格与布尔代数

一、环与域

0. 预备知识

广群：运算封闭

半群：运算可结合的广群

独异点：存在幺元的半群

群：任何元素存在逆元的独异点

阿贝尔群：运算可交换的群

有限循环群：形如$\{a, a^2, a^3, \cdots, a^n = e\}$的群

循环群：任何元素都由a的幂组成的群

1. 定义

（1）设$< A, \star, * >$是一个代数系统，如果满足：

> $< A, \star >$是一个阿贝尔群
>
> $< A, * >$是半群
>
> 运算*对于运算⋆是可分配的

则称$< A, \star, * >$是**环**

（2）设$< A, +, \cdot >$

如果$< A, \cdot >$是可交换的，则称$< A, +, \cdot >$是**交换环。**

如果$< A, \cdot >$含有幺元，则称$< A, +, \cdot >$是**含幺环。**

（3）设$< A, +, \cdot >$是一个代数系统，如果满足：

> $< A, + >$是阿贝尔群
>
> $< A, \cdot >$是可交换独异点，且无零因子（$a, b \in A - \{\theta\}, s.t. a \cdot b \in A - \{\theta\}$）
>
> 运算 $\cdot$ 对于运算$+$可分配

则称$< A, +, \cdot >$是**整环。**

（3）设$< A, +, \cdot >$是一个代数系统，如果满足：

> $< A, + >$是阿贝尔群
>
> $< A - \{\theta\}, \cdot >$是阿贝尔群
>
> 运算 $\cdot$ 对于运算$+$可分配

则称$< A, +, \cdot >$是**域**

2. 定理

（1）设$< A,+,\cdot >$是一个环，则对任意的$a,b,c \in A$，有:

- $a \cdot \theta = \theta \cdot a = \theta$
- $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$
- $(-a) \cdot (-b) = a \cdot b$
- $a \cdot (b-c) = a \cdot b - a \cdot c$
- $(b-c) \cdot a = b \cdot a - c \cdot a$

（2）整环中的无零因子条件等价于乘法消去律，即$c \neq \theta$和$c \cdot a = c \cdot b$，必有$a = b$

（3）域一定是整环。

证明：$$

设任意域$< A,+,\cdot >$，1是乘法幺元，对任意$a,b,c \in A$，满足$a \cdot b = a \cdot c$

如果$a \neq \theta$，则有$b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot (a \cdot c) = (a^{-1} \cdot a) \cdot c = 1 \cdot c = c$，则乘法消去律成立，

即无零因子条件成立，由于$< A-\{\theta\},\cdot >$显然是可交换独异点，则域$< A,+,\cdot >$是整环。

（4）有限整环必定是域。

证明：$$

设有限整环$< A,+,\cdot >$，对任意$a,b,c \in A$，且$a \neq \theta$，则$a \cdot b = a \cdot c \iff b = c$

则$a \cdot A = A$。对$1 \in A$，必定存在$d \in A$，使得$a \cdot d = 1$，则$A-\{\theta\}$中的任意元素都有逆元，

故$< A-\{\theta\},\cdot >$是阿贝尔群，即有限整环一定是域。

二、格

1. 定义

（1）设$< A,\leq >$是一个偏序集，如果A中任意两个元素都有最小上界和最大下界，则称$< A,\leq >$为**格**

（2）设$< A,\leq >$为格，如果在A上定义两个二元运算$\vee$和$\wedge$，使得对任意的$a,b \in A$，$a \vee b$等于a和b的最小上界，$a \wedge b$等于a和b的最大下界，那么称$< A,\vee,\wedge >$为格$< A,\leq >$诱导的代数系统。

（3）设$< A,\leq >$是一个格，由$< A,\leq >$诱导的代数系统为$< A,\vee,\wedge >$，设$B \subseteq A$，且$B \neq \varnothing$，如果A的两个运算$\vee,\wedge$关于B封闭，则称$< B,\leq >$是$< A,\leq >$的子格。

