

大学初年次における数学教材の提案（その 30）

～ガロア群～

貴田研司^{*1}

A Suggestion on Mathematical Materials for Freshman Education Vol. 30

～ The Galois Groups ～

by

Kenshi KIDA ^{*1}

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

あらまし

ガロア拡大，およびガロア群の基本的な概念の紹介を目的とする．本論文では，特に，多項式のガロア群について詳しく扱うことにするが，解説の後に具体的に 2 つの分離多項式を挙げて，そのそれぞれのガロア群を求める過程について詳述する．

Abstract

The purpose of this paper is to present fundamental concepts of the Galois extensions and the Galois groups. In particular, we afford detailed explanations and several concrete examples of the Galois groups of separable polynomials.

キーワード：ガロア群，ガロア拡大，分離多項式

Keywords: Galois Group, Galois Extension, Separable Polynomial

1. はじめに

大学初年次の数学科目において専攻を問わず皆に学んで欲しいとの思いを込めて，ガロア拡大，そしてガロア群の概念の基本的な部分を紹介する．そのために，体の代数拡大について述べることから始める．それから，最小多項式，最小分解体，単純拡大などのガロア群を学ぶのに必要な概念の紹介を行う．そして，ガロア群の中でも特に，多項式のガロア群についての詳しい解説をしたのちに，具体的な例として 2 つの分離多項式を挙げて，そのそれぞれのガロア群を構成していく方法について丁寧に述べる．

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⁾，横井秀夫・裕野敏博共著「代数演習」²⁾を大いに参考にした．

2. 体の拡大

体 L の部分集合 K が， L と同じ演算で体をなすとき， L を K の拡大体， K を L の部分体といい， L/K で表す．

体の拡大 L/K において， L は K 上の線形空間とみられる． L が K 上の線形空間として有限次元であるとき， L/K は有限次拡大，または有限拡大という． L/K の線形空間としての次元を，その拡大次数といい， $[L : K]$ と表す．また， L/K の線形空間としての基底を， L の K 上の基底という．

^{*1} 高輪教養教育センター 准教授

Liberal Arts Education Center, Takanawa Campus, Associate
Professor

定理 2.1

$L/F, F/K$ が共に有限次拡大で

$$[L:F] = s, \quad \alpha_1, \alpha_2, \dots, \alpha_s \text{ を } L \text{ の } F \text{ 上の基底}$$

$$[F:K] = t, \quad \beta_1, \beta_2, \dots, \beta_t \text{ を } F \text{ の } K \text{ 上の基底}$$

とする. このとき st 個の元

$$\alpha_i \beta_j \quad (i = 1, 2, \dots, s; j = 1, 2, \dots, t)$$

は, L の K 上の基底である. すなわち L/K も有限次拡大で

$$[L:K] = [L:F][F:K]$$

が成り立つ.

体の拡大 L/K において, L の元 $\alpha_1, \alpha_2, \dots, \alpha_m$ (有限個) と K を含む最小の体を, K 上 $\alpha_1, \alpha_2, \dots, \alpha_m$ によって生成された体, または K に $\alpha_1, \alpha_2, \dots, \alpha_m$ を添加して得られる体といい, $K(\alpha_1, \alpha_2, \dots, \alpha_m)$ と表す. 特に, ただ一つの元 α を添加して得られる体 $K(\alpha)$ を単純拡大といい, α を $K(\alpha)$ の原始元という.

体の拡大 L/K において, L の元 α を根にもつような, K 上の多項式 $f(x) \neq 0$ が存在するとき, α を K 上の代数的元という. また, L の任意の元が K 上の代数的元であるとき, L/K は代数的拡大, または単に代数拡大であるという. これについては, 以下のことが知られている.

定義 (最小多項式)

体の拡大 L/K において, L の元 α が K 上の代数的元であるとき, α を根とする K 上の多項式の中で次数が最低のものを, α の K 上の最小多項式という. これは, K の定数因子を除いて一意に定まり, K 上既約である. その最小多項式の次数を, 代数的元 α の K 上の次数という.

定義 (K -同型)

体 K の 2 つの拡大 L/K と L'/K の間の同型 $\sigma: L \rightarrow L'$ が K の元を不変にすると K -同型であるという.

