本稿では、代数的整数論における「円分体での不分岐な有理素数の分解」について解説します。環の自然な同型関係（$\mathbb{Z}[\zeta_n]/(p) \cong \mathbb{F}_p[x]/(\overline{\Phi}_n(x))$）を用いることで、代数体における素イデアルの分解という一見複雑な現象が、有限体上の多項式の因数分解へと鮮やかに帰着される様子を、自己完結的（self-contained）に証明します。

円分体における不分岐な有理素数の分解：環の同型対応によるアプローチ

1. 基本概念の準備

1の原始 n 乗根 (primitive n-th root of unity) と円分体 (cyclotomic field)

n を正の整数とする。複素数 $\zeta_n = e^{2\pi i/n}$ を1の原始 n 乗根という。有理数体 $\mathbb{Q}$ に ζ_n を添加して得られる拡大体 $K = \mathbb{Q}(\zeta_n)$ を円分体 (cyclotomic field) と呼ぶ。

円分体 K の整数環 (ring of integers) $\mathcal{O}_K$ は $\mathbb{Z}[\zeta_n]$ に完全に一致することが知られている。この環はDedekind整域 (Dedekind domain) であり、任意のゼロでないイデアルは素イデアルの積として一意に分解される。

円分多項式 (cyclotomic polynomial)

円分多項式 $\Phi_n(x)$ は、1の原始 n 乗根すべてを根に持つ最高次係数が1の多項式であり、有理数体 $\mathbb{Q}$ 上で既約 (irreducible) な整数係数多項式である。その次数は Euler のトーティエント関数 $\varphi(n)$ に等しい。ζ_n は $\Phi_n(x)$ の根であるため、代数的な関係式として環の同型 $\mathbb{Z}[\zeta_n] \cong \mathbb{Z}[x]/(\Phi_n(x))$ が成り立つ。

2. 定理の主張

定理：円分体における素数の分解

p を素数、n を p で割り切れない ($p \nmid n$) 正の整数とする。乗法群 $(\mathbb{Z}/n\mathbb{Z})^\times$ における p の位数 (order) を f とする。すなわち、$p^f \equiv 1 \pmod{n}$ を満たす最小の正の整数が f である。また、$g = \varphi(n)/f$ とおく。

このとき、以下の関係が成り立つ。

1. $\Phi_n(x)$ **の** $\bmod p$ **での分解：**
   n 次の円分多項式 $\Phi_n(x)$ は有限体 $\mathbb{F}_p$ 上で、次数がすべて f である相異なる g 個の既約多項式の積に分解される。

$$\Phi_n(x) \equiv P_1(x)P_2(x)\cdots P_g(x) \pmod{p}$$

2. p **の** $\mathbb{Z}[\zeta_n]$ **での分解：**
   円分体の整数環 $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$ において、有理素数 (p) は相対次数がすべて f である相異なる g 個の素イデアルの積に完全に分解される。

$$(p) = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_g$$

   ここで、各素イデアルは $\mathfrak{p}_i = (p, P_i(\zeta_n))$ で与えられる。

3. 同型対応を用いた簡素な証明

証明：

Step 1: 剰余環の自然な同型対応

円分体の整数環 $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$ は、多項式環の剰余環 $\mathbb{Z}[x]/(\Phi_n(x))$ と同型である。イデアル (p) による剰余環 $\mathcal{O}_K/(p)$ を考えると、準同型定理により以下の自然な同型関係の連鎖が得られる。

$$\mathcal{O}_K/(p) \cong \mathbb{Z}[\zeta_n]/(p) \cong \mathbb{Z}[x]/(\Phi_n(x), p) \cong \mathbb{F}_p[x]/(\overline{\Phi}_n(x))$$

ここで $\overline{\Phi}_n(x)$ は $\Phi_n(x)$ を法 p で還元した有限体 $\mathbb{F}_p$ 上の多項式である。この美しい同型関係により、左辺の「イデアルの構造」が、右辺の「有限体上の多項式の分解」に完全に翻訳される。

Step 2: 中国剰余定理 (Chinese remainder theorem) による直和分解

仮定より $p \nmid n$ であるため、多項式 $x^n - 1$ の導関数 nx^{n-1} は $\mathbb{F}_p$ 上で恒等的に 0 ではなく、$x^n - 1$ と共通根を持たない。ゆえにその約数である $\overline{\Phi}_n(x)$ も $\mathbb{F}_p$ 上で重根を持たず、相異なる既約多項式の積に一意に分解される。

$$\overline{\Phi}_n(x) = \overline{P}_1(x)\overline{P}_2(x)\cdots\overline{P}_g(x)$$

ここで、環に対する中国剰余定理 (Chinese remainder theorem) を右辺 $\mathbb{F}_p[x]/(\overline{\Phi}_n(x))$ に適用すると、互いに素なイデアルによる剰余環の直和に分解される。

$$\mathbb{F}_p[x]/(\overline{\Phi}_n(x)) \cong \bigoplus_{i=1}^{g} \mathbb{F}_p[x]/(\overline{P}_i(x))$$

各 $\overline{P}_i(x)$ は既約多項式であるため、それぞれの直和成分 $\mathbb{F}_p[x]/(\overline{P}_i(x))$ は有限体となる。

Step 3: 素イデアル分解の決定

一方、Dedekind整域 $\mathcal{O}_K$ において、イデアル (p) が素イデアルの積 $(p) = \mathfrak{p}_1^{e1} \cdots \mathfrak{p}_k^{ek}$ に分解されたとする。同様に中国剰余定理を左辺 $\mathcal{O}_K/(p)$ に適用すると、

$$\mathcal{O}_K/(p) \cong \bigoplus_{j=1}^{k} \mathcal{O}_K/\mathfrak{p}_j^{e_j}$$

