静岡県立大学短期大学部
研究紀要 16-w 号 (2002 年度)-5

Thaine の Proposition について

舘山光一

Thaine's Proposition

Koichi TATEYAMA

1 Introduction

k を有理数体 $\mathbf{Q}$ 上の有限次拡大体とする。N を正の整数、c を k の ideal class とするとき、$\mathbf{Q}$ 上一次の k の prime ideal $\mathfrak{p}$ の集合 $L(c,\ N)$ を次のように定義する。

$$L(c,\ N) = \{\mathfrak{p} \in c : \mathrm{N}_{K/\mathbf{Q}}\wp \equiv 1 \bmod N\}.$$

k が実アーベル体で $L(c,\ N)$ が無限集合の時、Thaine は
On the ideal class groups of real abelian number fields. Ann. of Math. 128 (1988) 1-18 で次の命題を証明した。

定理 1.1 α を k の元とする。有限個の例外を除いて、全ての $L(c,\ N)$ の元 $\mathfrak{p}$ に対して $\alpha \bmod \mathfrak{p}$ が $O_k/\mathfrak{p}$ で N 乗になるなら、α^2 は k 上で N 乗になる。ここで, O_k は k の整数環を表す。

この定理は次のように考えることができる。まず、最初の条件 「$\alpha \bmod \mathfrak{p}$ が $O_k/\mathfrak{p}$ で N 乗」 というのは、N と $\mathfrak{p}$ が互いに素であることから local で N 乗になることに等しい。従って local で N 乗なら global で N 乗 (正確には $N/2$ 乗) になるという Hasse のの原理 (local-global principle) の成立するケースと酷似している。しかし、決定的に異なる点もある。通常の Hasse の原理の場合、ほとんど全ての素点に関して命題が成立した場合、global でも成立するというものだが、上の定理の場合は、local な命題の成立を仮定する素点の数が、無限個ではあるが「ほとんど全て」ではない。素点の density で考えても $1/h$ 程度の仮定で十分ということになる。

ここでは上記の定理 1.1 を、cohomology 群を用いて証明する。それによって、Thaine の複雑な証明が系列の完全性に帰着されることがわかる。さらに、一般的に拡張できることも容易にみてとれることであろう。尚、証明の経過を単純にするために N 乗になる k の元を、一般的にではなく単数として証明しているが、これは本質的な部分ではなく、拡張も容易である。

2 Cohomology Group

K を有理数体 $\mathbf{Q}$ 上有限次の拡大体、L を K の N を割る素イデアル以外分岐しない最大の代数拡大体、$G = \mathrm{Gal}(L/K)$ とおく。ここで、$\mathcal{E},\ E$ をそれぞれ $L,\ k$ の単数群とすると、N 乗の写像：

$$p_N\ :\ \alpha\ \longrightarrow\ \alpha^N$$

は $\mathcal{E}$ 上 onto になることから、μ_N を 1 の N 乗根全体とすると、次の完全系列が得られる。

$$0\ \longrightarrow\ \mu_N\ \longrightarrow\ \mathcal{E}\ \xrightarrow{p_N}\ \mathcal{E}\ \longrightarrow\ 0$$

これより、Galois cohomology の完全系列を導くと、

$$0\ \longrightarrow\ \mu_N \cap K\ \longrightarrow\ E\ \longrightarrow\ E\ \longrightarrow\ H^1(G,\ \mu_N)\ \longrightarrow\ H^1(G,\ \mathcal{E})$$

となるから、次の完全系列が導かれる。

$$0\ \longrightarrow\ E/E^N\ \longrightarrow\ H^1(G,\ \mu_N)$$

この単数群から cohomology 群への写像は、$\alpha \in E,\ \sigma \in G$ とするとき、$(\sqrt[N]{\alpha})^{\sigma-1} = \zeta_\sigma \in \mu_N$ より、

$$\alpha \in k^\times\ \longrightarrow\ \{\zeta_\sigma\}_{\sigma \in G_k} \in Z^1(G,\ \mu_N)$$

