# 离散数学

Fan

2023年秋季

## 目录



**摘要**

本笔记结合离散课堂内容以及*Logic in Computer Science*和*concrete mathmatics*.

表 1: 常用记号

| 含义 | 记号 |
|---|---|
| $\neg$ | 否定联结词 |
| $\vee$ | 析取联结词 |
| $\wedge$ | 合取联结词 |
| $\rightarrow$ | 蕴含联结词 |
| $\neg p$ | 非p |
| $p \vee q$ | p或q |
| $p \wedge q$ | p和q |
| $p \rightarrow q$ | 如果p那么q |

成绩组成为:

1. 50%平时成绩
    - 考勤
    - 课堂提问
    - 作业完成情况
2. 50%期末考试

# 1 命题逻辑

在研究逻辑时,我们通常不关注语句的具体含义,而只关注其逻辑结构.

## 1.1 命题

为了能让我们的语言体现出其逻辑结构,我们使用命题逻辑的语言,它基于命题, 或是能够被判断真假的陈述句.

例. “哥德巴赫猜想是正确的”这句话是命题.

一般地,只要某句话能够被赋予真值,我们便认为它是命题,尽管有可能该真值并不能反映出这句话实际上的真值.

命题的真值即命题的判断结果,真为1,假为0,若为真则称之为真命题,否则为假命题

一个句子若是命题,它首先是一个陈述句,其次有唯一的真值.

注. 因此悖论不属于命题,例如‘这句话是假话’.

我们把不可分解的命题称为‘原子命题’(‘简单命题’),例如‘1是奇数’.我们通常用小写字母来代表他们. 我们通过 $\neg, \vee, \wedge, \rightarrow$等联结词将原子命题联结成更复杂的复合命题.

注. 为了统一，一般将句子命题化时，原子命题对应的都是肯定句，否定句的原子命题则表示为其肯定句的原子命题的否定。

注. “虽然p，但是q”用命题逻辑来表示为 $p \wedge q$。

注. 在命题形式化的过程中，要注意区分“相容或”和“排斥或”的区别。“A是男或女”便是排斥或。

注. $\vee$指的是至少有一个成立,而非只有一个成立.

在数理逻辑中,‘$\rightarrow$’,即‘如果,就’前后的事件不要求一定具有因果含义,它只表示真值的保持.

对于 $p \rightarrow q$,我们称该式为 $p$与 $q$的蕴含式,称 $p$为蕴含式的前件, $q$为后件, $q$是 $p$的必要条件.我们规定 $p \rightarrow q$为假当且仅当 $p$为真且 $q$为假.

注. ‘如果 $p$,则 $q$’有许多等价的说法,例如‘只要 $p$,就 $q$’,‘因为 $p$,所以 $q$’, ‘只有 $q$才(有可能)$p$’,‘除非 $q$才(有可能)$p$’,‘除非 $q$,否则非$p$’

根据定义,当蕴含式的前件为假时,该蕴含式一定为真.

同时我们还有等价联结词 $\leftrightarrow$,我们规定 $p \leftrightarrow q$为真当且仅当 $p$与 $q$同时为真或同时为假.

注. ‘$p \leftrightarrow q$‘可以理解为 $p$与 $q$互为充分必要条件.它与 $(p \to q) \wedge (q \to p)$的逻辑关系完全一致.

以上五个联结词组成一个联结词集.由其中的一个联结词与两个原子命题(对于否定联结词只有一个) 组成的复合命题称为基本复合命题.

为了避免歧义,我们约定这几个连接词的优先级从高到底为 $\neg, \wedge, \vee, \to, \leftrightarrow$, 同时, $\to$是右结合的,即

$$p \to q \to r即p \to (q \to r).$$

注. $\wedge$ 比 $\vee$优先级更高,这一关系类似于乘法比加法的优先级更高.

简单命题称为命题常项,而正值可以变化的陈述句称为命题变项.我们一般也用小写字母来表示命题变项. 而命题公式定义为:

- 单个命题变项是合式公式,称为原子命题公式
- 若 $A$是合式公式,则 $(\neg A)$也是合式公式
- 若 $A, B$是合式公式,则 $(A \wedge B), (A \vee B), (A \to B), (A \leftrightarrow B)$ 也是合式公式.
- 只有有限次地应用以上三条规则所形成的符号串才是合式公式

设 $A$是合式公式, $B$是其中的一部分,若 $B$是合式公式,则称 $B$是 $A$的子公式.

若命题公式 $A$是单个命题变项,则称 $A$为0层公式.我们称命题 $A$是 $n+1(n \geq 0)$层公式,只要 $A$ 是下列情况之一:

1. $A = \neg B$,$B$是 $n$层公式
2. $B, C$分别为 $i$层和 $j$层公式,且 $\max(i, j) = n$,则由 $\wedge, \vee, \to, \leftrightarrow$ 其中一个将他们联结起来所得到的合式公式为 $A$

注. 实际上层数即一个合式公式的当个命题变量被联结符所操控的次数的最大值.

由于命题公式中有命题变项,故其真值一般是不确定的,当公式中的所有命题变项都解释成具体的命题后, 命题公式就成了真值确定的命题了.

设在命题公式 $A$中出现的所有命题变项为 $p_1, p_2, \cdots, p_n$,给它们指定一个真值,称为对公式 $A$的一个赋值. 若该赋值使 $A$的真值为1,则称该赋值为$A$的成真赋值,否则称为 $A$的成假赋值.

将命题公式 $A$在所有赋值下的取值情况列成表,该表便是 $A$的真值表.

设 $A$是一个命题公式,如果 $A$在各种赋值下取值总为1,则称 $A$为永真式或重言式. 若 $A$在各种赋值下取值总为0,则称 $A$是永假式或矛盾式. 若 $A$不是矛盾式,则称 $A$为可满足式.

由于给定 $n$个命题变项,共有 $2^n$可能的赋值,而同时每个赋值下公式只能取值真或假,因此含有 n个命题变项的公式其真值表有 $2^{2^n}$种情况.然而我们可以使用联结词和括号,在这 $n$个命题变式的基础上构造出无穷个命题公式,因此必有无穷个公式有相同的真值表.

注. $n$个命题变项,每个可以取真或假,整体有 $2^n$种可能,而对于其中的每一种可能,整个公式的取值又只有真或假两种可能, 所以整个公式的取值有 $2^{2^n}$种可能.

设公式 $A$,$B$中总共含有命题变项 $p_1, p_2, \cdots, p_n$,但 $A$或 $B$并不全含有这些变项. 如果某个变项未在公式 $A$中出现,则称该变项为 $A$的哑元.在讨论 $A$与 $B$是否有相同的真值表时, 应将哑元考虑在内.

