§8. 多項式の剰余とユークリッドの互除法

一般に、多項式を多項式で割り切ることはできないが、整数の場合と同様に、商と余りを考えることができる。また、2 個 (以上の) 多項式に対して最大公約数 (= 整数の場合と同じ役割を果たす多項式) を考えることができ、それをユークリッドの互除法の多項式版を用いて求めることができる。ここでは、これらの理論を学ぶ。

● 8 - 1 : 除法の定理

除法の原理の多項式版を述べよう。

定理 8 - 1 - 1 (除法の定理)

任意の多項式 $f, g \in \mathbb{K}[X],\ g \neq 0$ に対して、次の条件 (i)(ii) を満たす多項式 $q, r \in \mathbb{K}[X]$ が一意的に存在する。

(i) $f = gq + r$.

(ii) $0 \leq \deg r < \deg g$ または $r = 0$.

q を、f を g で割ったときの**商** (quotient) といい、r を、f を g で割ったときの**剰余** (remainder) または**余り**という。

(**証明**)

証明の便宜上、$\deg 0 := -1$ と定める（この証明の中だけで通用する定義)。

I. q, r の存在の証明：

$\deg f$ に関する数学的帰納法で証明する。

① $\deg f = -1$ の場合：

$f = 0$ であるから、$q := 0,\ r = 0$ とおけばよい。

② n を 0 以上の整数とし、$\deg f < n$ を満たすすべての多項式 $f \in \mathbb{K}[X]$ について、定理は成り立つと仮定する。

$\deg f = n$ を満たす任意の多項式 $f \in \mathbb{K}[X]$ を考える。

- $\deg g > n$ のときには、$q = 0,\ r = f$ とおけばよい。
- $\deg g \leq n$ のときには、

$$f = a_0 + a_1 X + \cdots + a_n X^n \qquad (a_n \neq 0,\ a_0, a_1, \ldots, a_n \in \mathbb{K})$$

と書き、$m = \deg g$ とおいて、

$$g = b_0 + b_1 X + \cdots + b_m X^m \qquad (b_m \neq 0,\ b_0, b_1, \ldots, b_m \in \mathbb{K})$$

と書く。このとき、

$$f_1 := f - \frac{a_n}{b_m} X^{n-m} g \quad \in \ \mathbb{K}[X]$$

とおくと、$\deg f_1 < n$ となる。帰納法の仮定から、$f_1 = q_1 g + r_1$ かつ $\deg r_1 < \deg g$ を満たす多項式 $q_1, r_1 \in \mathbb{K}[X]$ が存在する。よって、

$$q := \frac{a_n}{b_m} X^{n-m} + q_1, \qquad r := r_1$$

とおけばよい。

II. q, r の一意性の証明：

f が次のように二通りに表わされたとする。

$$f = gq + r = gq' + r', \qquad \deg r,\ \deg r' < \deg g$$

このとき、$q = q'$ かつ $r = r'$ となることを証明すればよい。まず、式変形して、

$$(*) \qquad g(q-q') = r'-r$$

を得る。ここで、$q-q' \neq 0$ と仮定すると、$r'-r = g(q-q') \neq 0$ であり、

$$\max\{\deg r,\ \deg r'\} \geq \deg(r'-r) = \deg g + \deg(q-q') \geq \deg g$$

を得る。これは、$\deg r,\ \deg r' < \deg g$ に矛盾する。よって、$q = q'$ であり、したがってまた、等式 $(*)$ より $r = r'$ である。 □

例 8 - 1 - 2 有理係数多項式 $f = X^5 - 3X - 2,\ g = X^4 + 2X^3 + 1$ に対して、f を g で割ったときの商と剰余を求めよ。

解；

$f - qg$ の次数が $\deg g = 4$ より小さくなるような多項式 $q \in \mathbb{R}[X]$ が求まればよい。

まず、f から X^5 の項を消すために Xg を引く。次に、$f - Xg = -2X^4 - 4X - 2$ から X^4 を消すために $-2g$ を引く。すると、$f - Xg + 2g = 4X^3 - 4X$ となる。これより、$q = X - 2,\ r = 4X^3 - 4X$ とおけば、$f - qg = r,\ \deg r < \deg g$ となるから、f を g で割ったときの商と剰余はそれぞれ $q = X - 2,\ r = 4X^3 - 4X$ である。 □

● 8 - 2 : 最大公約数

2 つの多項式 $f, g \in \mathbb{K}[X]$ に対して、$f = gh$ となる $h \in \mathbb{K}[X]$ が存在するとき、g は f の**約数** (divisor) である、あるいは、f は g で**割り切れる** (divisible)、あるいは、f は g の**倍数** (multiple) であるといい、記号で $g|f$ と書く。

