体構造の復元を通した遠アーベル幾何学入門

辻村昇太 (京都大学数理解析研究所)

目次

導入 1

1 群や体に関する復習 2

2 絶対 Galois 群 9

3 Kummer 理論 13

4 局所体と大域体 14

5 非アルキメデス的局所体や大域体に関連する復元定理の紹介 20

補足 25

参考文献 26

導入

遠アーベル幾何学では、様々な幾何学的/スキーム論的設定において、エタール基本群等の被覆の対称性のなす群が元の幾何学的/スキーム論的構造の情報をどの程度保持しているかについて考察する分野である。本講義の目標は、比較的初等的な言葉で主張を述べることが可能な題材を通してこの遠アーベル幾何学という分野の紹介を行うことである。(比較的初等的な言葉で議論可能だというだけで、紹介する定理そのものは深いものである。)

本稿タイトル内の体 (たい) とは、一言で述べると、集合 K とその上の適切な条件を満たす足し算や掛け算のような二種類の二項演算(つまり、二つの元から一つの元を与える操作)

$$+_K \colon K \times K \longrightarrow K, \quad \times_K \colon K \times K \longrightarrow K$$

の組のことである。(ちなみに、$K \times K$ の中の $\times$ は集合としての積を意味する記号であって、$K \times K$ は単に K の二元の組のなす集合のことである。)例えば、有理数の集合 $\mathbb{Q}$ や実数の集合 $\mathbb{R}$ とその上の通常の足し算や掛け算の組は体になり、有理数体や実数体などと呼ばれる。体上の

二種類の演算は非常に複雑に絡まっており、その両方の性質に深く関連する問題の中には、フェルマー予想や abc 予想等非常に難しい問題が含まれる。このような二種類の演算を備えた対象に対して、一種類の演算のみを備えた群と呼ばれるまた別の概念が存在する。それは、集合 G とその上の適切な条件を満たす一種類の二項演算

$$G \times G \longrightarrow G$$

の組のことである。本稿の第 2 節で説明するが、体に対し絶対 Galois（ガロア）群という拡大体の対称性のなす群を定義することができる。この文脈では遠アーベル幾何学とは、二種類の演算からなる体構造を一種類の演算からなる絶対 Galois 群の群構造によって捉えてしまおうという思想に基づいた学問である。もちろんいつでも完全に捉えられるわけではなく、可能な場合と不可能な場合が存在する。広義には、絶対 Galois 群の群構造のような対称性のなすより弱い構造からどの程度元の構造が捉えられるか/復元できるか（あるいは捉えられないか — 不定性）をいろいろな設定で研究する学問と言える。

本稿のより具体的な目標は、体構造がその絶対 Galois 群からどの程度復元できるかという遠アーベル幾何学の基本的な問題に関して、

- 絶対 Galois 群の群構造と元の体の乗法群構造は、Kummer（クンマー）理論や類体論等を通して比較的結びつきやすいこと、
- p 進局所体の場合には絶対 Galois 群の群構造と元の体の（既に得られた乗法構造と両立的な形で) 加法構造を復元することは一般には不可能なこと、
- Neukirch（ノイキルヒ）-内田によって示された数体等に対する復元定理

を紹介することである。様々な予備知識が必要な証明等を説明したいわけではなく、どういった定理が存在しているかということの紹介が目的である。講義の大雑把な計画として、初日は §1, 二日目は §2, 三日目は §4, 四日目は §5 の内容について（もちろん全てはできないが）解説することを考えている。つまり、前半では群や体、絶対 Galois 群の説明を行い、後半では p 進局所体、数体等の数論的に特別な体の紹介及びそれらに対する遠アーベル幾何学的結果の紹介を行う予定である。（現在の版は、講義後の加筆修正版である。）

1　群や体に関する復習

本節では、以降の準備のためにいくつかの群論的・体論的概念を簡単に復習する。（詳細は学部生向けの代数学の教科書等をご参照ください。）また、講義では群や体の正確な定義を述べる等は時間の都合上行わないため、詳細が気になる方はこれらについて目を通していただければ幸いである。一方で、群や体に関して導入で述べたような粗い認識でも、ある程度聴いていただけるようにはしたい。

