西安交通大学
XI'AN JIAOTONG UNIVERSITY

离散数学复习

软件73班 曹大华 QQ 940141567
软件73班 田丰瑞 QQ 747458467

2021.1.11

主要内容

一、集合论

二、关系

三、函数

四、代数系统

五、图论

西安交通大學
XI'AN JIAOTONG UNIVERSITY

集合论

集合论

掌握每个符号的基本定义

$a \in S, a \notin S, 2^A, A', A \cap B, A \cup B, A \backslash B, A \oplus B, A \otimes B$

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

$A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$

教材出现过的定理（最好）掌握其推导过程

（教材p89定理3.7）进一步思考，集合吸收率（$A = A \cup (A \cap B)$）能否由此证明？

集合宏运算的运算法则

（教材p90定理3.8中6、7）

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

这个式子将∩换成∪还成立吗？

（教材p91定理3.9中10）

如果$A \oplus B = A \oplus C$，那么$B = C$

环和(对称差)有消去律

集合论的一些定理和运算法则等

教材p89定理3.6 集合的De Morgan定律

教材p89定理3.7 设A,B为两个集合，那么下面三种说法是等价的。

$$A \subseteq B \Leftrightarrow A \cup B = B \Leftrightarrow A \cap B = A$$

$$A \setminus B = \{x \mid x \in A \wedge x \notin B\}$$

$$(6) A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$$

$$(7) A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$$

教材p91集合的环和运算，p92集合的环积运算，p93页集合的大并与大交

教材p91定理3.9（10） 如果$A \oplus B = A \oplus C$，那么$B = C$

教材p97习题3（3）$\emptyset \subseteq \{\emptyset\}$易错

例p98 11（3）充分条件证明（另一种思路）

下证 $A \cap B = A \cup B \Rightarrow A = B$

$$A \cap B = A \cup B \Rightarrow \boxed{(A \cap B) \cup B' = (A \cup B) \cup B'}$$

$$\Leftrightarrow (A \cup B') \cap (B \cup B') = A \cup (B \cap B')$$

$$\Leftrightarrow (A \cup B') \cap X = A \cup X$$

$$\Leftrightarrow A \cup B' = X$$

同理可证 $A \cap B = A \cup B \Rightarrow (A \cap B) \cup A' = (A \cup B) \cup A'$

$$\Leftrightarrow B \cup A' = X$$

那么，$B = B \cap X$

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

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

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

$$= A \cap B$$

同理可证

$$A = A \cap X = A \cap (B \cup A') = A \cap B$$

因此 $A = A \cap B = B$

西安交通大學
XI'AN JIAOTONG UNIVERSITY

关系

关系

关系基本概念

集合的叉积的子集

空关系，全关系，幺关系，前域，后域，关系的图形和矩阵表示法，逆关系，

复合运算，复合幂，闭包

二元关系基本性质

自反，反自反；对称，反对称；传递；

等价，等价类，商集，秩，划分，相容关系；

半序关系，Hasse图；最大元，最小元；极大元，极小元；上界，下界；上方有界，下方有界；有界集合，无界集合；上确界，下确界；（判断）

全序关系，良序关系，直接后继

注意教材上的定理和例题！

一些定义：自反关系与反自反关系

教材p120定义4.14 **自反关系**：设R是非空集合X上的二元关系。若对**每个**$x \in X$，**都有**$(x,x) \in R$，则称R是X上的自反关系；

教材p121定义4.15 **反自反关系**：设R是非空集合X上的二元关系。若对**每个**$x \in X$，**都有**$(x,x) \notin R$，则称R是X上的反自反关系；

- 有没有一种关系可以即不是自反关系，也不是反自反关系？ 但含有

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

不是么. 相同对

教材p121例4.26，例4.28 在实数范围上，等于关系是自反关系；小于关系是反自反关系，那小于等于关系呢？（教材p128例4.50）

关系

一些定义：对称关系、反对称关系与传递关系

教材p121定义4.16 对称关系：$(\forall x, y \in X)((x,y) \in R \Rightarrow (y,x) \in R)$

仅有

教材p121定义4.17 反对称关系：$(\forall x, y \in X)((x,y) \in R \wedge (y,x) \in R \Rightarrow x = y)$

$(\forall x, y \in X)((x,y) \in R \wedge x \neq y \Rightarrow (y,x) \notin R)$

不等不出现

教材p122定义4.18 传递关系：$(\forall x, y, z \in X)((x,y) \in R \wedge (y,z) \in R \Rightarrow (x,z) \in R)$

如果一个关系是自反的和对称的，那么他是否是传递关系？

如果一个关系是对称的和传递的，那么他是否是自反关系？（教材p134习题21）

有没有一种关系既是对称关系又是反对称关系？（教材p122例4.38）

- 全关系是自反的，对称的，传递的；
- 幺关系是自反的，对称的，反对称的，传递的；
- 空关系是反自反的，对称的，反对称的，传递的

关系

一些概念和性质：关于等价关系，划分，半序关系等

教材p126定理4.15　$R_{\Pi_R} = R$

教材p126定理4.16　$\Pi_{R_\Pi} = \Pi$

关于划分一点个人经验：划分一般用于具体的关系，而若想证明某个关系是等价关系一般只能从自反、对称和传递关系上证明，想证明这个关系构成了一种划分比较困难。（例如教材p134习题23（1）个人曾设想证明其构成划分，但最终失败）

- 整除关系，实数间小于等于关系，子集关系都是一种半序关系；
- 半序关系的逆关系仍是一种半序关系；（教材p128）

教材p128定理4.27 半序集若存在最大（小）元则**最大（小）元唯一**；

- 在一个非空的有限半序集上，必有极大元和极小元，但极大元和极小元的个数不确定。在无穷半序集中，极大元或极小元不一定存在。当极大元或极小元存在且唯一时，此时的极大元或极小元就成为最大元或最小元。（教材p129定义4.28后面一段话）

关系

一些概念和性质：关于等价关系，划分，半序关系等

- 对于一个半序集 A 的子集而言，在原来半序关系的作用下，仍为一半序集。但对 A 的子集而言未必由上（下）界存在。其次，即使有上（下）界存在，上（下）界也未必唯一。子集B的上（下）界可以是B中的元素，也可以不在B中而在A中；当子集B有上界时，称B上方有界；当子集B有下界时，称B下方有界；当B有上界和下界时，称B是有界集合；否则称B是无界集合。（教材p129定义4.29后面一段话）

- 只有在B有上（下）界的前提下才能讨论B的上（下）确界的问题，但在B有上（下）界的前提下，不能保证B有上（下）确界。若将B的上（下）确界存在，则B的上下确界一定是唯一的。同时B的上（下）确界可能在B中，也可能不在B中。（教材p129定义4.30后面一段话）

关系

一些概念和性质：关于全序关系，直接后继，良序关系等

教材p130例4.53，例4.54 整数的小于等于关系，实数的小于等于关系均为全序关系，但实数的小于等于关系中实数**不存在**直接后继。

关于良序关系：教材p130定义4.33，例4.55与p131定理4.18，例4.56进一步阐释了全序集和良序集之间的关系。

关系

教材p132 11(1) 设R是A上的二元关系，证明：R是自反的当且仅当$I_A \subseteq R$。

- 下证充分性：

$\forall x \in A$.

对于任意的$x \in A$，由I_A的定义知$(x,x) \in I_A$，又由$I_A \subseteq R$知$(x,x) \in R$，故R是自反的。

有$(x,x) \in I_A$

- 下证必要性：

I_A中所有元组

对于任意的$(x,x) \in I_A$，即$x \in A$，由R是自反的知$(x,x) \in R$，故$I_A \in R$。

教材p132 11(3) 设R是A上的二元关系，证明：R是对称的当且仅当$R = \tilde{R}$。

- 下证充分性：

$\forall (x,y) \in R$ 有$(x,y) \in \tilde{R}$

对于任意的$(x,y) \in R$，由$R = \tilde{R}$ 可知$(x,y) \in \tilde{R}$，则$(y,x) \in R$，故R是对称的。

- 下证必要性：

$R \subseteq \tilde{R}$

对于任意的$(x,y) \in R$，由R是对称的可知$(y,x) \in R$，而$(y,x) \in \tilde{R}$，从而$R \subseteq \tilde{R}$；

对于任意的$(x,y) \in \tilde{R}$，有$(y,x) \in R$，由R是对称的知$(x,y) \in R$，故$\tilde{R} \subseteq R$；

综上$\tilde{R} = R$。

关系

教材p132 11(1) 设R是A上的二元关系，证明：R是反对称的当且仅当$R\cap\tilde{R}\subseteq I_A$。

- 下证充分性：

对于任意的$(x,y)\in R$且$(y,x)\in R$，有$(x,y)\in R$且$(x,y)\in\tilde{R}$，即$(x,y)\in R\cap\tilde{R}$，而$R\cap\tilde{R}\subseteq I_A$，故$(x,y)\in I_A$，于是$x=y$，故$R$是反对称的。

- 下证必要性：

因为这会过滤掉不同元素的二元组

对于任意的$(x,y)\in R\cap\tilde{R}$，有$(x,y)\in R$且$(x,y)\in\tilde{R}$ $(x,y)\in R$且$(y,x)\in R$，而R是反对称的，因此$x=y$，于是$(x,y)=(x,x)\in I_A$，故$R\cap\tilde{R}\subseteq I_A$。

教材p132 11(5) 设R是A上的二元关系，证明：R是传递的当且仅当$R\circ R\subseteq R$。

- 下证充分性：

对于任意的$(x,y,z)\in R$ A $(x,y)\in R$且$(y,z)\in R$时，有$(x,z)\in R\circ R$，而$R\circ R\subseteq R$，那么$(x,z)\in R$，故R是传递的。

- 下证必要性：

对于任意的$(x,y)\in R\circ R$，均存在$z\in A$使$(x,z)\in R$ 且$(z,y)\in R$，由R是传递的，则$(x,y)\in R$，故$R\circ R\subseteq R$。

关系

教材p132 11(2) 设R是A上的二元关系，证明：R是反自反的当且仅当$I_A \cap R = \emptyset$。

必

充分

- 下证充分性：

假设其不是反自反的，则存在$x_0 \in A$，有$(x_0, x_0) \in R$。由 $(x_0, x_0) \in I_A$知$(x_0, x_0) \in I_A \cap R$，与$I_A \cap R = \emptyset$矛盾，故其必为反自反关系。

