非可換の世界を覗いてみよう

筑波大学数学系　星野光男

意識したことはないと思いますが、我々が扱っている数（実数または複素数）というのは「掛け算の順序が交換可能である」という著しい性質を持っています。つまり、我々は可換の世界で暮らしているわけです。従って、非可換の世界（即ち、掛け算の順序が交換可能でない様な数を基にした世界）においては、我々の常識が必ずしも通用しないという事態が起こり得ます。実際、可換から遠く離れた世界では、ちょっと想像出来ない様な現象が起こります。ここでは、非可換の世界をほんのちょっとだけ覗いてみることにしましょう。

1　環

整数全体の集合を $\mathbb{Z}$ で表すことにします。本節では、$\mathbb{Z}$ が持っている代数的な構造を抽出して、「環」の概念を導入しましょう。

先ず、範囲が確定したものの集まりのことを**集合**と呼びます。また、もの a が集合 A に属するとき、$a \in A$ と書き a のことを集合 A の**元**または**要素**と呼びます。特に、元をひとつも持たない集合も考え、それを**空集合**と呼びます。

定義１　空でない集合 A に２種類の演算（それぞれ**和**、**積**と呼ばれる）

$$A \times A \to A,\ (a,b) \mapsto a+b, \quad A \times A \to A,\ (a,b) \mapsto ab$$

が定義されていて、以下の条件（１）～（７）がみたされるとき、A のことを**環**と呼びます：

（１）任意の $a, b \in A$ に対して $a+b=b+a$ が成り立つ；

（２）任意の $a, b, c \in A$ に対して $(a+b)+c=a+(b+c)$ が成り立つ；

（３）ある特別な元 $0 \in A$ が存在して、任意の $a \in A$ に対して $a+0=a$ が成り立つ（この元 0 のことを A の**零元**と呼びます）；

（４）任意の $a \in A$ に対して、$a+x=0$ をみたす $x \in A$ が存在する（この x のことを $-a$ と書きます。また、$a+(-b)$ のことを $a-b$ と書きます）；

（５）任意の $a, b, c \in A$ について、$(ab)c=a(bc)$ が成り立つ；

（６）ある特別な元 $1 \in A$ が存在して、任意の $a \in A$ に対して $1a=a1=a$ が成り立つ（この 1 のことを A の**単位元**と呼びます）；

（７）任意の $a, b, c \in A$ に対して $(a+b)c=ac+bc,\ a(b+c)=ab+ac$ が成り立つ。

演習問題１　環 A について、次の（１）～（６）を証明しなさい。
（１）零元 0 は一意である。
（２）任意の $a \in A$ に対して、$-a$ は一意である。
（３）単位元 1 は一意である。
（４）任意の $a \in A$ に対して、$a0 = 0a = 0$ が成り立つ。
（５）任意の $a, b \in A$ に対して、$(-a)b = a(-b) = -ab$ が成り立つ。
（６）もし $0 = 1$ が成り立てば、A の元は 0 だけである。

以下においては、演習問題１の（６）を考慮に入れて、環はすべて条件“ $0 \neq 1$ ”をみたすと仮定しましょう。

定義２　環 A において、任意の $a, b \in A$ に対して $ab = ba$ が成り立つとき、A のことを**可換環**と呼びます。更に、“ $a \neq 0, b \neq 0 \ \Rightarrow \ ab \neq 0$ ”をみたす可換環のことを**整域**と呼びます。

さて、$\mathbb{Z}$ が整域であることは明らかですが、整域ではない可換環の例を紹介しましょう。

例１　自然数 $p \geq 2$ をかってに固定します。整数 $a, b \in \mathbb{Z}$ に対して、$a - b$ が p で割り切れるとき、a と b とは p を**法として合同**であると言い

$$a \equiv b \pmod{p}$$

と書くことにします。各 $n \in \mathbb{Z}$ に対して、$\mathbb{Z}$ の部分集合

$$[n] = \{a \in \mathbb{Z} \mid a \equiv n \pmod{p}\}$$

のことを（p を法とする）n の合同類と呼びます。このとき、

$$[n] = [m] \ \Leftrightarrow \ n \equiv m \pmod{p}$$

が成り立ちます。互いに異なる合同類全体の集合を $\mathbb{Z}/(p)$ で表すことにします。このとき、

$$\mathbb{Z}/(p) = \{[n] \mid 0 \leq n \leq p - 1\}$$

が成り立ちます。さて、$\mathbb{Z}/(p)$ における和、積をそれぞれ

$$[n] + [m] = [n + m], \qquad [n][m] = [nm]$$

と定義すれば、$\mathbb{Z}/(p)$ は可換環となります。更に、p が素数であることと $\mathbb{Z}/(p)$ が整域であることとは同値です。

