情報数学 2B および演習

宮本 暢子

April 6, 2023

Outline

同値関係

Definition

A 上の同値関係 E とは，次の条件を満たす二項関係 $E \subseteq A \times A$ である．

(1) $\forall x \in A$ に対し，$(x, x) \in E$ である．(反射律)

(2) $(x, y) \in E$ ならば，$(y, x) \in E$ である．(対称律)

(3) $(x, y) \in E$ かつ $(y, z) \in E$ ならば，$(x, z) \in E$ である．(推移律)

同値類

$x \in A$ に対して，x と同値関係 E にあるすべての要素の集合

$$[x]_\sim = \{y \in A : y \sim x\}$$

を同値類といい，そのときの x を代表元という．集合 A のすべての同値類の集合を $A/\sim = \{[x]_\sim : x \in A\}$ と書き，A の同値関係 $\sim$ に関する商集合と呼ぶ．

代数系

ある集合 G が G 上で定義されるある演算 $\circ$ に関して閉じている，すなわち

$$a, b \in G \quad \text{ならば} \quad a \circ b \in G$$

であるとき，G と演算 $\circ$ の組 $(G, \circ)$ を**代数系**という．

Definition

代数系 $(G, \circ)$ が次の性質を満たすとき，$(G, \circ)$ は**群**であるという．

(1) 任意の $a, b, c \in G$ に対して，
$(a \circ b) \circ c = a \circ (b \circ c)$ が成り立つ．(**結合法則**)

(2) ある元 $e \in G$ が存在して，任意の元 $a \in G$ に対して $e \circ a = a \circ e = a$ が成り立つ．
（e を**単位元**という）

(3) 任意の元 $a \in G$ に対して，ある元 a^{-1} が存在して $a \circ a^{-1} = a^{-1} \circ a = e$ が成り立つ．
（a^{-1} を a の**逆元**という）

可換群

Definition

群が次の条件を満たすとき，可換群という．

(4) 任意の $a, b \in G$ に対して，$a \circ b = b \circ a$ が成り立つ．(交換法則)

環

Definition

次の性質を満たす２つの二項演算子 $+, \cdot$ を持つ代数系 $(R, +, \cdot)$ を**環**という．

(1) $(R, +)$ は可換群である．
(2) $(R \setminus \{0\}, \cdot)$ は逆元の存在を除いては，乗法群の定義を満たす．ここで 0 は加法単位元とする．
(3) 分配法則を満たす．すなわち任意の $a, b, c \in R$ に対して，

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (a + b) \cdot c = a \cdot c + b \cdot c$$

が成り立つ．

乗法について可換な環は**可換環**と呼ばれる．

体

Definition

次の条件を満たす代数系 $(F, +, \cdot)$ を**体**という．

(1) $(F, +, \cdot)$ は可換環である．

(2) 任意の $x \in F (x \neq 0)$ に対し，逆元 x^{-1} が存在する．

F が有限集合で $(F, +, \cdot)$ が体となるとき，F を**有限体**または**ガロア体**と呼ぶ．有限体 F の元の数を F の**位数**と呼び，位数 q の有限体を $\mathrm{GF}(q)$ と書く．

多項式環

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$
$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0 \in \mathbb{Z}[x],$$

$(m \geq n)$ に対して，和と積を定義する．

和

$$f(x)+g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + (a_n + b_n) x^n + \cdots + (a_1 + b_1) x + a_0 + b_0$$

積

$$\begin{aligned} f(x) \cdot g(x) &= (a_n \cdot b_m) x^{n+m} + \cdots + (a_1 b_0 + a_0 b_1) x + a_0 b_0 \\ &= \sum_k \left(\sum_{i+j=k} a_i b_j \right) x^k \end{aligned}$$

定理　3

$(\mathbb{Z}[x], +, \cdot)$ は環である.

定理 4

$\mathbb{Z}[x]$ の任意の多項式 $f(x) \in \mathbb{Z}[x]$ とモニックな l 次多項式 $(l \geq 1)$ $g(x) \in \mathbb{Z}[x]$ について,

$$f(x) = g(x) \cdot q(x) + r(x) \quad (\deg(r(x)) \leq l - 1)$$

となる商 $q(x)$ と剰余 $r(x)$ が一意に存在する.

定理 5

$\mathbb{Z}[x]$ 上の多項式 $f(x), g(x), d(x), k(x)$ に対して，
$d(x)|f(x)$ かつ $d(x)|g(x)$ を満たすことは
$d(x)|g(x)$ かつ $d(x)|(f(x) - k(x)g(x))$ となるための必要十分条件である.
つまり，$\gcd(f(x), g(x)) = \gcd(g(x), f(x) - k(x)g(x))$ が成り立つ.

問題 2

整数 a, b の最大公約数を求めるためのユークリッドアルゴリズムのように，定理 5 を用いて $\mathbb{Z}[x]$ 上の多項式 $f(x), g(x)$ の最大公約多項式を求めることができるかどうか考えなさい.

F: 体

定理 6

$(\mathbb{F}[x], +, \cdot)$ は環である.

