－ 離散数学･補足資料④ －

代数系

2011.7/25 徳久雅人

1 代数系とは

集合 $\boldsymbol{X}$ と $\boldsymbol{X}$ における**演算子** ○ の組を ($\boldsymbol{X}$; ○)と書き，**代数系**という．ここで，**演算**とは，**2項演算**のことを指している．2 項演算とは，$\boldsymbol{f}$: $\boldsymbol{X}\times\boldsymbol{X} \rightarrow \boldsymbol{X}$ という関数 $\boldsymbol{f}$ である．たとえば，整数の集合を $\boldsymbol{Z}$ とするとき，($\boldsymbol{Z}$; +)は，整数の足し算という代数系である．

1.1 代数系の性質

集合 $\boldsymbol{X}$ と 2 項演算子 ○, ● に関して次の性質が議論される．なお，$\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in \boldsymbol{X}$ とする．

《1》結合律：$\boldsymbol{u}$ ○（$\boldsymbol{v}$ ○ $\boldsymbol{w}$）＝（$\boldsymbol{u}$ ○ $\boldsymbol{v}$）○ $\boldsymbol{w}$

《2》単位元の存在： $\boldsymbol{u}$ ○ $\boldsymbol{e}$ = $\boldsymbol{e}$ ○ $\boldsymbol{u}$ = $\boldsymbol{u}$ となる $\boldsymbol{e} \in \boldsymbol{X}$ が存在

《3》逆元の存在：$\boldsymbol{u}$ ○ $\boldsymbol{u}^{-1}$ = $\boldsymbol{u}^{-1}$ ○ $\boldsymbol{u}$ = $\boldsymbol{e}$ となる $\boldsymbol{u}^{-1} \in \boldsymbol{X}$ が存在

《4》交換律：$\boldsymbol{u}$ ○ $\boldsymbol{v}$ = $\boldsymbol{v}$ ○ $\boldsymbol{u}$

《5》分配律：$\boldsymbol{u}$ ● ($\boldsymbol{v}$ ○ $\boldsymbol{w}$) = ($\boldsymbol{u}$ ● $\boldsymbol{v}$) ○ ($\boldsymbol{u}$ ● $\boldsymbol{w}$)

($\boldsymbol{u}$ ○ $\boldsymbol{v}$) ● $\boldsymbol{w}$ = ($\boldsymbol{u}$ ● $\boldsymbol{w}$) ○ ($\boldsymbol{v}$ ● $\boldsymbol{w}$)

たとえば，($\boldsymbol{Z}$; +)は，《1》,《2》,《3》,《4》が成り立つ．単位元は 0 であり，$\boldsymbol{u}$ の逆元は $-\boldsymbol{u}$ である．一方，($\boldsymbol{Z}$; −)は，《1》,《2》,《3》は成り立つが,《4》が成り立たない．たとえば，1−2 と 2−1 は等しくないので，整数の引き算は交換律が成り立たない．さらに，正方行列の集合を $\boldsymbol{M}$ とするとき，($\boldsymbol{M}$; ･)は，《1》,《2》は成り立つが,《3》,《4》が成り立たない．正方行列の積において，単位元とは単位行列のことである．逆元，すなわち，逆行列は存在しないことがあるので,《3》は成り立たない．

1.2 群 (p.168)

代数系の性質に基づき代数系の分類をする．群という分類を考える際，1 つの集合と 1 つの演算子，すなわち，($\boldsymbol{X}$; °) に注目する．

表 1 群の分類

#	分類名	満たすべき性質	例
1	半群	《1》	
2	単位的半群（モノイド）	《1》,《2》	正方行列の積
3	群	《1》,《2》,《3》	整数の引き算
4	可換半群	《1》, 《4》	
5	可換モノイド	《1》,《2》, 《4》	整数の積
6	可換群	《1》,《2》,《3》,《4》	実数の積，整数の足し算

1.3 環と体 (p.159)

1 つの集合 X と 2 つの演算子（加法の演算子+と乗法の演算子 •）に注目する．すなわち，($\boldsymbol{X}$; +, •, $\boldsymbol{c}$, $\boldsymbol{e}$) に注目する．ここで，$\boldsymbol{c}$ は加法の単位元，$\boldsymbol{e}$ は乗法の単位元である．

