数理解析研究所講究録
第589巻 1986年 123-135

アーベル拡大の Genus Group とその応用

新潟大教養　竹内照雄　(Teruo Takeuchi)

§1. 序

kを有限次代数体，K/kを有限次ガロワ拡大とする。$\tilde{K}$をKの絶対類体，K'を$\tilde{K}$に含まれるk上最大アーベル拡大とする。このとき，$K\cdot K'$をK/kの genus field K^*，$Gal(K^*/K)$をK/kの genus group，$\#(Gal(K^*/K))$をK/kの genus number とそれぞれ定義する。genus number については，genus公式[3]が良く知られている。必ずしもガロワでない拡大へのこの公式の拡張も得られている([4])。又 mod $\mathfrak{m}$ の genus number についても研究されている([6])。しかし，genus field や genus group については，$k=\mathbb{Q}$又は$(h(k),[K:k])=1$等の場合以外，あまり研究されていない。但し$h(k)$はkの類数を表す。

ここではまず，genus 公式を精密化して，genus group について対応する公式を作る(§2)。次にこの公式を手掛りにして，色々な条件を満たす genus group をもつアーベル拡大

の構成を考える。その為に上の公式に現れる量を Kummer 理論を用いて，Čebotarev の密度定理の使い易い形に表す（§3）。更に巡回拡大の存在条件を §3 でのものと同じ用語を用いて表す（§4）。以上のことを用いると，k のイデアル類群 $Cl(k)$ の任意の有限アーベル拡大 M に対し，$Gal(K^*/K) \cong M$ となる巡回拡大 K/k の存在を示すことができる。又，大きなイデアル類群をもつ代数体で，今迄知られていない型のものの存在を示すこともできる（§5）。

以下 ℓ を固定された 1 つの素数とし，簡単の為 §3 以後では $\ell \neq 2$ と仮定する。

§2. Genus group

記号を上の通りとする。K/k での最大アーベル部分体を K_0 とする。v を K/k で分岐する素点，V を v の K での 1 つの素因子とする。V，v による K，k の完備化を K_V，k_v とそれぞれ表す。K_V/k_v での最大アーベル部分体を $(K_V)_1$，$(K_V)_1/k_v$ の惰性群を T_V、conductor を $\mathfrak{f}_V$ と表す。T_V、$\mathfrak{f}_V$ は V の取り方には依存しないから，それぞれ T_v、$\mathfrak{f}_v$ と表す。そして $\mathfrak{f} = \prod \mathfrak{f}_v$ と置く。K/k がアーベルならば $\mathfrak{f}$ は K/k の conductor である。genus number について，次の式は良く知られている。

$$[K^*:K] = h(k)\frac{\prod \#(T_v)}{[K_0:k][E_k:E_{K/k}]} \quad (\text{genus 公式}),$$

但し $E_{K/k}$ はすべての素点で K からの局所ノルムとなる k の単数の成す群を表す。この公式を精密化して、$\mathrm{Gal}(K^*/K)$ の構造について公式を作るのがこの節の目標である。

その為に１つの素数 l を固定して、$i=0,1,2,\cdots$ に対し $F_i = \{x \in k^\times \mid (x) = \mathfrak{A}^{l^i}\}$，$F_i(\mathfrak{f}) = F_i \cap k(\mathfrak{f})$，$\mathcal{N}_i(\mathfrak{f}) = k(\mathfrak{f})^{l^i} N_{K/k}(K(\mathfrak{f}))k_{\mathfrak{f}}$ と置く。但し、$k(\mathfrak{f})$ は $\mathfrak{f}$ と素な k の元全体，$k_{\mathfrak{f}}$ は $\mathfrak{f}$ を法とする k の ray number group である。更に一般に，有限アーベル群 A に対して，A の l^i-階数を $\mathrm{rank}_i(A) = \mathrm{rank}(A^{l^{i-1}}/A^{l^i})$ と定義する。

<u>命題１</u>（[9, Theorem]）. $i \geqq 1$ に対して，

$$\mathrm{rank}_i(\mathrm{Gal}(K'/k)) = \mathrm{rank}_i(\mathcal{C}l(k)) + \sum_v \mathrm{rank}_i(T_v) + \log_l\left\{\frac{\#(F_{i-1}(\mathfrak{f})/F_{i-1}(\mathfrak{f}) \cap \mathcal{N}_{i-1}(\mathfrak{f}))}{\#(F_i(\mathfrak{f})/F_i(\mathfrak{f}) \cap \mathcal{N}_i(\mathfrak{f}))}\right\}$$

