数理解析研究所講究録 1200 巻 2001 年 195-209

On pro-p extensions of algebraic number fields
(Recent topics related to Greenberg's generalized conjecture)

Yasutaka Ihara, RIMS, Kyoto University
(京都大学数理解析研究所 伊原康隆)

この講演の内容は，岩澤理論に於る "一般 Greenberg 予想" ("Greenberg's generalized conjecture"，以下 GGC と略記)，及びそれをめぐる極く最近の話題の紹介です．R. Greenberg 氏の 1971 年の学位論文 [G_1] に端を発する "従来の Greenberg 予想" に関しては，日本人による寄与も多く，又それについては約 3 年前，尾崎学氏がここでの同様の研究集会で優れた解説をして下さった ([O] 参照) ので，多くの方々になじみ深い事と思います．ところで最近, Greenberg 氏は，より一般化した予想を提出されました．([G_2] Conjecture 3.5)．この予想 (GGC) をめぐって， Lannuzel-Nguyen Quang Do [LN]， McCallum [Mc] 等，興味深い成果が相次いで得られ，更に 2000 年秋， Sharifi [Sh] は [Mc] の結果を用いて，私が $\mathbb{P}^1 - \{0, 1, \infty\}$ の pro-p 基本群の数論的性質に関して提出した問題 [Ih] の一部の条件つき解決 ((GGC) 等を仮定) も得ました．これらについて最近学び得たことを簡単に紹介させていただきます．尚、岩澤理論や従来の Greenberg 予想についても、予備知識としては仮定せず、必要な部分は (簡単にですが) 復習します。

岩澤理論では，一つ素数 p を固定して数体の pro-p アーベル拡大の (そのまた) pro-p アーベル拡大を考えるのですが，前者としては "$\mathbb{Z}_p$ 拡大" よりも最大 ($\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$) 拡大を考え，後者も不分岐なものだけでなく， p の外で不分岐なものも考えます ($\mathbb{Z}_p$ は p 進整数環の加法群)．しかし，より広く，与えられた代数体の p の外で不分岐な pro-p 拡大全体の中で考えるのが自然なので，その枠組の定式化の復習から始めます．これは無論， Safarevic, Koch, ... 等による独立した出発点も持つ古典的枠組

1 $k(p)/k$ とそのガロア群

1.1

代数体 k と素数 p の対 (k,p) を一組取って固定します．問題にするのは (k,p) で定まる，ある種の "大局的対象" の性質です．p の上の k の素点全体の集合を S_p と書きます．又，簡単の為，以下 $p>2$ とします.(従って，k の任意の pro-p 拡大に於て k の無限素点は自動的に不分岐です.)

まず，$k(p)/k$ を S_pの外で 不分岐な k の最大 pro-p 拡大とします．そのガロア群 $G_k(p) = Gal(k(p)/k)$ は無限 pro-p 群ですが，その位相群としての生成元の最小個数 $h^1 = h^1(G_k(p))$ $(= \dim H^1(G_k(p),\mathbb{Z}/p))$ と関係式の最小個数 $h^2 = h^2(G_k(p))$ $(= \dim H^2(G_k(p),\mathbb{Z}/p))$ は共に有限であり，それらの間に簡単な関係

$$h^1 - h^2 = r_2 + 1 \quad (r_2 = r_2(k) \text{ は } k \text{ の虚素点の個数})$$

が成立ちます．h^2 を与える公式も知られていて（例えば [NSW] Th 8.7.3 参照），特に，$h^2 = 0$ 即ち $G_k(p)$ が自由 pro-p 群（この場合，階数は r_2+1）となる為の必要十分条件も知られています（§5-1 で復習します）．

1.2

ガロア拡大 $k(p)/k$ の最大アーベル部分体を $k(p)^{ab}$ で表わし，ガロア群 $G_k(p)$ のアーベル化を $G_k(p)^{ab}$ で表わします．即ち $G_k(p)^{ab} = Gal(k(p)^{ab}/k)$．このとき，$G_k(p)^{ab}$ の生成元の最小個数は $G_k(p)$ のそれと同じ h^1 であり（Burnside の原理），一方，$G_k(p)^{ab}$ は pro-p アーベル群ゆえ $\mathbb{Z}_p$ 加群と見なせるので，$\mathbb{Z}_p^{h^1}$ の商です．この $G_k(p)^{ab}$ を $\mathbb{Z}_p^{h^1}$ の商として表わすとき必要な基本関係式は，元の $G_k(p)$ に関する h^2 個のそれのうち "アーベル化しても無駄にならないもの" で，従ってその個数は h^2 以下です．従って，上ツキ tor で torsion 部分群を表すとき，単因子論により，

$$G_k(p)^{ab} \cong \mathbb{Z}_p^r \times (G_k(p)^{ab})^{tor}, \tag{1.2.1}$$

$$r \geq h^1 - h^2 = r_2 + 1, \tag{1.2.2}$$

と分解します．(1.2.2)に於て等式が成立つだろう，というのが Leopoldt 予想です．より正確には，k の単数群（の non-torsion 部分）の p 進独立性に関する有名な Leopoldt 予想と（類体論によって）同値です．この予想は k が $\mathbb{Q}$ 上

