代数学入門

花木 章秀

2007 年前期
(2007/11/06)

目次

Chapter 3

環と体

3.1 定義と例

集合 R 上に加法と乗法が定義されているとする。R が**環** (ring) であるとは

(R1) R は加法に関して加群である。

(R2) R は乗法に関して半群である。

(R3) [**分配法則**] 任意の $a, b, c \in R$ について $a(b+c) = ab + ac$, $(a+b)c = ac + bc$ が成り立つ。

を満たすことをいう。更に

(R4) [**単位元の存在**] 乗法に関する単位元 $1_R (\neq 0)$ が存在する。

が成り立つとき、R を**単位元をもつ環**という。
(R1), (R2), (R3) が成り立ち、かつ

(R5) [**交換法則**] 任意の $a, b \in R$ に対して $ab = ba$ が成り立つ。

が満たされるとき R を**可換環** (commutative ring) という。
環 R の加法に関する単位元を**零元**といい 0 または 0_R と書く。R が単位元をもつ環であるとき、乗法に関する単位元を単に**単位元**といい 1 または 1_R と書く。

問 3.1.1. 環 R の任意の元 x について $0x = x0 = 0$ であることを示せ。(この 0 は R の加群としての単位元 0_R のことで、$0_{\mathbb{Z}} \in \mathbb{Z}$ とは違う意味である。しかしこの問題によって $0_R x$ と $0_{\mathbb{Z}} x$ を区別する必要はなくなる。)

R が単位元をもつ環のとき、R は乗法についてモノイドであるから、その単数群 $U(R)$ が考えられる。$U(R)$ を環 R の**単数群** (unit group) といい、その元を R の**正則元**、または**単数** (unit) という。(正則元を扱うときには常に、考える環が単位元をもつと仮定する。)
単位元をもつ環 R において、0 以外のすべての元が正則元であるとき R を**斜体** (skew field, division ring) という。特に可換な斜体を**体** (field)、または**可換体** (commutative field) という。

例 3.1.2 (零環)**.** ただ一つの元 a をもつ集合に $a+a=a$, $aa=a$ で演算を定めれば、これは環になる。これを**零環**という。零環は単位元をもたない。

例 3.1.3 (有理整数環)**.** $\mathbb{Z}$ は通常の加法と乗法で単位元をもつ可換環である。これを**有理整数環** (rational integer ring) という。

例 3.1.4 (有理数体、実数体、複素数体)**.** $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ は通常の加法と乗法で体である。これをそれぞれ**有理数体** (rational number field)、**実数体** (real number field)、**複素数体** (complex number field) という。

例 3.1.5 (全行列環)**.** R を (可換とは限らない) 環とする。R の元を成分とする n 次正方行列の全体は通常の演算で環になる。これを R 上 n 次の**全行列環** (full matrix ring) といい $M(n,R)$、または $M_n(R)$ と書く。R が単位元をもてば $M(n,R)$ も単位元をもつ。

R を環とする。$0\neq a\in R$ が R の**左零因子** (left zero divisor) であるとは、ある $0\neq b\in R$ が存在して $ab=0$ となることである。同様に $0\neq a\in R$ が R の**右零因子** (right zero divisor) であるとは、ある $0\neq b\in R$ が存在して $ba=0$ となることである。0 は左 (右) 零因子とはいわないことにする。

命題 3.1.6. 単位元をもつ環 R の正則元は左 (右) 零因子ではない。特に R が斜体ならば R に左 (右) 零因子は存在しない。

証明. a を正則元であり、かつ左零因子であるとする。ある $0\neq b\in R$ が存在して $ab=0$ である。このとき

$$b=1b=a^{-1}ab=a^{-1}0=0$$

となり $b\neq 0$ に矛盾する。 □

R が可換環であるときには a が左零因子であることと、右零因子であることは同値であり、左右の区別をする必要がない。このとき a を単に**零因子** (zero divisor) という。

単位元をもつ可換環 R が**整域** (integral domain) であるとは、R に零因子が存在しないことである。

例 3.1.7. 体は整域である。また有理整数環 $\mathbb{Z}$ は体ではないが整域である。

問 3.1.8. A を整域とし、集合として有限集合であるとする。このとき A は体になることを示せ。

問 3.1.9. 有理整数環 $\mathbb{Z}$ 上の全行列環 $M(n,\mathbb{Z})$ の単数はどの様なものか決定せよ。

3.2 整数の合同によって定義される環

$n\in\mathbb{N}$, $n\geq 2$ を一つ固定する。前と同じように $a,b\in\mathbb{Z}$ に対して、ある $\ell\in\mathbb{Z}$ が存在して $a-b=n\ell$ となるとき $a\equiv b \pmod n$ と書くことにする (問 **??**)。このときこの関係は同値関係である。その a を含む同値類は

$$a+n\mathbb{Z}=\{b\in\mathbb{Z}\mid a\equiv b \pmod n\}=\{a+n\ell\mid \ell\in\mathbb{Z}\}$$

