1 の素数乗根全体で生成される体のアーベル拡大体のガロア群について

朝田　衞
（京都工芸繊維大学工芸科学研究科）

§1　動機

1-1　有限次代数体と有限体上の代数関数体（代数曲線）との類似はよく知られていますが、大きな違いのひとつに、代数体の場合、関数体と異なり、定数拡大というものがない、ということがあります。定数拡大の類似物の候補として、昔から考えられているものに、1 のべき根をすべて添加した最大円分体があります。（註 1））最大円分体を定数拡大の類似物とみなす理由は、恐らく、有限体の代数閉包は 1 のべき根をすべて添加して得られる、という事実によるのだと思います。もう少し新しいものとしては、無論、素数 p をひとつ固定して、1 の p べき乗根をすべて添加した円分拡大体もあります。

今回は、類似物の別の候補として、有限次代数体 k_0 に「すべての 1 の素数乗根を添加した体 k_1」を考えます。

これが、定数拡大の類似物とみなせる理由を説明する前に、関数体の定数拡大が持つ性質を確認しておきます。まず、定数拡大は、至る処不分岐な拡大体です。次に、そのガロア群、すなわち有限体 $\mathbf{F}_q$ の絶対ガロア群は、q 乗フロベニウス写像によって生成され、加法群 $\mathbf{Z}$ の profinite completion $\hat{\mathbf{Z}}$ に同型です。

さて、ガロア群 $\mathrm{Gal}(k_1/k_0)$ は位数 $l-1$ （l はすべての素数）の巡回群の直積の開部分群と同型であり、定数拡大体のガロア群とは全く異なっているため、類似であるという見方がしにくいかもしれません。しかし、この見方を支持する状況もいくつかあります。

ひとつは、有限体の代数閉包は 1 の素数乗根だけをすべて添加しても得られる、という事実です。（註 2））

別の状況証拠を説明するため、k_0 の有限素点 v を 1 つ固定します。v の惰性体を F, 分解体を F_D とし、拡大体 F/F_D のガロア群を G とします。

このとき、上に述べた事実から、まず

(i) G は v のフロベニウス置換により生成される $\hat{\mathbf{Z}}$ に同型な群である

ということがわかります。拡大体 k_1/k_0 における各素点の惰性群はすべて有限群で、群 $\hat{\mathbf{Z}}$ は torsion-free ですから、これより

(ii) F/F_D はいたるところ不分岐である

ということが従います。これは有限体上の関数体の定数拡大体の状況と非常によく似ています。(ガロア群 $\mathrm{Gal}(k_1/k_0)$ ではなく、その subquotient G に着目する、ということです。)

群 G は F 上の種々のアーベル拡大体のガロア群に自然に作用しますから、それらの G の作用も込めた構造はどのようなものか、ということに興味がわくわけです。

なお、(ii) より、体 F_D が

(iii) 拡大体 $F_D/\mathbf{Q}$ において、有限個の素数 l を除いて、l-素点の分岐指数は $l-1$ である

という性質をもつことが従いますが、これが、次の節で述べる主結果の証明の、数論的なポイントになっていることを付け加えておきます。

§2　主結果

2-1　群 $G(=\mathrm{Gal}(F/F_D))$ が作用する F 上のアーベル拡大体のガロア群でもっとも興味深いのは、F 上の最大不分岐アーベル拡大体のガロア群だとおもいますが、この群の G の作用も込めた構造については、今のところ、よくわかりません。今回得られた結果は、分岐を許したアーベル拡大体のガロア群の構造に関するものです。

以下では、$k_0=\mathbf{Q}$, $v=p>2$ とし、次のふたつの F のガロア拡大体を考えます；

M_p^{ab} : p の外で不分岐な F の最大アーベル pro-p 拡大体

M_p : p の外で不分岐な F の最大 pro-p 拡大体

これらはいずれも、その最大性により、F_D 上のガロア拡大体でもあります。従って、ガロア群 $\mathrm{Gal}(M_p^{ab}/F)$ には自然に G が作用します。このガロア群は、pro-p アーベル群ですから、G の p 進整数環上の完備群環 $\mathbf{Z}_p[[G]]$ 上の加群となります。