アーベル，又は虚2次体上アーベルのときには成立することが知られています（A. Brumer 等）．

1.3

$\mathbb{Z}_p$ を p 進整数環の加法群，$F_d^{(p)}$ $(d=1,2,\dots)$ を階数 d の自由 pro-p 群とします．従って $F_1^{(p)} \cong \mathbb{Z}_p, (F_d^{(p)})^{ab} \cong \mathbb{Z}_p^d$ （上ツキ ab はここでもアーベル化を表わす）．次の命題は，$\mathbb{Z}_p$ の場合（岩澤），$F_d^{(p)}$ の場合（山岸 - 朝田）等，順次示されましたが，証明は非常に簡単です．

命題. k 上のガロア拡大でガロア群が $\cong \mathbb{Z}_p^d$，又は $\cong F_d^{(p)}$ なるものはすべて $k(p)$ に含まれる．

証明．ガロア群の pro-p 性は明らか．一方，これが S_p の外で不分岐なることは，$\mathbb{Z}_p^d$ や $F_d^{(p)}$ が（∞ や $v \nmid p$ の上の惰性群（この場合 cyclic）の生成元やフロベニウス置換から生ずるところの）

$$\tau^2 = 1, \quad \tau \neq 1,$$

なる元も，

$$\sigma\tau\sigma^{-1} = \tau^{l^f},\ \tau \neq 1,\ l: \text{素数} \neq p,\ f \geq 1,$$

なる元 σ, τ の組も含み得ないことより明らか．（$\mathbb{Z}_p^d$ は torsion をもたず，$F_d^{(p)}$ の閉部分群はすべて自由 pro-p 群！）． □

注意. 上の証明より，この命題は，$p=2$ でも成立ちます．

1.4

$k(p)^{ab}/k$ のガロア群 $G_k(p)^{ab}$ の torsion 部分群と対応する中間体を K とおくと，(1.2.1)により，$Gal(K/k) \cong \mathbb{Z}_p^r$．一方 §1.3 の命題によって k 上の $\mathbb{Z}_p^d$ 型拡大はすべて $k(p)$ に含まれ，この場合アーベル拡大なので $k(p)^{ab}$ にも含まれます．一方 $\mathbb{Z}_p^d$ 拡大と $\mathbb{Z}_p^{d'}$ 拡大の合成も $\mathbb{Z}_p^{d''}$ 型拡大となるので，結局，K は k 上のすべての $\mathbb{Z}_p$ 拡大の合成に等しく，又 k の最大 $\mathbb{Z}_p^d$ 型拡大でもあるわけです．この体 K を後に“基礎体”として使います．

尚 $k(p)^{ab}$ と K の差，$(G_k(p)^{ab})^{tor} = Gal(k(p)^{ab}/K)$ が何であるかは，かなり微妙な問題のようです．

一方，k 上の $F_d^{(p)}$ 拡大も §1.3 によって $k(p)$ に含まれるので，k 上の $F_d^{(p)}$ 拡大の研究は $G_k(p)$ の pro-p 自由商の研究と同じです．これについて知られていることも少ないですが，§5 で触れるつもりです．

2 拡大体 L/K と $\mathbb{Z}_p[[t_1,\dots,t_r]]$-加群 $X = Gal(L/K)$

2.1

まず，一般に $k \subset K \subset L \subset k(p)$ なる中間体 K, L であって，K/k 及び L/K はアーベル拡大，L/k はガロア拡大となるものを考え，$X = Gal(L/K)$ を（pro-p アーベル群ゆえ）$\mathbb{Z}_p$ 加群と考えます．このとき $\Gamma = Gal(K/k)$ は X に共役によって

$$X \ni x \to \gamma(x) = \tilde{\gamma} x \tilde{\gamma}^{-1} \in X$$

($\gamma \in \Gamma$) と作用します．ここで $\tilde{\gamma} \in Gal(L/k)$ は γ の延長（$\gamma(x)$ は $\tilde{\gamma}$ のとり方によらない）．これら $\mathbb{Z}_p$ と Γ の作用を，$\mathbb{Z}_p$ 線形性と連続性を用いて，完備群環 $\Lambda = \mathbb{Z}_p[[\Gamma]]$ の X への作用に延ばすことが出来，これによって X を Λ-加群と見なします．

2.2

歴史的には，K として k の一つの $\mathbb{Z}_p$ 拡大（例えば円分 $\mathbb{Z}_p$ 拡大），L としては K の最大不分岐 pro-p アーベル拡大をとり，$X = Gal(L/K)$ の $\Lambda = \mathbb{Z}_p[[\mathbb{Z}_p]]$-加群としての性質を研究したのが岩澤理論の発端でした．より正確には，Serre によってこの形で見通しよく捉え直され，その上に発展しました．1970 年頃，Greenberg は k 上の $\mathbb{Z}_p$ 拡大 K を動かしたときの Λ 加群 X の変化を調べる為，K が k 上の $\mathbb{Z}_p^d$ 拡大 ($d \geq 1$) の場合も考えました．このとき Λ は $\mathbb{Z}_p$ 上の d 変数形式的巾級数環と同型になります．より正確には，$\mathbb{Z}_p^d$ の生成元 $\gamma_1,\dots,\gamma_d$ をとり，$t_i = \gamma_i - 1$ $(1 \leq i \leq d)$ とおくとき，$\mathbb{Z}_p[[\mathbb{Z}_p^d]] = \mathbb{Z}_p[[t_1,\dots,t_d]]$．これは UFD（一意分解環）でネーター環です．次の定理は $d = 1$ のときの岩澤の定理の（その方法を用いての）Greenberg による拡張です．

