

代数系と符号理論 (O) 第7回板書プリント

制作：植松友彦

2014.5.28

第6回の復習

- 環の定義
- 剰余類環と多項式環
- イデアルの定義
- 環の準同型写像の定義
- 素因数分解の一意性

1 体の定義

[定義 8.1] 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。

F1 F は加法に対して可換群である。

F2 任意の元 $a, b \in F$ に対し、 $a \cdot b \in F$ である。また非零元は乗法のもとに可換群をなす。

F3 (分配則) 任意の元 $a, b, c \in F$ 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。

[定義 8.2] 元の個数が有限である体を有限体 (finite field) あるいはガロア体 (Galois field) と呼び、特に q 個の元からなる有限体を $\mathbb{F}_q$ あるいは $GF(q)$ と書く。

[例 1] 今までの例 8.3 と 8.4 を参考にして、大岡君は $\{0, 1, 2, 3\}$ が下記の演算 (法 4 による加法と乗法) について $\mathbb{F}_4$ となるか調べた。

$+$	0	1	2	3	$\cdot$	0	1	2	3
0	0	1	2	3	0	0	0	0	0
1	1	2	3	0	1	0	1	2	3
2	2	3	0	1	2	0	2	0	2
3	3	0	1	2	3	0	3	2	1

その結果、2 には乗法逆元がない (2 と乗算して 1 になる元がない) ので Z_4 は体 $\mathbb{F}_4$ にはならないことが分った。そこで、大岡君は乗法のみを下表のように変えたところ、結合法則が成り立たないことに気がついた。たとえば、

$$3 \cdot (1 + 1) = 3 \cdot 1 + 3 \cdot 1 = 3 + 3 = 2 \text{ だが } 3 \cdot (1 + 1) = 3 \cdot 2 = 1$$

である。そこで、更に加法を下表のように変えたところ、

$\cdot$	0	1	2	3	$+$	0	1	2	3
0	0	0	0	0	0	0	1	2	3
1	0	1	2	3	1	1	0	3	2
2	0	2	3	1	2	2	3	0	1
3	0	3	1	2	3	3	2	1	0

体 $\mathbb{F}_4$ になるのが分った。各自確かめよ。

[定理 8.1] (有限体 $\mathbb{F}_p$) $Z_p = \{0, 1, \dots, p-1\}$ における加法と乗法を $\text{mod } p$ による加算と乗算によって定義したものが剰余類環 Z_p である (例 7.2 参照)。 p が素数ならば、剰余類環 Z_p は p 個の元からなる有限体 $\mathbb{F}_p$ である。

[例 2] 例 8.4 で示した $\mathbb{F}_3$ の加法と乗法は、3 が素数なので $\text{mod } 3$ による加算と乗算に一致しているが、例 1 で示した $\mathbb{F}_4$ の加法と乗法は $\text{mod } 4$ による加算と乗算に一致していない。

2 多項式環

「体 F 上の多項式」と呼ばれる体 F の元を係数としてもつ多項式 $f(x)$

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \quad (1)$$

を考えよう。但し、 $a_n \neq 0$ 、 $a_i \in F$ ($i = 0, 1, \dots, n$) である。

多項式に関連する用語

- 最高次の係数が 1 であるとき、すなわち

$$f(x) = x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

であるとき、 $f(x)$ を「モニック多項式」という。

- 多項式 $f(x)$ における x の最高次の次数を $f(x)$ の「次数」といい、 $\deg f(x)$ と書く。
- F 上の x の多項式の全体の集合を $F[x]$ によって表す。

[定理 8.2] (多項式の剰余定理) $a(x), b(x) \in F[x]$, $b(x) \neq 0$ とする。このとき、

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

を満足し、かつ次数が $\deg r(x) < \deg b(x)$ となる多項式の組 $q(x), r(x) \in F[x]$ が一意的に存在する。

[定理 8.3] (代数学の基本定理) 体 F 上の n 次多項式は、 F 上で高々 n 個の (相異なる) 根を持つ。

多項式の因数に関連する用語

多項式 $a(x), b(x), m(x) \in F[x]$ に対して、 $a(x) = m(x)b(x)$ が成り立つとき、

- $b(x)$ は $a(x)$ を割り切るといい、 $a(x)$ を $b(x)$ の「倍数」、 $b(x)$ を $a(x)$ の「因数」という。
- α を F の元とすると、多項式 $p(x) \in F[x]$ が $\alpha p(x)$ か α によってのみ割り切られる場合、すなわち $p(x)$ が F 上の多項式の積に因数分解できない場合、 $p(x)$ のことを「既約多項式 (irreducible polynomial)」という。
- $a(x), b(x)$ 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 (the greatest common divisor)」といい、 $(a(x), b(x))$ によって表す。
- $(a(x), b(x)) = 1$ のとき、 $a(x)$ と $b(x)$ は「互いに素」であるという。
- $a(x)$ と $b(x)$ の両方の倍数のうち最小次数のモニック多項式を $a(x)$ と $b(x)$ の「最小公倍多項式 (the least common multiple)」といい、 $\text{LCM}(a(x), b(x))$ によって表す。

