

$\frac{\varphi(n)}{n}$ によって定まる同値類について

梶田光

2025/08/14

1. はじめに

飯高先生は $F(n) := \frac{\sigma(n)}{n}$ によって定まる同値類の性質を考察した.

このアイデアをオイラー関数に持ち込んだのが φ 同値である.

主定理の前にいくつか簡単な議論をしておく.

定義 1.1: $\frac{\varphi(n)}{n} = \frac{\varphi(m)}{m}$ が成り立つとき, n と m は φ 同値であるといい, $n \sim_{\varphi} m$ と書く.

補題 1.1: $\text{rad}(n) = \text{rad}(m)$ ならば $n \sim_{\varphi} m$.

ここで $\text{rad}(n)$ は n の根基, つまり n の相異なる素因数の積を表す.

具体的には, $\text{rad}(n) = \prod_{p \mid n} p$ である.

今回の主定理はこの補題の逆である.

Proof: $\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$ より, $\frac{\varphi(n)}{n} = \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$ である.

さて, n と m の素因数の組が等しければ, $\frac{\varphi(n)}{n} = \frac{\varphi(m)}{m}$ が成り立つことは上の式から明らかであろう. ■

補題 1.2: n を無平方数とする.

自然数 a, b について $ab = n$ が成り立つならば, $\gcd(a, b) = 1$ で, a, b も無平方数.

無平方数とは, $\text{rad}(n) = n$ が成り立つ自然数のことである.

言い換えると, 任意の素数 p について $\nu_p(n) < 2$ が成り立つ自然数のことである.

Proof: $\gcd(a, b) = 1$ からまず証明する.

$\gcd(a, b) = d > 1$ と仮定すると, d には素因数 p が存在する.

さて, $n = ab = \frac{a}{d} \cdot \frac{b}{d} \cdot d^2$ と書け, さらに $\frac{a}{d}, \frac{b}{d}$ は整数であるから, n は d^2 で割れ, よって n は p^2 の倍数である.

これは n が無平方数であることに矛盾.

次に, a が無平方数でないと仮定すると, $p^2 \mid a$ を満たす素数 p が存在するが, この p は $p^2 \mid n$ も満たすことになるので n が無平方数であるという仮定に反する.

b についても同様. ■

2. 主定理

定義 2.1: $\lambda(n) := \gcd(\varphi(n), n), \lambda'(n) := \frac{n}{\lambda(n)}$ と定義する.

そして, 非負整数 k について, $\lambda^k(n) = \begin{cases} n & \text{if } k = 0, \\ \lambda(\lambda^{k-1}(n)) & \text{otherwise} \end{cases}$ と定義する.

命題 2.1: α, β を $\alpha \sim_{\varphi} \beta$ を満たす無平方数とすると, $\lambda'(\alpha) = \lambda'(\beta)$ かつ $\lambda(\alpha) \sim_{\varphi} \lambda(\beta)$ が成り立つ.

Proof: $\gcd(\alpha, \varphi(\alpha)) = \gcd(\lambda(\alpha)\lambda'(\alpha), \varphi(\alpha)) = \lambda(\alpha)$ より, $\gcd(\lambda'(\alpha), \varphi(\alpha)) = 1$ である.

よって, $\frac{\varphi(\alpha)}{\alpha} = \frac{\varphi(\alpha)}{\lambda(\alpha)\lambda'(\alpha)} = \frac{\left(\frac{\varphi(\alpha)}{\lambda(\alpha)}\right)}{\lambda'(\alpha)}$ と変形するとこれは既約分数形である.

よってユークリッドの補題からある整数 k が存在して $\beta = k\lambda'(\alpha), \varphi(\beta) = k\frac{\varphi(\alpha)}{\lambda(\alpha)}$ と書ける.

このとき, $\lambda(\beta) = \gcd\left(k\lambda'(\alpha), k\frac{\varphi(\alpha)}{\lambda(\alpha)}\right) = k \gcd\left(\lambda'(\alpha), \frac{\varphi(\alpha)}{\lambda(\alpha)}\right) = k$ である.

よって, $\beta = \lambda(\beta)\lambda'(\alpha)$ から, $\lambda'(\alpha) = \lambda'(\beta)$.

