数理解析研究所講究録
第658巻 1988年 43-55

円分体に関するいくつかの問題

岩澤健吉 (Kenkichi Iwasawa)

p を任意の奇素数，k を円の p 分体とし，k に関するいくつかの問題を簡単に説明します。殆ど皆よく知られたことばかりですが，この研究集会のような機会にそれらの問題を一応整理しておくのもいくらか意義があるかと考える次第です。

§1. 上記 k の有理数体上のガロア群を Δ，Δ の指標群を $\hat{\Delta}$，k のイデアル類群を C とする。周知のように $\hat{\Delta}$ は $\bmod p$ の Dirichlet 指標の成す群と同一視される。Δ は C の上に自然に作用するから，k の complex conjugation を J とする時 ($J \in \Delta$) C の部分群 C^{χ} を

(1) $$C^{+} = \mathrm{Ker}(1-J : C \to C), \quad C^{-} = \mathrm{Ker}(1+J : C \to C)$$

により定義する。k の最大実部分体を k^{+} とし，k^{+} のイデアル類群を C_{+} とすれば，自然な同型 $C/C^{-} \simeq C_{+}$ が存在する[1]。よ

って C, C^-, C_+ の位数を h, h^-, h^+ とすると

$$h = h^- h^+ .$$

定義により h, h^+ はそれぞれ代数体 k, k^+ の類数である。この $h^\pm$ について次の古典的な類数公式が知られている：

I. $\quad h^- = 2p \prod_\chi \left(\frac{1}{2} h_\chi\right)$;

ここに右辺の $\prod$ は $\chi(-1) = \chi(J) = -1$ を満足する凡ての $\chi \in \hat{\Delta}$ の上に亘る積で，又

(2) $$h_\chi = -\frac{1}{p} \sum_{a=1}^{p-1} \chi(a)^{-1} a .$$

II. $\quad h^+ = [E^+ : E_c]$.

但し E^+ は k^+ の単数群，E_c は E^+ に含まれる円単数から成る E^+ の部分群である。

上の I, II は解析的方法，詳しく言えば k の zeta 函数や Dirichlet の L 函数を用いて証明される公式であって，それの純数論的証明は今の所知られていない。そこで公式 I, II の持つ数論的な内容をもう少し深く調べて見たいと言うのが以下に述べるいくつかの問題の出発点である。

§2. 有理整数環 $\mathbb{Z}$ 上の Δ の群環を $\mathfrak{R}$ とする：$\mathfrak{R} = \mathbb{Z}[\Delta]$, $\mathfrak{R}$ は明らかに C の上に作用し，C は $\mathfrak{R}$-加群と考えられる。$\mathfrak{R}$ の Stickelberger イデヤルを $\mathfrak{s}$ とすれば $\mathfrak{s} \cdot C = 0$[2]。$\mathfrak{R}$, $\mathfrak{s}$ の部分群 $\mathfrak{R}^\pm$, $\mathfrak{s}^\pm$ を (1) の $C^\pm$ と同様に定義すると次の Lemma が成立つ：

Lemma 1. I の右辺 $= [\mathfrak{K}^- : \gamma^-]$ [3].

よって公式 I を次のように二つの有限アーベル群の位数の間の等式として書き直すことが出来る：

I. $\quad |C^-| = |\mathfrak{K}^-/\gamma^-|$.

同様に II は次の如く書ける：

II. $\quad |C_+| = |E^+/E_0|$.

I を上のように書いて見れば，誰でも思いつくのは，C^- と $\mathfrak{K}^-/\gamma^-$ との間には単に位数が等しいと言うばかりでなくもっと深い群論的な関係，例えば同型関係，が存在するのではなかろうか，と言うことである。ガロア群 Δ は C^- にも $\mathfrak{K}^-/\gamma^-$ にも自然に作用するから

C^- と $\mathfrak{K}^-/\gamma^-$ とは Δ-同型ではなかろうか？

と言う推測も生まれる。同様に

C_+ と E^+/E_0 とは Δ-同型か？

然しこれらの推測は実はいずれも成立しない：はじめの方は例えば $p = 3299$ に対し，又後の方は $p = 32009$ に対して成立しないことが容易に示される。(このような p は沢山ある。)

