数理解析研究所講究録
第230巻 1975年 13-25

代数体の絶対ガロア群について

東京工大　理学部　　小松啓一

標数0の体Fに対して，$\bar{F}$によってFの代数的閉包，G_FによってFの絶対ガロア群，即ちFと$\bar{F}$の間の位相的ガロア群をあらわす。この小論では絶対ガロア群どうしの同型は位相群としての同型を意味する。$\mathbb{Q}$を有理数体，k_1，k_2を有限次代数体，即ち$\mathbb{Q}$の有限次拡大体とし，さらに次のような記号を用いる。

$\zeta_{k_i}(s)$；k_iのzeta関数　　$C(k_i)$；k_iのイデアル類群

h_i；k_iの類数　　R_i；k_iのregulator

D_i；k_iの判別式　　$k_{iA}^{\times}$；k_iのイデール群

ただし$i=1,2$である。この小論では次の定理の証明を目標とする。

定理1．有限次代数体k_1，k_2について，それらの絶対ガロア群をG_{k_1}，G_{k_2}とする。このとき，$G_{k_1}\cong G_{k_2}$ならば$\zeta_{k_1}(s)=\zeta_{k_2}(s)$，$C(k_1)\cong C(k_2)$，$R_1=R_2$，$D_1=D_2$，$k_{1A}^{\times}\cong k_{2A}^{\times}$となる。

定理2．有限次代数体 k_1, k_2 で $\zeta_{k_1}(s)=\zeta_{k_2}(s)$ 且つ $G_{k_1}\not\cong G_{k_2}$ となるものが存在する。

さてここで次の補題を引用する。

補題1．（[2]の363ページ参照） $L/\mathbb{Q}$ を有限次ガロア拡大 k_1, k_2 を L の部分体．$G=Gal(L/\mathbb{Q})$．$H_i=Gal(L/k_i)$ とし．$\sigma\in G$ に対して $C(\sigma)=\{\tau^{-1}\sigma\tau \mid \tau\in G\}$ とする。このとき次は互いに同値である。

(i) $\zeta_{k_1}(s)=\zeta_{k_2}(s)$

(ii) $\forall\sigma\in G$ に対して $card(C(\sigma)\cap H_1)=card(C(\sigma)\cap H_2)$

（$card(C(\sigma)\cap H_i)$ は $C(\sigma)\cap H_i$ の元の個数をあらわす。）

系1．記号は補題1のままとする。$k_1/\mathbb{Q}$ が有限次ガロア拡大で．$\zeta_{k_1}(s)=\zeta_{k_2}(s)$ ならば $k_1=k_2$ となる。

証明．H_1 は G の正規部分群だから $\sigma\in G$ に対して．$C(\sigma)\cap H_1$ は $C(\sigma)$ か又は空集合である。(ii)より $C(\sigma)\cap H_1=C(\sigma)\Leftrightarrow C(\sigma)\cap H_2=C(\sigma)$ 又．$C(\sigma)\cap H_1$ が空集合 $\Leftrightarrow$ $C(\sigma)\cap H_2$ が空集合。よって $H_1=H_2$。即ち $k_1=k_2$。

系2．記号は補題1のままとする。M_i を k_i に含まれる $\mathbb{Q}$ の最大のガロア拡大とする。（$i=1,2$） このとき $\zeta_{k_1}(s)=\zeta_{k_2}(s)$ ならば $M_1=M_2$ となる。

証明．G の中で $\bigcup_{\sigma\in G}\sigma^{-1}H_i\sigma$ によって生成される部分群を $<\bigcup_{\sigma\in G}\sigma^{-1}H_i\sigma>$ とすれば．$Gal(L/M_i)=<\bigcup_{\sigma\in G}\sigma^{-1}H_i\sigma>$ となる。(ii)

より $\bigcup_{\sigma\in G}\sigma^{-1}H_1\sigma = \bigcup_{\sigma\in G}\sigma^{-1}H_2\sigma$ となるから $M_1 = M_2$ を得る。

