离散数学及其应用教学课件

《离散数学及其应用》（清华大学出版社，杨振启等编）编写组

January 31, 2018

back

序言

- **教材:**
  - 离散数学及其应用, 清华大学出版社, 杨振启等编, 2018年1月.
- **参考书:**
  - Discrete Mathematics and Its Applications Sixth Edition, (美) Kenneth H. Rosen 著.
  - 离散数学(第3版), 方世昌 编著. 西安电子科技大学出版社.

序言

- **教材:**
  - 离散数学及其应用, 清华大学出版社, 杨振启等编, 2018年1月.
- **参考书:**
  - Discrete Mathematics and Its Applications Sixth Edition, (美) Kenneth H. Rosen 著.
  - 离散数学(第3版), 方世昌 编著. 西安电子科技大学出版社.

目录

目录

1.1命题和连接词

数理逻辑研究的中心问题是推理.
推理的前提和结论都是表达判断的陈述句.
表达判断的陈述句构成了推理的基本单位.
关于什么是命题, 有下列定义.

定义 1.1

能判断真假而不是可真可假的陈述句称为**命题**.

back

1.1 命题和连接词

作为命题的陈述句所表达得到的判断结果称为命题的**真值**.
真值只取两个: 真与假.
真值为真的命题称为真命题.
真值为假的命题称为假命题.
命题通常用大写英文字母如P, Q, R等表示.

1.1 命题和连接词

例 1.1

判断下列语句是否为命题.

1. 4是素数.
2. 2025年人类将到达火星.
3. 今天是星期二.
4. $2+3=5$.
5. 这朵花真美丽啊!
6. 离散数学是计算机科学的基础课程.
7. 严禁随地吐痰!
8. 她身体好吗?
9. $x=3$.
10. 我在说谎.
11. 如果 $a>b$且$b>c$, 则$a>c$.

back

1.1 命题和连接词

解: 其中陈述句4, 6, 11所陈述的内容与事实相符, 是真命题, 简记为T 或数字1.
陈述句1是错的, 称为假命题, 简记为F 或数字0.
陈述句2是命题, 但命题真值暂时不能定, 要等到2025年才能确定. 陈述句3是命题, 真值根据具体情况而定.
语句5 是感叹句, 7 是祈使句, 8 是疑问句, 这三句都不是陈述句, 不是命题.
语句9, 10虽然都是陈述句, 但都不是命题, 其中9没有确定的真值, 10 是悖论(矛盾）.

back

1.1 命题和连接词

命题是陈述性语句, 而不能是疑问句, 祈使句, 感叹句等;
命题有明确的真或假值(有时需根据论及该命题的时间空间来确定).
判断结果不唯一确定的陈述句不是命题 ; 陈述句中的悖论不是命题.

back

1.1 命题和连接词

几个相关概念:
原子命题或简单命题: 不能分解成更简单的语句的命题.
复合命题: 多个原子命题由联结词和圆括号联结起来构成的命题. 复合命题的真假值只与原子命题的真假值有关.
命题常项或命题常元: 已知真假值的命题. 可以用字母表示, 也可以直接用T, F表示.
命题变项或命题变元: 真值可以变化的陈述句为命题变项或命题变元. 命题变项不是命题.

例如, 在例1.1中, 语句1, 2, 3, 4和6都是原子命题, 语句11 是复合命题.

1.1 命题和连接词

逻辑推理研究方法的主要特征是将论述或推理中的各种要素都符号化. 即构造各种符号语言来代替自然语言. 同时, 也将自然语言中的的联结词符号化, 并消除其消除其二义性.

在命题逻辑中有以下几个基本的联结词: $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$.

下面分别介绍.

1.1 命题和连接词

定义 1.2

非, 否定 $(\neg)$
给定命题P, 若命题R当且仅当P为假时为真, 则称R为P的否定或非P, 记为: $\neg P$. 符号$\neg$ 称作否定联结词. 其定义可用下面的表来表示:

Table 1.1: $\neg P$

P	$\neg P$
0	1
1	0

类似表1.1可用来表示命题的真假, 这种表通常称为**真值表**. 需要注意的是, 在一个命题的真值表中, 要列出其所有的可能值, 既包括真也包括假.

1.1 命题和连接词

把语言叙述的命题用符号来表示, 就是命题的符号化, 例如.

例 1.2

符号化命题“今天不下雨”.
解: 用P表示今天下雨, 则原命题为$\neg P$.

back

1.1 命题和连接词

定义 1.3

合取 $(\wedge)$
给定两个命题P, Q, 若命题R当且仅当P和Q同时为真时为真, 则称R为P与Q的合取, 记为: $P \wedge Q$. 该定义可用如下真值表表示:

Table 1.2: $P \wedge Q$

P	Q	$P \wedge Q$
0	0	0
0	1	0
1	0	0
1	1	1

back

1.1 命题和连接词

例 1.3

将下列命题符号化.

1. 张三和李四都是三好学生.
2. 王芳不仅用功而且聪明.
3. 王芳虽然聪明, 但不用功.
4. 我们去看电影并且房间里有十张桌子.

back

1.1 命题和连接词

解:

1. 设P: 张三是三好学生; Q: 李四是三好学生. 则第1个命题为 $P \wedge Q$.
2. 设P: 王芳用功; Q: 王芳聪明. 则第2个命题为$P \wedge Q$.
3. 设P: 王芳用功; Q: 王芳聪明. 则第3个命题为$Q \wedge \neg P$.
4. 设P: 我们去看电影; Q: 房间里有十张桌子. 则第4个命题为 $P \wedge Q$.

back

1.1 命题和连接词

自然语言中的“既……又……”，“不但……而且……”，“虽然……但是……”，“一面……一面……”等联结词都可以符号化为∧;.

自然语言中的,并非所有的“和”都表示“合取”.
例如,“王五和赵六是兄弟”是一个原子命题,不可以用逻辑中的∧来表示. 当命题描述对象之间的关系时不能用合取;

命题辑关心的只是构成复合命题的各原子命题之间的真值关系,并不关心各语句的具体内容.

back

1.1 命题和连接词

定义 1.4

析取 $(\vee)$

给定两个命题P和Q, 若命题R当且仅当P与Q同时为假时为假, 则称R为P和Q的析取, 记为: $P \vee Q$. 该定义可用如下真值表表示:

Table 1.3: $P \vee Q$

P	Q	$P \vee Q$
0	0	0
0	1	1
1	0	1
1	1	1

back

1.1 命题和连接词

例 1.4

将下列命题符号化.

1. 郑莉爱跳舞或爱听音乐.
2. 夏群只能挑选202或203房间.
3. 他今天做了十或二十道习题.

back

1.1 命题和连接词

解: 第1题设P: 郑莉爱跳舞; Q: 郑莉爱听音乐. 则原命题为: $P \vee Q$. P和Q允许同时为真, 是一种相容或.
第2题设P: 夏群挑选202房间; Q: 夏群挑选203房间. 因为夏群只能挑选其中的一个房间, 这里的“ 或”表达的是排斥或, 所以原命题不能表示为: $P \vee Q$, 应表示为: $(P \wedge \neg Q) \vee (\neg P \wedge Q)$也就是$(P \vee Q) \wedge \neg(P \wedge Q)$.
第3题这句是原子命题, 因为“ 或” 只表示了习题的近似数目. 用P 表示.

1.1 命题和连接词

自然语言中的“或”具有二义性, 用它联结的命题有时具有相容性, 有时具有排斥性, 对应的联结词分别称为相容或和排斥或, 相容或就是前面介绍的析取, 排斥或后面再作介绍.

back

1.1 命题和连接词

定义 1.5

蕴涵 $(\rightarrow)$
给定两个命题P和Q, 复合命题“如果P, 则Q” 称作P与Q的蕴涵式, 记作$P \rightarrow Q$, 并称P是蕴涵式的前件, Q为蕴涵式的后件, $\rightarrow$ 称作蕴涵联结词. 规定$P \rightarrow Q$ 为假当且仅当P为真Q假时. 该定义可用如下真值表表示:

Table 1.4: $P \rightarrow Q$

P	Q	$P \rightarrow Q$
0	0	1
0	1	1
1	0	0
1	1	1

1.1 命题和连接词

按照定义, $P \to Q$的逻辑关系表示“如果P, 则Q”. 该逻辑关系还有下面的这些说法:

Q 是P 的必要条件.

P 是Q 的充分条件.

只要P 就Q.

因为P 所以Q.

P仅当Q.

只有Q 才P.

除非Q才P.

back

1.1 命题和连接词

例 1.5

将下列命题符号化, 并求出其真值.

1. 如果2加3等于5, 则天是蓝的.
2. 2加3等于5仅当天是蓝的.
3. 除非天是蓝的, 2加3才等于5.
4. 只有天是蓝的, 2加3才等于5.
5. 只要2加3不等于5, 则天是蓝的.
6. 如果我有车, 那么我去接你 .

back

1.1 命题和连接词

解: 设P: 2加3等于5, Q: 天是蓝的. 命题1到4反映的都是同一个逻辑关系, 可符号化均为$P \to Q$.
第5题的命题符号化为$\neg P \to Q$.
对于第6题, 设P: 我有车, Q: 我去接你. 原命题命题符号化为$P \to Q$, 真值依具体情况而定.

back

1.1 命题和连接词

定义 1.6

等价 $(\leftrightarrow)$

给定两个命题P, Q, 复合命题“P当且仅当Q” 称作P与Q的等价式, 记作$P \leftrightarrow Q$, $\leftrightarrow$称作等价联结词, 并规定$P \leftrightarrow Q$为真当且仅当P与Q的值相同. 该定义可用如下真值表表示:

Table 1.5: $P \leftrightarrow Q$

P	Q	$P \leftrightarrow Q$
0	0	1
0	1	0
1	0	0
1	1	1

back

1.1 命题和连接词

例 1.6

将下列命题符号化, 并求出其真值.

1. π是无理数当且仅当加拿大位于亚洲.
2. 2加3等于5的充要条件是π是无理数.
3. 若两圆A, B的面积相等, 则它们的半径相等; 反之亦然.
4. 当王小红心情愉快时, 就唱歌; 反之, 她唱歌时, 一定心情愉快.

back

1.1 命题和连接词

解: 第1题, 设P: π是无理数, Q: 加拿大位于亚洲, 符号化为$P \leftrightarrow Q$.
第2题, 设P: 2加3等于5, Q: π是无理数. 命题符号化为$P \leftrightarrow Q$.
第3题, 设P: 两圆A, B的面积相等, Q: 两圆A, B的半径相等. 命题符号化为$P \leftrightarrow Q$.
第4题, 设P: 王小红心情愉快, Q: 王小红唱歌. 命题符号化为$P \leftrightarrow Q$.

back

1.1 命题和连接词

$P \leftrightarrow Q$ 的逻辑关系为P与Q 互为充分必要条件;
$(P \to Q) \wedge (Q \to P)$ 与$P \leftrightarrow Q$ 的逻辑关系完全一致.

back

1.1 命题和连接词

以上介绍的5种连接词是命题逻辑中最常用, 最重要的连接词, 它们组成的集合是

$$\{\neg \ \wedge \ \vee \ , \rightarrow \ , \leftrightarrow\}$$

其中$\neg$为一元联接词, 其余的为二元联接词. 可多次使用集中的联结词, 组成更为复杂的复合命题.
求复合命题的真值时, 需要先明确联接词的优先级. 若将公式中的括号也算在内, 规定的联结词优先顺序为:

$$(), \neg, \wedge, \vee, \rightarrow, \leftrightarrow$$

对于同一优先级的联结词, 先出现者先运算.

1.2重言式

将已有的命题用命题连接词和括号可以构造复合命题. 复合命题也称为**命题表达式**或**命题公式**或**合式公式**.

命题表达式形成时, 必须遵守一定的规则, 下面就来介绍这些规则.

1.2重言式

定义 1.7

合式公式

(1) 单个命题常项和变项是合式公式, 并称为原子命题公式.
(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) 有限次地应用(1)～(3)形式的符号串得到的式子才是合式公式.

back

1.2重言式

合式公式的定义是递归的. (1)是递归的基础, 由(1)开始, 使用(2), (3)规则, 可以得到任意的合式公式; 定义中A, B代表任意的命题公式, $(\neg A)$, $(A \wedge B)$等公式单独出现时, 外层括号可以省去, 写成$\neg A$, $A \wedge B$. 另外, 公式中不影响运算次序的括号也可以省去, 如公式$(P \vee Q) \vee (\neg R)$可以写成$P \vee Q \vee \neg R$.

按照定义:
$(P \to Q) \wedge (Q \leftrightarrow R)$, $(P \wedge Q) \wedge \neg R$, $P \wedge (Q \wedge \neg R)$是合式公式.
$PQ \leftrightarrow R$, $(P \to Q) \to (\wedge Q)$ 不是合式公式.

back

1.2重言式

真值表的构造

一个含有命题变项的命题公式, 其值是不确定的, 只有对它的每个命题变项用指定的命题常项代替后, 该命题公式的值才能确定.

给定命题公式A, 对A中出现的每个命题变项都指定一个具体的值1或者0, 这些1和0每一个具体的组合方式叫做公式A的一种 **指派**或者说一个**解释**.

若给定的一个指派值使A为1, 则称这组值为A的**成真赋值**; 若使A为0, 则称这组值为A的**成假赋值**.

back

1.2重言式

例 1.7

设公式A为$(\neg P \vee Q) \rightarrow R$，若将$P$，$Q$和$R$的值都取0，则组合$(0,0,0)$是公式$A$的一个解释，在这种解释下，$A$的真值为假，$(0,0,0)$称为$A$的成假赋值. 公式$A$的其它7种解释分别是$(0,0,1)$，$(0,1,0)$，$(0,1,1)$，$(1,0,0)$，$(1,0,1)$，$(1,1,0)$，$(1,1,1)$，也不难计算出$A$在这7种解释下的值.

容易看出，含$n(n \geq 1)$个命题变项的公式共有2^n个不同的解释或指派.

1.2重言式

将A的所有可能的指派以及在每一个指派下的取值列成一个表,就得到命题公式A的**真值表**.
真值表以表的形式可以更好的反应命题公式的真值情况.
由于对每个命题变项可以有两个值T和F被指派, 所以有n个命题变项的命题公式$A(P_1, P_2, \cdots, P_n)$的真值表有2^n 行. 为有序地列出$A(P_1, P_2, \cdots, P_n)$的真值表, 可将F看成0, T看成1, 按二进制数次序列表.

back

1.2重言式

构造真值表的具体步骤如下:
(1) 对公式中的所有命题变项按英文字母字典序进行排列, 如A, B, C, $\cdots$; 对带有下标的命题变元, 则按下标由小到大的数序排列, 如P_1, P_2, $\cdots$
(2) 对公式所有解释, 以二进制从小到大(或从大到小)的顺序列出.
(3) 对每一种解释, 按照公式中出现连接词的优先级逐步求得公式的值.

1.2重言式

例 1.8

求下列公式的真值表, 并求成真赋值和成假赋值.

1. $\neg(P \to Q) \wedge Q$
2. $(Q \to P) \wedge Q \to P$
3. $(\neg P \vee Q) \to R$

back

1.2重言式

解: 公式1的真值表见表1.6. 公式1的赋值都是成假赋值, 没有成真赋值. 公式2的真值表见表1.7, 公式2的赋值都是成真赋值, 没有成假赋值. 公式3的真值见表1.8, 公式3的成假赋值是000, 010, 110, 其余的均是成真赋值.

Table 1.6: $\neg(P \to Q) \wedge Q$的真值表

P	Q	$P \to Q$	$\neg(P \to Q)$	$\neg(P \to Q) \wedge Q$
0	0	1	0	0
0	1	1	0	0
1	0	0	1	0
1	1	1	0	0

back

1.2重言式

Table 1.7: $(Q \to P) \wedge Q \to P$ 的真值表

P	Q	$Q \to P$	$(Q \to P) \wedge Q$	$(Q \to P) \wedge Q \to P$
0	0	1	0	1
0	1	0	0	1
1	0	1	0	1
1	1	1	1	1

back

1.2重言式

Table 1.8: $(\neg P \vee Q) \rightarrow R$ 的真值表

P	Q	R	$\neg P$	$\neg P \vee Q$	$(\neg P \vee Q) \rightarrow R$
0	0	0	1	1	0
0	0	1	1	1	1
0	1	0	1	1	0
0	1	1	1	1	1
1	0	0	0	0	1
1	0	1	0	0	1
1	1	0	0	1	0
1	1	1	0	1	1

back

1.2重言式

前面曾通过简单的例子理解了什么叫命题的符号化. 这里再作一些说明和符号化时应注意的一些问题.

定义 1.8

命题符号化

把一个用自然语言叙述的命题相应地写成由命题变项, 联结词和圆括号表示的命题公式, 称为命题的符号化.

符号化时应注意: 确定给定句子是否为命题; 自然语言中的联结词是否为命题连接词; 要正确地表示原子命题和适当选择命题联结词.

back

1.2重言式

例 1.9

将下列命题符号化.

1. 我和他既是兄弟又是同学 .
2. 张三或李四都可以做这件事.
3. 仅当我有时间且天不下雨, 我将去镇上.
4. 张刚总是在图书馆看书, 除非图书馆不开门或张刚生病.
5. 风雨无阻, 我去上学.

解: (1) 设P: 我和他是兄弟, Q: 我和他是同学.
则命题可符号化为: $P \wedge Q$.
(2) 设P: 张三可以做这件事, Q: 李四可以做这件事.
则命题可符号化为: $P \vee Q$.
(3)对于“仅当”, 实质上是“当”的逆命题. “当A, 则B”是$A \to B$, 而“仅当A, 则B”是$B \to A$. 设P: 我有时间, Q: 天不下雨, R: 我将去镇上.
则命题可符号化为: $R \to (P \wedge Q)$.

back

1.2重言式

(4)对于“除非”, 要记住, “除非” 是条件. 设P: 张刚在图书馆看书, Q: 图书馆不开门, R: 张刚生病.
故命题可符号化为: $\neg(Q \vee R) \rightarrow P$.
(5)可理解为“不管是否刮风, 是否下雨, 我都去上学” .
设P:天刮风, Q:天下雨, R: 我去上学.
则命题可符号化为: $(P \wedge Q \rightarrow R) \wedge (P \wedge \neg Q \rightarrow R) \wedge (\neg P \wedge Q \rightarrow R) \wedge (\neg P \wedge \neg Q \rightarrow R)$ 或$(P \wedge Q \wedge R) \vee (P \wedge \neg Q \wedge R) \vee (\neg P \wedge Q \wedge R) \vee (\neg P \wedge \neg Q \wedge R)$

back

1.2重言式

逻辑关系比较复杂的命题符号化时, 要准确确定原子命题, 先将其形式化; 选用恰当的联结词; 涉及到的否定词的位置要准确; 必需要的括号不能省略; 即使可以省略的括号, 若需要提高公式可读性时最好也不要省略; 另外还要注意命题的形式化未必是唯一的.

back

1.2重言式

通过构造命题公式的真值表, 我们发现公式在各种赋值下会有不同的取值情况, 一些形式不同的公式确有着相同的真值表, 为此需要进一步研究公式的分类及不同公式的联系特征及性质等内容.

定义 1.9

设A为任一命题公式
(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**.

back

1.2重言式

从定义可以看出以下几点:

1. 重言式是可满足式, 可满足式不一定是重言式.
2. 矛盾式是不可满足式, 非矛盾式是可满足式.
3. 若真值表最后一列全为1, 则公式为重言式.
4. 若真值表最后一列全为0, 则公式为矛盾式.
5. 若真值表最后一列中至少有一个1, 则公式为可满足式.

back

1.2重言式

n个命题变项共产生2^n个不同赋值; 含n个命题变项的公式的真值表有2^{2^n}种不同情况.

从例1.8可以看出:
表1.6中的公式$\neg(P \to Q) \wedge Q$ 为矛盾式;
表1.7中的公式$(Q \to P) \wedge Q \to P$ 为重言式;
表1.8中的公式$(\neg P \vee Q) \to R$ 为非重言式的可满足式.

back

1.2重言式

重言式具有以下重要性质:

定理 1.1

若A是重言式, 则$\neg A$是矛盾式.

证明: 由重言式和矛盾式的定义可知, 二者的真值互为否定.

back

1.2重言式

定理 1.2

两个重言式的合取或析取, 仍然是一个重言式.

证明: 设A和B为两个重言式. 不论A和B的命题变项指派任何真值, 总有A的真值为T, B的真值为T, 故$A \wedge B$, $A \vee B$的真值均为T.

定理 1.3

对重言式同一分量出现的每一个位置用任何合式公式置换后, 所得公式仍为重言式.

证明: 由于重言式的真值与分量的指派无关, 故对同一分量以任何合式公式置换后, 重言式的真值仍为真.

back

1.2重言式

矛盾式也有类似性质;
两重言式的合取式, 析取式, 蕴涵式和等价式等都仍是重言式.

back

1.2重言式

逻辑等价

抽象地看, 两个公式的真假取值完全相同时可认为表达的逻辑关系相同, 代表相同的命题, 也称这两个公式逻辑等价. 下面是具体定义

定义 1.10

给定两个命题公式A和B, 设P_1, P_2, $\cdots$, P_n为所有出现于A和B中的命题变元, 若对P_1, P_2, $\cdots$, P_n的任一组指派, A和B的值都相同, 则称A和B是等价的或逻辑等价. 记作

$$A \Leftrightarrow B$$

back

1.2重言式

需要注意的是“$\Leftrightarrow$”不是逻辑联接词, 因而“$A \Leftrightarrow B$”不是命题公式, 只是表示两个命题公式之间的一种等价关系, 即若$A \Leftrightarrow B$, A和B没有本质上的区别, 最多只是A和B的形式不同而已.

“$\Leftrightarrow$” 具有如下的性质:

(1) 自反性: $A \Leftrightarrow A$; (2) 对称性: 若$A \Leftrightarrow B$, 则$B \Leftrightarrow A$; (3) 传递性: 若$A \Leftrightarrow B$, $B \Leftrightarrow C$, 则$A \Leftrightarrow C$.

n个命题变项, 可以形成许多个形式各异的公式, 这其中有许多形式不同, 真值表却相同的公式. 引入公式等价的概念, 其目的就是将复杂的公式简化.

利用真值表可以判断任何两个公式等价.

back

1.2重言式

例 1.10

证明: $P \leftrightarrow Q \Leftrightarrow (P \rightarrow Q) \wedge (Q \rightarrow P)$
证明: 从下面的表格可知公式$P \leftrightarrow Q$与公式$(P \rightarrow Q) \wedge (Q \rightarrow P)$等价.

Table 1.9: $P \leftrightarrow Q$与$(P \leftrightarrow Q) \wedge (Q \leftrightarrow P)$ 的真值表

P	Q	$P \rightarrow Q$	$Q \rightarrow P$	$(P \rightarrow Q) \wedge (Q \rightarrow P)$	$P \leftrightarrow Q$
0	0	1	1	1	1
0	1	1	0	0	0
1	0	0	1	0	0
1	1	1	1	1	1

back

1.2重言式

例 1.11

见课本.

在用真值表法判断$A \leftrightarrow B$是否为重言式时, 真值表的最后一列可以省略.

判断两个命题公式是否等价主要有三种方法:

(1) **真值表法**. 用真值表法可以判断两个命题公式是否等值(当命题变项较多时, 此方法工作量较大).

(2) **等价式法**. 利用基本的等价式进行复杂公式等价证明法.

(3) 下节介绍的**范式法**.

下面来学习基本的等价公式.

back

1.2重言式

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. 结合律: $(A \vee B) \vee C \Leftrightarrow A \vee (B \vee C)$
   $(A \wedge B) \wedge C \Leftrightarrow A \wedge (B \wedge C)$
5. 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)
6. 德·摩根律: $\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B, \quad \neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$
7. 吸收律: $A \vee (A \wedge B) \Leftrightarrow A, A \wedge (A \vee B) \Leftrightarrow A$

back

1.2重言式

8. 零律 $A \vee 1 \Leftrightarrow 1, A \wedge 0 \Leftrightarrow 0$
9. 同一律 $A \vee 0 \Leftrightarrow A, A \wedge 1 \Leftrightarrow A$
10. 排中律 $A \vee \neg A \Leftrightarrow 1$
11. 矛盾律 $A \wedge \neg A \Leftrightarrow 0$
12. 蕴涵等值式 $A \rightarrow B \Leftrightarrow \neg A \vee B$
13. 等价等值式 $A \leftrightarrow B \Leftrightarrow (A \rightarrow B) \wedge (B \rightarrow A)$
14. 假言易位 $A \rightarrow B \Leftrightarrow \neg B \rightarrow \neg A$
15. 等价否定等值式 $A \leftrightarrow B \Leftrightarrow \neg A \leftrightarrow \neg B$
16. 归谬论 $(A \rightarrow B) \wedge (A \rightarrow \neg B) \Leftrightarrow \neg A$

back

1.2重言式

上述16组基本等价公式包含的等值式中, 其中的A, B, C可以代表任意的公式.
基本等价公式有很多用途, 如化简命题公式, 判断命题公式的类型, 证明等价公式, 计算命题公式的范式, 命题逻辑中的推理等等. 以后会逐一遇到这些内容.

1.2重言式

代入规则与替换规则

定理 1.4

在一个永真式A中，任何一个命题变项R出现的每一处用另一个公式代入，所得的公式B仍为永真式.

back

1.2重言式

每个等值式都可以给出无穷多个同类型的具体的等值式.
利用此方法, 可以推出一些新的等值式.

例如, 对于蕴涵等值式 $A \to B \Leftrightarrow \neg A \vee B$:
取$A = P, B = Q$, 得等值式 $P \to Q \Leftrightarrow \neg P \vee Q$.
取$A = P \vee Q \vee R, B = P \wedge Q$时,
得等值式$(P \vee Q \vee R) \to (P \wedge Q) \Leftrightarrow \neg(P \vee Q \vee R) \vee (P \wedge Q)$.

back

1.2重言式

定理 1.5

设X是合式公式A的子公式, 若$X \Leftrightarrow Y$, 如果将A 中的X 用Y来置换, 所得到公式B与公式A等价, 即$A \Leftrightarrow B$.

证明: 这是显然的. 因为$X \Leftrightarrow Y$, 所以在相同变元的任一种指派下, X 与Y 真值相同. 以Y取代X后, 公式B 与公式A 在相应的指派情况下, 其真值必相同, 故$A \Leftrightarrow B$.

back

1.2重言式

有了上述的等价公式及代入规则和替换规则后, 就可以推演出更多的等价公式. 由已知等价公式推出另外一些等价公式的过程称为**等值演算**. 利用等值演算可以验证两个命题公式等值, 也可以判别命题公式的类型, 还可以用来解决许多实际问题. 下面举一些等值演算的例子.

back

1.2重言式

例 1.12

证明两个公式等值
$(P \to Q) \to R \Leftrightarrow (P \vee R) \wedge (\neg Q \vee R)$

解: $(P \to Q) \to R$
$\Leftrightarrow (\neg P \vee Q) \to R$ (蕴含等值式, 置换规则)
$\Leftrightarrow \neg(\neg P \vee Q) \vee R$ (蕴含等值式, 置换规则)
$\Leftrightarrow (P \wedge \neg Q) \vee R$ (德·摩根律, 置换规则)
$\Leftrightarrow (P \vee R) \wedge (\neg Q \vee R)$ (分配律, 置换规则)
从左边公式可以进行等值演算, 也可以从右边公式开始演算. 等值演算中因为每一步都用到置换规则, 故可以不用写出. 等值演算熟练后, 基本等值式也可以不用写出. 通常不用等值演算直接证明两个公式不等值.

1.2重言式

例 1.13

证明两个公式等值
$(P \vee Q) \rightarrow (P \wedge Q) \Leftrightarrow P$

解: $(P \vee Q) \rightarrow (P \wedge Q)$

$\Leftrightarrow (P \vee Q) \vee (P \wedge Q)$ (德·摩根律)

$\Leftrightarrow (P \wedge Q) \vee (P \wedge Q)$ (德·摩根律)

$\Leftrightarrow (P \wedge Q) \vee (P \wedge Q)$ (双重否定律)

$\Leftrightarrow P \wedge (Q \vee Q)$ (分配律)

$\Leftrightarrow P \wedge \mathsf{T}$ (排中律)

$\Leftrightarrow P$ (同一律)

back

1.2重言式

例 1.14

化简公式
$\neg(P \wedge Q) \rightarrow (\neg P \vee (\neg P \vee Q))$

解: $\neg(P \wedge Q) \rightarrow (\neg P \vee (\neg P \vee Q))$

$\Leftrightarrow \neg\neg(P \wedge Q) \vee ((\neg P \vee \neg P) \vee Q)$ (德·摩根律,结合律)

$\Leftrightarrow (P \wedge Q) \vee (\neg P \vee Q)$ (双重否定律, 幂等律)

$\Leftrightarrow (P \wedge Q) \vee (Q \vee \neg P)$ (交换律)

$\Leftrightarrow ((P \wedge Q) \vee Q) \vee \neg P$ (结合律)

$\Leftrightarrow Q \vee \neg P$ (吸收律)

back

1.2重言式

例 1.15

用等值演算判断下列公式的类型
(1). $Q \wedge \neg(P \rightarrow Q)$
(2). $(P \rightarrow Q) \leftrightarrow (\neg Q \rightarrow \neg P)$
(3). $((P \wedge Q) \vee (P \wedge \neg Q)) \wedge R$

解: (1) $Q \wedge \neg(P \rightarrow Q)$
$\Leftrightarrow Q \wedge \neg(\neg P \vee Q)$ (蕴涵等值式)
$\Leftrightarrow Q \wedge (P \wedge \neg Q)$ (德·摩根律)
$\Leftrightarrow P \wedge (Q \wedge \neg Q)$ (交换律, 结合律)
$\Leftrightarrow P \wedge 0$ (矛盾律)
$\Leftrightarrow 0$ (零律)
由最后一步可知, 该式为矛盾式.

1.2重言式

(2) $(P \to Q) \leftrightarrow (\neg Q \to \neg P)$

$\Leftrightarrow (\neg P \vee Q) \leftrightarrow (Q \vee \neg P)$ (蕴涵等值式)

$\Leftrightarrow (\neg P \vee Q) \leftrightarrow (\neg P \vee Q)$ (交换律)

$\Leftrightarrow 1$

由最后一步可知, 该式为重言式.

(3) $((P \wedge Q) \vee (P \wedge \neg Q)) \wedge R$

$\Leftrightarrow (P \wedge (Q \vee \neg Q)) \wedge R$ (分配律)

$\Leftrightarrow P \wedge 1 \wedge R$ (排中律)

$\Leftrightarrow P \wedge R$ (同一律)

这不是矛盾式, 也不是重言式, 而是非重言式的可 满足式.

如101是它的成真赋值, 000是它的成假赋值.

back

1.2重言式

例 1.16

某件事情是甲, 乙, 丙和丁4人中某一个人做的. 询问4人后回答如下: (1) 甲说是丙做的; (2) 乙说我没做; (3) 丙说甲讲的不符合事实; (4) 丁说是甲做的. 若其中3人说的是真话, 一人说假话, 问是谁做的?

解: 设: A: 这件事是甲做的. B: 这件事是乙做的. C: 这件事是丙做的. D: 这件事是丁做的.
4个人所说的命题分别用P, Q, R, S表示, 则(1), (2), (3), (4)分别符号化为:

back

1.2重言式

$P \Leftrightarrow \neg A \wedge \neg B \wedge C \wedge \neg D$;
$Q \Leftrightarrow \neg B$;
$R \Leftrightarrow \neg C$;
$S \Leftrightarrow A \wedge \neg B \wedge \neg C \wedge \neg D$;
那么3人说真话, 一人说假话的命题K符号化为:
$K \Leftrightarrow (\neg P \wedge Q \wedge R \wedge S) \vee (P \wedge \neg Q \wedge R \wedge S) \vee (P \wedge Q \wedge \neg R \wedge S) \vee (P \wedge Q \wedge R \wedge \neg S)$

1.2重言式

因为K表达式的第1项:

$$\neg P \wedge Q \wedge R \wedge S \Leftrightarrow (A \vee B \vee \neg C \vee D) \wedge \neg B \wedge \neg C \wedge A \wedge \neg D$$

$$\Leftrightarrow (A \wedge \neg B \wedge \neg C \wedge \neg D) \vee (B \wedge \neg B \wedge \neg C \wedge A \wedge \neg D) \vee (\neg C \wedge \neg B \wedge \neg C \wedge A \wedge \neg D) \vee (D \wedge \neg B \wedge \neg C \wedge A \wedge \neg D)$$

$$\Leftrightarrow A \wedge \neg B \wedge \neg C \wedge \neg D$$

K表达式的其它3项:

$$P \wedge \neg Q \wedge R \wedge S \Leftrightarrow P \wedge Q \wedge \neg R \wedge S \Leftrightarrow P \wedge Q \wedge R \wedge \neg S \Leftrightarrow 0$$

所以, 当K为真时, $A \wedge \neg B \wedge \neg C \wedge \neg D$ 为真, 推出这件事是甲做的.

back

1.2重言式

对偶原理 从前面列出的等价公式看出, 有很多是成对出现的. 这就是等价公式的对偶性.

back

1.2重言式

定义 1.11

对偶式 在一个只含有联结词$\neg$, $\vee$, $\wedge$的公式A中, 将$\vee$ 换成$\wedge$, $\wedge$换成$\vee$, T换成F, F换成T, 其余部分不变, 得到另一个公式A^*, 称A^*为A的对偶式.

按照定义, 对偶式是相互的.

从定义不难看出, $(A^*)^*=A$.

back

1.2重言式

例如, 下面的每一对公式分别互为对偶式.
$Q \wedge R$ 与$Q \vee R$;
$(P \vee Q) \wedge R$ 与$(P \wedge Q) \vee R$;
$(P \vee Q) \vee 0$ 与 $(P \wedge Q) \wedge 1$

一个仅含有逻辑连接词$\neg$, $\vee$, $\wedge$的命题公式和它的对偶式之间具有如下等值关系:

1.2重言式

定理 1.6

设A和A^*互为对偶式, $P_1, P_2, \cdots, P_n$, 是出现在A和A^*中的命题变项, 则

(1) $\neg A(P_1, P_2, \cdots, P_n) \Leftrightarrow A^*(\neg P_1, \neg P_2, \cdots, \neg P_n)$;

(2) $A(\neg P_1, \neg P_2, \cdots, \neg P_n) \Leftrightarrow \neg A*(P_1, P_2, \cdots, P_n)$.

证明: 由德·摩根律

$P \wedge Q \Leftrightarrow \neg(\neg P \vee \neg Q), P \vee Q \Leftrightarrow \neg(\neg P \wedge \neg Q)$

故 $\neg A(P_1, P_2, \cdots, P_n) \Leftrightarrow A^*(\neg P_1, \neg P_2, \cdots, \neg P_n)$

同理 $A(\neg P_1, \neg P_2, \cdots, \neg P_n) \Leftrightarrow \neg A^*(P_1, P_2, \cdots, P_n)$

back

1.2重言式

定理 1.7

设A, B为两个命题公式, 若$A \Leftrightarrow B$, 则$A^* \Leftrightarrow B^*$.

证明: 设$P_1, P_2, \cdots, P_n$是出现在命题公式A, B中所有的命题变项, 因为$A \Leftrightarrow B$, 即 $A(P_1, P_2, \cdots, P_n) \Leftrightarrow B(P_1, P_2, \cdots, P_n)$,
所以有$\neg A(P_1, P_2, \cdots, P_n) \Leftrightarrow \neg B(P_1, P_2, \cdots, P_n)$,
由定理1.6得, $A^*(\neg P_1, \neg P_2, \cdots, \neg P_n) \Leftrightarrow B^*(\neg P_1, \neg P_2, \cdots, \neg P_n)$.
即$A^*(\neg P_1, \neg P_2, \cdots, \neg P_n) \leftrightarrow B^*(\neg P_1, \neg P_2, \cdots, \neg P_n)$为重言式,
故$A^*(P_1, P_2, \cdots, P_n) \leftrightarrow B^*(P_1, P_2, \cdots, P_n)$ 也为重言式.
故$A^* \Leftrightarrow B^*$.
这个定理也称为**对偶原理**.

back

1.2重言式

由对偶原理可知, 若A为重言式, 则A^*必为矛盾式. 这是因为1与0互为对偶式, 若A为重言式, 则$A \Leftrightarrow 1$, 因而A的对偶式A^*应与1的对偶式0等值, 即$A^* \Leftrightarrow 0$.

已知$A \Leftrightarrow B$, 且B是比A简单的命题公式, 则由对偶原理可直接求出较简单的B^*与A^*等值. 例如

$$(P \wedge Q) \vee (\neg P \vee (\neg P \vee Q)) \Leftrightarrow \neg P \vee Q,$$

则

$$(P \vee Q) \wedge (\neg P \wedge (\neg P \wedge Q)) \Leftrightarrow \neg P \wedge Q.$$

back

1.3公式中的范式

一个公式可以具有多种相互等价的表达方式, 例如:
$P \leftrightarrow Q \Leftrightarrow (P \rightarrow Q) \wedge (Q \rightarrow P) \Leftrightarrow (P \wedge Q) \vee (\neg P \wedge \neg Q)$.
为了减少同一公式的不同表达形式对解决推理问题所带来的麻烦, 需要将公式标准化.
已知使用真值表, 公式推导和对偶原理可判断两个公式是否等价. 除此之外, 还可以通过比较公式的标准形式的方法来判断公式的等价性, 公式的标准形式即也就是规范的表达方式简称为范式.

下面开始讨论范式有关的问题.

back

1.3公式中的范式

从基本定义开始.

定义 1.12

命题变项及其否定统称作**文字**.

如P, $\neg Q$等均为文字.

定义 1.13

由有限个文字构成的析取式称作**简单析取式**.
由有限个文字构成的析取式称作**简单合取式**.

例如, $P \vee Q$, $\neg P \vee Q$, $\neg P \vee \neg Q$, $\neg P \vee Q \vee \neg Q$ 均是简单析取式.
$P \wedge Q$, $\neg P \wedge Q$, $\neg P \wedge \neg Q$, $\neg P \wedge Q \wedge \neg Q$均是简单合取式.
P, Q, $\neg P$, $\neg Q$既是简单合取式, 也是简单析取式. 也就是说文字既是简单析取式, 又是简单合取式.

1.3公式中的范式

从定义中可以看出两点:
(1) 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形式.
(2) 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形式.
例如, 简单析取式$P \vee \neg P \vee Q$是重言式. 简单合取式$P \wedge \neg P \wedge Q$是矛盾式.

定义 1.14

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**.

析取范式与合取范式统称为范式.

1.3公式中的范式

例如, $(P \wedge Q) \vee (\neg P \wedge \neg Q)$, $(\neg P \wedge Q) \vee \neg R$, $P \wedge Q$, $\neg Q$ 均是析取范式.

$(\neg P \vee Q) \wedge (P \vee \neg Q)$, $(P \vee Q) \wedge (\neg P \vee R) \wedge \neg R$, $P \wedge Q$, $\neg Q$ 均是合取范式.

注意, $\neg P \wedge Q \wedge R$的公式可以看作一个简单合取式构成的析取范式, 也可以看作三个简单析取式构成的合取范式.

相似地, $P \vee \neg Q \vee R$的公式可以看作三个简单合取式的析取范式, 又是含一个简单析取式的合取范式.

析取范式与合取范式有下列性质:

(1) 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.

(2) 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.

1.3公式中的范式

下面的结论表明: 对于任何命题公式, 都能求出与之等值的析取范式与合取范式, 这就是所谓的**范式存在定理**.

定理 1.8

任一命题公式都存在着与之等值的析取范式与合取范式.

证明: 若在公式中出现$\rightarrow$与$\leftrightarrow$连接词, 可使用等值式消除:

$A \rightarrow B \Leftrightarrow \neg A \vee B$;

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

命题公式中若出现形如$\neg\neg A$,$\neg(A \wedge B)$, $\neg(A \vee B)$ 的公式, 可将否定号消去或内移:

$\neg\neg A \leftrightarrow A$;

$\neg(A \wedge B) \leftrightarrow \neg A \vee \neg B$;

$\neg(A \vee B) \leftrightarrow \neg A \wedge \neg B$;

1.3公式中的范式

求析取公式时, 对命题公式中出现的形如$A\wedge(B\vee C)$的公式, 可以利用“$\wedge$”对“$\vee$”的分配率:

$$A\wedge(B\vee C)\Leftrightarrow(A\wedge B)\vee(A\wedge C)$$

求合取范式时, 对命题公式中出现的形$A\vee(B\wedge C)$的公式, 可以利用“$\vee$”对“$\wedge$”的分配率:

$$A\vee(B\wedge C)\Leftrightarrow(A\vee B)\wedge(A\vee C)$$

每一个命题公式A, 经过以上步骤, 即得到一个与之等值的析取范式或合取范式.

要注意公式的范式存在, 但不是惟一的.

back

1.3公式中的范式

上述分析不但给出了命题公式范式存在性的证明, 也给出了求其范式的具体步骤, 即

(1) 将公式中的联结词化归成只有$\neg$,$\wedge$及$\vee$;
(2) 利用双重否定率和德摩根定律将否定号消去或内移;
(3) 利用分配律, 结合律将公式归纳为合取范式或析取范式.

下面是例子.

1.3公式中的范式

例 1.17

求下面公式的合取范式与析取范式: $(P \to Q) \leftrightarrow R$

1) 求合取范式

解:

$(P \to Q) \leftrightarrow R$

$\Leftrightarrow (\neg P \vee Q) \leftrightarrow R$ (消去$\to$)

$\Leftrightarrow ((\neg P \vee Q) \to R) \wedge (R \to (\neg P \vee Q))$ (消去$\leftrightarrow$)

$\Leftrightarrow (\neg(\neg P \vee Q) \vee R) \wedge (\neg R \vee \neg P \vee Q)$ (消去$\to$)

$\Leftrightarrow ((P \wedge \neg Q) \vee R) \wedge (\neg P \vee Q \vee \neg R)$ (否定号内移)

$\Leftrightarrow (P \vee R) \wedge (\neg Q \vee R) \wedge (\neg P \vee Q \vee \neg R)$ ($\vee$ 对$\wedge$分配律)

back

1.3公式中的范式

2) 求析取范式

解:

$(P \to Q) \leftrightarrow R$

$\Leftrightarrow (\neg P \vee Q) \leftrightarrow R$ (消去$\to$)

$\Leftrightarrow ((\neg P \vee Q) \to R) \wedge (R \to (\neg P \vee Q))$ (消去$\leftrightarrow$)

$\Leftrightarrow (\neg(\neg P \vee Q) \vee R) \wedge (\neg R \vee \neg P \vee Q)$ (消去$\to$)

$\Leftrightarrow ((P \wedge \neg Q) \vee R) \wedge (\neg P \vee Q \vee \neg R)$ (否定号内移)

$\Leftrightarrow (P \wedge \neg Q \wedge \neg P) \vee (P \wedge \neg Q \wedge Q) \vee (P \wedge \neg Q \wedge \neg R)$
$\vee (R \wedge \neg P) \vee (R \wedge Q) \vee (R \wedge \neg R)$ ($\wedge$对$\vee$分配率)

$\Leftrightarrow (P \wedge \neg Q \wedge \neg R) \vee (\neg P \wedge R) \vee (Q \wedge R)$ (矛盾律和同一律)

由此例可知, 命题公式的析取范式不唯一. 同样, 合取范式也是不唯一的.

1.3公式中的范式

主析取范式

公式的析取范式与合取范式的形式是不唯一的. 为了使任意一个命题公式, 化成唯一的等价命题的标准形式, 下面给出主范式的有关概念.

定义 1.15

对n个命题变项$p_1, p_2, \cdots, p_n$组成的简单合取式, 若每个命题变项和它的否定二者之一出现且仅出现一次, 且第i个命题变项或它的否定式出现在从左算起的第i位上, 称这样的简单合取式为**极小项**.

n个命题变项共可产生2^n个不同的极小项. 其中每个极小项都有且仅有一个成真赋值. 若成真赋值所对应的二进制数转换为十进制数i, 就将所对应极小项记作m_i.

1.3公式中的范式

下面的两个表分别是由P, Q两个命题变项形成的全部(4个)极小项以及由P, Q, R三个命题变项形成的全部(8个)极小项.

Table 1.10: P, Q形成的极小项

公式	成真赋值	名称
$\neg P \wedge \neg Q$	00	m_0
$\neg P \wedge Q$	01	m_1
$P \wedge \neg Q$	10	m_2
$P \wedge Q$	11	m_3

back

1.3公式中的范式

Table 1.11: P, Q, R形成的极小项

公式	成真赋值	名称
$\neg P \wedge \neg Q \wedge \neg R$	000	m_0
$\neg P \wedge \neg Q \wedge R$	001	m_1
$\neg P \wedge Q \wedge \neg R$	010	m_2
$\neg P \wedge Q \wedge R$	011	m_3
$P \wedge \neg Q \wedge \neg R$	100	m_4
$P \wedge \neg Q \wedge R$	101	m_5
$P \wedge Q \wedge \neg R$	110	m_6
$P \wedge Q \wedge R$	111	m_7

1.3公式中的范式

由真值表可得到极小项具有如下性质:
(1) 各极小项的真值表都不相同.

(2) 对于极小项m_i, i对应的二进制使其为真, 其余$2^n - 1$ 种方式使其为假.

(3) 任意两个不同极小项的合取式是矛盾式.

(4) 全体极小项的析取式为永真式.

back

1.3公式中的范式

对于析取范式作进一步的要求便有下面的定义.

定义 1.16

若由n个命题变项构成的析取范式中所有的简单合取式都是极小项, 该析取范式为**主析取范式**.

任何命题公式可以表示成析取范式的形式, 但可能不唯一. 对于于主析范式的情况如何? 下面的定理给予回答.

定理 1.9

任何命题公式都存在着与之等值的主析取范式, 并且是惟一的.

back

1.3公式中的范式

证明: (1)证明存在性.
设A是任一含n个命题变项的公式.
由定理1.9可知, 存在与A等值的析取范式A', 即$A \Leftrightarrow A'$, 若A'的某个简单合取式A_i 中既不含命题变项P_j, 也不含它的否定式$\neg P_j$, 则将A_i 展成如下形式:

$$A_i \Leftrightarrow A_i \wedge 1 \Leftrightarrow A_i \wedge (P_j \vee \neg P_j) \Leftrightarrow (A_i \wedge p_j) \vee (A_i \wedge \neg P_j)$$

继续这个过程, 直到所有的简单合取式都含任意命题变项或它的否定式.
上述演算过程中出现重复的命题变项以及极小项和矛盾式时, 可以采用用P 代替$P \wedge P$, m_i代替$m_i \vee m_i$, 0代替矛盾式等.
最后就将A 化成与之等值的主析取范式A''.

back

1.3公式中的范式

(2) 证明唯一性.
假设某一命题公式A存在两个与之等值的主析取范式B和C, 即$A \Leftrightarrow B$ 且$A \Leftrightarrow C$, 则$B \Leftrightarrow C$.
由于B和C是不同的主析取范式, 必然存在极小项m_i只出现在B中, 而不出现在C中.
因为i的二进制使B的成真, 使C的成假, 这与$B \Leftrightarrow C$ 矛盾, 因而B与C必相同.

上面给出求公式主析取范式的方法就是等值演算法.

还有一个从公式的真值表求其主析取范式的方法.

back

1.3公式中的范式

真值表求主析取范式的具体过程:

(1) 求出A的真值表.
(2) 找出A的成真赋值.
(3) 求出每个成真赋值对应的极小项(用名称表示) , 按下标从小到大的顺序析取.

back

1.3公式中的范式

下面是个例子.

例 1.18

利用真值表求$\neg(P \wedge Q)$的主析取范式:

back

1.3公式中的范式

解: $\neg(P \wedge Q)$的真值表如下:

Table 1.12: $\neg(P \wedge Q)$的真值表

P	Q	$\neg(P \wedge Q)$
0	0	1
0	1	1
1	0	1
1	1	0

back

1.3公式中的范式

通过观察看出, 该公式在其真值表的00行, 01行, 10行处取值1, 所以 $\neg(P \wedge Q) \Leftrightarrow m_0 \vee m_1 \vee m_2 \Leftrightarrow (\neg P \wedge \neg Q) \vee (\neg P \wedge Q) \vee (P \wedge \neg Q)$.

当然, 不难由等值演算方法求其主析取范式, 留作练习.

back

1.3公式中的范式

下面是另外一个求主析取范式的公式.

例 1.19

利用等值演算法求$(P \to Q) \leftrightarrow R$的主析取范式:

back

1.3公式中的范式

解: $(P \to Q) \leftrightarrow R$

$\Leftrightarrow (P \wedge \neg Q \wedge \neg R) \vee (\neg P \wedge R) \vee (Q \wedge R)$(这个析取范式的结论前面的例子已经给出.)

$P \wedge \neg Q \wedge \neg R \Leftrightarrow m_4$

$\neg P \wedge R \Leftrightarrow \neg P \wedge (\neg Q \vee Q) \wedge R$

$\Leftrightarrow (\neg P \wedge \neg Q \wedge R) \vee (\neg P \wedge Q \wedge R)$

$\Leftrightarrow m_1 \vee m_3$

$Q \wedge R \Leftrightarrow (\neg P \vee P) \wedge Q \wedge R$

$\Leftrightarrow (\neg P \wedge Q \wedge R) \vee (P \wedge Q \wedge R)$

$\Leftrightarrow m_3 \vee m_7$

$(P \to Q) \leftrightarrow R \Leftrightarrow m_1 \vee m_3 \vee m_4 \vee m_7$

back

1.3公式中的范式

最后把利用等值演算法求公式主析取范式的方法作个总结:

(1) 将公式表示为析取范式.
(2) 除去析取范式中所有永假的析取项.
(3) 将析取式中重复出现的合取项和相同的变元合并.
(4) 对合取项补入没有出现的命题变元, 即添加如$(P \vee \neg P)$式, 然后应用分配律展开公式.

1.3公式中的范式

主析取范式主要具有以下用途:

1. 比较方便地求出公式的成真赋值与成假赋值
设A中含n个命题变项, A的主析取范式含$s(0 \leqslant s \leqslant 2^n)$个极小项, 则$A$有$s$个成真赋值, 它们是所含极小项角标的二进制表示, 其余$2^n - s$个赋值都是成假赋值.
对于前面的例子, $(P \to Q) \leftrightarrow R \Leftrightarrow m_1 \vee m_3 \vee m_4 \vee m_7$. 因而公式的成真赋值为001, 011, 100, 111, 其余的为成假赋值.

back

1.3公式中的范式

2. 容易判断公式的类型 设公式A中含n个命题变项, 不难看出:

若A主析取范式包含全部2^n个极小项, 则A重言式;
若A的主析取范式不含任何极小项, 则A为矛盾式;
若A的主析取范式含有至少一个极小项,表明A为可满足式.

back

1.3公式中的范式

例 1.20

判断下列命题公式的类型:

(1) $((P \to Q) \wedge P) \to Q$

(2) $\neg(P \to Q) \wedge Q$

(3) $(P \to Q) \wedge Q$

解: (1) $((P \to Q) \wedge P) \to Q$

$\Leftrightarrow ((\neg P \vee Q) \wedge P) \to Q$

$\Leftrightarrow \neg((\neg P \vee Q) \wedge P) \vee Q$

$\Leftrightarrow (P \wedge \neg Q) \vee \neg P \vee Q$

$\Leftrightarrow (P \wedge \neg Q) \vee (\neg P \wedge (Q \vee \neg Q)) \vee ((P \vee \neg P) \wedge Q)$

$\Leftrightarrow (P \wedge \neg Q) \vee (\neg P \wedge Q) \vee (\neg P \wedge \neg Q) \vee (P \wedge Q) \vee (\neg P \wedge Q)$

$\Leftrightarrow m_0 \vee m_1 \vee m_2 \vee m_3$

1.3公式中的范式

(2) $\neg(P \to Q) \wedge Q$
$\Leftrightarrow \neg(\neg P \vee Q) \wedge Q$
$\Leftrightarrow (P \wedge \neg Q) \wedge Q$
$\Leftrightarrow 0$

命题公式(2)为永假式.

back

1.3公式中的范式

(3)$(P \to Q) \wedge Q$
$\Leftrightarrow (\neg P \vee Q) \wedge Q$
$\Leftrightarrow (\neg P \wedge Q) \vee Q$
$\Leftrightarrow (\neg P \wedge Q) \vee (\neg P \vee P) \wedge Q)$
$\Leftrightarrow (\neg P \wedge Q) \vee (\neg P \wedge Q) \vee (P \wedge Q)$
$\Leftrightarrow (\neg P \wedge Q) \vee (P \wedge Q)$
$\Leftrightarrow m_1 \vee m_3$

因此命题公式(3)为可满足式.

back

1.3公式中的范式

3. 判断两个命题公式是否等价

两个命题的主析取范式相同, 则等价; 否则, 不等价.

例 1.21

判断下面两组公式是否等价:

(1) P与$(P \wedge Q) \vee (P \wedge \neg Q)$

(2)$(P \to Q) \to R$与$(P \wedge Q) \to R$

解: (1)P

$\Leftrightarrow P \wedge (\neg Q \vee Q)$

$\Leftrightarrow (P \wedge \neg Q) \vee (P \wedge Q)$

$\Leftrightarrow m_2 \vee m_3$

$(P \wedge Q) \vee (P \wedge \neg Q) \Leftrightarrow m_2 \vee m_3$

两公式等价.

1.3公式中的范式

(2)$(P \to Q) \to R$
$\Leftrightarrow m_1 \vee m_3 \vee m_4 \vee m_5 \vee m_7$

$(P \wedge Q) \to R \Leftrightarrow m_0 \vee m_1 \vee m_2 \vee m_3 \vee m_4 \vee m_5 \vee m_7$

两个公式不等价.

1.3公式中的范式

4. 应用主析取范式解决实际问题

例 1.22

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. 由于工作原因, 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. 问应如何安排?

一般分析:

(1) 将简单命题符号化.

(2) 写出各复合命题.

(3) 写出由(2)中复合命题组成的合取式(前提) .

(4) 将(3)中公式化成析取式(最好是主析取范式) .

(5) 这样每个小项就是一种可能产生的结果. 去掉不符合题意的小项, 即得结论.

back

1.3公式中的范式

解: 设 P: 派A去, Q: 派B去, R: 派C去.

由已知条件可得公式
$(P \to R) \wedge (Q \to \neg R) \wedge (\neg R \to (P \vee Q))$
经过演算可得 $(P \to R) \wedge (Q \to \neg R) \wedge (\neg R \to (P \vee Q)) \Leftrightarrow m_1 \vee m_2 \vee m_5$

由于 $m_1 = \neg P \wedge \neg q \wedge r$, $m_2 = \neg P \wedge q \wedge \neg R$, $m_5 = P \wedge \neg Q \wedge R$

可知选派方案有3种:
(a) C去, A,B不去. (b) B去, A,C不去. (c) A,C 去, B不去.

back

1.3公式中的范式

主合取范式

前面讨论的是主析取范式, 现在讨论主合取范式.

定义 1.17

对n个命题变项$p_1, p_2, \cdots, p_n$组成的简单析取取式, 若每个命题变项和它的否定二者之一出现且仅出现一次, 且第i个命题变项或它的否定式出现在从左算起的第i位上, 称这样的简单析取式为**极大项**.

n个命题变项共可产生2^n个不同的极大项. 每个极大项有仅有一个取值方式使其成假. 若成假赋值所对应的二进制数转换为十进制数为i, 就将所对应极大项记作M_i.

back

1.3公式中的范式

下述的两个表是由P, Q两个命题变项及由P, Q, R 三个命题变项分别形成的全部极大项.

Table 1.13: P, Q形成的极大项

公式	成假赋值	名称
$\neg P \vee \neg Q$	11	M_3
$\neg P \vee Q$	10	M_2
$P \vee \neg Q$	01	M_1
$P \vee Q$	00	M_0

back

1.3公式中的范式

Table 1.14: P, Q, R形成的极大项

公式	成假赋值	名称
$\neg P \vee \neg Q \vee \neg R$	111	M_7
$\neg P \vee \neg Q \vee R$	110	M_6
$\neg P \vee Q \vee \neg R$	101	M_5
$\neg P \vee Q \vee R$	100	M_4
$P \vee \neg Q \vee \neg R$	011	M_3
$P \vee \neg Q \vee R$	010	M_2
$P \vee Q \vee \neg R$	001	M_1
$P \vee Q \vee R$	000	M_0

back

1.3公式中的范式

由真值表可得到极大项具有如下性质:

(1) 各极大项的真值表都不相同.

(2) 对极大项M_i, 只有i的二进制使其为假, 其余2^n-1种为真.

(3) 任意两个不同极大项的析取式是永真式.

(4) 所有极大项的合取式为永假式.

back

1.3公式中的范式

定义 1.18

若n个命题变项构成的合取范式中所有的简单析取式都是极大项, 该合取范式称为**主合取范式**.

定理 1.10

任何命题公式都存在着与之等值的主合取范式, 并且是唯一的.

证明方法与主析取范式的存在唯一性类似, 这里不再赘述.
同主析取范式的求法类似, 也可以通过两种方法求主合取范式. 一是由公式的真值表得出; 另一种是由基本等价公式推出.

back

1.3公式中的范式

方法一, 真值表法
(1) 求出A的真值表.
(2) 找出A的成假赋值.
(3) 求出每个成假赋值对应的极大项(用名称表示) , 按下标从小到大顺序合取.
下面是一个例子.

例 1.23

利用真值表求$(P \to Q) \wedge Q$的主合取范式:

back

1.3公式中的范式

解: $(P \to Q) \wedge Q$的真值表见下表.

Table 1.15: $(P \to Q) \wedge Q$的真值表

P	Q	$P \to Q$	$(P \to Q) \wedge Q$
0	0	1	0
0	1	1	1
1	0	0	0
1	1	1	1

该公式在其真值表的00行, 10行处取真值0, 将两行对应的极大项作合取, 便有

$(P \to Q) \wedge Q \Leftrightarrow (P \vee Q) \wedge (\neg P \vee Q) \Leftrightarrow M_0 \wedge M_2$.

1.3公式中的范式

方法二, 等值演算法
方法与求主析取范式的步骤相似. 下面是求主合取范式的主要步骤为:
(1) 求出合取范式.
(2) 除去合取范式中所有永真的项.
(3) 将合取式中重复出现的项和相同的变元合并.
(4) 合取式中的某些项补入没有出现的命题变元, 即添加如$(P \wedge \neg P)$ 式, 然后应用分配律展开公式.

back

1.3公式中的范式

例 1.24

利用等值演算法求$(P \to Q) \leftrightarrow R$的主合取范式:

解: $(P \to Q) \leftrightarrow R$

$\Leftrightarrow (P \vee R) \wedge (\neg Q \vee R) \wedge (\neg P \vee Q \vee \neg R)$ (该结果之前的例子已经求出)

$\neg P \vee Q \vee \neg R \Leftrightarrow M_5$

$P \vee R \Leftrightarrow P \vee (Q \wedge \neg Q) \vee R \Leftrightarrow (P \vee Q \vee R) \wedge (P \vee \neg Q \vee R) \Leftrightarrow M_0 \vee M_2$

$\neg Q \vee R \Leftrightarrow (P \wedge \neg P) \vee \neg Q \vee R$

$\Leftrightarrow (P \vee \neg Q \vee R) \wedge (\neg P \vee \neg Q \vee R)$

$\Leftrightarrow M_2 \vee M_6$

$(P \to Q) \leftrightarrow R \Leftrightarrow M_0 \vee M_2 \vee M_5 \vee M_6$

back

1.3公式中的范式

极小项与极大项之间是否有某些联系?

主析取范式由极小项析取构成; 主合取范式由极大项合取构成.

根据极小项和极大项的定义, 有:

定理 1.11

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
$\neg m_i \Leftrightarrow M_i$, $\neg M_i \Leftrightarrow m_i$

back

1.3公式中的范式

主析取范式与主合取范式之间是否有某些联系?

设公式A含n个命题变项. 已知A的主析取范式含$s(0 < s < 2^n)$个极小项, 即

$A \Leftrightarrow m_{i_1} \vee m_{i_2} \vee \cdots \vee m_{i_s}, 0 \leq i_j \leq 2^n - 1, j = 1, 2, \cdots, s$

没有出现的极小项设为$m_{j_1}, m_{j_2}, \cdots, m_{j_{2^n - s}}$

它们的下标的二进制使A为假, 从而使$\neg A$为真. 按照一个公式主析取范式的真值表求法, $\neg A$ 的主析取范式为

$\neg A \Leftrightarrow m_{j_1} \vee m_{j_2} \vee \cdots \vee m_{j_{2^n - s}}$

$$
\begin{aligned}
A &\Leftrightarrow \neg\neg A \\
&\Leftrightarrow \neg(m_{j_1} \vee m_{j_2} \vee \cdots \vee m_{j_{2^n - s}}) \\
&\Leftrightarrow \neg m_{j_1} \wedge \neg m_{j_2} \wedge \cdots \wedge \neg m_{j_{2^n - s}} \\
&\Leftrightarrow M_{j_1} \wedge M_{j_2} \wedge \cdots \wedge M_{j_{2^n - s}}
\end{aligned}
$$

1.3公式中的范式

因此, 可以由A的主析取范式求其主合取范式, 步骤为:

(1) 找出A的主析取范式中没有包含的极小项.
(2) 找出与(1)中极小项的角码相同的极大项.
(3) 将(2)中极大项进行合取, 即为A的主合取范式.
根据以上方法, 只要掌握了求主析取范式的方法, 就可以即求其主合取范式.

例 1.25

已知下面两个公式的主析取范式, 求其主合取范式:
(1) $A \Leftrightarrow m_1 \vee m_2$ (已知A中含两个命题变项P,Q)
(2) $B \Leftrightarrow m_1 \vee m_2 \vee m_3$ (已知B 中含三个命题变项P,Q,R)

back

1.3公式中的范式

解: (1) $A \Leftrightarrow M_0 \wedge M_3$
(2) $B \Leftrightarrow M_0 \wedge M_4 \wedge M_5 \wedge M_6 \wedge M_7$

主合取范式和主析取范式用途一样, 通过它也可以求公式的成真赋值与成假赋值; 判断公式的类型; 判断两个命题公式是否等价等等.

1.4命题连接词的扩充与规约

前面介绍了5种常用的逻辑连接词$\neg, \wedge, \vee, \rightarrow, \leftrightarrow$.

从更广泛的意义上反映命题之间的逻辑联系, 这5个连接词可能还不够. 下面再介绍3种连接词.

back

1.4命题连接词的扩充与规约

定义 1.19

已知P, Q为两命题. 复合命题“P, Q之中恰有一个成立” 称为P 与Q 的**排斥或**或**异或**, 记作$P \oplus Q$. 相应地$\oplus$ 叫作**排斥或连接词**或**异或联结词**. 其定义可用如下真值表表示:

Table 1.16: $P \oplus Q$

P	Q	$P \oplus Q$
0	0	0
0	1	1
1	0	1
1	1	0

1.4命题连接词的扩充与规约

从定义及真值表可知, $P \oplus Q \Leftrightarrow (P \wedge \neg Q) \vee (\neg P \wedge Q)$.
利用真值表法, 可得“$\oplus$” 具有如下性质:

(1) $P \oplus Q \Leftrightarrow Q \oplus P$
(2) $(P \oplus Q) \oplus R \Leftrightarrow P \oplus (Q \oplus R)$
(3) $P \wedge (Q \oplus R) \Leftrightarrow (P \wedge Q) \oplus (P \wedge R)$
(4) $P \oplus Q \Leftrightarrow (P \wedge \neg Q) \vee (\neg P \wedge Q)$
(5) $P \oplus Q \Leftrightarrow \neg(P \leftrightarrow Q)$
(6) $P \oplus P \Leftrightarrow F$; $F \oplus P \Leftrightarrow P$; $T \oplus P \Leftrightarrow \neg P$

back

1.4命题连接词的扩充与规约

定义 1.20

已知P, Q为两命题, 复合命题“ P与Q的否定” 称为P与Q的**与非式**, 记作 $P \uparrow Q$. $\uparrow$ 称作**与非联结词**. $P \uparrow Q$为真当且仅当P, Q不同时为真. 其定义可用如下真值表表示:

Table 1.17: $P \uparrow Q$

P	Q	$P \uparrow Q$
0	0	1
0	1	1
1	0	1
1	1	0

1.4命题连接词的扩充与规约

从定义及真值表可知, $P \uparrow Q \Leftrightarrow \neg(P \wedge Q)$.