（4）设$< A_1,\leq_1 >$和$< A_2,\leq_2 >$是两个格，它们分别诱导的代数系统为$< A_1,\vee_1,\wedge_1 >$和$< A_2,\vee_2,\wedge_2 >$，如果存在一个从A_1到A_2的映射f，使得对任意$a,b \in A_1$，有:

$f(a \vee_1 b) = f(a) \vee_2 f(b)$

$f(a \wedge_1 b) = f(a) \wedge_2 f(b)$

则称f为从$< A_1,\vee_1,\wedge_1 >$到$< A_2,\vee_2,\wedge_2 >$的**格同态**，称$< f(A_1),\leq_2 >$是$< A_1,\leq_1 >$的**格同态象。**

当f为双射时，称f为从$< A_1,\vee_1,\wedge_1 >$到$< A_2,\vee_2,\wedge_2 >$的**格同构**，称$< A_1,\leq_1 >$和$< A_2,\leq_2 >$是**同构**的。

2. 定理

（1）在一个格$<A,\leq>$中，对任意$a,b\in A$，有：

> $a\leq a\vee b,\quad b\leq a\vee b$
>
> $a\wedge b\leq a,\quad a\wedge b\leq b$

（2）在一个格$<A,\leq>$中，对任意$a,b,c,d\in A$，如果

$a\leq b,c\leq d$，则：

> $a\vee c\leq b\vee d$
>
> $a\wedge c\leq b\wedge d$

（3）在一个格$<A,\leq>$中，对任意$a,b,c\in A$，如果

$b\leq c$，则：（保序性）

> $a\vee b\leq a\vee c$
>
> $a\wedge b\leq a\wedge c$

（4）在一个格$<A,\leq>$中，对任意$a,b,c,d\in A$，有：（析取同理）

> $a\vee b=b\vee a$ 交换律
>
> $a\vee(b\vee c)=(a\vee b)\vee c$结合律
>
> $a\vee a=a$ 等幂律
>
> $a\vee(a\wedge b)=a$ 吸收律

（5）设$<A,\vee,\wedge>$是一个代数系统，其中$\vee,\wedge$都是二元运算且满足吸收律，则$\vee,\wedge$都满足等幂律。（吸收律和等幂律等价）

（6）设$<A,\vee,\wedge>$是一个代数系统，其中$\vee,\wedge$都是二元运算且满足交换性、结合性和吸收性，则A上存在偏序关系$\leq$，使得$<A,\leq>$是一个格。

证明：$$

设偏序关系为$a\wedge b=a\iff a\leq b$

证明该偏序关系是自反的、可传递的、反对称的。

其次证明$a\wedge b$是a,b的最大下界，$a\vee b$是a,b的最小上界。

（7）在一个格$<A,\leq>$中，对任意$a,b,c\in A$，都有：*（括号里为"并"的在右侧）*

> $a\vee(b\vee c)\leq(a\vee b)\wedge(a\vee c)$
>
> $(a\wedge b)\vee(a\wedge c)\leq a\wedge(b\vee c)$

（8）设$<A,\leq>$是一个格，那么对于任意$a,b\in A$,有

$a\leq b\iff a\wedge b=a\iff a\vee b=b$

右侧等价符号只需要等幂律成立即可。

$a\wedge b=a\Rightarrow a\leq b$显然。

$a\leq b\Rightarrow a\wedge b=a$证明：$$

$a\leq a,a\leq b\Rightarrow a\leq a\wedge b$

又因$a \wedge b \leq a$，则$a = a \wedge b$成立。

（9）设$< A, \leq >$是一个格，对于任意$a, b, c \in A$，有（模格取等号）

$a \leq c \iff a \vee (b \wedge c) \leq (a \vee b) \wedge c$（同样以括号内符号为大小判断方式）

证明：$$

$a \leq c, a \leq a \vee b \Rightarrow a \leq (a \vee b) \wedge c$

$b \wedge c \leq b \leq (a \vee b), b \wedge c \leq c \Rightarrow b \wedge c \leq (a \vee b) \wedge c$