このとき、以下の結果が得られます。

主結果 **(I)** X は $\mathbf{Z}_p[[G]]$-加群として $\mathbf{Z}_p[[G]]$ の可算無限個の直積と同型である。

主結果 **(II)** ガロア群 $\mathrm{Gal}(M_p/F_D)$ は projective profinite group である。

(I), (II) の関連について説明します。(I) を示すために、X より大きなガロア群 $\mathrm{Gal}(M_p/F_D)$ が強い性質（射影性）を持つことを示すと（(II)）、これより、X が射影的 $\mathbf{Z}_p[[G]]$-加群であることが簡単に従います。そこで次に、(I) より弱い次の主張 (III) を示します：

(III) 任意の「初等的な」有限 $\mathbf{Z}_p[[G]]$-加群 $\mathbf{F}_p[G_n]^{\oplus m}$ $(m,\ n = 1, 2, ...)$ に対して、X から $\mathbf{F}_p[G_n]^{\oplus m}$ への全射準同型が存在する。ここで、G_n は G の唯一つの位数 n の商群（n 次巡回群）を表し、$\mathbf{F}_p[G_n]$ はその $\mathbf{F}_p$ 上の群環を、射影 $G \to G_n$ を通して $\mathbf{Z}_p[[G]]$-加群とみなしたものを表します。

これより、$\mathbf{Z}_p[[G]]$ の可算無限個の直積の（ embedding problem による）特徴付け（[1]）を適用して、(I) が得られるというようになっています。

講演時にも質問がありましたが、以上のような証明方法ですから、X の $\mathbf{Z}_p[[G]]$-加群としての具体的な生成元については、今のところ、何もわかっていません。具体的な生成元を求めるのは、ひとつの基本的な問題だと思います。

なお、基礎体 k_0 は有理数体 $\mathbf{Q}$ としていますが、主結果 (II) は、基礎体 k_0 が一般の有限次代数体でも、(p に関する）条件を満たせば成り立ちます。(III) については、（まだチェックしていないのですが、多分）基礎体が一般の有限次代数体の場合でも成り立つだろうと思います。

さらに、素点 v の剰余標数 p と異なる素数 l について、l の外で不分岐な F の最大アーベル pro-l 拡大体のガロア群の構造も問題となりますが、これについては、まだあまりよく考えていません。

今回は、(II) について、証明の方法とその概略を説明します。

2-2　まず、profinite group X が projective とは、任意の profinite group の完全列

$$1 \longrightarrow A \longrightarrow B \xrightarrow{\alpha} C \longrightarrow 1$$

と任意の準同型 $\varphi : X \longrightarrow C$ に対して、準同型 $\psi : X \longrightarrow B$ で、$\alpha\psi = \varphi$ を満たすものが存在することを言います。profinite group X が projective であるための必要十分条件は、任意の素数 l について、X の l-Sylow 部分群が free pro-l 群であることが知られています。（例えば Serre[7, I, 5.9] 参照。）

いま、$X = \mathrm{Gal}(M_p/F_D)$ について、その l-Sylow 部分群がどのようなものか考えてみます。X の商 $G = \mathrm{Gal}(F/F_D)$ は $\widehat{\mathbf{Z}}$ に同型ですから、X は pro-p

部分群 $\mathrm{Gal}(M_p/F)$ と G との半直積に同型です。これより直ちに、$l \neq p$ なら、X の l-Sylow 部分群は $\mathbf{Z}_l$ に同型であることがわかります。$l = p$ については、$\tilde{k}$ を F/F_D の中間体で $\mathrm{Gal}(F/\tilde{k})$ が $\mathbf{Z}_p$ に同型になる唯一のものとすると、$\mathrm{Gal}(M_p/\tilde{k})$ が X の l-Sylow 部分群となります。