§3. そこで今度は公式 I，II に出てくる有限アーベル群の p-Sylow 群を考える[4]。その為 p 進整数環 $\mathbb{Z}_p$ 上の Δ の群環を R とする：$R = \mathbb{Z}_p[\Delta]$。$R = \mathfrak{K} \otimes \mathbb{Z}_p$ であるから $S = \gamma \otimes \mathbb{Z}_p$ は

R のイデヤルとなる。又 Δ の位数は $p-1$ であるから，任意の $\sigma\in\Delta$，$\chi\in\hat{\Delta}$ に対し $\chi(\sigma)$ は 1 の $p-1$ 乗根であるが，$\mathbb{Z}_p$ は 1 の $p-1$ 乗根を $p-1$ 個含むから，複素数の $p-1$ 乗根の全体を予め $\mathbb{Z}_p$ に埋め込んでおけば $\chi(\sigma)$ は $\mathbb{Z}_p$ の元と考えることが出来る。以下 $\chi(\sigma)$ はいつもこのように解釈する。さて任意の R-加群 M が与えられた時，$M^{\pm}$ を (1) の $C^{\pm}$ と同様に定義し，又 $\chi\in\hat{\Delta}$ に対して

$$M_\chi=\{x\in M\mid \sigma\cdot x=\chi(\sigma)x,\ \forall\sigma\in\Delta\}$$

とおけば，M は次のように直和分解される：

$$M=M^+\oplus M^-=\bigoplus_{\chi\in\hat{\Delta}}M_\chi .$$

この分解を R-加群である R，S に適用すれば

$$R=R^+\oplus R^-=\bigoplus_\chi R_\chi,\quad S=S^+\oplus S^-=\bigoplus_\chi S_\chi$$

を得る。更にイデヤル類群 C の p-Sylow 群 A も自然に R-加群となるから

$$A=A^+\oplus A^-=\bigoplus_\chi A_\chi .$$

以上の準備をして，又 C_+ と C^+ の p-Sylow 群が一致することに注意すれば，I，II から直ちに次の公式が得られる：

I_p $\quad |A^-|=|R^-/S^-|$,

II_p $\quad |A^+|=|(E^+/E_c)(p)|$,

但し $(E^+/E_c)(p)$ は E^+/E_c の p-Sylow 群をあらわす。そこでこの I_p，II_p から §2 の終りに述べたと同様な考えで次の問題が

導かれる：

P 1. (問題1)　　A^- と R^-/S^- とは R-同型か？

P 2. (問題2)　　A^+ と $(E^+/E_c)(p)$ とは R-同型か？

以下この二つの問題についていくつかの comments を述べよう。

注意. 同様にして，任意の素数 q に対し I，II の有限アーベル群の q-Sylow 群の間の Δ-同型を問題にすることも出来るが，$q \neq p$ の場合これは不成立ではなかろうか。(q を与えた時，不成立であるような $p\,(\neq q)$ が存在するという意味。) これも一つの問題である。

§4. 先ず次の Lemma は容易にわかる：

Lemma 2.　P 1 は次の i)，ii) のどちらとも同値である：

i)　$\mathbb{Z}_p$-同型：$A_\chi \simeq R_\chi/S_\chi$ が凡ての $\chi \in \hat{\Delta}$，但し $\chi(-1) = -1$，に対して成り立つ，

ii)　$A^- = Rx$ を満足する A^- の元 x が存在する。

次に ω を mod p の Teichmüller 指標とする：$\omega \in \hat{\Delta}$，$\omega(-1) = -1$，$\hat{\Delta} = \langle \omega \rangle$。この ω に対しては $A_\omega = 0$，$R_\omega/S_\omega = 0$ が直ちに言えるから，i) において $\chi \neq \omega$ としてもよい。

