数理解析研究所講究録
1154巻 2000年 137-143

代数体の最大Abel拡大上の不分岐Galois拡大の構成について

北大 理　　大溪幸子 (Sachiko Ohtani)

本稿では，代数体の最大Abel拡大上の不分岐Galois拡大の構成について，特にAbel多様体の等分点を用いたものについて述べる．第1章では今まで知られている結果を簡単に紹介し，問題の背景について述べる．第2章ではある種の半安定なAbel多様体の等分点を用いた構成について述べる．最後に第3章では特に有理数体$\mathbb{Q}$上の具体的な楕円曲線を用いた構成について述べる．

講演後，防衛大の山村健先生と学習院大の中野伸先生に大変貴重なアドバイスをいただきました．この場を借りて厚く御礼を申し上げたいと思います．

1 序

まず次のような問題がある．

問題1. 与えられた代数体Kに対し，K上の不分岐Galois拡大を構成せよ．

しかしK上では一般に困難なため，ここではその最大Abel拡大K^{ab}上で構成することを考える．

問題1′. 与えられた代数体Kに対し，K^{ab}上の不分岐Galois拡大を構成せよ．

例えば，K^{ab}上の不分岐Abel拡大については多くの人々が研究していて，Cornel [4]，Brumer [3], Kurihara [9] などの論文がある．またK^{ab}上の最大不分岐可解拡大のGalois群の構造については，Uchida [15]や，それを一般化したHorie [8]がある．そしてK^{ab}上の不分岐非可解拡大について，Asada [1]，[2]がある．これら2つの論文では，有理数体$\mathbb{Q}$上のある楕円曲線の等分点を用いてその体を構成している．それらの主結果の一部をここで紹介する．

定理A-1 (Asada [2], Theorem 3). pを5以上の有理素数とし，rを正整数とする．このとき，$\mathbb{Q}^{\mathrm{ab}}$上線形独立な不分岐Galois拡大で，$\mathbb{Q}^{\mathrm{ab}}$上のGalois群として$PSL_2(\mathbb{Z}/p^r\mathbb{Z})$を持つようなものが無限個存在する．

註．ここでの“線形独立”は“linearly disjoint”の意で用いられている (cf. Asada [2])．以後この語を同様の意味で用いる．

この定理の証明に用いられた楕円曲線の j-不変量は次の式で与えられている:

$$j(n) = -\frac{1}{(\varepsilon p)^{3n}}\{(1-3(\varepsilon p)^n)(1+3^2(\varepsilon p)^n)\}^3, \qquad \varepsilon = \left(\frac{-1}{p}\right).$$

ここで n は

$$p^r \mid n, \quad n : \text{odd} \quad (p=5 \text{のときは}, n \equiv 11 \pmod{16})$$

を満たす正整数とする. このような n の列 $\{n_\alpha\}_{\alpha\geq 1}$ をとり, それらから定まる $j(n_\alpha)$ を j-不変量に持つような $\mathbb{Q}$ 上の楕円曲線 $E^{(\alpha)}$ が定義される. そこで定理の体は, この $E^{(\alpha)}$ の p^r 等分点の x 座標を $\mathbb{Q}^{\mathrm{ab}}$ に添加した体として得られる.

また至る所 potential good reduction を持ち, その supersingular prime p ($\neq 2,3$) で good reduction を持つような $\mathbb{Q}$ 上の楕円曲線 E に関しても次のような結果が与えられている.

定理 A-2 (Asada [1], Theorem 3). E, p を上記のものとし, k を p がそこで惰性するような二次体, さらに K を $E \otimes_{\mathbb{Q}} K$ が至る所 good reduction を持つような有限次代数体とする. このとき $F = Kk$ とおくと, $F(E[p^\infty])/F^{\mathrm{ab}}$ は不分岐 Galois 拡大になる. ここで $F(E[p^\infty])$ は F に E の p 冪等分点を全て添加した体とする.

註. この定理の E と F の例が Asada [2] で与えられている. その曲線を用いて得られた拡大が $SL_2(\mathbb{Z}_p)$-拡大となることも示されている.

定理 A-1 で用いられた楕円曲線の族は非常に特殊に見え, 定理 A-2 の族は至る所 potential good reduction を持つ. そこで次のようなことに興味を持った.

> より一般的な楕円曲線の族, さらには Abel 多様体の等分点を用いるとどのような状況が起こるであろうか?

一般的な状況を考えた分, 基礎体は大きくなったものの, いくつかのことが分かった. 以後の章で, Abel 多様体の等分点を用いた不分岐 Galois 拡大 (非可解なものを含む) の構成を与える.