定義 1.1. 群とは、集合 G とその上の二項演算

$$*\colon G \times G \longrightarrow G, \quad (g_1, g_2) \mapsto g_1 * g_2$$

の組で次の条件を満たすものである。

(a) $*$ は結合律を満たす。つまり、任意の三元 g_1, g_2, g_3 に対し、$g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$ が成立する。

(b) (一意的に定まる）単位元が存在する。つまり、任意の元 $g \in G$ に対し $g * e = e * g = g$ を満たす元 $e \in G$ が存在する。

(c) 各元に対し (一意的に定まる）逆元が存在する。つまり、任意の元 $g \in G$ に対し $g * g^{-1} = g^{-1} * g = e$ を満たす元 $g^{-1} \in G$ が存在する。

注意 1.1.1. 慣習として群 $(G, *)$ を G と略記するが、集合と演算の組であることは忘れてはならない。また本稿では、$*$ を省略して $g_1 * g_2$ のことを $g_1 g_2$ と書くことが多い。

例 1.2.

(i) 整数の集合 $\mathbb{Z}$（や有理数の集合 $\mathbb{Q}$、 実数の集合 $\mathbb{R}$ 等) とその上の通常の加法の組は群である $(e = 0)$。

(ii) $\mathbb{Q}$ や $\mathbb{R}$ から 0 を除いた集合とその上の通常の乗法の組は群である $(e = 1)$。

(iii) 正の整数 n に対し、n 個の元からなる整数の集合 $\{0, 1, \ldots, n-1\}$ を考える。この n 元集合上に二項演算を通常の整数の足し算を行ってから n で割った余りを取るという操作で定義すれば単位元を 0 とする群になることが確認できる。そのような群を $\mathbb{Z}/n\mathbb{Z}$ と書く。

これらの例は任意の二元 g_1, g_2 に対し、$g_1 * g_2 = g_2 * g_1$ が成立するので可換群（アーベル群）と呼ばれる種類の群である。行列群や対称群等、重要かつ非可換な群もたくさん存在し、遠アーベル幾何学では非可換度の高い群を扱うことが多い。また、$\mathbb{Z}$ や $\mathbb{Z}/n\mathbb{Z}$ のように一元で生成される（ある元 x が存在して任意の元が $x * x * \cdots * x$ の形で書ける）アーベル群は特別な名前が付いていて、巡回群と呼ばれる。

定義 1.3. 体とは、集合 F とその上の二種類の二項演算

$$+_F\colon F \times F \longrightarrow F, \quad (f_1, f_2) \mapsto f_1 +_F f_2, \qquad \times_F\colon F \times F \longrightarrow F, \quad (f_1, f_2) \mapsto f_1 \times_F f_2$$

の組で次の条件を満たすものである。

(a) 組 $(F, +_F)$ はアーベル群である。(その単位元を 0 と書く。)

(b) 任意の元 $f \in F$ に対し $0 \times_F f = f \times_F 0 = 0$、及び、0 でない任意の二元 $f_1, f_2 \in F$ に対し、$f_1 \times_F f_2 \neq 0$ が成立する。(特に、$\times_F$ は $F \setminus \{0\}$ 上の二項演算

$$F \setminus \{0\} \times F \setminus \{0\} \longrightarrow F \setminus \{0\}, \quad (f_1, f_2) \mapsto f_1 \times_F f_2$$

を誘導する。この演算も $\times_F$ と書く。)

(c) 組 $(F \setminus \{0\}, \times_F)$ はアーベル群である。(その単位元を 1 と書く。)

(d) $0 \neq 1$。

(e) 分配律が成立する。つまり、任意の三元 $f_1, f_2, f_3 \in F$ に対し、$(f_1 +_F f_2) \times_F f_3 = f_1 \times_F f_3 +_F f_2 \times_F f_3$ を満たす。

注意 1.3.1. 慣習として体 $(F, +_F, \times_F)$ を F と略記するが、こちらも集合と演算の組であることを忘れてはならない。

注意 1.3.2. 体 F に対し、$F^\times \overset{\text{def}}{=} F \setminus \{0\}$, $+ \overset{\text{def}}{=} +_F$ のように略記する。そして、$\times_F$ は注意 1.1.1 と同様省略して書くことにする。($+$ まで省略してしまうとどちらの演算のことか分からなくなるので、加法側の記号は残す。) また、体 F の元 f に対し ($f \neq 0$ のとき) 乗法的逆元を f^{-1}, 加法的逆元を $-f$ と書く。

例 1.4.

