数理解析研究所講究録
第721巻 1990年 80-86

楕円曲線の等分点の体について

大阪大学 理学部 山本芳彦

0. Introduction.

E を代数体 k 上定義された elliptic curve (= abelian variety of dimension 1) とする. ℓ を素数として E の ℓ 等分点全体を $E[\ell]$, k に $E[\ell]$ の座標全体をつけ加えてできる体を K とすると K / k は galois 拡大で,その galois 群を G とかく. $E[\ell]$ は $Z/\ell Z$ 上 rank 2 の free module で G の各元がその自己同型を引き起こすことより G の忠実な表現

$$\rho : G \to GL(E[\ell]) = GL(2, Z/\ell Z)$$

が得られる. E が虚数乗法をもつときには K / k は本質的には abel 拡大であって虚数乗法論によって, 像 $\rho(G)$ はもちろん K / k の整数論的性質は詳しく調べられている. E が虚数乗法をもたないときには, K / k は一般には non-solvable な GL(2)-拡大であって, その整数論的な性質についてはあまりよく知られていない. ここでは, K を生成する方程式の具体的な構成について考える.

以下で紹介する公式は本質的には古典的な保形関数論のなかで得られているものであるが, 実際に計算するとなると困難であることが多い. 最近, computer による数式処理system が使いやすくなって, 以前なら非常に複雑で技巧的なプログラムを必要とした計算が容易に短時間でできるようになった. ここでは, REDUCE を使用してできたいくつかの計算結果を紹介する.

1. K / k の中間体

E は虚数乗法をもたないとする. このとき, 有限個の例外の ℓ を除いて, $\rho(G) = GL(2, Z/\ell Z)$ であることが知られている([Se]).

以下では簡単のために, $k = Q$ かつ $\rho(G) = GL(2, Z/\ell Z)$ と仮定し, そのとき, $GL(2, Z/\ell Z)$ の各部分群に対応する中間体を次のように表す.

部分群	体
1	$K = Q(x(P), y(P);\ P \in E[\ell])$
$\{\pm 1\}$	$K' = Q(x(P);\ P \in E[\ell])$
$(Z/\ell Z)^*$	$M = Q(w(P);\ P \in E[\ell])$
$SL(2, Z/\ell Z)$	$F = Q(\zeta)$ $(\zeta = 1$ の原始 ℓ-乗根$)$
$GL^+(2, Z/\ell Z)$	$F^+ = Q(\sqrt{m})$ $(m = \pm\ell \equiv 1 \pmod 4)$
$GL(2, Z/\ell Z)$	$k = Q$

ここで，$x(P)$, $y(P)$ はそれぞれ $P \in E$ の x- 座標，y- 座標を表し，

$$GL^+(2, Z/\ell Z) = \{A \in GL(2, Z/\ell Z);\ \det A \in (Z/\ell Z)^{*2}\},$$
$$w(P) = (x(P) + x(2P) + \cdots + x(((\ell - 1)/2)P)$$

とする．

$\ell \geqq 5$ のとき，$SL(2, Z/\ell Z)/\{\pm 1\}$ は非可換単純群であることより 体拡大 $K'/Q(\zeta)$がもっとも興味深い部分である．以下では，この体について考える．

体 K' は invariant $j = j(E)$ のみで定まることは容易にわかる．従って，

$$E:\ Y^2 = 4X^3 - aX - a \qquad (j = 1728a/(a-27),\ j \neq 0, 1728)$$

とおいてよい．$\ell > 2$ のとき，E の点 P について，$Q = ((\ell - 1)/2)P$, $Q' = ((\ell + 1)/2)P$ とおくと，$x(Q)$, $x(Q')$ はともに $x(P)$ の有理式であって，

