

6 第6回

6.1 多項式環

体 F 上の多項式 $f(x)$

$$f(x) = f_{n-1}x^{n-1} + f_{n-2}x^{n-2} + \cdots + f_1x + f_0$$

但し、 $f_{n-1} \neq 0$ 、 x は不定元、 $f_i \in F$ ($i = 0, 1, \dots, n-1$)。 $f_{n-1} = 1$ のとき、 $f(x)$ をモニック多項式という。係数 $f_m \neq 0$ を有する x の最高次数を多項式 $f(x)$ の次数といい $\deg f(x)$ と書く。

$F[x]$: F 上の全ての多項式の集合

6.2 多項式環の演算

$\forall f(x), g(x) \in F[x]$ に対し、多項式の加法と乗法をそれぞれ

$$f(x) + g(x) = \sum_{i=0}^{\max(\deg f(x), \deg g(x))} (f_i + g_i) x^i$$
$$f(x)g(x) = \sum_{i=0}^{\deg f(x) + \deg g(x)} \left(\sum_{j=0}^i f_j g_{i-j} \right) x^i$$

によって定義すれば、 $F[x]$ は環をなす。但し、 $f_i + g_i$ と $f_j g_{i-j}$ は F 上の加法と乗法を表す。

(例) $GF(2)$ 上の多項式 $f(x) = x + 1$ について

$$f(x) + f(x) = x + 1 + x + 1 = (1 + 1)x + (1 + 1) = 0$$

($GF(2)$ では $1 + 1 = 0$)

$$f(x) \cdot g(x) = (x + 1)^2 = x(x + 1) + (x + 1) = x^2 + 1$$

6.3 倍数と因数

$m(x), a(x), b(x) \in F[x]$ に対し

$$a(x)m(x) = b(x)$$

と書けるとき、 $a(x)$ は $b(x)$ を割り切るといふ。

$b(x) : a(x)$ の倍数

$a(x) : b(x)$ の因数

$p(x)$ の因数が $\alpha p(x)$ か α のみ ($\alpha \in F$) のとき、 $p(x)$ を既約多項式 (irreducible polynomial) と呼ぶ。特にモニック多項式である既約多項式を素多項式という。

$a(x)$ と $b(x)$ の両方を割り切る最大次数のモニック多項式を最大公約多項式といい、 $(a(x), b(x))$ と書く。

定理 12 $\forall a(x), b(x) \in F[x]$ に対し

$$b(x) = a(x)q(x) + r(x)$$

$$\deg r(x) < \deg a(x)$$

となる商 $q(x) \in F[x]$ および剰余 $r(x) \in F[x]$ が一意的に定まる。

(証明) $\forall a(x), b(x) \in F[x]$ に対し

$$b(x) = a(x)q_1(x) + r_1(x) \quad \deg r_1(x) < \deg a(x)$$

$$b(x) = a(x)q_2(x) + r_2(x) \quad \deg r_2(x) < \deg a(x)$$

と 2 通りに表されたとする。このとき

$$a(x)q_1(x) + r_1(x) = a(x)q_2(x) + r_2(x)$$

から

$$a(x)(q_1(x) - q_2(x)) = r_2(x) - r_1(x)$$

が得られ ($-q_2(x)$ は $q_2(x)$ の加法逆元)、

$$\deg(r_2(x) - r_1(x)) < \deg a(x)$$

なので、 $r_2(x) \neq r_1(x)$ とすると両辺の次数が一致せず矛盾する。従って、 $r_2(x) = r_1(x)$ であり、このとき、 $q_1(x) = q_2(x)$ でなければならない。□

以下では

$$b(x) = a(x)q(x) + r(x) \quad \deg r(x) < \deg a(x)$$

を

$$r(x) = R_{a(x)}[b(x)] \quad \text{または} \quad r(x) \equiv b(x) \pmod{a(x)}$$

と書くことにする。

定理 13 1. $R_{a(x)}[b(x) + c(x)] = R_{a(x)}[b(x)] + R_{a(x)}[c(x)]$

2. $R_{a(x)}[b(x) \cdot c(x)] = R_{a(x)}[R_{a(x)}[b(x)] \cdot R_{a(x)}[c(x)]]$

証明は整数環のときと同様に行えるので省略する。

定理 14 (因数分解の一意的性) 非零の多項式 $f(x) \in F[x]$ は、体 F 上の素多項式と体 F のある定数の積に一意的に因数分解される。すなわち