利用真值表法, 可得“$\uparrow$” 具有如下性质:

(1) $P \uparrow P \Leftrightarrow \neg(P \wedge P) \Leftrightarrow \neg P$

(2) $(P \uparrow Q) \uparrow (P \uparrow Q) \Leftrightarrow \neg(P \uparrow Q) \Leftrightarrow P \wedge Q$

(3) $(P \uparrow P) \uparrow (Q \uparrow Q) \Leftrightarrow \neg P \uparrow \neg Q \Leftrightarrow P \vee Q$

back

1.4命题连接词的扩充与规约

定义 1.21

已知P, Q为两命题, 复合命题“ P或Q的否定” 称为P与Q的**或非式**, 记作$P \downarrow Q$. $\downarrow$称作**或非联结词**. $P \downarrow Q$ 为真当且仅当P,Q同时为假. 其定义可用如下真值表表示:

Table 1.18: $P \downarrow Q$

P	Q	$P \downarrow Q$
0	0	1
0	1	0
1	0	0
1	1	0

1.4命题连接词的扩充与规约

从定义及真值表可知, $P \downarrow Q \Leftrightarrow \neg(P \vee Q)$.

利用真值表法, 可得“$\downarrow$” 具有如下性质:

(1)$P \downarrow P \Leftrightarrow \neg(P \vee P) \Leftrightarrow \neg P$

(2)$(P \downarrow Q) \downarrow (P \downarrow Q) \Leftrightarrow \neg(P \downarrow Q) \Leftrightarrow P \vee Q$

(3)$(P \downarrow P) \downarrow (Q \downarrow Q) \Leftrightarrow \neg P \downarrow \neg Q \Leftrightarrow P \wedge Q$

back

命题联结词的归约

已经学习了8个联结词, 后面的3个体现的逻辑关系可由其它的5个来反映. 这表明表达命题时, 所有的连接词并不是缺一不可. 这就产生了所需要联结词数量多少的问题, 如果任一**命题公式**都可以用事先给定的某些连接词(不一定为全部)来表示, 那么这些连接词组成的集合称为全功能集. 有n个命题变项的命题公式的真值表反映了2^n种取值方式与$\{0,1\}$之间的对应关系. 可以将这种对应关系看作一个函数, 这就是所谓的真值函数.

定义 1.22

称定义域为$\{00\cdots0, 00\cdots1, \cdots11\cdots1\}$, 值域为$\{0,1\}$的函数是$n$元**真值函数**, 定义域中的元素是长为$n$的0,1串. 常用$F:\{0,1\}^n \to \{0,1\}$表示$F$是$n$元真值函数.

back

1.4命题连接词的扩充与规约

n个命题变项共可以形成2^{2^n}个不同的真值函数, 每个真值函数可对应无穷多个命题公式, 它们彼此都是等值的.

两个命题变项对应的16个真值函数见课本.

对于任何一个含n个命题变项的命题公式A, 都存在 惟一的一个n元真值函数F为A的真值表, 等值的公式对应的真值函数相同.

back

1.4命题连接词的扩充与规约

例如: $P \to Q, \neg P \vee Q, (\neg P \vee Q) \vee (\neg(P \to Q) \wedge Q)$等都对应表中的$F_{14}$.
在一个由连接词组成的集合中, 某些对于另外的一些可能是多余的.

定义 1.23

在一个联结词的集合中, 如果一个联结词可 由集合中的其他联结词定义, 则称此联结词为**冗余 的联结词**, 否则称为**独立的联结词**.

back

1.4命题连接词的扩充与规约

例如,在联结词集$\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$中, 由于$P \rightarrow Q \Leftrightarrow \neg P \vee Q$, 所以, $\rightarrow$为冗余的联结词; 类似地, $P \leftrightarrow Q \Leftrightarrow (\neg P \vee Q) \wedge (\neg Q \vee P)$,$\leftrightarrow$ 也是冗余的联结词.

又考虑到在$\{\neg, \wedge, \vee\}$中, 由于 $P \wedge Q \rightarrow \neg(\neg P \vee \neg Q)$, 说明“$\wedge$” 和“$\wedge$” 可以互相替换. 所以, $\wedge$ 是冗余的联结词. 类似地, $\vee$也是冗余的联 结词. 但在$\{\neg, \wedge\}$中无冗余的联结词, 与此类似, $\{\neg, \vee\}$ 中也无冗余的联结词.

back

1.4命题连接词的扩充与规约

定义 1.24

设S是一个联结词集合, 如果任何$n(n \geq 1)$元 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**联结词全功能集**. 如果在S中去掉任何一个联结词后都不再具有这种性质, 则称它是**极小全功能集**.

若S是联结词全功能集, 则任何命题公式都可用S 中的联结词表示.

back

1.4命题连接词的扩充与规约

可以证明$\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$, $\{\neg, \wedge, \vee\}$, $\{\neg, \vee\}$, $\{\neg, \wedge\}$, $\{\neg, \rightarrow\}$, $\{\uparrow\}$, $\{\downarrow\}$等都是全功能集, 其中$\{\neg, \vee\}$, $\{\neg, \wedge\}$, $\{\neg, \rightarrow\}$, $\{\uparrow\}$, $\{\downarrow\}$等是极小全功能集.

例 1.26

若已知$\{\neg, \rightarrow\}$是全功能集, 证明$\{\neg, \vee\}$ 也是全功能集.

证明　由于$\{\neg, \rightarrow\}$是全功能集, 因而任一真值函数均可仅由含$\{\neg, \rightarrow\}$中的联结词的命题公式表示. 而对于任意的命题形式A, B, 有$A \rightarrow B \Leftrightarrow \neg A \vee B$, 因而任一真值函数均可仅由含$\{\neg, \vee\}$中的联结词的命题公式表示, 所以它是全功能集.

1.5基于命题的推理

数理逻辑的主要任务是用数学的方法来研究推理的规律.
推理是指从前提出发推出结论的思维过程.
前提是已知命题公式集合.
结论是从前提出发应用推理规则推出的命题公式.
证明是描述推理的过程.

要研究推理, 首先应该明确什么样的推理是有效的或正确的.

back

1.5基于命题的推理

定义 1.25

若$(A_1 \wedge A_2 \wedge \cdots \wedge A_k) \rightarrow B$为重言式，则称$A_1, A_2, \cdots, A_k$推出结论$B$的推理正确，$B$是$A_1, A_2, \cdots, A_k$的**逻辑结论或有效结论**. 称表达式$(A_1 \wedge A_2 \wedge \cdots \wedge A_k) \rightarrow B$为由前提$A_1, A_2, \cdots, A_k$推出结论$B$的推理的形式结构. 记作$A_1, A_2, \cdots, A_k \Rightarrow B$.

back

1.5基于命题的推理

注意, 在推理逻辑中, 按照所谓“正确推理”的定义, 只有在给定前提$A_1, A_2, \cdots, A_k$都是真的情况下, 推理过程推出的结论B才是正确的. 在前提是假的情况下, “正确推理”下的有效结论可以是假.

推理注重的是形式正确, 并不要求结论一定正确.

下面讨论推理方法.

1.5基于命题的推理

既然可以利用真值表可以判断公式的真假, 也就有 **基于真值表的推理.**
构造公式$A_1 \wedge A_2 \wedge \cdots \wedge A_k \rightarrow B$的真值表, 若它为重言式, 则结论$B$是有效的.

例 1.27

判断下面推理是否正确.
(1) $P \wedge Q \Rightarrow P$
(2) $P, (Q \rightarrow P) \Rightarrow Q$

back

1.5基于命题的推理

解: (1) 推理正确. 只需证明$P \wedge Q \rightarrow P$为重言式,真值表见表1.19.

Table 1.19: $P \wedge Q \rightarrow P$的真值表

P	Q	$P \wedge Q$	$P \wedge Q \rightarrow P$
0	0	0	1
0	1	0	1
1	0	0	1
1	1	1	1

真值表的最后一列全是1, 因而(1)是重言式, 所以推理正确.

back

1.5基于命题的推理

(2) 推理不正确. 只需证明 $P\wedge(Q\rightarrow P)\rightarrow Q$ 不为重言式, 真值表见表1.20.

Table 1.20: $P\wedge(Q\rightarrow P)\rightarrow Q$ 的真值表

P	Q	$P\wedge(Q\rightarrow P)$	Q	$P\wedge(Q\rightarrow P)\rightarrow Q$
0	0	0	0	1
0	1	0	1	1
1	0	1	0	0
1	1	1	1	1

可以看出, 真值表的最后一列不全是1, 因而(2)不是重言式, 所以推理不正确.

back

1.5基于命题的推理

例 1.28

判断以下推理是否正确:
一份统计表格的错误是由于材料有误或者是由于计算有误;
已知表格错误不是材料有误, 因此计算有误.

解: 设P: 表格的错误是由于材料有误. Q: 表格的错误是由于计算有误.
前提: $P \vee Q, \neg P$.
结论: Q.
推理的形式结构为:

back

1.5基于命题的推理

$P \vee Q, \neg P \Rightarrow Q$, 只需证明 $(P \vee Q) \wedge \neg P \rightarrow Q$为重言式, 真值表见表1.21.

Table 1.21: $(P \vee Q) \wedge \neg P \rightarrow Q$ 的真值表

P	Q	$P \vee Q$	$\neg P$	$(P \vee Q) \wedge \neg P \rightarrow Q$
0	0	0	1	1
0	1	1	1	1
1	0	1	0	1
1	1	1	0	1

真值表的最后一列全是1, 因而$(P \vee Q) \wedge \neg P \rightarrow Q$ 是重言式, 所以推理正确.

back

1.5基于命题的推理

当命题变项比较少时, 可以利用用真值表的方法判断形式推理

$$A_1, A_2, \cdots, A_k \Rightarrow B$$

是否正确.

back

1.5基于命题的推理

在推理过程中, 如果命题变项较多, 真值表的方法是不方便的, 这时可以采用**构造证明**的方法. 这种方法是由一组前提条件, 利用**公认的推理规则**(这些规则下面会以序号的方式给出), 推导得到有效结论.

构造证明是一个命题公式序列, 序列中的每个命题公式或者是已知前提, 或者是由前提应用推理规则得到的结论, 该序列描述了推理过程.

若$A_1, A_2, \cdots, A_k \Rightarrow B$, 在证明的序列中可以将$B$ 加入到序列中作为条件, 这称为**引入**B, 可以理解为证明过程中的结论作为条件继续后面的证明.

下面给出构造证明中公认的常用推理规则:

back

1.5基于命题的推理

(1) 前提引入规则: 在证明的任何步骤上都可以引入前提.
(2) 结论引入规则: 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, 得到公式序列中的又一个公式. 例如, 可用$\neg P \vee Q$置换$P \to Q$ 等.
(4) 假言推理规则: $A \to B, A \Rightarrow B$.
(5) 附加规则: $A \Rightarrow A \vee B$.
(6) 化简规则: $A \wedge B \Rightarrow A$.
(7) 拒取式规则: $A \to B, \neg B \Rightarrow \neg A$.

back

1.5基于命题的推理

8) 假言三段论规则: $A \to B, B \to C \Rightarrow A \to C$.
(9) 析取三段论规则: $A \vee B, \neg B \Rightarrow A$.
(10) 构造性二难规则: $A \to B, C \to D, A \vee C \Rightarrow B \vee D$.
(11) 破坏性二难规则: $A \to B, C \to D, \neg B \vee \neg D \Rightarrow \neg A \vee \neg C$.
(12) 合取引入规则: $A, B \Rightarrow A \wedge B$.

下面通过例题说明如何运用以上规则构造证明.

1.5基于命题的推理

例 1.29

构造下面推理的证明:

(1) 前提: $\neg P \vee Q, R \vee \neg Q, R \rightarrow S$.

结论: $P \rightarrow S$.

(2) 前提: $P \rightarrow (Q \rightarrow R), P \wedge Q$.

结论: $\neg R \rightarrow S$.

1.5基于命题的推理

证明(1)①$\neg P \vee Q$	前提引入
②$P \to Q$	① 置换
③$R \vee \neg Q$	前提引入
④$Q \to R$	③ 置换
⑤$P \to R$	②④ 假言三段论
⑥$R \to S$	前提引入
⑦$P \to S$	⑤⑥ 假言三段论

1.5基于命题的推理

(2)① $P \rightarrow (Q \rightarrow R)$ 前提引入
② $P \wedge Q$ 前提引入
③ P ②化简
④ Q ②化简
⑤ $Q \rightarrow R$ ①③ 假言推理
⑥ R ④⑤假言推理
⑦ $R \vee S$ ⑥附加
⑧ $\neg R \rightarrow S$ ⑦ 置换

back

1.5基于命题的推理

例 1.30

构造下面推理的证明:
如果我学习, 那我数学会及格. 如果我不玩扑克, 那么我会学习. 现在我数学不及格. 因而我玩扑克了.

解: 设P: 我学习. Q: 我数学及格. R: 我玩扑克.
形式结构为:
前提: $P \to Q, \neg R \to P, \neg Q$.
结论: R.

1.5基于命题的推理

证明: ①$P \to Q$	前提引入
②$\neg Q$	前提引入
③$\neg P$	①②拒取式
④$\neg R \to P$	前提引入
⑤$\neg\neg R$	③④ 拒取式规则
⑥R	⑤置换

back

1.5基于命题的推理

上面的证明方法称为**直接证明法**. 下面再介绍分别称为**附加前提法**和**归谬法**的两种方法. 这两种方法也叫间接证法.

1. 附加前提证明法

若推理的形式具有如下结构：

前提: $A_1, A_2, \cdots A_k$, 结论: $C \to B$

可将结论中的前件C作为推理的前提, 使结论只为B, 变为推理形式:

前提: $A_1, A_2, \cdots A_k, C$, 结论: B

1.5基于命题的推理

上述两种推理形式等价. 原因在于:

$$
\begin{aligned}
&(A_1 \wedge A_2 \wedge \cdots \wedge A_k) \rightarrow (C \rightarrow B) \\
&\Leftrightarrow \neg(A_1 \wedge A_2 \wedge \cdots \wedge A_k) \vee (\neg C \vee B) \\
&\Leftrightarrow \neg(A_1 \wedge A_2 \wedge \cdots \wedge A_k \wedge C) \vee B \\
&\Leftrightarrow (A_1 \wedge A_2 \wedge \cdots \wedge A_k \wedge C) \rightarrow B
\end{aligned}
$$

back

1.5基于命题的推理

用附加前提证明法推理示例.

例 1.31

如果小张和小王去看电影, 则小李也去; 小赵不去看电影或小张去看电影; 小王去看电影. 所以, 当小赵去看电影时, 小李也去看电影.

解: 设P:小张去看电影. Q:小王去看电影. R:小李去看电影. S: 小赵去看电影.
形式结构为:
前提: $(P \wedge Q) \rightarrow R, \neg S \vee P, Q$.
结论: $S \rightarrow R$.

1.5基于命题的推理

证明: ① S	附加前提引入
② $\neg S \vee P$	前提引入
③ P	①②析取三段论
④ $(P \wedge Q) \rightarrow R$	前提引入
⑤ Q	前提引入
⑥ $P \wedge Q$	③⑤合取
⑦ R	④⑥ 假言推理

由附加前提证明法, 推理正确.

back

1.5基于命题的推理

2. 归谬法(又称反证法)

若推理的形式具有如下结构：
前提: $A_1, A_2, \cdots, A_k$, 结论: B
可将$\neg B$作为前提推出矛盾, 即推理的形式变成结构:
前提: $A_1, A_2, \cdots, A_k, \neg B$, 结论: 矛盾

back

1.5基于命题的推理

归谬法的依据:

$$
\begin{aligned}
&(A_1 \wedge A_2 \wedge \cdots \wedge A_k) \rightarrow B \\
&\Leftrightarrow \neg(A_1 \wedge A_2 \wedge \cdots \wedge A_k) \vee B \\
&\Leftrightarrow \neg(A_1 \wedge A_2 \wedge \cdots \wedge A_k \wedge \neg B)
\end{aligned}
$$

若$A_1 \wedge A_2 \wedge \cdots \wedge A_k \wedge \neg B$为矛盾式, 则说明$(A_1 \wedge A_2 \wedge \cdots \wedge A_k) \rightarrow B$为重言式.

1.5基于命题的推理

归谬法推理示例.

例 1.32

如果小张守第一垒并且小李向B队投球, 则A队将取胜; A队未取胜或者A队获得联赛第一名; A队没有获得联赛的第一名; 小张守第一垒. 因此, 小李没有向B队投球.

back

1.5基于命题的推理

解: 设

P: 小张守第一垒.
Q: 小李向B队投球.
R: A队取胜.
S: A队获得联赛第一名.

形式结构为:

前提: $(P \wedge Q) \rightarrow R, \neg R \vee S, \neg S, P.$ 结论: $\neg Q.$

1.5基于命题的推理

证明: ①Q	结论的否定引入
②$\neg R \vee S$	前提引入
③$\neg S$	前提引入
④$\neg R$	②③ 析取三段论
⑤$(P \wedge Q) \rightarrow R$	前提引入
⑥$\neg(P \wedge Q)$	④⑤ 拒取式
⑦$\neg P \vee \neg Q$	⑥ 置换
⑧P	前提引入
⑨$\neg Q$	⑦⑧析取三段论
⑩$Q \wedge \neg Q$	①⑨ 合取

由于最后一步为矛盾式, 所以推理正确.

back

1.5基于命题的推理

从逻辑的角度来讲, 间接证明法与直接证明法同样有效, 方便程度会因问题不同而异。可根据实际问题选择其一。

back

目录

2.1谓词公式

命题逻辑的特点是以单句为基本处理对象, 不再对单句进行分解. 然而现实生活中的许多问题, 若仅以单句为处理对象, 则无法探究命题的内部结构、成份, 也无法细划命题间的内部关系. 因此, 即使一些简单的问题若仅仅采用命题逻辑相关知识, 很难得出正确的结论. 比如, 考虑下面的推理:

所有学生应以学习为重. 张三是位学生. 所以, 张三应以学习为重.

2.1谓词公式

这个推理显然是个真命题, 但却无法用命题逻辑相关知识来判断它的正确性.
原因在于, 在命题逻辑中, 问题的解决是以单句为基本处理对象, 将上例中出现的3个单句依次符号化为p, q, r, 于是上述问题的符号化结果为:

$$p \wedge q \rightarrow r$$

然而, 简单分析即可发现, 上式不是重言式, 所以不能由它来判断上例为真命题.

2.1谓词公式

原因何在？问题出在于命题逻辑求解问题的思路不考虑命题单句之间的内在联系和数量关系．把"所有学生应以学习为重＂作为一个简单命题来处理，这也就失去了问题的本质含义．为了真实地表达上例的内在含义，还需要进一步的对单句进行拆分，即拆分出＂所有＂，＂学生＂，＂...，以学习为重＂等内容．这也就是谓词逻辑所研究的内容，谓词逻辑又称为一阶逻辑．

2.1谓词公式

为了更好地描述单句中的内在联系和数量关系，在谓词逻辑中首先引入个体词，谓词，量词3个基本元素．下面首先讨论这3个元素．

定义 2.1

独立存在的具体或者抽象的客体称为**个体词**

个体词可以是一个具体的事物，也可以是一个抽象的概念．例如，梅西，足球，离散数学，整数，思想，定义等都可以作为个体词．如同命题有命题常项和命题变项之分．个体词也可简单分为**个体常项**和**个体变项**．

2.1谓词公式

表示具体的或者特定的个体的词称为**个体常项**, 个体常项一般用小写的英文字母$a, b, c, \cdots$表示. 表示抽象或泛指的个体词称为**个体变项**, 个体变项常用$x, y, z, \cdots$表示. 并称个体变项的变化范围为**个体域**. 个体域可以是有限的集合, 例如, {14计1, 14 电本, 14电气2}, { 计算机专业, 电子专业, 自动化专业}; 也可以是无限的集合, 例如整数集合Z, 实数集合R等等. 在个体域中有一个特殊的个体域即由宇宙间的一切事物组成的个体域, 称为**全总个体域**.

2.1谓词公式

定义 2.2

描述刻画主体词的性质、状态或者表达个体词之间关系的词称为**谓词**.

谓词常用$F, G, H, \cdots$表示.

例 2.1

考虑下面几个语句, 分析其中出现的个体常项, 个体变项, 谓词.

(1) 皇家马德里是欧冠冠军球队.

(2) x是变量.

(3) 小张与小王是同学.

(4) p与q有关系.

2.1谓词公式

解: 在上例中, 皇家马德里, 小张, 小王, 是个体常项, x, p, q是个体变项.

"…是欧冠冠军球队";

"…是变量";

"…与…是同学";

"…与…有关系"

是谓词, 上述谓词可简单用F, G, H, M来描述. 这样上例中的语句可简单用下式表达:

(1) F(皇家马德里);

(2) $G(x)$;

(3) $H(a,b)$ (其中a表示小张, b 表示小王);

(4) $M(p,q)$.

2.1谓词公式

定义 2.3

生活中常见的数量词称为**量词**.

共有两大类量词:

(1) 全称量词. 现实生活中, 常用到的"所有的", "一切的", "每一个", " 全", " 都"等词都统称为**全称量词**, 用符号$\forall$表示. $\forall x$ 表示个体域中的所有个体x. 例如$\forall xF(x)$表示个体域中所有的x都具有性质F.

(2) 存在量词. 日常生活中, 常用到的"存在", "有一个", "某一些", "不是所有", "至少一个"等词都统称为**存在量词**, 用符号$\exists$表示, $\exists x$ 表示个体域中, 存在一个或者一些个体x.例如$\exists xF(x)$表示个体域中存在着x 具有性质F.

2.1谓词公式

谓词逻辑的符号化问题:

谓词逻辑中由于引入了个体词、谓词、量词等概念, 其命题的符号化问题要比命题逻辑困难很多.
同一个命题在不同的个体域下, 可能有不同的符号化形式, 其取值也可能存在差异. 因此, 在对自然语言进行命题的符号化时, 一定要先明确个体域（个体词的取值范围）.

2.1谓词公式

下面通过一些实例来讨论谓词逻辑中命题的符号化问题.

例 2.2

在个体域分别限定为(a)和(b)情况下, 将下面命题符号化.
(1) 所有人都喝水.
(2) 有人勇敢.
(a)个体域D_1为人类集合; (b)个体域D_2为全总个体域;

2.1谓词公式

解:
(a) 令$F(x):x$喝水. $G(x):x$勇敢. 在个体域为D_1的前体下, 上例可公式化为:
$(1)\quad \forall xF(x)$;
$(2)\quad \exists xG(x)$;
(b)在个体域为D_2的背景下, 除人之外, 还有其它生物. 在公式化时, 需要把人先分离出来. 为此, 令$M(x):x$是人; 此时, 上例可公式化为:
$(1)\quad \forall x(M(x)\rightarrow F(x))$;
$(2)\quad \exists x(M(x)\wedge G(x))$;

2.1谓词公式

讨论完个体词、谓词及量词等概念, 结合命题逻辑中的命题常元、命题变元、个体常元、个体变元以及几大类联结词, 给出谓词逻辑公式的抽象定义.
为更清晰直觉地描述谓词公式, 先给出项的概念.

定义 2.4

(1) 任意的个体常量符$a, b, c, \cdots$或任意的个体变量符$x, y, z, \cdots$是**项**;
(2) 设$t_1, t_2, \cdots, t_n$是项, $f(x_1, x_2, \cdots, x_n)$是n元函数符, 则$f(t_1, t_2, \cdots, t_n)$是**项**;
(3)有限次的使用规则(1), (2)得到的符号串才是项.

2.1谓词公式

定义 2.5

若$F(x_1, x_2, \cdots, x_n)$是n元 谓 词，t_1，t_2，$\cdots$，t_n是 项，则称$F(t_1, t_2, \cdots, t_n)$为 **原子谓词公式**, 简称为**原子公式**.

2.1谓词公式

下面是**谓词公式**的定义.

定义 2.6

(1) 原子公式是谓词公式;
(2) 若A, B是谓词公式, 则$(\neg A), (\neg B), (A \wedge B), (A \vee B), (A \rightarrow B), (A \leftrightarrow B)$也是.
(3) 如果A是谓词公式, x是个体变元, 则$(\forall xA)$、$(\exists xA)$ 也是谓词公式;
(4) 有限次的使用规则(1)、(2)、(3)产生的表达式才是谓词公式;
谓词公式, 也称合式公式, 简称**公式**.

在不引起混淆的情况下, 谓词公式最外层的括号可以省略, 如$(\neg A), (A \wedge B)$可以写成$\neg A, A \wedge B$.

2.1谓词公式

例如:
$(\forall x)(\forall y)(\neg F(f(x,y),x)), \forall x(F(x) \rightarrow \exists y(G(y) \wedge H(x,y))).$
都是公式,

而$(\forall x)((F(x) \rightarrow (G(x), (\exists y)(\forall x)(\wedge(F(x,y)).$
则都不是合法的谓词公式, 前者括号不匹配, 后者量词后面的内容不符合定义.

2.2约束

一般情况下, 变元都有具体的含义和应用背景, 从上下文中即可将其进行区分.但在谓词公式中, 变元的含义不需要考虑, 如此情况下, 对变元就需要从形式上进行严格的区分, 并作如下定义.

定义 2.7

在谓词公式$\forall xA$和$\exists xA$中, 称x为量词的**指导变元**, A为量词的**辖域**. 在量词$\forall x$ 以及$\exists x$的辖域内, 变元x的一切出现都称为**约束出现**, 此时的变元x称为**约束变元**. 若**辖域**中变元不是约束出现, 则称它为**自由出现**, 此时的变元称为**自由变元**.

back

2.2约束

例 2.3

指出下列谓词公式中的约束变元、自由变元, 及量词的辖域
(1) $(\exists x)F(x) \wedge G(x,y)$.
(2) $(\forall x)(F(x) \rightarrow (\exists y)G(x,y))$.

解:
在(1)中, 存在量词$(\exists x)$的辖域为$F(x)$, $F(x)$中的x为约束出现, 是约束变元, $G(x,y)$中的变元x, y不受任何量词的限制, 它们的出现均为自由出现, 是自由变元.
在(2)中, 全称量词$(\forall x)$的辖域为$(F(x) \rightarrow (\exists y)G(x,y))$, 此辖域内的变元$x$均为约束出现, 是约束变元. 存在量词$(\exists y)$的辖域为$G(x,y)$, 此辖域内的变元$x$, y均是约束变元.

back

2.2约束

定义 2.8

设A是任意的逻辑公式，若A中所有的变元均是约束变元，则称A 为**封闭的式子**，简称为**闭式**.

易知，例2.3中的(1)式不是闭式，而(2)式是闭式.
例2.3中的(1)式中的同一个变元(如x)，既是约束出现，又是自由出现. 为了避免混淆，使公式看上去在结构和形式上统一，在同一个式子中，我们可以通过**换名规则和代替规则**将表达不同含义的个体变元用不同的变量符号来进行表示.

back

2.2约束

首先引入两个规则.

规则1：换名规则(公式中约束变元符号的换名)需遵守如下规则：

(1) 将量词中的变元, 以及该量词辖域内此变元的所有约束出现位置处, 都用新的变元符号替换.

(2) 新的换名符号一定是量词辖域内未出现过的某变项符号.

只有按照此换名规则, 约束变元的换名才是正确, 有效的, 否则是错误的.

2.2约束

公式中的自由变元也允许更换, 自由变元的更换亦要遵守一定的规则, 这一规则被称为代替规则.

规则2: 代替规则(公式中自由变元的代替)需遵守如下规则:

(1) 将公式中该自由变元的每一位置处, 都用新的变元符号替换.

(2) 新的代替变元符号一定是在公式中未出现过的变项符号.

只有按照此代替规则, 自由变元的替换才是正确, 有效的, 否则是错误的.

2.2约束

例 2.4

将公式$\forall xP(x,y,z) \to \exists yQ(x,y,z)$进行等值变换，使其不含既约束出现又自由出现的个体变项.

解：公式中的变元x,y都同时是约束变元和自由变元，可以使用换名规则以及代替规则来解决这种问题.

$\forall xP(x,y,z) \to \exists yQ(x,y,z)$
$\Leftrightarrow \forall uP(u,y,z) \to \exists yQ(x,y,z)$(换名规则)
$\Leftrightarrow \forall u(P(u,y,z) \to \exists vQ(x,v,z)$(换名规则)

也可以采用代替规则解决问题.

$\forall xP(x,y,z) \to \exists yQ(x,y,z)$
$\Leftrightarrow \forall x(P(x,u,z) \to \exists yQ(x,y,z)$(代替规则)
$\Leftrightarrow \forall x(P(x,u,z) \to \exists yQ(v,y,z)$(代替规则)

back

2.2约束

对于给定的现实问题, 通过谓词逻辑符号化为谓词公式; 反之, 对于给定的谓词公式, 它所表达的是何种含义? 这涉及到谓词逻辑的解释问题. 在命题逻辑的解释过程中, 只需要对命题公式内的变元进行赋值, 即可判断该公式的真假. 然而, 在谓词逻辑中, 由于引入了量词、谓词等内容, 情况将变得很复杂. 它需要对谓词公式中的每一个常量项、变量项、函数项以及谓词变项一一赋值, 这就是**谓词公式的解释**. 下面介绍其定义.

2.2约束

定义 2.9

谓词公式A中的**解释**I由如下四部分构成：
(1) 非空的个体域集合D;
(2) 对公式A中的每一常量符号，用一个D中的元素进行指派；
(3) 对公式A中的每一函数变项符号，用D中的某个函数进行指派；
(4) 对公式A中的每一谓词符号，用D中的某个特定的谓词进行指派.

2.2约束

例 2.5

给定如下解释I:
(1) D=实数集R;
(2) D上的特定元素$a=2$;
(3) D上的函数$f(x,y)=x-y$;
(4) D上的谓词$F(x,y)=x<y$;

在解释I下求下式的真值情况.
(1) $(\forall x)F(f(a,x),a)$.
(2) $(\forall x)(\forall y)\neg F(f(x,y),x)$.

back

2.2约束

解:
(1) 因为在解释I下, 对实数集R中任意的x及个体常项a,有$f(a,x) = a - x$, 以及$F(f(a,x),a) = (a - x) < a$, 成立.
将$a = 2$代入, 得$(2 - x) < 2$, 即$-x < 0$, 显然为假, 所以$(\forall x)F(f(a,x),a)$, 取值为0.
(2) 因为在解释I下, 对实数集R中任意的x, y, $F(f(x,y),x) = (x - y) < x$, $\neg F(f(x,y),x) = (x - y) \geq x$为假,
所以, $(\forall x)(\forall y)\neg F(f(x,y),x)$真值为0.

2.3谓词公式中的永真式

同命题公式类似, 在谓词逻辑中, 公式之间也存在相互等价的关系.

定义 2.10

设F与G是谓词逻辑中的任意两个公式, 若$F \leftrightarrow G$是永真式, 则称F与G等价, 记作$F \Leftrightarrow G$.

按照定义, 判断两公式F与G是否为等价式在于判断公式$F \leftrightarrow G$是否为永真式.

back

2.3谓词公式中的永真式

同命题逻辑的等值式判定一样, 人们也给出了一些重要的谓词公式等值式.

1. **量词消去等值式.**

设个体域为有限域$D = \{a_1, a_2, \cdots a_n\}$, 则有

(1) $\forall x F(x) \Leftrightarrow F(a_1) \wedge F(a_2) \wedge \cdots \wedge F(a_n)$.

(2) $\exists x F(x) \Leftrightarrow F(a_1) \vee F(a_2) \vee \cdots \vee F(a_n)$.

2. **量词否定等值式.**

(1) $\neg \forall x F(x) \Leftrightarrow \exists x \neg F(x)$

(2) $\neg \exists x F(x) \Leftrightarrow \forall x \neg F(x)$

back

2.3谓词公式中的永真式

上述的量词否定等值式可做如下解释: (1)式可以理解为"并不是所有的x都具有特性F", 等值于"存在x不具备特性F". (2)式"不存在具有特性F 的x" 等值于"所有的x都不具备特性F".

3. 量词辖域收缩与扩张等值式.

设公式$F(x)$含有个体变项x, G中不含个体变项x.

(1).

$$\forall x(F(x) \vee G) \Leftrightarrow \forall x F(x) \vee G$$

$$\forall x(F(x) \wedge G) \Leftrightarrow \forall x F(x) \wedge G$$

$$\forall x(F(x) \rightarrow G) \Leftrightarrow \exists x F(x) \rightarrow G$$

$$\forall x(G \rightarrow F(x)) \Leftrightarrow G \rightarrow \forall x F(x)$$

2.3谓词公式中的永真式

(2).

$\exists x(F(x) \vee G) \Leftrightarrow \exists x F(x) \vee G$

$\exists x(F(x) \wedge G) \Leftrightarrow \exists x F(x) \wedge G$

$\exists x(F(x) \rightarrow G) \Leftrightarrow \forall x F(x) \rightarrow G$

$\exists x(G \rightarrow F(x)) \Leftrightarrow G \rightarrow \exists x F(x)$

4. 量词分配等值式.

设$F(x), G(x)$含有个体变项x,则

(1)$\forall x(F(x) \wedge G(x)) \Leftrightarrow \forall x F(x) \wedge \forall x G(x)$

(2)$\exists x(F(x) \vee G(x)) \Leftrightarrow \exists x F(x) \vee \exists x G(x)$

back

2.3谓词公式中的永真式

定义 2.11

设A为任一谓词公式,

1. 若A在其所有解释下, 取值都是真, 则称A是永真式.
2. 若A在其所有解释下, 取值都是假, 则称A是矛盾式.
3. 若存在一种解释使A为真, 则称A是可满足式.

2.3谓词公式中的永真式

例 2.6

判断下列谓词公式的类型

(1) $\forall x(F(x) \to \exists y(G(y) \wedge H(x,y)))$.

(2) $\forall x \forall y((F(x) \wedge G(y)) \to H(x,y))$.

解: (1) 取个体域为全总个体域. 解释I_1 : $F(x)$: x为有理数, $G(y)$: y 为整数, $H(x,y)$: $x < y$.

在I_1下: $\forall x(F(x) \to \exists y(G(y) \wedge H(x,y)))$ 为真命题;

解释I_2 : $F(x), G(y)$同I_1, $H(x,y)$:y整除x.

在I_2下: $\forall x(F(x) \to \exists y(G(y) \wedge H(x,y)))$为假命题, 所以该公式是可满足式.

(2) 该式是一个非永真式的可满足式, 请读者给出一个成真解释和一个成假解释.

2.4谓词公式中的范式

在命题逻辑中，主析取范式和主合取范式为命题公式提供了两种统一、规范的表达形式. 这种规范化的表达方式，为系统化的研究公式的特点起到了重要的作用.
同命题逻辑类似，谓词逻辑中也有规范化的表达形式，这就是**前束范式**.

2.4谓词公式中的范式

定义 2.12

设A为一个谓词逻辑公式, 若A可等值化简为如下形式
$Q_1x_1Q_2x_2\cdots Q_nx_nM$. 其中, $Q_i(1 \leq i \leq n)$为$\exists$量词或者$\forall$量词, 而M中不含量词, 则称A为**前束范式**.

例如,
$\exists xG(x)$, $\forall x\forall y((F(x) \wedge G(y)) \rightarrow H(x,y))$是前束范式;
$\forall x(F(x) \rightarrow \exists y(G(y) \wedge H(x,y)))$不是前束范式.

2.4谓词公式中的范式

定理 2.1

(前束范式存在定理)任一谓词公式都存在与之等值的前束范式.

本定理证明略去.

本定理说明, 任一谓词公式的前束范式都是存在的, 一般情况下由于前束范式中量词的顺序可以不同, 所以前束范式可能不唯一.

2.4谓词公式中的范式

例 2.7

求下列谓词公式的前束范式.
$\exists x(\exists y P(x,y) \vee (\neg \exists y Q(y) \vee R(x)))$

解：$\exists x(\exists y P(x,y) \vee (\neg \exists y Q(y) \vee R(x)))$
$\Leftrightarrow \exists x(\exists y P(x,y) \vee (\forall y \neg Q(y) \vee R(x)))$ (量词否定等值式)
$\Leftrightarrow \exists x(\exists y P(x,y) \vee \forall z \neg Q(z) \vee R(x))$ (换名规则)
$\Leftrightarrow \exists x \exists y \forall z(P(x,y) \vee \neg Q(y) \vee R(x))$(量词辖域的收缩与扩张等值式)

back

2.5谓词推理

与命题逻辑的推理系统类似, 谓词推理也是一种形式化的推理系统.

给定一组前提$A_1, A_2, \cdot, A_k$, 以及结论B的推理形式结构, 依然采用如下的蕴含式形式: $(A_1 \wedge A_2 \wedge \cdots \wedge A_k) \rightarrow B$

若上式为永真式, 则称结论B为前提$A_1, A_2, \cdots, A_k$的 **有效结论**.

在谓词逻辑中, 由于量词和谓词的存在, 证明上述公式为永真式, 要比命题逻辑公式永真式的证明一般要复杂许多.

back

2.5谓词推理

为了有效地构造谓词公式推理系统, 下面给出4个重要的谓词逻辑推理规则, 即量词消去规则和量词引入规则.

1. 全称量词消去规则(简记为UI规则或者UI)

$\forall x P(x) \Rightarrow P(y)$ 或者$\forall x(P(x) \Rightarrow P(c)$

此规则使用时要求:

(1) y为任意的不在$P(x)$中约束出现的个体变元.

(2) c为任意的个体常量.

(3) 用y或者c去替代$P(x)$中的x时一定要全部完成替代.

2. 全称量词引入规则(简记为UG规则或者UG)

$P(y) \Rightarrow \forall x P(x)$

2.5谓词推理

此规则使用时要求:
(1) y为常量时不能使用此规则.
(2) $P(y)$的取值应该为真.
(3) 取代y的x也不能在$P(y)$中约束出现.

3. 存在量词引入规则(简记为EG规则或者EG)

$P(c) \Rightarrow \exists x P(x)$

此规则使用时要求:
(1) c为特定的个体常量.
(2) 取代c的x也不能在$P(c)$中约束出现.

4. 存在量词消去规则(简记为EI规则或者EI)

$\exists x P(x) \Rightarrow P(c)$

back

2.5谓词推理

此规则使用时要求：
(1) c不在$P(x)$中出现.
(2) c为使$P(x)$为真的某一个体常量.
(3) $P(x)$ 中除x外还有其它自由变元时, 此规则不能使用.
这四个规则非常重要, 其作用是在证明过程中, 可以首先使用EI以及UI规则将谓词逻辑中的量词消去, 此时就可以采用命题逻辑的推理方案来解决谓词逻辑的推理问题, 最后采用EG以及UG规则, 将量词添加. 以此, 达到了使用命题逻辑推理解决谓词逻辑推理的目的.

2.5谓词推理

例 2.8

构造下面推理的证明. 前提：$\forall x(P(x) \to Q(x)), \exists x P(x)$
结论：$\exists x Q(x)$

证明：
(1)$\exists x P(x)$； 前提引入
(2)$P(c)$； (1)EI规则
(3)$\forall x(P(x) \to Q(x))$； 前提引入
(4)$P(c) \to Q(c)$； (3)UI规则
(5)$G(c)$； (2)(4)假言推理
(6)$\exists x P(x)$； (5)EG规则

back

2.5谓词推理

例 2.9

利用谓词推理, 求解经典苏格拉底三段论问题"凡人都是要死的, 苏格拉底是人, 所以苏格拉底是要死的"
设$H(x)$:x是人; $M(x)$:x是要死的; c:苏格拉底.
前提: $\forall x(H(x) \to M(x)), H(c)$
结论: $M(c)$

证明:
(1)$H(c)$; 前提引入
(2)$\forall x(H(x) \to M(x))$; 前提引入
(3)$H(c) \to M(c)$; (2)UI规则
(4)$M(c)$; (1)(3)假言推理

back

目录

3.1基本概念

集合

一般地, 把一些确定的、可以区分的事物放在一起构成的整体称为集合, 简称集.

组成集合的每个事物称为集合的元素（或成员）.

通常我们用大写的英文字母$A, B, C, \cdots$,表示集合; 用小写的英文字母$a, b, c, \cdots$表示集合的元素.

如果元素a属于集合A, 记作$a \in A$, 读作“a属于A”. 如果a不属于A, 记作$a \in A$或$a \notin A$, 读作“a不属于A”.

back

3.1基本概念

列元素法：把集合中的全部元素一一列举出来，元素之间用逗号“,”隔开，并把它们用花括号“{}”括起来.
例如，$A = \{1, 2, 3, 4, 5\}$.
描述法：将集合的元素特性描述出来，例如，方程$x^2 - 1 = 0$的实数解集合可表示为

$$B = \{x | x \in R \wedge (x^2 - 1 = 0)\}$$

文氏图法：多数讨论集合的情况总是将集合局限在某个框架内. 例如，讨论的集合总是实数集合的一部分，某些英文字母集合总是全部26个英文字母集的一部分. 这里的全体实数组成的集合和全部26个英文字母集叫做全集. 在文氏图中全集用长方形表示. 在长方形内部，圆或其他几何图形用于表示集合，有时用点表示集合中特定的元素.

back

3.1基本概念

(1) 组成一个集合的各个元素之间是彼此不同的, 如果同一个元素在集合中多次出现应该认为是一个元素.
例如,$\{1,1,2,2,4\}=\{1,2,4\}$.
(2) 集合的元素是无序的. 例如, $\{1,2,3\}=\{2,3,1\}$.
(3) 任一元素是否属于一个集合, 回答是确定的.
(4) 集合的元素可以是任何事物, 元素之间通常有联系, 但不是必然的.
例如, $\{a,\{1,2\},p,\{q\}\}$
(5) 元素和集合之间的关系是隶属关系, 即属于或不属于.

back

3.2集合间的关系

子集

定义 3.1

设A, B是任意两个集合, 如果A中的每一个元素都是B中的元素, 则称A是B的子集合, 简称子集. 也称A被B包含, 或B包含A . 记作$A \subseteq B$或$B \supseteq A$.

包含的符号化表示为

$$A \subseteq B \Leftrightarrow \forall x(\ x \in A \rightarrow\ x \in B)$$

如果A不被B包含, 则记作$A \nsubseteq B$, 符号化表示为

$$A \nsubseteq B \Leftrightarrow \exists x(\ x \in A \wedge\ x \notin B)$$

back

3.2集合间的关系

例如,$A = \{a, b\}$,$B = \{a, b, c\}$,$C = \{b, c, d\}$,则有$A \subseteq B$,,但$A \nsubseteq C$,.

注意符号“$\in$”和“$\subseteq$”的区别:

“$\in$”表示元素与集合间的“属于”关系,“$\subseteq$”表示集合间的“包含”关系.

3.2集合间的关系

集合相等

定义 3.2

设A, B是两个集合, 如果$A \subseteq B$且$B \subseteq A$, 则称A与B相等, 记作$A = B$.

符号化表示为

$$A = B \Leftrightarrow A \subseteq B且B \subseteq A$$

如果A与B不相等, 则记作$A \neq B$.
该定义给出了一个重要原则: 要证明两个集合相等, 唯一的方法就是证明每一个集合中的任一元素均是另一个集合的元素.

back

3.2集合间的关系

真子集

定义 3.3

设A, B是两个集合, 如果A是B的子集, 而B中至少有一元素不属于A, 则称A为B的真子集, 记作$A \subset B$.

符号化表示为

$$A \subset B \Leftrightarrow \forall x(x \in A \rightarrow x \in B) \wedge \exists x(x \in A \wedge x \notin B)$$

或$A \subset B \Leftrightarrow A \subseteq B \wedge A \neq B$

如果A不是B的真子集, 则记作$A \not\subset B$.
例如, 集合$\{a,b\}$是$\{a,b,c\}$的真子集, 但$\{a,b,c\}$和$\{b,c,d\}$都不是$\{a,b,c\}$的真子集

back

3.2集合间的关系

空集

定义 3.4

不含任何元素的集合叫做空集, 记作$\varnothing$.

空集的符号化表示为

$$\varnothing = \{x | \ x \neq x\}$$

例如, $A = \{x | x \in R \wedge x^2 + 2 = 0\}$是方程$x^2 + 2 = 0$的实数解集, 因为该方程无实数解, 所以$A = \varnothing$.

注意: $\varnothing \neq \{\varnothing\}$.

back

3.2集合间的关系

定理 3.1

对于任意集合A, 有
(1)$\varnothing \subseteq A$, 且空集是唯一的; (2)$A \subseteq A$.

证明: (1)假设$\varnothing \subseteq A$为假, 则至少存在一个元素x, 使$x \in \varnothing$且$x \notin A$, 因为空集$\varnothing$不包含任何元素, 所以这是不可能的. 设$\varnothing_1$与$\varnothing_2$都是空集, 由上述可知, $\varnothing_1 \subseteq \varnothing_2$且$\varnothing_2 \subseteq \varnothing_1$, 根据集合相等的定义得$\varnothing_1 = \varnothing_2$, 所以, 空集是唯一的.
(2)根据子集的定义可得, 对于任意集合A, 有$A \subseteq A$.

back

3.2集合间的关系

定义 3.5

含有n个元素的集合叫n元集.

n元集合的有$m\,(m \leq n)$ 个元素的子集叫m元子集.
给定n元集合, 如何求出它的全部子集呢?

例 3.1

$A = \{1, 2, 3\}$, 将A的子集分类:
0元子集, 也就是空集, 只有一个: $\varnothing$;
1元子集, 即单元集: $\{1\}, \{2\}, \{3\}$;
2元子集: $\{1, 2\}, \{1, 3\}, \{2, 3\}$;
3元子集: $\{1, 2, 3\}$.

back

3.3集合的运算

一般的, 对于n元集, 它的m元子集有C_n^m个, 所以不同的子集总数是
$C_n^0 + C_n^1 + C_n^2 + ,C_n^n = 2^n$.

定义 3.6

设A, B是任意两个集合, 由A或B中的元素构成的集合, 称为集合A与B的并集, 记作$A \cup B$.

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

例如, $A = \{1, 2, 4\}$, $B = \{2, 4, 5\}$, 则 $A \cup B = \{1, 2, 4, 5\}$.

back

3.3集合的运算

并集的概念可以推广.

设$A_1, A_2, \cdots, A_n$是任意n个集合, 则这n个集合的并可简记为$\bigcup_{i=1}^{n} A_i$, 即

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n = \{x \mid x \in A_1 \vee x \in A_2 \vee \cdots \vee x \in A_n\}$$

并运算还可以推广到无穷多个集合的情况:

$$\bigcup_{i=1}^{\infty} A_i = A_1 \cup A_2 \cup \cdots \cup A_n \cup \cdots$$

back

3.3集合的运算

交集

定义 3.7

设A, B是任意两个集合, 由既在A中又在B中的元素构成的集合, 称为集合A与B的交集, 记作$A \cap B$.

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

如果两个集合A, B的交集为空集, 则称A, B不相交.
例如, $A = \{1, 2, 4\}, B = \{2, 4, 5\}, C = \{1, 3\}$,
则 $A \cap B = \{2, 4\}, B \cap C = \varnothing$, 所以$B$和$C$是不相交的.

back

3.3集合的运算

推广:

设$A_1, A_2, \cdots, A_n$是任意n个集合, 则这n个集合的交可简记为$\bigcap_{i=1}^{n} A_i$, 即

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \cdots \cap A_n = \{x \mid x \in A_1 \wedge x \in A_2 \wedge \cdots \wedge x \in A_n\}$$

交运算还可以推广到无穷多个集合的情况:

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

back

3.3集合的运算

相对补集

定义 3.8

设A, B是任意两个集合，由只属于集合A而不属于B的所有元素构成的集合，称为集合B对于A的相对补集（或A和B的差集），记作$A - B$.

$$A - B = \{x | x \in A \wedge x \notin B\}$$

例如，$A = \{1, 2, 4\}, B = \{2, 4, 5\}$,
则 $A - B = \{1\}, B - A = \{5\}$.

back

3.3集合的运算

绝对补集

定义 3.9

设E为全集, $A \subseteq E$, 则称集合A对于E的相对补集为A的绝对补集, 记作$\sim A$.

$$\sim A = E - A = \{x | \, x \in E \wedge \, x \notin A\}$$

例如, $E = \{1,2,3,4,5\}$, $A = \{1,2,4\}$, $B = \{1,2,3,4,5\}$, $C = \varnothing$,
则 $\sim A = \{3,5\}$, $\sim B = \varnothing$, $\sim C = E$.

back

3.3集合的运算

对称差

定义 3.10

设A, B是任意两个集合, 由属于集合A但不属于B或者属于集合B但不属于A的所有元素构成的集合, 称为集合A与B的对称差, 记作$A \oplus B$.

$$A \oplus B = \{x | (x \in A \wedge x \notin B) \vee (x \notin A \wedge x \in B)\}$$

或$A \oplus B = (A - B) \cup (B - A)$

例如, $A = \{a, b, c\}$, $B = \{b, d\}$, 则 $A \oplus B = \{a, c, d\}$.
从对称差定义容易看出

$$A \oplus B = (A \cup B) - (A \cap B)$$

3.3集合的运算

设A, B, C为任意三个集合, 对称差运算有以下性质:

(1) $A \oplus B = B \oplus A$;

(2) $A \oplus \varnothing = A$;

(3) $A \oplus A = \varnothing$;

(4) $A \oplus B = (A \cap \sim B) \cup (\sim A \cap B)$;

(5) $(A \oplus B) \oplus C = A \oplus (B \oplus C)$;

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

back

3.3集合的运算

集合的运算律

(1)幂等律 $A \cup A = A, A \cap A = A.$

(2)交换律 $A \cup B = B \cup A, A \cap B = B \cap A.$

(3)结合律 $(A \cup B) \cup C = A \cup (B \cup C),$
$(A \cap B) \cap C = A \cap (B \cap C).$

(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)吸收律 $A \cup (A \cap B) = A, A \cap (A \cup B) = A.$

(6)同一律 $A \cup \varnothing = A, A \cap E = A.$

(7)零律 $A \cup E = E, A \cap \varnothing = \varnothing.$

(8)排中律 $A \cup \sim A = E.$

(9)矛盾律 $A \cap \sim A = \varnothing.$

back

3.3集合的运算

(10)余补律 $\sim \varnothing = E, \sim E = \varnothing.$

(11)双重否定律 $\sim (\sim A) = A.$

(12)补交转换律 $A - B = A \cap \sim B.$

(13)德·摩根律 $\sim (A \cup B) = \sim A \cap \sim B,$

$\sim (A \cap B) = \sim A \cup \sim B;$

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

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

back

3.3集合的运算

证明集合等式常用的方法

（1）逻辑公式等值演算法. 证明的关键是要灵活运用逻辑基本等值式和集合运算的性质.

基本思想: 设P, Q为集合公式, 根据集合相等的定义, 要证$P = Q$, 只需证 $P \subseteq Q \wedge Q \subseteq P$为真.

也就是要证对于任意的x有

$$x \in P \Leftrightarrow x \in Q.$$

（2）恒等代换法. 该方法的实质就是利用集合运算的性质和已知的集合恒等式, 把一个集合用与之相等的集合代换, 从而完成证明.

back

3.3集合的运算

例 3.2

利用等值演算的方法证明下列恒等式:

（1）分配律: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;

（2）排中律: $A \cup \sim A = E$;

（3）德·摩根律: $\sim (A \cup B) = \sim A \cap \sim B$.

证明 （1）对于任意的x,

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

3.3集合的运算

（2）对于任意的x,

$$
\begin{aligned}
& x \in A \cup \sim A \\
\Leftrightarrow\ & x \in A \vee x \in \sim A \\
\Leftrightarrow\ & x \in A \vee x \notin A \\
\Leftrightarrow\ & x \in A \vee \neg x \in A \\
\Leftrightarrow\ & 1 \\
\Leftrightarrow\ & x \in E
\end{aligned}
$$

所以, $A \cup \sim A = E$.

3.3集合的运算

（3）对于任意的x,

$$
\begin{aligned}
& x \in \sim (A \cup B) \\
\Leftrightarrow\ & x \notin (A \cup B) \\
\Leftrightarrow\ & (x \notin A) \wedge (x \notin B) \\
\Leftrightarrow\ & (x \in \sim A) \wedge (x \in \sim B) \\
\Leftrightarrow\ & x \in (\sim A \cap \sim B)
\end{aligned}
$$

所以, $\sim (A \cup B) = \sim A \cap \sim B$.

3.3集合的运算

例 3.3

利用恒等代换的方法证明吸收律

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

back

3.3集合的运算

关于集合运算性质的一些重要结果

(14) $A \cap B \subseteq A, A \cap B \subseteq B.$

(15) $A \subseteq A \cup B, B \subseteq A \cup B.$

(16) $A - B \subseteq A.$

(17) $A \subseteq B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B \Leftrightarrow A - B = \varnothing.$

back

3.3集合的运算

例 3.4

证明 $A-(B-C)=(A-B)\cup(A\cap C)$

证明 方法一: 对于任意的x,

$$
\begin{aligned}
& x\in A-(B-C)\\
\Leftrightarrow\ & x\in A\wedge x\notin(B\cap\sim C)\\
\Leftrightarrow\ & x\in A\wedge x\in\sim(B\cap\sim C)\\
\Leftrightarrow\ & x\in A\wedge x\in(\sim B\cup C)\\
\Leftrightarrow\ & x\in A\wedge(x\in\sim B\vee x\in C)\\
\Leftrightarrow\ & x\in A\wedge(x\notin B\vee x\in C)\\
\Leftrightarrow\ & (x\in A\wedge x\notin B)\vee(x\in A\wedge x\in C)\\
\Leftrightarrow\ & x\in(A-B)\cup(A\cap C)
\end{aligned}
$$

所以, $A-(B-C)=(A-B)\cup(A\cap C)$.

3.3集合的运算

方法二: $A-(B-C)$
$=A\cap\sim(B\cap\sim C)$
$=A\cap(\sim B\cup C)$
$=(A\cap\sim B)\cup(A\cap C)$
$=(A-B)\cup(A\cap C)$

back

3.3集合的运算

例 3.5

设集合A, B满足条件$A \cap B = \varnothing, A \cup B = E$, 证明 $A = \sim B$.

证明
$$\begin{aligned} A &= A \cap E \\ &= A \cap (B \cup \sim B) \\ &= (A \cap B) \cup (A \cap \sim B) \\ &= \varnothing \cup (A \cap \sim B) \\ &= (B \cap \sim B) \cup (A \cap \sim B) \\ &= (B \cup A) \cap \sim B \\ &= E \cap \sim B \\ &= \sim B \end{aligned}$$

back

3.3集合的运算

例 3.6

化简下列集合表达式.

（1）$(B-(A\cap C))\cup(A\cap B\cap C)$;

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

解: （1）$(B-(A\cap C))\cup(A\cap B\cap C)$

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

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

$=B\cap E$

$=B$

back

3.3集合的运算

(2) 因为$A \cup B \subseteq A \cup B \cup C, A \subseteq A \cup (B - C)$, 则有

$$
\begin{aligned}
&((A \cup B \cup C) \cap (A \cup B)) - ((A \cup (B - C) \cap A) \\
&= (A \cup B) - A \\
&= (A \cup B) \cap \sim A \\
&= (A \cap \sim A) \cup (B \cap \sim A) \\
&= \varnothing \cup (B \cap \sim A) \\
&= B - A
\end{aligned}
$$

back

3.4包含排斥原理

包含排斥原理

定义 3.11

设集合$A=\{a_1,a_2,\cdots,a_n\}$, 它有n个不同元素, 则称集合A的基数是n, 记作$CardA=n$ 或$|A|=n$.

基数是表示集合中所含元素多少的量.
如果集合A的基数是n, 这时称A为有限集.
显然, 空集的基数是0, 即$|\varnothing|=0$.
如果A不是有限集, 则称A为无限集.

back

3.4包含排斥原理

定理 3.2

（包含排斥原理）设A, B为有限集合, 则

$$|A \cup B| = |A| + |B| - |A \cap B|$$

包含与排斥原理也称为容斥原理.

证明 （1）当A、B不相交, 即$A \cap B = \varnothing$ 时, 有 $|A \cup B| = |A| + |B|$.
（2）当$A \cap B \neq \varnothing$时, 不妨设$A \cap B = \{a_1, a_2, \cdots, a_k\}$,
$A = \{a_1, a_2, \cdots, a_k, x_1, x_2, \cdots, x_n\}$, $B = \{a_1, a_2, \cdots, a_k, y_1, y_2, \cdots, y_m\}$,
则$|A| + |B| - |A \cap B| = n + k + m + k - k$,
$|A \cup B| = n + m - k$,
从而, $|A \cup B| = |A| + |B| - |A \cap B|$.
综上所述, 可知 $|A \cup B| = |A| + |B| - |A \cap B|$.

3.4包含排斥原理

例 3.7

假设50名青年中有16名是工人, 21名是学生, 其中既是工人又是学生的青年有4名, 问既不是工人又不是学生的青年的有几名?

解: 设E为50名青年组成的集合, A为工人组成的集合, B 为学生组成的集合, 则

$|E| = 50, |A| = 16, |B| = 21, |A \cap B| = 4$

根据包含排斥原理, 有

$|A \cup B| = |A| + |B| - |A \cap B| = 16 + 21 - 4 = 33$

$|E| - |A \cup B| = 50 - 33 = 17$

所以, 既不是工人又不是学生的青年的有17名.

back

3.4包含排斥原理

定理 3.3

（包含排斥原理的推广）A中至少具有n个性质之一的元素个数为

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n+1} |A_1 \cap A_2 \cap \cdots \cap A_n|$$

其中，有限集A的元素具有n个不同的性质P_1，P_2，$\cdots$，P_n．A中具有性质P_i的元素组成的子集记为A_i，$i = 1, 2, \cdots, n$；$A_i \cap A_j (i \neq j)$表示A中同时具有性质P_i和P_j的元素组成的子集；$A_i \cap A_j \cap A_k (i \neq j \neq k)$表示$A$中同时具有性质$P_i$，$P_j$和$P_k$的元素组成的子集；$\cdots$；$A_1 \cap A_2 \cap \cdots \cap A_n$表示$A$中同时具有性质$P_1$，$P_2$，$\cdots$，$P_n$的元素组成的子集．

3.4包含排斥原理

例 3.8

设X是由从1到250的正整数构成的集合，X中有多少个元素能被2、3、7中的任意一个整除？

解： 设A, B, C分别表示X中能被2、3、7整除的正整数构成的集合，则

$$|A| = \left\lfloor \frac{250}{2} \right\rfloor = 125, |B| = \left\lfloor \frac{250}{3} \right\rfloor = 83, |C| = \left\lfloor \frac{250}{7} \right\rfloor = 35,$$

$$|A \cap B| = \left\lfloor \frac{250}{2\times 3} \right\rfloor = 41, |A \cap C| = \left\lfloor \frac{250}{2\times 7} \right\rfloor = 17, |B \cap C| = \left\lfloor \frac{250}{3\times 7} \right\rfloor = 11,$$

$$|A \cap B \cap C| = \left\lfloor \frac{250}{2\times 3\times 7} \right\rfloor = 5,$$

根据包含排斥原理，有

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$
$$= 125 + 83 + 35 - 41 - 17 - 11 + 5 = 179$$

所以，X中能被2、3、7中的任意一个整除的正整数有179个.

3.4包含排斥原理

借助文氏图解决有限集合的计数问题.
首先根据已知条件画出相应的文氏图. 一般地说, 每一条性质决定一个集合, 有多少条性质, 就有多少个集合. 如果没有特殊说明, 任何两个集合一般都画成相交的. 通常从n个集合的交集填起, 根据计算的结果将数字逐步填入所有的空白区域. 如果交集的数字是未知的, 可以设为x. 根据题目中的条件, 列出相应的方程或方程组, 解出未知数即可求得所需要的结果.

back

3.4包含排斥原理

例 3.9

在30个学生中有18个爱好音乐, 12个爱好美术, 15个爱好体育, 10个既爱好音乐又爱好体育, 8个既爱好美术又爱好体育, 11个既爱好音乐又爱好美术, 但有6个学生这三种爱好都没有. 试求这三种爱好都有的人数.

解: 设A, B, C分别表示爱好音乐、美术、体育的学生的集合. 设三种爱好都有的学生人数为x, 仅爱好音乐的学生人数为y_1, 仅爱好美术的学生人数为y_2, 仅爱好体育的学生人数为y_3, 则既爱好音乐又爱好体育, 但不爱好美术的学生人数为$10-x$, 既爱好美术又爱好体育, 但不爱好音乐的学生人数为$8-x$, 既爱好音乐又爱好美术, 但不爱好体育的学生人数为$11-x$,

3.4包含排斥原理

根据题意, 有

$$\begin{cases} 11-x+10-x+x+y_1=18 \\ 11-x+8-x+x+y_2=12 \\ 10-x+8-x+x+y_3=15 \\ 11-x+10-x+8-x+x+y_1+y_2+y_3+6=30 \end{cases}$$

解得 $x=8, y_1=5, y_2=1, y_3=5$

所以, 三种爱好都有的人数为8人.

3.5幂集合与笛卡尔乘积

幂集合

定义 3.12

设A为一个集合，由A的所有子集为元素构成的集合，称为A的幂集合，简称幂集，记作$P(A)$(或2^A). 符号化表示为

$$P(A) = \{x | x \subseteq A\}$$

back

3.5幂集合与笛卡尔乘积

例 3.10

设$A=\varnothing, B=\{1,3,5\}, C=\{1,\{2,3\}\}$. 求$A, B$和$C$的幂集.

解: 集合$A=\varnothing$, 它只有0元子集$\varnothing$,
所以, $P(A)=\{\varnothing\}$.
集合B的0元子集为: $\varnothing$;
1元子集为: $\{1\}, \{3\}, \{5\}$;
2元子集为: $\{1,3\}, \{1,5\}, \{3,5\}$;
3元子集为: $\{1,3,5\}$.
所以, $P(B)=\{\varnothing,\{1\},\{3\},\{5\},\{1,3\},\{1,5\},\{3,5\},\{1,3,5\}\}$.
同理可求, $P(C)=\{\varnothing,\{1\},\{\{2,3\}\},\{1,\{2,3\}\}\}$.

back

3.5幂集合与笛卡尔乘积

例 3.11

设$|A| = n$. 求A的幂集$P(A)$中所包含元素的个数.

解:

A的没有元素的子集是空集$\varnothing$子集, 有C_n^0 个;
A的1子集有C_n^1个;
$\vdots$
A的n子集有C_n^n个;

故$|P(A)| = C_n^0 + C_n^1 + C_n^2 + \cdots + C_n^n = 2^n$.

3.5幂集合与笛卡尔乘积

例 3.12

设A, B为任意集合, 证明

（1）$A \subseteq B \Leftrightarrow P(A) \subseteq P(B)$;

（2）$P(A) = P(B) \Leftrightarrow A = B$.

