東海大学紀要情報通信学部
Vol.12,No.2,2019,pp.44-48

トピックス

大学初年次における数学教材の提案（その 32）
～ガロア群の軌道～

貴田研司[*1]

A Suggestion on Mathematical Materials for Freshman Education Vol. 32
~ The Orbits of Galois Groups ~

by

Kenshi KIDA [*1]

(received on Nov. 29, 2019 & accepted on Jan. 9, 2020)

あらまし

分離多項式のガロア群の根の全体の集合への作用について，この場合に群の軌道がどうなるかを明らかにする．それから，具体的な計算例を挙げることにより，理解を助けることとする．

Abstract

First, we explain the orbits of Galois groups of separable polynomials with respect to actions to the set of the roots of polynomials. Further, we present examples of the orbits of Galois groups.

キーワード：ガロア群の軌道，多項式の根，群の作用
Keywords: *Orbit of Galois Group, Roots of Polynomial, Action of Group*

1. はじめに

n 次分離多項式$f(x)$ のガロア群 G は，$f(x)$ のn 個の異なる根の全体からなる集合の置換群として捉えられる．この論文では，ガロア群 G の，$f(x)$ のn 個の異なる根の全体からなる集合への作用を考えたときの群の軌道について解説する．さらに，具体的に計算した例を挙げるが，特に有限体の場合が興味深い．

本論文の執筆にあたっては，増田真郎「応用のための代数系入門」[1)]を大いに参考にした．

2. 群の作用 [2)]

群 G と集合 Ω に対して，写像

$$G \times \Omega \ni (a, x) \mapsto ax \in \Omega$$

が次の 2 つの条件を満たすとき，Ω 上のG の作用という．

(i) $(ab)(x) = a(bx) \quad (a, b \in G, x \in \Omega)$

(ii) $ex = x \quad (e \text{ は} G \text{ の単位元})$

Ω 上のG の作用が定義されているとき，G をΩ 上の変換群といい，(G, Ω) と表す．

*1 高輪教養教育センター 准教授
Liberal Arts Education Center, Takanawa Campus, Associate Professor

定理

$a \in G$ を固定する．このとき写像

$$T_a : \Omega \ni x \mapsto ax \in \Omega$$

は 1 対 1 かつ上への写像である．言い換えれば，T_a は Ω の置換である．

$\Omega \ni x, y$ に対して

$$x \sim y \iff \text{ある} a \in G \text{ が存在して，} ax = y$$

と定義すれば，$\sim$ は同値関係である．

この同値関係 $\sim$ で類別したときの各同値類のことをGの軌道という．

3. ガロア群の軌道

$K[x]$の分離多項式$f(x)$ のガロア群をG とする．また，$f(x)$ の根全体からなる集合を

$$W = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$$

とする．$f(x)$ の$K[x]$ における既約多項式への分解を

$$f(x) = p_1(x)p_2(x)\cdots p_r(x)$$

とするとき，$p_i(x)$ $(i = 1,2,\cdots,r)$ の根の全体からなる集合を C_i とすれば，W は

$$W = C_1 \cup C_2 \cup \cdots \cup C_r, \qquad C_j \cap C_k = \phi \quad (j \neq k)$$

のように類別される．

一方，α を C_i の任意の元とするとき，$\beta \in W$ に対して

$$p_i(\beta) = 0 \iff \beta = \sigma(\alpha) \text{ であるような} \sigma \in G \text{ が存在する}$$

であることが知られている．

したがって，各C_i はG の元によって互いに写り得る$f(x)$ の根の全体になっている．この意味で，各 C_i をW におけるG の軌道という．

次に，有限体のガロア群の軌道について述べる．F を有限体$K = GF(q)$ のf 次拡大体，$G = G(F/K)$ をガロア拡大F/K のガロア群とする．F はK上の分離多項式

$$\varphi(x) = x^{q^f} - x$$

の根の全体であるから，F はG の軌道に分解され，G の軌道と$\varphi(x)$ の$K[x]$ における既約多項式とが 1 対 1 に対応する．

一方，$\varphi(x)$ はf の約数を次数にもつ，$K[x]$ のすべてのモニックな既約多項式の積となる．すなわち

$$\varphi(x) = \prod_{d|f} p_i(x) \qquad (\deg p_i(x) = d)$$

が成り立つ．

したがって，F をG の軌道に分解することによって，次数がf の約数である$K[x]$ のすべての既約多項式が求められる．

また，ガロア群G は$\sigma : \beta \mapsto \beta^q$ によって生成される．

4. ガロア群の軌道の例

例 1

分離多項式 $f(x) = x^4 - 8x^2 + 15 \in \mathbb{Q}[x]$のガロア群の軌道について考える．

$f(x)$の$\mathbb{Q}[x]$ における因数分解は，$f(x) = (x^2 - 3)(x^2 - 5)$である．

さらに$f(x) = \left(x + \sqrt{3}\right)\left(x - \sqrt{3}\right)\left(x + \sqrt{5}\right)\left(x - \sqrt{5}\right)$であるから，その根の全体の集合を$W$ とすると

$$W = \{\sqrt{3}, -\sqrt{3}, \sqrt{5}, -\sqrt{5}\}$$

である．また，$x^2 - 3$ の根全体の集合を$C_1 = \{\sqrt{3}, -\sqrt{3}\}$として，$x^2 - 5$ の根全体の集合を$C_2 = \{\sqrt{5}, -\sqrt{5}\}$とすれば

$$W = \{\sqrt{3}, -\sqrt{3}\} \cup \{\sqrt{5}, -\sqrt{5}\} = C_1 \cup C_2$$

が成り立つ．

さて，$f(x)$の最小分解体は $L = \mathbb{Q}\left(\sqrt{3}, \sqrt{5}\right)$ で，$[L: \mathbb{Q}] = 4$ である．