体 F に対して μ_F によって，F に含まれる 1 のべき根全体をあらわす。

補題2．r_1，r_2 をそれぞれ k_1 の実素点，複素素点の個数とし，r_1'，r_2' をそれぞれ k_2 の実素点，複素素点の個数とする。このとき，$\zeta_{k_1}(s) = \zeta_{k_2}(s)$ ならば $r_1 = r_1'$，$r_2 = r_2'$，$D_1 = D_2$，$h_1R_1 = h_2R_2$ となる。

証明．$\zeta_{k_1}(s)$ は $s = -1$ で r_2 位の零点をもち，$s = -2$ で r_1+r_2 位の零点をもつ。よって $\zeta_{k_1}(s) = \zeta_{k_2}(s)$ より $r_1 = r_1'$，$r_2 = r_2'$ となる。

$$Z_{k_1}(s) = \left(\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\right)^{r_1}\left((2\pi)^{1-s}\Gamma(s)\right)^{r_2}\zeta_{k_1}(s)$$

$$Z_{k_2}(s) = \left(\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\right)^{r_1'}\left((2\pi)^{1-s}\Gamma(s)\right)^{r_2'}\zeta_{k_2}(s)$$

と置く。このとき $Z_{k_1}(s) = Z_{k_2}(s)$ となる。M_1，M_2 を補題1の系2のようにとる。$\mu_{k_i} = \mu_{M_i}$ 且つ $M_1 = M_2$ より $\mu_{k_1} = \mu_{k_2}$ となる。さらに a_i を μ_{k_i} の元の個数とすれば $a_1 = a_2$ となる。よく知られているように，

$$\lim_{s\to 0} s\,Z_{k_1}(s) = -\frac{2^{r_1}(2\pi)^{r_2}h_1R_1}{a_1}$$

$$\lim_{s\to 0} s\,Z_{k_2}(s) = -\frac{2^{r_1'}(2\pi)^{r_2'}h_2R_2}{a_2}$$ となる。（[9]の129ページ参照）$r_1 = r_1'$，$r_2 = r_2'$，$a_1 = a_2$ より $h_1R_1 = h_2R_2$ を得る。さらに

$$\lim_{s\to 1}(s-1)\zeta_{k_1}(s) = |D_1|^{-\frac{1}{2}}\frac{2^{r_1}(2\pi)^{r_2}h_1R_1}{a_1}$$

$$\lim_{s\to 1}(s-1)\zeta_{k_2}(s) = |D_2|^{-\frac{1}{2}}\frac{2^{r_1'}(2\pi)^{r_2'}h_2R_2}{a_2}$$

となる事が知られている。（[9]の129ページ参照）

よって $|D_1|=|D_2|$ となり．D_1 の符号は $(-1)^{r_2}$ D_2 の符号は $(-1)^{r_2'}$ より．$D_1=D_2$ を得る。（証明終り）

補題1，系1，系2，補題2から $\zeta_{k_1}(s)=\zeta_{k_2}(s)$ ならば．$k_1\cong k_2$ が成立するのでわないかという問題が考えられるがそれに対しては次のような Gassmann による反例がある（[3]参照）補題1の記号をもちいて．$Gal(L/\mathbb{Q})=S_6$，$H_1=\{1,(1,2)(3,4),(1,3)(2,4),(1\ 4)(2\ 3)\}$，$H_2=\{1,(1\ 2)(3\ 4),(1\ 2)(5\ 6),(3\ 4)(5\ 6)\}$（ただし S_6 は6次対称群．$(i\ j)$ は互換である。）このとき H_1，H_2 は補題1の(ii)の条件を満足するが．S_6 の中で共役でない。

$\mathbb{Q}$ の代数的閉包 $\overline{\mathbb{Q}}$ の非アルキメデス的附値を $\bar{v}$ とし．$\bar{v}$ の $\mathbb{Q}$ への制限が有理素数 p に対応しているとする。$k/\mathbb{Q}$ を有限次拡大とし．$\bar{v}$ の k への制限を v とする。k の v による完備化を k_v とすれば．k_v の中での $\mathbb{Q}$ の位相的閉包は p-進体 $\mathbb{Q}_p$ となる。さらに $k_v/\mathbb{Q}_p$ は有限次である。

$D_k(\bar{v})=\{\sigma\in G_k \mid \bar{v}(x^\sigma)=\bar{v}(x)\ \forall x\in\overline{\mathbb{Q}}\}$ と置く。$\overline{\mathbb{Q}}$ を $\overline{k_v}$ の中へ適当に埋蔵してやれば．

