現代数学への流れ　第1回

復習　可換環

R：集合，$+$，$\cdot$：R上の二つの演算

$(R, +, \cdot)$が可換環であるとは，次の条件たちをみたすことである．

(i)　$(R, +)$はアーベル群．単位元を0で表す．

(ii)　ある$1 \in R$が存在して，任意の$r \in R$について$r \cdot 1 = 1 \cdot r = r$がいえる．

(iii)　任意の$r_1, r_2, r_3 \in R$に対して

$$(r_1 \cdot r_2) \cdot r_3 = r_1 \cdot (r_2 \cdot r_3)$$

がいえる

(iv)　任意の$r_1, r_2 \in R$に対して$r_1 \cdot r_2 = r_2 \cdot r_1$が成り立つ．

(v)　任意の$r_1, r_2, r_3 \in R$に対して$r_1 \cdot (r_2 + r_3) = r_1 \cdot r_2 + r_1 \cdot r_3$

が成り立つ．

可換環 R が体であるとは，さらに以下の２つの条件が成り立つことをいう．

(vi) $0 \neq 1$．

(vii) 任意の $r \in R \setminus \{0\}$ について $r^{-1} \in R$ が存在して $r \cdot r^{-1} = 1$ がいえる．

例 $\mathbb{Z}$：可換環，体ではない．

例 $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$；体

例 $d \in \mathbb{Z} \setminus \{0, 1\}$ を平方因子を持たない整数とする．

このとき，$\sqrt{d} \notin \mathbb{Z}$ がいえる．

$$\mathbb{Z}[\sqrt{d}] = \{ x + y\sqrt{d} \mid x, y \in \mathbb{Z} \}$$

は可換環になる．

$\mathbb{Z}[\sqrt{d}]$ が和と積で閉じていることを確認する.

$x+y\sqrt{d}$, $z+w\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ について

$$(x+y\sqrt{d})+(z+w\sqrt{d}) = (x+z)+(y+w)\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$$

$$(x+y\sqrt{d})(z+w\sqrt{d}) = (xz+ywd)+(xw+yz)\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$$

//

例 $n \in \mathbb{Z}$

$\mathbb{Z}/n\mathbb{Z}$ $\quad \bar{x}+\bar{y}=\overline{x+y} \quad \bar{x}\cdot\bar{y}=\overline{x\cdot y}$

により. $\mathbb{Z}/n\mathbb{Z}$ は可換環になる.

$\mathbb{Z}/n\mathbb{Z}$ が体 $\iff$ n は素数.

A, B : 可換環

写像 $\phi : A \to B$ が 環の準同型であるとは 以下が成り立つことをいう.

(i) 任意の $x, y \in A$ について $\phi(x+y) = \phi(x) + \phi(y)$ が成り立つ

(ii) 任意の $x, y \in A$ について $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$ が成り立つ.

(iii) $\phi(1_A) = 1_B$ がいえる.

<u>例</u>

$$\begin{array}{ccc} \phi : \mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ x & \mapsto & \overline{x} \end{array}$$

環の準同型 $\phi : A \to B$ が 同型であるとは, ϕ が 全単射のことをいう.

命題1　$\phi : A \to B$, $\psi : B \to C$: 環の準同型

(i) $\psi \circ \phi : A \to C$ も準同型

(ii) ϕ が同型ならば、$\phi^{-1} : B \to A$ も同型.

(∵) 略
//

定義2　R : 可換環

R が整域であるとは以下をみたすことをいう.

(i) $0 \neq 1$

(ii) $r_1, r_2 \in R \setminus \{0\}$ について $r_1 \cdot r_2 \neq 0$ がいえる.

$r \in R$ が零因子であるとは、$r' \in R \setminus \{0\}$ で $r \cdot r' = 0$ が成りたつものが存在することである. R が整域とは R の零因子が 0 のみのことをいう.

