円分体とガロア理論、およびArtin写像を用いた平方剰余の相互法則の完全な証明

本稿では、奇素数 p によって生成される円分体 $\mathbb{Q}(\zeta_p)$ に含まれる2次体が唯一 $\mathbb{Q}(\sqrt{p^*})$ であることを証明し、その事実を用いてGauss和の性質、および類体論の基本的な道具であるArtin写像（フロベニウス自己同型）を用いた「平方剰余の相互法則」の2通りの証明を解説する。すべての論証はself-contained（自己完結的）になるように、基本的な定義や具体例から構成する。

1. 準備と基本概念の定義

定義 1.1（ルジャンドル記号）
p を奇素数とし、a を整数とする。a が p で割り切れないとき、合同式 $x^2 \equiv a \pmod{p}$ が解を持つならば a は p を法とする**平方剰余**であるといい、解を持たないならば**平方非剰余**であるという。ルジャンドル記号（Legendre symbol） $\left(\frac{a}{p}\right)$ を次のように定義する。

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & (a \text{ が平方剰余のとき}) \\ -1 & (a \text{ が平方非剰余のとき}) \\ 0 & (a \text{ が } p \text{ の倍数のとき}) \end{cases}$$

定義 1.2（オイラーの規準）
奇素数 p と整数 a に対して、以下の合同式が成立する。これをオイラーの規準 (Euler's criterion) と呼ぶ。

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$$

例（ルジャンドル記号とオイラーの規準の具体例）
$p = 7$ とする。$a = 2$ のとき、$2^{\frac{7-1}{2}} = 2^3 = 8 \equiv 1 \pmod{7}$ である。したがって $\left(\frac{2}{7}\right) = 1$ であり、2 は平方剰余である。実際、$3^2 = 9 \equiv 2 \pmod{7}$ であり解を持つ。
一方 $a = 3$ のとき、$3^3 = 27 \equiv -1 \pmod{7}$ であるため、$\left(\frac{3}{7}\right) = -1$ であり、3 は平方非剰余である。

定義 1.3（円分体とガロア群）
p を奇素数とし、$\zeta_p = \exp(2\pi i/p)$ を 1 の原始 p 乗根とする。有理数体 $\mathbb{Q}$ に ζ_p を添加した体 $K = \mathbb{Q}(\zeta_p)$ を p 次**円分体** (cyclotomic field) と呼ぶ。
$K/\mathbb{Q}$ は有限次Galois拡大であり、そのGalois群 $G = \mathrm{Gal}(K/\mathbb{Q})$ は乗法群 $(\mathbb{Z}/p\mathbb{Z})^\times$ と同型である。具体的な同型対応は、各 $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ に対して $\sigma_a(\zeta_p) = \zeta_p^a$ で定まる自己同型 $\sigma_a \in G$ を対応させることで与えられる。

2. 円分体が含む唯一の2次体が $\mathbb{Q}(\sqrt{p^*})$ であることの証明

円分体 $K = \mathbb{Q}(\zeta_p)$ はいくつかの部分体を含むが、その中で拡大次数が2であるもの（すなわち2次体）はただ一つであること

を示し、それが具体的にどのような体であるかを特定する。

定理 2.1
奇素数 p に対して、円分体 $\mathbb{Q}(\zeta_p)$ が含む2次体は唯一 $\mathbb{Q}(\sqrt{p^*})$ のみである。ただし $p^* = (-1)^{\frac{p-1}{2}} p$ である。

