

# 代数方程式の性質

Joh @物理のかぎプロジェクト

2006-06-21

この辺りで代数方程式の基本的な性質を復習しておきます。主なトピックは、中学校や高校で習う因数分解や剰余定理などです。体の概念が新しいかも知れませんが、それ以外に難しい話はないと思います。

## 代数方程式の定義

(このセクションは [代数学の基本定理](#) に載せた定義を再掲します。)

有限個の数や文字を、『 $+$ ,  $-$ ,  $\times$ ,  $\div$ ,  $\sqrt{\quad}$ 』の5つの演算だけを組み合わせで作った式を **代数式** と呼びます。(それに対して、 $e^x$  や  $\log x$  の入っている式を **超越式** と呼びます)。

未知数が代数式の形で表される方程式を **代数方程式** と呼びます。これは既にみなさんのよく知っている次の形の方程式です。

$$a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n = 0$$

## 体と多項式

すでに [体に関する基本的なこと](#) で触れましたが、代数方程式を解く (多項式  $= 0$  を満たす解を見つける) ことは、体論抜きには考えられません。多項式の係数が体  $F$  に含まれる数であるとき、これを『 $F$  上の多項式』と呼びます。

$$f(x) = c_0 + c_1x + \dots + c_nx^n \quad (c_i \in F) \tag{1}$$

ここで  $x$  の最高次数 (この場合  $n$ ) をこの多項式の **次数** と呼び、 $\deg f = n$  のように書きます。最高次の項の係数 (この場合  $c_n$ ) を **主係数** と呼びます。二つの多項式を足したり掛けたりしたとき、次数に関し

---

\*1 左辺の部分を **多項式** と呼びます。方程式を解くとは、多項式  $= 0$  を満たす変数 (多項式の **零解** と呼びます) を見つけることと見ても良いわけです。今後、上式の左辺だけを指す場合に多項式、多項式の零解を見つけることを念頭に置いている場合には方程式と呼ぶようにしますが、方程式を解くことを多項式を解くと言ってしまう人もいます。しかし、意図する意味は明快ですし、それで混乱して困るようなこともありませんので、それほどこの用語に神経質になる必要はないと思います。

て次の関係が成り立ちます。

$$\deg(f + g) \leq \max\{\deg f, \deg g\} \quad (2)$$

$$\deg(fg) = \deg f + \deg g \quad (3)$$

この関係は、ちょっと例を考えてみればすぐに分かることなので、証明は省略します。定数関数  $f(x) = c$  の次数は 0 です。 $f(x) = 0$  には次数を定めません。

## 商の定理と剰余定理

多項式を多項式で割る、という操作を定義できます。多項式  $f(x)$  を、それより次数の低い多項式  $g(x)$  を使って、次のように表現できます。

$$f(x) = q(x)g(x) + r(x) \quad \deg r(x) < \deg g(x)$$

ここで  $q(x)$  を商、 $r(x)$  を剰余と呼びます。 $f(x)$  が  $g(x)$  で割り切れない場合、剰余の次数は商の次数より小さくなります。例えば、 $f(x) = 3x^3 + 4x^2 + 2x + 5$  を  $g(x) = x^2 - 2x^2 + 1$  で割ると次のように書けます。

$$f(x) = (3x + 10)g(x) + 19x - 5$$

こんな計算練習問題を、中学校や高校でやったことがあると思います。 $r(x) = 0$  のとき、 $f(x)$  は  $g(x)$  で割り切れると言います。

## 剰余定理

特に  $g(x) = x - \alpha$  の形するとき、 $f(x) = (x - \alpha)q(x) + r(x)$  と書けますが、 $x = \alpha$  を代入すると  $f(\alpha) = r(\alpha)$  となりますので、剰余の部分を次のように書き換えられます。

$$f(x) = (x - \alpha)q(x) + f(\alpha)$$

これを 剰余定理 と呼びます。

## 方程式の解

体  $F$  上の点  $a$  が  $f(x) = 0$  の解であるとは、 $a$  が  $f(a) = 0$  を満たすことです。剰余定理を使えば、 $(x - a)$  が  $f(x)$  を割り切ることであり換えても良いでしょう。