证明: (1)

左$\Rightarrow$ 右:

任给x, $x \in P(A) \Rightarrow x \subseteq A \Rightarrow x \subseteq B \Rightarrow x \in P(B) \Rightarrow P(A) \subseteq P(B)$.

右$\Rightarrow$ 左:

$A \in P(A) \subseteq P(B) \Rightarrow A \in P(B) \Rightarrow A \subseteq B$.

(2) 根据(1)可证.

3.5幂集合与笛卡尔乘积

笛卡尔积

定义 3.13

将两个元素x和y（x与y可以为同一个元素）用一对尖括号(也可以用圆括号)括起来，表示成$< x, y >$，叫做一个有序对，也叫序偶. 其中x称为有序对$< x, y >$的第一元素，y称为有序对$< x, y >$的第二元素.

定义 3.14

若两个序对的第一元素与第一元素，第二元素与第二元素分别相等，则称两个序对相等，否则称为不相等.

back

3.5幂集合与笛卡尔乘积

根据定义, 我们有

（1）当$x \neq y$时, $< x, y > \neq < y, x >$;
（2）$< x, y > = < u, v >$的充要条件是$x = u$且$y = v$.

序对也叫2元组. 类似地可以定义3元组, $\cdots$, n元组等等, 这里不再赘述.

back

3.5幂集合与笛卡尔乘积

定义 3.15

设A, B为任意两个集合, 由A中元素为第一元素, B中元素为第二元素的所有有序对构成的集合称为A和B的笛卡尔积, 记作$A \times B$. A和B的笛卡尔积记作

$$A \times B = \{< x, y > | x \in A \wedge y \in B\}$$

back

3.5幂集合与笛卡尔乘积

例如, $A=\{1,2,3\}$, $B=\{a,b\}$, 则

$$A\times B=\{<1,a>,<1,b>,<2,a>,<2,b>,<3,a>,<3,b>\}$$
$$B\times A=\{<a,1>,<a,2>,<a,3>,<b,1>,<b,2>,<b,3>\}$$
$$A\times A=\{<1,1>,<1,2>,<1,3>,<2,1>,<2,2>,<2,3>,<3,1>,<3,2>,<3,3>\}$$
$$B\times B=\{<a,a>,<a,b>,<b,a>,<b,b>\}$$

back

3.5幂集合与笛卡尔乘积

定义 3.16

设$A_1, A_2, \cdots, A_n$为任意n个集合, 称集合

$$A_1 \times A_2 \times \cdots \times A_n = \{< x_1, x_2, \cdots, x_n > | x_i \in A_i, 1 \leq i \leq n\}$$

为$A_1, A_2, \cdots, A_n$的笛卡尔积.

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

back

3.5幂集合与笛卡尔乘积

根据笛卡尔积的定义, 有

（1）笛卡尔乘积运算不满足交换律. 即一般情况下$A \times B \neq B \times A$;

（2）对任意集合A, B, 有$A \times \varnothing = \varnothing \times B = \varnothing$;

（3）笛卡儿积运算对并和交运算满足分配律, 即

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

back

3.5幂集合与笛卡尔乘积

例 3.13

设A, B, C为任意集合, 判断以下命题是否为真并说明理由.

（1）$A \times B = A \times C \Rightarrow B = C$;

（2）$A - (B \times C) = (A - B) \times (B - C)$;

（3）存在集合A, 使得$A \subseteq A \times A$.

解: （1）不一定为真.

当$A = \varnothing, B = \{1\}, C = \{2\}$时, 有$A \times B = A \times C$, 但$B \neq C$.

back

3.5幂集合与笛卡尔乘积

（2）不一定为真.
当$A=B=\{1\}, C=\{2\}$时, 有$A-(B\times C)=\{1\}-\{<1,2>\}=\{1\}$,
$(A-B)\times(B-C)=\varnothing\times\{1\}=\varnothing$

(3)为真.
当$A=\varnothing$时, $A\subseteq A\times A$成立.

back

3.6集合运算与基数概念的扩展

广义并集

定义 3.17

设$\mathcal{A}$为一个集合族, 由$\mathcal{A}$中所有元素的元素构成的集合称为$\mathcal{A}$的广义并集, 记为$\cup\mathcal{A}$. 符号化表示为

$$\cup\mathcal{A} = \{x|\exists z(\ z \in \mathcal{A} \wedge x \in z)\}$$

back

3.6集合运算与基数概念的扩展

例 3.14

设$\mathcal{A}_1 = \{\{a,b,d\},\{c,d\},\{d,e,f\}\}$, $\mathcal{A}_2 = \{b,\{c,d\}\}$, $\mathcal{A}_3 = \{\{a,b\}\}$, $\mathcal{A}_4 = \varnothing$, 求它们的广义并集.

解: $\cup\mathcal{A}_1 = \{a,b,c,d,e,f\}$

$\cup\mathcal{A}_2 = b \cup \{c,d\}$

$\cup\mathcal{A}_3 = \{a,b\}$

$\cup\mathcal{A}_4 = \varnothing$

back

3.6集合运算与基数概念的扩展

广义交集

定义 3.18

设$\mathcal{A}$为一个非空集合族, 由$\mathcal{A}$中所有元素的公共元素构成的集合称为$\mathcal{A}$的广义交集, 记为$\cap\mathcal{A}$. 符号化表示为

$$\cap\mathcal{A} = \{x|\forall z(\ z \in \mathcal{A} \rightarrow x \in z)\}$$

对于例6.1中的集合, 有$\cap\mathcal{A}_1 = \{d\}$, $\cap\mathcal{A}_2 = b \cap \{c,d\}$, $\cap\mathcal{A}_3 = \{a,b\}$. 因为$\cap\varnothing$不是集合, 它在集合论中是没有意义的.

back

3.6集合运算与基数概念的扩展

集合运算的优先顺序:
称广义并、广义交、幂集、绝对补运算为一类运算, 并、交、相对补、对称差运算为二类运算.

一类运算优先于二类运算; 一类运算之间按由右向左顺序进行运算; 二类运算之间由括号决定运算的先后顺序, 多个括号并排或无括号部分按由左向右的顺序进行运算.

back

3.6集合运算与基数概念的扩展

例 3.15

设$\mathcal{A}=\{\{a,b\},\{a,c\}\}$, 计算$\cup\cup\mathcal{A}$, $\cap\cap\mathcal{A}$, $\cup\cup\mathcal{A}-\cup\cap\mathcal{A}$.

解: $\cup\mathcal{A}=\{a,b,c\}$

$\cap\mathcal{A}=\{a\}$

$\cup\cup\mathcal{A}=a\cup b\cup c$

$\cap\cap\mathcal{A}=a$

$\cup\cap\mathcal{A}=a$

$\cup\cup\mathcal{A}-\cup\cap\mathcal{A}=(a\cup b\cup c)-a=(b\cup c)-a$

back

1.6 集合运算和基数概念的扩展

前面对有限集的基数给出了明确的定义。有限集A 的基数就是A中元素的个数。由于无限集中的元素没有个数的概念, 为了给出无限集的基数的定义, 先做些准备。

定义 3.19

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**, 且x映射到y, 记作$y = f(x)$.

当x映射到y时, y叫做x的**像**, x叫做y的**原像**.

1.6 集合运算和基数概念的扩展

定义 3.20

设f是A到B的一个映射，若对任意的$a \in A, b \in A$，当$a \neq b$时，有$f(a) \neq f(b)$，则称映射f是A到B的一个**单映射**，简称**单射**。

back

1.6 集合运算和基数概念的扩展

集合A到集合B的映射只是强调了集合A中的每个元素都有像. 并没有说集合B中的每个元素都有原像. 下面给满足这种情况的映射一个说法.

定义 3.21

设f是A到B的一个映射, 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**满映射**, 简称**满射**.

定义 3.22

A到B的一个映射f既是单射又是满射时, 称f是A到B的**一一映射**或**一一对应**.

back

1.6 集合运算和基数概念的扩展

例 3.16

设$A = \{a_1, a_2, a_3\}$, $B = \{1, 2, 3\}$, 令$\phi(a_i) = i, i = 1, 2, 3.$ 则A与B之间的对应规则ϕ是一一对应. 设$A_1 = \{a_2\}$, 因A_1是A的真子集, A到A_1之间不存在一一对应.

不难看出, 一个有限集合A是不可能与其真子集一一对应的. 而集合A不是有限集的时候, 这个“不可能”情况会发生改变. 见下例.

1.6 集合运算和基数概念的扩展

例 3.17

设
$N = \{0, 1, 2, 3, 4, 5, 6, \cdots\}$,
$Z = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$.
定义N到Z的对应关系ϕ:

N	0	1	2	3	4	5	6	7	$\cdots$
	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\cdots$
Z	0	-1	1	2	-2	3	-3	4	$\cdots$

则可见上述对应关系ϕ使N与Z是一一对应的.

back

1.6 集合运算和基数概念的扩展

按照一一对应的定义, 若两个有限集合A和B之间存在一一对应关系, 可知它们有相同的元素个数, 即相同的基数. 反之, 当两个有限集合有相同的基数时, 它们之间也可以建立一一对应. 因此可以说两个有限集合基数是否相同, 就看它们之间是否可以建立一一对应.

前面学习了有限集合的基数就是集合中元素的个数. 至此, 还是没有明确无限集合的基数是什么? 由于一般的无限集合不好把握, 我们先对一些特殊的无限集合的基数给出一个说法.

back

1.6 集合运算和基数概念的扩展

自然数集合N和实数集R的基数作出以下规定.

(1) 自然数集合N的基数记作$\aleph_0$, 即$|N| = \aleph_0$.
(2) 实数集R的基数记作$\aleph$, 即$|R| = \aleph$.

$\aleph$是希伯来语, 希伯来字母表的第一个字母. 把$\aleph$读作阿列夫, $\aleph_0$ 读作阿列夫零.
一个集合A可以与自然数集合或者实数集合建立一一对应时, 我们就说集合A的基数也是$\aleph_0$或者$\aleph$.

3.6集合运算与基数概念的扩展

从更广泛意义上说, 有

定义 3.23

对于任何集合A和B, 若它们之间能建立一一对应, 则称集合A与集合B 有相同的基数.

back

1.6 集合运算和基数概念的扩展

也可以将两个有限集合的个数可以比较大小这个概念进行推广.

定义 3.24

设A, B是两个集合, 假如A与B的某子集一一对应, 而A不能与B一一对应, 我们说A的基数$|A|$小于B的基数$|B|$, 记作$|A| < |B|$, 或$|B| > |A|$.

符号$|A| \leq |B|$的含义表示$|A| < |B|$或者$|A| = |B|$.

1.6 集合运算和基数概念的扩展

古典集合理论有以下两个著名的结论.

定理 3.4

设A与B为二集合, 则下述情况恰有一个成立.
$|A| < |B|$,
$|A| > |B|$,
$|A| = |B|$.

定理 3.5

设A与B为二集合, 若$|A| \leq |B|$且$|B| \leq |A|$, 则 $|A| = |B|$.

这两个结论看上去都是那么直观, 证明却超出本课程的范围.

back

1.6 集合运算和基数概念的扩展

受自然数集合$\{1,2,\cdots,\}$启发, 给出“可数集”的概念.

定义 3.25

凡是与自然数集N有相同基数的集合称为可数集. 集合A是可数集时, 就称集合A的元素是可数的.

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

$$1,2,3,4,5,\cdots,n,\cdots.$$

因此任何可数集合M也一定可以将其排成无穷序列形式

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

反之, 若一无限集合M, 它的元素可排成上述序列形式, 则M一定是可数的.

1.6 集合运算和基数概念的扩展

关于可数集有：

定理 3.6

任意无穷集合A, 含有一可数集.

证明: 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$A \supseteq A'$.

1.6 集合运算和基数概念的扩展

定理 3.7

可数集的无限子集还是一可数集.

证明: 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N^*是自然数集合N 的一个子集, 而N 的任一子集中的元素都可按其元素的大小排成一列, 故N^* 是一可数集, 从而A^* 是一可数集. 证毕.

还有不少可数集的结论, 如两个可数集的并集是可数集; 可数个可数集的并集还是可数集等等, 这里就不再继续讨论了.

back

目录

4.1 基本概念

定义 4.1

由序对组成的集合(包括空集)称为一个二元关系，简称关系，关系通常用符号R表示.

对于二元关系R:
如果$< x, y > \in R$, 记作xRy, 读作x与y有关系R;
如果$< x, y > \notin R$, 则记作$x\not Ry$, 读作x与y没有关系R.

例 4.1

$R_1 = \{< 1, 2 >, < a, b >\}$, $R_2 = \{< 1, 2 >, a, b\}$, 则R_1是二元关系，R_2不是二元关系. 根据关系的记法有$1R_12$, aR_1b, a与c没有关系R_1 等等.

back

4.1 基本概念

定义 4.2

给定集合A与B, $A \times B$的子集R叫做从A到B的关系. 特别当$A = B$时, A到A的二元关系简称为A上的关系.

集合$\{x|\exists y \in B, < x, y > \in R\}$叫做关系$R$的**前域**, 记作$domR$.

集合$\{y|\exists x \in A, < x, y > \in R\}$叫做关系$R$的**值域**, 记为$rangeR$.

R的前域和值域并集叫作R的**域**, 记作FLD.

从上述符号的加法看出: $domR \subseteq A, rangeR \subseteq B$.

back

4.1 基本概念

例 4.2

$A=\{0,1\}, B=\{1,2,3\}$, 那么 $R_1=\{<0,2>\}, R_2=A\times B$, $R_3=\emptyset$, $R_4=\{<0,1>\}$都是从A到B的二元关系, 而R_3和R_4同时也是A上的二元关系.

例 4.3

$A=\{1,2,3,5\}, B=\{1,2,4\}, H=\{<1,2>,$
$<1,4>,<2,4>,<3,4>\}$, 求: $domH, rangeH, FLDH$.

解:

back

4.1 基本概念

一个集合A上的几个关系比较特殊, 下面给他们一些特殊的说法.

定义 4.3

给定集合A:
空集合叫做A上的**空关系**.
集合$A \times A$记作E_A, 叫做A上的**全关系**;
集合$\{< x, x > | x \in A\}$记作I_A, 叫做A上的**恒等关系**.

例 4.4

$A = \{1, 2\}$, 则

$$E_A = \{< 1, 1 >, < 1, 2 >, < 2, 1 >, < 2, 2 >\},$$
$$I_A = \{< 1, 1 >, < 2, 2 >\}.$$

例 4.5

设$A=\{1,2,3,4\}$, 下面的四个集合都是A上的关系, 试列出它们的元素.

(1) $R_1=\{<x,y> \mid x,y\in A, x是y的倍数\}$

(2) $R_2=\{<x,y> \mid x,y\in A, (x-y)^2\in A\}$

(3) $R_3=\{<x,y> \mid x,y\in A, x/y是素数\}$

(4) $R_4=\{<x,y> \mid x,y\in A, x\neq y\}$

解:

back

4.1 基本概念

给定一个序对，可以根据序对是否属于某个代表关系的集合来判断组成序对的两个元素是否有关系. 因此，用集合表示关系，是一个不错的方法. 另外，还有表示关系的其他方法，即下面将要介绍的矩阵和图的方法. 不过，这些关系需要限定为一个有限集合上的关系. 下面先介绍用矩阵表示关系.

设$A=\{x_1,x_2,\cdots,x_n\}$，R是A上的关系. 令

$$r_{ij}=\begin{cases}1 & \text{若}<x_i,x_j>\in R\\ 0 & \text{若}<x_i,x_j>\notin R\end{cases}\quad(i,j=1,2,\cdots,n)$$

称n阶矩阵 $M_R=\begin{bmatrix}r_{11} & r_{12} & \cdots & r_{1n}\\ r_{21} & r_{22} & \cdots & r_{2n}\\ \vdots & \vdots & \vdots & \vdots\\ r_{n1} & r_{n2} & \cdots & r_{nn}\end{bmatrix}$ 为R的关系矩阵.

4.1 基本概念

例 4.6

$A = \{1, 2, 3, 4\}$.
$R = \{< 1, 1 >, < 1, 2 >, < 2, 3 >, < 2, 4 >, < 3, 2 >\}$.
试求R的关系矩阵.

解: 按照定义, R的关系矩阵为$M_R = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$

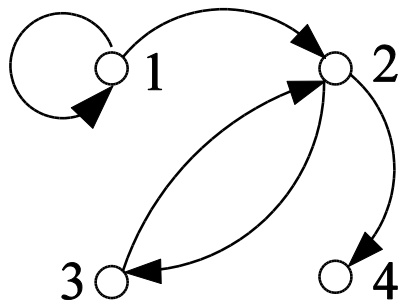
4.1 基本概念

下面是关系的图表示方法.

给定集合$A = \{x_1, x_2, \cdots, x_n\}$, R是A上的关系. 按照下面的方法画一个图:

用$x_1, x_2, \cdots, x_n$表示图的n个结点. 如果$< x_i, x_j > \in R$, 就在图中画一条从x_i到x_j带有方向的边, 边的方向指向x_j. 这个图记作G_R, 就叫R的**关系图**.

上个例子中, R的关系图为



4.2 关系的运算

关系既然是一个特殊的集合, 当然可以有集合涉及的运算.

例 4.7

设$A = \{1,2,3,4\}$, $H = \{< x,y > | \frac{x-y}{2}$是整数$\}$和$S = \{< x,y > | \frac{x-y}{3}$是整数$\}$是$A$上的两个关系. 求$H \cup S, H \cap S, \overline{H}, S - H, H - S, H \oplus S$.

解: 先把上面用描述方法表示的两个关系H和S变换为序对作成的集合的形式:

$H = \{< 1,1 >, < 1,3 >, < 2,2 >, < 2,4 >, < 3,3 >, < 3,1 >, < 4,4 >, < 4,2 >\}$;

$S = \{< 4,1 >\}$.

4.1 基本概念

然后进行题目中所要求的运算, 有

$H \cup S = \{< 1,1 >, < 1,3 >, < 2,2 >, < 2,4 >, < 3,3 >, < 3,1 >, < 4,4 >, < 4,2 >, < 4,1 >\}$;
$H \cap S = \Phi$
$\overline{H} = A \times A - H = \{< 1,2 >, < 2,1 >, < 2,3 >, < 3,2 >, < 3,4 >, < 4,3 >, < 1,4 >, < 4,1 >\}$;
$S - H = S = \{< 4,1 >\}$;
$H - S = H$;
$S \oplus H = H \cup S$.

它们依然还是集合A上的关系.

4.2 关系的运算

一般情况下, 下面的结论也成立.

定理 4.1

若R和S是从集合A到集合B的两个关系, 则R与S的并、交、补、差仍是A到B的关系.

定义 4.4

设R是A到B的关系, S是B到C关系. $A \times C$的子集合

$$\{< a, c > | (a \in A) \wedge (c \in C) \wedge \exists b((b \in B) \wedge (< a, b > \in R) \wedge (< b, c > \in S))\}$$

记作$R \circ S$, 称为关系R与S的复合关系, 这里“$\circ$” 可以看作复合运算符.

back

4.2 关系的运算

设R是集合A上的关系, 规定:
R^0代表I_A;
R^1代表R;
R^2代表$R \circ R$;
R^3代表$R^2 \circ R$;
$\cdots$
$R^{n+1} = R^n \circ R$, n是自然数.

例 4.8

设$A = \{a, b\}$, $B = \{1, 2, 3, 4\}$, $C = \{5, 6, 7\}$
$R = \{< a, 1 >, < a, 2 >, < b, 3 >\}$,
$S = \{< 2, 6 >, < 3, 7 >, < 4, 5 >\}$.
则$R \circ S = \{< a, 6 >, < b, 7 >\}$, $S \circ R = \emptyset$.

4.2 关系的运算

例 4.9

设$A=\{1,2,3,4\}$, A上的关系,
$R=\{<1,1>,<1,2>,<2,4>\}$,
$S=\{<1,4>,<2,3>,<2,4>,<3,2>\}$,
求$R\circ S$, $S\circ R$, R^2, R^3.

解:

$R\circ S=\{<1,4>,<1,3>\}$, $S\circ R=\{<3,4>\}$,
$R^2=R\circ R=\{<1,1>,<1,2>,<1,4>\}$,
$R^3=R^2\circ R=\{<1,1>,<1,2>,<1,4>\}$.

4.2 关系的运算

例 4.10

设R和S是自然数集合N上的两个二元关系，其定义为

$$R = \{< x, y > | (x \in N) \wedge (y \in N) \wedge (y = x^2)\},$$
$$S = \{< x, y > | (x \in N) \wedge (y \in N) \wedge (y = x + 1)\};$$

则

$$R \circ S = \{< x, y > | (x \in N) \wedge (y \in N) \wedge (y = x^2 + 1)\};$$
$$S \circ R = \{< x, y > | (x \in N) \wedge (y \in N) \wedge (y = (x + 1)^2)\}.$$

back

4.2 关系的运算

下面的结论表明, 关系复合运算满足结合律.

定理 4.2

设$R \subseteq A \times B, S \subseteq B \times C, T \subseteq C \times D$, 则
$(R \circ S) \circ T = R \circ (S \circ T)$.

推论:
设m, n为非负整数, R是集合A上的关系. 则
$R^m \circ R^n = R^{m+n}$,
$(R^m)^n = R^{mn}$.

4.2 关系的运算

定理 4.3

设$R \subseteq A \times B, S \subseteq B \times C, T \subseteq B \times C, U \subseteq C \times D$, 则有

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

(2) $(S \cup T) \circ U = (S \circ U) \cup (T \circ U)$

(3) $R \circ (S \cap T) \subseteq (R \circ S) \cap (R \circ T)$

(4) $(S \cap T) \circ U \subseteq (S \circ U) \cap (T \circ U)$.

back

4.2 关系的运算

两个关系复合以后形成的关系的关系矩阵与这两个关系的矩阵之间有何联系?

现在讨论**复合关系的关系矩阵**$M_{R\circ S}$的求法.

$$M_{R\circ S} = M_R \cdot M_S = (d_{ik})_{m\times p}, \text{其中} d_{ik} = \bigvee_{j-1}^{n}(r_{ij} \wedge s_{jk})$$

“$\vee$”表示逻辑加, 规则为:

$$1 \vee 1 = 1, 1 \vee 0 = 1, 0 \vee 1 = 1, 0 \vee 0 = 0.$$

“$\wedge$”表示逻辑乘, 规则为:

$$1 \wedge 1 = 1, 1 \wedge 0 = 1, 0 \wedge 1 = 1, 0 \wedge 0 = 0.$$

back

4.2 关系的运算

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

则$M_{R\circ S} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

4.2 关系的运算

定义 4.5

设R是A到B的关系，B到A的关系

$$\{< y, x > \mid < x, y > \in R\}$$

叫做R的**逆关系**，记为R^c或R^{-1}.

由定义可以看出:
R的逆关系R^c的关系图是把R的关系图中有向弧的方向反置后形成的图;
R^c的关系矩阵是M_R的转置矩阵.

back

4.2 关系的运算

例 4.11

现有自然数集合上的关系

$$R = \{< x, y > | (x \in N) \wedge (y \in N) \wedge (y = x + 1)\}$$

那么

$$R^c = \{< x, y > | (x \in N) \wedge (y \in N) \wedge (y = x - 1)\}$$

back

4.2 关系的运算

下面是两个涉及到逆关系的结论, 证明参见课本.

定理 4.4

设R, S都是A到B的二元关系, 则下列各式成立:

(1) $(R^c)^c = R$

(2) $(R \cup S)^c = R^c \cup S^c$

(3) $(R \cap S)^c = R^c \cap S^c$

(4) $(A \times B)^c = B \times A$

(5) $\overline{R} = (A \times B) - R$

(6) $(\overline{R})^c = \overline{R^c}$

(7) $(R - S)^c = R^c - S^c$.

back

4.2 关系的运算

定理 4.5

设R是A到B的二元关系，S是B到C的二元关系，
则$(R \circ S)^c = S^c \circ R^c$.

按照集合上关系的定义，不难看出，即使一个元素个数很少的集合，其上的关系数量也是很多的. 因此有必要挑出一些**具有特殊性质的关系**.

4.3 一些特殊的关系

定义 4.6

设R为定义在集合X上的关系.

(1) 若任意$x \in X$, 都有$< x, x > \in R$, 则称X上的二元关系R具有**自反性**, 简称R是自反的.

(2) 对任意$x, y \in X$, 当$< x, y > \in R$时, 就有$< y, x > \in R$, 则称集合关系R具有**对称性**, 简称R是对称的.

(3) 任意$x, y, z \in X$, 当$< x, y > \in R, < y, z > \in R$时, 就有$< x, z > \in R$, 则称$R$在$X$上具有**传递性**, 简称$R$是传递的.

back

4.3 一些特殊的关系

再给出两个特殊的关系.

定义 4.7

设R为定义在集合X上的关系.

(1) 若对于任意的$x \in X$, 都有$< x, x > \notin R$, 则称关系R具有**反自反性**, 简称R是反自反的.

(2) 如果对任意的$x, y \in X$, 当$< x, y > \in R$, $< y, x > \in R$, 必有$x = y$, 则称R在X上具有**反对称性**, 简称R是反对称的.

需要注意的是:
“反自反的”不是“自反的”的对立面.
“反对称的”不是“对称的”的对立面.

back

4.3 一些特殊的关系

例 4.12

对于集合$A=\{1,2\}$,
A上的关系$R=\{<1,2>\}$不是自反的, 是反自反的.
A上的关系$S=\{<1,1>,<1,2>\}$不是自反的, 也不是反自反的. 这个关系就可以表明“反自反的”不是“自反的”对立面.

例 4.13

对于集合$A=\{2,3,5,7\}$,
A上的关系$R=\{<1,2>,<2,3>,<3,2>\}$, 不是对称的, 也不是反对称的. 这个关系就可以表明“反对称的”不是“对称的”对立面.

4.3 一些特殊的关系

例 4.14

对于任意给定的集合A, 有

(a) 集合A上的恒等关系I_A是自反的, 对称的, 传递的, 但不是反自反的;

(b) 实数集合R上的关系“$\leqslant$”是自反的, 反对称的和传递的, 但不是对称的;

(c) 平面三角形上的全等关系“$\cong$”是自反的, 对称的, 传递的, 但不是反自反的;

(d) 平面三角形上的相似关系“$\sim$”是自反的, 对称的, 传递的, 但不是反自反的.

back

4.4 关系的闭包

定义 4.8

设R是集合A上的二元关系，若存在另一个关系R'满足下列条件：

(1) R'是自反的(对称的,传递的)；

(2) $R' \supseteq R$；

(3) 若还有A上自反的(对称的,传递的)的关系R''包含R，则必有$R'' \supseteq R'$.

则称R'为R的**自反闭包**(**对称闭包**,**传递闭包**)，记为$r(R)$ $(s(R), t(R))$.

back

4.4 关系的闭包

一个关系R的自反闭包(对称闭包, 传递闭包), 直观上理解就是包含R的“最小”的自反关系(对称关系, 传递关系).
下面讨论对于给定的关系, 如何求它的三种闭包? 先从简单的情况说起.

定理 4.6

设R是集合A上的二元关系, 则

(1) 若R 是自反的, 则$r(R) = R$;

(2) 若R 是对称的, 则$s(R) = R$;

(3) 若R 是传递的, 则$t(R) = R$.

back

4.4 关系的闭包

当R是一般的关系时, 有下面的结论.

定理 4.7

设R是集合A上的二元关系, 则

(1) $r(R) = R \cup I_A$;

(2) $s(R) = R \cup R^c$;

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

back

4.4 关系的闭包

例 4.15

若$A=\{1,2,3\}$上的关系$R=\{<1,2>,<2,3>,<3,1>\}$，试求$r(R)$、(R)和$t(R)$.

解:

$r(R)=\{<1,1>,<1,2>,<2,2>,<2,3>,<3,1>,<3,3>\}$;

$s(R)=\{<1,2>,<2,1>,<2,3>,<3,2>,<3,1>,<1,3>\}$;

由于$R^2=\{<1,3>,<2,1>,<3,2>\}$,

$R^3=\{<1,1>,<2,2>,<3,3>\}$,

$R^4=R$,

$R^5=R^2$,

$\cdots$

一般情况下, 有$R^{3n+1}=R$, $R^{3n+2}=R^2$, $R^{3n}=R^3(n=1,2,\cdots)$.

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

4.4 关系的闭包

例 4.15

若$A=\{1,2,3\}$上的关系$R=\{<1,2>,<2,3>,<3,1>\}$,
试求$r(R)$、(R)和$t(R)$.
解:
$r(R)=\{<1,1>,<1,2>,<2,2>,<2,3>,<3,1>,<3,3>\}$;
$s(R)=\{<1,2>,<2,1>,<2,3>,<3,2>,<3,1>,<1,3>\}$;
由于$R^2=\{<1,3>,<2,1>,<3,2>\}$,
$R^3=\{<1,1>,<2,2>,<3,3>\}$,
$R^4=R$,
$R^5=R^2$,
$\cdots$
一般情况下, 有$R^{3n+1}=R$, $R^{3n+2}=R^2$, $R^{3n}=R^3(n=1,2,\cdots)$.
故$t(R)=\bigcup_{i=1}^{\infty} R^i=R\cup R^2\cup R^3=A\times A$.

4.4 关系的闭包

计算$t(R)$时，在一般来说是较麻烦的，但当A是有限集合时，计算A上关系的传递闭包可以来的简单些，看下面的结论.

定理 4.8

设集合A是有限集，$|A| = n$，R是A上的关系，则存在正整数k，使得

$$t(R) = R \cup R^2 \cup \cdots \cup R^k$$

这里$k \leq n$.

这个定理表明，有限集合上关系的传递闭包不需要求无限多个集合的并集.

4.5 集合的划分和覆盖

定义 4.9

若把一个非空集合A分成若干个叫做分块的非空子集，使得A中每个元素属于其中的一个分块，这些分块的全体构成的集合叫做A的一个**覆盖**. 进而当A中每个元素恰好属于一个分块时，此时的覆盖也叫**划分**，也称分划.

back

4.5 集合的划分和覆盖

上面的定义可以解释为:

给定集合$A \neq \emptyset$, $S = \{A_1, A_2, \cdots, A_m\}$, A_1, A_2, $\cdots$, A_m是A的非空子集, 且$\bigcup_{i=1}^{m} A_i = A$, 则集合$S$叫作集合$A$的覆盖. 进一步, 若$A_i \cap A_j = \emptyset (i \neq j, i, j = 1, 2, \cdots, m)$, 那么, S 叫做A的一个划分.

按照定义, 划分一定是覆盖, 但覆盖不一定是划分.

4.5 集合的划分和覆盖

例 4.16

对于集合$A = \{a, b, c\}$, 考虑下列由A的某些子集作成的集合:

$D = \{\{a\}, \{b, c\}\}$,
$G = \{\{a, b, c\}\}$,
$E = \{\{a\}, \{b\}, \{c\}\}$,
$S = \{\{a, b\}, \{b, c\}\}$,
$F = \{\{a\}, \{a, c\}\}$,
$Q = \{\{a\}, \{a, b\}, \{a, c\}\}$.

按照定义, 可知D, G, E, S和Q是A的覆盖, D, G和E是A 的划分. F不是覆盖, 自然不是划分.

4.5 集合的划分和覆盖

例 4.16

对于集合$A = \{a, b, c\}$, 考虑下列由A的某些子集作成的集合:

$D = \{\{a\}, \{b, c\}\}$,
$G = \{\{a, b, c\}\}$,
$E = \{\{a\}, \{b\}, \{c\}\}$,
$S = \{\{a, b\}, \{b, c\}\}$,
$F = \{\{a\}, \{a, c\}\}$,
$Q = \{\{a\}, \{a, b\}, \{a, c\}\}$.

按照定义, 可知D, G, E, S和Q是A的覆盖, D, G和E是A 的划分. F不是覆盖, 自然不是划分.

4.5 集合的划分和覆盖

定义 4.10

设$A = \{A_1, A_2, \cdots, A_m\}$, $B = \{B_1, B_2, \cdots, B_n\}$ 是集合X的两个不同的划分, 称集合

$$S = \{A_i \cap B_j \mid (A_i \cap B_j \neq \emptyset, i = 1, 2, \cdots, m;\ j = 1, 2, \cdots, n)\}$$

叫作A与B 的交叉.

定理 4.9

设$A = \{A_1, A_2, \cdots, A_m\}$, $B = \{B_1, B_2, \cdots, B_n\}$ 是集合X的两个不同的划分, 则A与B的交叉是集合X的一个划分.

back

4.5 集合的划分和覆盖

定义 4.11

给定集合X的任意两个划分$A = \{A_1, A_2, \cdots, A_m\}$与$B = \{B_1, B_2, \cdots, B_n\}$，若对每个$A_i$均有$B_j$使得$A_i \subseteq B_j$，则称划分$A$为划分$B$的**加细**.

定理 4.10

任何两种划分的交叉划分都是原各划分的一种加细.

back

4.6 序关系

实数集R上的小于等于关系“$\leqslant$”是自反的, 反对称的和传递的. 两个实数可以比较大小, 这体现是一种数的顺序特性, 下面就介绍有关序的一种关系.

定义 4.12

设R是集合A上的关系. 若R是自反的、反对称的和传递的, 则称R为A 上的**偏序关系**, 集合A连同其上的偏序关系R所形成的二元组$< A, R >$ 叫做偏序集.

back

4.6 序关系

例 4.17

实数集R上的小于等于关系“$\leqslant$”是偏序关系. $<R, \leq>$是偏序集.

例 4.18

非空集合A所有子集组成的集合$P(A)$上的包含关系“$\subseteq$”是偏序关系, $<P(A), \subseteq>$是偏序集.

例 4.19

设Z^+是正整数集合, $a, b \in Z^+$, 若a整除b, 记为$a \mid b$, 整除关系“$|$” 是不是Z^+上的偏序关系?

back

4.6 序关系

上面列举了几个偏序集. 今后, 为了方便直观, 我们用符号$\preccurlyeq$表示偏序关系(用这个符号的原因可以认为平时的$\leq$就是一个特殊的偏序关系). 这样偏序集就可以写成$<A, \preccurlyeq>$的样子.

对于偏序集A的两个元素x, y, 若x与y有偏序关系$\preccurlyeq$, 即$x \preccurlyeq y$, 我们不妨将此符号读成“x小于等于y”, 进而, 若x 与y不相等, 则可以说x小于y或者y大于x. 不过需要注意, 这只是借用平时的读法而已.

4.6 序关系

在画偏序关系的关系图时, 一些内容可以简化, 下面讨论这个问题.

定义 4.13

设$<A, \preccurlyeq>$是一个偏序集, 若$x, y \in A$, $x \preccurlyeq y$, $x \neq y$且没有其它元素$z \in A$ 满足$x \preccurlyeq z \preccurlyeq y$, 则称元素$y$**盖住**元素$x$.
令

$$COV(A) = \{< x, y > | x, y \in A, y\text{盖住}x\}$$

称$COV(A)$为$<A, \preccurlyeq>$的**盖住关系**.

back

4.6 序关系

例 4.20

现有$A = \{1,2,3,4,6,12\}$和偏序集$< A, |>$是偏序集, 这里“$|$”是整除关系. 试求$COV(A)$.

解:

$$COV(A) = \{< 1,2 >, < 1,3 >, < 2,4 >, < 2,6 >, < 3,6 >, < 4,12 >, < 6,12 >\}.$$

4.6 序关系

例 4.20

现有$A = \{1, 2, 3, 4, 6, 12\}$和偏序集$< A, | >$是偏序集, 这里“$|$”是整除关系. 试求$COV(A)$.

解:

$COV(A) = \{< 1, 2 >, < 1, 3 >, < 2, 4 >, < 2, 6 >, < 3, 6 >, < 4, 12 >, < 6, 12 >\}$.

4.6 序关系

利用盖住关系作"$\preccurlyeq$"的哈斯图既简单又层次清楚. **哈斯图的作图规则是:**

(1) 用小圆圈（或小圆点）代表元素;

(2) 如果$x \preccurlyeq y$且$x \neq y$, 则将代表y的小元点画在代表x的小元点的上面;

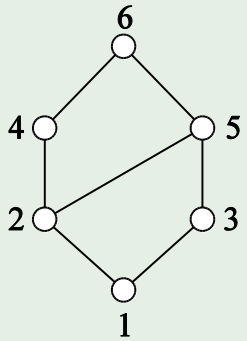
(3) 如果$< x, y > \in COV(A)$, 则在x与y之间用直线连接.

back

4.6 序关系

例 4.21

$A = \{1, 2, 3, 4, 5, 6\}$, $< A, |>$, $|$是A上的某关系关系,哈斯图为:



试问求A的关系图, 需要补上那些有向边?

解:

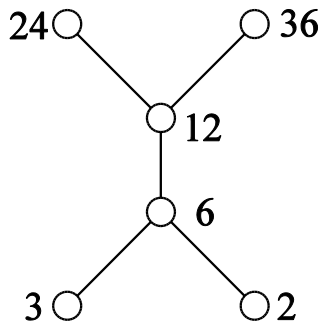
back

4.6 序关系

例 4.22

设$A = \{2, 3, 6, 12, 24, 36\}$, $|$是A上的整除关系, 求偏序集$< A, | >$的哈斯图.

解: $COV(A) = \{< 2, 6 >, < 3, 6 >, < 6, 12 >, < 12, 24 >, < 12, 36 >\}$, 哈斯图为:



Hasse图其实就是将偏序关系常规定义下的关系图去掉每个结点上的环边和去掉由于传递而产生的边以及两个有关系的元素小的放在下边, 再去掉每条边的方向后的图.

4.6 序关系

定义 4.14

设$<A, \preccurlyeq>$为偏序集, B是A的子集, $b \in B$.

(1) 若在B中不存在比b还大的元素, 则称b是B的极大元.

(2) 若在B中不存在比b还小的元素, 则称b是B的极小元.

(3) 若B中的每个除去b元素都比b小, 则称b是B的最大元.

(4) 若B中的每个除去b元素都比b大, 则称b是B的最小元.

注意上述概念的差别:

集合B的最大元一定为极大元, 发过来未必.
集合B的最小元一定为极小元, 发过来未必.

back

4.6 序关系

例 4.23

$A = \{2, 3, 6, 12, 24, 36\}$, 整除“$|$”是$A$上的偏序关系,
A有极小元2, 3, 有极大元24, 36, A没有最大元和最小元.

对于A的子集$B_1 = \{2, 3, 6, 12\}$,
B_1的极小元是2, 3, B_1没有最小元, B_1的极大元是12, 12 也是最大元.

对于A的子集$B_2 = \{6, 12, 24\}$, B的极小元和最小元都是6,
B的极大元和最大元都是是24.

back

4.6 序关系

上面的例子表明极大元或者极小元都不是唯一的, 最大元和最小元都是唯一的.
一般情况下也有

定理 4.11

设$< A, \preccurlyeq >$为偏序集, B是A的子集, 若B有最大元(最小元), 则最大元(最小元)都是唯一的.

back

4.6 序关系

定义 4.15

设$<A, \preccurlyeq>$为偏序集, B是A的非空子集,

(1) 若A中存在元素a, 使B中的每个元素都小于等于a, 则称a为B的上界.

(2) 若A中存在元素a, 使B中的每个元素都大于等于a, 则称a为B的下界.

(3) 设C是B的所有上界作成的集合, 即$C = \{y \mid y$是B的上界$\}$, C的最小元若存在, 称为B的上确界.

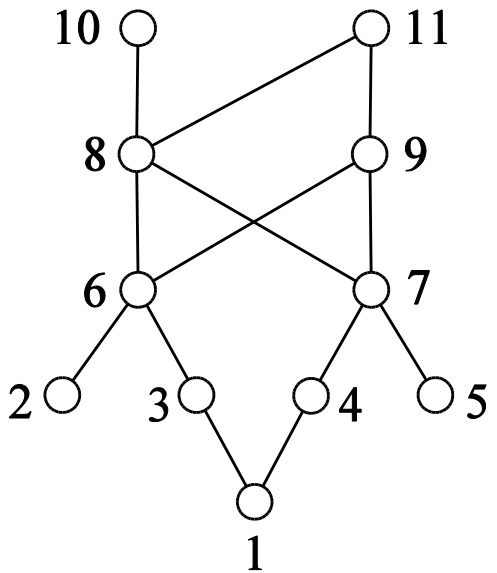
(4) 设C是B的所有下界作成的集合, 即$C = \{y \mid y$是B的下界$\}$, C的最大元若存在, 称为B的下确界.

back

4.6 序关系

例 4.24

设集合$A = \{1,2,3,4,5,6,7,8,9,10,11\}$，偏序集的$<A, \preccurlyeq>$哈斯图如下图所示.



,

back

4.6 序关系

集合$B_1 = \{1, 2, 3, 4, 5, 6, 7\}$的上界有8, 9, 10, 11.

集合$B_2 = \{8, 9, 10, 11\}$的下界有1, 2, 3, 4, 5, 6, 7.

2, 3, 4, 5都不是集合$B_3 = \{6, 7, 8, 9\}$的下界.

集合$B_4 = \{6, 7, 8, 9, 10, 11\}$的下确界是1.

$B = \{2, 3, 4, 5\}$的上确界不存在.

back

4.7 等价关系与等价类

定义 4.16

若集合A上的二元关系R, 同时具有自反性、对称性和传递性, 则称R是A上的**等价关系**.

例 4.25

平面上所有三角形组成集合上的三角形之间的相似关系是等价关系.

back

4.7 等价关系与等价类

例 4.26

设Z为整数集，m是给定的正整数. 定义Z上的二元关系R为：

$$R = \{(a,b) \mid a \equiv b \pmod{m}\}$$

则R是Z上的等价关系.

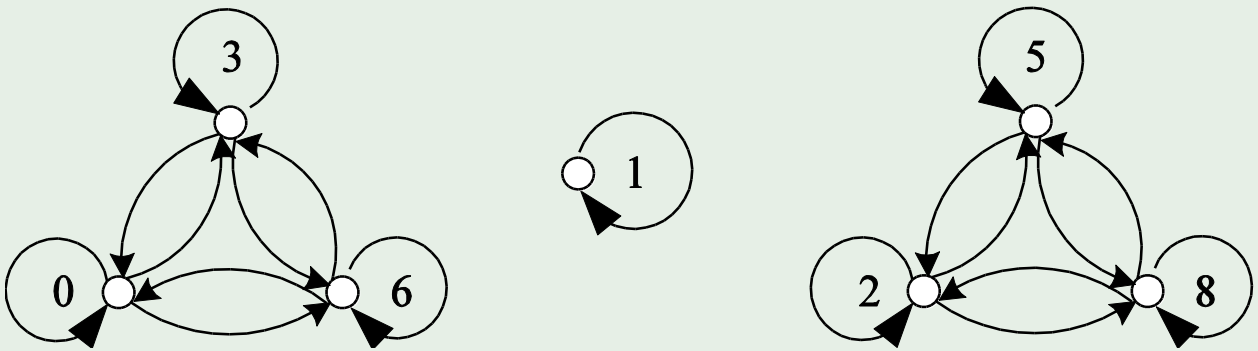
解：

back

4.7 等价关系与等价类

例 4.27

设$A=\{0,1,2,3,5,6,8\}$, R为Z上的模3等价关系, 则
$R=\{<0,0>,<1,1>,<2,2>,<3,3>,<5,5>,$
$<6,6>,<8,8>,<0,3>,<3,0>,<0,6>,<6,0>,$
$<2,5>,<5,2>,<2,8>,<8,2>,<3,6>,<6,3>,$
$<5,8>,<8,5>\}$,
R的关系图如下.



4.7 等价关系与等价类

定义 4.17

设R是非空集合A上的等价关系，任取$a \in A$，A中所有与a有关系的元素作成的集合

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

叫做由关系R确定的a的等价类，简记为$[a]$.

例 4.28

整数集合Z上的模3等价关系的等价类有：
$[0] = \{\cdots, -6, -3, 0, 3, 6, \cdots\}$，所有3的倍数的整数.
$[1] = \{\cdots, -5, -2, 1, 4, 7, \cdots\}$，所有3的倍数的整数+1.
$[2] = \{\cdots, -4, -1, 2, 5, 8, \cdots\}$，所有3的倍数的整数+2.

4.7 等价关系与等价类

定理 4.12

设R是集合A上的等价关系, 则

(1) 对任意$a, b \in A$, 或者$[a] = [b]$或者$[a] \cap [b] = \varnothing$;

(2) $\bigcup_{a \in A} [a] = A$.

定理 4.13

设R是集合A上的等价关系. 任取$a, b \in A$, 有

$$aRb \text{当且仅当} [a]_R = [b]_R$$

back

4.7 等价关系与等价类

定义 4.18

设R为集合X上的等价关系, 所有等价类作成的集合

$$\{[a]_R \mid a \in X\}$$

叫做X关于R的**商集**, 记作X/R.

例 4.29

整数集合Z上的模3的等价关系的商集是

$$Z/R = \{[0]_R, [1]_R, [2]_R\}.$$

back

4.7 等价关系与等价类

定理 4.14

集合X上的等价关系R, 决定了X的一个划分, 该划分就是商集X/R.

定理 4.15

集合X上的一个划分确定X中元素间的一种等价关系.

back

4.7 等价关系与等价类

定理 4.16

设R_1与R_2都是集合X上的等价关系，则

$$R_1 = R_2 \text{当且仅当} X/R_1 = X/R_2.$$

例 4.30

设$X = \{a, b, c, d, e\}$，试求划分$S = \{\{a, b\}, \{c\}, \{d, e\}\}$确定的等价关系.

解:

back

4.8 函数

函数是一个基本的数学概念，这里我们把函数作为一种特殊的关系进行研究，例如，计算机中把输入输出间的关系看成是一种函数；类似地，在开关理论、自动机理论和可计算性理论等领域中函数都有着及其广泛的应用.

back

4.8 函数

定义 4.19

设X, Y是两个集合，f是X到Y的一个关系，

(1) 若对任一$x \in X$, 都有唯一的$y \in Y$, 使得$< x, y > \in f$, 则称f为X到Y的**函数**, 记作: $f : X \to Y$.

(2) 若$< x, y > \in f$, y叫做x的**象**, 记作$y = f(x)$, x叫y的原像.所有像的集合记作$f(X)$, 叫做函数f的**象集**.

(3) $f : X \to Y$, X称为函数f的**定义域**, 记为 $domf$, 称像集$f(X)$为函数f的**值域**, 记为$rangef$, Y 称为函数f的**共域**.

值域是共域的子集.

4.8 函数

设$X=\{a,b,c\}$, $Y=\{0,1\}$, X到Y的关系共有$2^6=64$个, 但可以叫做函数的关系只有$2^3=8$个, 它们是:

$$f_0=\{<a,0>,<b,0>,<c,0>\}$$
$$f_1=\{<a,0>,<b,0>,<c,1>\}$$
$$f_2=\{<a,0>,<b,1>,<c,0>\}$$
$$f_3=\{<a,0>,<b,1>,<c,1>\}$$
$$f_4=\{<a,1>,<b,0>,<c,0>\}$$
$$f_5=\{<a,1>,<b,0>,<c,1>\}$$
$$f_6=\{<a,1>,<b,1>,<c,0>\}$$
$$f_7=\{<a,1>,<b,1>,<c,1>\}$$

back

4.8 函数

定理 4.17

设$|X| = m$, $|Y| = n$, 则从X到Y最多可定义n^m个不同的函数.

定义 4.20

设$f : X \to Y$,

(1) 若$rangef = Y$, 则称f为**满射函数**(Y中的每个元素都有原像).

(2) $\forall x_1, x_2 \in X$, 若$x_1 \neq x_2$, 则$f(x_1) \neq f(x_2)$, 称f为**单射函数**(原像不同, 则像也不同).

(3) 若函数f既是满射函数又是单射函数, 则称f为**一一映射函数**.

back

4.8 函数

从一一对应函数的定义可以看出，两个有限集合之间要是存在一一对应函数的话，则两个集合的基数必须相同，反之亦然.

也有下面的结论:

定理 4.18

设A, B是有限集，f是A到B的函数，则:
f是单射函数时，有$|A| \leq |B|$.
f是满射函数时，有$|A| \geq |B|$.

back

4.8 函数

例 4.31

设$A=\{0,1,2\}$, $B=\{0,1\}$.

若 f: $f(0)=0, f(1)=0, f(2)=0$, 则f是A到B的函数, 不是单射, 不是满射.

若 $g: g(0)=0, g(1)=0, g(2)=1$, 则$g$是$A$到$B$的函数, 是满射, 不是单射.

back

4.8 函数

例 4.32

设N是非负整数集, 对任意$n \in N$, 试问
(1) 函数$f : N \to N$, 其中$f(n) = n(mod 3)$, f是什么函数?
(2) 函数$g : N \to N$, 其中$g(n) = \lfloor \sqrt{n} \rfloor$, g是什么函数?

解:
(1) f不是单射函数, 也不是满射函数.
(2) g不是单射函数, 是满射函数.

4.8 函数

例 4.32

设N是非负整数集, 对任意$n \in N$, 试问
(1) 函数$f : N \to N$, 其中$f(n) = n(mod 3)$, f是什么函数?
(2) 函数$g : N \to N$, 其中$g(n) = \lfloor \sqrt{n} \rfloor$, g是什么函数?

解:
(1) f不是单射函数, 也不是满射函数.
(2) g 不是单射函数, 是满射函数.

4.8 函数

前面我们曾经将集合X到Y的关系R中的序对元素的位置进行交换而定义了R的逆关系R^c, R^c是Y到X的关系.
对于函数f来说, 不能简单地用交换其序对顺序的办法定义逆函数f^c, 这是因为当函数$f: X \to Y$的值域仅是Y的一个真子集时(f不是满射函数), 这时Y中的某些元素不会有像, 这不符合函数的要求. 另外, 若函数$f: X \to Y$不是单射函数, 简单地将f中的序对颠倒过来会导致Y中的某个元素至少对应两个不同的数对, 这也与函数的定义不符.

经过这些分析后可知, 一个函数为一一对应函数时, 将函数中序对元素的位置进行交换可定义另外一个函数.

back

4.8 函数

定义 4.21

设f为X到Y的一一对应函数，把f中的序对都颠倒过来所确定的Y到X的关系叫做函数f的逆函数，记为f^{-1}.

定理 4.19

设$f: X \to Y$是一个一一对应函数，那么$f^c: Y \to X$也是一一对应函数.

例 4.33

设$A = \{1,2,3\}$, $B = \{a,b,c\}$, $f = \{< 1,a >, < 2,c >, < 3,b >\}$是$A$到$B$的一一对应函数，$f$的逆关系$f^c = \{< a,1 >, < c,2 >, < b,3 >\}$是$B$到$A$的一一对应函数.

4.8 函数

下面考虑两个函数的复合问题.

定义 4.22

设$f: X \to Y, g: W \to Z$, 若$f(X) \subseteq W$, 则称

$$\{< x, z > | \exists y(y \in Y) \wedge (< x, y > \in f) \wedge (< y, z > \in g)\}$$

叫做为f与g的**复合函数**, 记作$g \circ f$.

注意f与g的复合函数记作$g \circ f$, 不是$f \circ g$, 主要是考虑到函数中经常将自变量放在函数符号的右边. $\circ$叫复合运算符.
f与g的复合函数$g \circ f$是将元素x映射到$g(f(x))$, 即$(g \circ f)(x) = g(f(x))$.

4.8 函数

定理 4.20

函数的复合运算满足结合律.

例 4.34

设$X=\{1,2,3\}$, $Y=\{p,q\}$, $Z=\{a,b\}$,
$f=\{<1,p>,<2,p>,<3,q>\}$,
$g=\{<p,b>,<q,b>\}$, 求$g\circ f$.

解： $g\circ f=\{<1,b>,<2,b>,<3,b>\}$.

4.8 函数

例 4.35

设R是实数集, 有下面三个R到R的函数:
$f(x)=x+2, g(x)=x-2, h(x)=3x.$
求$f\circ g, g\circ f, f\circ f, (f\circ h)\circ g.$

解

$$(f\circ g)(x)=f(g(x))=f(x-2)=x-2+2=x,$$
$$(g\circ f)(x)=g(f(x))=g(x+2)=x+2-2=x,$$
$$(f\circ f)(x)=f(f(x))=f(x+2)=(x+2)+2=x+4,$$
$$(f\circ h)\circ g(x)=f(h(g(x)))=f(h(x-2))=f(3(x-2))$$
$$=3(x-2)+2=3x-4.$$

4.8 函数

定理 4.21

若$g \circ f$是一个复合函数,

(1) 如果g和f为满射函数, 则$g \circ f$为满射函数.

(2) 如果g和f为单射函数, 则$g \circ f$为单射函数.

(3) 如果g和f为一一映射函数, 则$g \circ f$为一一映射函数.

定理 4.22

设$f : X \to Y$是一一映射函数, 则

(1) $f \circ I_X = I_Y \circ f = f$;

(2) $(f^{-1})^{-1} = f$;

(3) $f^{-1} \circ f = I_X, f \circ f^{-1} = I_Y$

4.8 函数

其中I_X, I_Y分别是集合X和Y上的恒等函数（即恒等关系）.

定理 4.23

设$f: X \to Y, g: Y \to Z$都是双射函数,则 $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

上述结论课的证明, 参见课本.

目录

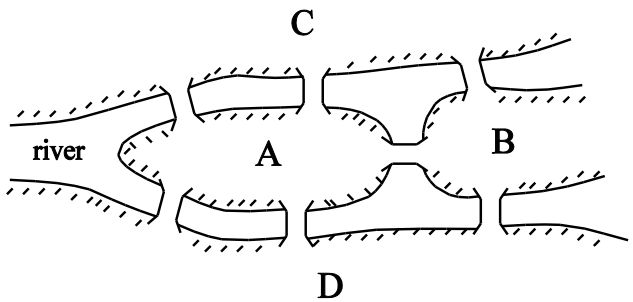
5.1 若干图论经典问题

图论是以图为研究对象的数学分支。图论中的图指的是一些点以及连接这些点的线的总体。通常用点代表事物，用连接两点的线代表事物间的关系。例如，国家用点表示，有外交关系的国家用线连接代表这两个国家的点，于是世界各国之间的外交关系就被一个图形描述出来了。用工艺流程图来描述某项工程中各工序之间的先后关系，用网络图来描述某通讯系统中各通讯站之间信息传递关系，用开关电路图来描述IC中各元件电路导线连接关系等等。事实上，任何一个包含了某种二元关系的系统都可以用图形来模拟。研究图的基本概念和性质、图的理论及其应用构成了图论的主要内容。

back

5.1 若干图论经典问题

哥尼斯堡七桥问题



东普鲁士的哥尼斯堡城位于普雷格尔（*Pregel*）河的两岸，河中有一个岛，城市被河的分支和岛分成了四个部分，各部分通过7座桥彼此相通，如图所示。该城的居民喜欢在星期日绕城散步。于是产生了这样一个问题：从四部分陆地任一块出发，按什么样的路线能做到每座桥经过一次且仅一次返回出发点。

5.1 若干图论经典问题

四色问题

四色问题是一个著名的数学定理：如果在平面上划出一些邻接的有限区域，那么可以不多于用四种颜色来给这些区域染色，使得每两个邻接区域染的颜色都不一样。四色问题又称四色猜想、四色定理，是世界三大数学猜想之一。一个多世纪以来，数学家们为证明这条定理绞尽脑汁，所引进的概念与方法刺激了拓扑学与图论的生长、发展。1976 年，凯尼斯.阿佩尔（*K.Appel*）和沃夫冈.哈肯（*W.Haken*）借助电子计算机首次得到一个完全的证明，四色问题也终于成为四色定理。

5.1 若干图论经典问题

环游世界问题

由天文学家哈密顿（*WilliamRowanHamilton*）提出，在一个世界地图网络中，寻找一条从给定的起点到给定的终点沿途恰好经过所有其他城市一次的路径。判断*Hamilton*环游世界问题是否有解，到目前为止还没有有效的算法。

这一时期同时出现了以图为工具去解决其它领域中一些问题的成果。1847 年德国的克希霍夫（*G.R.Kirchoff*）将树的概念和理论应用于工程技术的电网络方程组的研究。1857年英国的凯莱（*A.Cayley*）也独立地提出了树的概念，并应用于有机化合物的分子结构的研究中。1936年匈牙利的数学家哥尼格（*D.Konig*）写出了第一本图论专著《有限图与无限图的理论》。

back

5.1 若干图论经典问题

平面图和印刷电路板的设计

1936年以后，由于生产管理、军事、交通运输、计算机和通讯网络等方面的大量问题的出现，大大促进了图论的发展。特别是电子计算机的大量应用，使大规模问题的求解成为可能。实际问题如电网络、交通网络、电路设计、数据结构以及社会科学中的问题所涉及到的图形都是很复杂的，需要计算机的帮助才有可能进行分析和解决。目前图论在物理、化学、运筹学、计算机科学、电子学、信息论、控制论、网络理论、社会科学及经济管理等几乎所有学科领域都有应用。

back

5.1 若干图论经典问题

平面图和印刷电路板的设计

平面图是要求我们把图能画在平面上，使得不是节点的地方不能有边交叉的图。印刷电路板（*PrintedCircuitBoard*）印刷电路板，在设计和制造印刷电路板时，首先要解决的问题是判定一个给定的电路图是否能印刷在同一层板上而使导线不发生短路？若可以，怎样给出具体的布线方案？将要印刷的电路图看成是一个无向简单连通图G，其中顶点代表电子元件，边代表导线，于是上述问题归结为判定G是否是平面图。平面图的判断问题，在数学上已由波兰数学家库拉托夫斯基（*Kuratowski*）于1930年解决。

back

5.1 若干图论经典问题

运输网络

自从克希霍夫运用图论从事电路网络的结构分析以来，网络理论的研究和应用就越来越广泛。特别是近几十年来，电路网络、运输网络、通讯网络等与工程和应用密切相关的课题受到了高度的重视。运输网络的实际意义是“货物从产地s（源），通过有限制容量的运输道路（有向边）及若干中转站，到达目的地t（汇）”这类情形的一般模型。给定运输网络，要求怎样使在单位时间内运输量最大。

back

5.1 若干图论经典问题

通讯网络

电话网络、计算机网络、管理信息系统、医疗数据网络、银行数据网络、开关网络等等。这些网络的基本要求是网络中各用户能够快速安全地传递信息，不产生差错和故障，同时使建造和维护网络所需费用低。通讯网络中最重要的整体问题是网络的拓扑结构。通讯网络还要考虑流量和控制问题、网络的可靠性等问题。

back

5.1 若干图论经典问题

二元树的应用

前缀码（哈夫曼编码）在通讯系统中，常用二进制来表示字符。但由于字符出现的频率不一样以及为了保密的原因，能否用不等长的二进制数表示不同的字符，使传输的信息所用的总码元尽可能少呢？但是不等长的编码方案给编码和译码带来了困难。*Huffman* 于1952 年提出一种编码方法，该方法完全依据字符出现概率来构造异字头的平均长度最短的码字，这个编码就叫做*Huffman*编码（有时也称为霍夫曼编码）。

back

5.1 若干图论经典问题

最短路问题

若网络中的每条边都有一个数值（长度、成本、时间等），则找出两节点（通常是源节点和终节点)之间总权和最小的路径就是最短路问题。最短路问题可用来解决管路铺设、线路安装、厂区布局和设备更新等实际问题。

最短路问题的一个典型应用是在路由器上，路由器能用最短路算法选择通畅快捷的近路。

最短路问题的另一个典型应用是用在自主导航中。

back

5.2 图的基本概念及矩阵表示

定义 5.1

一个**图**G是一个二元组$G =< V(G), E(G) >$，其中$V(G)$是一个有限的非空集合，称为顶点集，其元素称为**结点**或**顶点**，通常用v表示顶点；$E(G)$是一个以顶点对为元素，并且元素可重复的集合，其元素称为**边**。

若$E(G)$是全部由无序对构成，称$G =< V(G), E(G) >$为**无向图**，无序对(u, v)对应连着顶点u和顶点v无向边。若$E(G)$是全部由有序对构成，称$G =< V(G), E(G) >$为**有向图**，有序对$< u, v >$对应从顶点u到顶点v的有向边。若$E(G)$是由无序对和有序对共同构成，称$G =< V(G), E(G) >$为**混合图**。

5.2 图的基本概念及矩阵表示

常常把$V(G)$和$E(G)$分别简记为V和E，因而常用$G=<V,E>$表示图，有时简单用图G表示图$G=<V,E>$。

无向图，有向图，混合图统称为图。

back

5.2 图的基本概念及矩阵表示

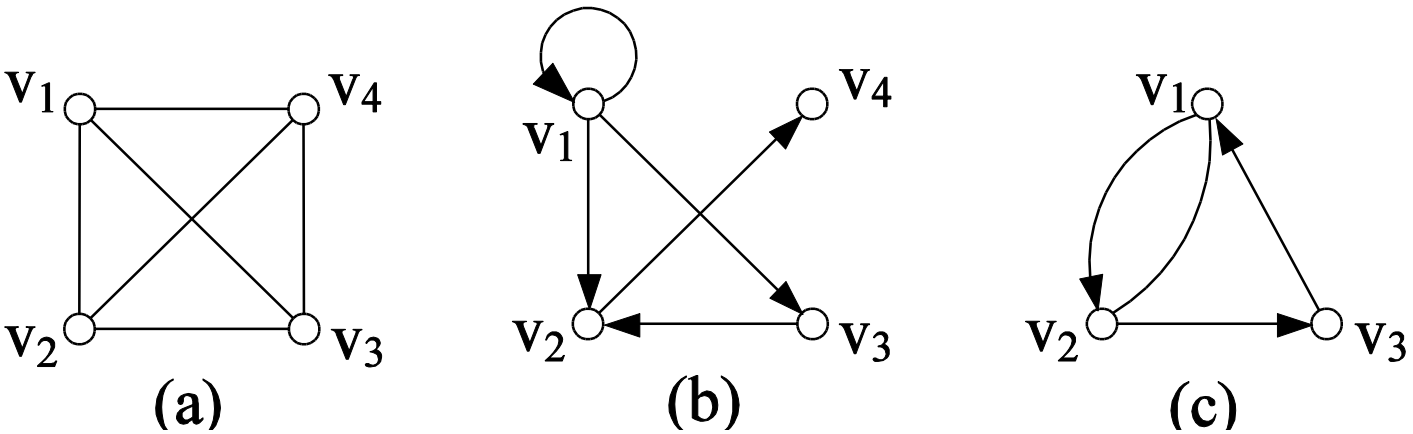
定义 5.2

图G的结点数称为G的**阶**，n个结点的图称为**n 阶图**。
常用e表示边，如$e =< v_1, v_2 >$ 表示e是一条从v_1到v_2 的有向边。

根据图的这种定义，很容易利用图形来表示图。图形的表示方法具有直观性，可以帮助我们了解图的性质。在图的图形表示中，每个结点用一个小圆点表示，每条边用一条分别以结点v和u为端点的联线表示。以后用图形来直接表示图。

back

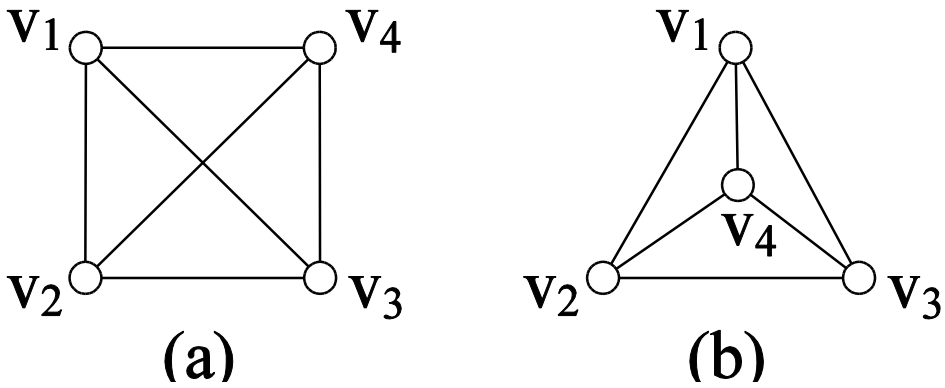
5.2 图的基本概念及矩阵表示



图（a）是无向图，图（b）是有向图，图（c）是混合图。

back

5.2 图的基本概念及矩阵表示



一个图的图形表示法可能不是唯一的。表示结点的圆点和表示边的线，它们的位置是没有实际意义的。因此，对于同一个图，可能画出很多表面不一致的图形来。上图是同一个图的二种画法，后面会讲到，这二个图是互相同构的。

back

5.2 图的基本概念及矩阵表示

定义 5.3

若$e=(u,v)$或$e=<u,v>$是图G的一条边，则称结点u和v是**相邻的**，并且称边e分别与u和v**关联**。若$e=<u,v>$是有向边，称u和v是边e的**始点和终点**，若图G的两条边e_1和e_2都与同一个结点关联，称e_1和e_2是**相邻的**。

