

---

# 离散数学笔记

## 第一章 命题逻辑

合取

析取

定义 1.1.3 否定：当某个命题为真时，其否定为假，当某个命题为假时，其否定为真

定义 1.1.4 条件联结词，表示“如果……那么……”形式的语句

定义 1.1.5 双条件联结词，表示“当且仅当”形式的语句

### 定义 1.2.1 合式公式

(1) 单个命题变元、命题常元为合式公式，称为原子公式。

(2) 若某个字符串 A 是合式公式，则  $\neg A$ 、 $(A)$  也是合式公式。

(3) 若  $A$ 、 $B$  是合式公式，则  $A \wedge B$ 、 $A \vee B$ 、 $A \rightarrow B$ 、 $A \leftrightarrow B$  是合式公式。

(4) 有限次使用(2)~(3)形成的字符串均为合式公式。

## 1.3 等值式

(1) $p \rightarrow q \Leftrightarrow \neg p \vee q \Leftrightarrow \neg q \rightarrow \neg p$	条件式的等值式、原命题 $\Leftrightarrow$ 逆否命题
(2) $p \leftrightarrow q \Leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p) \Leftrightarrow (p \wedge q) \vee (\neg p \wedge \neg q)$	双条件的等值式
(3) $p \Leftrightarrow \neg \neg p$	双重否定律
(4) $p \Leftrightarrow p \wedge p \Leftrightarrow p \vee p$	幂等律
(5) $p \vee q \Leftrightarrow q \vee p$ , $p \wedge q \Leftrightarrow q \wedge p$	交换律
(6) $p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r$ $p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r$	结合律
(7) $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$	分配律
(8) $p \vee (p \wedge r) \Leftrightarrow p$ $p \wedge (p \vee r) \Leftrightarrow p$	吸收律(多吃少)
(9) $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$ $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$	德摩律

注意：符号 “ $\Leftrightarrow$ ” 不是一个联结词，它表明两个公式的值相等。符号 “ $\leftrightarrow$ ” 是联结词，表示“当且仅当”、“充分必要”。

**定理 1.3.1 置换规则：**当将公式  $A$  中的  $B$  换成  $C$  得到公式  $D$  后，若  $B \Leftrightarrow C$ ，那么  $A \Leftrightarrow D$ 。

当将一个公式的局部进行等值替换后，仍与原公式等值，这也是我们在代数等数学最常见方法，不断对局部进行等值替换的操作，称为“等值演算”。

## 1.4 析取范式与合取范式

---

**定义 1.4.1 文字:** 命题变项(变元)及其否定称为文字。如: $p$ 、 $q$ 、 $r$ 、 $\neg p$ 、 $\neg q$ 、 $\neg r$ 。

**定义 1.4.2 简单析取式:** 仅由有限个文字构成的析取式。如: $p \vee q$ 、 $\neg p \vee q$ 、 $p \vee \neg q$ 、 $\neg p \vee \neg q$ 、 $p \vee q \vee r$ 。

**定义 1.4.3 简单合取式:** 仅由有限个文字构成的合取式。如: $p \wedge q$ 、 $\neg p \wedge q$ 、 $p \wedge \neg q$ 、 $\neg p \wedge \neg q$ 、 $p \wedge q \wedge r$ 。

**定理 1.4.1**

(1)简单析取式  $A_i$  是重言式  $\Leftrightarrow$  同时含有某命题变元及其否定式, 如  $A_i = p \vee \neg p \vee \dots$ 。

(2)简单合取式  $A_i$  是矛盾式  $\Leftrightarrow$  同时含有某个命题变元及其否定式, 如  $A_i = p \wedge \neg p \wedge \dots$ 。

**定义 1.4.4 析取范式:** 由有限个简单合取式的析取构成的命题公式。

如:  $(p \wedge q) \vee (\neg p \wedge q)$ 、 $(p \wedge q) \vee (\neg p \wedge \neg q) \vee (p \wedge \neg q \wedge r)$ 。

由析取的性质可知, 仅当每个简单合取式为假时, 析取范式为假。

范式中只出现 $\neg$ (否定)、 $\vee$ (析取)、 $\wedge$ (合取)三种符号, 其中 $\vee$ 、 $\wedge$ 交替出现, 因为最外层的运算符号是析取, 从而将这种范式称为“析取范式”。如果最外层的符号是合取则称为“合取范式”。

**定义 1.4.5 合取范式:** 由有限个简单析取式的合取构成的命题公式。

如:  $(p \vee q) \wedge (\neg p \vee q)$ 、 $(p \vee \neg q) \wedge (\neg p \vee \neg q) \wedge (p \vee q \vee r)$

由合取的性质可知, 仅当每个简单析取式为真时, 合取范式才为真。

**定理 1.4.2**

(1)析取范式是矛盾式  $\Leftrightarrow$  该范式中每个简单合取式是矛盾式。

(2)合取范式是重言式  $\Leftrightarrow$  该范式中每个简单析取式是重言式。

**将一个普通公式转换为范式的基本步骤**

1、肯定转换 $\rightarrow$ : 利用  $A \rightarrow B \Leftrightarrow \neg A \vee B$ , 将条件式运算符转换为 $\neg$ 、 $\vee$ 。

2、恰当转换 $\leftrightarrow$ : 利用  $A \leftrightarrow B \Leftrightarrow (A \rightarrow B) \wedge (B \rightarrow A) \Leftrightarrow (\neg A \vee B) \wedge (A \vee \neg B)$

利用  $A \leftrightarrow B \Leftrightarrow (A \wedge B) \vee (\neg A \wedge \neg B)$

3、否定到底: 利用  $\neg\neg A \Leftrightarrow A$ 、 $\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$ 、 $\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$

4、适当分配:  $A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$   $A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$

**定理 1.4.3(范式存在定理)**

(1)不是永假的命题公式, 存在析取范式。

(2)不是永真的命题公式, 存在合取范式。

**定义 1.4.4 小项:** 在含有 n 个变元的简单合取式中, 每个命题变元或其否定仅出现一次, 且各变元按其字母顺序出现, 则该简单合取式为小项或极小项。

如:  $p \wedge q \wedge r, p \neg \wedge q \wedge r, p \wedge q \neg \wedge r, \neg p \wedge q \wedge r$  是小项, 而  $\neg p \wedge r, q \wedge r$  不是小项。