$$P \in E[\ell] \Leftrightarrow Q = -Q' \Leftrightarrow x(Q) = x(Q')$$

より，分母を払って $X = 2x(P)$ と置きなおして，ℓ-等分方程式

$$f_\ell(X) = 0$$

を得る．このとき，K' は $f_\ell(X)$ の最小分解体として定まる．たとえば，

$\ell = 2$ $f_2(X) = 4X^3 - aX - a$

$$\ell = 3 \quad f3(X) = 3X^{4} - 6aX^{2} - 24aX^{2} - a$$

$$\ell = 5 \quad f5(X) = 5X^{12} - 62aX^{10} - 760aX^{9} - 105a^{2}X^{8} + 480a^{2}X^{7} + 60a^{2}(5a - 16)X^{6}$$
$$+ 1392a^{3}X^{5} - 5a^{3}(25a - 1536)X^{3} - 160a^{4}(a - 80)X^{3}$$
$$+ 10a^{4}(5a - 96)X^{4} + 8a^{4}(25a - 640)X^{2} + a^{4}(a^{2} + 128a - 4096)$$

$\ell = 7$

$$f7(X) = 7X^{24} - 308aX^{22} - 7888aX^{21} - 2954a^{2}X^{20} - 224a^{2}X^{19} + 28a^{2}(709a - 6128)X^{18}$$
$$+ 185136a^{3}X^{17} - 7a^{3}(5033a - 326784)X^{16} - 896a^{3}(71a - 7408)X^{15}$$
$$+ 8a^{4}(10283a - 307680)X^{14} + 19040a^{4}(17a - 896)X^{13} - 28a^{4}(3997a^{2}$$
$$- 42496a + 530432)X^{12} - 448a^{5}(2715a - 46496)X^{11} + 56a^{5}(753a^{2}$$
$$- 85200a + 941056)X^{10} + 224a^{2}(3801a^{3} - 133120a^{2} + 222208)X^{9}$$
$$+ 7a^{6}(2239a^{2} + 475392a - 16158720)X^{8} - 128a^{2}(841a^{6} - 82160a^{3}$$
$$+ 1781760)X^{7} - 28a^{6}(527a^{3} + 27200a^{2} - 1310720a + 6422528)X^{6}$$

$$- 112a^{7}(1023a^{2} + 12032a - 1056768)X^{5} + 14a^{7}(93a^{3} - 38400a^{2} + 450560a$$

$$+ 13893632)X^{4} + 224a^{7}(15a^{3} - 5440a^{2} + 118784a + 458752)X^{3}$$

$$- 28a^{8}(7a^{3} - 528a^{2} + 55296a - 1245184)X^{2} - 112a^{8}(7a^{3} - 512a^{2} + 18432a$$

$$- 262144)X - a^{8}(a^{4} + 640a^{3} - 53248a^{2} + 1572864a - 16777216)$$

$\ell = 11$

$$f11(X) = 11X^{60} - 2794aX^{58} - 185768aX^{57} - 207691a^{2}X^{56} - 2332576a^{2}X^{55}$$

$$+ 44a^{2}(115749a^{2} - 1677968)X^{54} + 137416752a^{3}X^{53}$$

$$- (52次\ から\ 1次の項\ まで\ 省略\ ) - a^{20}(a^{10} + 4480a^{9} - 1208320a^{8}$$

$$+ 244318208a^{7} - 23035117568a^{6} + 1022202216448a^{5} - 17386027614208a^{4}$$

$$- 219902325555200a^{3} + 14073748835532800a^{2} - 216172782123783808a$$

$$+ 1152921504606846976)$$

奇素数 ℓ については,

$$\deg(f_\ell) = (\ell^2 - 1)/2$$

$$[K' : Q] = \ell(\ell^2 - 1)(\ell^2 + 1)/2$$

が成り立つ.

2. K, K' における素イデアルの分解

素数 p の K / k における分解の様子を調べることは non-solvable galois 拡大に対する 相互法則 の一般化の可能性を秘める対象として多くの研究者の注目するところである.