（10）设$< A, \leq >$是一个格，对于任意$a, b, c \in A$，有：

> $(a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee (a \wedge c))$
>
> $a \vee (b \wedge (a \vee c)) \leq (a \vee b) \wedge (a \vee c)$

证明：$$

$a \wedge b \leq a, a \wedge c \leq a \Rightarrow (a \wedge b) \vee (a \wedge c) \leq a$

$a \wedge b \leq b \leq b \vee (a \wedge c), a \wedge c \leq b \vee (a \wedge c) \Rightarrow (a \wedge b) \vee (a \wedge c) \leq (b \vee (a \wedge c))$

同理可得第二个式子成立。

如果利用定理（9），则根据$a \leq a \vee c$可得第二个式子成立；根据$a \wedge c \leq a$可得第一个式子成立。

（11）设f是格$< A_1, \leq_1 >$到$< A_2, \leq_2 >$的格同态，则对任意$x, y \in A_1$，
$x \leq_1 y \Rightarrow f(x) \leq_2 f(y)$

证明：$$

$a \leq_1 b \Rightarrow a \wedge_1 b = a \Rightarrow f(a) = f(a \wedge_1 b) = f(a) \wedge_2 f(b) \Rightarrow f(a) \leq_2 f(b)$

由于f不一定为单射，故$f(b) = f(a \wedge_1 b) \nRightarrow a = a \wedge_1 b$，即反之未必成立。

（12）设f是格$< A_1, \leq_1 >$到$< A_2, \leq_2 >$的格同构，则对任意的$x, y \in A_1$，
$x \leq_1 y \iff f(x) \leq_2 f(y)$

证明：$$

$a \leq_1 b \Rightarrow a \wedge_1 b = a \Rightarrow f(a) = f(a \wedge_1 b) = f(a) \wedge_2 f(b) \Rightarrow f(a) \leq_2 f(b)$

$f(a) \leq_2 f(b) \Rightarrow f(a) = f(a) \wedge_2 f(b) = f(a \wedge_1 b) \Rightarrow a = a \wedge_1 b \Rightarrow a \leq_1 b$

三、分配格

1. 定义

（1）设$< A, \vee, \wedge >$是由格$< A, \leq >$所诱导的代数系统，如果对任意$a, b, c \in A$，满足

> $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$
>
> $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

则称$< A, \leq >$是分配格。

（2）设$< A, \leq >$是一个格，由它诱导的代数系统为$< A, \vee, \wedge >$，如果对于任意的$a, b, c \in A$，当$b \leq a$时，有：

$a \wedge (b \vee c) = b \wedge (a \vee c)$**，则称$< A, \leq >$为模格。（一般情况下取$\geq$）**

2. 定理

（1）一个格是分配格的充要条件是在该格中没有任何子格与M_5或N_5同构。

（2）交对并可分配 $\Longleftrightarrow$ 并对交可分配

证明：$$

$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \Rightarrow$

$(a \vee b) \wedge (a \vee c) = ((a \vee b) \wedge a) \vee ((a \vee b) \wedge c) = a \vee (a \wedge c) \vee (b \wedge c) = a \vee (b \wedge c)$

同理可证必要性成立。

（3）每个链是分配格。

（4）设$< A, \leq >$是一个分配格，那么对于任意$a, b, c \in A$，

如果$a \wedge b = a \wedge c, a \vee b = a \vee c$成立，则必有$b = c$。

证明：$$

$b = b \vee (b \wedge a) = b \vee (c \wedge a) = (b \vee c) \wedge (b \vee a) = (b \vee c) \wedge (c \vee a) = c \vee (a \wedge b) = c \vee (a \wedge c) = c$

（5）格$< A, \leq >$是模格，当且仅当不含有适合下述条件的元素u, v, w，使得：

$v < u,\ u \vee w = v \vee w,\ u \wedge w = b \wedge w$

证明：$$反证法

若存在使得上述条件成立的a, b, c，使得$a < b, a \vee c = b \vee c, a \wedge c = b \wedge c$，

则$\mathbf{b \wedge (a \vee c) = b \wedge (b \vee c) = b\ \ a \vee (b \wedge c) = a \vee (a \wedge c) = a}$，则不是模格。

