

今日のテーマ

《割り算の原理(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よう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、「どこで割り算が終わ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。そこで次のような定義をする。

定義 8.1. 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 $\rho: R \rightarrow W$ (「重さ」を調べる写像) があって、次の性質を満たすときに言う

- (1) R の元 a の「重さ」 $\rho(a)$ 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 $W = \mathbb{N}$ と思っても実用上は充分である。)

補題 8.1 (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こともよく使う。

補題 8.2 (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 8.2. 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 8.1. ユークリッド環は単項イデアル環である。

系 8.1. 整数 a, b が与えられているとし、その最小公約数を d とおく。このとき、

$$al + bm = d$$

をみたす整数 l, m が存在する。

系 8.2. k を体とする。 k 上の多項式 a, b が与えられているとし、その最小公約数を 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 8.1 (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なう

$$72 \div 56 = 1 \text{ 余り } 16 \quad 72 = 56 \times 1 + 16 \quad \begin{pmatrix} 72 \\ 56 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 56 \\ 16 \end{pmatrix}$$

$$56 \div 16 = 3 \text{ 余り } 8 \quad 56 = 16 \times 3 + 8 \quad \begin{pmatrix} 56 \\ 16 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 16 \\ 8 \end{pmatrix}$$

$$16 \div 8 = 2 \text{ 余り } 0 \quad 16 = 8 \times 2 + 0 \quad \begin{pmatrix} 16 \\ 8 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 8 \\ 0 \end{pmatrix}$$

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) $l = -3, m = 4$.

次の補題は単項イデアルの包含関係を生成元の関係に翻訳しなおしている。

補題 8.3. 単位元をもつ可換環 R の元 a, b に対して、次の二つは同値である。

- (1) イデアルの包含関係 $(a) \subset (b)$ がある。
- (2) a は b の倍元である。すなわち、ある $c \in R$ があって、 $a = bc$ が成り立つ。

レポート問題

つぎのうち一問を選択して解きなさい。(期限: 次の講義の終了時まで。)

(I) 等式

$$(X^3 + 2X^2 + 3X + 4)f(X) + (X^3 + 2X + 2)g(X) = 1$$

を満たす多項式 $f, g \in \mathbb{C}[X]$ 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

$$7 + 24\sqrt{-1}, \quad 25$$

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。