であった。異なる同値類全体の集合は

$$\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z},\ 1 + n\mathbb{Z},\ \cdots,\ (n-1) + n\mathbb{Z}\}$$

である。例 **??** で $\mathbb{Z}/n\mathbb{Z}$ は加群 $\mathbb{Z}$ の部分加群 $n\mathbb{Z}$ による剰余群で

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z}$$

で加法が矛盾なく定義できることを見た。同じように

$$(a + n\mathbb{Z})(b + n\mathbb{Z}) = ab + n\mathbb{Z}$$

で $\mathbb{Z}/n\mathbb{Z}$ に乗法が矛盾なく定義できることを確認する。

$a + n\mathbb{Z} = a' + n\mathbb{Z}$, $b + n\mathbb{Z} = b' + n\mathbb{Z}$ とする。ある $\ell, \ell' \in \mathbb{Z}$ が存在して $a' = a + n\ell$, $b' = b + n\ell'$ である。このとき

$$a'b' = (a + n\ell)(b + n\ell') = ab + n(a\ell' + b\ell + n\ell\ell') \in ab + n\mathbb{Z}$$

であるから $a'b' + n\mathbb{Z} = ab + n\mathbb{Z}$ であり、乗法は矛盾なく定義される。

$\mathbb{Z}/n\mathbb{Z}$ は加群であり、乗法については $1 + n\mathbb{Z}$ を単位元とするモノイドである。また分配法則、交換法則が成り立つことは容易に確かめられ、したがって $\mathbb{Z}/n\mathbb{Z}$ は可換環の構造を持つ。以下では文脈から n が明らかなときには $a + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ を $\bar{a}$ とも書くことにする。$\mathbb{Z}/n\mathbb{Z}$ の単数、および零因子を考える。

例 3.2.1. $\mathbb{Z}/9\mathbb{Z}$ を考える。乗法に関する演算表は以下のようになる。

	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

行に 1 を含むものが単数で、0 との積以外に 0 を含むものが零因子である。したがって単数群は $U(\mathbb{Z}/9\mathbb{Z}) = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$ であり、零因子は $\bar{3}, \bar{6}$ である。単数どうしの積は、また単数であることも確認しておこう。

一般の場合を扱うために以下の定理を用意する。

定理 3.2.2. $a, b \in \mathbb{N}$ とする。$\gcd(a, b) = d$ であるならば、ある $x, y \in \mathbb{Z}$ が存在して

$$ax + by = d$$

となる。

証明. $a > b$ と仮定してかまわない。このとき b に関する帰納法で示す。$b = 1$ ならば $\gcd(a, b) = 1$ で $x = 0$, $y = 1$ とすればよい。$b > 1$ とする。

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

なる $q, r \in \mathbb{Z}$ が存在する。

$\gcd(a, b) = \gcd(b, r)$ であることを示す。$d \mid b$ とする。このとき $d \mid a$ ならば $d \mid a - bq = r$ である。また $d \mid r$ ならば $d \mid bq + r = a$ である。よって d が a, b の公約数であることと b, r の公約数であることは同値である。したがって $\gcd(a, b) = \gcd(b, r)$ が成り立つ。

$r = 0$ ならば $\gcd(a, b) = \gcd(b, 0) = b$ で $x = 0$, $y = 1$ とすればよい。

$d = \gcd(a, b)$ とおく。$0 < r$ とすれば $b > r$ なので b, r に帰納法の仮定を適用することができ、ある $x', y' \in \mathbb{Z}$ が存在して $bx' + ry' = d$ となる。このとき

$$d = bx' + ry' = bx' + (a - bq)y' = ay' + b(x' - qy')$$

となるから $x = y'$, $y = x' - qy'$ とおけばよい。 □

この定理を用いて、一般の $\mathbb{Z}/n\mathbb{Z}$ の単数を決定することができる。

定理 3.2.3. $a + n\mathbb{Z}$ が $\mathbb{Z}/n\mathbb{Z}$ の単数であるための必要十分条件は $\gcd(a, n) = 1$ となることである。すなわち

$$U(\mathbb{Z}/n\mathbb{Z}) = \{a + n\mathbb{Z} \mid \gcd(a, n) = 1\}$$

である。

証明. $\gcd(a, n) = 1$ とする。このとき定理 3.2.2 より、ある $x, y \in \mathbb{Z}$ が存在して $ax + ny = 1$ である。この両辺を n を法として考えれば $\bar{a}\,\bar{x} = \bar{1}$ となり $\bar{a}$ は単数である。

$\bar{a}$ が単数であるとする。ある $b \in \mathbb{Z}$ が存在して $\bar{a}\,\bar{b} = \bar{1}$ である。したがって $\ell \in \mathbb{Z}$ が存在して $ab - 1 = n\ell$ である。変形して $1 = ab - n\ell$ を得る。この式の右辺は $\gcd(a, n)$ で割り切れるので、左辺の 1 も $\gcd(a, n)$ で割り切れ $\gcd(a, n) = 1$ となる。 □

