

代数系と符号理論 (O) 第6回板書プリント

制作：植松友彦

2014.5.21

第5回の復習

- 重み分布と重み分布母関数
- MacWilliams の恒等式
- 群の定義
- (群の) 位数
- 可換群
- 部分群
- 巡回群と生成元
- 元の位数
- 部分群による類別
- 準同型写像
- 同型写像と群の同型

1 環

[定義 7.1] 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 (閉包) 任意の元 $a, b \in R$ に対し、 $a \cdot b \in R$ である。

R3 (結合則) 任意の元 $a, b, c \in R$ に対し、

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

が成り立つ。[注意] 乗法 $\cdot$ について単位元や逆元は存在しなくてもよい。

R4 (分配則) 任意の元 $a, b, c \in R$ に対し、

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

が成り立つ。

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

[例 1] (4 元数) $1, i, j, k$ を基底とする実数 R 上の 4 次元の線形空間

$$H = \{a1 + bi + cj + dk : a, b, c, d \in R\}$$

において、 H の元の積を

$$\begin{aligned}(a1 + bi + cj + dk)(a'1 + b'i + c'j + d'k) \\= (aa' - bb' - cc' - dd')1 + (ab' + ba' + cd' - dc')i \\+ (ac' - bd' + ca' + db')j + (ad' + bc' - cb' + da')k\end{aligned}$$

によって定義する。すなわち、 1 を乗法の単位元、 $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$ が成り立つとすれば、 H は環になる。明らかに H は可換環ではない。尚、4 元数は、数学者ハミルトンが複素数を 3 次元に拡張しようとした際に生まれたものであり、物理学や 3D グラフィクス等で用いられる。

[定義 P.1] (部分環) S を環 R の空でない部分集合とする。 S における加法と乗法を R と同様に定義し、 S が環となっているとき、 S を R の部分環という。

[例 2] 整数環 Z において、偶数全体の集合 S は部分環である。このとき、 Z は乗法単位元 1 をもつが、 S は乗法単位元をもたない。

[例 3] 整数 Z を要素とする n 次元正方行列全体の集合は、通常の加法と乗法に関して環となる。これを Z 上の n 次全行列環といい、 $M_n(Z)$ によって表す。上三角行列全体の集合 S は $M_n(Z)$ の部分環であって、 $M_n(Z)$ と同じ乗法単位元を持つ。

2 準同型写像とイデアル

[定義 7.2] (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。

1. 任意の元 $a, b \in R$ について、

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

2. 任意の元 $a, b \in R$ 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 4] $a \in Z$ とし、写像 $f: Z[x] \rightarrow Z$ を $f(g(x)) \mapsto g(a)$ (a を多項式 $g(x)$ の x に代入する) によって定めると、 f は準同型写像である。なぜならば、

$$\begin{aligned} f(g(x) + h(x)) &= g(a) + h(a) = f(g(x)) + f(h(x)) \\ f(g(x) \cdot h(x)) &= g(a)h(a) = f(g(x)) \cdot f(h(x)) \end{aligned}$$

が成り立つからである。

[定義 7.3] (イデアル) 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¹。

I1 I は R の加法に関して部分群である。

I2 任意の元 $a \in I$ と任意の元 $r \in R$ について、 $r \cdot a \in I$ である。

[例 5] 剰余類環 $Z_4 = \{0, 1, 2, 3\}$ のイデアルを全て求めてみよう。まず、 $\{0\}$ はイデアルであることが容易に分る。また、1 を含むイデアルは、任意の Z_4 の要素を左から 1 に乗じて得られる 0, 1, 2, 3 がそのイデアルに含まれるので、結局 Z_4 自身となる。次に 2 を含む最小のイデアルを考えよう。 Z_4 の任意の要素を左から 2 に乗じると 0 か 2 が得られるので、0 を含まねばならない。ここで、 $\{0, 2\}$ は加法について部分群になっているのでイデアルである。最後に、3 を含む最小のイデアルは、 Z_4 の任意の元を左から 3 に乗じることで 0, 3, 2, 1 が得られるので、 Z_4 に他ならない。以上のことから、 Z_4 のイデアルは、 $\{0\}$, $\{0, 2\}$, Z_4 の 3 種類である。

[例 6] 整数を要素にする 2×2 行列の環において、 $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ という形の行列全体の集合は左イデアルである。なぜなら、この集合が加法について群をなすのは明らか (加法について閉じており、単位元は零行列、行列 M の逆元は $-M$)。また、

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} xa + yb & 0 \\ za + wb & 0 \end{pmatrix}$$

から、イデアルの性質 I2 を満足するからである。同様に、 $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ という形の行列全体の集合は右イデアルである。

3 整数環の性質

[定義 7.4] (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。

4 素因数分解の一意性

[定理 7.7] (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。すなわち以下のことが成り立つ。

¹性質 I2 を $a \cdot r \in I$ で置き換えて得られるものを右イデアルと呼ぶ。可換環では右イデアルと左イデアルは一致する。

1. a は有限個の素数の積である。
2. m 個の素数 $p_1, p_2, \dots, p_m$ と n 個の素数 $q_1, q_2, \dots, q_n$ について、

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

が成り立つならば $m = n$ であり、しかも $q_1, q_2, \dots, q_m$ の順序を適当に入れ換えれば、 $p_i = q_i (i = 1, 2, \dots, m)$ 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述べる。