が成立する。但し，$\mathcal{C}l(k)$ は k のイデアル類群である。

<u>注意</u>. $\#(\mathrm{Gal}(K^*/K)) = \#(\mathrm{Gal}(K'/k))/[K_0:k]$ だから，すべての l，i について上の式を合わせれば，genus 公式を得る。即ち上の命題は genus 公式の精密化になっている。

一般には，$\mathrm{Gal}(K'/k)$ と $\mathrm{Gal}(K/k)$ から $\mathrm{Gal}(K^*/k)$ を決定することはできない。しかし，kの素点からなる，ある有限集合 T に対して，$\mathrm{Gal}(K_0/k)=\prod_{v\in T} T_v$（直積）となれば，$\mathrm{Gal}(K^*/k)$ の構造が決まる。実際このとき，

$$\mathrm{Gal}(K'/k) \cong \mathrm{Gal}(K_0/k) \oplus \mathrm{Gal}(K'/K_0)$$

だから，$\mathrm{Gal}(K^*/k) \cong \mathrm{Gal}(K'/K_0)$ より

$$\mathrm{rank}_i(\mathrm{Gal}(K^*/k)) = \mathrm{rank}_i(\mathrm{Gal}(K'/k)) - \mathrm{rank}_i(\mathrm{Gal}(K_0/k))$$

を得る。

§3. Kummer理論

命題1の右辺の最後の項を Čebotarev の密度定理を使い易い形に変形するのがこの節の目標である。以後簡単の為 $l \neq 2$ と仮定する。又 K/k で無限素点は不分岐とする。（以下の議論は，$l=2$ の時も K/k で分岐する素イデアル $\mathfrak{q}$ がすべて $N\mathfrak{q} \equiv 1 \pmod 4$ を満たせば同様に成立する。従って §5 での存在についてのことは $l=2$ でも大体成立する。）

整数 $i \geq 1$ に対して，ζ_i を 1の原始 l^i 乗根とし，$k_i = k(\zeta_i)$ と置く。F を $k^\times$の部分群で，$K_i(F) = k_i(\sqrt[l^i]{F})$ としたとき，$[K_i(F):k_i] < \infty$ となるものとする。$G_i(F) = \mathrm{Gal}(K_i(F)/k_i)$ とし，Kummer pairing $\langle\ ,\ \rangle_i : G_i \times F \longrightarrow \langle \zeta_i \rangle$ を $\langle \sigma, a \rangle_i = \sigma(\sqrt[l^i]{a})/\sqrt[l^i]{a}$ によって定義する。$\mathfrak{Q} \mid \mathfrak{f}$ となる

kのイデアル$\mathfrak{m}$に対して、$\mathfrak{n}(\mathfrak{m}) = N_{K/k}(K(\mathfrak{m}))k_{\mathfrak{m}}$ と置く。このとき、$l \neq 2$ だから、$F \cap \mathfrak{n}(\mathfrak{m})k^{\times l^i} = F \cap \mathfrak{n}(\mathfrak{m})k_i^{\times l^i}$ が成立する。従って、$F/F \cap \mathfrak{n}(\mathfrak{m})k^{\times l^i}$ の指標は自然に $F/F \cap \mathfrak{n}(\mathfrak{m})k_i^{\times l^i}$ の指標になり、Kummer pairing を用いて、$G_i(F)$ の元と見なすことができる。

そこで、$F = F_i$ 又は $F = F_i(\mathfrak{m}) = F_i \cap k(\mathfrak{m})$ とする。F_iの定義に注意すれば、$1 \leqq j \leqq i$ に対して、$K_j(F_i) = K_j(F_i(\mathfrak{m}))$、$[K_j(F_i) : k_j] < \infty$ となることが判る。

<u>定義</u>. $F_i/F_i \cap \mathfrak{n}(\mathfrak{m})k^{\times l^j}$ の指標群を $G_j(F_i)$ の部分群と見なした時、これを $Z_{K/k}(\mathfrak{m}, F_i)_j$ と表す。特に $Z_{K/k}(\mathfrak{m}, F_i)_i$ を $Z_{K/k}(\mathfrak{m})_i$ と表す。

