宇宙间一切事物，如果事物是人，则他要犯错误.

（2）在万物中，存在着既聪明又美丽的人，故(1)，(2)符号化应分别为

$$\forall x(M(x)\rightarrow F(x)),$$

$$\exists x(M(x)\wedge G(x)\wedge H(x)).$$

在例 2 中，当个体域 D 是全总个体域时，要将人从其他事物中区别出来，为此引进了谓词 $M(x)$，像这样的谓词称为特性谓词. 在命题符号化时一定要正确使用特性谓词.

请读者注意以下几点：

（1）如果没有明确个体域，则认为个体域是全总个体域.

（2）在全总个体域中，要引进特性谓词.

（3）对全称量词，特性谓词常作蕴含式的前件.

（4）对存在量词，特性谓词常作合取项.

二、谓词公式

在命题逻辑中，我们定义了命题公式，从而进行了演算和推理. 为了进行谓词逻辑演算和推理，下面给出谓词公式等有关的概念.

定义 1

（1）一个命题常元是原子谓词公式；

（2）一个命题变元是原子谓词公式；

（3）由 n 个个体变项 x_1，x_2，…，x_n 和 n 元谓词 P 构成的命题函数 $P(x_1,x_2,\cdots,x_n)$ 也是一个原子谓词公式.

定义 2

（1）一个原子谓词公式是一个谓词公式；

（2）若 A 是谓词公式，则$\neg A$ 也是谓词公式；

（3）若 A 和 B 是谓词公式，则 $A\wedge B$、$A\vee B$、$A\to B$、$A\leftrightarrow B$ 也是谓词公式；

（4）若 A 是谓词公式，x 是 A 中的个体变项，则 $\forall xA$，和 $\exists xA$ 也是谓词公式；

（5）只有有限次地运用规则（1），（2），（3），（4）所得到的符号串才是谓词公式.

例如，$F(a,b)$，$A(x)\wedge B(x)$，$\forall x(M(x)\to N(x))$，$\exists x(F(x)\wedge G(x)\vee \forall yN(y))$，$\forall x\exists y(A(x)\wedge B(y)\to H(x,y))$ 等都是谓词公式.

定义 3 在谓词公式 $\forall xA$ 或 $\exists xA$ 中称 x 为指导变元，公式 A 称为量词 $\forall x$ 或 $\exists x$ 的辖域. 在辖域中，x 的所有出现称为 x 在 A 中的约束出现. 约束出现的变元称为约束变元. A 中不是约束出现的其他变元称为自由出现. 自由出现变元称为自由变元.

例 3 指出下列公式的指导变元，辖域，约束变元和自由变元.

（1）$\forall x(A(x)\to\exists yB(x,y))$.

（2）$\forall x\forall y(P(x,y)\wedge Q(y,z))\wedge(\exists x)P(x,y)$.

解 （1）$\forall x$ 中指导变元为 x，$\forall x$ 的辖域是 $A(x)\to\exists yB(x,y)$，$\exists y$ 中的指导变元为 y，$\exists y$ 的辖域是 $B(x,y)$. 对于 $\exists y$ 而言，y 为约束出现，x 是自由出现，所以 y 为约束变元，而 x 是自由变元. 对于 $\forall x$ 的辖域来说，x 和 y 都是约束出现. x 约束出现两次，y 约束出现一次.

（2）$\forall x$ 中指导变元为 x，$\forall x$ 的辖域是

$$\forall y(P(x,y)\wedge Q(y,z)),$$

其中 x，y 是约束出现，z 是自由出现，即 x 与 y 是约束变元，z 是自由变元. $\exists x$ 中指导变元为 x，$\exists x$ 的辖域 $P(x,y)$. 其中 x 是约束变元，y 为自由变元. 在整个公式中，x 是约束出现，y 既是约束出现，又是自由出现，z 是自由出现.

从例 3 中可以看出，在谓词公式中，有的个体变项既是约束变元，又是自由变元，为了避免混淆，采用下面两个规则：

（1）**换名规则** 将量词辖域中某个约束出现的个体变项及相应指导变元换成本辖域中未曾出现过的个体变元，其余不变.

（2）**代入规则** 对自由变元进行代入，即对自由变元用与原公式中所有

变元符号不同的符号去代替，并且处处代替.

例 4　将下面公式化成与之等值的公式，使它不含有既是约束出现的又是自由出现的个体变项.

$$\forall xP(x,y)\to\exists yQ(x,y,z).$$

解　$\forall xP(x,y)\to\exists yQ(x,y,z)\Leftrightarrow\forall tP(t,y)\to\exists wQ(x,w,z)$　（换名规则）

或　$\forall xP(x,y)\to\exists yQ(x,y,z)\Leftrightarrow\forall xP(x,u)\to\exists yQ(v,y,z)$　（代替规则）

三、谓词演算的等值式与蕴含式

设个体域 D 是有限的，$D=\{a_1,a_2,\cdots,a_n\}$，

则　$\forall xA(x)\Leftrightarrow A(a_1)\wedge A(a_2)\wedge\cdots\wedge A(a_n).$　(5.1)

$\exists xA(x)\Leftrightarrow A(a_1)\vee A(a_2)\vee\cdots\vee A(a_n).$

例如，$D=\{a,b,c\}$，$A(x)$：x 是男生，

则　$\forall xA(x)$，即是 $A(a)\wedge A(b)\wedge A(c)$.

$\exists xA(x)$，即是 $A(a)\vee A(b)\vee A(c)$.

在谓词公式中，当个体变项由确定的个体取代，命题变元用确定的命题取代时，称作对谓词公式的解释(或赋值).

设解释 I 如下：

$$D=\{2,3\},\ f(2)=3,\ f(3)=2,\ F(2,2)=1,\ F(2,3)=0,$$
$$F(3,2)=0,\ F(3,3)=1.$$

例 5　试求下面公式在 I 下的真值

(1) $\forall x\exists yF(y,f(x))$.

(2) $\exists y\forall xF(y,f(x))$.

解　(1) $\forall x\exists yF(y,f(x))$

$\Leftrightarrow\forall x(F(2,f(x))\vee F(3,f(x)))$

$\Leftrightarrow(F(2,f(2))\vee F(3,f(2)))\wedge(F(2,f(3))\vee F(3,f(3)))$

$\Leftrightarrow(F(2,3)\vee F(3,3))\wedge(F(2,2)\vee F(3.2))$

$\Leftrightarrow(0\vee 1)\wedge(1\vee 0)$

$\Leftrightarrow 1\wedge 1$

$\Leftrightarrow 1.$

(2) $\exists y\forall xF(y,f(x))$

$\Leftrightarrow\exists y(F(y,f(2))\wedge F(y,f(3)))$

$\Leftrightarrow(F(2,f(2))\wedge F(2,f(3)))\vee(F(3,f(2))\wedge F(3,f(3)))$

$\Leftrightarrow(F(2,3)\wedge F(2,2))\vee(F(3,3)\wedge F(3,2))$

$\Leftrightarrow(0\wedge 1)\vee(1\wedge 0)$

$$\Leftrightarrow 0 \vee 0$$
$$\Leftrightarrow 0.$$

本例题的结果说明量词的次序不能随意颠倒，即量词是有序的.

定义 4 设 A 为一个谓词公式，若 A 在任何解释下，A 的真值恒为真，则称 A 是永真式；若 A 的真值恒为假，则称 A 是永假式.

定义 5 设 A，B 是两个谓词公式，若 $A \to B$ 是永真式，则称 A 与 B 是等值的. 记作 $A \Leftrightarrow B$.

在谓词逻辑等值演算过程中，常常需要下面的重要等值式，请读者熟记.

$$\begin{aligned}
&E_{21} \quad \neg \forall x A(x) \Leftrightarrow \exists x \neg A(x).\\
&E_{22} \quad \neg \exists x A(x) \Leftrightarrow \forall x \neg A(x).\\
&E_{23} \quad \forall x (A(x) \wedge B(x)) \Leftrightarrow \forall x A(x) \wedge \forall x B(x).\\
&E_{24} \quad \exists x (A(x) \vee B(x)) \Leftrightarrow \exists x A(x) \vee \exists x B(x).\\
&E_{25} \quad \forall x (A \vee B(x)) \Leftrightarrow A \vee \forall x B(x).\\
&E_{26} \quad \exists x (A \wedge B(x)) \Leftrightarrow A \wedge \exists x B(x).\\
&E_{27} \quad \forall x B(x) \to A \Leftrightarrow \exists x (B(x) \to A).\\
&E_{28} \quad \exists x (A(x) \to B(x)) \Leftrightarrow \forall x A(x) \to \exists x B(x).\\
&E_{29} \quad \forall x (B(x) \to A) \Leftrightarrow \exists x B(x) \to A.\\
&E_{30} \quad \forall x (A \to B(x)) \Leftrightarrow A \to \forall x B(x).\\
&E_{31} \quad \exists x (A \to B(x)) \Leftrightarrow A \to \exists x B(x).
\end{aligned} \tag{5.2}$$

在公式 E_{25}，E_{26}，E_{27}，E_{29}，E_{30}，E_{31} 中，$B(x)$ 为有 x 自由出现的任意的公式，A 中则不含有 x 的出现.

定义 6 设 A，B 是两个谓词公式，若 $A \to B$ 为永真式，则称 A 永真蕴含 B. 记作 $A \Rightarrow B$.

在谓词逻辑的推理中，经常用到下面的永真蕴含式：

$$\begin{aligned}
&I_{15} \quad \forall x A(x) \vee \forall x B(x) \Rightarrow \forall x (A(x) \vee B(x)).\\
&I_{16} \quad \exists x (A(x) \wedge B(x)) \Rightarrow \exists x A(x) \wedge \exists x B(x).\\
&I_{17} \quad \exists x A(x) \to \forall x B(x) \Rightarrow \forall x (A(x) \to B(x)).\\
&I_{18} \quad \forall x (A(x) \to B(x)) \Rightarrow \forall x A(x) \to \forall x B(x).\\
&I_{19} \quad \exists x (A(x) \to B(x)) \Rightarrow \exists x A(x) \to \exists x B(x).
\end{aligned} \tag{5.3}$$

例 6 **证明** $\exists x A(x) \to \forall x B(x) \Rightarrow \forall x (A(x) \to B(x))$.