在图的定义中，$E(G)$如果有重复元素，或序对的二个元素相同，则图G是一个**多重图**。在多重图中，与同一对结点关联的两条或两条以上的边或$E(G)$中相同序对对应的边称为**平行边**，关联同一个结点的一条边称为**环**或**自回路**。没有平行边和环的图称为**简单图**。

5.2 图的基本概念及矩阵表示

定义 5.4

在一个图中不与任何结点相邻接的结点，称为**孤立点**，只由孤立点构成的图叫**零图**，仅由一个孤立点构成的图叫**平凡图**，若图中的顶点集$V = \emptyset$，称该图为**空图**。将多重图的平行边代之以一条边，去掉环，就可以得到一个简单图。这样得到的简单图称为原来图的**基图**。在研究某些图论问题，如连通，点着色，点独立集，哈密顿图和平面性问题时只要考虑对应的基图就行了。因此，简单图将是本教程的主要讨论对象。

back

5.2 图的基本概念及矩阵表示

简单图$G=<V,E>$中若每一对结点间都有边相连，则称该图为**完全图**。有n个结点的无向完全图记作K_n。每对结点之间皆有边联结的简单有向图称为**有向完全图**。n个结点的完全图的边数为$\frac{n(n-1)}{2}$。

定义 5.5

图G中结点v的度数$d_G(v)$是G中与v关联的边的数目，简称为**度**，记为$d(v)$。每个环在计算度时算作两条边。对有向图，顶点v作为边的终点的次数为v的**入度**，记为$d^-(v)$，顶点v作为边的始点的次数为v的**出度**，记为$d^+(v)$。

back

5.2 图的基本概念及矩阵表示

令 $\Delta(G) = max\{d(v)|v \in V(G)\}$,$\delta(G) = min\{d(v)|v \in V(G)\}$ 分别称为图G的**最大度**和**最小度**，简记为：Δ，δ。

1736年欧拉给出握手定理，是图论的基本定理。

定理 5.1

每一个图结点度数的总和等于边数的两倍。

由于每条有向边在计算入度和出度时各只计算一次，所以有如下定理：

定理 5.2

在任意有向图中，所有结点入度之和等于所有结点出度之和，都等于边数。

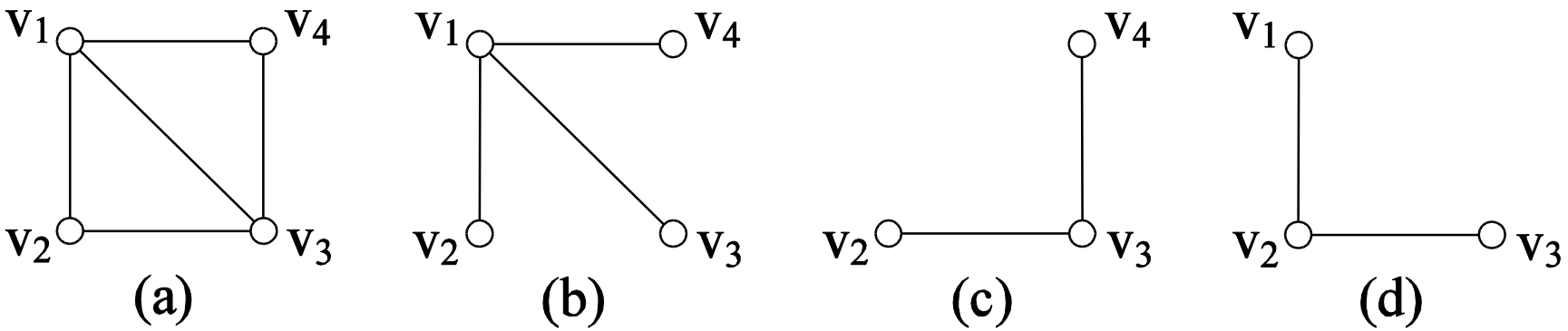
5.2 图的基本概念及矩阵表示

定义 5.6

设$G=<V,E>$和$G'=<V',E'>$是两个图，若满足$V'\subseteq V$且$E'\subseteq E$，则称G'是G的**子图**。特别地，当$V'=V$时，称G'是G的**生成子图**；当$V'\subset V$或$E'\subset E$时，称G'是G的**真子图**；当$V'=V$且$E'=E$或$E'=\emptyset$时，称G'是G的**平凡子图**；对任意$u\in V',v\in V'$，若$(u,v)\in G$必有$(u,v)\in G'$，或边$<u,v>\in G$必有$<u,v>\in G'$，称G'是G的**导出子图**。

back

5.2 图的基本概念及矩阵表示



上图中（b）是（a）的生成子图，（c）是（a）的导出子图，（d）是（a）的子图，但不是生成子图，也不是导出子图。

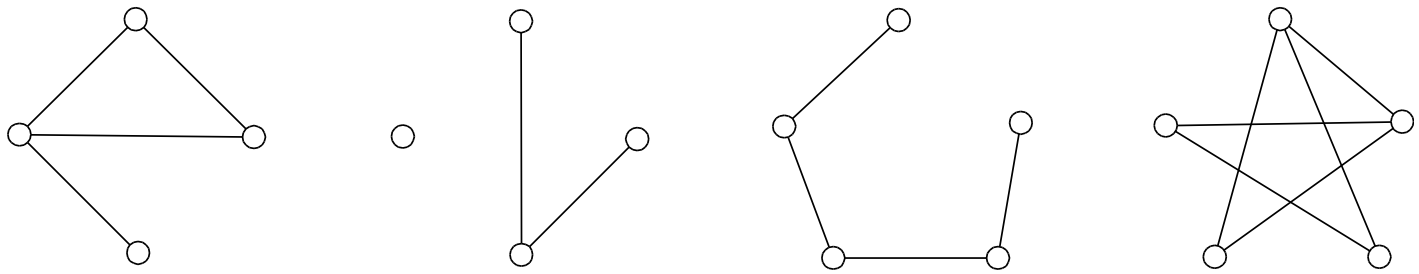
back

5.2 图的基本概念及矩阵表示

定义 5.7

设$G=<V,E>$为n阶无向简单图，令
$\overline{E}=\{(u,v)|u\in V\wedge v\in V\wedge u\neq v\wedge <u,v>\notin E\}$
称$\overline{G}=<V,\overline{E}>$为$G$的**补图**。

显然，图G也是图$\overline{G}$的补图，称它们互为补图。图（a）与图（b）互为补图，图（c）与图（d）互为补图。



back

5.2 图的基本概念及矩阵表示

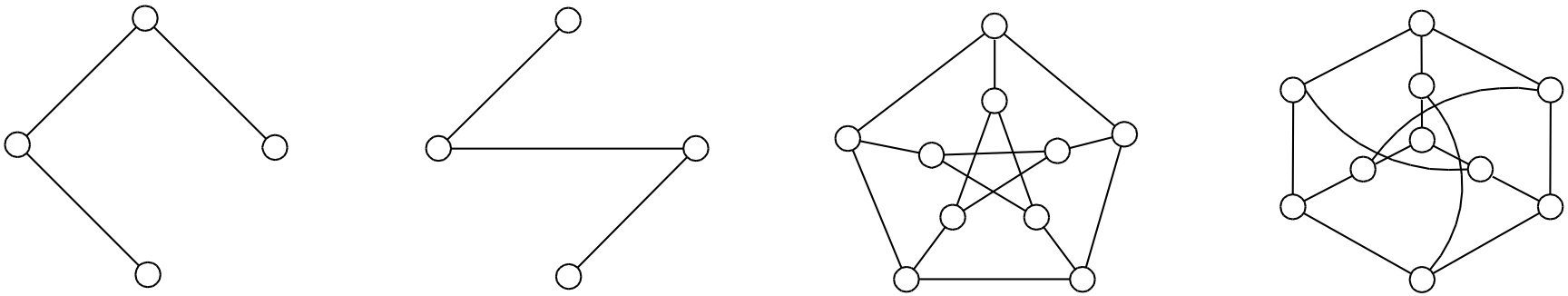
一个图的图形表示不一定是唯一的，但有很多表面上看来似乎不同的图却可以有着极为相似图形表示，这些图之间的差别仅在于结点和边的名称的差异，而从邻接关系的意义上看，它们本质上都是一样的，可以把它们看成是同一个图的不同表现形式，这就是图的同构概念。同构的图有同样的性质，可以作为同一类图来研究。

定义 5.8

设$G=<V,E>$和$G'=<V',E'>$是两个图，如果存在双射$\varphi:V\to V'$，使得
$(u,v)\in E\Leftrightarrow(\varphi(u),\varphi(v))\in E'$
或$<u,v>\in E\Leftrightarrow<\varphi(u),\varphi(v)>\in E'$，则称图$G$和图$G'$**同构**，并记之为$G\cong G'$。

5.2 图的基本概念及矩阵表示

图（a）和图（b）同构，图（c）和图（d）同构图。
图（c）和图（d）叫做彼得松（*Peterson*）图。



back

5.2 图的基本概念及矩阵表示

定义 5.9

设$G=<V,E>$是一n阶图，构造矩阵$A=(a_{ij})_{n\times n}$，其中，

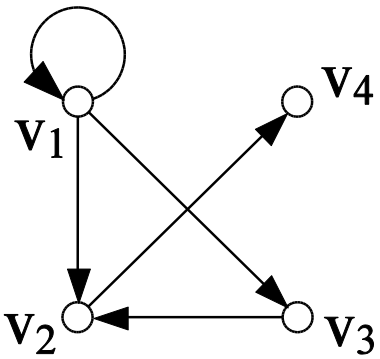
$$a_{ij}=\begin{cases}1 & <v_i,v_j>\in E\text{或}(v_i,v_j)\in E\text{或}(v_j,v_i)\in E\\ 0 & <v_i,v_j>\notin E\text{且}(v_i,v_j)\notin E\end{cases}$$

则称A为有向图G的**邻接矩阵**。

back

5.2 图的基本概念及矩阵表示

无向图的邻接矩阵是个对称阵，第i行元素之和恰为结点v_i的度。有向图的邻接矩阵一般不对称，第i行元素之和是结点v_i的出度，第j列元素之和是结点v_j的入度。
左图的邻接矩阵如右所示。



$$A=\begin{bmatrix}1&1&1&0\\0&0&0&1\\0&1&0&0\\0&0&0&0\end{bmatrix}$$

5.2 图的基本概念及矩阵表示

定义 5.10

设无向图$G=(V,E)$，$V=\{v_1,v_2,\cdots,v_n\}$，$E=\{e_1,e_2,\cdots,e_m\}$，令m_{ij}为顶点v_i与边e_j的关联次数，则称$M=(m_{ij})_{n\times m}$为**无向图G的关联矩阵**，记作$M(G)$。

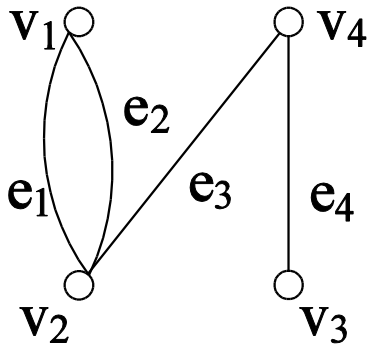
设有向图$G=(V,E)$中无环，$V=\{v_1,v_2,\cdots,v_n\}$，$E=\{e_1,e_2,\cdots,e_m\}$，令

$$m_{ij}=\begin{cases}1 & v_i\text{为}e_j\text{的始点}\\ 0 & v_i\text{与}e_j\text{不关联}\\ -1 & v_i\text{为}e_j\text{的终点}\end{cases}$$

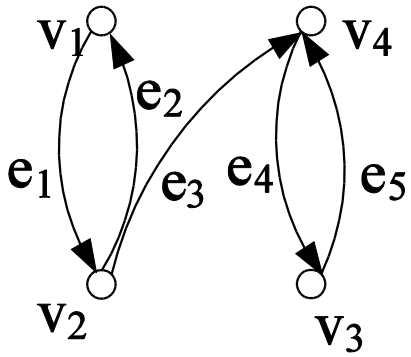
则称$M=(m_{ij})_{n\times m}$为**有向图G的关联矩阵**，记作$M(G)$。

back

5.2 图的基本概念及矩阵表示



G_1



G_2

图G_1和G_2的关联矩阵分别是：

$$M_1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \quad M_2 = \begin{bmatrix} 1 & -1 & 0 & 0 & 0 \\ -1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 \\ 0 & 0 & -1 & 1 & -1 \end{bmatrix}$$

back

5.3 路与连通度

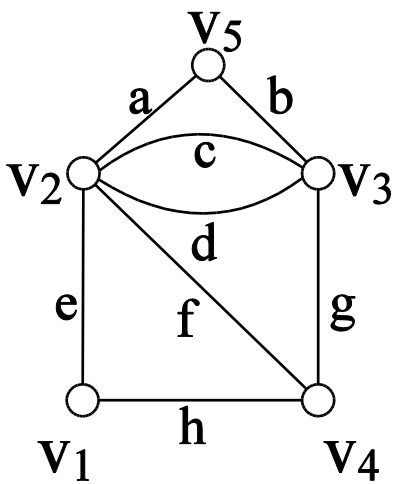
定义 5.11

无向图（或有向图）$G=<V,E>$中的非空结点和边的交替序列$p=v_0e_1v_1e_2v_2,\cdots,e_kv_k$，称为$G$的一条由起点$v_0$到终点$v_k$的**路（或有向路）**，这里对所有的$1\leqslant i\leqslant k$，边$e_i$的起点是$v_{i-1}$，终点是$v_i$，边的数目$k$是路的长度。

当起点和终点相同时，这条路称作**回路**。若一条路中所有的边均不相同，这条路称作**迹**。若一条路中所有的结点均不同，这条路称作**通路**。闭的通路，即除$v_0=v_k$外，其余的结点均不相同的路，就称作**圈**或**回路**。长度为奇数的圈称为**奇圈**，长度为偶数的圈称为**偶圈**。

back

5.3 路与连通度



图中$v_2fv_4gv_3bv_5av_2ev_1$是长度为5的路，$v_2fv_4gv_3bv_5av_2$是长度为4的回路，这二条路也是迹，但$v_2fv_4gv_3bv_5av_2ev_1$不是通路，$v_2fv_4gv_3bv_5av_2$是圈，是偶圈。

5.3 路与连通度

定义 5.12

设$G=<V,E>$是一n阶无向图，构造矩阵$P=(p_{ij})_{n\times n}$，其中，

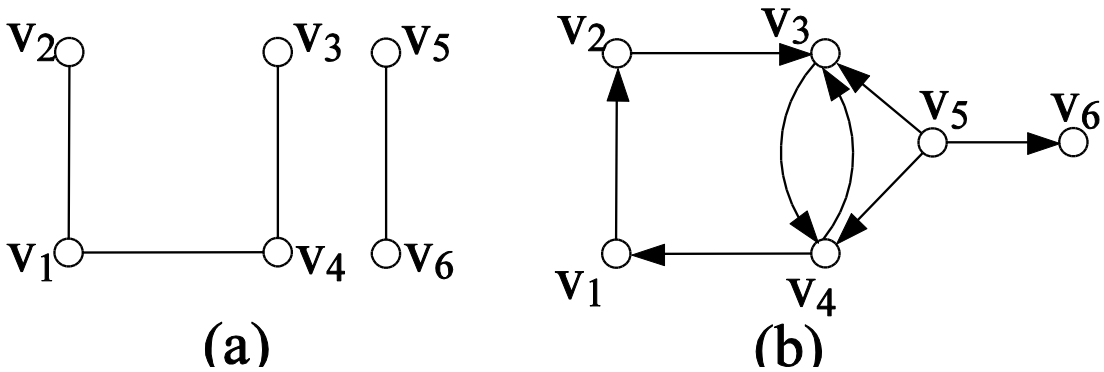
$$p_{ij}=\begin{cases}1 & \text{从}v_i\text{到}v_j\text{存在一条路，或i=j}\\ 0 & \text{从}v_i\text{到}v_j\text{不存在路，}\end{cases}$$

称矩阵P为**可达性矩阵**。

如果是有向图，则将路改为有向路即可。

求可达性矩阵可用$Warshell$算法。

5.3 路与连通度



图（a）和图（b）的可达性矩阵分别为：

$$P_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}, \quad P_2 = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

5.3 路与连通度

定理 5.3

在一个具有n个结点的图中，如果从结点u到结点v存在一条路，则从结点u到结点v存在一条不多于$n-1$条边的路。

推论 在具有n个结点的圈中，若从结点v_j到结点v_k存在一条路，则存在一条从结点v_j到结点v_k不多于n条边的路。

back

5.3 路与连通度

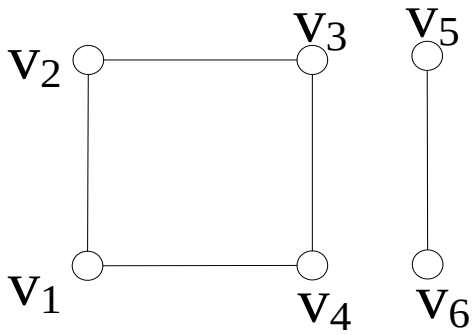
定理 5.4

在一个具有n个结点的图中，如果从结点u到自身存在一条回路，则从结点u到自身存在一条不多于n条边的回路。

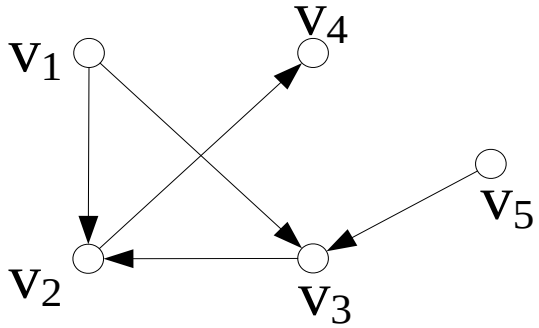
在一个无向图G中，结点u和v之间若存在一条路，则称结点u和v在G中是**连通**的。在有向图中，结点u到v有一条有向道路，则称u 到v是有向连通的，或称为u可达于v，记为$u \to v$。有向连通性又称为**可达性**。

back

5.3 路与连通度



(a)



(b)

图中v_1、v_2、v_3、v_4彼此都是连通的，但v_1与v_5不连通。
（b）中v_1可达v_4，但v_4 不可达v_1。
在一个无向图中，连通作为一种关系满足自反性，对称性和传递性，连通作为一种关系是等价关系。
在一个有向图中，连通作为一种关系只满足自反性和传递性，不具备对称性，所以它不是等价关系。

5.3 路与连通度

定义 5.13

对应于无向图连通关系，存在着图G的结点集V的一个划分$V_1, V_2, \cdots, V_k$，使得G中任何两个结点u和v连通当且仅当u和v属于同一个分块$V_i(1 \leqslant i \leqslant k)$，这个划分就是顶点集$V$关于顶点之间的连通关系作为一种等价关系的一个等价类。称导出子图$G(V_i)$为G的一个**连通分支**。连通分支是G的极大连通子图。图G的**连通分支数**记为$\omega(G)$。

无向图中任何二点都是连通的图(只有一个连通分支)称为**连通图**，连通分支数大于1的图称为非连通图。上一页图（a）中有二个连通分支，$V_1 = \{v_1, v_2, v_3, v_4\}$，$V_2 = \{v_5, v_6\}$，它不是个连通图。

5.3 路与连通度

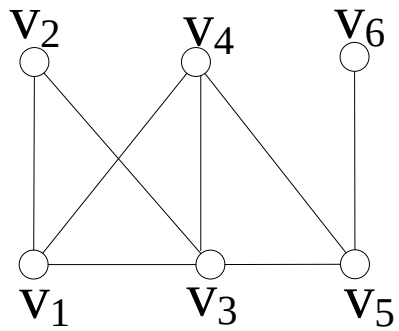
定义 5.14

设$G=<V,E>$是无向图，若存在$V' \subseteq V$，使$\omega(G-V') > \omega(G)$，且对于任意的$V'' \subset V'$，均有$\omega(G-V'')=\omega(G)$，则称V'是G的一个**点割集**；特别地，当v是G的点割集时，称点v是G的**割点**。

设$G=<V,E>$是无向图，若存在$E' \subseteq E$，使$\omega(G-E') > \omega(G)$，且对于任意的$E'' \subset E'$，均有$\omega(G-E'')=\omega(E)$，则称E'是G的一个**边割集**（简称割集）。特别地，当e是G的边割集时，称边e是G的**割边或桥**。

back

5.3 路与连通度



图中$\{v_3, v_4\}$是一个点割集，$\{v_1, v_3, v_4\}$不是一个点割集。v_5是割点。显然，完全图K_n没有点割集，它的连通性能是最好的。

$E' = \{(v_1, v_2), (v_1, v_3), (v_1, v_4)\}$是一个边割集，但

$E'' = \{(v_1, v_2), (v_1, v_3), (v_1, v_4), (v_2, v_4)\}$不是一个边割集。

边(v_5, v_6)是割边。

back

5.3 路与连通度

定义 5.15

设图G是无向连通图，则称$\kappa(G)=\min\{|V'||V'$为G的点割集$\}$为G的**点连通度**，$\kappa(G)$有时简记为κ，又若$\kappa(G)\geqslant k(k\geqslant 1)$，则称$G$为$k$连通图。

点连通度是由连通图G产生一个非连通子图，或由K_n产生一个结点的子图所需要删去的最少的结点的数目，显然，$\kappa(K_n)=n-1$。非连通图的点连通度为0。

back

5.3 路与连通度

定义 5.16

设图G是无向连通图，则称

$\lambda(G)=\min\{|E'||E'$为G的边割集$\}$
为G的**边连通度**，$\lambda(G)$有时简记为λ，又若
$\lambda(G)\geqslant r(r\geqslant 1)$，则称$G$为$r$边连通图。 前二页的图点连通度和边连通度都是1。边连通度是由连通图G产生一个非连通子图所需要删去的最少的边的数目。

定理 5.5

对于任何图G，皆有$\kappa(G)\leqslant\lambda(G)\leqslant\delta(G)$。

5.3 路与连通度

下面讨论有向图的连通性。

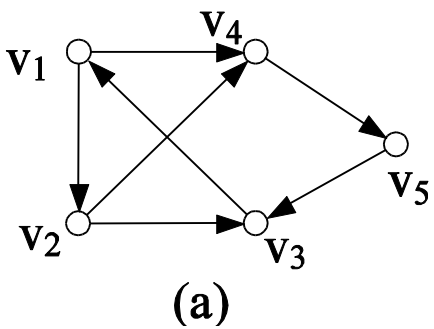
定义 5.17

简单有向图$G=<V,E>$中，任意一对结点间，至少有一个结点到另一个结点是可达的，则称这个图为**单侧连通图**。如果对于图G中的任意两个结点两者之间是互相可达的，则称这个图为**强连通图**。如果在图G中略去方向，将它看成是无向图，图是连通的，则称该有向图为**弱连通图**，弱连通图简称为连通图。

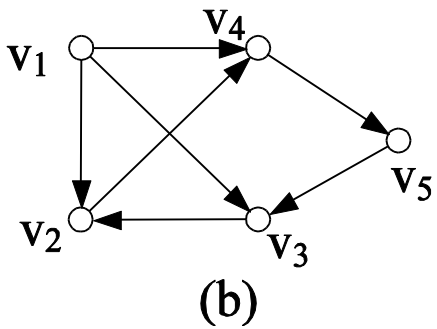
从前面的定义可以看出，强连通图必是单侧连通的，单侧连通必是弱连通的。它们的逆命题都不真。

back

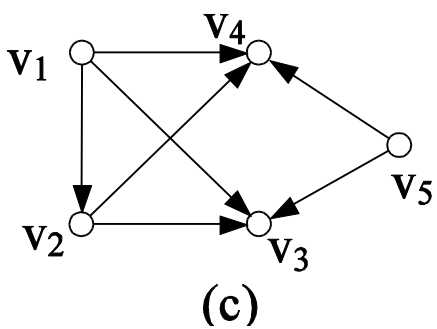
5.3 路与连通度



(a)



(b)



(c)

图中（a）是强连通图，（b）是单侧连通图，（c）是弱连通图。

back

5.3 路与连通度

定理 5.6

一个有向图是强连通的，当且仅当G中有一个回路，它至少包含每个结点一次。

定理 5.7

一个有向图是单向连通的，当且仅当G中有一个经过每个结点至少一次的通路。

back

5.3 路与连通度

定义 5.18

设u和v是图G中的两个结点，若u到v存在路，称u到v之间的最短道路之长为u到v之间的**距离**，记之为$d(u,v)$。若u到v没有路，规定$d(u,v)=\infty$。

在处理有关图的实际问题时，往往有值的存在，比如公里数，运费，城市，人口数以及造价等。一般这个值称为**权值**。

设图$G=<V,E>$，对G的每一条边e，给定一个数值$W(e)$，称为边e的权，把这样的图称为**带权图**，记为$G=<V,E,W>$。带权图有时也称赋权图或网络。

back

5.3 路与连通度

定义 5.19

给定非负带权图$G =< V, E, W >$及顶点u和v，求从顶点u到v的最短路的方法称为**最短路问题**。

不难看出，如果$v_0v_1v_2, \cdots, v_k$是从$u = v_0$到$v = v_k$的最短路，则对每一个$t(1 \leqslant t \leqslant i-1)$，$v_0v_1v_2, \cdots, v_t$，也是$u = v_0$到$v = v_t$的最短路。这叫最优性原理。

back

5.3 路与连通度

据最优性原理，*E.W.Dijkstra*1959年给出了最短路算法。算法给出从起点s到每一点的最短路径。计算过程中，赋予每一个顶点v一个标号$l(v) = (l_1(v), l_2(v))$。标号分永久标号和临时标号。在v的永久标号$l(v)$ 中，$l_2(v)$ 是从 s 到v的距离，$l_1(v)$是从s到v的最短路径上v的前一个顶点。当$l(v)$是临时标号时，$l_1(v)$和$l_2(v)$分别是从s经过永久标号的标点到v的长度最短路径上v的前一个顶点和这条路径的长度。

back

5.3 路与连通度

Dijkstra标号法

输入：带权图$G=<V,E,W>$和$s\in V$，其中$|V|=n,\forall e\in E,W(e)\geqslant 0$

输出：s到G中每一顶点的最短路径及距离

1.令$l(s)\leftarrow(s,0),l(v)\leftarrow(s,+\infty)(v\in V-s),i\leftarrow 1,l(s)$是永久标号，其余标号均为临时标号，$u\leftarrow s$;

2.*for*与u关联的临时标号的顶点v;

3.*if* $l_2(u)+W(u,v)<l_2(v)$ *then*令$l(v)\leftarrow(u,l_2(u)+W(u,v))$;

4.计算$l_2(t)=min\{l_2(v)|v\in V$且有临时标号$\}$，把$l(t)$改为永久标号;

5.*if* $i<n$ *then*令$u\leftarrow t,i\leftarrow i+1$转2;

计算结束时，对每一个顶点$u,d(s,u)=l_2(u)$，利用$l_1(u)$从u开始回溯找到从u到v的最短路径。

5.3 路与连通度

*E.W.Dijkstra*的最短路算法只能计算给定起始点到终点的最短路，如果要计算任意二点间的最短路，这个算法就有缺陷了。

*Robert W.Floyd*在1962年找出了一个有n个节点的加权连通图中任意二点间最短距离的算法。

*Floyd*算法通过求n个n阶矩阵$D^{(1)},\cdots,D^{(k-1)},D^{(k)},\cdots,D^{(n)}$来计算一个$n$节点加权图的最短距离矩阵，最后的$D^{(n)}$便是任何二点间的最短路矩阵，相应地可以得到$n$个$n$阶路径回溯矩阵$R^{(1)},\cdots,R^{(k-1)},R^{(k)},\cdots,R^{(n)}$。

矩阵$D^{(k)}$表示矩阵中任意一对节点间的最短路径长，矩阵$R^{(k)}$相应表示任意一对节点间的最短路径回溯矩阵，该路径上的最大编号节点不大于k。

5.3 路与连通度

令

$$d_{ij}^{(0)} = w_{ij}$$

$$r_{ij}^{(0)} = \begin{cases} i & if\ w_{ij} \neq \infty \\ \infty & 否则 \end{cases} \quad 对1 \leqslant k \leqslant n$$

计算

$$d_{ij}^{(k)} = min\{d_{ij}^{(k-1)}, d_{ik}^{(k-1)} + d_{kj}^{(k-1)}\}$$

$$r_{ij}^{(k)} = \begin{cases} k & d_{ij}^{(k-1)} > d_{ik}^{(k-1)} + d_{kj}^{(k-1)} \\ r_{ij}^{(k-1)} & 否则 \end{cases}$$

从定义可知，矩阵R中r_{ij}的值是从v_i到v_j的最短路径上紧跟v_i后的一个点的序号，从而可以回溯v_i到v_j的最短路径。

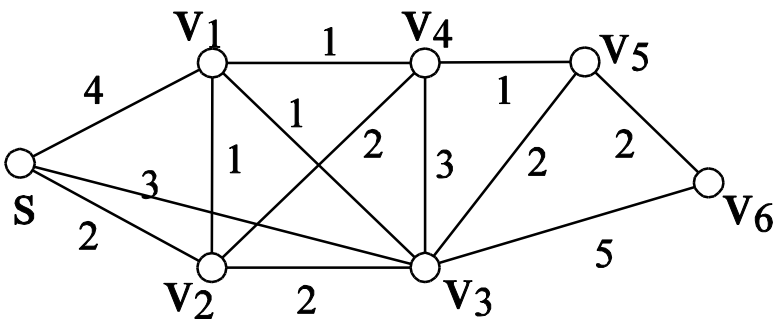
back

5.3 路与连通度

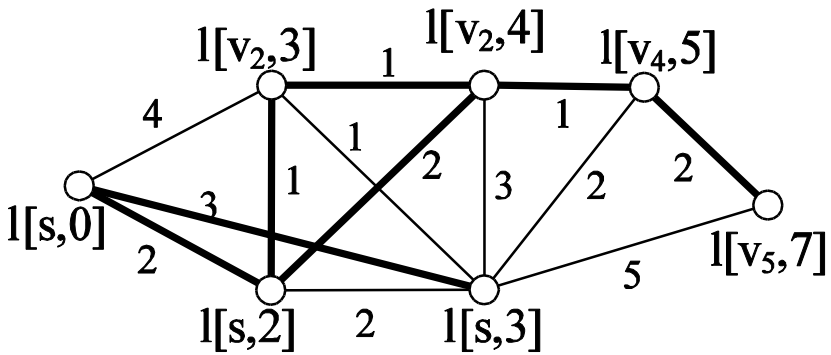
例 5.1

用Dijkstra算法求图（a）中点s到其它各点的最短距离。

由算法得出的最短路径如下图（b）所示，s到v_6的路径是$sv_2v_4v_5v_6$或$sv_2v_1v_4v_5v_6$，最短距离为7。



(a)



(b)

5.4 欧拉图与哈密尔顿图

欧拉在1736年解决著名的哥尼斯堡七桥难题中，建立了欧拉图类存在性的完整理论。图论的研究方法也随之进入了数学的广大领域。

定义 5.20

经过图中所有顶点且每条边恰好经过一次的通路叫**欧拉通路**，经过图中所有顶点且每条边恰好经过一次的回路叫**欧拉回路**，有欧拉回路的图叫**欧拉图**，具有欧拉通路但没有欧拉回路的图叫**半欧拉图**。

back

5.4 欧拉图与哈密尔顿图

判断一个图是不是欧拉图，方法比较简单，有如下的定理。

定理 5.8

无向图G为欧拉图当且仅当G连通且无奇度顶点。

定理 5.9

无向图G是半欧拉图当且仅当G连通且恰有两个奇度顶点。

back

5.4 欧拉图与哈密尔顿图

定理 5.10

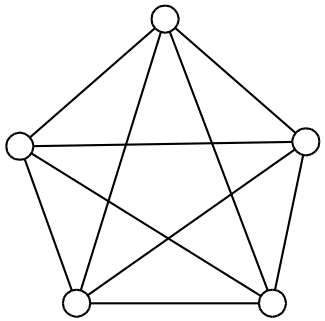
有向图D是欧拉图当且仅当D连通且每个顶点的入度都等于出度。

定理 5.11

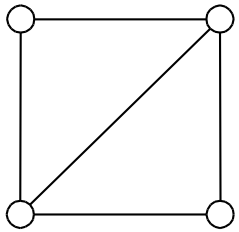
有向图D是半欧拉图当且仅当D连通且恰有两个奇度顶点，其中一个入度比出度大1，另一个出度比入度大1，其余顶点的入度等于出度。

判断一个图是不是能一笔画出，其实就是判断这个图是不是具有欧拉通路或具有欧拉回路。

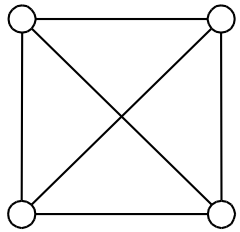
5.4 欧拉图与哈密尔顿图



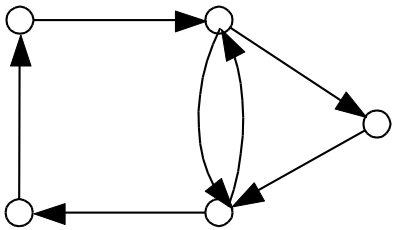
(a)



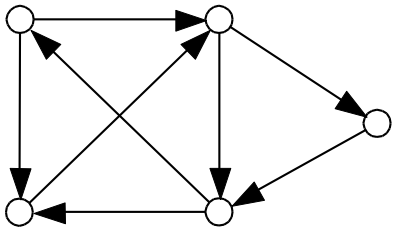
(b)



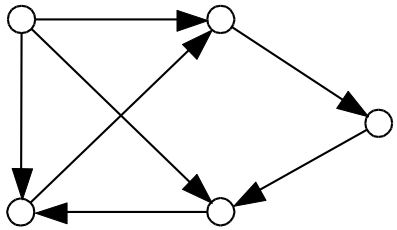
(c)



(d)



(e)



(f)

上图中（a）（d）是欧拉图，（b）（e）是半欧拉图，（c）（f）不是欧拉图。

5.4 欧拉图与哈密尔顿图

定义 5.21

经过图中所有顶点一次且仅一次的通路叫**哈密顿通路**，经过图中所有顶点一次且仅一次的回路叫**哈密顿回路**，具有哈密顿回路的图叫**哈密顿图**，具有哈密顿通路但没有哈密顿回路的图叫**半哈密顿图**。

back

5.4 欧拉图与哈密尔顿图

对于判断一个图是不是哈密顿图，到目前为止，还没有找到充分必要条件。下面的定理是判断哈密顿图的充分条件或必要条件。

定理 5.12

设无向图$G=<V,E>$是哈密顿图，则对结点V的每一个非空子集S，均有$\omega(G-S)\leqslant|S|$。

推论 设无向图$G=<V,E>$是半哈密顿图，则对结点V的每一个非空子集S，均有$\omega(G-S)\leqslant|S|+1$。

5.4 欧拉图与哈密尔顿图

定理 5.13

设G是$n(n \leqslant 3)$阶无向简单图，若任意两个不相邻的顶点的度数之和大于等于$n-1$，则G中存在哈密顿通路。

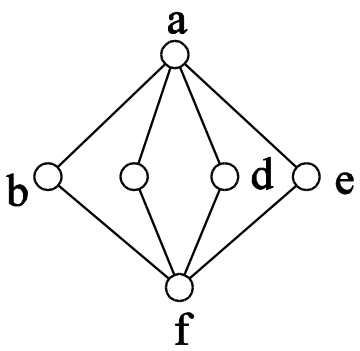
推论 若任意两个不相邻的顶点的度数之和大于等于n，则G中存在哈密顿回路，即G为哈密顿图。

显然，k_n都是哈密顿图。

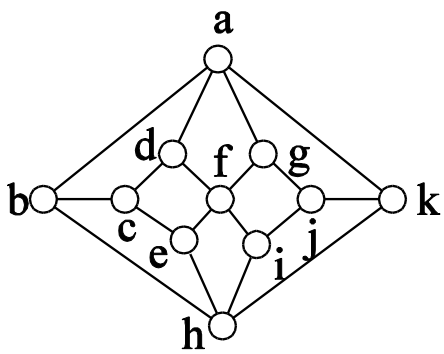
至今还没有找到解决哈密顿回图存在性问题的有效算法。

back

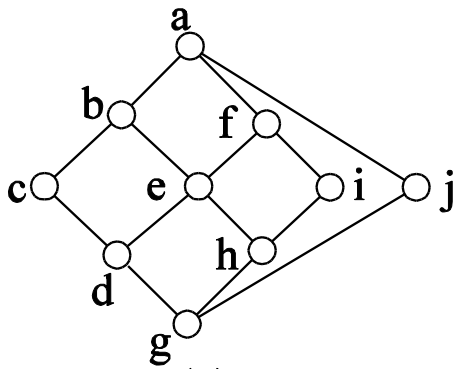
5.4 欧拉图与哈密尔顿图



(a)



(b)



(c)

上图中哪个是哈密顿图，哪个是半哈密顿图，哪个不是密顿图？为什么？

back

5.5 二部图与匹配

定义 5.22

设无向图$G =< V, E >$，若能将V划分成非空的二个子集V_1和$V_2(V_1 \cup V_2 = V, V_1 \cap V_2 = \emptyset)$，使得$G$中的每条边的两个端点都是一个属于$V_1$，另一个属于$V_2$，则称$G$为**二部图(二分图，偶图)**，称$V_1$和$V_2$为**互补顶点集**，常将二部图记为$G =< V_1, V_2, E >$。若$G$为简单二部图，$V_1$中每个顶点均与$V_2$中所有顶点相邻，则称$G$为**完全二部图**，记为$K_{r,s}$，其中$r = |V_1|$，$s = |V_2|$。

back

5.5 二部图与匹配

定理 5.14

一个无向图G是二部图当且仅当G中无奇数长度的回路。

可用结点标记法判断已知图G是否为二部图。

back

5.5 二部图与匹配

定义 5.23

设$G=<V_1,V_2,E>$是二部图，若$E^* \subseteq E$，且E^*中任意两条边都是不相邻的，则E^*称为G的一个**匹配（边独立集）**，若在E^*中再加入任何一条边都不是匹配，称E^*为**极大匹配**，边数最多的极大匹配为**最大匹配**，最大匹配中边的条数称为G的**匹配数**，记为β。令M是G的一个匹配，若结点v与M中的边关联，则称v是***M*饱和点**；否则称v是***M*非饱和点**；若G中的每个结点都是M饱和点，则称M是**完美匹配**。

显然，每个完美匹配是最大匹配，但反之不真。

back

5.5 二部图与匹配

定义 5.24

设$G =< V_1, V_2, E >$为一个二部图，M为G中一个最大匹配，若$|M| = min\{|V_1|, |V_2|\}$，称$M$为$G$中的一个**完备匹配**，且若$|V_1| \leqslant |V_2|$，称$M$为$V_1$到$V_2$的一个完备匹配；若$|V1| = |V2|$，此时$M$为$G$的完美匹配；

显然，完美匹配是完备匹配，反之不真。

定理 5.15

（*Hall*定理）设二部图$G =< V_1, V_2, E >$，$|V_1| \leqslant |V_2|$，G中存在从V_1到V_2的完备匹配当且仅当V_1中任意k个顶点至少邻接V_2中的k个顶点。（相异性条件）

5.5 二部图与匹配

定理 5.16

设二部图$G =< V_1, V_2, E >$，如果:（1）V_1中每个顶点至少关联$t(t > 0)$条边；（2）V_2中每个顶点至多关联t条边（t条件）；则G中存在V_1到V_2的完备匹配。

满足t条件的二部图一定满足相异性条件；反之不真。
二部图的最大匹配运用较广，许多问题可以转化为在一个二部图中寻求最大匹配，譬如集合划分问题，不同类型的排序问题，指派问题，边覆盖问题，边着色问题，排课问题，高级运输问题等等。

back

5.5 二部图与匹配

定义 5.25

求二部图的最大匹配问题运用迭代改进技术。即先求一个初始匹配，再寻求增益路径。设U和V是二部图$G =< V, E >$的二个互补顶点集，M是一个初始匹配。如果G有一条简单路径起点连着U中的M非饱和点，而终点连着V中的M非饱和点，路径上的边交替出现在$E - M$和M中，即路径的第一条边不在M，第二条边在M中，第三条边不在M，以此类推，直到最后一条边不在M中。

这样的路径称为M的**增益路径**。

back

5.5 二部图与匹配

求一个初始匹配的方法如下：

（1）初始化$Q \leftarrow U$，$R \leftarrow V$，$M \leftarrow \emptyset$，$i \leftarrow 1$。

（2）若$i = |U| + 1$，结束。否则，取$u_i \in Q$。

（3）找$v_i \in R$，使得$(u_i, v_i) \in E$，若不存在这样的v_i，令$i \leftarrow i + 1$，转（2）。否则

（4）令$M \leftarrow M \cup \{(u_i, v_i)\}$，$Q \leftarrow Q - u_i$，$R \leftarrow R - v_i$，$i \leftarrow i + 1$，转（2）。

back

5.5 二部图与匹配

寻求增益路径的方法类似图的深度优先搜索：

（1）初始化Q为U中所有M非饱和点。

（2）若$Q=\varnothing$，终止。否则，初始化S为V中所有未标记点，即$S\leftarrow V$，$i\leftarrow 1$，取$u_i\in Q$。

（3）$Q\leftarrow Q-u_i$，取$v_i\in S$且$(u_i,v_i)\in E$，若v_i不存在或v_i是V中最后一个点且v_i是M饱和的，则从u_1开始没有M增益路径，转（2）。若v_i存在且v_i是M非饱和的，则找到一条增益路，令$M\leftarrow M\cup\{(u_i,v_i)\}$，转（2）。否则

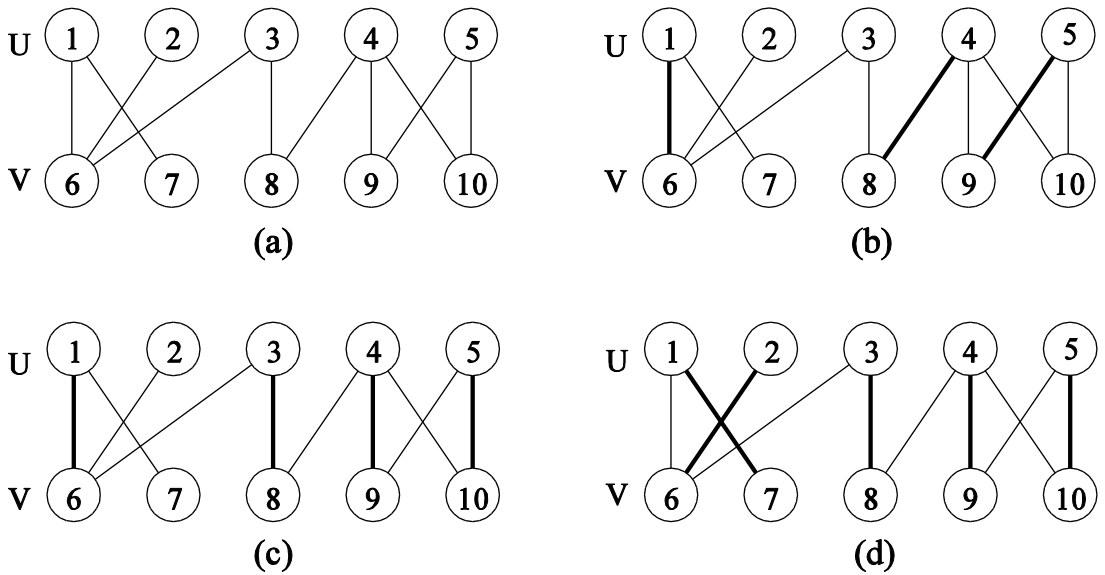
（4）v_i是M饱和点，设$(u_{i+1},v_i)\in M$，令
$M\leftarrow M\cup(u_i,v_i)$，$M\leftarrow M-(u_{i+1},v_i)$，$S\leftarrow S\cup\{v_i\}$。
$i\leftarrow i+1$，转（3）。

back

5.5 二部图与匹配

例 5.2

求下图（a）中的最大匹配。



back

5.5 二部图与匹配

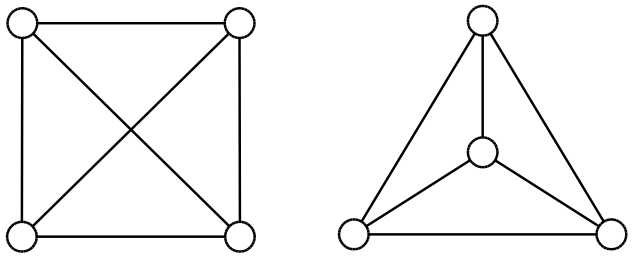
解（1）先求图中的初始匹配，得图（c）。(2)在图（c）中找一条增益路径，它是$2,6,1,7$，将边$(1,6)$从M中删除，将边$(2,6),(1,7)$ 加入M 中，得到图（d），这时M已经是最大匹配，它还是完美匹配。

back

5.6 平面图

定义 5.26

若简单图$G = < V, E >$的图形在平面上能画成如下形式：(1)没有两个结点重合；(2)除结点外每条边不相交。则称G是具有平面性的图，或简称为**平面图**。



上图是k_4的二个图形，（a）图有二条边相交，但我们可以画成（b）的平面性图，所以k_4是平面图。

5.6 平面图

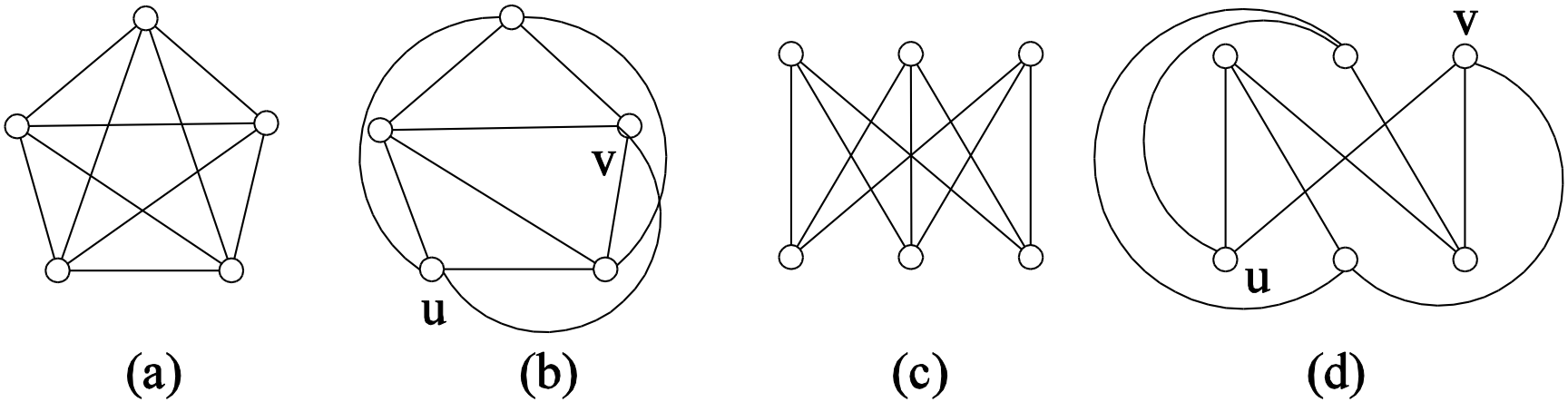
图的平面性问题有着许多实际的应用。例如在电路设计中常常要考虑布线是否可以避免交叉以减少元件间的互感影响。如果必然交叉，那么怎样才能使交叉处尽可能的少？或者如何进行分层设计，才使每层都无交叉？这些问题实际都与图的平面表示有关。

确实存在着大量的图，它们没有对应的平面图形表示。例如K_5和$K_{3,3}$，无论怎么画，总会出现边的交叉，这样的图称为非平面图。

back

5.6 平面图

下图（a）是K_5，（c）是$K_{3,3}$，它们可以画成（b）和（d）的形式，但（b）和（d）二个图的边(u,v)无论怎么画，总会与其它的边交叉，所以K_5和$K_{3,3}$是非平面图。



back

5.6 平面图

定义 5.27

设G是一个平面图。若G的图形中由边围城的封闭区域不能再分割成两个或两个以上的包含更少边数的子区域，则称这个封闭区域为G的**面**，包围这个区域的边称为**面的边界**，其中有一个面的区域为这个平面图的外部边界组成，这个面称为**外部面**。面的边界中的边数称为**面的度**（割边在计度时算作两条边）。

若一条边不是割边，它必是两个面的公共边界；割边只能是一个面的边界。两个以一条边为公共边界的面称为**相邻的面**。

back

5.6 平面图

平面图的结点数v，边数e以及面的数目r之间有着密切的关系，这就是重要的**欧拉公式**。

定理 5.17

(欧拉公式)设连通平面图$G=<V,E>$的顶点数，边数和面数分别为v，e和r，则有$v-e+r=2$。

推论 设平面图$G=<V,E>$有k个连通分支，它的顶点数，边数和面数分别为v，e和r，则有$v-e+r=k+1$。

由于在计算G的面的度时，每条边被计算了两次，因此有下面定理。

back

5.6 平面图

定理 5.18

设G是连通简单平面图，则面的度之和等于边数的二倍。

由 欧拉公式可得：

定理 5.19

设G是一个阶数大于2的连通简单平面图，顶点数和边数分别为v，e，则$e \leqslant 3v - 6$。

推论 在任何简单连通平面图中，至少存在一个其度不超过5的结点。

由上面定理及其证明方法，可以证明$K_{3,3}$和K_5都是非平面图

5.6 平面图

在图G的边(u,v)上新增加一个2度结点w，称为图G的细分，所得的新图称为原图的细分图。容易知道，若G'是G的细分图，则G'与G同为平面图或同为非平面图。

定理 5.20

*(Kuratowski)*一个图是平面图当且仅当它不包含与K_5 和$K_{3,3}$的细分图同构的子图。

例 5.3

证明*Petersen*图不是平面图。

back

5.6 平面图

在图论发展史上，“四色问题”曾经起过巨大的推动作用。所谓“四色问题”，就是考虑在一张各国地域连通，并且相邻国家有一段公共边界的平面地图上，是否可以用四种颜色为地图着色，使得相邻国家着有不同的颜色。这是一个著名的数学难题，一百多年中曾吸引过许多优秀的数学家，但是谁也未能从理论上严格证明这个问题的答案是肯定的。直到1979年才由美国的*K.Appel*和*W.Haken*利用计算机给出了证明，宣布这一问题得到了解决。在理论研究中，虽然未能证明“四色定理”，然而1890年*Heawood*在*Kempe* 证明方法的基础上建立了五色定理。

back

5.6 平面图

从下面对偶图的定义可以得出，平面图的平面着色可以转化为它的对偶图的顶点着色。顶点着色已有比较成熟的定理和方法。

定义 5.28

设$G=<V,E>$是一个平面图，构造图$G^*=<V^*,E^*>$如下：

（1）G的面$f_1,f_2,\cdots,f_k$与V^*中的点$v_1^*,v_2^*,\cdots,v_k^*$一一对应；
（2）若面f_i和面f_j邻接，则v_i^*与v_j^*邻接；
（3）若G中有一条边e只是面f_i的边界，则v_i^*有一环。

称图G^*是G的**对偶图**。

如果图G的对偶图G^*同构于G，则称G是**自对偶的**。

5.6 平面图

定义 5.29

图G的顶点正常着色（或简称为着色）是指对它的每一个结点指定一种颜色，使得没有两个相邻的结点有同一种颜色。如果图G在着色时用n种颜色，我们称G为**n-色的**或**n-色图**。对图G进行着色时，需最少颜色数称为**着色数**，记作$\chi(G)$。

back

5.6 平面图

虽然到现在还没有一个简单通用的方法，可以确定任一图G是否是n-色的。但我们可用**韦尔奇.鲍威尔法**（*WelchPowell*）对图G进行着色，其方法是：

(1)将图G的结点按照度数的递减次序进行排列（这种排列可能并不是唯一的，因为有些点有相同的度数）。

(2)用第一种颜色对第一点进行着色，并且按排列次序，对前面着色点不邻接的每一点着上同样的颜色。

(3)用第二种颜色对尚未着色的点重复(2)，用第三种颜色继续这种做法，直到所有的点全部着上色为止。

back

5.6 平面图

定理 5.21

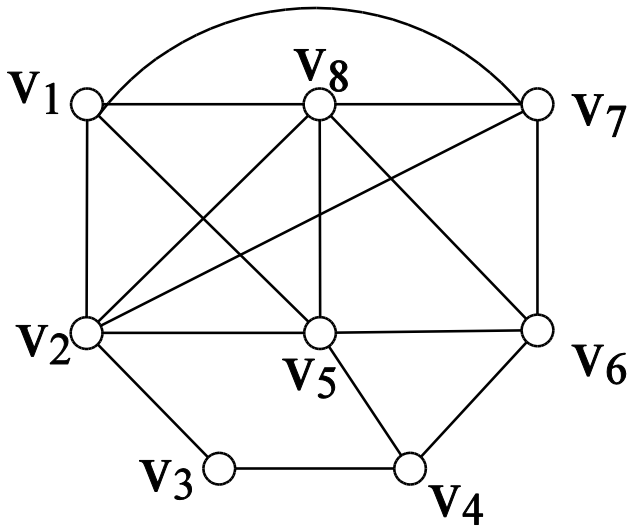
任意连通平面图G最多是5-色的。

back

5.6 平面图

例 5.4

用韦尔奇.鲍威尔法对下图着色。



可以得出，图G是四色的，所以$\chi(G)=4$。

back

5.7 树

树是图论中最主要的概念之一，而且是最简单的图之一。它在计算机科学中应用非常广泛。

定义 5.30

一个连通且无回路的无向图称为**树**。在树中度数为*1*的结点称为**树叶**，度数大于*1* 的结点称为**分枝点**或**内点**。如果一个无回路的无向图的每一个连通分图是树，称为**森林**。

back

5.7 树

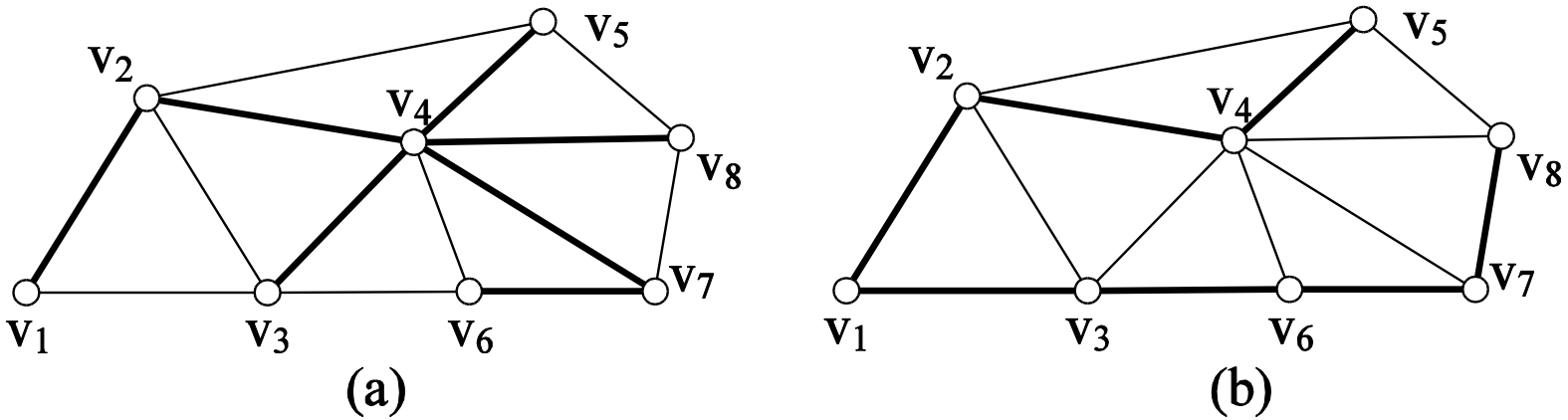
给定图T，以下关于树的定义是等价的：
(1)无回路的连通图；
(2)无回路且$e = v - 1$，其中e为边数，v为结点数；
(3)连通且$e = v - 1$；
(4)无回路且增加一条新边，得到一个且仅一个回路；
(5)连通且删去任何一个边后不连通；
(6)每一对结点之间有一条且仅一条路。

back

5.7 树

定义 5.31

若图G的生成子图是一棵树，则该树称为G的**生成树**。设图G有一棵生成树T，则T中的边称作**树枝**。图G中不在生成树上的边称为**弦**。所有弦的集合称为生成树T相对于G的补。



5.7 树

定义 5.32

假定G是一个有n个结点和m条边的连通图，则G的生成树正好有$n-1$条边。因此要确定G的一棵生成树，必须删去G中的$m-(n-1)=m-n+1$条边。该数$m-n+1$称为连通图G的秩。

定理 5.22

连通图至少有一棵生成树。

定理 5.23

一条回路和任意一棵生成树的补至少有一条公共边。

5.7 树

定理 5.24

一个边割集和任何生成树至少有一条公共边。

现在讨论带权图的情况。

定义 5.33

假定图G是具有n个结点的连通图。对应于G的每一条边e，指定一个正数$c(e)$，把$c(e)$称作边e的**权**，（可以是长度、运输量、费用等）。G的每棵生成树具有一个树权$c(T)$，它是T的所有边权的和。

back

5.7 树

在带权的图G的所有生成树中，树权最小的那棵生成树，称作**最小生成树**。设图G中的一个结点表示一个城市，各边表示城市间道路的连接情况，边的权表示道路的长度，如果我们要用通讯线路把这些城市连接起来，要求沿道路架设线路时，所用的线路最短，这就要求在图G中求一棵最小生成树。

back

5.7 树

求最小生成树有许多方法，这里介绍避圈法（**Kruskal算法**）。

设图G有n个结点，以下算法产生最小生成树。

（1）选择最小权边e_1，如果有多条这样的边，选序号最小的边，置边数$i \leftarrow 1$；

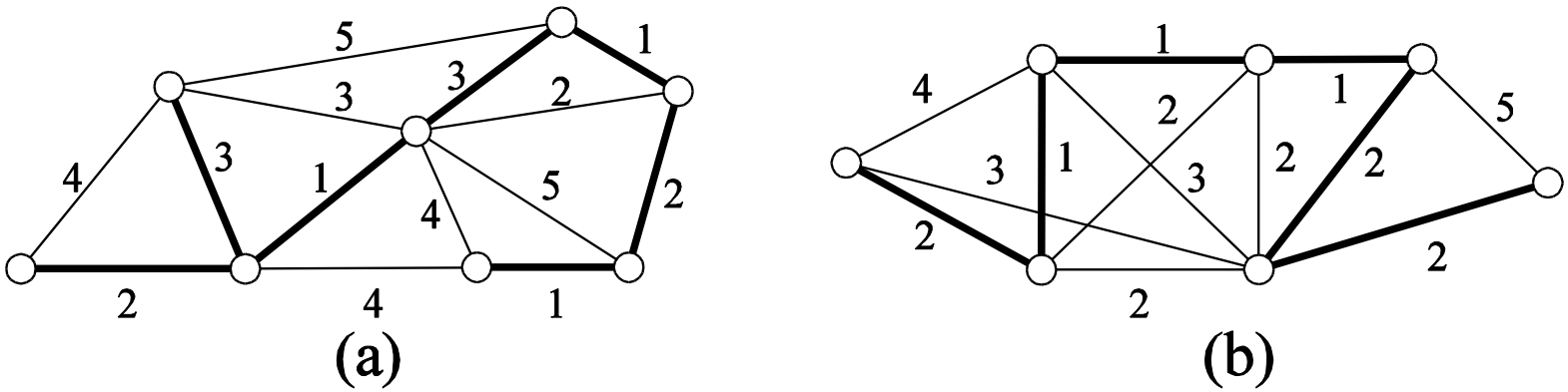
（2）$i = n - 1$结束，否则转（3）；

（3）设定已选定$e_1, e_2, \cdots, e_i$，在G中选取不同于$e_1, e_2, \cdots, e_i$的边e_{i+1}，使$e_1, e_2, \cdots, e_i, e_{i+1}$无回路且$e_{i+1}$是满足此条件的最小边，如果有多条这样的边，选序号最小的边。

（4）$i \leftarrow i + 1$，转（2）。

back

5.7 树



上图中给出了二个带权连通图。图中粗线是按上述算法得到的二个最小生成树。

back

5.7 树

前面我们讨论的树，都是一个无向图，下面我们讨论有向图的树。

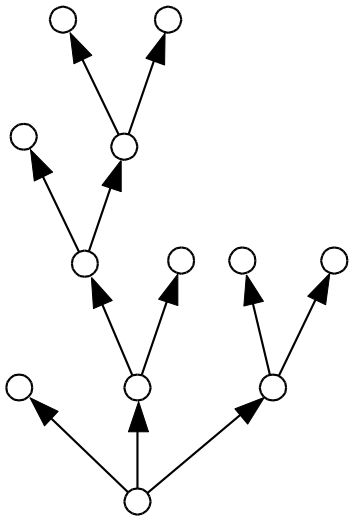
定义 5.34

如果一个有向图在不考虑边的方向时是一棵数，那么，这个有向图称为**有向树**。一棵有向树，如果恰有一个结点的入度为*0*，其余所有结点的入度都为*1*，则称为**根树**。入度为*0*的结点称为**根**，出度为*0*的结点称为**叶**，入度为*1*出度不为*0*的结点称为**分支点**，根和分支点统称为**内点**，从树根到顶点*v*的路径的长度（路径中的边数）称为*v*的**层数**，所有顶点的最大层数称为**树高**。

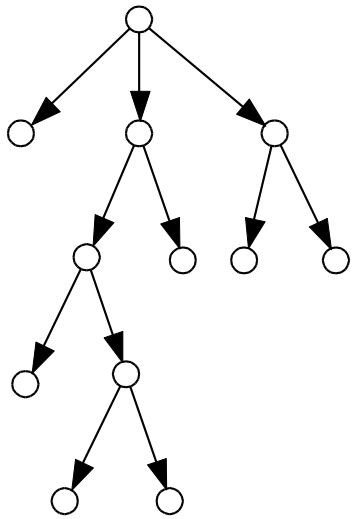
back

5.7 树

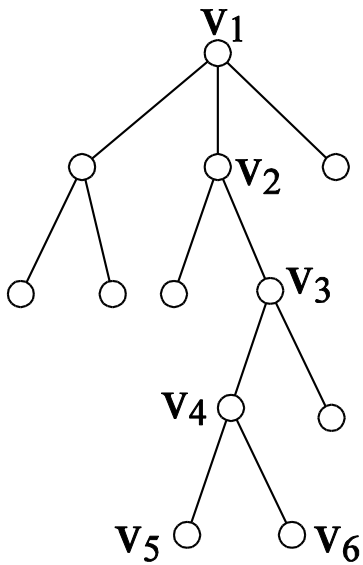
对于一棵根树，通常将树根画在上方，有向边的方向向下或斜向下方，并省去各边的箭头。图中（a）为根树自然表示法，（b）和（c）是都是由树根往下生长，它们是同构图。指明了根树中的结点或边的次序的树称为**有序树**。



(a)



(b)



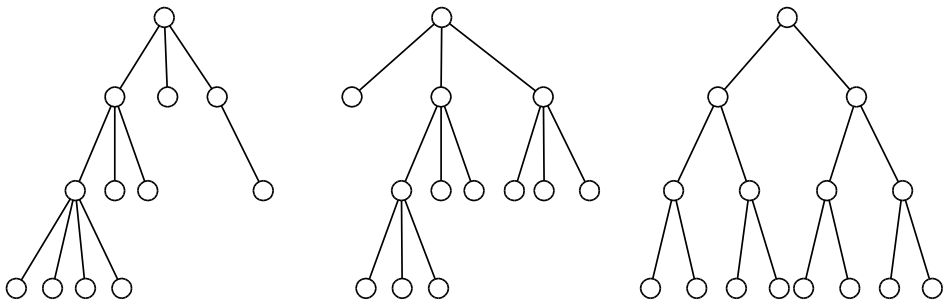
(c)

5.7 树

定义 5.35

在根树中，若每一个结点的出度小于或等于m，则这棵树称为**m叉树**。如果每一个结点的出度恰好等于m或零，则这棵树称为**完全m叉树**。若所有的树叶层次相同，则这棵树称为**正则m叉树**，若$m = 2$时，称为**二叉树**。

下图(a)是4叉树,(b)是完全3叉树,(c)是正则2叉树。



5.7 树

在实际应用中，二叉树特别有用。一方面因为它便于用计算机表示，另一方面还因为任何一个有序树，甚至有序森林都可以变换一个对应的二叉树。把一个有序树变成二叉树可以分以下的两步完成：

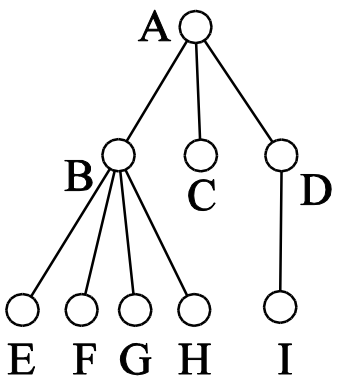
第一步，对有序树的每个分枝点u，保留它的最左一条出边（如果只有一条出边，把它作为左儿子），再把u的位于同一层的各个儿子用一条有向道路从左到右连接起来；

第二步，在由第一步得到的图中，对每个结点u，将位于u下面一层的直接后继（如果存在）作为左儿子，在同一水平线上相邻的二个结点中右结点作为左结点的右儿子，以此类推。

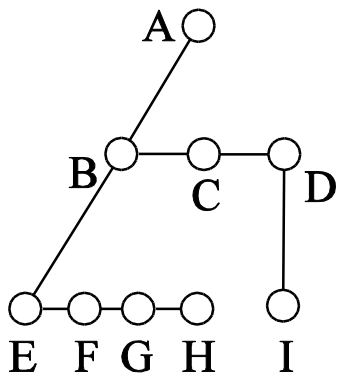
如果是森林，先把各树处理成二叉树，再作如下处理：左右二棵树中右边树作为左边树根的右子树处理。

5.7 树

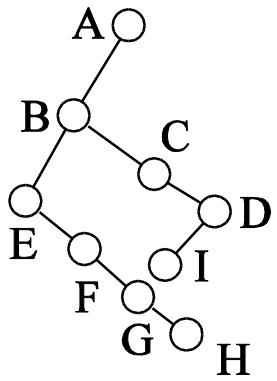
下图中（a）是一棵4叉树，（B）是中间转化过程，（C）是它转化成的2叉树。



(a)



(b)



(c)

back

5.7 树

定理 5.25

设有完全m叉树，其树叶数为t，分枝点数为i，则$(m-1)i=t-1$。

例 5.5

设有30盏灯，拟共用一个电源插座，问需用多少块具有四种插座的接线板。

解　将四叉树每个分枝点看作是具有四插座的接线板，树叶看作电灯，则$(4-1)i \geqslant 30-1$，$i=10$，所以需要10块具有四插座的接线板。

5.7 树

定义 5.36

在根树中，一个结点的通路长度，就是从树根到此结点的通路中的边数。我们把分枝点的通路长度称作**内部通路长度**，树叶的通路长度称作**外部通路长度**。

定理 5.26

若完全二叉树有n个分枝点，且内部通路长度总和为I，外部通路长度总和为E，则$E = I + 2n$。

back

5.7 树

二叉树的一个重要应用就是最优树问题。

定义 5.37

设有一棵二叉树，共有t片树叶，分别带权$w_1, w_2, \cdots, w_t$，该二叉树称为**带权二叉树**。

在带权二叉树中，若带权为w_i的树叶，其通路长度为$L(w_i)$，我们把$w(T) = \sum_{i=1}^{t} w_i L(w_i)$称为该带权二叉树的权。在所有带权$w_1, w_2, \cdots, w_t$的二叉树中，找到一棵使$w(T)$最小的那棵树，称为**最优树**。

back

5.7 树

假若给定一组权$w_1, w_2, \cdots, w_t$，构造一棵最优树，我们要用下面的二个定理：

定理 5.27

设T为带权$w_1 \leqslant w_2 \leqslant, \cdots, \leqslant w_t$的最优树，则

（1）带权为w_1，w_2的树叶是兄弟。
（2）以树叶为v_{w_1}，v_{w_2}儿子的分枝点，其通路长度最长。

定理 5.28

设T为带权$w_1 \leqslant w_2 \leqslant, \cdots, \leqslant w_t$的最优树，若将以带权$w_1$，$w_2$的树叶为儿子的分枝点改为带权$w_1 + w_2$的树叶，得到一棵新树$T'$，则$T'$也是最优树。

5.7 树

根据上面两个定理，要求一棵带有t个权的最优树，可简化为求一棵带有$t-1$个权的最优树，而又可简化为求一棵带$t-2$个权的最优树，依此类推。具体的做法是：首先找出两个最小权值，设为w_1和w_2，然后对$t-1$个权$w_1+w_2, w_3, \cdots, w_t$求作一棵最优树，并且将这棵最优树的结点$v_{w_1+w_2}$分叉生成两个儿子$v_1$和$v_2$，依此类推。此称为*Huffman*算法。

例 5.6

设一组权为1,1,2,3,3,4,5,5，求相应的最优树。

back

5.7 树

二叉树的另一个应用，就是前缀码问题。
在远距离通讯中，常常用0和1的字符串作为英文字母传送信息，但是由于字母使用的频繁程度不同，为了减少信息量，人们希望用较短的序列表示频繁使用的字母。当使用不同长度的序列表示字母时，我们要考虑的另一个问题是如何对接收的字符串进行译码？办法之一就是使用由0和1组成的2元前缀码。

back

5.7 树

定义 5.38

给定一个由*0*和*1*组成的序列集合，若没有一个序列是另一个序列的前缀，该序列集合称为**2元前缀码**，简称为**前缀码**。

例如$000, 001, 01, 10$是前缀码，而$1, 0001, 000$就不是前缀码。

back

5.7 树

定理 5.29

任何一棵二叉树的树叶可对应一个前缀码。

定理 5.30

任何一个前缀码都对应一棵二叉树的树叶。

back

目录

6.1 整数和除法

本章介绍初等数论的有关知识, 包括同余、 剩余系、 剩余定理和指数算术, 最后介绍原根在密码学中的应用.