(i) $\mathbb{Q}$ や $\mathbb{R}$ とその上の通常の加法、乗法の組は体になる。一方で、$\mathbb{Z}$ とその上の通常の加法、乗法の組は (± 1 以外の元は乗法に関する逆元を持たないため) 体にならない。

(ii) 素数 p に対し、p 個の元からなる整数の集合 $\{0, 1, \ldots, p-1\}$ を考える。この p 元集合上に二種類の二項演算を通常の整数の足し算や掛け算を行ってから p で割った余りを取るという操作で定義すれば実は体になることが確認できる。そのような体を $\mathbb{F}_p$ と書く。これは有限体 (有限個の元からなる体) の最も基本的な例である。例 1.2, (iii) の状況と異なり素数であることを課しているが、この条件がないと 0 でない元が常に乗法的逆元を持つことが確認できないためである。(つまり、定義 1.3 の条件 (c) が確認できないためである。) p が素数であることで、$a \in \{1, \ldots, p-1\} = \mathbb{F}_p \setminus \{0\}$ に対し、a 倍してから p で割った余りを取るという操作が、全単射

$$\{0, 1, \ldots, p-1\} \xrightarrow{\sim} \{0, 1, \ldots, p-1\}$$

を誘導することが観察できる。(この写像の定義域と値域の元の数が同じなので、単射さえ分かれば良いが、それはまさに素数の性質から従う。) 特に、ある元 $b \in \{1, \ldots, p-1\}$ が存在して $ab = 1 \in \mathbb{F}_p$ となるので、体になることが確認できる。

定義 1.5. G_1, G_2 を群、F_1, F_2 を体とする。

(i)

$$\sigma \colon G_1 \longrightarrow G_2$$

を写像とする。σ が G_1 や G_2 の群構造と両立的である、つまり、任意の $(x, y) \in G_1 \times G_1$ に対し、

$$\sigma(xy) \;=\; \sigma(x)\sigma(y)$$

が成立するとき、σ を群の準同型写像という。さらに σ が全単射のとき、σ を群の同型写像という。また、σ が群の同型写像かつ $G_1 = G_2$ のとき、特に σ を G_1 の自己同型写像と

いう。さらに、G_1 の自己同型写像の内ある元による共役を取る操作で得られる特別な種類の自己同型写像

$$G_1 \xrightarrow{\sim} G_1, \quad x \mapsto g^{-1}xg$$

を G_1 の内部自己同型写像という。

(ii) G_1 と G_2 の間に群の同型写像が存在するとき、G_1 と G_2 は同型であるという。

(iii)

$$\sigma\colon F_1 \longrightarrow F_2$$

を写像とする。σ が F_1 や F_2 の体構造と両立的である、つまり、

$$\sigma(0) \;=\; 0, \quad \sigma(1) \;=\; 1$$

及び、任意の $(x, y) \in F_1 \times F_1$ に対し、

$$\sigma(x+y) \;=\; \sigma(x)+\sigma(y), \quad \sigma(xy) \;=\; \sigma(x)\sigma(y)$$

の両方が成立するとき、σ を体の準同型写像という。さらに σ が全単射の時、σ を体の同型写像という。また、σ が体の同型写像かつ $F_1 = F_2$ のとき、特に σ を F_1 の自己同型写像という。

(iv) F_1 と F_2 の間に体の同型写像が存在するとき、F_1 と F_2 は同型であるという。

注意 1.5.1. 体の準同型写像は必ず単射になる。実際、二元 $a, b \in F_1$ に対し $\sigma(a) = \sigma(b)$ が成立する状況を考える。このとき、準同型写像の定義から $\sigma(a-b) = \sigma(a) - \sigma(b) = 0$ となる。$a - b \neq 0$ であれば、体の定義から、$c(a-b) = 1$ を満たす元 $c \in K$ が存在する。すると、準同型の定義から $1 = \sigma(1) = \sigma(c(a-b)) = \sigma(c)\sigma(a-b) = 0$ となり矛盾する。つまり、$a = b$ である。

定義 1.6. E を体とする。$1 \in E$ を有限回足しても $0 \in E$ と一致しないとき、E の標数を 0 と定義する。$1 \in E$ を有限回足して $0 \in E$ になるとき、その最小の回数を E の標数と定義する。体の t 定義からこの最小の回数は素数になる。

例 1.7. $\mathbb{Q}$ や $\mathbb{R}$ の標数は 0 である。また、有限体の標数は素数である。

定義 1.8.

