代数系の基礎要綱 #5

2002–5–23　　河野

群は演算が 1 種類であった。次に整数や実数等のように 2 種類の演算が定義されている代数系を取り扱う。最初は環，次に体を取り上げる。

3　環

定義 3.1 集合 R が**環** (*ring*) であるとは 2 種類の演算 (通常加法・乗法と呼ばれ「$+, \cdot$」と表される) が定義されて次の条件を満たすものをいう。

(1) 演算「$+$」に関し可換群をなす。即ち

1) 演算「$+$」は結合法則を満たす：$(a+b)+c = a+(b+c)$

2) 加法に関する単位元 (零元と呼び 0 で表す) が存在する：$\exists 0 \in R \forall a \in R; a+0 = a0+a$

3) 任意の $a \in R$ に対し逆元 $-a$ が存在する：$\exists -a \in R\, a+(-a) = -a+a = 0$

4) 交換法則が成り立つ：$a+b = b+a$

(2) 演算「$\cdot$」は結合法則を満たす：$(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(3) 分配法則が成り立つ：$a \cdot (b+c) = a \cdot b + a \cdot c$, $(a+b) \cdot c = a \cdot c + b \cdot c$

乗法の単位元が存在するとき，環 R の単位元といい，1 で表す。乗法が可換のとき R を**可換環** (*commutative ring*) と呼ぶ。

R が単位元を持つとき，R の元のなかで乗法の逆元を持つ元を可逆元または単元という。可逆元全体の集合を R^* または $U(R)$ と書く。R^* は乗法に関し群をなす ($\to$ 演習問題 3.1)。

体については次節で扱うが，ここで定義をしておこう。単位元を持つ環 F に対し $F^* = F - \{0\}$ が成立するとき，即ち 0 以外の元がすべて乗法に関する逆元を持つとき F を**体** (*field*) と呼ぶ。

演習問題 3.1　単位元を持つ環 R に対し R^* は乗法に関し群をなす事を示せ。

幾つか例をあげよう。最初は $R = \boldsymbol{Z}$。これが環になることは明らか。単位元を持つ可換環である。$\boldsymbol{Z}^* = \{\pm 1\}$ である。

$R = \boldsymbol{Q}, \boldsymbol{R}, \boldsymbol{C}$ も環である。この場合もっと強く体になっている。

m を 2 以上の自然数とするとき $R = \boldsymbol{Z}_m$ は環である。m が素数のときは体になるが，素数でないときは体ではない。例えば $m = 12$ のとき $\boldsymbol{Z}_{12}^* = \{1, 5, 7, 11\}$ なので $\boldsymbol{Z}_{12}^* \neq \boldsymbol{Z}_{12} - \{0\}$ である。$3 \cdot 4 = 0$ である。このような 3,4 を零因子と呼ぶ。

R を環とする。R の元を係数とする X 変数多項式全体のつくる集合を $R[X]$ と書く。多項式には通常の様に和と積を定義できる。この和と積に関し $R[X]$ が環になることはすぐ分かる。この環を R 上の (1 変数) **多項式環** (*polymonial ring*) という。ここでは $\boldsymbol{Z}_2$ 上の多項式環 $R = \boldsymbol{Z}_2[X]$ を少し具体的に見てみよう。R の定数多項式は $0, 1$ の 2 つである。1 次式は $X, X+1$ の 2 つ，2 次式は

$$X^2,\ X^2+1,\ X^2+X,\ X^2+X+1$$

である。R に於ける計算は，$(X+1)(X^2+X+1) = X^3+1$, $(X^2+1)^2 = X^4+1$ 等となる。$\boldsymbol{R}[X]$ の多項式 X^2+1 は 1 次式の積に分解できないが，$\boldsymbol{Z}_2[X]$ では $X^2+1 = (X+1)(X+1)$ と因数分解できる。$\boldsymbol{Z}_2[X]$ の 2 次式で既約 (1 次式に因数分解できない) なのは X^2+X+1 だけである。

$R = \boldsymbol{Z}_3[X]$ の場合最高次係数が 1 である 2 次式は

$$X^2, X^2+1, X^2+2, X^2+X, X^2+X+1, X^2+X+2, X^2+2X, X^2+2X+1, X^2+2X+2$$

の 9 個存在する。既約なのは X^2+1,X^2+X+2,X^2+2X+2 の 3 個である。

$\boldsymbol{Z}_5[X]$ の場合はどうであろう。実は実際に求めなくても最高次係数が 1 である 2 次の既約多項式の個数は $\dfrac{5^2-5}{2} = 10$ 個ある事が分かる。実は $\boldsymbol{Z}_2[X]$ のときは $\dfrac{2^2-2}{2} = 1$, 実は $\boldsymbol{Z}_3[X]$ のときは $\dfrac{3^2-3}{2} = 3$ が成立している。$\boldsymbol{Z}_2[X]$ で最高次係数が 1 の既約 3 次式の場合は $\dfrac{2^3-2}{3} = 2$ 個ある。この謎解きは有限体を扱ったときに。