2 Abel 多様体の等分点を用いた構成

A を代数体 K 上至る所半安定な Abel 多様体とし, ある 5 以上の素数 p で A は bad reduction を持つとする. また $\mathcal{A}$ を K の付値 v での Néron Model, $\mathcal{A}_v^0$

を $\mathcal{A}$ の special fibre の単位元を含む連結成分とする．このような A/K にいくつか仮定をつけることで，次のように不分岐 Galois 拡大を構成できる．

定理 1. F を K に A の p 冪等分点を全て添加した体とすると，次の $(a), (b)$ が成り立つ．
(a) A が bad reduction を持つような K の全ての付値 v に対し，上記の $\mathcal{A}_v^0$ が split torus となるなら，$FK(\zeta_{p^\infty})^{\mathrm{ab}}$ は $K(\zeta_{p^\infty})^{\mathrm{ab}}$ 上不分岐 Galois 拡大になる．ここで $K(\zeta_{p^\infty})$ は K に 1 の p 冪乗根を全て添加した体とする．
(b) p を割る K の全ての付値 v に対し，$\mathcal{A}_v^0$ が split torus となるなら，$F(K\mathbb{Q}^{\mathrm{ab}})^{\mathrm{ab}}$ は $(K\mathbb{Q}^{\mathrm{ab}})^{\mathrm{ab}}$ 上不分岐 Galois 拡大になる．

証明. まず代数体の最大 Abel 拡大上の不分岐 Galois 拡大を構成するのに重要な，Ihara による補題を述べる．

補題 I (Asada [1], Proposition 1). k を代数体，K を k 上有限次 Galois 拡大とする．このとき次の 2 条件は同値．
(i) Kk^{ab} が k^{ab} 上不分岐．
(ii) K の全ての素因子に対し，その K/k における分解群が可換．

ここで r を任意の正整数とし，F_r を K に A の p^r 等分点を添加した体とする．この補題により定理を示すには，K の全ての非アルキメデス付値 v に対し，(a) では $F_rK_v(\zeta_{p^r})/K_v(\zeta_{p^r})$ が Abel 拡大であること，(b) では $F_rK_v\mathbb{Q}^{\mathrm{ab}}/K_v\mathbb{Q}^{\mathrm{ab}}$ が Abel 拡大であることが示されればよいことがわかる．そこで A の各付値における reduction の様子で場合分けをする．

v が good な付値である場合．このとき“Criterion of Néron-Ogg-Shafarevich” (Serre-Tate [14], Theorem 1，以下 (NOS)) より，絶対惰性群が A の p 進 Tate module に自明に作用するので，F_rK_v/K_v は不分岐，特に Abel 拡大である．

v が bad な付値である場合．まず $v \mid p$ のとき，定理の仮定より $(a),(b)$ いずれの場合も $\mathcal{A}_v^0$ が split torus となるので，Faltings-Chai [5] による“Mumford's Construction”を用いると，次を得る．

$$F_rK_v \simeq K_v\left(\zeta_{p^r}, \{q_{ij}^{1/p^r}\}_{1\le i,j\le \dim A}\right),$$

ここで q_{ij} たちはある K_v^* の元．これより，$F_rK_v/K_v(\zeta_{p^r})$ が Abel 拡大となることがわかる．

最後に $v \nmid p$ なる bad な付値の場合．(a) では $\mathcal{A}_v^0$ が split torus となるので上と同様．(b) では v が半安定であるということから，“Galois criterion of semi-stable reduction”の系 (Grothendieck [7], Proposition 3.5, Corollary 3.5.2) を適用すれば，$F_rK_v^{\mathrm{nr}}/K_v^{\mathrm{nr}}$ が Abel 拡大となることがわかる．ここで，K_v^{nr} は K_v の最大不分岐拡大とする．以上のことをまとめると定理を得る． □

例. level p の modular 曲線を $X_0(p)$ とし，その Jacobian を J とすると，J は p の外 good reduction を持つような Abel 多様体であり，Mazur [11], Appendix, Theorem (A.1) より，ある $\mathbb{Q}$ 上の有限次 Galois 拡大 K が存在して，J/K は定理 1 (a) の仮定を満たす．

3 楕円曲線の等分点を用いた構成

整でない j-不変量を持つ楕円曲線は定理 1 の仮定を満たす 1 つの例だが，$\mathbb{Q}$ 上の具体的な楕円曲線を用いると，不分岐性だけでなく Galois 群を決定することもできる．

