

アーベル拡大の Genus Group とその応用

新潟大教養 竹内照雄 (Terno 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。 $\bar{K}$ を K の絶対類体, $K' \subseteq \bar{K}$ に含まれる k 上最大アーベル拡大とする。このとき, $K \cdot K' \subseteq \bar{K}$ の genus field K^* , $\text{Gal}(K^*/K)$ を K/k の genus group, $\#(\text{Gal}(K^*/K))$ 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 $\mathcal{M}$ 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かりにして, 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 $\mathcal{Q}(k)$ の任意の有限アーベル拡大 M に対し, $\text{Gal}(K^*/k) \cong M$ 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と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 $l \neq 2$ と仮定する。

§2. Genus group

記号を上のようにする。 K/k の最大アーベル部分体を K_0 とする。 v を K/k で分岐する素数, 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 の最大アーベル部分体を $(K_v)_1$, $(K_v)_1/k_v$ の慣性群を 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 $E_{K/k}$ はすべての素数で 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、 $\text{Gal}(K^*/K)$ の構造について公式を作るのがこの節の目標である。

その為には 1 つの素数 l を固定して、 $i = 0, 1, 2, \dots$ に対し $F_i = \{x \in k^* \mid (x) = \mathfrak{m}^{l^i}\}$, $F_i(\mathfrak{f}) = F_i \cap k(\mathfrak{f})$, $\mathcal{N}_i(\mathfrak{f}) = k(\mathfrak{f})^{l^i} N_{K/k}(K(\mathfrak{f})) k_{\mathfrak{f}}$ 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 $\text{rank}_i(A) = \text{rank}(A^{l^{i-1}}/A^{l^i})$ と定義する。

命題 1 ([9, Theorem]). $i \geq 1$ に対して、

$$\begin{aligned} \text{rank}_i(\text{Gal}(K^*/k)) &= \text{rank}_i(\mathcal{Q}(k)) + \sum_v \text{rank}_i(T_v) \\ &\quad + \log_l \left\{ \frac{\#(F_{i-1}(\mathfrak{f})/F_{i-1}(\mathfrak{f}) \cap \mathcal{N}_{i-1}(\mathfrak{f}))}{\#(F_i(\mathfrak{f})/F_i(\mathfrak{f}) \cap \mathcal{N}_i(\mathfrak{f}))} \right\} \end{aligned}$$

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

注意. $\#(\text{Gal}(K^*/K)) = \#(\text{Gal}(K^*/k))/[K_0:k]$ 故に、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, $\text{Gal}(K'/k)$ と $\text{Gal}(K/k)$ から $\text{Gal}(K^*/k)$ を決定することはできない。しかし, k の素数からなる, ある有限集合 T に対して, $\text{Gal}(K_0/k) = \prod_{v \in T} T_v$ (直積) となれば, $\text{Gal}(K^*/k)$ の構造が決まる。実際このとき,

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

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

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

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。以後簡単の爲 $l \neq 2$ と仮定する。又 K/k で無限素数は不岐とする。(以下の議論は, $l=2$ の時も K/k で分岐する素イデアル $\mathfrak{p}$ がすべて $N\mathfrak{p} \equiv 1 \pmod{4}$ を満たせば同様に成立する。従って §5 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, $\zeta_i \neq 1$ の原始 l^i 乗根とし, $k_i = k(\zeta_i)$ と置く。 $F \subseteq k^*$ 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。 $G_i(F) = \text{Gal}(K_i(F)/k_i)$ とし, Kummer pairing $\langle, \rangle_i : G_i \times F \rightarrow \langle \zeta_i \rangle \cong \langle \alpha, a \rangle_i = \alpha(\sqrt[l^i]{a})/\sqrt[l^i]{a}$ によって定義する。 $l \nmid \#$ とする

k のイデアル $\mathfrak{A}$ に対して, $\mathcal{N}(\mathfrak{A}) = N_{K/k}(K(\mathfrak{A})k_{\mathfrak{A}})$ と置く。
 このとき, $\ell \neq 2$ だから, $F \cap \mathcal{N}(\mathfrak{A})k^{\times \ell^i} = F \cap \mathcal{N}(\mathfrak{A})k_i^{\times \ell^i}$
 が成立する。従って, $F/F \cap \mathcal{N}(\mathfrak{A})k^{\times \ell^i}$ の指標は自然に
 $F/F \cap \mathcal{N}(\mathfrak{A})k_i^{\times \ell^i}$ 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 $F = F_i(\mathfrak{A}) = F_i \cap k(\mathfrak{A})$ とする。 F_i の
 定義に注意すれば, $1 \leq j \leq i$ に対して, $K_j(F_i) = K_j(F_i(\mathfrak{A}))$,
 $[K_j(F_i): k_j] < \infty$ となることが判る。

定義. $F_i/F_i \cap \mathcal{N}(\mathfrak{A})k^{\times \ell^j}$ の指標群を $G_j(F_i)$ の部分群と
 見なした時, これを $\Sigma_{K/k}(\mathfrak{A}, F_i)_j$ と表す。特に $\Sigma_{K/k}(\mathfrak{A}, F_i)_i$
 を $\Sigma_{K/k}(\mathfrak{A})_i$ と表す。