先从一些基本基本概念开始.

6.2 整数

初等数论中得到的整数的许多性质都要直接或间接地涉及整除性, 整除性是初等数论的基础, 因此这章我 们首先讨论整除性的基本理论. 我们知道, **自然数**或者**正整数**指的是数$1, 2\cdots$,, 而**整数**指的是数 $0, \pm 1, \pm 2, \cdots$. 全体整数的集合记作Z, 而全体正整数或自然数的集合记作 Z^+.

显然, 对任意$a, b \in Z$, 有$a+b, a-b, ab \in Z$, 即Z关于加、减、乘是封闭的, 但存在$a, b \in Z$, 使得$a/b \notin Z$. 因此我们需要考虑整除, 即研究什么时候$a/b \in Z$. 为此, 我们引入下面的概念.

6.2 整数

定义 6.1

设$a, b \in Z$, 且$b \neq 0$. 如果存在$q \in Z$, 使得$a = bq$, 则称b整除a, 记作$b|a$. 此时, b叫做a的**因数**, a叫做b的**倍数**.

如果b不能整除a, 则用记号$b \nmid a$表示.

对任意整数a, 显然$1|a$, 即1是任意整数的因数; 当$a \neq 0$时, 有$a|0$和$a|a$, 即是任意整数的倍数, 任意非零整数是自身的因数也是自身的倍数.

如果一个整数是2的倍数, 我们称它为**偶数**; 否则称它为**奇数**.

因为一个非零数的因数的绝对值不大于该数本身的绝对值, 所以任一非零数的因数只有有限多个.

back

6.2 整数

由整除的定义, 我们不难证明下面这些基本性质.

命题 6.1

设$a, b, c \in Z$.
(1) 如果$c|b, b|a$, 那么$c|a$.
(2) 如果$b|a, c \neq 0$, 那么$cb|ca$.
(3) 如果$c|a, c|b$那么对任意$m, n \in Z$, 有$c|ma + nb$.
(4) 如果$b|a, a|b$那么$a = b$或$a = -b$.

因为$|a|$和 a 的所有因数都相同, 所以我们讨论因数时可以只就正整数来讨论.

6.2 整数

下面是整除的基本定理, 也称为**带余除法**, 它是初等数论的证明中最基本、最常用工具.

定理 6.1

设$a, b \in Z$, 且$b \neq 0$, 则存在惟一的$q, r \in Z$, 使得

$$a = bq + r, \quad 0 \leq r < |b|. \tag{6.1}$$

back

6.2 整数

证明 考虑整数序列

$$\cdots ,, -2|b|, -|b|, 0, |b|, 2|b|, \cdots ,$$

则a必在上述序列的某相邻两项之间. 不妨假定

$$q|b| \leq a < (q+1)|b|$$

于是$0 \leq a - q|b| < |b|$, 令$r = a - q|b|$, 则$0 \leq r < |b|$, 因此, 当$b > 0$时, 有$a = bq + r$; 当$b < 0$ 时, 有$a = b(-q) + r$. 这样, 我们证明了q和r的存在性.
下面证明q, r的惟一性. 假设存在另外一组$q', r' \in Z$使得(6.1)式成立, 即 $a = bq' + r', 0 \leq r' < |b|$, 则有

6.2 整数

$$-|b| < r - r' = b(q' - q) < |b|$$

因此$b(q'-q)=0$, 从而$r-r'=0$, 即$q'=q, r'=r$所以惟一性成立.

例如, 当$a=17, b=5$时, $17=5\times 3+2$, 这时$q=3, r=2$;

而$a=-17, b=5$ 时,$-17=5\times(-4)+3$, 这时$q=-4, r=3$.

back

6.2 整数

定义 6.2

称(6.1)式中的q为用b除a得出的**不完全商**，称r为用b除a得到的**最小非负余数**，也简称为**余数**，常记作$\langle a\rangle_b$或$a \bmod b$.

注：在不致引起混淆时，$\langle a\rangle_b$中的b常略去不写．为方便起见，以后除非特别说明，我们总假定除数b以及因数都大于零.

back

6.2 整数

在本节的最后, 我们给出余数的几个基本性质.

定理 6.2

设$a_1, a_2, b \in Z$, 且$b > 0$则

(1) $\langle a_1 + a_2 \rangle = \langle \langle a_1 \rangle + \langle a_2 \rangle \rangle$

(2) $\langle a_1 - a_2 \rangle = \langle \langle a_1 \rangle - \langle a_2 \rangle \rangle$

(3) $\langle a_1 a_2 \rangle = \langle \langle a_1 \rangle \langle a_2 \rangle \rangle$

back

6.2 整数

证明 (1)~(3)的证明类似, 这里仅证明(1). 设$a_1 = bq_1 + \langle a_1 \rangle$, $a_2 = bq_2 + \langle a_2 \rangle$, $\langle a_1 \rangle + \langle a_2 \rangle = bq_3 + \langle \langle a_1 \rangle + \langle a_2 \rangle \rangle$, 于是

$$\begin{aligned} a_1 + a_2 &= b(q_1 + q_2) + \langle a_1 \rangle + \langle a_2 \rangle \\ &= b(q_1 + q_2 + q_3) + \langle \langle a_1 \rangle + \langle a_2 \rangle \rangle \end{aligned}$$

因此$\langle a_1 + a_2 \rangle = \langle \langle a_1 \rangle + \langle a_2 \rangle \rangle$, 所以断言 (1) 成立.

6.3 素数

在正整数中, 1只能被它本身整除. 任何大于1的整数都至少能被1和它本身整除.

定义 6.3

如果正整数a大于1且只能被1和它自己整除, 则称a是素数. 如果a 大于1 且不是素数, 则称a是合数. 素数也称为质数.

如2, 11为素数, 6为合数.
素数在数论中有着极其重要的地位, 以后若无特别提示, 素数总是指正整数.

6.3 素数

定义 6.4

若正整数a有一因数b, 而b又是素数, 则称b为a的素因数或素因子.

如$12 = 3 \times 4$, 其中3是12的素因数, 而4不是.

命题 6.2

p为素数, a, b, c, d为整数.

(1) 如果$p|ab$, 那么$p|a$或$p|b$;
(2) 如果$d > 1, d|p$,有$d = p$;
(3) a是大于1的合数当且仅当$a = bc$, 其中$1 < b, c < a$;
(4) 若a为合数, 则存在素数p, 使得$p|a$. 即合数必有素数因子.

back

6.3 素数

证明：这里仅证明(4). 令$a = d_1 d_2 \cdots d_k$. 不妨设d_1是其中最小的. 若d_1不是素数, 则存在$e_1 > 1, e_2 > 1, d_1 = e_1 e_2$, 因此, e_1 和e_2也是a的正因数, 这与d_1的最小性矛盾. 因此, d_1是素数. 证毕.

根据上述命题, 任何大于1的整数, 要么是素数, 要么可以分解成素数的乘积. 表明素数是构成整数的“基本元素”. 于是有下面的定理.

6.3 素数

定理 6.3

(算术基本定理) 设整数$a > 1$, 则a能被惟一分解为

$$a = p_1 p_2 \cdots p_n$$

其中$p_i (1 \leq i \leq n)$是满足$p_1 \leq p_2 \leq \cdots \leq p_n$的素数.

back

6.3 素数

证明 我们先证明分解的存在性. 如果a是素数, 取$p_1 = a$即可. 如果a 是合数, 则a有大于1 的最小因数, 记作p_1, 其为素数. 设$a = p_1q_2$, 如果q_2是素数, 取$p_2 = q_2$; 否则, 可取p_2为q_2的大于1的最小因数, 且$q_2 = p_2q_3$. 同理, 可根据q_3取p_3, 依次下去, 取$p_4, \cdots, p_i, \cdots$, 因为$a > q_2 > q_3 > \cdots$, 所以该过程必终止. 假设在第n 步终止, 则由p_i的取法, 有$a = p_1p_2 \cdots p_n$, 且易见$p_1 \leq p_2 \leq \cdots \leq p_n$.

back

6.3 素数

下面证明分解的惟一性. 假设存在大于1的整数, 该整数有两个不同的分解, 不妨假设a是这种数中的最小的. 设

$$a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$$

其中$p_i(1 \leq i \leq n)$是满足$p_1 \leq p_2 \leq \cdots \leq p_n$的素数, $q_i(1 \leq i \leq m)$是满足$q_1 \leq q_2 \leq \cdots \leq q_m$的素数, 则有$p_1 \neq q_1$, 否则$a$不是最小的有两个不同分解的正整数. 因为$p_1 | q_1 q_2 \cdots q_m$, 存在$q_i(i > 1)$, 使得$p_1 | q_i$, 因为$q_i$是素数, 所以$p_1 = q_i$. 这样$q_i = p_1 \geq q_1$, 同理可以得到$q_1 \geq p_1$, 因此$p_1 = q_1$, 矛盾. 故满足要求的分解是惟一的.

back

6.3 素数

如果把算术基本定理中$a = p_1 p_2 \cdots p_n$里相同的素数集中起来, 就可得到

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \tag{6.2}$$

这里$\alpha_i (1 \leq i \leq k), p_1 < p_2 < \cdots < p_k$. 式(6.2) 叫做$a$的**标准分解式**.

例如, 72 的标准分解式是$2^3 \times 3^2$, 100的标准分解式是$2^2 \times 5^2$.

back

6.3 素数

由算术基本定理立即得到下面的推论.

推论 6.1

对任一正整数a进行素因子分解, $a = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, 则$a$有$(r_1+1)(r_2+1)\cdots(r_k+1) = \prod_{i=1}^{k}(r_i+1)$个正因子.

例 6.1

(1) 20328有多少个正因子?
(2)20!的二进制表示中从最低位数起有多少个连续的0.

back

6.3 素数

解：(1) $20328 = 2^3 \times 3 \times 7 \times 11^2$, 由推论得20328正因子个数$4 \times 2 \times 2 \times 3 = 48$个.
(2) 只需求20!含有多少个因子2. 不超过20含有因子2的数(即为偶数)有2, $4 = 2^2$, $6 = 2 \times 3$, $8 = 2^3$, $10 = 2 \times 5$, $12 = 2^2 \times 3$, $14 = 2 \times 7$, $16 = 2^4$, $18 = 2 \times 3^2$, $20 = 2^2 \times 5$. 故20!含有18$(1+2+1+3+1+2+1+4+1+2 = 18)$个因子2, 从而20!的二进制表示中从最低位数起有18 个连续的0.

back

6.3 素数

素数在数论中的地位非常重要, 有必要对素数作进一步的讨论.

命题 6.3

(1) 任何大于1的合数a必有一个不超过$\sqrt{a}$的素因数;
(2) 素数有无限个.

证明: (1) 用合数a可以表示成若干个素数之积, 立即得证.
(2) 反证法. 假设只有有限个素数, 设为$p_1, p_2, \cdots, p_n$, 令$m = p_1 p_2 \cdots p_n + 1$, 因为$m$ 比每一个素数都大, 所以m是合数, 这样m 有一个素数因子p_i, 根据$p_i \mid m$, 可以得出$p_i \mid 1$, 这是个矛盾.

back

6.3 素数

此命题可以判断整数是否为素数.

例 6.2

判断127和133是否是素数.

解：2, 3, 5, 7, 11是小于等于$\sqrt{127}$和$\sqrt{133}$的所有素数. 因为$2 \nmid 127, 3 \nmid 127, 5 \nmid 127, 7 \nmid 127, 11 \nmid 127$. 所以127为素数. 因为$7|133$, 所以133为合数.

6.4 最大公约数和最小公倍数

定义 6.5

设$a_1, a_2, \cdots, a_n$是不全为零的整数，d是非零整数，$n \geq 2$. 若$d|a_i, 1 \leq i \leq n$，则整数d是$a_1, a_2, \cdots, a_n$的公因子或公约数. 所有公约数中最大的那一个，称为$a_1, a_2, \cdots, a_n$的最大公约数. 记为$(a_1, a_2, \cdots, a_n)$.

若$(a_1, a_2, \cdots, a_n) = 1$，称$a_1, a_2, \cdots, a_n$是互素的.

6.4 最大公约数和最小公倍数

定义 6.6

设$a_1, a_2, \cdots, a_n$和m都是正整数，$n \geq 2$. 若$a_i | m, 1 \leq i \leq n$, 则称m是$a_1, a_2, \cdots, a_n$的公倍数. 所有非零公倍数中最小的那一个, 称为$a_1, a_2, \cdots, a_n$的最小公倍数. 记为$[a_1, a_2, \cdots, a_n]$

对于正整数a, 显然有 $(0, a) = a, (1, a) = 1, [1, a] = a$.

back

6.4 最大公约数和最小公倍数

根据定义, 最大公约数和最小公倍数有下述性质:

1. 若$a|m, b|m$, 则$[a,b]|m$;
2. 若$d|a, d|b$, 则$d|(a,b)$;
3. 若$a = qb + r$, 其中a, b, q, r都是整数, 则$(a,b) = (b,r)$.

证明: (1) 记$M = [a,b]$, 设$m = qM + r, 0 \leq r < M$, 由$a|m$, $a|M$可知$a|r$, 同理, $b|$, 即r是a和b的公倍数, 若$r \neq 0$, 则$M \leq r$, 这与$0 \leq r < M$不相符, 必有$r = 0$, 从而$M|m$.
(2) 记$D = (a,b)$, 令$m = [d,D]$. 若$m = D$, 则有$d|D$, 结论成立. 否则$m > D$, 注意到$d|a, D|a$, 由(1), 得$m|a$. 同理$m|b$, 即m是a和b的公因子, 而$m > D$, 这与D是最大的不相符.

back

6.4 最大公约数和最小公倍数

(3) 只需证明a、b的公因子和b、r的公因子相同即可. 设d是 a 与 b 的公因子, 即$d|a$, $d|b$. 注意到$r = a - qb$, 则有$d|r$. 从而, $d|b$且$d|r$, 即d也是b与r的公因子. 反之一样, 设d是b与r的公因子, 即$d|b$且$d|r$. 注意到, $a = qb + r$, 故有$d|a$. 从而, $d|a, d|b$, 即d也是a与b的公因子.

根据上述性质, 下节介绍最大公约数与最小公倍数的方法.

back

6.4 最大公约数和最小公倍数

方法一： 利用整数的素因子分解法

$$a = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}, b = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$$

其中$p_1, p_2, \cdots, p_k$是不同的素数，$r_1, r_2, \cdots, r_k, s_1, s_2, \cdots, s_k$是非负整数. 则

$$(a,b) = p_1^{\min(r_1,s_1)} p_2^{\min(r_2,s_2)} \cdots p_k^{\min(r_k,s_k)}$$

$$[a,b] = p_1^{\max(r_1,s_1)} p_2^{\max(r_2,s_2)} \cdots p_k^{\max(r_k,s_k)}$$

back

6.4 最大公约数和最小公倍数

例 6.3

求84和600的最大公约数和最小公倍数.

解：对84和600进行素因子分解, 得

$$84 = 2^2 \times 3 \times 7, \quad 600 = 2^3 \times 3 \times 5^2$$

将它们都写成$84 = 2^2 \times 3^1 \times 5^0 \times 7^1, 600 = 2^3 \times 3^1 \times 5^2 \times 7^0$.
所以

$$(84, 600) = 2^2 \times 3^1 \times 5^0 \times 7^0 = 12$$

和

$$[84, 600] = 2^3 \times 3^1 \times 5^2 \times 7^1 = 4200$$

back

6.4 最大公约数和最小公倍数

方法二： 设a,b为整数，$b\neq 0$. 做带余除法，$a=q_1b+r_2,0\leq r_2<|b|$. 若$r_2>0$，对b和r_2做带余除法，得$b=q_2r_2+r_3,0\leq r_3<r_2$. 重复上述过程，由于$|b|>r_2>r_3>\cdots\geq 0$，存在$k$使得$r_{k+1}=0$. 于是有

$$\begin{aligned}
&a=q_1b+r_2,1\leq r_2<|b|\\
&b=q_2r_2+r_3,1\leq r_3<r_2\\
&r_2=q_3r_3+r_4,1\leq r_4<r_3\\
&\quad\vdots\\
&r_{k-2}=q_{k-1}r_{k-1}+r_k,1\leq r_k<r_{k-1}\\
&r_{k-1}=q_kr_k.
\end{aligned}$$

则有$(a,b)=(b,r_2)=(r_2,r_3)=\cdots=(r_{k-1},r_k)=r_k$.

6.4 最大公约数和最小公倍数

此法称为欧几里得(Euclid)算法. 又称辗转相除法.

例 6.4

用欧几里得算法求126与27的最大公约数.

解：$126 = 4 \times 27 + 18, 27 = 1 \times 18 + 9, 18 = 2 \times 9$, 所以$(126, 27) = 9$.
根据上述例子, 可得$9 = 27 - 18 \times 1 = 27 - 1 \times (126 - 4 \times 27) = -1 \times 126 + 5 \times 27$.

这表示$(126, 27)$是126和27的线性组合, 这个结论具有一般性.

back

6.4 最大公约数和最小公倍数

定理 6.4

若$(a,b)=d$, 则存在$x,y\in Z$, 使得$xa+yb=d$.

证明略.

上述$xa+yb=d$, 也称为d是a,b的线性组合.

如$(168,300)=12$, $12=9\times 168-5\times 300$.

back

6.4 最大公约数和最小公倍数

本节最后再讨论一下两整数互素的一些性质.

1. a与b互素的充分必要条件：存在 $x, y \in Z$,使$ax+by=1$.
2. 若$a|c$, $b|c$, 且a与b互素, 则$ab|c$.

证明：(1) 先证必要性. 若a, b互素, 即$(a, b)=1$,根据前述结论, 存在$x, y \in Z$, 有$ax+by=1$.

6.4 最大公约数和最小公倍数

再证充分性. 设$ax+by=1, x, y \in Z$, 又设$d>0$是a和b的公因子, 则$d|xa+by$, 即$d|1$. 所以$d=1$.

(2) a, b互素, 存在$x, y \in Z$, 有$ax+by=1$. 则有$axc+byc=c$. 又由$a|xa, b|c$, 可得$ab|axc$, 同理$ab|byc$. 于是有$ab|(axc+byc)$, 即$ab|c$.

bac

6.5 同余

用一个固定的数去除所有整数，有相同余数的整数组成一个类，可将全体整数分成有限个类，可以从这有限个类推测整数集合的特性.

定义 6.7

设$a, b \in Z$, m是一个正整数，如果用m分别去除a和b，所得余数相同，则称a和b关于模m**同余**，用符号$a \equiv b \pmod{m}$表示；如果余数不同，则称a和b 关于模m**不同余**，用符号$a \not\equiv b \pmod{m}$表示.

back

6.5 同余

根据定义容易得知: $a \equiv b \pmod{m} \Leftrightarrow$存在整数$k$, 使得$a = b + km$.
同余与通常的相等类似, 是Z上的等价关系, 即满足下面的性质.

命题 6.4

设$a, b, c \in Z$, m是任意正整数, 则模m同余是Z上的等价关系, 即下列性质成立.
(1) $a \equiv a \pmod{m}$.
(2) 如果$a \equiv b \pmod{m}$, 那么$b \equiv a \pmod{m}$.
(3) 如果$a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$, 那么$a \equiv c \pmod{m}$.

证明: 证明略.

back

6.5 同余

定理 6.5

设$a,b,c,d \in Z$, m是任意正整数.
(1) 若$a \equiv b(\mathrm{mod}\ m)$, 那么$ac \equiv bc(\mathrm{mod}\ m)$.
(2) 若$a \equiv b(\mathrm{mod}\ m)$, $c \equiv d(\mathrm{mod}\ m)$,则$(a+c) \equiv (b+d)(\mathrm{mod}\ m)$.
(3) 若$a \equiv b(\mathrm{mod}\ m)$, $c \equiv d(\mathrm{mod}\ m)$, 那么 $ac \equiv bd(\mathrm{mod}\ m)$.
(4) 若$a \equiv b(\mathrm{mod}\ m)$, 则对任意正整数$n$, 有$a^n \equiv b^n(\mathrm{mod}\ m)$.

back

6.5 同余

证明: (1) 如果$a \equiv b(\mathrm{mod}\ m)$, 则有$m|a-b$, 因此有$m|(a-b)c$, 即$m|ac-bc$, 所以$ac \equiv bc(\mathrm{mod}\ m)$.

(2) 由$a \equiv b(\ \mathrm{mod}\ \ m), c \equiv d(\ \mathrm{mod}\ \ m)$知, $m|(a-b)$且$m|(c-d)$, 所以$m|(a-b+c-d)$, 即$m|(a+c)-(b+d)$, 于是有$(a+c) \equiv (b+d)(\mathrm{mod}\ m)$.

(3) 由假设知$m|(a-b)$, $m|(c-d)$, 因此$m|(a-b)c+b(c-d)$, 即$m|(ac-bd)$, 所以$ac \equiv bd(\ \mathrm{mod}\ \ m)$.

6.5 同余

(4) 对n用归纳法. 当$n = 1$时, 结论显然成立. 假设结论对$n = k(\geq 1)$也成立, 即$a^k \equiv b^k \pmod{m}$. 则当$n = k+1$时, 由(3)有$aa^k \equiv bb^k \pmod{m}$,即$a^{k+1} \equiv b^{k+1} \pmod{m}$. 因此对任意正整数$n$, 都有$a^n \equiv b^n \pmod{m}$.

下面的推论易知.

推论 6.2

如果$a \equiv b \pmod{m}$, 那么对任意整系数多项式

$$f(x) = r_k x^k + \cdots + r_1 x + r_0,\ r_i \in \mathbf{Z},\ 0 \leq i \leq k$$

有$f(a) \equiv f(b) \pmod{m}$.

6.5 同余

定理 6.6

证明:
(1) 如果$a \equiv b(\mathrm{mod}\ m)$, 正整数$d|m$, 那么$a \equiv b(\mathrm{mod}\ d)$.
(2) 如果$ac = bc(\mathrm{mod}\ m)$, 则$a \equiv b(\mathrm{mod}\ m/(c,m))$.

证明: (1) 由$a \equiv b(\mathrm{mod}\ m)$知, $m|(a-b)$. 因为$d|m$, 所以$d|(a-b)$, 故$a \equiv b(\mathrm{mod}\ d)$.
(2) 令$d = (c,m)$. 由$ac = bc(\mathrm{mod}\ m)$知, 存在$k \in Z$, 使得$ac - bc = km$, 于是有$(a-b)\frac{c}{d} = k\frac{m}{d}$. 又因为$d = (c,m)$, 所以$(\frac{c}{d}, \frac{m}{d}) = 1$. 从而有$\frac{m}{d}|(a-b)$, 即$a \equiv b(\mathrm{mod}\ m/d)$, 故结论成立.

back

6.6 剩余系

模m同余是Z上的等价关系，该关系将全体整数划分为m个等价类，我们用Z_m表示全体等价类组成的集合. 例如，模3同余的3个等价类如下：

$$\{\cdots, -6, -3, 0, 3, 6, \cdots\},$$
$$\{\cdots, -5, -2, 1, 4, 7, \cdots\},$$
$$\{\cdots, -4, -1, 2, 5, 8, \cdots\}.$$

同一等价类中的元素具有相同的余数，每个等价类中的元素有相同的余数r，这里$r = 0, 1, 2$. 用$[r]$表示该等价类. 令$Z_3 = \{[0], [1], [2]\}$. 有时直接用余数表示等价类，在这种记号下，$Z_3 = \{0, 1, 2\}$.

back

6.6 剩余系

定义 6.8

设$S \subseteq Z$, 如果任意整数都与S中正好一个元素关于模m同余, 则称S 是模m的一个**完全剩余系**(或简称为**剩余系**).

因为任一整数用m去除得到的最小非负余数必定是$0, 1, 2, \cdots, m-1$ 中的某个数, 即任一整数关于模m必定与$0, 1, 2, \cdots, m-1$ 中某一数同余, 这样$S = \{0, 1, 2, \cdots, m-1\}$是模$m$的一个完全剩余系, 该完全剩余系称作**标准剩余系**, 记作Z_m. 模m的完全剩余系恰好有m个元素.

6.6 剩余系

下面的定理给出了集合$S \subseteq Z$是完全剩余系的充要条件.

定理 6.7

设$S = \{a_1, a_2, \cdots, a_k\} \subseteq Z$, 则$S$是模$m$的一个完全剩余系的充要条件为

(1) $k = m$.

(2) 当$i \neq j$时, $a_i \not\equiv a_j \pmod{m}$.

back

6.6 剩余系

证明: $\Rightarrow$: 设S是模m的一个完全剩余系, 由定义知$|S| = m$. 因为任何整数都只与S中一个元素同余, 自然S中的每个元素只能与S中的一个元素同余, 而S中的元素与自身同余, 所以S中的不同元素关于模m不同余, 必要性成立.

$\Leftarrow$: 设$k = m$, 且S中任意两个元素关于模m均不同余, 那么S中每个元素都属于Z_m中不同的等价类, 于是任意整数都与S中正好一个元素关于模m同余, 根据定义, S是模m的一个完全剩余类系.

back

6.6 剩余系

上述定理表明, 任意m个模m互不同余的数构成模m的一个完全剩余系.

从一个给定的完全剩余系, 我们可以使用下面的定理构造新的完全剩余系.

back

6.6 剩余系

定理 6.8

设$S=\{a_1,a_2,\cdots,a_m\}$是模m的一个完全剩余系，$(k,m)=1$，则$S'=\{ka_1+b,ka_2+b,\cdots,ka_m+b\}$也是模$m$的一个完全剩余系，这里$b$是任意整数.

证明： 只需证明：当$i\neq j$时，$ka_i+b\neq ka_j+b(\mathrm{mod}\ m)$即可. 下面用反证法. 假设$ka_i+b\equiv ka_j+b(\mathrm{mod}\ m)$，那么必然有$ka_i\equiv ka_j(\mathrm{mod}\ m)$，即$m|k(a_i-a_j)$. 因为$(k,m)=1$，所以$m|a_i-a_j$，即$a_i\equiv a_j(\mathrm{mod}\ m)$，这与$S$是模$m$的一个完全剩余系矛盾，因此定理成立.

back

6.6 剩余系

例 6.5

设m是正偶数，$\{a_1, a_2, \cdots, a_m\}$和$\{b_1, b_2, \cdots, b_m\}$都是模$m$的完全剩余系，试证

$$\{a_1 + b_1, a_2 + b_2, \cdots, a_m + b_m\}$$

不是模m的完全剩余系.

证明： 因为$\{a_1, a_2, \cdots, a_m\}$是模$m$的完全剩余系，所以

$$\sum_{i=1}^{m} a_i \equiv \sum_{i=1}^{m} i = \frac{m(m+1)}{2} \equiv \frac{m}{2} (\mathrm{mod}\ m)$$

back

6.6 剩余系

同理有

$$\sum_{i=1}^{m} b_i \equiv \frac{m}{2} (\mathrm{mod}\ m)$$

如果$\{a_1 + b_1, a_2 + b_2, \cdots, a_m + b_m\}$也是模$m$的完全剩余系，则同理也有

$$\sum_{i=1}^{m} (a_i + b_i) \equiv \frac{m}{2} (\mathrm{mod}\ m)$$

back

6.6 剩余系

但是

$$\sum_{i=1}^{m}(a_i+b_i)=\sum_{i=1}^{m}a_i+\sum_{i=1}^{m}b_i\equiv\frac{m}{2}+\frac{m}{2}=m\equiv 0(\mathrm{mod}\ m)$$

所以$\frac{m}{2}\equiv 0(\mathrm{mod}\ m)$, 矛盾. 故$\{a_1+b_1,a_2+b_2,\cdots,a_m+b_m\}$不是模$m$ 的完全剩余系.

back

6.6 剩余系

在模m的一个完全剩余系S中, 有的数与m互素, 有的数与m不互素, 所有与m 互素的数构成的集合称作模m的一个**既约剩余系**, 同理有**标准既约剩余系**.

因为1与任何数都互素, 所以任意正整数都有既约剩余系. 要问既约剩余系中元素的个数, 只需求出标准既约剩余系中元素的个数即可, 欧拉用$\phi(m)$表示模m的既约剩余系所含元素的个数. 换言之, 对任意正整数m, $\phi(m)$ 表示所有不大于m且与m互素的正整数的个数, 这样得到的函数ϕ: $N \to N$ 称作**欧拉函数**.

由定义可知, 显然$\phi(1) = \phi(2) = 1, \phi(3) = \phi(4) = 2, \phi(5) = 4, \cdots$. 一般地, 若正整数$m$ 是素数, 则$\phi(m) = m-1$; 若m是合数, 则$\phi(m) < m-1$.

6.6 剩余系

与完全剩余系类似, 我们有如下判定一个集合是否是既约剩余系的结论.

定理 6.9

设$S = \{a_1, a_2, \cdots, a_k\} \subseteq Z$, 则$S$是模$m$的一个既约剩余系的充要条件是

(1) $k = \phi(m)$

(2) 当$i \neq j$时, $a_i \not\equiv a_j \pmod{m}$

(3) 对任意$a_i \in S$, 都有$(a_i, m) = 1$

证明: 必要性由定义即得.

back

6.6 剩余系

下面考虑从充分性. 因为$a_i \not\equiv a_j \pmod{m}$, 所以$S$中的$k$个数属于$Z_m$的 k 个不同的等价类, 又因为$k = \phi(m)$以及S中每个元素都与m互素, 所以$a_1, a_2, \cdots, a_k$ 是模m 的完全剩余系中所有与m互素的数, 因此S是模m的既约剩余系.

任意$\phi(m)$个与m互素且两两关于模m 不同余的数构成模m的一个既约剩余系.

back

6.6 剩余系

从一个既约剩余系, 也可以产生另一个既约剩余系.

定理 6.10

设$S=\{a_1,a_2,\cdots,a_{\phi(m)}\}$是模$m$的一个既约剩余系, $(k,m)=1$, 则$S'=\{ka_1,ka_2,\cdots,ka_{\phi(m)}\}$也是模$m$的一个既约剩余系.

证明: 因为当$i\neq j$时, $a_i\not\equiv a_j(\mathrm{mod}\ m)$, 又$(k,m)=1$, 所以$ka_i\not\equiv ka_j(\mathrm{mod}\ m)$. 另外, 对任意$ka_i\in S'$, 因为$(k,m)=1$和$(a_i,m)=1$, 所以$(ka_i,m)=1$, 于是, S' 是模m 的一个既约剩余系, 定理成立.

back

6.6 剩余系

下面是一个称为欧拉定理的一个结论, 有着十分广泛的应用.

定理 6.11

(欧拉(Euler)定理) 设$a \in Z$, m是正整数, 如果$(a, m) = 1$, 那么

$$a^{\phi(m)} \equiv 1 (\mathrm{mod}\ m)$$

证明: 设$S = \{a_1, a_2, \cdots, a_{\phi(m)}\}$模$m$的一个既约剩余系, 则$S' = \{aa_1, aa_2, \cdots, aa_{\phi(m)}\}$也是模$m$的一个既约剩余系. S'中任一数恰好与S的一个数关于模m同余, 于是有

6.6 剩余系

$$a^{\phi(m)}\prod_{i=1}^{\phi(m)}a_i=\prod_{i=1}^{\phi(m)}(aa_i)\equiv\prod_{i=1}^{\phi(m)}a_i(\mathrm{mod}\ m)\qquad(6.3)$$

即$m\left|(a^{\phi(m)}-1)\prod_{i=1}^{\phi(m)}a_i\right.$. 另一方面, 由既约剩余系定义知, 对所有$1\leq i\leq\phi(m)$, 都有$(a_i,m)=1$, 所以$\left(\prod_{i=1}^{\phi(m)}a_i,m\right)=1$, 从而$m\left|a^{\phi(m)}-1\right.$, 即$a^{\phi(m)}\equiv 1(\mathrm{mod}\ m)$, 故定理成立.

6.6 剩余系

例如, 当$a = 5, m = 6$时, 显然有$(5,6) = 1, \phi(6) = 2$, 计算得$5^{\phi(6)} = 5^2 \equiv 1 (\mathrm{mod}\ 6)$, 与欧拉定理结论一致.
欧拉定理的一种特殊情形是$m = p$, 这里p是素数. 此时$\phi(p) = p - 1$, 代入(6.3) 式即得下面的Fermat(Fermat)定理.

定理 6.12

((Fermat))定理 如果$a \in Z, p$是素数, 则

$$a^p \equiv a (\mathrm{mod}\ p)$$

特别地, 若$p \nmid a$, 则

$$a^{p-1} \equiv a (\mathrm{mod}\ p).$$

6.6 剩余系

证明: 若$p|a$, 则$a^p \equiv a(\mathrm{mod}\ p)$显然成立. $p \nmid a$, 则有$(p,a) = 1$, 于是由欧拉定理知, $a^{p-1} = a^{\phi(p)} \equiv 1(\mathrm{mod}\ p)$, 即$a^{p-1} \equiv a(\mathrm{mod}\ p)$, 用$a$ 乘该同余式两边即得$a^p \equiv a(\mathrm{mod}\ p)$. 这就证明了定理.

上面定理说, 如果p是素数, 那么对任意正整数a, 都有$a^p \equiv a(\mathrm{mod}\ p)$. 因此, 若存在整数$b$, 使得$b^n \not\equiv b(\mathrm{mod}\ n)$, 那么$n$必定不是素数. 例如, 63不是素数, 因为$2^{63} = (2^6)^{10} \times 2^3 \equiv 2^3 \not\equiv 2(\mathrm{mod}\ 63)$.

值得注意的是, 这种判定n是合数的方法不需要对n进行分解.

back

6.6 剩余系

例 6.6

求$3^{301} \pmod{11} = ?$

解 由Fermat定理知, $3^{10} \equiv 1 \pmod{11}$, 所以

$$3^{301} = (3^{10})^{30} \times 3 \equiv 3 \pmod{11}$$

于是$3^{301} \pmod{11} = 3.$

6.7 EULER函数计算

对于正整数m, 要求$\phi(m)$, 根据定义需要检查1到m每一个数是否与m 互素, 这种方法是比较耗时的. 例如, $m \approx 10^3$, 会耗费许多时间. 对$m \approx 10^{100}$ 这么大的数, 则几乎是不可能的. 本节讨论计算欧拉函数$\phi(m)$ 的一般方法, 以及与欧拉函数的计算方法.

下面的定理为计算$\phi(m)$提供了基础.

back

6.7 EULER函数计算

定理 6.13

(1) 如果p是素数且$\alpha \geq 1$, 则

$$\phi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1} \tag{6.4}$$

(2) 如果$(a,b) = 1$, 那么

$$\phi(ab) = \phi(a)\phi(b) \tag{6.5}$$

back

6.7 EULER函数计算

证明: (1) 考虑模p^α的完全剩余系$S = \{1, 2, \cdots, p^\alpha\}$, 在$S$中与$p^\alpha$不互素的数只有$p$的倍数, 即

$$p, 2p, \cdots, p^{\alpha-1}p$$

这些数总共有$p^{\alpha-1}$个, 其余$p^\alpha - p^{\alpha-1}$个数都是与p^α互素的, 因此p^α的既约剩余系含有$p^\alpha - p^{\alpha-1}$ 个元素, 故$\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

(2) 设$S_a = \{x_1, x_2, \cdots, x_{\phi(a)}\}$和$S_b = \{y_1, y_2, \cdots, y_{\phi(b)}\}$分别是模$a$和模$b$的既约剩余系. 作集合

$$S_{ab} = \{bx_i + ay_j | 1 \le i \le \phi(a), 1 \le j \le \phi(b)\}$$

back

6.7 EULER函数计算

若$bx_i+ay_j=bx_{i'}+ay_{j'}$, 这里$1\leq i,i'\leq\phi(a)$和$1\leq j,j'\leq\phi(b)$, 推知$x_i\equiv x_{i'}\pmod{}$和$y_j\equiv y_{j'}\pmod{b}$. 由此可知集合$S_{ab}$中含有$\phi(a)\phi(b)$个数. 欲证(6.5)式, 只需证明$S_{ab}$是$ab$的一个既约剩余系即可, 下面分三步来证明:.

先证S_{ab}中任意两个数关于模ab均不同余. 设bx_i+ay_j, $bx_{i'}+ay_{j'}\in S_{ab}$, $bx_i+ay_j\neq bx_{i'}+ay_{j'}$, 则$x_i\not\equiv x_{i'}\pmod{}$和$y_j\not\equiv y_{j'}\pmod{b}$至少一个成立. 如果$bx_i+ay_j\equiv bx_{i'}+ay_{j'}\pmod{ab}$, 那么必有$bx_i+ay_j\equiv bx_{i'}+ay_{j'}\pmod{a}$, 于是$bx_i\equiv bx_{i'}\pmod{a}$. 因为$(a,b)=1$, 所以$x_i\equiv x_{i'}\pmod{a}$. 同理可得$y_i\equiv y_{i'}\pmod{b}$, 这是一个矛盾. 因此$S_{ab}$中任意两个数关于模$ab$是不同余的.

back

6.7 EULER函数计算

再证S_{ab}中任一数都与ab互素. 对任意的$bx_i + ay_j \in S_{ab}$, 因为$(x_i, a) = 1, (b, a) = 1$, 所以$(bx_i, a) = 1$, 故$(bx_i + ay_j, a) = 1$. 同理有$(bx_i + ay_j, b) = 1$. 于是$(bx_i + ay_j, ab) = 1$, 这表明S_{ab}中任一数都与ab互素.

back

6.7 EULER函数计算

最后证任一与ab互素的数都与S_{ab}中某个数关于模ab同余.
假设整数c与ab互素, 即$(c, ab) = 1$. 因为$(a, b) = 1$, 所以存在$x_0, y_0 \in Z$, 使得$bx_0 + ay_0 = 1$, 于是$bcx_0 + acy_0 = c$. 令$x = cx_0$, $y = cy_0$, 则有$bx + ay = c$. 因为$(c, ab) = 1$, 所以$(c, a) = 1$, 即$(bx + ay, a) = 1$, 故$(bx, a) = 1$, 从而有$(x, a) = 1$. 因此存在$x_i \in S_a$, 使得$x \equiv x_i (\mathrm{mod}\ a)$. 同理, 存在$y_j \in S_b$, 使得$y \equiv y_j (\mathrm{mod}\ b)$. 因此有$bx \equiv bx_i (\mathrm{mod}\ ab)$, $ay \equiv ay_j (\mathrm{mod}\ ab)$, 即$c \equiv (bx_i + ay_j) (\mathrm{mod}\ ab)$. 这说明与$ab$互素的数都与$S_{ab}$中某个数关于模$ab$同余.
综上可知, S_{ab}是ab的一个既约剩余系, 故(6.5)成立.

back

6.7 EULER函数计算

有了上面这些结果, 我们很容易得到计算$\phi(m)$的一般公式.

定理 6.14

设m的标准分解为$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, 则

$$\phi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right) \tag{6.6}$$

back

6.7 EULER函数计算

证明: 由(6.5)式和(6.4)式, 有

$$\begin{aligned}
\phi(m) &= \phi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) \\
&= \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2}) \cdots \phi(p_k^{\alpha_k}) \\
&= (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1}) \\
&= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right) \\
&= m \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)
\end{aligned}$$

所以定理成立.

back

6.7 EULER函数计算

例如, $\phi(300)=\phi(2^2\times3\times5^2)=300\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)=80$. 把公式(6.6)稍作变形, 可得

$$\phi(m)=p_1^{\alpha_1-1}p_2^{\alpha_2-1}\cdots p_k^{\alpha_k-1}(p_1-1)(p_2-1)\cdots(p_k-1)$$

也可将(6.6) 式写成

$$\phi(m)=m\cdot\prod_{p|m}\left(1-\frac{1}{p}\right)$$

这里p是素数.
因为当$m>2$时, m或者有$2^k(k\geq2)$因子或者有大于2的素数因子, 所以$\phi(m)$总是偶数.

6.7 EULER函数计算

两个数a,b互素时，$\phi(ab)$是$\phi(a)$ 与$\phi(b)$的乘积，下面讨论一般情况.

定理 6.15

(1) 设$(a,b)=d$，那么

$$\phi(ab)=\phi(a)\phi(b)\frac{d}{\phi(d)}$$

(2) 如果$a|b$，那么$\phi(a)|\phi(b)$.

back

6.7 EULER函数计算

证明:

$$\begin{aligned}\frac{\phi(ab)}{ab} &= \prod_{p|ab}\left(1-\frac{1}{p}\right)\\ &= \frac{\prod\limits_{p|a}\left(1-\frac{1}{p}\right)\cdot\prod\limits_{p|b}\left(1-\frac{1}{p}\right)}{\prod\limits_{p|(a,b)}\left(1-\frac{1}{p}\right)}\\ &= \frac{\frac{\phi(a)}{a}\cdot\frac{\phi(b)}{b}}{\frac{\phi(d)}{d}}\\ &= \frac{1}{ab}\phi(a)\phi(b)\frac{d}{\phi(d)}\end{aligned}$$

因此, $\phi(ab)=\phi(a)\phi(b)\frac{d}{\phi(d)}$.

6.7 EULER函数计算

(2) 因为$a|b$, 可设$b=ac$, $(a,c)=e$, 则由(1)知,

$$\begin{aligned}\frac{\phi(b)}{\phi(a)} &= \frac{ac\cdot\prod\limits_{p|ac}\left(1-\frac{1}{p}\right)}{a\cdot\prod\limits_{p|a}\left(1-\frac{1}{p}\right)}\\ &= \frac{c\cdot\prod\limits_{p|a}\left(1-\frac{1}{p}\right)\cdot\prod\limits_{p|\frac{c}{e}}\left(1-\frac{1}{p}\right)}{\prod\limits_{p|a}\left(1-\frac{1}{p}\right)}\\ &= e\cdot\frac{c}{e}\cdot\prod_{p|\frac{c}{e}}\left(1-\frac{1}{p}\right)\\ &= e\cdot\phi\left(\frac{c}{e}\right) \text{ 是整数.}\end{aligned}$$

因此$\phi(a)|\phi(b)$, 定理成立.

6.7 EULER函数计算

♣ 附注: 因为$(a,c)=e$, 可设$e=p_1^{k_1}p_2^{k_2}\cdots p_t^{k_t}$, $a=ep_{t+1}^{k_{t+1}}\cdots p_n^{k_n}$, $c=ep_{n+1}^{k_{n+1}}\cdots p_m^{k_m}$, 这里的$p_i$都是素数. 这样$ac$的全体素数因子是

$$p_1,p_2,\cdots,p_t,p_{t+1},\cdots,p_n,p_{n+1}\cdots,p_m$$

这些素数因子也就是a的素数因子和$\frac{c}{e}$的素数因子. 于是(2)的证明过程中的第2个等号成立. ♣

6.8 一次同余方程

代数学中，经常遇到解方程的问题. 在同余理论中，也有同余方程这样的说法.

定义 6.9

设$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$，其中$a_i \in Z$，$i = 0, 1, \cdots, n$. 则称

$$f(x) \equiv 0 (\mathrm{mod}\ m) \tag{6.7}$$

为模m的一元同余方程. 如果$m \nmid a_n$，则n称作方程(6.7) 的**次数**. 如果x_0满足$f(x_0) \equiv 0(\mathrm{mod}\ m)$，那么所有满足$x \equiv x_0(\mathrm{mod}\ m)$的$x$都满足$f(x) \equiv 0(\mathrm{mod}\ m)$，我们称作方程(6.7)的**解或根**. 若方程(6.7)的两个解关于模m 互不同余，那么称它们是不相同的解.

back

6.8 一次同余方程

根据定义, 将模m的标准剩余系中的每个元素代入(6.7)式即可确定它的所有解, 因此, 解同余方程一般来说比解一般意义下的方程容易. 例如解$x^5+2x^4+x^3+2x^2-2x+3\equiv 0(\mathrm{mod}\ 7)$, 我们只需把模7的标准剩余系中的元素$0,1,2,3,4,5,6$代入验算, 从而可以得到它的全部解为$x\equiv 1,5,6(\mathrm{mod}\ 7)$. 代入法是求解同余方程的基本方法, 但对于模数较大的情形, 计算量很大. 另外, 我们应该注意到有些同余方程没有解, 如$x^2\equiv 3(\mathrm{mod}\ 10)$. 这也很容易理解, 因为毕竟有许多普通方程也没有(实数)解, 如$x^2=-1$.

back

6.8 一次同余方程

本节将讨论一次同余方式的公式解, 即讨论一个一次同余方程是否有解, 有多少个不同的解, 如何用公式给出它的所有解等问题.

我们先讨论一元一次同余方程的求解问题. 一元一次同余方程的一般形式是$ax \equiv b(\mathrm{mod}\ m)$, 其中$a, b, m \in Z$, $m > 0$且$m \nmid a$. 下面分$(a, m) = 1$和$(a, m) > 1$ 两种情况来讨论它的解.

♣ 注: 当$m|a$ 时, 可设$a = km$, 于是方程变为$kmx \equiv b\ (\mathrm{mod}\ m)$. 容易看出, 若$b$是$m$ 的倍数, 则任何整数都是方程的解; 若b不是m的倍数, 则方程无解. 因此, 一般情况下, 都首先要求$m \nmid a$, 另外, 既然要求$m \nmid a$, 所以$m > 1$. ♣

back

6.8 一次同余方程

定理 6.16

设$(a,m)=1$, 那么一元一次同余方程$ax \equiv b \pmod{m}$有且仅有一个解$x \equiv ba^{\phi(m)-1} \pmod{m}$.

证明: 由欧拉定理知, $a^{\phi(m)} \equiv 1 \pmod{m}$, 于是$a(ba^{\phi(m)-1}) \equiv b \pmod{m}$, 这说明$x \equiv ba^{\phi(m)-1} \pmod{m}$是同余方程$ax \equiv b \pmod{m}$的解.

对于方程的任意两个解x_1和x_2, 因为$ax_1 \equiv b \pmod{m}$, $ax_2 \equiv b \pmod{m}$, 所以$a(x_1 - x_2) \equiv 0 \pmod{m}$, 而$(a,m)=1$, 故$x_1 \equiv x_2 \pmod{m}$, 方程的解唯一.

back

6.8 一次同余方程

例 6.7

解同余方程$3x \equiv 7 (\mathrm{mod}\ 80)$.

解 因为$(3, 80) = 1$, 所以$3x \equiv 7 (\mathrm{mod}\ 80)$有惟一解.

$$\phi(80) = \phi(2^4 \times 5) = \phi(2^4)\phi(5) = (2^4 - 2^3) \times 4 = 32$$

故由定理6.16知, 该惟一解为

$$x \equiv 7 \times 3^{\phi(80)-1} \equiv 7 \times 3^{31} \equiv 7 \times 3^3 \times (3^4)^7 \equiv 7 \times 3^3 \equiv 29 (\mathrm{mod}\ 80),$$

即$x \equiv 29 (\mathrm{mod}\ 80)$.

back

6.8 一次同余方程

对于一般情形, 我们有下面的定理.

定理 6.17

设$(a,m)=d$. 则有以下结论:
(1) 一元一次同余方程

$$ax \equiv b(\mathrm{mod}\ m) \tag{6.8}$$

有解当且仅当$d|b$.
(2) 若方程(6.8)有解, 则恰有d个解

$$x \equiv x_0 + k\frac{m}{d}(\mathrm{mod}\ m),\quad k=0,1,2,\cdots,d-1$$

其中x_0是方程(6.8)的一个特解.

6.8 一次同余方程

证明: 先证定理的第一部分.

$\Rightarrow$. 设方程(6.8)有解. 存在$x_0, k \in Z$, 使得$ax_0 = b + km$. 因为$(a, m) = d$, 所以$d|a$, $d|m$, 于是$d|b$.

$\Leftarrow$. 设$d|b$. 由$(a, m) = d$, 可知$(\frac{a}{d}, \frac{m}{d}) = 1$, 根据定理 6.16知, 同余方程

$$\frac{a}{d}x \equiv \frac{b}{d}\left(\mathrm{mod}\ \frac{m}{d}\right) \tag{6.9}$$

有唯一解, 设为$x \equiv x_0(\mathrm{mod}\ \frac{m}{d})$. 易见$x \equiv x_0(\mathrm{mod}\ m)$是方程(6.8)的解.

第一部分证完.

6.8 一次同余方程

再证定理的第二部分.

设方程(6.8)有解x_0, 由前面的结论知$d|b$, 这样(6.9)式有意义, 显然x_0是方程(6.9) 的解. 另外, 方程(6.8)的解是方程(6.9) 的解, 方程(6.9)的解也是方程(6.8)的解. 于是解方程(6.8)就转化为解方程(6.9)了. 需要注意的是, 方程(6.8)和方程(6.9)的模不同, 方程(6.9)的模$\frac{m}{d}$相同的解不一定就是方程(6.8) 模m相同的解.

back

6.8 一次同余方程

设方程(6.9)的惟一解为$x \equiv x_0 (\mathrm{mod}\ \frac{m}{d})$. x_1是方程(6.8)的任意一个解. 因为x_1也是方程(6.9)的解, 由方程(6.9)解的唯一性知,

$$x_1 \equiv x_0 \left(\mathrm{mod}\ \frac{m}{d}\right)$$

这样$x_1 = x0 + k \cdot \frac{m}{d}$, 这里$k$是整数. 这就是说方程(6.8)的任意解都具有$x_1 = x0 + k \cdot \frac{m}{d}$这种形式, 不难验证这种形式的任何数也是方程(6.8)的解. 因此, 只要在所有形如$x_0 + k\frac{m}{d}$的数中找出所有模m不同的数即可, 这些数是

$$x_0, x_0 + \frac{m}{d}, \cdots, x_0 + (d-1)\frac{m}{d}$$

它们就是方程(6.8)的所有解.

back

6.8 一次同余方程

例 6.8

解同余方程$9x \equiv 21 \pmod{240}$.

解: 因为$(9, 240) = 3 | 21$, 所以$9x \equiv 21 \pmod{240}$有3 个解. 前面的例子已经得到$3x \equiv 7 \pmod{80}$的惟一解$x \equiv 29 \pmod{80}$, 从它得出方程的全部解为

$$
\begin{aligned}
x &\equiv 29 \pmod{240}, \\
x &\equiv 29 + 80 = 109 \pmod{240}, \\
x &\equiv 29 + 2 \times 80 = 189 \pmod{240}.
\end{aligned}
$$

back

6.9 剩余定理

定理 6.18

(剩余定理) 设$m_1, m_2, \cdots, m_k$是k个两两互素的正整数, $m = m_1 m_2 \cdots m_k$, $M_i = m/m_i, 1 \leq i \leq k$, 那么同余方程组

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv b_k \pmod{m_k} \end{cases}$$

有惟一解

$$x \equiv \sum_{i=1}^{k} b_i M_i M_i' \pmod{m}$$

其中M_i'满足$M_i M_i' \equiv 1 \pmod{m_i}$.

6.9 剩余定理

证明: 对于$i = 1, 2, \cdots, k$, 由于$M_i = M/m_i$, 即M_i是除去m_i所有其它m_j的乘积, 所以$(M_i, m_i) = 1$, 故存在整数M_i' 是方程$M_i x \equiv 1 \pmod{m_i}$的解. 即$M_i M_i' \equiv 1 \pmod{m_i}$, 于是$b_i M_i M_i' \equiv b_i \pmod{m_i}$. 在$k$个相加的项$\sum_{i=1}^{k} b_i M_i M_i'$中, 只有$b_i M_i M_i'$这一项与$b_i$模$m_i$相等. 其余的$k-1$项的每一项都是$m_i$的倍数, 从而与0模$m_i$ 相等. 所以有

$$\sum_{i=1}^{k} b_i M_i M_i' \equiv b_i \pmod{m_i}$$

因此, $x = \sum_{i=1}^{k} b_i M_i M_i'$是一元同余方程组的解, 因为$m$是$m_i$的倍数, 不难验证与$x$模$m$同余的任何一个整数$y$都是方程组的解,

back

6.9 剩余定理

即满足

$$y \equiv \sum_{i=1}^{k} b_i M_i M_i' \pmod{m}$$

的整数y也为方程组的解.

最后证明解的唯一性. 设x_1, x_2都是同余方程组的解. 则对所有的$i(1 \leq i \leq n)$有

$$x_1 \equiv x_2 \pmod{m_i}$$

所以$x_1 \equiv x_2 \pmod{[m_1, m_2, \cdots, m_k]}$. 因为$m_1, m_2, \cdots, m_k$是两两互素的, 所以$[m_1, m_2, \cdots, m_k] = m_1 m_2 \cdots m_k$, 于是有

$$x_1 \equiv x_2 \pmod{m}$$

故方程的解唯一.

6.9 剩余定理

例 6.9

解同余方程组

$$\begin{cases} x \equiv 2 (\mathrm{mod}\ 3), \\ x \equiv 1 (\mathrm{mod}\ 5), \\ x \equiv 6 (\mathrm{mod}\ 7). \end{cases}$$

back

6.9 剩余定理

解 直接利用中国剩余定理求解. 这里$m_1 = 3, m_2 = 5, m_3 = 7, m = 105, M_1 = 35, M_2 = 21, M_3 = 15$. 分别解同余方程

$$35M_1' \equiv 1(\mathrm{mod}\ 3), 21M_2' \equiv 1(\mathrm{mod}\ 5), 15M_3' \equiv 1(\mathrm{mod}\ 7)$$

得

$$M_1' \equiv 2(\mathrm{mod}\ 3), M_2' \equiv 1(\mathrm{mod}\ 5), M_3' \equiv 1(\mathrm{mod}\ 7)$$

于是同余方程组的解为

$$x \equiv 2\times 35\times 2+1\times 21\times 1+6\times 15\times 1(\mathrm{mod}\ 105) \equiv 41(\mathrm{mod}\ 105)$$

back

6.10 原根

设n为正整数, 根据欧拉定理, 对于任意一个与n互素的整数a是, 都有

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

这说明, 方程$a^x \equiv 1 \pmod{n}$有正整数解. 因而, 存在一个最小的正整数是该同余方程的解. 下面对这种最小的正整数给出一个定义.

定义 6.10

设整数a和正整数n互素. 使得$a^x \equiv 1 \pmod{n}$成立的最小的正整数x 称为a模n的阶数或者次数, 记作$ord_n a$.

back

6.10 原根

注:
作代数除法, 设$a = kn + r$, 则$a \equiv r \pmod{n}$, 由于$(n, r) = (a, n) = 1$, 所以r也存在模n次数的概念, 并且$ord_n a = ord_n r$, 这样我们只考虑求$1 \leq a < n$这样的a的次数即可.

6.10 原根

例 6.10

找出2模7的阶数.
解: 通过计算发现:

$$2^1 \equiv 2(\mathrm{mod}7), \quad 2^2 \equiv 4(\mathrm{mod}7), \quad 2^3 \equiv 1(\mathrm{mod}7).$$

因此有$ord_7 2 = 3$.
类似地, 为了找到3模7的阶数, 作如下计算:

$$3^1 \equiv 3(\mathrm{mod}7), \quad 3^2 \equiv 2(\mathrm{mod}7), \quad 3^3 \equiv 6(\mathrm{mod}7),$$

$$3^4 \equiv 4(\mathrm{mod}7), \quad 3^5 \equiv 5(\mathrm{mod}7), \quad 3^6 \equiv 1(\mathrm{mod}7).$$

我们得到$ord_7 3 = 6$.

6.10 原根

为了找到同余式$a^x \equiv 1 \pmod{n}$的全部解, 需要下面的定理.

定理 6.19

设整数a和n互素且$n > 0$, 那么正整数x是同余方程

$$a^x \equiv 1 \pmod{n}$$

的一个解当且仅当$ord_n a | x$.

back

6.10 原根

证明: ($\Leftarrow$). 设正整数x 满足$ord_n a | x$, $x = k \cdot ord_n a$, 其中k为正整数, 我们有:

$$a^x = a^{k \cdot ord_n a} = (a^{ord_n a})^k \equiv 1 \pmod{n}$$

说明x是方程的一个解.