## 1.2 命题逻辑的等值演算

**定义.** 如果命题公式 $A$与 $B$的真值表相同,那么称 $A$与 $B$是等价的,记作 $A \Leftrightarrow B$

人们将一组经检验为正确的等值式作为等值式模式,通过公式之间的等值演算来判断两公式是否等值. 常用的等值式模式有:

1. 双重否定律:$A \Leftrightarrow \neg(\neg A)$
2. 幂等律: $A \Leftrightarrow A \vee A, A \Leftrightarrow A \wedge A$
3. 交换律: $A \vee B \Leftrightarrow B \vee A, A \wedge B \Leftrightarrow B \wedge A$
4. 分配律:
   - $A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$($\vee$对 $\wedge$的分配律)
   - $A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$($\wedge$对 $\vee$的分配律)
5. 德摩根律: $\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B, \neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$
6. 吸收律: $A \vee (A \wedge B) \Leftrightarrow A, A \wedge (A \vee B) \Leftrightarrow A$
7. 零律: $A \vee 1 \Leftrightarrow 1, A \wedge 0 \Leftrightarrow 0$

8. 同一律: $A \vee 0 \Leftrightarrow, A \wedge 1 \Leftrightarrow A$

9. 排中律: $A \vee \neg A \Leftrightarrow 1$

10. 矛盾律: $A \wedge \neg A \Leftrightarrow 0$

11. 蕴含等值式: $A \to B \Leftrightarrow \neg A \vee B$

12. 等价等值式: $(A \leftrightarrow B) \Leftrightarrow (A \to B) \wedge (B \to A)$

13. 假言易位: $A \to B \Leftrightarrow \neg B \to \neg A$

14. 等价否定等值式: $A \Leftrightarrow B \Leftrightarrow \neg A \leftrightarrow \neg B$

15. 归谬论: $(A \to B) \wedge (A \to \neg B) \Leftrightarrow \neg A$

16. $A \to (B \to C) \Leftrightarrow (A \wedge B) \to C$

注. 这里的零律可以理解为信息的坍缩.

注. 在处理括号时，记得使用吸收律和逆用结合律。

利用这16组24个等值式可以推演出更多的等值式。由已知的等值式推演出另一些等值式的过程称为等值演算。在等值演算中,经常用到如下置换规则,即 “设 $\Phi(A)$是含有公式 $A$的命题公式,$\Phi(B)$是用公式 $B$置换了 $\Phi(A)$中所有的 $A$后所得的公式,若 $B \Leftrightarrow A$,则 $\Phi(B) \Leftrightarrow \Phi(A)$”

**定义.** 命题变项及其否定统称作文字. 仅由有限个文字构成的析取式称作简单析取式;仅由有限个文字构成的合取式称作简单合取式.

注. 单个文字既是简单析取式,又是简单合取式.

**定理 1.1.** 一个简单析取式是重言式当且仅当它同时含有某个命题变项及其否定式.

**定理 1.2.** 一个简单合取式是矛盾式当且仅当它同时含有某个命题变项及其否定式.

**定义.** 由有限个简单合取式构成的析取式称为析取范式;由有限个简单析取式构成的合取式称为合取范式; 析取范式和合取范式统称为范式.

注. 由于幂等律,单个的简单析取式既可以看作是析取范式(由有限个文字组成的析取式,每个文字对自己合取),也可以看作是合取范式(把整个看作是一个简单析取式,然后自己对自己合取).

**定理 1.3.** 一个析取范式是矛盾式当且仅当它的每个简单合取式都是矛盾式.
一个合取范式是重言式当且仅当它的每个简单析取式都是重言式.

**定理 1.4** (范式存在定理)**.** 任一命题公式都存在着与之等值的析取范式与合取范式.

注. 一般求给定公式的范式的步骤为:

1. 用蕴含等值式与等价等值式分别消去蕴含联结词与等价联结词.
2. 运用双重否定律消去双重否定并用德摩根律来使得对于简单析取式或者简单合取式的否定转化为语句的否定(这是范式所必须满足的)
3. 利用析取联结词对于合取联结词的分配律求合取范式;利用合取联结词对于析取联结词的分配律求析取范式.

这样求出来的范式是不唯一的,例如在求析取范式时,如果有一个简单合取式是一个矛盾式,那么消去其前后都是合理的范式. 求合取范式也有类似的情况.

**定义.** 在含有 $n$个命题变项的简单合取式（简单析取式）中，若每个命题变项和它的否定式中，恰好出现一个，且只出现一次，并且命题变项或其否定式按下标从小到大或按字典序排序，则称该简单合取式（简单析取式）为极小项（极大项）。

注. 合取即取交集，越交越小，从而对应极小项。相应地，析取对应极大项。

易知， $n$个命题变项共可产生 $2^n$个不同的极小项。每个极小项仅有一个成真赋值，若一个极小项的成真赋值对应的二进制数转化为十进制数为 $i$，则将该极小项记为 $m_i$。类似地，每一个极大项也有对应成假赋值和十进制数 $i$，记为 $M_i$。

**定理 1.5.** 设 $m_i$与 $M_i$是命题变项 $p_1, p_2, \cdots, p_n$形成的极小项和极大项，则 $\neg m_i \Leftrightarrow M_i, \neg M_i \Leftrightarrow m_i$。

**定义.** 如果由 $n$个命题变项构成的析取范式（合取范式）中所有的简单合取式（简单析取式）都是极小项（极大项），则称该析取式（合取式）为主析取范式（主合取范式）。

**定理 1.6.** 任何命题公式都存在着与之等值的主析取范式和主合取范式，并且是唯一的。

注. 主析取范式和主合取范式的求法：

1. 先通过等值推演将所给的命题公式华为析取范式（合取范式）；
2. 若某个简答合取式（简单析取式） $A$中既不含变项 $p_i$，又不含变项 $\neg p_i$，则通过

$$A \Leftrightarrow A \wedge 1 \Leftrightarrow (p_i \vee \neg p_i) \Leftrightarrow (A \wedge p_i) \vee (A \wedge \neg p_i)$$

$$A \Leftrightarrow A \vee 0 \Leftrightarrow (p_i \wedge \neg p_i) \Leftrightarrow (A \vee p_i) \wedge (A \vee \neg p_i)$$

   补齐变项。

3. 消去重复变项和矛盾式，如用 $p, m_i, 0$分别代替 $p \wedge p, m_i \vee m_i$和矛盾式，等。

主析取范式和主合取范式有许多应用：

1. 求公式的成真与成假赋值：对于含有 $n$个变项的命题公式，若其主析取范式含 $s(0 \leq s \leq 2^n)$个极小项，则 $A$有 $s$个成真赋值，它们是极小项下标的二进制表示，其余 $2^n - s$个赋值都是成假赋值。
2. 进一步，可以用来判断公式的类型：设公式 $A$中含有 $n$个变项，则 $A$为重言式当且仅当 $A$的主析取范式含有全部 $2^n$个极小项； $A$为矛盾式当且仅当 $A$的主析取范式不含任何极小项； $A$为可满足式当且仅当 $A$的主析取范式中至少含一个极小项。
3. 设公式 $A, B$共有 $n$个变项。按 $n$个变项求出 $A, B$的主析取范式。若 $A$与 $B$有相同的主析取范式，则 $A \Leftrightarrow B$,否则 $A \not\Leftrightarrow B$。

**定理 1.7.** 主合取范式可有主析取范式直接得到：

设公式 $A$含有 $n$个变项， $A$的主析取范式为

$$A \Leftrightarrow m_{i_1} \vee m_{i_2} \vee \cdots \vee m_{i_l}, 0 \leq i_r \leq 2^n - 1, r = 1, 2, \cdots, l$$

