The Fundamental Theorem of Galois Theory

ver 0.1

Akari(@akari0koutya)

2021 年 12 月 30 日

概要

これは前作 [Akari] の続編でり，これを読むにあたっては [Akari] の記述を全て仮定して進めてきます．
また，これは私の備忘録でもあるので証明は雑であったり，過分であったりします．

This is your last chance. After this, there is no turning back. You take the blue pill, the story ends, you wake up in your bed and believe whatever you want to believe. You take the red pill, you stay in Wonderland and I show you how deep the rabbit-hole goes.

— *Morpheus*

目次

Notation.

$\mathbb{N} = \{0, 1, 2, \dots\}$
$\mathbb{Z}$ = 整数環
$\mathbb{R}$ = 実数体
$\mathbb{C}$ = 複素数体
$\mathbb{F}_{p^n}$ = 素数 p の正整数冪を位数にもつ体
G = 群 (可換であるとは限らない．)
A, R = 単位元を持つ可換環
K, L = 可換体
$\overline{K}$ = K の代数閉包

$\mathrm{Hom}_A(M, N)$ M, N が A 代数のとき A 準同型全体 (本稿では A-加群については扱わない．)
$\mathrm{ch}\, K$ K の標数
$\deg f$ 多項式 f の次数

$\deg 0 = -\infty$ として扱う．また，$\varnothing$ の生成するイデアルは (0)，故に $\gcd(0,0) = \gcd(\varnothing) = 0$ であるものとする．これは，定義から明らかなものであるが，念の為に明示しておく．

集合の包含関係は $\subseteq$ で表し，$\subset$ で真部分集合であるものとする．

1 分離拡大

代数閉体 を思い出そう．体 K に対して $f(x) \in K[x] \backslash K$ が K に根を持つことをいう．次に **代数閉包** を思い出そう．これは L/K が代数拡大であり L が代数閉体となる L のことをいう．Steinitz により K の代数閉包は一意に存在するのであった．以降，K の代数閉包は $\overline{K}$ で表すものとする．

何故分離拡大による議論が必要があるのかというと，今後扱うであろうガロア理論というのは，ガロア群の部分群と中間体が一対一対応を持つという主張であり，体の有限次拡大がガロア拡大であることと正規拡大かつ分離拡大となることと同値になるのである．そのことを念頭に置いて読んでほしい．

α が $f(x)$ の **重根** であるとは，$f(x) \in K[x]$，$\alpha \in \overline{K}$ であり，$f(x)$ が $\overline{K}[x]$ において $(x-\alpha)^2$ で割り切られることをいう．多項式が **分離的** であるとは $f(x) \in K[x]$ が $\overline{K}$ で重根を持たないことをいい，そうでなければ **非分離的** であるという．また，これを **分離多項式** といったりもする．α が K 上 **分離的** であるとは $\alpha \in \overline{K}$ の K 上最小多項式が分離的であることをいい，そうでなければ **非分離的** であるという．L/K が代数拡大であり，L の全ての元が K 上分離的なら，L を K の **分離拡大** であるといい，そうでなければ **非分離拡大** であるという．最後に，K のすべての代数拡大が分離拡大であるならば，K を **完全** であるといい，これを**完全体**という．

> **Proposition 1.1**
> L/K が代数拡大，$\alpha \in L$ で，$K \subset M \subset L$ を中間体とする．このとき，α が K 上分離的なら，M 上でも分離的である．

Proof. α の M 上の最小多項式 $g(x)$ は K 上の最小多項式 $f(x)$ を割り切る．故に，$f(x)$ が重根を持たなければ，$g(x)$ も重根を持たない． □

これは，$\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{2}] \subset \mathbb{C}$ において，$\sqrt[3]{2}$ は $\mathbb{Q}$ 上であるなら最小多項式は $x^3 - 2$ であり，$\mathbb{Q}[\sqrt[3]{2}]$ 上であるなら最小多項式は $x - \sqrt[3]{2}$ であることを考えると簡単にわかるだろう．

$R[x]$ の元 $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + x^n$ に対して **微分** を

$$f'(x) = a_1 + 2a_2 x + 3a_3 x^2 + \cdots + n x^{n-1} \tag{1.1}$$

で定める．このとき，

$$\{f(x) + g(x)\}' = f'(x) + g'(x) \tag{1.2}$$
$$\{f(x)g(x)\}' = f'(x)g(x) + f(x)g'(x) \tag{1.3}$$

が成り立つ．

> **Proposition 1.2**
> $f(x) \in K[x]$，$\alpha \in \overline{K}$ に対して，$f(\alpha) = 0$ とする時，以下は同値である．
>
> (1) α は $f(x)$ の重根である．
> (2) $f'(\alpha) = 0$ である．

Proof. (1) $\Rightarrow$ (2)：仮定より，ある $g(x) \in \overline{K}[x]$ が存在し $f(x) = (x-\alpha)^2 g(x)$ となる．微分して $f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x)$ となるため $f'(\alpha) = 0$ となる．

(2) ⇒ (1) : α が重根でないとすると，ある $g(x) \in \overline{K}[x]$ が存在し，$f(x) = (x-\alpha)g(x)$ となり，また，$g(\alpha) \neq 0$ である．このとき，$f'(x) = g(x) + (x-\alpha)g'(x)$ より $f'(\alpha) \neq g(\alpha) \neq 0$ である．これは仮定に矛盾する． □

