代数系と符号理論　第6回板書プリント

植松友彦 2007.5.8

1　環の続き

1.1　環の準同型写像

2つの環 R, R' が与えられたとき、写像 $f : R \to R'$ 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。

1.2　イデアル (ideal)

準同型写像 $f : R \to R'$ において、$f(a) = f(b)$ となる為の元 $a, b \in R$ の条件を考えよう。準同型の定義から、

$$f(a) = f(b) \longleftrightarrow f(a-b) = 0' \quad (0' \in R')$$

が導かれ、f によって R' の単位元 $0'$ に写像されるような R の元の集合が分れば良い。前節の最後の例 $(a \mapsto a \bmod m)$ では、m の倍数の集合がそのような性質を有していた。このとき、m の倍数の集合は加法と乗法のもとで閉じており、Z の任意の整数の乗法についても閉じている。この概念を一般化したものがイデアルである。

[定義] 環 R の部分集合 I で、次の2つの性質を有するものを（左）イデアルと呼ぶ。

I1 I は R の加法に関して部分群である。

I2 $\forall a \in I, \forall r \in R$ について、$r \cdot a \in I$ である。

[例 **1**] m を正の整数とする。整数環 Z において m の倍数全体の集合

$$\{0, \pm m, \pm 2m, \pm 3m, \cdots\}$$

はイデアルである。

[例 **2**] 多項式環において定数項が 0 であるような多項式全体の集合 I はイデアルである。(x の倍多項式全体の集合はイデアルである。)

[定理 **2.7**] 環 R から環 R' への任意の準同型写像 $f : R \to R'$ において「核 (Kernel)」と呼ばれる集合

$$\mathrm{Ker}f \stackrel{\triangle}{=} \{a \in R : f(a) = 0'\}$$

は R のイデアルである。

(証明) 任意の $a, a' \in \mathrm{Ker}f$ について、

$$f(a + a') = f(a) + f(a') = 0' + 0' = 0'$$

であり、$\mathrm{Ker}f$ の元は加法について閉じている。また、a の逆元 $-a$ は、

$$f(-a) = -f(a) = 0'$$

から、$-a \in \mathrm{Ker}f$ である。従って、$\mathrm{Ker}f$ は加法に関して部分群をなす。

他方、任意の $r \in R$ と任意の $a \in \mathrm{Ker}f$ について、

$$f(r \cdot a) = f(r) \cdot f(a) = f(r) \cdot 0' = 0'$$

から、$r \cdot a \in \mathrm{Ker}f$ である。以上のことから、$\mathrm{Ker}f$ はイデアルである。 □

[定理 **2.8**] 環 R の準同型写像による像

$$\mathrm{Im}f \stackrel{\triangle}{=} \{f(a) : a \in R\}$$

はイデアル $\mathrm{Ker}f$ によって決定する。(但し、同型な環は同一視する。)

(証明) 環 R から環 R' および R'' の上への準同型写像を $f : R \to R'$ および $g : R \to R''$ によって定める。以下では、$f(a) = 0'$ であるときに限り $g(a) = 0''$ ならば、R' と R'' が同型であることを示す。

ある $a \in R$ について、$f(a) = a'$, $g(a) = a''$ のとき、$a' \in R'$ と $a'' \in R''$ が対応するといい、$a' \leftrightarrow a''$ と書くことにする。このとき、この対応 $a' \leftrightarrow a''$ は一対一対応であることを示す。

まず、f は上への写像なので、$\forall a' \in R'$ について、ある $a \in R$ が存在して $f(a) = a'$ となるので、a' は R'' の少なくとも 1 つの元 $a'' = g(a)$ に写像される。