- 下证必要性：

假设$I_A \cap R \neq \emptyset$，

$$
\begin{aligned}
\text{则必有}\ (x_0, y_0) \in I_A \cap R &\Rightarrow (x_0, y_0) \in I_A \wedge (x_0, y_0) \in R \\
&\Rightarrow \boxed{(x_0 = y_0)} \wedge (x_0, y_0) \in R \\
&\Rightarrow \boxed{(x_0, x_0)} \in R
\end{aligned}
$$

这与R为反自反关系矛盾，故假设不成立。

西安交通大学
XI'AN JIAOTONG UNIVERSITY

函数

函数

函数基本概念和性质

函数，定义域，值域，特征函数（和集合的联系），幺函数；

满射，单射，双射，逆函数，复合函数（教材p140书写顺序），幂等函数；

教材p141定理5.4；

教材p137例5.6 **集合的特征函数**

集合的基数

等势；有穷集，无穷集，可数集，基数（与教材p85页定理3.1相对比）

教材p144-146 定理5.9，定理5.12，定理5.13（证明都很有意思）

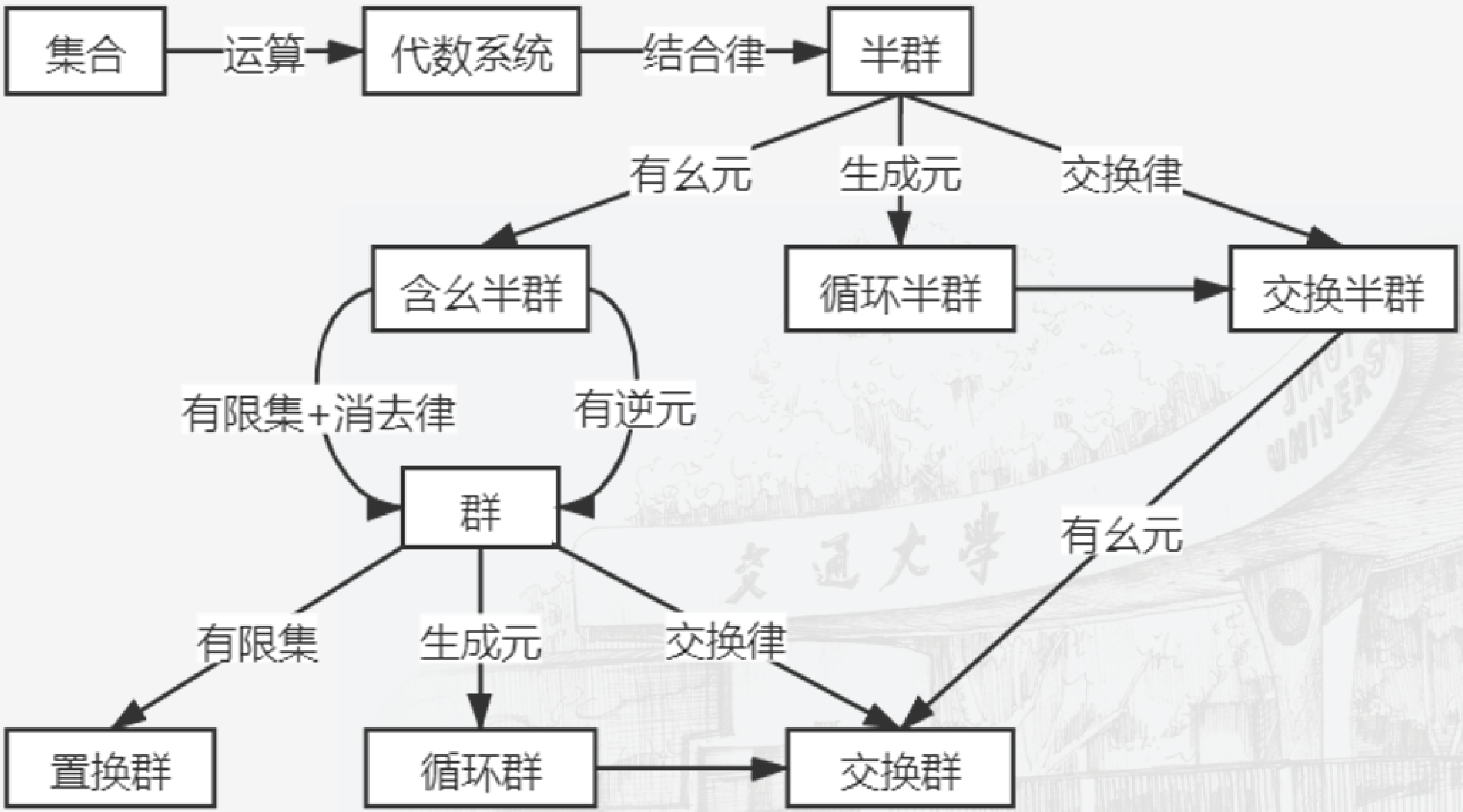
函数习题：关于证明题

教材p158习题7

代数系统

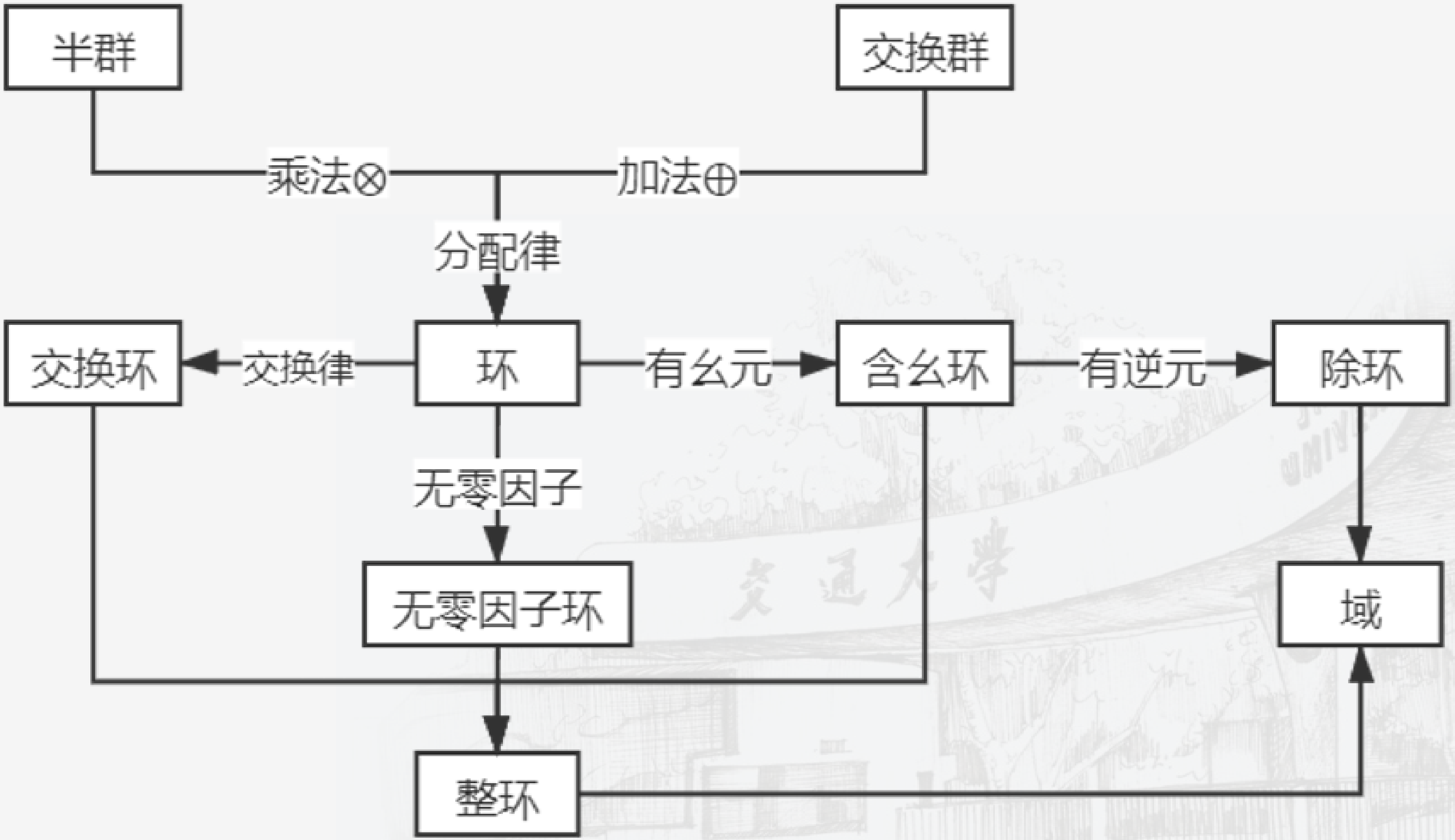
(代数结构/抽象代数/近世代数)

群代数的基本框架

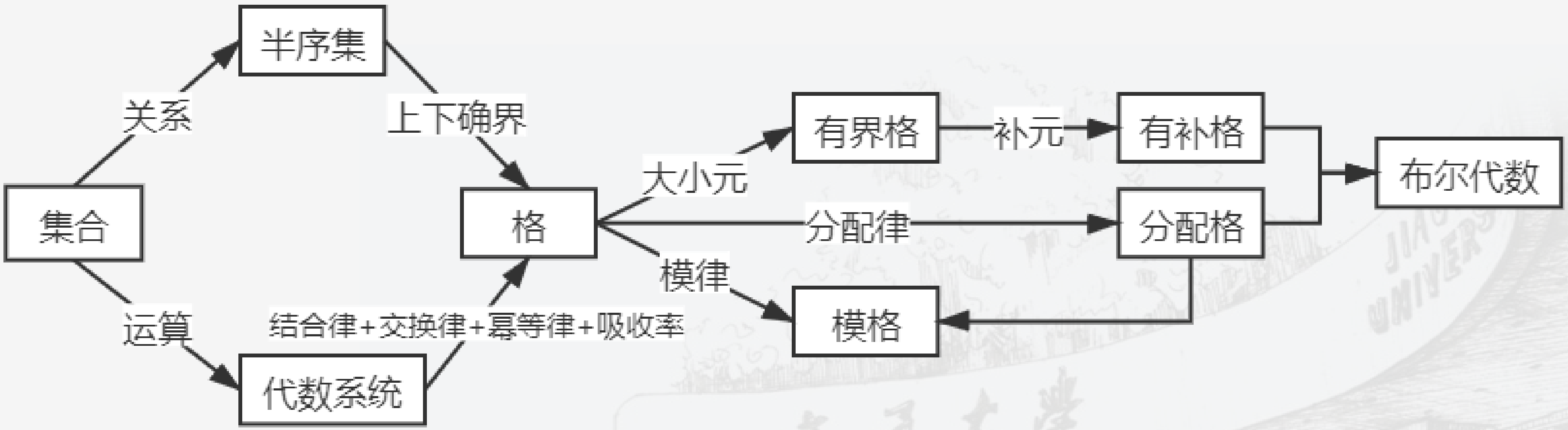


集合
运算
代数系统
结合律
半群
有幺元
生成元
交换律
含幺半群
循环半群
交换半群
有限集+消去律
有逆元
群
有幺元
有限集
生成元
交换律
置换群
循环群
交换群