定理 (Iwasawa, Greenberg). *K を k の $\mathbb{Z}_p^d$ 拡大 $(1 \leq d \leq r)$，L/K を最大不分岐アーベル pro-p 拡大とする．（従って $L \subset k(p)$.）このとき，$X = Gal(L/K)$ は $\Lambda = \mathbb{Z}_p[[Gal(K/k)]] \cong \mathbb{Z}_p[[t_1,\dots,t_r]]$ 上の加群として有限生成で，しかも torsion*

加群である．即ち

$$X = \Lambda\xi_1 + \cdots + \Lambda\xi_s,$$
$$fX = 0,$$

なる $\xi_1, \ldots, \xi_s \in X$, $f \in \Lambda$, $f \neq 0$ が存在する．

この証明の数論的なポイントは代数体の類数の有限性（K/k の部分拡大に適用）であり，代数的ポイントは Λ- 加群についての中山のレンマですが，結果として示されたこと —— すべての X を消す Λ の元 $f \neq 0$ が存在する —— は，驚くべきことの一つだと思います．簡単の為，K/k は不分岐な中間体の拡大を含まないと仮定して，類体論によって K/k の有限次部分ガロア拡大 k'/k のイデアル類群の p-Sylow 群 $Cl(\mathcal{O}_{k'})^{(p)}$ への群環 $\mathbb{Z}_p[Gal(k'/k)]$ の作用の言葉に翻訳すると，これは $Cl(\mathcal{O}_{k'})^{(p)}$ 全体を消す元 $f_{k'} \in \mathbb{Z}_p[Gal(k'/k)]$ であって，k' に関して compatible でしかも k' が十分大きければ $f_{k'} \neq 0$ なるもの，の存在を意味しています．（ノルム $\sum_\sigma \sigma$ は compatible にならない．倍数がどんどんかかる．）円分体での Stickelberger 作用素のようなものが，一般的にも存在することを示しています．

さて，ではこういう f はどの位沢山あるのでしょうか？それに関する基本的予想が (GGC) です．その記述の前に，体 K, L を次にように特定します．

2.3

以下 K としては 1.4 で定めた体，従って

$$k \subset K \subset k(p)^{ab}, \quad \begin{matrix}[k(p)^{ab} : K] < \infty, \\ Gal(K/k) \cong \mathbb{Z}_p^r,\end{matrix}$$

L としては，K の最大不分岐アーベル pro-p 拡大（従って $L \subset k(p)$）更に “もう一つの L” として

$$M: \quad K\text{の } k(p) \text{ 内での最大アーベル拡大}$$
$$= S_p\text{の外で不分岐な } K \text{ の最大アーベル pro-}p \text{ 拡大},$$

を考え，

$$X = Gal(L/K),\ Y = Gal(M/K)$$

を共に $\Lambda = Gal(K/k) \cong \mathbb{Z}_p[[t_1, \ldots, t_r]]$ 上の加群と見なします．§2.2 の定理により X は有限生成 torsion Λ- 加群です．(Y については §4.2 参照.)

3 一般 Greenberg 予想 (GGC)

3.1

K, L を §2.3 の体とし，$\Lambda = \mathbb{Z}_p[[Gal(K/k)]] \simeq \mathbb{Z}_p[[t_1, \ldots, t_r]]$, $X = Gal(L/K)$ とおき，X を Λ- 加群と見ます．X の annihilator

$$Ann_\Lambda(X) = \{\lambda \in \Lambda; \lambda x = 0 \ \forall x \in X\}$$

は Λ のイデアルで，§2.2 の定理により $Ann_\Lambda(X) \neq (0)$ ですが，これはどの位大きいのでしょうか？ (GGC) は次の予想です (cf. [G_2] Conj. 3.5).

予想 (GGC). Λ のイデアル $Ann_\Lambda(X)$ は高さ *2* 以上であろう，即ち Λ の高さ 1 の素イデアルにはふくまれないであろう．

注意. Λ は *UFD* なので，その素イデアル $\neq (0)$ が高さ $1 \leftrightarrow$ 単項．よって，上の予想は次のように云いかえられます．

(*) $Ann_\Lambda(X)$のすべての元を割る Λ の元は可逆元以外にないであろう．

これは又，次のようにも云いかえられます．

(**) $Ann_\Lambda(X)$は互いに素な 2 つの元 f, g を含む．

ここで $f, g \in \Lambda$ が互いに素とは，f, g 双方を割る Λ の元は可逆元に限ること．

尚，$|S_p| = 1$ で k の類数が p で割れないときは $X = 0$ となり，従ってこの場合 (GGC) は自明に成立しています．（その証明は，やはり有限 p 群 G に関する Burnside の原理 $\cdots G$ の部分群 I の G^{ab} での像が G^{ab} 全体なら $I = G \cdots$ これを $k(p)/k$ の部分有限次拡大 k' の p-Hilbert 類体 k'^H のガロア群 $G = Gal(k'^H/k)$ と p 上の惰性群 I に適用.）

