数理解析研究所講究録
第 759 巻 1991 年 162-167

楕円曲線の rank について —— いくつかの計算例

名古屋大学教養　中野　伸　(Shin Nakano)

有理数体 Q 上定義された楕円曲線 E に対し、E(Q) をその有理点全体のなす群(Mordell-Weil群)とする. このとき、E/Q の Shafarevich-Tate群 Ш および、2-descent に対する Selmer 群 S_2 というものが定義され

$$(1) \qquad 1 \longrightarrow E(Q)/2E(Q) \longrightarrow S_2 \longrightarrow Ш_2 \longrightarrow 1$$

なる完全系列が成り立つ. ただし $Ш_2$ は Ш の 2-torsion 部分群である.

ここで E の位数２の点（それらは３つある）がどれも有理点でないとすると、そのうちのひとつを Q に添加した体 K は３次体であり、他の点を添加した体と Q 上共役となる. このような場合、以下のようにして S_2 を $K^\times/K^{\times 2}$ の部分群とみなすことができる. まず E(Q) から $K^\times/K^{\times 2}$ への準同型 λ および、局所的な単射準同型 λ_p が定義され、次のような可換図式が成り立つ.

$$\begin{array}{ccc} E(Q) & \xrightarrow{\lambda} & K^\times/K^{\times 2} \\ {\scriptstyle \iota_p}\downarrow & & \downarrow{\scriptstyle \iota_p} \\ E(Q_p) & \xrightarrow[\lambda_p]{} & K_p^\times/K_p^{\times 2}. \end{array}$$

ここで、$K_p = K \otimes Q_p$、また、ι_p は $Q \to Q_p$ から induce される自然な準同型

である．このとき

$$S_2 = \{ a \in K^\times/K^{\times 2} \ ; \ \iota_p(a) \in \mathrm{Im}\,\lambda_p \ \text{for all} \ p \leqq \infty. \}$$

と定義され、(1)の準同型 $E(Q)/2E(Q) \to S_2$ は λ によって実現される．

一方、N を K から Q へのnorm写像とし

$$H_2 = \{ a \in K^\times/K^{\times 2} \ ; \ (a) = A^2 \ \text{for some ideal}\ A \ \text{of}\ K \ \text{and}\ Na > 0. \}$$

の元 a に対して $A^2 = (a)$ なる K の ideal A をとり、その class を対応させることにより、H_2 から K の ideal類群の 2-torsion 部分群 C_2 への全射準同型が定まる．その核 を U_2 とすれば

$$(2) \qquad 1 \longrightarrow U_2 \longrightarrow H_2 \longrightarrow C_2 \longrightarrow 1$$

なる完全系列を得る．ここで U_2 の rank は K の単数群の free-rank (= 1 または 2) に等しい．

ここでは、E(Q)/2E(Q) と C_2 との関係を S_2 および H_2 を経由して調べたことを報告する．

I． 上に述べたように、有理点 P に対して $\lambda(P)$ は $K^\times/K^{\times 2}$ に属する．そこで、もし E(Q)/2E(Q) で独立な有理点の集り {P, Q, R,…} で λ による像が H_2 に含まれるようなものがあれば、C_2 の rank を大きくすることができる．すなわち、大雑把に言って、大きな rank を持つ Q上の楕円曲線、およびその Mordell-Weil群の生成系が与えられれば、それらを使ってideal類群の 2-rank が大きい３次体を構成できることになる．具体的には、そのような無限個の３次体を構成するために、一変数（多変数でも良い）関数体 Q(t) 上の“都合の

良い”楕円曲線を見いだし、その特殊化として Q 上の楕円曲線を作る. これについては本講究録に掲載(予定)の長尾孝一氏の仕事とも関連する.

たとえば、Shioda[6]の例は Q(t) 上の楕円曲線で、その定義方程式、およびMordell-Weil群の生成系が具体的に与えられているので、上の方法を適用し易い. 実際、rank $C_2 \geqq 7$ なる3次体を無数に構成できる. また、Nakata[5]の楕円曲線は三変数関数体上に定義されているが、これを使えば、rank $C_2 \geqq 8$ とすることができる.

II. 純3次体(2項方程式で定義される3次体)で rank $C_2 \geqq 6$ なるものを構成するために、[4]では、曲線 $Y^2=4X^3+D$ の有理点に関する Craig[2]の方法を用いた. Craig は関数体上に7つの有理点を持つような D の作り方を示しているが、純3次体に対してはそのうちの6つしか使えなかった. 実際に、これら7つの点の間に一次関係があることが計算機によって確かめられる. (これは、いくつかの素数 p について modulo p での計算結果から予想することによって得られた.) したがって、純3次体について rank $C_2 \geqq 6$ より良い評価を得ることは、Craig の方法ではできないことになる.