$F_i(\mathfrak{A})/F_i(\mathfrak{A}) \cap \mathcal{N}_i(\mathfrak{A}) \cong F_i/F_i \cap \mathcal{N}(\mathfrak{A})k^{\times \ell^i}$ に注意すれば,

$$\#(F_i(\mathfrak{f})/F_i(\mathfrak{f}) \cap \mathcal{N}_i(\mathfrak{f})) = \#(\Sigma_{K/k}(\mathfrak{f})_i)$$

を得る。更にここで,

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

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

さて, $1 \leq j \leq h \leq i$ とするとき, $F_i/F_i \cap \mathcal{N}(\mathfrak{A})k^{\times \ell^j}$ の
 指標群は $F_i/F_i \cap \mathcal{N}(\mathfrak{A})k^{\times \ell^h}$ 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. $1 \leq j \leq h \leq i$ に対して, 次の条件 (1) (2) を満たす
単準同型 $V_h^j : \Sigma_{K/k}(\mathcal{U}, F_i)_j \rightarrow \Sigma_{K/k}(\mathcal{U}, F_i)_h$ が唯一
つ存在する。

(1) $(\sigma, a) \in \Sigma_{K/k}(\mathcal{U}, F_i)_j \times F_i$ に対して,

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

(2) $1 \leq j \leq s \leq h$ 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, $(g, l) = 1$ の場合, $\Sigma_{K/k}(\mathcal{U}_g)$
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. g を l と素な k の素イデアル, $e = e_g \in T_g$ の位数
の l -指数 (即ち, $l^e \parallel \#(T_g)$) とする。このとき,

$$\Sigma_{K/k}(\mathcal{U}_g)_i = \Sigma_{K/k}(g)_i = \begin{cases} \langle \left(\frac{k_i(F_i)/k_i}{\mathfrak{p}_i} \right) \rangle & (i \leq e \text{ のとき}), \\ V_i^e \left(\langle \left(\frac{k_e(F_i)/k_e}{\mathfrak{p}_e} \right) \rangle \right) & (i > e \text{ のとき}) \end{cases}$$

が成立する。但し, $\mathfrak{p}_i$ は g の k_i における 1 つの素因子,
(—) 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 $\mathfrak{p} \in T$ に対して, $\mathfrak{p}$ の中 $\mathfrak{f}_{\mathfrak{p}}$ 及び, $k(\mathfrak{p})/k_{\mathfrak{f}_{\mathfrak{p}}}$ の指標 $\chi_{\mathfrak{p}}$ で conductor が $\mathfrak{f}_{\mathfrak{p}}$, 位数が $l^{e_{\mathfrak{p}}}$ となるものが与えられているとする。このとき, 各 $\mathfrak{p} \in T$ でのみ分岐し, 慣性群が $k(\mathfrak{p})/\ker(\chi_{\mathfrak{p}})$ 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。

$e = \max e_{\mathfrak{p}}$, $\mathfrak{f} = \prod \mathfrak{f}_{\mathfrak{p}}$ と置く。 $\chi_{\mathfrak{p}}$ は $F_i(\mathfrak{f})/F_i(\mathfrak{f}) \cap \ker(\chi_{\mathfrak{p}})$ の指標を引起すから, $i \geq e$ 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 $\varepsilon_T(\mathfrak{p})_i$ と表す。このとき K/k の存在について, 次の示すことができる。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。

命題 3. $i \geq e$ とする。 $G_i(F_i)$ で,

$$(*) \quad \prod_{\mathfrak{p} \in T} \varepsilon_T(\mathfrak{p})_i^{n_{\mathfrak{p}}} = 1 \quad , \quad (n_{\mathfrak{p}}, l) = 1$$

となる自然数 $n_{\mathfrak{p}}$ が存在すれば, ある l^n ($n \leq i$) 次巡回拡大 K/k で, K/k で $\mathfrak{p} \in T$ のみ分岐し, $k(\mathfrak{p})/\ker(\chi_{\mathfrak{p}})$ 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、 $\langle \varepsilon_T(\mathfrak{f})_i \rangle = \Sigma_{k/k}(\mathfrak{f})_i$ となる。

逆に上のような $\mathbb{Q}^n$ 次巡回拡大 K が存在すれば、 $n \geq e$ で、
 $i = n$, $n_{\mathfrak{f}} = 1$, $\varepsilon_{\mathfrak{f}}$ を K の $\mathfrak{f}$ 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 , $\varepsilon_{\mathfrak{f}}$ に対して
 適当な素イデアル $\mathfrak{f}$ を一つ加えて、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。