3.2

k が総実のとき，Leopoldt 予想のもとで $r = r_2 + 1 = 1, \Lambda \simeq \mathbb{Z}_p[[t]]$．このとき，

$$\text{上の予想} \longleftrightarrow \Lambda/Ann_\Lambda(X) : \text{有限} \longleftrightarrow X : \text{有限}$$

これが元来のGreeberg予想であり，これについては日本人の寄与も大きい（[O]参照）．ただ，(k,p)についてのGreenberg予想がすべての素数pに対して示されている総実代数体kは，未だに$k=\mathbb{Q}$だけのようです．$k=\mathbb{Q}$のときは，Kは円分$\mathbb{Z}_p$拡大で$L=K$, $X=0$．一方，$k\supsetneq\mathbb{Q}$のときは，Greenberg予想が非自明であるpは有限個ではありません．類数を割るpだけでなく，$|S_p|\geq 2$，つまり$k/\mathbb{Q}$で分解するpすべてに対して検証を要しますから，数値計算だけですべてのpに対して証明することは出来ません．

$k=\mathbb{Q}(\mu_p)^+=\mathbb{Q}(\cos\frac{2\pi}{p})$に対する$(k,p)$のとき（Leopoldt予想は正しいので$r=1$）は，有名なVandiver予想が$X=0$を予想しており，それは$p<12,000,000$なるすべての$p$について確かめられています．従って，この場合（$(k,p)$に関する）Greenberg予想は，単にVandiver予想を弱めたものになっています．

3.3

予想(GGC)の「哲学的根拠」は[G_2]でも少し触れられていますが，私には十分理解できていません．私としては，特にp進Artin L関数（$\neq 0$の存在）との関連に興味があります．Greenberg氏にメールで問合わせ，彼の考えていた二，三の根拠を教わりましたが，それについては，私の理解も不十分だし，ここで書く事はさし控えます．ここでは，次の“次元論的説明”にとどめたいと思います．

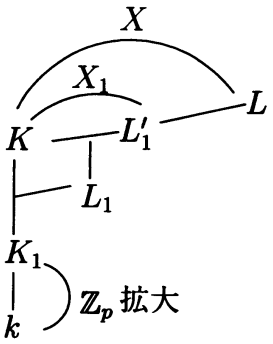
$Ann_\Lambda(X)$が高さ≥ 2という事は，$\psi:\Lambda\twoheadrightarrow\mathbb{Z}_p[[t]]$なる全射準同型（勿論沢山ある）の核$\mathrm{Ker}\psi$（高さ$(r+1)-2=r-1$）と合わせると$\Lambda$のイデアル$(Ann_\Lambda(X)+\mathrm{Ker}\psi)$は“大抵は”（つまり“一般の$\psi$”に対しては）高さ$2+(r-1)=r+1$，即ち

$$\Lambda/(Ann_\Lambda(X)+\mathrm{Ker}\psi)$$

が有限になる，ということです．そこでK/k内の$\mathbb{Z}_p$拡大K_1/kを一つとり，γを$Gal(K_1/k)\simeq\mathbb{Z}_p$の生成元，$t=\gamma-1$とおき，一方$Gal(K/k)\simeq\mathbb{Z}_p^r$の生成元$\gamma_1,\dots,\gamma_r$をとり，$\gamma_i|_{K_1}=\gamma^{a_i}$ $(a_1,\dots,a_r\in\mathbb{Z}_p$，少くも一つは$\not\equiv 0 \pmod p)$, $t_i=\gamma_i-1$ $(1\leq i\leq r)$とおくと，制限射$Gal(K/k)\to Gal(K_1/k)$は

$$\psi:\Lambda=\mathbb{Z}_p[[t_1,\dots,t_r]]\to\mathbb{Z}_p[[t]];\ t_i\to(1+t)^{a_i}-1$$

$(1\leq i\leq r)$なる全射準同型を導く．さて$X_1=X/(\mathrm{Ker}\psi)X$は，$Gal(K/K_1)$が自明に作用する$X$の最大の商に等しく，従って$X_1=Gal(L/L_1')$となります．ここで$L_1'$は$L/K_1$内の$K/K_1$の最大中心拡大体（それは勿論$K$を含む）．



L_1 は K_1 の最大不分岐 pro-p アーベル拡大

さて制限射 $X_1 \to Gal(L_1/K_1)$ は一般には全射とも単射とも限らないので，どちらが他よりも大きくなる理由もありますが，仮りに (GGC) が成立つとすると，“一般の K_1” に対しては X_1 は有限 $\Lambda/(Ann_\Lambda(X) + \mathrm{Ker}\psi)$- 加群ゆえ，$|X_1| < \infty$，従って問題の $Gal(L_1/K_1)$ のうち k 上のアーベル拡大から来ない難しい部分 $Gal(L_1/K \cap L_1)$ が有限，ということを意味します．逆方向はよくわかりませんが，例えば K の p 上の素点が唯一つ（特に $|S_p| = 1$）で $X = (\Lambda/Ann_\Lambda(X))^s$ のような場合を想定すると，一つでも $Gal(L_1/K_1)$ が有限なる $\mathbb{Z}_p$ 拡大 K_1/k があると（このときは $L_1K = L'_1$ となるので），$\Lambda/(Ann_\Lambda(X) + \mathrm{Ker}\psi)$ の有限性が（その ψ に対して）成立ち，これより $Ann_\Lambda(X)$ の高さ ≥ 2 でなくてはならないことがわかります．