**定义 1.4.5 大项:** 在含有 n 个变元的简单析取式中, 每个命题变元或其否定仅出现一次, 且各变元按其字母顺序出现, 则该简单析取式为大项或极大项。

如:  $p \vee q \vee r, p \neg \vee q \vee r, p \vee q \neg \vee r, \neg p \vee q \vee r$  是大项, 但  $p \vee r, \neg q \vee r$  不是大项。

【帮你记忆】: 因为  $p \wedge q$  的结果是这两值中最小者, 即  $p \wedge q = \min(p, q)$ , 所以将形如 “ $p \wedge q$ ” 的公式称为小项。类似  $p \vee q$  结果是这两值中最大者, 即  $p \vee q = \max(p, q)$ , 所以将形如 “ $p \vee q$ ” 的公式称为大项。

**定义 1.4.6 主合取范式:** 一个合取范式中, 如果所有简单析取式均为大项, 则称为主合取范式。

如  $(p \vee q \vee r) \wedge (p \vee \neg q \vee r) \wedge (\neg p \vee \neg q \vee r) \wedge (\neg p \vee q \vee \neg r)$  是主合取范式。

又如  $(p \vee r) \wedge (\neg q \vee r) \wedge (\neg p \vee q \vee \neg r)$  前 2 个简单析取式变元不全, 因而不是大项, 故不是主合取范式。

**定义 1.4.7 主析取范式:** 一个析取范式中, 如果所有简单合取式均为小项, 则称为主析取范式。

如  $(\neg p \wedge r) \vee (q \wedge r) \vee (p \wedge \neg q \wedge \neg r)$ , 因其前 2 个简单合取式中少变元不是小项, 从而不是主析取范式

又如:  $(\neg p \wedge q \wedge r) \vee (\neg p \wedge \neg q \wedge r) \vee (p \wedge q \wedge r) \vee (p \wedge \neg q \wedge \neg r)$  是主析取范式。

现构造  $(p \rightarrow q) \leftrightarrow r$ 、其主析取范式、其主合取范式的真值表, 其中  $m_{001} \vee m_{011} \vee m_{100}$   $\vee m_{111}$  为  $(\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge r) \vee (p \wedge \neg q \wedge \neg r) \vee (p \wedge q \wedge r)$ ,  $M_{000} \wedge M_{010} \wedge M_{101} \wedge M_{110}$  为  $(p \vee q \vee r) \wedge (p \vee \neg q \vee r) \wedge (\neg p \vee q \vee \neg r) \wedge (\neg p \vee \neg q \vee r)$ 。

表 1.17

p q r	$(p \rightarrow q) \leftrightarrow r$ 原式(记为 A)	$m_{001} \vee m_{011} \vee m_{100} \vee$	$M_{000} \wedge M_{010} \wedge M_{101} \wedge$
		$m_{111}$ 主析取范式(记为 B)	$M_{110}$ 主合取范式(记为 C)
0 0 0	0	$0 \vee 0 \vee 0 \vee 0=0$	$0 \wedge 1 \wedge 1 \wedge 1=0$
0 0 1	1	$1 \vee 0 \vee 0 \vee 0=1$	$1 \wedge 1 \wedge 1 \wedge 1=1$
0 1 0	0	$0 \vee 0 \vee 0 \vee 0=0$	$1 \wedge 0 \wedge 1 \wedge 1=0$
0 1 1	1	$0 \vee 1 \vee 0 \vee 0=1$	$1 \wedge 1 \wedge 1 \wedge 1=1$
1 0 0	1	$0 \vee 0 \vee 1 \vee 0=1$	$1 \wedge 1 \wedge 1 \wedge 1=1$
1 0 1	0	$0 \vee 0 \vee 0 \vee 0=0$	$1 \wedge 1 \wedge 0 \wedge 1=0$
1 1 0	0	$0 \vee 0 \vee 0 \vee 0=0$	$1 \wedge 1 \wedge 1 \wedge 0=0$
1 1 1	1	$0 \vee 0 \vee 0 \vee 1=1$	$1 \wedge 1 \wedge 1 \wedge 1=1$

从表 1.17 可发现  $(p \rightarrow q) \leftrightarrow r$ 、与其主析取范式、主合取范式的真值表完全一样, 说明三者互相等值, 因此我们得到如下定理。

#### 定理 1.4.4

- (1) 不是永假的命题公式, 其主析取范式等值于原公式。
- (2) 不是永真的命题公式, 其主合取范式等值于原公式。

## 1.6 推理

定义 1.6.1 设  $A$  与  $C$  是两个命题公式，若  $A \rightarrow C$  为永真式、重言式，则称  $C$  是  $A$  的有效结论，或称  $A$  可以逻辑推出  $C$ ，记为  $A \Rightarrow C$ 。（用等值演算或真值表）

# 第二章 谓词逻辑

## 2.1、基本概念

$\forall$ : 全称量词       $\exists$ : 存在量词

一般情况下，如果个体变元的取值范围不做任何限制即为全总个体域时，带“全称量词”的谓词公式形如 " $\forall x(H(x) \rightarrow B(x))$ "，即量词的后面为条件式，带“存在量词”的谓词公式形如 " $\exists x(H(x) \vee WL(x))$ "，即量词的后面为合取式。

例题

$R(x)$  表示对象  $x$  是兔子， $T(x)$  表示对象  $x$  是乌龟， $H(x,y)$  表示  $x$  比  $y$  跑得快， $L(x,y)$  表示  $x$  与  $y$  一样快，则兔子比乌龟跑得快表示为： $\forall x \forall y(R(x) \wedge T(y) \rightarrow H(x,y))$

有的兔子比所有的乌龟跑得快表示为： $\exists x \forall y(R(x) \wedge T(y) \rightarrow H(x,y))$

## 2.2、谓词公式及其解释

定义 2.2.1、非逻辑符号：个体常元(如  $a,b,c$ )、函数常元(如表示  $x^2 + y^2$  的  $f(x,y)$ )、谓词常元(如表示人类的  $H(x)$ )。