(i) G を群とする。G の部分集合 H が G の部分群であるとは、
- H が G の単位元を含み、
- G 上の演算に関して H が閉じていて（つまり、$*(H \times H) \subseteq H$)、
- 任意の H の元の (G の演算に関する）逆元は H の元である

ことと定義する。G の部分群は G から誘導される (つまり、この場合単に定義域を制限することで得られる）演算とのペアを考えることで群になる。

(ii) E を体とする。E の部分集合 F が E の部分体であるとは、
- F は $(E, +_E)$ の部分群で（特に $0 \in F$)、

- $F \setminus \{0\}$ は $(E^\times, \times_E)$ の部分群である

ことと定義する。E の部分体は E から誘導される演算とのペアを考えることで体になる。また、F が E の部分体であるとき、E は F の拡大体であるという。

例 1.9.

(i) n を正の整数とする。$\mathbb{Z}$ の n の倍数全体からなる部分集合 $n\mathbb{Z} \subseteq \mathbb{Z}$ は部分群である。

(ii) G_1, G_2 を群とし、$\sigma\colon G_1 \to G_2$ を群の準同型写像とする。このとき、σ の核

$$\mathrm{Ker}(\sigma) \overset{\text{def}}{=} \{x \in G_1 \mid \sigma(x) = 1\}$$

(等式内の 1 は G_2 の単位元のこと）は G_1 の部分群である。正の整数 n に対し (n で割った余りを取ることで得られる）自然な全射準同型写像 $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$ の核は $n\mathbb{Z}$ である。

(iii) $\mathbb{Q}$ は $\mathbb{R}$ の部分体であり、$\mathbb{R}$ は $\mathbb{Q}$ の拡大体である。

(iv) K を体とする。不定元 (変数）を t とする K 係数の一変数多項式の集合を $K[t]$ と書く。つまり、

$$K[t] \overset{\text{def}}{=} \left\{ \sum_{0 \le i \le m} a_i t^i \mid a_i \in K, m \in \mathbb{N} \right\}$$

という意味である。$f(t) \in K[t]$ を既約多項式（つまり、定数でなく、$f(t) = g_1(t)g_2(t)$ なら $g_1(t)$ もしくは $g_2(t)$ が定数となるような多項式）とする。高校数学でも習うように、整数の場合と同様、多項式の世界にも割って余りを取るという操作が存在する。$K[t]$ の元を $f(t)$ で割った余りのなす集合を

$$K[t]/(f(t))$$

と書く。例 1.2, (ii) の場合と同様に、普通の多項式の和や積を考えてから $f(t)$ で割った余りを考える操作を考えれば、$K[t]/(f(t))$ は体になる。体になることを確認するには、既約多項式 $f(t)$ が素数のような性質（つまり、$f(t)$ が $h_1(t)h_2(t)$ を割るならば $h_1(t)$ か $h_2(t)$ の少なくともどちらか一方を割る）を示す必要がある。このことは（適切に多項式で割った余りを考える等で）多項式の次数に関する帰納法によって証明できる。そして、自然な包含

$$K \subseteq K[t]/(f(t))$$

は体の拡大である。t を $K[t]/(f(t))$ の元として考えれば、当たり前だが $f(t) = 0$ である。一方で、この当たり前な観察が何を意味しているかというと、既約多項式の根が存在するような拡大体が構成できるということである。本節で紹介する体論的な性質に関して、証明は行わないが、このような構成を利用しながら行うものが多いことを述べておく。

命題 1.10 (Lagrange)**.** G を有限群（有限個の元からなる群）とし、H を G の部分群とする。このとき、H の位数（元の数）は G の位数を割る。特に、G の位数を n と書けば、任意の G の元は n 乗すれば 1 になる。