若不是模格，即$a < b \Rightarrow a \vee (b \wedge c) \leq b \wedge (a \vee c)$

则$(a \vee (b \wedge c)) \vee c = a \vee (b \wedge c) \vee c = a \vee c$

$a < b, a \leq a \vee c \Rightarrow a \leq b \wedge (a \vee c) \leq (b \wedge (a \vee c)) \vee c$

$c \leq (b \wedge (a \vee c)) \vee c \Rightarrow$

$\mathbf{a \vee c \leq (b \wedge (a \vee c)) \vee c \leq a \vee c = (a \vee (b \wedge c)) \vee c}$

又因$a \vee (b \wedge c) \leq b \wedge (a \vee c) \Rightarrow \mathbf{(a \vee (b \wedge c)) \vee c \leq (b \wedge (a \vee c)) \vee c}$

故$(a \vee (b \wedge c)) \vee c = (b \wedge (a \vee c)) \vee c$。同理可得$(a \vee (b \wedge c)) \wedge c = (b \wedge (a \vee c)) \wedge c$。

即存在满足上述条件的a, b, c。

（6）一般的格中：以下三个式子成立：

> $a \vee (b \wedge c) \leq ((a \vee b) \wedge (a \vee c))$
>
> $((a \wedge b) \vee (a \wedge c)) \leq a \wedge (b \vee c)$
>
> $((a \wedge b) \vee (b \wedge c) \vee (a \wedge c)) \leq ((a \vee b) \wedge (b \vee c) \wedge (a \vee c))$

在模格中，讲上述三个式子的$\leq$改为$=$，则三个式子等价。

前两个等号显然等级，且前两个等号成立时，第三个等号显然成立。下证：第三个等号可以推出第一个等号成立。

证明：$$（吸收律-条件-全等式模格-结论）

$a \vee (b \wedge c) = a \vee (a \wedge b) \vee (a \wedge c) \vee (b \wedge c) = a \vee ((a \vee b) \wedge (b \vee c) \wedge (a \vee c))$

由$a \leq (a \vee b) \wedge (a \vee c)$且为模格，可得

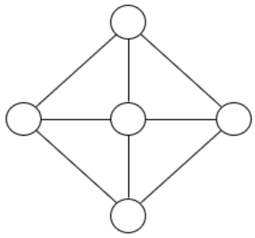
$a \vee (((a \vee b) \wedge (a \vee c)) \wedge (b \vee c)) = (a \vee (b \vee c)) \wedge ((a \vee b) \wedge (a \vee c))$

则原式$= (a \vee b \vee c) \wedge (a \vee b) \wedge (a \vee c) = (a \vee b) \wedge (a \vee c)$

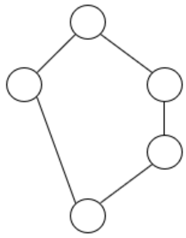
（7）分配格一定是模格。

设$a \leq b$，则$b \wedge (a \vee c) = (b \wedge a) \vee (b \wedge c) = a \vee (b \wedge c)$，得证。

3. 特殊格



M_5



N_5

M_5格：模格但不是分配格

N_5格：既不是模格也不俗分配格

四、有补格

1. 定义

（1）设$< A, \leq >$是一个格，如果存在元素$a \in A$，对于任意$x \in A$，都有$a \leq x$，则称a为格$< A, \leq >$的**全下界**，记**0**。

存在元素$b \in A$，对于任意$x \in A$，都有$x \leq b$，则称b为格$< A, \leq >$的**全上界**，记**1**。

（2）如果一个格存在全上界和全下界，则称该格为**有界格。**

（3）设$< A, \leq >$是一个有界格，对于A中的一个元素a，如果存在$b \in A$，使得$a \vee b = 1$和$a \wedge b = 0$，则称元素b是元素a的**补元。**