従って、主結果 (II) は次の定理と同値です。

定理 (2-2) $\mathrm{Gal}(M_p/\tilde{k})$ は free pro-p 群である。

free pro-p 群のコホモロジー群による特徴付けによれば、$\mathrm{H}^2(\mathrm{Gal}(M_p/\tilde{k}); \mathbf{Z}/p\mathbf{Z}) = 0$ といっても同じです。

注意 体 M_p の最大性から、この体は（無限次代数体）$\tilde{k}$ 上でも、p の外で不分岐な最大 pro-p 拡大体となっています。

§3　代数体の分岐を制限した pro-p 拡大体

3-1　一般に k を有限次代数体、p を素数としたとき、分岐を制限した k の pro-p 拡大体のガロア群については、Shafarevich の先駆的な研究に始まり、Koch, O. Neumann 等、今日までいろいろと研究されています。定理 (2-2) の証明は、これらの結果を（極限をとることで）基礎体が無限次代数体 $\tilde{k}$ の場合のガロア群 $\mathrm{Gal}(M_p/\tilde{k})$ に適用します。ここでは、そのために必要な部分について、簡単に復習します。

まず、S を k の無限素点及び p-素点の全体からなる集合とし、

k_S：S の外で不分岐な k の最大ガロア拡大体

$k_S(p)$：S の外で不分岐な k の最大 pro-p 拡大体

とし、それぞれの k 上のガロア群を G_S, $G_S(p)$ とします；$G_S = \mathrm{Gal}(k_S/k)$, $G_S(p) = \mathrm{Gal}(k_S(p)/k)$.

pro-p 群のコホモロジーの一般論により、1 次コホモロジー群 $\mathrm{H}^1(G_S(p); \mathbf{Z}/p\mathbf{Z})$ の $\mathbf{F}_p$ 上の次元は $G_S(p)$ の生成系の最小個数に等しく、2 次コホモロジー群 $\mathrm{H}^2(G_S(p); \mathbf{Z}/p\mathbf{Z})$ の $\mathbf{F}_p$ 上の次元は $G_S(p)$ の関係式系の最小個数に等しくなっています。1 次コホモロジー群の次元は、類体論を応用することで、直ちに基礎体 k の種々の不変量によって表すことが出来ますが、2 次コホモロジー群の次元をとらえるのは難しく、Shafarevich によるものです。現代風の説明は、以下に述べるように、コホモロジーの localization map を基礎にしています。

k の任意の素点 v について、k_S から $\bar{k}_v$ (k の v 進完備化 k_v の代数閉包) への埋め込み φ をひとつ与えます。これより、k_v の絶対ガロア群 G_{k_v} から G_S への制限写像が定まり、コホモロジー群の間の準同型 $\mathrm{H}^2(G_S;\mathbf{Z}/p\mathbf{Z}) \to \mathrm{H}^2(G_{k_v};\mathbf{Z}/p\mathbf{Z})$ が誘導されます。これは、φ の選び方に依らないこと、v が S に含まれていないならば 0-map であること、がわかります。従って、これらをすべての素点について合わせて準同型写像

$$\rho_k : \mathrm{H}^2(G_S;\mathbf{Z}/p\mathbf{Z}) \to \oplus_{v\in S}\mathrm{H}^2(G_{k_v};\mathbf{Z}/p\mathbf{Z})$$

が定まります。これを localization map と呼びます。(註 3))

群 $G_S(p)$ は G_S の商群ですから、inflation map

$$\mathrm{H}^2(G_S(p);\mathbf{Z}/p\mathbf{Z}) \to \mathrm{H}^2(G_S;\mathbf{Z}/p\mathbf{Z}) \tag{3.1}$$

が定まりますが、O. Neumann[4] の基本的な結果は、これは 同型 である、というものです。

3-2　定理の証明に関係があるのは、$G_S(p)$ がいつ free pro-p 群になるか、ということですが、以上により、局所的な条件

(C1)　$$\mathrm{H}^2(G_{k_v};\mathbf{Z}/p\mathbf{Z}) = \{0\} \quad (v \in S)$$

及び大域的な条件

(C2)　$$\mathrm{Ker}\rho_k = \{0\}$$

が成り立っていれば、$\mathrm{H}^2(G_S(p);\mathbf{Z}/p\mathbf{Z}) = \{0\}$, 即ち $G_S(p)$ が free pro-p 群になることがわかります。

