行列で「数」を作ろう(2018年公開講座)

斎藤秀司

2018年11月23日

小学生の頃より親しんできた数の概念. 最初は自然数

$$\mathbb{N} = \{0, 1, 2, 3, \dots\},$$

整数

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\},$$

有理数

$$\mathbb{Q} = \{a/b \mid a, b \in \mathbb{Z},\ b \neq 0\}.$$

さらに実数，そして複素数と数の世界は広がっていきます. 実数全体の集合を $\mathbb{R}$ で表すと複素数全体の集合は

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

と書けます. ここで $i = \sqrt{-1}$ は虚数単位，つまり二乗して -1 になる数です. しかしながらいったいそんな数がどうして存在すると確信できるのでしょうか？この講義では行列を使うことによりそのような「数」が有理数から作りだせることを解説します.

1　環：数の抽象化

この説では、「環」という概念を使って、「数」を抽象化します。

定義 1.1 環とは、$\mathbb{C}$ の部分集合 K で加法と乗法の演算について閉じているものである.

例 1.2 $\mathbb{Q}, \mathbb{R}$.

例 1.3 $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$.

例 1.4 $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

ここで環の概念をさらに少し広げてみましょう. 有理数を成分に持つ2行2列の行列全体

$$M_2(\mathbb{Q}) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Q}\}$$

とその部分集合

$$K_0 = \{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{Q}\}$$

を考えます．$M_2(\mathbb{Q})$ は加法と乗法という二つの演算をもちます，K_0 はこれらに関して閉じています．また写像

$$f : \mathbb{Q} \to K_0 \,;\, a \to \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

は明らかに集合としての一対一写像 (全単射) を与えますが、それぞれの集合がもつ演算に関して整合的です．つまり

$$f(a+b) = f(a) + f(b),\ f(ab) = f(a)f(b)\ \ (a, b \in \mathbb{Q})$$

が成り立ちます[1]．このよう写像を「環の同型」といいます．これにより $\mathbb{Q}$ と K_0 を演算を込めて同一視することができます．このことは環の概念をさらに抽象化して，「適当な公理を満たす加法と乗法をもつ集合」として定義することを示唆しています．これについては講義の中で解説しましょう．

次に $M_2(\mathbb{Q})$ の部分集合

$$K_1 = \{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a \in \mathbb{Q}\}$$

と写像

$$g : \mathbb{Q}(i) \to K_1 \,;\, a + bi \to \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

を考えます．これが環の同型であることが簡単に確かめられます．

それでは $M_2(\mathbb{Q})$ の部分集合 K_2 と環の同型 $h : \mathbb{Q}(\sqrt{2}) \to K_2$ を構成することができるでしょうか？それには $A \in M_2(\mathbb{Q})$ で

$$A^2 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$$

なるものを探し出して

$$K_2 = \{a + bA \mid a, b \in \mathbb{Q}\}$$

として h を

$$h(a + b\sqrt{2}) = a + bA\ \ (a, b \in \mathbb{Q})$$

と定義すればいいわけです．つまり有理数を成分として持つ行列を使って $\sqrt{2}$ の役目を果たすものが作り出せればいいわけです．そのような A としては例えば

$$A = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

がとれますが，ほかにも無限個のチョイスが存在します．それらをすべて求めるには次の定理を使います．

---

[1] 正確には $f(0) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ という性質も必要

定理 1.5

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Q})$$

にたいし X を変数とする多項式

$$\phi_A(X) = X^2 - (a+d)X + (ad - bc)$$

を A の特性多項式と呼ぶ．このとき

$$\phi_A(A) = A^2 - (a+d)A + (ad-bc)I = O$$

が成り立つ．ただし

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad O = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

上の定理により，$A^2 = 2I$ から

$$(a+d)A = (ad - bc + 2)I$$

が導かれ，これから

$$A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}, \quad a^2 + bc = 2$$

がすべてのチョイスを与えることがわかります.[2]

2 不可能の証明

それでは 2 の実数 3 乗根 $\sqrt[3]{2}$ を同様にして行列から作り出すことはできるでしょうか？つまり $A \in M_2(\mathbb{Q})$ で $A^3 = 2I$ となるものは存在するでしょうか？実はこれは不可能です．これを証明してみましょう．

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

とおけば，定理 1.5 により，$\phi_A(A) = O$ がなりたちます．一方，$f(X) = X^3 - 2$ とおけば仮定から $f(A) = O$ が成り立ちます．ここで $f(X)$ を $\phi_A(X)$ で割り算して

$$f(X) = \phi_A(X)q(X) + r(X)$$

と書きます．ここで $q(X), r(X)$ は $\mathbb{Q}$-係数の多項式で，$q(X) = X - c$ は 1 次式で，$r(X) = 0$ または $r(X)$ は 1 次式です．$r(X) = 0$ とすれば $X^3 - 2 = \phi_A(X)(X-c)$ となり $X^3 - 2$ が $\mathbb{Q}$ に根をもつことになり矛盾です．$r(X) = X - d$ が 1 次式とすると

$$O = A^3 - 2I = \phi_A(A)q(A) + r(A) = A - dI = 0$$

となります．$A^3 = 2I$ なので $d^3 = 2$ でなくてはなりませんが，$d \in \mathbb{Q}$ であったのでこれも矛盾です．以上で不可能の証明が完了です．

[2] くわしいことは講義で解説します.

$A^3 = 2I$ となる $\mathbb{Q}$ に成分をもつ行列は2行2列では存在しませんでしたが，3行3列では可能です．例えば

$$A = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

がこの条件を満たします．もっと一般に与えられた $\mathbb{Q}$-係数の n 次多項式

$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_0$$

にたいし n 次正方行列

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ & & & 1 & -a_{n-1} \end{pmatrix}$$

を考えると $f(A) = 0$ をみたすことが示せます．

それでは $\mathbb{Q}$ に成分をもつ n 次正方行列を使って円周率 π を作り出すことは可能でしょうか？問題を正確に定式化すると次のようになります．複素数であって，適当な $\mathbb{Q}$-係数の多項式 $f(X)$ にたいし $f(\pi)$ とかけるもの全体を $\mathbb{Q}[\pi]$ とします．すると L は定義 1.1 の意味で環となります．問題は

問題 2.1 自然数 n と $M_n(\mathbb{Q})$ の部分環[3] L で環の同型 $\mathbb{Q}[\pi] \simeq L$ が存在するものがあるか？

実は，これが不可能であることが1882年にフェルディナント・フォン・リンデマンによって証明された次の定理から従います[4]．

定理 2.2 π は超越数である。つまり、$\mathbb{Q}$-係数の多項式の根とはならない。

この定理より、古代ギリシアの三大作図問題の内の一つ「円積問題」（与えられた長さを半径とする円と等積の正方形を作図すること）が不可能であることが従います。

[3]行列の演算で閉じている部分集合
[4]詳しいことは講義で説明します．