注意 1：f が g で割り切れないことを $g \nmid f$ によって表わす。

注意 2：$f \neq 0$ ならば $g \neq 0$ であり、$\deg g \leq \deg f$ となる。

注意 3：多項式なのに約数、倍数と呼ぶのは少し変な気がするが、このような呼び方（翻訳）が定着している。英語の“divisor”“multiple”は、それぞれ“割るもの”“何倍かされたもの”という意味であり、“数”に限らず使うことができる。

例 8 - 2 - 1 有理数係数多項式 $f = 2X^4 + 2X^3 - X^2 + X - 1$ は、$\mathbb{Q}[X]$ において、$f = (2X^2 + 1)(X^2 + X - 1)$ と書けるので、$2X^2 + 1$ は f の約数である。また、$f = (X^2 + \frac{1}{2})(2X^2 + 2X - 2)$ とも書けるので、$X^2 + \frac{1}{2}$ も f の約数である。

上の例からわかるように、一般に、$g \in \mathbb{K}[X]$ が $f \in \mathbb{K}[X]$ の約数であれば、g に 0 でない定数 $a \in \mathbb{K}$ を掛けて得られる多項式 ag もまた f の約数になる。通常、多項式の約数・倍数を考える際には、0 でない定数倍の違いは無視する。

定理 8 - 2 - 2

n 個の多項式 $f_1, \ldots, f_n \in \mathbb{K}[X]$ $(f_1 \neq 0)$ に対して、次の条件 (i)(ii) を満たす多項式 $d \in \mathbb{K}[X]$ が定数倍を除いて一意的に存在する。

(i) $d|f_i$ $(i = 1, \ldots, n)$.

(ii) $d'|f_i$ $(i = 1, \ldots, n)$ を満たす任意の $d' \in \mathbb{K}[X]$ について $\deg d' \leq \deg d$.

また、このような多項式 d は $\mathbb{K}[X]$ の部分集合

$$\{\ a_1f_1+\cdots+a_nf_n \mid a_1,\ldots,a_n\in\mathbb{K}[X]\ \}$$

の中の 0 でない次数最小の元として特徴づけられる。したがって、この集合は d の倍数の全体に一致する：

$$\{\ a_1f_1+\cdots+a_nf_n \mid a_1,\ldots,a_n\in\mathbb{K}[X]\ \}=\{\ ad \mid a\in\mathbb{K}[X]\ \}.$$

条件 (i)(ii) を満たす多項式 d の中で最高次の係数が 1 のものを $f_1,\ldots,f_n$ の**最大公約数** (the greatest common divisor) といい、$\gcd(f_1,\ldots,f_n)$ または、単に、$(f_1,\ldots,f_n)$ で表わす。

(**証明**)

ここでは $n=2$ の場合に証明する（一般の場合も全く同様に証明できる）。

以下、$f=f_1,\ g=f_2$ とおく。

I. d の存在の証明：

$$I:=\{\ af+bg \mid a,b\in\mathbb{K}[X]\ \}$$

とおく。$0\neq f\in I$ であるから、I は 0 でない元を含む。したがって、I の中に、0 でない多項式 d_0 であって、次数最小のものが存在する（自然数の整列性）。この d_0 が (i)(ii) を満たすことを示す。

(i) は任意の $h\in I$ に対して $d_0|h$ となることから従う。詳細は演習問題とする (演習 8-1)。

(ii) $d'\in\mathbb{K}[X]$ が $d'|f$ かつ $d'|g$ を満たしているとする。すると、任意の $a,b\in\mathbb{K}[X]$ に対して、$d'|(af+bg)$ となる。したがって、任意の $h\in I$ に対して、$d'|h$ となる。$d_0\in I$ だから、$d'|d_0$ を得る。特に、$\deg d'\leq\deg d_0$ を得る。

Ⅱ. d の一意性の証明：

条件 (i)(ii) を満たす $d\in\mathbb{K}[X]$ は、I の証明の中の d_0 と定数倍を除いて一致することを示せばよい。まず、d が (i) の条件を満たすことと I(ii) の証明より、$d|d_0$ を得る。よって、

$$(*)\qquad d_0=dq\quad(q\in\mathbb{K}[X])$$

と書くことができる。一方、d,d_0 は条件 (i)(ii) を満たすから、

$$(**)\qquad \deg d=\deg d_0$$

が成り立つ。$(*)(**)$ により、$q\in\mathbb{K}$ でなければならない（$d_0\neq0$ より $q\neq0$ に注意）。

Ⅲ. (i)(ii) を満たす多項式が I の中の 0 でない次数最小の元として特徴づけられること：

I の中の 0 でない次数最小の元が (i)(ii) を満たすことは、I の中で証明されている。逆に、(i)(ii) を満たす多項式 d をとると、Ⅱ の証明から、$d_0=dq\ \ (q\in\mathbb{K}-\{0\})$ となる。よって、$d=q^{-1}d_0\in I$ であり、d は I の中の 0 でない次数最小の元（のうちの 1 つ）である。 □

