

代数系と符号理論 第5回板書プリント

植松友彦 2007.4.27

1 群の続き

1.1 部分群による類別

G を群、 $H = \{h_1 = e, h_2, h_3, \dots, h_n\}$ を G の部分群とすると、任意の $x \in G$ に対し、集合 xH を

$$xH = \{x \circ h_1, x \circ h_2, x \circ h_3, \dots, x \circ h_n\}$$

によって定める。このとき、次の性質が成り立つ。

1. 集合 xH の要素は全て異なる。なぜなら、もしそうでないとすると、ある $i \neq j$ について

$$x \circ h_i = x \circ h_j$$

であり、左から x^{-1} を乗じると $h_i = h_j$ となり、これは仮定 $h_i \neq h_j (i \neq j)$ に矛盾する。

2. $y \notin xH$ ならば $yH \cap xH = \emptyset$ であり、 yH と xH は共通元をもたない。なぜなら、もしそうでないとすると、ある i, j について

$$yH \ni y \circ h_i = x \circ h_j \in xH$$

が成り立つ。右から h_i^{-1} を乗じると

$$(y \circ h_i) \circ h_i^{-1} = (x \circ h_j) \circ h_i^{-1}$$

すなわち

$$y = x \circ (h_j \circ h_i^{-1})$$

となる。ここで、 H は部分群なので、ある $h_k \in H$ が存在して

$$h_k = h_j \circ h_i^{-1}$$

が成り立つ。従って、 $y = x \circ h_k \in xH$ となり、これは $y \notin xH$ に矛盾する。

さて、以上の結果のもとに図のような群 G の類別を考えよう。

H	コセット代表元	$h_1 = e$	h_2	h_3	$\dots$	h_n
g_2H		$g_2 \circ h_1 = g_2$	$g_2 \circ h_2$	$g_2 \circ h_3$	$\dots$	$g_2 \circ h_n$
g_3H		$g_3 \circ h_1 = g_3$	$g_3 \circ h_2$	$g_3 \circ h_3$	$\dots$	$g_3 \circ h_n$
$\vdots$						
g_mH		$g_m \circ h_1 = g_m$	$g_m \circ h_2$	$g_m \circ h_3$	$\dots$	$g_m \circ h_n$

但し、 $g_1 = e$ であり、 g_i ($i = 2, 3, \dots$) は、 $g_1H \cup g_2H \cup \dots \cup g_{i-1}H$ に含まれない G の元である。
このとき、性質 (1) と (2) から、この分類は次のような性質を有する

(a) 全ての G の元は、この表に出現する。(もし、そうでないならば、出現していない g を g_{m+1} としてこの操作を繰り返せば良い)

(b) この表に G の元は唯一回ずつ出現する。

このような類別を H による (左) 類別とよび、各類 g_iH のことを (左) コセットあるいは (左) 剰余類と呼ぶ。また、一番左側の要素 g_i のことをコセット代表元 (コセットリーダー) と呼ぶ。

[例 1] $G = \{1, 2, 3, 4, 5, 6\}$ において、演算 $x \circ y$ を $x \circ y = xy \bmod 7$ で定める。 $H = \{2, 4, 1\}$ とするとき、 H による左類別は、たとえば

H	1	2	4
$3H$	3	6	5

となる。この場合、コセットリーダーは 1 と 3 である。

他方、 $H = \{1, 6\}$ とするとき、 H による左類別は

H	1	6
$2H$	2	5
$3H$	3	4

となる。

[例 2] 2 元体上の 2 元符号

$$C = \{000000, 100110, 010101, 001011, 110011, 101101, 011110, 111000\}$$

による 2 元体上の 6 次元ベクトル空間 G の類別を考えよう。 G は明らかにベクトルの加法について群をなす。また、 C は G の部分群である。従って、部分群 C による類別を行うと、

C	000000	100110	010101	001011	110011	101101	011110	111000
$100000 + C$	100000	000110	110101	101011	010011	001101	111110	011000
$010000 + C$	010000	110110	000101	011011	100011	111101	001110	101000
$001000 + C$	001000	101110	011101	000011	111011	100101	010110	110000
$000100 + C$	000100	100010	010001	001111	110111	101001	011010	111100
$000010 + C$	000010	100100	010111	001001	110001	101111	011100	111010
$000001 + C$	000001	100111	010100	001010	110010	101100	011111	111001
$100001 + C$	100001	000111	110100	101010	010010	001100	111111	011001

が得られる。これは、シンドローム復号法のときに用いたコセットの表に一致する。(第 3 回板書プリント p.5 参照)

このとき次の定理が成り立つ。

[定理 2.2] H が有限群 G の部分群であるならば、 H の位数は G の位数を割り切る。

(証明) 上の類別が m 行 n 列の表になることから明らか。 $\square$

注意: G の位数の任意の約数の位数を持つ部分群が存在するか否かは G によって異なる。(群論の難しさ!)