定理 2.2

体 K 上の代数的元 α を K に添加して得られる単純拡大 $K(\alpha)$ は, α の K 上の最小多項式 $p(x)$ を法とする多項式環 $K[x]$ の剰余類体 $K[x]/(p(x))$ に K -同型である. したがって, 拡大 $K(\alpha)/K$ は有限次拡大で, その拡大次数は α の K 上の次数に等しい.

定理 2.3

体 K 上の代数的元 α の, K 上の次数を n とするとき, 単純拡大 $K(\alpha)$ の元は

$$k_0 + k_1\alpha + \cdots + k_{n-1}\alpha^{n-1} \quad (k_i \in K; i = 0, 1, \dots, n-1)$$

の形に一意的に表される.

定理 2.4

体の拡大 L/K が有限次拡大であるための必要十分条件は, L が K 上の代数的元 $\alpha_1, \alpha_2, \dots, \alpha_m$ (有限個) を添加して得られる体であること, すなわち

$$L = K(\alpha_1, \alpha_2, \dots, \alpha_m)$$

となることである.

定義 (最小分解体)

体の拡大 L/K に対して, K 上の多項式 $f(x)$ が L において 1 次式の積に分解されるとき, すなわち, $f(x)$ の根がすべて L に属するとき, L を $f(x)$ の分解体という. 特に, L のいかなる真の部分体も $f(x)$ の分解体にならないとき, すなわち, $f(x)$ の根をすべて K に添加して L が得られるとき, 体 L を $f(x)$ の K 上の最小分解体という.

最小分解体について, 次のことが知られている.

定理 2.5

体 K 上の任意の多項式 $f(x)$ に対して, $f(x)$ の K 上の最小分解体は必ず存在して, それは K 上の同型を除いて一意的に定まる.

定義 (分離多項式)

体 K 上の多項式 $f(x)$ がその分解体において重根をもたないとき, 分離多項式と呼ばれる.

3. ガロア群

体 L の自己同型写像, すなわち L から L 自身の上への同型写像の全体からなる集合を $\text{Aut}(L)$ と記す. $\text{Aut}(L)$ は, 写像の合成に関して群をなすから, L の自己同型群と言われる.

K が L の部分体であるとき, L の K - 自己同型写像, すなわち

$$\sigma(a) = a \quad (a \in K)$$

であるような $\text{Aut}(L)$ の元の全体からなる集合を $G(L/K)$ と記す. これは, $\text{Aut}(L)$ の部分群である.

S を $\text{Aut}(L)$ の空でない部分集合とすると, S の各々の元によって不変であるような L の元の全体からなる集合

$$F = \{\alpha \in L \mid \sigma(\alpha) = \alpha \text{ (任意の } \sigma \in S) \}$$

は、 L の部分体となる．これを L における S の不変体（または、固定体）といい、 $i(S)$ と表す．

L/K を体の拡大とする． L の K -自己同型群 $G(L/K)$ の L における不変体が K に一致するとき、すなわち

$$i(G(L/K)) = K$$

が成り立つとき、体の拡大 L/K をガロア拡大という．このとき $G(L/K)$ を、ガロア拡大の L/K のガロア群という．

これについて、以下のことが知られている．

定理 3.1

L/K を有限次拡大とすると、次の条件(1), (2), (3)は同値である．

- (1) L/K はガロア拡大である．
- (2) $\text{Aut}(L)$ の部分群 G で $K = i(G)$ となるものが存在する．
- (3) L は、 $K[x]$ のある分離多項式 $f(x)$ の K 上の最小分解体である．

これらが成り立つとき

$$G = G(L/K), \quad |G(L/K)| = [L : K]$$

となっている．

[分離多項式のガロア群]

有限次拡大 L/K がガロア拡大であるとき、定理 3.1 により、 L は、 $K[x]$ のある分離多項式 $f(x)$ の K 上の最小分解体である．

今、 $f(x)$ を $K[x]$ の分離多項式として、 $f(x)$ の K 上の最小分解体を L とする．ガロア拡大の L/K のガロア群 $G(L/K)$ のことを、多項式 $f(x)$ のガロア群（または、代数方程式 $f(x) = 0$ のガロア群）という．