最初の条件 (C1) は、Tate の local duality （例えば Neukirch-Schmidt-Wingberg[3, VII, §2], Serre[7, II, 5.2]）により $\mathrm{H}^0(G_{k_v};\mu_p) = \{0\}$ に同値で (μ_p : 1 の p 乗根のなす群)、それゆえ、$k_v^* \cap \mu_p = \{1\}$ と同値となります。

次に２番目の条件 (C2) ですが、これは、Neukirch により、embedding problem に関する条件として言い換えることができます。

一般に、体 k とそのガロア拡大体 L が与えられたとき、ガロア群 $\mathrm{Gal}(L/k)$ に対する embedding problem とは、図式

$$\begin{array}{ccccccccc} & & & & & & \mathrm{Gal}(L/k) & & \\ & & & & & & \downarrow\varphi & & \\ 1 & \longrightarrow & A & \longrightarrow & E & \xrightarrow{\alpha} & G & \longrightarrow & 0 \end{array}$$

のことを言います。ただし、下の短完全列は、profinite group の短完全列で、φ は全射準同型です。

これに対して、準同型 $\psi : \mathrm{Gal}(L/k) \longrightarrow E$ で、$\alpha\psi = \varphi$ を満たすものをこの embedding problem の weak solution と言い、 ψ が更に全射のとき、solution と言います。

さて、いま、embedding problem としては、$L = \bar{k}$ で、$A = \mathbf{Z}/p\mathbf{Z}$, E 及び G は有限群、φ は G_S を経由する、という条件を満たすものだけを考えます。このとき、(C2) が成り立つための必要十分条件は、「このような embedding problem がもし weak solution を持つならば、G_S を経由する weak solution を持つ」ことです（Neukirch[2, Satz 8.1]）。

§4　定理の証明 (概略)

4-1　前節の Neukirch の結果により、定理の証明を embedding problem に関する問題に帰着させることができます。

まず、$\tilde{k}$ を (2-2) で定めた（無限次の）代数体とし、$\tilde{k}$ に含まれる有限次代数体 k を考えます。$M_p(k)$ を k の p の外で不分岐な最大 pro-p 拡大体とすると、体 M_p は、すべての k についての $M_p(k)$ の合成体となります。

従って、$\mathrm{H}^2(\mathrm{Gal}(M_p/\tilde{k}); \mathbf{Z}/p\mathbf{Z}) = 0$ を示すためには、

$$(\tilde{\mathrm{C}}1) \qquad \varinjlim \mathrm{H}^2(G_{k_v}; \mathbf{Z}/p\mathbf{Z}) = \{0\} \quad (v \in S)$$

$$(\tilde{\mathrm{C}}2) \qquad \varinjlim \mathrm{Ker}\rho_k = \{0\}$$

を示せばよいわけです。

p は $F/\mathbf{Q}$ で不分岐で $p > 2$ ですから、$k_v^* \cap \mu_p = \{1\}$, すなわち (C1) が成り立つことから、 条件 $(\tilde{\mathrm{C}}1)$ も成り立ちます。次に条件 $(\tilde{\mathrm{C}}2)$ についてです。まず、$\tilde{k}$ の絶対ガロア群を $G_{\tilde{k}}$, $G_{\tilde{k}}$ の最大 pro-p 商を $G_{\tilde{k}}(p)$ とすると、inflation map

$$\mathrm{H}^2(G_{\tilde{k}}(p);\mathbf{Z}/p\mathbf{Z}) \to \mathrm{H}^2(G_{\tilde{k}};\mathbf{Z}/p\mathbf{Z})$$

が、(3.1) と同様にして、同型であることがわかっています（Neukirch-Schmidt-Wingberg[3, (10.4.8)]）。そこで、これを用いると、(C̃2) が満たされることを示すことは、次の、有限 p-群 に関する embedding problem についての命題を示すことに帰着します。