2 同型写像と群の同型

[定義] 群 G から群 G' への写像 $f: G \rightarrow G'$ について、任意の $x, y \in G$ に対し

$$f(x \circ y) = f(x) \circ f(y)$$

が成り立つとき、 f を準同型写像という。

[定理 2.3] $f: G \rightarrow G'$ を準同型写像とすると、

- (i) $f(e) = e'$ 但し e' は G' の単位元
- (ii) 任意の $x \in G$ に対し、 $f(x^{-1}) = \{f(x)\}^{-1}$

(証明)

(i) $f(e) = f(e \circ e) = f(e) \circ f(e)$ なので、両辺に $\{f(e)\}^{-1}$ を乗じて $e' = f(e)$ を得る。

(ii) $f(x^{-1}) \circ f(x) = f(x^{-1} \circ x) = f(e) = e'$ から $f(x^{-1}) = \{f(x)\}^{-1}$ $\square$

[例 3] G を群とする。 $a \in G$ に対し、整数の加法群 Z からの写像

$$f: Z \rightarrow G, \quad n \mapsto a^n$$

は準同型写像である。なぜならば、

$$a^{m+n} = a^m \circ a^n \iff f(m+n) = f(m) \circ f(n)$$

が成り立つからである。

[定義] 群 G から群 G' の全単射準同型写像 (一対一対応) $f: G \rightarrow G'$ を G から G' への同型写像という。群 G から G' への同型写像が存在するとき、 G と G' は同型であるといい、 $G \cong G'$ と書く。

[例 4] 実数の加法群 R と正の実数全体の乗法群 $R^+ = \{x \in R : x > 0\}$ において、写像

$$f: R \rightarrow R^+, \quad x \mapsto e^x$$

は同型写像である。事実、

$$f(x+y) = e^{x+y} = e^x \cdot e^y = f(x)f(y)$$

であり、 f の逆写像は、

$$f^{-1}: R^+ \rightarrow R, \quad x \mapsto \log_e x$$

である。

[例 5] 乗法群 Z_5^+ と加法群 Z_4 を下記の演算表によって定める。

5 を法とする 0 でない整数の乗法群 Z_5^+

$\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

4 を法とする整数の加法群 Z_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

このとき、 Z_5^+ と Z_4 は同型である。同型写像 $f: Z_5^+ \rightarrow Z_4$ は、

$$f(1) = 0, f(2) = 1, f(3) = 3, f(4) = 2$$

によって定まる。

同型な群は抽象的には同一であり、その相違はただ元の表し方だけである。

[例 6] 位数 n の巡回群 G は、法 n での加法群 G' と同型である。すなわち

$$G = \{a^1, a^2, \dots, a^n = e\}$$

$$G' = \{0, 1, \dots, n-1\}$$

とすれば、写像 $f: G' \rightarrow G$, $f(i) \mapsto a^i$ は、

$$f(i+j) = a^{i+j} = a^i \circ a^j = f(i) \circ f(j)$$

から準同型であり、明らかに f は一対一写像なので、同型写像を与える。

3 環 (ring)

[定義] 環 R は、次の 4 つの性質を満足する 2 種の 2 項演算、加法 $+$ および乗法 $\cdot$ をもつ集合である。

R1 R は加法 $+$ に対して可換群である。

R2 $\forall a, b \in R$ に対し、 $a \cdot b \in R$ (閉包)

R3 $\forall a, b, c \in R$ に対し、 $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (結合則)

R4 $\forall a, b, c \in R$ に対し、

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

$$(b + c) \cdot a = b \cdot a + c \cdot a \quad (\text{分配則})$$

特に、 $\forall a, b \in R$ に対し、 $a \cdot b = b \cdot a$ (可換則) が成り立つとき、可換環 (commutative ring) という。

[定理 2.4] 環 R の加法 $+$ に対する単位元を 0 で表し、 a の逆元を $-a$ によって表す。このとき、任意の $a, b \in R$ に対して次の 2 性質が成り立つ。

$$(1) \quad a \cdot 0 = 0 \cdot a = 0$$

$$(2) \quad a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$$

(証明) (1)

$$a \cdot 0 \stackrel{R1}{=} a \cdot (0 + 0) \stackrel{R4}{=} a \cdot 0 + a \cdot 0$$

両端の式に $-(a \cdot 0)$ を加えると $0 = a \cdot 0$ を得る。 $0 = 0 \cdot a$ も同様。

(2)

$$0 = a \cdot 0 \stackrel{R1}{=} a \cdot (b + (-b)) \stackrel{R4}{=} a \cdot b + a \cdot (-b)$$