未在主析取范式中出现的极小项设为

$$m_{j_1}, m_{j_2}, \cdots, m_{j_{2^n - l}},$$

则 $A$的主合取范式为：

$$A \Leftrightarrow M_{j_1} \wedge M_{j_2} \wedge \cdots \wedge M_{j_{2^n - l}}$$

与主析取范式类似地有：

因为重言式无成假赋值，因而其主合取范式中无任何极大项。重言式的主合取范式记为1；矛盾式无成真赋值，故其主合取范式含有所有 $2^n$个极大项。

含 $n$个变项的所有公式，共有 $2^{2^n}$种不同的主析取范式（主合取范式），这是因为 $2^n$个极小项（极大项）可以选择出现或不出现。

$A \Leftrightarrow B$当且仅当 $A$与 $B$有相同的真值表，有当且仅当 $A$与 $B$有相同的主析取范式（主合取范式）。因此，真值表与主析取范式（主合取范式）式描述命题公式标准形式的两种不同的等价形式。

**定义.** 称映射 $F : 0,1^n \to 0,1$为 $n$元真值函数。其中 $0,1^n$表示由 $0,1$组成的长为 $n$的字符串集合。

由定义可知， $n$元真值函数有$2^{2^n}$个。

注. 每个真值函数与唯一的主析取范式(主合取范式)）等值，而每个主析取范式(主合取范式)对应无穷多个与之等值的命题公式。因此每个真值函数对应无穷多个与之等值的命题公式。另一方面，由于每个命题公式与唯一的主析取范式（主合取范式）等值，每个命题公式都有唯一一个真值函数与之等值。

**定义.** 设 $S$是一个联结词集合。如果任何 $n$元 $(n \geq 1)$真值函数都可以由仅含 $S$中的联结词构成的公式表示，则称 $S$是联结词完备集。

**定理 1.8.** 1. $\{\neg, \wedge, \vee\}$

2. $\{\neg, \wedge, \vee, \to, \leftrightarrow\}$

3. $\{\neg, \wedge\}$

4. $\{\neg, \wedge\}$

5. $\{\neg, \vee\}$

6. $\{\neg, \to\}$

均是联结词完备集。

**定义.** 设 $p, q$为两个命题。符合命题 “$p$与 $q$的否定式（ $p$或 $q$的否定式）”称为 $p, q$的”与非式“（”或非式“），记作 $p \uparrow q(p \downarrow q)$。符号 $\uparrow$称作与非联结词（ $\downarrow$称为或非联结词）。

即 $p \uparrow q = \neg(p \wedge q), p \downarrow q = \neg(p \vee q)$。 $p \uparrow q$为证当且仅当 $p$与 $q$不同时为真； $p \downarrow q$为真当且仅当 $p$与 $q$同时为假。

**定理 1.9.** {↑}与 {↓}都是联结词完备集。

## 1.3 自然推理

在自然推理中,我们有一套证明规则,他们允许我们从一些公式中推导出其他公式. 通过连续运用这些规则,我们能从一些前提条件推到出最终的结论.

设 $A_1, A_2, \cdots, A_k$和 $B$是命题公式，若对于 $A_1, A_2, \cdots, A_k, B$中出现的命题变项的任一组赋值， $A_1 \wedge A_2 \wedge \wedge \cdots \wedge A_k \rightarrow B$ 永真，则称由前提 $A_1, A_2, \cdots, A_k$推出的 $B$的推理是有效的（或正确的），并称 $B$是有效的结论。

将一个推理的诸前提的集合记为 $\Gamma$，则由 $\Gamma$推出结论 $B$的推理记为 $\Gamma \vdash B$。若该推理是正确的，则记为 $\Gamma \models B$或 $(\Gamma \Rightarrow B)$，否则记为 $\Gamma \not\models B$或$(\Gamma \not\Rightarrow B)$。称 $\Gamma \vdash B$和 $\{A_1, A_2, \cdots, A_k\} \vdash B$为推理的形式结构。

注. 推理正确，并不能保证结论 $B$一定为真，因为前提可能是假的。

**定理 1.10.** 命题公式 $A_1, A_2, \cdots, A_k$推 $B$的推理正确，即 $\{A_1, A_2, \cdots, A_k\} \models B$ 当且仅当 $(A_1 \wedge A_2 \wedge \cdots \wedge A_k) \rightarrow B$为永真式。

因此 $\{A_1, A_2, \cdots, A_k\} \vdash$可以用 $(A_1 \wedge A_2 \wedge \cdots \wedge A_k) \rightarrow B$ 来表示，$\{A_1, A_2, \cdots, A_k\} \models B$也可以用 $A_1 \wedge A_2 \wedge \cdots \wedge A_k \Rightarrow B$。

注. 命题是对于一件事物的描述. 命题的真值是以我们的真实世界为判断标准的,而在自然演绎中,我们并不去考虑前提的真值,我们只关注给定这些前提,我们能推导出什么样的结论. 例如有前提‘如果我是人,我不会吃饭’,‘我吃饭’,可以推出‘我不是人’.用符号来描述就是 ‘$p \rightarrow \neg q, q \vdash \neg p$’, 这里的否定联结词表示的是命题的否定形式.也就是说,推导的过程便是假设前提中的描述都是成立的,然后寻找在此前提下我们还能有什么描述是成立的. 虽然推出的结论可能真值为0,但是这仍然是一个有用的结论.

判断推理是否正确的三种直接方法为：1.真值表法 2.等值演算法2.主析取范式法

常用的推理定理可以在推理过程中直接引用，常见的推理定律有：

1. 附加律：$A \Rightarrow A \vee B$

2. 化简律：$A \wedge B \Rightarrow A$

3. 假言推理：$(A \to B) \wedge A \Rightarrow B$

4. 拒取式：$(A \to B) \wedge \neg B \Rightarrow \neg A$

5. 析取三段论：$(A \vee B) \wedge \neg B \Rightarrow A$

6. 假言三段论：$(A \to B) \wedge (B \to C) \Rightarrow (A \to C)$

7. 等价三段论：$(A \leftrightarrow B) \wedge (B \leftrightarrow) \Rightarrow (A \leftrightarrow C)$

8. 构造性二难：$(A \to B) \wedge (C \to D) \wedge (A \vee C) \Rightarrow (B \vee D)$

   特殊形式为：$(A \to B) \wedge (\neg A \to B) \wedge (A \vee \neg A) \Rightarrow B$

9. 破坏性二难：$(A \to B) \wedge (C \to D) \wedge (\neg B \vee \neg D) \Rightarrow (\neg A \vee \neg C)$

之前的等值式可以在推理的过程中使用。下面再给出一些等值式：

1. $A \Leftrightarrow (A \wedge B) \vee (A \wedge \neg B)$

2. $\neg(A \to B) \Leftrightarrow A \wedge \neg B$

3. $A \to (B \to C) \Leftrightarrow (A \wedge B) \to C$

4. $(A \leftrightarrow B) \Leftrightarrow (A \wedge B) \vee (\neg A \wedge \neg B)$