环代数的基本框架



格代数的基本框架



半序集
关系
上下确界
集合
格
运算
结合律+交换律+幂等律+吸收率
代数系统
大小元
有界格
补元
有补格
布尔代数
分配律
分配格
模律
模格

代数系统复习建议

掌握每种代数系统的定义，典型例子要熟悉，各章节中的代数系统都可能出小题，对代数系统的判断很重要。

在群、环、域、格中，群是重中之重，而且大题大概率是群，环、域、格尤其是环、域出大题的可能性低，复习时应有侧重。

西安交通大学
XI'AN JIAOTONG UNIVERSITY

6.1 基本概念

6.1 基本概念

运算：设X是一非空集合， X^{n}是X的n重叉积集合，$n \in \mathrm{N}$，$*$是从X^{n}到X的关系。若$*$是从X^{n}到X的函数，则称$*$是X上的n元运算。

记作$*(x_1, x_2, \cdots, x_n) = x$

特别地，当$n = 2$时，通常记作$x_1 * x_2 = x$

证明$*$是X上的运算：证明封闭性和唯一性（即证明$*$是从X^n到X的函数）

封闭性：$\forall x_1, x_2, \cdots, x_n \in X, \exists y \in X$, 使得$*(x_1, x_2, \cdots, x_n) = y$

唯一性：$\forall x_1, x_2, \cdots, x_n \in X$, 若$*(x_1, x_2, \cdots, x_n) = y_1$且$*(x_1, x_2, \cdots, x_n) = y_2$，则$y_1 = y_2$

6.1 基本概念

代数系统：设X是一非空集合，若$*_1,*_2,\cdots,*_n$分别是X上的运算，则称$*_1,*_2,\cdots,*_n$组成的系统为代数系统。

通常记为$n+1$元组$A=<X,*_1,*_2,\cdots,*_n>$，即一个集合与定义在该集合上的运算构成代数系统。

若X是有穷集合，则A为有限代数系统
若X是无穷集合，则A为无限代数系统

子代数系统：设$A=<X,*_1,*_2,\dots,*_n>$是代数系统，其中$*_1,*_2,\dots,*_n$分别是X上的$p_1,p_2,\cdots,p_n$元运算。设S是X的非空子集，$\Delta_1,\Delta_2,\cdots,\Delta_n$分别是$*_1,*_2,\dots,*_n$的子关系，若$\Delta_1,\Delta_2,\cdots,\Delta_n$分别是$X$上的$p_1,p_2,\cdots,p_n$元运算，则称$<S,\Delta_1,\Delta_2,\cdots,\Delta_n>$是$A$的子代数系统。

定理：设$<X,*>$是一个代数系统，其中$*$是X上的运算。设$S\subseteq X$且$S\neq\emptyset$，那么$<S,*>$构成$<X,*>$的子代数系统的充要条件是运算$*$在S中满足封闭性。（可推广到$<X,*_1,*_2,\dots,*_n>$）

性质：结合律、交换律、消去律、分配律有继承性。幺元e和零元0若在子代数系统的集合S中，则也有继承性（即子代数系统中e也是幺元，0也是零元）。

二元运算的性质

1. 结合律：$(x * y) * z = x * (y * z)$
2. 交换律：$x * y = y * x$
3. 消去律：$x * y = x * z \Rightarrow y = z$（左消去律）且$y * x = z * x \Rightarrow y = z$（右消去律）
4. x_0是幺元：$x_0 * x = x$（左幺元）且$x * x_0 = x$（右幺元）(幺元常记为e)
5. x_0是零元：$x_0 * x = x_0$（左零元）且$x * x_0 = x_0$（右零元）
6. y_0是x_0的逆元：$y_0 * x_0 = e$（左逆元）且$x_0 * y_0 = e$（右逆元）
7. $*$对Δ满足分配律：$x * (y \Delta z) = (x * y) \Delta (x * z)$（左分配律）

   且$(y \Delta z) * x = (y * x) \Delta (z * x)$（右分配律）

(以上x, y, z均为$\forall$的)

【例1】设N_+、I、R、R_+、Q_+ 表示正整数、整数、实数、正实数、正有理数集

(1) $< N_+, +, \times >$是代数系统；

(2) $< N_+, +, - >$不是代数系统；（$1 - 2 = -1 \notin N_+$）

(3) $< I, +, - >$是代数系统；

(4) $< N_+, \times, \div >$不是代数系统；（$1 \div 2 = 0.5 \notin N_+$）

(5) $< Q_+, \times, \div >$是代数系统；

(6) $< R_+, \times, \div >$是代数系统；

(7) $< R, +, -, \times, \div >$不是代数系统。（不存在实数$a$，使得$1 \div 0 = a$）

【例2】设S是非空集合，2^S是S的幂集，$\cap, \cup, ', \setminus, \oplus$分别是交、并、补、差、对称差运算，则$< 2^S, \cap, \cup, ', \setminus, \oplus >$是代数系统。

6.1 基本概念

【例3】设M_n是n阶实方阵组成的集合，$+$和$\times$分别是矩阵加法和矩阵乘法，则$< M_n,+,\times>$是代数系统。

【例4】设$N_m = \{[0]_m,[1]_m,[2]_m,\dots,[m-1]_m\}$，　$+_m$和$\times_m$是模m加法和乘法，则$< N_m,+_m,\times_m>$是代数系统。

【例5】若$A = \{a,b,c\}$，下表给出两种A^2到A的关系$*_1$和$*_2$：

$*_1$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$*_2$	a	b	c
a	b	c	d
b	c	d	e
c	d	e	f

则$< A,*_1>$是代数系统，　$< A,*_2>$不是代数系统（因为不满足封闭性）。

【例6】在代数系统$< 2^{\{a,b,c\}},\cup,\cap >$中，下列哪些子集$S$可以构造出子代数系统$< S,\cup,\cap >$？

$S_1=\{\emptyset,\{a\}\}$ √　$S_2=\{\emptyset,\{a\},\{b\}\}$ ×　$S_3=\{\emptyset,\{a\},\{b\},\{a,b\}\}$ √

$S_4=\{\emptyset,\{a\},\{b,c\},\{a,b,c\}\}$ √　$S_5=\{\{a\},\{a,b\},\{a,c\},\{a,b,c\}\}$ √

【例7】设$< \{f_1,f_2,f_3,f_4\},\circ >$是代数系统，其中$\circ$是函数的复合运算。(a)是运算表，判断哪些是其子代数系统。

$\circ$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_2	f_2	f_2
f_3	f_3	f_3	f_3	f_3
f_4	f_4	f_3	f_2	f_1

(a)

$\circ$	f_1	f_2	f_3
f_1	f_1	f_2	f_3
f_2	f_2	f_2	f_2
f_3	f_3	f_3	f_3

是

$\circ$	f_1	f_2	f_4
f_1	f_1	f_2	f_4
f_2	f_2	f_2	f_2
f_4	f_4	f_3	f_1

不是

$\circ$	f_1	f_2
f_1	f_1	f_2
f_2	f_2	f_2

是

$\circ$	f_1	f_4
f_1	f_1	f_4
f_4	f_4	f_1

是

$\circ$	f_2
f_2	f_2

是

$\circ$	f_4
f_4	f_1

不是

$\circ$	f_3	f_4
f_3	f_3	f_3
f_4	f_2	f_1

不是

结合律

(1) 对于整数运算，加法$+$和乘法$\times$满足结合律；减法$-$不满足结合律。
(2) 对于集合运算，交$\cap$、并$\cup$、环和$\oplus$都满足结合律；差$\backslash$不满足结合律。
(3) 对于矩阵运算，加法$+$和乘法$\times$满足结合律。
(4) 对于同余集合N_m，加法$+_m$和乘法$\times_m$都满足结合律。
(5) 对于运算表，结合律没有明显特征。

交换律

(1) 对于整数运算，加法+、乘法×满足交换律；而减法−不满足交换律。
(2) 对于集合运算，交∩、并∪、环和⊕满足交换律，差\不满足交换律。
(3) 对于矩阵运算，加法+满足交换律，乘法×不满足交换律。
(4) 对于同余集合N_m，加法$+_m$和乘法$\times_m$都满足交换律。
(5) 对于运算表，若满足交换律，则该表沿主对角线对称。

$*_1$	a	b	c
a	a	b	c
b	b	a	a
c	c	a	a

满足交换律

$*_2$	a	b	c
a	a	b	a
b	c	c	b
c	a	b	c

不满足交换律

消去律

(1)对于整数运算，加法+满足消去律，乘法×不满足消去律；而在正整数运算中，乘法×满足消去律；

(2)对于集合运算，交∩、并∪都不满足消去律，环和⊕满足消去律。

(3)对于矩阵运算，加法+满足消去律，乘法×不满足消去律。在满秩矩阵运算中，乘法×满足消去律。

(4)对于同余集合N_m，加法$+_m$满足消去律，乘法$\times_m$不满足消去律。

(5)对于运算表，左消去律是同一行各个元素不同，右消去律是同一列各个元素不同，消去律是同行或同列各个元素不同。

$*_1$	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

满足左消去律，不满足右消去律

$*_2$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

满足消去律

幺元

(1) 对于整数运算，加法+的幺元是0，乘法×的幺元是1。
(2) 对于集合运算，交∩的幺元是全集，并∪的幺元是空集，环和⊕的幺元是空集。
(3) 对于矩阵运算，加法+的幺元是零矩阵，乘法×的幺元是单位阵。
(4) 对于同余集合N_m，加法$+_m$的幺元是$[0]_m$，乘法$\times_m$的幺元是$[1]_m$。
(5) 对于运算表，左幺元对应行与表头相同，右幺元对应列与表头相同，幺元对应行和对应列与表头相同。

