虚数乗法と Lubin Tate 理論

志賀明日香 otheiio323.com@gmail.com

2022 年　9/7

1　概要

Rubin の "Tate shafarevich group of elliptic curves with complex multiplication"(1987) に記載されている lem 3 (ここでは定理 1) について、本文と引用先では sketch のみが与えられていた. 本稿では定理 1 の Lubin Tate 拡大のガロア群を埋め込む方法による詳しい証明をまとめる.

定理 1　K：虚二次体, O_K を K の整数環, E/K を K で虚数乗法を持つ楕円曲線とする. さらに, p は K の素イデアルで E は p で良い還元を持つとする. この時, $K(E[p])/K$ は $O_K/p-1$ 次のアーベル拡大であり, p において完全分岐である.

注意 1　上記の設定のもと,K の類数は自動的に 1 である. 実際、E は K 上定義されていることから E の j 不変量 $j(E)$ は K の元であり, 虚数乗法論から $Cl(K) \cong Gal(K(j(E))/K)$ であるから $Cl(K)$ は自明.

証明においては、次の補題を用いる.

補題 1　上の定理の設定のもとで, 楕円曲線の形式群 $\hat{E}$ は K_p(K の p における完備化) のある素元 π についての Lubin Tate の形式群である.

2　補題 1 の略証

素元 π として何を取るかがポイントである.

ψ を E/K の量指標とし, $\pi = \psi(p)$ と取ると, $\pi \in R_K$ であり, π は K_p の素元である ($\because h$ を ψ の導手 f を法とする ray 類群の位数とすると, $p^h = (\alpha)$ があ

る $\alpha \equiv 1 mod f \in K^{\times}$ について成り立ち, $\psi(p)^h = \psi(p^h) = \psi((\alpha)) = \alpha$ であるから $p = (\pi)$ であり, π は素元).$[\pi] \in EndE$ に対応する $[\pi](t) \in End\hat{E}$ は $mod\pi$ で $[\pi]$ は q 乗 Frobenius に還元する ("Advanced topics in the arithmetic of elliptic curves",prop 10.4) ので, $[\pi]((x,y)) = (\phi_1(x,y), \phi_2(x,y))$ となるとすると, $[\pi](t) = -\phi_1(x(t),y(t))/\phi_2(x(t),y(t)) \equiv -x(t)^q/y(t)^q \equiv t^q mod\pi$($q$ は K_p の剰余体の位数) である.

また、ω_E を E の不変微分として,$[\pi]^* \omega_E = \pi\omega_E$ であるように同型 $O_K \cong End(E)$ は固定されているので, 形式群について $[\pi]^* \hat{\omega}_E = \pi\hat{\omega}_E$ が成り立ち, 両辺を積分することで $[\pi](t) = \pi t +$(2 次以上) が成り立つことがわかる.

以上より $[\pi](t)$ は Frobenius の準同型であり, 対応する $\hat{E}$ は Lubin Tate の形式群. □

例 1 $E/\mathbb{Q}$: $y^2 = x^3 + x$ は $\mathbb{Z}[\sqrt{-1}]$ において虚数乗法を持つ. 判別式は -64 なので, 7 において E は良い還元を持つ. $\sharp E(\mathbb{F}_7) = 8$ より $E/\mathbb{F}_7$ は supersingular であるから、$\hat{E}$ の高さは 2 なので、$[7](t) mod 7$ は t^{49} の冪級数で書け, $[7](t)$ は t^{49}の項まではmod7で 0 になる. コンピューターによるt^{49} の係数は 661609619065682693232195492602970112 であり,7 で割ると 6 余り, $[7](t) \equiv 6t^{49} mod 7$. よって $[-7](t) = -7t + ... + 661609619065682693232195492602970112t^{49} + ...$ は mod7 で $[-7](t) \equiv t^{49} mod 7$ を満たし、素元 -7 についての Lubin Tate の形式群となる。このことはコンピューターを用いなくとも,$\tilde{[7]} = Fr_7 \cdot \hat{Fr}_7 = Fr_7 \cdot (-Fr_7) = -Fr_{49}$ としてもわかる。なお, $\hat{Fr}_7$ は 7 倍フロベニウス写像の dual isogeny であり,2 つ目の＝は E が mod7 で supersingular であることから $Fr_7 + \hat{Fr}_7 = [7 + 1 - \sharp E[\mathbb{F}_7]] = 0$ よりわかる.

