数理解析研究所講究録
971巻 1996年 40-49



# 与えられた number knot を持つ代数体のメタアーベル拡大について

東大 数理　藤田 司

$K/k$ を有限次代数体の有限次拡大とするとき、次式によって $K/k$ の number knot $\nu(K/k)$ が定義される。

$\nu(K/k) = (\text{local norms})/(\text{global norms}) = (k^\times \cap N_{K/k} J_K)/N_{K/k} K^\times$

($J_K$ は $K$ の idele group, $N_{K/k}$ は norm map)

定義により、$\nu(K/k)=0$ ということは、$K/k$ に Hasse norm principle が成り立つことを意味する。また $\nu(K/k)$ は有限群であり、特に $K/k$ が Galois 拡大の場合には次の Tate の定理によりその群が群論的に計算される。

<u>定理 [6]</u>　$K/k$: Galois, $G=\mathrm{Gal}(K/k)$ とすると, $\nu(K/k)$ は $\mathrm{Coker}(\bigoplus_v H_2(G^v,\mathbb{Z}) \xrightarrow{\oplus \mathrm{cor}_v} H_2(G,\mathbb{Z}))$ と canonical に同型である。ここで $\bigoplus_v$ は $k$ の全ての素点 $v$ にわたる直和、$G^v$ は $v$ 上にある $K$ のある素点の分解群、$\mathrm{cor}_v$ は corestriction map

この定理により、次の"逆問題" $\mathbb{P}(k,G,K)$ が考えられる。

<u>$\mathbb{P}(k, G, K)$</u>: 有限次代数体$k$, 有限群$G$、$H_2(G, \mathbb{Z})$の部分群$K$が与えられたとする。このときGalois拡大$K/k$及び同型$\varphi: Gal(K/k) \to G$で次の可換図式をinduceするものが存在するか？

$$\begin{tikzcd} H_2(Gal(K/k), \mathbb{Z}) \arrow[r, "\cong", "\varphi_*"'] \arrow[d] & H_2(G, \mathbb{Z}) \arrow[d] \\ \mathfrak{N}(K/k) \arrow[r, "\cong"] & H_2(G, \mathbb{Z})/K \end{tikzcd}$$

もし$H_2(G, \mathbb{Z}) = 0$なら自動的に$K = 0$となるので、$\mathbb{P}(k, G, K)$は通常のGalois逆問題となる。従って特に$G$が可解で$H_2(G, \mathbb{Z}) = 0$を満たすときには$\mathbb{P}(k, G, K)$は任意の有限次代数体$k$に対して成立する。$G$が可換群のときには、$\mathbb{P}(k, G, K)$が成り立つためには$K$が$H_2(G, \mathbb{Z})$の"typical subgroup"であることが必要十分であることが知られている（[2], [5]）

そこで、今回は$G$が簡単な非可換群のときに上の問題を考察してみた。考えてみたのは次の2通りの場合である。

(1) $G = D_4 = \langle a, b \mid a^4 = b^2 = 1,\ bab = a^{-1} \rangle$ dihedral のとき

(2) $G$が位数$p^3$の非可換群のとき（$p$: 素数）

結果を先に述べる。

<u>結論</u> $G$が上の(1)(2)いずれの場合でも、任意の$k$, 任意の部分群$K < H_2(G, \mathbb{Z})$に対し$\mathbb{P}(k, G, K)$は真となる。

以下この証明の概略を示す。

## 1. $G$ が dihedral group の場合

$G = D_n = \langle a, b \mid a^n = b^2 = 1, \ bab = a^{-1} \rangle$ とする。

定理([1]) $H_2(D_n, \mathbb{Z}) = \begin{cases} 0 & (n\text{が奇数のとき}) \\ \mathbb{Z}/2\mathbb{Z} & (n\text{が偶数のとき}) \end{cases}$

$n$ が奇数のときは $H_2(G, \mathbb{Z}) = 0$ であり、さらに $G$ は可解なので、Intro で述べたように $P(k, G, K)$ は真である。

そこで以下 $n$ は偶数として考察する。その場合 $H_2(G, \mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$ なので、$\nu(K/k) = 0$, $\nu(K/k) = \mathbb{Z}/2\mathbb{Z}$ の二つの場合に対応する $D_n$ 拡大 $K/k$ を構成することが問題となる。

定理1. $n$：偶数，$L/k$：有限次代数体 $k$ の二次拡大とする。

このとき、

(a) $n$ 次巡回拡大 $K/L$ で、$Gal(K/k) = D_n$, $\nu(K/k) = \mathbb{Z}/2\mathbb{Z}$ となるものが存在する

