累開冪拡大とガロア群の関係

Joh @物理のかぎプロジェクト

2007-03-03

方程式の可解性を考える準備は，いよいよ大詰めです．累開冪拡大体の列と，ガロア群の関係を明らかにします．この記事の最初で，後の議論のために **ラグランジェのリゾルベント** と言われる量を導入します．後半で，ガロアの定理の証明に決定的に大事になる定理を証明します．（この定理は，ガロアの定理のための補題というよりは，それ自体でとても重要な定理だと思います.）気合を入れていきましょう．

ラグランジェのリゾルベント

まず，ラグランジェのリゾルベントと言われる量を導入します．ラグランジェのリゾルベントとは，n 次方程式 $f(x) = x^n + a_1 x^{n-1} + ... + a_{n-1}x + a_n = 0$ に対し，その解 $\theta_0, \theta_1, ..., \theta_{n-1}$ と，1 の n 乗根の一つ ζ を，次のように順番に掛け合わせて足し合わせた量です．

$$L(\zeta, \theta_i) = \theta_0 + \zeta\theta_1 + \zeta^2\theta_2 + ... + \zeta^{n-1}\theta_{n-1} \tag{1}$$

式 (1) を念頭に，$f(x)$ を体 F 上の代数方程式だとし，拡大体 $E = F(\theta)$ を考えます．いま，**ガロア群が巡回群** $\mathcal{G}(E/F) = \{1, \phi, \phi^2, ..., \phi^{n-1}\}$ だとすると（ **この仮定が重要！** ），解 $\theta_0, \theta_1, ..., \theta_{n-1}$ は $\theta_0, \phi\theta_0, \phi^2\theta_0, ..., \phi^{n-1}\theta_0$ のように，θ_0 と ϕ だけを使って書き換えることができます．（ただし，順番も同順とは限りません.）簡単のため，F は 1 の n 乗根 $1, \zeta, \zeta^2, ..., \zeta^{n-1}$ を含み，θ_0 を単に θ と書くことにすれば，式 (1) を次のように書き換えることができます．

$$\begin{aligned} L(\zeta^k, \theta) &= \theta + \zeta^k(\phi\theta) + \zeta^{2k}(\phi^2\theta) + ... + \zeta^{(n-1)k}(\phi^{n-1}\theta) \\ &= \sum_{m=0}^{n-1} \zeta^{km}(\phi^m\theta) \end{aligned} \tag{2}$$

後で，この形でラグランジェのリゾルベントを利用します．また，ここでは仮に，1 の n 乗根 $1, \zeta, \zeta^2, ..., \zeta^{n-1}$ は，F に含まれるとしておきます．（このため，$|\mathcal{G}(E/F)| = n$ と考えます.）式 (2) で両辺の総和を取ってみます．

$$\begin{aligned} \sum_{k=0}^{n-1} L(\zeta^k, \theta) &= \sum_{k=0}^{n-1}\sum_{m=0}^{n-1} \zeta^{km}(\phi^m\theta) \\ &= \sum_{m=0}^{n-1} \left(\sum_{k=0}^{n-1} (\zeta^m)^k \right) (\phi^m\theta) \end{aligned} \tag{3}$$

式 (3) の右辺の括弧部分は，$1+\zeta^m+\zeta^{mk}+...$ のように等比級数の和ですから，公式通りに $\frac{1-(\zeta^m)^k}{1-\zeta^m}$ のように表現できますが，これは $m \equiv 0 \mod.n$ の場合に $1+1+...+1=n$ となり，それ以外の場合には 0 になります.

$$\sum_{k=0}^{n-1}(\zeta^m)^k = 1+\zeta^m+\zeta^{mk}+...+\zeta^{m(k-1)}$$
$$= \begin{cases} n & (m \equiv 0 \mod.n) \\ \frac{1-(\zeta^m)^k}{1-\zeta^m} = 0 & (otherwise) \end{cases}$$

そこで，式 (3) の Σ で生き残るのは，$m=0$ の場合だけなので，$\phi^0=1$ を考えると，式 (3) は次のように変形できます.

$$\sum_{k=0}^{n-1} L(\zeta^k,\theta) = \sum_{k=0}^{n-1}\sum_{m=0}^{n-1}\zeta^{km}(\phi^m\theta) = n\theta$$

式 (3) より，$f(x)=0$ の解 θ を次のように表現することが出来ます．これが，ラグランジェのリゾルベントを使った方程式の解の表現で，このようにして方程式の解を表す方法を **ラグランジェの方法** と呼びます.