E が mod p に関して good reduction を持つとき, その GF(p)-有理点の個数を $1 - a(p) + p$ とおいて, $a(p)$ を定める. p が $\ell\Delta(E)$ を割り切らないとき p は galois 拡大 K / k で不分岐である. このとき p の Frobenius 置換を $\sigma(p)$ とすると,

$$\det(t1 - \rho(\sigma(p))) \equiv t^2 - a(p)t + p \pmod{\ell}$$

が成り立つ(cf. [Sh]). これより, p が K / k で完全分解するなら

$$p \equiv 1, \quad a(p) \equiv 2 \pmod{\ell}$$

が成り立つ.残念ながら, $a(p)$ だけで, p が K で完全分解する十分条件を与えることはできていない. また, $a(p)$ を知ることもむずかしい問題である.

$p \mid \ell\Delta$ のときは,一般に p は分岐する. 分岐の様子については [Se] にあるが, 詳しいことはわかっていない.

一般に, galois 拡大 L / k が k 上の 既約多項式 $f(X)$ の最小分解体として定義されているとき, k の素イデアル p の L における分解の様子は, p が f の判別式 $D(f)$ と互いに素な限り, p の剰余体 における $f(X)$ の既約分解により定まる. $p \mid D(f)$ のときも, f を用いて分岐の様子がわかる.

特に L / k が abel 拡大の時には

$$[L : k] = \deg f$$

が成り立つ．それに対して，galois 群が non-abelian のときには，deg f は拡大次数 [L : k] に比べてかなり小さくとれる．たとえば，Gal(L/k) が n 次対称群 Sn なら，拡大次数 n! に対して deg f = n ととれる．このときには，相互法則 はともかく，与えられた素数 p が完全分解するかどうかは，f を mod p で見るとき完全分解するかどうかと同じだから容易に確かめられる．

L = K' の場合，

$$[K' : Q] / \deg f_\ell = \ell (\ell - 1)$$

であるが，ℓ -等分方程式 f_ℓ の次数はまだかなり大きい．1. において，

$$K' = M(\xi) = M \cdot F, \quad F^+ = M \cap F$$
$$Gal(K'/F) = Gal(M/F^+) = PSL(2, Z/\ell Z)$$

に注目すると，p の K' における分解は，p の M における分解さえわかればよい．w(P) は定義より，点 P の生成する位数 ℓ の部分群のみで定まるから，k 上 ℓ +1 次の元であり，その定義方程式を

$$g_\ell (X) = 0$$

とすると，$g_\ell (X)$ は w(P) の x(P) による表示と等分方程式 $f_\ell (X) = 0$ から求めることができる．

実際，

$$w(P) = r(X)/s(X), \quad (r, s \in Z[X])$$
$$\gcd(s(X), f_\ell (X)) = 1$$

より

$$s(X)t(X) + f(X)u(X) = 1, \quad (t, u \in Q[X])$$

を満たす s, t を見つけると

$$w(P) = r(X)t(X) \in Q[X]$$

と書ける．K' = Q[X] は Q上の 有限次元 vector space だから w(P) のみたす方程式が計算できる．

しかし，この一連の計算の実行は容易ではない．ここに，数式処理システムをうまく使うことが必要となる．

$\ell = 3$ のときは，g3(X) = f3(X) となりつまらないが，$\ell = 5, 7$ のときには次のようになる．

$$g5(X) = X^6 - 5aX^4 - 40aX^3 - 5a^2X^2 - 8a^2X - 5a^2$$

$$D(g5) = -2^6 3^6 5^5 a^{10} (a - 27)^4$$

$$g7(X) = X^8 - 84aX^6 - 3024aX^5 - 1890a^2X^4 - 18144a^2X^3 - 28a^2(23a + 3024)X^2 - 11664a^3X - 567a^4$$

$$D(g7) = -2^{64} 3^{16} 7^7 a^{20} (a - 27)^6 (2809a - 84035)^2$$

<References>

[Se]:

J.-P. Serre, Proprietes galoisiennes des points d'ordre fini des courbes elliptiques, Inv. Math. 15(1972), 259-331.

[Sh]:

G. Shimura, A reciprocity law in non-solvable extensions, J. fur reine u anwew. Mathematik, Band 221(1966),209-220.