3　代数方程式の可解性

以下では K:体 $\supset \mathbb{Q}$ (とくに標数 $\mathrm{char}(K)=0$)(標数は次の章で詳しく述べる) で $f=\sum_{i=0}^{n} c_i X^i \in K[X]$ とする。

定義 3.1. 方程式 $f(X)=0$ が 代数的に解けるとは f の任意の根が f の係数 c_i と加減乗除と $\sqrt[m]{\ }(m\in\mathbb{N})$ を使って書けること。

定義 3.2. L/K_0 が冪根拡大とはある n_i, l と $a_i \in K_i$ によって

$$K_0 \subset K_1 \subset \cdots \subset K_l = L$$
$$K_i = K_{i-1}(\sqrt[n_i]{a_{i-1}})$$

となるような形の拡大のこと。

つまり、定義 (3.1) は $K_0 := \mathbb{Q}(c_0,\ldots,c_n), \alpha_1,\ldots,\alpha_n : f$ の解とするとき、 $\alpha_j \in (K_0$の$^{\exists}$冪根拡大) ということ。または、 $K_0(\alpha_1,\ldots,\alpha_n) \subset (K_0$の$^{\exists}$冪根拡大) になるということ。

定義 3.3. ある群 G における交換子 (commutator)とは G の元 x,y によってできる $xyx^{-1}y^{-1}$ という形の元のこと。そしてその群における交換子群 (commutatorsubgroup) (G,G) とは G の任意の交換子によって生成される群である。つまり $(G,G) := \langle ghg^{-1}h^{-1} | g,h \in G\rangle$ と定義される。

定理 3.4. 群 G に対してその交換子群は正規部分群であり、商群 $G/(G,G)$ は Abel 群である。さらに (G,G) は G/H が Abel 群になるような任意の正規部分群 H のうち最小の正規部分群である。この $G/(G,G)$ を G の最大 Abel 商といい G^{ab} と書く。

Proof. ・正規部分群になること

任意の交換子 $xyx^{-1}y^{-1}$ のどのような共役な元も

$$g(xyx^{-1}y^{-1})g^{-1} = (gxg^{-1})(gyg^{-1})(gxg^{-1})^{-1}(gyg^{-1})^{-1}$$

となり交換子として書けるので交換子群に含まれる。(G,G) の任意の元は交換子の積 $c_1c_2\cdots c_k$ で表せられるので

$$g(c_1c_2\cdots c_k)g^{-1} = (gc_1g^{-1})(gc_2g^{-1})\cdots(gc_kg^{-1})$$

となり右辺のそれぞれが (G,G) に含まれるので任意の交換子群の元の共役元はその交換子群に含まれるから (G,G) は G の正規部分群。

・ $G/(G,G)$ が Abel 群になること

$x,y\in G$ に対して $xyx^{-1}y^{-1}\in(G,G)$ より $(G,G)xyx^{-1}y^{-1}=(G,G)$ なので $(G,G)xy=(G,G)yx$ となるので $G/(G,G)$ は Abel 群である。

・ 最小になること

G/H が Abel 群で H が正規部分群であるとする。このとき $^{\forall}x,y\in G$ に対して $Hxy=Hyx$ であるから $Hxyx^{-1}y^{-1}=H$ より任意の交換子 $xyx^{-1}y^{-1}\in H$ でなければならない。よって G/H が Abel 群となるような任意の正規部分群 H は (G,G) を含むためそのような正規部分群のうち最小である。

□

定義 3.5. 群 G が可解であるとは交換子群 $(G_j, G_j) = \langle ghg^{-1}h^{-1} | g, h \in G \rangle$ としたときある有限な l で以下のようになること。この包含関係の列を可解列という。

$$G \supset G_1 \supset G_2 \supset \cdots \supset G_l = 1$$
$$G_j = (G_{j-1}, G_{j-1})$$

定義 3.6. Galois 拡大 L/K が 可解拡大 (solvable extension)とは $\mathrm{Gal}(L/K)$ が可解であること。

Galois 拡大 L/K が Abel 拡大 (abelian extension)とは $\mathrm{Gal}(L/K)$ が Abel 群であること。

定理 3.7. 可解拡大は Abel 拡大を繰り返し行うことでできる拡大である。

Proof. 有限次可解拡大 L/K がありその Galois 群を G とする。このとき G の交換子群 $G_1 = (G, G)$ に対応する体を M_1 とする。ここで Galois 理論の基本定理 (**??**) の (4) から $(G, G) \lhd G$ より M_1/K が Galois で $\mathrm{Gal}(M_1/K) \cong G/(G, G)$ なので $G/(G, G)$ が Abel より $\mathrm{Gal}(M_1/K)$ も Abel なので M_1/K は Abel 拡大となる。

同様に L/K の可解列 $G \subset G_1 \subset \cdots \subset G_l = 1$ の $G_i = (G_{i-1}, G_{i-1})$ に対応する部分体 M_i を考えると $G_i \lhd G_{i-1}$ より基本定理の (4) から M_i/M_{i-1} は Galois で $G_{i-1}/(G_{i-1}, G_{i-1}) = G_{i-1}/G_i \cong \mathrm{Gal}(M_i/M_{i-1})$ となり同様に $\mathrm{Gal}(M_i/M_{i-1})$ は Abel なので M_i/M_{i-1} は Abel 拡大となる。

1 に対応する体は L より上記のことを $i = l$ まで行えば L/M_l まで Abel 拡大になるので有限次可解拡大 L/K は 有限次 Abel 拡大 M_i/M_{i-1} $(1 \leq i \leq l, M_0 = K, M_l = L)$ の繰り返しでできる拡大となっている。 □

定理 3.8. 有限次 Galois 拡大 M/K について

$$M \text{ は } K \text{ の}^{\exists}\text{冪根拡大に含まれる} \Leftrightarrow M/K \text{ が可解拡大}$$

がなりたつので

$$\text{方程式 } f(X) = 0 \text{ が代数的に解ける} \Leftrightarrow K_0(\alpha_1, \ldots, \alpha_n)/K_0 \text{が可解拡大}$$

という代数方程式の可解性に関する必要十分条件が言える。