数理解析研究所講究録
第 797 巻 1992 年 66-80

代数体の p 分岐最大 p 拡大のガロア群について

東大・理　山岸　正和(Masakazu YAMAGISHI)

いろいろな体の、分岐を制限した最大ガロア拡大 ― 特にそのガロア群の構造 ― は、数論の興味深い研究対象のひとつであろう。例えば Šafarevič [Š1] には、局所体、代数体、関数体の場合に、このようなガロア群の構造と関連する種々の数論的問題が挙げられている。また pro-p 群のほうが一般の pro-finite 群よりは扱い易いため、分岐を制限した最大 pro-p 拡大を考察することもあるが、多くの場合それでもじゅうぶん面白い。

ここでは、代数体の場合に、このタイプのガロア群について得られた結果を報告します。

記号：p を素数，k を体，S を k の素点からなるある集合としたとき、k 上 S の外で不分岐な最大 pro-p 拡大を k_S、その k 上のガロア群を G_S と書く。また k の最大 pro-p 拡大、すなわち S が全素点よりなるときの k_S を $k(p)$ と書く。

§1 Riemann面

代数体とRiemann面の理論の類似性はよく知られているが、これが以下の考察のひとつの動機でもあるので、まずRiemann面の場合に知られていることをいくつか述べる。

kを複素数体上の1変数代数関数体，gをその種数，Xを対応するRiemann面とし、素点の集合SをXの部分集合と見なす。$\#(S)<\infty$のとき、Riemannの存在定理によれば，G_Sは$X \setminus S$の位相的基本群のpro-p完備化と同型となる。このことから次がわかる。

(a) 生成元・関係式による表示、(pro-p群として)

$$G_S = \langle u_1, \cdots, u_m, s_1, t_1, \cdots, s_g, t_g \mid u_1 \cdots u_m \cdot [s_1, t_1] \cdots [s_g, t_g] = 1 \rangle$$

但し$m=\#(S)$，また$[\ ,\ ]$は交換子。特に$S \neq \phi$ならばG_Sは階数$2g+m-1$の自由pro-p群であり、また$S=\phi$ならばG_Sはいわゆる種数gの曲面群(のpro-p完備化)である。

(b) 自由積分解

$S=\{P_1, \cdots, P_m\}$とし，P_iの惰性群を$G_i\ (\subset G_S)$とする。$g=0$のとき，$G_S \cong G_1 * \cdots * G_{m-1}$となる。ここで$*$はpro-$p$群としての自由積を表わす。

(c)中心の自明性

G_Sが非アーベル群のとき、その中心は自明。これは(a)のG_Sの表示を抽象群として見れば組合わせ群論的にわかるが、pro-p完備化の場合それ以上の議論がいるようである。[Am]参照。

注：(a)〜(c)はpro-pのみならず、最大ガロア拡大，すなわちpro-finite完備化でも成立することが知られている。

以下の§2，§3では、局所体，代数体の場合にそれぞれ(a)〜(c)にあたることがどうなっているかを見る。

§2　局所体

kを$\mathbb{Q}_\ell$の有限次拡大とする。Sはkの唯一の素点からなるとする。すなわちこの場合$k_S = k(p)$。

(a)生成元・関係式による表示（[Ko]，§10参照）

$\ell \neq p$のとき、$k(p)/k$はtamely ramifiedな拡大で、G_Sの構造はよく知られている（岩澤）。

$\ell = p$のとき。μ_pを1のp乗根全体のなす群，$n=[k:\mathbb{Q}_p]$とおく。次の(1)はŠafarevič，(2)はDemuškin他による。

(1)　$k \not\ni \mu_p$　$\Rightarrow$　G_Sは階数$n+1$の自由pro-p群。

(2)　$k \supset \mu_p$　$\Rightarrow$　G_Sは階数$n+2$のDemuškin群で、生

成元・関係式による表示が知られている。例えば $p \geq 3$ ならば（このとき n は偶数）、

$$G_S = \langle x_1, \cdots, x_n \mid x_1^q [x_1, x_2][x_3, x_4] \cdots [x_{n-1}, x_n] = 1 \rangle$$