次に $\mathbb{Z}/n\mathbb{Z}$ の零因子を決定しよう。

定理 3.2.4. $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ について以下の条件は同値である。

(1) $\bar{a}$ は零因子である。

(2) $\bar{a}$ は単数ではない。

(3) $\gcd(a, n) > 1$ である。

証明. (2) $\Longleftrightarrow$ (3) は定理 3.2.3 で示されている。零因子は単数ではないので (1) $\Longrightarrow$ (2) も成り立つ。

(3) $\Longrightarrow$ (1) $\gcd(a, n) = d > 1$ とする。このとき $n = d\ell$ とすれば $1 < \ell < n$ となる。$a = da'$ とすれば $\bar{\ell} \neq \bar{0}$ であって $\bar{a}\,\bar{\ell} = \bar{a'}\,\bar{n} = \bar{0}$ となる。よって $\bar{a}$ は零因子である。 □

定理 3.2.5. $\mathbb{Z}/n\mathbb{Z}$ について以下の条件は同値である。

(1) $\mathbb{Z}/n\mathbb{Z}$ は体である。

(2) $\mathbb{Z}/n\mathbb{Z}$ は整域である。

(3) n は素数である。

証明. 前の定理より (1) $\Longleftrightarrow$ (2) が成り立つ。

(3) $\Longrightarrow$ (1) n が素数ならば、任意の $1 \leq a < n$ に対して $\gcd(a, n) = 1$ であるから $\bar{a}$ は単数であり $\mathbb{Z}/n\mathbb{Z}$ は体である。

(1) $\Longrightarrow$ (3) $\mathbb{Z}/n\mathbb{Z}$ が体ならば、任意の $1 \leq a < n$ に対して $\gcd(a, n) = 1$ でなくてはならず n は素数である。 □

問 3.2.6. 全行列環 $M_2(\mathbb{Z}/2\mathbb{Z})$ の元をすべて書け。またその単数群を決定せよ。

3.3 部分環

R を環とする。R の部分集合 S が R の**部分環** (subring) であるとは

- $a, b \in S$ ならば $a - b \in S$, $ab \in S$ である。

を満たすこととする。S が R の部分環であるとき S 自身は 環である。

例 3.3.1. $\mathbb{Z}$ は $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ の部分環である。

例 3.3.2. $R = M(n, \mathbb{R})$ とする。

$$S = \{(a_{ij}) \in R \mid i > j \text{ ならば } a_{ij} = 0\} = \left\{ \left(\begin{array}{cccc} a_{11} & a_{12} & \cdots & a_{1n} \\ & a_{22} & \cdots & a_{2n} \\ & & \ddots & \vdots \\ 0 & & & a_{nn} \end{array} \right) \middle| \, a_{ij} \in \mathbb{R} \right\}$$

とおけば S は R の部分環であることを確認する。

$A = (a_{ij}), B = (b_{ij}) \in S$ とする。$A - B \in S$ は明らかであるから $AB \in S$ を示せばよい。$AB = (c_{ij})$ とおくと

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$$

である。$i > j$ とする。$i > k$ ならば $a_{ik} = 0$ で $k > j$ ならば $b_{kj} = 0$ である。よって $i \leq k \leq j$ のときのみ $a_{ik} b_{kj} \neq 0$ となり得るが $i > j$ であるから、すべての k に対して $a_{ik} b_{kj} = 0$ であり $c_{ij} = 0$ となる。よって $AB \in S$ である。

この例の S が環になることを定義から直接示すのは、いろいろな条件を満たすことを確かめなければならず、なかなか大変である。しかし R の部分集合で、その演算も R の演算を用いて定義されているため、部分環であることを示しさえすれば S 自身が環であることを示すことができる。一般の場合にも、ある集合がある演算で環になることを示したいときには、それが良く知られた環の部分集合として得られていないかどうかを考えることが有効であることが多い。

例 3.3.3. 可換環 $\mathbb{Z}/6\mathbb{Z}$ とその部分集合 $S = \{\bar{0}, \bar{2}, \bar{4}\}$ を考える。このとき S は部分環になる。$\mathbb{Z}/6\mathbb{Z}$ は単位元 $\bar{1}$ をもち、S は単位元 $\bar{4}$ をもつ。このように部分環と元の環の単位元は必ずしも一致しない。

問 3.3.4. $R = M(2, \mathbb{R})$ の部分集合

$$S = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \middle| \, a, b \in \mathbb{R} \right\}$$

は R の部分環であることを示せ。

3.4 イデアルと剰余環

群 G とその正規部分群 N に対して、剰余群 G/N を定義することができた。同様に、環 R のその “ある性質” を満たす部分集合 I に対して、剰余環 R/I を定義することを考える。どのような性質を持つ I に対して剰余環は定義できるのであろうか。