(1) $G_{k_v}\cong G_{\overline{\mathbb{Q}}\cap k_v}=D_k(\bar{v})$ を得る。

よって $D_{\mathfrak{P}}(\bar{v})$ は $G_{\mathbb{Q}_p}$ の開部分群と位相群として同型になる。$G_{\mathbb{Q}}$ の元 σ に対して、$\bar{v}^{\sigma}$ を $\bar{v}^{\sigma}(x) = \bar{v}(x^{\sigma})$ $\forall x \in \bar{\mathbb{Q}}$ によって定義する。v の $\bar{\mathbb{Q}}$ への延長を $\bar{v}$ とすれば、$G_{\mathfrak{P}}$ の元 τ で $\bar{v}' = \bar{v}^{\tau}$ となるものが存在する事が知られている。よって

(2) $D_{\mathfrak{P}}(\bar{v}') = \tau D_{\mathfrak{P}}(\bar{v}) \tau^{-1}$ となる。

定義 G を pro-finite group とし、p を有理素数とする。G が $G_{\mathbb{Q}_p}$ の開部分群と位相群として同型なとき、G は L_p-group といわれる。（[7] 参照）

ここで次の補題を引用する。

補題3.（[7] 参照）$\mathfrak{P}/\mathbb{Q}$ を有限次拡大、$K/\mathfrak{P}$ を代数拡大とする。このとき次は同値である。（p は有理素数とする。）

(i) G_K は $G_{\mathfrak{P}}$ の（包含関係についての）maximal L_p-group。

(ii) p の上にある $\bar{\mathbb{Q}}$ の valuation（附値）$\bar{v}$ で $D_{\mathfrak{P}}(\bar{v}) = G_K$ となるものがある。

上のような $\bar{v}$ は同値な附値を除いて一意的にきまる。

$\mathfrak{P}_i/\mathbb{Q}$ を有限次拡大、$\mathcal{O}_{\mathfrak{P}_i}$ を $\mathfrak{P}_i$ の整数環、$\mathrm{Spec}(\mathcal{O}_{\mathfrak{P}_i})$ を $\mathcal{O}_{\mathfrak{P}_i}$ の素イデアル全体とする。（$i=1,2$）$G_{\mathfrak{P}_1} \cong G_{\mathfrak{P}_2}$ とし、$G_{\mathfrak{P}_1}$ から $G_{\mathfrak{P}_2}$ の上への同型写像を入とする。このとき Neukirch は次のようにして、$\mathrm{Spec}(\mathcal{O}_{\mathfrak{P}_1})$ から $\mathrm{Spec}(\mathcal{O}_{\mathfrak{P}_2})$ への bijection $\underline{\text{入}}_{\mathfrak{P}_1}$ を導いた。（[7] 参照）$\mathfrak{P}_1 \in \mathrm{Spec}(\mathcal{O}_{\mathfrak{P}_1})$ とし、$\mathfrak{P}_1$ は有理素数 p

の上にあるとする。即ち $\mathfrak{P}_1$ は ideal $p\mathcal{O}_{k_1}$ を割り切る。$\mathfrak{P}_1$ に対応する k_1 の附値を v_1 とし、v_1 の Ω への延長を $\bar{v}_1$ とする。補題3より $D_{k_1}(\bar{v}_1)$ は G_{k_1} の maximal L_p-group である。よって $\lambda(D_{k_1}(\bar{v}_1))$ は G_{k_2} の maximal L_p-group となり、補題3より p の上にある Ω の附値 $\bar{v}_2$ で $D_{k_2}(\bar{v}_2)=\lambda(D_{k_1}(\bar{v}_1))$ となるものが存在して、同値なものを除いて一意にきまる。$\bar{v}_2$ の k_2 への制限に対応する素イデアルを $\mathfrak{P}_{\lambda,k_1}(\mathfrak{P}_1)$ と定義する。$\mathfrak{P}_{\lambda,k_1}$ が well-defined なる事を示す。v_1 の Ω への延長のしかたに無関係に $\mathfrak{P}_{\lambda,k_1}$ がきまる事をいえばよい。v_1 の Ω への延長を $\bar{v}_1'$ とする。(2)より G_{k_1} の元 τ_1 で $D_{k_1}(\bar{v}_1')=\tau_1 D_{k_1}(\bar{v}_1)\tau_1^{-1}$ となるものがある事がわかる。よって $\lambda(D_{k_1}(\bar{v}_1'))=\lambda(\tau_1)\lambda(D_{k_1}(\bar{v}_1))\lambda(\tau_1)^{-1}=D_{k_2}(\bar{v}_2^{\lambda(\tau_1)})$ となる。$\lambda(\tau_1)\in G_{k_2}$ より $\bar{v}_2^{\lambda(\tau_1)}$ の k_2 への制限と $\bar{v}_2$ の k_2 への制限は一致する。よって $\mathfrak{P}_{\lambda,k_1}$ は well-defined。λ の逆写像 $\lambda^{-1}; G_{k_2}\xrightarrow{\sim} G_{k_1}$ に対して $\mathfrak{P}_{\lambda^{-1},k_2}$ を考えれば、