($\Rightarrow$) 设正整数x满足$a^x \equiv 1 \pmod{n}$, 用带余除法记为:

$$x = q \cdot ord_n a + r, \quad 0 \leq r < ord_n a$$

于是

$$a^x = a^{q \cdot ord_n a + r} = (a^{ord_n a})^q a^r \equiv a^r \pmod{n}$$

已知$a^x \equiv 1 \pmod{n}$, 所以$a^r \equiv 1 \pmod{n}$. 从不等式$0 \leq r < ord_n a$ 和$ord_n a$是使得$a^{ord_n a} \equiv 1 \pmod{n}$ 成立的最小的正整数, 可得$r = 0$, 这样, $x = q \cdot ord_n a$, 即$ord_n a | x$.

6.10 原根

例 6.11

确定$x=10$和$x=15$是否是方程$2^x \equiv 1 (\mathrm{mod} 7)$ 的解.

解: 前面的例子知$ord_7 2 = 3$. 因为$3 \nmid 10$, $3 \mid 15$, 所以$x=10$不是$2^x \equiv 1 (\mathrm{mod} 7)$的解, $x=15$是$2^x \equiv 1 (\mathrm{mod} 7)$ 的解.

定理 6.20

若整数a与n互素且$n>0$, 那么$ord_n a | \phi(n)$.

证明: 因为$(a,n)=1$, 由欧拉定理可知$a^{\phi(n)} \equiv 1 \pmod{n}$, 于是$ord_n a | \phi(n)$.

back

6.10 原根

从定理(6.20), 可知$ord_n a$是$\phi(n)$ 的因子. 这就表明, 在$\phi(n)$的因子中求$ord_n a$即可.

例 6.12

计算7模9的次数.

首先注意到$\phi(9) = 6$. 因为6的正因子只有$1, 2, 3$和6, 根据定理6.20, 可知$ord_9 7$是$1, 2, 3$和6之一. 由小至大验证如下:

$$7^1 \equiv 7(\mathrm{mod}9), 7^2 \equiv 4(\mathrm{mod}9), 7^3 \equiv 1(\mathrm{mod}9)$$

故$ord_9 7 = 3$.

back

6.10 原根

下面要叙述的定理对于后面一些结论的讨论非常的重要.

定理 6.21

若整数a与正整数n互素, 那么$a^i \equiv a^j \pmod{n}$, 当且仅当$i \equiv j \pmod{ord_n a}$, 其中$i$和$j$是非负整数.

证明: ($\Leftarrow$) 设$i \equiv j \pmod{ord_n a}$, $0 \leq j \leq i$. 则$i = j + k \cdot ord_n a$, 其中k是一个非负整数. 因为$a^{ord_n a} \equiv 1 \pmod{n}$, 于是

$$a^i = a^{j+k\cdot ord_n a} = (a^{ord_n a})^k a^j \equiv a^j \pmod{n}$$

back

6.10 原根

($\Rightarrow$) 设$a^i \equiv a^j \pmod{n}$, 不妨$i \geq j$. 于是$n|(a^i - a^j)$, 即$n|a^j(a^{i-j} - 1)$, 因为$(a, n) = 1$, 所以$(a^j, n) = 1$, 这样便有$n|(a^{i-j} - 1)$, 也就是$a^{i-j} \equiv 1 \pmod{n}$. 于是, $ord_n a|(i - j)$, 或者等价地说

$$i \equiv j(\bmod\ ord_n a).$$

back

6.10 原根

例 6.13

证明: $3^5 \equiv 3^{11} \pmod{14}$, $3^9 \not\equiv 3^{20} \pmod{14}$.
解: 令$a = 3$, $n = 14$. 可知$(a, n) = 1$, $\phi(14) = 6$. 已知$ord_{14}3 | \phi(14)$, 所以3的模14的阶数$ord_{14}3$只能是1, 2, 3 和 6 其中之一, 经过验证$ord_{14}3 = 6$, 又因为

$$5 \equiv 11 \pmod{6}, \quad 9 \not\equiv 20 \pmod{6}$$

于是根据定理(6.21), 便知

$$3^5 \equiv 3^{11} \pmod{14}, \quad 3^9 \not\equiv 3^{20} \pmod{14}$$

back

6.10 原根

经过前面的讨论, 我们知道, 对于任何一个与n互素的整数a, 都有$ord_n a | \phi(n)$. 自然有这样的问题: 对于任何正整数n, 是否存在整数a, 使得a的模n 的阶数最大, 即$ord_n a = \phi(n)$?
先对这样的数给一个定义.

定义 6.11

设整数a与正整数整数n互素. 若$ord_n a = \phi(n)$, 则称a是模n的一个**原根**.

back

6.10 原根

例 6.14

前面例6.10已经求得$ord_7 3 = 6 = \phi(7)$. 按定义, 3是模7的一个原根. 通过计算可知$ord_7 5 = 6$, 故5也是模7的一个原根.

下面的例子6.15说明, 并非所有整数都有原根.

例 6.15

证明模8没有原根.
证明: 按定义, 一个数的原根不超过该数且与该数互素, 注意到所有比8小且与8 互素的整数只有1, 3, 5, 7, 并且

$$ord_8 1 = 1, ord_8 3 = ord_8 5 = ord_8 7 = 2$$

它们都不等于$\phi(8) = 4$, 故8没有原根.

back

6.10 原根

原根的用途之一就是下面的定理.

定理 6.22

设r和正整数n互素. 若r是模n的一个原根, 那么下列整数

$$r^1, r^2, \cdots, r^{\phi(n)}$$

构成了模n的既约剩余系.

证明: 为了证明原根r的前$\phi(n)$个幂构成模n的既约剩余系, 按照模n既约剩余系的定义, 只需证明它们都与n互素且任何两个都不是模n同余的即可. 首先, 因为$(r,n)=1$, 所以对任意正整数k有$(r^k,n)=1$. 于是这$\phi(n)$个数都与n互素. 其次, 再证明它们中任何两个都不是模n同余的. 因为对于$1 \le i \le \phi(n)$及$1 \le j \le \phi(n)$, 若

$$r^i \equiv r^j \pmod{n}$$

back

6.10 原根

根据定理6.21, 可知$i \equiv j \pmod{\phi(n)}$, 于是$\phi(n) \mid (i-j)$, 从而有$i-j=0$. 因此

$$r^1, r^2, \cdots, r^{\phi(n)}$$

中任何两个都不是模n同余的, 从而这r个数构成模n的一个既约剩余系.

back

6.10 原根

当某整数有原根时, 原根通常不止一个. 为了证明这个结论, 先证明下面的定理.

定理 6.23

设整数a与正整数n互素且$ord_n a = t$. 则对任何一个正整数u, 有

$$ord_n(a^u) = t/(t,u)$$

证明: 首先注意到因为a与n互素, 所以a^u也与n互素. 令$s = ord_n(a^u)$, $v = (t,u)$, 设$t = t_1 v$, $u = u_1 v$. 可知$(t_1, u_1) = 1$. 因为$t_1 = t/(t,u)$, 为了证明$ord_n(a^u) = t_1$, 只要证明$s|t_1$ 和$t_1|s$就可以了.

back

6.10 原根

先来证明, $s|t_1$. 由于$ord_n(a) = t$, 于是$a^t \equiv 1 \pmod{n}$. 而$(a^u)^{t_1} = (a^{u_1 v})^{t/v} = (a^t)^{u_1} \equiv 1 \pmod{n}$. 所以$s|t_1$.
再来证明$t_1|s$. 因为s是a^u的次数, 所以

$$(a^u)^s = a^{us} \equiv 1 \pmod{n}$$

得a的次数$t|us$. 即$t_1 v|u_1 vs$, 于是$t_1|u_1 s$. 由于$(t_1, u_1) = 1$, 可得$t_1|s$.
以上分别证明了$s|t_1$和$t_1|s$, 所以$s = t_1 = t/v = t/(t,u)$.

back

6.10 原根

例 6.16

已经知道, $ord_7\ 3 = 6$, 可得$ord_7\ 3^4 = 6/(6,4) = 6/2 = 3$.

推论 6.3

设r是模n的原根, 其中n是一个大于1的整数, 那么r^u是模n的一个原根当且仅当$(u, \phi(n)) = 1$.

证明: 因为

$$ord_n r^u = \frac{ord_n r}{(u, ord_n r)} = \frac{\phi(n)}{(u, \phi(n))}$$

故$ord_n r^u = \phi(n)$(即r^u是模n的一个原根)当且仅当$(u, \phi(n)) = 1$.

back

6.10 原根

例 6.17

如果正整数n有一个原根, 那么它一共有$\phi(\phi(n))$个不同的原根.

证明: 设r是模n的一个原根. 那么, 根据定理 6.22, 可知r^1, r^2, $\cdots$, $r^{\phi(n)}$构成了模n的一个既约剩余系. 对于模n的任意一个原根a , 因为a与n互素, 所以a与r^1, r^2, $\cdots$, $r^{\phi(n)}$中某一个模n相等. 这样, 要找出模n的所有原根, 只要在r^1, r^2, $\cdots$, $r^{\phi(n)}$中找出即可. 而r^u是模n的原根当且仅当$(u, \phi(n)) = 1$. 因为有$\phi(\phi(n))$个这样的u, 相应地也就有$\phi(\phi(n))$个模n的原根.

back

6.10 原根

例 6.18

验证2是模11的一个原根.

解: 易知$\phi(11) = 10$, 并且

$$
\begin{aligned}
&2^1 \equiv 2 \pmod{11}, \quad 2^2 \equiv 4 \pmod{11}, \quad 2^3 \equiv 8 \pmod{11},\\
&2^4 \equiv 5 \pmod{11}, \quad 2^5 \equiv 10 \pmod{11}, \quad 2^6 \equiv 9 \pmod{11},\\
&2^7 \equiv 7 \pmod{11}, \quad 2^8 \equiv 3 \pmod{11}, \quad 2^9 \equiv 6 \pmod{11},\\
&2^{10} \equiv 1 \pmod{11}.
\end{aligned}
$$

按照模11原根的定义可知, 2是模11的一个原根.

back

6.10 原根

例 6.19

找出模11的所有原根.

解: 因为$\phi(11) = 10$, $\phi(\phi(11)) = 4$. 所以模11共有4个不同的原根. 通过例6.18知2是模11的原根. 所以, 所有的原根都可以从2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}中找出来. 具体就是在这些数中挑出其幂与10互素的数, 也就是2^1, 2^3, 2^7, 2^9. 又因为$2^1 \equiv 2 \pmod{11}$, $2^3 \equiv 8 \pmod{11}$, $2^7 \equiv 7 \pmod{11}$, $2^9 \equiv 6 \pmod{11}$, $2^1 \equiv 2 \pmod{11}$. 这样, $2, 6, 7, 8$就是模11的全部不同余的原根.

back

6.10 原根

通过前面的讨论, 我们发现有的正整数有原根, 有的没有原根. 现在开始讨论一个给定的正整数是否有原根的问题.
我们先证明每一个素数都有一个原根.

定义 6.12

假设$f(x)$是一个次数非零的整系数多项式. 若

$$f(c) \equiv 0 \pmod{m}$$

则称整数c是$f(x)$的一个模m的根.

不难验证, 若c是一个$f(x)$模m的根, 则对每一个形如$km + c$的整数, 也就是每个与c模m同余的整数, 也是$f(x)$模m的根.

back

6.10 原根

例 6.20

验证:
(1) $x \equiv 2 \pmod 7$和$x \equiv 4 \pmod 7$是多项式$f(x) = x^2 + x + 1$两个模7的根.
(2) 多项式$f(x) = x^2 + 2$没有模5的根.

解: (1) 分别将2和4带入方程$f(x) = x^2 + x + 1$得到21和7, 它们都是7的倍数, 按照定义2和4是多项式$f(x) = x^2 + x + 1$的模7的根. 进而$x \equiv 2 \pmod 7$和$x \equiv 4 \pmod 7$都是多项式$f(x) = x^2+x+1$ 模7的根.

6.10 原根

(2) 因为整数c是多项式$f(x) = x^2 + 2$模5的根，当且仅当与c模5同余的数是多项式$f(x) = x^2 + 2$模5的根，这样只需验证0, 1, 2, 3, 4 都不是多项式$f(x) = x^2 + 2$模5的根便可，分别代入验证即知. 这里略去.

例 6.21

Fermat定理说，与素数p互素的任何整数a都有$a^{\phi(p)} \equiv 1 \pmod{p}$，也就是$a^{p-1} - 1 \equiv 0 \pmod{p}$. 因为$1, 2, \cdots, p-1$每个都与$p$互素，所以$1, 2, \cdots, p-1$都满足方程$x^{p-1} - 1 \equiv 0 \pmod{p}$，也就都是多项式$f(x) = x^{p-1} - 1$模$p$的根. 因此，$x \equiv 1 \pmod{p}$, $x \equiv 2 \pmod{p}$, $\cdots$, $x \equiv p-1 \pmod{p}$也是多项式$f(x) = x^{p-1} - 1$ 的模p的根.

back

6.10 原根

对于给定的素数p, 什么样的多项式存在模p 的根? 该多项式模p根有多少? 下面的结论是一个关于多项式模p的根的重要的定理.

定理 6.24

设p是素数,

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x^1 + a_0$$

是一个次数为$n(n \geq 1)$, 首项系数a_n不能被p整除的整系数多项式. 那么$f(x)$至多有n个模p不同余的根.

back

6.10 原根

证明: 用数学归纳法来证明这个定理.
当$n=1$时, $f(x)=a_1x+a_0$, $p\nmid a_1$. 需要证明$f(x)$至多有一个模p 不同的根. 事实上, 因为$p\nmid a_1$, 所以$(a_1,p)=1$. 这样, 存在两个整数u,v 使得

$$a_1u+pv=1$$

等式的两端同时乘以$-a_0$并整理可得

$$a_1(-ua_0)+a_0+(-a_0pv)=0$$

于是$a_1(-ua_0)+a_0+(-a_0pv)\equiv a_1(-ua_0)+a_0\equiv 0 \pmod p$. 这样方程$f(x)\equiv 0 \pmod p$有一个解$x\equiv(-ua_0) \pmod p$. 再设$x\equiv x_1 \pmod p$ 和 $x\equiv x_2 \pmod p$是方程$a_1x+a_0\equiv 0 \pmod p$ 的两个解.

6.10 原根

于是 $a_1x_1 + a_0 \equiv 0 \pmod{p}$和$a_1x_2 + a_0 \equiv 0 \pmod{p}$, 这样便得$a_1(x_1 - x_2) \equiv 0 \pmod{p}$, 即$p|a_1(x_1 - x_2)$. 因为$p \nmid a_1$, 故$p|x_1 - x_2$, 也就是$x_1 \equiv x_2 \pmod{p}$, 所以方程$f(x) \equiv 0 \pmod{p}$的解唯一, 这样也就证明了方程至多有一个解.

设定理对次数为$n-1$的多项式成立. 令$f(x)$是一个次数为n且首项系数不被p整除的多项式. 若$f(x)$有$n+1$个模p不同余的根, 记为$c_0, c_1, \cdots, c_n$, 则$f(c_k) \equiv 0 \pmod{p}$, $k = 0, 1, 2, \cdots, n$. 令

$$\begin{aligned} f(x) - f(c_0) &= a_n(x^n - c_0^n) + a_{n-1}(x^{n-1} - c_0^{n-1}) + \cdots + a_1(x - c_0) \\ &= (x - c_0)g(x) \end{aligned}$$

back

6.10 原根

这里$g(x)$是一个首项系数为a_n(与p互素)的次数为$n-1$的多项式. 下面将要证明$c_1, \cdots, c_n$都是$g(x)$模p不同余的根. 事实上, 因为$c_0, c_1, \cdots, c_n$都是$f(x)$模p不同余的根, 可知当$k = 1, 2, \cdots, n$时, 有$f(c_k) \equiv 0 \pmod{p}$和$f(c_0) \equiv 0 \pmod{p}$, 因而

$$f(c_k) - f(c_0) = (c_k - c_0)g(c_k) \equiv 0 \pmod{p}$$

因为$c_k - c_0 \not\equiv 0 \pmod{p}$, 所以$g(c_k) \equiv 0 \pmod{p}$. 这表示次数为$n-1$的首项系数不能被$p$整除的多项式$g(x)$有$n$个模$p$不同的根, 这与归纳假设相矛盾. 所以$f(x)$的模$p$不同余的根的个数不会超过$n$, 证完.

6.10 原根

定理 6.25

假设p为素数且d是$p-1$的因子. 那么多项式x^d-1恰有d个模p不同余的根.

证明: 根据题意, 设$p-1=de$. 那么有

$$\begin{aligned} x^{p-1}-1 &= (x^d)^e-1 \\ &= (x^d-1)(x^{d(e-1)}+x^{d(e-2)}+\cdots+x^d+1) \\ &= (x^d-1)g(x) \end{aligned}$$

back

6.10 原根

由Fermat定理知, $x^{\phi(p)}-1=x^{p-1}-1$有仅有$p-1$个模p不同余的根. 对于任何一个$x^{p-1}-1$的模p的根α, 有$p|(\alpha^d-1)g(\alpha)$, 因为p 是素数, 或者$p|(\alpha^d-1)$, 即α是$x^{p-1}-1$模p的根; 或者$p|g(\alpha)$, 即α是$g(x)$ 的模p的根. 因为二者模p根的个数之和就是$x^{p-1}-1$的模p的根的个数$p-1$, 从$g(x)$是一个次数为$d(e-1)=p-d-1$ 的首项与p互素的多项式, 可知其模p不同余的根至多有$p-d-1$, 类似地, x^d-1 模p 不同余的根的个数至多是d, 但二者之和为$p-1$, 所以多项式x^d-1必须有d 个模p不同余的根.

back

6.10 原根

定理6.20告诉我们, 若a与n互素, 则$ord_n a$一定是$\phi(n)$的因子. 现在让n等于一个素数p, 因为小于p的正整数$1, 2, \cdots, p-1$都与p互素, 所以这$p-1$数中的每一个数的阶数是$\phi(p) = (p-1)$ 的因子.

现在的问题是: 给定$p-1$的因子d, $1, 2, \cdots, p-1$中有没有以d为阶数的数?

定理 6.26

设p是一个素数且正整数d是$p-1$的因子, 那么, 小于p的正整数$1, 2, \cdots, p-1$中模p阶为d的数的个数至多是$\phi(d)$.

back

6.10 原根

证明: 对于给定的$p-1$的正因子d, 令$F(d)$表示小于p的正整数中模p的阶为d的数的个数.
第一种情况: $F(d)=0$. 显然有$F(d) \leq \phi(d)$.
第二种情况: $F(d) \neq 0$. 这时存在一个模p的阶为d的整数a, 即$ord_p a = d$. 因为d是最小的使得$a^d \equiv 1 \pmod{p}$的正整数, 故d个整数

$$a, a^2, \cdots, a^d$$

back

6.10 原根

是模p不同余的, 原因是上面的d个整数中如果有两个是模p同余的, 则其对应的两个阶数之差是d的倍数, 这显然是不可能的. 对于任何$k(1 \leq k \leq d)$, 由于$(a^k)^d = (a^d)^k \equiv 1 \pmod{p}$. 所以$d$个数$a, a^2, \cdots, a^d$是$x^d - 1$模$p$的$d$个根也是其所有的根. 注意到模$p$ 阶为d的数的个数是$F(d)$, 这些数中的每一个也是$x^d - 1$模p的根, 因而每一个恰好与$a, a^2, \cdots, a^d$这d个数中的某一个模p同余, 那么模p的阶为d的$F(d)$个数只要在这d个数中寻找即可. 已知a^k 次数是$\frac{d}{(k,d)}$, 而$a, a^2, \cdots, a^d$ 的幂中恰好有$\phi(d)$ 个k满足$(k, d) = 1$, 所以$a, a^2, \cdots, a^d$ 恰好有$\phi(d)$个元素的次数为d, 从而有$\phi(d)$个模p阶为d 的元素. 此时, $F(d) = \phi(d)$.

综合以上两种情况, 我们有$F(d) \leq \phi(d)$, 证完.

6.10 原根

定理 6.27

设n为一个正整数, 那么

$$n = \sum_{d|n} \phi(d)$$

证明: 令A是$1, 2, \cdots, n$这n个整数组成集合. 现在对集合A中的n个整数进行分类: 任取$m \in A$, 若$(m, n) = d$, 则令m属于集合C_d. 即$m \in C_d$当且仅当$(m, n) = d$或者$(m/d, n/d) = 1$. 所以, C_d 类就是由不超过n且与n的最大公因子是d的整数组成的, 或者等价地说C_d类就是由不超过n/d且和n/d互素的整数组成的, 从而集合C_d中的元素个数就是$\phi(n/d)$.

back

6.10 原根

由于1到n的这些整数中的每一个一定属于其中的一个类而且只能属于一个类, 这样所有类含有的整数个数之和为n, 故

$$n = \sum_{d|n} \phi(n/d)$$

因为当d遍历n的所有正因子时, n/d也遍历所有n的正因子, 从而

$$n = \sum_{d|n} \phi(n/d) = \sum_{d|n} \phi(d)$$

定理证完.

back

6.10 原根

例 6.22

设$n = 18$, d是n的一个因子. 对于整数m, $1 \leq m \leq 18$, $m \in C_d$当且仅当$(m, 18) = d$, 例如$d = 1$时, $1, 2, \cdots, 18$中所有与18互素的数作成集合C_1; 当$d = 2$时, $1, 2, \cdots, 18$中所有与18的最大公因子为2的数作成集合C_2, 等等. 通过计算, 可知

$$\begin{aligned} C_1 &= \{1, 5, 7, 11, 13, 17\}, & C_6 &= \{6, 12\}, \\ C_2 &= \{2, 4, 8, 10, 14, 16\}, & C_9 &= \{9\}, \\ C_3 &= \{3, 15, \}, & C_8 &= \{18\}. \end{aligned}$$

我们看到, $d = 1, 2, 3, 6, 9, 18$, C_d类包含$\phi(18/d)$个整数, 并且有

$$18 = \phi(18) + \phi(9) + \phi(6) + \phi(3) + \phi(2) + \phi(1).$$

back

6.10 原根

现在进一步讨论$F(d)$和$\phi(d)$ 的关系.

定理 6.28

设p是一个素数, 正整数d是$p-1$的一个因子, 那么模p阶为d且不同余的整数的个数为$\phi(d)$.

证明: 由Fermat定理, 可知$1,2,\cdots,p-1$中的任何一个数都是方程$x^{p-1} \equiv 1 \pmod{p}$的解, 若其中某个数的次数是$d$, 根据定理6.20, d是$\phi(p)=p-1$的因子. 在$1,2,\cdots,p-1$ 这些数中挑出模p的阶为d的所有数组成集合F_d, 并且用$F(d)$表示集合F_d中元素的个数. 按照这种记法, 若$d' \neq d$是$p-1$的另一个不同于d的因子, 因为一个数的次数不可能既是d又是d', 于是$F_d \cap F_{d'} = \phi$,

6.10 原根

这样

$$p-1=\sum_{d|p-1}F(d)$$

因为根据定理6.27, 可知

$$p-1=\sum_{d|p-1}\phi(d)$$

所以

$$\sum_{d|p-1}F(d)=\sum_{d|p-1}\phi(d) \tag{6.10}$$

于是$F(d)=\phi(d)$.

back

6.10 原根

定理 6.29

每个素数p都有原根.

证明: 已知p是一个素数, 取$p-1$的因子$p-1$, 根据定理6.28, 可知存在$\phi(p-1)$个模p的阶为$p-1$且不同余的整数, 显然这些数中的每一个都是原根, 这就证明了每个素数p都存在原根而且原根还共有$\phi(p-1)$ 个.

后续的工作是确定存在原根的其它正整数.

6.10 原根

为了证明每个奇素数p的幂$p^{\alpha}(\alpha \geq 2)$都有原根. 先证明每个奇素数$p$的平方有原根.

定理 6.30

设p是一个奇素数. 若r是p的原根, 则r或$r+p$是p^2的原根, 也就是说p^2有原根.

证明: 已知r是模p的一个原根, 于是$ord_p r = \phi(p) = p-1$. 因为$(r,p) = 1$, 所以$(r,p^2) = 1$, 于是r模p^2的次数$ord_{p^2}\ r$ 存在, 可令$n = ord_{p^2}\ r$.

6.10 原根

这样

$$r^n \equiv 1 \pmod{p^2}$$

模p^2同余的两个数也一定模p同余, 故有

$$r^n \equiv 1 \pmod{p}$$

因为$p-1 = ord_p\ r|n$, 另一方面, $n = ord_{p^2}\ r$和$r^{\phi(p^2)} \equiv 1 \pmod{p^2}$(欧拉定理), 再因为$n|\phi\left(p^2\right)$, 而$\phi(p^2) = p(p-1)$, 即$n|p(p-1)$. 又由于$p-1|n$, 可设$n = q(p-1)$, 这样$q(p-1)|p(p-1)$, 推出$q|p$, 从而$q = 1$或者$q = p$, 也就是$n = p-1$或者$n = p(p-1)$. 下面分情况进行讨论.

back

6.10 原根

当$n = p(p-1)$ 时, 即$ord_{p^2} r = \phi\left(p^2\right)$, 这时, r是模p^2 的一个原根.

当$n = p - 1$ 时,

$$r^{p-1} \equiv 1(\mathrm{mod}\ p^2) \tag{6.11}$$

令$s = r + p$. 由于$s \equiv r(\mathrm{mod}\ p)$, s也是模p的一个原根. 按照前面的证明类似地可以得到, $ord_{p^2}\ s$ 为$p-1$或$p(p-1)$. 我们将通过证明$ord_{p^2}\ s = p - 1$是错误的, 也就得到得到$ord_{p^2}\ s = p(p-1)$. 为了证明$ord_{p^2}\ s \neq p - 1$, 首先利用二项式定理

back

6.10 原根

$$s^{p-1} = (r+p)^{p-1} = r^{p-1} + (p-1)r^{p-2}p + \binom{p-1}{2} r^{p-3}p^2 + \cdots + p^{p-1}$$
$$\equiv r^{p-1} + (p-1)pr^{p-2} (\mathrm{mod}\ p^2).$$

因此, 利用公式6.11, 可以得到

$$s^{p-1} \equiv 1 + (p-1)pr^{p-2} \equiv 1 - pr^{p-2} (\mathrm{mod}\ p^2)$$

于是

$$s^{p-1} - 1 \equiv -pr^{p-2} \pmod{p^2}$$

我们说

$$s^{p-1} \not\equiv 1 (\mathrm{mod}\ p^2)$$

若不然, 则$s^{p-1} \equiv 1 \pmod{p^2}$, 于是$p^2 | pr^{p-2}$, 推出$p | r^{p-2}$, 从而$p|r$. 这显然与$(p,r) = 1$相矛盾. 这样, 由于$ord_{p^2} s \neq p-1$, 可知$ord_{p^2} s = p(p-1) = \phi\left(p^2\right)$. 此时, $s = r+p$是模p^2的一个原根, 证完.

back

6.10 原根

例 6.23

根据例6.10, 可知$r = 3$是素数$p = 7$一个原根. 从定理6.30的证明过程可以得知, $r = 3$ 模7^2的阶数$ord_{7^2}3 = 7 - 1 = 6$ 或者$ord_{7^2}3 = 7(7 - 1) = 42$. 但因

$$r^{p-1} = 3^6 \not\equiv 1(\mathrm{mod}\ 49)$$

必有$ord_{49}3 = 42$. 因此, 3也是$p^2 = 49$的一个原根.

back

6.10 原根

下面定理说明了每个奇素数的任意次幂都有原根.

定理 6.31

设p是一个奇素数. 若r是模p^2的原根, 则对任意的$k \geq 3$, r也是模p^k的原根.

证明: 已知p有原根, 可设a是p的原根, 于是$a+p$也是模p 的原根. 因为当a不是模p^2的原根时, $a+p$一定为模p^2的原根. 所以总是存在一个整数r, r既是模p的一个原根, 又是模p^2的一个原根. 因为$ord_{p^2} r = \phi(p^2) = p(p-1) > p-1$, 根据次数的最小性可知,

6.10 原根

$$r^{p-1} \not\equiv 1 \pmod{p^2}$$

稍后利用数学归纳法, 我们将会证明这个原根r, 对所有的正整数$k \geq 2$都满足

$$r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k} \tag{6.12}$$

back

6.10 原根

下面先在这个(6.12)式成立的基础上来证明r也是模p^k的一个原根. 令$n = ord_{p^k} r$. 则$n|\phi(p^k)$. 因 $\phi(p^k) = p^{k-1}(p-1)$, 即$n|p^{k-1}(p-1)$. 由$ord_{p^k} r$的定义得知, $r^n \equiv 1 \pmod{p^k}$, 从而$r^n \equiv 1 \pmod{p}$. 于是$ord_p r = \phi(p) = p-1$可以整除n, 即$p-1|n$, 这样从$p-1|n$和$n|p^{k-1}(p-1)$, 可得$n = p^t(p-1)$, 其中t是一个满足$0 \le t \le k-1$的整数. 可以断言: $t = k-1$. 不然, $0 \le t \le k-2$. 因为

$$r^{p^{k-2}(p-1)} = \left(r^{p^t(p-1)}\right)^{p^{k-2-t}} \equiv (r^n)^{p^{k-2-t}} \equiv 1 \pmod{p^k}$$

back

6.10 原根

这与(6.12)矛盾. 因此, $ord_{p^k} r = p^{k-1}(p-1) = \phi(p^k)$. 所以$r$也是模$p^k$的一个原根.

用数学归纳法证明最后剩下的(6.12)式.

$k = 2$的情形可直接根据r是p^2的原根得出$r^{p-1} \not\equiv 1 (\mathrm{mod}\ p^2)$.

设结论对整数$k \geq 2$成立, 即

$$r^{p^{k-2}(p-1)}) \not\equiv 1 (\mathrm{mod}\ p^k) \tag{6.13}$$

back

6.10 原根

来证明$k+1$的时候成立. 由$(r,p)=1$可得$(r,p^{k-1})=1$. 根据欧拉定理可知,

$$r^{\phi(p^{k-1})}=r^{p^{k-2}(p-1)}\equiv 1(\mathrm{mod}\ p^{k-1})$$

因此, 存在一个整数d, 满足

$$r^{p^{k-2}(p-1)}=1+dp^{k-1} \tag{6.14}$$

由(6.13)式, 可知$p\nmid d$. (6.14)式的两边同时取p次方, 得到

back

6.10 原根

$$\begin{aligned} r^{p^{k-1}(p-1)} &= (1+dp^{k-1})^p \\ &= 1+p(dp^{k-1})+\binom{p}{2}(dp^{k-1})^2+\cdots+(dp^{k-1})^p \\ &\equiv 1+dp^k \pmod{p^{k+1}} \end{aligned}$$

由$p \nmid d$, 可知$p^{k+1} \nmid dp^k$, 而$p^{k+1} \mid r^{p^{k-1}p-1}-1-dp^k$, 所以$p^{k+1} \nmid r^{p^{k-1}p-1}-1$, 或者

$$r^{p^{k-1}p-1} \not\equiv 1 \pmod{p^{k+1}}$$

这也就是$k+1$的时候成立, 根据归纳法原理, (6.12)式得证.

back

6.10 原根

至此, 我们证明了

推论 6.4

任意的正整数t, 存在模p^t的原根.

例 6.24

前面例6.10说明3是模7和模7^2的原根. 因此, 对所有正整数t, 3 也是模7^t 的原根.

back

6.10 原根

奇素数幂的原根情况已经讨论完了. 现在来讨论素数2的幂这类数的原根的问题. 不难验证1和3分别是2和$2^2 = 4$的原根, 而对$2^\alpha(\alpha \geq 3)$, 情况就完全不同了. 下面将会证明这些数不存在原根.

定理 6.32

设a是一个奇数, k是一个整数, $k \geq 3$. 那么,

$$a^{\phi(2^k)/2} = a^{2^{k-2}} \equiv 1 \pmod{2^k}$$

证明: 用数学归纳法证明这个结论. 当$k = 3$时, 需要验证$a^2 \equiv 1 \pmod 8$成立. 这是因为a为奇数, 可设$a = 2b + 1$, b为整数. 有

$$a^2 = (2b+1)^2 = 4b^2 + 4b + 1 = 4b(b+1) + 1$$

back

6.10 原根

因为b和$b+1$中有一个偶数, 故有$8|4b(b+1)$, 从而$8 \mid a^2-1$, 即

$$a^2 \equiv 1 \pmod 8 \tag{6.15}$$

归纳假设k时成立, 也就是

$$a^{2^{k-2}} \equiv 1 \pmod{2^k}$$

于是存在整数d满足

$$a^{2^{k-2}} = 1 + d \cdot 2^k \tag{6.16}$$

(6.16)等式的两边平方得

$$a^{2^{k-1}} = 1 + d2^{k+1} + d^2 2^{2k}$$

所以

$$a^{2^{k-1}} \equiv 1 \pmod{2^{k+1}}$$

这说明$k+1$时成立, 归纳得证.

6.10 原根

推论 6.5

设$k \geq 3$为整数, 则2^k没有原根.

证明: 要证明2^k没有原根, 根据原根的定义, 需要验证每一个与2^k 互素的整数都不是原根, 而与2^k互素的整数只有奇数, 只需要验证每个奇数都不是原根即可. 事实上, 设a是任意一个奇数, 对于任意的$k \geq 3$, 因为

$$a^{\phi(2^k)/2} \equiv 1 \pmod{2^k}$$

这样, a的次数$ord_{2^k}a$最大为$\frac{\phi(2^k)}{2}(< \phi(2^k))$. 也就得出$a$不会是$2^k$的原根, 这就证明了$2^k$ $(k \geq 3)$没有原根.
虽然当$k \geq 3$时, 2^k没有原根, 但是却存在有最大阶$\phi(2^k)/2$的数.

back

6.10 原根

定理 6.33

假设$k \geq 3$是一个整数, 则有

$$ord_{2^k}5 = \phi(2^k)/2 = 2^{k-2}$$

证明: 由定理6.32, 当$k \geq 3$时, 有

$$5^{2^{k-2}} \equiv 1 \pmod{2^k}$$

因为, $ord_{2^k}5 | 2^{k-2}$. 因此, 如果证明$ord_{2^k}5 \nmid 2^{k-3}$, 就会得到

$$ord_{2^k}5 = 2^{k-2} = \phi(2^k)/2$$

为了证明$ord_{2^k}5 \nmid 2^{k-3}$, 下面将会用数学归纳法来证明对$k \geq 3$ 有

$$5^{2^{k-3}} \equiv 1 + 2^{k-1} \pmod{2^k}$$

6.10 原根

当$k=3$时, 有

$$5 \equiv 1+4 \pmod 8$$

假设k时成立, 即

$$5^{2^{k-3}} \equiv 1+2^{k-1} \pmod{2^k}$$

那么, 存在一个正整数d满足下式

$$5^{2^{k-3}} = (1+2^{k-1}) + d \cdot 2^k$$

两边同时平方得

$$5^{2^{k-2}} = (1+2^{k-1})^2 + 2(1+2^{k-1}) \cdot d \cdot 2^k + (d \cdot 2^k)^2$$

注意到等号右边的后两项都有2^{k+1}因子, 于是

$$5^{2^{k-2}} \equiv (1+2^{k-1})^2 = 1+2^k+2^{2k-2} \equiv 1+2^k \pmod{2^{k+1}}$$

所以结论对于$k+1$的情况成立. 因此我们证明了当$k \geq 3$有

$$5^{2^{k-3}} \equiv 1+2^{k-1} \pmod{2^k}$$

因为$1+2^{k-1} \not\equiv 1 \pmod{2^k}$, 所以$5^{2^{k-3}} \not\equiv 1 \pmod{2^k}$, 所以$ord_{2^k}5 \nmid 2^{k-3}$, 因此$ord_{2^k}5 = 2^{k-2} = \phi(2^k)/2$, 证完.

6.10 原根

下面是前面的讨论的一个总结.

$n = p^\alpha$(p是素数, $\alpha \geq 1$)的原根情况:

(1) 当p为奇素数时, p^α有原根;

(2) 当p为偶素数数($p = 2$). 若$\alpha = 1$或$\alpha = 2$, n有原根, 否则n 无原根.

这样, 像素数幂这种数的原根情况都清楚了.

下面讨论不是素数幂的整数是否存在原根的问题, 也就是可以被两个或更多的素数整除的整数原根情况. 我们将会证明: 不是素数的幂却存在原根的正整数, 刚好是奇素数幂二倍的整数.

先排除掉没有原根的数. 看以下结论.

6.10 原根

定理 6.34

若正整数n不是一个素数的幂或者不是一个素数的幂的2倍，则n不存在原根.

证明: 设正整数n不是一个素数的幂也不是一个奇素数的幂的2 倍, 则n 有素幂因子分解如下:

$$n = p_1^{t_1} p_2^{t_2} \cdots p_m^{t_m}$$

这个分解式至少有两项, 所以$m \geq 2$, 如果$p_1, p_2, \cdots, p_m$ 有一个是2, 可令$p_1 = 2$, 那么$t_1 \geq 2$. $t_2 \geq 1, \cdots, t_m \geq 1$, 设正整数$r$ 与n 互素, 即$(r, n) = 1$, 所以$\left(r, p_k^{t_k}\right) = 1$, $1 \leq k \leq m$. 根据欧拉定理, 可知

6.10 原根

$$r^{\phi(p_k^{t_k})} \equiv 1 \pmod{p_k^{t_k}}$$

用U表示$\phi(p_1^{t_1}), \phi(p_2^{t_2}), \cdots, \phi(p_m^{t_m})$的最小公倍数, 也就是

$$U = [\phi\left(p_1^{t_1}\right), \phi(p_2^{t_2}), \cdots, \phi(p_m^{t_m})]$$

由于$\phi(p_i^{t_i}) \mid U$, 故当$i = 1, 2, \cdots, m$有

$$r^U \equiv 1 (\mathrm{mod}\ p_i^{t_i}).$$

注意到$p_1^{t_1}, p_2^{t_2}, \cdots, p_m^{t_m}$两两互素, 有

$$r^U \equiv 1 \pmod{n}$$

这就是说有

$$ord_n r \leq U$$

back

6.10 原根

根据两个互素整数乘积的欧拉函数值是两个整数各自欧拉值的乘积, 可得

$$\phi(n) = \phi(p_1^{t_1} p_2^{t_2} \cdots p_m^{t_m}) = \phi(p_1^{t_1})\phi(p_2^{t_2}) \cdots \phi(p_m^{t_m})$$

因为当$k = 1, 2, \cdots, m$时, 有$\phi(p_k^{t_k}) = p_k^{t_k - 1}(p_k - 1)$都是2 的倍数, 故$U \leq \frac{1}{2}\phi(n)$, 既然存在一个比$\phi(n)$小的数$U$ 使得

$$r^U \equiv 1 \pmod{n}$$

表明r的次数不可能是$\phi(n)$, 也就是r不会是n的原根, n没有原根.

back

6.10 原根

通过前面的讨论, 已经把所要观察的对象限制为形如$n = 2p^t$的整数, 这里p是一个奇素数, t是一个正整数. 下面证明所有这种形式的整数都有原根.

定理 6.35

形如$2p^t$的整数都存在原根. 这里p为奇素数, t是正整数. 事实上, 若r是p^t的原根, 则, 当r是奇数时, r是$2p^t$的原根; 当r是偶数时, $r + p^t$ 是$2p^t$的原根.

back

6.10 原根

证明: 已知p^t是有原根的, 设r为其中之一, 于是

$$r^{\phi(p^t)} \equiv 1 (\mathrm{mod}\ p^t)$$

因为$\phi(2p^t) = \phi(2)\phi(p^t) = \phi(p^t)$, 于是,

$$r^{\phi(2p^t)} \equiv 1 \pmod{p^t} \tag{6.17}$$

下面我们分r是奇数和r是偶数来讨论.
(1) 当r是奇数时. $r^{\phi(2p^t)} - 1$ 有偶数因子$r-1$, 于是

$$r^{\phi(2p^t)} \equiv 1 \pmod{2} \tag{6.18}$$

back

6.10 原根

公式(6.17)和公式(6.18)中的两个模p^t和2 是互素的, 可得

$$r^{\phi(2p^t)} \equiv 1 \pmod{2p^t} \tag{6.19}$$

因为$\phi(2p^t) = \phi(p^t)$, r是模p^t的一个原根, 所以没有比$\phi(2p^t)$更小的数满足公式(6.19). 这就证明了r是$2p^t$的一个原根.

(2) 当r是偶数时. $r + p^t$是奇数, 因为$(r + p^t)^{\phi(2p^t)} - 1$是偶数$r + p^t - 1$的倍数, 自然也是2的倍数, 所以

$$(r + p^t)^{\phi(2p^t)} \equiv 1 \pmod{2} \tag{6.20}$$

back

6.10 原根

从r是偶数可知$(r, p^t) = 1$, 因此$(r + p^t, p^t) = 1$, 又$\phi(2p^t) = \phi(p^t)$, 由欧拉定理,

$$(r + p^t)^{\phi(2p^t)} \equiv 1 (\mathrm{mod}\ p^t) \tag{6.21}$$

结合(6.20)式和6.21式, 可知,

$$(r + p^t)^{\phi(2p^t)} \equiv 1 (\mathrm{mod}\ 2p^t) \tag{6.22}$$

注意到$r + p^t$是p^t的一个原根, 故没有比$\phi(2p^t)$更小的次数满足公式(6.22). 因此, $r+p^t$是模$2p^t$的一个原根.

6.10 原根

例 6.25

根据例6.24, 对所有的正整数t, 3是模7^t的原根. 由于3是奇数, 根据定理6.35, 可知3是模$2 \cdot 7^t$的原根. 例如, 当$t = 1$, 3是14的一个原根.

类似地, 对所有的正整数t, 2是模5^t的一个原根. 因为$2 + 5^t$是奇数, 可知, 对所有的正整数t, $2 + 5^t$模$2 \cdot 5^t$的一个原根. 例如, 取$t = 2$, 则27是50的一个原根.

back

3.10 指数的算术

本节介绍怎样利用原根进行算术运算.
设r是模m的一个原根, 已知下列整数

$$r, r^2, \cdots, r^{\phi(m)}$$

构成模m的一个既约剩余系. 因此, 若a是一个与m互素的整数, 则存在一个唯一的正整数x, $1 \leq x \leq \phi(m)$, 使得

$$r^x \equiv a \pmod{m}$$

这就引出了下面的定义.

定义 6.13

设r是正整数m的原根, 整数a与m互素. 使得同余式

$$r^x \equiv a \pmod{m}$$

成立的唯一的整数x, $1 \leq x \leq \phi(m)$, 叫做a对模m的以r为底的指数(或叫做离散对数). 若记$x = ind_r a$, 那么

$$r^{ind_r a} \equiv a \pmod{m}.$$

6.11 指数的算术

按照定义6.13, 若x是a对模m的以r为底的指数, $x = ind_r a$ 显然与m有关. 指数的记法中没有体现m是因为m是一个事先设定的数.

设a, b都与m互素且$a \equiv b \pmod{m}$, 那么$r^{ind_r a} \equiv a \equiv b \equiv r^{ind_r b} \pmod{m}$. 这样

$$ind_r a \equiv ind_r b \pmod{\phi(m)}$$

又因为, $1 \leq ind_r a, ind_r b \leq \phi(m)$, 所以必有$ind_r a = ind_r b$, 这就是说模$m$相等数的指数相同.

6.11 指数的算术

例 6.26

$m = 7$时, $\phi(7) = 6$. 已知3是模7的一个原根, 可知3^1, 3^2, 3^3, 3^4, 3^5, 3^6是模7的一个既约剩余系, 因为

$$3^1 \equiv 3 \pmod 7,\ 3^2 \equiv 2 \pmod 7,\ 3^3 \equiv 6 \pmod 7,$$
$$3^4 \equiv 4 \pmod 7,\ 3^5 \equiv 5 \pmod 7,\ 3^6 \equiv 1 \pmod 7.$$

因此, 对模7有

$$ind_3 1 = 6,\ ind_3 2 = 2,\ ind_3 3 = 1,$$
$$ind_3 4 = 4,\ ind_3 5 = 5,\ ind_3 6 = 3.$$

back

6.11 指数的算术

例 6.27

设$m = 7$, 因为5是模7的一个原根, 可知$5^1, 5^2, 5^3, 5^4, 5^5, 5^6$是模7的一个既约剩余系, 因为

$$5^1 \equiv 5 \pmod 7, 5^2 \equiv 4 \pmod 7, 5^3 \equiv 6 \pmod 7,$$
$$5^4 \equiv 2 \pmod 7, 5^5 \equiv 3 \pmod 7, 5^6 \equiv 1 \pmod 7.$$

因此, 对模7有

$$ind_5 1 = 6, ind_5 2 = 4, ind_5 3 = 5,$$
$$ind_5 4 = 2, ind_5 5 = 1, ind_5 6 = 3.$$

back

6.11 指数的算术

下面给出指数的一些性质. 只要将普通指数中的等式用模$\phi(m)$的同余式代替, 离散对数就拥有和普通对数相似的一些性质.

定理 6.36

设r是正整数m的原根, a, b都是与m互素的整数. 那么有
(1) $ind_r 1 \equiv 0 \pmod{\phi(m)}$,
(2) $ind_r(ab) \equiv ind_r a + ind_r b \pmod{\phi(m)}$,
(3) $ind_r a^k \equiv k \cdot ind_r a \pmod{\phi(m)}$, 其中$k$为正整数.

证明: (1) 因为r是模m的原根, 所以$r^{\phi(m)} \equiv 1 \pmod{m}$, 而且没有更小的$r$的方幂满足这个同余式, 根据指数的定义有$ind_r 1 = \phi(m)$, 当然有

6.11 指数的算术

$$ind_r 1 = \phi(m) \equiv 0 \pmod{\phi(m)}$$

(2) 由定义可知,

$$r^{ind_r a} \equiv a \pmod{m} \tag{6.23}$$

$$r^{ind_r b} \equiv b \pmod{m} \tag{6.24}$$

$$r^{ind_r (ab)} \equiv ab \pmod{m} \tag{6.25}$$

back

6.11 指数的算术

由(6.23)和(6.24)可知

$$r^{ind_r a} \cdot r^{ind_r b} = r^{ind_r a + ind_r b} \equiv ab \pmod{m} \tag{6.26}$$

由(6.25)和(6.26)可知

$$r^{ind_r(ab)} \equiv r^{ind_r a + ind_r b} \pmod{m} \tag{6.27}$$

再由(6.27), 可知

$$ind_r(ab) \equiv ind_r a + ind_r b \pmod{\phi(m)} \tag{6.28}$$

back

6.11 指数的算术

(3) 首先从指数的定义可以得到

$$r^{ind_r a^k} \equiv a^k \pmod{m} \tag{6.29}$$

$$r^{ind_r a} \equiv a \pmod{m} \tag{6.30}$$

由(6.30)可知,

$$r^{k \cdot ind_r a} = \left(r^{ind_r a}\right)^k \equiv a^k \pmod{m} \tag{6.31}$$

back

6.11 指数的算术

由(6.29)和6.31可知

$$r^{k\cdot ind_r a} \equiv r^{ind_r a^k} \pmod{m} \tag{6.32}$$

最后根据(6.32)可知

$$k \cdot ind_r a \equiv ind_r a^k \pmod{\phi(m)}. \tag{6.33}$$

back

6.12 原根在密码学中的应用

先介绍加密和解密的一般原理.

现代通信中, 所传信息的安全性无容讳言. 密码学就是基于这一要求产生的研究通信安全性的学科. 网络上的两个用户在发送和接收数据时, 若要防止他人窃听数据, 发送者可以对发送的**明文**数据进行**加密**变成加密后的**密文**数据, 使窃听者读不懂加密后的数据, 而达到安全通信的目的. 只有真正的接收方才可将收到密文后通过某种称为**解密**的变换或者说加密逆变换将密文还原成明文. 密码学技术的研究自然应涉及到加密方法和解密方法, 从这个意义上理解, 加密方法和解密方法是不能公开的. 但好的安全通信方法除了涉及到的加密算法和解密算法之外, 还涉及到与之相伴的称为"加密密钥"和"解密密钥"的参数, 由于它们之间的相互作用, 现在可以做到只要解密密钥参数秘密保管, 即使加密算法、解密算法和加密密钥都公开, 也不会影响通信的安全性. 只有拥有解密密钥的人, 才是可以解密密文的唯一用户. 任何第三方即使知道加密算法、解密算法和加密密钥也无法解密密文. 关于这方面的详细知识, 可参考有关密码学方面的书籍.

back

6.12 原根在密码学中的应用

人们习惯图6.1这个模型来描述安全的通信过程.

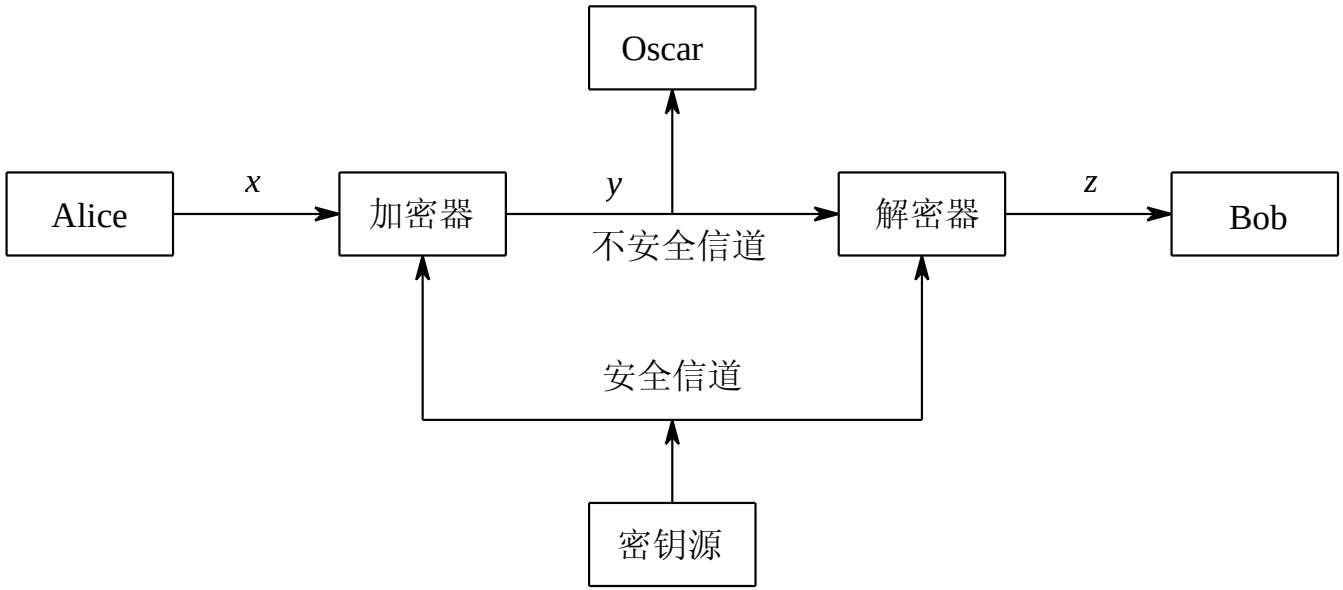


Figure 6.1: 保密通信模型

back

6.12 原根在密码学中的应用

具体说, 设加密算法、解密算法、加密密钥和解密密钥分别为E、D、p_a 和s_a, 加密器将明文X经过加密算法E和加密密钥p_a进行运算得到密文Y. 这个过程用下面的公式6.34 来描述.

$$Y = E_{p_a}(X) \tag{6.34}$$

密文Y经网络传输到解密器, 解密器用解密算法D和解密密钥s_b可解出明文X, 这个过程可用下面的公式6.35来描述.

$$D_{s_b}(Y) = D_{s_b}(E_{p_a}(X)) = X \tag{6.35}$$

back

6.12 原根在密码学中的应用

这个模型描述了信息安全通信的整个过程. 为了保证信息安全中的数字签名需要, 与(6.35)相对应的另外公式$E_{p_a}(D_{s_a}(x)) = X$也要成立.

当(6.35)中的p_a和s_b 相同时, 这种加密和解密体制称为**对称密码体制**. 其特点是发送者和接受者共享同一个秘密密钥. 在这种情况下, 当通信的参与者较多时, 发送者与不同用户之间的通信密钥应该不同, 这给发送者的密钥管理带来不便, 这一状况持续了很长时间. 幸运的是, 后人找到一个称为公钥密码体制的方法解决了这个长期困惑人们的问题.公钥密码体制是由Stanford大学的研究人员Diffie和Hellman于1976 年提出的. 其思想是在已有加密算法E和解密算法D的前提下, 每个通信用户拥有一对密钥, 加密密钥p和解密密钥即私钥s. 公有的加密算法E、解密算法D和每个用户的加密钥可对网络中的所有用户都公开, 但每个用户解密密钥由该用户秘密保管, 不能公开.

6.12 原根在密码学中的应用

设有通信中的两个用户A和B, 按照公钥体制通信的思想, A的公钥p_a 和B的公钥p_b可对网络中的所有用户都公开, A的私钥s_a和B的私钥s_b 则分别秘密保管. A与B安全通信时, A用p_b对明文信息采用加密算法E加密后发给B, 接收方B 用s_b 和解密算法D 进行解密. 从上面的讨论可知, 拥有s_b就意味着可以采用已公开的解密方法D将密文解密. 私钥s_b能解密出p_b加密的信息, 表明s_b与p_b之间有必然的联系. 既然B的p_b已经公开了, 第三方用户比如C尝试用公开的p_b来导出s_b, 以达解密的目的, C有这种想法完全是可能的. 公钥密码算法必须保证这种企图是不能实现的, 这也正是公钥密码算法设计的难度所在. 公钥密码算法的设计原则必须保证根据公钥推导私钥若在理论上做不到不可行, 起码在计算上应该是不可行的.

6.12 原根在密码学中的应用

再介绍数字签名的一般原理.

某些信息是可以公开的, 但不能被伪造和篡改. 一般情况下, 纸质书信或文件是根据信息发布人的亲笔签名或印章来证明其真实性的. 为了证明网络通信中电子文稿的真实性, 电子文稿又如何“签名”或者“盖章”呢? 这就是数字签名要解决的问题. 数字签名必须保证以下三点.

1. 接收方能够核实发送方对报文的签名
2. 发送方事后不能抵赖对报文的签名
3. 不能伪造报文的签名

back

6.12 原根在密码学中的应用

数字签名可以采用公钥密码方案来解决, 下面是其原理.
设加密和解密函数分别是$E(x)$和$D(x)$. 发送方A的私钥和公钥分别是s_a 和p_a, 发送方A要对信息x进行数字签名, 接收方B对签名后的报文进行验证, 以确保x的真实性.
下面是签名和验证的过程.
(1) 签名: 发送方用s_a对报文x进行计算得$D_{s_a}(x)$, $D_{s_a}(x)$ 便是所谓的签名报文, 然后将原始报文x和签名后报文的合成结果$(x, D_{s_a}(x))$发送至接收方B, .

6.12 原根在密码学中的应用

(2) 验证: 接受方使用发送方的公钥p_a进行计算得出

$$E_{p_a}(D_{s_a}(x)) = x$$

因为接受方恢复出报文x用的是A的公钥p_a, 所以接收方判断报文$(x, D_{s_a}(x))$是A签名发送的, 这就验证了报文的签名. 每个用户的公钥和私钥通常是从权威的第三方机构获取的. 利用签名来保证信息的真实性的技术能够保证任何除A之外的用户不能伪造A的签名消息, 原因是这种伪造的报文无法用A的公钥恢复出来. 同样地, 用户A也不能抵赖发出过签名的报文, 因为接受方可以把签名报文$(x, D_{s_a}(x))$出示给有权威的第三方, 第三方若用公钥p_a恢复出报文x, 那么, 拥有p_a者即A也就是报文的签名人.

back

6.12 原根在密码学中的应用

1985年ElGamal提出了一个利用原根理论可以进行加密和数字签名的方案. 在介绍具体的方案之前, 先介绍模重平方计算法.

在离散对数公钥方案中, 常常要对大正整数m和n, 计算

$$b^n \pmod m$$

这里b是一个小于n的正整数. 例如, 计算$12996^{227} \pmod{37909}$. 我们可以递归地计算

$$b^n \pmod m = (b^{n-1} \pmod m \cdot b) \pmod m$$

但这种计算较为费时, 须作$n-1$次乘法.

back

6.12 原根在密码学中的应用

现在, 将n写成二进制

$$n = n_0 + n_1 2 + \cdots + n_{k-1} 2^{k-1} + n_k 2^k$$

其中$n_i \in \{0, 1\}, i = 0, 1, \cdots, k-1$, 则$b^n \pmod m$的计算可归纳为

$$\underbrace{\underbrace{\underbrace{b^{n_0}(b^2)^{n_1}}(b^4)^{n_2}}(b^8)^{n_3} \cdots (b^{2^{k-2}})^{n_{k-2}}}(b^{2^{k-1}})^{n_{k-1}}(b^{2^k})^{n_k} \pmod m$$

这种计算方法叫做“模重复平方计算方法”. 具体算法如下:

back

6.12 原根在密码学中的应用

初始化: 令$a=1$, 将n按2的幂展开

$$n = n_0 + n_1 2 + \cdots + n_{k-1}2^{k-1} + n_k 2^k$$

(0) 如果$n_0 = 1$, 计算$a_0 = ab \pmod m$, 否则取$a_0 = a$, 即

$$a_0 = ab^{n_0} \pmod m$$

再计算$b_1 = b^2 \pmod m$. (第0步计算出a_0和b_1.)
(1) 如果$n_1 = 1$, 则计算$a_1 = a_0 b_1 \pmod m$, 否则取$a_1 = a_0$, 即计算

$$a_1 = a_0 b_1^{n_1} \pmod m$$

再计算$b_2 = b_1^2 \pmod m$. (第1步计算出a_1和b_2.)

back

6.12 原根在密码学中的应用

(2) 如果$n_2 = 1$, 则计算$a_2 = a_1 b_2 \pmod m$, 否则取$a_2 = a_1$, 即计算

$$a_2 = a_1 b_2^{n_2} \pmod m$$

再计算$b_3 = b_2^2 \pmod m$. (第2步计算出a_2和b_3.)

(3) 如果$n_3 = 1$, 则计算$a_3 = a_2 b_3 \pmod m$, 否则取$a_3 = a_2$, 即计算

$$a_3 = a_2 b_3^{n_3} \pmod m$$

再计算$b_4 = b_3^2 \pmod m$. (第3步计算出a_3和b_4.)

.....

back

6.12 原根在密码学中的应用

(k-2) 如果$n_{k-2}=1$, 则计算$a_{k-2}=a_{k-3}b_{k-2} \pmod m$, 否则取$a_{k-2}=a_{k-3}$, 即计算

$$a_{k-2}=a_{k-3}b_{k-2}^{n_{k-2}} \pmod m$$

再计算$b_{k-1}=b_{k-2}^2 \pmod m$. (第$k-2$步计算出$a_{k-2}$和$b_{k-1}$.)

(k-1) 如果$n_{k-1}=1$, 则计算$a_{k-1}=a_{k-2}b_{k-1} \pmod m$, 否则取$a_{k-1}=a_{k-2}$, 即计算

$$a_{k-1}=a_{k-2}b_{k-1}^{n_{k-1}} \pmod m$$

再计算$b_k=b_{k-1}^2 \pmod m$. (第$k-1$步计算出a_{k-1}和b_k.)

(k) 如果$n_k=1$, 则计算$a_k=a_{k-1}b_k \pmod m$, 否则取$a_k=a_{k-1}$, 即计算

$$a_k=a_{k-1}b_k^{n_k} \pmod m$$

最后a_k就是

6.12 原根在密码学中的应用

例 6.28

计算$12996^{227} \pmod{37909}$.

解: 设$m = 37909, b = 12996, a = 1$, 将227写成二进制,

$$227 = n_0 + n_1 2 + \cdots + n_{k-1}2^{k-1} + n_k 2^k = 1 + 2 + 2^5 + 2^6 + 2^7$$

可知, $n_0 = 0, n_1 = 1, n_2 = n_3 = n_4 = 0, n_5 = 1, n_6 = 1, n_7 = 1$.
运用模重复平方法, 依次计算可得
(0) $n_0 = 1$, 计算

$$a = a \cdot b \equiv 12996, b_1 \equiv b^2 \equiv 11421 (\text{mod } 37909)$$

(1) $n_1 = 1$, 计算

$$a_1 = a \cdot b_1 \equiv 13581, b_2 \equiv b_1^2 \equiv 32281 (\text{mod } 37909)$$

6.12 原根在密码学中的应用

(2) $n_2 = 0$, 计算

$$a_2 = a_1 \equiv 13581, b_3 \equiv b_2^2 \equiv 20369 (\text{mod } 37909)$$

(3) $n_3 = 0$, 计算

$$a_3 = a_2 \equiv 13581, b_4 \equiv b_3^2 \equiv 20065 (\text{mod } 37909)$$

(4) $n_4 = 0$, 计算

$$a_4 = a_3 \equiv 13581, b_5 \equiv b_4^2 \equiv 10645 (\text{mod } 37909)$$

back

6.12 原根在密码学中的应用

(5) $n_5 = 1$, 计算

$$a_5 = a_4 \cdot b_5 \equiv 22728, b_6 \equiv b_5^2 \equiv 6024 (\mathrm{mod}\ \ 37909)$$

(6) $n_6 = 1$, 计算

$$a_6 = a_5 \cdot b_6 \equiv 24073, b_7 \equiv b_6^2 \equiv 9663 (\mathrm{mod}\ \ 37909)$$

(7) $n_7 = 1$, 计算

$$a_7 = a_6 \cdot b_7 \equiv 7775 (\mathrm{mod}\ \ 37909)$$

最后, 计算出

$$12996^{227} \equiv 7775 (\mathrm{mod}\ \ 37909).$$

back

6.12 原根在密码学中的应用

下面就是离散对数ElGamal公钥加密方案.

(1) 用户甲选取一个大素数p和p的一个原根g, 再随机选取一个整数$a(1 \leq a \leq p-2)$. 计算

$$b = g^a \pmod{p}$$

b和a分别为用户甲的公钥和私钥, 用户甲对外公开(p, g, b), a不公开.

(2) 若用户乙需要将加密信息发送给用户甲. 加密过程为:

(2.1) 用户乙获取用户甲的(p, g, b). 对将要发送的明文信息M表示成整数$m(1 \leq m \leq p-1)$.

(2.2) 用户乙随机选取一个整数$k(1 \leq k \leq p-1)$, 计算

$$m_1 = g^k \pmod{p}, \quad m_2 = b^k m \pmod{p}$$

(2.3) 用户乙将(m_1, m_2)发送给用户甲, 此时(m_1, m_2)就是信息m的密文.

back

6.12 原根在密码学中的应用

(3) 用户甲收到密文后进行解密, 解密方法是: 对收到的密文(m_1, m_2)利用私钥a计算,

$$\left(m_2 \cdot m_1^{p-1-a}\right) \pmod{p}$$

结果为明文m.

back

6.12 原根在密码学中的应用

离散对数公钥算法证明:

证明: 只要证明算法的第三步, $(m_2 \cdot m_1^{p-1-a}) \pmod p$ 结果为m即可.
事实上, 因为$b = g^a \pmod p$, 可得$b \equiv g^a \pmod p$, 故$b^k \equiv g^{ak} \pmod p$, $b^k m \equiv g^{ak} m \pmod p$, 于是

$$m_2 = b^k m \pmod p = g^{ak} m \pmod p$$

back

6.12 原根在密码学中的应用

已知$m_1 = g^k \pmod p$, 可得$m_1 \equiv g^k \pmod p$, 故$m_1^{p-1-a} \equiv g^{k(p-1)-ka} \pmod p$, 于是

$$m_1^{p-1-a} \pmod p = g^{k(p-1)-ka} \pmod p$$

这样

$$\begin{aligned}(m_2 \cdot m_1^{p-1-a}) \pmod p &= ((g^{ak}m) \pmod p \cdot g^{k(p-1)-ka} \pmod p) \pmod p \\ &= (g^{ak}m \cdot g^{k(p-1)-ka}) \pmod p \\ &= (g^{k(p-1)}m) \pmod p \\ &= ((g^{p-1})^k m) \pmod p \\ &= m \pmod p \\ &= m.\end{aligned}$$

证完.

back

6.12 原根在密码学中的应用

例 6.29

已知用户甲选择的素数$p = 2357$, $g = 2$是p的一个原根, $a = 1751$是用户甲的密钥. 若用户乙发送给用户甲的信息表示成$m = 2035$, 且用户乙选取的$k = 1520$. 那么经过ElGamal公钥密码体制, 用户乙发送给用户甲的密文是什么? 用户甲如何恢复出明文m?