$*_1$	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

a，b，c都是左幺元，没有右幺元

$*_2$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

a是幺元

6.1 基本概念

零元

(1) 对于整数运算，加法+无零元，乘法×的零元是0。

(2) 对于集合运算，交∩的零元是空集，并∪的零元是全集，环和⊕无零元。

(3) 对于矩阵运算，加法+无零元，乘法×的零元是零矩阵。

(4) 对于同余集合N_m，加法$+_m$五零元，乘法$\times_m$的幺元是$[0]_m$。

(5) 对于运算表，左零元与其对应行各个元素相同，右零元与其对应列各个元素相同，零元与其对应行和对应列各个元素相同。

$*_1$	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

a，b，c都是右零元，没有左零元

$*_2$	a	b	c
a	a	b	c
b	b	b	c
c	c	c	c

c是零元

逆元

(1) 对于整数运算，a关于加法+的逆元是-a，关于乘法×只有1和-1的逆元是本身，其余元素无逆元。
(2) 对于集合运算，全集关于交∩的逆元是全集，空集关于并∪的逆元是空集，其余元素关于交∩、并∪无逆元，每个元素关于环和⊕的逆元是本身。
(3) 对于矩阵运算，关于加法+的逆元是相反数矩阵，关于乘法×只有满秩矩阵有逆元，是其逆矩阵。
(4) 对于同余集合N_m， $[i]_m$关于加法$+_m$的逆元是$[m-i]_m$，关于乘法$\times_m$的逆元没有通式，需要具体分析。
(5) 对于运算表，先找幺元，元素所在行出现幺元，则幺元对应列的表头元素为右逆元；元素所在列出现幺元，则幺元对应行的表头元素为左逆元；左右逆元相同即为逆元。

$*_1$	a	b	c
a	a	b	c
b	b	a	a
c	c	a	a

a是幺元。a的逆元是a，b的逆元是b和c，c的逆元也是b和c。

$*_2$	a	b	c
a	a	b	a
b	c	c	b
c	a	b	c

c是幺元。c的逆元是c，a和b无逆元，a和b的左逆元是b，b的右逆元是a和b

分配律

(1) 对于整数运算，乘法×对于加法+满足分配律。
(2) 对于集合运算，交∩对于并∪ 满足分配律，并∪对于交∩满足分配律，交∩对于环和⊕满足分配律。
(3) 对于矩阵运算，乘法×对于加法+满足分配律。
(4) 对于同余集合N_m，乘法$\times_m$对于加法$+_m$满足分配律。
(5) 对于运算表，分配律无明显特征。

【例8】设$< X,*>$是代数系统，$*$是X上的二元运算。证明：
(1) 如果$*$有幺元，则幺元是唯一的。
(2) 如果$*$有零元，则零元是唯一的。
(3) 如果$*$满足结合律，元素$a \in X$有逆元，则a的逆元是唯一的。

证明：(1) 设e_1和e_2都是幺元。对于$x \in X$，$e_1 * x = x$，取$x = e_2$时，有$e_1 * e_2 = e_2$；对于$x \in X$，$x * e_2 = x$，取$x = e_1$时，有$e_1 * e_2 = e_1$。根据运算$*$的唯一性知，$e_1 = e_2$。
(2) 设e_1和e_2都是零元。对于$x \in X$，$e_1 * x = e_1$，取$x = e_2$时，有$e_1 * e_2 = e_1$；对于$x \in X$，$x * e_2 = e_2$，取$x = e_1$时，有$e_1 * e_2 = e_2$。根据运算$*$的唯一性知，$e_1 = e_2$。
(3) 设b_1和b_2都是a的逆元，则$b_1 = b_1 * e = b_1 * (a * b_2) = (b_1 * a) * b_2 = e * b_2 = b_2$。

西安交通大学
XI'AN JIAOTONG UNIVERSITY

6.2 同构与同态

同态公式

定义：设$< X,*>$和$< Y,\Delta >$是两个代数系统，$*$和Δ分别是X和Y上的n元运算，若有一函数$h: X \to Y$，使得对任意$(x_1, x_2, \cdots, x_n) \in X^n$，有$h\left(*\,(x_1, x_2, \cdots, x_n)\right) = \Delta\left(h(x_1), h(x_2), \cdots, h(x_n)\right)$，则称函数h对$*$和$\Delta$保持运算。红色式子称为同态公式。

同态和同构

定义：设$A_1 =< X,*_1,*_2,\cdots,*_m>$和$A_2 =< Y,\Delta_1,\Delta_2,\cdots,\Delta_m >$是两个同类型（同类型指运算的个数相等，对应运算的阶相等）的代数系统。若存在函数$h: X \to Y$，对A_1和A_2中每一对相应的运算满足同态公式，则称h是从A_1到A_2的同态函数，称A_1到A_2同态，称$< h(X),\Delta_1,\Delta_2,\cdots,\Delta_m >$为$A_1$的同态象。

(1) 若h是单射的，则称h是从A_1到A_2的单同态函数，称$< h(X),\Delta_1,\Delta_2,\cdots,\Delta_m >$为$A_1$的单同态象。

(2) 若h是满射的，则称h是从A_1到A_2的满同态函数，称A_2为A_1的满同态象。

(3) 若h是双射的，则称h是从A_1到A_2的同构函数，称A_1和A_2同构。

6.2 同构与同态

同态系统运算性质继承性

设$< X,*>$和$< Y,\Delta >$是代数系统，其中$*$和Δ分别是X上和Y上的二元运算，$< h(x),\Delta >$是$< X,*>$的同态像。

(1) 若在$< X,*>$中$*$满足结合律，则在$< h(x),\Delta >$中Δ满足结合律。

(2) 若在$< X,*>$中$*$满足交换律，则在$< h(x),\Delta >$中Δ满足交换律。

(3) 若在$< X,*>$中$*$有幺元e，则在$< h(x),\Delta >$中Δ有幺元$h(e)$。

(4) 若在$< X,*>$中$*$有零元0，则在$< h(x),\Delta >$中Δ有零元$h(0)$。

(5) 若在$< X,*>$中x有逆元y，则在$< h(x),\Delta >$中$h(x)$有幺元$h(y)$。

(6) 消去律在单射条件下有继承性。

本节要点

(1) 核心是找同态函数

(2) 找同态函数可通过画运算表观察以辅助寻找 (看Y域.元素少 可试试

(3) 注意同态是单向的，同构是双向的（因此运算性质的继承性也相应地是单向和双向的）

【例1】$< N_+,\times >$到$< \{F,T\},\wedge >$同态（满同态）。

证明：取（满射）函数$h: N_+ \to \{F,T\}$如下：

$$h(i) = \begin{cases} T, & i\text{是奇数} \\ F, & i\text{是偶数} \end{cases}$$

对于任意的$i,j \in N_+$，验证$h(i\times j) = h(i) \wedge h(j)$：

1) i是偶数，j是偶数时，$i\times j$是偶数，$h(i\times j) = F$，$h(i) \wedge h(j) = F \wedge F = F$

2) i是奇数，j是偶数时，$i\times j$是偶数，$h(i\times j) = F$，$h(i) \wedge h(j) = T \wedge F = F$

3) i是偶数，j是奇数时，$i\times j$是偶数，$h(i\times j) = F$，$h(i) \wedge h(j) = F \wedge T = F$

4) i是奇数，j是奇数时，$i\times j$是奇数，$h(i\times j) = T$，$h(i) \wedge h(j) = T \wedge T = T$

证毕。

【例2】$< 2^{\{a,b,c\}}, \cup, \cap, ' >$到$< \{F,T\}, \vee, \wedge, \neg >$同态。

【分析】取函数$h: 2^{\{a,b,c\}} \to \{F,T\}$如下：

$$h(S) = \begin{cases} T, & S = \emptyset, \{a\}, \{c\}, \{a,c\} \\ F, & S = \{b\}, \{a,b\}, \{b,c\}, \{a,b,c\} \end{cases}$$

验证过程略。

（同态函数有时不易找到，判断同态时想清楚是没找到还是找不到。不过这里一般不会出太难）

6.2 同构与同态

【例3】设N是自然数集合（包括0），E_+是非负偶数集合。则$< N,+>$与$< E_+,+>$同构。

证明：取$h: N \rightarrow E_+$为，$h(i) = 2i$，由初等数学知识，h是双射函数，而且，$h(i+j) = 2(i+j) = 2i + 2j = h(i) + h(j)$满足同态公式。故$< N,+>$与$< E_+,+>$同构。

【例4】设m是正整数，则$< N_m, +_m >$到$< N'_m, +'_m >$ 同态。其中$N'_m = \{0,1,2,\dots,m-1\}$，$+'_m$的定义如下：

$$i +'_m j = (i+j)\ (mod\ m)$$

证明：定义函数$h: N_m \to N'_m$为：$h([i]_m) = i\ (mod\ m)$，很显然h是双射，而且，$h([i]_m +_m [j]_m) = h([i+j]_m) = (i+j)(mod\ m) = i+'_m j = h([i]_m) +'_m h([j]_m)$，故$h$满足同态公式。

例如m=3时，运算表如下图所示，各对应位置完全一致。

$+_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[1]_3$	$[1]_3$	$[2]_3$	$[0]_3$
$[2]_3$	$[2]_3$	$[0]_3$	$[1]_3$

$+'_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

XI'AN JIAOTONG UNIVERSITY

6.3 半群

6.3 半群

半群

定义：设X是一非空集合，$< X,* >$是代数系统，其中$*$是X上的二元运算，若$*$满足结合律，则称$< X,* >$是半群。

当X是有限集时，称$< X,* >$是有限半群。

当X是无限集时，称$< X,* >$是无限半群。

交换半群

定义：设$< X,* >$是半群，若$*$满足交换律，则称$< X,* >$是交换半群。

交换半群

定义：设$< X,* >$是半群，若关于$*$有幺元，则称$< X,* >$是含幺半群。

既是交换半群又是含幺半群可称交换含幺半群或含幺交换半群。

6.3 半群

代数系统中的乘幂

乘幂的定义：设$<X,*>$是代数系统，$*$是二元运算，则任意$x \in X$，$x^1 = x$， $x^{m+1} = x^m * x(m = 1,2,\cdots)$