$$\mathfrak{P}_{\lambda,k_1}\circ\mathfrak{P}_{\lambda^{-1},k_2}=\mathrm{Id}_{\mathrm{Spec}(\mathcal{O}_{k_2})}$$

$$\mathfrak{P}_{\lambda^{-1},k_2}\circ\mathfrak{P}_{\lambda,k_1}=\mathrm{Id}_{\mathrm{Spec}(\mathcal{O}_{k_1})}$$

となる事は簡単にわかる。従って $\mathfrak{P}_{\lambda,k_1}; \mathrm{Spec}(\mathcal{O}_{k_1})\to\mathrm{Spec}(\mathcal{O}_{k_2})$ は bijection。$\mathfrak{P}_1$ に対応する k_1 の附値 v_1 による k_1 の完備化を $k_{1\mathfrak{P}_1}$ と記せば、(1)より

$$G_{k_{1\mathfrak{P}_1}}\cong G_{k_{2\mathfrak{P}_{\lambda,k_1}(\mathfrak{P}_1)}}\qquad \forall\mathfrak{P}_1\in\mathrm{Spec}(\mathcal{O}_{k_1}) \tag{3}$$

を得る。

K_1/k_1 を有限次拡大とすれば、G_{K_1} は G_{k_1} の開部分群だから $\lambda(G_{K_1})$ は G_{k_2} の開部分群となり、k_2 の有限次拡大 K_2 で $\lambda(G_{K_1})=G_{K_2}$

となるものが存在する事がわかる。λ の G_{K_1} への制限 $\lambda|_{G_{K_1}}$ に対して Neukirch の bijection $\text{重}_{\lambda|_{G_{K_1}}, K_1} ; Spec(\mathcal{O}_{K_1}) \to Spec(\mathcal{O}_{K_2})$ を考えられるが、これを $\text{重}_{\lambda, K_1}$ と略記する。$\mathfrak{P}_1 \in Spec(\mathcal{O}_{\mathfrak{k}_1})$ に対して $\mathfrak{P}_1$ の $\mathfrak{k}_1/\mathbb{Q}$ における分岐指数を $e_{\mathfrak{k}_1}(\mathfrak{P}_1)$ であらわす。$Spec(\mathcal{O}_{\mathfrak{k}_2})$ $Spec(\mathcal{O}_{K_1})$, $Spec(\mathcal{O}_{K_2})$ の元についても同様の記号をもちいる。

$F_i/\mathbb{Q}_p$ を m_i 次拡大とし、f_i を相対次数、e_i を分岐指数、μ_{F_i} の p-sylow 群の位数を p^{δ_i} とする。$(i=1,2)$ (G_{F_i}, G_{F_i}) によって G_{F_i} の topological commutator group を表わす。このとき局所類体論より次の事がわかる。

(4) $G_{F_i}^{ab} \overset{Art}{\cong} G_{F_i}/(G_{F_i}, G_{F_i}) \cong \prod_{\ell} \mathbb{Z}_\ell \times \mathbb{Z}_p^{m_i} \times \mathbb{Z}/(p^{f_i}-1)\mathbb{Z} \times \mathbb{Z}/p^{\delta_i}\mathbb{Z}$