表 2 環と体の条件

#	分類名	満たすべき性質
1	**環**	+ が可換群の性質を持つこと
		$\bullet$ が半群の性質を持つこと
		次の分配律が成立すること
		$\boldsymbol{x} \bullet (\boldsymbol{y} + \boldsymbol{z}) = (\boldsymbol{x} \bullet \boldsymbol{y}) + (\boldsymbol{x} \bullet \boldsymbol{z})$
		$(\boldsymbol{x} + \boldsymbol{y}) \bullet \boldsymbol{z} = (\boldsymbol{x} \bullet \boldsymbol{z}) + (\boldsymbol{y} \bullet \boldsymbol{z})$
2	**可換環**	環であり，かつ，$\bullet$ が可換であること
3	**体**	環であり，かつ，$\bullet$ が群であること

たとえば，整数の集合 $\boldsymbol{Z}$ における加算+と乗算 $\bullet$ は，$(\boldsymbol{Z}; +, \bullet, 0, 1)$ という代数系である．この系は，可換環である．なぜならば，整数の足し算は，《1》,《2》,《3》,《4》を満たすので可換群の性質があり, 整数の乗算は,《1》を満たすので半群の性質があり, そして, 表 2 の分配律が成立するので環である．さらに，整数の乗算は《4》を満たすので可換であるから，$(\boldsymbol{Z}; +, \bullet, 0, 1)$ は可換環である．

正方行列の集合 $\boldsymbol{M}$ における加算と乗算は，$(\boldsymbol{M}; +, \bullet, 0, \boldsymbol{E})$という代数系である．$\boldsymbol{E}$ は単位行列である．この系は，可換ではない環である．

実数の集合 $\boldsymbol{R}$ における代数系 $(\boldsymbol{R}; +, \bullet, 0, 1)$ は，実数の乗算が,《1》,《2》,《3》の性質を持つので群の性質があるので，体である．

一方，$(\boldsymbol{Z}; +, \bullet, 0, 1)$ は，整数の乗算が逆元を持たないので，群の性質が無い．ゆえに，体ではない．

2 ブール代数とは

ブール代数とは，集合 $\boldsymbol{X} = \{0, 1\}$，2 項演算子 $op2 = \{+, \cdot\}$，単項演算子 $op1 = \{\ \overline{\ }\ \}$で定義される代数系である. 演算子の優先順位は, 高いものから低いものへと並べると, $\overline{\ }$, $\cdot$, + の順である．$\boldsymbol{x}, \boldsymbol{y} \in \boldsymbol{X}$ とするとき，各演算子は次のように計算する．

表 3 演算子の計算方法

$\boldsymbol{x}$	$\boldsymbol{y}$	$\boldsymbol{x} + \boldsymbol{y}$	$\boldsymbol{x} \cdot \boldsymbol{y}$	$\overline{\boldsymbol{x}}$
0	0	0	0	1
0	1	1	0	1
1	0	1	0	0
1	1	1	1	0

たとえば，ブール代数の式（**ブール多項式**という） $\boldsymbol{z}_1 = \boldsymbol{x} \cdot \overline{\boldsymbol{y}} + \overline{\boldsymbol{x}} \cdot \boldsymbol{y}$ は，$\boldsymbol{x} \neq \boldsymbol{y}$ のときに 1 となる式である．また $\boldsymbol{z}_2 = \boldsymbol{x} \cdot \boldsymbol{y}$ は，$\boldsymbol{x} = \boldsymbol{y} = 1$ のときに 1 となる式である．ブール代数は, 計算機の基本である．ここに紹介した $\boldsymbol{z}_1$ と $\boldsymbol{z}_2$ は，2 進数の足し算を計算するための式である．2 進数では 1+1=10 である．$\boldsymbol{z}_1$ は 1 桁目，$\boldsymbol{z}_2$ は 2 桁目である．