定义 2.2.2、逻辑符号：个体变元、量词( $\forall \exists$ )、联结词( $\neg \vee \wedge \rightarrow \leftrightarrow$ )、逗号、括号。

定义 2.2.3、项的定义：个体常元、变元及其函数式的表达式称为项(item)。

定义 2.2.4、原子公式：设  $R(x_1 \dots x_n)$  是  $n$  元谓词， $t_1 \dots t_n$  是项，则  $R(t)$  是原子公式。原子公式中的个体变元，可以换成个体变元的表达式(项)，但不能出现任何联结词与量词，只能为单个的谓词公式。

定义 2.2.5 合式公式：(1)原子公式是合式公式；(2)若  $A$  是合式公式，则  $(\neg A)$  也是合式公式；(3)若  $A, B$  合式，则  $A \vee B, A \wedge B, A \rightarrow B, A \leftrightarrow B$  合式；(4)若  $A$  合式，则  $\forall x A, \exists x A$  合式；(5)有限次使用(2)~(4)得到的式子是合式。

定义 2.2.6 量词辖域： $\forall x A$  和  $\exists x A$  中的量词  $\forall x / \exists x$  的作用范围， $A$  就是作用范围。

定义 2.2.7 约束变元：在  $\forall x$  和  $\exists x$  的辖域  $A$  中出现的个体变元  $x$ ，称为约束变元，这是与量词相关的变元，约束变元的所有出现都称为约束出现。

定义 2.2.8 自由变元：谓词公式中与任何量词都无关的量词，称为自由变元，它的每次出现称为自由出现。一个公式的个体变元不是约束变元，就是自由变元。

注意：为了避免约束变元和自由变元同名出现，一般要对“约束变元”改名，而不对自由变元改名。

定义 2.2.9 闭公式是指不含自由变元的谓词公式

从本例(已省)可知，不同的公式在同一个解释下，其真值可能存在，也可能不存在，但是对于没有自由变元的公式(闭公式)，不论做何种解释，其真值肯定存在

**谓词公式**的类型：重言式(永真式)、矛盾式(永假式)、可满足公式三种类型

**定义 2.2.10** 在任何解释下，公式的真值总存在并为真，则为重言式或永真式。

**定义 2.2.11** 在任何解释下，公式的真值总存在并为假，则为矛盾式或永假式。

**定义 2.2.12** 存在个体域并存在一个解释使得公式的真值存在并为真，则为可满足式。

**定义 2.2.13 代换实例** 设  $p_1, p_2, \dots, p_n$  是命题公式  $A_0$  中的命题变元， $A_0, A_1, \dots, A_n$  是  $n$  个谓

词公式，用  $A_i$  代替公式  $A_0$  中的  $p_i$  后得到公式  $A$ ，则称  $A$  为  $A_0$  的代换实例。

**如**  $A(x) \vee \neg A(x), \forall x A(x) \vee \neg \forall x A(x)$  可看成  $p \vee \neg p$  的代换实例， $A(x) \wedge \neg A(x), \forall x A(x) \wedge \neg \forall x A(x)$  可看成  $p \wedge \neg p$  的代换实例。

**定理 2.2.1** 命题逻辑的永真公式之代换实例是谓词逻辑的永真公式，命题逻辑的永假公式之代换实例是谓词逻辑的永假式。(代换前后是同类型的公式)

### 2.3、谓词公式的等值演算

**定义 2.3.1** 设  $A, B$  是两个合法的谓词公式，如果在任何解释下，这两个公式的真值都相等，则称  $A$  与  $B$  等值，记为  $A \Leftrightarrow B$ 。

当  $A \Leftrightarrow B$  时，根据定义可知，在任何解释下，公式  $A$  与公式  $B$  的真值都相同，故  $A \leftrightarrow B$  为永真式，故得到如下的定义。

**定义 2.3.2** 设  $A, B$  是两个合法谓词公式，如果在任何解释下， $A \leftrightarrow B$  为永真式，则  $A$  与  $B$  等值，记为  $A \Leftrightarrow B$ 。

一、利用代换实例可证明的等值式( $p \leftrightarrow \neg \neg p$  永真，代换实例  $\forall x F(x) \leftrightarrow \neg \neg \forall x F(x)$  永真)

二、个体域有限时，带全称量词、存在量词公式的等值式

**如：**若  $D = \{a_1, a_2, \dots, a_n\}$ ，则  $\forall x A(x) \Leftrightarrow A(a_1) \wedge A(a_2) \wedge \dots \wedge A(a_n)$

三、量词的德摩律

1、 $\neg \forall x A(x) \Leftrightarrow \exists x \neg A(x)$                           2、 $\neg \exists x A(x) \Leftrightarrow \forall x \neg A(x)$

四、量词分配律

1、 $\forall x(A(x) \wedge B(x)) \Leftrightarrow \forall x A(x) \wedge \forall x B(x)$       2、 $\exists x(A(x) \vee B(x)) \Leftrightarrow \exists x A(x) \vee \exists x B(x)$

**记忆方法：** $\forall$  与  $\wedge$ ，一个尖角朝下、一个尖角朝上，相反可才分配。2 式可看成 1 式的对偶式

五、量词作用域的收缩与扩张律

$A(x)$  含自由出现的个体变元  $x$ ， $B$  不含有自由出现的  $x$ ，则有：

1、 $\forall / \exists (A(x) \vee B) \Leftrightarrow \forall / \exists A(x) \vee B$       2、 $\forall / \exists (A(x) \wedge B) \Leftrightarrow \forall / \exists A(x) \wedge B$

对于条件式  $A(x) \leftrightarrow B$ ，利用“基本等值一”将其转换为析取式，再使用德摩律进行演算

六、置换规则

若  $B$  是公式  $A$  的子公式，且  $B \Leftrightarrow C$ ，将  $B$  在  $A$  中的每次出现，都换成  $C$  得到的公式记为  $D$ ，则  $A \Leftrightarrow D$

