代数体の階乗型 Diophantus 方程式の自明解の有限性

武田 渉 (名古屋大学)

概 要

本稿は 2018 年 8 月 28 日, 29 日に行われた第 12 回福岡数論研究集会における私の講演に基づくものである. 本研究では階乗からなる Diophantus 方程式 $l_1! \cdots l_{m-1}! = l_m!$ を代数体に一般化し, ある性質を満たす解の有限性を与えた. また, 時間の関係上お話しできなかった補題の証明および講演後にいただいた質問の回答についても説明する.

1 導入

m 個の整数 $2 \leq l_1 \leq \cdots \leq l_{m-1} < l_m$ に対して, 階乗からなる Diophantus 方程式

$$l_1! \cdots l_{m-1}! = l_m! \tag{1}$$

を考える. このとき, 任意の $l_1, \cdots, l_{m-2}$ に対して, $N = l_1! \cdots l_{m-2}!$ とすると $(l_1, \ldots, l_{m-2}, N-1, N)$ は (1) の解となる. つまり, この方程式は解を無限個持つということが分かる. このような自明に構成されるような解, つまり $l_{m-1} - l_m = 1$ を満たす解を自明解と呼ぶ. このとき, 自明でない解, つまり非自明解については以下の予想が存在する.

Conjecture. Diophantus 方程式 (1) の非自明解は有限個である.

この予想は未だに示されていないが, $l_m < 10^6$ までで現在見つかっている非自明解が $(6, 7, 10)$, $(3, 5, 7, 10)$, $(2, 5, 14, 16)$, $(2, 3, 3, 7, 9)$ のみであることが分かっている ([Ca94]). また Luca により ABC 予想の仮定のもとで $l_{m-2}, l_m - l_{m-1}, l_m$ の間の評価式が与えられた. その評価式を満たす 3 つ組 (l_{m-2}, l_{m-1}, l_m) は有限個であるため, それにより非自明解の有限性が ABC 予想のもとで示された ([Lu07]).

本講演では方程式 (1) を一般の代数体に一般化したときの結果についてお話しした.

K を代数体, $\mathcal{O}_K$ を整数環とする. 代数体上に一般化した階乗関数 $\Pi_K(l)$ を以下のように定める:

$$\Pi_K(x) = \prod_{\mathfrak{Na} \leq x} \mathfrak{Na} = \prod_{n \leq x} n^{a(n)}.$$

ここで $a(n)$ は $\mathcal{O}_K$ のイデアル $\mathfrak{a}$ で $\mathfrak{Na} = n$ となるものの数である. このイデアル個数関数 $a(n)$ は以下の乗法的性質を満たす: $\gcd(m, n) = 1$ のとき

$$a(mn) = a(m)a(n).$$

ここで一般化した階乗関数に対して Diophantus 方程式を以下のように定める: m 個の整数 $2 \leq l_1 \leq \cdots \leq l_{m-1} < l_m$ に対して

$$\Pi_K(l_1) \cdots \Pi_K(l_{m-1}) = \Pi_K(l_m). \tag{2}$$

方程式 (2) は $K = \mathbf{Q}$ のとき方程式 (1) に一致する．一般の代数体の場合，方程式 (2) の解 $(l_1, \ldots, l_m)$ が自明解であるとは，$l_{m-1} < \mathfrak{N}\mathfrak{a} < l_m$ となるイデアル $\mathfrak{a}$ が存在しないことと定める．例えば $K = \mathbf{Q}(\sqrt{-3}), m = 3$ のとき，$\mathcal{O}_K = \mathbf{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ での素数の分解について以下のことが分かる:

素数 p	$\mathcal{O}_K$での振る舞い	$k \geq 1$ に対して $a(p^k)$ の値
$p \equiv 1 \mod 3$	(p) は完全分解	$a(p^k) = k+1$
$p \equiv 2 \mod 3$	(p) は $\mathcal{O}_K$ 上の素イデアル	$a(p^{2k-1}) = 0, a(p^{2k}) = 1$
$p = 3$	(3) は分岐する	$a(p^k) = 1$