证
$$\begin{aligned}
\exists x A(x) \to \forall x B(x) &\Leftrightarrow \neg \exists x A(x) \vee \forall x B(x) && (E_{16})\\
&\Leftrightarrow \forall x \neg A(x) \vee \forall x B(x) && (E_{22})\\
&\Rightarrow \forall x (\neg A(x) \vee B(x)) && (I_{15})
\end{aligned}$$

$$\Leftrightarrow \forall x(A(x) \to B(x)). \qquad (E_{16})$$

四、前束范式

定义 7　一个公式，如果量词均在全式的开头，它们的作用域延伸到整个公式的末尾，则该公式称作前束范式.

例如，$\forall x \exists y(F(x,y) \wedge H(x) \to S(x,y))$，$\forall x \exists y \exists z(F(x) \vee G(z) \wedge H(y) \to S(x,y,z))$

都是前束范式，而

$$\forall x \exists y(F(x,y) \wedge H(x) \to \forall y S(x,t)),$$
$$\forall x \forall y(F(x) \vee G(z) \wedge H(y) \to \exists z S(x,y,z))$$

都不是前束范式.

定理 1（前束范式存在定理）

任意一个谓词公式都存在与之等值的前束范式.

例 7　求公式的前束范式

$$\forall x F(x,y) \to \exists y G(x,y)$$

解

$$\forall x F(x,y) \to \exists y G(x,y)$$
$$\Leftrightarrow \forall t F(t,y) \to \exists u G(x,u) \qquad \text{（换名规则）}$$
$$\Leftrightarrow \exists t(F(t,y) \to \exists u G(x,u)) \qquad (E_{27})$$
$$\Leftrightarrow \exists t \exists u(F(t,y) \to G(x,u)) \qquad (E_{31})$$

或者

$$\forall x F(x,y) \to \exists y G(x,y)$$
$$\Leftrightarrow \exists x F(x,t) \to \exists y G(u,y) \qquad \text{（代替规则）}$$
$$\Leftrightarrow \exists x \exists y(F(x,t) \to G(w,y)). \qquad (E_{27},E_{31})$$

五、谓词演算的推理理论

谓词演算的很多等值式和永真蕴含式是命题演算有关公式的推广. 谓词演算的推理是命题演算的扩张，所以命题演算中的推理规则，如 P 规则、T 规则和 CP 规则都可以作为谓词演算中的推理规则. 除此以外，我们还需使用下面四条重要规则.

1. 全称量词消去规则（简称 US 规则）

$$\frac{\forall x A(x)}{\therefore A(c)} \quad \text{或} \quad \frac{\forall x A(x)}{\therefore A(y)},$$

两式成立的条件是：

（1）在第一式中，c 为任意个体常项.

（2）在第二式中，y 为任意不在 $A(x)$ 中约束出现的个体变项.

(3) x 是 $A(x)$ 中自由出现的个体变项.

2. 全称量词引入规则(简称 UG 规则)

$$\frac{A(y)}{\therefore\ \forall xA(x)}$$

该式成立的条件是:

(1) y 是 $A(y)$ 中自由出现的个体变项,不论 y 取何值时,$A(y)$ 均为真.

(2) 取代 y 的 x 不能在 $A(y)$ 中约束出现.

3. 存在量词引入规则(简称 EG 规则)

$$\frac{A(c)}{\therefore\ \exists xA(x)}.$$

该式成立的条件是:

(1) c 是使 $A(x)$ 为真的特定的个体常项.

(2) 取代 c 的 x 不能在 $A(c)$ 中出现.

4. 存在量词消去规则(简称 ES)

$$\frac{\exists xA(x)}{\therefore A(c)}$$

该式成立的条件是:

(1) c 不在 $A(x)$ 中出现.

(2) c 是使 $A(x)$ 为真的特定的个体常项.

(3) $A(x)$ 中除 x 外,还有其他自由出现的个体变项时,该规则不能使用.

读者注意:US,UG,ES,EG 规则仅使用于前束范式.

例 8 证明下面推理.

凡人要死,苏格拉底是人,所以苏格拉底要死.

证明 将命题符号化

$M(x)$:x 是人;

$N(x)$:x 要死;

a:苏格拉底.

前提:$\forall x(M(x)\to N(x))$,$M(a)$

结论:$N(a)$

(1)	$\forall x(M(x)\to N(x))$	P
(2)	$M(a)\to N(a)$	US
(3)	$M(a)$	P
(4)	$N(a)$	$T(2),(3),I$

例 9 证明

$$\forall x(F(x)\to G(x))\wedge\exists x(F(x)\wedge H(x))\Rightarrow\exists x(G(x)\wedge H(x)).$$

证明

(1) $\exists x(F(x) \wedge H(x))$ 　　P

(2) $F(c) \wedge H(c)$ 　　$T(1)$，ES

(3) $\forall x(F(x) \to G(x))$ 　　P

(4) $F(c) \to G(c)$ 　　$T(3)$，US

(5) $F(c)$ 　　$T(2)$，I

(6) $G(c)$ 　　$T(4)$，(5)，I

(7) $H(c)$ 　　$T(2)$，I

(8) $(G(c) \wedge H(c))$ 　　$T(6)$，(7)，I

(9) $\exists x(G(x) \wedge H(x))$ 　　$T(8)$，EG

注意　在证明序列中先引进带存在量词的前提.

例 10　证明　$\forall x(F(x) \to M(x)) \Rightarrow \forall xF(x) \to \forall xM(x)$.

证明

(1) $\forall x(F(x) \to M(x))$ 　　P

(2) $F(y) \to M(y)$ 　　$T(1)$，US

(3) $\forall xF(x)$ 　　**附加前提**

(4) $F(y)$ 　　$T(3)$，US

(5) $M(y)$ 　　$T(4)$，(5)，I

(6) $\forall xM(x)$ 　　$T(5)$，UG

(7) $\forall xF(x) \to \forall xM(x)$ 　　CP

练习题 5－5

1. **在谓词逻辑中将下面命题符号化.**

(1) **小王不是博士.**

(2) **凡是有理数都能被** 2 **整除.**

(3) **有的有理数能被** 2 **整除.**

(4) **有的兔子比所有的乌龟跑得快.**

2. **指出下列公式中的指导变元，量词的辖域，各个体变项的自由出现和约束出现.**

(1) $\forall x(A(x) \to B(y)) \to \exists x(F(x) \wedge G(x))$.

(2) $\forall x(x = y \wedge x^2 + x < 5 \to x < z) \to x = 5y^2$.

(3) $\forall x \exists y(F(x,y) \wedge G(y,z)) \vee \exists xH(x,y,z)$.

3. **给定个体域** $D = \{2,3\}$，$a = 0$，$f(2) = 3$，$f(3) = 2$，$s(2) = 0$，$s(3) = 1$，$G(2,2) = 1$，$G(3,2) = 1$，$L(2,2) = L(3,3) = 1$，$L(2,3) = L(3,2) = 0$.

在上述解释下，求下列各式的真值

(a) $\forall x(S(x) \wedge G(x,a))$.

(b) $\exists x(S(f(x)) \wedge G(x,f(x)))$.

(c) $\forall x \exists y L(x,y)$.

4. **设个体域** $D=\{a,b,c\}$，**消去下列各式的量词：**

(1) $\forall x F(x) \to \forall y G(y)$.

(2) $\exists x(F(x,y) \to \forall y G(y))$.

(3) $\exists x \forall y(F(x) \wedge G(y))$.

(4) $\forall x \forall y(F(x) \vee G(y))$.

5. **求下列各式的前束范式：**

(1) $\forall x F(x) \vee \square \exists x G(x)$.

(2) $\forall x(F(x) \to \exists y G(x,y))$.

(3) $\square(\forall x F(x,y) \vee \exists y G(x,y))$.

(4) $\exists x P(x) \to \forall x Q(x) \vee \exists y R(y)$.

6. **学术委员会的每个成员都是博士，并且是教授. 有些成员是青年人，因此有的成员是青年教授. 请用谓词推理理论证明上述推理.**

7. **试证明下列各式**

(1) $\exists x(A(x) \wedge B(x)) \Rightarrow \exists x A(x) \wedge \exists x B(x)$.

(2) $\forall x(\square A(x) \to B(x)) \wedge \forall x \square B(x) \Rightarrow \exists x A(x)$.

(3) $\forall x(F(x) \vee G(x)) \Rightarrow \square \forall x F(x) \to \exists x G(x)$.

(4) $\exists x F(x) \to \forall x G(x) \Rightarrow \forall x(F(x) \to G(x))$.

(5) $\forall x(P(x) \to Q(y) \wedge R(x)) \wedge \exists x P(x) \Rightarrow Q(y) \wedge \exists x(P(x) \wedge R(x))$.

复 习 题 五

1. **将下列命题符号化.**

(1) **除非** $1+1=3$，**否则太阳从西边升起.**

(2) **王刚与李强在打球.**

(3) **他住** 101 **房间或** 102 **房间.**

(4) **四边形** $ABCD$ **是平行四边形，当且仅当它的对边平行.**

(5) **人人遵守宪法.**

(6) **乌鸦都是黑色的.**

(7) **在美国留学的学生未必都是亚洲人.**

(8) **有的男同学留着长发.**

(9) **大学生都勤奋，王华不勤奋，所以王华不是大学生.**

(10) **相等的两个角未必都是对顶角.**

2. **判断下列公式的类型**

(1) $P \leftrightarrow Q \to (P \wedge Q) \vee (\neg P \wedge \neg Q)$.