> 多くの場合、数学のテキストや講義では、まずある概念の定義を与え、その後でいろいろな性質などを学ぶ。しかし実際には後の議論がうまくいくように定義を行っているのであり、思考の順序と学ぶ順序は逆になっている。ここではどの様な思考から定義が行われるのかを見てみよう。

まず、R/I を定義するために同値関係が必要である。そこで $a, b \in R$ に対して、関係 $a \sim b$ を $a - b \in I$ となることで定め、$\sim$ が同値関係になるための条件を考える。

- 任意の $a \in R$ に対して $a \sim a$ となるためには $0 = a - a \in I$ が必要十分である。
- 「$a \sim b$ ならば $b \sim a$」が成り立つためには「$a - b \in I$ ならば $-(a-b) = b - a \in I$」となることが必要十分で、さらにこれは「$a \in I$ ならば $-a \in I$」となることと同値である。
- 「$a \sim b$, $b \sim c$ ならば $a \sim c$」が成り立つには「$a - b \in I$, $b - c \in I$ ならば $(a - b) + (b - c) = a - c \in I$」となることが必要十分で、さらにこれは「$a \in I$, $b \in I$ ならば $a + b \in I$」となることと同値である。

以上より $\sim$ が同値関係になることと I が R の部分加群であることは同値である。これによって同値類の集合 $R/I = \{r + I \mid r \in R\}$ が考えられる。

I を R の部分加群とし、R/I における演算を

$$\begin{aligned} (s + I) + (t + I) &= (s + t) + I \\ (s + I)(t + I) &= st + I \end{aligned}$$

で定め、この演算が矛盾なく定義されるような条件を考える。まず加法については加群とその部分加群による剰余群となっているので問題ない。乗法について考える。

- $s+I=s'+I$, $t+I=t'+I$ とする。$st+I=s't'+I$ となる条件を考えればよい。ある $i,i'\in I$ が存在して $s'=s+i$, $t'=t+i'$ である。このとき

$$s't'=(s+i)(t+i')=st+it+si'+ii'$$

である。$i=0$ とすれば $si'\in I$ でなければならない。$i'=0$ とすれば $it\in I$ でなければならない。よって乗法が矛盾なく定義されるためには「$s\in R$, $i\in I$ ならば $si\in I$」かつ「$t\in R$, $i\in I$ ならば $it\in I$」が成り立つことが必要十分である。

以上より、R/I に加法と乗法が矛盾なく定義されるためには

(I1) $a,b\in I$ ならば $a-b\in I$ である。

(I2) $s\in R$, $i\in I$ ならば $si\in I$ である。

(I3) $s\in R$, $i\in I$ ならば $is\in I$ である。

が成り立つことが必要十分である。乗法に関する結合法則、左右の分配法則が成り立つことは容易に確かめられ R/I は環になる。これを R の I による**剰余環** (factor ring) という。またこのとき I を R の**イデアル** (ideal) という。(I1), (I2) を満たす集合 I は**左イデアル** (left ideal) とよばれ、(I1), (I3) を満たす集合 I は**右イデアル** (right ideal) とよばれる。イデアルを左 (右) イデアルと区別するために**両側イデアル** (two-sided ideal) ともいう。

問 3.4.1. $n\in\mathbb{N}$ に対して $n\mathbb{Z}=\{n\ell\mid\ell\in\mathbb{Z}\}$ は $\mathbb{Z}$ のイデアルであることを示せ。(このときの剰余環が $\mathbb{Z}/n\mathbb{Z}$ である。)

問 3.4.2.

$$R=\left\{\begin{pmatrix}a&b\\0&c\end{pmatrix}\,\middle|\,a,b,c\in\mathbb{R}\right\},\quad I=\left\{\begin{pmatrix}0&b\\0&0\end{pmatrix}\,\middle|\,b\in\mathbb{R}\right\}$$

とおくと I は R のイデアルであることを示せ。

環 R において、R 自身と $\{0_R\}$ は R のイデアルである。これを R の**自明なイデアル** (trivial ideal) という。

問 3.4.3. 単位元を持つ環 R とそのイデアル I について、$I=R$ であることと $1_R\in I$ であることは同値である。これを示せ。

問 3.4.4. R を可換環とし $a\in R$ とする。$aR=\{ar\mid r\in R\}$ は R のイデアルであることを示せ。(この aR を a で生成される**単項イデアル** (principal ideal) という。)

問 3.4.5. R を可換でない環とし $a\in R$ とする。$\{r_1ar_2\mid r_1,r_2\in R\}$ は R のイデアルとは限らないことを示せ。また a を含むイデアルのうち、最小のものは何かを考えよ。