命題 (4-1) embedding problem

$$\begin{array}{ccccccccc} & & & & & & G_{\tilde{k}}(p) & & \\ & & & & & & \downarrow\varphi & & \\ 1 & \longrightarrow & \mathbf{Z}/p\mathbf{Z} & \longrightarrow & E & \xrightarrow{\alpha} & G & \longrightarrow & 0 \end{array}$$

において、E, G は有限 p-群、$\varphi : G_{\tilde{k}}(p) \to G$ は $\mathrm{Gal}(M_p/\tilde{k})$ を経由する、という条件を満たすものを考える。

この embedding problem がもし weak solution を持つならば、 $\mathrm{Gal}(M_p/\tilde{k})$ を経由する weak solution を持つ。

4-2　命題 (4-1) は、短完全列が split している場合は、自明に成立していますので、問題は、短完全列が split していない場合で、このとき、weak solution は自動的に solution になります。結局、solution を持つとき、それを取り替えて、分岐を制限した solution を作れる、ということを示すことになります。これを示す方針は、Scholz[6], Reichardt[5], Shafarevich[8] による、有限 p 群をガロア群に持つ $\mathbf{Q}$ 上のガロア拡大体の構成の方法です。そこでは、有限 p-群をガロア群に持ち、かつ分岐に関するある条件を満たすガロア拡大体が構成されています。これは、有限 p-群の組成列の長さによる帰納的な構成ですが、長さをひとつ増やすステップは、一度拡大体を構成するステップと、それを分岐に関する条件を満たすものに取り替える（分岐を減らす）ステップに分かれます。

この「分岐を減らす」手法がちょうど、命題 (4-1) の証明に使えるのです。そのときの数論的なポイントは、§1 に述べた条件 (iii), すなわち、拡大体 $\tilde{k}/\mathbf{Q}$ において、有限個の素数 l を除いて、l-素点の分岐指数は $l-1$ である、という事実です。（これは無論、$\tilde{k}$ が十分大きい（無限次）ために初めて成り立ちうることです。）

§5　註

1））例えば、Artin, Tate : Class field theory の中にも、相互律の証明手法に関して、そのような記述があります。

2））例えば、藤崎源二郎著「体とガロア理論（定理 3.10)」参照。

3）localization map については、その核及び像を記述することもできます（Poitou-Tate の duality, 例えば Neukirch-Schmidt-Wingberg[3, VIII, §6], Serre[7, II, 6.3] 参照)。それと、この後に述べた O. Neumann の結果を合わせると、2 次コホモロジー群 $\mathrm{H}^2(G_S(p); \mathbf{Z}/p\mathbf{Z})$ の $\mathbf{F}_p$ 上の次元、すなわち $G_S(p)$ の関係式系の最小個数がわかるわけです。

文献

[1] M. Asada, On Galois groups of abelian extensions of the maximal cyclotomic field, Tohoku Math. J. 60(2008), 135–147.

[2] J. Neukirch, Über das Einbettungsproblem der algebraischen Zahlentheorie, Invent. Math. 21(1973), 59–116.

[3] J. Neukirch, A. Schmidt, K. Wingberg, Cohomology of Number Fields, Second edition, Springer, 2008.

[4] O. Neumann, On p-closed number fields and an analogue of Riemann's existence theorem. In : A. Fröhlich(ed.), Algebraic Number Fields, Academic Press London 1977, 625–647.

[5] H. Reichardt, Konstruction von Zahlkörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung, J. Reine Angew. Math. 177(1937), 1–5.

[6] A. Scholz, Konstruction algebraischer Zahlkörper mit beliebiger Gruppe von Primzahlpotenzordnung, Math. Z. 42(1936), 161–188.

[7] J.P. Serre, Cohomologie Galoisienne, Lecture Notes in Mathematics 5, Springer 1964 (5. édition 1994).

[8] I. R. Shafarevich, On the construction of fields with a given Galois group of order l^{α}, Izv. Akad. NaukSSSR, Ser. Mat. 18(1954), 261–296.