定理：设$<X,*>$是半群，任取$x \in X$，对任意$m,n \in N_+$，有：

（1） $x^m * x^n = x^{m+n}$

（2） $(x^m)^n = x^{mn}$

循环半群

定义：设$<X,*>$是半群，若存在$x_0 \in X$，对任意的$x \in X$，存在$n \in N$，使得$x = x_0^n$，则称$<X,*>$为循环半群，称x_0为该循环半群的生成元。

定理：循环半群一定是交换半群。

【证明】设$<X,*>$是循环半群， a是其生成元，则对任意$x,y \in X$，存在$m,n \in N$，使得$x = a^m$，$y = a^n$。因此$x * y = a^m * a^n = a^{m+n} = a^{n+m} = a^n * a^m = y * x$。因此$*$满足交换律。故$<X,*>$是交换半群。

子半群

定义：设$< X,*>$是半群，$S \subseteq X$，$S \neq \emptyset$，若$< S,*>$是$< X,*>$的子代数系统且$< S,*>$是半群，则称$< S,*>$是$< X,*>$的子半群。

定理：设$< X,*>$是半群，$S \subseteq X$，$S \neq \emptyset$，$< S,*>$是$< X,*>$的子半群的充要条件是$*$在S中满足封闭性。（因为：①子代数系统的充要条件是运算的封闭性；②结合律可以通过子代数系统的方式继承）

6.3 半群

【例1】设N、Z、R_+ 表示自然数、整数、正实数集合。
$< N,+>$，$< N,\times>$是交换含幺半群；
$< Z,+>$，$< Z,\times>$是交换含幺半群，$< Z,->$不是半群；
$< R_+,+>$，$< R_+,\times>$是交换含幺半群，$< R_+,\div>$不是半群。

【例2】设X是非空集合，2^X是X的幂集。
$< 2^X,\cup>$，$< 2^X,\cap>$，$< 2^X,\oplus >$都是交换含幺半群；
$< 2^X,\backslash >$不是半群。

【例3】设$M_{n\times n}$是$n\times n$阶实矩阵的集合。
$< M_{n\times n},+>$是交换含幺半群；$< M_{n\times n},\times>$是含幺半群。

【例4】设$N_m=\{[0]_m,[1]_m,[2]_m,\ldots,[m-1]_m\}$。
$< N_m,+_m>$和$< N_m,\times_m>$都是交换含幺半群。

【例5】 证明$< 2^{A\times A},\circ>$是含幺半群。其中A是非空集合，$2^{A\times A}$是由A上所有二元关系的集合，$\circ$表示关系的复合。

证明：

(代数系统)任取$R_1,R_2 \in 2^{A\times A}$，即$R_1,R_2 \subseteq A\times A$。由关系的复合定义知，$R_1\circ R_2=\{(a_1,a_2)|a_1\in A\wedge a_2\in A\wedge(\exists a_3\in A)\big((a_1,a_3)\in R_1\wedge(a_2,a_3)\in R_2\big)\}\subseteq A\times A$(封闭性)，且$R_1\circ R_2$是唯一的(唯一性)。因此$< 2^{A\times A},\circ>$是代数系统。

(结合律)任取 $R_1,R_2,R_3\in 2^{A\times A}$ ，根据课本P111定理4.6 (4)可知，$(R_1\circ R_2)\circ R_3=R_1\circ(R_2\circ R_3)$。即$\circ$满足结合律。

(幺元)取I_A是A上的幺函数： $I_A=\{(x,x)|x\in A\}$，根据复合函数的性质知，任意$R\in 2^{A\times A}$， $I_A\circ R=R\circ I_A=R$。因此I_A是$\circ$的幺元。

【例6】在$<\{a,b,c,d\},*>$中，$c^1=c,c^2=a,c^3=c,c^4=a,\cdots$ $b^1=b,b^2=c,b^3=d,b^4=a,\cdots$这说明$c$不是生成元，$b$是生成元。

*	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

西安交通大學
XI'AN JIAOTONG UNIVERSITY

6.4 群

6.4 群

群

定义：设$<G,*>$是含幺半群，若G中每个元素都有逆元，则称$<G,*>$为群。通常将x的逆元记作x^{-1}。

当G是由n个元素组成的有限集时，称$<G,*>$是有限群，也称n阶群，记作n-群。

当G是无限集合时，称$<G,*>$是无限群。

交换群

定义：满足交换律的群称作交换群。

群的基本性质

定理1：设$< G,* >$是群，$|G| \geq 2$，则

(1) G中每个元素的逆元是唯一的；

(2) G中无零元。

证明：(1) 因为$< G,* >$是群，所以$*$满足结合律，所以G中每个元素的逆元是唯一的。

(2) 假设G中有零元0。一方面，0有唯一逆元0^{-1}，使得$0 * 0^{-1} = 0^{-1} * 0 = e$。另一方面，由零元的性质知，$0 * 0^{-1} = 0^{-1} * 0 = 0$。因此$0 = e$。所以对任意$x \in G$，$x = x * e = x * 0 = 0$，即$G$中只有一个元素0，与$|G| \geq 2$矛盾。

定理2：设$< G,* >$是群，则对任意$x, y \in G$，有

(1) $(x^{-1})^{-1} = x$；

(2) $(x * y)^{-1} = y^{-1} * x^{-1}$。

(证明略，用逆元的定义证即可)

6.4 群

群的基本性质

定理3： 设$<G,*>$是群，则运算$*$满足消去律。

证明：若$a*b=a*c$，则$b=e*b=(a^{-1}*a)*b=a^{-1}*(a*b)=a^{-1}*(a*c)=(a^{-1}*a)*c=e*c=c$。同理可知$b*a=c*a\Rightarrow b=c$。
所以$*$满足消去律。

定理4： 设$<G,*>$是有限群，$|G|=n$，则在$*$的运算表中，G中每个元素在每行（列）出现且仅出现一次。

(由消去律可知最多出现一次，又由每行（列）n个元素互不相同知每个元素必出现)

群中元素的乘幂

定义：设$<G,*>$是群，G中元素x的乘幂定义如下：

$$x^0=e,\quad x^1=x,\quad x^{i+1}=x^i*x,\quad x^{-i}=(x^{-1})^i$$

性质：设$<G,*>$是群，设$x\in X$，对于整数m,n，有：

$$x^{-n}=(x^n)^{-1}(n>0),\quad x^m*x^n=x^{m+n},\quad (x^m)^n=x^{mn}$$

群中元素的阶

定义：设$<G,*>$是群，对每个$x\in G$，称使得$x^k=e$成立的最小正整数k是x的阶。若不存在这样的k，则x的阶为无穷。

定理1：设$<G,*>$是群，则G中元素x与x^{-1}的阶相同。
定理2：设$<G,*>$是群，G中元素x的阶若为k，则$x^1,x^2,\cdots,x^k$两两不同；G中元素x的阶若为无穷，则$x^1,x^2,x^3,\cdots$两两不同；
定理3：设$<G,*>$是群，则G中元素的阶不超过群的阶。
定理4：设$<G,*>$是群，G中元素x的阶为k，若$x^m=e(m\in N_+)$，则$k|m$。

循环群

定义： 设$<G,*>$是群，如果有$a\in G$，对任意$x\in G$，均有整数i，使得$x=a^i$。则称$<G,*>$为循环群，称a为该循环群的生成元。

定理1： 循环群一定是交换群。

证明：设$<G,*>$是循环群，a是生成元。任取$x,y\in G$，必有整数m,n，使得$x=a^m,y=a^n$。所以$x*y=a^m*a^n=a^{m+n}=a^{n+m}=a^n*a^m=y*x$。即运算$*$满足交换律。所以$<G,*>$是交换群。

定理2： 设$<G,*>$是循环群，a是生成元。

(1) 若a的阶为k，则$<G,*>$同构于$<N_k,+_k>$；

(2) 若a的阶为无穷，则$<G,*>$同构于$<N,+>$。

(证明略)

置换的表示

置换式：

$$p=\begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ a_1{}' & a_2{}' & a_3{}' & \cdots & a_n{}' \end{pmatrix}$$

轮换式：$(a_1, a_2, a_3, \cdots, a_n)$表示：

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_{n-1} & a_n \\ a_2 & a_3 & \cdots & a_n & a_1 \end{pmatrix}$$

例如：$S=\{1,2,3,4,5,6\}$，S上的置换$p_1=\{(1,2),(2,3),(3,4),(4,1)\}$和$p_2=\{(1,4),(2,1),(3,3),(4,2)\}$可用下述形式表示：

$$p_1=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}=(1234),\qquad p_2=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}=(142)$$

置换群

定义： 设$S=\{a_1,a_2,\cdots,a_n\}$是n个元素构成的有限集合，$\diamond$是函数的复合。

(1) P是m个S上的置换组成的集合。若$<P,\diamond>$是群，则称其为n次置换群（m阶）。

(2) P_S是所有由S上的置换组成的集合。称$<P_S,\diamond>$为n次对称群（$n!$阶）。

注意：

(1) 不是任何S上置换组成的集合P都可以构成群。

(2) 所有S上的置换组成的集合P_S一定可以构成群。

Cayley定理： 设$<G,*>$是n-群，则$<G,*>$同构于一个n次置换群。

子群

定义：设$< G,* >$是群，$S \subseteq G$且$S \neq \emptyset$。如果$< S,* >$是群，则称$< S,* >$是$< G,* >$的**子群**。

在群$< G,* >$中称$< \{e\},* >$和$< G,* >$是**平凡子群**，其他子群统称为**非平凡子群**。

子群的三个充要条件

定理1：设$< G,* >$是群，$S \subseteq G$且$S \neq \emptyset$。那么$< S,* >$是$< G,* >$的子群的充要条件是：(1)$\forall a, b \in S$，$a * b \in S$；(2)$\forall a \in S$，$a^{-1} \in S$

定理2：设$< G,* >$是群，$S \subseteq G$且$S \neq \emptyset$。那么$< S,* >$是$< G,* >$的子群的充要条件是：$\forall a, b \in S$，$a * b^{-1} \in S$