これと先に指摘したイデアルの個数関数の乗法性から，$a(n)$ の値をすべて求めることができ，(2) の解として $(4, 9, 12)$，$(12, 247, 252)$，$(16, 111, 117)$ が見つかる．ここで，$a(10) = a(11) = a(248) = a(249) = a(250) = a(251) = 0$ であることから $(4, 9, 12)$，$(12, 247, 252)$ は自明解であり，$a(112) = 2$ であることから $(16, 111, 117)$ は非自明解となる．

いままで $K \neq \mathbf{Q}$ の場合に方程式 (2) の解の数については何も知られていなかったが，今回私は自明解の有限性を示した ([Ta18])．

Theorem 1. 任意の代数体 $K \neq \mathbf{Q}$ に対して，Diophantine 方程式 (2) の自明解は有限個である．

冒頭で指摘したように $\mathbf{Q}$ のときは自明解の無限性が知られていたが，Theorem 1 は $\mathbf{Q}$ 以外の代数体では Diophantine 方程式 (2) の自明解は有限個であることを主張している．つまり，$\mathbf{Q}$ のときとそれ以外では本質的な違いがあるということがわかる．

2 補題

この章では Theorem1 の証明のために 2 つ補題を証明する．まず，m 個の組 $(l_1, \ldots, l_m)$ が自明解であることの必要十分条件を与える．

Lemma 2. 以下の 2 つの主張は同値である．

1. m 個の組 $(l_1, \ldots, l_m)$ が自明解である．
2. $l_m = \prod_p p^{r_p}$ としたとき，

$$\Pi_K(l_1) \cdots \Pi_K(l_{m-2}) = l_m^{a(l_m)} = \left(\prod_p p^{r_p}\right)^{\prod_p a(p^{r_p})}$$

が成立．

Proof. まず $(l_1, \ldots, l_m)$ が自明解であると仮定する．このとき，$\Pi_K(l_1) \cdots \Pi_K(l_{m-1}) = \Pi_K(l_m)$ は両辺を $\Pi_K(l_{m-1})$ で割ることで

$$\Pi_K(l_1) \cdots \Pi_K(l_{m-2}) = \prod_{l_{m-1} < \mathfrak{N}\mathfrak{a} \leq l_m} \mathfrak{N}\mathfrak{a}$$

と変形できる．ここで自明解であることから，

$$\prod_{l_{m-1} < \mathfrak{N}\mathfrak{a} \leq l_m} \mathfrak{N}\mathfrak{a} = l_m^{a(l_m)}$$

がわかるため, 2 の主張を得る. 2 つ目の等号はイデアル個数関数の乗法性から $a(l_m) = \prod_p a(p^{r_p})$ が得られることから従う.

逆に $\Pi_K(l_1)\cdots\Pi_K(l_{m-2}) = l_m^{a(l_m)}$ であるとき, $l_{m-1} = \max\{\mathfrak{N}\mathfrak{a} \mid \mathfrak{a} : \text{ideal}\} \cap [l_{m-2}, l_m)$ とする. このとき,

$$\Pi_K(l_m) = l_m^{a(l_m)}\Pi_K(l_{m-1}) = \Pi_K(l_1)\cdots\Pi_K(l_{m-1})$$

が成り立つため, m 個の組 $(l_1, \ldots, l_m)$ は解である. さらに l_{m-1} の定義から $\mathfrak{N}\mathfrak{a} \in (l_{m-1}, l_m)$ となるようなイデアル $\mathfrak{a}$ は存在しないため, $(l_1, \ldots, l_m)$ は自明解である. 以上で証明された. □

つぎに完全分解する素数の Bertrand 型の結果を証明する. Bertrand は 1845 年に任意の正の整数 n に対して, $n < p \leq 2n$ を満たす素数 p が存在するということを予想した. この予想は 1852 年に Chebyshev によって証明され, その一般化は様々な形で行われている. 今回は完全分解する素数についての Bertrand 型の結果を与えた.

