体の元の共役と正規拡大体

Joh @物理のかぎプロジェクト

2006-06-25

いよいよこの記事の次はガロア理論に進みます．あと少しです．

体上の元の共役

体 F 上の代数的な元 x, y を考えます．この二つの元の最小多項式が等しいとき，x, y は F **上共役である** と言います．もしくは『x, y は F 上の共役元である』のように言います．

$$\mathrm{Irr}(x, F) = \mathrm{Irr}(y, F) \iff x \sim y \text{ over F}$$

例えば，有理数体 Q 上で $x^2 = 2$ は解を持たず，これ以上の因数分解も不可能ですが，拡大体 $Q(\sqrt{2})$ 上には解 $\pm\sqrt{2}$ を持ちます．このとき，$Q(\sqrt{2})$ は Q の代数的拡大体になっていて，$\pm\sqrt{2}$ の最小多項式は $x^2 = 2$ です．よって，定義に従って $\sqrt{2}$ と $-\sqrt{2}$ は共役です．

ちょっとイメージが湧いてきましたか？もう一つ例を考えましょう．有理数体 Q 上の二次方程式 $ax^2 + bx + c = 0$ を解の公式を使って解くと，解は一般に $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ と表されましたが，根号の部分が 0 にならないなら，この解は Q の拡大体 $Q(\sqrt{b^2 - 4ac})$ 上の元です．そして，この二つの解は同一の Q 上既約な方程式の解ですから，定義より Q 上共役なわけです．そういえば高校の数学でも，このように解の公式を使って解くときにセットで出てくる解を **共役** と呼んでいたような気がします．

正規拡大体

元の共役の概念を使って，正規拡大体を定義します．とてもとても大事な概念です．

Important

体 F とその代数的拡大体 E を考えます．E の任意の元に対し，その全ての共役元を E が含むとき，E を F の正規拡大体と呼びます．

つまり，E を F の正規拡大体とするとき，F 上の方程式の解が一つでも正規拡大体 E に含まれるならば，E は同じ方程式の他の解も全て漏れなく含むということです．方程式の解を議論する際，正規拡大体の概念が大事なことが察せられると思います．

共役や正規拡大体の概念に慣れるために，ここで一つ定理を証明してみましょう．ここまでの知識を総動員すれば簡単に証明できる定理です．頭の体操だと思って，証明を読む前に自分で考えてみてください．

theorem

拡大次数 2 の代数的拡大体は，正規拡大体になります．

proof

体 F の代数的拡大体を E とし，$[E:F]=2$ とします．E は F に何か一つだけ代数的元を加えて作られた拡大体だと考えられます．E には属し，F には属さない元 α を一つ選ぶと，$E=F(\alpha)$ が言え，$\mathrm{Irr}(\alpha,F)$ は二次方程式のはずです．そこで $\mathrm{Irr}(\alpha,F)=X^2+aX+b$ と書き，α の共役元を β と書くと，解と係数の関係より $\alpha+\beta=-a,\alpha\beta=b$ が言え，β もやはり E の元であることが示せます．よって拡大次数 2 の拡大体は正規拡大体です．■

正規拡大体と最小分解体の関係

二次方程式を解けば二つの解が，三次方程式を解けば三つの解がセットになって出てきますが，正規拡大体にはこれらの解がどれも含まれるということでした．そこで，体 F 上の既約な n 次方程式 $f(x)$ を考えるとき，F の正規拡大体 E は $f(x)$ の解を全て含むのですから，$f(x)$ は E 上で一次式の積に因数分解できると考えられます．

$$f(x)=c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)\text{ over }E,\ \alpha_i\in E$$