例. $\mathfrak{f} \nmid e$ とする。このとき、 $\mathfrak{f}$ のみがか岐し、 $\mathfrak{f}$ が完全
 分岐する $\mathbb{Q}^n$ 次巡回拡大が存在する為の必要十分条件は、 $\mathfrak{f}$
 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 $\mathbb{Q}^n$ 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 $\mathfrak{f}$ に対する
 $\Sigma_{k/k}(\mathfrak{f})_i$ 、又は $\varepsilon_T(\mathfrak{f})_i$ 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. $p_i \equiv 1 \pmod{l}$ となる素数, $K_i/\mathbb{Q}$ が p_i のみで分岐する 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 $p_1, \dots, p_n$ の存在が判る。即ち

$$\text{rank}_1(\mathcal{O}(K_1 \cdots K_n)) \geq \frac{l^n - 1}{l - 1} - n$$

となる素数の組 $p_1, \dots, p_n$ が無限に存在する。

証明. 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。 $p_{n+1} \equiv 1 \pmod{l}$ より, p_{n+1} のみで分岐する 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 $p_{n+1} = \wp_1 \cdots \wp_{l^n}$ と分解する。 $K = K_{n+1} k$ として前の議論を適用すると, $\sum_{K/k} (\wp_i) = \{1\}$ 従って,

$$\text{rank}_1(\text{Gal}(K^*/K)) = \text{rank}_1(\mathcal{O}(K)) + l^n - 1 \geq \frac{l^{n+1} - 1}{l - 1} - (n+1)$$

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えば, 特に, 分岐する素数が少なくても, 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

$$\text{rank}_1(\mathcal{O}(M_n N)) \geq \text{rank}_1(\mathcal{O}(N)) + n([N:\mathbb{Q}] - 1)$$

となるものが無限に存在する。

証明．更に $[M_n N : M_n] = [N:\mathbb{Q}]$ ともできることを， n についての帰納法で示す。 $K = M_n N$ と置き，前の記号を用いる。 $K_1(\sqrt[n]{F_1})/\mathbb{Q}$ で完全分解する素数 p_{n+1} をとり， f を M_n での1つの素因子とする。このとき f は $M_n N$ で $f = p_1 \cdots p_m$ ， $m = [N:\mathbb{Q}]$ と分解される。一方 f 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，

$$\begin{aligned} \text{rank}_1(\mathcal{O}(M_{n+1} N)) &\geq \text{rank}_1(\text{Gal}(K^*/K)) \\ &= \text{rank}_1(\mathcal{O}(M_n N)) + [N:\mathbb{Q}] - 1 \geq \text{rank}_1(\mathcal{O}(N)) + (n+1)([N:\mathbb{Q}] - 1) \end{aligned}$$

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， $n \leq 3$ のとき， $M_n/\mathbb{Q}$ を初等アベル拡大にとれる

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 $\text{rank}_1(\mathcal{C}(M_1, M_2)) \geq 3(\ell^3 - 1)$ となるものが無限にあることが判る。

5.3. M を $\mathcal{C}(k)$ 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。

$(C_1, \dots, C_s)$ を k のイデアル類群 $\mathcal{C}(k)$ 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 $s \leq t$ なる自然数、 $d_1, \dots, d_{t+r}$ を任意の ℓ -巾数 ≥ 1 とする。 $d_0 = d = \max d_i$ と置き、 $s < t$ の時は、 $C_{s+1} = \dots = C_t = 1$ 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 $\mathfrak{f}_0, \dots, \mathfrak{f}_{t+r}$ が分岐し、 $\mathfrak{f}_i$ 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 $(C_1 d_1, \dots, C_t d_t)$ となる。

証明は少し複雑である ([10])。ここで $\mathfrak{f}_i$ 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 $\mathcal{O}(k)$ の l -部分として実現できる ([11])。ここで $\text{Gal}(k/\mathbb{Q})$ 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, $\text{Gal}(k/\mathbb{Q})$ 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, $(\mathbb{Z}/l^m\mathbb{Z})^m \hookrightarrow \mathcal{O}(L)$ 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。

証明. 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, $(\mathbb{Z}/l^m\mathbb{Z})^m \hookrightarrow \mathcal{O}(k)$ 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, $g_0, \dots, g_m$ のみか岐し, $(\mathbb{Z}/l^m\mathbb{Z})^m \hookrightarrow \text{Gal}(K^*/k)$ となるものが存在する。このとき g_i は k_i/k で完全分解するから, $p_i = g_i \cap \mathbb{Q}$ とすると, $k/\mathbb{Q}$ が l や次がロワであることに注意して, $p_i \equiv 1 \pmod{l}$ となる。そこで $L'/\mathbb{Q} \cong p_0, \dots, p_m$ が岐する 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 は不岐である。従って, K^*L/L は不岐アーベル拡大になる。従って $\text{Gal}(K^*L/L) \hookrightarrow (\mathbb{Z}/l^m\mathbb{Z})^m$ より求める結果を得る。■

同様にして, $N = \mathbb{Q}(\sqrt[l]{a_1}, \dots, \sqrt[l]{a_n}), a_i \in \mathbb{Z}$ の形で,
 $(\mathbb{Z}/l^n\mathbb{Z})^m \hookrightarrow \mathcal{C}(N)$ 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 Existenzsatz 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 , Tôhoku 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.