より導かれる。

以下この section では $\mu_N \subset K$ を仮定する。

ここで、$\mathfrak{p}$ を N を割らない K の素イデアル、$\mathfrak{P}$ をその上にある L の素イデアルとする。$K_\mathfrak{p}$ を K の素点 $\mathfrak{p}$ での完備化、$L_\mathfrak{P}$ を L/K の有限次の中間体の $\mathfrak{P}$ での完備化の合成体とする。$U_\mathfrak{P},\ U_\mathfrak{p}$ をそれぞれ $L_\mathfrak{P},\ K_\mathfrak{p}$ の単数とすると、

$$0\ \longrightarrow\ \mu_N\ \longrightarrow\ U_\mathfrak{P}\ \xrightarrow{p_N} U_\mathfrak{P}\ \longrightarrow\ U_\mathfrak{P}/U_\mathfrak{P}^N\ \longrightarrow\ 0$$

となるが、イデアル $\mathfrak{P}$ が N を割らないことから N 乗写像 p_N は $1+\mathfrak{P}$ 上では自己同型写像となる。また、$L_\mathfrak{P}$ は 1 の N 巾乗根をすべてもつことから p_N は $U_\mathfrak{P}$ 上 onto であることがわかる。よって、次の完全系列

$$0\ \longrightarrow\ \mu_N\ \longrightarrow\ U_\mathfrak{P}\ \xrightarrow{p_N}\ U_\mathfrak{P}\ \longrightarrow\ \ \longrightarrow\ 0$$

より、global な場合と同様に以下の完全系列を得る。

$$0\ \longrightarrow\ \mu_N\ \longrightarrow\ U_\mathfrak{p}\ \xrightarrow{p_N}\ U_\mathfrak{p}\ \longrightarrow\ H^1(L_\mathfrak{P}/K_\mathfrak{p},\ \mu_N)\ \longrightarrow\ H^1(L_\mathfrak{P}/K_\mathfrak{p},\ U_\mathfrak{P})\ \longrightarrow$$

$L_\mathfrak{P}$ は $K_\mathfrak{p}$ 上不分岐であるから、アーベル拡大となる。$K_\mathfrak{p}$ 上有限次の $L_\mathfrak{P}$ の部分体を L_i $(i = 0, 1, 2, ...)$、L_i の単数群を V_i とすると、$L_i/K_\mathfrak{p}$ は不分岐アーベル拡大になることから $H^1(L_0/K_\mathfrak{p}, V_i) = 0$ である。よって、

$$H^1(L_\mathfrak{P}/K_\mathfrak{p},\ U_\mathfrak{P}) = \varinjlim H^1(L_i/K_\mathfrak{p},\ V_i) = 0$$

となるので、次の同型を示すことができる。

$$H^1(L_\mathfrak{P}/K_\mathfrak{p},\ \mu_N)\ \cong\ U_\mathfrak{p}/U_\mathfrak{p}^N$$

以上で、単数が N 乗になるかどうかという情報が、local か global かに関わらず cohomology 群で表されることが示された。ここで目標としている Hasse の原理タイプの関係を導くためには、cohomology 群の間の関係を導く必要があるが、これは以下述べるように、一般的な local-global principle の議論を使うことができる。

ideal $\mathfrak{P}$ の K 上の分解群を $G_{\mathfrak{P}}$ とすると、 $\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \cong G_{\mathfrak{P}} \subset G$ であるから、cohomology 群の制限写像

$$Res \ : \ H^1(G,\ \mu_N) \ \longrightarrow \ H^1(G_{\mathfrak{P}},\ \mu_N)$$

より、次の準同型写像 $\phi = \phi(S,\ N)$ が導かれる。

$$\phi \ : \ H^1(L/K,\ \mu_N) \ \longrightarrow \ \prod_{\mathfrak{p}\ \in\ S} H^1(L_{\mathfrak{P}}/K_{\mathfrak{p}},\ \mu_N)$$

