代数体の整数環と24次円分体における素数分解および円分単数の構造

本稿では、24次円分体 (cyclotomic field) における整数環 (ring of integers) の生成元に関する考察、素数のイデアル分解の法則、および単数群における「円分単数 (cyclotomic unit)」の具体的な構造について、自己完結的 (self-contained) に解説します。抽象的な代数学の理論が、具体的な代数的数の計算においてどのように美しい調和を見せるのかを確認していきましょう。

1. 代数体と整数環の基礎知識

まず、議論の前提となる基本概念を厳密に定義しておきます。数論において、有理数体に適当な数を添加してできる体を考え、その中で「整数」に相当する要素を集めた環を考えることは極めて重要です。

定義 (代数体と整数環)

有理数体 $\mathbb{Q}$ の有限次代数拡大体 K を**代数体 (algebraic number field)** と呼ぶ。複素数 $\alpha \in \mathbb{C}$ が最高次係数が 1 であるモニックな整係数多項式の根となるとき、α を**代数的整数 (algebraic integer)** と呼ぶ。代数体 K に属する代数的整数の全体は環をなし、これを K の**整数環 (ring of integers)** と呼び $\mathcal{O}_K$ と表記する。
なお、$\mathcal{O}_K$ は $\mathbb{Z}$ を含むが、一般の代数体では分母に整数が現れる代数的整数も存在する点に注意が必要である。

定義 (円分体)

n を正の整数とし、$\zeta_n = e^{2\pi\sqrt{-1}/n}$ を 1 の原始 n 乗根とする。$\mathbb{Q}$ に ζ_n を添加した体 $\mathbb{Q}(\zeta_n)$ を n 次**円分体 (cyclotomic field)** と呼ぶ。円分体の整数環は $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$ となることが知られている。

2. $\mathbb{Q}(\sqrt{-1}, \sqrt{-2}, \sqrt{-3})$ の整数環の決定

$\sqrt{-1}, \sqrt{-2}, \sqrt{-3}$ という3つの虚数の平方根で生成される体について、その整数環がどのように記述されるかを見ていきましょう。単純に元の環の生成元を並べた $\mathbb{Z}[\sqrt{-1}, \sqrt{-2}, \sqrt{-3}]$ は、真の整数環よりも真に小さい環（部分環）になってしまいます。

命題 1

合成体 $K = \mathbb{Q}(\sqrt{-1}, \sqrt{-2}, \sqrt{-3})$ は 24次円分体 $\mathbb{Q}(\zeta_{24})$ と一致する。したがって、その整数環 $\mathcal{O}_K$ は以下のように記述される。

$$\mathcal{O}_{\mathbb{Q}(\sqrt{-1},\sqrt{-2},\sqrt{-3})} = \mathbb{Z}[\zeta_{24}]$$

証明

まず、各平方根がどの円分体に属するかを明らかにする。
1. $\sqrt{-1}$ は 1 の原始4乗根 ζ_4 そのものである。すなわち $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(\zeta_4)$。

2. $\mathbb{Q}(\sqrt{-3})$ は3次円分体 $\mathbb{Q}(\zeta_3)$ と一致する。実際、$\zeta_3 = \frac{-1+\sqrt{-3}}{2}$ であり、$\sqrt{-3} = 2\zeta_3 + 1$ が成り立つ。
3. $\sqrt{-2} = \sqrt{2}\sqrt{-1}$ であるから、$\mathbb{Q}(\sqrt{-1}, \sqrt{-2}) = \mathbb{Q}(\sqrt{-1}, \sqrt{2})$ となる。8次円分体について $\zeta_8 = \frac{\sqrt{2}+\sqrt{-2}}{2}$ であり、これより $\mathbb{Q}(\zeta_8) = \mathbb{Q}(\sqrt{-1}, \sqrt{2})$ である。
したがって、$\mathbb{Q}(\sqrt{-1}, \sqrt{-2}, \sqrt{-3})$ は $\mathbb{Q}(\zeta_4), \mathbb{Q}(\zeta_8), \mathbb{Q}(\zeta_3)$ の合成体となる。
$\mathbb{Q}(\zeta_4) \subset \mathbb{Q}(\zeta_8)$ であるため、この合成体は $\mathbb{Q}(\zeta_8)$ と $\mathbb{Q}(\zeta_3)$ の合成体である。円分体の性質から、互いに素な n, m について $\mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{nm})$ となるため、

$$\mathbb{Q}(\zeta_8)\mathbb{Q}(\zeta_3) = \mathbb{Q}(\zeta_{24})$$

が得られる。円分体 $\mathbb{Q}(\zeta_{24})$ の整数環は $\mathbb{Z}[\zeta_{24}]$ であるため、命題は示された。（証明終）