七、约束变元改名规则

将公式  $A$  中某量词的指导变元及辖域中约束变元每次约束出现，全部换成公式中未出现的字母，所得到的公

式记为  $B$ , 则  $A \Leftrightarrow B$

例  $\forall x(A(x) \rightarrow B) \Leftrightarrow \exists x A(x) \rightarrow B$

证明步骤:

$$\begin{aligned} & \forall x(A(x) \rightarrow B) \\ \Leftrightarrow & \forall x(\neg A(x) \vee B) \quad \text{命题公式 } p \rightarrow q \Leftrightarrow \neg p \vee q \text{ 的代换实例} \\ \Leftrightarrow & \forall x \neg A(x) \vee B \quad \text{量词作用域的收缩与扩张律} \\ \Leftrightarrow & \neg \exists x A(x) \vee B \quad \text{德摩律} \\ \Leftrightarrow & \exists x A(x) \rightarrow B \quad p \Leftrightarrow \neg \neg p \text{ 的代换实例} \end{aligned}$$

## 2.4、谓词公式的范式

定义 2.4.1 一个谓词公式, 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, 则该公式称为前束范式。

如:  $\forall x \exists y F(x) \wedge G(y)$ ,  $\forall y \exists x (\neg P(x,y) \rightarrow G(y))$  是前束范式。

但  $\forall x(F(x) \rightarrow \exists y(G(y) \vee H(x,y)))$  不是前束范式。

定理 2.4.1 任意一个谓词公式, 都有与之等值的前束范式。

从定理证明过程, 可得到获取前束范式的步骤:

- (1) 剔除不起作用的量词;
  - (2) 如果约束变元与自由变元同名, 则约束变元改名;
  - (3) 如果后面的约束变元与前面的约束变元同名, 则后面的约束变元改名;
  - (4) 利用代换实例, 将  $\rightarrow$ 、 $\leftrightarrow$  转换为  $\vee \wedge$  表示;
  - (5) 利用德摩律, 将否定深入到原子公式或命题的前面;
  - (6) 利用量词辖域的扩张与收缩规律或利用量词的分配律, 将量词移到最左边
- 例题 2.4.1 把公式  $\forall x P(x) \rightarrow \exists x Q(x)$  转换为前束范式
- 解: 由于没有空量词, 即没有不约束任何变元的量词, 现有的约束变元也不与自由变元同名, 但  $\exists x$  的约束变元与前面  $\forall x$  中的  $x$  同名, 后者改名。
- $$\begin{aligned} & \forall x P(x) \rightarrow \exists x Q(x) \\ \Leftrightarrow & \forall x P(x) \rightarrow \exists y Q(y) \quad \text{后方约束变元改名} \\ \Leftrightarrow & \neg \forall x P(x) \vee \exists y Q(y) \quad \text{条件式的代换实例} \\ \Leftrightarrow & \exists x \neg P(x) \vee \exists y Q(y) \quad \text{德摩律} \\ \Leftrightarrow & \exists x \exists y (\neg P(x) \vee \exists y Q(y)) \quad \text{量词辖域的扩张} \end{aligned}$$

## 2.5、谓词推理

定义 2.5.1 若在各种解释下  $A_1 \wedge A_2 \wedge \dots \wedge A_n \rightarrow B$  只能为真即为永真, 则称为前提  $A_1 \wedge A_2 \wedge \dots \wedge A_n$  可推出结论  $B$ 。

定义 2.5.2 在所有使  $A_1 \wedge A_2 \wedge \dots \wedge A_n$  为真的解释下,  $B$  为真, 则称为前提  $A_1 \wedge A_2 \wedge \dots \wedge A_n$  可推出结论  $B$ 。

谓词逻辑的推理方法分为以下几类:

---

一、谓词逻辑的等值演算原则、规律：代换实例、量词的德摩律、量词的分配律、量词管辖域的扩张与收缩、约束变元改名。

二、命题逻辑的推理规则的代换实例，如假言推理规则、传递律、合取与析取的性质律、CP 规则、反证法等。

三、谓词逻辑的推理公理

(1)  $\forall x A(x) \vee \forall x B(x) \Rightarrow \forall x(A(x) \vee B(x))$  全称量词展开可推出合并

(2)  $\exists x(A(x) \wedge B(x)) \Rightarrow \exists x A(x) \wedge \exists x B(x)$  存在量词的合并可推出展开，别记反了

(3) 全称量词的指定 US 或  $\forall^-$ :  $\forall x A(x) \Rightarrow A(x)$

$x_0$  是论域中的任意个体。该规则可理解为：谓词公式  $\forall x A(x)$  在某个解释下为真，即论域中所有个体都在此解释下使  $A$  为真时，论域中的任意个体  $x_0$  在此解释下使  $A$  为真。

(4) 全称量词的推广 UG 或  $\forall^+$ :  $A(x_0) \Rightarrow \forall x A(x)$

$x_0$  是论域中的任意个体，它是由某个全称量词指定时确定个体。该规则可理解为：在某个解释下，论域中的任意个体  $x_0$  都使公式  $A$  为真，那么论域中的所有个体在此解释下，都使  $A$  为真，意即谓词公式  $\forall x A(x)$  为真。

(5) 存在量词的指定 ES 或  $\exists^-$ :  $\exists x A(x) \Rightarrow A(c)$

$c$  为某个特定的个体，不是任意的个体，这是它与全称量词的区别。该规则可理解为：

当  $\exists x A(x)$  在某个解释下为真时，至少有一个个体常元  $c$  在该解释下使得公式  $A$  为真，即  $A(c)=1$ 。

(6) 存在量词的推广 EG 或  $\exists^+$ :  $A(c) \Rightarrow \exists x A(x)$

$c$  为某个体，可以是某个存在量词指定时确定的个体，也可以是全称量词指定时的个体。该规则可理解为：在某个解释下有 1 个个体  $c$  使公式  $A$  为真，就可认为  $\exists x A(x)$  该解释下为真。

例题 2.5.3 证明  $\forall x(F(x) \rightarrow G(x)), \exists x(F(x) \wedge H(x)) \Rightarrow \exists x(G(x) \wedge H(x))$