ここで、S は N と素な素点の集合とする。以下 S は、次の条件を満たす K の prime ideal $\mathfrak{p}$ 全体とする。

- $\mathfrak{p}$ は K の ideal class c の元である。
- $\mathfrak{p}$ は、$\mathbf{Q}$ 上完全分解している。
- $\mathfrak{p}$ は N と素である。

ここで、K の Hilbert 類体を K_{nr}、ideal class group を C_K とすると、類体論より次の写像が同型となる。

$$\begin{array}{ccc} C_K & \longrightarrow & \mathrm{Gal}(K_{nr}/K) \\ \mathfrak{p} \in c_0 & \longrightarrow & \mathrm{Frob}(\mathfrak{p}) \in \mathrm{Gal}(K_{nr}/K) \end{array}$$

ここで、c_0 は K の ideal class、$\mathrm{Frob}(\mathfrak{p})$ は $\mathfrak{p}$ 上の Frobenius automorphism を表す。この写像で c に対応する $\mathrm{Gal}(K_{nr}/K)$ の元を σ_c、σ_c で生成される $\mathrm{Gal}(K_{nr}/K)$ の部分群を G_c、G_c の不変体を K_c とする。以下の系列が完全系列となることを証明するのが、この section の目的である。

$$0 \ \longrightarrow \ H^1(K_c/K,\ \mu_N) \ \xrightarrow{inf} \ H^1(L/K,\ \mu_N) \ \xrightarrow{\phi} \ \prod_{\mathfrak{p}\ \in\ S} H^1(L_{\mathfrak{P}}/K_{\mathfrak{p}},\ \mu_N)$$

ここで写像 inf は inflation map を表す。inflation map によって L/K の中間体 F において、$H^1(F/K,\ \mu_N)$ は $H^1(L/K,\ \mu_N)$ の部分群とみることができる。従って、証明すべきことは次のようになる。

定理 2.1 $\ker(\phi) = H^1(K_c/K,\ \mu_N)$

証明） $\mathfrak{p}$ を S の元、ideal $\mathfrak{P}$ を $\mathfrak{p}$ 上にある L の prime ideal とし、$K_c \cap \mathfrak{P}$ での K_c の完備化を $K_{c,\ \mathfrak{p}}$ とする。$\mathrm{Frob}(\mathfrak{p}) = \sigma_c$ は K_c 上は恒等写像であるから、$\mathfrak{p}$ は K_c 上完全分解する。従って、$K_{c,\ \mathfrak{p}} = K_{\mathfrak{p}}$ となり $\phi(H^1(K_c/K,\ \mu_N))$ は $\prod_{\mathfrak{p}\ \in\ S} H^1(L_{\mathfrak{P}}/K_{\mathfrak{p}},\ \mu_N)$ で trivial となる。

一方、$\delta \in \ker(\phi)$ とすると、$\mu_N \subset K$ より、$H^1(L/K,\ \mu_N) = \mathrm{Hom}(\mathrm{Gal}(L/K),\ \mu_N)$ であるから、δ は有限位数の character とみることができる。よって、$G_\delta = \ker(\delta)$ とおくと、G_δ の不変体 $L^{G_\delta} = K_\delta$ は K 上有限次の巡回拡大体となる。

$K_\delta \subset K_c$ ならばなにも証明することはない。$K_\delta \cap K_c = F$ とし、$1 \neq \tau \in \mathrm{Gal}(K_\delta/F)$ かつ $\delta(\tau) \neq 1$ となる元 τ が存在するとする。このとき、K_δ と K_{nr} は F 上 linearly disjoint であるから、$\sigma|_{K_\delta} = \tau$, $\sigma|_{K_{nr}} = \sigma_c$ となる $\mathrm{Gal}(K_{nr}K_\delta)/F)$ の元 σ が存在する。