(2) $\neg(P \vee Q) \leftrightarrow \neg P \vee \neg Q$.

(3) $(P \vee Q) \wedge (P \to R) \wedge (\neg Q \vee R) \to R$.

(4) $Q \vee \neg((\neg P \vee Q) \wedge P)$.

(5) $\neg(P\to Q)\wedge Q$.

3. **求下列公式的主析取范式和主合取范式**.

(1) $R\to(P\vee Q)$.

(2) $\neg(P\to Q)\wedge Q$.

(3) $P\vee(P\to(P\vee Q))$.

(4) $(P\to Q)\wedge(P\to R)$.

(5) $(P\vee Q)\wedge(P\to R)\wedge(Q\to S)$.

4. **判断下列公式是否等值**

(1) $(P\to Q)\wedge(P\to R)$ **与** $Q\to P\wedge R$.

(2) $\neg(P\leftrightarrow Q)$ **与** $(P\vee Q)\wedge\neg(P\wedge Q)$.

(3) $P\vee(P\to(P\vee Q))$ **与** $\neg P\vee\neg Q\vee(P\wedge Q)$.

(4) $P\vee(Q\wedge\neg R)$ **与** $((P\vee Q)\to R)\to P$.

5. **求下列公式的前束范式**

(1) $\forall xP(x)\to\exists yQ(x,y)$.

(2) $\exists x(\neg\exists yP(x,y))\to(\exists ZQ(z)\to R(x)))$.

(3) $\exists x(P(x)\to\forall y(Q(y)\wedge H(x,y)))$.

6. **构造下面推理的证明**

(1) $(S\to\neg Q)\wedge(R\vee S)\wedge\neg R\wedge(\neg P\leftrightarrow Q)\Rightarrow P$.

(2) $(P\vee Q)\wedge(P\to\neg R)\wedge(S\to T)\wedge(\neg S\to R)\wedge\neg T\Rightarrow Q$.

(3) $(W\to(\neg(R\wedge S)\to\neg Q))\wedge W\wedge\neg S\Rightarrow\neg Q$.

(4) $(\neg P\vee Q)\wedge(R\to\neg Q)\Rightarrow P\to\neg R$.

7. **构造下面推理证明**

(1) **前提**：$\exists xF(x)\to\forall y((F(y)\vee G(y))\to R(y))$，$\exists xF(x)$.

结论：$\exists xR(x)$.

(2) **前提**：$\forall x(F(x)\to(G(y)\wedge R(x)))$，$\exists xF(x)$.

结论：$\exists x(F(x)\wedge R(x))$.

(3) **前提**：$\forall x(F(x)\vee G(x))$，$\forall x(\neg G(x)\vee\neg R(x))$.

$\forall xR(x)$.

结论：$\forall xF(x)$.

(4) **前提**：$\forall x(P(x)\vee Q(x))$.

结论：$\neg(\forall xP(x))\to\exists xQ(x)$.

习题答案

第一章　习 题 答 案

练习题 1－1

1. 能组成集合的有：(1)、(2)、(3)、(4)、(5).

不能组成集合的有：(6)、(7). 在(6)、(7)中，“高个人”和“难题”是模糊的，不确定的.

2. 不正确的是：(1)、(5). 正确的是：(2)、(3)、(4).

3，4，5，6，略.

练习题 1－2

1. $A \cup B = \{0,1,2,3,4,6\}$.

$A \cap B = \{2,4\}$.

$A - B = \{0,1,3\}$.

$B - A = \{6\}$.

$A \oplus B = \{0,1,3,6\}$.

2. $A \cup B = \{a,b,c,l,k,o\}$.

$A \cap B = \{b,k\}$.

$A - B = \{o\}$.

$B - A = \{a,c,l\}$.

$A \oplus B = \{a,c,l,o\}$.

3. 略.

4. (1) $A \cup B$；(2) $A \cup B$；(3) $A \cup B$；(4) $A \cup B$；(5) $\varnothing$.

5，6，7. 略.

8. (a) $\{0,1,2,3,4,5,6,7,8,9,12,15,16,18,21,24,27,30,32,64\}$.

(b) $\varnothing$.

(c) $\{4,5\}$.

(d) $\{0,1,2,3,4,5,6,8,16,32,64\}$.

9. (a) 不一定，例如 $A=\{a\}$，$B=\{a,c\}$，$C=\{c\}$，则有 $A\cup B=A\cup C$，但 $B\neq C$.

(b) 不一定，例如 $A=\varnothing$，$B=\{a\}$，$C=\{a,b\}$，则 $A\cap B=A\cap C=\varnothing$，但 $B\neq C$.

(c) 一定有 $B=C$ 这是因为，对于 $\forall x\in B$，

(1) 若 $x\in A\Rightarrow x\in A\cap B\Rightarrow x\notin A\oplus B\Leftrightarrow x\notin A\oplus C$，
由 $x\in A$ 且 $x\notin A\oplus C\Rightarrow x\in A\cap C\Rightarrow x\in C$，所以 $B\subseteq C$.

(2) $x\notin A\Rightarrow x\notin A\cap B$，因为 $x\in B\Rightarrow x\in A\cup B$.
由 $x\notin A\cap B$ 且 $x\in A\cup B\Rightarrow x\in A\oplus B\Rightarrow x\in A\oplus C$.
但 $x\notin A$ 且 $x\in A\oplus C\Rightarrow x\in C$.
即 $B\subseteq C$.
故 $A\oplus B=A\oplus C$ 时，必有 $B=C$.

练习题 1-3

1. $\rho(A)\times A=\{(\varnothing,a),(\varnothing,b),(\{a\},a),(\{b\},a),(\{a\},b),(\{b\},b),(\{a,b\},a),(\{a,b\},b)\}$；

$A\times\rho(A)=\{(a,\varnothing),(b,\varnothing),(a,\{a\}),(a,\{b\}),(b,\{a\}),(b,\{b\}),(a,\{a,b\}),(b,\{a,b\})\}$；

$\rho(A)\times\rho(A)=\{(\varnothing,\varnothing),(\varnothing,\{a\}),(\varnothing,\{b\}),(\varnothing,\{a,b\}),(\{a\},\{a\}),(\{a\},\{b\}),(\{a\},\{a,b\}),(\{a\},\varnothing),(\{b\},\varnothing),(\{b\},\{a\}),(\{b\},\{b\}),(\{b\},\{a,b\}),(\{a,b\},\varnothing),(\{a,b\},\{a\}),(\{a,b\},\{b\}),(\{a,b\},\{a,b\})\}$.

2. (a) $A\times\{1\}\times B=\{(0,1,1),(0,1,2),(1,1,1),(1,1,2)\}$.

(b) $A^2\times B=\{(0,0,1),(0,0,2),(1,1,1),(1,1,2),(0,1,2),(1,0,1),(1,0,2)\}$.

(c) $\{((1,0),(1,0)),((1,0),(1,1)),((1,0)(2,0)),((1,0),(2,1)),((1,1),(1,0)),((1,1),(1,1)),((1,1),(2,0)),((1,1),(2,1)),((2,0),(1,0)),((2,0),(1,1)),((2,0),(2,0)),((2,0),(2,1)),((2,1),(1,0)),((2,1),(1,1)),((2,1),(2,0)),((2,1),(2,1))\}$.

5. $\rho(A)=\{\varnothing\}$. $\rho(\rho(A))=\{\varnothing,\{\varnothing\}\}$. $\rho(\rho(\rho(A)))=\{\varnothing,\{\varnothing\},\{\{\varnothing\}\},\{\varnothing,\{\varnothing\}\}\}$

6. (a)、(b)、(c) 都不成立；(d)、(e) 都成立.

练习题 1－4

1. (a) 不一定. 若 $A=\mathbf{N}$，$B=\{x \mid x$ 是小于 0 的整数$\}$，则 $A\cap B=\varnothing$.

   (b) 不一定. 若 $A=\mathbf{Q}$，$B=Q^{*}=\mathbf{Q}-\{0\}$，则 $A-B=\{0\}$.

   (c) 一定成立.

3. (1) $\left[\frac{1-n}{n}, \frac{n-1}{n}\right]$；$(-1,1)$

   (2) $\{0\}$，$\{0\}$.

4. $\bigcup_{n=1}^{\infty} A_n=\{-1,1\}-\{-1\}-\{1\}=(-1,1)$.

   $\bigcap_{n=1}^{\infty} A_n=\{0\}$.

复 习 题 一

1. (1)、(3) 不成立，其余均成立.

   对于(1)应为 $\{a\}\in\{\{a\}\}$.

   对于(3)应为 $\{a\}\in\{\{a\}\}$.

2. (1) 不一定.

   若$A=\{0\}$，$B=\{0,\{0\}\}$，$C=\{1,\{0,\{0\}\}\}$，则

   $A\in B$，$B\in C$，而 $A\notin C$.

   (2) 真. 因为 $B\subseteq C$，故 $A\in B\Rightarrow A\in C$.

   (3) 假. 例如 $A=\{a\}$，$B=\{b,\{a\}\}$，$C=\{d,b,\{a\}\}$，则 $A\in B$，$B\subseteq C$，但 $A\notin C$.

   (4) 假. 例如 $A=\{1\}$，$B=\{1,2\}$，$C=\{1,2,3\}$，则 $A\subseteq B$，$B\subseteq C$，但 $A\notin C$.

   (5)、(6) 略.

   (7) 假. 例如 $A=\varnothing$，$B=\{\varnothing,1\}$ 则 $A\subseteq B$ 且 $A\in B$.

10. (a) $\varnothing$，$\{\varnothing\}$.

    (b) $\varnothing$，$\{\varnothing\}$，$\{\{\varnothing\}\}$，$\{\varnothing,\{\varnothing\}\}$.