Proposition 1.3

$f \in K[x]$ を定数でない既約多項式とする．このとき，次の主張は同値である．

(1) f は $\overline{K}$ で重根を持つ．
(2) $K[x]$ 上 $\gcd(f, f') \neq 1$ である．
(3) $\mathrm{ch}\, K = p > 0$ であり，f は x^p の多項式となる，すなわち f に対し g が存在し $f(x) = g(x^p)$ となる．
(4) 全ての f の根は $\overline{K}$ で重根となる．

Proof. (1) ⇒ (2) : $\alpha \in \overline{K}$ を f の重根とすると $f = (x-\alpha)^m g(x)$ と表せる $(m \geq 2)$．このとき，

$$f'(x) = m(x-\alpha)^{m-1}g(x) + (x-\alpha)^m g'(x) \tag{1.4}$$

であるため，f と f' は共通因子 $(x-\alpha)$ を持つ．

(2) ⇒ (3) : f を任意の既約多項式とし，$\deg(f') < \deg(f)$ とするとき，

$$\gcd(f, f') \neq 1 \Rightarrow f' = 0 \tag{1.5}$$

を示せばいい．$f(x) = a_0 + a_1 x + \cdots + a_d x^d$，$\deg f > 0$ とおく．このとき，$f'(x) = a_1 + 2a_2 x + \cdots + d a_d x^{d-1}$ が零多項式となる必要十分条件は $\mathrm{ch}\, K = p > 0$ かつ，任意の α_i が p で割り切れることである．もし，$f' \neq 0$ ならば，ある $g(x) = \gcd(f, f')$ ($g(x)$ は定数であってもいい) が存在し，$f(x) = p(x)g(x)$，$f'(x) = q(x)g(x)$ と書けるが，$f(x)$ は既約であるから矛盾．よって $f' = 0$ である (**Remark**. $\gcd(f, f) = \gcd(f, 0) = f$ である．詳しくは [nLab][Wiki][MSE] を参照のこと)．

(3) ⇒ (4) : 仮定より，$f(x) = g(x^p)$ を満たす $g(x^p) \in K[x]$ が存在する．$g(x) = \prod_i (x - a_i)^{m_i}$ とする．このとき，任意の a_i に対し $\alpha \in \overline{K}$ が存在し，$a_i = \alpha_i^p$ を満たす．ここで，

$$f(x) = g(x^p) = \prod_i (x^p - a_i)^{m_i} = \prod_i (x - \alpha_i)^{p m_i} \tag{1.6}$$

あり (**Remark**. $\mathrm{ch}\, K = p > 0$ のとき，二項定理から $(x+y)^p = x^p + y^p$ であることを思い出そう)，これは $f(x)$ の根が少なくとも p 重根であることを示している．

(4) ⇒ (1) : これは明らか． □

Corollary 1.4

$f \in K[x]$ を 0 でない多項式とする．このとき，次の主張は同値である．

(1) $f(x)$ は $\overline{K}$ で重根を持たない．すなわち，単根のみを持つ．
(2) $K[x]$ 上で $\gcd(f, f') = 1$ である．

Proof. (1) ⇒ (2) : は **Proposition 1.3** より明らかである．

(2) ⇒ (1) : 仮定より，$p(x)f(x) + g(x)f'(x) = 1$ を満たす $p(x), g(x) \in K[x]$ が存在する．もし $f(x)$ が重根を持つなら **Proposition 1.2** より $f'(\alpha) = 0$ を満たす $\alpha \in \overline{K}$ が存在するが，$p(\alpha)f(\alpha) + g(\alpha)f'(\alpha) = 0$ となり矛盾する． □

これは多項式が **分離的** であるということの定義そのものである．

体 K の **characteristic exponent** とは $\mathrm{ch}\, K = 0$ なら 1 であり，$\mathrm{ch}\, K = p > 0$ なら p である．こう定義すると，q が characteristic exponent，n は正整数であるとき，K から K の中への同型写像 $x \mapsto x^{q^n}$) が存在する．このことから，すべての $a \in K$，$n \in \mathbb{N}$ に対して $x^{q^n} = a$ となる $x \in \overline{K}$ がただ一つ存在する．

Proposition 1.5

体 K，K の characteristic exponent q に対して，次の主張は同値である．

(1) K は完全体である．
(2) $K = K^q$ が成り立つ．

参考文献

[雪江 10] 雪江明彦. 代数学 2 環と体のガロア理論. 日本評論社. 2010.

[AT69] M. F. Atiyah and I. G. MacDonald. Introduction to commutative algebra. Addison Wesley Publishing Company, 1969.

[加藤 12] 加塩 朋和. 代数学 III. 2012. https://www.rs.tus.ac.jp/a25594/2012_Galois%20Theory.pdf.

[Mil21] J.S. Milne. Fields and Galois Theory (v5.00). 2021. https://www.jmilne.org/math/CourseNotes/FT.pdf.

[Stacks] The Stacks project authors. The Stacks project. -2022. https://stacks.math.columbia.edu/.

[nLab] nLab authors. nLab. -2022. https://ncatlab.org/nlab/show/HomePage.

[MSE] Mathematics Stack Exchange - What is $\gcd(0, a)$, where a is a positive integer?. -2022. https://math.stackexchange.com/questions/27719/what-is-gcd0-a-where-a-is-a-positive-integer

[Wiki] Wikipedia - 最大公約数. -2022. https://ja.wikipedia.org/wiki/%E6%9C%80%E5%A4%A7%E5%85%AC%E7%B4%84%E6%95%B0

[Rot12] J. Rotman. 関口次郎（訳). 改訂新版 ガロア理論. 丸善出版. 2012.

[alg-d] alg-d. 圏論―壱大整域. http://alg-d.com/math/kan_extension/.

[Akari] Akari. 群・環・体. 2021.