Boolean Algebra

paner

2020 年 6 月 6 日

1 束

束は, 環や体と同じく 2 つの二項演算により定義される代数系で, ブール代数やハイティング代数は束の特殊なものである. ブール代数を考察するにあたり, 束の基本的な概念を記す.

1.1 join と meet

定義 (束)

L を空でない集合, $\vee$ と $\wedge$ を join と meet という二項演算とする. 次の条件を満たすとき,L を束という. 任意の $x, y, z \in L$ に対し,

$L1$ (a) $x \vee (y \vee z) = (x \vee y) \vee z$
(b) $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ (結合律)

$L2$ (a) $x \vee y = y \vee x$
(b) $x \wedge y = y \wedge x$ (交換律)

$L3$ (a) $x \wedge (x \vee y) = x$
(b) $x \vee (x \wedge y) = x$ (吸収律)

$L3$ の (a) において, $y = x \vee y$ とすると,

$$x = x \wedge (x \vee y) = x \wedge (x \vee (x \wedge y)) = x \wedge x$$

となり, 重要な性質が導かれる.

定義 (束) 続き

$L4$ (a) $x \vee x = x$
(b) $x \wedge x = x$ (ベキ等律)

$L1 - L4$ では, $\vee$ と $\wedge$ は対称な形で表せる. つまり, $\vee$ と $\wedge$ を入れ替えて定義しても同じ束が導かれる. このことを, 束における双対原理という.

1.2 順序集合と束

定義 (順序集合)

ある集合 A における二項演算 $\leq$ が次の条件を満たすとき, $(A, \leq)$ を順序集合という. 任意の $x, y, z \in A$ に対し

$P1$ $\quad a \leq a$ (反射律)

$P2$ $\quad a \leq b$ かつ $b \leq a \Rightarrow a = b$ (反対称律)

$P3$ $\quad a \leq b$ かつ $b \leq c \Rightarrow a \leq c$ (推移律)

順序集合において, 任意の $a, b \in A$ に対し $a \leq b$ または $b \leq a$ のどちらかが成り立つとき,$(A, \leq)$ を全順序集合という.

1.3 上限と下限

定義 (極大元と最大元)

a を順序集合 $(A,\leq)$ の要素とする. $a < x$ を満たす要素 x が A に存在しないとき, a を極大元という. 極大元の双対概念を極小元という。すなわち, $x < a$ を満たす要素 x が A に存在しないとき, a を極小元という.
A のすべての要素 x に対して $x < a$ であるとき, a を最大元という. 最大元の双対概念を最小元という.

最大元ならば極大元であり, 最小元ならば極小元であるが, 逆は必ずしも成立しない。
A が全順序集合であるとき,$a < x$ をみたす要素 x が P に存在しないことと,A のすべての要素 x に対して $x <= a$ であることとは同値となり, 極大元と最大元とは一致する。同様に,A が全順序集合であるとき, 極小元と最小元とは一致する.

定義 (上界)

X を順序集合 A の任意の部分集合とする. X のすべての要素 x に対して,$x <= a$ である A の要素 a を X の上界という. X の上界の双対概念を X の下界という.

ここで, 順序集合 A の任意の部分集合 X は A の順序関係によって順序集合となることを注意.

定義 (上限)

X の最小上界, すなわち X の上界全体からなる代数系と部分順序集合の最小元が存在すれば, それを X の上限といい, $\sup\{X\}$ で表す.
X の上限の双対概念を X の下限という. すなわち, X の最大下界が存在すれば, それを X の下限といい, $\inf\{X\}$ で表す.

1.4　定義の同値性

命題

次の二つの束の定義は同値である.

$P1$　ある集合 L が $L1-L4$ を満たす (1.1 における定義)

$P2$　ある集合 L において上限と下限が存在する (1.3 における定義)

証明

$\Rightarrow$) L において $a \leq b$ を $a = a \wedge b$ と定義すると $\leq$ が順序となることを示す.