[定理 8.4] (ユークリッドの互除法) 2つの多項式 $a(x), b(x) \in F[x]$ ($\deg a(x) \geq \deg b(x)$) が与えられたとき、 $a_0(x) = a(x)$, $a_1(x) = b(x)$ とおき、 $n = 1, 2, \dots$ に対して、 $a_n(x) = 0$ でない限り、

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

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

[系 8.1] (拡張ユークリッドの互除法) 任意の多項式 $a(x), b(x) \in F[x]$ に対し、

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

を満たす多項式 $y(x), z(x) \in F[x]$ が存在する。

[例 3] $\mathbb{F}_2[x]$ 上の多項式 $a(x) = x^5 + x$ と $b(x) = x^3 + 1$ の最大公約多項式を求めてみよう。 $a_0(x) = x^5 + x$, $a_1(x) = x^3 + 1$ として、ユークリッドの互除法を行うと

$$x^5 + x = x^2(x^3 + 1) + x^2 + x$$

から $a_2(x) = x^2 + x$ が得られる。更に、

$$x^3 + 1 = (x + 1)(x^2 + x) + x + 1$$

から $a_3(x) = x + 1$ が得られ、最後に

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

となるので、 $(x^5 + x, x^3 + 1) = x + 1$ である。

更に、これらの式を行列で表示すると、

$$\begin{pmatrix} x^3 + 1 \\ x^2 + x \end{pmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & x^2 \end{bmatrix} \begin{pmatrix} x^5 + x \\ x^3 + 1 \end{pmatrix}$$

$$\begin{pmatrix} x^2 + x \\ x + 1 \end{pmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & x + 1 \end{bmatrix} \begin{pmatrix} x^3 + 1 \\ x^2 + x \end{pmatrix}$$

$$\begin{pmatrix} x + 1 \\ 0 \end{pmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & x \end{bmatrix} \begin{pmatrix} x^2 + x \\ x + 1 \end{pmatrix}$$

一番下の式に、下の式から順に代入を行うことで、

$$\begin{aligned} \begin{pmatrix} x+1 \\ 0 \end{pmatrix} &= \begin{bmatrix} 0 & 1 \\ 1 & x \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & x+1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & x^2 \end{bmatrix} \begin{pmatrix} x^5+x \\ x^3+1 \end{pmatrix} \\ &= \begin{bmatrix} x+1 & x^3+x^2+1 \\ x^2+x+1 & x^4+x^3+x^2+x \end{bmatrix} \begin{pmatrix} x^5+x \\ x^3+1 \end{pmatrix} \end{aligned}$$

を得る。この式の1行目から、系8.1に示した関係

$$x+1 = (x+1)(x^5+x) + (x^3+x^2+1)(x^3+1)$$

の成立が分る。

多項式環 $F[x]$ において既約多項式は、整数環における素数と同じ働きをする。従って、任意の多項式は既約多項式の積として一意に表すことができる。

[例 8.5] 符号理論でよく用いる $\mathbb{F}_2$ 上の5次以下の既約多項式を表8.1に示す。表中で原始多項式(定義9.4参照)には下線を引いている。4次以下の既約多項式は全て覚えておくこと。

表 8.1 $\mathbb{F}_2$ 上の既約多項式

次数	既約多項式
1	<u>$x, x+1$</u> (1次式は全部既約)
2	<u>x^2+x+1</u> (既約は1つだけ)
3	<u>x^3+x+1, x^3+x^2+1</u>
4	<u>x^4+x+1, x^4+x^3+1</u> $x^4+x^3+x^2+x+1$
5	<u>$x^5+x^2+1, x^5+x^4+x^3+x^2+1$</u> <u>$x^5+x^4+x^2+x+1, x^5+x^3+x^2+x+1$</u> <u>$x^5+x^4+x^3+x+1, x^5+x^3+1$</u>

$\mathbb{F}_2$ 上の5次以下の多項式の既約判定法

1. 多項式が2次か3次の場合、定数項が零でなく、かつ項の数が奇数ならば既約である。
2. 多項式が4次か5次の場合、上記の条件を満足し、かつ x^2+x+1 で割り切れなければ既約である。

3 多項式環を基礎とした有限体

[定義 8.3] (剰余類環) 体 F 上のモノック多項式を $p(x)$ とする。このとき任意の多項式 $a(x), b(x) \in F[x]$ について、加法と乗法を

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

によって定める。但し、 $R_{p(x)}[c(x)]$ は多項式 $c(x)$ を $p(x)$ で割ったときの余りを表す。 $\deg p(x)$ 未満の次数を有する全ての多項式の集合に、この演算を導入したものを「剰余類環」といい、 $F_{p(x)}[x]$ によって表す。

