ガロア群と可解群

Joh @物理のかぎプロジェクト

2007-03-03

復習になりますが，体 F の代数方程式 $f(x) = 0$ が解の公式を用いて解けるとは，『加・減・乗・除の四つの演算と，開冪（根号を取ること）により，F 上の数を有限回組み合わせることで解を表現できる』という意味です．

五次方程式に解の公式が存在しないことはアーベルによって証明されましたが，方程式の可解性についてより包括的に一般論を完成させたのはガロア (Evariste Galois (1811-1832)) です．ガロアは高校で数学を始め，わずか 21 歳にして決闘に斃れますので，実質的に数年間しか数学の勉強をしていないわけですが，ガロアがいなければ数学が 100 年は遅れていたであろうというほどの貢献をしました．ガロアの人生については，また後に触れます．実は，ガロアが高校生のとき，ノルウェー人のアーベルは一回パリを訪れています．恐らく，直線距離で二人の間は数キロと離れていなかったと想像されますが，もちろん当時はこの二人が方程式の可解性について決定的な仕事をすることをお互いに知りませんでした．

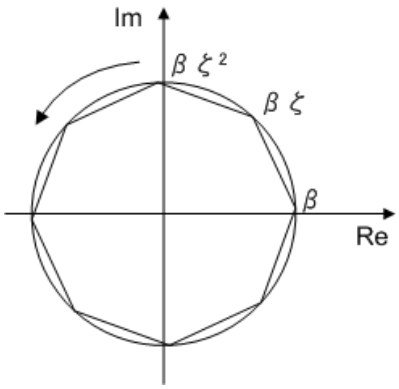
図 1　ちょっと変わった顔だ．

円分体で復習

既に $x^n=1$ という円周等分方程式の解については，１のｎ乗根，作図できる正多角形，正五角形の作図，正十七角形の作図 で議論を重ねてきましたので，一般の方程式に進む前にもう一度円周等分方程式から議論をスタートさせましょう．

まず F 上の円周等分方程式 $x^n=1$ を復習します．$\zeta=e^{\frac{2\pi i}{n}}$ とすると，他の解は $\zeta^2,\zeta^3,...,\zeta^{n-1}$ と与えられるところまでは大丈夫でしょう．次に，$x^n=\alpha$ という，右辺が 1 ではない方程式を考えてみます．基本的な解の振る舞いは同じで，一つの解を β とすると，他の解は $\beta\zeta,\beta\zeta^2,...,\beta\zeta^{n-1}$ で与えられることになります．（ β は $\sqrt[n]{\alpha}$ と ζ を掛けた形になっている訳です．）

このとき，もし $x^n=1$ の最小分解体 E が β と $\beta\zeta$ を含めば，$\zeta=\frac{\beta\zeta}{\beta}$ より E は ζ も含むこととなり，このようにして全ての解 $\beta\zeta,\beta\zeta^2,...,\beta\zeta^{n-1}$ が表現できます．そこで，$E=F(\zeta,\beta)$ が言えるでしょう．



このとき，$E=F(\zeta,\beta)$ は F 上既約な多項式 $x^n=\alpha$ の最小分解体ですので，F のガロア拡大になっています．（ 対称式への応用 参照．） $\mathcal{G}(F/E)$ の元は F を固定体に保つ同型写像で，$x^n=\alpha$ の解 $\{\beta,\beta\zeta,\beta\zeta^2,...,\beta\zeta^{n-1}\}$ を置換します．これは例えば ϕ $(\in E)$ に対して，$\phi(\beta)=\beta\zeta^k$ $(k<n)$ を満たす k が一つ決まり，かつ $\phi(\zeta)=\zeta^m$，$(m,n)=1$ を満たす m も一つ決まるということです．（ １のｎ乗根 参照．）

ここで，$\mathcal{G}(F/E)$ について次の定理がなりたちます．可解群の定義を忘れてしまった人は 組成列と単純群 を参照して下さい．

theorem

体 F 上の多項式 $x^n=\alpha$ の最小分解体を E とするとき，ガロア群 $\mathcal{G}(F/E)$ は可解群になります．

*1 直観的イメージとして，半径 β の円上に解がグルリと並んでいる様子を想像して下さい．最初の解を β とすると，次の解は $\zeta\beta$ で表わされます．ζ の偏角は $\frac{2\pi}{n}$ 度です．β から始めて順次 ζ を掛けていくことで，全ての解を表わせるようになっています．

