ガロア理論と代数方程式

Joh @物理のかぎプロジェクト

2007-03-03

ここまでに，色々な定理や概念を考えて来ましたので，随分長い道のりでしたが，いよいよこれが最後の定理です．この後は，二次方程式，三次方程式などを例に取り，実際に定理を使って方程式の可解性を考えますので，定理の証明に疲れている人も，もう少し頑張って下さい．

theorem

【ガロアの定理】 F 上の多項式 $f(x)$ と，その最小分解体 E を考えます．方程式 $f(x)=0$ が代数的に解ける（解の公式が存在する）ことの必要十分条件は，$\mathcal{G}(E/F)$ が可解群であることです．

体 F 上の方程式 $f(x)$ が代数的に解けるということは，$f(x)$ の最小分解体 E が F の累開冪拡大になっている，と言い換えることも出来ました．そこで，E が F の累開冪拡大であることと，$\mathcal{G}(E/F)$ が可解群であることが同値であることを証明すればよいことになります．

【 $f(x)=0$ が代数的に解ける$\Rightarrow \mathcal{G}(E/F)$ が可解群である，ことの証明】

まず，F を根体とするガロア拡大の列を考えます．

$$F = F_0 \subset F_1 \subset F_2 \subset .... \subset F_n \tag{1}$$

もし，E が F の累開冪拡大だとすれば，このようなガロア拡大の列で $E \subset F_n$ を満たすものが取れます．F_n は，F_0 を含む各 F_i のガロア拡大であって，ガロア理論の基本定理により，この体の拡大列に対応して，次のようなガロア群の組成列を考えることが出来ます．

$$\{e\} = G_0 \subset G_1 \subset ... \subset G_n = \mathcal{G}(F_n/F_0) \tag{2}$$

さらに，ガロア理論の基本定理 により，添字が隣り合うガロア群の商群について，次の関係式も分かりま

---

*1 ガロア理論が難しい感じがするのは，方程式の可解性の話題に到達するまでに，非常に多くの定理や補題が必要であり，特に多くの教科書では，最短のコースを取らずに，枝葉の定理も取り上げているため，『定理と証明』というページが長すぎて，初学者が迷子になってくじけやすいことあると思います．しかも，似たような定理が多く，厳密に意味が分かっていないと，細かな部分で混乱しがちです．（一応，この記事の最後に，おさらいとして定理の関係をまとめておきます．）もちろん，それ自体で興味深い定理もありますし，ガロア理論よりもさらに上を目指す人にとっては，ここは単なる通過点ですから，じっくり裾野を広げることも大事だと思いますが，やはり初学者は，さっさと方程式の可解性を勉強して，まずはガロア理論の大枠を感じてみることが必要だと思います．このような観点から，標数が非零の場合などを一切考えずに，ここまで最短で来てしまいました．だいたいの粗筋が分かった人は，もっと本格的な本でしっかり勉強して下さい．

す.（添え字の関係の反変性を確認してください.）

$$\frac{G_i}{G_{i-1}} = \frac{\mathcal{G}(F_n/F_{n-i})}{\mathcal{G}(F_n/F_{n-i+1})} \sim \mathcal{G}(F_{n-i+1}/F_{n-i}) \tag{3}$$

さらに，ガロア群と可解群 の最後に証明した定理を使うと，$\mathcal{G}(F_{n-i+1}/F_{n-i})$ は可解群だということが分かります．これより，$\mathcal{G}(F_n/F_0)$ は正規部分群の列を持ち，その隣り合う正規部分群の商群が可解群であるので，$\mathcal{G}(F_n/F_0)$ 自身も可解群だということが言えます．（ ガロア群と可解群 参照.）■

【 $\mathcal{G}(E/F)$ が可解群である$\Rightarrow$ $f(x)=0$ が代数的に解ける，ことの証明】

逆に，$\mathcal{G}(E/F)$ が可解群だとすれば，次のような正規部分群の組成列を考えることが出来ます．

$$\{e\} = G_0 \subset G_1 \subset ... \subset G_n = \mathcal{G}(E/F) \tag{4}$$

これに対し，ガロア理論の基本定理を用いれば，群 G_{n-i} の固定体を F_i として，次のようなガロア拡大体の列を対応させることが出来るはずです．

$$F = F_0 \subset F_1 \subset ... \subset F_n = E \tag{5}$$

ここで，$\mathcal{G}(E/F_i) = G_{n-i}$ という関係が成り立っています．ここでもガロア理論の基本定理を用いれば，式 (3) の逆で，F_i が F_{i-1} のガロア拡大であることを示すことが出来ます．