となる。Step 1 で示した同型により、この2つの直和分解は環として完全に一致しなければならない。右辺が「体の直和」であることから、左辺の各成分も体でなければならず、すべての分岐指数は $e_j = 1$ となる（無分岐 (unramified)）。さらに、直和成分の個数も一致するため $k = g$ である。

対応関係から、各素イデアル $\mathfrak{p}_i$ の剰余体 $\mathcal{O}_K/\mathfrak{p}_i$ は、$\mathbb{F}_p[x]/(\overline{P}_i(x))$ と同型になる。これにより、素イデアル $\mathfrak{p}_i$ は多項式 $P_i(x)$ を用いて $\mathfrak{p}_i = (p, P_i(\zeta_n))$ と表され、その相対次数 $f_i = [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{F}_p]$ は、まさに既約多項式 $\overline{P}_i(x)$ の次数に等しいことがわかる。

Step 4: 既約多項式の次数と位数の関係

最後に、各 $\overline{P}_i(x)$ の次数が f になることを示す。$\overline{P}_i(x)$ の根を α とし、その次数を d とすると、α は $\mathbb{F}_p$ の d 次拡大体 $\mathbb{F}_{p^d}$ を生成する。α は $\overline{\Phi}_n(x)$ の根でもあるため、$\mathbb{F}_{p^d}$ において1の原始 n 乗根として振る舞い、その乗法群における位数は n である。

有限体 $\mathbb{F}_{p^d}$ の乗法群の位数は $p^d - 1$ であるから、Lagrangeの定理より $n \mid (p^d - 1)$、すなわち $p^d \equiv 1 \pmod{n}$ が成り立つ。α がより小さな部分体に属さないため、d はこの合同式を満たす最小の正の整数、すなわち群 $(\mathbb{Z}/n\mathbb{Z})^\times$ における p の位数 f と完全に一致する。

したがって、すべての既約多項式の次数（および素イデアルの相対次数）は f であり、全体の次数が $\varphi(n)$ であることから、その個数は $g = \varphi(n)/f$ となる。(証明終)

4. 具体的な計算例

定理の具体的な振る舞いを観察するための計算例を示す。同型対応からわかる通り、イデアルの相対次数と多項式の次数が完全に連動している。

例	p	n	$\varphi(n)$	f (位数 / 相対次数)	g (個数)	分解のタイプ
1	2	3	2	2	1	惰性 (inertia)
2	3	4	2	2	1	惰性 (inertia)
3	5	4	2	1	2	完全分解 (completely split)
4	13	3	2	1	2	完全分解 (completely split)
5	2	5	4	4	1	惰性 (inertia)
6	11	5	4	1	4	完全分解 (completely split)

7	2	7	6	3	2	部分分解 (partially split)
8	3	8	4	2	2	部分分解 (partially split)
9	5	8	4	2	2	部分分解 (partially split)
10	7	12	4	2	2	部分分解 (partially split)

具体的な分解の計算

以下に、各例における $\bmod p$ での $\Phi_n(x)$ の分解と、$\mathbb{Z}[\zeta_n]$ における (p) の素イデアル分解が対応している様子を示す。

例3: $p=5, n=4$ **(完全分解)**

- 位数: $5^1 \equiv 1 \pmod 4$ より $f=1, g=2$。
- 多項式: $\Phi_4(x) = x^2+1 \equiv x^2-4 \equiv (x-2)(x-3) \pmod 5$。
- イデアル: $(5) = (5, \zeta_4 - 2)(5, \zeta_4 - 3)$ （2つの相対次数1の素イデアルに完全分解する）。

例6: $p=11, n=5$ **(完全分解)**

- 位数: $11^1 \equiv 1 \pmod 5$ より $f=1, g=4$。
- 多項式: $\Phi_5(x) = x^4+x^3+x^2+x+1 \equiv (x-3)(x-4)(x-5)(x-9) \pmod{11}$。
- イデアル: $(11) = (11, \zeta_5 - 3)(11, \zeta_5 - 4)(11, \zeta_5 - 5)(11, \zeta_5 - 9)$。

例7: $p=2, n=7$ **(部分分解)**

- 位数: $2^3 \equiv 1 \pmod 7$ より $f=3, g=2$。
- 多項式: $\Phi_7(x) = x^6+x^5+x^4+x^3+x^2+x+1 \equiv (x^3+x+1)(x^3+x^2+1) \pmod 2$。
- イデアル: $(2) = (2, \zeta_7^3 + \zeta_7 + 1)(2, \zeta_7^3 + \zeta_7^2 + 1)$ （2つの相対次数3の素イデアルに部分分解する）。

例10: $p=7, n=12$ **(部分分解)**

- 位数: $7^2 \equiv 1 \pmod{12}$ より $f=2, g=2$。
- 多項式: $\Phi_{12}(x) = x^4 - x^2 + 1 \equiv (x^2+2)(x^2+4) \pmod 7$。
- イデアル: $(7) = (7, \zeta_{12}^2 + 2)(7, \zeta_{12}^2 + 4)$。

参考文献

- Neukirch, J. (1999). *Algebraic Number Theory*. Springer-Verlag. https://link.springer.com/book/10.1007/978-3-662-03983-0
- Washington, L. C. (1997). *Introduction to Cyclotomic Fields* (2nd ed.). Springer-Verlag. https://link.springer.com/book/10.1007/978-1-4612-1934-7