- |   |                                     |
|---|-------------------------------------|
| (1) $\exists x(F(x) \wedge H(x))$ 为真      | (前提)                                |
| (2) $F(c) \wedge H(c)$ 为真                 | (存在指称，至少存在 $c$ 使 $F(c)$ 为真，先使用存在指定) |
| (3) $F(c)$ 为真                             | ((2) $\wedge$ 的定义)                  |
| (4) $H(c)$ 为真                             | ((2) $\wedge$ 的定义)                  |
| (5) $\forall x(F(x) \rightarrow G(x))$ 为真 | (前提)                                |
| (6) $F(c) \rightarrow G(c)$ 为真            | (全称指定，任意 $x_0$ 都为真，尤其 $x_0=c$ 时为真)  |
| (7) $G(c)$ 为真                             | ((2), (4) 假言推理的代换实例)                |
| (8) $G(c) \wedge H(c)$ 为真                 | ((4)(7) 合取)                         |
| (9) $\exists x(G(x) \wedge H(x))$ 为真      | ((5) 存在推广，有一个 $c$ 使公式为真，则存在量词可加)    |

### 第三章 集合与关系

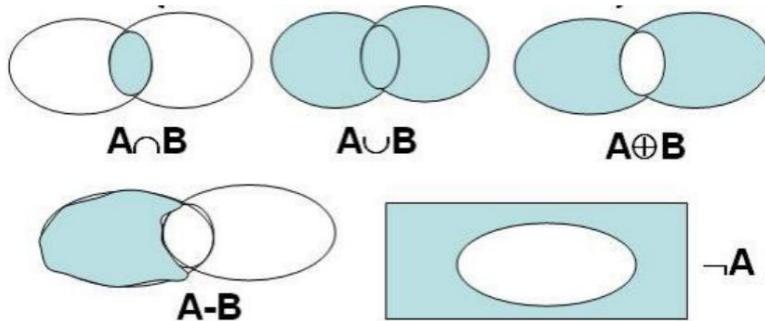
#### 3.1、基本概念

在离散数学称“不产生歧义的对象的汇集一块”便构成集合。常用大写字母表示集合，如  $R$  表示实数， $N$  表示自然数， $Z$  表示整数， $Q$  表示有理数， $C$  表示复数。描述一个集合一般有“枚举法”与“描述法”，“枚举法”。元素与集合之间有“属于  $\in$ ”或“不属于  $\notin$ ”两种关系。

定义 3.1.1 设  $A, B$  是两个集合，如果  $A$  中的任何元素都是  $B$  中的元素，则称  $A$  是  $B$  的子集，也称  $B$  包含于  $A$ ，记为  $B \subseteq A$ ，也称  $A$  包含  $B$ ，记为  $A \supseteq B$ 。

## 3.2 集合运算性质

**定义 3.2.1** 设  $A, B$  为集合,  $A$  与  $B$  的并集  $A \cup B$ ,  $A$  与  $B$  的交集  $A \cap B$ ,  $A-B$  的定义:  $A \cup B = \{x | x \in A \vee x \in B\}$ ,  $A \cap B = \{x | x \in A \wedge x \in B\}$ ,  $A-B = \{x | x \in A \wedge x \notin B\}$



**定义 3.2.2** 设  $A, B$  为集合,  $A$  与  $B$  的对称差, 记为  $A \otimes B = \{x | (x \in A \wedge x \notin B) \vee (x \notin A \wedge x \in B)\} = A \cup B - A \cap B$ 。

**定义 3.2.3** 设  $A, B$  是两个集合, 若  $A \subseteq B, B \subseteq A$  则  $A=B$ , 即两个集合相等。

**幂等律**  $A \cup A = A, A \cap A = A$

**结合律**  $A \cup B \cup C = A \cup (B \cup C) = (A \cup B) \cup C$

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

**交换律**  $A \cup B = B \cup A, A \cap B = B \cap A$

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

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

**同一/零律**  $A \cup \emptyset = A, A \cap \emptyset = \emptyset$

**排中/矛盾律**  $A \cup \neg A = E, A \cap \neg A = \emptyset$

**吸收律(大吃小)**  $A \cap (B \cup A) = A, A \cup (B \cap A) = A$

**德摩律**  $\neg(A \cap B) = \neg A \cup \neg B, \neg(A \cup B) = \neg A \cap \neg B$

**双重否定**  $\neg \neg A = A$

## 3.3、有穷集的计数

**定理 3.3.1** 二个集合的包含排斥原理  $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$

## 3.4、序偶

**定义 3.4.2** 令  $\langle x, y \rangle$  与  $\langle u, v \rangle$  是二个序偶, 如果  $x=u, y=v$ , 那么  $\langle x, y \rangle = \langle u, v \rangle$  即二个序偶相等。

**定义 3.4.3** 如果  $\langle x, y \rangle$  是序偶, 且  $\langle \langle x, y \rangle, z \rangle$  也是一个序偶, 则称  $\langle x, y, z \rangle$  为三元组。

## 3.5、直积或笛卡尔积

**定义 3.5.1** 令  $A, B$  是两个集合, 称序偶的集合  $\{\langle x, y \rangle | x \in A, y \in B\}$  为  $A$  与  $B$  的直积或笛卡尔积, 记为  $A \times B$ 。

如:  $A=\{1,2,3\}$ ,  $B=\{a,b,c\}$  则  $A \times B = \{1,2,3\} \times \{a,b,c\} = \{\langle 1,a \rangle, \langle 1,b \rangle, \langle 1,c \rangle, \langle 2,a \rangle, \langle 2,b \rangle, \langle 2,c \rangle, \langle 3,a \rangle, \langle 3,b \rangle, \langle 3,c \rangle\}$

#### 直积的性质

- 1、 $A \times (B \cup C) = A \times B \cup A \times C$
- 2、 $A \times (B \cap C) = A \times B \cap A \times C$
- 3、 $(B \cup C) \times A = B \times A \cup C \times A$
- 4、 $(B \cap C) \times A = B \times A \cap C \times A$
- 5、 $A \subseteq B \Leftrightarrow A \times C \subseteq B \times C \Leftrightarrow C \times A \subseteq C \times B$
- 6、 $A \subseteq B, C \subseteq D \Leftrightarrow A \times C \subseteq B \times D$

定义 3.5.2 令  $A_1, A_2, \dots, A_n$  是  $n$  个集合, 称  $n$  元组的集合  $\{x_1, x_2, \dots, x_n\}$