次に、$a' \leftrightarrow a''$ かつ $a' \leftrightarrow b''$ ならば、ある $a, b \in R$ について、

$$f(a) = a',\ g(a) = a'',\ f(b) = a',\ g(b) = b''$$

が成り立つ。すると、$f(a - b) = a' - a' = 0'$。従って、仮定から

$$0'' = g(a - b) = g(a) - g(b) = a'' - b''$$

が得られ、$a'' = b''$ でなければならない。

最後に、この対応は和と積を保存する。なぜなら、$a' \leftrightarrow a''$, $b' \leftrightarrow b''$ ならば、

$$\begin{aligned} a' + b' = f(a + b) \quad &\leftrightarrow \quad g(a + b) = g(a) + g(b) = a'' + b'' \\ a' \cdot b' = f(a \cdot b) \quad &\leftrightarrow \quad g(a \cdot b) = a'' \cdot b'' \end{aligned}$$

となるからである。従って、R' と R'' は同型である。 □

2　整数環とその性質

[定理 **2.9**] $\forall a, b \in Z$ に対し

$$b = aq + r, \quad 0 \leq r < |a|$$

となる $\exists q, r \in Z$ が一意的に定まる。特に、q を商、r を剰余という。

(証明)

$$b = aq_1 + r_1, \quad 0 \leq r_1 < |a|$$
$$b = aq_2 + r_2, \quad 0 \leq r_2 < |a|$$

と 2 通りに定まるとすれば、

$$aq_1 + r_1 = aq_2 + r_2$$
$$a(q_1 - q_2) = r_2 - r_1$$

が得られる。ここで、もし $r_2 - r_1 \neq 0$ ならば、$|r_2 - r_1| < |a|$ から $q_1 - q_2 = 0$ でなければならず、これは $r_2 - r_1 \neq 0$ に矛盾する。従って、$r_1 = r_2$ かつ $q_1 = q_2$ である。　Q.E.D.

以下では、$b = aq + r$ と書くかわりに、$r = R_a[b]$ と書くことにする。すなわち、b を a で割った余りを $R_a[b]$ で表す。

2.1　最大公約数とユークリッドの互除法

[定義] (最大公約数)
整数 a と b の両方を割り切る最大の整数を最大公約数と呼び、(a, b) と書く。特に、$(a, b) = 1$ のとき、a と b を互いに素という。

[定理 **2.10**] 2 つの整数 $\forall a > 0, b > 0 (a \geq b)$ が与えられたとき、$a_0 = a, a_1 = b$ とおき、$n = 1, 2, \cdots$ に対して $a_n > 0$ である限り

$$a_{n-1} = a_n q_n + a_{n+1}, \quad 0 \leq a_{n+1} < a_n$$

によって a_{n+1} を再帰的に定める。このとき、ある自然数 $N (\geq 1)$ が存在し、$a_{N+1} = 0$ かつ $a_N = (a, b)$ である。

[例] $a = 14, b = 6$ とすると

$$a_0 = 14, \quad a_1 = 6$$
$$14 = 2 \times 6 + 2 \implies a_2 = 2$$
$$6 = 3 \times 2 + 0 \implies a_3 = 0$$

従って、$(a, b) = a_2 = 2$。

[系 **1**] 任意の整数 a, b に対し、$(a, b) = xa + yb$ となる整数 x, y の組が存在する。

[例] 33019 と 10947 の最大公約数

$$\begin{array}{r} 3 \\ 10947\overline{)\,33019} \\ \underline{32841} \\ 178 \end{array} \qquad \begin{array}{r} 61 \\ 178\overline{)\,10947} \\ \underline{10680} \\ 267 \\ \underline{178} \\ 89 \end{array} \qquad \begin{array}{r} 2 \\ 89\overline{)\,178} \\ \underline{178} \\ 0 \end{array}$$

従って、$(33019, 10947) = 89$ である。また、このプロセスを行列で表すと

$$\begin{bmatrix} 10947 \\ 178 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & \underline{-3} \end{bmatrix} \begin{bmatrix} 33019 \\ 10947 \end{bmatrix}$$

$$\uparrow \text{商}$$

$$\begin{bmatrix} 178 \\ 89 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -61 \end{bmatrix} \begin{bmatrix} 10947 \\ 178 \end{bmatrix}$$

$$\begin{bmatrix} 89 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} \begin{bmatrix} 178 \\ 89 \end{bmatrix}$$