$P1$　$L4(b)$ より $a = a \wedge a$ なので $a \leq a$

$P2$　仮定より, $a \leq b$ かつ $b \leq a$. すなわち, $a = ab$, $b = b \wedge a$. $L2(b)$ より,

$$a = a \wedge b = b \wedge a = b$$

したがって, $a = b$

$P3$　仮定より, $a \leq b$ かつ $b \leq c$ なので, $a = ab$, $b = b \wedge c$. したがって,

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

となるので, $\leq$ の定義より $a \leq c$

この順序によって上限が存在することを示す.
$L4$ と $L2$ より $a = a \wedge (a \vee b)$, $b = b \wedge (b \vee a) = b \wedge (a \vee b)$ となるので, $a \leq a \vee b$ かつ $b \leq a \vee b$.
これより, $a \vee b$ は a と b の上界となる.
任意の上界の元 u に対して $a \leq u$, $b \leq u$ とすると, $a = a \wedge u$ なので $a \vee u = (a \wedge u) \vee u = u \because L4$.
同様に, $b \vee u = u$ が示せる.
したがって, $(a \vee u) \vee (b \vee u) = u \vee u = u$. $u = (a \vee u) \vee (b \vee u) = ((a \vee b) \vee u)$ であることに注意すると,

$$(a \vee b) \wedge u = (a \vee b) \wedge \{(a \vee b) \vee u\} = a \vee b \because L4$$

よって, 順序の定義より $a \vee b \leq u$. $\therefore a \vee b = \sup\{a, b\}$
同様に下限が存在することを示せる.
$\Leftarrow$) $a \vee b = \sup\{a, b\}$, $a \wedge b = \inf\{a, b\}$ とすると $L1 - L4$ を満たすことを示せばよい.
ここでは (a) についてのみ示す.

$L1$　$a \vee (b \vee c) = \sup\{a,\ \sup\{b, c\}\} = \sup\{a, b, c\} = \sup\{\ \sup\{a, b\}, c\} = (a \vee b) \vee c$

$L2$　$a \vee b = \sup\{a, b\} = \sup\{b, a\} = b \vee a$

$L3$　計算すると $a = \sup\{a, \inf\{a, b\}\}$ が成り立つことが分かる.

$L4$　$a \vee a = sup\{a, a\} = a$

1.5 分配束とモジュラー束

定義 (分配束)

次の分配律を満たす束を分配束という.

$D1 \quad x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$

$D2 \quad x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$

命題

束 L において次は同値

$$L \text{ が } D1 \text{ を満たす} \Leftrightarrow L \text{ が } D2 \text{ を満たす}$$

証明 $\Rightarrow$)

$$\begin{aligned} x \vee (y \wedge z) &= (x \vee (x \wedge z)) \vee (yz) \because L4 \\ &= x \vee (z \wedge x) \vee (z \wedge y) \because L2 \\ &= x \vee (z \wedge (x \vee y)) \because D1 \\ &= (x \wedge (x \vee y)) \vee (z \wedge (x \vee y)) \because D4 \\ &= ((x \vee y) \wedge x) \vee ((x \vee y) \wedge z) \because L1 \\ &= (x \vee y) \wedge (x \vee z) \because D1 \end{aligned}$$

逆も同様に示せる.

定義 (モジュラー束)

次のモジュラー束を満たす束をモジュラー束という.

$$M\colon\ x \leq y \Rightarrow x \vee (y \wedge z) = y \wedge (x \vee z)$$

束において,$x \vee (y \wedge z) \leq y \wedge (x \vee z)$ は常に成り立つ.
したがって,$x \leq y \Rightarrow y \wedge (x \vee z) \leq x \vee (y \wedge z)$ を示せば十分である.

系

任意の分配束はモジュラー束である

証明 仮定より $x \leq y$ なので $x = x \wedge y$ $(\star)$. したがって,

$$\begin{aligned} y \wedge (x \vee z) &= (y \wedge x) \vee (y \wedge z) \because D2 \\ &= x \vee (y \wedge z) \because (\star) \end{aligned}$$

2　ブール代数

2.1　ブール代数

定義 (ブール代数)

代数系 $<B,\vee,\wedge,',0,1>$ が次の条件を満たすとき, B をブール代数という.

$B1$　$<B,\vee,\wedge>$ は分配束である

$B2$　$x \wedge 0 = 0 \quad x \vee 1 = 1$

$B3$　$x \wedge x' = 0 \quad x \vee x' = 1$

補題

ブール代数 B は次を満たす.