従って乱暴にまとめれば，(GGC) は，k 上の “一般の $\mathbb{Z}_p$ 拡大” K_1 に対して $Gal(L_1/K_1)$ の “実質部分” が有限になりやすいという予想だ，と云えると思います．

4 (GGC) の別の見方，帰結，等 [LN][Mc]

4.1

従来の Greenberg 予想と同様，(GGC) も K/k 内でのイデアルの “capitulation” と密接に関係しています．

定理 ([LN]Th4.4). $k \supset \mu_p$ 且つ K/k のすべての有限次部分拡大体 F で p に対する Leopoldt 予想が成立つと仮定する．このとき

$$(\mathrm{GGC}) \longleftrightarrow \varinjlim_F Cl\left(\mathcal{O}_F\left[\frac{1}{p}\right]\right)^{(p)} = 0.$$

ここで $\mathcal{O}_F$ は F の整数環，$Cl\left(\mathcal{O}_F\left[\frac{1}{p}\right]\right)$ は $\mathcal{O}_F\left[\frac{1}{p}\right]$ のイデアル類群（即ち $\mathcal{O}_F$ のイデアル類群を p の素因子で代表される類で生成される部分群で割った群），上つき (p) はその p 成分を表わす．

4.2

一方，(GGC) を $Y = Gal(M/K)$ (§2.3) の言葉に移すと：

定理 ([Mc]Cor14). $k \supset \mu_p$，且つ各 $\mathfrak{p} \in S_p$ に対して K/k での $\mathfrak{p}$ の分解群の $\mathbb{Z}_p$ 階数 ≥ 3 とする（$p > 3$ なら満される）．このとき

$$(\mathrm{GGC}) \longleftrightarrow Y \text{ が } \Lambda\text{-torsion free.}$$

この証明には，Y と $X' = Gal(L'/K)$ の間の Jannsen の双対性などが使われています．ここで L'/K は S_p の上の K のすべての素点が完全分解する L/K の最大部分体です．定理の仮定から X と X' は “近いもの” になります．

注意. Y は Λ-加群として一般に（上の定理の仮定と無関係に）有限生成です．その証明は，$G_k(p)$ が有限生成 pro-p 群であることと Y の群論的定義だけからでも容易に得られます．

【4.1 と 4.2 の関係】 $|S_p| = 1$ のときの一方向の説明．

$$N = K\left(\varepsilon^{1/p^n}; n \geq 1, \quad \varepsilon \in \mathcal{O}_K\left[\frac{1}{p}\right]^{\times}\right)$$

とおくと，$K \subset N \subset M$ だが，$k \supset \mu_p$，（このとき $K \supset \mu_{p^\infty}$ に注意）$|S_p| = 1$ のとき，$Gal(N/K)$ は Λ-torsion free ([Mc]Th3)．もし $\varinjlim_F Cl\left(\mathcal{O}_F\left[\frac{1}{p}\right]\right)^{(p)} = 0$ なら M/K の Kummer 拡大としての構成を考えばわかるように，$M = N$．よって Y も Λ-torsion free となる．

4.3 $(\mathbb{Q}(\mu_p), p)$ に対する (GGC) ([Mc]).

p が $\mathbb{Q}(\mu_p)$ の類数を割るとき p は regular prime，割らないとき irregular prime といいます．

p: regular のときは $X = 0$ ゆえ (GGC) は自明．

p: irregular のとき：

定理 ([Mc]Th1). p ： irregular prime で更に次の (1)(2) を満たすとする.

(1) $\mathbb{Q}(\mu_p)$ の類数の p 成分は丁度 p に等しい.

(2) $\mathbb{Q}(\mu_p)$ の単数群を E, $\mathbb{Q}_p(\mu_p)$ のそれを U, また E の U 内での p 進閉包を $\bar{E}$ とかくとき, $U/\bar{E}$ の p 巾 torsion 部分群 $(U/\bar{E})[p^\infty]$ は $\mathbb{Z}/p$ と同型.

このとき $(\mathbb{Q}(\mu_p), p)$ に対して (GGC) が成り立つ.

McCallum の数値実験によると, $p < 400$ と $3600 < p \leq 4001$ の範囲の irregular primes のうち約 3/4 が条件 (1) と (2) を共に満すそうである.