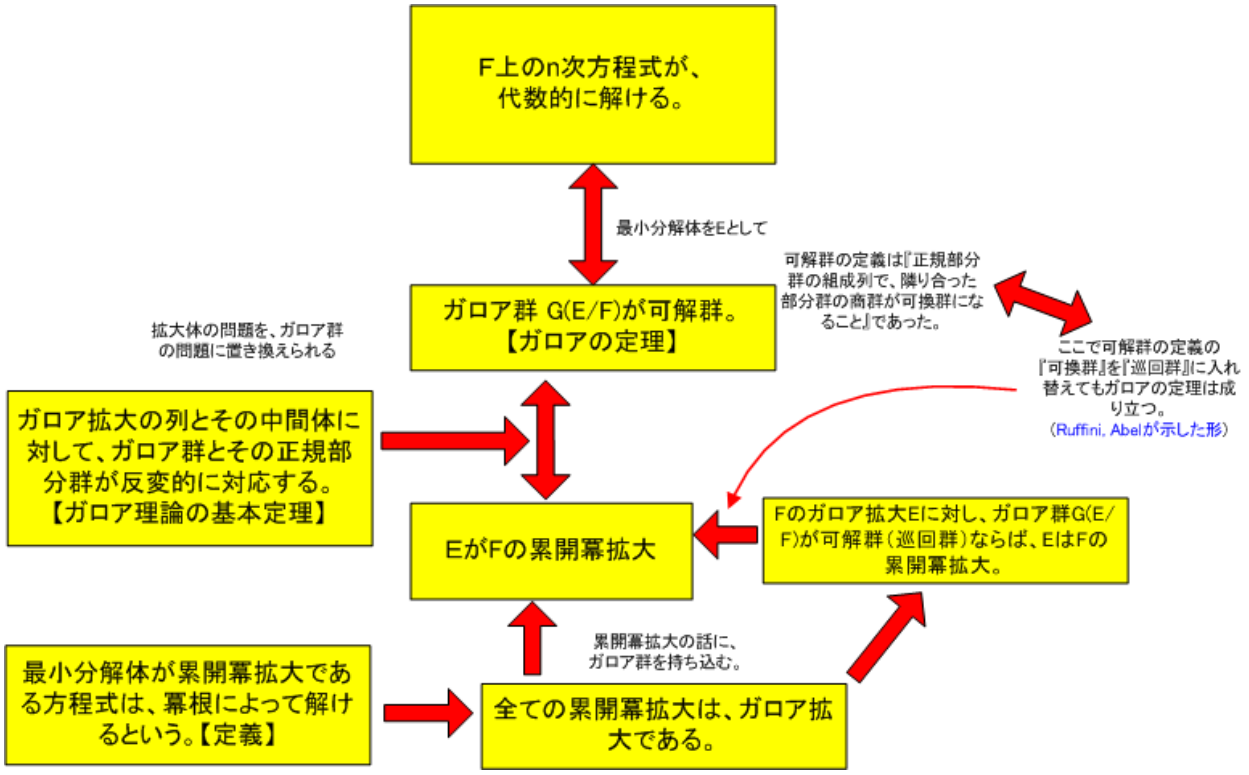
$$\mathcal{G}(F_i/F_{i-1}) \sim \frac{\mathcal{G}(E/F_{i-1})}{\mathcal{G}(E/F_i)} = \frac{G_{n-i+1}}{G_{n-i}} \tag{6}$$

ここで，$\mathcal{G}(E/F)$ は可解群と仮定しているので，$\frac{G_{n-i+1}}{G_{n-i}}$ は可換群であり，$\mathcal{G}(F_i/F_{i-1})$ もまた可換群であることが分かります．累開冪拡大体とガロア群の関係 で証明した定理により，このとき F_i は F_{i-1} の開冪拡大であり，結局，$E = F_n$ は $F_0 = F$ の累開冪拡大体であることが分かります．■

この定理によって，代数方程式の可解性を考えるには，ガロア群が可解群になっているかどうかを調べればよいことが分かりました．さっそく，次の記事からは，例を考えて行きます．最終目標は，五次方程式以上に解の公式は存在しないことを示すことです．とりあえず，少し一休みしましょう．フゥ〜.

おさらい

ここまでに出てきた定理や定義を整理して，『方程式が代数的に解ける』という話と，ガロア拡大，ガロア群，可解群といった話がどうつながっているのかをフローチャートにしてみました.（おかしな点があれば，ご指摘ください．m(_ _)m）


F上のn次方程式が、
代数的に解ける。
最小分解体をEとして
ガロア群 G(E/F)が可解群。
【ガロアの定理】
可解群の定義は『正規部分群の組成列で、隣り合った部分群の商群が可換群になること』であった。
ここで可解群の定義の『可換群』を『巡回群』に入れ替えてもガロアの定理は成り立つ。
(Ruffini, Abelが示した形)
拡大体の問題を、ガロア群の問題に置き換えられる
ガロア拡大の列とその中間体に対して、ガロア群とその正規部分群が反変的に対応する。
【ガロア理論の基本定理】
EがFの累開冪拡大
Fのガロア拡大Eに対し、ガロア群G(E/F)が可解群(巡回群)ならば、EはFの累開冪拡大。
累開冪拡大の話に、ガロア群を持ち込む。
最小分解体が累開冪拡大である方程式は、冪根によって解けるという。【定義】
全ての累開冪拡大は、ガロア拡大である。