担当教員：宮地 兵衛　研究室：A433　E-mail:miyachi@math.nagoya-u.ac.jp

多項式と互除法

作成日：November 07, 2011　Version：1.2

このプリントの目標

多項式の「最大公約数」,「互いに素」という概念と, それに関連する基本事項について学習する. 今日扱うトピックは線形代数学をはじめ, 現代数学においては最も基礎的である.

多項式とは？

定義 1. 一つの文字 x と, 複素数 $a_0, a_1, \ldots, a_n$ から作られる式

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \tag{1}$$

を, 文字 x の 複素数係数多項式という. $a_n \neq 0$ のとき, n を多項式 (1) の次数という. 但し, 0 という多項式の次数は -1 と定義する. 以下では, 文字 x の 複素数係数多項式を単に多項式と呼び, 多項式 $f(x)$ の次数を $\deg f(x)$ で表す. 多項式の等号 (=文字式としての等号) を恒等式という.

多項式の商と剰余

定理 1. 多項式 $f(x), g(x)$ $(g(x) \neq 0)$ に対して, 恒等式

$$f(x) = g(x)\,q(x) + r(x) \qquad (\text{但し } \deg r(x) < \deg g(x))$$

が成り立つような多項式 $q(x), r(x)$ がちょうど一組存在する.

定義 2. 定理 1 の状況で, $q(x)$ を, $f(x)$ を $g(x)$ で割った商, $r(x)$ を, $f(x)$ を $g(x)$ で割った余りと呼ぶ. $r(x) = 0$ であるとき, $f(x)$ は $g(x)$ で割り切れる, または, $g(x)$ は $f(x)$ を割り切るといい, $g(x)|f(x)$ と書く. 0 は任意の多項式 $g(x)(\neq 0)$ で割り切れることに注意.

問題 1. 次の $f(x), g(x)$ に対して $f(x)$ を $g(x)$ で割った商と余りを求めよ.

(1) $f(x) := 1, \quad g(x) := x^2$.

(2) $f(x) := x, \quad g(x) := 2i$ (i は虚数単位).

(3) $f(x) := x^3 + 5x^2 + 1, \quad g(x) := x^2 + 3$.

問題 2. 定理 1 を用いて, 次の剰余の定理を証明せよ.

> 剰余の定理：多項式 $f(x)$ を $x - a$ $(a \in \mathbb{C})$ で割った余りは $f(a)$ に等しい.

問題 3. 正方行列の最小多項式は固有多項式を割り切ることを示せ.

問題 4. 0 でない 2 つの多項式 $f(x), g(x)$ が 「$g(x)|f(x)$ かつ $f(x)|g(x)$」 という条件をみたすならば, $f(x) = c\,g(x)$ (c は零でない複素数) であることを示せ.

担当教員：宮地 兵衛　研究室：A433　E-mail:miyachi@math.nagoya-u.ac.jp

最大公約式と「互いに素」

定義 3. 多項式 $h(x) \neq 0$ が多項式 $f_1(x), f_2(x), \ldots, f_m(x)$ の各々を割り切る時, $h(x)$ は $f_1(x), f_2(x), \ldots, f_m(x)$ の公約式であるという. 次数の最も高い公約式で, 最高次の係数が 1 であるものを最大公約式とよぶ. 最大公約式は一意に定まる. $f_1(x), f_2(x), \ldots, f_m(x)$ の最大公約式が 1 であるとき, $f_1(x), f_2(x), \ldots, f_m(x)$ は互いに素であるという.

公倍式, 最小公倍式も同様に定義することができるが, ここでは省略する.

定義からすぐに分かる例： 0 でない多項式 $f(x)$ に対し,

(1) $f(x)$ と 0 の最大公約式は $c^{-1}f(x)$ (c は $f(x)$ の最高次の係数) である.

(2) $f(x)$ と a (a は 0 でない複素数) の最大公約式は 1 である.

(3) $f(x)$ と $x-a$ (a は複素数) の最大公約式は, $f(a) \neq 0$ ならば 1, $f(a) = 0$ ならば $x-a$ である. (剰余の定理を使って確かめよ.)

問題 5. 次の各命題の真偽を判定し, 真ならば証明を, 偽ならば反例を与えよ.

(1) 多項式 $f_1(x), f_2(x), \ldots, f_m(x)$ の最大公約式を $d(x)$ とするとき, $d(x)$ と多項式 $f_{m+1}(x)$ の最大公約式は $f_1(x), f_2(x), \ldots, f_m(x), f_{m+1}(x)$ の最大公約式である.

(2) 多項式 $f_1(x)$, $g_1(x)$ が互いに素で, かつ 多項式 $f_2(x)$, $g_2(x)$ が互いに素ならば, $f_1(x)\,f_2(x)$ と $g_1(x)\,g_2(x)$ も互いに素である.