証明
まず、唯一性について証明する。円分体 $K = \mathbb{Q}(\zeta_p)$ の有理数体 $\mathbb{Q}$ 上の拡大次数は $[K : \mathbb{Q}] = p - 1$ である。
前述の通り、Galois群 $G = \mathrm{Gal}(K/\mathbb{Q})$ は $(\mathbb{Z}/p\mathbb{Z})^\times$ と同型である。$(\mathbb{Z}/p\mathbb{Z})^\times$ は原始根を持つため、位数 $p-1$ の巡回群となる。したがって G も位数 $p-1$ の巡回群である。
Galois理論の基本定理により、K に含まれる $\mathbb{Q}$ の中間体 L は、G の部分群 H と一対一に対応し、その対応において拡大次数 $[L : \mathbb{Q}]$ は部分群の指数 $[G : H]$ に等しい。
L が2次体であることは $[L : \mathbb{Q}] = 2$ すなわち $[G : H] = 2$ と同値である。p は奇素数であるから $p-1$ は偶数であり、G は偶数位数の巡回群である。偶数位数の巡回群において、指数が2の部分群 H はただ一つ存在する。したがって、K に含まれる2次体は唯一である。

次に、その唯一の2次体が $\mathbb{Q}(\sqrt{p^*})$ であることを、Gauss和を用いて構成的に証明する。
ルジャンドル記号を用いて、以下の要素 $g \in K$ を定義する。これを**Gauss和** (Gauss sum) と呼ぶ。

$$g = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta_p^a$$

g の平方 g^2 を計算する。

$$g^2 = \left(\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta_p^a\right) \left(\sum_{b=1}^{p-1} \left(\frac{b}{p}\right) \zeta_p^b\right)$$

$$g^2 = \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) \zeta_p^{a+b}$$

ここで、a を固定するごとに、b を p を法として $b \equiv ac \pmod{p}$ となる変数 $c \in (\mathbb{Z}/p\mathbb{Z})^\times$ に変換する。a が固定されていれば、b が 1 から $p-1$ まで動くとき、c も 1 から $p-1$ まで過不足なく動く。ルジャンドル記号の完全乗法性により $\left(\frac{a}{p}\right)\left(\frac{ac}{p}\right) = \left(\frac{a^2 c}{p}\right) = \left(\frac{c}{p}\right)$ となるため、式は次のように変形できる。

$$g^2 = \sum_{a=1}^{p-1} \sum_{c=1}^{p-1} \left(\frac{c}{p}\right) \zeta_p^{a+ac} = \sum_{c=1}^{p-1} \left(\frac{c}{p}\right) \sum_{a=1}^{p-1} \zeta_p^{a(1+c)}$$

内側の和 $\sum_{a=1}^{p-1} \zeta_p^{a(1+c)}$ を評価する。
$c = p-1$（すなわち $c \equiv -1 \pmod{p}$）のとき、$1 + c \equiv 0 \pmod{p}$ であるから $\zeta_p^{1+c} = \zeta_p^0 = 1$ となり、内側の和は $p-1$ となる。
$c \neq p-1$ のとき、$1 + c \not\equiv 0 \pmod{p}$ であるから ζ_p^{1+c} は 1 以外の 1 の p 乗根である。等比数列の和の公式より $\sum_{a=1}^{p-1} (\zeta_p^{1+c})^a = -1$ となる。
これらを元の式に代入する。

$$g^2 = \left(\frac{p-1}{p}\right)(p-1) + \sum_{c=1}^{p-2} \left(\frac{c}{p}\right)(-1)$$

すべての $c \in (\mathbb{Z}/p\mathbb{Z})^\times$ にわたるルジャンドル記号の和は 0 である。すなわち $\sum_{c=1}^{p-1} \left(\frac{c}{p}\right) = 0$ であり、これより $\sum_{c=1}^{p-2} \left(\frac{c}{p}\right) = -\left(\frac{p-1}{p}\right)$ を得る。したがって、

$$g^2 = \left(\frac{p-1}{p}\right)(p-1) - \left(-\left(\frac{p-1}{p}\right)\right) = \left(\frac{p-1}{p}\right)p$$