proof

ここまでの議論と記号を使い，$F=E(\beta,\zeta)$ と表わします．E と F に対して中間体 $B=F(\zeta)$ を考えると，B は $x^n=1$ の最小分解体なので F のガロア拡大で，ガロア理論の基本定理 により，$\mathcal{G}(E/B)$ は $\mathcal{G}(E/F)$ の正規部分群になります．$\mathcal{G}(E/B)$ の元となるのは，$\mathcal{G}(E/F)$ の元である同型写像のうち，ζ を動かさない写像だけです．つまり，$\psi\in\mathcal{G}(E/B)$ に対し，$\psi(\zeta)=\zeta$ が言えます．（一般に $\mathcal{G}(E/F)$ の元は ζ を ζ^k（ただし，k と n は互いに素）に移すわけですが，特に $k=1$ の場合が $\mathcal{G}(E/B)$ の元だと考えられます．）引き続き，$\mathcal{G}(E/B)$ の元 ψ を考えます．ψ は β に対しては $\psi(\beta)=\beta\zeta^m$ のような写像として働きますが（$\because$ ψ は $\beta,\beta\zeta,...,\beta\zeta^{n-1}$ を互いに置換するからです），写像の一意性により，逆にこの指数 m によって ψ を特定することが可能です．よって，$\mathcal{G}(E/B)$ の元を $1,2,3,...,n$ に一対一対応させることができ，実際，$\beta\zeta^n=1$ より，有限巡回群 $\mathcal{G}(E/B)$ は Z_n と同型だと言えます．ここで 可解群について補足 で証明した定理を用いると，$\mathcal{G}(E/B)$ は可解群だということが分かります．さて，$\mathcal{G}(E/F)$ の元（ F を不動に保つ E の同型写像）のうち，B を B 自身に写す部分群を考えれば，それが $\mathcal{G}(B/F)$ だと言えます．$\mathcal{G}(E/F)$ の元 ϕ のうち，特に B を B 自身に写すものを $\phi|B$ と書くことにすると，$\mathcal{G}(E/F)\to\mathcal{G}(B/F)$ という写像は，元について $\phi\to\phi|B$ と表わせることが分かります．さて，$x^n-\alpha=0$ の解を $\beta,\beta\zeta,\beta\zeta^2,...,\beta\zeta^{n-1}$ とすると，一般に ϕ はこの解を置換し，適当な整数 k $(n,k)=1$ を使って，その作用を $\phi(\zeta)=\zeta^k$ と書けたわけですが，この k を決めることで，$\phi\longmapsto\phi|B$ という写像を決定することが可能なはずです．そこで $\phi|B\longmapsto k$ という写像が一意的に決められることになり，この写像によって $\mathcal{G}(E/B)$ は適当な有限巡回群 Z_m $(m<n)$ と同型だと言えます． Z_m は Z_n の部分群のはずで，先ほどと同様にして $\mathcal{G}(E/B)$ も可解群だと言えます．いま，$\mathcal{G}(E/F)$ と $\mathcal{G}(E/B)$ が可解群なので，可解群について補足 で示した定理により，$\mathcal{G}(B/F)$ も可解群だと言うこと分かります．■

定理の証明が長くなったので，ひとまず一休みしましょう．ここまでに，方程式 $x^n-\alpha=0$ の解に関して，ガロア拡大と可解群の関係を見てきました．ガロア拡大体の列（ $E\supset B\supset F$ ）と，ガロア群の列 $\mathcal{G}(E/B)\subset\mathcal{G}(E/F)$ という二つの話が反変的に対応しているという点をもう一度確認して下さい．

*2 拡大体の列と部分群の列は，普通は別の話なわけですが，ガロア理論によって，この両者の間に美しい関係があることが分かったわけです．ここでは，ガロア拡大の話と可解群の話が結びつきました．別々に作っていた部品が，最後に次々と組み合わさって美しい一つの芸術作品を作っていくような趣があります．あと少し定理の証明が続きますが，一つ一つの定理が各部品の連結の役割を果たしています．ガロア理論という芸術品を眺めるために，もう少し大事な定理を見ていきましょう．

*3 方程式 $x^n=1$ は，n が五次以上でも $x=\sqrt[n]{1}$ として簡単に代数的に解けることが明らかですから，ガロア群が可解群になるのは当然だと言えます．ちょっとした発展版の $x^n=\alpha$ も，$x=\sqrt[n]{\alpha}$ という解が簡単に求められますので，ガロア群が可解群になって当然です．このあと，一般の n 次方程式の可解性を論じるときも，1 の n 乗根の話が土台として何度も出てきますので，この定理の結果は大事な基礎になります．