例 2 例 1 の $E/\mathbb{Q}$ は $(1 + 2\sqrt{-1})$ で良い還元を持つ. $[1 + \tilde{2}\sqrt{-1}]^* \tilde{\omega}_E = (1 + \tilde{2}\sqrt{-1})\tilde{\omega}_E = (1 + 2 \cdot 2)\tilde{\omega}_E = 5\tilde{\omega}_E = 0$ より, $[1 + 2\sqrt{-1}]$ は非分離であり, 射の次数は 5 だから純非分離である. よって $\hat{E}$ は $1 + 2\sqrt{-1}$ の $Aut(\mathbb{Z}[\sqrt{-1}]) = \pm 1, \pm i$ 倍の４つのいずれかについての Lubin Tate の形式群となる. ４つのうちのどれになるかは, dual と自身を足して $5 + 1 - \sharp E[F_5] = 2$ 倍写像になることから,$[1 + 2\sqrt{-1}]$ であることがわかる.

3　補題 1 から定理 1 を導く

$L = K(E[p])$ とし,P を p の上にある素イデアルとする. $Gal(L_P/K_p)$ から $Gal(L/K)$ への制限 $\sigma|_L$ は単射である ($\because LK_P$ は完備だから $LK_P = L_p$ であり,$\sigma|_L = id$ とすると, σ は L と K_p の元を動かさないので,$LK_P = L_P$ を動かさない. よって $\sigma = id_P$). $Gal(K_P(E_1[\psi((p)])/K_p) \cong Gal(L_P/K_p) \hookrightarrow Gal(L/K)$ という図式が得られる (左端の同型は,$Gal(K_P(E[\psi((p)])/K_p)$ から $Gal(K_P(E_1[\psi((p)])/K_p)$ への単射があり, さらに $reduction$ の ker がGal($K_P(E_1[\psi((p)])/K_p$) となるような剰余体のガロア群への全射があることから言える). 左端のガロア群はGal($K_P(\hat{E}[\psi((p)])/K_p$) に同型である. そして Lubin Tate 拡大の性質 (Neukirhi Theorem 5.4,Schneider Prop.1.3.12) より,$Gal(K_P(\hat{E}[\psi((p))])/K_p) \cong (O_K/p)^\times$.

また, $Gal(L/K) \hookrightarrow Aut(E[p]) = Aut_{R_K}(R_K/I) = (O_K/p)^\times$ であるから L/K はアーベル拡大である.

位数が全て等しいので包含は全て同型であり、$Gal(L/K) \cong (O_K/p)^\times$. よって $[L : K] = O_K/p - 1$.

さらに, $Gal(L/K)$ は p の上にある素イデアル全体の集合に推移的に作用するので軌道固定群定理より, D_P を $Gal(L/K)$ の分解群とすると $\sharp D_P = [L : K]/(p$ の上にある素イデアルの個数) である.$D_P \cong Gal(L_P/K_p)(\because \sigma \in Gal(L/K)$ に対し, $\sigma \in Gal(L_P/K_p) \Leftrightarrow \sigma|_{K_p} = id \Leftrightarrow \sigma(P) = P)$ に注意すると (K の上にある素イデアルの個数)$= 1$ であるから, L_P/K_p は完全分岐拡大であることと合わせて, L/K も完全分岐拡大である. □

注意 2　Lubin Tate 理論と関係のある形式群はもっぱら形式乗法群で, 形式加法群や楕円曲線の形式群は無関係だと思っていたが, 楕円曲線の形式群も虚数乗法を持つときは Lubin Tate である. 最初勘違いしていたのだが、例 1 で述べたように安直に基礎体の素元についての Lubin-Tate 形式群になるわけではなく, 虚数乗法の主定理を使って定義される楕円曲線に付随する量指標による素イデアルの像についての Lubin Tate となるところに虚数乗法論と Lubin Tate 理論の接点が感じられる. $Gal(L/K)$ を調べるときに, 今回は Local な方が Lubin Tate 拡大になっていてよくわかるので, 対応する Local なガロア群 (分解群と同型) を埋め込むことでガロア群がわかるとともに完全分岐であることも判明するという流れであった.

4 参考文献

[1]K.Rubin "Tate shafarevich group of elliptic curves with complex multiplication"

[2]Ph.Cassou M.J.Taylor "Elliptic functions and rings of integers"

[3]J.H.Silverman "Advanced topics in the arithmetic of elliptic curves"

[4]Neukirhi "Albebraic number theory"