ここで Tschebotareff の密度定理を用いると、K 上に $\mathrm{Frob}(\mathfrak{q}) = \sigma$ となる $\mathbf{Q}$ 上 1 次の prime ideal $\mathfrak{q}$ が無数に存在する。さらに、$\sigma|_{K_{nr}} = \sigma_c$ より $\mathfrak{q}$ は c の元となるから、$\mathfrak{q} \in S$ である。$\mathfrak{q}$ とその上の prime ideal で完備化した体をそれぞれ $K_{\mathfrak{q}}$, $K_{\delta,\mathfrak{q}}$ とおくと、$\mathrm{Gal}(K_{\delta,\mathfrak{q}}/K_{\mathfrak{q}})$ は $\mathrm{Frob}(\mathfrak{q})$ で生成される。従って、$\delta(\tau) \neq 1$ より次の準同型

$$H^1(K_\delta/K,\ \mu_N) \ \longrightarrow\ H^1(K_{\delta,\mathfrak{q}}/K_{\mathfrak{q}},\ \mu_N)$$

は trivial にならない。これは $\delta \in \ker(\phi)$ に矛盾する。よって、$K_\delta \subset K_c$ である。以上で定理は証明された。

定理 2.1 を、local の N 乗と global の N 乗の問題に戻すと、次のようになる。

系 2.2 η を $K_{\mathfrak{p}}$ $(\mathfrak{p} \in S)$ で N 乗となる K の単数とする。このとき、$K(\sqrt[N]{\eta})$ は K_c の部分体となる。

証明) $F = K(\sqrt[N]{\eta})$ とおく。$H^1(F/K,\ \mu_N) = \mathrm{Hom}(\mathrm{Gal}(F/K),\ \mu_N)$ の生成元 ρ は次のように与えられる。

$$\rho(\sigma) = \sqrt[N]{\eta}^{\sigma-1}$$

$inf(\rho) \in H^1(L/K,\ \mu_N) = \mathrm{Hom}(\mathrm{Gal}(L/K),\ \mu_N)$ より、ρ は $\mathrm{Gal}(L/K)$ の元と考えることができる。$\mathfrak{p}$ を S の元とすると、仮定より ρ は $\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ 上 trivial であるから、$\phi(inf(\rho)) = 0$ となる。よって、定理 2.1 より $ker(\rho) \supset \mathrm{Gal}(L/K_c)$ である。従って、$K(\sqrt[N]{\eta})$ は K_c の部分体となる。

定理 2.1 はもう少し拡張することができる。$c_1,\ c_2,\ \ldots\ldots\ldots\ldots,\ c_r$ を K の ideal class、対応する $\mathrm{Gal}(K_{nr}/K)$ の元をそれぞれ、$\sigma_1,\ \sigma_2,\ \ldots\ldots\ldots\ldots,\ \sigma_r$ とする。K の素 ideal $\mathfrak{p}$ の集合 T を次のように定義する。

T は、次の条件を満たす K の prime ideal 全体とする。

- $\mathfrak{p}$ は K の ideal class c_i $(i = 1,\ 2,\ \ldots\ldots\ldots\ldots\ldots\ldots,\ r)$ の元である。
- $\mathfrak{p}$ は、$\mathbf{Q}$ 上完全分解している。
- $\mathfrak{p}$ は N と素である。

また、$\sigma_1,\ \sigma_2,\ \ldots\ldots\ldots\ldots,\ \sigma_r$ で生成される $\mathrm{Gal}(K_{nr}/K)$ の部分群を G_T、それに対応する K_{nr} の部分体を K_T とする。このとき次の定理が成立する。尚、以下で ψ は定理 2.1 の ϕ 同様、各成分は制限写像 (Res) である。

定理 2.3 次の系列が完全系列となる。

$$0 \ \longrightarrow\ H^1(K_T/K,\ \mu_N) \ \xrightarrow{inf}\ H^1(L/K,\ \mu_N) \ \xrightarrow{\psi}\ \prod_{\mathfrak{p}\ \in\ T} H^1(L_{\mathfrak{P}}/K_{\mathfrak{p}},\ \mu_N)$$