さて, $\varphi(\beta) = k\frac{\varphi(\alpha)}{\lambda(\alpha)} = \lambda(\beta)\frac{\varphi(\alpha)}{\lambda(\alpha)}$ に, $\alpha = \lambda(\alpha)\lambda'(\alpha), \beta = \lambda(\beta)\lambda'(\beta)$ を代入して 補題 1.2 を適用すると $\varphi(\lambda(\beta))\varphi(\lambda'(\beta)) = \lambda(\beta)\frac{\varphi(\lambda(\alpha))\varphi(\lambda'(\alpha))}{\lambda(\alpha)}$ を得る.

両辺を $\varphi(\lambda'(\beta)) = \varphi(\lambda'(\alpha))$ で割って整理すると $\frac{\varphi(\lambda(\beta))}{\lambda(\beta)} = \frac{\varphi(\lambda(\alpha))}{\lambda(\alpha)}$, よって $\lambda(\alpha) \sim_{\varphi} \lambda(\beta)$ が示された. ■

定理 2.1: $n \sim_{\varphi} m$ ならば $\text{rad}(n) = \text{rad}(m)$.

Proof: この定理を証明するには,

命題 (A): 無平方数 α, β について $\alpha \sim_{\varphi} \beta$ ならば $\alpha = \beta$

を示すことができれば十分である.

というのも, 一般の自然数 n について, 補題 1.1 と rad が冪等であることから $n \sim_{\varphi} \text{rad}(n)$.

したがって, $n \sim_{\varphi} m$ というのは $\text{rad}(n) \sim_{\varphi} \text{rad}(m)$ と同値である.

任意の自然数 n について $\text{rad}(n)$ は無平方数であるから, もし命題 (*) が示されれば $n \sim_{\varphi} m \iff \text{rad}(n) \sim_{\varphi} \text{rad}(m) \iff \text{rad}(n) = \text{rad}(m)$ が示せる.

そこで, 命題 (A) を証明しよう.

さて, $\lambda(n)$ の定義上 $n > 1$ のとき $\lambda(n) < n$ であるから, $\lambda^i(\alpha) = 1$ となる正整数 i が存在する.

今, 命題 2.1 が繰り返し適用できることに注目しよう.

つまり, $\lambda'(\alpha) = \lambda'(\beta)$ かつ $\lambda(\alpha) \sim_{\varphi} \lambda(\beta)$ であるが, 補題 1.2 より $\lambda(\alpha), \lambda(\beta)$ も無平方数である.

したがって, $\lambda'(\alpha) = \lambda'(\beta)$ かつ $\lambda'(\lambda(\alpha)) = \lambda'(\lambda(\beta))$ かつ $\lambda^2(\alpha) \sim_{\varphi} \lambda^2(\beta)$.

このような議論で, $\alpha \sim_{\varphi} \beta$ に 命題 2.1 を i 回適用すると, すべての $0 \leq j < i$ について $\lambda'(\lambda^j(\alpha)) = \lambda'(\lambda^j(\beta))$ かつ $\lambda^i(\alpha) \sim_{\varphi} \lambda^i(\beta)$ が成り立つことがわかる.

さて, $\lambda^i(\alpha) = 1$ であるから $\lambda^i(\beta) \sim_{\varphi} 1$.

よって, $\lambda^i(\beta) = 1$ である.

ここで, $\lambda'(\lambda^{i-1}(\alpha)) = \lambda'(\lambda^{i-1}(\beta))$ なので, $\lambda^i(\alpha) = \lambda^i(\beta)$ を $\lambda(\lambda^{i-1}(\alpha)) = \lambda(\lambda^{i-1}(\beta))$ と考えれば $\lambda^{i-1}(\alpha) = \lambda^{i-1}(\beta)$ が得られる. (これは $\lambda(n)\lambda'(n) = n$ から.)

同様に, $\lambda'(\lambda^{i-2}(\alpha)) = \lambda'(\lambda^{i-2}(\beta))$ なので, $\lambda^{i-1}(\alpha) = \lambda^{i-1}(\beta)$ を $\lambda(\lambda^{i-2}(\alpha)) = \lambda(\lambda^{i-2}(\beta))$ と考えれば $\lambda^{i-2}(\alpha) = \lambda^{i-2}(\beta)$ も得られる.

これを繰り返すと, $\alpha = \beta$ が得られる. ■

最後の命題 (A) の証明を図解すると以下のようなになる.