$$\theta = \frac{1}{n}\sum_{k=0}^{n-1} L(\zeta^k,\theta) \tag{4}$$

もう一つ，重要な関係式を導いておきます．式 (2) の両辺に ζ^{-k} を掛けてみます.

$$\zeta^{-k}L(\zeta^k,\theta) = \zeta^{-k}\theta+\phi\theta+\zeta^k\phi^2\theta+...+\zeta^{k(n-2)}\phi^{n-1}\theta \tag{5}$$

右辺第一項を，$\phi^n\theta=\theta$, $\zeta^{kn}=1$ であることを使って，少し強引ですが $\zeta^{-k}\theta=\zeta^{k(n-1)}(\phi^n\theta)$ と変形すれば，式 (5) を次のように変形できます.（二行目から三行目は，単に順番を見やすいように並べ替えただけです.）

$$\begin{aligned}\zeta^{-k}L(\zeta^k,\theta) &= \zeta^{-k}\theta+\phi\theta+\zeta^k\phi^2\theta+...+\zeta^{k(n-2)}\phi^{n-1}\theta \\ &= \zeta^{k(n-1)}(\phi^n\theta)+\phi\theta+\zeta^k\phi^2\theta+...+\zeta^{k(n-2)}\phi^{n-1}\theta \\ &= \phi\theta+\zeta^k\phi^2\theta+...+\zeta^{k(n-2)}\phi^{n-1}\theta+\zeta^{k(n-1)}(\phi^n\theta) \\ &= L(\zeta^k,\phi\theta)\end{aligned} \tag{6}$$

よって，次の関係式が得られました.

$$L(\zeta^k,\phi\theta) = \zeta^{-k}L(\zeta^k,\theta) \tag{6}$$

---

*1 これは，ラグランジェ (Joseph-Louis Lagrange (1736-1813)) が提案した方程式の解法で，ラグランジェの方法と呼ばれています．ここまでの議論は，ガロア群が巡回群である，という仮定に基づいていますが（もう一度確認してみて下さい），これがもし巡回群でないと，式 (4) によって簡単に方程式の解を示すことは出来ません．つまり，ガロア群が巡回群かどうか，というのがこの方法のポイントになってきます．ラグランジェは，まだ群論さえなかった時代に，既に巡回群に似た概念に到達し，それが方程式の可解性の要点であることを見抜いていました．ガロアも，まずラグランジェの著作を読み，ガロア群が巡回群になることと方程式の可解性の関係に気づき，そこから数日間のうちにガロア理論を完成させたと言います．ラグランジェの業績あってのガロア理論と言えそうです.

また，ϕ が ζ を不動に保つことを考えると，$\phi L(\zeta^k,\theta)=L(\zeta^k,\phi\theta)$ が言えますから，式 (6) とまとめて，次の関係を得ます．

$$\phi L(\zeta^k,\theta)=L(\zeta^k,\phi\theta)=\zeta^{-k}L(\zeta^k,\theta) \tag{7}$$

さらに，$\zeta^{-kn}=1$ を使って，式 (7) から次式を導くことが出来ます．

$$\begin{aligned}(L(\zeta^k,\theta))^n&=\zeta^{-kn}(L(\zeta^k,\theta))^n\\&=(\zeta^{-k}L(\zeta^k,\theta))^n\\&=(L(\zeta^k,\phi\theta))^n\\&=(\phi L(\zeta^k,\theta))^n\\&=\phi L(\zeta^k,\theta)\cdot\phi L(\zeta^k,\theta)\cdots\phi L(\zeta^k,\theta)\\&=\phi(L(\zeta^k,\theta))^n\end{aligned} \tag{8}$$

最後のところでは，ϕ が準同型写像であること，つまり一般に $\phi(AB)=\phi(A)\phi(B)$ を満たすことを利用しています．式 (8) の最初と最後を比べて見れば，ϕ が $(L(\zeta^k,\theta))^n$ を不動に保つということが分かります．

$$\phi(L(\zeta^k,\theta))^n=(L(\zeta^k,\theta))^n \tag{9}$$

ラグランジェのリゾルベントの導入が長くなりましたが，ここまでの議論を使って，次に大事な定理を証明します．

定理

theorem

体 F のガロア拡大 E を考えます．もしガロア群 $\mathcal{G}(E/F)$ が可換群（または巡回群）ならば，E は F の開冪拡大だと言えます．

この定理は非常に重要で，これによって開冪拡大の列とガロア群の列が関係づけられます．有限巡回群は可解群だと言えましたので（すでに こちら で証明しました），定理の可解群という部分を有限巡回群と読み換えても良いです．可解群という言葉に触れずに巡回群だけで説明してある教科書もあり，どちらでも良いと思います．

