論文の内容の要旨

論文題目

On uniform lower bound of the Galois images associated to elliptic curves

（楕円曲線に伴うガロア表現の像の一様な下界について）

氏名　　新井 啓介

K を代数体、G_K を K の絶対ガロア群、p を素数、E を K 上の楕円曲線とする。E の p-進 Tate 加群 T_pE への G_K の作用が定める表現

$$\rho_{E/K,p} : \mathrm{G}_K \longrightarrow \mathrm{Aut}(T_pE) \cong \mathrm{GL}_2(\mathbb{Z}_p)$$

を考える。もし E が虚数乗法をもたなければ、$\rho_{E/K,p}$ の像はすべての素数 p に対して開であり、有限個の素数 p を除いて、$\rho_{E/K,p} \bmod p$ 及び $\rho_{E/K,p}$ が全射であるという、Serre により証明された定理 ([Se]) がある。そこで、代数体 K と素数 p を固定し、K 上の楕円曲線 E を動かしたときに、$\rho_{E/K,p}$ の像はどう振る舞うかを考える。例えば、K が有理数体 $\mathbb{Q}$ の場合を考える。$p > 163$ ととれば、$\rho_{E/\mathbb{Q},p} \bmod p$ の像が Borel 部分群に入るような楕円曲線 $E/\mathbb{Q}$ は存在しないことを Mazur が示している ([Ma3])。また、Momose の研究 ([Mo]) によれば、$\rho_{E/\mathbb{Q},p} \bmod p$ の像が split Cartan 部分群の正規化群に入るような楕円曲線 $E/\mathbb{Q}$ は虚数乗法をもつだろう、と考えられる。そして私は、固定された代数体 K 上の虚数乗法をもたない楕円曲線 E が定める表現 $\rho_{E/K,p}$ の像は、楕円曲線 E を動かしても下に有界であることを証明した。すなわち、代数体 K と素数 p に依存した自然数 n が存在して、K 上の虚数乗法をもたない任意の楕円曲線に対して、$\rho_{E/K,p}$ の像は $1 + p^n\mathrm{M}_2(\mathbb{Z}_p)$ を含むことを証明した。より詳しく、この n の K と p による具体的な評価を、有限個の j-不変量をもつ楕円曲線を除き決定した。本論文の主定理を述べる。

定理 1 p を素数とする。整数 $n(p)$ を次のように定義する。

$$n(p)=\begin{cases}0 & \text{if } p\geq 23,\\ 1 & \text{if } p=19,\ 17,\ 13,\ 11,\\ 2 & \text{if } p=7,\\ 3 & \text{if } p=5,\\ 5 & \text{if } p=3,\\ 11 & \text{if } p=2.\end{cases}$$

K を代数体とする。このとき p に依存した K の有限部分集合 Σ が定まり、K 上の楕円曲線 E で $j(E)\notin\Sigma$ となるものに対して、$\rho_{E/K,p}$ の像は $(1+p^{n(p)}\mathrm{M}_2(\mathbb{Z}_p))^{\det=1}$ を含む。ここで $1+p^0\mathrm{M}_2(\mathbb{Z}_p):=\mathrm{GL}_2(\mathbb{Z}_p)$ とおいている。

さらに、G_K の p-進円分指標の像が $1+p^r\mathbb{Z}_p$ $(r\geq 0)$ を含むとすれば、K 上の楕円曲線 E で $j(E)\notin\Sigma$ となるものに対して、$\rho_{E/K,p}$ の像は $1+p^{r+n(p)}\mathrm{M}_2(\mathbb{Z}_p)$ を含む。ただし、$p=2$ のときは $r\geq 2$ ととっている。ここで $1+p^0\mathbb{Z}_p:=\mathbb{Z}_p^\times$ とおいている。

定理 1 は、p が 23 以上であれば、

$$\begin{cases}p\not\equiv\pm 3 \bmod 8 \text{ のとき } K\not\supset(\mathbb{Q}(\zeta_p)\text{ の 2 次部分体}),\\ p\equiv\pm 3 \bmod 8 \text{ のとき 体の埋め込み } K\hookrightarrow\mathbb{Q}_p \text{ が存在する}\end{cases}$$