定理 7

$F[x]$ の任意の多項式 $f(x) \in F[x]$ と $g(x) \in F[x]$ について，

$$f(x) = g(x) \cdot q(x) + r(x) \quad (\deg(r(x)) \leq l - 1)$$

となる商 $q(x)$ と剰余 $r(x)$ が一意に存在する.

定理 8

$F[x]$ 上の多項式 $f(x), g(x), d(x), k(x)$ に対して，
$d(x)|f(x)$ かつ $d(x)|g(x)$ を満たすことは
$d(x)|g(x)$ かつ $d(x)|(f(x) - k(x)g(x))$ となるための必要十分条件である．

問題 3

$\mathbb{Z}_5$ 上の多項式 $f(x) = x^4 + 3x^3 + x$, $g(x) = 2x^3 + 3x + 2$ に対して, $f(x)$ と $g(x)$ の最大公約多項式を求めよ.

定理 9

$F[x]$ の多項式 $f(x)$, $g(x)$ に対し，

$$\gcd(f(x), g(x)) = f(x)u(x) + g(x)v(x)$$

なる $F[x]$ の多項式 $u(x)$,$v(x)$ が存在する.
また，$f(x)$, $g(x)$ は共に 0 でないとすると

$$\deg(u(x)) < \deg(g(x)), \deg(v(x)) < \deg(f(x))$$

なる $u(x)$, $v(x)$ が一意に存在する.

問題 4

$\mathbb{Z}_5$ 上の多項式 $f(x) = x^4 + 3x^3 + x$, $g(x) = 2x^3 + 3x + 2$ に対して

$$\gcd(f(x), g(x)) = f(x)u(x) + g(x)v(x)$$

を満たす $u(x)$ と $v(x)$ を求めよ.

F: 体
$m(x)$: 多項式環 $F[x]$ のある多項式

Definition

$f(x), r(x) \in F[x]$ に対して，次のような二項関係を定義する.

$$f(x) \sim r(x) \Leftrightarrow m(x) | f(x) - r(x)$$

このとき，$f(x)$ と $r(x)$ は $m(x)$ を法として合同であるという.

定理 10

二項関係 $\sim$ は $F[x]$ 上の同値関係であり，その同値類 ($m(x)$ を法とする**剰余類**という）がなす $F[x]$ の商集合 $F[x]/(m(x))$ は，$m(x)$ を法とする多項式の和と積を加法と乗法として**環**となる.
特に，$m(x)$ が **F 上既約である**ならば，$F[x]/(m(x))$ は**体**である.

問題 5

(1) 二項関係 $\sim$ は $F[x]$ 上の同値関係であることを示せ.

(2) $m(x)$ が F 上既約であるならば, $f(x) \in F[x]/(m(x))$ が乗法逆元を持つことを示せ.

$F = \mathrm{GF}(2)$ 上の 2 次の既約多項式 $m(x) = x^2 + x + 1$ を法として得られる剰余類環 $F[x]/(m(x))$ は，位数が 2^2 の有限体 $\mathrm{GF}(4)$ をなす.

$$F[x]/(m(x)) = \{\overline{0}, \overline{1}, \overline{x}, \overline{x+1}\}$$

問題 6

$\mathbb{Z}_2[x]$ の多項式 $m(x) = x^3 + x + 1$ を考える.

(1) $m(x)$ は $\mathbb{Z}_2$ 上既約であるか答えよ.

(2) 剰余類環 $\mathbb{Z}_2[x]/(m(x))$ の代表元を答えよ.

素数 p に対して，$\mathbf{Z}_p$ は位数が p の有限体であり，$\mathrm{GF}(p)$ とも表す.

$m(x) = x^2 + x + 1 = 0$ は，GF(2) 上では根をもたないので，α を GF(2) には属さない虚根であると仮定するしよう.
そのとき，

$$\alpha^2 + \alpha + 1 = 0$$

という関係式が成り立ち，

$$\alpha^2 = \alpha + 1$$

であることに注意すると，

$$\begin{array}{rcl}
\alpha^0 & = & 1 \\
\alpha^1 & = & \alpha \\
\alpha^2 & = & \alpha + 1 \\
\alpha^3 & = & \alpha^2 + \alpha = \alpha + 1 + \alpha = 1 \\
\alpha^4 & = & \alpha \\
 & \vdots &
\end{array}$$

という関係式が成り立つ.

α の 2 次以上の多項式は，α の 1 次以下の多項式に書き換えることができる.
α の 1 次以下の多項式全体からなる集合を

$$K = \{0, 1, \alpha, \alpha + 1\}$$

とする.

K は加法，乗法の演算に関して閉じており，さらに体である.

K 上の演算

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

$\cdot$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

$K = \{0, 1, \alpha, \alpha^2\}$
α を原始元という.

定理 11

体 F 上の多項式 $m(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ が既約である場合，$m(x) = 0$ の１つの根を α とすると，

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

である.
F 上の α の $n-1$ 次以下の多項式の全体を K とするとき，K は体となり，$F[x]/(m(x))$ と同型である.
この体 K を F の拡大体と呼び，F を基礎体と呼ぶ.