例 $\mathbb{Z}$：整域

例 F：体　このとき、Fは整域。

∵ $a \in F \setminus \{0\}$ が零因子とすると、$ab=0$ となる $b \in F \setminus \{0\}$ が存在するが、このとき、$b = a^{-1}ab = 0$ より $b \neq 0$ に矛盾。

∴ aは零因子ではなく、Fは整域。 //

例 $\mathbb{Z}/6\mathbb{Z}$ は整域でない。

∵ $\overline{2} \neq \overline{0}$　$\overline{3} \neq \overline{0}$ だが

$\overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$

//

多項式環

R: 可換環

R-係数多項式環を

$$R[x] = \{ a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in R \}$$

で定める。このとき、$f(x) = a_0 + \cdots + a_n x^n$ について

$g(x) = b_0 + \cdots + b_m x^m$

$$f(x) = g(x) \iff a_i = b_i \text{ for any } i = 0, \ldots$$

とする。$R[x]$ には以下により和と積が定まる。

$f(x) = a_0 + \cdots + a_n x^n$ に対して

$g(x) = b_0 + \cdots + b_m x^m$

$$f(x) + g(x) = a_0 + b_0 + \cdots + (a_i + b_i) x^i + \cdots$$

$$f(x)\,g(x) = \sum_{d=0}^{m+n} \Bigl(\sum_{\substack{i+j=d \\ i \geq 0,\ j \geq 0}} a_i b_j \Bigr) x^d$$

これにより、$R[x]$ は可換環になる.

$r \in R$ について

$$\begin{array}{cccc} \phi_r : & R[x] & \longrightarrow & R \\ & \in & & \in \\ & f(x) & \longmapsto & f(r) \end{array}$$

は 環の準同型になる.

<u>定義3</u> $f(x) \in R[x] \neq 0$ について $a_n \neq 0$ のとき, n を f の次数と呼び,

$$f(x) = a_0 + \cdots + a_n x^n \qquad \deg f(x) = n$$

と表す, $f(x) = 0$ のとき $\deg f(x) = -\infty$ とする.

例 $\mathbb{C}[x] \ni x^3 - 2x^2 + 1 = f(x)$ $\qquad \deg f(x) = 3$.

命題4 $f(x),\ g(x) \in R[x] - \{0\}$ について

(i) $\deg(f(x)+g(x)) \leqq \max\{\deg f(x),\ \deg g(x)\}$

(ii) $f(x)$、または $g(x)$ の最高次係数が零因子でないとき、

$$f(x)\cdot g(x) \neq 0$$

がいえ、$\deg f(x)g(x) = \deg f(x) + \deg g(x)$ がいえる。

(iii) R が整域のとき、$R[x]$ も整域

略 //

命題5 K: 体　$f(x),\ g(x) \in K[x]$ で $g(x) \neq 0$ とする。

このとき、$q(x),\ r(x) \in K[x]$ が存在して

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

がいえる。

(∵) $f(x)=0$ のとき $q(x)=0$, $r(x)=0$ とできるので.
$f(x)\neq 0$ とする. $\deg f(x) < \deg g(x)$ のとき $q(x)=0$ $r(x)=f(x)$ で良い.

そこで $\deg f(x) \geqq \deg g(x)$ とする.

$f(x)= a_0 + \cdots + a_n x^n$ $(a_n \neq 0)$

$g(x) = b_0 + \cdots + b_m x^m$ $(b_m \neq 0)$

としたとき. $g_1(x) = f(x) - \dfrac{a_n}{b_m} x^{n-m} g(x)$ とおけば.

$\deg g_1(x) < \deg f(x) = n$

がいえる. ∴ 帰納法より.

$g_1(x) = g(x) q_1(x) + r_1(x)$ $(\deg r_1(x) < \deg g(x))$

とする $q_1(x)$, $r_1(x) \in K[x]$ が見つかる.

$$\therefore f(x) = g_1(x) + \frac{a_n}{b_m} x^{n-m} g(x) = g(x)\left(\frac{a_n}{b_m}x^{n-m} + q_1(x)\right) + r_1(x)$$

がいえ。 $q(x) = \frac{a_n}{b_m} x^{n-m} + q_1(x)$ $r(x) = r_1(x)$ とすれば良い。 //

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

$$
\begin{array}{r}
x - 2 \\
x^2+2x+1 \overline{) x^3 + 1} \\
x^3 + 2x^2 + x \\
\hline
-2x^2 - x + 1 \\
-2x^2 - 4x - 2 \\
\hline
3x + 3
\end{array}
$$

$\therefore$ $x^3 + 1 = (x^2+2x+1)(x-2) + 3x + 3$.