但し q は k に含まれる1の p 巾乗根のうちの最大位数。

注：局所体の絶対ガロア群の表示も得られている（Jannsen-Wingberg、1982）。

(b) 自由積分解は、素点が1個なのであまり意味がない。

(c) 中心の自明性

自由 pro-p 群については中心の自明性は既知であるが、Demuškin 群については次が成り立つ（既知かも知れません）。

定理1　G を (pro-p) Demuškin 群とするとき、次の3種の例外を除けば、G の中心は自明である。

$G = \mathbb{Z}/2\mathbb{Z}$,　$p = 2$

$G = \mathbb{Z}_p \times \mathbb{Z}_p$,　p は任意

$G = \langle a, b \mid ab^{-1}ab = 1 \rangle$, $p = 2$。

このうち最後の G の中心は b^2 で生成され、$\cong \mathbb{Z}_2$ である。

証明は省くが、§3の結果の証明と同じ方針である。

系　kが上の意味の局所体（すなわち$[k:\mathbb{Q}_\ell]<\infty$）とする。

(i)　$\ell \neq p$, $k \not\ni \mu_p$　$\Rightarrow$　$G_S \cong \mathbb{Z}_p$、

(ii)　それ以外のとき，G_Sの中心は自明。

§3　代数体

kを有限次代数体とし，$p=2$のときは総虚と仮定する。Sは，p上の全素点の集合S_pを含むkの素点の有限集合とする。この場合G_Sの構造に関してはまだわかっていないことも多く、また数論の未解決問題でG_Sの構造と関連するものも多い。例：kとpに関するLeopoldt予想は、$H^2(G_S, \mathbb{Q}_p/\mathbb{Z}_p)=0$と同値である。

以下，§1との類似性の観点から述べる。

(a)生成元・関係式による表示（[Ko]，§11参照）

Šafarevič [Š2]は一般のS（$S \supset S_p$とは仮定せず）に対し、G_Sの生成元の最少個数の計算および関係式の最少個数の上からの評価をした。特に$S=\phi$の場合は、その後の類体塔問題の解決にも応用された。また$S \supset S_p$の場合は，Šafarevičの結果とPoitou-Tateのglobal dualityより，関係式の最少個数がきちんと計算出来る。

例（[Š2]，§4）　$k=\mathbb{Q}(\mu_p)$，pが正則素数（すなわちkの

類数が p と素）のとき、$S=S_p$ に対し G_S は階数 $\frac{p+1}{2}$ の自由 pro-p 群。

しかし、適当な生成元を選んで関係式のかたちまで決定されているのは、特別な場合に限られている（Koch, Wingberg, Nguyen-Quang-Do 等の仕事がある）。

(b) 自由積分解

G_S が分解群の自由積に（大体）分解されるための，k, p, S に関する必要十分条件が，Wingberg [Wi] により求められている。簡単のため，$p \geqq 3$, $k \supset \mu_p$ とするとき、

定理 [Wi]　k_S/k で分解しない k の素点 v_0 が存在するとき（あれば $v_0|p$ がわかる）、そのときに限り、

$$G_S \simeq \mathop{*}_{v\in S\setminus\{v_0\}} \mathcal{G}_v * \mathcal{F},$$

ここで，$\mathcal{G}_v = \mathrm{Gal}(k_v(p)/k_v)$，また $\mathcal{F}$ は自由 pro-p 群で，$\mathrm{rk}\,\mathcal{F} = 1+[k_{v_0}:\mathbb{Q}_p]-\#S-(r_2-1)$　（r_2 は虚素点の個数）。

