

与之らした number knot を持つ代数体の $\mathbb{A}^1$ -拡大に
ついて

東大 数理 藤田 司

$K/\mathbb{R}$ を有限次代数体の有限次拡大とすると、次式によ
り $K/\mathbb{R}$ の number knot $\nu(K/\mathbb{R})$ が定義される。

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

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

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

定理 [6] $K/\mathbb{R}$: Galois, $G = \text{Gal}(K/\mathbb{R})$ とすると、 $\nu(K/\mathbb{R})$ は
 $\text{Coker}(\bigoplus H_2(G^v, \mathbb{Z}) \xrightarrow{\text{cor}} H_2(G, \mathbb{Z}))$ と canonical に同型である。こ
こで $\bigoplus$ は $\mathbb{R}$ の全ての素点 v に関する直和、 G^v は v 上にある K
のある素点 $\mathfrak{p}$ の分解群、 cor は corestriction map

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

$P(K, G, K)$: 有限体代数体 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 $\varphi: \text{Gal}(K/K) \rightarrow G$ が次の可換図式を induce するものも存在するか?

$$\begin{array}{ccc} H_2(\text{Gal}(K/K), \mathbb{Z}) & \xrightarrow[\varphi_*]{\cong} & H_2(G, \mathbb{Z}) \\ \downarrow & & \downarrow \\ \mathcal{U}(K/K) & \xrightarrow{\cong} & H_2(G, \mathbb{Z})/K \end{array}$$

もし $H_2(G, \mathbb{Z}) = 0$ なら自動的に $K = 0$ となるので、 $P(K, G, K)$ 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 $P(K, G, K)$ は任意の有限体代数体 K に対して成立する。 G が可換群 q のときには、 $P(K, G, K)$ 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 が単純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) $G = D_n = \langle a, b \mid a^n = b^2 = 1, bab = a^{-1} \rangle$ dihedral のとき

(2) G が位数 p^2 の非可換群のとき (p : 素数)

結果を先に述べる。

結論 G が上の (1)(2) のいずれの場合でも、任意の K , 任意の部分群 $K \leq H_2(G, \mathbb{Z})$ に対し $P(K, G, K)$ 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
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。この場合 $H_2(G, \mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$
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 2 次拡大とする。

このとき、

- (a) n 次巡回拡大 K/L で、 $\text{Gal}(K/K) = D_n$, $\nu(K/K) = \mathbb{Z}/2\mathbb{Z}$ となるもの
が存在する
- (b) n 次巡回拡大 K/L で、 $\text{Gal}(K/K) = D_n$, $\nu(K/K) = 0$ 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
わかる。そこでこの章の残りでこれを証明して置く。

証明を主に用いるのは次の補題である。

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

こうして $\mathcal{L}(K/\mathbb{Q})$ 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、分解群がどのような条件を満たす D_n 拡大 $K/\mathbb{Q}$ を以下構成していく。まず補題をこの準備しておく。

補題2 $K/\mathbb{Q}$: 2次拡大, $K/\mathbb{Q}$: n 次 cyclic とする。このとき、
 $K/\mathbb{Q}$ が D_n 拡大 $\iff C_K \subset N_{\mathbb{Q}} C_K$ ($C_K = J_K/\mathbb{Q}^\times$ idèle class group)

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

定理1. (ii) の証明の方針

$G = D_n$ の奇数位数の部分群で最小のものを H としたとき、任意の G/H 拡大 $K'/\mathbb{Q}$ はある G 拡大 $K/\mathbb{Q}$ に埋め込まれる (cf. [4])。従って、補題3によりいはいはこの中をあると仮定してよい。

$S_1 = \text{Ram}_L(K) \stackrel{\text{def}}{=} (K \text{ を分岐する } L \text{ の素点全体})$ とおき、
 finite subset $S_2 \subset \text{Spl}_L(K) \stackrel{\text{def}}{=} (K \text{ を完全に分解する } L \text{ の素点全体})$
 を (i) S_2 は $\text{Gal}(K/L)$ -集合、(ii) $\forall w \in S_2, m | (Nw - 1)$, の二条件をみたすようにとる。(S_2 の位数はいくらでも小さくできる。)