3.5 多項式環

R を可換環とする。R の元を係数とする文字 x の整式

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \quad (a_i \in R)$$

を x に関する R 上の**多項式** (polynomial) という。$f(x)$ を単に f とも書く。x を**不定元** (indeterminate) または**変数**という。不定元 x に関する R 上の多項式全体の集合を $R[x]$ と書く。

$R[x]$ における加法と乗法を通常の場合と同じように定義する。すなわち、加法は

$$f(x) = a_0 + a_1x + \cdots + a_nx^n, \quad g(x) = b_0 + b_1x + \cdots + b_mx^m$$

に対して

$$f(x) + g(x) = \sum_{i=0}^{\ell}(a_i + b_i)x^i$$

である。ただし $\ell = \max(n, m)$ で、定義されていない係数は 0 とする。また乗法は

$$f(x)g(x) = \sum_{k=0}^{n+m} c_kx^k, \quad c_k = \sum_{i+j=k} a_ib_j$$

とする。これによって $R[x]$ は可換環となる。これを x に関する R 上の**多項式環** (polynomial ring) という。

$f(x) = a_0 + a_1x + \cdots + a_nx^n$ において $a_n \neq 0$ のとき、n を $f(x)$ の**次数** (degree) といい $\deg f(x)$ または $\deg f$ と書く。$f(x) = 0$ のときには、形式的に $\deg 0 = -\infty$ とする。非負整数 d、または $d = -\infty$ に対して $-\infty \leq d$, $-\infty + d = -\infty$ とする。

以下では R を整域とする。$f(x),\ g(x) \in R[x]$ に対して

$$\begin{aligned} \deg(f+g) &\leq \max(\deg f,\ \deg g) \\ \deg(fg) &= \deg f + \deg g \end{aligned}$$

が成り立つ。特に $f(x) \neq 0$, $g(x) \neq 0$ ならば $f(x)g(x) \neq 0$ であり、$R[x]$ は整域である。$\deg f(x) = 0$ である $f(x)$、または $f(x) = 0$ は R の元と思うことができ、これによって $R \subset R[x]$ とみなす。

問 3.5.1. 整域でない R と $\deg(fg) < \deg f + \deg g$ となるような $f(x), g(x) \in R[x]$ の例を具体的にあげよ。

定理 3.5.2. R を整域とする。$f(x),\ g(x) \in R[x]$ に対して $g(x)$ の最高次の係数が R の正則元であるならば、ある $q(x),\ r(x) \in R[x]$ が存在して

$$f(x) = g(x)q(x) + r(x), \quad \deg r < \deg g$$

と一意的に表される。

証明. $f(x) = a_0 + a_1x + \cdots + a_nx^n$, $g(x) = b_0 + b_1x + \cdots + b_mx^m$ とする。まず $q(x)$, $r(x)$ の存在を $n = \deg f$ に関する帰納法で示す。$g(x) \neq 0$ であるから $\deg g \geq 0$ である。$n = \infty$、または $n < m$ のときは $q(x) = 0$, $r(x) = g(x)$ とすればよい。$n \geq m$ とする。$h(x) = f(x) - a_n{b_m}^{-1}x^{n-m}g(x)$ とおくと $\deg h < n$ で、帰納法の仮定より

$$h(x) = g(x)q_1(x) + r(x), \quad \deg r < \deg g$$

なる $q_1(x), r(x) \in R[x]$ が存在する。このとき

$$f(x) = h(x) + a_n{b_m}^{-1}x^{n-m}g(x) = g(x)(q_1(x) + a_n{b_m}^{-1}x^{n-m}) + r(x)$$

となり、これは求める式である。

次に一意性を示す。

$$f(x) = g(x)q(x) + r(x) = g(x)q'(x) + r'(x), \quad \deg r, \deg r' < \deg g$$

と仮定する。このとき

$$g(x)(q(x) - q'(x)) = r'(x) - r(x)$$

である。$q(x) \neq q'(x)$ であるならば、左辺の次数は $\deg g$ 以上であり、右辺の次数は $\deg g$ 未満である。これは矛盾なので $q(x) = q'(x)$、よって $r(x) = r'(x)$ も成り立ち記述の一意性が示される。 □

この定理は特に

- R が体であるとき、
- $g(x)$ の最高次係数が 1 であるとき、

に適用できる。最高次係数が 1 である多項式を**モニック** (monic) な多項式という。

定理 3.5.2 の $q(x)$, $r(x)$ を、それぞれ $f(x)$ を $g(x)$ で割ったときの**商**、**余り**という。特に $r(x) = 0$ のとき $f(x)$ は $g(x)$ で**割り切れる**といい $g(x) \mid f(x)$ と書く。

$f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$ と $\alpha \in R$ に対して

$$f(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n \in R$$

を $f(x)$ に α を**代入した値**という。$f(\alpha) = 0$ であるとき α は $f(x)$ の**根** (root) であるという。