$x_1 \in A_1, x_2 \in A_2, \dots, x_n \in A_n\}$ , 为  $A_1, A_2, \dots, A_n$  的直积或笛卡尔积, 记为  $A_1 \times A_2 \times \dots \times A_n$ 。

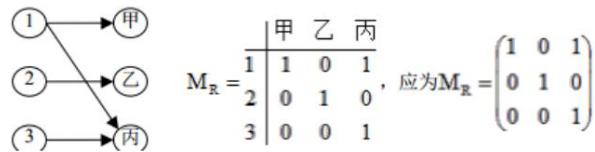
## 3.6、关系

定义 3.6.1 称直积中部分感兴趣的序偶所组成的集合为“关系”, 记为  $R$ 。

如在直积  $\{1,2,3,4,5,6,7,8\} \times \{1,2,3,4,5,6,7,8\}$  中, 只对第 1 个元素是第 2 个元素的因数的序偶感兴趣, 即只对  $R = \{\langle 1,1 \rangle, \langle 1,2 \rangle, \langle 1,3 \rangle, \langle 1,4 \rangle, \langle 1,5 \rangle, \langle 1,6 \rangle, \langle 1,7 \rangle, \langle 1,8 \rangle, \langle 2,2 \rangle, \langle 2,4 \rangle, \langle 2,6 \rangle, \langle 2,8 \rangle, \langle 3,3 \rangle, \langle 3,6 \rangle, \langle 4,4 \rangle, \langle 4,8 \rangle, \langle 5,5 \rangle, \langle 6,6 \rangle, \langle 7,7 \rangle, \langle 8,8 \rangle\}$ ,  $R \subseteq A \times A$  ( $A = \{1,2,3,4,5,6,7,8\}$ )

定义 3.6.2 如果序偶或元组属于某个关系  $R$ , 则称序偶或元组具有关系  $R$ 。

关系图, 关系矩阵



## 3.7、关系的复合

定义 3.7.1 若关系  $F \subseteq A \times A$ , 关系  $G \subseteq A \times A$ , 称集合  $\{(x,y) | \exists t \text{ 使得 } \langle x,t \rangle \in F, \langle t,y \rangle \in G\}$  为  $F$  与  $G$  的复合, 记为  $F \circ G$ 。

例题 3.7.1 令  $A = \{1,2,3\}$ ,  $F = \{\langle 1,1 \rangle, \langle 1,2 \rangle\}$   $G = \{\langle 2,2 \rangle, \langle 1,3 \rangle, \langle 1,1 \rangle\}$  则

解:  $F \circ G = \{\langle 1,3 \rangle, \langle 1,1 \rangle, \langle 1,2 \rangle\}$ ,  $G \circ F = \{\langle 1,2 \rangle, \langle 1,1 \rangle\}$ , 因此关系的复合不满足交换律。

采用复合的定义去计算, 只适合于人工计算, 为了编程实现, 故采用矩阵表示关系。

$$\begin{aligned} M_F \circ M_G &= \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \circ \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \\ M_G \circ M_F &= \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \circ \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \end{aligned}$$

**说明:**  $M_F$  的第  $i$  行与  $M_G$  的第  $j$  列相乘时, 乘法是合取  $\wedge$ , 加法是析取  $\vee$ , 如  $MF$  的 1 行与  $MG$  的第 3 列相乘是:  $(1 \wedge 1) \vee (1 \wedge 0) \vee (0 \wedge 0)$ , 结果为 1。

**定义 3.7.2** 若关系  $F \subseteq A \times A$ , 称集合  $\{(y, x) | (x, y) \in F\}$  为  $F$  的逆, 记为  $F^{-1}$

**例题 3.7.2** 令  $A = \{1, 2, 3\}$ ,  $F = \{(1, 2), (1, 3), (2, 1)\}$ , 则  $F^{-1} = \{(2, 1), (3, 1), (1, 2)\}$ 。

### 3.8、关系的分类

**定义 3.8.1** 若  $\forall x \in A$  都有  $(x, x) \in R$ , 则  $R$  是**自反关系**。(自己到自己的关系全属于  $R$ )

**定义 3.8.2** 若  $\forall x \in A$  都有  $(x, x) \notin R$ , 则  $R$  是**反自反的**。(自己到自己的关系全不属于  $R$ )

$$M_{R1} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad M_{R2} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad M_{R3} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

自反关系  $R1$  的关系矩阵  $M_{R1}$  的对角线全为 1, 凡关系矩阵的对角线全是 1 是自反关系。

反自反关系  $R2$  的关系矩阵  $M_{R2}$  的对角线全为 0, 凡关系矩阵的对角线全是 0 的反自反。

而关系  $R3$  的关系矩阵的主角线不全是 1, 也不全是 0, 故既不是自反的, 也不是反自

**定义 3.8.4** 如果所有形如  $(x, x)$  的序偶都在关系  $R$  中,  $R$  也只有这种形式的序偶, 则称  $R$  为恒等关系, 记为  $I_A$ 。

对于恒等关系而言, 其关系矩阵是单位矩阵, 即其主对角线全是 1, 其他位置全是 0, 对关系图是每个点都有自旋, 仅只有自旋, 没有其他边。

**定义 3.8.5** 令关系  $R \subseteq A \times A$ , 如果当  $(x, y) \in R$  时  $(y, x) \in R$ , 则称  $R$  为**对称关系**。

**定义 3.8.6** 令关系  $R \subseteq A \times A$ , 如果当  $(x, y) \in R$  且  $x \neq y$  时  $(y, x) \notin R$ , 则称  $R$  为**反对称关系**。

$$M_{R1} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad M_{R2} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad M_{R3} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

**定义 3.8.8** 令关系  $R \subseteq A \times A$ , 若当  $(x, y) \in R, (y, z) \in R$  时有  $(x, z) \in R$ , 则称  $R$  为可传递关系。

从  $R \circ R$  的关系矩阵可知, 其非 0 元素在  $R$  的关系矩阵都出现, 即  $M_{R \circ R} \leq M_R$ , 凡满足这个不等式的关系, 肯定为可传递关系。

$$M_R = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad M_{R \circ R} = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix} \circ \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