定理 2. p を 5 以上の有理素数とすると，$\mathbb{Q}(\zeta_{p^\infty})^{\mathrm{ab}}$ 上線形独立な不分岐 Galois 拡大で，$\mathbb{Q}(\zeta_{p^\infty})^{\mathrm{ab}}$ 上の Galois 群として $SL_2(\mathbb{Z}_p)$ を持つようなものが無限個存在する．

註. この定理では，定理 A-1 で構成した体とは異なる体を構成している．

証明. この定理の証明では次のような楕円曲線を用いる:

$$E^{(n)} : y^2 = x(x-p)(x+p_n).$$

ここで p_n は p と異なる 5 以上の素数で，この曲線の j-不変量と導手は次のようになっている:

$$j(E^{(n)}) = 2^8 \frac{(p^2+pp_n+p_n^2)^3}{p^2p_n^2(p+p_n)^2}, \qquad \mathrm{cond}(E^{(n)}) = \mathrm{rad}(pp_n(p+p_n)).$$

この曲線は Frey 曲線であり，至る所半安定であることが知られている (cf. Serre [13], §4). そこで適当な素数列 $\{p_n\}_{n\geq 1}$ をとり，それらから $\mathbb{Q}$ 上の楕円曲線 $E^{(n)}$ を定義する．定理の体は，この $E^{(n)}$ の p 冪等分点を $\mathbb{Q}(\zeta_{p^\infty})^{\mathrm{ab}}$ に全て添加した体として得られる．

では証明について述べる．以後，r を任意の正整数とし，$F_r^{(n)}$ を $\mathbb{Q}$ に $E^{(n)}$ の p^r 等分点を添加した体とする．

（不分岐性）

定理 A-1 と同様に補題 I を用いて，全ての素数 l に対し，$F_r^{(n)}\mathbb{Q}_l(\zeta_{p^r})/\mathbb{Q}_l(\zeta_{p^r})$ が Abel 拡大であることが示されればよい．l が good prime なら (NOS) より定理 A-1 と同様．l が bad prime なら，“Tate's theory” (cf. Lang [10], Serre [12]) より，$F_r^{(n)}\mathbb{Q}_l(\zeta_{p^r})/\mathbb{Q}_l(\zeta_{p^r})$ は Abel 拡大となることがわかる．

註. 定理 A-1 で用いた " Mumford's Construction " は " Tate's theory " の一般化である.

（Galois 群の決定）

$\mathbb{Q}$ に $E^{(n)}$ の p 等分点を添加した体 $F_1^{(n)}$ の $\mathbb{Q}$ 上の Galois 群が $GL_2(\mathbb{Z}/p\mathbb{Z})$ となること，すなわち p 進表現

$$\rho_p \ : \ \mathrm{Gal}\,(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}\,(E[p]) \cong GL_2(\mathbb{Z}/p\mathbb{Z})$$

が全射であることを示す. これが示されれば，$k = \mathbb{Q}(\zeta_{p^\infty})$ とおくと，

$$\mathrm{Gal}\,(F_1^{(n)}k^{\mathrm{ab}}/k^{\mathrm{ab}}) \cong SL_2(\mathbb{Z}/p\mathbb{Z})$$

となるので，Serre による補題 (Serre [12], Ch.IV, 3.4, Lemma 3) より結果を得る.

実際に ρ_p が全射となることは，Serre [12], Ch.IV, 3.2, Lemma 2 より，次の 3 条件が成り立っていることを確かめれば示される:

(i) $\det G_p = (\mathbb{Z}/p\mathbb{Z})^*$. ここで $G_p = \mathrm{Im}\ \rho_p$ とおく.

(ii) G_p は，$E[p]$ の適当な基底に関して，$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ を含む.

(iii) $E[p]$ は G_p-加群として既約.

条件 (i) は，$F_1^{(n)}$ が ζ_p を含むことより成り立つ. 条件 (ii) も，Serre [12], Ch.IV, 3.2, Lemma 1 より成り立つ. 最後に条件 (iii) についても Serre [13], §4, Proposition 6 より成り立つ.

註. この証明の今までのことはもう少し一般的な形で証明できる.

（線形独立性）

p と異なる 5 以上の素数 p_1 をとり，p_2 を $E^{(2)}$ が p_1 で good reduction を持つようにとる. この条件は，$p_1 \nmid (p+p_2)$ ということと同値であり，このような素数 p_2 は無限個存在することが，Dirichlet の算術級数定理からわかる. このとき，

$$F_1^{(1)} \cap F_1^{(2)} = \mathbb{Q}(\zeta_p) \qquad (*)$$

となることを示す. これが示されれば，上記の Serre による補題より，

$$F_1^{(1)}k^{\mathrm{ab}} \cap F_1^{(2)}k^{\mathrm{ab}} = k^{\mathrm{ab}}$$

となり. 後は帰納的に p_n の列をとることにより定理を得る.