すると，分解体の定義に従い，E は $f(x)$ の分解体になっているとも言えるでしょう．実は，E が F の有限次正規拡大体であれば，E を最小分解体とする F 上の方程式が必ず存在します．

theorem

『E は F の有限次正規拡大体です』⇔『F 上の多項式で，E を最小分解体とするものが存在します』

*1 色々な言葉が出てきて混乱している人がいると思うので，分解体の定義を復習しておきましょう．F 上の多項式 $f(x)$ の最小分解体とは，$f(x)$ を一次式の積に因数分解できる，F の拡大体の中で最小のものです．因数分解の仕方は $f(x)$ 自身によります．解を全て F 上に持っている多項式ならば，そもそも拡大体を考える必要がありませんし，$f(x)=x^2-2$ ならば $Q(\sqrt{2})$ で済むので，複素数体まで拡大する必要はありません．拡大の程度は個々の多項式によるわけです．このように，最小分解体は個々の多項式に応じて一つ決まるものですから，F 上の全ての多項式の最小分解体を考えると，最小分解体には F 自身から複素数体 C まで，色々なものが出てくるわけです．一方，正規拡大体 E の定義ではあくまで元が主役です．E の元の最小多項式に対して，E は分解体になっているわけですが，どの程度の拡大体なのかは，E の含む元によって決まります．最小分解体にせよ，正規拡大体にせよ，ある多項式をその上で一次式の積に因数分解できる拡大体なわけですが，その定義の出発点がちょっと違うのですね．体 F 上には色々な多項式があり，個々の多項式によって最小分解体にも色々あるわけですから，F のある正規拡大体に対し，その正規拡大体を最小分解体とする多項式も存在していそうなものです．次の定理は，この予想を裏付けるものです．

proof

(→の証明) E **は** F **の代数的拡大体ですので，**F **上の代数的な元** $x_1, x_2, ..., x_n$ **を使って** $E = F(x_1, x_2, ..., x_n)$ **と書けます．**x_i **に対応する** F **上の最小多項式を** $f_i(x) = \mathrm{Irr}(x_i, F)$ **と書くことにし，これらの積を** $g(x) = f_1(x)f_2 \cdots f_n = \prod_{i=1}^{n} f_i(x)$ **と置きます．個々の最小多項式は** E **上，**$f_i(x) = \prod_{j=1}^{m_i}(x - \alpha_{i,j})$ **と因数分解できるはずです．**$\alpha_{i,j}$ **は** $f_i(x)$ **の** j **番目の解を意味するとします．これより** $g(x)$ **は** E **上で** $g(x) = \prod_{i=1}^{n}\prod_{j=1}^{m_i}(x - \alpha_{i,j})$ **と表現できます．これは** $E = F(\alpha_{1,1}, \alpha_{1,2}, ..., \alpha_{n,m_i})$ **の形の拡大体と見ることができますので，**E **は** $g(x)$ **の最小分解体になっています．**■

逆の証明はやや難しく，今までに紹介していない定理を含みますので，とりあえず今は証明の方針だけを示すにとどめます．厳密に興味のある人は，適当な代数の教科書を参考にして自分で調べるようにして下さい．

proof

(←の証明の方針) E **上の任意の元** x **に対し，その** F **上の共役元** y **を考えます．**y **は** $\mathrm{Irr}(x, F)$ **の最小分解体** D **に属するのは確かです．いま，**y **が** E **には属さないと仮定するため** $D = E(y) \supset E$ **とします．**E **は** $\mathrm{Irr}(x, F)$ **の** F **上の最小分解体であり，**D **は** $\mathrm{Irr}(x, F)$ **の** $F(y)$ **上の最小分解体になっています．**F **上共役な元** x, y **に対し，**$F(x) \longmapsto F(y)$ **を満たす同型写像** τ **が存在しますが，この同型写像は** $\tau : E \longmapsto E(y)$ **という単射準同型写像にまで拡張できます (これは要証明)．一般に** F **上の多項式の最小分解体** K **を，その拡大体** K' **に移す** F **上の単射準同型写像** $\pi : K \longmapsto K'$ **があれば，**$\pi(K) = K$ **が成り立つことが知られています (これも要証明) ので，**$D = E(y) = \tau(E) = E$ **が示せて，**$y \in E$ **であり，**E **は正規拡大体であることが示せます．**□