(満たす例) $p = 37, 59, 67, 101, 103, 131, 149, \ldots$

(満たさない例) $p = 157, 353, \ldots, 691, \ldots$

注意. $k(p)^{ab}/k$ の最大不分岐部分拡大, 即ち k の Hilbert p- 類体を k^H/k とするとき, (1)(2) はそれぞれ

(1)′ $Gal(k^H/k) \cong \mathbb{Z}/p$,

(2)′ $Gal(k(p)^{ab}/k^H)^{\mathrm{tor}} \cong \mathbb{Z}/p$

と同値. (1)′ より $h^1\big(G_k(p)\big) = \frac{p+1}{2}+1$, $h^2\big(G_k(p)\big) = 1$, 従って $G_k(p) = Gal\big(k(p)/k\big)$ は階数 $\frac{p+1}{2}+1$ の自由 pro-p 群を 1 つの関係式で割った群になっています. 尚この場合, $Gal(k^H/k)$, $Gal(k(p)^{ab}/k^H)$ それぞれが p-torsion をもつが, $Gal(k(p)^{ab}/k)$ は $\frac{p+1}{2}+1$ 個の生成元と 1 つの関係式をもち, 従って (1)′(2)′ と合わせると $Gal(k(p)^{ab}/k) \cong \mathbb{Z}_p^{\frac{p+1}{2}} \times \mathbb{Z}/p^e$ ($e = 1$ または 2).

5 k 上の自由 pro-p 拡大の階数との関係について

5.1

一般に階数 $d \geq 1$ の自由 pro-p 群 $F_d^{(p)}$ をガロア群とする k のガロア拡大があると, それは $k(p)$ に含まれる (§1.3) ので, そういう拡大がある事と $G_k(p)$ が $F_d^{(p)}$ を商群に持つことは同値です. ではこういう d の最大値 $\rho_k(p)$ は何でしょうか? $F_d^{(p)}$ のアーベル化が $\mathbb{Z}_p^d$ ですから, 当然 $\rho_k(p) \leq r$ です. 山岸氏は [Y]§4 で K. Wingberg の結果を用いて, $\rho_k(p) < r = r_2 + 1$ なる実例を与えています.

まず $G_k(p)$ 自身が自由 pro-p 群，即ち §1.1 の記号で $h^2(G_k(p)) = 0$ となる為の条件は（例えば [NSW]Th8.7.3 参照；我々は $p > 2$ としていることに注意）：

$h^2(G_k(p)) = 0 \leftrightarrow$ 次の (i)(ii) が成り立つ．

$$\begin{cases} \text{(i)} & \mu_p \not\subset k \text{ なら } \mu_p \not\subset k_{\mathfrak{p}} \quad (\forall \mathfrak{p} \in S_p), \\ & \mu_p \subset k \text{ なら } |S_p| = 1. \\ \text{(ii)} & \alpha \in k^\times \text{ が，} k \text{ のすべての有限素点 } v \text{ に対して } \mathrm{ord}_v(\alpha) \equiv 0 \pmod{p} \text{ を満し，} \\ & \text{更に } v \in S_p \text{ に対して } \alpha \in (k_v^\times)^p \text{ も満すなら } \alpha \in (k^\times)^p. \end{cases}$$

特に $\mu_p \subset k$ のとき (ii) は

(ii)′ $Cl(\mathcal{O}_F[\frac{1}{p}])^{(p)} = 0$

と同値です．

例えば $k = \mathbb{Q}$ のとき $h^1 - h^2 = 1$, $h^2 = 0$ で $G_{\mathbb{Q}}(p) \cong \mathbb{Z}_p = F_1^{(p)}$ $(p > 2)$．また $k = \mathbb{Q}(\mu_p)$ （且つ $p > 2$）のときは

$$h^1 - h^2 = \frac{p+1}{2}, \quad h^2 = 0 \leftrightarrow p : \text{regular}.$$

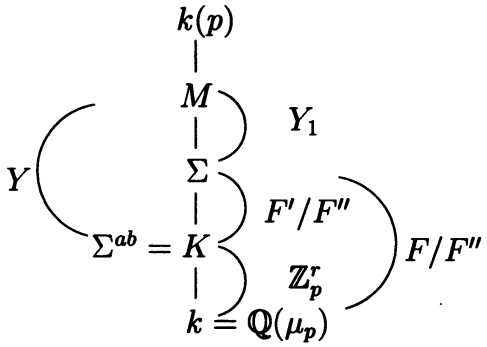
従って，p : regular のときは $G_{\mathbb{Q}(\mu_p)}(p) \simeq F_{\frac{p+1}{2}}^{(p)}$ で，p : irregular のときは $h^2 > 0$ です．（ちなみに，[NSW]Th8.7.3 の公式より，h^2 は $\mathbb{Q}(\mu_p)$ のイデアル類群の p-Sylow 群の最大 $(p, \cdots, p)$ 型商群の階数と等しい．）兎に角，$k = \mathbb{Q}(\mu_p)$, p : irregular のとき，$G_{\mathbb{Q}(\mu_p)}(p)$ は $F_{\frac{p+1}{2}}^{(p)}$ を商群にもつかどうかが問題の一つとなります．

5.2

定理 ([Mc]Th2). *p : irregular prime とする．$(\mathbb{Q}(\mu_p), p)$ が (GGC) を満せば，$G_{\mathbb{Q}(\mu_p)}(p)$ は $F_{\frac{p+1}{2}}^{(p)}$ を商群に持ち得ない．*

実は，これより少し強く，同じ条件のもとで，$F = F_{\frac{p+1}{2}}^{(p)}$, $F' = (F, F)$, $F'' = (F', F')$ とするとき，$G_{\mathbb{Q}(\mu_p)}(p)$ は F/F'' と同型な商群を持ち得ない事が示せます．ただし，$(\ ,\ )$ は位相群の交換子群．今迄の話のつながりを理解する助けになるかと思いますので，以下その略証を述べます（上記 [Mc]Th2 の証明とは少々異る）．