(*) が成り立つことだが，p_1 は $F_1^{(2)}$ で不分岐で，$F_1^{(1)}$ では分岐するので，まず $F_1^{(1)} \neq F_1^{(2)}$ がわかる. 先の結果より，

$$\mathrm{Gal}\,(F_1^{(i)}/\mathbb{Q}(\zeta_p)) \cong SL_2(\mathbb{Z}/p\mathbb{Z}) \qquad (i = 1, 2)$$

だったので，$SL_2(\mathbb{Z}/p\mathbb{Z})$ の正規部分群 $\{\pm 1\}$ に対応する $F_1^{(i)}/\mathbb{Q}(\zeta_p)$ の部分体を $F_1'^{(i)}$ とすると，$F_1^{(1)}\mathbb{Q}_{p_1}/\mathbb{Q}_{p_1}$ の分岐指数が2よりも大きくなることから，$F_1'^{(1)} \neq F_1'^{(2)}$ となることもわかる．そこで

$$\mathrm{Gal}\,(F_1'^{(i)}/\mathbb{Q}(\zeta_p)) \cong PSL_2(\mathbb{Z}/p\mathbb{Z})$$

より (*) が成り立つ． □

註．定理2では，無限次代数体上に $SL_2(\mathbb{Z}_p)$-不分岐 Galois 拡大を構成した．では有限次代数体上に同様に $SL_2(\mathbb{Z}_p)$-不分岐 Galois 拡大を構成できるかという問題が考えられるが，“ Fontain-Mazur の予想 ” (cf. Fontaine-Mazur [6], 田口 [16], 予想 UR) が正しければ構成できないことがわかる．

参考文献

[1] Asada, M.: On unramified Galois extensions over maximum abelian extensions of algebraic number fields, Math. Ann. **270** (1985), 477-487.

[2] Asada, M.: Construction of certain non-solvable unramified Galois extensions over the total cyclotomic field, J. Fac. Sci. Univ. Tokyo. sect.IA, Math. **32** (1985), 397-415.

[3] Brumer, A.: The class group of all cyclotomic integers, J. Pure Appl. Algebra **20**, (1981), 107-111.

[4] Cornel, G.: Abhyanker's lemma and the class group, Lecture Notes in Math. **751**, Springer, Berlin-Heiderberg-New York, (1979), 82-88.

[5] Faltings, G. and Chai, C.L.: Degeneration of abelian varieties, Ergeb. Math. Grenzgeb. (3) **22**, Springer-Verlag, Berlin, 1990.

[6] Fontaine, J.-M. and Mazur, B.: Geometric Galois representations, Proc. Conf. on elliptic curves and modular forms, Hong Kong,1993, International Press, 1995, 41-78 (第2版では 190-227).

[7] Grothendieck, A.: Modèles de Néron et monodromie, in Groupes de monodromie en géometrie algébrique, SGA7 I, A. Grothendieck, ed., Lecture Notes in Math. **288**, Springer, Berlin-Heidelberg-New York, (1972), 313-523.

[8] Horie, K.: CM-fields with all roots of unity, Compositio Math. **74** (1990), 1-14.

[9] Kurihara, M.: On the ideal class groups of the maximal real subfields of number fields with all roots of unity, J. Eur. Math. Soc. **1** (1999), 35-49.

[10] Lang, S.: Elliptic functions, Addison Wesley. Reading. Mass, (1970).

[11] Mazur, B.: Modular curves and the Eisenstein ideal, Publ. math. I.H.E.S. **47** (1977), 33-186.

[12] Serre, J.-P.: Abelian l-adic representations and elliptic curves, Benjamin. NewYork, 1968.

[13] Serre, J.-P.: Sur les représentation modulaires de degré 2 de Gal $(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. **54** (1987), 179-230.

[14] Serre, J.-P. and Tate, J.: Good reduction of abelian varieties, Ann. of Math. **88** (1968), 492-517.

[15] Uchida, K.: Galois groups of unramified solvable extensions, Tohoku Math. J. (2) **34** (1982), 311-317.

[16] 田口雄一郎 : Fontaine-Mazur 予想の紹介,『代数的整数論とその周辺』(1998), 数理解析研究所講究録, vol. 1097, 1999, 37-49.

〒 060-0810 北海道大学理学部数学教室
E-mail: sohtani@math.sci.hokudai.ac.jp