Proof. 任意の G の元 g に対し、

$$gH \overset{\text{def}}{=} \{gh \mid h \in H\} \subseteq G$$

という元の数が H の位数に等しい G の部分集合を定義する。このとき、群や部分群の定義から有限個の G の元 $g_1, g_2, \cdots, g_m$ が存在して、G を非交和

$$G = \bigsqcup_{1 \leq i \leq m} g_i H$$

で書ける。このことから命題は直ちに従う。 □

定義 1.11. $F \subseteq E$ を体の拡大とする。このとき、E は F 上のベクトル空間とみなせるが、その次元を $[E : F]$ で表し、拡大の次数と呼ぶ。$[E : F]$ が有限であるとき $F \subseteq E$ を有限次拡大と呼ぶ。$[E : F]$ が有限でないとき、$F \subseteq E$ を無限次拡大と呼ぶ。E が F 上代数拡大であるとは、E の各元が F 上 (F 係数) のある多項式の根となっていることと定義する。

注意 1.11.1. 有限次拡大は代数拡大である。実際、$F \subseteq E$ が有限次拡大 ($n = [E : F]$) のとき、$x \in E$ に対し、$n + 1$ 個の元 $\{1, x, \ldots, x^n\}$ は F 上一次従属である。

例 1.12. 体拡大

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{-1}) \overset{\text{def}}{=} \{a + b\sqrt{-1} \mid a, b \in \mathbb{Q}\}$$

や

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \overset{\text{def}}{=} \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$$

はそれぞれ拡大次数 2, 3 の有限次拡大である。例 1.9, (iv) で紹介した体拡大

$$K \subseteq K[t]/(f(t))$$

の拡大次数は多項式 $f(t)$ の次数に一致する。また、$\mathbb{Q} \subseteq \mathbb{R}$ は代数拡大ではない。実際、自然対数の底 e や円周率 π 等様々な超越数 (有理数係数多項式の根にならない複素数）の存在が知られている。

定義 1.13. $F \subseteq E$ を体の拡大とする。このとき、

$$\mathrm{Aut}_F(E)$$

を体の同型写像 $\sigma : E \xrightarrow{\sim} E$ で、σ の F への制限が F の恒等写像になるものの集合とする。そして、$\mathrm{Aut}_F(E)$ の二元 σ, τ に対し合成写像 $\sigma \circ \tau$ を考えることで得られる二項演算によって、$\mathrm{Aut}_F(E)$ を群とみなす。

注意 1.13.1. 一般に有限次拡大 $F \subseteq E$ に対して、群 $\mathrm{Aut}_F(E)$ は有限群で、その位数（元の数）は拡大次数 $[E : F]$ 以下であることが証明できる。

注意 1.13.2. $F \subseteq E$ を代数拡大とする。$\mathrm{Aut}_F(E)$ はいわゆる対称性のなす群であるが、多項式の根の置換の概念と密接に関わっている。$x \in E$, $\sigma \in \mathrm{Aut}_F(E)$ を取る。$F \subseteq E$ は代数拡大なので、x はある F 上の多項式 $f(t) \in F[t]$ の根になっている。σ は F の元を動かさない準同型なので、

$$f(\sigma(x)) \ = \ \sigma(f(x)) \ = \ \sigma(0) \ = \ 0$$

である。つまり、$\sigma(x)$ はまた $f(t)$ の根である。このことは $\mathrm{Aut}_F(E)$ が多項式の根の置換を誘導することを示している。x の行先の候補が高々 $f(t)$ の次数個しかないことも示しており、基本的にはこの性質から注意 1.13.1 のような性質が証明できる。（実際に、例 1.9, (iv) で紹介したような有限次拡大 $K \subseteq K[t]/(f(t))$ に関しては、t の行き先で $\mathrm{Aut}_K(K[t]/(f(t)))$ の元が決まるため既に証明になっている。）

例 1.14.

(i) $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{-1}))$ の位数は 2 で、その生成元は $a + b\sqrt{-1}$ を $a - b\sqrt{-1}$ に移す全単射である。実際、$\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{-1}))$ に対し、体の準同型写像の定義から σ は $\sqrt{-1}$ の行先で決まることが分かる。そして、$\sigma(\sqrt{-1})^2 = \sigma(\sqrt{-1}^2) = \sigma(-1) = -1$ なので、$\sigma(\sqrt{-1})$ は $\sqrt{-1}$ もしくは $-\sqrt{-1}$ だと分かる。$\sigma(\sqrt{-1}) = -\sqrt{-1}$ のとき生成元となる。