5. $\neg(A \leftrightarrow B) \Leftrightarrow A \leftrightarrow \neg B$

6. $\neg A \Rightarrow A \to B$

7. $B \Rightarrow A \to B$

8. $A \to B \Rightarrow (A \vee C) \to (B \vee C)$

9. $A \to B \Rightarrow (A \wedge C) \to (B \wedge C)$

“证明”是一个描述推理过程的命题公式序列，其中的每个公式或是已知前提，或者是由某些前提应用推理规则得到的结论。

**定义.** 一个形式系统 $I$由下面四个部分组成：

1. 非空的字母表集，记作 $A(I)$

2. $A(I)$中符号构造的合式公式集，记作 $E(I)$

3. $E(I)$中一些特殊的公式组成的公理集，记作 $A_X(I)$

4. 推理规则集，记作 $R(I)$。

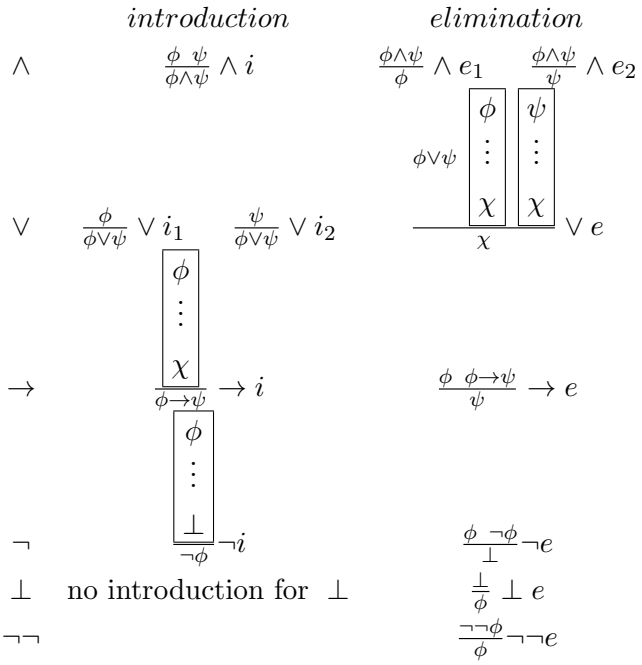
这样可以将 $I$记作4元组 $< A(I), E(I), A_X(I), R(I) >$。其中 $< A(I), E(I) >$ 是 $I$的形式语言系统， $< A_X(I), R(I) >$为 $I$的形式演算系统。

形式系统一般分为自然推理系统，另外的则是公理推理系统。前者中，可以从任意给定的前提出发，应用系统的推理规则进行推理演算，得到的最后命题公式是推理的结论。在后者中则只能从若干给定的公理出发，应用系统的推理规则进行推理演算，得到的结论是系统中的重言式，称为系统中的定理。

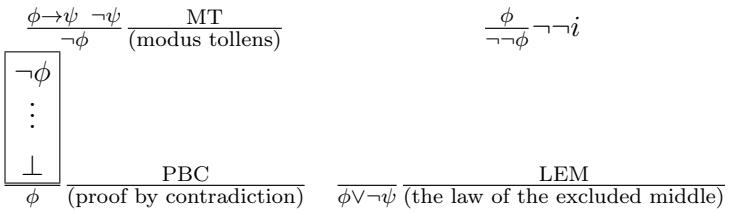
**定义.** 自然推理系统 $P$由一下三部分要素组成：

1. 字母表：
   (a) 命题变项符号： $p, q, r, \cdots$
   (b) 联结词符号: $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$
   (c) 逗号和括号： $,, (, )$
2. 合适公式集
3. 推理规则：
   (a) 前提引入规则：在证明的任何步骤上都可以引入前提
   (b) 结论引入规则：在证明的任何步骤上所得到的结论都可以作为后续证明的前提
   (c) 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

自然演绎的基本规则如下




在此基础之上我们可以推到出一些有用的规则:




式中的括号意味着引入一条或多条只有在该方框内才存在的条件,例如假设,或者消除析取式时的分类讨论,方框后紧跟着的语句应该体现出引入该方框的目的.

**定义.** 假设 $\phi$和 $\psi$是两个公式,我们称它们是 *provably equivalent*当且仅当 $\phi\vdash\psi$和$\psi\vdash\phi$同时成立,此时我们记作 $\phi\dashv\vdash\psi$

**定理 1.11** (Soundness)**.** 假设 $\phi_1,\phi_2,\cdots,\phi_n$和 $\psi$ 均为命题逻辑公式。如果 $\phi_1,\phi_2,\cdots,\phi_n\vdash\psi$成立，则 $\phi_1,\phi_2,\cdots,\phi_n\models\psi$成立。

该定理的一大应用是证明从某些条件无法证明某一结论。

**定理 1.12** (Soundness and Completeness)**.** 假设 $\phi_1,\phi_2,\cdots,\phi_n,\psi$是命题逻辑公式。那么 $\phi_1,\phi_2,\cdots,\phi_n\models\psi$成立当且仅当 $\phi_1,\phi_2,\cdots,\phi_n\vdash\psi$成立。

**定义.** 假设 $\phi$和 $\psi$是命题公式，我们称它们是 'semantically equivalent' 当且仅当 $\phi \models \psi$并且 $\psi \models \phi$，此时记作 $\phi \equiv \psi$。

## 2 谓词逻辑

命题逻辑有其缺陷，例如对于陈述句“每个学生都比一些老师年轻”，在命题逻辑中，它只是一个命题 $q$，其中“每个”,”比……年轻“,”一些“这些信息都丢失了，为此，我们需要谓词逻辑，也被称为一阶逻辑。

谓词逻辑命题符号化的三个基本要素为：

1. 个体词：研究对象中可以独立存在的具体的或抽象的客体。
   - 表示具体或特定客体的个体词称为个体常项，一般用小写字母$a, b, c, \cdots$表示具体或特定客体的个体词称为个体常项，一般用小写字母$a, b, c, \cdots$来表示。
   - 表示抽象或泛指的个体词称为个体变项，一般用小写字母 $x, y, z, \cdots$来表示。
   - 个体变项的取值范围称为个体域（或论域），可以是有限集或是无限集。由宇宙间一切事物组成的个体域称为全总个体域。
2. 谓词：用来刻画个体词的性质或个体词之间的相互关系的词
   - 常用大写字母 $F, G, H$等来表示谓词常项
   - 表示具体性质或关系的谓词称为谓词常项，表示抽象或泛指的性质或关系的谓词称为谓词变项
   - 一般地，用 $P(x_1, x_2, \cdots, x_n)$表示含有 $n(n \geq 1)$个命题变项 $x_1, x_2, \cdots, x_n$的 $n$元谓词。它可以看成是以个体域为定义域，以 $\{0, 1\}$为值域的 $n$元函数关系。
   - 当一个谓词为谓词常项，且它不含个体变项，或所含的都是个体常项时，可以将其视为一个命题。
   - 特性谓词：从全总个体域中分离出一个集合，定义的谓词
3. 量词：表示个体常项或变项之间数量关系的词，有且仅有全称量词和存在量词。
   - 全称量词：表示“全部”含义的词，符号化为 $\forall$。