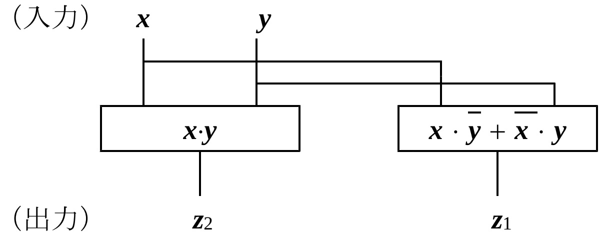

図 1 2 進数の足し算

3 ブール代数の性質

3.1 変形方法

ブール代数は，命題論理と同じように計算できる．すなわち，0 が **F** に， 1 が **T** に対応し，+が ∨ に，· が ∧ に対応する．したがって，ドモルガンの法則などが同様に成り立つ．このことは，真理値表で確認できる．

表 4 ドモルガンの法則

x	y	$\overline{(x+y)}$	$\overline{x}\cdot\overline{y}$	$\overline{(x\cdot y)}$	$\overline{x}+\overline{y}$
0	0	1	1	1	1
0	1	0	0	1	1
1	0	0	0	1	1
1	1	0	0	0	0

3.2 加法標準形と乗法標準形

記号論理で，選言標準形と呼んでいたものに対応するのが，加法標準形である．連言標準形と呼んでいたものに対応するのが，乗法標準形である．

問 1 次のブール代数の式を計算せよ

（1） $0 + 0 =$　（2） $1 + 1 =$　（3） $1 + 0 =$　（4） $\overline{(1 + 0)} =$

（5） $0 + \overline{0} =$　（6） $0 \cdot 0 =$　（7） $1 \cdot 1 =$　（8） $0 \cdot 1 =$

（9） $(1+0)\cdot 1 =$　（10） $(1+1)\cdot(0+0)=$

問 2

（1） ブール代数の代数系を考えよう．集合 $\boldsymbol{B} = \{0, 1\}$とする．ブール代数の加法 + の代数系は，$(\boldsymbol{B};\, +)$ と書く．この系が最も適切に対応する群の分類を，表 1 から選択して述べよ．また，その理由を述べよ．

（2） (1) と同様に，ブール代数の乗法 · の代数系 $(\boldsymbol{B};\, \cdot)$ に最も適切な群の分類を述べよ．また，その理由を述べよ．

（3） ブール代数の代数系 $(\boldsymbol{B};\, +, \cdot)$ は，環，可換環，体と言えるか？ また，その理由を述べよ．

(4) ブール代数においても排他的論理和 ⊕ が定義できる．$0 \oplus 0=0$, $0 \oplus 1=1$, $1 \oplus 0=1$, $1 \oplus 1=1$ である．そこで，($\boldsymbol{B}$; ⊕) に最も適切な群の分類を述べよ．

(5) ブール代数の代数系 ($\boldsymbol{B}$; ⊕, ·)は，環，可換環，体と言えるか？ また，その理由を述べよ．

4 式の作成方法

4.1 真理値表から加法標準形を簡単に作る方法

真理値表で，1 となる行の $\boldsymbol{x}$ や $\boldsymbol{y}$ を参照し，もし 1 ならば $\boldsymbol{x}$ や $\boldsymbol{y}$ とし，0 ならば $\overline{\boldsymbol{x}}$ や $\overline{\boldsymbol{y}}$ として，$\boldsymbol{x}$ や $\boldsymbol{y}$ を積 · で繋ぐ．別の行も同様に積で繋いだものを作り，それらを和+で繋ぐ．

(例) 表 5 の真理値表は，入力が $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$ であり出力が $\boldsymbol{s}$ である．$\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$ を用いて $\boldsymbol{s}$ を表す式を作成しよう．

表 5 練習用の真理値表

$\boldsymbol{x}$	$\boldsymbol{y}$	$\boldsymbol{z}$	$\boldsymbol{s}$
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	0

$\boldsymbol{s} = 1$ となる行より，$\boldsymbol{s} = \overline{\boldsymbol{x}} \cdot \overline{\boldsymbol{y}} \cdot \overline{\boldsymbol{z}} + \overline{\boldsymbol{x}} \cdot \overline{\boldsymbol{y}} \cdot \boldsymbol{z} + \boldsymbol{x} \cdot \overline{\boldsymbol{y}} \cdot \overline{\boldsymbol{z}}$ となる．