    (c) $\varnothing$，$\{\{a\}\}$，$\{\{\varnothing,a\}\}$，$\{\{a\},\{\varnothing,a\}\}$.

    (d) $\varnothing$，$\{\{a,b\}\}$.

11. (a) 若 $A=\{a\}$，$B=\{b\}$，$C=\{\{a\}\}$，则

    当 $A\in B$ 且 $B\notin C$，有 $A\in C$；

    (b) 若 $A=\{a\}$，$B=\{\{a\},b\}$，$C=\{\{a\},c\}$，则

    当 $A\in B$ 且 $B\notin C$，有 $A\in C$；

(c) 若 $A=\varnothing$，$B=\{b\}$，$C=\{c\}$，则
当 $A\subset B$ 且 $B\notin C$，有 $A\in C$.

12. $\varnothing\cap\{\varnothing\}=\varnothing$；$\{\varnothing\}\cap\{\varnothing\}=\{\varnothing\}$；
$\{\varnothing,\{\varnothing\}\}-\varnothing=\{\{\varnothing\},\varnothing\}$
$\{\varnothing,\{\varnothing\}\}-\{\varnothing\}=\{\{\varnothing\}\}$
$\{\varnothing,\{\varnothing\}\}-\{\{\varnothing\}\}=\{\varnothing\}$

13. (1) E；(2) $\varnothing$；(3) $A\cup B$；(4) $A\cup B$.

14. (1) $\bigcup_{k=1}^{n}A_k=\left\{0,\frac{1}{2^{n-1}},\frac{2}{2^{n-1}},\frac{3}{2^{n-1}},\cdots,\frac{2^{n-1}-1}{2^{n-1}},1\right\}$.

(2) $\bigcap_{k=1}^{n}A_k=\{0,1\}$.

(3) $\bigcup_{k=1}^{\infty}A_k=\left\{0,1,\frac{1}{4},\frac{3}{4},\frac{1}{8},\frac{3}{8},\frac{5}{8},\frac{7}{8},\cdots,1\right\}$.

(4) $\bigcap_{k=1}^{\infty}A_k=\{0,1\}$.

15. (1) $\{\varnothing,\{a\},\{b\},\{c\},\{a,b\},\{a,c\},\{b,c\},\{a,b,c\}\}$
(2) $\{\varnothing,\{\{c\}\},\{\{a,b\}\},\{\{a,b\},\{c\}\}\}$
(3) $\{\varnothing,\{a\},\{\{b\}\},\{a,\{b\}\}\}$
(4) $\{\varnothing,\{1\},\{\varnothing\},\{\{\varnothing\}\},\{1,\varnothing\},\{1,\{\varnothing\}\},\{\varnothing,\{\varnothing\}\},\{1,\varnothing,\{\varnothing\}\}\}$

16. $\rho(S_{n+1})=\rho(S_n)\cup\{\{a_{n+1}\},\{a_0,a_{n+1}\},\{a_1,a_{n+1}\},\cdots,\{a_n,a_{n+1}\},\{a_0,a_1,a_{n+1}\},\{a_0,a_2,a_{n+1}\},\cdots,\{a_0,a_n,a_{n+1}\},\cdots,\{a_0,a_1,\cdots,a_n,a_{n+1}\}\}$

17. (2)、(3)、(7)、(8)、(9) 都是正确的；
(1)、(4)、(5)、(10) 都是错误的.

第二章　习题答案

练习题 2-1

1. (a) $S=\{(0,0),(0,2),(2,0),(2,2)\}$.
(b) $S=\{(1,1),(4,2)\}$.

2. $R\cup S=\{(1,2),(1,3),(2,4),(3,3),(4,2)\}$.
$R\cap S=\{(2,4)\}$.
$R-S=\{(1,2),(3,3)\}$.

$D(R)=\{1,2,3\}$.

$D(S)=\{1,2,4\}$.

$D(R\cup S)=\{\{1,2,3,4\}$.

$C(R)=\{2,3,4\}$.

$C(S)=\{2,3,4\}$.

$C(R\cap S)=\{4\}$.

3. (a)

$$S_R=\begin{pmatrix}0&1&0\\0&1&0\\1&0&0\end{pmatrix}.$$

(b)

$$S_R=\begin{pmatrix}0&1&1&1\\0&1&1&1\\0&1&1&1\\0&1&1&1\end{pmatrix}$$

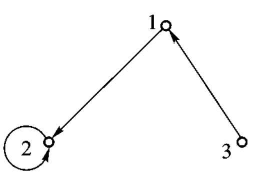
(c)

$$S_R=\begin{pmatrix}1&1&0\\1&1&1\\1&1&1\\1&1&1\end{pmatrix}$$

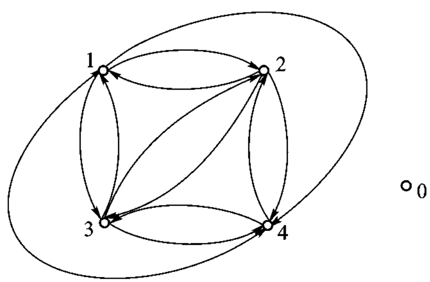
(d)

$$S_R=\begin{pmatrix}0&0&0&0&0&0&0\\0&0&0&0&0&0&0\\0&0&0&1&0&1&0\\0&0&0&0&0&0&0\\0&0&0&0&0&0&0\\0&0&0&0&0&0&0\\0&0&0&0&0&0&0\end{pmatrix}$$

4.



(a)



(b)

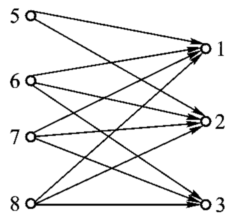
6. $R_1\circ R_2=\{(b,a),(b,d)\}$.

$R_2\circ R_1=\{(d,a)\}$.

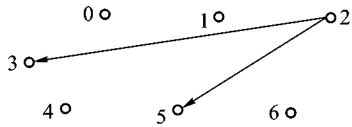
$R_1^{-1}=\{(b,b),(c,b),(a,c)\}$.

$R_2^{-1}=\{(a,b),(d,c),(a,c),(c,d)\}\}$.

$R_1^2=\{(b,b),(b,c),(b,a)\}$.



(c)



(d)

$R_2^3 = \{(c,d), (c,a), (d,c)\}$.

8.

$$\boldsymbol{M}_R = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\boldsymbol{M}_S = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\boldsymbol{M}_{R\circ S} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

练习题 2－2

1. 略.
2. (1)、(2) 正确.
   (3)、(4) 不正确.
   (5) $R\cap S$ 是传递的，正确，
   $R\cup S$ 是传递的，不正确.
3. 自反的有：S.
   对称的：S.
   传递的：R，S，T.
   非对称的：R，T.
4. 因为：$(3,1)\in R$ 且 $(1,2)\in R$，但 $(3,2)\notin R$，所以 R 不是传递的.
   $R_1 = \{(1,1), (4,2), (3,2), (4,1)\}\cup R$.

$R_2 = A \times A$.

5. 对称的：$R = R^{-1}$.

6. (a) 传递的，非对称的.

(b) 自反的，对称的，传递的.

(c) 对称的，非自反的.

(d) 非对称的.

(e) 非自反的，传递的.

(f) 非自反的，非对称的.

练习题 2-3

1. (1) $r(R) = R \cup Q = \{(a_1,a_1),(a_2,a_2),(a_3,a_3),(a_4,a_4),(a_1,a_2),(a_1,a_3),(a_2,a_3),(a_3,a_4)\}$.

$s(R) = R \cup R^{-1} = \{(a_1,a_2),(a_2,a_1),(a_1,a_3),(a_3,a_1),(a_2,a_3),(a_3,a_2),(a_3,a_4),(a_4,a_3)\}$.

$t(R) = \{(a_1,a_2),(a_1,a_3),(a_2,a_3),(a_3,a_4),(a_1,a_4),(a_2,a_4)\}$.

(2) $r(R) = R \cup Q = \{(x_1,x_1),(x_2,x_2),(x_3,x_3),(x_4,x_4),(x_5,x_5),(x_1,x_2),(x_1,x_4),(x_2,x_4),(x_3,x_5)\}$.

$s(R) = R \cup R^{-1} = \{(x_1,x_2),(x_2,x_1),(x_1,x_4),(x_4,x_1),(x_2,x_4),(x_4,x_2),(x_3,x_5),(x_5,x_3)\}$.

$t(R) = \{(x_1,x_2),(x_1,x_4),(x_2,x_4),(x_3,x_5)\}$.

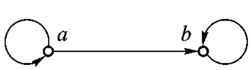
2. (a) $r(R)$的关系图

$r(R) = \{(a,a),(b,b)\}$

$s(R)$和$t(R)$的关系图

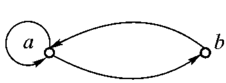
$s(R) = \{\quad\} = \varnothing$；$t(R) = \varnothing$

(b) $r(R)$的关系图



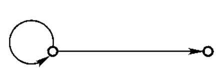
$r(R) = \{(a,a),(b,b)\}$.

$s(R)$的关系图



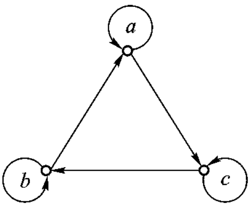
$s(R) = \{(a,a),(a,b),(b,a)\}$.

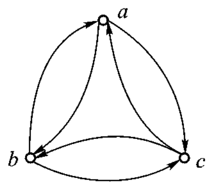
$t(R)$的关系图

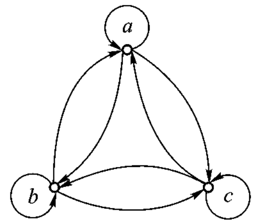


$t(R) = \{(a,a),(a,b)\}$.

(c) $r(R)$ 的关系图； $s(R)$ 的关系图； $t(R)$ 的关系图





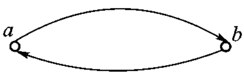


即：$r(R)=\{(a,a),(b,b),(c,c),(a,c),(c,b),(b,a)\}$.