演習問題２　例１の主張を確かめなさい。

この節の最後に、可換ではない環の例を挙げましょう。

例２　$\mathbf{F}_2 = \mathbb{Z}/(2)$ とおきます。例１でみたように、$\mathbf{F}_2$ は $[0], [1]$ の２個の元から成る整域です。さて、$\mathbf{F}_2$ の元を成分に持つ２次の行列のなかで

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$$

の形のもの全体の集合を A としましょう。このとき、通常の行列の和、積に関して A は可換でない環になります。

演習問題３　例２の主張を確かめなさい。

実は、例２の環は可換でない環のなかで元の個数が最小のものです。先ず、例２の環は８個の元から成ることがすぐ判ります。他方、元の個数が７個以下の環は可換です。少し難しいかもしれませんが、これの証明に挑戦してみてください。

演習問題４　元の個数が７個以下の環は可換であることを証明しなさい。

２　体

実数全体の集合を $\mathbb{R}$ と書くことにします。本節では、$\mathbb{R}$ が持っている代数的な構造を抽出して「体」の概念を導入しましょう。

定義３　環 A の元 $0 \neq a \in A$ に対して、$ax = xa = 1$ をみたす $x \in A$ が存在するとき、この元 x のことを a^{-1} と書き a の**逆元**と呼びます。

演習問題５　環 A について、次の（１）～（３）を証明しなさい。
（１）元 $0 \neq a \in A$ に対して、$ax = ya = 1$ をみたす $x, y \in A$ が存在すれば、$x = y$ である。
（２）元 $0 \neq a \in A$ に対して、もし a^{-1} が存在すれば a^{-1} は一意である。
（３）元 $a, b \in A$ に対して、逆元 a^{-1}, b^{-1} がともに存在すれば、$(ab)^{-1}$ が存在し、$(ab)^{-1} = b^{-1}a^{-1}$ が成り立つ。

定義４　環 A において、すべての $0 \neq a \in A$ が逆元 a^{-1} を持つとき、A のことを**斜体**と呼びます。特に、可換な斜体のことを**体**と呼びます。

演習問題６　有限個の元から成る整域は体であることを証明しなさい。

さて、$\mathbb{R}$ が体であることは明らかですが、その他の体の例を紹介しましょう。

例３　有理数全体の集合を $\mathbb{Q}$ で表すことにします。このとき、任意の $q \in \mathbb{Q}$ に

対して、$\mathbb{R}$ の部分集合

$$\mathbb{Q}(\sqrt{q}) = \{a + b\sqrt{q} \mid a, b \in \mathbb{Q}\}$$

は通常の和、積に関して体になります。

演習問題７　例３の主張を確かめなさい。

例４　例２において p が素数のとき、$\mathbf{F}_p = \mathbb{Z}/(p)$ は p 個の元からなる体になります。

演習問題８　例４の主張を確かめなさい。

さて、次節で体ではない斜体の例を構成してみせますが、その前に複素数の構成を復習しましょう。

例５　集合 $\mathbb{R}^2 = \{(a, b) \mid a, b \in \mathbb{R}\}$ における和、積をそれぞれ

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

$$(a_1, b_1)(a_2, b_2) = (a_1a_2 - b_1b_2, a_1b_2 + b_1a_2)$$

によって定義します。また、文字 i を用いて

$$(a, b) = a + bi$$

と書くことにします。ただし、

$$a + 0i = a, \quad 0 + bi = bi, \quad a + (-b)i = a - bi$$

と書きます。このとき、集合

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$$

における和、積がそれぞれ

$$(a_1 + b_1i) + (a_2 + b_2i) = (a_1 + a_2) + (b_1 + b_2)i$$

$$(a_1 + b_1i)(a_2 + b_2i) = (a_1a_2 - b_1b_2) + (a_1b_2 + b_1a_2)i$$

によって定義され、$\mathbb{C}$ は体になります。この体 $\mathbb{C}$ のことを**複素数体**と呼びます。特に、$i^2 = -1$ であることに注意して下さい。この文字 i のことを**虚数単位**と呼び、$\sqrt{-1}$ とも書きます。

