数理解析研究所講究録
第378巻 1980年 47-60

岩沢類数公式の一般化

東大 理　　片岡 俊孝

§0. Introduction.

p を素数、k を有限次代数体、K をその無限次代数拡大とする。

もし、K/k が $\mathbb{Z}_p$-拡大 (i.e. K/k は Galois 拡大であって、$\mathrm{Gal}(K/k)$ は、位相群として $\mathbb{Z}_p$ と isomorphic) であるとすれば、拡大 K/k の中間体は次のように書ける。

(α) 整数 $n \geqq 0$ に対して、k 上の拡大次数が p^n である K/k の中間体 k_n が唯一つ存在する。

(β) $k = k_0 \subset k_1 \subset k_2 \subset \cdots \subset k_n \subset \cdots \subset K$。

(γ) $K = \bigcup_{n=0}^{\infty} k_n$。

このとき、k_n の p-class group (i.e. イデアル類群の p-Sylow group) の位数について次のことが言える。

定理（岩沢）. p、k、K、k_n は上のとおりとする。k_n の p-class group の位数を h_n とおく。すると、非負整数 λ、μ と整数 ν が存在して

$$h_n = p^{e_n},\quad e_n = \lambda n + \mu p^n + \nu$$

が十分大きな n に対して成り立つ。

さて、この岩沢の定理を、(α)～(γ)をみたす有限次代数体 k 上の無限次代数拡大 K に対して拡張することを考えよう。素数 p に対して、(α)～(γ)をみたす拡大 K/k に対して、k_n の p-class group の位数を h_n とかく。

次の(1)及び(2)の拡大に対しては拡張できる。

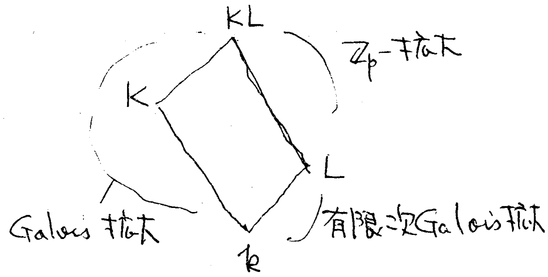
(1) 次の$(*)_p$をみたす拡大 K/k。ただし、p は奇素数。

$(*)_p$ $\exists L$; k 上の有限次Galois拡大 s.t.

(1) KL/k : Galois拡大,

(2) KL/L : $\mathbb{Z}_p$-拡大,

(3) $K \cap L = k$.



(2) $k = \mathbb{Q}$、K は k に p の p 巾乗根（$\in \mathbb{R}$）をすべて添加した体 $\mathbb{Q}(\sqrt[p^\infty]{p})$。ただし、$p$ は regular prime。このときは、$k_n = \mathbb{Q}(\sqrt[p^n]{p})$、$h_n = 1$ となる。

Remark 1. $(*)_p$ をみたす拡大 K/k は、(α)〜(δ)をみたす。

Remark 2. 拡大 K/k が(α)〜(δ)をみたし、しかも、K の k 上の Galois closure M に対して $\mathrm{Gal}(M/k)$ が1次元 p-adic Lie group (i.e. $\mathbb{Z}_p$ と isomorphic な open subgroup をふくむ群) であれば、ある整数 $n_0 \geq 0$ が存在して、K/k_{n_0} は $(*)_p$ をみたす。

以後、(1)の Case のみを扱う。この Case では、岩沢の類数公式は次のように拡張される。

<u>定理1.</u>　p を奇素数とする。k を有限次代数体、K を $(*)_p$ をみたす k 上の無限次代数拡大とする。すると、非負整数 λ、μ と整数 ν が存在して

$$h_n = p^{e_n}, \quad e_n = \lambda n + \mu \frac{p^n - 1}{m} + \nu$$

が十分大きな n に対して成り立つ。ただし、m は K の k 上の Galois closure を M とすると、$[M:K]$ である。

Remark 1. m は、$p-1$ の約数である。

Remark 2. $m=1$ である必要十分条件は、K/k が $\mathbb{Z}_p$-拡大となることである。

$\mathbb{Z}_p$-拡大の理論については、Iwasawa[4], Lang[5] を参照。

§1. $(*)_p$ をみたす拡大の記述.