- 存在量词：表示“存在”含义的词，符号化为 $\exists$。

注. 若要表示特定个体域中的两个不同个体，不能只是连续使用两个量词以及特性谓词，还需要使用一个用于判断两个个体不相同的谓词。

注. 如果问题中没有指明个体域，则默认为全总体域。

注. 一般地，对全称量词，特性谓词应作为蕴含式的前件，因为所有"A"都有性质“B”即是“A”可以推出“B”。

一般地，对于存在量词，特性谓词应作为合取式的一项，因为存在"A"有性质"B"即存在是”A“且有"B"。

注. 在不同个体域中，同一命题的符号化形式可能不同，其真值也有可能不同。

**定义.** 设 $L$是一个非逻辑符号，由 $L$生成的一阶语言 $\mathcal{L}$的语言表包括如下符号：

- 非逻辑符号

  1. $L$中的个体常项符号： $a, b, c, \cdots; a_i, b_i, c_i, \cdots, i \geq 1$
  2. $L$中的函数符号： $f, g, h, \cdots; f_i, g_i, h_i, \cdots, i \geq 1$
  3. $L$中的谓词符号： $F, G, H, \cdots; F_i, G_i, H_i, \cdots, i \geq 1$

- 逻辑符号

  1. 个体变项符号： $x, y, z, \cdots; x_i, y_i, z_i, \cdots, i \geq 1$
  2. 符号： $\forall, \exists$
  3. 联结词符号： $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$
  4. 逗号与括号： $,, (,)$

**定义.** 一阶语言 $\mathcal{L}$的项定义为：

1. 个体常量符号和个体变项符号是项
2. 若 $\phi(x_1, x_2, \cdots, x_n)$是 $n$元函数符号， $t_1, t_2, \cdots, t_n$是 $n$个项，则 $\phi(t_1, t_2, \cdots, t_n)$是项。
3. 所有项都是有限次使用（1），（2）得到的。

**定义.** 设 $R(x_1, x_2, \cdots, x_n)$是一阶语言 $\mathcal{L}$中的 $n$元谓词符号。 $t_1, t_2, \cdots, t_n$是 $\mathcal{L}$的 $n$个项，则称 $R(t_1, t_2, \cdots, t_n)$ 是 $\mathcal{L}$的原子公式。

**定义.** 一阶语言 $\mathcal{L}$中的合式公式（也称谓词公式或公式）的定义如下：

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 $A$、 $B$是合式公式，则 $(A \wedge B), (A \vee B), (A \to B), (A \leftrightarrow B)$ 也是合式公式
4. 若 $A$是合式公式，则 $\forall x A, \exists x A$也是合式公式
5. 只有有限次应用（1）（4）构成的符号串才是合式公式。

**定义.** 在公式 $\forall x A$和 $\exists x A$中，称 $x$为指导变元， $A$为相应量词的辖域。在 $\forall x$和 $\exists x$的辖域中， $x$的所有出现都称为约束出现， $A$中不是约束出现的其他变项都称为自由出现。

注. 可以通过绘制语法树来判断个体变项是否被约束以及得到相应量词的辖域。

各个量词的辖域之间没有重叠部分，语法树中的任意一个部分所属的辖域即从那个部分向上搜寻到的第一个量词的辖域。

**定义.** 设 $A$是任意的公式，若 $A$中不含自由出现的个体变项，则称 $A$为封闭的公式，简称公式。

**定义.** 对公式 $A$指定其中个体域的范围，并指定其中谓词的具体含义使其成为命题，称为对公式 $A$的一个解释。

设 $\mathcal{L}$是由 $L$生成的一阶语言， $\mathcal{L}$的解释 $I$由下面4部分组成：

1. 非空个体域 $D_I$
2. 对每一个个体常项符号 $a \in L$，有一个 $\bar{a} \in D_I$，称 $\bar{a}$为 $a$在 $I$中的解释
3. 对每一个 $n$元函数符号 $f \in L$，有一个 $D_I$ 上的 $n$元函数 $\bar{f}$，称 $\bar{f}$为 $f$在 $I$中的解释
4. 对每一个 $n$元谓词符号 $F \in L$，有一个 $D_I$上的 $n$元谓词 $\bar{F}$，称 $\bar{F}$为 $F$在 $I$中的解释

**定义.** 任给一个个体变项 $x$，一个项 $t$，一个公式 $\phi$。我们将 $\phi[t/x]$定义为通过将 $\phi$中所有出现的未被约束的个体变项 $x$替换为 $t$来得到的公式。

注. 这种替换可能会产生副作用，例如如果用于替换的项中包含一个个体变项 $y$，而被替换的个体变项处于 $\forall y$的辖域中，那么替换后得到的公式中，新增的个体变项 $y$是被约束的，这会导致信息的丢失。我们应该避免该情况发生。

**定理 2.1.** 闭式在任何解释下都可以变成命题。

**定义.** 设 $A$为一个公式，若 $A$在任何解释下均为真，则称 $A$为永真式（或逻辑有效式）。若 $A$在任何解释下均为假，则称 $A$为矛盾式（或逻辑矛盾式）。若至少存在一个解释使 $A$为真，则称 $A$为可满足式。

**定义.** 设 $A_0$是含命题变项 $p_1, p_2, \cdots, p_n$的命题公式， $A_1, A_2, \cdots, A_n$是 $n$个谓词公式。用 $A_i(1 \leq i \leq n)$处处代替 $A_0$中的 $p_i$，所得公式 $A$ 称为 $A_0$的代换实例。

例. $F(x) \to G(x), \forall x F(x) \to \exists y G(y)$都是 $p \to q$ 的代换实例。

**定理 2.2.** 重言式的代换实例都是永真式，矛盾式的代换实例都是矛盾式。

注. 因为谓词最终都会变为真值。

注. 只有当涉及的谓词公式较少时，使用代换实例来判断永真式，永假式才有意义。有些时候可能公式中的一部分可以用代换逻辑来判断。

## 2.1 一阶逻辑等值式与置换规则

**定义.** 设 $A$、 $B$式一阶逻辑中任意两个公式，若 $A \leftrightarrow B$是永真式，则称 $A$与 $B$是等值的，记作 $A \Leftrightarrow B$，并称它为等值式。

命题逻辑中的等值式模式的代换实例都是一阶逻辑的等值式。同时，一阶谓词逻辑中还有一些特有的基本等值式：

1. 消去量词等值式：设个体域为 $D = \{a_1, a_2, \cdots, a_n\}$，则
   (a) $\forall x A(x) \Leftrightarrow A(a_1) \wedge A(a_2) \wedge \cdots \wedge A(a_n)$
   (b) $\exists x A(x) \Leftrightarrow A(a_1) \vee A(a_2) \vee \cdots A(a_n)$
2. 量词否定等值式：设 $A(x)$含自由出现个体变项 $x$，则