（4）在一个有界格中，如果每个元素都至少有一个补元素，则称此格为**有补格。**

（5）一个格如果它既是有补格，又是分配格，则称它为**有补分配格**，把有补分配格中任一元素a的唯一补元记为$\overline{a}$。

2. 定理

（1）格$< A, \leq >$若有全上界（全下界），则是唯一的。

设$a, b \in A$，使得$a \leq x$，且$b \leq x$，则$a \leq b$，$b \leq a$，即$a = b$

（2）设$< A, \leq >$是一个有界格，则对任意$a \in A$，必有

$a \vee 1 = 1,\ a \wedge 1 = a,\ a \vee 0 = a,\ a \vee 1 = 1$

只证一个：$a \vee 1 \in A$，则$a \vee 1 \leq 1$；又因$1 \leq a \vee 1$，则$a \vee 1 = 1$

（3）在有界分配格中，若有一个元素有补元素，则必定是唯一的。

设a有两个补元素b, c，则$a \vee b = a \vee c = 1$，$a \wedge b = a \wedge c = 0$，则$a = b$

五、布尔代数

1. 定义

（1）一个有补分配格称为**布尔格。**

（2）由布尔格$<A,\le>$，可以诱导一个代数系统$<A,\vee,\wedge,^{-}>$，这个代数系统称为**布尔代数。**

（3）具有有限个元素的布尔代数称为**有限布尔代数。**

（4）设$<A,\vee,\wedge,^{-}>$和$<B,\vee,\wedge,^{-}>$是两个布尔代数，如果存在着A到B的双射f，对于任意的$a,b\in A$，都有：

> $f(a\vee b)=f(a)\vee f(b)$
>
> $f(a\wedge b)=f(a)\wedge f(b)$

则称$<A,\vee,\wedge,^{-}>$和$<B,\vee,\wedge,^{-}>$**同构。**

（5）设$<A,\le>$是一个格，且具有全下界0，如果有元素a*盖住*0，则称元素a为**原子。**

2. 定理

（1）【德摩根定律】对于布尔代数中的任意两个元素a,b，必有：
$\overline{(\overline{a})}=a$, $\overline{a\vee b}=\overline{a}\wedge\overline{b}$, $\overline{a\wedge b}=\overline{a}\vee\overline{b}$

（2）设$<A,\le>$是一个具有全下界0的有限格，则对于任意一个非零元素b，至少存在一个原子a，使得$a\le b$。

如果b不是原子，则必存在b_1，使得$0<b_1<b$，如果b_i是原子，则定理得证，如果b_1不是原子，则存在b_2。。。

（3）在一个布尔格中，$b\wedge\overline{c}=0 \iff b\le c$。

$b\wedge\overline{c}=0\Rightarrow(b\wedge\overline{c})\vee c=c\Rightarrow b\vee c=c\Rightarrow b\le c$

$b\le c\Rightarrow b\wedge c=b\Rightarrow b\wedge\overline{c}=(b\wedge c)\wedge\overline{c}=0$

（4）设$<A,\vee,\wedge,^{-}>$是一个有限布尔代数，$b\in A$，且$b\ne 0$，$a_1,a_2,\cdots,a_k$是满足$a_i\le b\quad(i=1,2\cdots,k)$的$A$中的所有原子，则$b=a_1\vee a_2\vee\cdots\vee a_k$是将$b$表示为原子的并的唯一形式。

证明：$$

设有另外一种表示方式$b=a_{j0}\vee a_{j1}\vee\cdots\vee a_{jt}$。显然$t\le k$。

若$t<k$，则必存在$a_i\in\{a_1,a_2,\cdots,a_k\}$,且$a_i\notin\{a_{j_0},a_{j1},\cdots,a_{j_t}\}$。

则$a_i\wedge b=a_i\wedge(a_{j0}\vee a_{j1}\vee\cdots\vee a_{jt})=a_i\wedge(a_1\vee a_2\vee\cdots\vee a_k)$