この S_1, S_2 に対し次の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。

- $C_K \subset N_{F/L} C_F$
- $\text{Ram}_L(F/L) \subset S_2 \subset \text{Spl}_L(K)$
- $S_1 \subset \text{Spl}_L(F/L)$

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/L は m 拡大であり、また K/L 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 $\nu(K/L) \cong \mathbb{Z}/2\mathbb{Z}$ 。

よって、 S_2 をうまくとれば $\text{Gal}(F/L)$ が n 次 cyclic な商群を持つことを示せばよい。

$$A = U_L / U_L \left(\prod_{w \in S_2} U_w^i \times \prod_{w \notin S_2} U_w \right) \text{ とおく。 } \begin{cases} U_w = \ker(J_L \rightarrow J_w), U_w: L_w \text{ の units} \\ U_w^i: L_w \text{ の principal units} \end{cases}$$

類体論により $\text{Gal}(F/L) \cong J_L$ の quotient として表わすことにより自然な準同型 $g: A \rightarrow \text{Gal}(F/L)$ を得る。 $\ker(g), \text{Coker}(g)$ を計算すると、これは有限群であり、 $|S_2|$ の大きさに depend した定数により位数が上から抑えられる。一方 A は $(\mathbb{Z}/n\mathbb{Z})^{\frac{1}{2}|S_2|}$ と同型の群を部分群に持つ有限群なので、 S_2 の大きさを十分小さくすると、この時 $\text{Gal}(F/L)$ は n 次 cyclic な商群を持つ。 $\square$

定理 1. (b) の証明の方針

ここでも u は 2 の中としてよい。 $u=2$ の場合は容易なので、 $4 \mid u$ として証明する。

定理 1 (a) で構成した D_u 拡大を $K/\mathbb{Q}$ とする。一方、 $K/\mathbb{Q}$ が分岐も分解もしない $\mathbb{Q}$ の素点 $\mathfrak{p}$ をとり、 $\mathfrak{p}$ が分岐するような $\mathbb{Q}$ の二次拡大 $E/\mathbb{Q}$ をとる。 G_E を $\mathbb{Q}$ の絶対 Galois 群として、 拡大 $K/\mathbb{Q}$, $E/\mathbb{Q}$ に対応する準同型を $\varphi: G_E \rightarrow D_u$, $\chi: G_E \rightarrow \mathbb{Z}/2\mathbb{Z}$ とする。 $\varphi(G_E)$ の位数 2 の部分群を $\text{Im}(\chi)$ と同一視することにより、 $\tilde{\chi}: G_E \rightarrow D_u$ が χ から induce される。 $\varphi'(g) = \varphi(g)\tilde{\chi}(g)$ ($g \in G_E$) により $\varphi': G_E \rightarrow D_u$ を定義する。 φ' は全射であることが示されるので、 ことから D_u 拡大 $K'/\mathbb{Q}$ が得られる。 K'/L は u -cyclic であり、 また $\mathfrak{p}$ の $K'/\mathbb{Q}$ における分解群は non-cyclic なので、 補題 1 により D_u 拡大 $K'/\mathbb{Q}$ は定理 1 (b) の条件を満たしている。 $\square$

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 $E_1 = \langle a, b \mid a^p = b^p = 1, b^{-1}ab = a^{1+p} \rangle$ 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。

定理 $H_2(Q_8, \mathbb{Z}) = 0$, $H_2(D_4, \mathbb{Z}) = \mathbb{Z} \oplus \mathbb{Z}$ ($p=2$)

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

Q_8 も E_1 も可解なので、Intro で述べたように $P(R, Q_8, K)$ 及び $P(R, E_1, K)$ 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。

補題 4 K/R : Galois 拡大, $G = \text{Gal}(K/R) \cong E_2$ とする。

(i) $G^v = G$ とする素点 v があれば $\nu(K/R) = 0$

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

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

$G^v = G$ とする v がなければ $\nu(K/R) = 0$

(iv) 以上の (i) ~ (iii) のいふいずれもなければ $\nu(K/R) \cong \mathbb{Z}/p\mathbb{Z}$.