(a) $\neg\forall x A(x) \Leftrightarrow \exists x \neg A(x)$

(b) $\neg\exists x A(x) \Leftrightarrow \forall x \neg A(x)$

3. 量词辖域收缩与扩张等值式：

(a) i. $\forall x(A(x) \vee B) \Leftrightarrow \forall x A(x) \vee B$

ii. $\forall x(A(x) \wedge B) \Leftrightarrow \forall x A(x) \wedge B$

iii. $\forall x(A(x) \to B) \Leftrightarrow \exists x A(x) \to B$

iv. $\forall x(B \to A(x)) \Leftrightarrow B \to \forall x A(x)$

(b) i. $\exists x(A(x) \vee B) \Leftrightarrow \exists x A(x) \vee B$

ii. $\exists x(A(x) \wedge B) \Leftrightarrow \exists x A(x) \wedge B$

iii. $\exists x(A(x) \to B) \Leftrightarrow \forall x A(x) \to B$

iv. $\exists x(B \to A(x)) \Leftrightarrow B \to \exists x A(x)$

4. 量词分配等值式：

(a) $\forall x(A(x) \wedge B(x)) \Leftrightarrow (\forall x A(x)) \wedge (\forall x B(x))$

(b) $\exists x(A(x) \vee B(x)) \Leftrightarrow (\exists x A(x)) \vee (\exists x B(x))$

**定理 2.3.** 1. 置换规则：设 $\Phi(A)$是含公式 $A$的公式， $\Phi(B)$是用公式 $B$取代 $\Phi(A)$中所有 $A$之后所得的公式。若 $A \Leftrightarrow B$，则 $\Phi(A) \Leftrightarrow \Phi(B)$

2. 换名规则：设 $A$为一公式，将 $A$中某量词辖域中一个约束变项的所有出现及相应的指导变元，改为该量词辖域中未曾出现过的某个体变项符号，公式中其余部分不变，所得公式记为 $A'$，则 $A \Leftrightarrow A'$。

3. 代替规则：设 $A$为一公式，将 $A$中某自由出现的个体变项的所有出现用A中未曾出现过的个体变项符号代替，其余部分不变，所得公式记为 $A'$, 则 $A \Leftrightarrow A'$。

# 3 代数系统

## 3.1 集合上的运算

**定义.** 设 $S$为集合，函数 $f : S \to S$称为 $S$上的一元运算，简称为一元运算。

注. 一元运算通常将运算符作为前缀，例如 $!x$, $x$等。

**定义.** 设 $S$为集合，函数 $f : S \times S \to S$称为 $S$上的二元运算，简称为二元运算。也称 $S$对 $f$封闭。

注. 所以一个运算要为 $S$上的运算，首先要满足函数的性质，即不能“一对多”，然后要封闭。

一般用运算表来表示一个有穷集上的运算

**定义.** 设 $\circ, *$为 $S$上的两个不同的二元运算，

1. 如果 $\forall x, y \in S$有 $x \circ y = y \circ x$，则称运算在 $S$上满足交换律。
2. 如果 $\forall x, y, z \in S$有 $(x \circ y) \circ z = x \circ (y \circ z)$，则称运算在 $S$上满足结合律。
3. 如果 $\forall x \in S$有 $x \circ x = x$，则称运算在 $S$上满足幂等律。
4. 如果 $\forall x, y, z \in S$有 $(x*y)\circ z = (x\circ z)*(y\circ z); z\circ(x*y) = (z\circ x)*(z\circ y)$，则称 $\circ$运算对* 运算满足分配律。
5. 如果 $\circ$和 $*$都可交换，且 $\forall x, y \in S$有 $x \circ (x * y) = x; x * (x \circ y) = x$，则称 $\circ$和*运算满足吸收律。

**定义.** 设 $\circ$为 $S$上的二元运算，如果存在 $e_l$（或 $e_r$） $\in S$，使得对于任意 $x \in S$都有 $e_l \circ x = x$（或 $x \circ e_r = x$），则称 $e_l$（或 $e_r$）是 $S$中关于 $\circ$运算的左（或右）单位元。

如果 $e \in S$关于 $\circ$既是左单位元，又是右单位元，则称 $e$为 $S$上关于 $\circ$运算的单位元，也叫做幺元。

**定义.** 设 $\circ$为 $S$上的二元运算，如果存在 $\theta_l$（或 $\theta_r$） $\in S$，使得对任意 $x \in S$都有 $\theta_l \circ x = \theta_l$（或 $x \circ \theta_r = \theta_r$），则称 $\theta_l$（或 $\theta_r$）是 $S$中关于 $\circ$运算的左（或右）零元。

若 $\theta \in S$关于 $\circ$运算既是左零元，又是右零元，则称 $\theta$为 $S$上关于运算 $\circ$的零元。

**定义.** 令 $e$为 $S$中关于运算 $\circ$的单位元，对于 $x \in S$，如果存在 $y_l$（或 $y_r$） $\in S$使得 $y_l \circ x = e$（或 $x \circ y_r = e$），则称 $y_l$（或 $y_r$）是 $x$的左逆元（或右逆元）。

关于 $\circ$运算，若 $y \in S$既是 $x$的左逆元，又是 $x$的右逆元，则称 $y$为 $x$的逆元。

如果 $x$的逆元存在，就称 $x$是可逆的。

**定理 3.1.** 设 $\circ$为 $S$上的二元运算， $e_l$和 $e_r$分别为 $S$中关于运算的左和右单位元，则 $e_l = e_r = e$为 $S$上关于 $\circ$运算的唯一的单位元。

注. 要证明该定理，首先要证明 $e_l = e_r$，其次要证明单位元唯一。

注. 证明满足某条件的元素是唯一的方法一般是假设还有另外一个元素也满足这些性质，然后导出这两个元素是相同的。

**定理 3.2.** 设 $\circ$为 $S$上的二元运算， $\theta_l$和 $\theta_r$分别为 $S$中关于运算的左和右零元，则 $\theta_l = \theta_r = \theta$为 $S$上关于 $\circ$的唯一零元。

**定理 3.3.** 当 $|S| \geq 2$时，单位元和零元是不同的。当 $|S| = 1$时，这个唯一的元素既是单位元，又是零元。

**定理 3.4.** 设 $\circ$为 $S$上可结合的二元运算， $e$为该运算的单位元，对于 $x \in S$如果存在左逆元 $y_l$和右逆元 $y_r$，则有 $y_l = y_r = y$，且 $y$是 $x$的唯一逆元。

对于可结合的二元运算，可逆元素 $x$只有唯一的逆元，记作 $x^{-1}$。

**定义.** 设 $\circ$为 $V$上的二元运算，如果 $\forall x, y, z \in V$，有

1. 若 $x \circ y = x \circ z$，且 $x$不是零元，则 $y = z$;
2. 若 $y \circ x = z \circ x$，且 $x$不是零元，则 $y = x$.