ただし，この方法では，式が冗長である．もっと簡単な式がある．冗長さをなくすためには，同値変形を用いる必要がある．

4.2 簡潔な式を作る方法

同値変形は手間がかかる．そこで，真理値表をカルノー図に書き換えてから，加法標準形の式を作る方法がある．

4.2.1 カルノー図の作成

カルノー図では，縦軸と横軸に「00, 01, 11, 10」を並べる．各軸を入力変数と対応させる．図の各マス目には出力変数の値を対応させる．

(例) 表 5 の真理値表からカルノー図を作成しよう．入力変数が 3 つなので，横軸は，「00, 01, 11, 10」とせず，「0,1」とする．

表 6 カルノー図

xy \ z	0	1
0 0	1	1
0 1	0	0
1 1	0	0
1 0	1	0

4.2.2 カルノー図の囲い作り

出力が 1 のマス目が隣接するところを丸で囲む．ここで，囲み方に制約条件がある．囲むとき四角形になるように囲むこと，面積が 1, 2, 4, 8, または 16 になるように囲むこと，である．なお，マス目は上と下は繋がっている，左と右は繋がっていると解釈する．さらに，囲みが重なっても構わない．

（例）表 6 のカルノー図に囲みを入れてみよう．$\boldsymbol{xy} = 00$ の行に注目して，横長に囲む（面積 2）．次に $\boldsymbol{xy} = 00, \boldsymbol{z} = 0$ と $\boldsymbol{xy} = 10, \boldsymbol{z} = 0$ の 2 つのマス目に注目して，縦長に囲む（面積 2）. この 2 マスは, 上下が繋がっていると解釈している. また, $\boldsymbol{xy} = 00$, $\boldsymbol{z} = 0$ のマス目では 2 つの囲みが重なっている．

表 7 囲み付きカルノー図

xy \ z	0	1
0 0	1	1
0 1	0	0
1 1	0	0
1 0	1	0

4.2.3 囲みから式を立てる

囲みを 1 つずつ参照する．囲みに対応する入力変数で，変化の無い変数に基づき，式を立てる．

（例）表 7 の囲みを参照しながら式を立てよう．横長の囲みは，$\boldsymbol{xy} = 00$ であり，$\boldsymbol{z} = 0$ または 1 であるので，変化の無い変数は $\boldsymbol{x}$ と $\boldsymbol{y}$ である．$\boldsymbol{x} = 0, \boldsymbol{y} = 0$ と対応しているので，$\overline{\boldsymbol{x}} \cdot \overline{\boldsymbol{y}}$ という式を立てる．次に縦長の囲みによると，$\boldsymbol{x} = 0$ または 1 なので，$\boldsymbol{x}$ は式に使わない．一方，$\boldsymbol{y} = 0, \boldsymbol{z} = 0$ と変化が無いので，$\overline{\boldsymbol{y}} \cdot \overline{\boldsymbol{z}}$ という式を立てる．以上より，$\boldsymbol{s} = \overline{\boldsymbol{x}} \cdot \overline{\boldsymbol{y}} + \overline{\boldsymbol{y}} \cdot \overline{\boldsymbol{z}}$ となる．