証明) $c = c_1$ とおき、$\chi \in ker(\psi) \subset H^1(L/K,\ \mu_N) = \mathrm{Hom}(\mathrm{Gal}(L/K),\ \mu_N)$ とする。χ は $\mathfrak{p} \in c$ とすると、$\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ への制限は trivial となる。定理 2.1 の記号をそのまま使用すると、定理 2.1

より $ker(\chi)$ は $\mathrm{Gal}(L/K_c)$ を含む。同様のことが、c_i $(i = 2,\ \ldots\ldots,\ r)$ にも成立することから $ker(\chi)$ は $\mathrm{Gal}(L/K_T)$ を含む。よって、$\chi \in inf(H^1(K_T/K,\ \mu_N))$ である。逆に、inflation map により、$H^1(K_T/K,\ \mu_N) \subset H^1(K_{c_i}/K,\ \mu_N)$ より、$inf(H^1(K_T/K,\ \mu_N)) \subset ker(\psi)$ である。これで、定理 2.3 は証明された。

3 Root of Unity

S_0 を K の素点の集合とする。当初の問題、「S_0 のすべての素点 $\mathfrak{p}$ に対し、K の完備化 $K_{\mathfrak{p}}$ で N 乗となる K の単数が K で N 乗となるか？」という問題に関しては、定理 2.3 は直接には解答を与えてはくれない。これは、単数の N 乗根を加えた体が不分岐になるか否か、の判定が困難なことが理由になっている。ところが、1 の巾根をそれ程含まない体に関しては定理 2.3 のような結果が有効に使える、というのが Thaine のうまいアイデアなのである。以下、そのような場合を考える。

k を実の embedding をもつ有理数体上の有限次拡大体とし、$K = k(\mu_N)$ とおく。c を k の ideal class とし、S を次の条件を満たす $\mathbf{Q}$ 上一次の prime ideal 全体とし、更にこの集合は空でないとする。

$$S = \{\mathfrak{p} \in c\ :\ N(\mathfrak{p}) \equiv 1 \bmod N\}$$

L を §2 同様 N を割る prime ideal 以外不分岐な k 上最大の Galois 拡大とする。もちろん、K 上最大な拡大体と一致する。このとき、次の完全系列を考える。

$$0 \longrightarrow ker(\phi) \longrightarrow H^1(L/k,\ \mu_N) \overset{\phi}{\longrightarrow} \prod_{\mathfrak{p}\ \in\ S} H^1(L_{\mathfrak{P}}/k_{\mathfrak{p}},\ \mu_N)$$

ここで、$u \in ker(\phi)$ とおくと、制限写像

$$Res_{K/k}\ :\ H^1(L/k,\ \mu_N) \longrightarrow H^1(L/K,\ \mu_N)$$

により、$Res(u) \in H^1(L/K,\ \mu_N) = \mathrm{Hom}(\mathrm{Gal}(L/K),\ \mu_N)$ となり、$Res(u)$ は $\mathrm{Gal}(L/K)$ の character と考えることができる。この character の kernel を G_u、G_u の不変体を K_u とする。また、§2 と同様に ideal class c の要素となる prime ideal が完全分解する最大の不分岐 abel 体を k_c とおく。このとき、

定理 3.1 K_u は Kk_c の部分体である。

証明） $\mathfrak{p}$ を S の元とすると、$\mathfrak{p}$ は K/k で完全分解することから K の ideal class c_0 で $N_{K/k}(c_0) = c$ となるものが存在する。この ideal class c_0 の元で、$\mathbf{Q}$ 上一次の prime ideal を $\mathfrak{q}$ とおくと、明らかに $N_{K/k}(\mathfrak{q}) \in S$ である。ここで、$N_{K/k}^{-1}(c)$ に含まれる K の ideal class を $c_1,\ c_2,\ \ldots\ldots,\ c_r$、それぞれの ideal class の要素となる $\mathbf{Q}$ 上一次の prime ideal の集合を、それぞれ $S_1,\ S_2,\ \ldots\ldots, S_r$ とする。$u \in ker(\phi)$ より、$Res_{K/k}(u)$ は任意の i $(i = 1,\ 2,\ \ldots\ldots\ldots\ldots,\ r)$ で、以下の写像の kernel となる。

$$H^1(L/K,\ \mu_N) \longrightarrow \prod_{\mathfrak{p}\ \in\ S_i} H^1(L_{\mathfrak{P}}/K_{\mathfrak{p}},\ \mu_N)$$