得到$0=a_i$，这与a_i是原子矛盾，故$t=k$。

（5）在一个布尔格$<A,\vee,\wedge,^{-}>$中，对A中任意一个原子a和另一个非零元素b，$a\le b$和$a\le\overline{b}$两式中有且仅有一式成立。

证明：$$

两式均不成立：则$b<a$且$\overline{b}<a$，与a是原子矛盾。

两式均成立：则$a\le b\wedge\overline{b}=0$，与$a$是原子矛盾。

$a\le b\Rightarrow a\wedge\overline{b}=0$则$a\le\overline{b}$一定不成立。

同理可证另外一种情况成立。

（6）【Stone表示定理】设$< A,\vee,\wedge,^- >$是由$< A,\leq>$诱导的有限布尔代数，S是布尔格$< A,\leq>$中所有原子的集合，则$< A,\vee,\wedge,^- >$与$< P(S),\cup,\cap,\sim>$同构。

证明：$$

设任意一个非零元素$x\in A$，$x=a_1\vee a_2\vee\cdots a_k$，设$S_x=\{a_1,a_2,\cdots,a_k\}$，则定义$f(x)=S_x$。

证f为双射$\rightarrow$证$< A,\vee,\wedge,^- >$与$< P(S),\cup,\cap,\sim>$同构。

$x\notin f(a)\iff x\not\leq a\iff x\in f(\overline{a})$

（7）有限布尔格的元素个数必定等于2^n，其中n是该布尔格中所有原子的个数。

（8）任何一个具有2^n元素的有限布尔格都是同构的。

六、布尔表达式

1. 定义

（1）设$< A,\vee,\wedge,^- >$是一个布尔代数，并在这个布尔代数上定义**布尔表达式**如下：

> 1. A中任意一个元素是一个布尔表达式
> 2. 任何变元是一个布尔表达式
> 3. 如果e_1和e_2是布尔表达式，那么$\overline{e}_1,(e_1\vee e_2),(e_1\wedge e_2)$也都是布尔表达式
> 4. 只有通过有限次运用规则2和3所构造的符号串式布尔表达式

（2）一个含有n个相异变元的布尔表达式，称为**含有n元的布尔表达式**。记为$E(x_1,x_2,\cdots,x_n)$，其中$x_1,x_2,\cdots,x_n$为变元。

（3）布尔代数$< A,\vee,\wedge,^- >$上的一个含有n元的**布尔表达式$E(x_1,x_2,\cdots,x_n)$的值**是指：将A中的元素作为变元$x_i(i=1,2,\cdots,n)$的值来代替表达式中的相应的变元，从而计算出来表达式的值。

（4）设布尔代数$< A,\vee,\wedge,^- >$上两个n元的布尔表达式为$E_1(x_1,x_2,\cdots,x_n)$和$E_2(x_1,x_2,\cdots,x_n)$，如果对于n个变元的任意赋值$x_i=\tilde{x_i},\tilde{x_i}\in A$，均有$E_1(\tilde{x_1},\tilde{x_2},\cdots,\tilde{x_n})=E_2(\tilde{x_1},\tilde{x_2},\cdots,\tilde{x_n})$则称这两个**布尔表达式等价**，记作$E_1(x_1,x_2,\cdots,x_n)=E_2(x_1,x_2,\cdots,x_n)$。

（5）设$< A,\vee,\wedge,^- >$是一个布尔代数，一个从A^n到A的函数，如果它能够用$< A,\vee,\wedge,^- >$上的n元布尔表达式来表示，那么这个函数杯称为**布尔函数**。

2. 定理

（1）对于两个元素的布尔代数$< \{0,1\},\vee,\wedge,^- >$，任何一个从$\{0,1\}^n$到$\{0,1\}$的函数都是布尔函数。

（2）设$E(x_1,x_2,\cdots,x_n)$是布尔代数$< A,\vee,\wedge,^- >$上任意一个布尔表达式，则它一定能写成析取范式。