$(*)_p$ をみたす拡大 K/k に対して $(*)_p$ の (1)〜(3) をみたす k 上の有限次 Galois 拡大 L の中で次のような自然なものがとれる。

<u>命題1.</u> p を奇素数とする。K/k を $(*)_p$ をみたす拡大とする。すると、与えられた拡大 K/k に対して $(*)_p$ の (1)〜(3) をみたす k 上の有限次 Galois 拡大 L で最小のものが存在する。そのような L について、次の (1)〜(4) が言える。

(1) L は k の m 次 cyclic extension,

(2) KL は K の k 上の Galois closure,

(3) $\mathrm{Gal}(KL/k)$ は、$\mathrm{Gal}(KL/K)$ と normal subgroup $\mathrm{Gal}(KL/L)$ との semi-direct product である。

(4) homomorphism
$$\varphi : \begin{array}{ccc} \mathrm{Gal}(KL/K) & \longrightarrow & \mathrm{Aut}(\mathrm{Gal}(KL/L)) \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ \sigma & \longmapsto & (x \longmapsto \sigma^{-1} x \sigma) \end{array}$$

は injective である。

さて、$(*)_p$ をみたす拡大 K/k（特に、$m \neq 1$ であるもの）がどの程度存在するか考えてみよう。

<u>命題2.</u> p を奇素数とする。k を有限次代数体とする。

すると、次の集合間の bijective な対応が存在する。

$\{K : K/k \text{ は } (*)_p \text{ をみたす}\}/\sim \longleftrightarrow \{(L, M) \mid (**)\}$。

ここに、$(*)_p$ をみたす K に対応する (L, M) は、$L = (*)_p$ の (1)〜(3) をみたす k 上の最小の Galois 拡大、$M = K$ の k 上の Galois closure である。逆に、$(**)$ をみたす (L, M) に対しては、$K = M^H$ (H は $Gal(M/k) = H \ltimes Gal(M/L)$ となる $Gal(M/k)$ の部分群) を対応させる。

ただし、"$\sim$" は k 上の共役であるという relation をあらわす。$(**)$ は、(L, M) に関する次のような条件(1)〜(4)のことである。

(1) M は、k 上の Galois 拡大,

(2) L は、M/k の中間体で、M/L は $\mathbb{Z}_p$ − 拡大,

(3) L/k は、cyclic of degree dividing $p-1$,

(4) homomorphism

$$\begin{array}{ccc} Gal(L/k) & \longrightarrow & Aut(Gal(M/L)) \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ \sigma & \longmapsto & (x \longmapsto x^{\sigma}) \end{array}$$

は、injective である。ただし x^{σ} は $\tilde{\sigma}$ を σ の M の auto. への拡張とすれば、$\tilde{\sigma}^{-1} x \tilde{\sigma}$ である。

$k = \mathbb{Q}$ のときは、命題2の対応にあらわれる L は、次のようなものである。

命題3。 pを奇素数とする。$k=\mathbb{Q}$とする。有限次代数体Lに対して次は同値である。

(1) (L, M)が命題2の(**)をみたすようなMが存在する。

(2) $L=\mathbb{Q}$、あるいは、Lは$\mathbb{Q}$上の imaginary cyclic extension of degree dividing $p-1$.

Remark. (2)⇒(1)は類体論。(1)⇒(2)をいうには、絶対アーベル体では、Leopoldt conjecture が成立する (A. Brumer [2]) ことをつかう。

以後、pは奇素数であるとし、(*)pをみたす有限次代数体k、及びk上の無限次代数拡大Kを固定する。K/kに対応する(L, M)は unique に定まるから、L、Mはそのようなものをあらわすものとする。