もし $\mathbb{Z}[\dots] = \mathbb{Z}[\zeta_{24}]$ という「要素を追加して環を生成する形」を維持したいのであれば、左辺に「分母を持った代数的整数」を追加する必要があります。次の命題がその答えです。

命題 2 (生成元による等式の訂正)

以下の環としての等式が成り立つ。

$$\mathbb{Z}\left[\sqrt{-1}, \frac{\sqrt{2}+\sqrt{-2}}{2}, \frac{-1+\sqrt{-3}}{2}\right] = \mathbb{Z}[\zeta_{24}]$$

証明

元の環 $\mathbb{Z}[\sqrt{-1}, \sqrt{-2}, \sqrt{-3}]$ が真の整数環とならない理由は、$1/2$ や $1/\sqrt{2}$ などの分母を持つ代数的整数が欠落しているためである。例えば $\mathbb{Q}(\sqrt{-3})$ の整数環は、判別式が $-3 \equiv 1 \pmod 4$ であることから $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$ となる。
左辺の生成元を観察すると：
・$\sqrt{-1} = \zeta_4$
・$\frac{\sqrt{2}+\sqrt{-2}}{2} = \zeta_8$
・$\frac{-1+\sqrt{-3}}{2} = \zeta_3$
これらは各部分体の整数環の真の生成元である。ζ_8 と ζ_3 から ζ_{24} を構成できる（例えばベズーの等式より $3 \cdot 3 - 1 \cdot 8 = 1$ を用いて $\zeta_{24} = \zeta_{24}^{9-8} = \zeta_8^3\zeta_3^{-1}$）ため、左辺が生成する環は $\mathbb{Z}[\zeta_{24}]$ に一致する。（証明終）

3. 24次円分体における円分単数の具体形

次に、整数環 $\mathbb{Z}[\zeta_{24}]$ の可逆元である「単数」について考えます。特に、1 の冪根の差の商として定義される「円分単数」は、代数的な計算において極めて重要な役割を果たします。

定義 (円分単数)

a を 24 と互いに素な整数とする。$\zeta = \zeta_{24}$ とおくとき、

$$u_a = \frac{\zeta^a - 1}{\zeta - 1}$$

で定義される元 u_a を**円分単数 (cyclotomic unit)** と呼ぶ。これらは $\mathcal{O}_{\mathbb{Q}(\zeta_{24})}$ の単数群 (unit group) の部分群を生成す

る。

命題 3 (多項式基底による簡約形)

$\mathbb{Z}[\zeta_{24}]$ は $\mathbb{Z}$ 上ランク8の自由加群であり、その標準的な基底は $\{1, \zeta, \zeta^2, \dots, \zeta^7\}$ である。この基底を用いて u_5, u_7, u_{11} を表現すると以下のようになる。
・$u_5 = 1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4$
・$u_7 = 1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6$
・$u_{11} = \zeta^3 + 2\zeta^4 + 2\zeta^5 + 2\zeta^6 + \zeta^7$

証明

24 次円分多項式は $\Phi_{24}(x) = x^8 - x^4 + 1$ である。ζ はこの根であるから、$\zeta^8 = \zeta^4 - 1$ が成り立つ。
等比数列の和の公式から、$u_a = 1 + \zeta + \cdots + \zeta^{a-1}$ である。
$a = 5, 7$ のときは次数が 7 以下であるため、そのままで基底による表現となっている。
$a = 11$ のとき、

$$u_{11} = 1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6 + \zeta^7 + \zeta^8 + \zeta^9 + \zeta^{10}$$