演習問題９　例５の主張を確かめなさい。

3　四元数体

本節では、例５における複素数体 $\mathbb{C}$ の構成を少し変えて、ハミルトンの四元数体と呼ばれる斜体を構成しましょう。

例６　集合 $\mathbb{R}^4 = \{(a,b,c,d) \mid a,b,c,d \in \mathbb{R}\}$ における和、積を次のように定義します：和は成分ごとの和

$$(a_1,b_1,c_1,d_1) + (a_2,b_2,c_2,d_2) = (a_1+a_2, b_1+b_2, c_1+c_2, d_1+d_2)$$

によって定義し、積は

$$(a_1,b_1,c_1,d_1)(a_2,b_2,c_2,d_2) = (a_3,b_3,c_3,d_3)$$

ただし

$$\begin{aligned} a_3 &= a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2 \\ b_3 &= a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2 \\ c_3 &= a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2 \\ d_3 &= a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2 \end{aligned}$$

によって定義します。また、文字 i,j,k を用いて

$$(a,b,c,d) = a + bi + cj + dk$$

と書くことにします。このとき、集合

$$\mathbf{H} = \{a + bi + cj + dk \mid a,b,c,d \in \mathbb{R}\}$$

における和、積がそれぞれ

$$\begin{aligned} &(a_1 + b_1i + c_1j + d_1k) + (a_2 + b_2i + c_2j + d_2k) \\ &\qquad = \ (a_1+a_2) + (b_1+b_2)i + (c_1+c_2)j + (d_1+d_2)k \end{aligned}$$

$$\begin{aligned} &(a_1 + b_1i + c_1j + d_1k)(a_2 + b_2i + c_2j + d_2k) \\ &\qquad = \quad (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) \\ &\qquad\quad + (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)i \\ &\qquad\quad + (a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)j \\ &\qquad\quad + (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)k \end{aligned}$$

によって定義され、$\mathbf{H}$ は斜体になります。この斜体 $\mathbf{H}$ のことを**ハミルトンの四元数体**と呼びます。また

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j$$

が成り立ちます。特に、$\mathbf{H}$ においては -1 の平方根が $\pm i, \pm j, \pm k$ の６個存在します。

演習問題１０　例６の主張を確かめなさい。

定義５　環 A に対して、すべての $x \in A$ に対して $ax = xa$ が成り立つような元 a 全体から成る集合を $Z(A)$ と書き、A の**中心**と呼びます。

演習問題１１　次の（１）～（３）を証明しなさい。
（１）任意の環に対して、中心は可換環である。
（２）斜体の中心は体である。
（３）ハミルトンの四元数体 $\mathbf{H}$ の中心は実数体 $\mathbb{R}$ である。

4　スコフィールドの定理

本節では、１９８０年代に A. Schofield によって証明された斜体の拡大に関する定理を紹介しましょう。（斜体のことを英語で skew field と呼びますが、名前がよく似てますね。）残念ながら、具体的な構成方法を紹介することはできません。ここでは、単に事実だけを述べることにします。

定理　任意の自然数 $n, m \geq 2$ に対して、次のような斜体 D, E が存在する：
（１）E は D の拡大である。即ち、E は D を含んでいて D の演算は E の演算を制限したものである。
（２）左拡大次数は n である。即ち、ある n 個の元 $v_1, \ldots, v_n \in E$ が存在して、任意の $x \in E$ は

$$x = a_1 v_1 + \cdots + a_n v_n, \quad a_1, \ldots, a_n \in D$$

の形に一意に表せる。
（３）右拡大次数は m である。即ち、ある m 個の元 $w_1, \ldots, w_m \in E$ が存在して、任意の $x \in E$ は

$$x = w_1 b_1 + \cdots + w_m b_m, \quad b_1, \ldots, b_m \in D$$

の形に一意に表せる。

これは驚くべき結果だと思うのですが、驚くためには素養が必要で、おそらくみなさんに驚いて貰えないのが残念です。
最後にひとつだけ注意をしておきましょう。

注意　上の定理において、D が中心上有限次元であったとしましょう。即ち、ある有限個の元 $u_1, \ldots, u_l \in D$ が存在して、任意の $y \in D$ が

$$y = c_1 u_1 + \cdots + c_l u_l, \quad c_1, \ldots, c_l \in Z(D)$$

の形に一意に表せると仮定しましょう。このとき、$nl = ml$ が成り立ち、従って $n = m$ が成り立ちます。つまり、中心上有限次元の斜体を扱う限りにおいては、そんなに不思議な現象は起こりません。

5　参考書

　スコフィールドの定理を除けば、本原稿の内容は代数学の入門書ならどの本にも書いてあります。例えば

・松阪和夫著「代数系入門」岩波書店

等を参照して下さい。スコフィールドの定理については、構成方法を理解するには何年もかかりますので、参考書は挙げません。