平方剰余の第1補充則 $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ より、$p-1 \equiv -1 \pmod{p}$ であるため、

$$g^2 = (-1)^{\frac{p-1}{2}}p = p^*$$

であることが導かれた。これより $g = \pm\sqrt{p^*}$ であり、$g \in K$ であるから $\sqrt{p^*} \in K$ となる。p は奇素数であるから $p^* \neq 1$ であり、$\sqrt{p^*}$ は無理数である。よって $\mathbb{Q}(\sqrt{p^*})$ は K に含まれる2次体であり、先述の唯一性により K が含む2次体は $\mathbb{Q}(\sqrt{p^*})$ に限られることが完全に証明された。

3. 平方剰余の相互法則の証明（Gauss和によるアプローチ）

前節で構成したGauss和 g の性質を用いて、平方剰余の相互法則を証明する。

定理 3.1（平方剰余の相互法則）

p, q を相異なる奇素数とする。このとき、以下の関係式が成り立つ。

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

証明

代数的整数環 $\mathbb{Z}[\zeta_p]$ におけるイデアル $q\mathbb{Z}[\zeta_p]$ を法とする合同関係を考える。標数 q の性質から、任意の要素 $x, y \in \mathbb{Z}[\zeta_p]$ に対して多項定理を用いると二項係数が q の倍数になるため、$(x+y)^q \equiv x^q + y^q \pmod{q\mathbb{Z}[\zeta_p]}$ が成り立つ。

これを用いてGauss和 g の q 乗である g^q を2通りの方法で計算し、比較する。

【計算方法1：直接 q 乗の展開】

和の q 乗の性質を用いると、

$$g^q = \left(\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\zeta_p^a\right)^q \equiv \sum_{a=1}^{p-1}\left(\frac{a}{p}\right)^q\zeta_p^{aq} \pmod{q\mathbb{Z}[\zeta_p]}$$

ルジャンドル記号の取る値は ± 1 であり、q は奇数であるため $\left(\frac{a}{p}\right)^q = \left(\frac{a}{p}\right)$ である。さらに $\left(\frac{a}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{q^2}{p}\right) = \left(\frac{aq}{p}\right)\left(\frac{q}{p}\right)$ と変形できる。これを代入すると、

$$g^q \equiv \sum_{a=1}^{p-1}\left(\frac{aq}{p}\right)\left(\frac{q}{p}\right)\zeta_p^{aq} = \left(\frac{q}{p}\right)\sum_{a=1}^{p-1}\left(\frac{aq}{p}\right)\zeta_p^{aq} \pmod{q\mathbb{Z}[\zeta_p]}$$

a が 1 から $p-1$ まで動くとき、q は p と互いに素であるから、aq も p を法として 1 から $p-1$ までの剰余類を全て走る。したがって、右辺の和の順序を並べ替えるとGauss和 g そのものに一致する。

$$g^q \equiv \left(\frac{q}{p}\right)g \pmod{q\mathbb{Z}[\zeta_p]}$$

【計算方法2： $g^2 = p^*$ の利用】

定理2.1で示した $g^2 = p^*$ と、定義1.2のオイラーの規準を用いて g^q を計算する。

$$g^q = g \cdot (g^2)^{\frac{q-1}{2}} = g \cdot (p^*)^{\frac{q-1}{2}}$$

オイラーの規準により、$\mathbb{Z}$ において $(p^*)^{\frac{q-1}{2}} \equiv \left(\frac{p^*}{q}\right) \pmod{q}$ が成り立つ。これは当然 $\mathbb{Z}[\zeta_p]$ においても $q\mathbb{Z}[\zeta_p]$ を法として成り立つため、

$$g^q \equiv \left(\frac{p^*}{q}\right) g \pmod{q\mathbb{Z}[\zeta_p]}$$

【結果の比較と結論】
得られた2つの合同式を比較する。

$$\left(\frac{q}{p}\right) g \equiv \left(\frac{p^*}{q}\right) g \pmod{q\mathbb{Z}[\zeta_p]}$$