ここで関係式を用いて次数を下げる。
・$\zeta^8 = \zeta^4 - 1$
・$\zeta^9 = \zeta \cdot \zeta^8 = \zeta^5 - \zeta$
・$\zeta^{10} = \zeta^2 \cdot \zeta^8 = \zeta^6 - \zeta^2$
これらを代入して整理する。

$$u_{11} = (1 - 1) + (\zeta - \zeta) + (\zeta^2 - \zeta^2) + \zeta^3 + (1 + 1)\zeta^4 + (1 + 1)\zeta^5 + (1 + 1)\zeta^6 + \zeta^7$$

$$u_{11} = \zeta^3 + 2\zeta^4 + 2\zeta^5 + 2\zeta^6 + \zeta^7$$

となり、簡約形が得られる。（証明終）

4. $\mathbb{Z}[\zeta_{24}]$ における素数の分解法則

ここでは、有理素数（通常の素数）が $\mathbb{Z}[\zeta_{24}]$ においてどのように因数分解されるかについて解説します。驚くべきことに、24次円分体においては「そのまま素数であり続ける（惰性する）」ような有理素数は一つも存在しません。

命題 4 (有理素数の分解)

任意の素数 p は $\mathbb{Z}[\zeta_{24}]$ において2つ以上の素元 (prime element) の積に分解される。すなわち、$\mathbb{Z}[\zeta_{24}]$ において惰性 (inert) する有理素数は存在しない。

証明

有理素数 p の代数体 $K = \mathbb{Q}(\zeta_{24})$ における素イデアル分解を考える。K の拡大次数は $\phi(24) = 8$ である。
よく知られているように、円分体 $\mathbb{Q}(\zeta_{24})$ の類数 (class number) は 1 である。したがってその整数環 $\mathbb{Z}[\zeta_{24}]$ は単項イ

デアル整域 (principal ideal domain) であり、任意の素イデアルは単項イデアルとしてある素元によって生成される。すなわち、イデアルの分解は直ちに元の因数分解に対応する。
素数 p が生成するイデアル (p) が $(p) = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}$ と分解されるとき、$K/\mathbb{Q}$ はガロア拡大 (Galois extension) であるため、分岐指数 (ramification index) は全て等しく $e_i = e$ であり、惰性次数 (inertial degree) も全て等しく $f_i = f$ となる。さらに基本公式 $efg = 8$ が成り立つ。素元への分解における因子数（重複度を含む）は $\sum e_i = e \cdot g$ となる。

ケース 1: $p \neq 2, 3$ の場合 (不分岐の素数)
p は 24 と互いに素であるため、不分岐 (unramified) であり $e = 1$ である。惰性次数 f は、乗法群 $(\mathbb{Z}/24\mathbb{Z})^\times$ における p の位数に等しい。
ここで、$(\mathbb{Z}/24\mathbb{Z})^\times = \{1, 5, 7, 11, 13, 17, 19, 23\}$ であるが、これらはすべて2乗すると $1 \pmod{24}$ となる（例えば $5^2 = 25 \equiv 1$、$7^2 = 49 \equiv 1$ など）。すなわち、群の任意の要素の位数は最大でも 2 である。
したがって $f \leq 2$ となる。$efg = 8$ より、$g = 8/f \geq 4$ を得る。すなわち、イデアル (p) は少なくとも4つの相異なる素イデアルの積に分解されるため、p 自身は少なくとも4つの素元の積に分解される。

ケース 2: $p = 2$ の場合
$24 = 2^3 \cdot 3$ である。$p = 2$ の分岐指数 e は $\mathbb{Q}(\zeta_8)$ における分岐指数に等しく、$e = \phi(8) = 4$ である。惰性次数 f は $2 \pmod{3}$ の位数であり $f = 2$ である。$efg = 8$ より $g = 1$ となる。
したがって $(2) = \mathfrak{p}^4$ となり、対応する素元 π を用いて $2 = u\pi^4$（u は単数）と表される。これは4つの素元の積（重複度を含む）への分解である。