§5 でこの定理の応用を述べる。

(c) 中心の自明性

次の定理が主結果である。

定理2　$S \supset S_p$, $\# S < \infty$　とする。

（i）kが総実でなければ、G_Sの中心は自明。

（ii）kが総実とする。k_S/k のすべての有限次中間体に対するpでのLeopoldt予想を仮定すれば、G_S の中心は自明か、またはG_S がアーベル群となる。更に、

G_S がアーベル群 $\Longleftrightarrow$ $G_S \cong \mathbb{Z}_p$ $\Longleftrightarrow$ $k_S = k_\infty$

（k_∞はkの円分$\mathbb{Z}_p$-拡大）が成り立つ。

例：pが正則のとき、$k = \mathbb{Q}(\mu_p)^+$（p-分体の最大実部分体）、$S = S_p$　に対し，$G_S \cong \mathbb{Z}_p$　。

定理2の証明の概略。

（i）k_∞ をkの円分$\mathbb{Z}_p$-拡大，$H_S = Gal(k_S/k_\infty)$ とおく。まず群論的考察により，G_S の中心が H_S に入ることがわかる（kが総実だと、ここの議論がうまく行かないようだ）。一方 strict cohomological dimension $scd(H_S) = 2$ が知られている。これは岩澤理論における弱Leopoldt予想が，円分$\mathbb{Z}_p$-拡大に対しては正しいことから従う（§4参照）。そこで次の補題をH_S に適用すればよい。

補題3　Gはpro-p群で，$scd(G) = 2$，かつ，Gから$\mathbb{Z}_p$への

非同型な全射が存在するとする。このとき G の中心は自明。

(ii) 後半の主張は，G_S に関して知られている事実（Euler-Poincaré 標数の計算，Leopoldt 予想との関係，[Wi] の結果等）を組合わせて得られる。次に前半の Leopoldt 予想に関する仮定は，実は $scd(G_S)=2$ と同値であるので（これは k が一般で成り立つ），G_S に補題3を適用すればよい。 $\square$

注：最近，中村氏により次が証明された。"pro-p 群 G に対し，Euler-Poincaré 標数 $\chi(G)=\sum_{i=0}^{\infty}(-1)^i \mathrm{rk}\, H^i(G, \mathbb{Z}/p\mathbb{Z})$ が定義され，かつ，$\chi(G)\neq 0$ ならば，G の中心は自明である"（[Na] 参照）。今の場合 $\chi(G_S)=r_2$ が知られているので，定理2(i) は，これからも従う。

ちなみに，代数体の絶対ガロア群の中心の自明性は知られており（F. K. Schmidt, 1934），絶対ガロア群の自己同型群の研究（池田，岩澤，Neukirch，内田）にも応用された。また，最大 pro-p 拡大のガロア群についても，中心の自明性は証明されている（広中-小林 [Hi]，鳥羽 [To]）。

これらの証明はいずれも付値論的手法を用いているが，それが G_S にはうまく適用出来なかったので，上のようなアプローチを試みた。G_S から $\mathbb{Z}_p$ への全射を考えるというアイ

ディアは，Riemann面の場合のM. Anderson [An] の証明を見習ったものである。

尚，この方法で，広中-小林，鳥羽 の定理の別証明が得られたことも付け加えておく。

§4 弱Leopoldt予想

ここで，Leopoldt予想，弱Leopoldt予想 (weak Leopoldt conjecture) について記号の導入をし，知られていることをまとめておく。[Ng] 参照。

pを素数、kを代数体とする。k，pに対する "Leopoldt defect" $\delta = \delta_p(k)$ を [Wa], p. 265 の如く定義する。$\delta = 0$がLeopoldt予想である。この予想と同値な言い換えがいくつか知られているが，例えば先にも書いたように，
$H^2(G_S, \mathbb{Q}_p/\mathbb{Z}_p) = 0$ もそのひとつである。

次にk_∞/kを$\mathbb{Z}_p$-拡大 (必らずしも円分でなくてよい)、k_nをそのp^n次中間体とし、$\delta_n = \delta_p(k_n)$ とおく。