Lemma 3.　$\chi \in \hat{\Delta}$，$\chi(-1) = -1$，$\chi \neq \omega$ とすれば，(2) の h_χ は 0 でない p 進整数であって，

$$h_\chi \cdot A_\chi = 0, \quad R_\chi/S_\chi \simeq \mathbb{Z}_p/h_\chi \mathbb{Z}_p .$$

この Lemma により

$$P1 \iff A_\chi \simeq \mathbb{Z}_p/h_\chi\mathbb{Z}_p, \quad \forall \chi \in \hat{\Delta},\ \chi(-1)=-1,\ \chi\neq\omega$$

右辺の同型が成立すれば明らかに

$|A_\chi| = h_\chi$ を割る最高の p 巾, $\forall \chi \in \hat{\Delta}$, $\chi(-1)=-1$, $\chi\neq\omega$

となる。即ち P1 から上の等式が得られるわけであるが, 実はこの等式は Magur-Wiles の基本定理の特別な場合として P1 とは independent に既に証明されている。これは P1 を支持する一つの証と見られるであろう.

上のように $\chi \in \hat{\Delta}$, $\chi(-1)=-1$, $\chi\neq\omega$ とし, $\omega\chi^{-1}$ に属する Leopoldt の p 進 L 函数を $L_p(s;\omega\chi^{-1})$ とする。($\omega\chi^{-1}\in\hat{\Delta}$, $\omega\chi^{-1}(-1)=1$ に注意.)

Lemma 4. 与えられた χ に対し, 次の條件を満足する $\mathbb{Z}_p[[T]]$ の巾級数 $g_\chi(T)$ が唯一つ存在する:

$$g_\chi((1+p)^s-1) = L_p(s;\omega\chi^{-1}), \quad \forall s\in\mathbb{Z}_p.$$

これは p 進 L 函数の基本的な性質の一つである。勿論 $g_\chi(T)\neq 0$ であるから Weierstrass の preparation theorem により $g_\chi(T)$ は次のように一意的に書かれる:

$$g_\chi(T) = \eta_\chi(T)\,p^{\mu_\chi} f_\chi(T)。$$

ここに $\eta_\chi(T)$ は $\mathbb{Z}_p[[T]]$ の巾級数でその定数項 $\eta_\chi(0)$ が p で割れぬもの, μ_χ は一般には 0 又は正の整数であるが今の場合 $g_\chi(T)$ に対しては Ferrero-Washington の定理により $\mu_\chi=0$ であ

ることが知られている。又 $f_\chi(T)$ は次のような $\mathbb{Z}_p[T]$ の多項式（所謂 distinguished polynomial）である：

$$f_\chi(T) = T^n + a_1 T^{n-1} + \cdots + a_n, \quad n \geq 0,\ a_i \in p\mathbb{Z}_p,\ i = 1, \cdots, n$$

この $f_\chi(T)$ に関して次の問題がある：

$(P3)_\chi$ $f_\chi(T)$ は $\mathbb{Q}_p[T]$ で既約か？

何故このようなことが問題になるかと言えば次の Lemma が成立するからである：

Lemma 5. $(P3)_\chi$, $\forall \chi \in \hat{\Delta}$, $\chi(-1) = -1$, $\chi \neq \omega \Longrightarrow P1$

注意. Mazur-Wiles の定理を使えばもっと精密に次のことも言われる。即ち χ を一つ定めた時

$$(P3)_\chi \Longrightarrow A_\chi \simeq R_\chi / S_\chi.$$

又 $f_\chi(T)$ が必ずしも既約でなくても、重複根を持たなければ同じ結論が得られる。

次に $(P3)_\chi$ が成立する為の十分条件として次の二つの問題も考えられる：

$(P4)_\chi$, $f_\chi(T)$ は $\mathbb{Z}_p[T]$ の Eisenstein 多項式か？

$(P5)_\chi$. $\deg f_\chi(T) \leq 1$ ？

この $(P4)_\chi$, $(P5)_\chi$ を特に掲げたのはこれらが Bernoulli 数 B_n に関する条件として言うことが出来るからである。χ を上の通りとする時

$$\chi = \omega^{1-i}, \quad 0 < i < p-1$$

を満足する偶数 i が一意的に定まる。この i を用いて：

Lemma 6. $(P4)_\chi \iff B_{1+ip} \not\equiv 0 \mod p^2$.