(ただし、$\prod_{\ell}$ はすべての素数 ℓ をわたり、$\mathbb{Z}$ は有理整数環 $\mathbb{Z}_\ell$ は ℓ-adic integer ring をあらわす。)

さらに F_i の乗法群を $F_i^\times$ とすれば

(5) $F_i^\times \cong \mathbb{Z} \times \mathbb{Z}_p^{m_i} \times \mathbb{Z}/(p^{f_i}-1)\mathbb{Z} \times \mathbb{Z}/p^{\delta_i}\mathbb{Z}$ となる事が知られている。

補題4. ([5]参照) 記号は上のとうりとする。

$G_{F_1} \cong G_{F_2} \Rightarrow F_1^\times \cong F_2^\times$, $e_1 = e_2$, $p^{f_1} = p^{f_2}$

証明. $G_{F_1} \cong G_{F_2}$ より $G_{F_1}^{ab} \cong G_{F_2}^{ab}$. よって (4) を用れば、

$\prod_{\ell} \mathbb{Z}_\ell \times \mathbb{Z}_p^{m_1} \times \mathbb{Z}/(p^{f_1}-1)\mathbb{Z} \times \mathbb{Z}/p^{\delta_1}\mathbb{Z} \cong \prod_{\ell} \mathbb{Z}_\ell \times \mathbb{Z}_p^{m_2} \times \mathbb{Z}/(p^{f_2}-1)\mathbb{Z} \times \mathbb{Z}/p^{\delta_2}\mathbb{Z}$

となる。$G_{F_1}^{ab}$ と $G_{F_2}^{ab}$ の maximal torsion subgroup は互いに同型だから、(6) $\mathbb{Z}/(p^{f_1}-1)\mathbb{Z} \times \mathbb{Z}/p^{\delta_1}\mathbb{Z} \cong \mathbb{Z}/(p^{f_2}-1)\mathbb{Z} \times \mathbb{Z}/p^{\delta_2}\mathbb{Z}$ を得る。

よって $p^{f_1} = p^{f_2}$ となる。$G_{F_1}^{ab}$ と $G_{F_2}^{ab}$ の p-sylow 群は互いに同型だから $\mathbb{Z}_p^{m_1+1} \times \mathbb{Z}/p^{s_1}\mathbb{Z} \cong \mathbb{Z}_p^{m_2+1} \times \mathbb{Z}/p^{s_2}\mathbb{Z}$ となる。よって $m_1 = m_2$ となり、$m_i = e_i f_i$ より $e_1 = e_2$ を得る。(5), (6) および $m_1 = m_2$ より $F_1^\times \cong F_2^\times$ を得る。(証明終り)

補題5.([5]参照) $k_1/\mathbb{Q}$, $k_2/\mathbb{Q}$, K_1/k_1 を有限次拡大とし、$G_{k_1} \cong G_{k_2}$ とする。G_{k_1} から G_{k_2} の上への同型写像を λ とし、$\lambda(G_{K_1}) = G_{K_2}$ とする。$\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_{k_1})$, $\mathfrak{P} \in \mathrm{Spec}(\mathcal{O}_{K_1})$ とする。このとき次が成立する。

(i) $e_{k_1}(\mathfrak{p}) = e_{k_2}(\underline{\lambda}_{,k_1}(\mathfrak{p}))$, $e_{K_1}(\mathfrak{P}) = e_{K_2}(\underline{\lambda}_{,K_1}(\mathfrak{P}))$

$N_{k_1/\mathbb{Q}}(\mathfrak{p}) = N_{k_2/\mathbb{Q}}(\underline{\lambda}_{,k_1}(\mathfrak{p}))$, $N_{K_1/\mathbb{Q}}(\mathfrak{P}) = N_{K_2/\mathbb{Q}}(\underline{\lambda}_{,K_1}(\mathfrak{P}))$

(ただし $N_{k_i/\mathbb{Q}}$, $N_{K_i/\mathbb{Q}}$ はイデアルの絶対ノルム)

(ii) $\mathfrak{P}$ が $\mathfrak{p}$ の上にある。$\iff$ $\underline{\lambda}_{,K_1}(\mathfrak{P})$ は $\underline{\lambda}_{,k_1}(\mathfrak{p})$ の上にある。