両辺に g を掛ける。

$$\left(\frac{q}{p}\right) g^2 \equiv \left(\frac{p^*}{q}\right) g^2 \pmod{q\mathbb{Z}[\zeta_p]}$$

$$\left(\frac{q}{p}\right) p^* \equiv \left(\frac{p^*}{q}\right) p^* \pmod{q\mathbb{Z}[\zeta_p]}$$

ここで、p と q は異なる素数であるため、p^* と q は互いに素である。また、合同式の両辺および p^* はすべて有理整数 (すなわち $\mathbb{Z}$ の元) であり、有理整数が $q\mathbb{Z}[\zeta_p]$ に属するための必要十分条件はそれが通常の意味で $\mathbb{Z}$ において q の倍数となることである。
したがって、上記の合同式から $\mathbb{Z}$ における合同式として p^* を割ることが正当化され、

$$\left(\frac{q}{p}\right) \equiv \left(\frac{p^*}{q}\right) \pmod{q}$$

を得る。両辺はともに $+1$ または -1 であり、その差は $0, 2, -2$ のいずれかである。q は奇素数であるため差が q の倍数になるには両者が完全に等しくなるほかない。よって、

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$$

が成り立つ。
最後に $p^* = (-1)^{\frac{p-1}{2}} p$ を右辺に代入し、ルジャンドル記号の完全乗法性と第1補充則 $\left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}}$ を用いて展開する。

$$\left(\frac{p^*}{q}\right) = \left(\frac{(-1)^{\frac{p-1}{2}} p}{q}\right) = \left(\frac{-1}{q}\right)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) = \left((-1)^{\frac{q-1}{2}}\right)^{\frac{p-1}{2}} \left(\frac{p}{q}\right)$$

$$= (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right)$$

これを先ほどの等式に代入し、両辺に $\left(\frac{p}{q}\right)$ を掛ける（$\left(\frac{p}{q}\right)^2 = 1$ に注意する）ことで、

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

が導出される。これが求める平方剰余の相互法則である。

4. 類体論・Artin写像を用いた平方剰余の相互法則の証明

以上のGauss和を用いた計算は美しいが、有理数体 $\mathbb{Q}$ に関する類体論（特にArtinの相互法則）を用いると、平方剰余の相互法則の構造を大域的・局所的な視点から非常に自然で見通しよく証明することができる。そのプロセスを以下に解説する。

定義 4.1（Artin記号 / フロベニウス自己同型）
p, q を相異なる奇素数とし、$L = \mathbb{Q}(\zeta_p)$ を p 次円分体とする。
素数 q が $L/\mathbb{Q}$ において不分岐であるため（$q \neq p$ より従う）、素数 q に対応する $L/\mathbb{Q}$ の**Artin記号**（フロベニウス自己同型） $\sigma_q = \left(\frac{L/\mathbb{Q}}{q}\right) \in \mathrm{Gal}(L/\mathbb{Q})$ が一意に定まる。これは L の整数環における q の上にある素イデアル $\mathfrak{q}$ を法とする剰余体において、すべての元 α に対して以下のフロベニウス写像の性質を満たす自己同型として定義される。