（略証） $r = \frac{p+1}{2}$, $F = F_r^{(p)}$ とするとき，仮りに $k(p)/k$ が (F/F'')- 拡大 Σ/k を含むとする；$Gal(\Sigma/k) = F/F''$. このとき Σ/k の最大アーベル部分体 Σ^{ab}/k は F/F'' の交換子群 F'/F'' と対応する Σ/k の部分体であり，$Gal(\Sigma^{ab}/k) = F/F' \cong \mathbb{Z}_p^r$ ゆえ，$\Sigma^{ab} = K$. また $Gal(\Sigma/K)$ はアーベル群ゆえ，$\Sigma \subset M$. $Y_1 = Gal(M/\Sigma)$ とおく.



さて純 (pro-p) 群論的に $F'/F''(= Y/Y_1)$ を $\Lambda = \mathbb{Z}_p[\![F/F']\!] \cong \mathbb{Z}_p[\![t_1, \cdots, t_r]\!]$ 加群とみると，既知の Blachfield-Lyndon 型定理により，

$$F'/F'' \underset{\Lambda}{\simeq} \{(\lambda_1, \cdots, \lambda_r) \in \Lambda^r; \quad \sum_{i=1}^{r} \lambda_i t_i = 0\}.$$

従って Λ の商体を Λ^0 とすると，$(F'/F'') \underset{\Lambda}{\otimes} \Lambda^0$ は Λ^0 上のベクトル空間として $r-1$ 次元. 一方，$Y = Gal(M/K)$ についても，Jannsen, Nguyen-Quang Do の構造定理より，Y は有限生成 Λ 加群で $\dim_{\Lambda^0}(Y \underset{\Lambda}{\otimes} \Lambda^0) = r-1$ （例えば [Mc]Th10 参照）. よって $\dim\left((Y/Y_1) \underset{\Lambda}{\otimes} \Lambda^0\right) = \dim(Y \underset{\Lambda}{\otimes} \Lambda^0)$. よって $Y_1 \underset{\Lambda}{\otimes} \Lambda^0 = 0$, 即ち Y_1 は Λ-torsion. しかし (GGC) によれば Y は torsion-free (§4.2). よって $Y_1 = 0$, 即ち $M = \Sigma$. しかし M/K は $k(p)/K$ の最大アーベル部分体ゆえ，$M \supset k(p)^{ab}$. しかし $M = \Sigma$ の中での最大アーベル部分体は $\Sigma^{ab} = K$ ゆえ，$K = k(p)^{ab}$. よって $Gal(k(p)^{ab}/k) \cong \mathbb{Z}_p^r$. これは p:regular のときに限る.

6 $\mathbb{P}^1 - \{0, 1, \infty\}$ の pro-p 基本群との関係について [Sh]

6.1

以下は極く最近の R. Sharifi [Sh] の研究の簡単な紹介です．二，三年前に私が提出した問 [Ih] Lect I §5-6 に対して，(GGC) と関係した条件つき解答を与えているものです．基本的定義について [Ih] も御参照下さい．以下 p は素数 > 2，$k = \mathbb{Q}(\mu_p)$ とします．

$\bar{\mathbb{Q}}$ 上の射影直線を $\mathbb{P}^1_{\bar{\mathbb{Q}}}$ とするとき，pro-p 基本群

$$\pi_1 = \pi_1^{\text{pro-}p}(\mathbb{P}^1_{\bar{\mathbb{Q}}} - \{0, 1, \infty\})$$

への $\mathbb{Q}$ の絶対ガロア群 $G_{\mathbb{Q}}$ の外作用を考え，それを $G_k = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\mu_p))$ へ制限すると，それは $G_k(p) = \mathrm{Gal}(k(p)/k)$ を通して作用します（忠実かどうかは未知）．さて π_1 の中心降下列を用いて $G_k(p)$ の filtration 及び graded Lie algebra

$$\mathfrak{g}_p = \bigoplus_{m \geq 3} gr^m \mathfrak{g}_p$$

が定義されます．各 $gr^m\mathfrak{g}_p$ は有限生成自由 $\mathbb{Z}_p$ 加群で，一方 $\mathfrak{g}_p$ は $\mathbb{Z}_p$ 上の Lie 環の構造を持ち，$[gr^m\mathfrak{g}_p, gr^n\mathfrak{g}_p] \subset gr^{m+n}\mathfrak{g}_p$ $(m, n \geq 3)$ が満されます．各奇数 $m \geq 3$ に対して Soulé character と呼ばれる $\mathbb{Z}_p$- 線形射 $(\neq 0)$

$$\kappa_m : gr^m\mathfrak{g}_p \to \mathbb{Z}_p$$

が定義されています．$gr^m\mathfrak{g}_p = \mathbb{Z}_p\sigma_m + \mathrm{Ker}(\kappa_m)$ を満す $\sigma_m \in gr^m\mathfrak{g}_p$ を各奇数 $m \geq 3$ に対して一つづつ選んでおきます．最近，Hain-Matsumoto [HM] により，$\mathfrak{g}_p \otimes \mathbb{Q}_p$ は $\mathbb{Q}_p$ 上の Lie 環として σ_m (m : 奇数 ≥ 3) 達で生成されることが示されました．一方，Deligne は（別の定式化でですが）次の予想を立てています．