定理 3.5.3. R を整域とし $f(x) \in R[x]$, $\alpha \in R$ とするとき以下が成り立つ。

(1) [**剰余定理**] ある $q(x) \in R[x]$ が存在して $f(x) = (x - \alpha)q(x) + f(\alpha)$ となる。

(2) [**因数定理**] $f(\alpha) = 0$ であるための必要十分条件は $x - \alpha \mid f(x)$ となることである。

証明. $f(x)$ と $g(x) = x - \alpha$ に定理 3.5.2 を適用すれば、ある $q(x)$, $r(x) \in R[x]$ が存在して

$$f(x) = (x - \alpha)q(x) + r(x), \quad \deg r < \deg(x - \alpha) = 1$$

である。よって $r(x) = r \in R$ である。この両辺に α を代入すれば $f(\alpha) = r$ である。よって剰余定理が成り立つ。

因数定理は剰余定理からすぐに分かる。 □

命題 3.5.4. R を整域とし $0 \neq f(x) \in R[x]$, $\deg f = n$ とする。このとき $f(x)$ の相異なる根は n 個以下である。

証明. n に関する帰納法で示す。$n = 0$ のときは $f(x) = r \neq 0$ で、根は 0 個である。よって命題は成り立つ。

$n \geq 1$ とする。$f(x)$ に根が存在しなければ命題は成立する。よって $f(x)$ に根が存在すると仮定してよく、α を一つの根とする。このとき

$$f(x) = (x - \alpha)g(x)$$

となる $g(x) \in R[x]$ が存在し $\deg g = n - 1$ である。帰納法の仮定より $g(x)$ の根は高々 $n - 1$ である。β を $f(x)$ の根とすれば

$$0 = f(\beta) = (\beta - \alpha)g(\beta)$$

であり、R が整域であることから $\beta - \alpha = 0$ または $g(\beta) = 0$ である。これは $f(x)$ の根が α であるか、または $g(x)$ の根であることを意味し、よって $f(x)$ の根は高々 n 個である。 □

命題 3.5.5. $f(x) \in R[x]$ とする。このとき写像 $f^* : R \to R$ $(\alpha \mapsto f(\alpha))$ が得られる。R が無限個の元を含む整域であるとき「$f(x) \neq g(x)$ ならば $f^* \neq g^*$」が成り立つ。

証明. $h(x) = f(x) - g(x)$ とおく。$h(x) \neq 0$ ならば $h(x)$ は高々 $\deg h$ 個の根をもつ。よって R が無限個の元を含むならば $h(\alpha) \neq 0$ となる $\alpha \in R$ が存在する。よって $0 \neq h(\alpha) = f^*(\alpha) - g^*(\alpha)$ であり $f^* \neq g^*$ である。 □

例 3.5.6. p を素数とし $R = \mathbb{Z}/p\mathbb{Z}$ とすれば R は整域である。このとき $f(x) = x^p - x$ とすれば任意の $\alpha \in R$ に対して $f(\alpha) = 0$ であり、よって $f^* = 0^*$ である。(証明はしないが、小さな素数 p について確かめることは容易である。)

多変数の多項式環 $R[x_1, x_2, \cdots, x_n]$ は帰納的に

$$R[x_1, x_2, \cdots, x_n] = R[x_1, x_2, \cdots, x_{n-1}][x_n]$$

($R[x_1, \cdots, x_{n-1}]$ 上の変数 x_n に関する多項式環) として定義される。その元は

$$f(x_1, x_2, \cdots, x_n) = \sum a_{i_1 i_2 \cdots i_n} {x_1}^{i_1} {x_2}^{i_2} \cdots {x_n}^{i_n}, \quad (a_{i_1 i_2 \cdots i_n} \in R)$$

と表される。これを $x_1, x_2, \cdots, x_n$ に関する R 上の**多項式** (polynomial) という。$a_{i_1 i_2 \cdots i_n} \neq 0$ のとき $a_{i_1 i_2 \cdots i_n} {x_1}^{i_1} {x_2}^{i_2} \cdots {x_n}^{i_n}$ を f の **項** (term) といい $i_1 + i_2 + \cdots + i_n$ をその**次数** (degree) という。

命題 3.5.7. R が整域のとき $R[x_1, x_2, \cdots, x_n]$ も整域である。また、その単数群は R の単数群と一致する。

証明. R が整域だから $R[x_1]$ は整域、よって $R[x_1, x_2] = R[x_1][x_2]$ も整域、これを繰り返して $R[x_1, x_2, \cdots, x_n]$ も整域である。

$U(R) = U(R[x])$ を示せば、上と同じような議論で $R[x_1, x_2, \cdots, x_n]$ の単数は R の単数と一致する。$f(x) \in R[x]$ を単数とする。ある $g(x) \in R[x]$ が存在して $f(x)g(x) = 1$ である。次数を比べると $\deg f + \deg g = 0$ であるから $\deg f = \deg g = 0$、すなわち $f(x), g(x) \in R$ である。よって $f(x)$ は R の単数であり $U(R[x]) \subset U(R)$ である。$U(R) \subset U(R[x])$ は明らかであり $U(R) = U(R[x])$ である。 □