所以不可传递。

从  $R \circ R$  的关系矩阵可知, 其非 0 元素出现在(1,1), (1,3), (2,2), (2,4), 在  $R$  的关系矩

阵都没出现, 不满足  $M_{R \circ R} \leq M_R$ , 不可传递关系。

$$M_R = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} M_{R \circ R} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \circ \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

### 3.9、关系的闭包

由前面的知识可知，有自反关系、对称关系、可传递关系，对于反自反或既不是自反，也不是反自反的关系，是否适当添加一些序偶，使之变成自反的关系，同时也要使添加的序偶尽可能少，类似对关系进行“投入”，使之发育成对称关系与可传递关系，同时要求“投入”刚刚好，这样得到的自反关系、对称关系、可传递关系，称为原关系的自反闭包(记为r(R))、对称闭包(记为s(R))、可传递闭包(t(R))，严格的数学定义如下。

定义 3.9.1 设  $R \subseteq A \times A$ ，若存在关系  $R' \subseteq A \times A$ ，满足如下条件则称为自反闭包。

- (1)  $R'$  是自反关系。
  - (2)  $R \subseteq R'$ 。
  - (3) 任意  $R'' \subseteq A \times A$  且  $R \subseteq R''$ ，那么  $R' \subseteq R''$ 。
- 即  $r(R)$  是包含  $R$  的所有自反关系中，序偶最少的一个。

定义 3.9.2 设  $R \subseteq A \times A$ ，若存在关系  $R' \subseteq A \times A$ ，满足如下条件则称为对称闭包。

- (1)  $R'$  是对称关系。
  - (2)  $R \subseteq R'$ 。
  - (3) 任意  $R'' \subseteq A \times A$  且  $R \subseteq R''$ ，那么  $R' \subseteq R''$ 。
- 即  $s(R)$  是包含  $R$  的所有对称关系中，序偶最少的一个。

定义 3.9.3 设  $R \subseteq A \times A$ ，若存在关系  $R' \subseteq A \times A$ ，满足如下条件则称为可传递闭包。

- (1)  $R'$  是可传递关系。
  - (2)  $R \subseteq R'$ 。
  - (3) 任意  $R'' \subseteq A \times A$  且  $R \subseteq R''$ ，那么  $R' \subseteq R''$ 。
- 即  $t(R)$  是包含  $R$  的所有可传递关系中，序偶最少的一个。

将关系矩阵的主角线上全部变成 1，即得到其**自反闭包**的关系矩阵，从而可得到其自反闭包。

### 3.10、等价关系与集合的划分

定义 3.10.1 设  $R \subseteq A \times A$ ，如果  $R$  是自反、对称、可传递的关系则称为**等价关系**。

定义 3.10.2 设  $R \subseteq A \times A$ ，如果  $R$  是等价关系， $B \subseteq A$ ， $B$  中任意二个元素之间都有关系  $R$ ，则  $B$  是一个**等价类**。

定义 3.10.3 设  $R \subseteq A \times A$ ,  $R$  是等价关系,  $A_0, A_1, \dots, A_k$  是基于  $R$  得到的等价类，则称集合  $\{A_0, A_1, \dots, A_k\}$  为  $A$  关于  $R$  的**商集**，记为  $A/R$ 。

定义 3.10.3 若  $A_0, A_1, \dots, A_{k-1}$  是  $A$  的子集，若  $i \neq j$  时  $A_i \cap A_j = \emptyset$ ，并且  $A = A_0 \cup A_1 \cup \dots \cup A_{k-1}$ ，

---

则称  $A_0, A_1, \dots, A_k$  是  $A$  的一个划分。

定理 3.10.1 设  $R \subseteq A \times A$ ,  $R$  是等价关系,  $A_0, A_1, \dots, A_{k-1}$  是利用  $R$  得到的  $k$  个不同的等价类, 则  $A_0, A_1, \dots, A_{k-1}$  为集合  $A$  的划分。

定理 3.10.2 设  $A_0, A_1, \dots, A_{k-1}$  是  $A$  的划分,  $R = A_0 \times A_0 \cup A_1 \times A_1 \cup \dots \cup A_{k-1} \times A_{k-1}$ , 则  $R$  是等价关系。

### 3.11、偏序关系

定义 3.11.1 设  $R \subseteq A \times A$ , 如果  $R$  是自反、反对称、可传递的关系则称为偏序关系。

如:  $R$  是实数中小于等于关系, 则  $R$  是偏序关系。

定义 3.11.2 设  $R \subseteq A \times A$ ,  $R$  偏序关系,  $x$  与  $y$  是  $A$  中的元素, 若序偶  $\langle x, y \rangle$  与  $\langle y, x \rangle$  至少有一个在  $R$  中, 则称  $x$  与  $y$  可比。

定义 3.11.3 设  $R \subseteq A \times A$ ,  $R$  偏序关系, 若  $A$  中任意二个元素都可比, 则称  $A$  为全序关系或线序关系。

定义 3.11.4 设  $R \subseteq A \times A$ ,  $R$  偏序关系, 将关系图绘制所有箭头都朝上, 然后去掉所有箭头、去掉自旋边、去掉复合边, 得到关系图的简化形式, 称为哈斯图。

定义 3.11.5 在哈斯图中, 如果某个元素  $y$  在元素  $x$  的直接上方, 则称  $y$  盖住了  $x$ 。记 COVA = { $\langle x, y \rangle$ }

定义 3.11.6 设  $R \subseteq A \times A$ ,  $R$  偏序关系, 将偏序关系与集合  $A$  一块称为偏序集, 记为  $\langle A, R \rangle$ , 表示是  $A$  上的偏序关系。以后说偏序关系时, 可简单地说偏序集  $\langle A, R \rangle$ 。

定义 3.11.7 在偏序集  $\langle A, R \rangle$  中,  $B \subseteq A$ ,  $y \in B$ , 若  $\forall x \in B$  都有  $\langle x, y \rangle \in R$ , 则称  $y$  是最大元。即最大元与  $B$  中每个元素都可比, 并且都比其大。

定义 3.11.8 在偏序集  $\langle A, R \rangle$  中,  $B \subseteq A$ ,  $y \in B$ , 若  $\forall x \in B$  都有  $\langle y, x \rangle \in R$ , 则称  $y$  是最小元。即最小元与  $B$  中每个元素都可比, 并且都比其小。