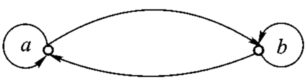
$s(R)=\{(a,c),(c,a),(a,b),(b,a),(b,c),(c,b)\}$.

$t(R)=\{(a,a),(b,b),(c,c),(a,b),(b,a),(b,c),(c,b),(a,c),(c,a)\}$.

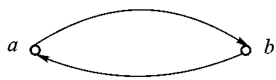
5.

图(a). 

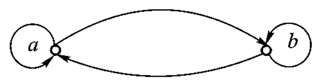
的 $r(R)$，$s(R)$，$t(R)$ 的关系图分别是：



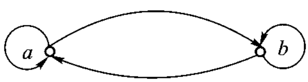
$r(R)$ 关系图



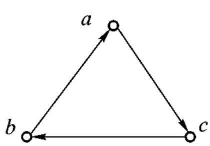
$s(R)$ 关系图



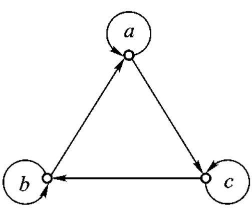
$t(R)$ 关系图



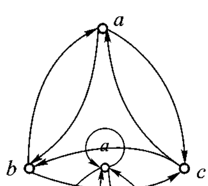
$tsr(R)$ 的关系图

图(b). 

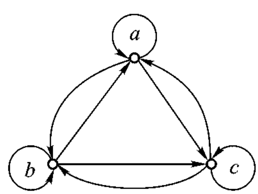
的 $r(R)$，$s(R)$，$t(R)$ 关系图如下：



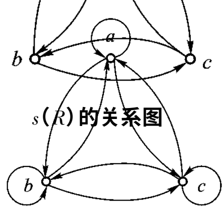
$r(R)$ 的关系图



$s(R)$ 的关系图



$t(R)$ 的关系图



$tsr(R)$ 的关系图：

6. (1) 若 $R=\{(a,b)\}$，则 R 是传递的，而 $s(R)=\{(a,b),(b,a)\}$ 不是传递的.

(2) 设 $R=\{(a,b)\}$，则

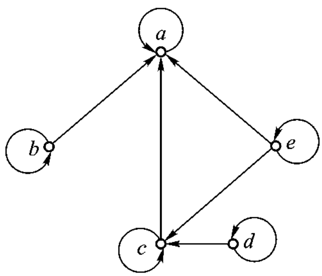
$st(R)=\{(a,b),(b,a)\}$.

$ts(R)=\{(a,a),(b,b),(a,b),(b,a)\}$.

练习题 2-4

2. (1) dRa 与 aRa 为真.

(2)



(3) A 的最大元素为 a，无最小元素.

(4) A 的极大元素为 a，极小元素为 e，d.

(5) 子集 $\{b,c,d\}$ 的上界为 a、下界为 d、上确界为 a 和下确界为 d.

子集 $\{c,d,e\}$ 的上界为 c，a，上确界为 c.

子集 $\{a,b,c\}$ 上(下)界和上(下)确界分别是：$a(d)$；$a(d)$.

3. B 的最大元不存在，最小元素为 $\varnothing$；B 的极大(小)元素为 $\{2,3,4\}$，$\{1,2,4\}$；($\varnothing$)；上界：$\{1,2,3,4\}$；下界：$\varnothing$；上确界：$\{1,2,3,4\}$；下确界为 $\varnothing$.

C 的最大元素为 $\{1,2,3,4\}$；最小元素不存在；极大元素 $\{1,2,3,4\}$；极小元素为 $\{1\}$，$\{2\}$，$\{3,4\}$；上界：$\{1,2,3,4\}$；下界：$\varnothing$；上确界；$\{1,2,3,4\}$；下确界：$\varnothing$.

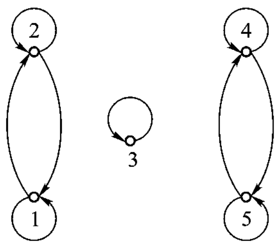
4. 代表偏序集合：(1)、(2)、(5)；

拟序集合：(3)；

线序集合：(2).

练习题 2－5

2.



关系矩阵：

$$\begin{pmatrix}1&1&0&0&0\\1&1&0&0&0\\0&0&1&0&0\\0&0&0&1&1\\0&0&0&1&1\end{pmatrix}$$

5.（1）$(A\times A)-R_1$ 不是 A 上的等价关系.

如：$A=\{a,b\}$，$R_1=\{(a,a),(b,b)\}$，

则 $(A\times A)-R_1=\{(a,b),(b,a)\}$.

所以 $(A\times A)-R_1$ 不是 A 上的等价关系.

（2）R_1-R_2 不是 A 上的等价关系.

例如：$A=\{a,b,c\}$，

$R_1=\{(a,b),(b,a),(b,c),(c,b),(a,c)\}\cup Q$.

$R_2=Q$，

则 $R_1-R_2=\{(a,b),(b,a),(b,c),(c,b),(a,c)\}$.

所以 R_1 和 R_2 是 A 上等价关系，

但 R_1-R_2 不是 A 上等价关系.

（3）R_1^2 是 A 上的等价关系.

（4）$r(R_1-R_2)$ 不是 A 上等价关系.

设 $A=\{a,b,c\}$，

$R_1=\{(a,a),(b,b),(c,c),(a,b),(b,a),(b,c),(c,b),(a,c),(c,a)\}$.

$R_2=\{(a,a),(b,b),(c,c),(b,c),(c,b)\}$.

$R_1-R_2=\{(a,b),(b,a),(a,c),(c,a)\}$.

$r(R_1-R_2)=\{(a,a),(b,b),(c,c),(a,b),(b,a),(a,c),(c,a)\}$，

不是 A 上的等价关系.

（5）$R_1\circ R_2$ 不是 A 上等价关系.

设 $A=\{1,2,3\}$

$R_1 = \{(1,1), (2,2), (3,3), (1,2), (2,1)\}$

$R_2 = \{(1,1), (2,2), (3,3), (1,3), (3,1)\}$

$R_1 \circ R_2 = \{(1,1), (2,2), (3,3), (1,3), (3,1), (1,2), (2,1), (2,3)\}$

故 $R_1 \circ R_2$ 不是 A 上的等价关系.

复习题二

1. $m=1$，$n=13$，$R=R^{13}$.

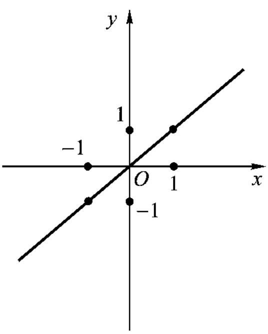
2. $A \times B$：表示在晚上 9 个时刻和 4 个电视频道所组成的电视节目，R_1，R_2 分别是 $A \times B$ 的两个子集，设：R_1：表示体育节目播出的时间表，R_2：表示音乐节目播出时间表，则 $R_1 \cup R_2$ 表示体育或音乐节目的播出时间表；$R_1 \cap R_2$：表示体育和音乐一起播出的时间表；$R_1 \oplus R_2$：表示体育节目表以及音乐节目表，但不是体育和音乐一起的节目表；$R_1 - R_2$：表示体育节目时间表而不是音乐时间表.

3. (1) 为真；(2)、(3)、(4)、(5) 均为假.

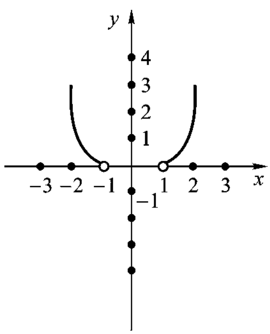
4. 记 $R_1 = \{(x,y) \mid x=y\}$.

$R_2 = \{(x,y) \mid x^2-1=0$ 且 $y>0\}$.

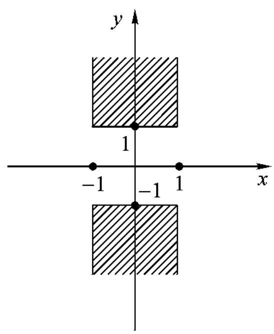
$R_3 = \{(x,y) \mid |x| \leqslant 1$ 且 $|y| \geqslant 1\}$.



R_1 是自反的，对称的和传递的.



R_2 是非自反的，非对称的.



R_3 是非对称的.

5. 提示：证 $R \circ (S \cup T) \subseteq R \circ S \cup R \circ T$.

$R \circ S \cup R \circ T \subseteq R \circ (S \cup T)$.

6. (1) $2^{n(n-1)}$.

(2) $2^{n(n-1)}$.

(3)、(4)、(5) 提示：A 上共有 2^{n^2} 个不同的二元关系.

9.

$$M_{R^{3n-2}}=M_R=\begin{pmatrix}0&0&0&1\\0&0&0&0\\1&1&0&0\\0&0&1&0\end{pmatrix}.$$

$$M_{R^{3n-1}}=M_{R^2}=\begin{pmatrix}0&0&1&0\\0&0&0&0\\0&0&0&1\\1&1&0&0\end{pmatrix}.$$

$$M_{R^{3n-2}}=M_{R^3}=\begin{pmatrix}1&1&0&0\\0&0&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}.$$

10. n^2 个.