命題6 K: 体 $\alpha_1, \cdots, \alpha_n \in K$: 相異なる元.

$f(x) \in K[x]$

任意の $i = 1, \cdots, n$ に対して $\cancel{f(x)} =$ $f(\alpha_i) = 0$ とする.

このとき $f(x) = g(x)(x_1 - \alpha_1) \cdots (x_n - \alpha_n)$ $g(x) \in K[x]$

とできる.

㊀ $f(x) = (x-\alpha_1)\cdots(x-\alpha_i)\,g_i(x)$ とできたとする.

このとき $f(\alpha_{i+1}) = (\alpha_{i+1}-\alpha_1)\cdots(\alpha_{i+1}-\alpha_i)\,g_i(\alpha_{i+1})$ より.

$\overset{\shortparallel}{0}$

$g_i(\alpha_{i+1}) = 0$ がいえる.

ところで 命題 より.

$g_i(x) = (x-\alpha_{i+1})\,g_{i+1}(x) + c \quad (c \in K)$

とできる. $g_i(\alpha_{i+1}) = 0$ より. $c = 0$ がいえる.

$\therefore\ f(x) = (x-\alpha_1)\cdots(x-\alpha_{i+1})\,g_{i+1}(x)$

とできる. //

系7 $f(x) \in K[x]$ $\deg f = n > 0$ のとき.

f は 高々 n 個の根を K 上に持つ.

多変数多項式環

R：可換環

帰納的に

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

で定める。このとき、$f(x_1, \cdots, x_n) \in R[x_1, \cdots, x_n]$ は

$$f(x) = \sum_{\substack{i_1 \geq 0 \cdots i_n \geq 0 \\ \text{有限和}}} a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}$$

と表される。

系8　R：整域のとき、$R[x_1, \cdots, x_n]$ も整域。

部分環

定義9 A: 可換環

$B \subset A$ が部分環であるとは、

A の和と積に関して B が環になり、かつ $1_A \in B$ が成り立つことをいう。

補題10 A: 可換環　$B \subset A$: 部分集合

B が A の部分環であることの必要十分条件は以下をみたすこと。

(i) B が和に関して A の部分群である。

(ii) $a, b \in B$ について $a \cdot b \in B$ が成り立つ。

(iii) $1_A \in B$

例 $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ は全て部分環

例 $d \neq 1$: 平方因子を持たない整数

$\mathbb{Z}[\sqrt{d}] = \{ x + y\sqrt{d} \mid x, y \in \mathbb{Z} \}$

このとき. $\mathbb{Z}[\sqrt{d}] \subset \mathbb{C}$ は 部分環

$\mathbb{C}$は 体で 整域 なので. $\mathbb{Z}[\sqrt{d}]$ も 整域

例　$\mathbb{C}[x^2] \subset \mathbb{C}[x]$: 部分環.

$$\mathbb{C}[x^2] = \{ a_0 + a_1 x^2 + \cdots + a_n x^{2n} \mid a_i \in \mathbb{C} \}$$

命題 11　$\phi : A \to B$: 環準同型

このとき. $\mathrm{Im}(\phi) = \{ \phi(a) \mid a \in A \} \subset B$ は Bの部分環.

∵ $\mathrm{Im}(\phi) \subset B$ が 和に関し 部分群 になるのは ok.

(ii) $\phi(a), \phi(b) \in \mathrm{Im}(\phi)$ について

$$\phi(a)\cdot\phi(b) = \phi(ab) \in \mathrm{Im}(\phi)$$

(iii) $1_B = \phi(1_A) \in \mathrm{Im}(\phi)$

//

イデアル

定義 12 R: 可換環 $I \subset R$: 部分集合.