多項式

$$f(x) = k_n x^n + k_{n-1} x^{n-1} + \cdots + k_1 x + k_0 \quad (k_i \in K; i = 0, 1, 2, \dots, n)$$

の、 L における根を α とするとき、任意の $\sigma \in G(L/K)$ に対して

$$\begin{aligned} f(\sigma(\alpha)) &= k_n \{\sigma(\alpha)\}^n + k_{n-1} \{\sigma(\alpha)\}^{n-1} + \cdots + k_1 \sigma(\alpha) + k_0 \\ &= k_n \sigma(\alpha^n) + k_{n-1} \sigma(\alpha^{n-1}) + \cdots + k_1 \sigma(\alpha) + k_0 \\ &= \sigma(k_n \alpha^n + k_{n-1} \alpha^{n-1} + \cdots + k_1 \alpha + k_0) \\ &= \sigma(f(\alpha)) \\ &= \sigma(0) \\ &= 0 \end{aligned}$$

であるから、 $\sigma(\alpha)$ もまた $f(x)$ の根である．

さらに、次のことが知られている。

定理 3.2

$f(x)$ を $K[x]$ の n 次分離多項式とすると、 $f(x)$ のガロア群 G は、 n 次対称群の部分群（ n 次置換群）に同型である。すなわち、 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なっている。

定理 3.3（分離多項式の既約性）

$K[x]$ の分離多項式 $f(x)$ が既約であるための必要十分条件は、 $f(x)$ のガロア群 G が推移的である、すなわち、 $f(x)$ の任意の 2 つの根 α, β について、ある $\sigma \in G$ が存在して $\sigma(\alpha) = \beta$ となることである。

4. 代数拡大の例

例

$$\mathbb{Q}(\sqrt[3]{2}, \omega) \quad (\omega \text{ は } 1 \text{ の原始 } 3 \text{ 乗根})$$

について考える。

（注意）

$$\omega = \frac{-1 + \sqrt{-3}}{2} \text{ とすれば } \omega^2 = \frac{-1 - \sqrt{-3}}{2} \text{ であり, } \omega = \frac{-1 - \sqrt{-3}}{2} \text{ とすれば } \omega^2 = \frac{-1 + \sqrt{-3}}{2} \text{ である.}$$

まず、 $\sqrt[3]{2}$ の $\mathbb{Q}$ 上の最小多項式は $x^3 - 2$ であり

$$\mathbb{Q}[x]/(x^3 - 2) \cong \mathbb{Q}(\sqrt[3]{2}), \quad \mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a, b, c \in \mathbb{Q}\}$$

となっている。

ここで、 $K_1 = \mathbb{Q}(\sqrt[3]{2})$ とおく。 $K_1[x] \supset \mathbb{Q}[x] \ni x^2 + x + 1 = (x - \omega)(x - \omega^2)$ について、 $\omega, \omega^2 \notin K_1$ である。したがって、 $x^2 + x + 1$ は $K_1[x]$ で既約であるから、 ω の K_1 上の最小多項式である。よって

$$K_1[x]/(x^2 + x + 1) \cong K_1(\omega) = \mathbb{Q}(\sqrt[3]{2}, \omega)$$

が成り立つ。

$K_1(\omega)$ の元 α は一意的に

$$\alpha = u + v\omega \quad (u, v \in K_1 = \mathbb{Q}(\sqrt[3]{2}))$$

と表される。したがって

$$u = a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2, \quad v = a' + b'\sqrt[3]{2} + c'(\sqrt[3]{2})^2 \quad (a, b, c, a', b', c' \in \mathbb{Q})$$

とすれば

$$\alpha = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2\} + \{a' + b'\sqrt[3]{2} + c'(\sqrt[3]{2})^2\}\omega = a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 + a'\omega + b'\sqrt[3]{2}\omega + c'(\sqrt[3]{2})^2\omega$$

と、一意的に表される. $K_1(\omega) = \mathbb{Q}(\sqrt[3]{2}, \omega)$ は, このような形の元全体からなる体であり

$$[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = 6$$

であることがわかる.

5. ガロア群の例

例題 1

分離多項式 $p(x) = x^3 - 2$ の $\mathbb{Q}$ 上のガロア群を求めよ.