両端の式に $-(a \cdot b)$ を加えると $-(a \cdot b) = a \cdot (-b)$ を得る。 $(-a) \cdot b = -(a \cdot b)$ も同様。 $\square$

3.1 環の例

[例 7] 整数の集合 Z は通常の加法と乗法に関して可換環をなす。また乗法に関して単位元 1 をもつ。これを整数環という。同様に、有理数全体の集合 Q 、実数全体の集合 R 、複素数全体の集合 C は通常の加法と乗法に関して可換環である。

[例 8] 整数の集合 $Z_m = \{0, 1, 2, \dots, m-1\}$ は、法 m での加法と乗法について可換環をなす。これを剰余類環という。

[例 9] 整数係数の x の多項式 $a(x)$ の集合は、通常の加法、乗法に関して可換環をなす。乗法に関しての単位元は $a(x) = 1$ である。これを多項式環という。

[例 10] $\{0, 1\}$ は次の演算に関して環をなす。

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \quad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array} \quad \text{または} \quad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 0 \end{array}$$

[例 11] 整数を要素とする 2×2 行列の集合は、通常の行列の加算と乗算に関して環をなす。但し、可換環ではない。

以下では、環 R の加法における単位元を 0 で表す。また、乗法における単位元がもしあれば、 1 で表す。更に乗法単位元を有する環 R において、ある元 $a \in R$ に対し、 $a \cdot b = 1$ となる元 b があれば、 b を a の右逆元といい、 $c \cdot a = 1$ となる元 c があれば、 c を a の左逆元という。

[定理 2.5] 乗法の単位元をもつ環 R について

1. 単位元 1 は唯一である。
2. a が右逆元 b と左逆元 c をもてば、 $b = c$ であり、 a は逆元をもつといい、 a の逆元を a^{-1} で表す。また、逆元は唯一である。
3. $(a^{-1})^{-1} = a$

(証明)

1. 1 と $1'$ を 2 つの異なる乗法単位元とすると、

$$1 = 1 \cdot 1' = 1'$$

から $1 = 1'$ である。

2. $1 = a \cdot b$ であるので、左から c を乗ずると

$$c \cdot 1 = c \cdot a \cdot b = 1 \cdot b$$

すなわち $c = b$ が得られる。また、 a^{-1} を a のもう一つの逆元とすると、

$$a^{-1} = a^{-1} \cdot (a \cdot a'^{-1}) = (a^{-1} \cdot a) \cdot a'^{-1} = a'^{-1}$$

3. $a^{-1} \cdot a = a \cdot a^{-1} = 1$ だから、 a は a^{-1} の逆元である。逆元は唯一なので

$$\frac{(a^{-1})^{-1}}{a^{-1} \text{ の逆元}} = a$$

□

逆元をもつ元を単元あるいはユニット (unit) という。 a, b が単元ならば、 $c = a \cdot b$ もまた単元である。なぜなら、 c の逆元は $c^{-1} = b^{-1} \cdot a^{-1}$ であるからである。従って、全ての単元の集合は乗法のもとで閉じている。

[定理 2.6] 環 R の乗法のもとで、単元の集合は群をなす。

(証明) G1 と G2 は R2 と R3 から自明。G3 は R が乗法の単位元を持たねばならないことから自明。G4 は単元の定義から明らか。 □

[例 12] 整数環において ± 1 のみが単元である。

[例 13] 多項式環において $a(x) = \pm 1$ のみが単元である。

[例 14] 実数を要素とする 2×2 行列は、行列の加法、乗法について環をなす。乗法に関する単位元は単位行列である。また、正則行列は単元である。

3.2 環の準同型写像

2 つの環 R, R' が与えられたとき、写像 $f: R \rightarrow R'$ が次の 2 条件を満たすとき、 R から R' への準同型写像という。

(条件 1) $\forall a, b \in R$ について、

$$f(a + b) = f(a) + f(b)$$

(条件 2) $\forall a, b \in R$ について、

$$f(a \cdot b) = f(a) \cdot f(b)$$

また、写像 f が全単射であるとき、「同型写像」であるといい、環 R と R' は同型であるという。

[例 15] 各整数 a から法 m に関する剰余への写像

$$f: \mathbb{Z} \rightarrow \mathbb{Z}_m, \quad a \mapsto (a \bmod m)$$

は整数環 $\mathbb{Z}$ から剰余数環 $\mathbb{Z}_m$ への準同型写像である。なぜなら、

$$f(a) + f(b) = (a + b) \bmod m = f(a + b)$$

および、

$$f(a \cdot b) = (a \cdot b) \bmod m = ((a \bmod m) \cdot (b \bmod m)) \bmod m = f(a) \cdot f(b)$$

が成り立つからである。