定理3：设$< G,* >$是有限群，$S \subseteq G$且$S \neq \emptyset$。那么$< S,* >$是$< G,* >$的子群的充要条件是：$\forall a, b \in S$，$a * b \in S$

6.4 群

陪集

定义：设$< G,*>$是群，$< H,*>$是$< G,*>$的子群。对于$a \in G$，构造下面的两个集合：

$$aH = \{a * h | h \in H\}, \qquad Ha = \{h * a | h \in H\}$$

分别称为由a确定的H在G中的左陪集和右陪集，称a为代表元。

注意：(1) 在一般条件下，一个元素的左陪集与右陪集不一定是相同集合。不过，如果$< G,*>$是交换群，则左陪集与右陪集一定相等。
(2) 特别提示：当$Ha = aH$时，并不表明：对于$h \in H$，满足$h * a = a * h$。更不意味着运算$*$满足交换律。（请认真理解两个集合相等的含义。）

定理1：设$< G,*>$是群，$< H,*>$是$< G,*>$的子群。
(1) 任取$a \in G$，均有$|H| = |aH| = |Ha|$。
(2) 设$S_l = \{aH | a \in G\}$，$S_r = \{Ha | a \in G\}$，则S_l，S_r均构成G上的划分，$|S_l| = |S_r|$。

定理2：设$< G,*>$是n-群，$< H,*>$是$< G,*>$的子群。若$< H,*>$是k-群，则$k | n$。(Lagrange定理的一个推论)

6.4 群

【例1】$<Z,+>$是交换群，$<N,+>$不是群；
$<R,+>$是交换群，$<R_+,+>$不是群；
$<N,\times>$不是群，$<Z,\times>$不是群；
$<R,\times>$不是群，$<R_+,\times>$是交换群。

【例2】$<2^X,\cup>$不是群；$<2^X,\cap>$不是群；$<2^X,\oplus>$是交换群；

【例3】$<M_{n\times n},+>$是交换群；$<M_{n\times n},\times>$不是群。

【例4】$<P[x],+>$是交换群；$<P[x],\times>$不是群。

【例5】$<N_m,+_m>$是交换群。

6.4 群

【例6】$< N_m, \times_m >$不是群。
（因为有零元$[0]_m$）

【例7】$< N_5\backslash\{[0]_5\}, \times_5 >$是交换群，$< N_6\backslash\{[0]_6\}, \times_6 >$不是群。

$\times_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$
$[1]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[2]_5$	$[0]_5$	$[2]_5$	$[4]_5$	$[1]_5$	$[3]_5$
$[3]_5$	$[0]_5$	$[3]_5$	$[1]_5$	$[4]_5$	$[2]_5$
$[4]_5$	$[0]_5$	$[4]_5$	$[3]_5$	$[2]_5$	$[1]_5$

$\times_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$
$[1]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[2]_6$	$[0]_6$	$[2]_6$	$[4]_6$	$[0]_6$	$[2]_6$	$[4]_6$
$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$
$[4]_6$	$[0]_6$	$[4]_6$	$[2]_6$	$[0]_6$	$[4]_4$	$[2]_6$
$[5]_6$	$[0]_6$	$[5]_6$	$[4]_6$	$[3]_6$	$[2]_6$	$[1]_6$

【例8】设R是实数集合，定义$R \times R$上的二元运算$*$为：对于$(x_1, y_1), (x_2, y_2) \in R \times R$

$$(x_1, y_1) * (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$

证明$< R \times R, * >$是交换群。

证明：(1) (运算) 对于任意的$(x_1, y_1), (x_2, y_2) \in R \times R$，即$x_1, y_1, x_2, y_2 \in R$，由实数加法的性质知，$x_1 + x_2, y_1 + y_2 \in R$，且结果唯一，因此$(x_1, y_1) * (x_2, y_2) \in R \times R$，且结果唯一。

(2) (结合律) 对于任意的$(x_1, y_1), (x_2, y_2), (x_3, y_3) \in R \times R$，有$\big((x_1, y_1) * (x_2, y_2)\big) * (x_3, y_3) = (x_1 + x_2, y_1 + y_2) * (x_3, y_3) = \big((x_1 + x_2) + x_3, (y_1 + y_2) + y_3\big) = \big(x_1 + (x_2 + x_3), y_1 + (y_2 + y_3)\big) = (x_1, y_1) * (x_2 + x_3, y_2 + y_3) = (x_1, y_1) * \big((x_2, y_2) * (x_3, y_3)\big)$。

(3) (交换律) 对于任意的$(x_1, y_1), (x_2, y_2) \in R \times R$，有$(x_1, y_1) * (x_2, y_2) = (x_1 + x_2, y_1 + y_2) = (x_2 + x_1, y_2 + y_1) = (x_2, y_2) * (x_1, y_1)$。

(4) (幺元) 对于任意的$(x, y) \in R \times R$，$(0,0) * (x, y) = (0 + x, 0 + y) = (x, y)$，由交换律又有$(x, y) * (0,0) = (x, y)$，因此$(0,0)$是幺元。

(5) (逆元) 对于任意的$(x, y) \in R \times R$，$(-x, -y) * (x, y) = (-x + x, -y + y) = (0,0)$，由交换律又有$(x, y) * (-x, -y) = (0,0)$，因此$(-x, -y)$是$(x, y)$的逆元。

【例9】在$<\{a,b,c,d\},*>$中，a是幺元，阶是1；
$c^1=c,c^2=a,c^3=c,c^4=a$，c的阶是2，不是生成元；
$b^1=b,b^2=c,b^3=d,b^4=a$，b的阶是4，是生成元；
$d^1=d,d^2=c,d^3=b,d^4=a$，d的阶是4，是生成元。
这说明该群是循环群。

*	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

【例10】$<\{f_1,f_2,f_3,f_4,f_5,f_6\},\circ>$由于不是交换群，故不是循环群。

$$f_1=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\quad f_2=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$

$$f_3=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\quad f_4=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$$

$$f_5=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\quad f_6=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_6	f_5	f_4	f_3
f_3	f_3	f_5	f_1	f_6	f_2	f_4
f_4	f_4	f_6	f_5	f_1	f_3	f_2
f_5	f_5	f_3	f_4	f_2	f_6	f_1
f_6	f_6	f_4	f_2	f_3	f_1	f_5

【例11】取$A=\{1,2,3,4\}$，f_1,f_2,f_3,f_4是A上的双射，$<\{f_1,f_2,f_3,f_4\},*>$是交换群，不是循环群。

$$f_1=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\quad f_2=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$$

$$f_3=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\quad f_4=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$$

$\circ$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

f_1是幺元，阶是1；
$(f_2)^2=f_1,(f_3)^2=f_1,(f_4)^2=f_1$，$f_2,f_3,f_4$的阶都是2，不是生成元。

交换群不一定是循环群！

【例12】例11的群，是4次置换群(4阶)。（Klein 4-群）

$\circ$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

*	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	1	2
4	4	3	2	1

6.4 群

【例13】例10的群，是3次对称群(6阶)。

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_6	f_5	f_4	f_3
f_3	f_3	f_5	f_1	f_6	f_2	f_4
f_4	f_4	f_6	f_5	f_1	f_3	f_2
f_5	f_5	f_3	f_4	f_2	f_6	f_1
f_6	f_6	f_4	f_2	f_3	f_1	f_5

*	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	6	5	4	3
3	3	5	1	6	2	4
4	4	6	5	1	3	3
5	5	3	4	2	6	2
6	6	4	2	3	1	5

【例14】同构意义下，1-群、2-群、3-群只有一种，4-群有两种。

*	e
e	e

1-群

*	e	a
e	e	a
a	a	e

2-群

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

3-群

$\circ$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

Klein 4-群

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$< N_4, +_4 >$

【例15】下列哪些构成<{实数},+>的非平凡子群?

<{整数},+> √ <{正实数},+> × <{有理数},+> √

<{偶数},+> √ <{奇数},+> ×

【例16】下列哪些构成$< N_6, +_6 >$的非平凡子群?

$< \{0,1,3,5\}, +_6 >$ ×

$< \{0,1,5\}, +_6 >$ ×

$< \{0,2,4\}, +_6 >$ √

$< \{0,1\}, +_6 >$ ×

$< \{0,3\}, +_6 >$ √

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

6.4 群

(0,1,2,3,4,5)

【例17】在群$< N_6, +_6 >$中，

(1) 在子群$< \{0,3\}, +_6 >$中，所有的左陪集/右陪集有：

$$\{0,3\}, \{1,4\}, \{2,5\}$$

(2) 在子群$< \{0,2,4\}, +_6 >$中，所有的左陪集/右陪集有：

$$\{0,2,4\}, \{1,3,5\}$$

求解过程：以求$H = \{0,2,4\}$在$< N_6, +_6 >$中的所有左陪集为例。

$0H = \{0 +_6 0, 0 +_6 2, 0 +_6 4\} = \{0,2,4\}$

$1H = \{1 +_6 0, 1 +_6 2, 1 +_6 4\} = \{1,3,5\}$

$2H = \{2 +_6 0, 2 +_6 2, 2 +_6 4\} = \{2,4,0\}$

$3H = \{3 +_6 0, 3 +_6 2, 3 +_6 4\} = \{3,5,1\}$

$4H = \{4 +_6 0, 4 +_6 2, 4 +_6 4\} = \{4,0,2\}$

$5H = \{5 +_6 0, 5 +_6 2, 5 +_6 4\} = \{5,1,3\}$

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

6.5–6.6 环、域

6.5-6.6 环、域

定义： 设$< R,\oplus,\otimes >$是代数系统，$\oplus$和$\otimes$是R上的两个二元运算。若(1)$< R,\oplus >$是交换群；(2)$< R,\otimes >$是半群；(3)$\otimes$对$\oplus$满足分配律。则称$< R,\oplus,\otimes >$是环。

若$\otimes$满足交换律，则称$< R,\oplus,\otimes >$是交换环。
若关于$\otimes$有幺元，则称$< R,\oplus,\otimes >$是含幺环。
既是交换环又是含幺环可称交换含幺环或含幺交换环。

一些记法：
$\oplus$的幺元记为0，x关于$\oplus$的逆元记为$-x$；
$\otimes$的幺元记为e（若有），x关于$\otimes$的逆元记为x^{-1}（若有）。
$x \oplus (-y)$简记为$x - y$。