$m=[M:K]=[L:k]$, $H=Gal(M/K)$, $\Gamma=Gal(M/L)$, $G=Gal(M/k)$とおく。すると命題1より

$$\begin{cases} H: m\text{次 cyclic}, \\ \Gamma \simeq \mathbb{Z}_p, \\ G=H\rtimes\Gamma \quad (H\text{と}\Gamma\text{の semi-direct product}). \end{cases}$$

$X(H)=\mathrm{Hom}(H, \mathbb{Z}_p^\times)$とおく。$\chi\in X(H)$に対応する idempotent を$e_\chi$とかく。すなわち、

$$e_\chi = \frac{1}{m}\sum_{\sigma\in H}\chi(\sigma^{-1})\sigma \quad \in \mathbb{Z}_p[H].$$

$\eta \in X(H)$を、$\tau^{-1} x \tau = x^{\eta(\tau)}$、$x \in \Gamma$、$\tau \in H$で定める。すると、命題1の(4)より、$X(H) = \langle \eta \rangle$である。

§2. K/kとKL/L。

定理1のλ, μは、K/kのみで定まるから、それぞれ、K/kのλ-invariant、μ-invariantと呼び、$\lambda(K/k)$、$\mu(K/k)$とかく。これはK/kが$\mathbb{Z}_p$-拡大のときは、通常の定義と一致する。K/kとKL/Lのλ-invariants及びμ-invariants間に次の関係がある。

<u>定理2.</u> (1) $\mu(KL/L) = \mu(K/k)$,

(2) $\lambda(KL/L) = m\,\lambda(K/k) - (m-1) + \sum_{\alpha=0}^{m-2}(m-1-\alpha)(d^{(3)}_{\eta^{\alpha}} - d^{(3)}_{\eta^{\alpha+1}})$.

ただし、$\chi \in X(H)$に対して、$d^{(2)}_{\chi}$、$d^{(3)}_{\chi}$は次のように定める。

$$d^{(2)}_{\chi} = \dim_{\mathbb{Q}_p} \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \varprojlim_n (E_L / N_{Lk_n/L}(E_{Lk_n}))^{e_\chi},$$

$$d^{(3)}_{\chi} = \dim_{\mathbb{Q}_p} \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathrm{Hom}_{\mathbb{Z}_p}(H^1(\Gamma, E_{KL})^{e_\chi}, \mathbb{Q}_p/\mathbb{Z}_p).$$

ここに、E_*は、$*$の単数群をあらわす。$H^1(\Gamma, E_{KL})$は、Galois cohomologyであって、自然に$\mathbb{Z}_p[H]$-moduleとみなせる。

Remark 1. 次のことに注意する。

$$H^1(\Gamma, E_{KL}) = \varinjlim_n H^1(\Gamma/\Gamma^{p^n}, E_{k_nL}),$$

$$H^1(\Gamma/\Gamma^{p^n}, E_{k_nL})^{e_\chi} \simeq (E_{k_nL/L} / E_{k_nL}^{1-\sigma})^{e_{\chi\eta}}, \quad n \geq 0,\ \chi \in X(H).$$

ただし、$\overline{\langle\sigma\rangle}=\Gamma$、$E_{k_nL/L}=\{x\in E_{k_nL}\mid N_{k_nL/L}(x)=1\}$である。
このことより、$d_\chi^{(3)}-d_{\chi\eta}^{(2)}$は、Herbrand quotientを$\mathbb{Z}_p[H]$の作用により細分したものと考えることができる。

Remark 2. $m=2$のときの$\lambda(KL/L)\pmod 2$についての議論が、Gillard [3]にある。

§3. Iwasawa algebra $\mathbb{Z}_p[[G]]$.