那么称 $\circ$运算满足消去律。

由二元运算的运算表可以判断出该运算所满足的算律：

1. 交换律：运算表关于主对角线对称
2. 幂等律：主对角线元素排列与表头顺序一致
3. 消去律：行与列中没有重复元素
4. 单位元：所在的行与列的元素排列都与表头一致
5. 零元：元素的行与列都由该元素自身构成

6. 可逆元：如果运算表中 $(i,j)$元与 $(j,i)$元都是单位元，则 $i,j$行（列）的表头互为逆元

7. 结合律：要通过枚举进行验证

注. 之所以“行与列中没有重复元素”可以推出有消去律，是因为这保证了消去后等式两边的元素是同一元素，只有这样，消去前等式两边的运算结果才一致。

## 3.2 代数系统

**定义.** 非空集合 $S$和 $S$上 $k$个一元或二元运算 $f_1, f_2, \cdots, f_k$组成的系统称为一个代数兄，简称代数，记作 $V =< S, f_1, f_2, \cdots, f_k >$。

$S$称为代数系统的载体， $S$和运算叫做代数系统的成分。有的代数系统指定了 $S$中的特殊元素，称为代数常数，例如二元运算的单位元。有时也将代数常数作为系统的成分。

**定义.** 如果两个代数系统中运算的个数相同，对应运算的元数相同，且代数常数的个数也相同，则称这两个代数系统具有相同的构成成分，也称它们是同类型的代数系统。

**定义.** 设 $V =< S, f_1, f_2, \cdots, f_k >$是代数系统， $B$是 $S$的非空子集，如果 $B$对 $f_1, f_2, \cdots, f_k$都封闭，且 $B$和 $S$含有相同的代数常数，则称 $< B, f_1, f_2, \cdots, f_k >$是 $V$的子代数系统，简称子代数。有时将子代数系统简记为 $B$。

最大的子代数就是 $V$本身。如果 $V$中的所有代数常数构成集合 $B$，且满足子代数的要求，则 $B$就构成了 $V$的最小子代数。最大和最小子代数统称为 $V$的平凡子代数。若 $B$是 $S$的真子集，则 $B$构成的子代数称为 $V$的真子代数。

## 3.3 群

**定义.** 1. 设 $V =< S, \circ >$是代数系统， $\circ$为二元运算，如果 $\circ$是可结合的，则称 $V$是半群。

2. 设 $V =< S, \circ >$是半群，若 $e \in S$是关于 $\circ$运算的单位元，则称 $V$是含幺半群，也叫做独异点，有时也记作 $V =< S, \circ, e >$.

3. 设 $V =< S, \circ >$是独异点，存在单位元 $e \in S$，并且对 $S$中的任何元素 $x$都有 $x^{-1} \in S$，则称 $S$为群。

**定义.** 设半群 $V =< S, \circ >$中， $\forall x \in S$，规定：

$$x^1 = x, \quad x^{n+1} = x^n \circ x, \quad n \in \mathbb{Z}^+$$

在独异点 $< S, \circ, e >$中， $\forall x \in S$，

$$x^0 = e, \quad x^{n+1} = x^n \circ x, \quad n \in \mathbb{N}$$

幂运算满足：

$$x^n \circ x^m = x^{n+m} \quad (x^n)^m = x^{nm},$$

在半群中$m, n \in \mathbb{Z}^+$，在独异点中 $m, n \in \mathbb{N}$。

**定义.** 半群与独异点的子代数分别称为子半群与子独异点。

**定义.** 设 $V_1 =< S_1, \circ >, V_2 =< S_2, * >$是半群， $\phi : S_1 \to S_2$. 若对任意的 $x, y \in S_1$有

$$\phi(x \circ y) = \phi(x) * \phi(y)$$

则称 $\phi$为半群 $V_1$到 $V_2$的同态映射，简称同态。

**定义.** 设 $V_1 =< S_1, \circ, e_1 >, V_2 =< S_2, *, e_2 >$是奇异点， $\phi : S_1 \to S_2$. 若对任意的 $x, y \in S_1$有

$$\phi(x \circ y) = \phi(x) * \phi(y), \quad \phi(e_1) = e_2.$$

则称 $\phi$为独异点 $V_1$到 $V_2$的同态映射，简称同态。

**定义.** 1. 若群 $G$是有穷集，则称 $G$是有限群，否则称为无限群。群 $G$的基数称为群 $G$的阶，有限群 $G$的阶记作 $|G|$。

2. 平凡群即只含单位元的群。

3. 若群 $G$中的二元运算是可交换的，则称 $G$为交换群或 Abel群。

**定义.** 设 $G$是群， $x \in G, n \in \mathbb{Z}$，则 $x$的 $n$次幂 $x^n$定义为

$$x^n = \begin{cases} e, & n = 0 \\ x^{n-1} \circ x, & n > 0 \\ (x^{-1})^{-n}, & n < 0 \end{cases}$$

**定义.** 设 $G$是群，使得等式 $x^k = e$成立的最小正整数 $k$称为 $x$的阶（或周期），记作 $|x| = k$，称 $x$为 $k$阶元。若不存在这样的正整数，则称其为无限阶元。

**定理 3.5.** 设 $G$为群，则 $G$中的幂运算满足：

1. $\forall a \in G, (a^{-1})^{-1} = a.$
2. $\forall a, b \in G, (ab)^{-1} = b^{-1}a^{-1}.$
3. $\forall a \in G, a^n a^m = a^{n+m}, n, m \in \mathbb{Z}.$
4. $\forall a \in G, (a^n)^m = a^{nm}, n, m \in \mathbb{Z}.$
5. 若 $G$为交换群，才有 $(ab)^n = a^n b^n.$

**定理 3.6.** $G$为群，则 $G$中适合消去律，即对任意 $a, b, c \in G$有

1. 若 $ab = ac$,则 $b = c.$
2. 若 $ba = ca$，则 $b = c.$

**定理 3.7.** $G$为群， $a \in G$且 $|a| = r$。设 $k$是整数，则

1. $a^k = e$当且仅当 $r|k$
2. $|a^{-1}| = |a|$

## 3.4 子群

**定义.** 设 $G$是群， $H$是 $G$的非空子集，如果 $H$关于 $G$中的运算构成群，则称 $H$ 是 $G$的子群，记作 $H \leq G$。

若 $H \leq G$，且 $H \subset G$，则称 $H$是 $G$的真子群，记作 $H < G$。

G 的平凡子群有 $G$和 $\{e\}$

**定理 3.8.** 有三条子群判定定理：

1. 设 $G$为群， $\varnothing \neq H \subseteq G$.则 $H \leq G$当且仅当
   (a) $\forall a, b \in H : ab \in H$
   (b) $\forall a \in H, a^{-1} \in H$

2. 群 $G, \varnothing \neq H \subseteq G$，则 $H \leq G$当且仅当 $\forall a, b \in H : ab^{-1} \in H$.