したがって，L のガロア群をGとすると $|G| = 4$ で，次の 4 つの元からなる．

$$1_L: \sqrt{3} \mapsto \sqrt{3},\ \sqrt{5} \mapsto \sqrt{5},$$

$$\sigma: \sqrt{3} \mapsto -\sqrt{3},\ \sqrt{5} \mapsto \sqrt{5},$$

$$\tau: \sqrt{3} \mapsto \sqrt{3},\ \sqrt{5} \mapsto -\sqrt{5},$$

$$\rho: \sqrt{3} \mapsto -\sqrt{3},\ \sqrt{5} \mapsto -\sqrt{5}$$

とすれば

$$1_L = \begin{pmatrix} \sqrt{3} & -\sqrt{3} & \sqrt{5} & -\sqrt{5} \\ \sqrt{3} & -\sqrt{3} & \sqrt{5} & -\sqrt{5} \end{pmatrix} \leftrightarrow 1,$$

$$\sigma = \begin{pmatrix} \sqrt{3} & -\sqrt{3} & \sqrt{5} & -\sqrt{5} \\ -\sqrt{3} & \sqrt{3} & \sqrt{5} & -\sqrt{5} \end{pmatrix} \leftrightarrow (1,2),$$

$$\tau = \begin{pmatrix} \sqrt{3} & -\sqrt{3} & \sqrt{5} & -\sqrt{5} \\ \sqrt{3} & -\sqrt{3} & -\sqrt{5} & \sqrt{5} \end{pmatrix} \leftrightarrow (3,4),$$

$$\rho = \begin{pmatrix} \sqrt{3} & -\sqrt{3} & \sqrt{5} & -\sqrt{5} \\ -\sqrt{3} & \sqrt{3} & -\sqrt{5} & \sqrt{5} \end{pmatrix} \leftrightarrow (1,2)(3,4).$$

よって

$$G \cong \{e, (1,2), (3,4), (1,2)(3,4)\}$$

である．この群では

$$\sigma^2 = \tau^2 = \rho^2 = 1_L,$$

$$\sigma\tau = \tau\sigma = \rho,$$

$$\tau\rho = \rho\tau = \sigma,$$

$$\rho\sigma = \sigma\rho = \tau$$

が成り立っているので，G は，クラインの四元群に同型であることがわかる．

さらに上記より，ガロア群 G の軌道が $C_1,\ C_2$ となっていることも示される．

以上

例 2（有限体のガロア群の軌道）

$p(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$ について考える．$\mathbb{Z}_2$上可約ならば 1 次因子 $x, x+1$ をもつ．ところが

$$p(0) = 1 \neq 0,\ p(1) = 1 \neq 0$$

なので，x でも $x+1$ でも割り切れないので$\mathbb{Z}_2$上既約である．

$K = GF(2) = \mathbb{Z}_2,\ F = GF(2^3)$ とする．ここで例えば

$$F = \mathbb{Z}_2[x]/(x^3 + x + 1),\ \alpha = x + (x^3 + x + 1), \alpha^3 + \alpha + 1 = 0$$

とすることができて

$$F = \{0,1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6\}$$

と表される．

F は $\varphi(x) = x^{2^3} - x = x^8 - x$ の最小分解体（根の全体）であり，$[F:\mathbb{Z}_2] = 3$ となっている．

また，$F/\mathbb{Z}_2$ はガロア拡大であり，ガロア群$G = G(F/\mathbb{Z}_2)$は

$$\sigma:\beta \mapsto \beta^2 \quad (\beta \in F)$$

で生成される位数 3 の巡回群$G = \{1_F, \sigma, \sigma^2\}$である．

まず，$\sigma(0) = 0,\ \sigma(1) = 1$ であるから，$C_0 = \{0\},\ C_1 = \{1\}$ である．

また，σ をF の 0 と 1 以外の元に次々に施すと

$$\alpha \mapsto \alpha^2 \mapsto \alpha^4 \mapsto \alpha^8 = \alpha,$$

$$\alpha^3 \mapsto \alpha^6 \mapsto \alpha^{12} = \alpha^5 \mapsto \alpha^{10} = \alpha^3$$

となるから，G の軌道は

$$C_0 = \{0\},\ C_1 = \{1\},\ C_2 = \{\alpha,\alpha^2,\alpha^4\},\ C_3 = \{\alpha^3,\alpha^5,\alpha^6\}$$

である．

さらに，軌道C_2に対応する $\mathbb{Z}_2[x]$ の既約多項式は

$$(x-\alpha)(x-\alpha^2)(x-\alpha^4)=x^3+x+1$$

であり，軌道C_3に対応する $\mathbb{Z}_2[x]$ の既約多項式は

$$(x-\alpha^3)(x-\alpha^5)(x-\alpha^6)=x^3+x^2+1$$

である．したがって

$$\varphi(x)=x^{2^3}-x=x^8-x=x(x+1)(x^3+x+1)(x^3+x^2+1)$$

が成り立つことがわかる．

以上

参考文献

1）増田真郎「応用のための代数系入門」サイエンス社，1981
2）桂利行「代数学 I 群と環」東京大学出版会，2004