(iii) $k_{1,\mathfrak{p}}^\times \cong k_{2,\underline{\lambda}_{,k_1}(\mathfrak{p})}^\times$, $K_{1,\mathfrak{P}}^\times \cong K_{2,\underline{\lambda}_{,K_1}(\mathfrak{P})}^\times$

証明. $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_{k_1})$ とし、$\mathfrak{p}$ は有理素数 p の上にあるとする。

(i) の証明. $\mathfrak{p}$ の $k_1/\mathbb{Q}$ における分岐指数 $e_{k_1}(\mathfrak{p})$ は $k_{1,\mathfrak{p}}/\mathbb{Q}_p$ の分岐指数に等しく、$k_{1,\mathfrak{p}}/\mathbb{Q}_p$ の相対次数を f とすれば、$N_{k_1/\mathbb{Q}}(\mathfrak{p}) = p^f$ となる。よって(3)および補題4から $e_{k_1}(\mathfrak{p}) = e_{k_2}(\underline{\lambda}_{,k_1}(\mathfrak{p}))$, $N_{k_1/\mathbb{Q}}(\mathfrak{p}) = N_{k_2/\mathbb{Q}}(\underline{\lambda}_{,k_1}(\mathfrak{p}))$ が成立する。$\mathfrak{P} \in \mathrm{Spec}(\mathcal{O}_{K_1})$ についても同様である。

(ii) の証明. $\mathfrak{P}$ が $\mathfrak{p}$ の上にあるとする。$\mathfrak{P}$ に対応する K_1 の附

値の $\bar{\mathbb{Q}}$ への延長を v_1 とする。v_1 の $\mathfrak{k}_1$ への制限は $\mathfrak{p}$ に対応する $\mathfrak{k}_1$ の附値である。補題3. および $\mathfrak{P}_{\lambda,\mathfrak{k}_1}$ の定義の仕方をみれば $\lambda(D_{\mathfrak{k}_1}(v_1)) = D_{\mathfrak{k}_2}(v_2)$ となる $\bar{\mathbb{Q}}$ の附値 v_2 で $\mathfrak{p}$ の上にあるものが存在する事がわかる。$D_{K_1}(v_1) = D_{\mathfrak{k}_1}(v_1) \cap G_{K_1}$, $\lambda(D_{K_1}(v_1)) = D_{\mathfrak{k}_2}(v_2) \cap G_{K_2} = D_{K_2}(v_2)$ よって $\mathfrak{P}_{\lambda,K_1}(\mathfrak{P})$ は v_2 の K_2 への制限に対応する K_2 の素イデアル $\mathfrak{P}_{\lambda,\mathfrak{k}_1}(\mathfrak{p})$ は v_2 の $\mathfrak{k}_2$ への制限に対応する $\mathfrak{k}_2$ の素イデアル。よって $\mathfrak{P}_{\lambda,K_1}(\mathfrak{P})$ は $\mathfrak{P}_{\lambda,\mathfrak{k}_1}(\mathfrak{p})$ の上にある。逆は $\mathfrak{P}_{\lambda^{-1},K_2}$, $\mathfrak{P}_{\lambda^{-1},\mathfrak{k}_2}$ を考える事によりわかる。

(iii) の証明. (3) および補題4から明らか。(証明終り)

上の補題5は [7] の Lemma 3 の精密化である。

K_1 を $\mathfrak{k}_1$ の絶対類体. 即ち最大不分岐 abel 拡大とする。このとき $\mathrm{Gal}(K_1/\mathfrak{k}_1) \cong C(\mathfrak{k}_1)$ なる事がしられている。補題5の仮定と記号のもとで. 補題5の (i), (ii) から K_2 は $\mathfrak{k}_2$ の不分岐拡大なる事がわかる。さらに $\mathrm{Gal}(K_1/\mathfrak{k}_1) \cong G_{\mathfrak{k}_1}/G_{K_1} \cong G_{\mathfrak{k}_2}/G_{K_2} \cong \mathrm{Gal}(K_2/\mathfrak{k}_2)$ より K_2 は $\mathfrak{k}_2$ の abel 拡大なる事がわかる。よって K_2' を $\mathfrak{k}_2$ の絶対類体とすれば $K_2' \supset K_2$ となる。$\lambda^{-1}(G_{K_2'}) = G_{K_1'}$ とすれば, K_1' は $\mathfrak{k}_1$ の不分岐 abel 拡大となり. $K_1 \supset K_1'$ となる。$G_{K_2} = \lambda(G_{K_1}) \subset \lambda(G_{K_1'}) = G_{K_2'}$ より $K_2 \supset K_2'$。よって $K_2 = K_2'$. 即ち K_2 は $\mathfrak{k}_2$ の絶対類体となる. 故に $C(\mathfrak{k}_1) \cong C(\mathfrak{k}_2)$ なる事がわかる。以上をまとめて次の系を得る。