その証明のために Lagarias と Odlyzko ([LO77]) によって示された Chebotarev 密度定理の誤差項に関する結果を用いる. 彼らの結果を説明するためにいくつか記号を定義する. まず L/K を Galois 拡大とし, $G = \mathrm{Gal}(L/K)$ とする. G の各共役類 C に対して, 個数関数 $\pi_C(x)$ を以下のように定める:

$$\pi_C(x) = |\{\mathfrak{p} \subset \mathcal{O}_K : \mathfrak{p} \text{ は } L \text{ で不分岐}, [(\mathfrak{p}, L/K)] = C, \mathfrak{N}\mathfrak{p} \leq x\}|.$$

ここで $[(\mathfrak{p}, L/K)]$ は $\mathfrak{p}$ に対応する Frobenius 写像の共役類である.

Lemma 3 ([LO77, Theorem 1.3])**.** L/K を Galois 拡大とし, $G = \mathrm{Gal}(L/K)$, $[L : \mathbf{Q}] = n$ とする. また L の判別式の絶対値を D_L とする. このとき計算可能な正の定数 c_1, c_2 が存在して以下を満たす: 任意の $x > \exp\left(10n(\log D_L)^2\right)$ に対して

$$\left|\pi_C(x) - \frac{|C|}{|G|}Li(x) + \frac{|C|}{|G|}(-1)^{\varepsilon_L}Li(x^\beta)\right| \leq c_1 x \exp\left(-c_2\sqrt{\frac{\log x}{n}}\right).$$

ここで $Li(x^\beta)$ の項は Dedekind ゼータ関数 ζ_L の例外零点 β が存在する場合のみ現れる. また ε_L は 0 または 1 で L に依存する.

もし $\mathfrak{p}$ が L で完全分解するならば Frobenius 写像 $(\mathfrak{p}, L/K)$ は恒等写像であり $|[(\mathfrak{p}, L/K)]| = 1$ となる. また ε_L の [LO77] における定義から, 完全分解するものを考える場合 $\varepsilon_L = 0$ ということも分かる. この補題を用いて以下の完全分解する素数についての Bertrand 型の結果を与える.

Theorem 4. 代数体 K に対して K^{gal} を拡大 $K/\mathbf{Q}$ の Galois 閉包とし, その拡大次数を $[K^{gal} : \mathbf{Q}] = k$ とする. さらに D を K^{gal} の判別式の絶対値とする. このとき, 任意の $A > 1$ に対して計算可能定数 $c_A > 0$ で次を満たすようなものが存在する. 任意の $x > \exp(c_A k(\log D)^2)$ に対して $x < p \leq Ax$ となるような完全分解する素数 p が存在する.

Proof. まず素数 p が K で完全分解することと Galois 閉包 K^{gal} で完全分解することは同値であることが知られている. つまり, 一般性を失わずに $K/\mathbf{Q}$ が Galois 拡大と仮定できる. まず $\pi_{s.c.}(x)$ を $p \leq x$ なる完全分解する素数 p の数とする. Lemma 3 と先の注意から以下の不等式を得る:

$$\begin{aligned}
&\pi_{s.c.}(Ax) - \pi_{s.c.}(x) \\
&\quad > \frac{1}{k}\left(Li(Ax) - Li(x)\right) - \frac{1}{k}\left(Li\left((Ax)^\beta\right) - Li(x^\beta)\right) - 2Ac_1 x \exp\left(-c_2\sqrt{\frac{\log x}{k}}\right).
\end{aligned}$$

この不等式の右辺が $x > \exp(c_A k(\log D)^2)$ で正であることを示せば良い.

ここで Stark ([St74]) によって $K/\mathbf{Q}$ が Galois 拡大で例外零点 β が存在するとき, 以下を満たす K によらない定数 $c > 0$ が存在することが知られている:

$$1 - \frac{1}{4\log D} < \beta < 1 - c\frac{1}{D^{\frac{1}{k}}}.$$

固定した $x > \exp\left(10k(\log D)^2\right)$ と $A > 1$ に対して $Li\left((Ax)^\beta\right) - Li(x^\beta)$ が β に関する単調増加関数であることから, $\beta_0 = 1 - cD^{-\frac{1}{k}}$ として, β に β_0 を代入した式

$$\frac{1}{k}\left(Li(Ax) - Li(x)\right) - \frac{1}{k}\left(Li\left((Ax)^{\beta_0}\right) - Li(x^{\beta_0})\right) - 2Ac_1 x \exp\left(-c_2\sqrt{\frac{\log x}{k}}\right) > 0$$