定理 2. $d(x)$ が多項式 $f_1(x), f_2(x), \ldots, f_m(x)$ の最大公約式ならば,

$$f_1(x)\,u_1(x) + f_2(x)\,u_2(x) + \cdots + f_m(x)\,u_m(x) = d(x)$$

となるような多項式 $u_1(x), u_2(x), \ldots, u_m(x)$ が存在する.

この定理の証明はそれほど難しくはない. 整数に関する類似の命題「d が自然数 $f_1, f_2, \ldots, f_m$ の最大公約数ならば, $f_1\,u_1 + f_2\,u_2 + \cdots + f_m\,u_m = d$ となる整数 $u_1, u_2, \ldots, u_m$ が存在する」と平行な議論で証明できる. 時間があれば考えてみると良い.

問題 6. (重要) 定理 2 を用いて, 次の 2 つの条件が同値であることを示せ.

(1) 多項式 $f_1(x), f_2(x), \ldots, f_m(x)$ が互いに素である.

(2) $f_1(x)\,u_1(x)+f_2(x)\,u_2(x)+\cdots+f_m(x)\,u_m(x) = 1$ となるような多項式 $u_1(x), u_2(x), \cdots, u_m(x)$ が存在する.

担当教員：宮地 兵衛　研究室：A433　E-mail:miyachi@math.nagoya-u.ac.jp

ユークリッドの互除法

ここでは 0 でない 2 つの多項式 $f(x)$, $g(x)$ の最大公約式を具体的に求める方法として, ユークリッドの互除法について説明する. 手順は整数についてのユークリッドの互除法と全く同じである.

$\deg f(x) \geq \deg g(x) \neq 0$ として, 次の一連の割り算を行う:

$$\left.\begin{array}{rcll} f(x) & = & g(x)\,q(x) + r_1(x) & \deg g(x) > \deg r_1(x), \\ g(x) & = & r_1(x)\,q_1(x) + r_2(x) & \deg r_1(x) > \deg r_2(x), \\ r_1(x) & = & r_2(x)\,q_2(x) + r_3(x) & \deg r_2(x) > \deg r_3(x), \\ \cdots & & \cdots & \cdots \\ r_{k-2}(x) & = & r_{k-1}(x)\,q_{k-1}(x) + r_k(x) & \deg r_{k-1}(x) > \deg r_k(x), \\ r_{k-1}(x) & = & r_k(x)\,q_k(x). & \end{array}\right\} \quad (2)$$

つまり, $r_{k-1}(x)$ が $r_k(x)$ で割り切れるような最初の $r_k(x)$ まで求めると, $c^{-1}r_k(x)$ (c は $r_k(x)$ の最高次の係数) は $f(x)$, $g(x)$ の最大公約式である. 実際, (2) を下から順に見て行けば, $r_k(x)$ は $f(x)$, $g(x)$ の公約式であることが分かる. また, $h(x)$ が $f(x)$, $g(x)$ の公約式ならば, (2) を上から順に見ることにより, $h(x)$ は $r_k(x)$ を割り切る. 従って, $r_k(x)$ は次数が最大であるような $f(x)$ と $g(x)$ の公約式であるので, $c^{-1}r_k(x)$ は $f(x)$ と $g(x)$ の最大公約式である

問題 7. 次の 2 つの多項式の最大公約式を求めよ.

(1) $x^5 + 2x^4 + x - 1$, $\quad x^4 + 3x^3 - 3x + 1$.

(2) $x^3 - x^2 - 4x + 4$, $\quad x^2 - 2x - 3$.

問題 8. 多項式 $f_1(x), f_2(x), \ldots, f_m(x)$ の係数がすべて実数であるとき, これらの最大公約式 $d(x)$ の係数もすべて実数である. これは何故か？

問題 9. a, b を互いに異なる複素数, m, n を自然数とするとき, $(x-a)^m$ と $(x-b)^n$ は互いに素か? 答えは yes である. では, 実際に $u(x)\,(x-a)^m + v(x)\,(x-b)^n = 1$ となるような多項式 $u(x)$, $v(x)$ を一組求めよ. (ヒント：まず $m = n = 1$ の場合から考えてみよ.)

おまけ：代数学の基本定理/解の公式

高校数学では実数係数の 2 次方程式の解の公式を学んだが, 方程式 $x^2 + 1 = 0$ の解を考えれば分かるように, 一般には解が実数であるとは限らない. では, 複素数係数多項式 $f(x)$ に対して, 方程式 $f(x) = 0$ の解は必ず複素数か？答えは yes である. これは 19 世紀初頭にガウスによって証明された定理で, 非常に重要かつ基本的であるので今日では代数学の基本定理と呼ばれている. 逆に 5 次以上の方程式の解の公式の非存在性がともに若くしてこの世を去ったアーベルやガロワ (例えば「栄光なき天才達」と人名で Google る) といった人々によって示されている. (もっと後で体論で勉強する.)