命題 3.5.8. R が無限個の元を含む整域とする。

(1) $f(x_1, x_2, \cdots, x_n)$ に対して、写像 $f^* : R \times R \times \cdots \times R \to R$ が定義される。このとき $f \neq g$ ならば $f^* \neq g^*$ である。

(2) $g_1, g_2, \cdots, g_r \in R[x_1, x_2, \cdots, x_n]$, $g_i \neq 0$ とする。$g \in R[x_1, x_2, \cdots, x_n]$ が

$$g_i(\alpha_1, \alpha_2, \cdots, \alpha_n) \neq 0 \quad (i = 1, 2, \cdots, r)$$

なる任意の $(\alpha_1, \alpha_2, \cdots, \alpha_n)$ に対して $f(\alpha_1, \alpha_2, \cdots, \alpha_n) = 0$ となるならば $f = 0$ である。

証明. (1) $f \neq 0$ ならば $f^* \neq 0^*$ であることを示せばよい。これを n に関する帰納法で示す。$n = 1$ のときは既に示した。f を $R[x_1, \cdots, x_{n-1}]$ を係数とする x_n の多項式と見て

$$f(x_1, \cdots, x_n) = \sum_{i=0}^{m} g_i(x_1, \cdots, x_{n-1}){x_n}^i$$

と書く。$f \neq 0$ だから、ある i について $g_i \neq 0$ である。帰納法の仮定より $g_i(\alpha_1, \cdots, \alpha_{n-1}) \neq 0$ となる $(\alpha_1, \cdots, \alpha_{n-1}) \in R \times \cdots \times R$ が存在する。このとき $0 \neq f(\alpha_1, \cdots, \alpha_{n-1}, x_n) \in R[x_n]$ であるから、ある $\alpha_n \in R$ が存在して $f(\alpha_1, \cdots, \alpha_{n-1}, \alpha_n) \neq 0$ である。よって $f^* \neq 0$ である。

(2) f が条件を満たせば $fg_1 \cdots g_r$ は $R \times \cdots \times R$ のすべての点で 0 となる。よって (1) より $fg_1 \cdots g_r = 0$ である。$R[x_1, \cdots, x_n]$ が整域で $g_i \neq 0$ であるから $f = 0$ である。 □

3.6 色々な体

K を体とする。$1 \in K$ に対して

$$1,\ 1+1,\ 1+1+1, \cdots$$

を考え、それぞれ単に $1,\ 2,\ 3, \cdots$ と書く。$0,\ -1,\ -2 = (-1) + (-1), \cdots$ も考えて

$$F = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$$

を考えれば F は K の部分環となる。K には零因子がないので F にも零因子はなく F は整域である。F は加群として 1 で生成される巡回群で、したがって $\mathbb{Z}/n\mathbb{Z}$ $(n \in \mathbb{N})$、

または $\mathbb{Z}$ と本質的に同じものである (命題 **??**)。これを同一視する。$F = \mathbb{Z}/n\mathbb{Z}$ であるとき F が整域であることにより n は素数になる (定理 3.2.5)。この素数を K の**標数** (characteristic) という。$F = \mathbb{Z}$ のときには K の標数は 0 であるという。標数 p $(\neq 0)$ の体において $p = 0$ である。標数が 0 でない体を**正標数**の体ともいう。

例 3.6.1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ は標数 0 の体である。$\mathbb{Z}/p\mathbb{Z}$ (p は素数) は標数 p の体である。

命題 3.6.2. K を標数 p $(\neq 0)$ の体とする。$a, b \in K$ に対して

$$(a+b)^p = a^p + b^p$$

が成り立つ。

証明. 二項定理により $(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}$ である。ここで $0 < i < p$ とすると

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}$$

であり、分子に p が現れるが分母には p は現れない。よって、これは p の倍数であり K において 0 である。 □

問 3.6.3. $F = \mathbb{Z}/5\mathbb{Z}$ とする。$n \in \mathbb{N}$ に対して、写像 $f_n : F \to F$ を $f(a) = a^n$ で定める。$n = 2, 3, 4, 5$ について、f_n は単射 (全射) であるか、それぞれ決定せよ。

問 3.6.4. p を素数とし $F = \mathbb{Z}/p\mathbb{Z}$ とする。任意の $a \in F$ に対して $a^p = a$ であることを示せ。