解: 按照算法,

(1) 用户甲先计算出自己的公钥

$$b = g^a \pmod p = 2^{1751} \pmod{2357} = 1185$$

后, 用户甲将信息$(p, g, b) = (2357, 2, 1185)$公开.

back

6.12 原根在密码学中的应用

(2) 用户乙得到$(p,g,b)=(2357,2,1430)$, 和选择了$k=1520$, 进行加密计算

$$m_1 = g^k \pmod p = 2^{1520} \pmod{2357} = 1430$$
$$m_2 = (b^k m) \pmod p = (1185^{1520}\cdot 2035) \pmod{2357} = 697$$

将密文$(m_1,m_2)=(1430,697)$发送给用户甲.
(3) 用户甲收到密文$(m_1,m_2)=(1430,697)$之后, 进行解密计算

$$\begin{aligned}(m_2 m_1^{p-1-a}) \pmod p &= (697\cdot 1430^{2357-1-1751}) \pmod{2357}\\ &= 2035\end{aligned}$$

恢复出明文2035.

back

6.12 原根在密码学中的应用

基于离散对数ElGamal数字签名方案:

设有发送签名消息的用户甲和验证签名消息的用户乙.

用户甲选取一个大素数p和p的一个原根g, 再随机选取一个整数$a(1 \leq a \leq p-2)$. 计算

$$b = g^a \pmod{p}$$

b和a分别为用户甲的公钥和私钥, 用户甲对外公开(p, g, b), a不公开.

用户甲对消息m签名的过程如下:

(1) 随机选择数一个与$p-1$互素的整数k;

(2) 计算$r = g^k \bmod p$;

(3) 计算$s = k^{-1}(m - ar) \bmod (p-1)$, 这$k^{-1}$是$k$模$p-1$的逆.

把(m, r, s)作为签名后的消息, 发送给用户乙.

back

6.12 原根在密码学中的应用

用户乙收到签名消息(m, r, s), 签名消息验证如下:
(1) 获取用户甲的公开信息(p, g, b).
(2) 计算$v_1 = b^r r^s \bmod p$和$v_2 = g^m \bmod p$;
(3) 若$v_1 = v_2$, 则签名消息有效; 否则, 无效.

ElGamal签名算法证明:

证明: 由于

6.12 原根在密码学中的应用

$$s = k^{-1}(m - ar) \bmod (p-1)$$

可知, $sk \equiv (m - ar) \bmod (p-1)$, $m \equiv (sk + ar) \bmod (p-1)$, 即 $m \equiv (sk + ar) \bmod \phi(p)$, 因而

$$g^m \equiv g^{sk+ar} \bmod p \tag{6.36}$$

已知$r = g^k \bmod p$, $b = g^a \bmod p$, 于是$g^k \equiv r \bmod p$, $g^a \equiv b \bmod p$, 进而有$(g^k)^s \equiv r^s \pmod p$, $(g^a)^r \equiv b^r \pmod p$, 于是

$$(g^k)^s \cdot (g^a)^r \equiv r^s \cdot b^r \pmod p \tag{6.37}$$

back

6.12 原根在密码学中的应用

根据式(6.36)和式(6.37)有

$$g^m \equiv g^{sk+ar} = (g^k)^s \cdot (g^a)^r \equiv r^s \cdot b^r \pmod{p}$$

可知

$$v_2 = g^m \pmod{p} = r^s \cdot b^r \pmod{p} = v_1$$

成立, 证完.

6.12 原根在密码学中的应用

下面是一个签名的具体例子.

(1) 用户甲取$p = 19$, 模19的一个原根$g = 2$和私钥$a = 5$. 那么用户甲的公钥为

$$b = g^a \pmod{p} = 2^5 \pmod{19} = 13.$$

用户甲将信息$(p, g, b) = (19, 2, 13)$公开.

(2) 用户甲将信息$m = 6$做数字签名, 取一个与$p - 1 = 18$互素的$k = 5$, 计算

$$r = g^k \pmod{19} = 2^5 \pmod{19} = 13,$$

back

6.12 原根在密码学中的应用

$$\begin{aligned} s &= k^{-1}(m - ar) \pmod{p-1} \\ &= 5^{-1}(6 - 5 \cdot 13) \pmod{18} \\ &= 11(6 - 5 \cdot 13) \pmod{18} \\ &= 17, \end{aligned}$$

用户甲将签名消息$(m, r, s) = (6, 13, 17)$发送给用户乙.

(3) 用户乙收到签名消息验证:

$$\begin{aligned} v_2 &= g^m \pmod{p} \\ &= 2^6 \pmod{19} \\ &= 13^{17} \cdot 13^{13} \pmod{19} \\ &= (r^s \cdot b^r) \pmod{p} \\ &= v_1. \end{aligned}$$

6.12 原根在密码学中的应用

ElGamal安全性讨论.

我们简要讨论一下ElGamal密码体制的安全性. 目前针对ElGamal 密码体制的主要攻击是求解离散对数问题: 给定g和$b = g^a \pmod p$, 求出a的值, 即计算$a = log_g b$. 如果密码分析这可以计算$a = log_g b$, 那么就可以使用它解密密文. 因此, 保证ElGamal密码体制安全性的一个必要条件就是p的离散对数是难解的. 到目前为止, 只要素数p选取适当, p 上的离散对数问题仍是难解的. 一般而言, 素数p 必须足够大, 且$p-1$至少包含一个足够大的素因数以防止使用Pohling-Hellman算法得到a.

如果p的离散对数是难解的, 即从p, g, b计算a是困难的, 那么是否可以在不知道a的情况下恢复明文x呢? 如果这样可以的话, 那么可以在不知道a和k的条件下使用x计算

$$xm_2^{-1} = b^{-k} mod p = m_1^{-a} mod p$$

即在不知道a和k时, 计算b^{-k}和m_1^{-1}, 这个问题也是困难的.

关于Pohling-Hellman算法可以参考文献[9].

back

目录

7.1 二元运算及性质

代数, 也称代数结构或代数系统, 是指定义有若干运算的集合. 例如, 整数集合, 在其上定义乘法和加法, 就成为一个代数系统. 用抽象方法研究各种代数系统性质的理论学科叫“近世代数”. 所谓抽象方法是指它并不关注组成代数系统的具体集合是什么, 也不关注集合上的运算如何定义, 而只假设这些运算遵循某些规则, 诸如结合律, 交换律, 分配律等等, 来讨论和和研究代数系统应有的性质, 所得的结论具有普遍意义.

本章将介绍代数系统的构成及其一般性质, 然后介绍几个重要的代数系统半群、群、环和域. 在介绍了相关知识的同时, 介绍了公钥密码系统RSA, 编码与纠错理论中的线性码和循环码的编码方案的应用.

7.1 二元运算及性质

利用映射的概念, 来定义代数运算这一概念.

定义 7.1

给定集合A, B和D, 一个$A \times B$到D的映射叫做一个$A \times B$到D 的**代数运算**.

按照定义, 对于A的任意元a和B的任意元b就可以通过映射代表的代数运算, 得到一个D的元d. 也可以说, 所给代数运算能够对a和b 进行运算, 而得到一个结果d. 这正是普通的计算法的特征. 例如, 普通加法就是能够把任意两个数加起来, 而得到另一个数.
我们用符号$\circ$表示代表运算的映射. 那么这个特殊的映射即运算可以表示成

$$\circ : \quad (a, b) \to d = \circ(a, b)$$

back

7.1 二元运算及性质

按照映射的表示方法, 元素(a,b)的像应该表示成$\circ(a,b)$, 由于我们将$\circ$看成运算, 元素(a,b)的像今后不写成$\circ(a,b)$, 而写成$a\circ b$. 这样, 我们描写代数运算的符号, 就变成

$$\circ: \quad (a,b)\to d=a\circ b$$

例 7.1

A={所有整数}, B={所有不等于零的整数}, D={所有有理数}.

$$\circ(a,b)\to \frac{a}{b}=a\circ b$$

是一个$A\times B$到D的代数运算, 也就是普通的除法.

back

7.1 二元运算及性质

例 7.2

设Z是整数集合, 一个$Z \times Z$到Z的映射:

$$\circ : \quad (a,b) \to a(b+1)$$

是Z上的一个代数运算.

例 7.3

设A是一个非空的集合, $\mathscr{P}(A)$是集合A的幂集, 则集合的并与交是幂集$\mathscr{P}(A)$上的两个代数运算.

back

7.1 二元运算及性质

在A和B都是有限集合的时候, 一个$A \times B$到D的代数运算, 可以用运算表来说明. 假定A有n个元$a_1, \cdots, a_n$, B 有m个元$b_1, \cdots, b_m$, $D = \{d_{ij} \mid i = 1, 2, \cdots, n; j = 1, 2, \cdots, m\}$, 则$A$, B到D的代数运算

$$\circ : \quad (a_i, b_j) \to d_{ij}$$

可以表示为

$\circ$	b_1	b_2	$\cdots$	b_m
a_1	d_{11}	d_{12}	$\cdots$	d_{1m}
$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$
a_n	d_{n1}	d_{n2}	$\cdots$	d_{nm}

back

7.1 二元运算及性质

当集合是有限集合的时候, 用运算表来说明一个代数运算, 常比用箭头或用等式的方法省事, 并且清楚.

$A \times B$到D的一般代数运算用到的时候比较少. 最常用的代数运算是$A \times A$到A的代数运算. 在这样的一个代数运算之下, 可以对A的任意两个元加以运算, 而且所得结果还是在A里面. 所以我们有

定义 7.2

假如$\circ$是一个$A \times A$到A的代数运算, 我们就说, 集合A对于代数运算$\circ$ 来说是闭的, 也说, $\circ$是A的代数运算或二元运算.

back

7.1 二元运算及性质

例 7.4

设F_2是实数域上的二阶非奇异方阵(行列式不等于0的矩阵)组成的集合, $\circ$ 是矩阵的普通乘法, 由于两个非奇异的矩阵的乘积还是一个非奇异矩阵, 因此, $\circ$ 是F_2上的二元运算.

例 7.5

正整数集合上的两个数的普通除法不是代数运算. 因为存在两个正整数的除法结果 不再是整数.

back

7.1 二元运算及性质

1. 结合律

给定集合A, 一个$A \times A$到A的代数运算$\circ$. 在A里任意取出三个元a, b, c来, 符号$a \circ b \circ c$在没有规定运算顺序的前提下是没有什么意义的, 因为代数运算只能对两个元进行运是来运算. 但是我们可以先对a 和b 进行运算, 而得到$a \circ b$, 因为$\circ$是$A \times A$到A 的代数运算, $a \circ b \in A$. 所以我们又可以把这个元同c来进行运算, 而得到一个结果. 这样得来的结果, 用加括号的方法写出来, 就是 $(a \circ b) \circ c$. 另外一种用加括号的方法写出来是$a \circ (b \circ c)$. 在一般情形之下, 由这两个不同的步骤所得的结果也未必相同.

back

7.1 二元运算及性质

例 7.6

设R是实数集, 对于R中的三个数$a=2, b=2$和$c=2$, $\circ$就是普通的减法, 显然有

$$(a \circ b) \circ c \neq a \circ (b \circ c)$$

定义 7.3

设集合A和A上的代数运算$\circ$, 假如对于A的任何三个元a, b, c都有

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

则称二元运算适合结合律.

7.1 二元运算及性质

例 7.7

设Z是整数集合, Z上的普遍加法和普通乘法都是适合结合律的代数运算.

上述例子中的运算都是常见的, 也可以是定义的其它运算.

例 7.8

设A是一个非空集合, $\circ$是A上的一个代数运算, 对于任意的$a, b \in A$ 有$a \circ b = b$, 证明$\circ$满足结合律.

证明: 对于任意三个元素$a, b, c \in A$, 有

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

于是$(a \circ b) \circ c = a \circ (b \circ c) = c)$, 可知$\circ$适合结合律.

back

7.1 二元运算及性质

例 7.9

判断有理数集合Q上的代数运算

$$\circ: \quad a \circ b = (a+b)^2$$

是否适合结合律?

解: 设$a=1, b=2, c=3$, 有

$$(a \circ b) \circ c = [(1+2)^2+3]^2 = (9+3)^2 = 144$$

$$a \circ (b \circ c) = [1+(2+3)^2]^2 = (1+25)^2 = 676$$

所以, 代数运算$\circ$不适合结合律.

back

7.1 二元运算及性质

在集合A里任意取出n个元$a_1, a_2, \cdots, a_n$来, 若没有指定运算步骤的话, 符号$a_1 \circ a_2 \circ \cdots \circ a_n$没有任何意义. 我们可以在元素之间加上一些括号代表一种运算步骤. 因为n是有限的, 故不同的运算方式也就是不同加括号的方法就是有限的. 可设所有加括号的方法总共N 个. 用

$$\pi_1(a_1 \circ a_2 \circ \cdots \circ a_n), \pi_2(a_1 \circ a_2 \circ \cdots \circ a_n), \cdots, \pi_N(a_1 \circ a_2 \circ \cdots \circ a_n)$$

来表示. 比方说, 当$n = 3$时, $N = 2$.

这样得来的N个结果一般情况下未必相等. 但是对于特定的运算(例如普通数的加法或乘法)来说它们也可能都相等. 规定:

7.1 二元运算及性质

定义 7.4

假如对于A的$n(n \geq 2)$个固定的元$a_1, a_2, \cdots, a_n$来说，所有的$\pi(a_1 \circ a_2 \circ \cdots \circ a_n)$都相等，我们就把由这些步骤可以得到的唯一的结果用$a_1 \circ a_2 \circ \cdots \circ a_n$来表示.

现在我们证明

定理 7.1

假如一个集合A的代数运算$\circ$适合结合律，那么对于A的任意个元$a_1, a_2, \cdots, a_n$来说，所有的$\pi(a_1 \circ a_2 \circ \cdots \circ a_n)$都相等. 因此符号$a_1 \circ a_2 \circ \cdots \circ a_n$也就总有意义.

back

7.1 二元运算及性质

证明:用数学归纳法.
$n = 3$时, 结论成立.
假定, 元的个数$\leq n-1$, 定理是对的. 对于任意的 $\pi(a_1 \circ a_2 \circ \cdots \circ a_n)$, 下面证明

$$\pi(a_1 \circ a_2 \circ \cdots \circ a_n) = a_1 \circ (a_2 \circ a_3 \circ \cdots \circ a_n) \tag{7.1}$$

注意到这一个$\pi(a_1 \circ a_2 \circ \cdots \circ a_n)$是经过一种加括号的步骤所得

back

7.1 二元运算及性质

来的结果, 这个步骤的最后一步总是对两个元进行运算:

$$\pi(a_1 \circ a_2 \circ \cdots \circ a_n) = b_1 \circ b_2$$

这里b_1是前面的若干个, 假定是i个元$a_1, a_2, \cdots, a_i$ 经过一个加括号的步骤所得的结果, b_2是其余的$n-i$个元a_{i+1}, a_{i+2}, $\cdots$, a_n经过一个加括号的步骤所得的结果. 因为i和$n-i$都$\leq n-1$, 由归纳法的假定,

$$b_1 = a_1 \circ a_2 \circ a_3 \circ \cdots \circ a_i, b_2 = a_{i+1} \circ a_{i+2} \circ \cdots \circ a_n$$

故

$$\pi(a_1 \circ a_2 \circ \cdots \circ a_n) = (a_1 \circ a_2 \circ \cdots \circ a_i) \circ (a_{i+1} \circ a_{i+2} \circ \cdots \circ a_n)$$

back

7.1 二元运算及性质

假如$i=1$, 那么上式就是(7.1)式, 我们用不着再证明什么.
假定$i>1$, 那么

$$\begin{aligned}\pi(a_1\circ a_2\circ\cdots\circ a_n) &= [a_1\circ(a_2\circ\cdots\circ a_i)]\circ(a_{i+1}\circ a_{i+2}\circ\cdots\circ a_n)\\ &= a_1\circ[(a_2\circ\cdots\circ a_i)]\circ(a_{i+1}\circ a_{i+2}\circ a_n)]\\ &= a_1\circ(a_2\circ a_3\circ\cdots\circ a_i\circ a_{i+1}\circ a_{i+2}\circ a_n)\end{aligned}$$

即(7.1)式仍然成立, 最后注意到(7.1)式等号的右端是一个固定的元素, 表明无论如何加括号, 运算结果总是相同, 所以元素个数为n时, 命题成立, 证完.

7.1 二元运算及性质

2. 交换律

定义 7.5

设$\circ$是$A \times A$到D的代数运算. 若对于A的任何两个元a, b, 总有

$$a \circ b = b \circ a$$

称运算$\circ$满足**交换律**, 简称可交换.

例 7.10

实数集合上的普通加法运算, 乘法运算都适合于交换律, 但减法和除法不适合交换律.

back

7.1 二元运算及性质

例 7.11

设Q为有理数集合, 对于Q中的任意两个元素a, b, 规定

$$\circ: \quad a \circ b = a + b + ab$$

则$\circ$适合交换律.

证明: 任取$a, b \in Q$, 因为

$$a \circ b = a + b + ab = b + a + ba = b \circ a$$

所以$\circ$适合交换律.

7.1 二元运算及性质

例 7.12

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

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

则$A\in S$且$B\in S$, 但

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

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

可见$A\circ B\neq B\circ A$.

7.1 二元运算及性质

我们有一个与上节的定理类似的

定理 7.2

假如一个集合A的代数运算$\circ$同时适合结合律与交换律, 那么在$a_1 \circ a_2 \circ \cdots \circ a_n$里, 元的次序可以调换.

证明: 用归纳法.
元的个数一个或两个元的时候, 定理是对的.
假定, 当元的个数$= n-1$时, 定理成立. 在这个假定之下, 我们证明, 若是把a_i 的次序任意颠倒一下, 而作成一个

$$a_{i_1} \circ a_{i_2} \circ \cdots \circ a_{i_n}$$

这里$i_1, i_2, \ldots, i_n$还是$1, 2, \cdots, n$这n个整数, 不过次序不同, 那么

$$a_{i_1} \circ a_{i_2} \circ \cdots \circ a_{i_n} = a_1 \circ a_2 \circ \cdots \circ a_n$$

$i_1, i_2, \cdots, i_n$中一定有一个等于n, 假定是i_k, 那么, 由于结合律, 交换律以及归纳法假定,

back

7.1 二元运算及性质

$$
\begin{aligned}
a_{i_1} \circ a_{i_2} \circ \cdots \circ a_{i_n} &= \left(a_{i_1} \circ \cdots \circ a_{i_{k-1}}\right) \circ \left[a_n \circ \left(a_{i_{k+1}} \circ \cdots \circ a_{i_n}\right)\right] \\
&= \left(a_{i_1} \circ \cdots \circ a_{i_{k-1}}\right) \circ \left[\left(a_{i_{k+1}} \circ \cdots \circ a_{i_n}\right) \circ a_n\right] \\
&= \left[\left(a_{i_1} \circ \cdots \circ a_{i_{k-1}}\right) \circ \left(a_{i_{k+1}} \circ \cdots \circ a_{i_n}\right)\right] \circ a_n \\
&= \left(a_1 \circ a_2 \circ \cdots \circ a_{n-1}\right) \circ a_n \\
&= a_1 \circ a_2 \circ \cdots \circ a_n
\end{aligned}
$$

证完.

back

7.1 二元运算及性质

结合律和或者交换律都只涉及一个代数运算, 下面介绍的分配率涉及到两个代数运算.

定义 7.6

设有集合A和B, $\odot$是一个$B \times A$的代数运算, $\oplus$是一个A上的代数运算. 若对于任何$b \in B$, 任何的$a_1, a_2 \in A$, 都有

$$b \odot (a_1 \oplus a_2) = b \odot a_1 \oplus b \odot a_2$$

则称代数运算$\odot$、$\oplus$适合第一分配率.

back

7.1 二元运算及性质

例 7.13

设A和B都是是全体实数的集合, $\cdot$ 和$+$就是普通的乘法和加法, 因为

$$b \cdot (a_1 + a_2) = b \cdot a_1 + b \cdot a_2$$

所以此例的代数运算$\cdot$、$+$适合第一分配率.

现在可以证明

定理 7.3

假如$\oplus$适合结合律, 而且$\odot$, $\oplus$适合第一分配律, 那么对于B 的任何b, A的任何$a_1, a_2, \cdots, a_n$来说,

$$b \odot (a_1 \oplus \cdots \oplus a_n) = (b \odot a_1) \oplus \cdots \oplus (b \odot a_n)$$

7.1 二元运算及性质

证明: 用归纳法. 当$n=1,2$的时候, 定理是对的. 假定, 当a_1, $a_2,\cdots$ 的个数只有$n-1$ 个的时候, 定理是对的, 看有n个a_i时的情形. 这时

$$\begin{aligned} b\odot(a_1\oplus\cdots\oplus a_n) &= (b\odot[(a_1\oplus\cdots\oplus a_{n-1})\oplus a_n] \\ &= [(b\odot(a_1\oplus\cdots\oplus a_{n-1})]\oplus(b\odot a_n) \\ &= [(b\odot a_1)\oplus\cdots\oplus(b\odot a_{n-1})]\oplus(b\odot a_n) \\ &= (b\odot a_1)\oplus\cdots\oplus(b\odot a_n) \end{aligned}$$

证完.

back

7.1 二元运算及性质

设$\odot$是一个$A\times B$到A的代数运算, $\oplus$是一个A 的代数运算. 那么 $(a_1\oplus a_2)\odot b$和$(a_1\odot b)\oplus(a_2\odot b)$ 都有意义.

定义 7.7

代数运算$\odot$, $\oplus$适合第二个分配律, 假如, 对于B的任何b, A 的任何a_1, a_2来说, 都有

$$(a_1\oplus a_2)\odot b=(a_1\odot b)\oplus(a_2\odot b)$$

定理 7.4

假如$\oplus$适合结合律, 而且$\odot$, $\oplus$适合第二分配律, 那么对于B 的任何b, A的任何$a_1, a_2, \cdots, a_n$来说,

$$(a_1\oplus\cdots\oplus a_n)\odot b=(a_1\odot b)\oplus\cdots\oplus(a_n\odot b)$$

证明: 和定理7.3的证明相似, 略.

7.2 代数系统

前面我们学习了$A \times B$到D的代数运算的定义，当A, B, D都是同一个集合的时候，这时二元运算就称为集合A上的二元运算. 例如，实数集合上上的加法就是一个二元运算. 实数集合上还有像减法、乘法等其它多种运算. 当然，一般集合上的二元运算也可以不止一个. 另外，除了这种涉及两个元素参与运算的双目运算符之外，集合可能还有只涉及单个元素运算的单目运算符和多于两个元素的运算符. 把这些一般因素都考虑到，下面给出代数系统的一般定义.

定义 7.8

一个非空集合A连同若干个定义在该集合上的运算$f_1, f_2, \cdots, f_k$所组成的系统就称为一个代数系统. 记作$(A, f_1, f_2, \cdots, f_k)$. 在不引起混淆的的情况下，代数系统$(A, f_1, f_2, \cdots, f_k)$有时也简单记作$A$.

back

7.2 代数系统

从代数系统的定义可以看出, 代数系统涉及到一个集合和集合上的几个运算, 每一个运算的运算结果还在集合中, 这一点称为运算对集合的封闭性. 我们以后只讨论有一个运算符的代数系统或者有两个运算符的代数系统.
代数系统的一个子集, 对于代数系统中的每个运算有可能还是封闭的.

定义 7.9

代数系统的A的一个子集M若还是代数系统, 则称M是A的子代数系统.

back

7.2 代数系统

例 7.14

设R是实数集合. $+$和$\times$是R上的普通加法和乘法, 那么$(R, +, \times)$ 是代数系统.

例 7.15

设A为一非空集合, $\mathscr{P}(A)$是A的所有子集作成的集合. $\cap$, $\cup$ 和$\sim$是集合通常的交, 并和求补运算. 那么$(\mathscr{P}(A), \sim, \cap, \cup)$ 是代数系统.

例 7.16

设Q是有理数集合. $+$和$\times$是Q上的普通加法和乘法, 那么$(Q, +, \times)$是例7.14中代数系统$(R, +, \times)$的子代数系统.

back

7.2 代数系统

从上面的一些例子看出，代数系统未必非得是集合A和集合A上的全部运算构成. 代数系统与集合上运算的数目没有必然的联系. 这样，集合A和A上的任意多个运算和可以构成代数系统，集合A和A上的一个代数运算也就可以构成代数系统.

同构和同态是代数系统中非常重要的概念. 下面将通过例子引入代数系统同态和同构的概念. 为了讨论问题方便，这里假设所有的代数系统都只有一个二元运算.

1.同构

设 $G=(R^+,\cdot)$, $S=(R,+)$, 这里R^+是所有正实数的集合，R 是所有实数的集合，运算“.”和“+”分别是实数的加法和乘法，容易验证$G=(R^+,\cdot)$ 和 $S=(R,+)$ 是两个代数系统. 我们在G 和 S 之间建立一个映射f:

$$f: \quad x \to \ln x, x \in R^+$$

7.2 代数系统

即对于任何正实数x, $f(x)=\ln x$. 由于当$x_1 \neq x_2$时, $f(x_1) \neq f(x_2)$, 并且对于任何实数y, 都存在正实数e^y, 使得$f(e^y)=\ln e^y = y$, 因此, f 是G 到S 上的一个一一映射.
对于任意的$x_1, x_2 \in G$, 有

$$f(x_1 \cdot x_2) = \ln(x_1 x_2) = \ln x_1 + \ln x_2 = f(x_1) + f(x_2)$$

这表示$(R^+, \cdot)$中任意二元素x_1和x_2, 按运算“$\cdot$”所得的结果$x_1 \cdot x_2$在f作用下的像$\ln(x_1 \cdot x_2)$, 恰好是这两个元素的像$\ln x_1$和$\ln x_2$在$(R, +)$中运算“$+$”所得结果$\ln x_1 + \ln x_2$. 可以说这个映射具有良好的性质.

7.2 代数系统

下面可以引入同构的定义.

定义 7.10

给定代数系统$(A, \circ)$和代数系统$(\overline{A}, \overline{\circ})$. 若在$A$和$\overline{A}$之间存在一一映射$\phi$, 对于任何的$a, b \in A$, 若

$$a \to \overline{a}, b \to \overline{b}$$

则

$$a \circ b \to \overline{a} \overline{\circ} \overline{b}$$

那么称代数系统A与$\overline{A}$同构, ϕ叫做A到$\overline{A}$ 之间的关于代数运算$\circ$和$\overline{\circ}$的**同构映射**.

back

7.2 代数系统

可以把两个代数系统同构归纳为:“两个代数系统之间一一映射是同构映射, 当且仅当任意两个元素运算结果的像等于这两个元素像的运算结果”. 也可以简单地说“两个代数系统同构当且仅当它们之间存在一个保持运算的一一映射”.

从代数结构上看, 可以把两个同构的代数系统视为同一个, 不过需要注意, 把同构的代数系统看做是相同的代数系统并没有说代数系统中的集合是相同的, 例如$(R^+,\cdot)$ 与$(R,+)$可以看做是相同的代数系统, 但R^+与R显然是两个不同的集合.

设ϕ是A与$\overline{A}$间的同构映射, 那么ϕ^{-1}就是$\overline{A}$ 与A间的同构映射. 因为, 在ϕ^{-1} 之下, 只要

$$\overline{a} \to a, \overline{b} \to b$$

显然就有

$$\overline{a} \overline{\circ} \overline{b} \to a \circ b$$

所以两个集合A和$\overline{A}$同构, 不需要考虑它们的顺序.

7.2 代数系统

2. 同态

当两个集合之间保持运算的映射不是一一映射, 只是一个普通的映射时, 我们有下面的定义.

定义 7.11

一个A到$\overline{A}$的映射ϕ,叫做一个对于代数运算$\circ$和$\bar{\circ}$来说的,A到$\overline{A}$的**同态映射**,假如,在ϕ之下,不管a和b是A的哪两个元,只要

$$a \to \overline{a}, b \to \overline{b}$$

就有

$$a \circ b \to \overline{a} \bar{\circ} \overline{b}$$

back

7.2 代数系统

下面看几个例子.

例 7.17

$A = \{\text{所有整数}\}$, A的代数运算是普通加法, $\overline{A} = \{1, -1\}$, $\overline{A}$的代数运算是普通乘法, 对于任意的$a \in A$

$$\phi_1 : \quad a \to 1$$

ϕ_1显然是一个A到$\overline{A}$的映射; 另外, 对于A的任意两个整数a和b来说, 总有

$$a \to 1, \quad b \to 1$$

$$a + b \to 1 = 1 \times 1$$

故ϕ_1是一个A到$\overline{A}$的同态映射.

7.2 代数系统

例 7.18

$A = \{\text{所有整数}\}$, A的代数运算是普通加法, $\overline{A} = \{1, -1\}$, $\overline{A}$的代数运算是普通乘法, 对于任意的$a \in A$

$$\phi_2\text{：}\ a \to 1, \text{若}a\text{是偶数；}\quad a \to -1, \text{若}a\text{是奇数}$$

则ϕ_2是一个A到$\overline{A}$的满射的同态映射.

back

7.2 代数系统

事实上, ϕ_2显然是A到$\overline{A}$的满射; 进一步, 对于A的任意两个整数a和b, 若a, b都是偶数, 那么

$$a \to 1 \quad , b \to 1$$

$$a + b \to 1 = 1 \times 1$$

若a, b都是奇数, 那么

$$a \to -1 \quad , b \to -1$$

$$a + b \to 1 = (-1) \times (-1)$$

若a奇, b偶, 那么

$$a \to -1 \quad , b \to +1$$

$$a + b \to -1 = (-1) \times (+1)$$

a偶, b奇时, 情形与上类似, 也有相同的结果.

7.2 代数系统

例 7.19

ϕ_3：$a \to -1$ (a是A的任一元)固然是一个A到$\overline{A}$ 的映射, 但不是同态映射. 因为, 取A的两个元素a和b, 使得

$$a \to -1 \quad , b \to -1$$

$$a + b \to -1 \neq (-1) \times (-1)$$

back

7.2 代数系统

A到$\overline{A}$的满射的同态映射对于我们比较重要. 我们约定: 今后所提到的同态映射都是指同态满射.

定理 7.5

假定, 对于代数运算$\circ$和$\overline{\circ}$来说, A与$\overline{A}$同态.那么,
(1) 若$\circ$适合结合律,$\overline{\circ}$也适合结合律;
(2) 若$\circ$适合交换律,$\overline{\circ}$也适合交换律.

证明: 我们用ϕ来表示A到$\overline{A}$的同态满射.

7.2 代数系统

(1) 假定$\bar{a},\bar{b},\bar{c}$是$\overline{A}$的任意三个元.那么，我们在A里至少找得出三个元a,b,c来，使得在ϕ之下，

$$a \to \bar{a}, b \to \bar{b}, c \to \bar{c}$$

于是，由于ϕ是同态满射，

$$(a \circ b) \circ c \to \overline{(a \circ b) \circ c} = \overline{a \circ b} \bar{\circ}\, \bar{c} = (\bar{a} \bar{\circ} \bar{b}) \bar{\circ} \bar{c}$$

$$a \circ (b \circ c) \to \overline{a \circ (b \circ c)} = \bar{a} \bar{\circ} \overline{b \circ c} = \bar{a} \bar{\circ} (\bar{b} \bar{\circ} \bar{c})$$

back

7.2 代数系统

但由题设,

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

这样, 和$\bar{a}\bar{\circ}(\bar{b}\bar{\circ}\bar{c})\bar{a}\bar{\circ}(\bar{b}\bar{\circ}\bar{c})$是$A$里同一元的象, 因而

$$\bar{a}\bar{\circ}(\bar{b}\bar{\circ}\bar{c}) = (\bar{a}\bar{\circ}\bar{b})\bar{\circ}\bar{c}$$

back

7.2 代数系统

(2) 我们看$\overline{A}$的任意两个元$\overline{a}, \overline{b}$, 并且假定, 在$\phi$之下,
$a \to \overline{a}$, $b \to \overline{b}$ （$a, b \in$）
那么,$a \circ b \to \overline{a} \circ \overline{b}$, $b \circ a \to \overline{b} \circ \overline{a}$,但$a \circ b = b \circ a$ 所以, $\overline{a} \circ \overline{b} = \overline{b} \circ \overline{a}$,
证完.

back

7.2 代数系统

定理 7.6

假定, $\odot$, $\oplus$ 都是集合A的代数运算, $\overline{\odot}$, $\overline{\oplus}$都是集合$\overline{A}$的代数运算, 并且存在一个A到$\overline{A}$的满射ϕ, 使得A与$\overline{A}$对于代数运算$\odot$, $\overline{\odot}$来说同态, 对于代数运算$\oplus$, $\overline{\oplus}$来说也同态. 那么, (1) 若$\odot$,$\oplus$适合第一分配律,$\overline{\odot}$,$\overline{\oplus}$也适合第一分配; (2) 若$\odot$,$\oplus$ 适合第二分配律,$\overline{\odot}$,$\overline{\oplus}$也适合第二分配律.

证明: 我们只证明(1), (2)可以完全类似地征明. 看$\overline{A}$的任意三个元$\overline{a}$,$\overline{b}$,$\overline{c}$,并且假定

$$a \to \overline{a} \quad , b \to \overline{b}, c \to \overline{c} \quad (a, b, c \in A)$$

那么

back

7.2 代数系统

$$a \odot (b \oplus c) \to \overline{a}\overline{\odot}(\overline{b \oplus c}) = \overline{a}\overline{\odot}(\overline{b}\overline{\oplus}\overline{c})$$
$$(a \odot b)\oplus (a\odot c) \to (\overline{a \odot b})\overline{\oplus}(\overline{a \odot c}) =(\overline{a}\overline{\odot}\overline{b})\overline{\oplus}(\overline{a}\overline{\odot}\overline{c})$$

但

$$a \odot (b \oplus c)=(a\odot b) \oplus (a\odot c)$$

所以

$$\overline{a}\overline{\odot}(\overline{b}\overline{\oplus}\overline{c})=(\overline{a}\overline{\odot}\overline{b})\overline{\oplus}(\overline{a}\overline{\odot}\overline{c}).$$

证完.

back

7.2 代数系统

最后我们还要规定一个名词. 一个集合A同A自己之间当然也可以有同构映射存在.

定义 7.12

若代数系统$(A, \circ)$到自身之间存在同构的的一一映射, 称该同构映射为A上的**自同构**.

back

7.2 代数系统

下面是一个自同构的例子.

例 7.20

$A = \{1, 2, 3\}$.代数运算$\circ$由下表给定:

$\circ$	1	2	3
1	3	3	3
2	3	3	3
3	3	3	3

那么

$$\phi: \quad 1 \to 2, \quad 2 \to 1, \quad 3 \to 3$$

是一个对于$\circ$来说的A上的自同构.

back

7.3 半群

群是一种具体的代数系统. 群论研究群的代数结构。群在代数系统中有最基本的重要地位：许多代数结构, 包括环、域可以看作是在群的基础上添加新的运算和公理而形成的. 群的研究方法对其他代数系统有重要影响. 目前, 许多不同的物理结构, 如晶体结构和氢原子结构都可以用群论方法来进行建模, 因此群论的重要性已体现在物理学和化学的研究中. 另外, 群在现代通信中数据的安全性方面, 也有很重要的应用. 本章主要涉及群的概念和性质等知识, 最后给出了群在公钥密码学方面的应用.

先从半群说起.

7.3 半群

半群是最简单的代数系统.

定义 7.13

设$(S,\circ)$是一个代数系统, 其中S为非空集合, $\circ$是其二元运算, 如果运算$\circ$是可结合的, 即对任意的$a,b,c\in S$有

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

则称$(S,\circ)$为**半群**.

定义 7.14

若半群$(S,\circ)$中的$\circ$是可交换的, 则称半群$(S,\circ)$叫做**可换半群**.

7.3 半群

例 7.21

设集合$S_k = \{x \mid x是整数且x \geq k\}$, $k \geq 0$, 其中$+$是普通的加法运算. 那么S_k 是一个半群.

解: 因为$+$在S_k上是封闭的, 故$(S_k, +)$是一个代数系统, 又因为普通加法运算是可结合的, 所以$(S_k, +)$是一个半群. 附带说明一下, $k \geq 0$这个条件是重要的. 否则, 若$k < 0$, 则运算$+$在S_k上将不是封闭的.

例 7.22

设$S = \mathscr{P}(A)$, A非空, 则$(S, \cap)$与$(S, \cup)$为两个半群, 且都是可换半群.

7.3 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

$$A_1 \cap A_2 = A_2 \cap A_1,$$

$$A_1 \cup A_2 = A_2 \cup A_1$$

附带说明一下, $(S, -)$不是半群, 这里运算“$-$”表示集合的减法. 因为取$A_1 = \{a, b\}, A_2 = \{c\}, A_3 = \{b, c\}$, 则

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

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

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

7.3 半群

例 7.23

设S是全体实数集合上所有二阶方阵的集合. 则$(S,\times)$与$(S,+)$是两个半群. 这里$\times$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.

解: 因为两个二阶方阵的和以及乘积还是二阶方阵, 并且矩阵的加法和乘法满足结合律, 且加法可交换, 故$(S,\times)$与$(S,+)$都是半群, $(S,+)$还是交换半群.

定义 7.15

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.

7.3 半群

定理 7.7

半群$(S, \circ)$的非空子集M是半群的充要条件是M关于$\circ$封闭.

证明: 根据子半群的定义, 该结论是显然的.

例 7.24

设S是元素为实数的所有二阶方阵的集合, 运算$\times$为矩阵乘法. 不难知道, $(S, \times)$ 是半群. 若M 是元素为实数的所有二阶非奇异矩阵之集合, 则$(M, \times)$ 是半群$(S, \times)$ 的子半群.

证明: 显然有M是S的子集. 任取$A, B, C \in M$, 那么$|A| \neq 0$, $|B| \neq 0$, 根据矩阵的乘法可知, $|AB| = |A||B| \neq 0$, 即M关于$\times$封闭. 另外, $(AB)C = A(BC)$, 故$(M, \times)$ 是$(S, \times)$ 的子半群.

7.3 半群

另外, 对于矩阵的加法是可交换的, 所以 $(S,+)$是可换半群, 但$(M,+)$ 却不是$(S,+)$ 的子半群, 自然不是可换的子半群. 事实上, 取

$$A_1=\begin{pmatrix}1&0\\0&1\end{pmatrix},A_2=\begin{pmatrix}-1&0\\0&-1\end{pmatrix},$$

则$A_1, A_2 \in M$, 但$A_1+A_2 \notin M$(A_1+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.

back

7.3 半群

实数集合中的0和1是比较特殊的数, 我们也关心代数系统中与此相似的元素.

定义 7.16

设$(S,\circ)$是一个半群.
(1) 若存在元素$e \in S$, 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**.
(2) 若存在元素$f \in S$, 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**.
(3) 若半群$(S,\circ)$ 的一个元素e既是左单位元, 又是右单位元, 则称该元素为半群$(S,\circ)$的**单位元**.

back

7.3 半群

一个半群, 可以有左单位元, 又有右单位元, 见例子7.25.

例 7.25

设A是所有正整数组成的集合, $\circ$是普通乘法运算, 则$(A, \circ)$, 是代数系统. 1 是左单位元, 也是右单位元.

一个半群, 可以没有左单位元, 也没有右单位元. 见例子7.26.

例 7.26

设A是所有偶数组成的集合, $\circ$是普通乘法运算, 则$(A, \circ)$, 是代数系统. $(A, \circ)$没有左单位元, 也没有右单位元.

back

7.3 半群

一个半群可以有左单位元, 但没有右单位元. 见例子7.27.

例 7.27

设S是一个集合, $|S| \geq 2$, 对于任意的$a, b \in S$, 规定:

$$a \circ b = b$$

则S是一个有左单位元, 但没有右单位元的半群.

证明: 由于任意的$a, b \in S$, 都有$a \circ b = b \in S$, 于是运算是封闭的, $(S, \circ)$ 是代数系统. 对于任意的$a, b, c \in S$, 有

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

运算$\circ$满足集合律, 所以$(S, \circ)$是代数系统. 按照定义, 代数系统的每个元素都是左单位元. S中的元素个数至少为2, 故对于任意的$b \in S$, 存在$a \in S$, 使得$a \neq b$, 因为$a \circ b = b \neq a$, 所以b不可能是$(S, \circ)$的右单位元, 由b 的任意性, 可知$(S, \circ)$没有右单位元.

back

7.3 半群

一个半群可以有右单位元, 但没有左单位元, 见例子 7.28.

例 7.28

设S是一个集合, $|S| \geq 2$, 对于任意的$a, b \in S$, 规定:

$$a \circ b = a$$

则S是一个有右单位元, 但没有左单位元的半群.

证明: 由于任意的$a, b \in S$, 都有$a \circ b = a \in S$, 于是运算是封闭的, $(S, \circ)$ 是代数系统. 对于任意的$a, b, c \in S$, 有

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

运算$\circ$满足集合律, 所以$(S, \circ)$是代数系统. 按照定义, 代数系统的每个元素都是右单位元. S中的元素个数至少为2, 故对于任意的$a \in S$, 存在$b \in S$, 使得$a \neq b$, 因为$a \circ b = a \neq b$, 所以a不可能是$(S, \circ)$的左单位元, 由a 的任意性, 可知$(S, \circ)$没有左单位元.

back

7.3 半群

综上所述, 存在半群既有左单位元, 也有右单位元; 存在半群既没有左单位元, 也没有右单位元; 存在半群有左单位元而没有右单位元素; 存在半群有右单位元素而没有左单位元素.

需要说明的是, 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. 因为我们有下述定理.

定理 7.8

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.

back

7.3 半群

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e_1和e_2都是$(S, \circ)$的单位元素, 则$e_1 \circ e_2 = e_1 = e_2$, 故$(S, \circ)$只能有一个单位元素. 证毕.

一个有单位元的半群, 其子半群可能没有单位元. 见例子7.29

例 7.29

设Z是整数集合, Z^+是正整数集合. $(Z, +)$与$(Z^+, +)$均是半群, 代数运算$+$ 为数的加法. $(Z^+, +)$ 是$(Z, +)$ 的子半群, 半群$(Z, +)$ 有单位元素0, 而其子半群$(Z^+, +)$ 却没有单位元.

back

7.3 半群

一个有单位元的半群S, 子半群有单位元, 但与S的单位元不相等, 见 例子7.30

例 7.30

设$A = \{a, b, c\}$, S是A的幂集$\mathscr{P}(A)$, 则$(S, \cap)$ 是有单位元A 的半群. 取S的子集$M = \{\{a\}, \{b\}, \{a, b\}, \phi\}$, 易证$(M, \cap)$ 是子半群, $(M, \cap)$的单位元素是$\{a, b\}$, 和$(S, \cap)$的单位元A不相等.

综上所述, 一个有单位元e的半群$(S, \circ)$, 其子半群未必有单位元素; 即使有的话, 也未必等于e.

back

7.3 半群

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 7.17

设$(S,\circ)$是有单位元素e的半群, $a \in S$.
(1) 若存在$a' \in S$, 使$a \circ a' = e$, 则称元素a是右可逆的, a'叫做a 的一个右逆元.
(2) 若存在$a'' \in S$, 使$a'' \circ a = e$, 则称元素a叫做左可逆的, a''叫做a 的一个左逆元.
(3) 若存在$b \in S$, 使得$ba = ab = e$, 则称元素a为可逆元, b叫做a的一个逆元.

back

7.3 半群

由定义可知, 可逆元一定既是左可逆元, 又是右可逆元. 而且可逆元a的逆元, 既是a 的左逆元, 又是a的右逆元. 又若S是交换群, 则左(右)可逆元一定是右(左)可逆元, 而且也是可逆元.

例 7.31

全体正整数的集合A是关于数的乘法是一个交换半群, 1是可逆的并且1的逆元是1, 对于其它任何一个正整数a, 显然不存在整数b, 使得$ab = 1$, 于是A中只有1是可逆的.

back

7.3 半群

例 7.32

设$A=\{a,b,c\}$, S是A的幂集$\mathscr{P}(A)$, 则$(S,\cap)$ 是有单位元A 的交换半群. 对于S中元素A, 因为$A\cap A=A$, 所以A是可逆的, A的逆元为自身. 对于S 中 其它的任何元素, M, $M\neq A$, 由于对任何元素$N\in S$, $M\cap N\neq A$, 于是M不是可逆的.

back

7.3 半群

定理 7.9

设$(S,\circ)$是有单位元素e的半群, $a \in S$, 若a既是右可逆的又是左可逆的, a' 是a 的一个右逆元, a''是a的一个左逆元, 则$a' = a''$. 即一个元既是右可逆的又是左可逆的时候, 它一定是可逆元.

证明: 因$a\circ a' = e, a''\circ a = e$,故有$a' = e\circ a' = (a''\circ a)\circ a' = a''\circ (a\circ a') = a''\circ e = a''$, 证完.

7.3 半群

定理 7.10

设$(S,\circ)$是有单位元素e的半群, 若$a \in S$是可逆的, 则a的逆元素唯一. 若用a^{-1}表示这个唯一的逆元, 还有有$(a^{-1})^{-1} = a$和$(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

证明: 假定a有两个逆元素b, c, 则$b = b \circ e = b \circ (a \circ c) = (b \circ a) \circ c = e \circ c = c$ 故可逆元素a 有惟一的逆元素, 若用符号 a^{-1} 来表示a 的唯一逆元, 那么

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

又由

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

可知

back

7.3 半群

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

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

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

证完.

back

7.3 半群

在一个半群里结合律是成立的, 所以

$$a_1 \circ a_2 \circ \cdots \circ a_n$$

有意义, 是半群的某一个元. 当这n个元都相等为a的时候. 这样得来的一个元用普通符号a^n 来表示:

$$a^n = \overbrace{aa\cdots a}^{n} \quad (n\text{是正整数})$$

并且也把它叫做a的n次乘方(简称n 次方).
设S是有单位元e的半群, $a \in S$是可逆的, n为正整数, 把$(a^{-1})^n$记作a^{-n}, 并且规定$a^0 = e$, 这样不难验证, 对于任何的整数m, n, 都有

$$a^m \circ a^n = a^{m+n}, \qquad (a^m)^n = a^{mn}$$

back

7.3 半群

S是所有整数的集合. S对于普通加法来说作成一个有单位元0的半群. 我们说, 这个半群的任何一个元素就都是1的乘方. 这一点假如把G的代数运算不用$+$ 而用$\circ$ 来表示就很容易看出. 因为1的逆元是-1. 假定m是任意正整数那么

$$m = \overbrace{1+1+\cdots+1}^{m} = \overbrace{1\circ 1\circ\cdots\circ 1}^{m} = 1^m$$

$$-m = \overbrace{(-1)+(-1)+\cdots+(-1)}^{m} = \overbrace{(-1)\circ(-1)\circ\cdots\circ(-1)}^{m} = 1^{-m}$$

back

7.3 半群

这样, G的不等于零的元都是1的乘方. 但是0是G的单位元, 照定义

$$0 = 1^0$$

这样G的所有元都是1的乘方(注意这里的乘方不是通常意义下的概念). 对于像这种性质的半群给出以下定义.

定义 7.18

若一个半群S的每一个都是S的某一个固定元a的乘方, 就把S叫做**循环半群**. 也说S 是由元a所生成的并且用符号

$$S = (a)$$

来表示. a叫做S的一个**生成元**.

7.4 群

上一节介绍了半群的有关知识, 现在来讨论群这个代数系统. 群也只有一种代数运算.

当一个代数系统只有一个运算的时候, 这个代数运算用什么符号来表示, 是可以由我们自由决定的, 有时可以用$\circ$, 有时可以用$\overline{\circ}$. 为书写方便起见, 有时不用$\circ$来表示, 而用普通乘法的符号来表示, 就是我们不写$a \circ b$, 而写ab. 也用a乘以b这种读法. 当然一个群的乘法一般不是普通的乘法.

back

7.4 群

定义 7.19

一个代数系统G称为一个群, 如果满足下列条件:
(1) 结合律成立, 即对任意的$a, b, c \in G$有$(ab)c = a(bc)$;
(2) 存在单位元素e: 即对任意的$a \in G$, 有$ea = ae = a$;
(3) 对G中任意元素a, 存在$a^{-1} \in G$, 使 $aa^{-1} = a^{-1}a = e$, 元素a称为可逆的, a^{-1}叫做a的一个可逆元.

一个是群的代数系统自然是一个半群, 因此, 我们在半群内得出一些结论, 比如单位元唯一, 一个可逆元的逆元唯一等, 就是自然成立的事了, 以后不再单独说明了.

back

7.4 群

定义 7.20

若群G满足交换律, 则称G为交换群, 或$Abel$群.

例 7.33

设Z, Q, R, C分别是整数集合, 有理数集合, 实数集合和复数集合, 则它们数的加法来说是一个群. 单位元素是0, 每个元素a 的逆元素为$-a$. 都是交换群.

back

7.4 群

例 7.34

设Q^*, R^*, C^*分别是非零有理数集合, 非零实数集合和非零复数集合, 则它们对数的乘法来说是一个群. 单位元素是1, 每个元素a 的逆元素为$\frac{1}{a}$. 都是交换群.

例 7.35

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E, 即为群$(S, \times)$的单位元素, 每个元素A的逆元素A^{-1}为A的逆阵. 因为矩阵的乘法不适合交换, S不是交换群.

back

7.4 群

例 7.36

设G是有理数集中去掉-1后的集合即$G = Q - \{-1\}$. 对于任意的$a, b \in G$, 定义

$$\circ : \qquad a \circ b = a + b + ab$$

则, G关于运算$\circ$称为一个群.

证明: 先说明$(G, \circ)$是一个代数系统. 事实上, 任意的$a, b \in G$, $a \circ b = a + b + ab \in Q$, 若$a + b + ab = -1$, 可知$(a+1)(b+1) = 0$, 也就是$a = -1$, 或者$b = -1$, 这与$a, b \in G$不符合. 故$a \circ b \in G$, 于是$(G, \circ)$是代数系统. 下面再来验证群定义的三个条件满足.

back

7.4 群

(1) 任取$a, bc \in G$. 因为

$$(a \circ b) \circ c = (a+b+ab)+c+(a+b+ab)c = a+b+c+ab+ac+bc+abc$$

$$a \circ (b \circ c) = a+(b+c+bc)+a(b+c+bc) = a+b+c+ab+ac+bc+abc$$

(2) $0 \in G$, 对于任意的$a \in G$, 有

$$0 \circ a = a \circ 0 = a$$

所以0是G的单位元.

back

7.4 群

(3) 设$a \in G$, 那么$\frac{-a}{a+1} \neq -1$, 于是$\frac{-a}{a+1} \in G$, 因为

$$a \circ \frac{-a}{a+1} = \frac{-a}{a+1} \circ a = \frac{-a}{a+1} + a + \frac{-a}{a+1} a = 0$$

G的每个元素都有逆元.

7.4 群

定理 7.11

若代数系统$(G,\circ)$中存在左单位元e, 并且每个元素关于e都是左可逆的, 则$(G,\circ)$ 是群.

证明: 我们只需证明左单位元e也是右单位元, 每个元素a关于e也是右可逆的即可.
先证每个元素a也是右可逆的. 事实上, 因为a是左可逆的, 存在$a \in G$, 使得$a'a = e$, 但a'也是左可逆的, 所以存在$a \in G$, 使得$a''a' = e$, 这样,

$$aa' = e(aa') = (a''a')(aa') = a''(a'a)a' = a''a' = e$$

所以a是右可逆的.
再证, e也是右单位元, 即对任意的$a \in G$, 都有$ae = a$即可. 事实上, 已证明元素a既是右可逆的又是左可逆的, 可设a'是a的右逆元和左逆元. 即$aa' = a'a = e$. 这样

$$ae = a(a'a) = (aa')a = ea = a$$

所以e是右单位元, 定理得证.

7.4 群

下面的结论和前面的类似. 就不再证明了.

定理 7.12

若代数系统$(G,\circ)$中存在右单位元e, 并且每个元素关于e都是右可逆的, 则$(G,\circ)$ 是群.

定义 7.21

一个代数系统G称为一个群, 如果满足下列条件:
(1) 结合律成立, 即对任意的$a,b,c\in G$有$(ab)c=a(bc)$;
(2) 存在左单位元素e: 即对任意的$a\in G$, 有$ea=a$;
(3) 对G中任意元素a都是左可逆的, 即存在左逆元$a'\in G$, 使 $a'a=e$.

7.4 群

定义 7.22

一个代数系统G称为一个群, 如果满足下列条件:
(1) 结合律成立, 即对任意的$a, b, c \in G$有$(ab)c = a(bc)$;
(2) 存在右单位元素e: 即对任意的$a \in G$, 有$ae = a$;
(3) 对G中任意元素a都是右可逆的, 即存在左逆元$a' \in G$, 使 $aa' = e$.

当验证一个代数系统是群的时候, 利用这两个定义, 稍微要简单一点.
下面是经常用到的几个名词和符号.

7.4 群

一个群G的元素的个数可以有限也可以无限. 我们规定

定义 7.23

一个群叫做**有限群**, 假如这个群的元的个数是一个有限整数. 不然的话, 这个群叫做**无限群**. 一个有限群的元的个数叫做这个**群的阶**.

下面是元素阶的概念.

定义 7.24

群G的一个元a. 能够使得

$$a^m = e$$

的最小的正整数m叫做a 的 **阶**, 记作$\circ(a) = m$. 若是这样的一个m不存在, 我们说, a 是无限阶的, 并记作$\circ(a) = \infty$.

back

7.4 群

例 7.37

G刚好包含$x^3=1$的三个根：

$$1, \varepsilon_1 = \frac{-1+\sqrt{-3}}{2}, \varepsilon_2 = \frac{-1-\sqrt{-3}}{2}$$

对于普通乘法来说这个G作成一个群.

事实上, 群定义中的

(1) 结合律显然成立;

(2) 1是G的单位元;

(3) 1的逆元1, ε_1的逆元是ε_2, ε_2的逆元是ε_1.

back

7.4 群

在这个群里1的阶是1, ε_1的阶是3, ε_2 的阶是3.

例 7.38

全体整数对于普通加法作成一个交换群, 0的阶是1, 其它非零整数的阶是无穷大.

元素的阶具有下列重要的性质.

定理 7.13

设群G的元素a的阶为某一正整数m, 即$\circ(a)=m$. 则

(1) $a^n=e \Leftrightarrow m|n$

(2) $a^h=a^k \Leftrightarrow m|h-k$

(3) $e=a^0,a,a^2,\cdots,a^{m-1}$两两不同.

(4) 对于整数r, $\circ(a^r)=\frac{m}{(m,r)}$. 其中$(m,r)$表示$m$ 与r 的最大公因子.

back

7.4 群

证明: (1) 设$m|n$, 则$n = mq$, 于是$a^n = a^{mq} = (a^m)^q = e^q = e$. 反之, 设$a^n = e$, 且$n = mq + r$, $0 \leq r < m$, 则$e = a^n = (a^m)^q a^r = a^r$. 因为$\circ(a) = m$, 由$m$的最小性, 可知$r = 0$, 由此, $m|n$.

(2) $a^h = a^k \Leftrightarrow a^{h-k} = e \Leftrightarrow m|h-k$.

(3) 若存在i, j, $0 \leq i \leq j \leq m-1$, 使得$a^i = a^j$, 则$0 < j - i \leq m-1$, 且$m|j-i$, 这是一个矛盾.

(4) 首先

$$(a^r)^{\frac{m}{(m,r)}} = (a^m)^{\frac{r}{(m,r)}} = e^{\frac{r}{(m,r)}} = e$$

所以$\circ(a^r)$是有限的. 现设$\circ(a^r) = n$, 则$n|\frac{m}{(m,r)}$, 而且$(a^r)^n = a^{rn} = e$, 于是$m|rn$, 从而$\frac{m}{(m,r)} \left| \frac{r}{(m,r)} n \right.$, 然而, $\left(\frac{m}{(m,r)}, \frac{r}{(m,r)}\right) = 1$, 所以, $\frac{m}{(m,r)} \mid n$, 因此, $n = \frac{m}{(m,r)}$.

7.4 群

推论 7.1

设$\circ(a) = m$.
(1) 对于任意的整数r, $a^r = m \Leftrightarrow (m, r) = 1$.
(2) 若$m = st$, t是正整数, 则$\circ(a^s) = t$.

定理 7.14

设$\circ(a) = \infty$.
(1) $a^n = e \Leftrightarrow n = 0$;
(2) $a^h = a^k \Leftrightarrow h = k$;
(3) $\cdots, a^{-2}, a^{-1}, a^0, a^1, a^2, \cdots$, 两两不等;
(4) 对于任意的非零整r, $\circ(a^r) = \infty$.

back

7.4 群

证明: (1) 由定义便知.
(2) $a^h = a^k \Leftrightarrow a^{h-k} = e \Leftrightarrow h - k = 0 \Leftrightarrow h = k$.
(3) 若$a^i = a^j$, 则由(2)可知, $i = j$.
(4) 若$\circ(a^r)$是有限的, 设$\circ(a^r)^n = e$, 也就是$a^{rn} = e$, 所以$\circ(a) \leq rn$, 这与$\circ(a) = \infty$矛盾.

定理 7.15

设G为有限群, 则G的任何元素的阶都是有限数.

back

7.4 群

证明: 对于G的任何元素a, $a, a^2, \cdots$不可能两两不同, 存在两个不同的正整数i, j, 使得$a^i = a^j$, 不妨设$i < j$, 于是$a^{j-j} = e$, 所以$\circ(a) \leq j - i$. 证完.

注意, 定理7.15的逆命题不成立. 因为存在每一个元素的阶都是有限数的无限群. 例如, 全体单位根组成的集合U, 这里

$$U = \bigcup_{m \in N} U_m = \{\varepsilon | \ \varepsilon \in C, \varepsilon^m = 1, m \in N\}$$

N是正整数集合.

7.4 群

现在我们讨论一下同态这一个概念在群上的应用, 以便以后可以随时把一个集合来同一个群比较, 或把两个群来比较.
设G是一个群, $\overline{G}$是一个不空集合, 并有一个代数运算. 这个代数运算我们 也把它叫做乘法, 也用普通表示乘法的符号来表示. $\overline{G}$的乘法当然同G 的乘法一般是完全不同的法则. 在$\overline{G}$同G的元的表示方法是有区别的前提下, 这两个乘法是不会搞混的.
现在我们证明

定理 7.16

设G是一个群, $\overline{G}$是一个代数系统, 假定G与$\overline{G}$ 对于它们的乘法来说同态, 那么$\overline{G}$也是一个群.

back

7.4 群

证明: G的乘法适合结合律, 而G与$\overline{G}$ 同态, 由 **??**页定理**??**, $\overline{G}$ 的乘法也适合结合律, 所以$\overline{G}$适合群定义的条件(1). 下面证明$\overline{G}$ 也适合(2), (3)两条.
(2). G有单位元e. 在所给同态满射之下, e有象$\bar{e}$:

$$e \to \bar{e}$$

事实上, $\bar{e}$就是$\overline{G}$ 的一个左单位元. 假定$\bar{a}$是$\overline{G}$ 的任意元, 而a是$\bar{a}$的一个逆象:

$$a \to \bar{a}$$

那么

$$ea \to \overline{ea} = \overline{a}\overline{e}$$

back

7.4 群

但

$$ea = a$$

所以

$$\bar{e}\bar{a} = \bar{a}$$

back

7.4 群

(3). 假定$\bar{a}$是$\bar{G}$的任意元, a是$\bar{a}$的一个逆象:

$$a \to \bar{a}$$

a是群G的元, a有逆元a^{-1}. 我们把a^{-1}的象叫做$\overline{a^{-1}}$:

$$a^{-1} \to \overline{a^{-1}}$$

那么

$$a^{-1}a \to \overline{a^{-1}}\bar{a}$$

但

$$a^{-1}a = e \to \bar{e}$$

所以

$$\overline{a^{-1}}\bar{a} = \bar{e}$$

这就是说, $\overline{a^{-1}}$是$\bar{a}$的左逆元, 也就是$\bar{a}$ 的逆元. 证完.

7.4 群

我们曾经给出循环半群的概念. 本节将要介绍循环群的知识. 在群的理论研究中, 循环群是一类结构非常清楚的群. 我们首先给出循环群的定义, 然后说明在同构的意义下, 循环群只有两类.

定义 7.25

若一个群G的每一个都是G的某一个固定元a的乘方, 就把G叫做**循环群**. 也说G是由元a所生成的并且用符号

$$G = (a)$$

来表示. a叫做G的一个**生成元**.

back

7.4 群

例 7.39

G是所有整数的集合. G的运算$\circ$是普通加法. 可以验证这是一个交换群, 而且这个群的全体的元就都是1的乘方. 事实上, 对于任意的正整数m, 有

$$m = \overbrace{1+1+\cdots+1}^{m} = \overbrace{1\circ 1\circ\cdots\circ 1}^{m} = 1^m$$

$$-m = \overbrace{(-1)+(-1)+\cdots+(-1)}^{m} = \overbrace{(-1)\circ(-1)\circ\cdots\circ(-1)}^{m} = 1^{-m}$$

这样, G的不等于零的元都是1的乘方. 但是0是G的单位元, 照定义

$$0 = 1^0$$

于是, G的所有元都是1的乘方(注意这里的乘方不是通常意义下的概念), 这个群也叫整数加群.

7.4 群

再看一个例子.
G是包含模n的所以个剩余类的集合.

$$G = \{[0], [1], [2], \cdots, [n-1]\}$$

按照剩余类的定义, 任何整数m, m 一定属于n个类中的某一个, 即存在$k, 0 \leq k \leq n-1$, 使得$[m] = [k]$. 下面规定一个G上的代数运算并用普通表示加法的符号$+$ 表示. 对于任意的$[a], [b] \in G$, 定义

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

back

7.4 群

注意, 等号左边的+是定义的运算符号, 等号右边的+是普通数的加法. 规定的这个运算首先应该是合理的, 也就是说当$[a'] = [a], [b'] = [b]$的时候, 必须有$[a+b] = [a'+b']$, 这一点也称剩余类的运算与代表元无关. 事实上, $[a'] = [a], [b'] = [b]$时, 就是说

$$a' \equiv a(n), \quad b' \equiv b(n)$$

也就是说

$$n|a'-a, \quad n|b'-b$$

因此

$$n|(a'-a)+(b'-b)$$
$$n|(a'+b')-(a+b)$$

于是

$$[a'+b'] = [a+b]$$

7.4 群

这样规定的$+$是一个G的代数运算, 该运算显然是封闭的, $(G,+)$是一个代数系统. 下面分别验证群的三个条件满足.

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

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

这就是说

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

并且

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

$$[-a]+[a]=[-a+a]=[0]$$

所以对于这个加法来说, G作成一个群. 这个群今后叫做模n的剩余类加群.

7.4 群

模n的剩余类加群的运算表如下.