5 カルノー図の囲みの例

出力の変数を s *とする.*

wx \ yz	00	01	11	10
00	0	0	0	0
01	1	1	1	1
11	1	1	0	0
10	0	0	0	0

$s = \overline{w} \cdot x + x \cdot \overline{y}$

wx \ yz	00	01	11	10
00	0	0	1	1
01	0	1	1	1
11	0	0	1	1
10	0	0	1	1

$s = \overline{w} \cdot x \cdot z + y$

wx \ yz	00	01	11	10
00	0	0	1	1
01	0	1	1	1
11	0	1	1	0
10	0	0	0	0

$s = \overline{w} \cdot y + x \cdot z$

wx \ yz	00	01	11	10
00	0	1	1	1
01	0	1	1	1
11	0	1	1	1
10	0	1	1	1

$s = z + y$

トリッキーな囲み方

wx \ yz	00	01	11	10
00	1	0	0	1
01	1	0	0	1
11	1	0	0	1
10	1	0	0	1

$s = \overline{z}$

wx \ yz	00	01	11	10
00	1	0	0	1
01	0	0	0	0
11	0	0	0	0
10	1	0	0	1

$s = \overline{x} \cdot \overline{z}$

wx \ yz	00	01	11	10
00	0	1	0	1
01	1	1	1	1
11	1	0	1	0
10	0	0	0	0

$s = x \cdot \overline{y} \cdot \overline{z} + \overline{w} \cdot \overline{y} \cdot z + x \cdot y \cdot z + \overline{w} \cdot y \cdot \overline{z}$

※ $wx = 01$ の行は囲まない

wx \ yz	00	01	11	10
00	0	1	0	1
01	1	0	1	0
11	0	1	0	1
10	1	0	1	0

$$\begin{aligned} s = {} & \overline{w} \cdot \overline{x} \cdot \overline{y} \cdot z + \overline{w} \cdot \overline{x} \cdot y \cdot \overline{z} \\ & + \overline{w} \cdot x \cdot \overline{y} \cdot \overline{z} + \overline{w} \cdot x \cdot y \cdot z \\ & + w \cdot x \cdot \overline{y} \cdot z + w \cdot x \cdot y \cdot \overline{z} \\ & + w \cdot \overline{x} \cdot \overline{y} \cdot \overline{z} + w \cdot \overline{x} \cdot y \cdot z \end{aligned}$$

※ $s = w \oplus x \oplus y \oplus z$ と同じ

問 3

次のカルノー図から，加法標準形で冗長性の無いブール多項式を作成せよ．出力の変数を $\boldsymbol{s}$ とする．

（1）

$xy \backslash z$	0	1
00	1	0
01	1	0
11	0	0
10	0	1

（2）

$xy \backslash z$	0	1
00	1	0
01	0	0
11	1	0
10	1	0

（3）

$xy \backslash z$	0	1
00	1	1
01	1	1
11	0	1
10	0	1

（4）

$xy \backslash z$	0	1
00	1	1
01	0	1
11	0	1
10	1	1

（5）

$wx \backslash yz$	00	01	11	10
00	1	1	0	0
01	1	0	1	0
11	1	0	0	0
10	1	0	0	0

（6）

$wx \backslash yz$	00	01	11	10
00	1	1	0	0
01	1	1	1	0
11	1	0	0	0
10	1	0	0	1

問の答え

問 1

（1）0　（2）1　（3）1　（4）0　（5）1　（6）0　（7）1　（8）0　（9）1　（10）0

問 2

（1）$(\boldsymbol{B};+)$ は可換モノイドである．

理由：$\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in \boldsymbol{B} = \{0, 1\}$ のとき, $\boldsymbol{x} + (\boldsymbol{y} + \boldsymbol{z}) = (\boldsymbol{x} + \boldsymbol{y}) + \boldsymbol{z}$ なので《1》は成り立つ. $\boldsymbol{x} + 0 = 0 + \boldsymbol{x} = \boldsymbol{x}$ なので 0 が単位元であり《2》は成り立つ．$\boldsymbol{x} + \boldsymbol{y} = \boldsymbol{y} + \boldsymbol{x} = 0$ となる $\boldsymbol{y}$ は存在しないので《3》は成り立たない．$\boldsymbol{x} + \boldsymbol{y} = \boldsymbol{y} + \boldsymbol{x}$ なので《4》は成り立つ.

（2）$(\boldsymbol{B};\cdot)$ は可換モノイドである．

理由：$\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in \boldsymbol{B} = \{0, 1\}$ のとき，$\boldsymbol{x} \cdot (\boldsymbol{y} \cdot \boldsymbol{z}) = (\boldsymbol{x} \cdot \boldsymbol{y}) \cdot \boldsymbol{z}$ なので《1》は成り立つ．$\boldsymbol{x} \cdot 1 = 1 \cdot \boldsymbol{x} = \boldsymbol{x}$ なので 1 が単位元であり《2》は成り立つ．$\boldsymbol{x} \cdot \boldsymbol{y} = \boldsymbol{y} \cdot \boldsymbol{x} = 1$ となる $\boldsymbol{y}$ は存在しないので《3》は成り立たない．$\boldsymbol{x} \cdot \boldsymbol{y} = \boldsymbol{y} \cdot \boldsymbol{x}$ なので《4》は成り立つ.