F の位数を q, $m(x)$ の次数を n とするとき，K は q^n 個の要素を持つので $\mathrm{GF}(q^n)$ と表される. 位数 q が素数であるとき，$\mathrm{GF}(q)$ は素体であるという.

問題 7

$F = \mathrm{GF}(2)$ 上の 3 次の既約多項式 $m(x) = x^3 + x + 1$ を用いて，F の拡大体 $K = \mathrm{GF}(2^3)$ を構成する.

(1) K の元を $m(x) = 0$ の根 α を用いて表せ.

(2) K の 0 を除くすべての元が α のベキ乗で表現できることを確認せよ.

(3) K の加法，乗法に関する演算表を作れ.

定義 6

K を位数 q の有限体とする. K の乗法単位元 1 に対して,

$$s1 = 0$$

となる最小の整数 s を K の標数という.

定理 12

有限体の標数は素数である

定理 13

有限体 K は位数が素数べき p^n (p は素数，n は $n \geq 1$ なる整数) のときに存在し，またそのときに限る.

定理 14

GF(q) の任意の元 a に対して，$a^q - a = 0$ が成り立つ.

つまり，GF(q) 上の多項式 $x^q - x$ は GF(q) 上で次のように因数分解できる.

$$x^q - x = x(x - a_1)(x - a_2)\cdots(x - a_{q-1})$$

ここで $a_1, a_2, \ldots, a_{q-1}$ は GF(q) の 0 以外の要素である.

定理 15

K を標数 p の有限体とするとき，K 上では次の式が成り立つ.

$$(x+y)^p = x^p + y^p$$

定理 16

p を素数とし，$q = p^n$ とする．$f(x)$ を $\mathrm{GF}(q)$ 上の多項式とし，α を $\mathrm{GF}(q)$ の拡大体 K 上での $f(x) = 0$ の根とすると，α^q もまた K 上での $f(x) = 0$ の根である．

K を $F = \mathrm{GF}(q)$ の拡大体とし，β を K の元とする. β を根とする次数最小の F 上の多項式 $m(x)$ を β の F 上の最小多項式という.
また $\mathrm{GF}(q)$ の原始元の最小多項式を原始既約多項式と呼ぶ.

例 1

問 7 の GF(2^3) の各元の GF(2) 上の最小多項式は以下の通りである.

β	$m(x)$
0	x
1	$x-1$
α	x^3+x+1
α^2	x^3+x+1
α^3	x^3+x^2+1
α^4	x^3+x+1
α^5	x^3+x^2+1
α^6	x^3+x^2+1

また，多項式 $x^8 - x$ は $\mathrm{GF}(2^3)$ 上で，

$$x^8 - x = x(x-1)(x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)(x-\alpha^5)(x-\alpha^6)$$

と因数分解され，さらに $\mathrm{GF}(2)$ 上で，

$$x^8 - x = x(x-1)(x^3+x+1)(x^3+x^2+1)$$

と因数分解される.

定理 17

同じ位数をもつ２つの有限体は同型である.

GF(2^4)

- $m(x) = x^4 + x + 1 = 0$：GF(2) 上の既約多項式
- $\alpha : m(x) = 0$ の根, $\alpha^4 + \alpha + 1 = 0$ が成り立つ

$$
\begin{array}{rcl rcl}
\alpha^0 & = & 1 & \alpha^8 & = & \alpha^4 + \alpha^2 + \alpha = \alpha^2 + 1 \\
\alpha^1 & = & \alpha & \alpha^9 & = & \alpha^3 + \alpha \\
\alpha^2 & & & \alpha^{10} & = & \alpha^4 + \alpha^2 = \alpha^2 + \alpha + 1 \\
\alpha^3 & & & \alpha^{11} & = & \alpha^3 + \alpha^2 + \alpha \\
\alpha^4 & = & \alpha + 1 & \alpha^{12} & = & \alpha^4 + \alpha^3 + \alpha^2 = \alpha^3 + \alpha^2 + \alpha + 1 \\
\alpha^5 & = & \alpha^2 + \alpha & \alpha^{13} & = & \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha^3 + \alpha^2 + 1 \\
\alpha^6 & = & \alpha^3 + \alpha^2 & \alpha^{14} & = & \alpha^4 + \alpha^3 + \alpha = \alpha^3 + 1 \\
\alpha^7 & = & \alpha^4 + \alpha^3 = \alpha^3 + \alpha + 1 & \alpha^{15} & = & \alpha^4 + \alpha = 1
\end{array}
$$

という関係式が成り立つ.

GF(2^4) の元の最小多項式

β	$m(x)$
0	x
1	$x-1$
$\alpha, \alpha^2, \alpha^4, \alpha^8$	x^4+x+1
$\alpha^3, \alpha^6, \alpha^{12}, \alpha^9$	$x^4+x^3+x^2+x+1$
α^5, α^{10}	x^2+x+1
$\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}$	x^4+x^3+1

$$x^{16}-x = x(x-1)(x^2+x+1)(x^4+x+1)(x^4+x^3+x^2+x+1)(x^4+x^3+1)$$