学籍番号		論文題目	ガロア理論と多項式のガロア群
氏名	小山拓也		

ガロア理論とは, 代数方程式や体の構造を, ガロア群という群を用いて調べる理論である. この理論を用いて, ガロアは5次以上の方程式に解の公式が存在しないことを証明した. 他にもガロア理論を用いることで, 角の三等分問題や円積問題といった問題にも証明を与えることができる. 発表では, 5次以上の方程式に解の公式が存在しないことと, 多項式 $x^{2p}+ax^p+b\in\mathbb{Q}[x]$ のガロア群について紹介する.

定理 1. $n\geq 5$ とする. そのとき n 次の一般多項式

$$f(x)=x^n+b_1x^{n-1}+b_2x^{n-2}+\cdots+b_n$$

は解の公式を持たない (= べき根によって解くことができない).

定理 2. $f\in K[x]$ がべき根によって解けるならば, f の K 上のガロア群は可解である.

定理1を示すための準備として, まずガロア群を定義する.

定義 1. K を体, E を K の拡大体とする. $G=G_{E/K}$ を E の K 上自己同型群とする. E が K の正規拡大であるとき, $G=G_{E/K}$ は E の K 上のガロア群とよぶ.

次にべき根によって解けるということを一般的に定義する.

定義 2. K を標数0の体とし, Ωを K の拡大体とする. 次の条件 (1), (2) を満たすΩの部分列

$$K=K_0\subset K_1\subset K_2\subset\cdots\subset K_{r-1}\subset K_r=\Omega$$

が存在するとき, Ωは K のべき根による拡大であるという.
(1) ある $n\in\mathbb{Z}^+$が存在して, K_1は K_0に1の原始 n 乗根 ζを添加した体 $K_1=K_0(\zeta)$ である.
(2) 各 $i(1\leq i\leq r-1)$ に対し, $K_{i+1}=K_i(\alpha_i),\ \alpha_i^{d_i}=a_i\in K_i$である. 言い換えれば, K_{i+1} は K_i上の多項式 $x^{d_i}-a_i$ の根 (a_iの d 乗根) を K_iに添加した体である. ただし, $d_i=2$ の場合を除き $d_i|n$ とする.

$f\in K[x]$ を定数でない多項式とする. K のべき根による拡大体Ωを適当にとり, f の K 上の分解体 E がΩに含まれるとき, f はべき根によって解けるという.

べき根によって解けるということを群を使って表すために, 可解群というものを定義する.

定義 3. G を群とする. G の部分群の減少列

$$G=G_0\supset G_1\supset G_2\supset\cdots\supset G_{r-1}\supset G_r=\{e\}$$

が G のアーベル列であるとは, 各 $i=1,\ldots,r$ に対し G_iが G_{i-1}の正規部分群であって, かつ商群 G_{i-1}/G_iがアーベル群になっていることをいう. アーベル列をもつような群を可解群という.

以下 3 つの定理は定理 1 の証明に必要であり, ここでは証明なしで認めるものとする.

定理 3. n 次の一般多項式

$$f(x) = x^n + b_1 x^{n-1} + b_2 x^{n-2} + \cdots + b_n$$

のガロア群は S_n と同型である.

定理 4. N を可解群 G の部分群とすると, N も再び可解群となる.

定理 5. 5 次交代群 A_5 の正規部分群は, $\{e\}$ と A_5 のみである.

$f(x) = x^4 + ax^2 + b$ を $\mathbb{Q}$ 上の既約多項式とするとき, $f(x)$ のガロア群 G は次のようになることが知られている [2].

(1) $\mathbb{Q}$ において b が平方数ならば, $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

(2) $\mathbb{Q}$ において b が平方数でなく, $b(a^2 - 4b)$ が平方数ならば, $G \cong \mathbb{Z}_4$.

(3) $\mathbb{Q}$ において $b, b(a^2 - 4b)$ のいずれも平方数でなければ, $G \cong D_4$.

$x^4 + ax^2 + b$ は, $m(x) = x^2 + ax + b$ に, $n(x) = x^2$ を代入した合成関数 $m(n(x))$ である. そこで $l(x) = x^p (p$ は素数$)$ とし, 合成関数 $m(l(x)) = x^{2p} + ax^p + b$ で, (1) の考え方を発展させることができないかと思い, 「b が $\mathbb{Q}$ において $b = c^p (c \in \mathbb{Q})$ を満たすとき」の $x^{2p} + ax^p + b$ のガロア群を考えた.

定理 6. p を素数とし, 多項式 $f(x) = x^{2p} + ax^p + b$ を $\mathbb{Q}$ 上の既約多項式とする. そして, ζ を 1 の原始 p 乗根, α を $f(x)$ の一つの根とする. b が $\mathbb{Q}$ において $b = c^p (c \in \mathbb{Q})$ を満たすとき $f(x)$ のガロア群を G とすると,

(i) $\zeta \notin \mathbb{Q}(\alpha)$ のとき, $G \cong D_p \rtimes C_{p-1}$,

(ii) $\zeta \in \mathbb{Q}(\alpha)$ のとき, $G \cong D_p$

となる. ただし, $D_2 = \mathbb{Z}_2 \times \mathbb{Z}_2$ とする.

今回は $x^4 + ax^2 + b$ の (1) を $x^{2p} + ax^p + b$ に対して拡張させることができたが, (2) と (3) に対しては拡張させることができなかった. 今後の課題は (2), (3) を $x^{2p} + ax^p + b$ に対して拡張させることである.

参考文献

[1] 松坂和夫, 代数系入門, 岩波書店, 1976.

[2] 永田雅宣, 大学院への代数学演習, 現代数学社, 2006.

[3] イアン・スチュアート, 明解ガロア理論, 講談社, 2008.

[4] 木村俊一, ガロア理論, 共立出版株式会社, 2012.