注意 1：条件 (i)(ii) を満たす多項式 d のことを $f_1,\ldots,f_n$ の最大公約数と呼ぶのが一般的であるが、この授業では一意性を重視して、最高次の係数が 1 のものだけを最大公約数と呼ぶ。

注意 2：定理 (の証明) より、$d\in\mathbb{K}[X]$ を $f_1,\ldots,f_n$ の最大公約数とするとき、d は $d'|f_i\ (i=1,\ldots,n)$ を満たす任意の $d'\in\mathbb{K}[X]$ によって割り切れることがわかる。

演習 8-1　上の定理の証明中の下線部分を証明せよ。

ヒント：h を d_0 で割った余りが 0 となることを示す。

0 でない多項式 $f_1,\ldots,f_n\in\mathbb{K}[X]$ の最大公約数が 1 のとき、$f_1,\ldots,f_n$ は**互いに素** (relatively prime) であるという。[定理 8-2-2] から直ちに次が導かれる。

系 8 - 2 - 3
0 でない多項式 $f_1, \ldots, f_n \in \mathbb{K}[X]$ に対して

$f_1, \ldots, f_n$ が互いに素
$\iff$ $a_1 f_1 + \cdots + a_n f_n = 1$ を満たす多項式 $a_1, \ldots, a_n \in \mathbb{K}[X]$ が存在する

● 8 - 3 : ユークリッドの互除法

最大公約数はユークリッドの互除法を用いて求めることができる。

命題 8 - 3 - 1
0 でない多項式 $f, g \in \mathbb{K}[X]$ に対して、$f = gq + r$ $(0 \leq \deg r < \deg g$ または $r = 0)$ を満たす $q, r \in \mathbb{K}[X]$ をとる。このとき、次が成り立つ：

$$\gcd(f, g) = \gcd(g, r).$$

(**証明**)

[定理 8 - 2 - 2] により $I = \{\, af + bg \mid a, b \in \mathbb{K}[X] \,\}$, $J = \{\, pg + qr \mid p, q \in \mathbb{K}[X] \,\}$ とおくとき、$I = J$ であることを証明すればよい。

• $I \subset J$ の証明：$f = gq + r$ と表わされるから $f \in J$ であり、$g = 1 \cdot g + 0 \cdot r$ と表わされるから $f \in J$ である。これより、任意の $a, b \in \mathbb{K}[X]$ に対して $af + bg$ は $pg + qr$ $(p, q \in \mathbb{K}[X])$ の形に表わされるから $af + bg \in J$ である。こうして、$I \subset J$ が示された。

• $I \supset J$ の証明：$g = 0 \cdot f + 1 \cdot g$ と表わされるから $g \in I$ である。$r = -f + gq$ と表わされるから $r \in I$ である。先と同じ議論により $J \subset I$ であることがわかる。

以上より、$I = J$ が証明された。 □

[命題 8 - 3 - 1] を $\deg f \geq \deg g$ の場合に適用することにより、f と g の最大公約数を求める問題が、より次数の小さい多項式 g と r の最大公約数を求める問題に帰着されることがわかる。したがって、[命題 8 - 3 - 1] を繰り返し適用していけば、最後には割り切れる状態になり、最大公約数が求まる。このようにして最大公約数を求めるアルゴリズムを**ユークリッドの互除法** (Euclidean algorithm) という。

例 8 - 3 - 2 $f = X^5 - 3X - 2$, $g = X^4 + 2X^3 + 1 \in \mathbb{R}[X]$ の最大公約数を求めよ。

解；

$$f = (X - 2)g + 4X^3 - 4X$$
$$g = (\tfrac{1}{4}X + \tfrac{1}{2})(4X^3 - 4X) + X^2 + 2X + 1$$
$$4X^3 - 4X = (4X - 8)(X^2 + 2X + 1) + 12X - 8$$
$$X^2 + 2X + 1 = (\tfrac{1}{12}X + \tfrac{2}{9})(12X - 8) + \tfrac{25}{9}$$

より、f と g の最大公約数は

$$\gcd(f, g) = \gcd(g, 4X^3 - 4X) = \cdots = \gcd(12X - 8, \tfrac{25}{9}) = 1$$

である。 □

演習 8-2* $f = X^4 - 12X^2 - 13X - 12$, $g = X^3 - 4X^2 - 9X + 36$, $h = X^3 + 2X^2 - 2X + 3 \in \mathbb{Q}[X]$ の最大公約数をユークリッドの互除法により求めよ。

ヒント：0 でない任意の $f, g, h \in \mathbb{K}[X]$ について、$\gcd(f, g, h) = \gcd(\gcd(f, g), h)$.