11.

$$M_{R^{-1}}=\begin{pmatrix}1&0&0\\1&1&0\\0&0&1\end{pmatrix};\qquad M_{S^{-1}}=\begin{pmatrix}1&0&0\\1&1&1\\0&0&1\end{pmatrix};$$

$$M_{(R\circ S)^{-1}}=\begin{pmatrix}1&0&0\\1&1&1\\0&0&1\end{pmatrix};\ M_{(R\circ R)^{-1}}=\begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix}.$$

12.

$$M_{r(R)}=\begin{pmatrix}1&0&1&0\\0&1&1&1\\1&0&1&0\\1&0&1&1\end{pmatrix};\ M_{s(R)}=\begin{pmatrix}1&0&1&1\\0&0&1&1\\1&1&1&1\\1&1&1&0\end{pmatrix};$$

$$M_{R^2}=\begin{pmatrix}1&0&1&0\\1&0&1&0\\1&0&1&0\\1&0&1&0\end{pmatrix};\qquad M_{R^3}=\begin{pmatrix}1&0&1&0\\1&0&1&0\\1&0&1&0\\1&0&1&0\end{pmatrix};$$

$$M_{R^4}=\begin{pmatrix}1&0&1&0\\1&0&1&0\\1&0&1&0\\1&0&1&0\end{pmatrix};$$

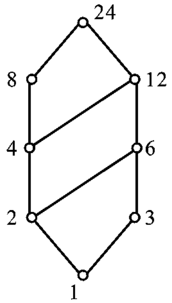
$$M_{t(R)}=\begin{pmatrix}1&0&1&0\\1&0&1&1\\1&0&1&0\\1&0&1&0\end{pmatrix}.$$

15. (1)、(2)、(3)、(4) 均为真；

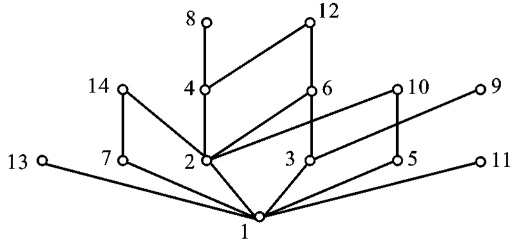
16. abc，$aaab$，bb.

17.

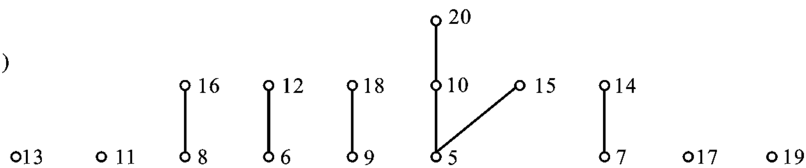
(1)



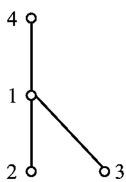
(2)



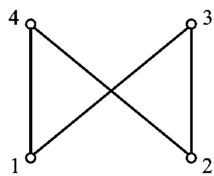
(3)



18.

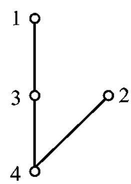


(a)



(b)

(c)



(d)

19. 设：$A = \{1,2,3,4\}$

(1) $R_1 = \{(1,1), (2,2), (3,3), (4,4), (1,3), (1,4), (2,3), (2,4)\}$，

若 $B=\{1,2\}$，则 B 没有最大元素.

(2) $R_2=\{(1,1),(2,2),(3,3),(4,4),(4,2),(4,1),(4,3),(3,1)\}$,

若 $B=\{2,3\}$，则 B 的最大下界 4，但没有最小元素。

(3) 令 R_3 为(1)中的 R_1，$B=\{1,2\}$，则 B 的上界 3，4，但没有最小上界.

20. 提示：参考 28 题.
21. 提示：在 Z 上构造小于关系.
22. $R=\{(0,0),(1,1),(2,2),(3,3),(0,3),(3,2),(2,1),(0,2),(0,1),(3,1)\}$.
23.

$$\boldsymbol{M}_{R^{-1}}=\begin{pmatrix}1&1&1\\0&1&1\\1&0&1\end{pmatrix};\ \boldsymbol{M}_{R^2}=\boldsymbol{M}_{R^3}=\begin{pmatrix}1&1&1\\1&1&1\\1&1&1\end{pmatrix};\ \boldsymbol{M}_{R\circ R^{-1}}=\begin{pmatrix}1&1&1\\1&1&1\\1&1&1\end{pmatrix}.$$

24. 提示：$\boldsymbol{M}_{R\circ S}$不是对称矩阵.
25. 恒等关系.
26. 提示：欲证 S 是自反、对称和传递的.
27. 提示：证 R 是自反的、对称的和传递的.

第三章　习 题 答 案

练习题 3-1

1. (1) 不封闭. (2) 封闭. (3) 封闭. (4) 封闭.
2. 不可交换.
3. (1)、(2)、(3) 可结合. (4) 不可结合.
4. $*$ 对 $\circ$ 也是不可分配的.
9. b 为生成元　$b^0=a$，$b^1=b$，$b^2=c$，$b^3=d$.　a 为单位元，a 为幂等元
10. (1) 是半群. (2) 是独异点、单位元为 c. (3) 不是循环独异点.
12. 提示：注意 A 中只有两个元素 a 和 b.
13. (1) 可交换、不等幂、a 为单位元、a 以自身为逆元、bc 互逆.
    (2) 可交换、不等幂、a 和 b 均以自身为逆元，b 和 c 都没有逆.
    (3) 不可交换、等幂、a 为单位元、b 和 c 都没有逆元.
    (4) 可交换、不等幂、a 为单位元、b 和 c 都没有逆元.

练习题 3－2

1. (1)、(2)、(6)、(8)、(9)是群 (3)不是、无逆元 (4)不是、无单位元 (5)不是、结合律不成立 (7)不是、有零元 (10)不是、结合律不成立

11. 生成元是 a 和 a^5，G 的所有子群有：$\{e\}$，$\{e, a^3\}$，$\{e, a^2, a^4\}$ 以及 G 本身.

14. 提示：只需证明同时期大于 2 的元素都是成对出现的即可.

15. 独异点，单位元素 $e=1$，不是群，因为存在零元素 0，

16. 提示：只需考虑 a 的 24 的因数次幂生成的子群.

练习题 3－3

4. $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 & 1 \end{pmatrix}$，$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 2 & 5 \end{pmatrix}$，$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix}$，

$\tau^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}$，$\sigma^{-1}\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}$.

练习题 3－4

1. 提示：令 $f(n)=2n$，$\forall n \in \mathbf{Z}$.

2. 提示：根据同构定义证.

6. 不同构. 提示：用反证法.

练习题 3－5

2. $G/H = \{[0], [1], [2]\}$

其中 $[i] = \{3z + i \mid z \in \mathbf{Z}\}$，$i=0$，1，2. 单位元素是[0]；运算“·”如下表所示.

·	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

练习题 3 –6

2.（1）不是整环. 没有乘法单位元.（2）不是整环. 对于加法不封闭.
（3）不是整环. $\forall x \neq 0$，不存在加法逆元.（4）、（5）是整环.

3.（1）不是域. 没有加法逆元.（2）是域.（3）不是域. 乘法逆元不存在.（4）是域（5）不是域. 没有乘法单位元.

复 习 题 三

2. 提示：逐个阶数的情况讨论.

14. 是交换环. 没有乘法单位元.
环中的零元素是 a，由 + 的运算表可见，

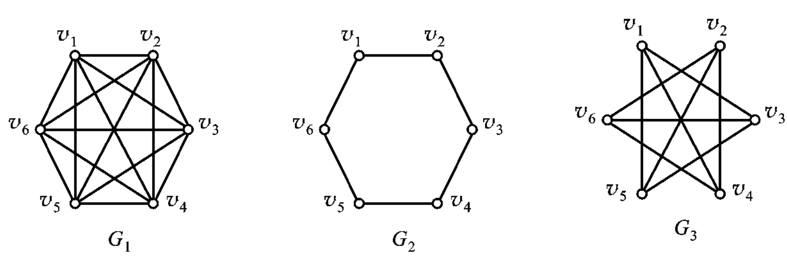
$$a^{-1}=a,\ c^{-1}=c,\ b^{-1}=d,\ d^{-1}=b.$$

16. 提示：根据定义逐项检查去证.

第四章 习 题 答 案

练习题 4 –1

5.



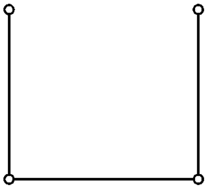
（1）$G_1=k_6$ （2）G_2 和 G_3 为互补图

6. 图 4 –16、图 4 –17 两对图不同构，图 4 –18 是同构.

点的对应关系：	边的对应关系：
$P_2 \leftrightarrow b_1$	$(P_2,P_4) \leftrightarrow (b_1,b_5)$
$P_1 \leftrightarrow b_3$	$(P_1,P_5) \leftrightarrow (b_2,b_3)$
$P_3 \leftrightarrow b_4$	$(P_1,P_3) \leftrightarrow (b_3,b_4)$
$P_4 \leftrightarrow b_5$	$(P_3,P_5) \leftrightarrow (b_2,b_4)$
$P_5 \leftrightarrow b_2$	$(P_3,P_4) \leftrightarrow (b_4,b_5)$

$$(P_4, P_5) \leftrightarrow (b_2, b_5)$$

7. (1)



(2) 不存在

(3) 提示：一个图是自补图，其对应的完全图的边数必为偶数.

练习题 4-2

2. (1) $ABCF$，$ABCEF$，$ABEF$，$ABECF$，$ADEF$，$ADECF$，$ADEBCF$.

(2) $d(A,F)=3$

(3) 不是欧拉图，是哈密顿图.

3. (a) 基本回路：$v_1v_2v_3v_4v_8v_7v_6v_5v_1$.

简单回路：$v_1v_5v_6v_7v_3v_6v_2v_1$.

(b) 基本回路：$a_1a_2a_3a_4a_1$.

简单回路：$a_1a_2a_3a_4a_1$.

(c) 基本回路：$b_1b_2b_3b_7b_6b_5b_1$.

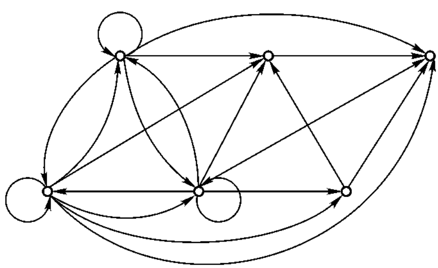
简单回路：$b_5b_2b_6b_5$.