3. 群 $G, \varnothing \neq H \subseteq G$.如果 $H$是有穷集合，则 $H \leq G$当且仅当 $\forall a, b \in H$有 $ab \in H$。

注. 在判断是否为子群时，可结合性自动满足，需要证明的是封闭性、“有幺元”和“均可逆”。事实上，“非空”、封闭、“均可逆”便能推出“有幺元”，判定定理一实际上就是这三个条件，判定定理二在此基础上进一步化简。而判定定理三则是在利用了有限群的性质进行化简。

**定义.** 设 $G$为群， $a \in G$，令 $H = \{a^k | k \in \mathbb{Z}\}$，则 $H \leq G$，称为由 $a$生成的子群，记作 $< a >$。

**定义.** 设 $G$为群，令

$$C = \{a | a \in G \wedge \forall x \in G(ax = xa)\},$$

则 $C \leq G$，称 $C$为 $G$的中心。

**定义.** 设 $G$为群，令 $S = \{H | H \leq G\}$是 $G$的所有子群的集合，定义 $S$上的偏序 $\leq$：

$$\forall x, y \in S, x \leq y \Leftrightarrow x \subseteq y,$$

那么 $< S, \leq >$构成格，称为 $G$的子群格。

### 3.5 陪集

**定义.** 设 $G$为群， $H \leq G, \forall a \in G$，令

$$Ha = \{ha | h \in H\}$$

称 $Ha$是子群 $H$在 $G$中的右陪集，简称为 $H$的右陪集，称 $a$叫做右陪集 $Ha$的代表元。

**定理 3.9.** 设 $G$为群， $H \leq G$，则

1. $H = He$

2. $\forall a \in G : a \in Ha$

**定理 3.10.** 设 $G$为群， $H \leq G$，则 $\forall a, b \in G$，有

$$a \in Hb \Leftrightarrow ab^{-1} \in H \Leftrightarrow Ha = Hb.$$

**定理 3.11.** 设 $G$是群， $H \leq G$，在 $G$上定义二元关系 $R$：

$$\forall a, b \in G, < a, b > \in R \Leftrightarrow ab^{-1} \in H.$$

则 $R$是 $G$上的等价关系，且 $[a]_R = Ha$.

**定理 3.12.** 设 $H$是群 $G$的子群，则

1. $\forall a, b \in G, Ha = Hb$或 $Ha \cap Hb = \varnothing$
2. $\bigcup\{Ha | a \in G\} = G$

即 $H$的所有右陪集的集合构成 $G$的一个划分。

**定理 3.13.** 设 $G$是群， $H \leq G$，则 $\forall a \in G, H \approx Ha$

类似地，我们可以定义左陪集。左陪集有着和右陪集一样的性质。

**定理 3.14.** 若 $H \leq G$，则 $H$的左右陪集的个数相同，记为 $[G : H]$

**定理 3.15** (拉格朗日定理)**.** 设 $G$是有限群， $H \leq G$，则 $|G| = |H| \cdot [G : H]$

**定理 3.16.** 1. 设 $G$是 $n$阶群，则 $\forall a \in G$， $|a|$是 $n$的因子，且有 $a^n = e$。

2. 对阶位素数的群 $G$，必存在 $a \in G$使得 $G =< a >$

注. 拉格朗日定理的逆命题不成立。

**定义.** 若 $\forall a \in G : Ha = aH$，则称 $H$为正规子群（或称不变子群）。

**定理 3.17.** 1. 群 $G$的平凡子群都是 $G$的正规子群。

2. 如果 $G$是 Abel 群，则所有子群都是正规子群。

3. 设 $N$是群 $G$的子群，则下列命题等价：

   (a) $N$是 $G$的正规子群

   (b) $\forall g \in G, \forall n \in N$，有 $gng^{-1} \in N$

   (c) $\forall g \in G$，有 $gNg^{-1} = N$。

## 3.6 循环群与置换群

**定义.** 设 $G$为群，若 $\exists a \in G$，使得

$$G = \{a^k | k \in \mathbb{Z}\},$$

即 $G$中的任意元素都由 $a$的幂表示，则称 $G$为循环群，并记 $< a >$。称 $a$为 $G$的生成元。

任给群 $G, a \in G$，则它的 $< a >$生成子群是循环群。

同时，素数阶群都是循环群。

设 $G =< a >$为循环群，则根据 $a$的阶可以将其分为： $n$阶循环群或无限循环群。

**定理 3.18.** 设 $G =< a >$，

1. 若 $G$是无限循环群，则 $G$只有两个生成元，即 $a$和 $a^{-1}$。
2. 若 $G$是 $n$阶循环群，则 $G$由 $\phi(n)$个生成元。对于任何小于等于 $n$且与 $n$互素的正整数 $r$， $a^r$是 $G$的生成元。

**定理 3.19.** 设 $G =< a >$是循环群，

1. $G$的子群仍是循环群。
2. 若 $G$是无限循环群，则 $G$的子群除了 $\{e\}$外，都是无限循环群。
3. 若 $G$是 $n$阶循环群，则对 $n$的每个正因子 $d$， $G$恰好含有一个 $d$阶子群。

**定义.** 设 $S = \{1, 2, \cdots, n\}$， $S$上的双射函数 $\sigma : S \to S$称为 $S$上的 $n$元置换。一般将 $n$元置换 $\sigma$记为

$$\sigma = \begin{bmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{bmatrix}$$

**定义.** 两个 $n$元置换的乘法就是函数的复合运算， $n$元置换的求逆就是求反函数。

**定义.** 设 $\sigma$是 $S = \{1, 2, \cdots, n\}$上的 $n$元置换。若

$$\sigma(i_1) = i_2, \sigma(i_2) = i_3, \cdots, \sigma(i_{k-1}) = i_k, \sigma(i_k) = i_i$$

且保持 $S$中的其他元素不变，则称 $\sigma$为 $S$上的 $k$阶轮换，记作 $(i_1, i_2, \cdots, i_k)$。若 $k = 2$，则称 $\sigma$为 $S$上的对换。

置换可以分解为轮换，轮换又可以进一步分解为对换。置换到轮换的分解如果不考虑顺序的话，则是唯一的。但轮换到对换的转换则是不唯一的，一种可行的方法是 $(i_1, i_2, \cdots, i_k) = (i_1 i_1)(i_1 i_2)\cdots(i_1 i_k)$

例.

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 6 & 4 & 2 & 1 & 8 & 7 \end{bmatrix} = (1\,5\,2\,3\,6)(7\,8) = (1\,5)(1\,2)(1\,3)(1\,6)(7\,8)$$

如果一个 $n$元置换在它的对换表达式中含有偶数个对换，则称为偶置换，否则称为奇置换。可知，奇置换和偶置换的个数都是 $n!/2$。

考虑所有的 $n$元置换构成的集合 $S_n$。 $S_n$关于置换的乘法是封闭的。且置换的乘法满足结合律。恒等置换是 $S_n$中的单位元。对于任何 $n$元置换 $\sigma \in S_n$，逆置换 $\sigma^{-1}$是 $\sigma$的逆元。

所以 $S_n$是关于置换的乘法的一个群，称为 $n$元对称群。 $n$元对称群的子群称为 $n$元置换群。

## 3.7 常用结论

设 $G$为群， $a$是 $G$的元素，则

1. 若 $|a| = 2$，则 $a = a^{-1}$
2. 若 $|a| > 2$，则 $a \neq a^{-1}$
3. $|a| = 1 \vee |a| = 2 \Leftrightarrow a = a^{-1} \Leftrightarrow a^2 = e$
4. $G$有且只有一个一阶元，也就是单位元
5. 若 $|G|$为偶数，则其中必定含有 2阶元