Lemma 7. $(P5)_\chi \iff \frac{B_i}{i} \not\equiv \frac{B_{i+p-1}}{i+p-1} \mod p^2$.

上述により，もし P1 が成り立たなければ $(P3)_\chi$ が不成立であるような χ が存在する。従ってその χ に対しては $(P4)_\chi$ も $(P5)_\chi$ も不成立となるから上の Lemma 6, 7 を用いれば

$$\frac{B_{i+\nu(p-1)}}{i+\nu(p-1)} \equiv 0 \mod p^2, \quad \forall \nu = 0, 1, 2, \cdots$$

が得られる。特に $B_i \equiv 0 \mod p^2$ でなければならない。然しこのような p と i は今の所発見されていない。実際 Wagstaff は Bernoulli 数を計算して，凡ての $p < 125000$ と凡ての $\chi \in \hat{\Delta}$, $\chi(-1) = -1$, $\chi \neq \omega$, に対し $(P4)_\chi$, $(P5)_\chi$ が共に成立することを確かめた。

さて Lemma 7 の右辺の合同式は $\mod p$ では常に成立する。これは Kummer の証明した Bernoulli 数に関する一連の合同式の一つであるが，他の合同式，例えば三個の Bernoulli 数の間の $\mod p^2$ の合同式が $\deg f_\chi(T) \leq 2$ と関係があるかどうか，と言うようなことも一応考えて見る価値があろう。更に，多項式 $f_\chi(T)$ の根 α は p 進 L 函数 $L_p(S; \omega\chi^{-1})$ の零点を与えるものであるから，函数体との類似を考えれば大いに興味のある対象である。例えば $(P3)_\chi$ が成立する時，p 進数体 $\mathbb{Q}_p(\alpha)$ はどんな意味を持っているか，等々。

§5. 以上専ら P1 について考えてきたが，次に P2 に関係のあることを少し述べる。

P6. (Kummer-Vandiver の予想) $p \nmid h^+$?

この P6 は Fermat の問題に関聯してよく知られた予想であるが，我々にとつても興味があるのは

$$P6 \Longrightarrow P1, P2$$

が容易に証明されるからである。

次に k の最大実部分体 k^+ の上の円分 $\mathbb{Z}_p$ 拡大体を K^+ とし，K^+/k^+ の不変量を λ, μ とする。一般に $\mathbb{Z}_p$ 拡大の不変量は 0 又は正の整数であるが，今の場合には Ferrero-Washington の定理により $\mu = 0$。ところで

P7. λ も 0 ではないか: $\lambda = 0$?

この P7 は Greenberg の予想と呼ばれる予想の special case であるが，P6 ⇒ P7 は直ちに証明される。P6 と P7 との関係を更によく見る為に，任意の $n = 0, 1, 2, \cdots$ に対し円の p^{n+1} 分体を k_n とし，k_n のイデヤル類群，単数群をそれぞれ C_n, E_n とする。$m \geq n \geq 0$ であれば $k_n \subseteq k_m$ であるから自然な準同型 $C_n \longrightarrow C_m$, $E_m \longrightarrow E_n$ が定義される。(後者はノルム写像。) ここに

Lemma 8. $C_n \longrightarrow C_m$ が単射 $\Longleftrightarrow$ $E_m \longrightarrow E_n$ が全射。

これは容易に言えるが，そこで次の問題：

P8. 凡ての $m \geq n \geq 0$ に対し $C_n \longrightarrow C_m$ は単射か？

が生れる。この P8 と先の P6, P7 との関係は次の Lemma による：

Lemma 9. $P6 \Longleftrightarrow P7 \,\&\, P8$.

更に P2 との関聯について言えば

Lemma 10. $P1 \,\&\, P8 \Longrightarrow P2$.