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ない。ゾーンの世界での数は、

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

だけである。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」になっている。除法については、次のように考える。数 m がゾーンで数 n を割るとは、ある数 $k \in E$ が存在して、 $n = mk$ と表せる場合とする。例えば、 $12 = 2 \cdot 6$ から、6 はゾーンでは 12 を割る。しかし、6 はゾーンでは 18 を割れない。なぜなら、 $18 = 6 \cdot k$ となる偶数 k が存在しないからである。

次にゾーンでの素数を考えよう。数 $p \in E$ が素数であるとは、どんな数でも割れない数のことを言う。(注意：ゾーンでは、数はその数自身で割り切れない!) これから、ゾーンでの素数の例は、

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

となる。さて、このゾーンでの因数分解を考えよう。整数 180 は、

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

と 3 種類の素因数分解ができることになる。従って、我々の数の世界での常識は、ゾーンではもはや成り立たない。

ゾーンの世界で素因数分解が成り立たない要因は、「整数の整除性定理」が成り立たないことにある。上の例では、180 は 2 で割れるが、 $180 (= 6 \cdot 30)$ の因数となっている 6 と 30 は 2 で割れず、整数の整除性が成り立っていない。

一歩先へ (整域とユークリッド整域)

[定義 P.2] (零因子と整域) 一般の環 R において、 $a \neq 0, b \neq 0$ であるが、 $ab = 0$ であるような元 a, b が存在することがある。このような元 a, b を R の「零因子」と呼ぶ。零因子をもたない可換環を「整域」と呼ぶ。

[例 7] 整数環 $\mathbb{Z}$ は整域である。また、整数要素の 2×2 行列の環において、

$$\begin{pmatrix} 1 & -1 \\ 2 & -2 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = O$$

が成り立つので、これらは零因子であり、この環は整域ではない。

[定義 P.3] (ユークリッド整域) 整域 R の非零の各元 a に対して、その大きさと呼ばれる整数 $d(a)(\geq 0)$ が定義され、条件

$$a = b \cdot q + r, \quad r = 0 \text{ または } d(r) < d(b)$$

を満たす $q, r \in R$ が存在するとき (一意でなくてもよい)、 R をユークリッド整域と呼ぶ。すなわち、定理 7.5 が上の意味で成り立つ整域をユークリッド整域という。

[例 8] (ガウスの整数) $Z[i] = \{x + yi | x, y \in Z\}$ をガウスの整数という。 $Z[i]$ における加法と乗法を通常の複素数の加法と乗法によって定めれば、 $Z[i]$ は環である。また、 $d(x + yi) = x^2 + y^2$ と定義すれば、定義 P.3 の条件を満たす $q, r \in Z[i]$ が存在する。実際、与えられた $a, b \in Z[i]$ に対して、 $d(a - z)$ を最小にする格子点 $\{b(m + ni) : m, n \in Z\}$ の元 z を一つ求め、 $r = a - z$ とすれば良い。

[定義 P.4] R を整域とし、 a, b を R の元とする。もし $a = b \cdot q$ となるような $q \in R$ が存在するならば、 a は b で割り切れるという。さらに、 a は b で割り切れかつ b は a で割り切れるならば、 a と b は同伴であるという。

[例 9] ガウスの整数 $Z[i]$ では、単元 $1, -1, i, -i$ は互いに同伴である。任意の $a \in Z[i]$ に対して、 $a, -a, ai, -ai$ もまた互いに同伴である。

[定義 P.5] (素元) R における元 p が素元であるとは、次の 2 条件が満たされることである。

- (1) p は単元ではない。
- (2) a が p を割り切るならば、 a は 1 と同伴か p と同伴である。

[例 10] 整数環 Z の素元は (正の) 素数および素数に -1 を乗じた数である。ガウスの整数 $Z[i]$ においては、 $d(x + yi)$ が素数ならば $x + yi$ は素元である (逆は成り立たない)。なぜならば、もし $x + yi = (a + bi)(c + di)$ と書けるならば、

$$d(x + yi) = d(a + bi)d(c + di)$$

が成り立ち、これは素数なので、 $d(a + bi)$ または $d(c + di)$ は 1 となり、 $a + bi$ と $c + di$ の一方は $1, -1, i, -i$ のいずれかであり 1 と同伴なので、 $x + yi$ は素元でなければならない。他方、 $2 = (1 + i)(1 - i)$ から 2 は素元ではないが、3 は素元である。なぜならば、 $d(3) = 3^2$ であるが、 $d(x + yi) = 3$ となる元が存在しないからである。

[定理 P.1] (ユークリッド整域における素因数分解の一意的性) ユークリッド整域 R では、 R の単元以外の元 $a(\neq 0)$ は、素元の積として、

$$a = p_1 p_2 \cdots p_n$$

と表される。しかも、この分解は順序と同伴の違いを除けば一意的である。

[例 11] ガウスの整数はユークリッド整域なので、任意の元は素元の積として一意的に表せる。

今後の講義日程 (6 月末まで)

6 月 4 日 (水)	講義 8
6 月 10 日 (火)	演習 5
6 月 11 日 (水)	講義 9
6 月 18 日 (水)	試験問題の演習
6 月 24 日 (火)	講義 10
6 月 25 日 (水)	中間試験
7 月 2 日 (水)	演習 6