演習問題 3.2　$\boldsymbol{Z}_5[X]$ の最高次係数が 1 である既約多項式をすべて求めよ。

整数に 2 次方程式の解を加えた集合を考える。ω を複素数とするとき $\boldsymbol{Z}[\omega] = \{\, a+b\omega \mid\ a,b \in \boldsymbol{Z}\,\}$ とする。一般の ω に対しては環にならないが，$\omega^2 \in R$ の場合は環になる。この環の可逆元の全体 $U(\boldsymbol{Z}[\omega])$ を求めてみよう。最初に $\omega = \dfrac{1+\sqrt{-3}}{2}$ とする。$\omega^2 = -1+\omega$ なので条件を満たしている。任意の元 $\alpha = a+b\omega \in \boldsymbol{Z}[\omega]$ に対し $|\alpha|^2 = \left|(a+\dfrac{b}{2}) + i\dfrac{b\sqrt{3}}{2}\right|^2 = \left(a+\dfrac{b}{2}\right)^2 + \left(\dfrac{b\sqrt{3}}{2}\right)^2 = a^2+ab+b^2$ となるので $\alpha \neq 0$ のときは $|\alpha| \geqq 1$ である。α が単元のとき $\alpha\beta = 1$ となる $\beta \in \boldsymbol{Z}[\omega]$ が存在するので，$|\alpha||\beta| = 1$ より，$|\alpha| = 1$ が分かる。$a^2+ab+b^2 = 1$ となる a, b は $a = \pm 1, 0$, $b = \pm 1, 0$ なので，$U(\boldsymbol{Z}[\omega]) = \{1, -1, \omega, -\omega, \omega-1, -\omega+1\}$ となる。

$\omega = \dfrac{1+\sqrt{-7}}{2}$ とする。$\omega^2 = -2+\omega$ なので条件を満たしている。任意の元 $\alpha = a+b\omega \in \boldsymbol{Z}[\omega]$ に対し $|\alpha|^2 = \left|(a+\dfrac{b}{2}) + i\dfrac{b\sqrt{7}}{2}\right|^2 = \left(a+\dfrac{b}{2}\right)^2 + \left(\dfrac{b\sqrt{7}}{2}\right)^2 = a^2+ab+2b^2$ となるので $\alpha \neq 0$ のときは $|\alpha| \geqq 1$ である。α が単元のとき $\alpha\beta = 1$ となる $\beta \in \boldsymbol{Z}[\omega]$ が存在するので，$|\alpha||\beta| = 1$ より，$|\alpha| = 1$ が分かる。$a^2+ab+2b^2 = 1$ となる a, b は $a = \pm 1, 0$, $b = \pm 1, 0$ なので，$U(\boldsymbol{Z}[\omega]) = \{1, -1\}$ となる。

今までの例は積も可換であった。最後に可換でない例をあげておく。実数を係数とする 2 次行列全体の集合を $M(2, \boldsymbol{R})$ と書くと，行列の和と積に関し環をなす。この環は単位元は持つが可換ではない。

演習問題 3.3　次の環 R の単元全体の集合 $U(R)$ を求めよ。

(1) $R = \boldsymbol{Z}[i] = \{\, a+ib \mid\ a,b \in \boldsymbol{Z}\,\}$　(i は虚数単位)

(2) $R = \boldsymbol{Z}[\sqrt{2}] = \left\{\, a+b\sqrt{2} \,\middle|\ a,b \in \boldsymbol{Z}\,\right\}$

演習問題 3.4　多項式 $X^4 - X^2 + 1$ が次の R を係数とする多項式環で因数分解される事を示せ。

(1) $R = \left\{\, a+b\sqrt{-1} \,\middle|\ a,b \in \boldsymbol{Z}\,\right\}$

(2) $R = \{\, a+b\omega \mid\ a,b \in \boldsymbol{Z}\,\}$　$(\omega = \dfrac{-1+\sqrt{-3}}{2})$

(3) $R = \left\{\, a+b\sqrt{3} \,\middle|\ a,b \in \boldsymbol{Z}\,\right\}$