も証明される。即ち P8 が成立すれば P2 は P1 に含まれる。このように P8 は中々面白い問題であるが，一番簡単な場合，即ち $m=1$, $n=0$ の場合に $C_0 \longrightarrow C_1$ が単射であることすら未だ解決されていない。もつともこの場合に証明出来れば一般の場合にも同様にして証明が得られそうな気がするが。

§6. 元来円の p 分体 k は Kummer が Fermat の問題を解こうとして研究した代数体であつて，それが今日の代数的整数論の端緒となつたことはよく知られている。よつて終りに，先の P1, P2 とは無関係だが，Fermat の問題といくらか関わりのある k についての問題を一つ付け加えておく。即ち：

P9. k 上の p-class field tower は有限か？

一般に任意の有限次代数体上の class field tower が有限で切れるであろうと言うのは古典的類体論が完成した頃からの有名な予想であつたが，1960 年代になつてそれは Golod-

Šafarevič により否定的に解決された。その時の方法を用いれば直ちに次のことが言われる。即ち，前のように k のイデヤル類群 C の p-Sylow 群を A とし，A の rank も r とする時

(3) $\qquad P9 \implies r < 2+\sqrt{2(p+1)}$.

この r は歴史的に Fermat の問題と関係の深い数で，例えば $r=0$，即ち $p \nmid h$，ならばその p についての Fermat の問題が解決されると言う Kummer の定理はよく知られている。r と Fermat の問題に関する多くの結果のうちで，次の Eichler の定理は特に重要である：

(4) $\qquad r < [\sqrt{p}]-1 \implies$ the first case of Fermat's problem.

明らかに $[\sqrt{p}]-1 < 2+\sqrt{2(p+1)}$ であるが，これらの二数はどちらも大体 $\sqrt{p}$ の大きさの数である。それ故例えば Golod－Šafarevič の結果を特に円分体 k の場合に精密化して (3) の限界 $2+\sqrt{2(p+1)}$ を $[\sqrt{p}]-1$ 迄引下げることは出来ないだろうか。乃至は Eichler の定理 (4) の限界 $[\sqrt{p}]-1$ を何とかして $2+\sqrt{2(p+1)}$ 迄引上げることは出来ないだろうか。もしそれが出来れば

$$P9 \implies \text{the first case of Fermat's problem}$$

となるわけで，これが上に述べた P9 と Fermat の問題との関聯である。然しこのような（希望的）関係を度外視しても，P9 はそれ自身十分興味ある問題であって，又たとえそれが否定的に解決されても面白い結果であると思う。もっと一般に，

F を任意の有限次代数体，L を F 上の最大不分岐（ガロア）p 拡大とする時，L/F が無限次拡大である場合（即ち F 上の p-class field tower が無限になる場合）に拡大 L/F の数論的性質を調べるという問題もあるが，このような一般的な問題に対しても $F=k$ の special case は critical であると思われる。

以上説明してきた円の p 分体 k に関する問題のなかには普通"予想"と呼ばれているものも含まれていますが，その大部分は私の極く大雑把な感じだけから，"こうなるのではなかろうか"とか"こうなつて欲しい"と言うようなことを述べたものであつて，私自身その成否についてそれ程確信があるわけではありません。特に $(P4)_\chi$，$(P5)_\chi$ などはたとえそれが計算により $p<125000$ 迄確かめられたとしても，不成立の可能性も十分考えるべきかと思います。そのような問題を持ち出したことについては，「数論の面白さは予測の当らない所にある」と言うことにして言いわけとします。

註

1) C^+ と C_+ とは 2-Sylow 群を除いて一致するが，必ずしも常に同型ではない。例：$p=29$.

2) γ の定義その他については Washington : Introduction to Cyclotomic fields を参照。以下に用いた円分体に関する色々な結果に関しても同様。

3) この Lemma は W. Sinnott により一般の円分体に対して拡張されている。

4) 何故 p-Sylow 群を考えるかと言うことについてはこの§の終りの注意参照。