従って

$$\begin{bmatrix} 89 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} \begin{bmatrix} 178 \\ 89 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -61 \end{bmatrix} \begin{bmatrix} 10947 \\ 178 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & -61 \\ -2 & 123 \end{bmatrix} \begin{bmatrix} 10947 \\ 178 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & -61 \\ -2 & 123 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -3 \end{bmatrix} \begin{bmatrix} 33019 \\ 10947 \end{bmatrix}$$

$$= \begin{bmatrix} -61 & 184 \\ 123 & -371 \end{bmatrix} \begin{bmatrix} 33019 \\ 10947 \end{bmatrix}$$

となり、1 行目から

$$89 = (-61) \times 33019 + 184 \times 10947$$

が分かる。

3 素因数分解の一意性

[定理 **2.11**](素因数分解の一意性)
a を正の整数とし、$a \neq 1$ とする。このとき、a は有限個の正の素数の積に一意的に分解される。すなわち

1. a は有限個の素数の積である。

2. m 個の素数 $p_1, p_2, \cdots, p_m$ と n 個の素数 $q_1, q_2, \cdots, q_n$ について、

$$p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$$

ならば $m = n$ であり、しかも $q_1, q_2, \cdots, q_m$ の順序を適当に入れ換えれば、$p_i = q_i \quad (i = 1, 2, \cdots, m)$ である。

このような定理がなぜ代数系では問題になるのかについて説明するために「偶数世界」というフィクションを次節で述べる。

3.1 偶数世界（ゾーン）

ゾーンという世界では、偶数以外には数が知られていません。ゾーンの世界での数は、

$$E = \{\cdots, -4, -2, 0, 2, 4, 6, \cdots\}$$

だけになります。ゾーンにおいては、偶数の和、差、積は偶数になるので、普通の整数と同様に加法、減法、乗法を定義でき、加法と乗法について「環」になっています。除法も扱えますが、数 m がゾーンで n を割るとは、ある数 $k \in E$ が存在して、$n = mk$ と表せることだとします。例えば、$12 = 2 \cdot 6$ から、6 はゾーンでは 12 を割ります。しかし、6 はゾーンでは 18 を割れません。なぜなら、$18 = 6 \cdot k$ となる偶数 k が存在しないからです。

次にゾーンでの素数を考えましょう。数 $p \in E$ が素数であるとは、どんな数でも割れないことを言います。（注意：ゾーンでは、数はその数自身で割り切れません！）ゾーンでの素数の例は、

$$2, 6, 10, 14, 18, 22, 26, 30, \cdots$$

などです。さて、このゾーンでの因数分解を考えてみましょう。整数 180 は、

$$180 = 6 \cdot 30 = 10 \cdot 18 = 2 \cdot 90$$

と 3 種類の因数分解ができることになってしまいます。ですから、私たちの数の世界での常識は、ゾーンではもはや成り立たなくなっています。

3.2 因数分解の一意性の証明

定理 2.11 の証明に先立ち、補助定理を一つ示す。

[補助定理]　p を素数とし、p は積 ab を割るものとする。このとき、p は a または b のいずれかあるいは両方を割る。

(証明) p が a を割らないと仮定して、p が b を割ることを示す。仮定と p が素数であるから、$(p, a) = 1$ が成り立つ。そこで、[系 1] を用いると

$$px + ay = 1$$

となる整数 x, y が存在する。この式の両辺に b を掛けて

$$bpx + bay = b$$

が得られ、左辺の bpx は p の倍数であり、$(ab)y$ は補助定理の仮定から p で割れるので、b は p で割れなければならない。 □

補助定理を 3 つ以上の整数の積に拡張したのが次の定理である。

[定理 **2.12**] (整数の整除性定理)
p を素数とし、p は積 $a_1a_2\cdots a_n$ を割るものとする。このとき、p は因数 $a_1, a_2, \cdots, a_n$ のなかの少なくとも一つを割る。

証明は各自やってみること。

(定理 2.11 の証明)