<u>系</u>. $\mathfrak{k}_1/\mathbb{Q}$, $\mathfrak{k}_2/\mathbb{Q}$ を有限次拡大とする。このとき $G_{\mathfrak{k}_1} \cong G_{\mathfrak{k}_2}$ な

らば $C(k_1) \cong C(k_2)$ となる。

ここまでくれば、定理1の証明は容易である。

定理1の証明. G_{k_1} から G_{k_2} の上への同型写像を入とする。複素数 s について、補題5より、

$$\zeta_{k_1}(s) = \prod_{\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_{k_1})} \left(1 - N_{k_1/\mathbb{Q}}(\mathfrak{p})^{-s}\right)^{-1} = \prod_{\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_{k_1})} \left(1 - N_{k_2/\mathbb{Q}}(\text{入}, k_1(\mathfrak{p}))^{-s}\right)^{-1} = \zeta_{k_2}(s)$$

$(\mathrm{Re}\, s > 1)$ よって補題2より $D_1 = D_2$, $h_1 R_1 = h_2 R_2$。補題5の系から $C(k_1) \cong C(k_2)$ より $h_1 = h_2$。よって $R_1 = R_2$。補題5の(iii)および補題2の $r_1 = r_1'$, $r_2 = r_2'$ より $k_{1A}^{\times} \cong k_{2A}^{\times}$ がわかる。

(証明終り)

補題6. $k_1/\mathbb{Q}$, $k_2/\mathbb{Q}$ を有限次拡大、L によって k_1 を含む $\mathbb{Q}$ の有限次ガロア拡大を表わす。$G_{k_1} \cong G_{k_2}$ ならば L つ k_2 且つ $\mathrm{Gal}(L/k_1) \cong \mathrm{Gal}(L/k_2)$ となる。

証明. G_{k_1} から G_{k_2} の上への同型写像を入とする。$\text{入}(G_L)$ は G_{k_2} の開部分群だから k_2 の有限次拡大 L' で $\text{入}(G_L) = G_{L'}$ となるものがある。定理1より $\zeta_L(s) = \zeta_{L'}(s)$ だから補題1の系1より $L = L'$ となり、L つ k_2 を得る。$\mathrm{Gal}(L/k_i) \cong G_{k_i}/G_L$ 且つ入により G_{k_1}/G_L から G_{k_2}/G_L の上への同型が導かれるから $\mathrm{Gal}(L/k_1) \cong \mathrm{Gal}(L/k_2)$。

(証明終り)

定理2を示すためには、補題6から、補題1の(ii)の条件をみたす H_1, H_2 で $H_1 \not\subset H_2$ となるものをみつければよい事になった。p を奇素数、H_1 を位数 p^3 の基本 abel 群、即ち $H_1 \cong (\mathbb{Z}/p\mathbb{Z})^3$。

H_2を位数p^3の非可換群で単位元e以外の元の位数はすべてpなるものとする。(その存在は[1]の187ページ例題8.2) S_{p^3}を$\{1, 2, \cdots, p^3\}$の置換全体のなす群とし、H_iの元をならべて$a_1, \cdots, a_{p^3}$とする。H_iの元aに対して、S_{p^3}の元σで

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_{p^3} \\ a_1 a & a_2 a & \cdots & a_{p^3} a \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \cdots & a_{p^3} \\ a_{\sigma(1)} & a_{\sigma(2)} & \cdots & a_{\sigma(p^3)} \end{pmatrix}$$

