代数的拡大体と最小多項式

Joh @物理のかぎプロジェクト

2006-06-24

代数方程式を体論で考えるとき，この代数的拡大体という概念が一番大事です．気合を入れて取り掛かってください！！まず，体 F に幾つかの元を添加して，拡大体 E を作ることを考えます．

$$F \subset E = F(a_1, a_2, ..., a_n)$$

もしも，E に含まれる全ての元が，F 上の方程式の解になっているならば，E を F の **代数的拡大体** と呼びます．『F 上の方程式の解になっている』というのは，つまり『その元を解とする代数方程式で，係数 $\in F$ である方程式がなにかしら存在する』という主張です．

ここで注意しなければならないのは，ある数が代数的数であることと，拡大体が代数的であることとは少し異なる概念だということです．ある数が代数的数であるとは，その数を解とする **有理係数の代数方程式が存在する** ことでした．F 上の代数拡大体の定義，すなわち，拡大体の任意の元を解とする F **係数の代数方程式が存在する** ことと比べてみましょう．もう気づいたかと思いますが，F が有理数体ではない場合，必ずしも代数的拡大体の元が全て代数的数になるとは限りません．

例えば $\sqrt{\pi}$ は $Q(\pi)$ 上の代数方程式 $x^2 - \pi = 0$ の解ですから，$Q(\sqrt{\pi})$ は $Q(\pi)$ の代数的拡大体になっています．しかし，π は超越数ですから，$Q(\pi)$ や $Q(\sqrt{\pi})$ の元が必ずしも代数的数だとは言えません．代数的拡大とは，あくまでも拡大の仕方に関する概念であって，そこに含まれる元が代数的であるかを規定する概念ではないのです．用語が紛らわしいですが，せっかくなので正確に定義を覚えましょう．

最小多項式

体 F から代数的拡大体 E を作ります．このとき E の元は全て，何らかの F 上の代数方程式の解になっているはずですが，このような代数方程式は無数にあります．

---

*1 体の元が代数的であるとは，その元が Q 上の代数方程式の解になっているということでした．上で例に挙げた $Q(\pi)$ や $Q(\sqrt{\pi})$ は，Q の代数的拡大体になっていませんので代数的ではない元が含まれたわけですが，Q の代数的拡大体として得られる体の元は全て代数的数になります．拡大体の昇鎖列（包含関係の列）が Q とつながっていない場合に注意が必要だということです．

*2 体 F の拡大体 E の元の中に，F 上の代数方程式の解にならないものが含まれるとき，これを超越的拡大体と呼びます．例えば Q の拡大体 $Q(\pi) = \{a + \pi b |\ a, b \in Q\}$ は超越的拡大体です．一般に超越数の話は難しく，この記事でも代数的拡大体の話題だけを取り上げます．

*3 例えば 2 は $x - 2 = 0$ の解ですが，$(x-4)(x-3)(x-2) = 0$ の解でもあります．本質的に，2 は $(x-2)$ の部分だけから出てくるわけですが，このように関係ない因数を加えて次数を上げていけば，2 を解とする代数方程式自体は無限にあるこ

拡大体 E の元 α を元とする F 上の代数方程式の中で，特に次数が最低のものを，α の **最小多項式** と呼びます．最小多項式には次の重要な性質があります．

1. 最小多項式は F 上既約です．
2. 最小多項式は α を解とする，F 上の全ての多項式を割ることが出来ます．

これらの性質は，上の注に補足したイメージを持っていれば明らかでしょう．最小多項式を $\mathrm{Irr}(\alpha, F)$ のように書きます．『α の F 上の最小多項式』と読みます．

最小多項式に関連した定理として，次のものが重要です．

theorem

体 F の代数的拡大体を E とし，α を E の元とします．E の部分体の中で，F と α を含む最小の部分体を $F(\alpha)$ とします．$F(\alpha)$ は F 上のベクトル空間です． $\mathrm{Irr}(\alpha, F) = n$ のとき，$\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ は $F(\alpha)$ の基底になります．

ここで $F(\alpha)$ は，F と α を単に合わせただけの集合ではありません．F の元と α を四則演算することで出てくる新たな元を全て含みますから，もっと広がりが出てきます．『何と何を足したか』という観点で見るときりがないので，『α を含む E の部分体全ての共通部分』として，E を削っていくようにして考えるのが良いでしょう．

この定理の証明は大事なのですが，とても長いのでひとまず省略して先へ進ませて下さい．(読者の要望が多ければ，証明を書くことも検討しますのでご意見をお寄せ下さい．)

この定理によって，$Q(\sqrt{2})$ の元が $a + b\sqrt{2}$ の形に書けること，$Q(\omega)$ (ω は 1 の三乗根) の元が $a + \omega b + \omega^2 c$ の形に書けること等が，よく納得できます．

有限次拡大

体 F の拡大体を E とします．E の F 上の拡大次数 $[E : F]$ を考えましょう．いま $[E : F]$ が有限だとします．($[E : F]$ は E を F 上のベクトル空間と考えたときのベクトル空間の次元でした．つまり，いま E が有限ベクトル空間だと仮定したわけです．)

$$[E : F] = n < \infty$$

このとき，E の元 x に対し $1, x, x^2, ..., x^n$ は $n + 1$ 個の元ですので，F 上一次従属になるはずです．つまり，零ではない F 上の係数 c_i を使って，$c_0 + c_1 x + c_2 x^2 + ... + c_n x^n = 0$ と表わすことが出来ます．これは代数方程式ですので，x は F 上代数的であり，E は F の代数的拡大体になっていることが分かりました．

対偶をとって，もしも $[E : F] = \infty$ ならば， E は F の代数的拡大体ではない，つまり超越的拡大体であることも示せます．

とが分かります．

*4 ただし，定数倍だけ異なるものを別の多項式と見なすなら，最小多項式も無数にあることになります．例えば $2(x - 2)$ と $3(x - 2)$ は どちらも 2 の最小多項式です．あまり，こういう細かいことにはこだわらないことにしましょう．

theorem

次数が有限の拡大体は代数的拡大体です．次数が無限の拡大体は超越的拡大体です．

この定理は非常に強力です．例えば，拡大体の列 $F = F_0 \subset F_1 \subset ... \subset F_n$ を考えるとき，F_0 と F_n の中間体は全て有限次拡大ですので，代数的だと言えます．

ここまでに出てきた定理を使う次の定理が証明できます．複素数の中には代数的数と超越数があるという主張です．

theorem

全ての代数的数を集めると，複素数の部分体になります．

証明は 数の階層 の記事で掲げます．この定理の重要な点は，複素数体の中に代数的数ではない部分があること，すなわち超越数の存在が暗示されていることです．