(b) $n$ 次巡回拡大 $K/L$ で、$Gal(K/k) = D_n$, $\nu(K/k) = 0$ となるものが存在する

この定理により $G$ が dihedral の場合 $P(k, G, K)$ が真であることが分かる。そこでこの章の残りでこれを証明していく。

証明で主に用いるのは次の補題である。

<u>補題1</u>([17]) $n$:偶数, $G=Gal(K/k)\cong D_n$ とするとき、$\nu(K/k)\cong \mathbb{Z}/2\mathbb{Z}$ となるための必要十分条件は、全ての $k$ の素点 $v$ に対して $G^v$ の2-Sylow群がcyclicになることである。

こうして $\nu(K/k)$ についての条件が分解群に関する条件に変換されたので、分解群がそのような条件を満たす $D_n$ 拡大 $K/k$ を以下構成していく。まず補題を二つ準備しておく。

<u>補題2</u> $L/k$ 2次拡大, $K/L$: $n$ 次cyclicとする。このとき、

$K/k$ が $D_n$ 拡大 $\Longleftrightarrow C_k \subset N_{K/L}C_K$ （$C_k = J_k/k^\times$ idele class group）

<u>補題3</u> $K/k$, $K'/k$ がともにGaloisで $k\subset K'\subset K$ となっているとき準同型 $\nu(K/k)\to\nu(K'/k)$ が自然に定義される。さらに $K/K'$ がcyclicで $(K:K')$ と $(K':k)$ が互いに素ならば、この準同型は同型となる。

<u>定理1.(a)の証明の方針</u>

$G=D_n$ の奇数位数の部分群で最大のものを $H$ としたとき、任意の $G/H$ 拡大 $K'/k$ はある $G$ 拡大 $K/k$ に埋め込まれる。(cf.[4]) 従って、補題3により $n$ は2の巾であると仮定してよい。

$S_1 = \mathrm{Ram}_L(L/k)$ $\stackrel{\mathrm{def}}{=}$ ($L/k$ で分岐する $L$ の素点全体) とおき、

finite subset $S_2 \subset \mathrm{Spl}_L(L/k)$ $\stackrel{\mathrm{def}}{=}$ ($L/k$ で完全分解する $L$ の素点全体)

を (i) $S_2$ は $\mathrm{Gal}(L/k)$-集合、(ii) $\forall w \in S_2$, $n \mid (Nw - 1)$, の2条件をみ

たすようにとる。($S_2$ の位数はいくらでも大きくできる。)

この $S_1, S_2$ に対し次の3条件を満たすアーベル拡大 $F/L$

の中で最大のものをとる。
- $C_k \subset N_{F/L} C_F$
- $\mathrm{Ram}_L(F/L) \subset S_2 \subset \mathrm{Spl}_L(L/k)$
- $S_1 \subset \mathrm{Spl}_L(F/L)$

もし $F/L$ が $n$ 次 cyclic な部分拡大 $K/L$ を持てば、補題2より

$K/k$ は $D_n$ 拡大であり、また $K/k$ における素点の分解群は上の

条件より全て cyclic となるので、補題1より $L(K/k) \cong \mathbb{Z}/2\mathbb{Z}$。

よって、$S_2$ をうまくとれば $\mathrm{Gal}(F/L)$ が $n$ 次 cyclic な商群を持

つことを示せばよい。

$A = U_L / U_k \left( \prod_{w \in S_2} U_w^1 \times \prod_{w \notin S_2} U_w \right)$ とおく。$\left( \begin{array}{l} U_L = \ker(J_L \to I_L),\ U_w : L_w \text{ の units} \\ U_w^1 : L_w \text{ の principal units} \end{array} \right)$

