Dedekindの定理における因数分解のサイクル型とGalois群の置換の不分岐性を交えた詳細な解説

本稿では、代数的整数論と Galois理論を結びつける基本定理の一つである **Dedekindの定理 (Dedekind's theorem)** について解説します。 有限体上での多項式の因数分解の次数パターンから、元の多項式の Galois群 (Galois group) に含まれる置換のサイクル型 (cycle type) を決定できるというこの定理は、Galois群の具体的な計算において極めて強力な道具となります。

本稿は自己完結的 (self-contained) な記述を目指し、必要な基本概念の定義、具体的な理解を助ける例、および定理の背後にある「不分岐性と判別式の関係」の丁寧な証明を網羅しています。

※記号の約束：本稿においては、集合の包含関係を $\subset$ で表し、空集合を $\varnothing$、集合の差を $\setminus$ で表します。

1. 基本概念の定義

定理の証明および理解に必要となる代数体および代数的整数論の基本概念を定義します。以下の定義および数学的命題の記述は「だである調」で統一します。

定義 1 (多項式の判別式)

$f(x) \in \mathbb{Z}[x]$ を次数 n のモニック多項式 (monic polynomial) とし、その $\mathbb{C}$ における根を $\alpha_1, \alpha_2, \ldots, \alpha_n$ とする。$f(x)$ の判別式 (discriminant) $\Delta(f)$ は次のように定義される：

$$\Delta(f) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2$$

定義 2 (代数的整数環と素イデアルの分解)

代数体 E の代数的整数環 (ring of algebraic integers) を $\mathcal{O}_E$ とし、有理素数 p が生成するイデアル $p\mathcal{O}_E$ の相異なる素イデアル (prime ideal) への分解を

$$p\mathcal{O}_E = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_g^{e_g}$$

とする。このとき、各指数 $e_i \ge 1$ を $\mathfrak{P}_i$ における 分岐指数 (ramification index) と呼ぶ。

定義 3 (不分岐)

定義2の分解において、すべての $i = 1, \ldots, g$ に対して $e_i = 1$ であるとき、素数 p は拡大 $E/\mathbb{Q}$ において **不分岐 (unramified)** であるという。 すなわち、分岐する（$e_i > 1$ となる）素イデアルの集合が空集合 $\varnothing$ であることと同値である。

定義 4 (分解群と慣性群)

$E/\mathbb{Q}$ を Galois拡大とし、$G = \mathrm{Gal}(E/\mathbb{Q})$ とする。p の上にある $\mathcal{O}_E$ の素イデアル $\mathfrak{P}$ ひとつに対して、分解群 (decomposition group) $D_{\mathfrak{P}}$ および 慣性群 (inertia group) $I_{\mathfrak{P}}$ は次のように定義される部分群である：

$$D_{\mathfrak{P}} = \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

$$I_{\mathfrak{P}} = \{\sigma \in G \mid \forall \alpha \in \mathcal{O}_E,\ \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}}\}$$

また、G の元のうち分解群に属さない元の集合は、集合の差を用いて $G \setminus D_{\mathfrak{P}}$ と表される。

定義 5 (Frobenius元)

剰余体拡大 $(\mathcal{O}_E/\mathfrak{P})/(\mathbb{Z}/p\mathbb{Z})$ を考える（ここで $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$ である）。この有限体 (finite field) の拡大の Galois群は、$\bar{x} \mapsto \bar{x}^p$ で定義される Frobenius自己同型 (Frobenius automorphism) Frob_p によって生成される巡回群 (cyclic group) である。 自然な群準同型写像

$$\phi : D_{\mathfrak{P}} \to \mathrm{Gal}((\mathcal{O}_E/\mathfrak{P})/\mathbb{F}_p)$$

を考えると、その核は定義より慣性群 $I_{\mathfrak{P}}$ に一致する。p が不分岐のとき $I_{\mathfrak{P}} = \{\mathrm{id}\}$ となるため ϕ は同型写像 (group isomorphism) を与える。このとき、$\phi(\sigma) = \mathrm{Frob}_p$ を満たす一意な元 $\sigma \in D_{\mathfrak{P}} \subset G$ を **Frobenius元 (Frobenius element)** と呼ぶ。