<u>弱Leopoldt予想</u>　$n \to \infty$ のとき，δ_nは有界であろう。

これについて知られていることをいくつか挙げておく。

(1) $H^2(k_S/k_\infty, \mathbb{Q}_p/\mathbb{Z}_p) = 0$ が，この予想と同値。

(2) k_∞/k が円分 $\mathbb{Z}_p$-拡大のとき，予想は正しい（例えば [Wa], Lemma 13.30 参照）。

(3) k に対する Leopoldt 予想が正しい $\Rightarrow$ k 上の任意の $\mathbb{Z}_p$-拡大に対する弱 Leopoldt 予想が正しい。

§5 自由 pro-p 拡大

Wingberg [Wi] の定理の応用を述べる。

自然数 d に対し，階数 d の自由 pro-p 群を F_d と書く。例えば $F_1 \cong \mathbb{Z}_p$ である。$\mathbb{Z}_p$-拡大の一般化として，代数体の F_d-拡大（ガロア群 $\cong F_d$ となるガロア拡大）を考察したい。その第一歩として，代数体 k を固定したとき，k 上に F_d-拡大が“どのように”存在するか調べるために，次の不変量を導入する。体 k，素数 p に対し，

$$\rho = \sup\{d \mid k \text{ が } F_d\text{-拡大を持つ}\}$$
$$= \sup\{d \mid \mathrm{Gal}(k(p)/k) \longrightarrow F_d \text{（全射）が存在}\}$$

と定義する。d は一般の濃度としてもよいが，以下では有限となる。

例：k が有限体のとき，すべての p に対し $\rho = 1$。

例：k が §2 の意味の局所体（$[k:\mathbb{Q}_\ell] < \infty$）のとき，

$$\rho = \begin{cases} 1 & \cdots\ l \neq p \quad \text{のとき} \\ n+1 & \cdots\ l = p,\ k \not\supset \mu_p \quad \text{のとき,} \\ [\frac{1}{2}n+1] & \cdots\ l = p,\ k \supset \mu_p \quad \text{のとき。} \end{cases}$$

但し，$l=p$ のとき，$n=[k:\mathbb{Q}_p]$ とおいた。また [ ] はガウス記号。これは，§2 で引用した局所体の最大 pro-p 拡大のガロア群の構造と，後で引用する J. Sonn の定理からわかる。

さて，以下 k は有限次代数体とする。この ρ が G_S と関連するのは次の理由による。

<u>補題4</u>　有限次代数体の F_d-拡大は p の外不分岐である。

（これは $d=1$ のときにはよく知られている。）

従って $S=S_p$ ととるとき，

$$\rho = \sup\{d \mid G_S \to F_d \text{（全射）が存在}\}$$

となる。

$G_S \to F_d$（全射）があれば，アーベル化することにより $G_S^{ab} \to \mathbb{Z}_p{}^d$（全射）が得られるが，$G_S^{ab}$ は有限生成 pro-p アーベル群でその $\mathbb{Z}_p$-階数は $r_2+1+\delta$ である（[Wa], Thm 13.4）から，次の ρ の評価が出来る：

（＊）　　$1 \leqq \rho \leqq r_2+1+\delta$。

例：§3 の Šafarevič の例（$k=\mathbb{Q}(\mu_p)$，p が正則）では

$\rho = r_2 + 1$ となっている。

ここで次のふたつの問題を考える。

問題A：出来るだけ条件を弱めて，$\rho \leqq r_2 + 1$ を示せ。

問題B：$\rho < r_2 + 1$ となる場合はあるか？

まず問題Aについては，次が成り立つ。

命題5　k 上のすべての $\mathbb{Z}_p$-拡大に対し弱Leopoldt予想が正しければ，$\rho \leq r_2 + 1$ が成り立つ。

これは §4 (3) により，上の不等式 (*) の精密化となっていることがわかる。出来れば無条件に $\rho \leq r_2 + 1$ を示したいところである。