とすれば、[Fa]、[Ma2] により得られる。また p が 17, 19 で K が有理数体のときには、[Fa]、[Ma1]、[Ma2] により得られる。

本論文は 6 つの節より成る。第 1 節、第 2 節で上記の定理 1 を紹介する。第 3 節では楕円曲線を modular curve の有理点と結び付ける。まず K を有限次拡大して、1 の原始 $p^{n(p)+1}$ 乗根を含むとする。楕円曲線 E/K について $\rho_{E/K,p}$ の像が $(1+p^{n(p)}\mathrm{M}_2(\mathbb{Z}_p))^{\det=1}$ を含まなかったとする。このとき、$\mathrm{SL}_2(\mathbb{Z}/p^{n(p)+1}\mathbb{Z})$ の部分群 H で $(1+p^{n(p)}\mathrm{M}_2(\mathbb{Z}/p^{n(p)+1}\mathbb{Z}))^{\det=1}$ を含まないものに対して、$\rho_{E/K,p}(G_K) \bmod p^{n(p)+1}$ は H に含まれる。よって、E/K は H に対応する modular curve X_H の有理点を定める。もし X_H の種数 $g(X_H)$ が 2 以上であれば、Faltings により証明された Mordell 予想 ([Fa]) によって、X_H の有理点は有限個しかないことになる。このような部分群 H は有限個しかないので、$\rho_{E/K,p}$ の像が $(1+p^{n(p)}\mathrm{M}_2(\mathbb{Z}_p))^{\det=1}$ を含まないような楕円曲線 E/K の j-不変量は有限しかないとわかり、定理 1 が従う。

第 4 節以降では、$g(X_H)$ が 2 以上であることを証明する。まず第 4 節で、X_H の種数の評価のための準備をする。$G=\mathrm{SL}_2(\mathbb{Z}/p^{n(p)+1}\mathbb{Z})$, $\sigma=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$, $\tau=\begin{pmatrix}1&1\\-1&0\end{pmatrix}$, $u=\begin{pmatrix}1&1\\0&1\end{pmatrix}$ とおき、また $\alpha=\sigma,\tau,u$ に対して $\mathrm{Conj}(\alpha)$ で α の共役元全体のなす集合を表す。Riemann-Hurwitz の公式により、H が -1 を含めば

$$g(X_H)=1+\frac{1}{12}[G:H](1-3\frac{\sharp H\cap\mathrm{Conj}(\sigma)}{\sharp\mathrm{Conj}(\sigma)}-4\frac{\sharp H\cap\mathrm{Conj}(\tau)}{\sharp\mathrm{Conj}(\tau)}-6\frac{\sharp\langle u\rangle\backslash G/H}{[G:H]})$$

と表される。そこで、$\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ やその極大部分群に含まれる σ,τ,u の共役元の数を計算する。第 5 節では、H の中の σ,τ,u の共役元の数の評価を行う。自然数 $1\leq m<n$ に対して、$f_{n,m}:\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})\longrightarrow$

$\mathrm{SL}_2(\mathbb{Z}/p^m\mathbb{Z})$ を法 p^m 還元とする。もし $n \leq 2m$ であれば、$\alpha = \sigma, \tau, u$ に対して $\alpha^{-1}(f_{n,m}^{-1}(\alpha) \cap \mathrm{Conj}(\alpha))$ は階数 2 の自由 $\mathbb{Z}/p^{n-m}\mathbb{Z}$ 加群になる。このことと H が $(1+p^{n(p)}\mathrm{M}_2(\mathbb{Z}/p^{n(p)+1}\mathbb{Z}))^{\det=1}$ を含まないことを組み合わせて、H の中の σ, τ, u の共役元の数を上からおさえる。第 6 節では、第 4 節、第 5 節の結果を用いて $g(X_H)$ が 2 以上であることを証明する。

最後になるが、指導教官の斎藤毅教授には、論文の構成の手直しや命題の改善等のご指導、及び執筆に際しての激励をいただき、心より感謝する。

参考文献

[Fa] G. Faltings, *Finiteness theorems for abelian varieties over number fields*, Translated from the German original [Invent. Math. 73 (1983), no. 3, 349-366; ibid. 75 (1984), no. 2, 381] by Edward Shipz. Arithmetic geometry (Storrs, Conn., 1984), 9-27, Springer, New York (1986).

[Ma1] B. Mazur, *Modular curves and the Eisenstein ideal*, I.H.E.S. Publ. Math. No. 47 (1977), 33-186.

[Ma2] B. Mazur, *Rational points on modular curves*, Modular functions of one variable V, Lecture Notes in Math., Vol. 601, Springer, Berlin (1977), 107-148.

[Ma3] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. 44 (1978), no. 2, 129-162.

[Mo] F. Momose, *Rational points on the modular curves* $X_{\mathrm{split}}(p)$, Compositio Math. 52 (1984), no. 1, 115–137.

[Se] J.-P. Serre, *Abelian l-adic representations and elliptic curves*, Lecture at McGill University, New York-Amsterdam, W. A. Benjamin Inc. (1968).