$$f(x) = \alpha p_1(x) \cdots p_m(x) \quad (\text{一意的})$$

$$\alpha \in F, p_1(x) \sim p_m(x): \text{素多項式}$$

証明はやや混み入っているので省略する。

定理 15 (ユークリッドの互除法) $\forall a(x), b(x) \in F[x] \deg a(x) \geq \deg b(x)$ とし

$$a_0(x) = a(x), a_1(x) = b(x)$$

とし、 $n = 1, 2, \dots$ に対し $a_n(x) \neq 0$ である限り $a_{n+1}(x)$ を

$$a_{n-1}(x) = a_n(x)q_n(x) + a_{n+1}(x), \deg a_{n+1}(x) < \deg a_n(x)$$

によって定義する。このとき、ある $N \geq 1$ に対し、 $a_{N+1}(x) = 0$ であり、

$$a_N(x) = (f(x), g(x))$$

である。

系 2 $\forall a(x), b(x) \in F[x]$ に対し、

$$(a(x), b(x)) = y(x)a(x) + z(x)b(x)$$

と表せる $y(x), z(x)$ の組が存在する。

(例) $GF(2)$ 上の多項式 $f_1(x) = x^3 + 1, f_2(x) = x^4 + x^3 + x^2 + 1$ の最大公約数を求めよ。

$$\begin{array}{r}
 x^3 + 1 \quad) \quad \begin{array}{r} x \quad +1 \\ x^4 + x^3 + x^2 \quad +1 \\ \hline x^4 \qquad \qquad \quad x \\ \hline x^3 + x^2 + x + 1 \\ x^3 \qquad \qquad \quad +1 \\ \hline x^2 + x \end{array} \\
 \begin{array}{r} x^3 \qquad \qquad \quad +1 \\ \hline x^2 + x \end{array} \quad) \quad \begin{array}{r} x \quad +1 \\ x^3 \qquad \qquad \quad +1 \\ \hline x^3 + x^2 \\ \hline x^2 \qquad \qquad \quad +1 \\ x^2 + x \qquad \quad x \\ \hline x \quad +1 \end{array} \quad) \quad \begin{array}{r} x^2 + x \\ x^2 + x \\ \hline 0 \end{array}
 \end{array}$$

従って、 $(f_1(x), f_2(x)) = x + 1$ 。このプロセスを行列で表すと、

$$\begin{aligned} \begin{bmatrix} x+1 \\ 0 \end{bmatrix} &= \begin{bmatrix} 0 & 1 \\ 1 & x \end{bmatrix} \begin{bmatrix} x^2+x \\ x+1 \end{bmatrix} \\ &\quad \text{商} \\ \begin{bmatrix} x^2+x \\ x+1 \end{bmatrix} &= \begin{bmatrix} 0 & 1 \\ 1 & x+1 \end{bmatrix} \begin{bmatrix} x^3+1 \\ x^2+x \end{bmatrix} \\ \begin{bmatrix} x^3+1 \\ x^2+x \end{bmatrix} &= \begin{bmatrix} 0 & 1 \\ 1 & x+1 \end{bmatrix} \begin{bmatrix} f_2(x) \\ f_1(x) \end{bmatrix} \end{aligned}$$

これから

$$\begin{aligned} \begin{bmatrix} x+1 \\ 0 \end{bmatrix} &= \begin{bmatrix} 0 & 1 \\ 1 & x \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & x+1 \end{bmatrix} \begin{bmatrix} x^3+1 \\ x^2+x \end{bmatrix} \\ &= \begin{bmatrix} 1 & x+1 \\ x & x^2+x+1 \end{bmatrix} \begin{bmatrix} x^3+1 \\ x^2+x \end{bmatrix} \\ &= \begin{bmatrix} 1 & x+1 \\ x & x^2+x+1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & x+1 \end{bmatrix} \begin{bmatrix} f_2(x) \\ f_1(x) \end{bmatrix} \\ &= \begin{bmatrix} x+1 & x^2 \\ x^2+x+1 & x^2+x+1 \end{bmatrix} \begin{bmatrix} f_2(x) \\ f_1(x) \end{bmatrix} \end{aligned}$$

1 行目から系に対応する関係式

$$x+1 = (x+1)f_2(x) + x^2f_1(x)$$

が得られる。

[定義] (剰余類環、商環)

体 F 上のモノック多項式を $f(x)$ 、 $\forall a(x), b(x) \in F[x]$ とする。このとき、

$$\begin{aligned} a(x) + b(x) &= R_{f(x)}[a(x) + b(x)] \\ a(x) \cdot b(x) &= R_{f(x)}[a(x) \cdot b(x)] \end{aligned}$$

で定める加法と乗法をもつ $F[x]$ 中の $\deg f(x)$ 未満の次数の全ての多項式の集合を剰余類環または商環といい、 $F_{f(x)}[x]$ と書く。

定理 16 $p(x)$ が素多項式の時、またそのときに限って剰余類環 $F_{p(x)}[x]$ は体をなす。

証明は剰余類環 Z_p のときとほぼ同様に行えるので省略する。

(例 1) $GF(2)$ 上の多項式 $p(x) = x^2 + x + 1$ は素多項式である。従って、 $F_{x^2+x+1}[x] = \{0, 1, x, x+1\}$ は体をなす。従って、

+	0	1	x	$x+1$	·	0	1	x	$x+1$
0	0	1	x	$x+1$	0	0	0	0	0
1	1	0	$x+1$	x	1	0	1	x	$x+1$
x	x	$x+1$	0	1	x	0	x	$x+1$	1
$x+1$	$x+1$	x	1	0	$x+1$	0	$x+1$	1	x

$x \times x = R_{x^2+x+1}[x^2] = x+1$ 等に注意

であり、 $F_{x^2+x+1}[x] = GF(4)$ である。前回の講義で示した $GF(4)$ は $x \rightarrow 2, x+1 \rightarrow 3$ として得られたものである。

(例 2) $GF(2)$ 上の多項式 $f(x) = x^2 + 1$ は素多項式ではない。なぜなら $f(x) = (x+1)^2$ である。従って、 $F_{x^2+1}[x] = \{0, 1, x, x+1\}$ は体をなさない。事実

·	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	1	$x+1$
$x+1$	0	$x+1$	$x+1$	0

から、 $x+1$ は乗法逆元をもたない。