を考える. この目標の不等式の $Li(x)$ に部分積分を用いることで以下の形にできる: 任意の $x > \exp\left(10k(\log D)^2\right)$ と $A > 1$ に対して

$$\begin{aligned}&\frac{Ax}{\log Ax} - \frac{(Ax)^{\beta_0}}{\beta_0 \log Ax} + \int_{(Ax)^{\beta_0}}^{Ax} \frac{dt}{(\log t)^2} \\ &\quad > \frac{x}{\log x} - \frac{x^{\beta_0}}{\beta_0 \log x} + \int_{x^{\beta_0}}^{x} \frac{dt}{(\log t)^2} + 2Akc_1 x \exp\left(-c_2\sqrt{\frac{\log x}{k}}\right).\end{aligned}$$

そして, $\int_{x^{\beta_0}}^{x} \frac{dt}{(\log t)^2}$ も $x > \exp(10k(\log D)^2)$ の範囲で x に関する単調増加関数であるため,

$$\frac{Ax\beta_0 - (Ax)^{\beta_0}}{\beta_0 \log Ax} > \frac{x\beta_0 - x^{\beta_0}}{\beta_0 \log x} + 2Akc_1 x \exp\left(-c_2\sqrt{\frac{\log x}{k}}\right)$$

と積分をなくしたものを得ることができれば十分である. さらに $x > 10$ で $\frac{x\beta_0 - x^{\beta_0}}{\beta_0 \log x} > 0$ であることに注意して, 両辺を $\frac{x\beta_0 - x^{\beta_0}}{\beta_0 \log x}$ で割ることで以下の式が得られる:

$$A\frac{\beta_0 - (Ax)^{\beta_0 - 1}}{\beta_0 - x^{\beta_0 - 1}} \frac{\log x}{\log Ax} > 1 + \frac{2A\beta_0 k c_1 \log x}{\beta_0 - x^{\beta_0 - 1}} \exp\left(-c_2\sqrt{\frac{\log x}{k}}\right). \tag{3}$$

これを十分大きな x で示すことが最終目標である. いま $x = \exp\left(c_A k(\log D)^2\right)$ とする. このとき右辺は

$$\frac{2\beta_0 A k^2 c_1 c_A (\log D)^2 D^{-c_2\sqrt{c_A}}}{\beta_0 - x^{\beta_0 - 1}} \tag{4}$$

であり, (4) の分母は $x > 10$ で単調増加かつ正である. 一方 (4) の分子

$$2\beta_0 A c_1 \frac{c_A}{D^{c_2\sqrt{c_A} - 3}} \left(\frac{k}{D}\right)^2 \frac{(\log D)^2}{D}$$

は $c_A > 4c_2^{-2}$ ならば単調減少するが, Minkowski bound ([La94])

$$\frac{k}{D} \leq \left(\frac{4}{\pi}\right)^k \frac{(k!)^2}{k^{2k-1}} \leq \frac{8}{\pi^2}$$

から c_A を K に依らずに選ぶことができる. よって, そのように c_A を取ると不等式 (3) の両辺は $x > \exp\left(c_A k(\log D)^2\right)$ で単調減少である. さらに $x \to \infty$ で左辺は A に収束し右辺は 1 に収束することも分かる. これらの結果より c_A が存在して $x > \exp\left(c_A k(\log D)^2\right)$ ならば不等式 (3) が成立. つまり $\pi_{s.c.}(Ax) - \pi_{s.c.}(x) > 0$ となることが分かる. □

3　主定理の証明

この章では本稿の主定理の証明をする.

