数理解析研究所講究録
1026巻 1998年 76-80

Kummer 拡大と楕円曲線の Mordell-Weil rank

九大 数理学研究科　佐藤尚宜　(Sato Hisayoshi)

§1. 序

有限次代数体 K 上に定義された楕円曲線 E を考える. このとき K 有理点の集合 $E(K)$ は有限生成 Abel 群であり, その free part の rank を E/K の (Mordell-Weil) rank という. また E/K に対し, L-関数 $L(E,K;s)$ が定義される. ここでは L/K を有限次拡大とするとき E の L 上での rank, 及び L-関数を K 上で定義されたもので記述することを考えたい. 例えばよく知られているように, 各 $\alpha\in K^{\times}\setminus K^{\times 2}$ に対し (2 次)twist と呼ばれる楕円曲線 E_{α}/K が存在し, $L=K(\sqrt{\alpha})$ とするとき Wordell-Weil rank に関して

$$\mathrm{rank}E(L)=\mathrm{rank}E(K)+\mathrm{rank}E_{\alpha}(K),$$

$$L(E,L;s)=L(E,K;s)L(E_{\alpha},K;s)$$

が成り立つ. この関係式は A. Sato[8], M. Kida[3] によってある条件をみたす Abel 多様体の場合に拡張されている (§2). また, [1],[2],[4],[7] にも関連した結果が与えられている.

今回は L/K が Kummer 拡大のとき楕円曲線 E/K の rank, 及び L-関数について考える.

§2. 準備

まず Sato, Kida の結果を紹介する.

A/K を Abel 多様体とし, $m\geq 2$ を自然数, $\mu_m(\subset\bar{K})$ を 1 の m 乗根の群とする. さらに

$$L(A,K;s)=\prod_{v\in M_K^0}\det(1-(N_v)^{-s}\cdot F_v\mid T_l(A))^{-1}$$

を A/K の L-関数とする. ただし M_K^0 は K の有限素点全体の集合, N_v は v での剰余体の元の個数, $T_l(A)$ は Tate module, F_v は Frobenius 自己準同型をあらわす.

次がみたされていると仮定する:

仮定 (A).

(1) 準同型 $\iota:\mathbf{Z}[\mu_m]\longrightarrow\mathrm{End}_K(A)$ が存在する.

(2) L/K は指数が m を割る有限次 Abel 拡大 ($G=\mathrm{Gal}(L/K)$ とおく).

このとき次が成り立つ:

$$\begin{aligned}\mathrm{rank}A(L)&=\sum_{\chi\in\hat{G}}\mathrm{rank}A_{\chi}(K),\\ L(A,L;s)&\sim\prod_{\chi\in\hat{G}}L(A_{\chi},K;s).\end{aligned}\qquad(1)$$

ただし A_χ/K は $\iota\circ\chi \in H^1(G, \mathrm{Aut}_L(A))$ に対応する twist, 記号 $\sim$ は有限個の Euler factor を除き一致することを意味する [3],[8].

次に素数 $l \geq 3$ を固定し, $\mu_l \subset K$ と仮定する. K 上の楕円曲線

$$E : Y^2 = f(X) = X^3 + aX^2 + bX + c \quad /K$$

を考える. (ここで一般性を失うことなく $c \neq 0$ としてよい.)

C_l を $y^2 = f(x^l)$ で定まる hyper elliptic curve とする. このとき $C_l \setminus \{y^2 = f(x^l)\}$ は唯一つの点からなり, それを P とする. P は K 有理点である. C_l の定義により, 写像 $\psi : C_l \to E$, $\psi((x,y)) = (x^l, y)$, $\psi(P) = O(=\infty)$ が存在する. $J = J(C_l)/K$ を C_l の Jacobi 多様体とし, $f^P : C_l \to J$ を P が定める写像とすると Abel 多様体の (K 上の) 準同型 $\phi : J \to E$ が一意に存在して次は可換である:

$$\begin{array}{ccc} C_l & \xrightarrow{f^P} & J \\ \psi\downarrow & \swarrow\phi & \\ E. & & \end{array}$$