(d) 基本回路：$c_1c_2c_6c_5c_1$.

简单回路：$c_1c_4c_5c_7c_1$.

4. $d(v_1,v_4)=3$；$d(v_2,v_5)=3$；$d(v_3,v_6)=3$ 不是传递的.

传递闭包：



5. (a) (3)；(b) (1)、(3)；(c) (3).

6. 图(1)、(2)存在欧拉路径.

图(1)、(2)、(3)存在哈密顿路径.

图(2)是欧拉图;图(1)、(2)、(3)是哈密顿图.

练习题 4-3

1. (a)

$$A=\begin{pmatrix}0&1&0&1\\0&0&1&1\\0&1&0&1\\0&1&0&0\end{pmatrix}$$

(b)

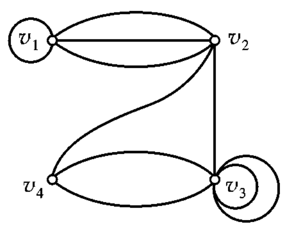
$$A^2=\begin{pmatrix}0&1&1&1\\0&2&0&1\\0&1&1&1\\0&0&1&1\end{pmatrix},\ A^3=\begin{pmatrix}0&2&1&2\\0&1&2&2\\0&2&1&2\\0&2&0&1\end{pmatrix},\ A^4=\begin{pmatrix}0&3&2&3\\0&4&1&3\\0&3&2&3\\0&1&2&2\end{pmatrix}.$$

从 v_1 到长度为 1,2,3,4 的路径各有:2 条;3 条;5 条;8 条.

(c)

$$P=\begin{pmatrix}1&1&1&1\\0&1&1&1\\0&1&1&1\\0&1&1&1\end{pmatrix}$$

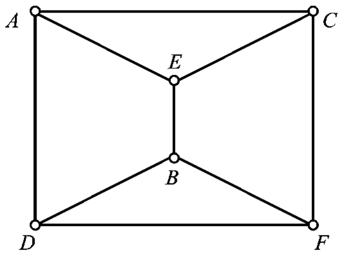
2.



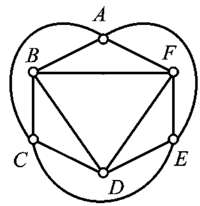
3. ①每一行(列)元素之和为偶数且无非 0 行(列)(无向图).
②第 i 行元素之和与第 i 列元素之和相等且无非 0 行(列),(有向图).

练习题 4-4

1. (a)、(b)是平面图;(c)不是平面图.
2. 是



(a)



(b)

$V_1 = \{v_1, v_3, v_5\}$；$V_2 = \{v_2, v_4, v_6, v_7\}$.

3. 提示：欧拉公式，面的次数之和为边的 2 倍.

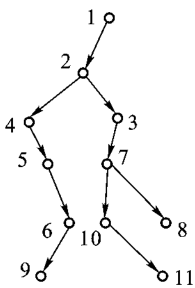
练习题 4 -5

1. （1）所有主对角线上元素为 0；

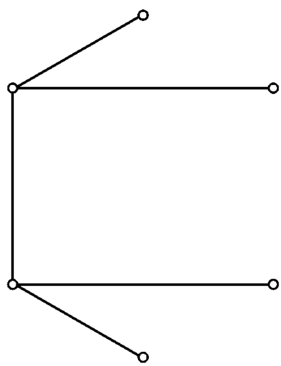
（2）矩阵中有一列元素全为 0，所有其他列中都恰有一个 1.

若一个邻接矩阵对应的有向图是树，则全零列对应的结点为根，而全零行对应的结点为树叶.

2.



4.



3. 9 个

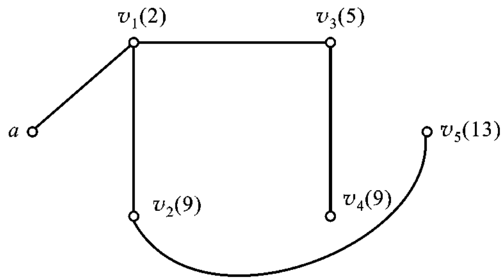
练习题 4 -6

1. $f_{xy} = 2$.

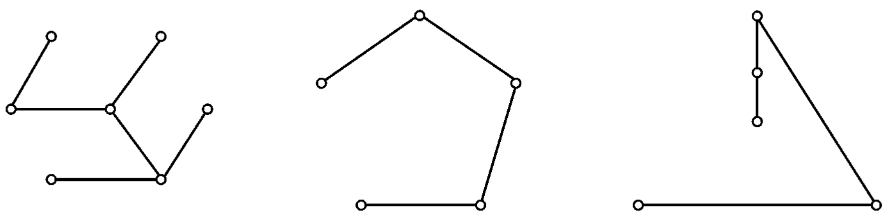
2. $f_{xy} = 5$.

练习题 4－7

1.

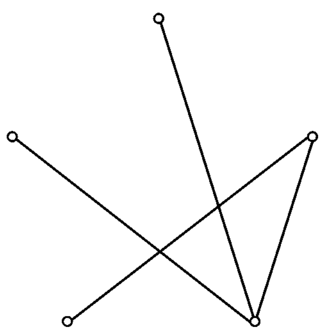


2.



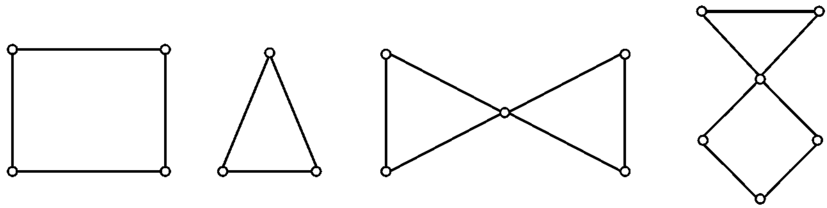
复习题四

1.



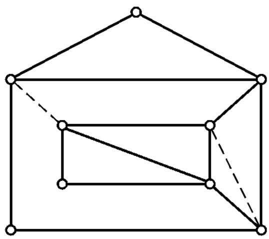
8.

图(a)是 n 与 m 为偶数的欧拉图；图(b)是 n 与 m 为奇数的欧拉图；图(c)是 n 为奇数，m 为偶数的欧拉图；图(d)是 n 为偶数，m 为奇数的欧拉图.



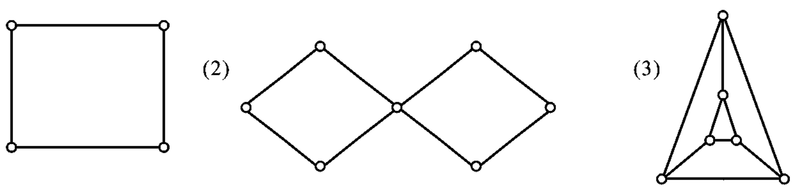
(a) (b) (c) (d)

9.（a）最少加 $k/2$ 条边.



（b）添加 2 条边，如上图所示（虚线）.

10.



(1) (a) (2) (b) (3) (c)

11. 没有哈密顿回路.

12. 长度为 2 的路径有 11 条，从 v_1 到 v_4 的长度为 2，路径为 $v_1v_2v_4$，长度为 4 的路径有 29 条，从 v_1 到 v_4 的长度为 4 的路径为 $v_1v_2v_3v_2v_4$，$v_1v_2v_4v_2v_4$，$v_1v_4v_2v_3v_4$.

$$\boldsymbol{A}=\begin{pmatrix}0&1&0&1\\0&0&1&1\\0&1&0&1\\0&1&0&0\end{pmatrix},\qquad \boldsymbol{A}^2=\begin{pmatrix}0&1&1&1\\0&0&1&1\\0&1&0&1\\0&1&0&0\end{pmatrix},$$

$$\boldsymbol{A}^3=\begin{pmatrix}0&2&1&2\\0&1&2&2\\0&2&1&2\\0&2&0&1\end{pmatrix},\qquad \boldsymbol{A}^4=\begin{pmatrix}0&3&2&3\\0&4&1&3\\0&3&2&3\\0&1&2&2\end{pmatrix}.$$

18. 若无向图 G 是二部图，则

（1）$A=(a_{ij})_{n\times n}$是对称矩阵.

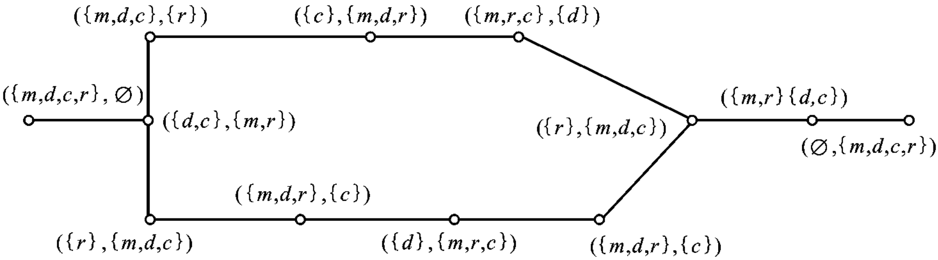
（2）$a_{ii}=0$；$i=1, 2, \cdots, n$.

（3）在每一行中，元素为 1 所对应的结点不相邻，即：若

$a_{is_1}=a_{is_2}=\cdots=a_{is_k}=1$,则结点 $v_{s_1},v_{s_2},\cdots,v_{s_k}$不相邻,其中 $k\leqslant n$.

如果能将结点集 V 分成两个子集 V_1 与 V_2，$V_1\cup V_2=V$ 且 $V_1\cap V_2=\varnothing$.

20.



第五章　习题答案

练习题 5－1

1.（1）是命题，真值为 1.

（2）是命题，真值为 0.

（3）是命题，真值为 1.

（4）不是命题.

（5）不是命题.