(解答)

$$p(x) = x^3 - 2 = (x - a)(x - a\omega)(x - a\omega^2) \in \mathbb{Q}[x] \quad (a = \sqrt[3]{2}, \omega \text{ は } 1 \text{ の原始 } 3 \text{ 乗根})$$

は, 既約な分離多項式であり, 最小分解体は $L = \mathbb{Q}(a, a\omega, a\omega^2) = \mathbb{Q}(a, \omega)$ であり. 第 4 章の例により, $[L : \mathbb{Q}] = 6$ と

なっていることがわかる. したがって, $p(x)$ のガロア群を G とすると, 定理 3.1 と定理 3.2 により

$$G = \text{Gal}(L/\mathbb{Q}), \quad |G| = [L : \mathbb{Q}] = 6, \quad G \cong S_3$$

であることがわかる.

定理 3.3 から, $\sigma \in G$ によって, a は a の $\mathbb{Q}$ 上の最小多項式 $p(x)$ の根 $a, a\omega, a\omega^2$ のいずれかにうつされ, そして, ω は ω の $\mathbb{Q}$ 上の最小多項式 $x^2 + x + 1 = (x - \omega)(x - \omega^2)$ の根 $\omega, \bar{\omega} = \omega^2$ のいずれかにうつされる.

したがって, G の元は

$$\sigma_0: a \mapsto a, \omega \mapsto \omega,$$

$$\sigma_1: a \mapsto a\omega, \omega \mapsto \omega,$$

$$\sigma_2: a \mapsto a\omega^2, \omega \mapsto \omega,$$

$$\tau_0: a \mapsto a, \omega \mapsto \omega^2,$$

$$\tau_1: a \mapsto a\omega, \omega \mapsto \omega^2,$$

$$\tau_2: a \mapsto a\omega^2, \omega \mapsto \omega^2$$

のいずれかとなるが, $|G| = 6$ であるからこれらが G の元のすべてである.

以上より, 定理 3.2 に述べられているように

$$\sigma_0 = \begin{pmatrix} a & a\omega & a\omega^2 \\ a & a\omega & a\omega^2 \end{pmatrix},$$

$$\sigma_1 = \begin{pmatrix} a & a\omega & a\omega^2 \\ a\omega & a\omega^2 & a \end{pmatrix},$$

$$\sigma_2 = \begin{pmatrix} a & a\omega & a\omega^2 \\ a\omega^2 & a & a\omega \end{pmatrix},$$

$$\tau_0 = \begin{pmatrix} a & a\omega & a\omega^2 \\ a & a\omega^2 & a\omega \end{pmatrix},$$

$$\tau_1 = \begin{pmatrix} a & a\omega & a\omega^2 \\ a\omega & a & a\omega^2 \end{pmatrix},$$

$$\tau_2 = \begin{pmatrix} a & a\omega & a\omega^2 \\ a\omega^2 & a\omega & a \end{pmatrix}$$

となっていることがわかる.

(解答終)

例題 2

分離多項式 $p(x) = x^4 - 2$ の $\mathbb{Q}$ 上のガロア群を求めよ.

(解答)

$$p(x) = x^4 - 2 = (x^2 + \sqrt{2})(x^2 - \sqrt{2}) = (x + bi)(x - bi)(x + b)(x - b) \in \mathbb{Q}[x] \quad (b = \sqrt[4]{2}, i \text{ は虚数単位})$$

は、既約な分離多項式であり、最小分解体は $L = \mathbb{Q}(bi, -bi, b, -b) = \mathbb{Q}(b, i)$ である. これから、第 4 章の例と同様な議論

を行う. まず、 $b = \sqrt[4]{2}$ の $\mathbb{Q}$ 上の最小多項式は $x^4 - 2$ であり

$$\mathbb{Q}[x]/(x^4 - 2) \cong \mathbb{Q}(\sqrt[4]{2}),$$

となっており、 $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ が成り立つ. ここで、 $K_1 = \mathbb{Q}(\sqrt[4]{2})$ とおくと、 $K_1[x] \supset \mathbb{Q}[x] \ni x^2 + 1 = (x + i)(x - i)$ について、 $i, -i \notin K_1$ である. よって、 $x^2 + 1$ は $K_1[x]$ で既約であるから、 i の K_1 上の最小多項式である. よって

$$K_1[x]/(x^2 + 1) \cong K_1(i) = \mathbb{Q}(\sqrt[4]{2}, i)$$

となり、 $[L : K_1] = 2$ が成り立つ.