予想 (D). σ_m (m : 奇数 ≥ 3) 達は $\mathfrak{g}_p \otimes \mathbb{Q}_p$ のLie 環としての free generators であろう．

しかし $G_k(p)$ の π_1 への作用の数論的性質の研究には，$\otimes\mathbb{Q}_p$ する前の $\mathfrak{g}_p$ の性質がより重要です．私は [Ih] で，$p = 691, m = 12$ （このとき $p|B_m$ （ベルヌイ数））のとき，$[\sigma_3, \sigma_9]$ と $[\sigma_5, \sigma_7]$ のある一次結合が "stable derivation algebra" の 12 次の成分 $gr^{12}\mathcal{D} \otimes \mathbb{Z}_p$ の中で満すある合同式 $(\mathrm{mod}\ p)$ から，p が irregular なとき $\mathfrak{g}_p$ 自身は σ_m 達では生成されない可能性が十分あることを指摘しました．Sharifi はこれに関して，次の事を示しました．

定理 (Sharifi [Sh]). 予想(D) を仮定すると次の(i) (ii) が成立つ.

(i) p: regular のとき, $\mathfrak{g}_p$ は σ_m (m : 奇数 ≥ 3) で生成され, $G_k(p)$ の π_1 への外作用は忠実.

(ii) p: irregular なとき, 更に p に関するVandiver 予想と (k,p) に関する(GGC) を仮定すると, $\mathfrak{g}_p$ は σ_m (m : 奇数 ≥ 3) 達では生成され得ない.

(ii) について, 更に定量的研究も進みつつあるようですが, $p = 691$ は (GGC) も示されておらず, 微妙なようです.

証明のアイデアは次の通り. 各 $gr^m\mathfrak{g}_p$ は $G_k(p)$ の部分商なので, σ_m を代表する適当な元 $\tilde{\sigma}_m \in G_k(p)$ をとるのですが, $\tilde{\sigma}_3, \tilde{\sigma}_5, \ldots, \tilde{\sigma}_p$ までとると, それと $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/k)$ ($\cong \mathbb{Z}_p$) の生成元の $G_k(p)$ への延長の一つ γ を用いて, 残りの $\tilde{\sigma}_m$ ($m = p+2, \ldots$) 達でよい性質を満すものを群論的に構成できる, というのが一つのポイントです. (Vandiver 予想はここで使っています.)

p: regular のときは, $G_k(p)$ は $\tilde{\sigma}_3, \ldots, \tilde{\sigma}_p, \gamma$ の上の自由 pro-p 群になり, それを用いて $\mathrm{Gal}(k(p)/K)$ が $\tilde{\sigma}_m$ (m : 奇数, ≥ 3) で生成される自由 pro-p 群であることを示し, (D) を仮定して残りの結論を出す.

p: irregular のときは, もし $\mathfrak{g}_p$ が σ_m 達で生成される free Lie algebra と同型とすると, $G_k(p)$ の π_1 への外作用の核と対応する体を $k(p)^*$ と書くとき, $\mathrm{Gal}(k(p)^*/k)$ は $\sigma_3, \ldots, \sigma_p, \gamma$ の上で自由 pro-p (階数 $\frac{p+1}{2}$) ということになり, 5.2 の結果と矛盾する, という方針です.

参考文献

[G_1] Ralph Greenberg (Thesis, Princeton University)(1971), "On some questions concerning the Iwasawa invariants".

[最近の Preprints] (2000 年のもの)

[G_2] R. Greenberg, "Iwasawa theory, Past and Present" preprint 2000; to appear in Advanced Studies in Pure Math.
http://www.math.washington.edu/~greenber/personal.html

[LN] A. Lannuzel, T. Nguyen Quang Do, "Conjectures de Greenberg et extensions pro-p-libres d'un corps de nombres" Manuscripta math. **102**(2000), 187–209.

[Mc] W.G. McCallum, "Greenberg's conjecture and units in multiple $\mathbb{Z}_p$-extensions", Algebraic Number Theory Preprint Archives, no.249, July 2000.

[Sh] R. Sharifi, "Relationships between conjectures on the structure of Galois groups of number fields", Preprint December 2000.

[関係引用]

[O] 尾崎 学, "Greenberg 予想について", 数理解析研 講究録 **1026**(1998), 20–27.

[HM] R. Hain and M. Matsumoto, "Weighted completion of Galois groups and some conjectures of Deligne", arXiv: math. AG/0006158, June 2000.

[Ih] Y. Ihara, "Some arithmetic aspects of Galois actions on the pro-p fundamental group of $\mathbb{P}^1 - \{0, 1, \infty\}$", Preprint, May 1999, RIMS-1229.

[NSW] J. Neukirch, A. Schmidt and K. Wingberg, "Cohomology of Number Fields", Springer GMW **323** (2000).

[Y] M. Yamagishi, "A note on free pro-p extensions of algebraic number fields", J. de théorie des nombres de Bordeaux 5 (1993), 165–178.