$F_i(\mathfrak{m})/F_i(\mathfrak{m}) \cap \mathfrak{n}_i(\mathfrak{m}) \cong F_i/F_i \cap \mathfrak{n}(\mathfrak{m})k^{\times l^i}$ に注意すれば、

$$\#(F_i(\mathfrak{f})/F_i(\mathfrak{f}) \cap \mathfrak{n}_i(\mathfrak{f})) = \#(Z_{K/k}(\mathfrak{f})_i)$$

を得る。更にここで、

$$Z_{K/k}(\mathfrak{f})_i = \prod_{\mathfrak{g} | \mathfrak{f}} Z_{K/k}(\mathfrak{f}_{\mathfrak{g}})_i$$

ともなる。但し $\mathfrak{f}_{\mathfrak{g}}$ は $\mathfrak{f}$ の $\mathfrak{g}$-成分である。

さて、$1 \leqq j \leqq h \leqq i$ とするとき、$F_i/F_i \cap \mathfrak{n}(\mathfrak{m})k^{\times l^j}$ の指標群は $F_i/F_i \cap \mathfrak{n}(\mathfrak{m})k^{\times l^h}$ の指標群の部分群と見なせる。このことを $G_j(F_i)$ と $G_h(F_i)$ を使って表せば、次を得る。

補題. $1 \leqq j \leqq h \leqq i$ に対して，次の条件(1)(2)を満たす単準同型 $V_h^j : Z_{K/k}(\mathfrak{N}, F_i)_j \longrightarrow Z_{K/k}(\mathfrak{N}, F_i)_h$ が唯1つ存在する。

(1) $(\sigma, a) \in Z_{K/k}(\mathfrak{N}, F_i)_j \times F_i$ に対して，

$$\langle \sigma, a \rangle_i = \langle V_h^j(\sigma), a \rangle_h$$

(2) $1 \leqq j \leqq s \leqq h$ に対して，

$$V_h^j = V_h^s \circ V_s^j$$

この補題の記号を用いると，$(\mathfrak{g}, l) = 1$ の場合，$Z_{K/k}(\mathfrak{f}_\mathfrak{g})$ をもっと具体的に表すことができる。即ち，類体論と Kummer 理論を用いて次が容易に示される。

命題2. $\mathfrak{g}$ を l と素な k の素イデアル，$e = e_\mathfrak{g}$ を $T_\mathfrak{g}$ の位数の l-指数（即ち，$l^e \parallel \#(T_\mathfrak{g})$ ）とする。このとき，

$$Z_{K/k}(\mathfrak{f}_\mathfrak{g})_i = Z_{K/k}(\mathfrak{g})_i = \begin{cases} \left\langle \left(\dfrac{K_i(F_i)/k_i}{\mathfrak{P}_i} \right) \right\rangle & (i \leqq e \text{ のとき}), \\[2ex] V_i^e\left(\left\langle \left(\dfrac{K_e(F_i)/k_e}{\mathfrak{P}_e} \right) \right\rangle \right) & (i > e \text{ のとき}) \end{cases}$$

が成立する。但し，$\mathfrak{P}_i$ は $\mathfrak{g}$ の k_i における1つの素因子，$\left(\overline{\quad\quad} \right)$ は Artin 記号を表す。

特に，K/k が tamely ramified ならば，$Z_{K/k}(\mathfrak{f})_i$ は上の命題から決定される。

§4. 巡回拡大の存在の判定

T を k の素イデアルの成す有限集合とし，各 $\mathfrak{g}\in T$ に対して，$\mathfrak{g}$ の巾 $\mathfrak{f}_{\mathfrak{g}}$ 及び，$k(\mathfrak{g})/k_{\mathfrak{f}_{\mathfrak{g}}}$ の指標 $\chi_{\mathfrak{g}}$ で conductor が $\mathfrak{f}_{\mathfrak{g}}$，位数が $l^{e_{\mathfrak{g}}}$ となるものが与えられているとする。このとき，各 $\mathfrak{g}\in T$ でのみ分岐し，惰性群が $k(\mathfrak{g})/Ker(\chi_{\mathfrak{g}})$ と自然に同型となる巡回拡大 K/k の存在する為の条件を考える。

