東海大学紀要情報通信学部
Vol.12,No.2,2019,pp.40-43

トピックス

大学初年次における数学教材の提案（その 31）
～有限体のガロア群～

貴田研司[*1]

A Suggestion on Mathematical Materials for Freshman Education Vol. 31
~ The Galois Groups of Finite Fields ~

by

Kenshi KIDA [*1]

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

あらまし

まず，有限体のガロア群がフロベニウス自己同型によって生成される巡回群であることを解説する．そして，具体的な計算例を挙げて理解を助けることとする．この例の中で，ガロア対応についても述べる．

Abstract

First, we explain the concept of Galois groups of finite fields. Further, we present an example of Galois groups of finite fields and show the Galois correspondences in this case.

キーワード：ガロア群，有限体，フロベニウス写像，ガロア対応
Keywords: *Fundamental Theorem of Galois Theory, Galois Group, Finite Field, Frobenius Map, Galois Correspondence*

1. はじめに

有限体の場合には，ガロア群の構造について簡明な結果が得られているのでこれについて紹介する．有限体の存在と一意性，そしてその構成方法から始めて，ガロア群がフロベニウス写像と呼ばれるものによって生成される巡回群であることについて述べ，そのあとで具体例を挙げることとする．また，ガロア対応についても触れる．

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)]を大いに参考にした．

2. 有限体のガロア群

有限体について以下のことが知られている[1)2)]．

定理2.1（有限体の構成方法）

$\varphi(x)$ を $\mathbb{Z}_p$ 上の n 次既約多項式とすれば，$\mathbb{Z}_p[x]/(\varphi(x))$ は $\mathbb{Z}_p$ の n 次拡大体で，元の個数が p^n の有限体である．

定理2.2（有限体の存在と一意性）

任意の素数 p と自然数 f に対して，元の個数が p^f となる有限体 F が存在する．このような F は素体 $\mathbb{Z}_p$ 上の分離多項式 $x^{p^f}-x$ の最小分解体に同型である．したがって，同型を度外視して一意的に定まる．

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

記号　q 個の元からなる体を$GF(q)$ と表す.

※有限体のことを発見者にちなんで，ガロア体（Galois Field）ともいう.

定理2.3

$K = GF(q)$ $(q = p^n)$ が有限体で，F をK の f 次拡大体とすると，$F = GF(q^f)$であり，F はK 上の分離多項式$x^{q^f} - x$の K 上の最小分解体である．したがって，有限体の有限次拡大はガロア拡大である.

定理 2.4（フロベニウス写像）

F を有限体 $K = GF(q)$ のf 次拡大体とする．このとき，ガロア群$G(F/K)$は，写像

$$\sigma : \beta \to \beta^q \quad (\beta \in F)$$

で生成される位数f の巡回群である.

一般に，ガロア拡大L/Kのガロア群$G(L/K)$ が巡回群であるときに，拡大L/K を巡回拡大という.

したがって，有限体 K の有限次拡大は巡回群である.

【有限体のガロア対応】

L/K を有限次ガロア拡大，$G = G(L/K)$ をそのガロア群とする．Mを L/K の中間体とするとき，L/M はガロア拡大でそのガロア群 $H = G(L/M)$ は，G の部分群である．そして，ガロア群の定義からのH 不変体（または，固定体）について，$i(H) = M$ が成り立つ.

特に，$K = GF(q),\ L = GF(q^f)$ のとき，$M = GF(q^e)$ が L/K の中間体であるならば，$e \mid f$ だから $f = es$ とおく．このとき L/M 拡大はガロア拡大で，$[L : M] = s$ であるから，そのガロア群$G(L/M)$は位数 s の巡回群である．$G(L/M)$ の生成元としてはσ^e がとられる.

ガロア拡大の中間体全体の集合とガロア群の部分群全体の集合には，1 対 1 の対応$(M \longleftrightarrow H)$ が存在する.

これをガロア対応という.

3. 有限体のガロア群の例

例

$K = GF(2) = \mathbb{Z}_2,\ F = GF(2^4)$ とする.

(付記)[1)]

$\mathbb{Z}_2[x]$の 4 次既約多項式は，$x^4 + x + 1,\ x^4 + x^3 + 1,\ x^4 + x^3 + x^2 + x + 1$ の 3 つのみであることが知られている.

そこで定理 2.1 より，例えば

$$F = \mathbb{Z}_2[x]/(x^4 + x + 1),\ \alpha = x + (x^4 + x + 1),\quad \alpha^4 + \alpha + 1 = 0$$

とすることができて

$$F = \{0,1,\alpha,\alpha^2,\alpha^3,\cdots\cdots,\alpha^{13},\alpha^{14}\}$$

と表される．

定理 2.2 または定理 2.3 より，F は $\varphi(x) = x^{2^4} - x = x^{16} - x$ の最小分解体であり，$[F:\mathbb{Z}_2] = 4$ となっている．

また，定理 2.3 により $F/\mathbb{Z}_2$ はガロア拡大である．そして，定理 2.4 よりガロア群$G = G(F/\mathbb{Z}_2)$は

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

で生成される位数 4 の巡回群$G = \{1_F,\sigma,\sigma^2,\sigma^3\}$である．

G の真部分群で単位群と異なるものは，σ^2 で生成される位数 2 の巡回群$H = \{1_F,\sigma^2\}$ のみである．H に対応する$F/\mathbb{Z}_2$ の中間体M は1_F と σ^2 によって不変に保たれるFの元の全体である．

さて，F の$0,1$ 以外の各元にσ^2 を施すと

$$\alpha \to \alpha^4,$$

$$\alpha^2 \to \alpha^8,$$

$$\alpha^3 \to \alpha^{12},$$

$$\alpha^4 \to \alpha^{16} = \alpha,$$

$$\alpha^5 \to \alpha^{20} = \alpha^5,$$

$$\alpha^6 \to \alpha^{24} = \alpha^9,$$

$$\alpha^7 \to \alpha^{28} = \alpha^{13},$$

$$\alpha^8 \to \alpha^{32} = \alpha^2,$$

$$\alpha^9 \to \alpha^{36} = \alpha^6,$$

$$\alpha^{10} \to \alpha^{40} = \alpha^{10},$$

$$\alpha^{11} \to \alpha^{44} = \alpha^{14},$$

$$\alpha^{12} \to \alpha^{48} = \alpha^3,$$

$$\alpha^{13} \to \alpha^{52} = \alpha^7,$$

$$\alpha^{14} \to \alpha^{56} = \alpha^{11}$$

であることから

$$M = \{0,1,\alpha^5,\alpha^{10}\} = GF(2^2)$$

となっていることがわかる.

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) 貴田研司,“大学初年次における数学教材の提案（その 11）～有限体入門～,”東海大学紀要情報通信学部, Vol. 10, No. 1, 2017, pp. 105-113