性质： (1) $a \otimes 0 = 0 = 0 \otimes a$;
(2) $a \otimes (-b) = (-a) \otimes b = -(a \otimes b)$;
(3) $(-a) \otimes (-b) = a \otimes b$;
(4) $a \otimes (b - c) = (a \otimes b) - (a \otimes c)$，$(b - c) \otimes a = (b \otimes a) - (c \otimes a)$

6.5-6.6 环、域

零因子：设$<R,\oplus,\otimes>$是环，设$a,b\in R$，$a\neq 0$，$b\neq 0$，$a\otimes b=0$。则称a是环的左零因子，b是环的右零因子。

含零因子环：含零因子的环。

无零因子环：不含零因子的环。

定理：设$<R,\oplus,\otimes>$是环。那么$<R,\oplus,\otimes>$是无零因子环的充要条件是，对任意的$x,y,z\in R$，当$z\neq 0$时，有

$$z\otimes x=z\otimes y\Rightarrow x=y$$
$$x\otimes z=y\otimes z\Rightarrow x=y$$

整环：无零因子含幺交换环。

除环：设$<R,\oplus,\otimes>$是环，若(1)关于$\otimes$有幺元，(2)任意$a\in R$，当$a\neq 0$时关于$\otimes$有逆元，则称$<R,\oplus,\otimes>$是除环。

域：设$<R,\oplus,\otimes>$是除环，$\otimes$满足交换律，则称$<R,\oplus,\otimes>$为域。

6.5-6.6 环、域

【例1】(整数环)$< Z,+,\times >$是整环，不是除环，不是域。

【例2】(矩阵环)$< M_{n\times n},+,\times >$是含幺环，不是整环，不是除环，不是域。

【例3】(整数模环) $< N_m,+_m,\times_m >$ 是含幺交换环，不是整环，不是除环，不是域。

【例4】(子集环)$< 2^X,\oplus,\cap >$是含幺交换环，不是整环，不是除环，不是域。

【例5】(多项式环) $< P[x],+,\times >$ 是整环，不是除环，不是域。

【例6】(有理数/实数/复数环/域)$< Q/R/C,+,\times >$是整环、除环、域。

7 格与布尔代数

格：设$< L,*,\oplus >$是代数系统，$*$和$\oplus$是L上的两个二元运算，如果对于所有的$x,y,z\in L$，

(1) 运算$*$和运算$\oplus$满足结合律

$$(x*y)*z=x*(y*z),\qquad (x\oplus y)\oplus z=x\oplus(y\oplus z)$$

(2) 运算$*$和运算$\oplus$满足交换律

$$x*y=y*x,\qquad x\oplus y=y\oplus x$$

(3) 运算$*$和运算$\oplus$满足幂等律

$$x*x=x,\qquad x\oplus x=x$$

(4) 运算$*$和运算$\oplus$满足吸收律

$$x*(x\oplus y)=x,\qquad x\oplus(x*y)=x$$

注意格中$*$和$\oplus$的“对称性”

定理1：设$< L,*,\oplus >$是格，则对于所有的$x, y \in L$，

$$x * y = x \Leftrightarrow x \oplus y = y$$

定理2：设$< L,*,\oplus >$是格，建立L上的二元关系R如下：对于$x, y \in L$，$xRy \Leftrightarrow x * y = x$。则

(1) R是L上的半序关系。

(2) L中任意两个元素x, y均有上下确界，而且

$$GLB\{x, y\} = x * y, \qquad LUB\{x, y\} = x \oplus y$$

定理3（格的第二种定义）：设$< L, \preccurlyeq >$是半序集。若L中任意两个元素x, y，均有下确界$GLB\{x, y\}$和上确界$LUB\{x, y\}$存在，建立L上的两种二元运算如下：

$$x * y = GLB\{x, y\}, \qquad x \oplus y = LUB\{x, y\}$$

则$< L,*,\oplus >$是格，也称$< L, \preccurlyeq >$是格，或称$< L, \preccurlyeq,*,\oplus >$是格。

格的四个性质

对偶原理：设$< L,\preccurlyeq,*,\oplus >$是格，则$< L,\succcurlyeq,\oplus,* >$也是格。（其中$\succcurlyeq$表示$\preccurlyeq$的逆关系）

保序性：设$< L,\preccurlyeq,*,\oplus >$是格，$a,b,c,d \in L$，如果$a \preccurlyeq b$且$c \preccurlyeq d$，那么$a * c \preccurlyeq b * d$，$a \oplus c \preccurlyeq b \oplus d$。

分配不等式：设$< L,\preccurlyeq,*,\oplus >$是格，对于$a,b,c \in L$，有

$$a \oplus (b * c) \preccurlyeq (a \oplus b) * (a \oplus c)$$

$$(a * b) \oplus (a * c) \preccurlyeq a * (b \oplus c)$$

模不等式：设$< L,\preccurlyeq,*,\oplus >$是格，对于$a,b,c \in L$，有

$$a \oplus \big(b * (a \oplus c)\big) \preccurlyeq (a \oplus b) * (a \oplus c)$$

$$(a * b) \oplus (a * c) \preccurlyeq a * \big(b \oplus (a * c)\big)$$

7 格与布尔代数

模格：设$< L,\preccurlyeq,*,\oplus >$是格，如果对任意$a,b,c \in L$，模不等式取等号，则称$< L,\preccurlyeq,*,\oplus >$是模格。

定理：设$< L,\preccurlyeq,*,\oplus >$是格，那么$< L,\preccurlyeq,*,\oplus >$是模格的充要条件是：对任意$a,b,c \in L$，如果$a \preccurlyeq c$，那么$a \oplus (b * c) = (a \oplus b) * c$。

分配格：设$< L,\preccurlyeq,*,\oplus >$是格，如果对任意$a,b,c \in L$，分配不等式取等号，则称$< L,\preccurlyeq,*,\oplus >$是分配格。

定理1：分配格一定是模格。

定理2：设$< L,\preccurlyeq,*,\oplus >$是分配格，对于任意$a,b,c \in L$，若$a * b = a * c$且$a \oplus b = a \oplus c$，则$b = c$。

定理3：设$< L,\preccurlyeq,*,\oplus >$是格，若$\preccurlyeq$是L上的全序关系，则$< L,\preccurlyeq,*,\oplus >$是分配格。

7 格与布尔代数

有界格：设$< L, \preccurlyeq, *, \oplus >$是格，如果存在$a, b \in L$，对任意的$x \in L$，满足$a \preccurlyeq x \preccurlyeq b$，则称$< L, \preccurlyeq, *, \oplus >$是有界格，称$a$和$b$分别为格的最小元和最大元。

表示法：通常用0和1分别代表最小元和最大元，并将有界格记作$< L, \preccurlyeq, *, \oplus, 0,1 >$

有限格一定是有界格，无限格可以是有界格。

补元：设$< L, \preccurlyeq, *, \oplus, 0,1 >$是有界格。设$x \in L$，如果存在$y \in L$，满足$x * y = 0$且$x \oplus y = 1$，则称$y$为$x$的补元。

定理：对于有界分配格，元素x如果有补元，则补元唯一。

有补格：设$< L, \preccurlyeq, *, \oplus, 0,1 >$是有界格。如果每个元素都有补元，则称$< L, \preccurlyeq, *, \oplus, 0,1 >$是有补格。

布尔代数：设$< B, \preccurlyeq, *, \oplus, 0,1 >$是有补的分配格，则称$< B, \preccurlyeq, *, \oplus, 0,1 >$是布尔代数。

说明：(1) 因为在有界分配格中，一个元素至多有一个补元，所以布尔代数中，每个元素有唯一补元。
(2) 在布尔代数中，通常用x'表示x的补元。同时，布尔代数可表示为$< B, \preccurlyeq, *, \oplus, ', 0,1 >$

定理1：设$< B, \preccurlyeq, *, \oplus, ', 0,1 >$是布尔代数。那么，对于$x, y, z \in B$，

$$(x')' = x, \qquad (x * y)' = x' \oplus y', \qquad (x \oplus y)' = x' * y',$$

$$x * y = x * z \wedge x' * y = x' * z \Rightarrow y = z,$$

$$x \oplus y = x \oplus z \wedge x' \oplus y = x' \oplus z \Rightarrow y = z$$

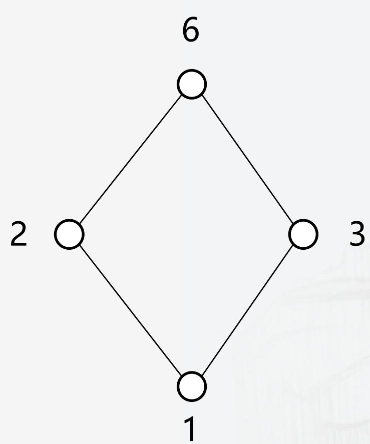
定理2：设$< B, \preccurlyeq, *, \oplus, ', 0,1 >$是布尔代数。那么以下四个说法等价：
(1) $x \preccurlyeq y$；(2) $y' \preccurlyeq x'$；(3) $x * y' = 0$；(4) $x' \oplus y = 1$。

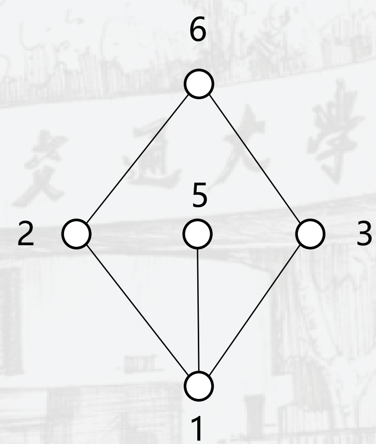
【例1】$< 2^X,\cap,\cup>$是格。

【例2】$< [0,1], min, max >$是格。

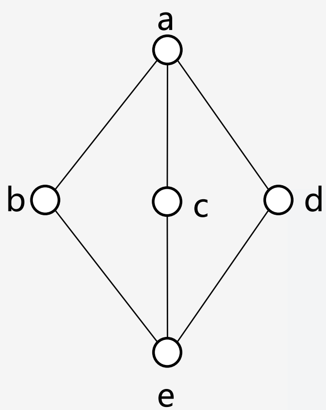
【例3】$< N_+, GCD, LCM >$是格。

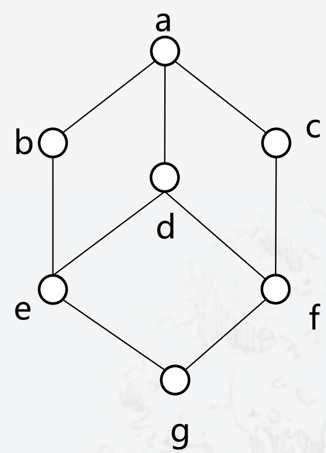
【例4】$< \{1,2,3,6\}, | >$是格，$< \{1,2,3,5,6\}, | >$不是格。