$e=\max e_{\mathfrak{g}}$，$\mathfrak{f}=\prod\mathfrak{f}_{\mathfrak{g}}$ と置く。$\chi_{\mathfrak{g}}$ は $F_i(\mathfrak{f})/F_i(\mathfrak{f})\cap Ker(\chi_{\mathfrak{g}})$ の指標を引起すから，$i\geqq e$ に対して，$G_i(F_i)$ の元と見なすことができる。このように得られる $G_i(F_i)$ の元を $z_T(\mathfrak{g})_i$ と表す。このとき K/k の存在について，次を示すことができる。これは本質的には，Grunwald - Hasse [5] の証明の中に含まれているが，このような形にすると，Grunwald の定理とは別の情報を与えてくれる。

<u>命題3</u>．$i\geqq e$ とする。$G_i(F_i)$ で，

$$(*)\qquad \prod_{\mathfrak{g}\in T} z_T(\mathfrak{g})_i^{\,n_{\mathfrak{g}}}=1\quad,\ (n_{\mathfrak{g}},l)=1$$

となる自然数 $n_{\mathfrak{g}}$ が存在すれば，ある l^n $(n\leqq i)$ 次巡回拡大 K/k で，K/k で $\mathfrak{g}\in T$ のみが分岐し，$k(\mathfrak{g})/Ker(\chi_{\mathfrak{g}})$ が

ノルム剰余記号で，その惰性群と同型になるものが存在する。そしてこのとき，$\langle \chi_T(\mathfrak{g})_i \rangle = Z_{K/k}(\mathfrak{g})_i$ となる。

逆に上のような l^n 次巡回拡大 K が存在すれば，$n \geq e$ で，$i = n$，$n_{\mathfrak{g}} = 1$，$\chi_{\mathfrak{g}}$ を K の $\mathfrak{g}$ でのノルム剰余記号として，(*)が成立する。

容易に判るように，任意に与えられた T，$\chi_{\mathfrak{g}}$ に対して適当な素イデアル $\mathfrak{g}$ を1つ加えて，上の(*)を満たすようにすることができる。これが普通の Grunwald の定理の少し弱い形のものである。上の命題からは，これ以外に例えば，次のようなことが判る。

<u>例</u>. $\mathfrak{g} \nmid l$ とする。このとき，$\mathfrak{g}$ のみが分岐し，$\mathfrak{g}$ が完全分岐する l^n 次巡回拡大が存在する為の必要十分条件は，$\mathfrak{g}$ が $K_n(F_n)/k$ で完全分解することである。

以上から，k 上の l^n 次巡回拡大 K の存在する為の条件と，その genus group の構造とが，分岐する素イデアル $\mathfrak{g}$ に対する $Z_{K/k}(\mathfrak{g})_i$，又は $\chi_T(\mathfrak{g})_i$ によって同じ $G_i(F_i)$ の中で表されることが判った。

§5. 応用例

5.1. p_i を $p_i \equiv 1 \pmod{l}$ となる素数，$K_i/\mathbb{Q}$ を p_i のみが分岐する l 次巡回拡大とする。これらの合成体 $K_1 \cdots K_n$ のイデアル類群の l-階数は，n が大きくなるにつれて，急速に大きくなることが知られている（[1]）。前節までの結果を使うと，更に大きくなる素数の組 $p_1, \cdots, p_n$ の存在が判る。即ち

$$\mathrm{rank}_1(\mathcal{C}l(K_1 \cdots K_n)) \geqq \frac{l^n - 1}{l-1} - n$$

となる素数の組 $p_1, \cdots, p_n$ が無限に存在する。

<u>証明</u>. n についての帰納法で示す。$k = K_1 \cdots K_n$ として前の記号を用いる。p_{n+1} を $k_1(\sqrt[l]{F_1})/\mathbb{Q}$ で完全分解する素数とする。このとき，$p_{n+1} \equiv 1 \pmod{l}$ より，p_{n+1} のみが分岐する l 次巡回拡大 $K_{n+1}/\mathbb{Q}$ が存在する。p_{n+1} の取り方より，p_{n+1} は k で $p_{n+1} = \mathfrak{P}_1 \cdots \mathfrak{P}_{l^n}$ と分解する。$K = K_{n+1}k$ として前の議論を適用すると，$Z_{K/k}(\mathfrak{P}_i) = \{1\}$ だから，

$$\mathrm{rank}_1(\mathrm{Gal}(K^*/K)) = \mathrm{rank}_1(\mathcal{C}l(k)) + l^n - 1 \geqq \frac{l^{n+1}-1}{l-1} - (n+1)$$

