環論 NO.9 要約

$\boxed{\text{今日のテーマ}}$

《余りを許した割り算のできる環 (ユークリッド環)》

これ以降、この講義では「環」と単に言えば可換環のことを指すことにする。

$\mathbb{Z}$ と $k[X]$ の二つにまず共通して言えることは、どちらも「余りのある割り算」が出来ることである。

余りのある割り算なら出来るのが当たり前のことに思えるかも知れない。しかし、たとえば
$\mathbb{Z}[X]$ の中で考えて X^2 を $2X+1$ で割った余りは？
$\mathbb{C}[X,Y]$ の中で考えて X^3+Y^3 を $XY+1$ で割った余りは？

などと聞かれると困ってしまう。ポイントは、「どこで割り算が終ったか分かるような尺度があるかどうか」という点にある。そこで次の定義をする。

定義 9.1. 環 R が**ユークリッド環**であるとは、整列順序集合 W と 写像 $\rho : R \to W$ があって、次の性質を満たすときに言う ($a \in R$ に対して $\rho(a)$ のことは a の「次数」「ノルム」などとよばれる。)

(1) R の元 a の「次数」 $\rho(a)$ が最小 $\Leftrightarrow a = 0$

(2) R の元 a, b $(a \neq 0)$ に対して、

$$b = aq + r, \quad q, r \in R, \quad \rho(r) < \rho(a)$$

となる q, r が存在する。

(「W が整列集合である」とは、W は順序集合であって、しかも「W の任意の部分集合 X は最小元を持つ」というときにいう。この定義が難しく感じられる諸君には $W = \mathbb{N}$ (もしくはそれと本質的には同じであるがずらしたようなもの) と思っても初級の段階には充分である。)

補題 9.2 (ユークリッド環の基本例)**.** $\mathbb{Z}$, $k[X]$ (k は体) はともにユークリッド環である。

割り算の原理としては次の補題 9.3 もよく使う。(最高次の係数が 1 である一変数多項式のことをモニックな多項式と呼ぶ。)

補題 9.3 (モニックな多項式による割り算)**.** R を単位元を持つ可換環とする。$R[X]$ の元 a がモニックならば、任意の $b \in R[X]$ に対して、

$$b = aq + r, \quad q, r \in R, \quad \deg(r) < \deg(a)$$

となる $q, r \in R[X]$ が存在する。

定義 9.4. 環 R のイデアル I が**単項イデアル**であるとは、ある $a \in R$ が存在して、 $I = (a)$ が成り立つときに言う。

R の全てのイデアルが単項イデアルであるとき、R は**単項イデアル環**であると言う。

定理 9.5. ユークリッド環は単項イデアル環である。

系 9.6. 整数 a, b が与えられているとし、その最大公約数を d とおく。このとき、

$$al + bm = d$$

をみたす整数 l, m が存在する。(ベズーの等式)

上に限らずベズーの等式は任意の単項イデアル環に対して成り立つ。

系 9.7. k を体とする。k 上の多項式 a, b が与えられているとし、その最大公約数を d とおく。このとき、

$$a(X)l(X) + b(X)m(X) = d(X)$$

をみたす k 上の多項式 l, m が存在する。

実際に l, m を計算するには、次のような方法が便利である。

例題 9.8 (ユークリッドの互除法). 等式

$$72l + 56m = 8$$

を満たす整数 l, m の組を一組求めよ。

(解答) まず次のような計算を行う

小学生の計算 (★)	数式訳	行列算
72 わる 56 は 1　あまり 16	$72 = 56 \times 1 + 16$	$\begin{pmatrix} 72 \\ 56 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 56 \\ 16 \end{pmatrix}$
56 わる 16 は 3　あまり 8	$56 = 16 \times 3 + 8$	$\begin{pmatrix} 56 \\ 16 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 16 \\ 8 \end{pmatrix}$
16 わる 8 は 2　あまり 0	$16 = 8 \times 2 + 0$	$\begin{pmatrix} 16 \\ 8 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 8 \\ 0 \end{pmatrix}$

(★小学生の計算の部分は諸君の分かりやすいように書き加えたが、本当の答案には書かないほうがよい。)

各々の行の行列算を組み合わせると、

$$\begin{pmatrix} 72 \\ 56 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 8 \\ 0 \end{pmatrix}$$

を得る。この式の右辺に現れる正方行列はすべて $M_2(\mathbb{Z})$ の元として可逆であることに注意して、上の式を次のように変形することが出来る。

$$\begin{aligned} \begin{pmatrix} 8 \\ 0 \end{pmatrix} &= \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} 72 \\ 56 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 72 \\ 56 \end{pmatrix} = \begin{pmatrix} -3 & 4 \\ 7 & 9 \end{pmatrix} \begin{pmatrix} 72 \\ 56 \end{pmatrix} \end{aligned}$$

この式の第一行に着目すると、$8 = (-3) \times 72 + 4 \times 56$ を得る。

(答え)　$l = -3, m = 4.$

上の行列算で

- b を a で割ると商が q で余りが r であること ($b = aq + r$) を行列算で
$$\begin{pmatrix} b \\ a \end{pmatrix} = \begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ r \end{pmatrix}$$
と書けること
- 出てくる行列 $\begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix}$ の逆行列が
$$\begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix}$$
と $\mathbb{Z}$ (もっと一般には、考えているユークリッド環) の範囲内で計算できること

が大事である。

問題

(I) $a(X) = X^3 + X + 1, b(X) = X^3 - 2X^2 + 5X$ のとき、等式

$$a(X)l(X) + b(X)m(X) = 1$$

を満たす多項式 $l, m \in \mathbb{C}[X]$ の組を一組見つけなさい。今回はその見付けかたまで込めて書くこと。

(II) $\mathbb{Z}[\sqrt{-1}]$ はユークリッド環である。(その証明は本問題では書かなくてもよいことにする。ρ としては《絶対値》を考え、q としては b/a にもっとも近い $\mathbb{Z}[\sqrt{-1}]$ の元をとればよい。($|b/a - q| \leq \sqrt{2}/2$ に出来る。)) このことを用いて、$\mathbb{Z}[\sqrt{-1}]$ の元

$$a = 21 - 28\sqrt{-1}, \quad b = 40$$

の最大公約数をユークリッドの互除法を用いて求めなさい。

ヒント:

$|a|^2 = 1225 < 1600 = |b|^2$ であるから、まずは b を a で割ることになる。

$$\frac{b}{a} = \frac{b\overline{a}}{|a|^2} = \frac{40(21 + 28\sqrt{-1})}{1225} \fallingdotseq 0.686 + 0.914\sqrt{-1}$$

であるから、商 q はこの値にもっとも近い $\mathbb{Z}[\sqrt{-1}]$ の元、すなわち $q = 1 + \sqrt{-1}$ である。余りは $r = b - qa$ で求められる。結局、最初の除法は

$$40 = (1 + \sqrt{-1})(21 - 28\sqrt{-1}) + (-9 + 7\sqrt{-1})$$

という具合になる。