+	[0]	[1]	$\cdots$	[n-2]	[n-1]
[0]	[0]	[1]	$\cdots$	[n-2]	[n-1]
[1]	[1]	[2]	$\cdots$	[n-1]	[0]
$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\vdots$
[n-1]	[n-1]	[0]	$\cdots$	[n-3]	[n-2]

back

7.4 群

由于G的每一个元也可以写成$[i],(1 \leq i \leq n)$的样子, 并且

$$[i] = \overbrace{[1] + [1] + \cdots + [1]}^{i}$$

这样得到的剩余类加群的任何一个元素也都是某个固定元素的乘方.

若把同构的群看做一样的话, 可以说循环群只有上面介绍的这两种, 这一点由下面的定理来保证.

7.4 群

定理 7.17

假定G是一个由元a所生成的循环群. 那么G的构造完全可以由a的阶来决定:
a的阶若是无限那么G与整数加群同构;
a的阶若是一个有限整数n, 那么G与模n的剩余类加群同构.

证明: 第一个情形: a的阶无限. 这时

$$a^h = a^k, \text{当而且只当} h = k \text{的时候.}$$

由$h = k$, 可得$a^h = a^k$ 显然. 假如$a^h = a^k$而$h \neq k$我们可以假定$h > k$ 而得到$a^{h-k} = e$ 与a的阶是无限的假定不合. 这样

$$a^k \to k$$

7.4 群

是G与整数加群$\overline{G}$间的一一映射. 但

$$a^h a^k = a^{h+k} \to h + k$$

所以

$$G \cong \overline{G}$$

第二种情形:a的阶是n, $a^n = e$. 这时

$$a^h = a^k \text{当而且只当} n|h-k \text{的时候}.$$

假如$n|h-k$, 那么$h-k = nq, h = k+nq$

7.4 群

$$a^h = a^{k+nq} = a^k a^{nq} = a^k (a^n)^q = a^k e^q = a^k$$

假如$a^h = a^k$, 叫$h - k = nq + r, 0 \leq r \leq n - 1$那么

$$e = a^{h-k} = a^{nq+r} = a^{nq} a^r = e a^r = a^r$$

由阶的定义$r = 0$, 也就是说$n | h - k$. 这样

$$a^k \to [k]$$

是G与剩余类加群$\overline{G}$间的一一映射. 但

$$a^h a^k = a^{h+k} \to [h + k] = [h] + [k]$$

所以

$$G \cong \overline{G}$$

证完.

7.4 群

若G是一个循环群, $G=(a)$. 当a的阶是无限大时, G的元是

$$\cdots, a^{-2}, a^{-1}, a^0, a^1, a^2 \cdots$$

G的乘法是

$$a^h a^k = a^{h+k}$$

当a的阶是n时, 那么 G的元可以写成

7.4 群

$$a^0, a^1, a^2, \cdots, a^{n-1}$$

G的乘法是

$$a^i a^k = a^{r_{ik}}$$

这里 $i + k = nq + r_{ik}, 0 \leq r_{ik} \leq n - 1.$

back

7.4 群

下面的定理7.18讨论了循环群中生成元的数量.

定理 7.18

设$G=(a)$是一个循环群.
(1) 若$\circ(a)=m>2$, 则G有$\varphi(m)$个生成元, 这里$\varphi(m)$表示$1,2,\cdots,m-1$中与m互素的元素个数, 若$(r,m)=1$, 那么a^r为生成元.
(2) 若$\circ(a)=\infty$, 则G只有两个生成元, a和a^{-1}.

证明: (1) 注意到循环群G中任意一个阶为m的元素都是生成元这一事实. 由于$\circ(a)=m$, $G=\{a^0,a^1,a^2,\cdots,a^{m-1}\}$, 因为元素$a^i$的阶是$\frac{m}{(i,m)}$, 所以$\circ(a^i)=m$当且仅当$(i,m)=1$, 这里$1\leq i\leq m-1$. (1) 得证.

back

7.4 群

(2) 因为a是生成元, 所以对任何的$b \in G$, 存在整数k, 使得$b = a^k$, 这样$b = (a^{-1})^{-k}$, 这就是说b也可以写成a^{-1}乘方的形式, 于是a^{-1}也是一个生成元, 显然有$a \neq a^{-1}$, 不然与a的阶无限相矛盾. 我们说, 其它的任何一个元素$c = a^t$ 都不会再是生成元了, 这里$|t| \geq 2$. 否则, 若c是生成元, 那么a 可以写成c 的乘方, 故存在整数s, 于是$a = c^s = (a^t)^s$, $a^{|st-1|} = e$, 可知$\circ(a) \leq |st-1|$, 这与a的阶是无穷大相矛盾. (2) 得证.

back

7.4 群

例 7.40

求出模12剩余类加群Z_{12}每一个元素的阶与所有的生成元.

解: 模12剩余类加群

$$Z_{12} = \{[0], [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11]\}$$

单位$[0]$ 的阶是1, 生成元$[1]$的阶是12, 我们可以这样求元素$[2]$的阶, 由于$[2] = [1]+[1] = [1]^2$, 所以$\circ([2] = \frac{12}{(2,12)} = 6$, 按照这个方法, 可以求出其它元素的阶是$\circ([3]) = 4$, $\circ([4]) = 3$, $\circ([5]) = 12$, $\circ([6]) = 2$, $\circ([7]) = 12$, $\circ([8]) = 6$,$\circ([9]) = 4$, $\circ([10]) = 6$, $\circ([11]) = 12$.

back

7.4 群

Z_{12}所有12阶的元素都是生成元, 它们是$[1]$, $[5]$, $[7]$, $[11]$.
对于一个素数p, 由于$1, 2, 3, \cdots, p-1$每一个都与p互素, 从而模p的剩余类加群Z_p除了单位元$[0]$的阶是1, 其它每个元素的阶都是p. 从而有下面的结论.

定理 7.19

对于一个素数p, 模p的剩余类加群Z_p 有$p-1$个生成元.

back

7.4 群

我们已经学习过映射、单射、满射和一一映射的概念. 本节讨论一个集合到自身的映射特别是一一映射的问题. 下面先对这种特殊的映射给出一个特殊的名字.

定义 7.26

一个集合到自身之间的一一映射称为变换.

相应地有单射变换, 满射变换和一一变换的概念, 这里就不再一一赘述了.

一个集合A在一般情形之下可以有若干个不同的变换, 下面是一个简单的例子.

7.4 群

例 7.41

$A=\{1, 2\}$.

$$\tau_1: \quad 1 \to 1, \quad 2 \to 1$$
$$\tau_2: \quad 1 \to 2, \quad 2 \to 2$$
$$\tau_3: \quad 1 \to 1, \quad 2 \to 2$$
$$\tau_4: \quad 1 \to 2, \quad 2 \to 1$$

是A的所有变换, 其中τ_3, τ_4是一一变换.

back

7.4 群

把给定是一个集合A的全体变换放在一起, 作成一个集合

$$S = \{\tau, \lambda, \mu, \cdots\}$$

规定S上的代数运算, 这个代数运算我们把它叫做乘法. 给定S的两个元τ 和λ, 规定τ 与 λ 的乘积$\tau\lambda$是先作变换λ 后作变换τ 复合的而得的变换. 由于S中的任意两个变换的复合变换还是一个变换, 所以这样定义的运算是封闭的.

back

7.4 群

例 7.42

对于例7.41中的集合A, A的所有变换作成的集合$S = \{\tau_1, \tau_2, \tau_3, \tau_4\}$, 取$\tau_1 \in S, \tau_2 \in S$, 那么, $\tau_1\tau_2(1) = \tau_1(\tau_2(1)) = \tau_1(2) = 1$, $\tau_1\tau_2(2) = \tau_1(\tau_2(2)) = \tau_1(2) = 1$, 所以

$$\tau_1\tau_2 = \tau_1$$

同样可以验证

$$\tau_3\tau_4 = \tau_4$$

back

7.4 群

例 7.43

设A是任何一个非空集合, S是A上的所有变换组成的集合, 那么S上的变换关于变换的复合运算满足结合律.

证明: 对于任意的τ, λ, μ, 因为, 对于任何的$a \in A$

$$(\tau\lambda)\mu(a) = \tau\lambda(\mu(a)) = \tau(\lambda(\mu(a)))$$

另一方面

$$\tau(\lambda\mu)(a) = \tau((\lambda\mu(a)) = \tau(\lambda(\mu(a)))$$

back

7.4 群

所以$(\tau\lambda)\mu = \tau(\lambda\mu)$, 即$S$的运算满足结合律.
我们已经验证S上的运算满足封闭性, 结合律. 若S关于这个运算是群的话, 那么S 中的单位元一定是A上的恒等变换. 事实上, 我们用ε表示A上的恒等变换, 即对任意的$a \in A$, 都有$\varepsilon(a) = a$, 并且设e是S的单位元, 由复合变换和单位元的定义我们有

$$\varepsilon = e\varepsilon = e$$

即恒等变换是S的单位元. 在恒等变换是单位元的前提下, S中的某些元素不一定有逆元, 因而, 一般情况下, S不是群.

back

7.4 群

例 7.44

对于例7.41中的集合A. $S=\{\tau_1,\tau_2,\tau_3,\tau_4\}$, 取$\tau_1\in S$, 因为对任意的$\tau\in S$, 都有$\tau_1\tau=\tau_1\neq\varepsilon$, 这样$S$不是群.

S不是群, S的一个子集有可能作成群.

例 7.45

$S=\{\tau_1,\tau_2,\tau_3,\tau_4\}$, 取$G=\{\tau_1\}$, 因为$\tau_1\tau_1=\tau_1$, 所以集合$G$关于变换的的乘法是封闭的, G 关于变换的乘法适合结合律, 显然单位元是τ_1, 元素τ_1的逆元素为自身, 根据群的定义, G是一个群.

back

7.4 群

例 7.46

设A是一个非空集合. G是A上的所有一一变换作成的集合. 则G关于变换的复合运算作成一个群.

证明: 取G任意的两个一一变换τ和λ, 我们将证明$\tau\lambda$ 也是一一变换, 也就是说集合G关于变换的乘法是封闭的. 事实上, 对于任意的$a \in A$, 因为τ是一一变换, 所以存在$b \in A$, 使得$\tau(b) = a$, 对于$b \in A$, 因为λ是一一变换, 所以存在$c \in A$, 使得$\lambda(c) = b$, 这样

7.4 群

$$a = \tau(b) = \tau(\lambda(c)) = \tau\lambda(c)$$

这说明变换$\tau\lambda$是满射. 再设$a, b \in A$, $a \neq b$, 由于λ 是一一变换, 所以$\lambda(a) \neq \lambda(b)$, 又因为$\tau$是一一变换, 所以$\tau(\lambda(a)) \neq \tau(\lambda(b))$, 也就是

$$\tau\lambda(a) \neq \tau\lambda(b)$$

这说明$\tau\lambda$是单射. 因此$\tau\lambda$是一一变换.
下面分别验证G满足群定义的三个条件.
首先, 因为变换满足结合律, 一一变换当然满足结合律. 其次, A上的恒等变换ε是一一变换, 所以$\varepsilon \in G$, 对于任意的$\tau \in G$, 由于

7.4 群

$$\varepsilon\tau = \tau\varepsilon = \tau$$

ε是G的单位元. 最后, 对于G中的任何变换τ的逆变换τ^{-1}, 因为τ^{-1}也是一一变换, 并且

$$\tau\tau^{-1} = \tau^{-1}\tau = \varepsilon$$

综上所述, G是群.

7.4 群

证明: 因为A上的恒等变换$\varepsilon \in G$, 所以ε是G的单位元. 对于任何$\tau \in G$, 我们首先证明τ是一一变换. 事实上, 设τ^{-1}是元素τ在群G中的逆元. 对于任何的$a \in A$, 因为$\tau\tau^{-1} = \varepsilon$, 所以

$$\tau\tau^{-1}(a) = \tau(\tau^{-1}(a)) = \varepsilon(a) = a$$

这就是说, $\tau^{-1}(a)$是a的原像, 于是τ是A到A的满射变换. 再设$a, b \in A$, $a \neq b$. 因为

$$a = \tau^{-1}\tau(a) = \tau^{-1}(\tau(a)) \neq \tau^{-1}(\tau(b)) = \tau^{-1}\tau(b) = b$$

back

7.4 群

而τ^{-1}是一一变换, 所以$\tau(a) \neq \tau(b)$. 这就证明了τ是一一变换.
其次, 对于任何的$\tau \in G$, 设τ^{-1}是τ在G中的逆元, 那么τ^{-1}是一一变换, 且因为对于任何的$a \in G$, 设$\tau(a) = b$, 则$a = \tau^{-1}\tau(a) = \tau^{-1}(b)$, 由逆变换的定义, τ^{-1}是τ的逆变换, 证完.

back

7.4 群

定义 7.27

一个集合A的若干个一一变换对于变换的复合运算作成的群叫做A的一个变换群.

本节讨论一个有限集合A的变换群的有关问题.

定义 7.28

一个有限集合的一个一一变换称为一个**置换**, 一个有限集合的若干个置换作成的群称为一个**置换群**.

back

7.4 群

设$A=\{a_1,a_2,\cdots,a_n\}$是一个有限集合. π是A的一个置换, 并且$\pi(a_i)=a_{k_i}, i=1,2,\cdots,n$. 这里$a_{k_1},a_{k_2},\cdots,a_{k_n}$是$a_1,a_2,\cdots,a_n$的一个排列. 这个置换$\pi$用

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_{k_1} & a_{k_2} & \cdots & a_{k_n} \end{pmatrix}$$

来表示. 由于我们主要关心集合A有几个元素, 以及集合A的元素之间的对应关系, 为了方便起见, 集合A的n个元素就用$1,2,\cdots,n$来表示, 这时置换π就变成

7.4 群

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ k_1 & k_2 & \cdots & k_n \end{pmatrix}$$

这里$k_1, k_2, \cdots, k_n$是$1, 2, \cdots, n$的一个排列. 在这种表示方法里第一行的n 个数字的次序显然没有什么关系, 也可用

$$\begin{pmatrix} 2 & 1 & 3 & \cdots & n \\ k_2 & k_1 & k_3 & \cdots & k_n \end{pmatrix}$$

back

7.4 群

来表示π. 最经常用到的还是$1, 2, \cdots, n$这个次序.
当集合A的元素个数为n时, 不难计算出集合A的一一置换的个数是$n!$. 由例7.46, 可知这些置换作成一个群.

定理 7.20

n个元素集合的所有一一置换作成一个置换群, 这个群用S_n来表示并称为n次对称群, S_n的阶为$n!$.

back

7.4 群

例 7.47

二次对称群s_2的阶为2, 两个元素分别是

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

由于

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$$

因此S_2的每个元素都可以用 $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ 来表示, 所以S_2是一个二阶循环群.

7.4 群

例 7.48

3次对称群S_3有6个元. 这6个元分别是

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

并且有

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

所以S_3不是交换群.

7.4 群

定义 7.29

设有非空集合A, G是A的一个置换群. 定义A上的二元关系$\sim$,

$$\sim: \quad a,b \in A, a \sim b \Leftrightarrow \text{存在} \pi \in G, \text{使得} \pi(a) = b$$

A上的二元关系$\sim$叫做由置换群G所诱导的关系.

定理 7.21

设G是非空集合A上的置换群. 则A上的G的诱导关系

$$\sim: \quad a,b \in A, a \sim b \Leftrightarrow \text{存在} \pi \in G, \text{使得} \pi(a) = b$$

是一个等价关系.

back

7.4 群

证明: 首先, 对于任何的元素$a \in A$, 因为恒等置换ε是置换群G的单位元并且有$\varepsilon(a) = a$, 于是$a \sim a$, 这样关系$\sim$是自反的. 其次, 设$a, b \in A, a \sim b$, 也就是说存在π, 使得$\pi(a) = b$. 设π^{-1}是置换π的逆变换, 于是$\pi^{-1}(b) = a$, 由于π^{-1}是π在群G的逆元, 所以$b \sim a$, 这样$\sim$是对称关系. 最后, 对于$a, b, c \in G$, 若$a \sim b$, $b \sim c$, 即存在$\pi, \sigma \in G$, 使得$\sigma(a) = b$, $\pi(b) = c$. 这样$\pi\sigma(a) = \pi(\sigma(a)) = c$, 因为$\pi\sigma \in G$, 所以$a \sim c$, 这样关系是传递的. 综合以上三个方面, 关系$\sim$是等价关系.

back

7.4 群

给定一个集合A和集合A上的一个置换群, 由G诱导的A上的等价关系必将产生A 的一个划分. 这个划分中的每一块都是一个等价类, 我们常常要计算划分中等价类的数目. 为此, 先介绍有关置换作用下不变元的概念.

定义 7.30

设A是一个非空有限集合, π是A的一个置换, 若对于$a \in A$, 有$\pi(a) = a$, 则称a是置换π的一个不变元. π的所有不变元的个数记作$\psi(\pi)$.

back

7.4 群

例 7.49

设集合$A=\{1,2,3,4\}$, 那么

$$\varepsilon=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\quad \tau=\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix},\quad \sigma=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix},$$

是A的三个置换, 按照定义$\psi(\varepsilon)=4$, $\psi(\tau)=2$和$\psi(\sigma)=0$.

定理 7.22

设非空有限集合A, G是A的一个置换群. 则由G诱导的等价关系将A划分所得的等价类的数目等于

$$\frac{1}{|G|}\sum_{g\in G}\psi(g)$$

back

7.4 群

证明: 首先, 对于任何一$a \in A$, 设$\eta(a)$表示G中使a不变的置换的个数. 由于$\sum_{g\in G}\psi(g)$和$\sum_{a\in A}\eta(a)$ 都是G 中置换作用下的不变元的总数, 因此

$$\sum_{g\in G}\psi(g)=\sum_{a\in A}\eta(a)$$

其次, 设a,b是同一个等价类中的两个元素, 则可以证明在G中恰好存在$\eta(a)$ 个将a映射到b的置换. 为此, 我们设

$$X_a=\{g_x \mid g_x(a)=a且g_x\in G\}$$

由于X_a的元素就是G中的所有将a映射到a的置换, 因此$|X_a|=\eta(a)$. 因为a,b在同一个等价类中, 于是存在一个置换$g\in G$, 使得$g(a)=b$. 构造集合

7.4 群

$$X = \{gg_x \mid g_x \in X_a\}$$

那么X中的每个置换都将a映射为b，并且若$g_{x_1}, g_{x_2} \in X_a$，$g_{x_1} \neq g_{x_2}$，显然有$gg_{x_1} \neq gg_{x_2}$，所以X中的每个元素都不相同，故有$|X| = |X_a| = \eta(a)$. 进一步可以证明，除了X中的置换外，G中不可能再有别的将a映射到b的置换了. 否则，设$\sigma \in G, \sigma \notin X, \sigma(a) = b$. 因为$g(a) = b$，所以

$$g^{-1}(b) = g^{-1}(\sigma(a)) = g^{-1}\sigma(a) = a$$

back

7.4 群

这样, $g^{-1}\sigma \in X_a$, 从而$g(g^{-1}\sigma) = \sigma \in X$, 这是一个矛盾. 因此在$G$中恰好有$\eta(a)$个置换将$a$映射到$b$.

最后, 设$a, b, c, \cdots, h$是A中属于同一个等价类的元素. 于是, G的任何一个置换只能将a映射到其所属等价类中的某一个元素. 于是G的所有置换分成以下各类: 将a 映射成a的类, 将a映射成b的类, 将a映射成c的类, $\cdots$, 将a 映射成h 的类. 所以, 我们有

$$\eta(a) = \frac{|G|}{\text{包含}a\text{的等价类中的元素个数}}$$

同理可知

$$\eta(b) = \eta(c) = \cdots = \eta(h) = \frac{|G|}{\text{包含}a\text{的等价类中的元素个数}}$$

back

7.4 群

因此, 对于A的任何一个等价类, 我们有

$$\sum_{a\in\text{该等价类}} \eta(a) = |G|$$

由此可知

$$\sum_{a\in A} \eta(a) = \text{划分}A\text{所得的等价类的数目} \times |G|$$

因此, 划分A所得的等价类的数目是

$$\frac{1}{|G|}\sum_{a\in A}\eta(a) = \frac{1}{|G|}\sum_{g\in G}\psi(g)$$

back

7.4 群

下面, 我们通过一个例子来验证一下定理.
集合$A = \{1,2,3\}$上的3次对称群S_3有6个元. 这6个元分别是

$$g_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, g_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, g_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$g_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, g_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, g_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

back

7.4 群

取$G_1 = \{g_1, g_2\}$, $G_2 = \{g_1, g_5, g_6\}$是S_3的两个子群, 因而是A 上的两个置换群. 由G_1所诱导的等价关系将集合$A = \{1, 2, 3\}$进行了划分, 方式为$A = A_1 + A_2$, 这里$A_1 = \{1\}$, $A_2 = \{2, 3\}$, 等价类的数目是2, 和

$$\frac{1}{|G|}\sum_{g\in G_1}\psi(g) = \frac{1}{2}(3+1) = 2$$

相吻合.

由G_2所诱导的等价关系将集合$A = \{1, 2, 3\}$进行了划分, 方式为$A = A$, 等价类的数目是1, 和

$$\frac{1}{|G|}\sum_{g\in G_1}\psi(g) = \frac{1}{3}(3+0+0) = 1$$

相吻合

7.4 群

引理 7.1

设G是一个有限群, H是G的子群, 对于G的元素$a \in G$, 定义G到G 的映射

$$\tau_a: \qquad \tau_a(x) = ax,\ x \in G$$

则

(1) τ_a是G的一个置换.

(2) $K = \{\tau_h \mid h \in H\}$关于置换的复合运算是$G$的一个置换群, 且$K$ 与H的元素个数相同.

证明: (1) 因为$a \in G$, G是群, 所以对于任意的$x \in G$, 都有$ax \in G$, 于是τ_a是一个G到G的映射. 下面只要证明τ_a是满射和单射就可以了. 因为对于任意的$y \in G$, 存在$a^{-1}y \in G$, 使得

$$\tau_a(a^{-1}y) = a(a^{-1}y) = y$$

back

7.4 群

和当$x_1, x_2 \in G$, $x_1 \neq x_2$时

$$\tau_a(x_1) = ax_1 \neq ax_2 = \tau_a(x_2)$$

于是τ_a是G的满射和单射, 这样τ_a是G的一个置换.
(2) 因为H是一个群, 对于H中的单位元$e \in H$, 由定义$\tau_e \in K$, 所以K 是一个非空集合. 设$\tau_a, \tau_b \in K$, 因为$a, b \in H$, 且$\tau_a\tau_b = \tau_{ab}$, 于是$\tau_a\tau_b \in K$, 这表明K关于变换的复合运算是封闭的. 不难知道τ_e是K的单位元, K的元素τ_a的逆元素是$\tau_{a^{-1}}$, 这样K是G的一个置换群. 最后, 因为H中的元素h和K中的元素τ_h之间的对应关系是一个一一对应关系, 便知道H和K的元素个数相同.
今后我们称K是由H导出的G的置换群.

back

7.4 群

利用群的一个子集来推测整个群的性质, 这种方法是比较常见和有效的.
从群G里取出一个子集H, 利用G的乘法可以把H的两个元相乘. 对于这个乘法来说H很可能也作成一个群.
整数加群Z可以看做实数加群的一个子群, 有理数群Q可以看成整数加群的一个子群, 也可以看成实数加群的一个子群.

定义 7.31

一个群G的一个子集非空子集H叫做G的一个子群, 假如H对于G的乘法来说作成一个群.

back

7.4 群

任意群G至少有两个子群, 它们是单位元组成的一个元素的群和G自身. 这两个子群一般称为群的平凡子群.
给定群的一个非空子集, 如何验证该子集是一个子群, 下面给出一个充要条件.

定理 7.23

一个群G的一个不空子集H作成G的一个子群的充分而且必要条件是:
(i) $a, b \in H \Rightarrow ab \in H$
(ii) $a \in H \Rightarrow a^{-1} \in H$

back

7.4 群

证明: 充分性. 即(i), (ii)成立$\Longrightarrow H$作成一个群.
下面验证群定义的三个条件满足.
(1) 由于(i), H是代数系统, 结合律在G中成立在H中自然成立.
(2) 因为H至少有一个元a, 由(ii), H也有元a^{-1}, 所以由(i)可知

$$a^{-1}a = e \in H$$

(3) 由(ii)对于H的任意元a来说H 有元a^{-1}使得

$$a^{-1}a = e$$

back

7.4 群

必要性. 即H作成一个群$\Longrightarrow$ (i), (ii)成立.
H是一个子群是封闭的, (i)显然成立. H 既然是一个群, H一定有一个单位元e'. 在子群H 内有 $e'e' = e'$, 在G内$e'e' = e'$自然也成立. 设e是G的单位元, 在G内有$ee' = e'$, 因此

$$e'e' = ee'$$

记e'在G内的逆元素时$(e')^{-1}$, 那么

$$e' = e'(e'(e')^{-1}) = (e'e')(e')^{-1} = (ee')(e')^{-1} = e(e'(e')^{-1}) = e$$

back

7.4 群

对于任意的$a \in H$, 令a'是a在H中的逆元素, 那么$a'a = e$, 此等式在G内也当然成立, 这表明a'是a在G中的逆元素, 故$a^{-1} = a' \in H$, 证完.

推论 7.2

假定H是群G的一个子群. 那么H的单位元就是G的单位元, H的任意元a在H里的逆元就是a在G里的逆元.

back

7.4 群

定理7.23中的(i), (ii)两个条件也可以用一个条件来代替.

定理 7.24

一个群G的一个不空子集H作成G的一个子群的充分而且必要条件是:

$$a, b \in H \Rightarrow ab^{-1} \in H$$

证明: 充分性. $a, b \in H \Rightarrow ab^{-1} \in H \Longrightarrow H$ 作成G 的子群.
事实上, 不空子集H内有元素a, 因此$e = aa^{-1} \in H$, 可知H内有单位元. 任取$a \in H$, 可知$ea^{-1} = a^{-1}$可知H中的每个元素有逆元素. 再设$a, b \in H$, 那么 $ab = a(b^{-1})^{-1} \in H$, 故$H$是封闭的. $H \subseteq G$, 元素当然是可结合的.
必要性显然成立.

back

7.4 群

当判断群的一个有限子集是否为子群的时候, 还有更简单的判别方法.

定理 7.25

一个群G的不空有限子集H作成G的一个子群的充分而且必要条件是:

$$a, b \in H \Rightarrow ab \in H$$

证明: 充分性. 设$G = \{a_1, a_2, \cdots, a_n\}$, 要证$G$是群, 我们将验证$G$ 满足群定义的三个条件. 条件(1) 即封闭性, 由已知条件直接可以得到.

(2) 存在左单位元. 用a_1从右边乘以G 的每一个元素, 得到集合$G' = \{a_1a_1, a_2a_1, \cdots, a_na_1\}$, 由消去律可知, G'中的元素两两不同, 由于$G' \subseteq G$, 因此$G = G'$, 所以存在a_k使得

7.4 群

$$a_k a_1 = a_1$$

下面证明a_k就是G的左单位元. 事实上用a_1从左边乘以G的每一个元素, 得到集合$G'' = \{a_1a_1, a_1a_2, \cdots, a_1a_n\}$, 由消去律可知, $G'' = G$. 于是对G 的任何元素a_i, 存在a_i'使得$a_1a_i' = a_i$, 那么

$$a_k a_i = a_k(a_1a_i') = (a_ka_1)a_i' = a_1a_i' = a_i$$

这表明, a_k是G的左单位元.

(3) 每个元素存在左逆元. 对于G的任何元素a_i, 用a_i从右边乘以G, 所得到的n 个元素一定有a_k, 设$a_ja_i = a_k$, 那么a_j便是a_i(关于a_k)的左逆元.

综上所述, G 是一个群.

back

7.4 群

下面给出几个例子.

例 7.50

设Z_{12}是模12的剩余类加群, 判断Z_{12}的子集H和S是否为子群.
(1) $H = \{[0], [4], [8]\}$
(2) $H = \{[1], [5], [9]\}$

解: H是Z_{12}的子群. 因为H是有限子集, 我们只要验证H中的两个元素$[a]$, $[b]$ 相加封闭即可. 又因为, 运算适合交换律, 所以两个元素相加的九中情况, 只要验证六种情况即可. 事实上$[0]+[0]=[0]\in H$, $[0]+[4]=[4]\in H$, $[0]+[8]=[8]\in H$, $[4]+[4]=[8]\in H$,$[4]+[8]=[0]\in H$, $[8]+[8]=[4]\in H$.

back

7.4 群

例 7.51

群G的两个子群H与K的交集$H \cap K$也是G的一个子群.

证明: 设G的单位元为e, 因为$e \in H$, $e \in K$, 可知$e \in K \cap K$, 从而$H \cap K \neq \emptyset$. 对于任意的$a, b \in H \cap K$, 因为H和K 都是子群, 所以$ab^{-1} \in H$ 和 $ab^{-1} \in K$, 从而$ab^{-1} \in H \cap K$, 这就证明了$H \cap K$ 是子群.

back

7.4 群

例 7.52

举例说明，一个群G的两个子群H与K的并集$H \cup K$可能不是G的一个子群.

解：对于模12的剩余类加群Z_{12}，不难验证$H = \{[0], [4], [8]\}$，$K = \{[0], [6]\}$是Z_{12}的两个子群，但是$H \cup K = \{[0], [4], [6], [8]\}$不是$Z_{12}$的子群，这是因为$[4] + [6] = [10] \notin H \cup K$.

back

7.4 群

一个循环群的子群还是循环群吗, 下面的定理给与了说明.

定理 7.26

循环的子群是循环群.

证明: 设$G = (a)$是循环群, e是G的单位元. H是G的子群. 若$H = \{e\}$, 那么$H = (e)$ 是循环群. 若$H \neq \{e\}$, 可知存在$c \in H, c \neq e$, 故存在非零整数n, 使得$c = a^n$, 于是$c^{-1} = a^{-n} \in H$, 这样

back

7.4 群

$$M = \{n | n是正整数, a^n \in H\}$$

是一个非空的集合. 令r是M中的最小正整数, 可以断言, 子群$H = (a^r)$. 事实上, 对于任意的$a^m \in H$, 设$m = rq + t$, 这里$0 \leq t \leq r - 1$. 则$a^t = a^{m-rq} = a^m(a^r)^{-q} \in H$, 由$r$的最小性, 可知$t = 0$, 于是$m = rq$, 这样$a^m = (a^r)^q$, 所以$H = (a^r)$. 证完.

back

7.4 群

例 7.53

设G是无限循环群群.
(1) H是G的子群, 若H不是单位元群, 那么H也是无限循环群.
(2) G的子群的个数是无限的.

证明: (1) 设H是$G = (a)$的不是单位元的子群, 根据定理7.26 可知, $H = (a^r)$, 这里r是一个不为零的整数. 若$\circ(a^r)$是一个有限数k, 那么$(a^r)^k = e$, 可知$a^{|kr|} = e$, 从而$\circ(a) \leq |kr|$, 这与$\circ(a) = \infty$ 相矛盾. 这样, $\circ(a^r) = \infty$, $H = (a^r)$是一个无限群.

back

7.4 群

(2) 为了证明G有无限个子群, 先看一看G的两个循环子群(a^t)和(a^s) 相等的必要条件, 这里t和s都不是零. 也就是说(a^t)和(a^s) 都不是单位元子群. 设$(a^t) = (a^s)$, 可知$a^t \in (a^s)$和$a^s \in (a^t)$, 于是存在整数k, m使得$a^s = (a^t)^k$, $a^t = (a^s)^m$, 这样

$$a^t = (a^s)^m = ((a^t)^k)^m = a^{tkm}$$

back

7.4 群

所以有$a^{t(1-km)} = e$, 由于$\circ(a) = \infty$, 必有$t(1-km) = 0$, 从而$1-km = 0$, 必有$k = 1, m = 1$或者$k = -1, m = -1$. 当$k = 1, m = 1$, $a^s = a^t$, 当$k = -1, m = -1$是$a^s = (a^t) - 1$. 这样, 我们得出G的两个循环子群(a^t)和(a^s)相等的必要条件是两个元素元素a^s, a^t 或者相等, 或者互为逆元. G 的元素序列$a, a^2, a^3, \cdots$任意两个元素既不相等, 也不互为逆元, 所以$(a), (a^2), (a^3), \cdots$是$G$的两两不相等的子群, 从而$G$有无限多个子群.

7.4 群

例 7.54

G是一个n阶循环群.
(1) 若H是G的m阶子群, 则$m|n$.
(2) 对于正整数m, 若$m|n$, 则G 有且只有一个阶是m 的子群, 从而G 的子群个数是n 的正因子个数.

证明: (1) 设$G = \{a^0, a, a^2, \cdots, a^{n-1}\}$, 因为循环群的子群还是循环群, 可设$H = (a^r)$, $0 \leq r \leq n-1$, H的阶m就是元素a^r的阶数$\circ(a^r)$, 而$\circ(a^r) = \frac{n}{(m,n)}$, 由此便知$m|n$. (1) 得证.

back

7.4 群

(2) 因为G的元素$a^{\frac{n}{m}}$的阶数就是m, 所以$(a^{\frac{n}{m}})$就是一个阶数为m的子群, 存在性得证. 设(a^k)是G 的任意一个阶数为m子群, 因为$\circ(a^k) = m$, 可知$(a^k)^m = e$, 即$a^{km} = e$, 从而$n|km$, 于是$\frac{n}{m}|k$, 于是$(a^k) \subseteq (a^{\frac{n}{m}})$, 因为$|(a^k)| = |(a^{\frac{n}{m}})| = m$, 因此$(a^k) = (a^{\frac{n}{m}})$, 证完.

例题7.54告诉我们, 要找出一个阶数是n的有限阶循环群$G = (a)$ 的所有子群, 只要找出n的每一个正因子m, 那么列出所有的$(a^{\frac{n}{m}})$, 也就找出了所有的子群.

back

7.4 群

例 7.55

模12的剩余类加群

$$Z_{12} = \{[0], [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11]\}$$

找出Z_{12}的所有子群.

解: Z_{12}是一个生成元为$[1]$的循环群. 12的所有正因数为1, 2, 3, 4, 6, 12, 所以Z_{12}存在阶数分别为$1, 2, 3, 4, 6, 12$的子群, 它们分别是由元素$[1]^{\frac{12}{1}}$, $[1]^{\frac{12}{2}}$, $[1]^{\frac{12}{3}}$, $[1]^{\frac{12}{4}}$, $[1]^{\frac{12}{6}}$,$[1]^{\frac{12}{12}}$ 生成的, 即它们分别是$[0], [6], [4], [3], [2], [1]$生成的, 这些子群分别是:

back

7.4 群

1阶级子群: $([0]) = \{[0]\}$
2阶级子群: $([6) = \{[0], [6]\}$
3阶级子群: $([4]) = \{[0], [4], [8]\}$
4阶级子群: $([3]) = \{[0], [3], [6], [9]\}$
6阶级子群: $([2]) = \{[0], [2], [4], [6], [8], [10]\}$
12阶级子群:
$([1]) = \{[0], [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11]\}$

7.4 群

本节内容主要利用群G的一个子群H来定义G上的一个等价关系, 此等价关系可以把G分类进行分类, 然后由这个分类推出几个重要的定理.

给定群G和G的一个子群H. 下面规定一个G的元中间的关系$\sim$:

$$a \sim b, \text{当而且只当} ab^{-1} \in H \text{的时候}$$

给了a和b, ab^{-1}或者属于H, 或者不属于H两种情况之一. 所以$\sim$ 是一个关系, 同时

back

7.4 群

(1) $aa^{-1} = e \in H$, 所以 $a \sim a$, 关系$\sim$ 是自反的.
(2) $ab^{-1} \in H \Rightarrow (ab^{-1})^{-1} = ba^{-1} \in H$, 所以 $a \sim b \Rightarrow b \sim a$, 关系$\sim$ 是对称的.
(3) $ab^{-1} \in H, bc^{-1} \in H \Rightarrow (ab^{-1})(bc^{-1}) = ac^{-1} \in H$, 所以$a \sim b, b \sim c \Rightarrow a \sim c$, 关系$\sim$ 是传递的.
这样$\sim$是G上的一个等价关系. 利用这个等价关系我们可以得到一个G 的分类. 对于任意的$a \in G$, 设a所在的类为$[a]_H$, 为了简单起见, 简记为$[a]$. 即

7.4 群

$$[a] = \{b | a \sim b, \text{或者} ab^{-1} \in H\}$$

下面, 考察G的元素a所在类$[a]$中都是一些什么样的元素.
任取$b \in [a]$, 即$a \sim b$, 由定义可知, $ab^{-1} \in H$, 故存在$h \in H$, 使得$ab^{-1} = h$, 也就是$b = h^{-1}a$, 因为H是群, 所以$h^{-1} \in H$, 这就说明与a 有关系的元b 可以写成子群H 的一个元素与a 的乘积.
反过来, 对于子群H中的任何一个元h与a的乘积ha来说, 令$b = ha$, 那么$ab^{-1} = a(ha)^{-1} = a(a^{-1}h^{-1}) = h^{-1} \in H$, 这说明$H$中的每一个元与$a$ 的乘积都与a有关系.

7.4 群

这样一个事实告诉我们,

$$[a] = \{ha \mid h \in H\}$$

也就是说, a所在的类恰好是用a从右边去乘H 的每一个元后形成的集合.
对于这样得来的G的一个元素a所在的类给出一个特殊的名字.

定义 7.32

由上面的等价关系$\sim$所决定的类叫做子群H的**右陪集**. 包含元a 的右陪集用符号Ha 来表示.

back

7.4 群

例 7.56

设G为模12的剩余类加群, $H=\{[0],[4],[8]\}$ 是G的一个子群, 求出H 将G 分成的所有右陪集.

解: 按照右陪集的定义, 有

$$H+[0]=H+[4]=H+[8]=\{[0],[4],[8]\}$$
$$H+[1]=H+[5]=H+[9]=\{[1],[5],[9]\}$$
$$H+[2]=H+[6]=H+[10]=\{[2],[6],[10]\}$$
$$H+[3]=H+[7]=H+[11]=\{[3],[7],[11]\}$$

是H将G分成的4个不同的右陪集.

7.4 群

右陪集是从等价关系$\sim$:

$$a \sim b, \text{当而且只当} ab^{-1} \in H \text{的时侯}$$

出发而得到的. 假如我们规定一个关系$\sim'$:

$$a \sim' b, \text{当而且只当} b^{-1}a \in H \text{的时侯}$$

那么同以上一样可以看出$\sim'$也是一个等价关系. 利用这个等价关系我们可以得到G的另一个分类.

定义 7.33

由等价关系$\sim'$所决定的类叫作子群H的**左陪集**. 包含元a的左陪集我们用符号aH来表示.

back

7.4 群

同以上一样我们可以证明：aH刚好包含所有可以写成

$$ah \quad (h \in H)$$

形式的G的元.
因为一个群的乘法不一定适合交换律, 所以一般来说$\sim$和$\sim'$两个等价关系所决定的元素a所在的类Ha和aH并不相同. 但是我们有

定理 7.27

一个子群H的右陪集的个数和左陪集的个数相等：它们或者都是无限大或者都有限并且相等.

证明：我们把H的右陪集所作成的集合叫做S_r, H的左陪集所作成的集合叫做S_l. 定义S_r与S_l的元素之间的对应关系

back

7.4 群

$$\phi: \quad Ha \to a^{-1}H$$

我们说, 这种定义的陪集之间的对应关系与陪集的代表元无关. 也就是说, 若$Ha = Hb$, 则$a^{-1}H = b^{-1}H$. 事实上,

$$Ha = Hb \Rightarrow ab^{-1} \in H \Rightarrow (ab^{-1})^{-1} = ba^{-1} \in H \Rightarrow a^{-1}H = b^{-1}H.$$

back

7.4 群

所以, 右陪集Ha的象与a的选择无关, ϕ是一个S_r到S_l的映射. 进一步可以断言, ϕ是一个S_r与S_l间的一一映射. 因为 S_l的任意元aH是S_r的元Ha^{-1}的象, 所以ϕ首先是一个满射; 再有

$$Ha \neq Hb \Rightarrow ab^{-1} \in H \Rightarrow (ab^{-1})^{-1} = ba^{-1} \in H \Rightarrow a^{-1}H \neq b^{-1}H$$

所以, ϕ又是一个S_r与S_l间的单射. 我们也就证明了ϕ是一一映射.

back

7.4 群

定义 7.34

一个群G的一个子群H的右陪集(或左陪集)的个数(相同的算作一个)叫做H 在G 里的**指数**, 记作$[G:H]$.

例 7.57

模12的剩余类加群G关于子群$H=\{[0],[4],[8]\}$ 的指数是$[G:H]=4$.

back

7.4 群

例 7.58

设G是非零有理数的集合, 不难验证, G对于有理数的乘法作成一个群, $H=\{1,-1\}$ 是G的一个子群. 对于任何的非零有理数a, a所在的等价类$Ha=\{a,-a\}$, 这样

$$G=\bigcup_{a\in Q^+} aH$$

其中, Q^+是全体正有理数组成的集合. G关于H的指数$[G:H]$ 为无穷大.

back

7.4 群

本书主要讨论$[G:H]$是有限的情形.
下面的引理说明了一个子群与该子群的每个陪集的基数是相同的.

引理 7.2

一个子群H与H的每一个右陪集Ha之间都存在一个一一映射.

证明: 在H与H的每一个右陪集Ha之间定义映射

$$\phi: \quad h \to ha$$

那么, ϕ是H与Ha 间的一一映射. 因为:

back

7.4 群

(1) H的每一个元h有一个唯一的象ha;
(2) Ha的每一个元ha是H的h 的象;
(3) 假如$h_1 \neq h_2$, 那么$h_1a \neq h_2a$, 证完.
由这个引理, 我们可以得到下面两个非常重要的结论, 定理7.28和定理7.30.

定理 7.28

假定H是一个有限群G的一个子群. 那么H的阶n和它在G里的指数j都能整除G 的阶N, 并且

$$N = nj$$

back

7.4 群

证明: G的阶N既是有限, H的阶n和指数j也都是有限正整数. G的N 个元被分成j个右陪集, 而且由引理每一个右陪集都有n个元所以

$$N = nj$$

证完.

定理 7.29

设G是一个有限群, H是G的一个子群, K是由H导出的G的置换群. 那么G 的 子群H的右陪集的个数就是由置换群K所诱导的G上的等价关系把集合G划分是所有等价类的数目.

证明: 我们看K所诱导的G上的等价关系$\sim$:

$$\sim: \quad a, b \in G, a \sim b \Leftrightarrow \text{存在}\pi_h \in K, \text{使得}\pi(a) = b$$

7.4 群

因为$\pi_h(a) = ha = b$, 那么$h = ba^{-1}$, 这样

$$a \sim b \Leftrightarrow \pi_h(a) = b \Leftrightarrow ha = b \Leftrightarrow b \in Ha$$

那么由置换群K所诱导的G上的等价关系对G的分类中的每一类恰好是子群H的一个右陪集. 而置换群K所诱导的G上的等价关系把集合G划分时, 所有等价类的数目是

$$\frac{1}{|K|}\sum_{\pi_h \in K}\psi(\pi_h) = \frac{1}{|K|}\psi(\pi_e) = \frac{1}{|K|}|G| = \frac{1}{|H|}|G|$$

所以G的子群H的右陪集个数 是$\frac{|G|}{|H|}$, 这和以前得到的结果相同.

back

7.4 群

定理 7.30

一个有限群G的任一个元a的阶n都整除G的阶.

证明: a生成一个阶是n的子群, 根据定理7.28可知, n整除G的阶. 证完.

定义 7.35

设H是群G的一个子群, 如果对任意的$a \in G$都有

$$aH = Ha$$

则称H是G的一个正规子群.

back

7.4 群

任何一个群G有两个显然的正规子群, 这就是由单位元组成的一个元素的群和G 本身.
设G是可换群, 则G的任意子群都是正规子群, 因

$$aH = \{ah \mid h \in H\} = \{ha \mid h \in H\} = Ha$$

如, $(Q - \{0\}, \times)$非零有理数关于数目乘法组成的群, 取$H = \{1, -1\}$, 则$(H, \times)$
是$(Q-\{0\}, \times)$的正规子群.

7.4 群

定理 7.31

设H是群G的一个正规子群, G/H表示H的所有陪集作成的集合, 设$aH, bH \in G/H$, 定义

$$(aH)(bH) = (ab)H$$

则G/H关于上面规定的陪的集乘法运算组成一个群.

证明: 我们首先证明两个陪集$aH, bH \in G/H$的乘积与代表元无关, 即所规定的陪集运算法则是G/H的一个运算. 设$aH, bH \in G/H$, 若$aH = xH, bH = yH$, 那么存在$n_1, n_2 \in H$, 使得$a = xn_1$且$b = yn_2$,

7.4 群

这时

$$ab = xn_1yn_2 = x(n_1y)n_2$$

由于H是正规子群,

$$n_1y \in Hy = yH$$

所以存在$n_3 \in H$, 使得$n_1y = yn_3$, 这样,

$$ab = x(n_1y)n_2 = xy(n_3n_2) \in (xy)H$$

故有

$$(ab)H = (xy)H$$

G/H关于运算是封闭的.

7.4 群

下面验证G/H满足群定义的三个条件.
(1) 对于任意的$a,b,c \in G$,

$$[(aH)(bH)]cH = (ab)HcH = [(ab)c]H = (abc)H$$

$$aH[(bH)(cH)] = aH(bc)H = [a(bc)]H = (abc)H$$

所以有$(aHbH)cH = aH(bHcH)$, 故运算是可结合的.
(2) $aHeH = (ae)H = aH$, 故eH是G/H的单位元素.
(3) aH的逆元素为$a^{-1}H$.

7.4 群

定义 7.36

群G关于其正规子群H的陪集作成的群G/H叫做G关于H的商群.

判断正规子群, 除定义外还有如下的方法.

定理 7.32

设H是G的子群, 则下面四个条件是等价的:
(1) H是G的正规子群;
(2) $aHa^{-1} = H, a \in H$;
(3) $aHa^{-1} \subseteq H, a \in G$;
(4) $aha^{-1} \in H, a \in G, h \in H$

back

7.4 群

证明: 按下面途径$(1) \Rightarrow (2) \Rightarrow (3) \Rightarrow (4) \Rightarrow (1)$从而四个条件等价.

(1) $\Rightarrow$(2). 因H是正规子群, 故对任意的$a \in G$, 有$aH = Ha$,于是$aHa^{-1} = (aH)a^{-1} = (Ha)a^{-1} = H(aa^{-1}) = He = H$, 即(2)成立.

(2) $\Rightarrow$(3). 对任意的$a \in G, aHa^{-1} = H$, 故$aHa^{-1} \subseteq H$.

back

7.4 群

(3) $\Rightarrow$(4). 由于$aHa^{-1} \subseteq H$, 故对任意的$a \in G, h \in H$, 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$ha = ah_2$, 也即$ah \in aH, Ha \subseteq aH$所以, 对任意$a \in G$, 有

$$aH = Ha$$

从而H是群G的正规子群, 证毕.

7.4 群

例 7.59

设H是群G的一个子群, 且H的任意两个左陪集的乘积仍是一个左陪集, 则H 是G的一个正规子群.

证明: 先证$aHbH = (ab)H$. 由已知, $aHbH$是一个左陪集, 设为cH, 但$ab = aebe \in aHbH$, 故$ab \in cH$, 即 $cH = (ab)H$.
任取$h \in H$, 则$aha^{-1}b \in aHa^{-1}H = (aa^{-1})H = H$, 于是$aha^{-1} \in H$, 对任意的$a \in G$, 即$H$是群$G$的正规子群.

7.5 群在密码学中的应用

本节主要介绍群理论在公钥密码学中的典型应用RSA算法.
对任意的大于1的正整数n, 作集合

$$Z_n = \{0, 1, 2, \cdots, n-1\}$$

定义集合Z_n上的二元运算$\oplus$: 任意的$i, j \in Z_n$,

$$i \oplus j = (i + j) \bmod n$$

back

7.5 群在密码学中的应用

这里$(i+j)(\mathrm{mod}\ n)$是整数$i+j$除以n的余数. $\oplus$显然是一个Z_n上的代数运算, 这个运算还满足交换律. 下面我们验证Z_n关于运算$\oplus$ 成为交换群.

首先, 因为对任意的$i \in Z_n$, 因为$0 \oplus i = i$, 所以0是Z_n的单位元.

其次, 对任意的$i \in Z_n$, 当$i \neq 0$ 时, i的逆元素是$n-i \in Z_n$, 当$i = 0$ 时, i的逆元素是其自身. 这样, Z_n的每个元素都有逆元素. 最后, 只要再验证运算$\oplus$ 满足结合律即可. 事实上, 对于Z_n中的任意三个元素$i, j, k \in Z_n$, 根据两个数a与b相加除以n的余数就是a与b分别除以n的余数相加再除以n 的余数这个原理, 有

7.5 群在密码学中的应用

$$\begin{aligned}(i \oplus j) \oplus k &= ((i+j) \bmod n + k) \bmod n \\ &= ((i+j) \bmod n + k \bmod n) \bmod n \\ &= (i+j+k) \bmod n\end{aligned}$$

相似地, 因为

$$\begin{aligned}i \oplus (j \oplus k) &= (i + (j+k) \bmod n) \bmod n \\ &= (i \bmod n + (j+k) \bmod n) \bmod n \\ &= (i+j+k) \bmod n\end{aligned}$$

所以运算$\oplus$满足结合律. 因此, Z_n是一个关于运算$\oplus$的群, 显然为交换群. 这个群Z_n叫做关于模n的加法群.

7.5 群在密码学中的应用

再来定义集合Z_n上的二元运算$\odot$: 任意的$i,j \in Z_n$,

$$i \odot j = (i \cdot j) \bmod n$$

这里$(i \cdot j) \bmod n$是整数$i \cdot j$除以n的余数. 这显然也是Z_n上的另外一个满足交换律的代数运算. 自然会问Z_n关于运算$\odot$成为交换群吗?

下面还是要看群的要求是否都满足. 首先不难验证1是Z_n关于运算$\odot$的单位元. 对于Z_n中的任意三个元素$i,j,k \in Z_n$, 根据两个数a与b的乘积除以n的余数就是a与b分别除以n的余数的乘积再除以n的余数这个原理, 有

7.5 群在密码学中的应用

$$\begin{aligned}(i \odot j) \odot k &= ((i \cdot j) \bmod n \cdot k) \bmod n \\ &= ((i \cdot j) \bmod n \cdot k \bmod) \bmod n \\ &= (i \cdot j \cdot k) \bmod n\end{aligned}$$

相似地, 因为

$$\begin{aligned}i \odot (j \odot k) &= (i \cdot (j \cdot k) \bmod n) \bmod n \\ &= (i \bmod n \cdot (j \cdot k) \bmod n) \bmod n \\ &= (i \cdot j \cdot k) \bmod n\end{aligned}$$

back

7.5 群在密码学中的应用

最后就剩下Z_n的每个元素关于$\odot$是否有逆元的问题了.
对于$0 \in Z_n$, 因为任何$j \in Z_n$, 有$0 \odot j = 0 \neq 1$. 这表明Z_n中找不到与元素0作运算等于单位元的元素, 这表明0没有逆元.
很遗憾, Z_n关于运算$\odot$ 不是群.

Z_n的某个子集关于运算$\odot$可能成为群吗?

对任意的$n > 1$,取Z_n子集$G_1 = \{0\}$和当$= 10$时, 取Z_n子集$G_2 = \{5\}$, 容易验证G_1和G_2都是关于运算$\odot$的Z_n的子群, 前者的单位元是0, 后者的单位元是5, 这两个子群的单位元都不是1.
我们还是关心Z_n是否存在包含1的关于运算$\odot$的子群. 这样的子群实际上也是存在的, 例如$G_3 = \{1\}$ 就是其中的一个, 顺便说一下0是不会出现在这种子群中的, 原因是0在这种子群中不可能含有逆元. 今后用符号Z_n^* 表示这种群中元素最多的一个.

7.5 群在密码学中的应用

下面的问题是: Z_n^*中都是一些什么样的元素?

若$a \in Z_n^*$, 因为Z_n^*中存在a的逆元, 所以存在$u \in Z_n^*$, 使得$a \odot u = 1$, 即$(au) \bmod n = 1$, 或者$n \mid (au - 1)$, 用d表示a和n 的最大公因子, 因为$d \mid a$和$d \mid n$, 推出$d \mid -1$, 这样必有$d = 1$, 这就是说, 若$a \in Z_n^*$, 那么Z_n^* 中的元素a 是一个与n互素的数, 这个数a当然是Z_n中的一个元素.

反过来, Z_n中任何一个与n互素的整数b也属于Z_n^*吗?

back

7.5 群在密码学中的应用

从Z_n中所有与n互素的元素中任取一个元素b, 根据"数论"中的一个知识: "两个整数x与y 的最大公因子为1(即两个数互素)当且仅当存在整数$u, v \in Z$, 使得$xu+yv=1$", 因为b与n互素, 所以存在整数u和v, 使得

$$bu+nv=1$$

于是$n \mid (1-bu)$, 我们说$n \nmid u$, 不然的话$n \mid (1-bu+bu)$, 即$n \mid 1$, 这和$n>1$不符. 设$u=nk+u_1$, 余数u_1满足$1 \leq u_1 \leq n-1$, 于是$u_1 \in Z_n$, 将$u=nk+u_1$带入等式$bu+nv=1$并整理可得

back

7.5 群在密码学中的应用

$$bu_1 + n(bk + v) = 1$$

这个表达式既表示u_1与n互素也表示u_1与b的乘积除以n的余数为1, 即$b \odot u_1 = 1$. 根据Z_n^*元素最多这一特点, 可知$b \in Z_n^*, u_1 \in Z_n^*$.
至此, 我们清楚了Z_n^*的结构: Z_n^*就是$1, 2, \cdots, n-1$中所有与n互素的元素构成的群.
下面把这个群Z_n^*叙述如下:

定理 7.33

对于正整数$n > 1$, 记所有小于n并且与互素的正整数作成的集合记为Z_n^*. 定义Z_n^*上的运算$\odot$: 若$i, j \in Z_n^*$, 令

$$i \odot j = (i \cdot j) \bmod n$$

则Z_n^*关于运算$\odot$作成一个群.

这就是现代计算机安全通信技术密码学领域用到的一个最重要的群.

7.5 群在密码学中的应用

对于正整数$n > 1$, 所有小于n并且与n互素的正整数的个数这样一个数, 数学家欧拉(Euler)最早给出了记号$\phi(n)$. 例如$\phi(2) = 1$, $\phi(8) = 4$等等. 按照这个符号的含义, 群Z_n^* 中的元素个数就是$\phi(n)$, 再根据群中的有关结论可知, 对任意$a \in Z_n^*$, 有

$$\overbrace{a \odot a \cdots \odot a}^{\phi(n)} = 1$$

这个等式的确切含义就是$a^{\phi(n)} \bmod n = 1$, 按照同余符号"$\equiv$" 的含义, 上式的等价表示就是

$$a^{\phi(n)} \equiv 1 \pmod{n} \tag{7.2}$$

back

7.5 群在密码学中的应用

可以验证公式(7.2)对于任何比n大且与之互素的整数a也成立并且公式(7.2)中的$n=1$时, 成立是显然的, 于是有下述结论

定理 7.34

设n为正整数, a是任何与n互素的整数, 则

$$a^{\phi(n)} \equiv 1 \pmod{n} \tag{7.3}$$

定理7.34就是著名的Euler定理, Euler定理在同余同余方程曾给出过, 这里我们从群的角度也给出了这一相同的结论.

back

7.5 群在密码学中的应用

公钥密码体制的提出时间和原理, 我们已经在第三章有所了解. 美国的三位科学家 Rivest, shamir 和 Adleman 在1978年正式发表了一个具体的公钥密码算法算法, 这个具有深远影响的算法后来用他们的名字RSA 命名, RSA的核心思想便是基于群Z_n^* 和数论中的大数分解原理.

RSA密码算法:

(1) 生成两个大素数p和q.

(2) $n \leftarrow pq$, $\phi(n) \leftarrow (p-1)(q-1)$.

(3) 作群$Z_{\phi(n)}^*$. 任意选一个随机数b, $1 < b < \phi(n)$, 使得$\gcd(b, \phi(n)) = 1$, 按照$Z_{\phi(n)}^*$定义, 可知$b \in Z_{\phi(n)}^*$.

(4) $a \leftarrow b^{-1}$, 这里b^{-1}是元素b在群$Z_{\phi(n)}^*$中的逆元.

(5) 公钥为(n, b), 私钥为(p, q, a).

7.5 群在密码学中的应用

设待加密的信息为x, 定义加密函数

$$y = E_b(x) = x^b \mod n$$

得到密文y, 定义解密函数

$$D_a(y) = y^a \mod n$$

下面的结论保证了RSA算法的正确性.

back

7.5 群在密码学中的应用

定理 7.35

设$n = pq$是两个不同素数之积. 如果E_b和D_a如上定义, 那么对任意$x \in Z_n$, 都有 $D_a(E_b(x)) = x$.

证明: 因为$y = x^b \mod n$, 可知存在整数k, 使得$x^b = nk + y$, 于是$(x^b)^a = (nk + y)^a$, 这表明$(x^b)^a$除以n的余数就是y^a除以n的余数. 要证明$x = y^a \mod n$, 只要证明$x = (x^b)^a \bmod n$即可. 换一个说法就是只要证明$(x^b)^a \equiv x (\mathrm{mod}\ n)$即可.
因为元素a与b在群$Z^*_{\phi(n)}$互为逆元. 于是$a \odot b = 1$, 即$ab \bmod \phi(n) = 1$或者$ab \equiv 1 (\mod \phi(n))$, 所以存在正整数$t$, 使得$ab = t\phi(n)+1$. 对任意明文$x \in Z_n$, 下面分情况讨论.

7.5 群在密码学中的应用

(1) $(x,n)=1$. 由欧拉定理有$x^{\phi(n)} \equiv 1 \pmod{n}$, 于是

$$(x^b)^a = x^{t\phi(n)+1} = (x^{\phi(n)})^t \cdot x \equiv x \pmod{n}$$

(2) $(x,n) \neq 1$. 因为n是素数p,q之积和$x < n$, 所以(x,n)等于p或q. 不妨设$(x,n)=p$, 则$(x,q)=1$. 由欧拉定理知$x^{q-1} \equiv 1 \pmod{q}$, 于是$x^{ab-1} = x^{t\phi(n)} = (x^{q-1})^{t(p-1)} \equiv 1 \pmod{q}$, 从而

back

7.5 群在密码学中的应用

$$x^{ab} \equiv x(\mathrm{mod}\ q)$$

因为$p|x$, 可得

$$x^{ab} \equiv x(\mathrm{mod}\ p)$$

因为$(p,q)=1$, 所以$x^{ab} \equiv x(\mathrm{mod}\ pq)$, 即

$$(x^b)^a \equiv x(\mathrm{mod}\ n)$$

综上所述, 对任意$x \in Z_n$, 都有$(x^b)^a \equiv x(\mathrm{mod}\ n)$, 证完.

back

7.5 群在密码学中的应用

下面是一个使用RSA密码体制加密解密示意性的一个例子. 设$p = 101, q = 113$, 则

$$n = pq = 101 \times 113 = 11413,$$
$$\phi(n) = (p-1)(q-1) = 100 \times 112 = 11200.$$

因为$\phi(n) = 2^6 \times 5^2 \times 7$, 所以1和11200之间任何不被2, 5 和7整除的数都可作为加密指数b. 信息的接收方选取$b = 3533$, 计算b 关于模11200的逆为$a = 6597$, 公开$n = 11413$和$b = 3533$.

back

7.5 群在密码学中的应用

信息的发送方得到b, 加密明文$x = 9726$, 得到密文

$$y = x^b \mod n = 9726^{3533} \mod 11413 = 5761$$

将密文$y = 5761$通过信道发出, 接收方收到$y = 5761$, 用a计算

$$y^a \mod n = 5761^{6597} \mod 11413 = 9726$$

还原出明文9726.
RSA算法也可以用于数字签名, 这里就不讨论了.

7.5 群在密码学中的应用

RSA密码体制的安全性是基于相信加密函数$E_b(x) = x^b \mod n$是一个单向函数, 所以对于攻击者来说, 试图解密密文是计算上不可行的. 允许第三方Bob 解密密文的陷门是分解$n = pq$的知识, 由于Bob知道这个分解, 所以他可以计算$\phi(n) = (p-1)(q-1)$, 然后用扩展的欧几里得算法计算解密指数a.

对RSA密码体制的一个明显的攻击就是密码分析者试图分解n.如果这点做到了, 那么便可以很简单地计算 $\phi(n) = (p-1)(q-1)$, 然后可以像Bob一样从b计算出解密指数a. 关于大整数的分解算法, 目前最有效的三种算法是二次筛法, 椭圆曲线分解算法和数域筛法, 其他作为先驱的著名算法包括J.Pollard的ρ方法和$p-1$算法, H.William的$p+1$算法, 连分式算法, 费马分解法及试除法等. 由于已经有大量文献研究或综述, 在此不花篇幅进行讨论. 若n被成功分解, 则RSA 密码便被破译. 尽管如此, 但还不能证明对RSA密码攻击的难度就和分解n相当, 只能说攻击RSA密码的困难程度不比分解大整数更难.

back

7.5 群在密码学中的应用

当然, 密码分析者可以考虑寻求不分解n而直接解密RSA密文的方法. 应该注意的是, 若从求$\phi(n)$入手对RSA密码进行攻击, 那么它的难度和分解n相当. 换言之, 计算$\phi(n)$并不比分解n简单. 事实上, 假设已知n和$\phi(n)$, n为两个素数p和q之积, 那么通过求解关于p和q的方程组

$$\begin{cases} n = pq, \\ \phi(n) = (p-1)(q-1) \end{cases}$$

可以容易地分解n.

7.5 群在密码学中的应用

密码分析者也可能既不分解n也不计算$\phi(n)$, 而直接基于解密指数a进行攻击. 可以证明, 如果解密指数a已知, 那么n可以通过一个随机算法在多项式时间内分解, 这表明直接计算解密指数a并不比分解n容易. 当然, 这也告诉我们, 如果a 被泄漏, 那么Bob重新选取一个加密指数是不够的, 他必须选择一个新的模数n. 另外, M.Wiener 提出了一种基于低解密指数的攻击方法, 当密钥满足$3a < n^{1/4}$ 和$q < p < 2q$时, 这种方法可以成功地计算出解密指数a. 有兴趣的读者可以参考相关的文献.

back

7.5 群在密码学中的应用

随着计算能力的日益增强和整数分解算法的不断改进, 为保证RSA密码的安全性, 在实际应用中选取的素数 p和q越来越大. 为避免选择容易分解的整数n, 1978年Rivest等人在正式发表的RSA公钥密码的论文 中就建议对素数p和q的选择应当满足以下三条:

(1) p和q要足够大, 在长度上应该相差不多, 且二者之差与p, q位数相近. 如果差值$p-q$太小 (不妨设$p>q$), 那么$(p+q)/2 \approx \sqrt{n}$, 并且$(p-q)/2$是个相当小的数. 因此等式

back

7.5 群在密码学中的应用

$$\left(\frac{p+q}{2}\right)^2 - n = \left(\frac{p-q}{2}\right)^2$$

的右端是一个相当小的平方数, 这样就可以利用费马分解法将n进行分解.

(2) $p-1$和$q-1$的最大公因数$d=(p-1,q-1)$应尽量小. 否则, 将有d^2个整数a, 使得n是基a的伪素数, 这就增加了对n进行分解的可能性.

(3) $p-1$和$q-1$都应该含有大的素因数, 否则就可能利用Pollard$p-1$算法求出n 的真因数. 关于此算法, 有兴趣的读者可以参考相关文献.

back