準同型 ϕ の核の単位元の成分を N とすると N は K 上の Abel 多様体で, 任意の有限次拡大 K'/K に対し次が成り立つ:

$$\begin{aligned} \mathrm{rank}J(K') &= \mathrm{rank}N(K') + \mathrm{rank}E(K'), \\ L(J,K';s) &= L(N,K';s)L(E,K';s). \end{aligned} \tag{2}$$

ζ_l を 1 の原始 l 乗根とし, 固定する. このとき C_l は P を P にうつす K 上の位数 l の自己同型

$$\varepsilon = \varepsilon_l : \quad \begin{array}{c} C_l \longrightarrow C_l \\ (x,y) \mapsto (\zeta_l x, y) \end{array}$$

を持つ. よって J も K上の位数 l の自己同型をもち, それも同じ記号 ε であらわす. このとき ϕ の一意性から次がわかる:

Lemma. 次の図式は可換:

$$\begin{array}{ccc} J & \xrightarrow{\varepsilon} & J \\ \phi\downarrow & \swarrow\phi & \\ E. & & \end{array}$$

よって特に $\varepsilon|_N \in \mathrm{Aut}_K(N)$.

L/K を l 次 Kummer 拡大, $G = \mathrm{Gal}(L/K)$ を Galois 群とし, 生成元 σ を固定する. $\hat{G}$ を G の指標群とし, $\chi \in \hat{G}$ を $\chi(\sigma) = \zeta_l$ なる元とする. さらに準同型 ι を

$$\iota : \mu_l \longrightarrow \mathrm{End}(J)^\times, \quad \iota(\zeta_l) = \varepsilon$$

で定義する.

$\iota \circ \chi^i \in H^1(G, \mathrm{Aut}_L(J))$ $(0 \leq i \leq l-1)$ に対応して J の twist J_i/K と, L 上の同型 $\theta_i : J_i \to J$ であって $\theta_i^\sigma \circ \theta_i^{-1} = \varepsilon^i$ をみたすものが存在する. このとき次のことがわかる:

(i) J_i は K 上の位数 l の自己同型 $\varepsilon_i := \theta_i^{-1} \circ \varepsilon \circ \theta_i$ を持つ.

(ii) J は仮定 (A) をみたすので

$$\mathrm{rank}J(L) = \sum_{i=0}^{l-1} \mathrm{rank}J_i(K), \quad L(J, L; s) \sim \prod_{i=0}^{l-1} L(J_i, K; s).$$

(iii) $N \subset J$ は余次元 1 なので, K 上定義されたある楕円曲線 $E' \subset J$ であって, $J = N + E'$, $N \cap E'$ は有限 なるものが存在する. さらに E' は ϕ により E と K 上同種.

§3. 主結果

2 つの場合に分ける:

(I) $\varepsilon|_N = id_N$ のとき. このとき $\varepsilon(E') \neq E'$ である. そこで

$$A = E' \times \varepsilon(E') \times \cdots \times \varepsilon^{l-1}(E')$$

とおく. ε は A の位数 l の K 上の自己同型 ε_A を導く. よって A は仮定 (A) をみたす.

$\theta_i^{-1}(E') \subset J$ は L 上の楕円曲線である. $B_i := R_{L/K}(\theta_i^{-1}(E'))$ $(1 \leq i \leq l-1)$ を Galois descent とする [3],[9]. また $B_0 := A$ とおく. このとき次が成り立つ:

Lemma. B_i は A の χ^i に関する twist である.