1. 帰納法による。$a = 2$ ならば、2 は素数なので 1. が成り立つ。$a < n$ のときに 1. が成り立つとし、$a = n$ のときの成立を示す。n が素数ならば明らかに 1. が成り立つ。n が合成数ならば、ある素数 p が存在して、$n = pn'$ と書ける。このとき、$n' < n$ なので、帰納法の仮定から n' は有限個の素数の積で書ける。従って 1. がいえた。

2. $a = p_1p_2\cdots p_m = q_1q_2\cdots q_n \quad (n \geq m)$ と 2 通りに分解されたとする。p_1 は素数なので、定理 2.12 から p_1 は $q_1 \sim q_n$ のどれかを割り切る。適当に順序を変えて q_1 を割り切るとすると、p_1 と q_1 は素数なので $p_1 = q_1$。

   $$a' = p_2p_3\cdots p_m = q_2q_3\cdots q_n$$

   とすると同様にして、適当に順序を変えて、p_2 は q_2 を割り切り、p_2 と q_2 は素数なので、$p_2 = q_2$。以下、同様にして、$p_3 = q_3, \cdots, p_m = q_n$ となり

   $$1 = q_{m+1}q_{m+2}\cdots q_n$$

   となるので、$n = m$ でなければならない。 □

3.3 体 (Field)

[定義] 体 F は、次の 3 つの性質を満足する 2 つの 2 項演算、加法+および乗法 $\cdot$ をもつ集合である。(教科書 p.21 定義 2.1.1)

F1 F は加法に対して可換群である。(1.-4.)

F2 $\forall a, b \in F$ ならば、$a \cdot b = c \in F$ (閉包) である。また非零元は乗法のもとに可換群をなす。(5.-8.)

F3 $\forall a, b, c \in F$ ならば分配則

$$\begin{aligned} a \cdot (b + c) &= a \cdot b + a \cdot c \\ (b + c) \cdot a &= b \cdot a + c \cdot a \end{aligned}$$

が成り立つ。(9.)

換言すると、乗法に関して単位元 1 をもち、すべての非零元が乗法に関し逆元をもつ可換環が体である。

[例 **1**] すべての実数 (あるいは有理数、複素数) の集合 R(あるいは Q,C) は通常の加法、乗法に関して体をなす。

[例 **2**] 整数の集合 Z は、± 1 以外の元が乗法に関する逆元をもたないので、通常の加法、乗法に関して 体ではない。

集合 S の濃度（位数）すなわち元の個数を $|S|$ によって表す。

[定義] $|S|$ が有限である体をガロア体あるいは有限体といい、要素数 q の有限体を $GF(q)$ あるいは F_q と書く。

位数の等しい有限体は全て同型であり、ガロア体の位数 (元の数)q は必ず $q = p^m$ (p は素数、$m = 1, 2, \cdots$) でなければならない。(証明は後述)

[例 **1**] $\{0, 1\}$ は下記の演算について $GF(2)$ となる。

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

[例 **2**] $\{0, 1, 2\}$ は下記の演算について $GF(3)$ となる。

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

[定理 **2.2.1**] p を素数とし、$S = \{0, 1, \cdots, p-1\}$ とおく、S における加法と乗法を法 p による加算と乗算によって定義する。このとき、$(S, +, \cdot)$ は p 個の元からなる有限体である。

(証明) 公理 1 から 7 までと公理 9 が成り立つことは S が法 p の加算と乗算のもとで可換環をなすことから明らか（既に説明済み)。従って、S の非ゼロの元が逆元を持つことを証明する。

$a \in S$ を非ゼロの元とすると、p は素数だから $(a, p) = 1$ である。ユークリッドの互除法の系 1 から、ある整数 x, y が存在して、

$$xa + yp = (a, p) = 1$$

を満足する。両辺の法 p を取ることで、

$$(x \bmod p) \cdot a = 1 \bmod p$$

が得られ、$x \bmod p$ が a の逆元であることが分る。 Q.E.D.