III. 上の2つのトピックスが定量的であるのに対して、以下では定性的な性質、特に S_2 と H_2 の関係について述べよう. まず、S_2 の元は K のほとんどすべての素idealについて偶数のorderを持つことから、S_2 は“ほとんど”H_2 に含まれていると考えられる. もし完全に含まれているならば、(2)の全準

同型 $H_2 \to C_2$ を S_2 に制限して完全系列

$$1 \longrightarrow U_2' \longrightarrow S_2 \longrightarrow C_2' \longrightarrow 1$$

を得る．ここで、U_2'，C_2' はそれぞれ U_2，C_2 の部分群である．これと(1)を並べることにより、S_2 を経由して C_2 と $Ш_2$，$E(Q)/2E(Q)$ の関係がつく．(詳しくは Washington〔7〕，Kawachi & Nakano〔3〕を参照.)

そこで $S_2 \subset H_2$ となるための条件をさがすことが問題となるが、これについてはまず次のような簡単な十分条件がある．

(3)　楕円曲線 E の判別式の素因子は K で分解しない．

たとえば、Washington〔7〕は $m \in Z$ に対して

$$Y^2 = X^3 + mX^2 - (m+3)X + 1$$

で与えられる楕円曲線を扱っているが、そこでは、右辺の多項式の判別式の平方根 m^2+3m+9 が平方因子を持たないことが条件となっている．このとき、その素因子は K で完全分岐する．一方 2 は K で惰性するが、上で与えた楕円曲線の判別式の素因子は 2 を除いて右辺の多項式の判別式の素因子と一致するから、(3)が満たされることになる．

さて、一般に Q 上の素点 p に対して、$K_p = K \otimes Q_p$ は p の上の素点 $\mathfrak{p}$ による K の完備化 $K_{\mathfrak{p}}$ の直和として書ける；$K_p = \bigoplus_{\mathfrak{p}|p} K_{\mathfrak{p}}$．さらにその可逆元全体のなす群は $K_p^\times = \bigoplus_{\mathfrak{p}|p} K_{\mathfrak{p}}^\times$ となるが、特に p が有限のとき、$K_{\mathfrak{p}}$ の単数群 $U_{\mathfrak{p}}$ を用いて $K_p^\times$ の部分群 $U_p = \bigoplus_{\mathfrak{p}|p} U_{\mathfrak{p}}$ が定義される．このとき、次のような完全系列が成り立つ．

$$1 \longrightarrow H_2 \cap S_2 \longrightarrow S_2 \longrightarrow \bigoplus_{p \neq \infty} \mathrm{Im}\,\lambda_p/(U_p K_p^{\times 2}/K_p^{\times 2} \cap \mathrm{Im}\,\lambda_p).$$

したがって、もし

(4)　すべての素数 p に対して $\mathrm{Im}\,\lambda_p \subset U_p K_p^{\times 2}/K_p^{\times 2}$

が満たされるならば、$S_2 \subset H_2$ となる．この条件が有効な例として

$$Y^2 = X^3 - a(X-1)$$

なる楕円曲線を考える．ただし $a = (b^2+27)/4$，b は 3 以上の奇数をとる．このとき、判別式は $\Delta = 2^4(ab)^2$ であるが、b を割る 3 より大きい素数 p は K で分解することがすぐに確かめられるので、条件(3)を使うことはできない．ところで Brumer & Kramer〔1〕によれば、p について non-split multiplicative reduction を持ち、さらに $\mathrm{ord}_p(\Delta) \equiv 0 \pmod 4$ ならば(6)の包含関係が成り立つ．これはさらに、$\left(\frac{2}{p}\right) = -1$ かつ $\mathrm{ord}_p(b)$ が偶数、という条件に書き直すことができる．このように、各素数 p についての reduction を詳しく調べることにより、$S_2 \subset H_2$ となる条件を書き下すことが可能な場合がある．

また、(4)が(3)から導かれることを注意しておく．したがって、上の例から(4)が(3)よりも真に弱い十分条件を与えていることがわかる．

References

〔1〕 A. Brumer and K. Kramer, The rank of elliptic curves, Duke Math. J. 44(1977),715-743.

〔2〕 M. Craig, A construction for irregular discriminants, Osaka J. Math. 14(1977),365-402.

〔3〕 M. Kawachi and S. Nakano, The 2-class groups of cubic fields and the 2-descents on elliptic curves, Preprint series, 1990, no.2, Nagoya Univ., Dept. of Math., College of General Education.

〔4〕 S. Nakano, Construction of pure cubic fields with large 2-class groups, Osaka J. Math. 25(1988),161-170.

〔5〕 K. Nakata, On some elliptic curves defined over Q of free rank ≧ 9, Manus. math. 29(1979), 183-194.

〔6〕 T. Shioda, Construction of elliptic curves over Q(t) with high rank: a preview, Proc Japan Acad. 66A(1990),57-60.

〔7〕 L. C. Washington, Class numbers of the simplest cubic fields, Math. Comp. 48(1987),371-384.