環(ring)

集合:A

A 上の２項演算：＋，・

１．(A, ＋)は可換群

２．(A, ・)は半群

３．分配律(distributive law)が成り立つ

$\forall a, b, c \in A$

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

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

(A, +, ・) を環とよぶ

(A, ＋)の単位元をゼロ元とよび 0 で表す

要素 $a \in A$ の＋に関する逆元：$-a$

例１ 整数全体の集合:Z

(Z, + ）は可換群

(Z, ･）は半群

$a, b, c \in Z$ ならば

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

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

分配律が成り立つ

↓

（Z, +, ･ ）は環

例２ $(2x^2 + 1) + (2x^3 + x^2 + 5x - 1)$

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

$(2x - 1)(4x^2 + 2x + 1) = (8x^3 - 1)$

実数係数の多項式の全体は環をなす

↓

多項式環（polynomial ring）

体（Field）

集合:A

A 上の２項演算：＋，・

１．（A, ＋）は可換群

２．（A－{ 0 }, ・）は群

　　0 は(A, ＋)のゼロ元

３．分配律が成り立つ

　　$\forall a, b, c \in A$

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

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

（A, +, ・） を体とよぶ

「体」という名称の由来

有機的に機能が働くという意味合いからドイツ語でKörper（身体の意味）と名付けられた

例

有理数全体の集合 : $\mathbb{Q}$

加算 : ＋, 乗算 : ･

1. ($\mathbb{Q}$, +)は可換群

　($\mathbb{Q}$, +)の零元 : 0

2. ($\mathbb{Q}-\{0\}$, ･)は群

3. 分配律が成り立つ

↓

($\mathbb{Q}$, +, ･) は体（有理数体）

実数, 複素数も体をなす（実数体, 複素数体）

整数は体をなさない

有限体（finite field）

$Z_n = \{ 0, 1, \cdots, n-1 \}$

+ : n を法とする剰余和

・: n を法とする剰余積

n が素数であるときのみ(Z_n, +, ・)は体になる

例　n=4 の場合，$Z_4 = \{ 0, 1, 2, 3 \}$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

・	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

　(Z_4, +)は可換群だが($Z_4 - \{ 0 \}$, ・)は群ではないので(Z_4, +, ・)は体ではない

一般に要素数が有限個（p 個）の体を有限体（finite field）とよぶ

体（F, ＋, ･）上の多項式（polynomial on field）

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

$a_i \in F\ (i = 0 \sim n),\quad a_n \neq 0$

F 上のすべての多項式の集合を $F[x]$で表す

体上の多項式の加算と乗算

係数の和と積の計算は F 上で行い，x のべき乗は今まで通り $x^i \cdot x^j = x^{i+j}$（i＋j は通常の加算）とすればよい

例　$Z_2 = \{0,1\}$上の多項式 $f(x) = x^2 + x + 1,\ g(x) = x+1$

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

$$= x^2$$

$$f(x) \cdot g(x) = (x^2 + x + 1) \cdot (x + 1) = x^3 + x^2 + x + x^2 + x + 1$$

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

$F[\mathrm{x}]$の加法単位元（ゼロ元）: 0（=F のゼロ元）

（ $F[\mathrm{x}]$, + ）は可換群

乗法単位元: 1（=F の乗法単位元）

($F[\mathrm{x}]$, ・ ）は半群

したがって（$F[\mathrm{x}]$,+,・）は環となる

→ 体 F 上の多項式環（polynomial ring over F）

($F[\mathrm{x}]-\{0\}$, ・)は群ではないので（$F[\mathrm{x}]$,+,・）は体ではない!

体上の多項式の減算と除算

例　$Z_2=\{0,1\}$上の多項式 $f(x)=x^2+x+1$, $g(x)=x+1$

f(x)の加法逆元: $-f(x)=(-1)x^2+(-1)x+(-1)$

-1 は Z_2 上の 1 の加法逆元なので $-1=1$

$-f(x)=x^2+x+1$ となるので

$g(x)-f(x)=g(x)+(-f(x))=(x+1)+(x^2+x+1)=x^2$

f(x)を g(x)で割ったときの商 q(x)と余り r(x)は

$$
\begin{array}{r|l}
 & x \\ \cline{2-2}
x+1 & x^2+x+1 \\
 & x^2+x \\ \cline{2-2}
 & \qquad\quad 1
\end{array}
$$

q(x)=x, r(x)=1 となる