代数体 K に対して拡大次数を $n=[K:\mathbf{Q}]$ とする. また K^{gal} を拡大 $K/\mathbf{Q}$ の Galois 閉包とし, その拡大次数を $k=[K^{gal}:\mathbf{Q}]$ とする. さらに D を K^{gal} の判別式の絶対値とする. まず $p_1=\min\{\mathfrak{N}\mathfrak{a} \mid \mathfrak{a}:\text{ideal of } \mathcal{O}_K\}\cap\mathbf{Z}_{>1}$ とする. つまり, 2 番目に小さなイデアルノルムである. Theorem 4 より, ある定数 c_{p_1} が存在して, 任意の $x\geq\exp(c_{p_1}k(\log D)^2)$ に対して $x<p\leq p_1x$ なる完全分解する素数 p が存在することがわかる. いま集合 $P_{s.c.}(x)$ を $\{p\leq x \mid K \text{ で完全分解}\}$ と定める. q を完全分解する素数で $q\geq\exp(c_{p_1}k(\log D)^2)$ と $n^{|P_{s.c.}(q)|}>n(m-2)$ を満たすものとする.

いま $q\leq l_{m-2}<p_1q$ に対して m 組 $(l_1,\dots,l_m)$ が自明解ならば, Lemma 2 から

$$\Pi_K(l_1)\cdots\Pi_K(l_{m-2})=\left(q^{r_q}\prod_{p\neq q}p^{r_p}\right)^{\prod_p a(p^{r_p})} \tag{5}$$

が成り立つ. ここで $r_p\geq 0$ であり $r_q\geq 1$ である.

ここで $r_q\geq 1$ かつ完全分解する素数 p に対して $a(p^{r_p})\geq n$ であるため, (5) の右辺は $q^{n^{|P_{s.c.}(q)|}}$ で割れる. $\Pi_K(l)$ に q の要素が q の次に現れるのは p_1q であるため, $q\leq l_{m-2}<p_1q$ という仮定から $\Pi_K(l_i)$ $(1\leq i\leq m-2)$ は最大で q^n でしか割れない. つまり, (5) の左辺 $\Pi_K(l_1)\cdots\Pi_K(l_{m-2})$ は最大で $q^{n(m-2)}$ でしか割れない. q は $n(m-2)<n^{|P_{s.c.}(q)|}$ を満たすものとして取っているためこれは矛盾. よって, $q\leq l_{m-2}<p_1q$ に対して m 組 $(l_1,\dots,l_m)$ は自明解になり得ない. また Theorem 4 から完全分解する素数 q_1 で $q<q_1\leq p_1q$ を満たすものが存在する.

ここで $q_1\geq\exp(c_{p_1}k(\log D)^2)$ かつ $n^{|P_{s.c.}(q_1)|}>n(m-2)$ であるため, 先と同じ議論ができ $q_1\leq l_{m-2}<p_1q_1$ に対して m 組 $(l_1,\dots,l_m)$ は自明解でなく, 完全分解する素数 q_2 で $q_1<q_2\leq p_1q_1$ を満たすものが存在する.

帰納法を用いることで $q\leq l_{m-2}$ に対して m 組 $(l_1,\dots,l_m)$ は自明解でないことがわかり, 自明解の有限性が得られる.

謝辞

第 12 回福岡数論研究集会における講演の機会を与えてくださった金子昌信先生, 権寧魯先生, 岸康弘先生, 高妻倫太郎先生にこの場をお借りして感謝いたします. また Lemma 2 について, 解になる仮定が不要であると指摘してくださった山本修司先生にもこの場をお借りして感謝いたします.

参考文献

[Ca94] C. Caldwell, The Diophantine equation $A!B!=C!$, J. Recreat. Math. **26** (1994), 128–133.

[LO77] J. C. Lagarias and A. M. Odlyzko, Effective versions of the Chebotarev density theorem, In: Algebraic number fields: L-functions and Galois properties, 409–464, Academic Press, London, 1977.

[La94] S. Lang, Algebraic number theory, second edition, Graduate Texts in Mathematics, 110, Springer-Verlag, New York, 1994.

[Lu07] F. Luca, On factorials which are products of factorials, Math. Proc. Cambridge Philos. Soc. **143** (2007), no. 3, 533–542.

[St74] H. M. Stark, Some effective cases of the Brauer–Siegel theorem, Invent. Math. **23** (1974), 135–152.

[Ta18] W. Takeda, The finiteness of solutions of Diophantine equation and primes splitting completely, preprint, 2018, arXiv:1808.00124.