$B4$　$a \wedge b = 0$ かつ $a \vee b = 1$ なら $a = b'$

$B5$　$x \wedge 0 = 0 \quad x \vee 1 = 1$

$B6$　$x \wedge x' = 0 \quad x \vee x' = 1$

証明

$B4$　仮定より $a \wedge b = 0$ なので,

$$a' = a' \vee 0 = a' \vee (a \wedge b) = (a' \vee a) \wedge (a' \vee b) = 1 \wedge (a' \vee b) = a' \vee b$$

したがって, 束の定義より $a' \geq b$. 同様に $a \vee b = 1$ なので,

$$a' = a' \wedge 1 = a' \wedge (a \vee b) = (a' \wedge a) \vee (a' \wedge b) = 0 \vee (a' \wedge b) = a' \wedge b$$

よって, $a' \leq b$ となるので,$a' = b$ となる.

$B5$　$a' \wedge a = 0$ かつ $a' \vee a = 1$ が $B3$ と $L2$ より成り立つので,$(a')' = a$ が成り立つ.

$B6$　$\cdot\ (x \vee y) \vee (x' \vee y') = x \vee \{(y \vee x') \wedge (y \vee y')\} = x \vee \{(y \vee x') \wedge 1)\} = (x \vee x') \vee y = 1 \vee y = 1$

$\cdot\ (x \vee y) \wedge (x' \vee y') = \{x \wedge (x' \wedge y')\} \vee \{y \wedge (x' \wedge y')\} = 0 \vee 0 = 0$

2.2　ブール環

定義

環 $R =< R, +, \cdot, -, 0, 1 >$ が $x^2 = x$ を満たすときブール環という.

系

R がブール代数なら,$x+x=0$ かつ $x \cdot y = y \cdot x$ が成り立つ.

証明

任意の $a, b \in R$ に対し, $(a+a)^2 = a+a$ より, $a^2+a^2+a^2+a^2 = a+a$. 仮定より, $a+a+a+a = a+a$. したがって, $a+a=0$

次に, $(a+b)^2 = a+b$ なので, $a^2 + a \cdot b + b \cdot a + b^2 = a+b$ 仮定より, $a^2 = a,\ b^2 = b$ なので, $a + a \cdot b + b \cdot a + b = a+b$. これより, $a \cdot b + b \cdot a = 0$

また, $a \cdot b + a \cdot b = 0$ であることを示したので, $a \cdot b + a \cdot b = a \cdot b + b \cdot a$. したがって, $a \cdot b = b \cdot a$.

定理

環 $R = < R, +, *, -, 0, 1 >$ が $x^2 = x$ を満たすときブール環という.

(a) $B = < B, \vee, \wedge, ', 0, 1 >$ をブール代数とする. $B^{\otimes}$ を代数系 $< B, +, \cdot, -, 0, 1 >$ とする. $a+b = (a \wedge b') \vee (a' \wedge b)$, $a \cdot b = a \wedge b$, $-a = a$ である. $B^{\otimes}$ はブール環である.

(b) $R = < R, +, \cdot, -, 0, 1 >$ をブール環とする. $R^{\otimes}$ を代数系 $< R, \vee, \wedge, ', 0, 1 >$ とする. $a \vee b = a + b + a \cdot b$, $a \wedge b = a \cdot b$, $a' = 1 + a$ である. $R^{\otimes}$ はブール代数である.

(c) B と R を上の定義とすると, $B^{\otimes\otimes} = B$, $R^{\otimes\otimes} = R$.

証明

(a) 任意の $a,\ b,\ c \in B$ を取る.

(I) $B^{\otimes}$ がアーベル群あることを示す.