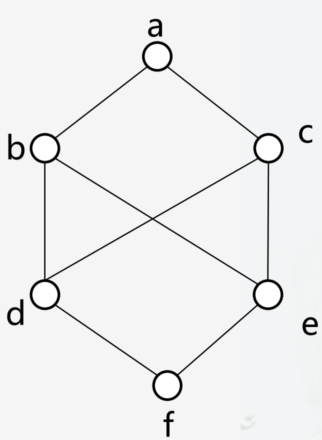


【例5】下列Hasse图构成格。

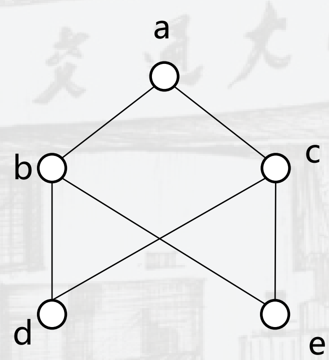




【例6】下列Hasse图不构成格。

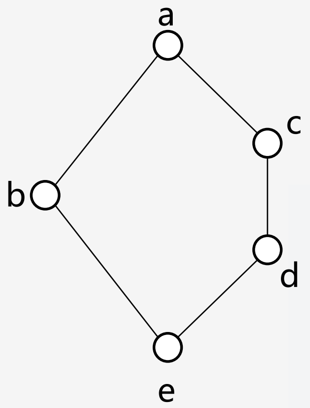


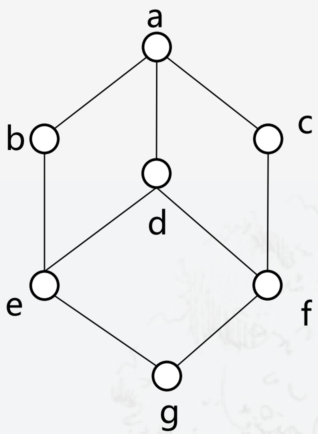
$LUB\{b,c\}, GLB\{d,e\}$不存在



$LUB\{b,c\}$不存在

【例7】有界格中的补元。





a的补元：e
b的补元：c,d
c的补元：b
d的补元：b
e的补元：a
（有补格）

a的补元：g
b的补元：c,f
e的补元：c,f
c的补元：b,e
f的补元：b,e
g的补元：a
d无补元
（非有补格）

参考资料

（1）《离散数学(第3版)》——陈建明,曾明,刘国荣
（2）2019-2020第二学期《图论与代数系统》课件——曾明

西安交通大學
XI'AN JIAOTONG UNIVERSITY

图论

图论

图论基本概念和性质

节点，边，起点，终点，端点，图，无向边，有向边，混合图，零图，平凡图，边临接，结点相邻，关联，孤立点，自环，平行边，重数，多重图，简单图，完全图，子图，真子图，生成子图，补图，节点的度，奇节点，偶节点，悬挂点，悬挂边，图的同构，途径，长度（即边条数），路，圈，简单路，简单圈，初级路，初级圈，可达，短程线，距离，连通与非连通，连通图与非连通图，连通支，强连通，单向连通，弱连通，强连通支，单项连通支，弱连通支，邻接矩阵

图论基本定理

教材p260定理8.3 无向图中奇节点的个数为偶数

教材p262 两图同构必要条件

教材p264 **关于初级路**：有路必有初级路；一条初级路（圈）必是一条简单路（圈）；初级路长度小于等于$n-1$

教材p267 关于无向图连通支：无向图每个节点和每条边恰属于一个连通支

教材p268定理8.5 关于有向图连通支

图论

图论算法与定理：Dijkstra，Euler图，Hamilton图，二分图等

教材p280 Dijkstra算法

教材p283定理8.7 Euler定理

- 无向连通图G是Euler图的充要条件：G中无奇结点
- 无向图G是Euler图的充要条件：G联通且无奇结点

教材p284推论8.7.1 无向连通图G中具有Euler路的充要条件：G恰好有两个奇结点

教材p284定义8.24 割边与Fleury弗罗莱算法（寻找Euler路）

教材p285定理8.8 关于Euler路（单向连通）与定理8.9 关于Euler圈（强连通）

教材p296 二分图，完全二分图，定理8.15，匹配，最大匹配（匈牙利方法），完美匹配，杆，饱和点，不饱和点

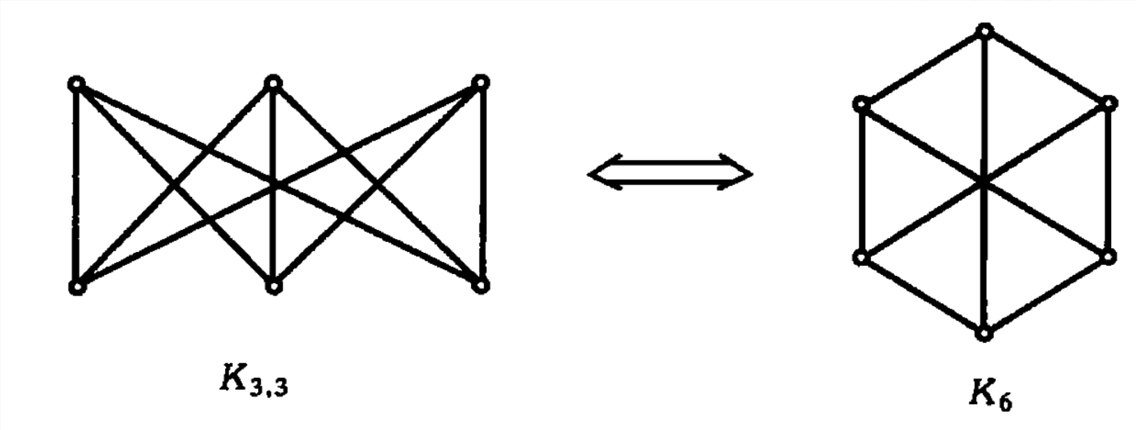
教材p289-293 定理8.11（必要条件，反证其不为Hamilton图），定理8.12（充分条件），定理8.13，例8.24，定义8.26（竞赛图），货郎担问题

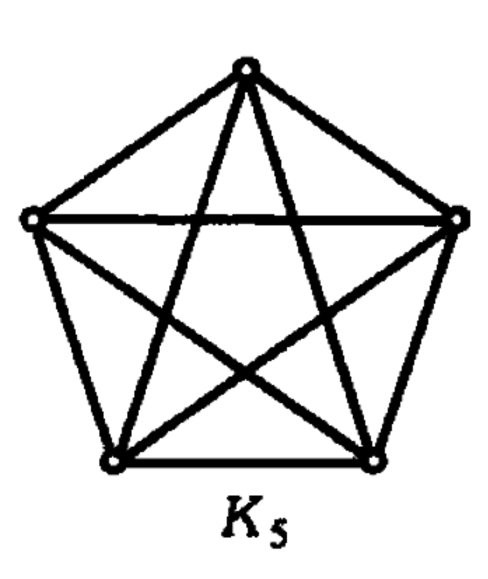
图论算法与定理：平面图，Kuratowski定理等

教材p303定理8.16 Euler公式和两个推论8.16.1，8.16.2

- Euler公式是Euler于1750年针对凸多面体的“点、线、面”之间提出的一个重要的量化关系
- 作为平面图的必要条件

教材p305定理8.17 Kuratowski定理





图论习题

教材p318习题14 求连通支问题中注意图中孤立点的情况；

教材p318习题16 Dijkstra算法

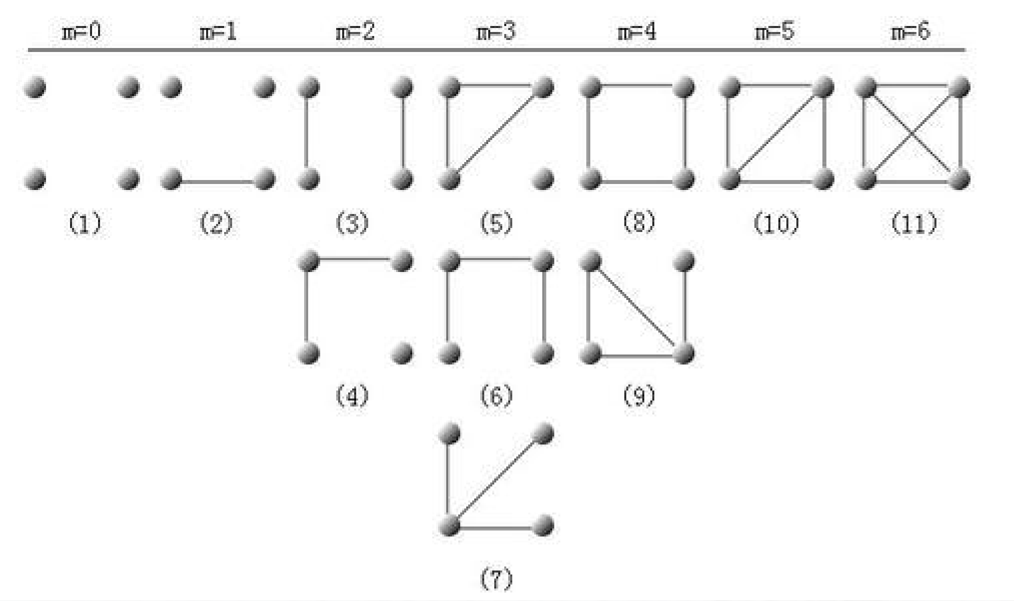
教材p318习题18 Euler定理应用

教材p320习题24 关于H-图：教材定理8.11的应用

教材p320习题33 平面图Euler公式

教材p320习题34 Kuratowski定理应用

- 关于图的同构



个人备考策略

第一遍（时间较长）

看书上概念+例题+定理

重做书上所有的题（不仅仅是作业题），对自己错的和认为重要的做好标记。

第二遍

只看标记的题；

标记的题重做或重新看；

谢谢大家

谢谢大家