$\mathcal{O}$、Λを、それぞれ、G、Γの$\mathbb{Z}_p$上のIwasawa algebra $\mathbb{Z}_p[[G]]$、$\mathbb{Z}_p[[\Gamma]]$とする。Rを$\mathcal{O}$のcenterとする。ここに、profinite group Nに対して、$\mathbb{Z}_p$上のIwasawa algebra $\mathbb{Z}_p[[N]]$とは、$\varprojlim \mathbb{Z}_p[N/N']$のことである。ただし、$N'$は$N$のopen normal subgroupをわたる。$\mathcal{O}$の構造は、m, ηのみによって定まることに注意する。Λは$\mathcal{O}$のsubringとみなせる。Gの元は自然に$\mathcal{O}$の元と思える。$\mathcal{O}$, Λ, Rについて次のことが言える。

<u>命題4.</u> (1) $R=\Lambda^H=\{\lambda\in\Lambda\mid \tau^{-1}\lambda\tau=\lambda,\ \forall\tau\in H\}$。

(2) $Y=\frac{1}{m}\sum_{x\in H}\eta(x^{-1})(\sigma-1)^x$とおく。ただし、$\sigma$は$\Gamma$のtopological generator。すると、$\tau\in H$に対して、

$$Y^\tau(=\tau^{-1}Y\tau)=\eta(\tau)Y.$$

(3) $\Lambda=\mathbb{Z}_p[[Y]]$, $R=\mathbb{Z}_p[[Y^m]]$.

(4) $\mathcal{O}$ は twisted group ring $\Lambda \circ H$ とみなせる。

$\chi \in X(H)$ に対して、e_χ によって生成される $\mathcal{O}$ の right ideal を Λ_χ とかく。これは、projective $\mathcal{O}$-module である。H の単位指標 $(\in X(H))$ を 1_H とかく。有限生成 $\mathcal{O}$-module N_1、N_2 に対して、N_1 から N_2 への $\mathcal{O}$-homomorphism φ で Kernel も Cokernel も有限となるものが存在すれば、N_1 は N_2 と pseudo isomorphic といい、φ を pseudo-isomorphism と呼ぶ。有限生成 right $\mathcal{O}$-module は、modulo pseudo-iso. で次のように決定できる。

<u>定理 3.</u> 有限生成 right $\mathcal{O}$-module は、次の modules たちの直和と pseudo-isomorphic である。

(1) Λ_χ, $\chi \in X(H)$,

(2) $\Lambda_{1_H}/\Lambda_{1_H}\mathfrak{f}^n$, $\mathfrak{f}$ は (γ^m) とことなる R の height 1 の素イデアル、n は自然数,

(3) $\Lambda_\chi/\Lambda_\chi \gamma^n$, $\chi \in X(H)$, n は自然数。

このような分解は unique である。

Remark. $m=1$ のときは、すでに得られている。(c.f. Bourbaki [1], Iwasawa [4], Serre [7])。

この定理は、定理2の証明に必要である。とくに、定理2 (i) は、直ちにでる。Orders の一般論については、I. Reiner [6] を参照。

§4. 定理1の証明について。

有限次代数体Nに対して、C_N でその p-class group をあらわす。さらに一般の代数体Nに対しても $\varinjlim C_{N'}$ を C_N とかく。ただし、N'はNの有限次部分体をわたる。定理1は、次の順序で証明する。

i) C_K には、自然にR-module の structure がはいり、R-module として有限生成かつ torsion である。

ii) index 有限な R-submodule C と十分大きな整数 n に対して定められたRの元よりなる列 $\{l_n\}_{n\gg 0}$ が存在して

(***) $$C_{k_n} \simeq C_K/C^{l_n}$$

が、十分大きな整数nに対して成立する。

iii) $\# C/C^{l_n}$ の計算。

このことをもう少しくわしくみてみよう。

i) について： 自然な同型 $C_K \simeq C_{KL}^{e_{in}}$ より、C_K に R-module の構造がはいる。C_K が R-module として、有限生成

かつ torsion であるのは、C_{KL} が Λ-module としてそうだからである。

ii) について： n_0 を、すべての $k_{n_0}L$ の素イデアルについて、それが拡大 $KL/k_{n_0}L$ で分岐するならば完全分岐となるような非負整数とする。自然な surjective homomorphism $C_K \longrightarrow C_{k_{n_0}}$ の kernel を C とおく。次に l_n を整数 $n \geqslant n_0$ に対して定めよう。まず、$f \in \Lambda$ に対して、$\tilde{f} \in R$ を