を得る。■

pure な l 次体の合成についても同様なことが成立する。このようなことを使うと，特に，分岐する素数が少なくて，類体塔が無限になるようなものの存在が判る（[7]，[8]）。

5.2. 一般に，拡大 $N/\mathbb{Q}$，$M/\mathbb{Q}$ に対して，$\ell \nmid h(N)$，$\ell \nmid h(M)$ であっても，$\ell \nmid h(MN)$ とは限らない。実際かなり ℓ で割れることが起る。即ち，

$N/\mathbb{Q}$ を任意の拡大，n を任意の自然数とするとき，ℓ^n 次の拡大 $M_n/\mathbb{Q}$ で，$\ell \nmid h(M_n)$ かつ

$$\mathrm{rank}_1(Cl(M_nN)) \geqq \mathrm{rank}_1(Cl(N)) + n([N:\mathbb{Q}]-1)$$

となるものが無限に存在する。

<u>証明</u>. 更に $[M_nN : M_n] = [N:\mathbb{Q}]$ ともできることを，n についての帰納法で示す。$k = M_nN$ と置き，前の記号を用いる。$k_1(\sqrt[\ell]{F_1})/\mathbb{Q}$ で完全分解する素数 p_{n+1} をとり，$\mathfrak{p}$ を M_n での1つの素因子とする。このとき $\mathfrak{p}$ は M_nN で $\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_m$，$m = [N:\mathbb{Q}]$ と分解される。一方 $\mathfrak{p}$ のみが分岐する ℓ 次巡回拡大 M_{n+1}/M_n が存在し，$\ell \nmid h(M_{n+1})$，$[M_{n+1}N : M_{n+1}] = [N:\mathbb{Q}]$ となる。$K = M_{n+1}N$ として前の議論を適用すると，

$$\mathrm{rank}_1(Cl(M_{n+1}N)) \geqq \mathrm{rank}_1(\mathrm{Gal}(K^*/K))$$
$$= \mathrm{rank}_1(Cl(M_nN)) + [N:\mathbb{Q}] - 1 \geqq \mathrm{rank}_1(Cl(N)) + (n+1)([N:\mathbb{Q}]-1)$$

を得る。■

上で $M_n/\mathbb{Q}$ はガロワとも限らない。しかし [2] の結果を用いると，$n \leqq 3$ のとき，$M_n/\mathbb{Q}$ を初等アーベル拡大にとれる

ことが示される。これは，初等アーベルℓ-拡大 $M_n/\mathbb{Q}$ が $\ell \nmid h(M_n)$ となる条件と，上のような構成の条件とが，独立な体での分解条件となることを示せばよい。特にこれから，ℓ^3 次初等アーベル体 M_1, M_2 の組で，$\ell \nmid h(M_i)$ $(i=1,2)$ かつ $\mathrm{rank}_1(Cl(M_1M_2)) \geqq 3(\ell^3-1)$ となるものが無限にあることが判る。

5.3. M を $Cl(k)$ の任意の有限アーベル拡大とすると，M は k 上の巡回拡大の genus group として実現できる。実際，より精密に次が成立する。

$(C_1, \cdots, C_s)$ を k のイデアル類群 $Cl(k)$ の ℓ-部分の不変数とする。r を E_k の自由部分の階数，t を $s \leqq t$ なる自然数，$d_1, \cdots, d_{t+r}$ を任意の ℓ-巾数 $\geqq 1$ とする。$d_0 = d = \max d_i$ と置き，$s<t$ の時は，$C_{s+1} = \cdots = C_t = 1$ と置く。このとき，次の条件を満たす d 次巡回拡大 K/k が無限に存在する。

(1) K/k では高々 $t+r+1$ 個の素イデアル $\mathfrak{g}_0, \cdots, \mathfrak{g}_{t+r}$ が分岐し，$\mathfrak{g}_i$ の分岐指数は d_i となる。