2. 理解を助ける具体的な例

定理の証明に先立ち、具体的にどのように因数分解のサイクル型と Galois群の元が対応するかを観察します。

例 (3次多項式における検証)

モニック多項式 $f(x) = x^3 - x - 1 \in \mathbb{Z}[x]$ を考える。 この多項式の判別式は、公式 $\Delta(x^3 + ax + b) = -4a^3 - 27b^2$ より、$\Delta(f) = -4(-1)^3 - 27(-1)^2 = 4 - 27 = -23$ である。 $f(x)$ の $\mathbb{Q}$ 上の Galois群 G は 3次対称群 (symmetric group) S_3 であることが知られている。判別式を割り切らないいくつかの素数 p について、$\mathbb{F}_p$ 上での因数分解の次数パターンを調べる。

(1) $p = 2$ の場合

$2 \nmid -23$ である。$f(x) \equiv x^3 + x + 1 \pmod{2}$ は $\mathbb{F}_2$ 上で根を持たない（$0^3 + 0 + 1 = 1, 1^3 + 1 + 1 = 1$）ため、3次の既約因子 (irreducible factor) そのものである。 したがって、既約因子の次数パターンは (3) である。Dedekindの定理が主張するのは、G にサイクル型 (3) の置換、すなわち長さ 3 の 巡回置換 (cyclic permutation) が含まれることである。実際に S_3 は 巡回置換 $(1\ 2\ 3)$ や $(1\ 3\ 2)$ を含んでいる。

(2) $p = 5$ の場合

$5 \nmid -23$ である。$f(x) \equiv x^3 - x - 1 \pmod{5}$ において、$x = 2$ を代入すると $2^3 - 2 - 1 = 5 \equiv 0 \pmod{5}$ となるため、$x - 2$ を因子に持つ。 多項式の除算を行うと、$\mathbb{F}_5[x]$ 上で次のように因数分解される：

$$f(x) \equiv (x-2)(x^2+2x+3) \pmod{5}$$

x^2+2x+3 は $\mathbb{F}_5$ 上に根を持たないため既約である。したがって、既約因子の次数パターンは $(1,2)$ である。Dedekindの定理より、G はサイクル型 $(1,2)$ の置換、すなわち互換を含む。実際に S_3 は $(1\ 2), (2\ 3), (1\ 3)$ という互換を含んでいる。

3. 不分岐性と判別式の関係

Dedekindの定理の前提となる、「判別式を割り切らない素数は不分岐である」という代数的整数論の重要命題の証明を与えます。

命題 1

$f(x) \in \mathbb{Z}[x]$ をモニック多項式とし、E をその $\mathbb{Q}$ 上の最小分解体とする。有理素数 p が $f(x)$ の判別式 $\Delta(f)$ を割り切らないならば、p は拡大 $E/\mathbb{Q}$ において不分岐である。

証明

本命題の対偶である「p が $E/\mathbb{Q}$ で分岐するならば、$p \mid \Delta(f)$ である」を証明する。

p が $E/\mathbb{Q}$ で分岐すると仮定する。このとき、定義2における分解において、少なくとも1つの素イデアルに対して分岐指数が $e_i > 1$ となる。そのような p の上にある素イデアルの1つを $\mathfrak{P}$ とおく。 代数的整数論の基本定理より、慣性群 $I_{\mathfrak{P}}$ の位数は分岐指数 e に等しい。今 $e > 1$ であるから、慣性群 $I_{\mathfrak{P}}$ は恒等写像ではない元 $\sigma \neq \mathrm{id}$ を含む。