$$\tilde{f} = \frac{1}{m} Tr_{\Lambda/R}(f) = \frac{1}{m} \sum_{x \in H} f^x$$

で定める。Iwasawa [4] にならって、整数 $0 \leqslant \alpha \leqslant \beta$ に対して、Λ の元 $\nu_{\alpha,\beta}$ を $\nu_{\alpha,\beta} = (\sigma^{p^\beta} - 1)/(\sigma^{p^\alpha} - 1)$ とおく。ただし、σ は Γ の topological generator である。整数 $n \geqslant n_0$ に対して、$l_n = \widetilde{\nu_{n_0,n}}$ とおく。すると、整数 $n \geqslant n_0$ に対して (＊＊＊) が成り立つ。このことを示すためには、次の命題が key になる。

<u>命題5.</u> 整数 $0 \leqslant \alpha \leqslant \beta$ に対して、$u \in \Lambda^\times$ が存在して、$\nu_{\alpha,\beta} = u\,\widetilde{\nu_{\alpha,\beta}}$ が成り立つ。

iii) について： 一般に有限生成 torsion R-module に対して次のことが言える。

<u>定理4.</u> V を有限生成 torsion R-module とする。非負整

数 n_0 に対して、すべての整数 $n \geqq n_0$ が $\# V/V\tilde{\omega}_{n_0,n} < +\infty$ をみたすならば、十分大きな整数 n に対して

$$\# V/V\tilde{\omega}_{n_0,n} = p^{e_n}, \quad e_n = \lambda n + \mu \cdot \frac{p^n - 1}{m} + \nu$$

が成り立つ。ただし、λ、μ、ν は n に依存しない整数で、λ, μ は非負である。

Remark 1. n_0 を十分大きくとれば $\# V/V\tilde{\omega}_{n_0,n} < +\infty$ はみたされる。

Remark 2. V が、R-module として

$$\sum_i \oplus R/Rp^{k_i} \oplus \sum_j \oplus R/Rf_j$$

と pseudo-isomorphic であるとする。ただし、k_i は自然数、f_j は Y^m に関する distinguished polynomial である。すると、定理の λ, μ は、それぞれ、$\sum_i k_i$、$\sum_j \deg_{Y^m} f_j$ である。

Remark 3. $m=1$ のときはすでに証明されている。(c.f. Iwasawa [4], Lang [5], Serre [7])。

$p=2$ のときについて簡単に述べる。このときも命題1へ3と同様のことが言える。ただし m は1又は2である。$m=1$ ならば、拡大 K/k は Z_2-拡大となるから、$m=2$ のときのみが問題である。C、Λ、R も同様に定義できる。このとき、上の i) は成立する。ii) の (***) のような記述を与えうるか否かは不明です。もし、(***) のような記述が与えられれば、

iii)はそれほど困難ではないように思われます。

Introduction で述べた(2)の型の拡大について、次のことを注意する。(2)の拡大で、p が irregular prime のときも、(***)型の記述を与えることができる。ただし作用している環は、$\mathbb{Z}_p$ 上の2次元の p-adic Lie group の Iwasawa algebra である。もしこのような algebra Σ の module について、適当な制限でのもとに、定理3のような modulo pseudo-isomorphism での分類ができれば、この Case にも拡張できるように思われる。

文献

[1] N. Bourbaki, Algèbre commutative Chapitre 7, Hermann, Paris, 1965.

[2] A. Brummer, On the units of algebraic number fields, Mathematika, 14, 1967, 121–124.

[3] R. Gillard, Remarques sur certaines extensions prodiédrales de corps de nombres, C. R. Acad. Sc. Paris, 282 (5 janvier 1976) Série A, 13–15.

[4] K. Iwasawa, On the $\mathbb{Z}_\ell$-extensions of algebraic number fields, Ann. of Math., 98 no 2, 1973, 246–326.

[5] S. Lang, Cyclotomic fields, Springer, New York, 1978.

[6] I. Reiner, Maximal orders, Academic press, London,

1975.

[7] J. P. Serre, Classes des corps cyclotomiques, Séminaire Bourbaki, Exposé 1974 (1958—1959).