類体論により $\mathrm{Gal}(F/L)$ を $J_L$ の quotient として表わすことにより

自然な準同型 $g : A \to \mathrm{Gal}(F/L)$ を得る。$\ker(g)$, $\mathrm{Coker}(g)$ を計

算すると、これは有限群であり、$|S_2|$ の大きさに depend しな

い定数により位数が上から抑えられる。一方 $A$ は $(\mathbb{Z}/n\mathbb{Z})^{\frac{1}{2}|S_2|}$

と同型な群を部分群に持つ有限群なので、$S_2$ の大きさを十分

大きくとると、その時 $\mathrm{Gal}(F/L)$ は $n$ 次 cyclic な商群を持つ。 ▨

定理1.(b)の証明の方針

ここでもnは2の巾としてよい。n=2の場合は容易なので、4|nとして証明する。

定理1(a)で構成した$D_n$拡大を$K/k$とする。一方、$K/k$で分岐も分解もしない$k$の素点$v$をとり、$v$が分岐するような$k$の2次拡大$E/k$をとる。$G_k$を$k$の絶対Galois群として、拡大$K/k$, $E/k$に対応する準同型を$\varphi : G_k \twoheadrightarrow D_n$, $\chi : G_k \twoheadrightarrow \mathbb{Z}/2\mathbb{Z}$とする。$\varphi(G_L)$の位数2の部分群を$\mathrm{Im}(\chi)$と同一視することにより、$\tilde{\chi} : G_k \to D_n$が$\chi$からinduceされる。$\varphi'(\sigma)=\varphi(\sigma)\tilde{\chi}(\sigma)$ $(\sigma \in G_k)$により$\varphi' : G_k \to D_n$を定義する。$\varphi'$は全射であることが示されるので、これから$D_n$拡大$K'/k$が得られる。$K'/L$はn次cyclicであり、また$v$の$K'/k$における分解群はnon-cyclicなので、補題1により$D_n$拡大$K'/k$は定理1(b)の条件を満たしている。☒

2. $G$が位数$p^3$の非可換群の場合

この場合、$p=2$なら$G$は$Q_8=\langle a,b \mid a^2=b^2,\ b^{-1}ab=a^{-1}\rangle$または$D_4$のいずれか、$p$が奇素数なら$G$は$E_1=\langle a,b \mid a^{p^2}=b^p=1,\ b^{-1}ab=a^{1+p}\rangle$または$E_2=\langle a,b,c \mid a^p=b^p=c^p=[a,c]=[b,c]=1,\ c=[a,b]\rangle$のいずれかである。これらの群の$H_2(G,\mathbb{Z})$は次のようになることが知ら

れている。

<u>定理</u> $H_2(Q_8,\mathbb{Z})=0$, $H_2(D_4,\mathbb{Z})=\mathbb{Z}/2\mathbb{Z}$ $(p=2)$

$H_2(E_1,\mathbb{Z})=0$, $H_2(E_2,\mathbb{Z})=\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$ $(p\neq 2)$

$Q_8$も$E_1$も可解なので、Introで述べたように$\mathbb{P}(k,Q_8,K)$及び$\mathbb{P}(k,E_1,K)$は常に真である。また$G=D_4$の場合は前章で扱ったので、ここでは$G=E_2$として考察していく。

$G=E_2$として計算すると次の補題が得られる。

<u>補題4</u> $K/k$: Galois拡大、$G=Gal(K/k)\cong E_2$とする。

(i) $G^v=G$となる素点$v$があれば$\nu(K/k)=0$

(ii) 任意の素点$v$に対し$G^v$がcyclicなら$\nu(K/k)\cong\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$

(iii) $G^{v_1}\neq G^{v_2}$, $|G^{v_1}|=|G^{v_2}|=p$ となる$v_1,v_2$が存在し、かつ

$G^v=G$となる$v$がなければ$\nu(K/k)=0$

(iv) 以上の(i)~(iii)のいずれでもなければ$\nu(K/k)\cong\mathbb{Z}/p\mathbb{Z}$

次の定理により、補題4の(ii)(iii)(iv)それぞれの条件に対して$E_2$拡大$K/k$が存在するので、$\mathbb{P}(k,E_2,K)$は真となる。($K_1,K_2$がともに位数$p$で$\varphi_1: Gal(K/k)\xrightarrow{\sim}E_2$が$\mathbb{P}(k,E_2,K_1)$の解とすると、この$K/k$及びある$\varphi_2: Gal(K/k)\xrightarrow{\sim}E_2$が$\mathbb{P}(k,E_2,K_2)$の解となる。)

<u>定理2.</u> 素数の組 $\{p_1, p_2\}$ で次の条件を満たすものが無数に存在する： $p_1 \in (\mathbb{Z}/p_2\mathbb{Z})^{\times p}$, $p_2 \in (\mathbb{Z}/p_1\mathbb{Z})^{\times p}$, $p_i \equiv 1 \pmod{p}$, $p_i \in Spl_{\mathbb{Q}}(k/\mathbb{Q})$
($i=1,2$)

$F_i/\mathbb{Q}$ ($i=1,2$) を conductor $p_i$ の $p$ 次巡回拡大として $L = F_1F_2$ とおく。すると $E_2$ 拡大 $k_0/\mathbb{Q}$ で $\mathbb{Q} \subset L \subset k_0$, $Ram_L(k_0/L) \subset Spl_L(k/\mathbb{Q})$ を満たすものが存在する。さらにこの拡大 $k_0/\mathbb{Q}$ として次に挙げる条件 (a) (resp. (b), (c)) を満たすものをとることが出来る。