E は $f(x)$ のすべての根 $\alpha_1, \alpha_2, \ldots, \alpha_n$ によって $\mathbb{Q}$ 上生成される最小分解体である。σ は恒等写像ではないため、すべての根を固定することはできない。したがって、ある相異なるインデックス $i \neq j$ が存在して、

$$\sigma(\alpha_i) = \alpha_j$$

を満たす。

一方で、σ は慣性群 $I_{\mathfrak{P}}$ の元であるため、慣性群の定義（定義4）より、任意の代数的整数に対して $\mathfrak{P}$ を法とする合同式において作用が不変である。根 α_i は $f(x)$ がモニック多項式であることから $\mathcal{O}_E$ の元であり、代数的整数である。ゆえに、

$$\sigma(\alpha_i) \equiv \alpha_i \pmod{\mathfrak{P}}$$

が成り立つ。これに $\sigma(\alpha_i) = \alpha_j$ を代入すると、

$$\alpha_j \equiv \alpha_i \pmod{\mathfrak{P}} \quad \Longrightarrow \quad \alpha_i - \alpha_j \in \mathfrak{P}$$

を得る。

多項式 $f(x)$ の判別式 $\Delta(f)$ は、根を用いて

$$\Delta(f) = \prod_{1 \leq k < l \leq n} (\alpha_k - \alpha_l)^2$$

と表される。この積の因子には、インデックスの順序を適切に選ぶことで $(\alpha_i - \alpha_j)^2$ が必ず含まれる。$\alpha_i - \alpha_j \in \mathfrak{P}$ であるから、その自乗も $\mathfrak{P}$ に属し、それを含む全体の積である判別式もまた $\mathfrak{P}$ に属する。すなわち、

$$\Delta(f) \in \mathfrak{P}$$

である。

ここで、$\Delta(f)$ は整数係数多項式の判別式であるから、有理整数環 (ring of rational integers) $\mathbb{Z}$ の元である。したがって、

$$\Delta(f) \in \mathfrak{P} \cap \mathbb{Z}$$

が成り立つ。素イデアル $\mathfrak{P}$ は p の上にあることから、$\mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$ である。ゆえに、

$$\Delta(f) \in p\mathbb{Z}$$

となり、これは p が $\Delta(f)$ を割り切ること（$p \mid \Delta(f)$）を意味する。

対偶が示されたため、元の命題も真である。 (Q.E.D.)

4. Dedekind の定理の証明

以上の準備のもとで、Dedekindの定理を直接的かつ自己完結的に証明します。

> **定理 1 (Dedekind の定理)**
>
> $f(x) \in \mathbb{Z}[x]$ をモニック多項式とする。判別式を割り切らない素数 p を法として $f(x)$ を有限体 $\mathbb{F}_p$ 上で因数分解したとき、その既約因子の次数が $(n_1, n_2, \ldots, n_k)$ であれば、$f(x)$ の Galois群はサイクル型が $(n_1, n_2, \ldots, n_k)$ である置換を含む。

証明

E を $f(x)$ の $\mathbb{Q}$ 上の最小分解体とし、$G = \mathrm{Gal}(E/\mathbb{Q})$ をその Galois群とする。$f(x)$ の E における相異なる根を $\alpha_1, \alpha_2, \ldots, \alpha_n$ とする。 $\mathcal{O}_E$ を E の代数的整数環とし、p の上にある $\mathcal{O}_E$ の素イデアルの1つを $\mathfrak{P}$ とする。

仮定より $p \nmid \Delta(f)$ であるため、命題1により p は拡大 $E/\mathbb{Q}$ において不分岐である。したがって、慣性群 $I_{\mathfrak{P}}$ は自明な群 $\{\mathrm{id}\}$ である。

自然な還元準同型写像 $\pi : \mathcal{O}_E \to \mathcal{O}_E/\mathfrak{P}$ を考え、要素 $a \in \mathcal{O}_E$ の像を $\bar{a}$ と表す。 $f(x)$ の根の集合 $R = \{\alpha_1, \ldots, \alpha_n\}$ に対する π の制限写像 $\pi|_R : R \to \mathcal{O}_E/\mathfrak{P}$ は単射 (injection) である。なぜなら、もし $i \neq j$ に対して $\bar{\alpha}_i = \bar{\alpha}_j$ と仮定すると、$\alpha_i - \alpha_j \in \mathfrak{P}$ となり、前節の議論から $p \mid \Delta(f)$ を導いてしまい矛盾