[定理 8.5] 体 $\mathbb{F}_q$ 上の m 次のモニックな既約多項式 $p(x)$ によって定まる剰余類環 $F_{p(x)}[x]$ は、 q^m 個の元からなる有限体 $\mathbb{F}_{q^m}$ である。

[例 8.6] $\mathbb{F}_2$ 上の 2 次の既約多項式 $f(x) = x^2 + x + 1$ によって得られる剰余類環は有限体 $\mathbb{F}_4$ である。 $\mathbb{F}_4$ の加法と乗法を定義 8.3 に従って定義したときの演算表を次に示す。

$\mathbb{F}_4$ の加算表					$\mathbb{F}_4$ の乗算表				
+	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

尚、この体 $\mathbb{F}_4$ は剰余類環 Z_4 とは一致しないことに注意する。尚、例 1 で作った体とこの体 $\mathbb{F}_4$ の間には、同型写像

$$f(0) = 0, f(1) = 1, f(2) = x, f(3) = x + 1$$

が存在する。

4 元の位数の性質

[定義 8.4](位数) 有限体 F の任意の非零の元を a とする。このとき、 $a^s = 1$ となる最小正整数 s を a の位数と呼び、 $\text{ord}(a)$ によって表す。

[補題 8.1] a, b を有限体 F の非零の元とする。このとき、以下の性質が成り立つ。

1. $a^j = 1$ であるための必要十分条件は、 $\text{ord}(a)$ が j を割り切ることである。
2. $\text{ord}(a^j) = \frac{\text{ord}(a)}{(\text{ord}(a), j)}$
3. $\text{ord}(a) = s, \text{ord}(b) = j, (s, j) = 1$ ならば、 $\text{ord}(ab) = sj$ である。

[例 4] $\mathbb{F}_{11} = \{0, 1, 2, \dots, 10\}$ において、各元の位数を求めたものを表に示す。

元	1	2	3	4	5	6	7	8	9	10
位数	1	10	5	5	5	10	10	10	5	2

これから、例えば $2^4 = 5$ と $2^5 = 10$ の位数について性質 2 が成り立つことが、

$$\frac{\text{ord}(2)}{(\text{ord}(2), 4)} = \frac{10}{(10, 4)} = 5, \quad \frac{\text{ord}(2)}{(\text{ord}(2), 5)} = \frac{10}{(10, 5)} = 2$$

から確かめられる。また、10 の位数は 2 であり、3, 4, 5, 9 の位数が 5 であることから、 $8 = 10 \cdot 3$, $7 = 10 \cdot 4$, $6 = 10 \cdot 5$, $2 = 10 \cdot 9$ の位数 $10 (= 2 \cdot 5)$ について性質 3 が成り立つことが確かめられる。

5 位数と原始元

[定義 8.5](原始元) 要素数が q の有限体 $\mathbb{F}_q$ において、位数 $q - 1$ の元のことを $\mathbb{F}_q$ の「原始元 (primitive element)」という。

[定理 8.6] 有限体 $\mathbb{F}_q$ は原始元をもつ。

有限体 $\mathbb{F}_q$ の原始元 α を用いると、 $\mathbb{F}_q$ の非零の元は、

$$\alpha, \alpha^2, \dots, \alpha^{q-2}, \alpha^{q-1} (= 1)$$

によって表されることに注意する (9.2 節のべき表現を参照)。

[注意] この定理は原始元の存在を保証しているが、通常、原始元は試行錯誤で求めるしかない。

[系 8.2] 有限体 $\mathbb{F}_q$ の任意の非零元の位数は $q - 1$ を割り切る。

[系 8.3] 有限体 $\mathbb{F}_q$ の任意の元 γ は、 $\gamma^q - \gamma = 0$ を満たす。

[系 8.4] 有限体 $\mathbb{F}_q$ の非零の元の集合は乗法に関して巡回群をなす。

[例 5] $\mathbb{F}_7$ の原始元の一つは 3 である。なぜなら、

$$3^2 \bmod 7 = 2, 3^3 \bmod 7 = 6, 3^4 \bmod 7 = 4, 3^5 \bmod 7 = 5, 3^6 \bmod 7 = 1$$

であり、3 の位数が $6 (= 7 - 1)$ であるからである。また、先の例から、 $\mathbb{F}_{11}$ の原始元は 2, 6, 7, 8 である。

[例 4] 有限体 $\mathbb{F}_4$ の原始元は x と $x + 1$ である。なぜなら、例 8.6 において、

$$x^2 = x + 1, x^3 = (x + 1)x = 1 \text{ ならびに } (x + 1)^2 = x, (x + 1)^3 = x(x + 1) = 1$$

が成り立つからである。