次の定理により、補題 4 の (ii) (iii) (iv) を満たす条件に対して E_2 拡大 K/R が存在するので、 $P(R, E_2, K)$ は真となる。(X_1, X_2 がともに位数 p で $\varphi_i: \text{Gal}(K/R) \xrightarrow{\sim} E_2$ が $P(R, E_2, K_i)$ の解となると、この K/R 及びある $\varphi_2: \text{Gal}(K/R) \xrightarrow{\sim} E_2$ が $P(R, E_2, K_2)$ の解となる。)

定理 2. 素数の組 $\{p_1, p_2\}$ が次の条件を満たすものが無数に存在する: $p_i \in (\mathbb{Z}/p_2\mathbb{Z})^{\times F}$, $p_2 \in (\mathbb{Z}/p_1\mathbb{Z})^{\times F}$, $p_i \equiv 1 \pmod{p}$, $p_i \in \text{Spl}_G(K/\mathbb{Q})$ ($i=1, 2$)

$F_i/\mathbb{Q}$ ($i=1, 2$) を conductor p_i の p -巡回拡大として $L = F_1 F_2$ とおく。すると F_2 -拡大 $K_0/\mathbb{Q}$ が $\mathbb{Q} \subset L \subset K_0$, $\text{Ram}_L(K_0/L) \subset \text{Spl}_L(L/\mathbb{Q})$ 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)) を満たすものがとれることが出来る。

(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

ここに構成した拡大 $K_0/\mathbb{Q}$ が条件 (a) (resp. (b), (c)) を満たせば、 F_2 -拡大 K/K_0 は補題 4 の (ii) (resp. iii), iv) を満たす。』

定理 2 の証明の方針

p_1, p_2 の存在は Chebotarev's density theorem にある。この p_1, p_2 に對して上のように $L/\mathbb{Q}$ をとると、 $L/\mathbb{Q}$ は次の条件を満たす F_2 -拡大 $K_0/\mathbb{Q}$ に延長される。(cf. [4])

• $\text{Gal}(K_0/L) = Z(\text{Gal}(K_0/\mathbb{Q})) := (\text{center of } \text{Gal}(K_0/\mathbb{Q}))$

• $K_0/\mathbb{Q}$ が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 $\phi: G_0 \rightarrow E_2$ が定まる。($\phi(G_0) = Z(E_2)$ が成立している)

次に $g \in \text{Spl}_{\mathbb{Q}}(L(\mathbb{Z}_p)/\mathbb{Q})$ として $F_g/\mathbb{Q}$ を conductor g の p -次巡回拡大とする。この拡大 $F_g/\mathbb{Q}$ により $\chi_g: G_0 \rightarrow \mathbb{Z}_p^\times$ が定まり、 $\mathbb{Z}_p^\times$ を $Z(E_2)$ と同一視することにより $\tilde{\chi}_g: G_0 \rightarrow E_2$ が得られる。

$\phi_g(g) = \phi(g) \tilde{\chi}_g(g)$ ($g \in G_0$) により $\phi_g: G_0 \rightarrow E_2$ を定義する。この ϕ_g は全射であることが示され、これから互拡大 $K_g/\mathbb{Q}$ が定まる。

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

$$(B) \quad g \in \text{Spl}_{\mathbb{Q}}(L(\mathbb{Z}_p)/\mathbb{Q}), \quad p_1 \notin (\mathbb{Z}/g\mathbb{Z})^{\times p}, \quad p_2 \notin (\mathbb{Z}/g\mathbb{Z})^{\times p}$$

$$(C) \quad g \in \text{Spl}_{\mathbb{Q}}(L(\mathbb{Z}_p)/\mathbb{Q}), \quad p_1 \in (\mathbb{Z}/g\mathbb{Z})^{\times p}, \quad p_2 \notin (\mathbb{Z}/g\mathbb{Z})^{\times p}$$

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

Remark

- 補題 4 (b) に対応する $K/\mathbb{Q}$ が一般の $\mathbb{Q}$ に対して存在するかは分かりませんでした。($G^v = E_2$ となるのは 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 $P(\mathbb{Q}, G, k)$ が真であるだけでなく、その解が無数に存在することも分かります。

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, Abelische 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