ケース 3: $p = 3$ の場合
$p = 3$ の分岐指数 e は $\mathbb{Q}(\zeta_3)$ の分岐指数に等しく $e = \phi(3) = 2$ である。惰性次数 f は $3 \pmod{8}$ の位数であり、$3^2 = 9 \equiv 1 \pmod{8}$ より $f = 2$ である。$efg = 8$ より $g = 2$ となる。
したがって $(3) = \mathfrak{q}_1^2\mathfrak{q}_2^2$ となり、同様に4つの素元の積に分解される。

以上より、すべての有理素数 p は $\mathbb{Z}[\zeta_{24}]$ において少なくとも4つの素元の積（重複度を含む）として表される。したがって「2つ以上の素元の積に分解される」という主張は真である。（証明終）

5. 対称形と実単数への分離

円分単数の美しい性質として、「ねじれ部分（1 の冪根）」と「自由部分（実数となる単数）」に分離できる点が挙げられます。これにより、幾何学的（三角関数）な表現が可能になります。

命題 5 (対称形・実単数による表現)

円分単数 u_a は、最大実部分体 $\mathbb{Q}(\zeta_{24})^+ = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ に属する実単数を用いて以下のように表現できる。

$$u_a = \zeta^{(a-1)/2} \frac{\sin\left(\frac{a\pi}{24}\right)}{\sin\left(\frac{\pi}{24}\right)}$$

証明

$u_a = \frac{\zeta^a - 1}{\zeta - 1}$ について、分子分母からそれぞれ半角の冪をくくり出す。

$$u_a = \frac{\zeta^{a/2}(\zeta^{a/2} - \zeta^{-a/2})}{\zeta^{1/2}(\zeta^{1/2} - \zeta^{-1/2})} = \zeta^{(a-1)/2} \frac{\zeta^{a/2} - \zeta^{-a/2}}{\zeta^{1/2} - \zeta^{-1/2}}$$

オイラーの公式 $\zeta^k - \zeta^{-k} = 2\sqrt{-1}\sin(2\pi k/24)$ を適用することで、

$$\frac{\zeta^{a/2} - \zeta^{-a/2}}{\zeta^{1/2} - \zeta^{-1/2}} = \frac{2\sqrt{-1}\sin\left(\frac{a\pi}{24}\right)}{2\sqrt{-1}\sin\left(\frac{\pi}{24}\right)} = \frac{\sin\left(\frac{a\pi}{24}\right)}{\sin\left(\frac{\pi}{24}\right)}$$

となる。この値は $\mathbb{Q}(\zeta_{24})$ の実数部分に含まれるため $\mathbb{Q}(\zeta_{24})^+$ の単数である。（証明終）

この結果を用いると、各 u_a の具体的な平方根（根号）による表現を展開形および因数分解形で計算することができます。因数分解形は単数群の構造を見事に反映しています。

命題 6 (平方根による展開形と因数分解形)

u_5, u_7, u_{11} は次のように展開、および因数分解される。

[展開形]

・$u_5 = \frac{6+3\sqrt{2}+2\sqrt{3}+\sqrt{6}}{4} + \frac{2\sqrt{-1}+\sqrt{-2}+2\sqrt{-3}+\sqrt{-6}}{4}$
・$u_7 = \frac{3+\sqrt{2}+\sqrt{3}+\sqrt{6}}{2} + \frac{3\sqrt{-1}+\sqrt{-2}+\sqrt{-3}+\sqrt{-6}}{2}$
・$u_{11} = \frac{4+\sqrt{2}+\sqrt{6}}{4} + \frac{8\sqrt{-1}+5\sqrt{-2}+4\sqrt{-3}+3\sqrt{-6}}{4}$

[因数分解形]

・$u_5 = \frac{(\sqrt{3}+\sqrt{-1})(1+\sqrt{3})(2+\sqrt{2})}{4}$
・$u_7 = \frac{(1+\sqrt{-1})(1+\sqrt{3})(\sqrt{2}+\sqrt{3})}{2}$
・$u_{11} = \frac{(\sqrt{3}+\sqrt{-1})(\sqrt{2}+\sqrt{-2})(1+\sqrt{2})(\sqrt{2}+\sqrt{3})}{4}$