以下は，この定理の証明です．

特殊な場合

まず，$|\mathcal{G}(E/F)|=n$ として，1 の n 乗根 $1,\zeta,\zeta^2,...,\zeta^{n-1}$ を F が含む特殊な場合を考えます．

式 (9) より，$(L(\zeta^k,\theta))^n$ の形で表わされる数（ $k=1,2,...,n-i$ の n 個あるので，$\alpha_k=(L(\zeta^k,\theta))^n$ と名づけておきます）は，$\phi\in\mathcal{G}(E/F)$ によって不動に保たれます．同じ議論が $\mathcal{G}(E/F)$ の他の元にも成り立ちますから，結局，α_k は F の元であるということが分かります．いま， F_i 上の方程式 $x^n-\alpha_i$ による分離拡大体を F_{i+1} と定義することで，累開冪拡大体の列を考えることができます．

$$F=F_0\subset F_1\subset ...\subset F_n \tag{10}$$

こ方程式 $x^n - \alpha_i = 0$ の解ということは，α_i の n 乗根を全て含むことになりますが，F_n は全ての $\alpha_k = (L(\zeta^k, \theta))^n$ の n 乗根を漏れなく含むことになりますので，結局，ラグランジェのリゾルベントの各項を全て含むことが示せます．これより，次の関係が言えます．

$$E = F(\theta) \subset F_n \tag{11}$$

$$\theta = \frac{1}{n}\sum_{k=0}^{n-1} L(\zeta^k, \theta) \in F_n \tag{12}$$

これより，E は F の累開冪拡大であることが示されました．■

一般の場合

まず特殊な場合として，1 の n 乗根が全て F に含まれる場合について，定理を示しましたが，定理は 1 の n 乗根が F に含まれない場合に対しても拡張することが出来ます．

まず E は，θ を解とする F 上の方程式 $f(x)$ の最小分解体になっており，ガロア拡大であることを確認しましょう．（最小分解体は，常にガロア拡大でした．）これに対し，F 上の方程式 $g(x) = (x^n - 1)f(x)$ と，g の最小分解体 $F(\zeta, \theta)$ を考えてみます．これもガロア拡大です．このとき，$F(\zeta, \theta)$ は $F(\theta)$ のガロア拡大でもある，ということも言え，$\mathcal{G}(F(\zeta, \theta)/F(\zeta)) \to \mathcal{G}(E/F)$ なる準同型写像を決めることが出来ます．このような準同型写像を H とすると，H の作用する被写像元を，E に制限することが出来ます．これを $H(\psi) = \psi|E$ のように書きます．（ ψ は H が作用するのですから，少なくとも $\mathcal{G}(F(\zeta, \theta)/F(\zeta))$ の元で，つまり $F(\zeta, \theta)$ の自己同型写像です．E を $F(\zeta, \theta)$ の部分体と考えることが出来ますから，ψ として E に制限されたものを考えることは可能なわけです．）さらに，この ψ として，一対一写像のものを決めることも出来ますから，も $\mathcal{G}(F(\zeta, \theta)/F(\zeta))$ と $\mathrm{Im}H$ に同型写像を決めることが出来ます．$\mathrm{Im}H$ は $\mathcal{G}(E/F)$ の部分群なので巡回群ですので，これより $\mathcal{G}(F(\zeta, \theta)/F(\zeta))$ も巡回群だと言うことが出来ます．また，$|\mathcal{G}(F(\zeta, \theta)/F(\zeta))| = m$ （ m は $|\mathcal{G}(E/F)| = n$ を割り切る適当な整数）と置くことが出来ます．結局，『 $\mathcal{G}(F(\zeta, \theta)/F(\zeta))$ は位数 m の巡回群である』ことが分かり，さらに $F(\zeta)$ は 1 の m 乗根 $\{1, \zeta^{n/m}, \zeta^{2n/m}, ..., \zeta^{(m-1)n/m}\}$ を全て含むのですから，ここから先は前セクションで証明した『特殊な場合』の証明に帰着させることが出来ます．すなわち，$\mathcal{G}\zeta, \theta)$ は $\mathcal{G}(\zeta)$ の累開冪拡大であり，$F(\zeta)$ が F の累開冪拡大であることを考えれば，$F(\zeta, \theta) \subset F_n$ という，前セクションと同じ結論を得ることが出来ます．■