I がイデアルとは以下が成り立つことをいう.

(i) I は和に関して R の部分群

(ii) $r \in R$ $a \in I$ $\Rightarrow$ $r \cdot a \in I$.

例 $R = \mathbb{Z}$ $I = n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$ はイデアル.

$n \in \mathbb{Z}$

例　R：可換環　$x_1, \cdots, x_n \in R$

$$(x_1, \cdots, x_n) := \{ r_1 x_1 + \cdots + r_n x_n \mid r_i \in R \}$$

は $x_1, \cdots, x_n$ を含む最小のイデアル。

$x_1, \cdots, x_n$ で生成されるイデアルという。

∵ (i)　$(x_1, \cdots, x_n) \subset R$：部分群

∵　$0 = 0 \cdot x_1 + \cdots + 0 \cdot x_n \in (x_1, \cdots, x_n)$

$r_1 x_1 + \cdots + r_n x_n + r_1' x_1 + \cdots + r_n' x_n = (r_1 + r_1') x_1 + \cdots + (r_n + r_n') x_n \in (x_1, \cdots, x_n)$

$-(r_1 x_1 + \cdots + r_n x_n) = (-r_1) \cdot x_1 + \cdots + (-r_n) x_n \in (x_1, \cdots, x_n)$　//

(ii)　$r \in R$　$r_1 x_1 + \cdots + r_n x_n \in (x_1, \cdots, x_n)$

$r \cdot (r_1 x_1 + \cdots + r_n x_n) = (r \cdot r_1) x_1 + \cdots + (r r_n) x_n \in (x_1, \cdots, x_n)$

∴ $(x_1, \cdots, x_n)$ はイデアル。

Iをイデアルで $x_1,\cdots,x_n \in I$ とすると.

(iii)より. $r_i x_i \in I$

∴ $r_1x_1+\cdots+r_nx_n \in I$

∴ $(x_1,\cdots,x_n) \subset I$.

よって $(x_1,\cdots,x_n)$ は $x_1,\cdots,x_n$ を含むイデアルの中で最小 //

命題13 $\phi: A \to B$: 環準同型

このとき. $\ker(\phi)=\{a\in A \mid \phi(a)=0\}$ は Aのイデアル.

$\ker(\phi)$ が Aの部分群はok.

$r\in A$ $a\in \ker(\phi)$ について

$\phi(ra) = \phi(r)\,\phi(a) = \phi(r)\cdot 0=0$

より. $ra \in \ker(\phi)$. //

例 K: 体 $X \subset K^n$: 部分集合.

$R = K[x_1, \dots, x_n]$

$I(X) = \{ f(x) \in R \mid f(a_1, \dots, a_n) = 0 \text{ for any } (a_1, \dots, a_n) \in X \}$

は R の イデアル.

∵ $0 \in I(X)$ は ok.

$f, g \in I(X)$ について $f(a_1, \dots, a_n) + g(a_1, \dots, a_n) = 0 + 0 = 0$

が $(a_1, \dots, a_n) \in X$ について いえる. ∴ $f + g \in I(X)$

$\forall h \in K[x_1, \dots, x_n]$ $f \in I(X)$ について $(a_1, \dots, a_n) \in X$ ならば

$h(a_1, \dots, a_n) f(a_1, \dots, a_n) = h(a_1, \dots, a_n) \cdot 0 = 0$

がいえる. ∴ $hf \in I(X)$

//

例 R：可換環　$I \subset R$：イデアル

$u \in R^{\times}$：単元

このとき、$I \ni u \iff I = R$ がいえる。

∵ $I \ni u \Rightarrow r = ru^{-1}u \in I \quad \therefore R = I$

$(\Leftarrow)$ は明らか。//

例 K：体　K のイデアルは

$\{0\}$ と K のみ

例 $\phi : K \to F$：体の準同型

このとき、$\ker(\phi) = \{0\}$

$\therefore$ ϕ は単射