一个子集中没有最大元或最小元时, 可能存在极大元或极小元。

定义 3.11.9 在偏序集  $\langle A, R \rangle$  中,  $B \subseteq A$ ,  $y \in B$ , 若不存在  $x \in B$  使得  $\langle y, x \rangle \in R$ , 则称  $y$  是极大元, 即  $B$  中不存在比  $y$  “大”的元素。即极大元与  $B$  中有些元素是否可比不做要求。

定义 3.11.10 在偏序集  $\langle A, R \rangle$  中,  $B \subseteq A$ ,  $y \in B$ , 若不存在  $x \in B$  都有  $\langle x, y \rangle \in R$ , 则称  $y$  是极小元, 不存在比  $y$  小的元素。即极小元与  $B$  中元素是否可比不做要求。

定义 3.11.11 在偏序集  $\langle A, R \rangle$  中,  $B \subseteq A$ ,  $y \in B$ , 若任意  $x \in B$  都有  $\langle x, y \rangle \in R$ , 则称  $y$  是  $B$  的上界。与  $B$  中每个元素都可比, 并且都比  $B$  中的元素大。

### 3.12、其它关系

定义 3.6.1 给定集合  $A$  上的关系  $\rho$ , 若  $\rho$  是自反的、对称的, 则称  $\rho$  是  $A$  上的相容关系。

定义 3.6.3 给定非空集合  $A$ , 设有集合  $S = \{S_1, S_2, \dots, S_n\}$ , 其中  $S_i \subseteq A$  且  $S_i \neq \Phi$ ,  $i=1, 2, \dots, m$ , 且

$S_i \cap S_j = \Phi (i \neq j)$ , 则称集合  $S$  称作  $A$  的覆盖。

定理 3.6.1 给定集合  $A$  的覆盖,  $S_1, S_2, \dots, S_n$ , 由它确定的关系:  $S_1 \times S_1 \cup \dots \cup S_n \times S_n$  是相容关系。

定义 3.7.1 设  $R$  为定义在集合  $A$  上的一个关系, 若  $R$  是自反的, 对称的, 传递的, 则  $R$  称为等价关系。(显然

---

等价关系一定是相容关系)。

定义 3.7.2 设给定非空集合  $A$ , 若有集合  $S=\{S_1, S_2, \dots, S_n\}$ , 其中  $S_i \subseteq A$  且  $S_i \neq \emptyset$  ( $i=1,2,\dots,n$ ), 且有

$S_i \cap S_j = \emptyset$  ( $i \neq j$ ), 同时有  $\bigcup_{i=1}^n S_i = A$ , 则称  $S$  为  $A$  的一个划分。(所有子集的并为  $A$ , 且子集的交为空, 则这些子集组成的集合为  $A$  的一个划分, 覆盖中, 子集的交集可不为空)

等价类  
商集

偏序关系(自反性, 反对称性, 传递性) $\langle A, \leq \rangle$ , 哈斯图, 可比的, 元素  $y$  盖住元素  $x$ , 全序关系, 极大元, 极小元, 最大元, 最小元

拟序关系(反自反的, 传递的) $\langle A, \prec \rangle$

## 第四章 代数系统

定义 4.3.1 设 $\circ$ 是集合  $S$  上的二元运算, 若  $\forall x, y \in S$  都有  $x \circ y = y \circ x$ , 则称 $\circ$ 在  $S$  上是可交换的, 或者说运算 $\circ$ 在  $S$  上满足交换律。

定义 4.3.2 设 $\circ$ 是集合  $S$  上的二元运算, 若  $\forall x, y, z \in S$  都有  $(x \circ y) \circ z = x \circ (y \circ z)$ , 则称 $\circ$ 在  $S$  上是可结合的, 或者说运算 $\circ$ 在  $S$  上满足结合律。

定义 4.3.3 设 $\circ$ 是集合  $S$  上的二元运算, 若  $\forall x \in S$  都有  $x \circ x = x$ , 则称 $\circ$ 在  $S$  上是幂等的, 或说运算 $\circ$ 在  $S$  上满足幂等律。

定义 4.3.4 设 $\circ$ 与 $*$ 是集合  $S$  上的两种运算, 若  $\forall x, y, z \in S$  都有  $x \circ (y \circ z) = (x \circ y) \circ (x \circ z)$  与  $(y \circ z) \circ x = (y \circ x) \circ (z \circ x)$ , 则称 $\circ$ 与 $*$ 是可分配的。

定义 4.3.5 设 $\circ$ 与 $*$ 是集合  $S$  上的两种可交换的二元运算, 若  $\forall x, y \in S$  都有  $x \circ (x \circ y) = x$  与  $x \circ (x \circ y) = x$  则称 $\circ$ 与 $*$ 是满足吸收律, 内外两种运算不一样, 运算符内外各出现一次, 以多吃少。

广群:

定义 4.6.1 对于代数系统 $\langle A, \heartsuit \rangle$ , 若其运算 $\heartsuit$ 是封闭的, 即  $\forall a, b \in A$ , 其运算结果  $a \heartsuit b \in A$ , 则称此代数系统为广群。

半群:

定义 4.6.2 对于代数系统 $\langle A, \heartsuit \rangle$ , 若其运算 $\heartsuit$ 是封闭的, 还是可结合的, 即  $\forall a, b, c \in A$ ,  $(a \heartsuit b) \heartsuit c = a \heartsuit (b \heartsuit c)$ , 则称此代数系统为半群。

群:

定义 4.7.1 若代数系统 $\langle A, \heartsuit \rangle$ 之运算 $\heartsuit$ 是封闭的、可结合的、存在单位元、 $\forall a \in A$  都有逆元  $a^{-1} \in A$ , 则称该代数系统为群。记为  $G$ , 即 Group 的首字母。

子群:

---

定义 4.8.1 代数系统 $\langle G, \circ \rangle$ 是群,  $\emptyset \neq H \subseteq G$ , 若代数系统 $\langle H, \circ \rangle$ 是群, 则称为 $\langle G, \circ \rangle$ 的子群, 也简称  $H$  是  $G$  的子群, 记为  $H \leq G$ 。若  $H \subset G$  则称  $H$  是  $G$  的真子群, 记为  $H < G$ 。