（6）是命题，真值为 1.

（7）是命题，真值为 0.

（8）不是命题.

（9）是命题，在十进制是假命题，真值为 0.

（10）是命题，真值现在不能确定.

（11）不是命题.

2.（1）P：煤球是黑色的，则符号化为□ P.

（2）P：天气冷；Q：我穿了毛衣，则符号化为 $P\rightarrow Q$.

（3）P：经一事；Q：长一智，则符号化为□ $P\rightarrow$□ Q.

（4）P：人犯我；Q：我犯人，则符号化为(□ $P\rightarrow$□ Q)$\wedge$($P\rightarrow Q$).

(5) P:天下大雨;Q:他骑自行车上班,则符号化为$\neg Q \to P$.

(6) P:刘洋与刘海是兄弟.

(7) P:6 是奇数;Q:8 能被 3 整除,则符号化为 $P \leftrightarrow Q$.

(8) P:天刮风;Q:天下雨;R:天中有太阳,则符号化为$\neg P \wedge \neg Q \wedge R$.

(9) P:他吃饭;Q:他听英语广播,则符号化为 $P \wedge Q$.

(10) P:王老师在 201 室上课;Q:王老师在 202 室上课,则符号化为$(P \wedge \neg Q) \vee (\neg P \wedge Q)$.

3. (1) 张丽是上海人,张丽是北京人.

(2) 我不看电视;我不去看电影;我准备去打球.

(3) 2 不是质数;5 大于 6.

练习题 5-2

1. (1)、(2)、(4)都是命题公式,(3)、(5)都不是命题公式.
2. (1)、(3)的真值均为 1,(2)、(4)的真值均为 0.
3. (1)

$P\quad Q\quad R$	$Q \vee R$	$P \wedge (Q \vee R)$
0 0 0	0	0
0 0 1	1	0
0 1 0	1	0
0 1 1	1	0
1 0 0	0	0
1 0 1	1	1
1 1 0	1	1
1 1 1	1	1

(2)

$P\ Q\ R$	$\neg Q$	$P \wedge \neg Q$	$Q \vee R$	$P \to (Q \vee R)$	$(P \wedge \neg Q) \to R$	$(P \to (Q \vee R)) \leftrightarrow ((P \wedge \neg Q) \to R)$
0 0 0	1	0	0	1	1	1
0 0 1	1	0	1	1	1	1
0 1 0	0	0	1	1	1	1
0 1 1	0	0	1	1	1	1
1 0 0	1	1	0	0	0	1
1 0 1	1	1	1	1	1	1
1 1 0	0	0	1	1	1	1
1 1 1	0	0	1	1	1	1

4. 真

5.（2）、（4）、（5）都是重言式；（1）矛盾式；（3）、（6）、（7）、（8）都是可满足式.

6.（1）、（2）不一定；（3）一定成立.

7. $P \wedge Q \wedge R \to S$

其中：P：居里夫人是波兰人；

Q：她是一个伟大的科学家；

R：她对科学事业作出了巨大的贡献；

S：她被授予诺贝尔奖金.

8. 提示：用等值演算法或主析取范式法.

如 （1）$P \Leftrightarrow (P \wedge Q) \vee (P \wedge \square\, Q)$

只要证明公式 $P \leftrightarrow (P \wedge Q) \vee (P \wedge \square\, Q)$ 为重言式即可.

9. 提示：如（1） $P \wedge (P \to Q) \Rightarrow Q$

只要证明公式 $P \wedge (P \to Q) \to Q$ 为重言式即可.

10.（1） R； （2） 1.

11.（1） A 是 D 的充分条件.

（2） B 是 D 的充要条件.

练习题 5 –3

1.（1） $\square (P \wedge Q) \wedge \square (\square\, P \wedge \square\, Q)$.

（2） $P \wedge \square (\square\, Q \wedge \square\, P)$.

2.（1） $m_0 \vee m_1 \vee m_2 \vee m_3$ 重言式.

（2） $M_0 \wedge M_1 \wedge M_2 \wedge M_3$ 矛盾式.

（3） $m_0 \vee m_1 \vee m_2 \vee m_7$；$M_3 \wedge M_4 \wedge M_5 \wedge M_6$ 可满足式.

3.（1） 不等值.

（2） 等值.

4.（1） $m_0 \vee m_2 \vee m_4 \vee m_6 \vee m_7$；$M_1 \wedge M_3 \wedge M_5$.

（2） $m_1 \vee m_2 \vee m_3 \vee m_4 \vee m_5 \vee m_7$；$M_0 \wedge M_6$.

5.（1） C 去，而 A，B 都不去；

（2） B 去，而 A，C 都不去；

（3） A，C 同去，而 B 不去.

练习题 5 –4

1.（1） R；（2） $\square\, P$ 或 Q 或 $\square\, R$；（3） $P \to S$；（4） R.

练习题 5－5

1. (1) $F(x)$：x 是博士，a：小王，则符号化为 $\neg F(a)$.

(2) $F(x)$：x 是有理数；$G(x)$：x 被 2 整除，则符号化为：$\forall x(F(x)\to G(x))$.

(3) $F(x)$：x 是有理数；$G(x)$：x 被 2 整除，则符号化为：$\exists x(F(x)\wedge G(x))$.

(4) $F(x)$：x 是兔子；$G(y)$：y 是乌龟；$H(x,y)$：x 比 y 跑得快，则符号化为：$\exists x(F(x)\wedge\forall y(G(y)\to H(x,y)))$ 或 $\exists x\forall y(F(x)\wedge(G(y)\to H(x,y)))$.

2. (1) 指导变元是 x，$\forall x$ 的辖域 $A(x)\to B(y)$. $\exists x$ 的辖域 $F(x)\wedge G(x)$；x 是约束出现，y 是自由出现.

(2) 指导变元是 x，$\forall x$ 的辖域：$(x=y\wedge x^2+x<5\to x<z)$，$x$ 既是自由出现，又是约束出现，y 是自由出现.

(3) 指导变元是 x，y；$\forall x$ 的辖域是：$\exists y(F(x,y)\wedge G(y,z))$，$\exists x$ 的辖域 $H(x,y,z)$，$\exists y$ 的辖域：$F(x,y)\wedge G(y,z)$；x，y 约束出现，z 是自由出现.

3. (a) 0；(b) 1；(c) 1.

4. (1) $F(a)\wedge F(b)\wedge F(c)\to G(a)\wedge G(b)\wedge G(c)$.

(2) $(F(a,y)\to G(a)\wedge G(b)\wedge G(c))\vee(F(b,y)\to G(a)\wedge G(b)\wedge G(c))\vee(F(c,y)\to G(a)\wedge G(b)\wedge G(c))$.

(3) $(F(a)\vee F(b)\vee F(c))\wedge(G(a)\wedge G(b)\wedge G(c))$.

(4) $(F(a)\wedge F(b)\wedge F(c))\vee(G(a)\wedge G(b)\wedge G(c))$.

5. (1) $\forall x(F(x)\vee\neg G(x))$. 或 $\forall x(G(x)\to F(x))$.

(2) $\forall x\exists y(F(x)\to G(x,y))$.

(3) $\forall x\exists y(\neg F(x,u)\to\neg G(v,y))$.

(4) $\forall x\exists y(F(x)\to Q(x)\vee R(y))$.

复 习 题 五

1. (1) $\neg Q\to P$，其中：P：$1+1=3$；Q：太阳从西边升起.

(2) P，其中 P：王刚与李强在打球.

(3) $(P\wedge\neg Q)\vee(\neg P\wedge Q)$，其中 P：他住 101 房间；Q：他住 102 房间.

(4) $P\to Q$，其中 P：四边形 $ABCD$ 是平行四边形，Q：它的对边平行.

(5) $\forall x(F(x)\to G(x))$；$F(x)$：x 是人，$G(x)$：x 是遵守宪法.

(6) $\forall x(F(x) \to G(x))$；$F(x)$：x 是乌鸦，$G(x)$：x 是黑色的.

(7) $\neg \forall x(F(x) \to G(x))$. 或 $\exists x(F(x) \wedge \neg G(x))$，其中 $F(x)$：x 是在美国留学的学生；$G(x)$：x 是亚州人.

(8) $\exists x(F(x) \wedge G(x))$，其中 $F(x)$：x 是男同学；$G(x)$：x 留着长发.

(9) $\forall x(F(x) \to G(x)) \wedge \neg G(a) \to \neg F(a)$，其中 $F(x)$：x 是大学生；$G(x)$：x 勤奋；a：王华.

(10) $\forall x \exists y(F(x) \wedge G(x,y) \wedge \neg H(x,y))$，其中 $F(x)$：x 是角；$G(x,y)$：x 与 y 相等；$H(x,y)$：x 与 y 是对顶角.

2. (1)、(4)为重言式；(2)、(3)为可满足式；(5)为矛盾式.

3. (1) 主析取范式：$m_6 = \sum(6)$.

主合取范式：$\prod(0,1,2,3,4,5,7)$.

(2) 主合取范式：$\prod(0,1,2,3)$，因为该公式是矛盾式，不含任何极小项，记主析取范式为：0.

(3) 主析取范式：$\sum(0,1,2,3)$，该公式是重言式，不含任何极大项，记该公式的主合取范式为：1.

(4) 主析取范式：$\sum(0,1,2,3,7)$.

主合取范式：$\prod(4,5,6)$.

(5) 主析取范式：$\sum(5,7,8,10,11,15)$.

主合取范式：$\prod(0,1,2,3,4,6,9,12,13,14)$.

4. (1) 不等值；(2)、(3)、(4)都等值.

5. (1) $\forall u \exists y(P(u) \to Q(x,y))$.

(2) $\forall x \exists y \forall z(P(x,y) \vee (Q(z) \to \neg R(u)))$.

(3) $\exists y \forall y(P(x) \to Q(y) \wedge H(x,y))$.