これと (1) 及び A の定義より

$$l\mathrm{rank}E(L) = l\mathrm{rank}E'(L) = \mathrm{rank}A(L) = \sum_{i=0}^{l-1} \mathrm{rank}B_i(K),$$

$$L(E, L; s)^l = L(E', L; s)^l = L(A, L; s) \sim \prod_{i=0}^{l-1} L(B_i, K; s)$$

がわかる. 一方, $\varepsilon|_N = id_N$ であるから $\theta_i^{-1}(N) \subset J_i$ は K 上定義された部分 Abel 多様体となりゆえに K 上の楕円曲線 $E_i' \subset J_i$ であって $J_i = E_i' + \theta_i^{-1}(N)$, $E_i' \cap \theta_i^{-1}(N)$ は有限, かつ θ_i, ϕ により E と L 上同種 なるものが存在する. そこで

$$A_i' = E_i' \times \varepsilon_i(E_i') \times \cdots \times \varepsilon_{i-1}^{l-1}(E_i'), \quad (1 \leq i \leq l-1)$$

とおくと Galois descent B_i の universality 等により A_i' は B_i と K 上同種であることがわかり

$$\mathrm{rank}B_i(K) = \mathrm{rank}A_i'(K) = l\mathrm{rank}E_i'(K),$$

$$L(B_i, K; s) = L(A_i', K; s) = L(E_i', K; s)^l.$$

よって

$$\mathrm{rank}E(L) = \sum_{i=1}^{l-1} \mathrm{rank}E_i'(K)$$

$$L(E,L;s) \sim \prod_{i=1}^{l-1} L(E'_i,K;s)$$

が成り立つ.

(II) $\varepsilon|_N \neq id_N$ のとき. このときは $\varepsilon|_N$ は N の K 上の位数 l の自己同型であり, よって (1) より

$$\mathrm{rank} N(L) = \sum_{i=0}^{l-1} \mathrm{rank} N_i(K),$$
$$L(N,L;s) \sim \prod_{i=0}^{l-1} L(N_i,K;s)$$

となる. ただし N_i/K は N の χ_i に対応する twist とする.

さらに $N_i \subset J_i$ とみなせて, よって K 上の楕円曲線 $E_i \subset J_i$ であって $J_i = E_i + N_i$, $E_i \cap N_i$ は有限, かつ θ_i, ϕ により E と L 上同種 なるものが存在し, (2) より

$$\mathrm{rank} J_i(K) = \mathrm{rank} N_i(K) + \mathrm{rank} E_i(K),$$

$$L(J_i,K;s) = L(N_i,K;s) L(E_i,K;s)$$

が成り立つ. よって (ii) とともに

$$\begin{aligned} \mathrm{rank} E(L) &= \mathrm{rank} J(L) - \mathrm{rank} N(L) \\ &= \sum (\mathrm{rank} J_i(K) - \mathrm{rank} N_i(K)) \\ &= \sum \mathrm{rank} E_i(K), \end{aligned}$$

$$L(E,L;s) \sim \prod_i L(E_i,K;s)$$

となる. 以上をまとめて次を得る:

Theorem. l を素数とし, K を 1 の l 乗根の群を含む有限次代数体, E/K を楕円曲線とする. l 次 Kummer 拡大 L/K に対し, K 上の楕円曲線 $E_0 = E, E_1, \ldots, E_{l-1}$ であって E と L 上同種 なるものが存在して

$$\mathrm{rank} E(L) = \sum_i \mathrm{rank} E_i(K), \quad L(E,L;s) \sim \prod_i L(E_i,K,s)$$

が成り立つ.

参考文献

[1] T. Honda, Isogenies, rational points and section points of group varieties, Japan. J. Math. **30**(1960), 84-101.

[2] M. Kida, On the rank of an elliptic curve in elementary 2-extensions, Proc. Japan Acad. **69**(1993), 422-425.

[3] —–, Galois dedescent and twists of an abelian variety, Acta Arith. **73**(1995), 51-57.

[4] J. S. Milne, On the arithmetic of abelian varieties, Invent. Math. **17**(1972), 177-190.

[5] —–, Abelian varieties, in: Arithmetic Geometry, G. Cornell and J. H. Silverman (eds.), Springer, 1986, 103-150.

[6] —–, Jacobian varieties, ibid., 167-212.

[7] T. Ono, On the relative Mordell-Weil rank of elliptic quartic curves, J. Math. Soc. Japan **32**(1980), 665-670.

[8] A. Sato, The behavior of Mordell-Weil groups under field extensions, preprint.

[9] A. Weil, Adeles and Algebraic Groups, Birkhäuser, 1982.