（3）$(\boldsymbol{B};+,\cdot)$ は，環，可換環，体のいずれでもない．

理由：$(\boldsymbol{B};\ +)$ は，《3》を満たさないので可換群ではない．ゆえに環，可換環，体のいずれでもない．

（4）$(\boldsymbol{B};\oplus)$ は，可換群である．

理由：$\boldsymbol{x} \oplus (\boldsymbol{y} \oplus \boldsymbol{z}) = (\boldsymbol{x} \oplus \boldsymbol{y}) \oplus \boldsymbol{z}$ なので，《1》は成り立つ．$\boldsymbol{x} \oplus 0 = 0 \oplus \boldsymbol{x} = \boldsymbol{x}$ なので，単位元は 0 であり《2》は成り立つ．$\boldsymbol{x} \oplus \boldsymbol{y} = \boldsymbol{y} \oplus \boldsymbol{x} = 0$ となる $\boldsymbol{y}$ は存在する．具体的には，$\boldsymbol{x} = 0$ のとき $\boldsymbol{y} = 0$ が $\boldsymbol{x}$ の逆元であり, $\boldsymbol{x} = 1$ のとき $\boldsymbol{y} = 1$ が $\boldsymbol{x}$ の逆元である．$\boldsymbol{x} \oplus \boldsymbol{y} = \boldsymbol{y} \oplus \boldsymbol{x}$ なので《4》は成り立つ.

（5）$(\boldsymbol{B};\oplus,\cdot,0,1)$ は，可換環である．

理由：$(\boldsymbol{B};\oplus)$ が可換群であり，かつ，$(\boldsymbol{B};\cdot)$ が可換モノイドであり半群の性質を持つ．下記の真理値表より，$\boldsymbol{x}\cdot(\boldsymbol{y} \oplus \boldsymbol{z}) = \boldsymbol{x}\cdot\boldsymbol{y} \oplus \boldsymbol{x}\cdot\boldsymbol{z}$ かつ$(\boldsymbol{x} \oplus \boldsymbol{y})\cdot\boldsymbol{z} = (\boldsymbol{x}\cdot\boldsymbol{z} \oplus \boldsymbol{y}\cdot\boldsymbol{z})$ であるので環である．さらに，$(\boldsymbol{B};\cdot)$ が可換であるので可換環である．

$x\ y\ z$	$y \oplus z$	$x\cdot(y \oplus z)$	$x\cdot y$	$x\cdot z$	$x\cdot y \oplus x\cdot z$	$x \oplus y$	$(x \oplus y)\cdot z$	$x\cdot z$	$y\cdot z$	$x\cdot z \oplus y\cdot z$
0 0 0	0	0	0	0	0	0	0	0	0	0
0 0 1	1	0	0	0	0	0	0	0	0	0
0 1 0	1	0	0	0	0	1	0	0	0	0
0 1 1	0	0	0	0	0	1	1	0	1	1
1 0 0	0	0	0	0	0	1	0	0	0	0
1 0 1	1	1	0	1	1	1	1	1	0	1
1 1 0	1	1	1	0	1	0	0	0	0	0
1 1 1	0	0	1	1	0	0	0	1	1	0

問 3

（1）$s = \overline{x} \cdot \overline{z} + x \cdot \overline{y} \cdot z$　（2）$s = \overline{y} \cdot \overline{z} + x \cdot \overline{z}$　（3）$s = \overline{x} + z$　（4）$s = \overline{y} + z$

（5）$s = \overline{y} \cdot \overline{z} + \overline{w} \cdot \overline{x} \cdot \overline{y} + \overline{w} \cdot x \cdot y \cdot z$　（6）$s = \overline{y} \cdot \overline{z} + \overline{w} \cdot \overline{y} + \overline{w} \cdot x \cdot z + w \cdot \overline{x} \cdot \overline{z}$