(i) $$\begin{aligned} a+(b+c) &= [a \wedge \{(b \wedge c') \vee (b' \wedge c)\}] \vee [a' \wedge \{(b \wedge c') \vee (b' \wedge c)\}] \\ &= [a \wedge \{(b \vee c') \wedge (b' \vee c)\}] \vee [a' \wedge \{(b \wedge c') \vee (b' \wedge c)\}] \\ &= (a \wedge b' \wedge c') \vee (a \wedge b \wedge c) \vee (a' \wedge b \wedge c') \vee (a' \wedge b' \wedge c) \\ &= (a \wedge b' \wedge c') \vee (a \wedge b \wedge c) \vee (a' \wedge b \wedge c') \vee (a' \wedge b' \wedge c) \\ &= (a+b)+c \end{aligned}$$

(ii) $a + 0 = (a \wedge 0') \vee (a' \wedge 0) = a \vee 0 = a$

(iii) $a + a = (a \wedge a') \vee (a' \wedge a) = 0 \vee 0 = 0 \because B3$

(iv) $a + b = (a \wedge b') \vee (a' \wedge b) = (a' \wedge b) \vee (a \wedge b') = b + a \because L2$

(II) $a \cdot 1 = a \wedge 1 = a = 1 \wedge a = 1 \cdot a$

(III) $a \cdot (b \cdot c) = a \wedge (b \wedge c) = a \wedge b \wedge c = (a \wedge b) \wedge c = (a \cdot b) \cdot c$

(IV) $a \cdot \{b + c\} = a \wedge \{(b \wedge c') \vee (b' \wedge c)\} = (a \wedge b' \wedge c) \vee (a \wedge b \wedge c')$

$(a \cdot b) + (a \cdot c) = \{(a \wedge b) \wedge (a \wedge c)'\} \vee \{(a \wedge b)' \wedge (a \wedge c)\} = (a \wedge b' \wedge) \vee (a \wedge b \wedge c')$

したがって, $a \cdot (b \cdot c) = (a \cdot b) + (a \cdot c)$.

$B^{\otimes}$ が環であることが示せたので, $a^2 = a$ を示せばよい. $a^2 = a \cdot a = a \wedge a = a$ より明らか.

(b) 任意の $a,\ b,\ c \in L$ を取る.

(I) $< R, \vee, \wedge >$ が分配束であることを示す.

(i) $a \vee (b \vee c) = a + (b \vee c) + a \cdot (b \vee c) = a + b + c + b \cdot c + a \cdot b + a \cdot c + a \cdot b \cdot c$

同様に $(a \vee b) \vee c = a + b + c + b \cdot c + a \cdot b + a \cdot c + a \cdot b \cdot c$ となり ok(結合律)

(ii) $a \vee b = a + b + a \cdot b = b + a + b \cdot a = b \vee a$ (交換律)

(iii) $a \vee (a \wedge b) = a + a \cdot b + a \cdot a \cdot b = a + a \cdot b + a \cdot b = a \because x + x = 0$ (吸収律)

(iv) $a \vee a = a + a + a \cdot a = a$(ベキ等律)

(v) $a \vee (b \wedge c) = a + b \cdot c + a \cdot b \cdot c$

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

したがって, $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ (分配律)

それぞれ $\wedge$ に関しては容易に示せる.

(Ⅱ) $a \wedge 0 = a \cdot 0 = 0,\ a \vee 1 = a + 1 + a \cdot 1 = 1$

(Ⅲ) $a \wedge a' = a \cdot (a + 1) = a + a \cdot a = a + a = 0$

$a \vee a' = a + (1 + a) + a \cdot (1 + a) = a + 1 + a + a + a \cdot a = 1 + a + a = 1$

(c) $B^{\otimes\otimes} = B$ を示す.

(i) $a \cdot b = a \wedge b$

(ii) $1 + a = (1 \wedge a') \vee (1' \wedge a) = a' \vee 0 = a'$

(iii) $a + b + a \cdot b = a + b \cdot (1 + a) = a + b \cdot a' = a \vee (a' \wedge b) = a \wedge b$

(c) $R^{\otimes\otimes} = R$ を示す.

(i) $(a \vee b') \wedge (a' \vee b) = [a \cdot (1 + b)] + [(1 + a) \cdot b] + [a \cdot (1 + b) \cdot (1 + a) \cdot b] = a + b + 0 = a + b$

(ii) $a \wedge b = a \cdot b$

参考文献

[1] A course in Algebra, Ernest Vinberg

[2] ブール代数とその応用, 成島弘・小高明夫

[3] 東京大学工学教程基礎系数学離散数学, 牧野和久

[4] ライブラリ情報学コア・テキスト 2 離散数学-グラフ・束・デザイン・離散確率-, 朝野孝夫

[5] 位相と論理, 田中俊一