となるものを対応させる。これによってH_iをS_{p^3}にうめこんだものを再びH_iと記す。このとき次が成立する。

補題7. H_1, H_2, S_{p^3}を上のようにとる。このとき

$\mathrm{card}(C(\sigma) \cap H_1) = \mathrm{card}(C(\sigma) \cap H_2)$が$S_{p^3}$のすべての元$\sigma$に対して成立する。

証明. H_iのS_{p^3}へのいれかたから、単位元e以外のH_iのすべての元τは$\tau(j) \neq j$ $(j = 1, \cdots, p^3)$さらに$\tau^p = e$。よってτを互いに共通文字を含まない巡回置換の積に分解すれば、$\tau = (j_{11} \cdots j_{1p}) \cdots (j_{p^2 1} \cdots j_{p^2 p})$というように長さpの巡回置換$p^2$個の積となる。$S_{p^3}$の2つの元が互いに共役であるための必要十分条件は両者の巡回因子分解の型が一致する事である。したがって$H_1 \cup H_2$のe以外の元τ_1, τ_2はS_{p^3}の中で共役である。よって

$$\mathrm{card}(C(\tau) \cap H_1) = \mathrm{card}(C(\tau) \cap H_2) = p^3 - 1 \quad \tau \in H_1 \cup H_2, \ \tau \neq e$$

$$\mathrm{card}(C(e) \cap H_1) = \mathrm{card}(C(e) \cap H_2) = 1$$

S_{p^3}の元$\sigma \neq e$について $C(\sigma) \cap H_1 = \phi \Leftrightarrow C(\sigma) \cap H_2 = \phi$

$C(\sigma)\cap H_1\neq\phi \Leftrightarrow C(\sigma)\cap H_2\neq\phi \Leftrightarrow \mathrm{card}(C(\sigma)\cap H_1)=\mathrm{card}(C(\sigma)\cap H_2)=p^3-1$ よってすべての元 σ に対して $\mathrm{card}(C(\sigma)\cap H_1)=\mathrm{card}(C(\sigma)\cap H_2)$。ただし ϕ は空集合を表わす。 (証明終り)

定理2の証明. よく知られているように S_{p^3} と同型なガロア群をもつ $\mathbb{Q}$ のガロア拡大は存在する。それを L とし, $\mathrm{Gal}(L/\mathbb{Q})$ から S_{p^3} の上への同型写像を φ とする。S_{p^3} の部分群 H_1, H_2 を上のようにとり, $\varphi(\mathrm{Gal}(L/k_i))=H_i$ となるように $L/\mathbb{Q}$ の中間体 k_1, k_2 をとる。H_1, H_2 は補題1の(ii)の条件を満足するから, $\zeta_{k_1}(s)=\zeta_{k_2}(s)$ となる。一方 $H_1\not\cong H_2$ より $G_{k_1}\not\cong G_{k_2}$ (証明終り)

定理1, 定理2から $\zeta_{k_1}(s)=\zeta_{k_2}(s)$ よりも $G_{k_1}\cong G_{k_2}$ の方が本当に強い条件である事がわかった。

文　献

[1] 浅野啓三, 永尾汎, 群論, 岩波書店, (1965)

[2] Cassels-Fröhlich, Algebraic Number Theory, Academic Press, London & New York (1967)

[3] F. Gassmann, Bemerkungen zur vorsthenden Arbeit von Hurwitz Math. Zeitsch. 25, 665-675 (1926)

[4] T. Kanno, Automorphisms of the Galois group of the algebraic closure of the rational number field, Kodai Math. Sem. Report, 25, 446-448 (1973)

[5] K. Komatsu, The Galois group of the algebraic closure of an algebraic number field, Kodai Math. Sem. Report, 26, 48-52 (1974)

[6] S. Nakatsuchi, A note on Kronecker's "Randwertsatz", Journal of Math. of Kyoto University, 13, 129-137, (1972)

[7] J. Neukirch, Kennzeichnung der p-adischen und der endlich algebraischen Zahlkörper, Inventiones Math., 6, 296-314 (1969)

[8] ———, Kennzeichnung der endlich-algebraischen Zahlkörper durch die Galoisgruppe der maximal auflösbaren Erweiterung, J. Reine Angew. Math., 238, 135-147 (1969)

[9] A. Weil, Basic Number Theory, Springer-Verlag (1967)