したがって、定理 2.1 により $[L : \mathbb{Q}] = [L : K_1][K_1 : \mathbb{Q}] = 2 \cdot 4 = 8$ となっていることがわかる. したがって、 $p(x)$ のガロア群を G とすると、定理 3.1 と定理 3.2 により

$$G = \text{Gal}(L/\mathbb{Q}), \quad |G| = [L : \mathbb{Q}] = 8, \quad G \cong (S_4 \text{ の部分群})$$

であることがわかる.

定理 3.3 から、 $\sigma \in G$ によって、 b は b の $\mathbb{Q}$ 上の最小多項式 $p(x)$ の根 $bi, -bi, b, -b$ のいずれかにうつされ、そして、 i は i の $\mathbb{Q}$ 上の最小多項式 $x^2 + 1 = (x + i)(x - i)$ の根 $i, -i$ のいずれかにうつされる.

したがって、 G の元は

$$1_G: b \mapsto b, i \mapsto i,$$

$$\rho_1: b \mapsto bi, i \mapsto i,$$

$$\rho_2: b \mapsto -b, i \mapsto i,$$

$$\rho_3: b \mapsto -bi, i \mapsto i,$$

$$\rho_4: b \mapsto b, i \mapsto -i,$$

$$\rho_5: b \mapsto bi, i \mapsto -i,$$

$$\rho_6: b \mapsto -b, i \mapsto -i,$$

$$\rho_7: b \mapsto -bi, i \mapsto -i$$

のいずれかとなるが, $|G| = 8$ であるからこれらが G の元のすべてである.

以上より, 定理 3.2 に述べられているように

$$\begin{aligned} 1_G &= \begin{pmatrix} b & -b & bi & -bi \\ b & -b & bi & -bi \end{pmatrix}, \\ \rho_1 &= \begin{pmatrix} b & -b & bi & -bi \\ bi & -bi & -b & b \end{pmatrix}, \\ \rho_2 &= \begin{pmatrix} b & -b & bi & -bi \\ -b & b & -bi & bi \end{pmatrix}, \\ \rho_3 &= \begin{pmatrix} b & -b & bi & -bi \\ -bi & bi & b & -b \end{pmatrix}, \\ \rho_4 &= \begin{pmatrix} b & -b & bi & -bi \\ b & -b & -bi & bi \end{pmatrix}, \\ \rho_5 &= \begin{pmatrix} b & -b & bi & -bi \\ bi & -bi & b & -b \end{pmatrix}, \\ \rho_6 &= \begin{pmatrix} b & -b & bi & -bi \\ -b & b & bi & -bi \end{pmatrix}, \\ \rho_7 &= \begin{pmatrix} b & -b & bi & -bi \\ -bi & bi & -b & b \end{pmatrix} \end{aligned}$$

となっていることがわかる.

さらに, ここで

$$\sigma = \rho_1: b \mapsto bi, i \mapsto i, \tau = \rho_4: b \mapsto b, i \mapsto -i$$

とおくと

$$\sigma^2: b \mapsto -b, i \mapsto i$$

$$\sigma^3: b \mapsto -bi, i \mapsto i$$

$$\sigma^4: b \mapsto b, i \mapsto i$$

なので $\sigma^4 = 1$ が成り立つ. また, $\tau^2: b \mapsto b, i \mapsto i$ により $\tau^2 = 1$ も成り立つ.

さらに

$$\sigma\tau^{-1}: b \mapsto bi, i \mapsto -i,$$

$$\tau\sigma\tau^{-1}: b \mapsto -bi, i \mapsto i$$

かつ

$$\sigma^{-1} = \sigma^3: b \mapsto -bi, i \mapsto i$$

により $\tau\sigma\tau^{-1} = \sigma^{-1}$ も得られた.

したがって, G は二面体群

$$D_4 = \langle \sigma, \tau \mid \sigma^4 = 1, \tau^2 = 1, \tau\sigma\tau^{-1} = \sigma^{-1} \rangle = \{1, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$$

に同型であることもわかる.

(解答終)

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) 横井秀夫・碓野敏博共著「代数演習」サイエンス社, 1989