するからである。 さらに、各 $\bar{\alpha}_i$ は $\mathbb{F}_p$ 上の多項式 $\bar{f}(x) = f(x) \bmod p$ の根であり、$\bar{f}(x)$ の次数も n であるため、$\pi|_R$ は $f(x)$ の根の集合から $\bar{f}(x)$ の根の集合への 全単射 (bijection) を与える。

次に、分解群 $D_{\mathfrak{P}}$ を考える。各 $\sigma \in D_{\mathfrak{P}}$ は、剰余体 $\mathcal{O}_E/\mathfrak{P}$ 上の自己同型 $\bar{\sigma}$ を次のように引き起こす：

$$\bar{\sigma}(\bar{\alpha}) = \overline{\sigma(\alpha)} \quad (\alpha \in \mathcal{O}_E)$$

これにより自然な群準同型写像 $\phi : D_{\mathfrak{P}} \to \mathrm{Gal}((\mathcal{O}_E/\mathfrak{P})/\mathbb{F}_p)$ が定まる。代数的整数論の一般論（参考文献 [2] を参照）により ϕ は全射 (surjection) である。また、今 p は不分岐であるから、ϕ の核である慣性群 $I_{\mathfrak{P}}$ は自明である。ゆえに ϕ は群同型写像である。

有限体の Galois理論より、群 $\mathrm{Gal}((\mathcal{O}_E/\mathfrak{P})/\mathbb{F}_p)$ は Frobenius自己同型 $\mathrm{Frob}_p : x \mapsto x^p$ によって生成される巡回群である。ϕ が同型であることから、$\phi(\sigma) = \mathrm{Frob}_p$ を満たす元 $\sigma \in D_{\mathfrak{P}} \subset G$ が一意に存在する。

ここで、$\bar{f}(x)$ の $\mathbb{F}_p$ 上での既約分解を

$$\bar{f}(x) = \bar{f}_1(x)\bar{f}_2(x)\dots\bar{f}_k(x)$$

とし、各既約因子 $\bar{f}_j(x)$ の次数を n_j とする。有限体上の既約多項式の根は、Frobenius自己同型 Frob_p の作用によって巡回的に置換され、長さ n_j の巡回軌道をなす（参考文献 [3] を参照）。各既約因子は互いに素であるため、Frob_p が $\bar{f}(x)$ の根全体に引き起こす置換のサイクル型は $(n_1, n_2, \dots, n_k)$ となる。

同型写像 ϕ の定義より、任意の根 $\alpha_i \in R$ に対して以下が成り立つ：

$$\sigma(\alpha_i) = \bar{\sigma}(\bar{\alpha}_i) = \mathrm{Frob}_p(\bar{\alpha}_i)$$

還元写像 $\pi|_R : \alpha_i \mapsto \bar{\alpha}_i$ は全単射であり、上の関係式はこの全単射写像によって G の元 σ の作用と Frob_p の作用が完全に一致することを示している。 したがって、σ が元の根 $\alpha_1, \dots, \alpha_n$ に引き起こす置換のサイクル型は、Frob_p のサイクル型、すなわち $(n_1, n_2, \dots, n_k)$ と完全に一致する。

以上より、Galois群 G はサイクル型 $(n_1, n_2, \dots, n_k)$ を持つ置換 σ を含む。 (Q.E.D.)

5. 参考文献

本稿の執筆にあたり参照した、および関連する正確な情報を含む文献のリストを以下に示します。

- [1] Conrad, K., *Galois groups over ℚ and factorizations mod p*, Explanatory Notes, University of Connecticut. Available at: https://kconrad.math.uconn.edu/blurbs/gradnumthy/galois-Q-factor-mod-p.pdf
- [2] Milne, J. S., *Fields and Galois Theory* (v5.10), 2026. Available at: https://www.jmilne.org/math/CourseNotes/FT.pdf
- [3] Neukirch, J., *Algebraic Number Theory*, Grundlehren der mathematischen Wissenschaften, Vol. 322, Springer-Verlag, Berlin, 1999. Available at: https://link.springer.com/book/10.1007/978-3-662-03983-0