ここで、次の定理がなりたちます。

\*2 方程式の係数体に応じて『 $F$  上の多項式』と呼ぶということでしたが、解  $x$  がどのような体に属する数なのかは、これだけでは何も言えません。有理係数の方程式を解いて複素数解が出てくることもあるわけですから、 $x$  は体  $F$  の範囲を『はみ出す』可能性が多いにあります。むしろ、解は係数体をはみ出るのが普通でしょう。今後、解を含む体に関して色々なことを考えていきます。

**theorem**

体  $F$  上の  $n$  次方程式は、 $F$  上に高々  $n$  個の解を持ちます。

**proof**

帰納法によって証明します。まず次数が零の方程式、つまり  $f = c$  は、 $x$  の方程式になっていませんから、 $x = \dots$  の形の解はありません。 $n - 1$  次方程式に対して仮定が正しく、高々  $n - 1$  個の解が存在するとします。このとき  $n$  次方程式  $f(x)$  を考えてみます。解が無ければ、議論はここで終わりですが、仮定には矛盾しません。また、少なくとも1つは解  $a$  を持つとすれば、 $f(x) = (x - a)q(x)$  ( $q(x)$  は  $n - 1$  次多項式) と書いて、仮定より  $q(x)$  は高々  $n - 1$  個の解を持ちますので定理が示されます。

解の個数は  $0 \sim n$  のいずれかで、それは係数の属する体によるわけですが、体が複素数体の場合に限って、 $n$  次方程式は常に  $n$  個の解を含むことが知られています。これは、『代数学の基本定理』の名で知られている大変有名かつ重要な定理です。

**theorem**

複素数体  $C$  上の  $n$  次方程式は、 $C$  上に  $n$  個の解を持つ。

この定理の証明は、体論の他に複素積分の知識を必要とするのでここでは示しません。(歴史的背景については [代数学の基本定理](#) を参照してください。)しかし、この定理の結果は今後とも非常に大事なもので、とりあえず結果だけを認めて先へ進むことにします。

既述した内容の繰り返しになりますが、ここで勉強した要点をおさらいしておきましょう。ある体  $F$  上の  $n$  次代数方程式は、 $0 \sim n$  個の解を持ちます。 $F$  上の解が  $n$  以下の場合には、残りの解が、 $F$  からみ出ているだけです。考える体を少し拡大すれば、もう少したくさん解が見つかるでしょう。そして、複素数体にまで拡大すれば、 $n$  個の解全てが見つかるということです。方程式の解の有無を、拡大体の考えを使って考えると、そのような仕組みが見えてきます。

## 因数分解

体  $F$  上の  $n$  次方程式  $f(x)$  が  $F$  上に  $n$  個全ての解を持つとき、 $f(x)$  は『 $F$  上で因数分解可能である』と言われます。このとき、解  $\alpha_1, \alpha_2, \dots, \alpha_n$  ( $\in F$ ) を使って  $f(x)$  を次のように一次式の積の形に式変形できます。

$$f(x) = c(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n), \quad c \in F \quad (4)$$

代数学の基本定理に従えば、このような式変形は複素数体  $C$  上では常に保証されますが、その他の体上の方程式では『 $C$  には含まれるけれども  $F$  からみ出ない』という解が幾つか存在する可能性があるため、一次式の積に因数分解できるとは限りません。

また、式 (4) は  $f(x)$  の解を明示的に示す形であり、最終的にこのように変形できれば、方程式の解が一目瞭然に分かります。代数学の基本定理は、どんな方程式でも複素数体上で考えれば、この形に書けることを保証しています。ところが『与えられた方程式を、どうやって式 (4) の形に変形したらいいのか?』

という肝心の部分の情報が一切不明です。つまり、代数学の基本定理は、ある代数方程式が『解ける』かどうかを保証するものではありません。解の存在を保証するだけです。

加・減・乗・除・開冪 ( $n$  乗根を求めること) の 5 つの方法を、有限回だけ繰り返して与えられた方程式を式 (4) の形に変形することを『方程式を代数的に解く』と言いますが、与えられた方程式が代数的に解けるかどうかはまた別の問題であり、ガロア理論で論じられることになります。

いま勉強したばかりの拡大体の考えを使うと、『体  $F$  上の方程式  $f(x)$  が解けるかどうか』という問題と、『 $F$  と  $C$  の間のどこかにある、 $f(x)$  の解を全て含む体に  $F$  を上手に拡大できるか』という問題が同値だということが分かるでしょう。