従って、各 ideal class $c_1,\ c_2,\ \ldots\ldots,\ c_r$ に対応する $\mathrm{Gal}(K_{nr}/K)$ の元を $\sigma_1,\ \sigma_2,\ \ldots\ldots\ldots\ldots,\ \sigma_r$、それらで生成される $\mathrm{Gal}(K_{nr}/K)$ の部分群を G_T とすると、定理 2.3 より $Res(u)$ の kernel は

$\mathrm{Gal}(L/K_{nr})$ を含む。よって $\chi = Res(u)$ は $\mathrm{Gal}(K_{nr}/K)$ の character と考えることができる。更に定理 2.3 より χ の kernel は G_T を含む。従って、示すべきことは G_T の不変体が Kk_c となることである。

$\mathrm{Gal}(K_{nr}/k)$ の部分群で、K に対応するのは $\mathrm{Gal}(K_{nr}/K)$ である。k_c に対応する群を H とおくと、Kk_c に対応する群は $H \cap \mathrm{Gal}(K_{nr}/K)$ となる。$\mathrm{Gal}(K_{nr}/K)$ は類体論より、K の ideal class group と同型になるが、K の ideal class に対応する $\mathrm{Gal}(K_{nr}/K)$ の元の k_{nr} への制限に対応する k の ideal class は元の ideal class のノルムになる。故に、 $H \cap \mathrm{Gal}(K_{nr}/K)$ に対応する K の ideal class group の部分群は $N_{K/k}^{-1}(c)$ となる。これで、定理 3.1 は証明された。

以下、最終的な結果を述べるが、整理のため記号の定義をもう一度しておく。

定理 3.2 N を $N \not\equiv 2 \bmod 4$ となる整数、k を原始 N 乗根を含まない有限次代数体とする。c を k の ideal class とし、S を次の条件を満たす $\mathbf{Q}$ 上一次の prime ideal 全体とする。

- $\mathfrak{p}$ は k の ideal class c の元である。
- $N(\mathfrak{p}) \equiv 1 \bmod N$

このとき、k の正の単数が全ての S の素点上 local に N 乗ならば、k 上で N/w 乗である。ここで、w は N が奇数ならば 1、偶数ならば 2 を表すとする。

証明） ε を k の正の単数とし、S に含まれるすべての素点上 N 乗であるとする。L を k 上 N を割らない素点では不分岐な最大の Galois 拡大体、$G = \mathrm{Gal}(L/k)$ とする。1-dimensional cocycle $u = \{u_\sigma\}_{\sigma \in G}$ を次のように定義する。ただし、N が偶数の場合は正の N 乗根をとるものとする。

$$u_\sigma = (\sqrt[N]{\varepsilon})^{\sigma - 1}$$

u で代表される $H^1(L/k,\ \mu_N)$ の cohomology class は、仮定より任意の S の素点上で trivial となる。従って、定理 3.1 より、u を $\mathrm{Gal}(L/k(\mu_N))$ に制限した character (Kummer character) の kernel の不変体は k 上 abel である。従って、$u_\sigma \in \mu_N$ は $k(\sqrt[N]{\varepsilon})$ に含まれる。$k(\sqrt[N]{\varepsilon})$ に含まれる 1 の巾根は ± 1 だけであるから、 $\sqrt[N]{\varepsilon^2}$ は k の元となる。よって、定理 3.2 は証明された。