(a) $p_1, p_2$ の分解群はともに cyclic

(b) $p_1, p_2$ の分解群はともに non-cyclic

(c) $p_1$ の分解群は cyclic で、$p_2$ の分解群は non-cyclic

ここで構成した拡大 $k_0/\mathbb{Q}$ が条件 (a) (resp. (b), (c)) を満たせば、$E_2$ 拡大 $kk_0/k$ は補題4の (ii) (resp. (iii), (iv)) を満たす。」

<u>定理2の証明の方針</u>

$\{p_1, p_2\}$ の存在は Chebotarev's density theorem による。この $p_1, p_2$ に対して上のように $L/\mathbb{Q}$ をとると、$L/\mathbb{Q}$ は次の条件を満たす $E_2$ 拡大 $k_0/\mathbb{Q}$ に延長される。(cf. [4])

- $Gal(k_0/L) = Z(Gal(k_0/\mathbb{Q})) := (\text{center of } Gal(k_0/\mathbb{Q}))$
- $k_0/\mathbb{Q}$ で分岐する素数は高々3個で、それらの分解群は全て位数 $p$.

明らかにこの拡大 $k_0/\mathbb{Q}$ は条件 (a) を満たしている。

今構成した、条件(a)を満たす拡大 $K_0/\mathbb{Q}$ により全射準同型
$\phi: G_{\mathbb{Q}} \twoheadrightarrow E_2$ が定まる。( $\phi(G_L) = Z(E_2)$ が成立している)

次に $q \in Spl_{\mathbb{Q}}(L(\zeta_p)/\mathbb{Q})$ として $F_q/\mathbb{Q}$ を conductor $q$ の $p$ 次巡回拡大とする。この拡大 $F_q/\mathbb{Q}$ により $\chi_q: G_{\mathbb{Q}} \twoheadrightarrow \mathbb{Z}/p\mathbb{Z}$ が定まり、$\mathbb{Z}/p\mathbb{Z}$ を $Z(E_2)$ と同一視することにより $\hat{\chi}_q: G_{\mathbb{Q}} \to E_2$ が得られる。

$\phi_q(g) = \phi(g)\hat{\chi}_q(g)$ ($g \in G_{\mathbb{Q}}$) により $\phi_q: G_{\mathbb{Q}} \to E_2$ を定義する。この $\phi_q$ は全射であることが示され、これから $E_2$ 拡大 $K_q/\mathbb{Q}$ が定まる。

素数 $q$ が次の条件(B)を満たせば $K_0 = K_q$ は定理2の条件(b)を満たし、$q$ が条件(C)を満たせば $K_0 = K_q$ は定理2の条件(c)を満たす:

(B) $q \in Spl_{\mathbb{Q}}(L(\zeta_p)/\mathbb{Q})$, $p_1 \notin (\mathbb{Z}/q\mathbb{Z})^{\times p}$, $p_2 \notin (\mathbb{Z}/q\mathbb{Z})^{\times p}$

(C) $q \in Spl_{\mathbb{Q}}(L(\zeta_p)/\mathbb{Q})$, $p_1 \in (\mathbb{Z}/q\mathbb{Z})^{\times p}$, $p_2 \notin (\mathbb{Z}/q\mathbb{Z})^{\times p}$

この条件(B),(C)を満たす素数 $q$ が無数に存在することは Čebotarev's density theorem によって示される。 $\blacksquare$

remark

- 補題4(b)に対応する $K/k$ が一般の $k$ に対して存在するかは分かりませんでした。( $G^v = E_2$ となる $v$ は $p$ 上の素点に限られてしまうので、上の手法は使えない)
- 定理1,2により $P(k, G, K)$ が真であるだけでなく、その解が無数に存在することが分かります。

参考文献

[1]. F. Gerth, The Hasse norm principle in metacyclic extensions of number fields, J. London Math. Soc. (2) 16 (1977) pp 203-208

[2] W. Jehne, On knots in algebraic number theory, J. reine angew Math 311 (1979) pp 215-254

[3] G. Karpilovsky, The Schur Multiplier, Oxford University Press, New York, 1987

[4] J. P. Serre, Topics in Galois Theory, Jones and Bartlett Publishers, Boston, 1992

[5] H-D. Steckel, Abelsche Erweiterungen mit vorgegebenem Zahlknoten, J. reine angew. Math 330 (1982) pp 93-99

[6] J. Tate, Global class field theory in Algebraic Number Theory (edited by Cassels-Fröhlich). London (1967) pp 162-203