6. 基本単数による表現の美しさ

最後に、因数分解形に現れた実数部分を、部分体の「基本単数」を用いて書き換えます。Dirichletの単数定理から、単数群のランク（自由度）が決定されますが、これらの基本単数が上位の体でどのように振る舞うかが極めて重要です。

定義 (基本単数)

実二次体 $\mathbb{Q}(\sqrt{d})$ の整数環における単数群は、± 1 と一つの単数 $\epsilon > 1$ （およびその冪）で生成される。この ϵ を**基本単数 (fundamental unit)** と呼ぶ。
本稿で扱う各部分体の基本単数は以下の通りである。
・$\mathbb{Q}(\sqrt{2})$ の基本単数: $\epsilon_2 = 1 + \sqrt{2}$
・$\mathbb{Q}(\sqrt{3})$ の基本単数: $\epsilon_3 = 2 + \sqrt{3}$
・$\mathbb{Q}(\sqrt{6})$ の基本単数: $\epsilon_6 = 5 + 2\sqrt{6}$

定理 7 (基本単数の平方根と u_a の表現)

最大実部分体 $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ において、ノルムが $+1$ である ϵ_3 と ϵ_6 は完全平方となり、その平方根が実在する。
・$\sqrt{\epsilon_3} = \frac{\sqrt{2}+\sqrt{6}}{2}$
・$\sqrt{\epsilon_6} = \sqrt{2} + \sqrt{3}$
これらを用いると、円分単数 u_a は 1 の冪根と基本単数（およびその平方根）を用いて次のように簡明に表される。

$$u_5 = \zeta_{24}^2 \cdot \epsilon_2\sqrt{\epsilon_3}$$

$$u_7 = \zeta_{24}^3 \cdot \sqrt{\epsilon_3\epsilon_6}$$

$$u_{11} = \zeta_{24}^5 \cdot \epsilon_2\sqrt{\epsilon_6}$$

証明

まず、平方根の存在を確認する。

$$\left(\frac{\sqrt{2}+\sqrt{6}}{2}\right)^2 = \frac{2+2\sqrt{12}+6}{4} = \frac{8+4\sqrt{3}}{4} = 2+\sqrt{3} = \epsilon_3$$

$$\left(\sqrt{2}+\sqrt{3}\right)^2 = 2+2\sqrt{6}+3 = 5+2\sqrt{6} = \epsilon_6$$

命題6の因数分解形の実単数部分を再考する。
u_5 の実単数部分は $\frac{(1+\sqrt{3})(2+\sqrt{2})}{2} = (1+\sqrt{2})\frac{1+\sqrt{3}}{\sqrt{2}}$ である。ここで $\frac{1+\sqrt{3}}{\sqrt{2}} = \frac{\sqrt{2}+\sqrt{6}}{2} = \sqrt{\epsilon_3}$ であるから、実部分は $\epsilon_2\sqrt{\epsilon_3}$ となる。また、$\frac{\sqrt{3}+\sqrt{-1}}{2} = \zeta_{24}^2$ であるため、u_5 の表現を得る。
u_7 の実単数部分は $\frac{(1+\sqrt{3})(\sqrt{2}+\sqrt{3})}{\sqrt{2}}$ である。これは $\frac{1+\sqrt{3}}{\sqrt{2}} \cdot (\sqrt{2}+\sqrt{3}) = \sqrt{\epsilon_3}\sqrt{\epsilon_6}$ に等しい。残りの因子は調整により ζ_{24}^3 となる。
u_{11} の実単数部分は $(1+\sqrt{2})(\sqrt{2}+\sqrt{3})$ であり、これは自明に $\epsilon_2\sqrt{\epsilon_6}$ である。残りの因子から ζ_{24}^5 を得る。
$\epsilon_2 = 1+\sqrt{2}$ はノルムが -1 であるため実数の範囲で平方根が取れず、ϵ_2 そのままの形で残る。この代数的性質が、表現の非対称性を生んでいる。（証明終）

以上のように、単に生成元を追加するだけの素朴な代数から出発し、円分単数という具体的な対象を掘り下げることで、基本単数やその平方根の存在といった、部分体が織りなす「単数群の構造の美しさ」を目の当たりにすることができます。

引用文献 (References)

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