次に問題Bについては，Wingberg の定理の応用として次が得られた。ここでも簡単のため $p \geqq 3$，$k \supset \mu_p$ とする。

定理6　k_{S_p}/k で分解しないような k の素点 v_0 が存在するとき，

$$\rho = r_2 + 1 - \frac{1}{2} \sum_{\substack{v|p \\ v \neq v_0}} [k_v : \mathbb{Q}_p]$$

が成り立つ。特に $\# S_p > 1$ ならば，$\rho < r_2 + 1$ となる。

例：$p=3$，$k=\mathbb{Q}(\sqrt{-3},\sqrt{15})$ のとき，$\rho=2$，$r_2+1=3$ である。

上の定理は $p=2$ でも適当な修正項を加えれば成り立つのだが，それを用いると次の面白い例が得られる。

例：$p=2$，$k=\mathbb{Q}(\sqrt{-l})$（l は素数で，$l\equiv 7 \bmod 8$）のとき，$\rho=1$，$r_2+1=2$。すなわち k 上には $\mathbb{Z}_2$-拡大以外の自由 pro-2 拡大は存在しないことがわかる。

このふたつの例においては，v_0 として p の素因子（ふたつあるがいずれでもよい）をとったとき，k_{S_p}/k で分解しないことがそれぞれ Kuz'min，Tsvetkov によって（こことは別の問題意識から）確かめられている。

定理6の証明の概略

まず，$S=S_p$ に対し

$$\rho=\sup\{d \mid G_S \longrightarrow F_d\ (\text{全射})\ \text{が存在}\}$$

であったが，仮定（v_0 の存在）から，G_{S_p} は自由積分解を持つ（Wingberg の定理）ので，この自由積を構成する各因子から自由 pro-p 群への全射について調べればよい。今の場合，各 $\mathcal{G}_v$ は Demuškin 群となるので，次の補題を用いることにより，ρ が計算される。 ▨

補題（J. Sonn [So]）　Demuškin群 G から $\mathbb{F}_d$ への全射が存在するための必要十分条件は、$d \leqq \frac{1}{2} rk(G)$ である。

一般の k, p に対する ρ の決定は難しそうである。

References

[An] M. Anderson, Exactness properties of profinite completion functors, Topology 13 (1974), 229-239.

[Hi] Y. Hironaka-Kobayashi, On the Galois groups of the maximal p-extensions of algebraic number fields, Natur. Sci. Rep. Ochanomizu Univ. 27 (1976), 99-105.

[ko] H. Koch, Galoissche Theorie der p-Erweiterungen, Springer-Verlag, 1970.

[Na] H. Nakamura, On the pro-p Gottlieb theorem, to appear.

[Ng] T. Nguyen-Quang-Do, Formations de classes et modules d'Iwasawa, in: Number Theory Noordwijkerhout 1983, Springer LNM 1068, 167-185.

[Š1] I. R. Šafarevič, Algebraic number fields (Russian), Proc. Int. Congr. Math. Stockholm 1962, 163-176, = AMS Transl. (2) 31 (1963), 25-39.

[Š2] I. R. Šafarevič, Extensions with given points of ramification (Russian), Publ. IHES 18 (1964), 295-319. = AMS Transl. (2) 59 (1966), 128-149.

[So] J. Sonn, Epimorphisms of Demushkin groups, Israel J. Math. 17 (1974), 176-190.

[To] G. Toba, On the center of the Galois group of the maximal p-extension (Japanese), manuscript, 1979.

[Wa] L. C. Washington, Introduction to cyclotomic fields, GTM 83, Springer-Verlag, 1982.

[Wi] K. Wingberg, On Galois groups of p-closed algebraic number fields with restricted ramification II, J. reine. Angew. Math. 416 (1991), 187-194.