例 3.6.5 (有理数体 $\mathbb{Q}$ の構成)**.** 有理整数環 $\mathbb{Z}$ から有理数体 $\mathbb{Q}$ を構成しよう。$\mathbb{Z}^* = \mathbb{Z} - \{0\}$ (非零因子全体の集合) とする。直積集合 $\mathbb{Z} \times \mathbb{Z}^*$ に関係 $\sim$ を「$at = bs$ のとき $(a, s) \sim (b, t)$」として定める。この関係は同値関係である。(a, s) を含む同値類を a/s と書くことにする。同値類全体の集合 $(\mathbb{Z} \times \mathbb{Z}^*)/\sim$ を R と書くことにする。R に加法と乗法を

$$\begin{aligned} a/s + b/t &= (at + bs)/st \\ (a/s)(b/t) &= (ab)/(st) \end{aligned}$$

で定めれば、この演算は矛盾なく定義され、結合法則、分配法則などが成り立つ。これによって R は可換環となる。単位元は $1/1$、零元は $0/1$、a/s $(a \neq 0)$ の逆元は s/a である。これにより R は体となる。この体を**有理数体**といい $\mathbb{Q}$ と書く。

問 3.6.6. 例 3.6.5 において以下のことを確認せよ。

(1) $\sim$ が同値関係であること。

(2) 加法と乗法が矛盾なく定義されること。

(3) 加法の結合法則、乗法の結合法則、乗法の交換法則、分配法則、が成り立つこと。

例 3.6.5 の構成は $\mathbb{Z}$ でなくても、一般の整域 D に対して行うことができる。このようにして作った体を整域 D の**商体** (quotient field) という。

例 3.6.7. R を整域とすると、R 上の多項式環 $R[x]$ は整域である。$R[x]$ の商体は

$$\left\{ \frac{f(x)}{g(x)} \;\middle|\; g(x) \neq 0 \right\}$$

である。これを R 上の**有理関数体**といい $R(x)$ と書く。

R の商体を K とすると、適当な同一視によって $K(x) = R(x)$ である。

$m \in \mathbb{Z}$ が**平方数**であるとは、$m = a^2$ となる $a \in \mathbb{Z}$ が存在することである。$m \in \mathbb{Z}$ が**平方自由** (square free) であるとは、$m \neq 0, 1$ であって m を割り切る 1 以外の平方数が存在しないことである。m が平方自由であるということは、簡単に言えば $\sqrt{m}$ がより簡単な形に変形できないということである。

例 3.6.8. 3, 15, -6, -105 などは平方自由である。0, 1, -4, 9, 12 などは平方自由ではない。

m を平方自由な整数とし

$$\begin{aligned} \mathbb{Q}[\sqrt{m}] &= \{a + b\sqrt{m} \mid a, b \in \mathbb{Q}\} \\ \mathbb{Q}(\sqrt{m}) &= \left\{ \frac{a + b\sqrt{m}}{c + d\sqrt{m}} \;\middle|\; a, b, c, d \in \mathbb{Q},\ c^2 + d^2 \neq 0 \right\} \end{aligned}$$

とおく。

命題 3.6.9. $\mathbb{Q}[\sqrt{m}]$ は体である。

証明. まず $R = \mathbb{Q}[\sqrt{m}] \subset \mathbb{C}$ と見て、これが部分環であることを示す。$1 \in R$ である。$\alpha, \beta \in R$ ならば $\alpha - \beta$, $\alpha\beta \in R$ も明らかで、よって R は可換環である。

$0 \neq a + b\sqrt{m}$ $(a, b \in \mathbb{Q})$ に対して、逆元が存在することを示せばよい。$(a + b\sqrt{m})(a - b\sqrt{m}) = a^b - b^2 m$ は m が平方自由なので 0 にはならない。$a + b\sqrt{m}$ の逆元は $\mathbb{C}$ には存在するので、それが R に含まれることをいえばよい。実際

$$\frac{1}{a + b\sqrt{m}} = \frac{a - b\sqrt{m}}{(a + b\sqrt{m})(a - b\sqrt{m})} = \frac{a}{a^2 - b^2 m} - \frac{b}{a^2 - b^2 m}\sqrt{m} \in \mathbb{Q}[\sqrt{m}]$$

である。よって $R = \mathbb{Q}[\sqrt{m}]$ は体である。 □

問 3.6.10. $\mathbb{Q}[\sqrt{m}] = \mathbb{Q}(\sqrt{m})$ であることを示せ。

$\mathbb{Q}[\sqrt{m}]$ を**二次体** (quadratic field) という。これは多項式環 $\mathbb{Q}[x]$ において $(x^2 - m)\mathbb{Q}[x]$ というイデアルを考え、それによる剰余環 $\mathbb{Q}[x]/(x^2 - m)\mathbb{Q}[x]$ を考えていることと同じである。

同様に $f(x) \in \mathbb{Q}[x]$ を既約多項式 (より小さい次数の多項式の積に分解しない多項式) とするとき、剰余環 $\mathbb{Q}[x]/f(x)\mathbb{Q}[x]$ は体となる。このような体を**代数体** (algebraic number field) という。

参考文献

[1] 代数学, 永尾汎, 朝倉書店

[2] 代数学入門, 石田信, 実教出版