$$\sigma_q(\alpha) \equiv \alpha^q \pmod{\mathfrak{q}}$$

円分体 $L = \mathbb{Q}(\zeta_p)$ においては、このArtin写像の作用は単に ζ_p を q 乗することとして具体的に記述できる。

$$\sigma_q(\zeta_p) = \zeta_p^q$$

証明（Artin写像を用いた相互法則の導出）

【ステップ1：二次部分体への制限とルジャンドル記号】
定理2.1で示した通り、$L = \mathbb{Q}(\zeta_p)$ には唯一の二次部分体 $K = \mathbb{Q}(\sqrt{p^*})$ が存在する。ただし $p^* = (-1)^{\frac{p-1}{2}} p$ である。
Artin写像の基本的な性質（関手性）により、σ_q を部分体 K に制限した $\sigma_q|_K$ は、部分拡大 $K/\mathbb{Q}$ におけるArtin記号 $\left(\frac{K/\mathbb{Q}}{q}\right)$ に等しくなる。
$\mathrm{Gal}(K/\mathbb{Q}) \cong \{\pm 1\}$ である。自己同型 $\sigma_q \in \mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ が部分群 $\mathrm{Gal}(L/K)$ に属する（すなわち $\sigma_q|_K$ が恒等写像になる）ための必要十分条件は、$q \pmod p$ が $(\mathbb{Z}/p\mathbb{Z})^\times$ において指数2の部分群に属すること、つまり平方剰余（偶数乗の元）であることである。
したがって、ルジャンドル記号 $\left(\frac{q}{p}\right)$ を用いると、σ_q の K の生成元 $\sqrt{p^*}$ への作用は次のように完全に符号で記述できる。

$$\sigma_q(\sqrt{p^*}) = \left(\frac{q}{p}\right)\sqrt{p^*} \quad \cdots (\mathrm{A})$$

【ステップ2：オイラーの規準を用いた別視点からの計算】
一方で、$\sigma_q|_K$ は二次拡大 $K/\mathbb{Q}$ におけるフロベニウス自己同型でもあるため、モジュロ q の上の素イデアル $\mathfrak{q}_K = \mathfrak{q} \cap \mathbb{Z}[\sqrt{p^*}]$ において次を満たさなければならない。

$$\sigma_q(\sqrt{p^*}) \equiv (\sqrt{p^*})^q = (p^*)^{\frac{q-1}{2}}\sqrt{p^*} \pmod{\mathfrak{q}_K}$$

オイラーの規準（定義1.2）によれば、$\mathbb{Z}$ 上の合同式として $(p^*)^{\frac{q-1}{2}} \equiv \left(\frac{p^*}{q}\right) \pmod q$ が成り立つ。したがってイデアル $\mathfrak{q}_K$ を法としても、

$$\sigma_q(\sqrt{p^*}) \equiv \left(\frac{p^*}{q}\right)\sqrt{p^*} \pmod{\mathfrak{q}_K}$$

となる。
(A) より $\sigma_q(\sqrt{p^*}) = \pm\sqrt{p^*}$ であるため、上記の合同式の両辺の係数は ± 1 のいずれかである。$q \neq 2$ であるから $1 \not\equiv -1 \pmod{\mathfrak{q}_K}$ であり、合同式はそのまま厳密な等式として成立する。

$$\sigma_q(\sqrt{p^*}) = \left(\frac{p^*}{q}\right)\sqrt{p^*} \quad \cdots (\mathrm{B})$$

【ステップ3：相互法則の完成】

(A) と (B) の結果を比較すると、直ちに以下の等式が得られる。

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$$

この式は、Gauss和を用いた証明の最終段階で得た式と全く同一である。ここで、ルジャンドル記号の完全乗法性と第一補充法則 $\left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}}$ を用いて右辺を再び展開する。

$$\left(\frac{p^*}{q}\right) = \left(\frac{(-1)^{\frac{p-1}{2}}p}{q}\right) = \left(\frac{-1}{q}\right)^{\frac{p-1}{2}}\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)$$

よって、最終的な結論として以下の式が導かれる。

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

これが類体論のArtin相互法則の観点に基づく、平方剰余の相互法則の証明である。このアプローチでは、「基礎体 $\mathbb{Q}$ の素数 q が、円分体 L の部分体 K でどう分解するか」という局所的な情報と、大域的なGalois群の構造がArtin写像（フロベニウス自己同型）を通して結びつくことで、この美しい対称性が生まれると解釈することができる。

参考文献

- Serre, J.-P. *A Course in Arithmetic*. Graduate Texts in Mathematics 7. Springer-Verlag, 1973. https://link.springer.com/book/10.1007/978-1-4684-9884-4
- Neukirch, J. *Algebraic Number Theory*. Grundlehren der mathematischen Wissenschaften 322. Springer-Verlag, 1999. https://link.springer.com/book/10.1007/978-3-662-03983-0