(2) K/k の genus group の ℓ-部分の不変数は $(C_1d_1, \cdots, C_td_t)$ となる。

証明は少し複雑である（[10]）。ここで $\mathfrak{g}_i$ は ℓ と素にとれる。

5.4. Mを有限アーベルl-群，その指数をl^nとする。良く知られているように，Mはl^n次巡回拡大$k/\mathbb{Q}$の$Cl(k)$のl-部分として実現できる([11])。ここで$Gal(k/\mathbb{Q})$が位数l^nの元をもつことは本質的である。一般に$\mathbb{Q}$上のgenus理論を用いて，位数l^nのイデアル類をもつアーベル拡大を構成する場合，$Gal(k/\mathbb{Q})$が位数l^nの元をもつことが必要になる。しかし，上の結果をくり返し用いると，次が示される。

n，mを任意の自然数とするとき，$(\mathbb{Z}/l^n\mathbb{Z})^m \hookrightarrow Cl(L)$となる$l^n$次初等アーベル拡大$L/\mathbb{Q}$が無限に存在する。

<u>証明</u>. nについての帰納法で証明する。$n=1$の時は明らか。$k/\mathbb{Q}$をl^n次初等アーベル拡大で，$(\mathbb{Z}/l^n\mathbb{Z})^m \hookrightarrow Cl(k)$となるものとする。このとき，5.3によれば，$l$次巡回拡大$K/k$で，$\mathfrak{q}_0, \cdots, \mathfrak{q}_m$のみ分岐し，$(\mathbb{Z}/l^{n+1}\mathbb{Z})^m \hookrightarrow Gal(K^*/K)$となるものが存在する。このとき$\mathfrak{q}_i$は$k_1/k$で完全分解するから，$p_i = \mathfrak{q}_i \cap \mathbb{Q}$とすると，$k/\mathbb{Q}$が$l$巾次ガロワであることに注意して，$p_i \equiv 1 \pmod{l}$となる。そこで$L'/\mathbb{Q}$を$p_0, \cdots, p_m$が分岐する$l$次巡回拡大とし，$L=kL'$と置く。このとき，Abhyankarの補題から$KL/L$は不分岐である。従って，$K^*L/L$は不分岐アーベル拡大になる。従って$Gal(K^*L/L) \hookleftarrow (\mathbb{Z}/l^{n+1}\mathbb{Z})^m$より求める結果を得る。■

同様にして，$N = \mathbb{Q}(\sqrt[\ell]{a_1}, \cdots, \sqrt[\ell]{a_n})$，$a_i \in \mathbb{Z}$ の形で，$(\mathbb{Z}/\ell^n\mathbb{Z})^m \hookrightarrow Cl(N)$ となるものが無限に存在することも判る。

REFERENCES

[1] G. Cornell, Exponential growth of the l-rank of the class group of the maximal real subfield of cyclotomic fields, Bull. Amer. Math. Soc. 8(1983), 55-57.

[2] A. Fröhlich, On the absolute class group of abelian fields, J. London Math. Soc. **29**(1954), 211-217.

[3] Y. Furuta, The genus field and the genus number in algebraic number fields, Nagoya Math. J. **29**(1967), 281-285.

[4] F. Halter-Koch, Zur Geschlechtertheorie algebraischer Zahlkörper, Arch. Math. **31**(1978), 137-142.

[5] H. Hasse, Zum Existenzatz von Grunwald in der Klassenkörpertheorie, J. reine. angew. Math. **188**(1950), 40-64.

[6] M. Horie, On the genus field in algebraic number fields, Tokyo J. Math. 6(1983), 363-380.

[7] T. Takeuchi, Notes on the class field towers of cyclic fields of degree l, Tōhoku Math. J. (2) **31**(1979), 301-307.

[8] ________, On the l-class field towers of cyclic fields of degree l, Sci. Rep. Niigata Univ. Ser. A **17**(1980), 23-25.

[9] ________, Genus groups of finite Galois extensions (to appear in Proc. Amer. Math. Soc.).

[10] ________, Construction of cyclic extensions of prescribed genus groups (preprint).

[11] O. Yahagi, Construction of number fields with prescribed l-class groups, Tokyo J. Math. **1**(1978), 275-283.