(ii) $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}))$ の位数は 1、つまり、恒等写像のみからなる。実際、$\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}))$ に対し、(i) と同様の議論から、$\sigma(\sqrt[3]{2})$ は 3 乗すれば 2 になる $\mathbb{Q}(\sqrt[3]{2})$ の元である。$\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ なので、そのような元は $\sqrt[3]{2}$ のみである。そのため $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ が従い、準同型写像の定義から σ が恒等写像であることが分かる。

定義 1.15. E を体 F 上の有限次拡大体とする。拡大次数 $[E : F]$ と群 $\mathrm{Aut}_F(E)$ の位数が一致するとき、E は F の Galois 拡大であるという。つまり、注意 1.13.1 から対称性の最も大きい種類の拡大ということである。拡大 $F \subseteq E$ が Galois のとき、$\mathrm{Aut}_F(E)$ を $\mathrm{Gal}(E/F)$ と書く。

注意 1.15.1. E を体 F 上の有限次 Galois 拡大体とする。Galois 理論は F の拡大体で E の部分体となっているもの（中間体）たちと $\mathrm{Gal}(E/F)$ の部分群たちの間の 1 対 1 の対応関係を記述する理論である。5 次以上の方程式に対する (べき根を取る操作と四則演算だけを用いた）解の公式の非存在等が Galois 理論の応用として従う。

例 1.16. 例 1.14 から 2 次拡大 $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{-1})$ は Galois 拡大だが、3 次拡大 $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ は Galois 拡大でない。

定義 1.17. E を体 F 上の (有限次とは限らない）代数拡大体とする。E が F の有限次 Galois 拡大の和集合で書けるとき、E は F の Galois 拡大であるという。有限次の時と同様、拡大 $F \subseteq E$ が Galois のとき、$\mathrm{Aut}_F(E)$ を $\mathrm{Gal}(E/F)$ と書く。

注意 1.17.1. E を体 F 上の (有限次とは限らない）代数拡大体とする。任意の E の元の F 上の最小多項式 (その元を根に持つ 0 でない F 係数多項式の中で次数が最小のもの）が重根を持たな

いとき、E は F の分離拡大であるという。任意の E の元に対し、その F 上の最小多項式を E 上の多項式とみなしたとき 1 次式の積に分解するならば、E は F の正規拡大であるという。代数拡大が Galois 拡大であることと正規かつ分離拡大であることは同値であることが証明できる（多くの教科書では定義として採用されている）。

定義 1.18. F を体とする。定数でない F 係数の多項式が常に F に根を持つとき、F を代数閉体という。

例 1.19. 代数学の基本定理により複素数体 $\mathbb{C}$ は代数閉体である。

定義 1.20. $F \subseteq E$ を代数拡大とする。E が代数閉体ならば、E を F の代数閉包という。

非自明な事実として次のことが知られている。

命題 1.21.

(i) 任意の体に対し代数閉包が存在する。

(ii) F_1, F_2 を体、Ω_1, Ω_2 を F_1, F_2 の代数閉包とする。このとき、任意の体の同型写像 $f\colon F_1 \xrightarrow{\sim} F_2$ に対し、体の同型写像 $\Omega_1 \xrightarrow{\sim} \Omega_2$ でその F_1 への制限が f に一致するもの（延長）が存在する。特に、代数閉包は同型を除いて一意的である。（つまり、体の二つの代数閉包は必ず同型である。）

注意 1.21.1. F を体とする。定義から F の代数閉包は F の正規拡大である。

2 絶対 Galois 群

本節では、遠アーベル幾何学における中心的な概念の一つである絶対 Galois 群を紹介する。これは体ごとに (同型を除いて）定義される群である。

定義 2.1. F を体とし、$\overline{F}$ を F の代数閉包とする。$\overline{F}$ 内の F 上分離的な元（最小多項式が重根を持たない元）全体を

$$F^{\mathrm{sep}}$$

と書く。(少し議論が必要ではあるが）F^{sep} は $\overline{F}$ の部分体で、$F \subseteq F^{\mathrm{sep}}$ は Galois 拡大であることが証明できる。このとき、

$$G_F \overset{\mathrm{def}}{=} \mathrm{Gal}(F^{\mathrm{sep}}/F)$$

を F の絶対 Galois 群という。

注意 2.1.1. F の標数が 0 の場合、F 係数の n 次多項式の微分が $n-1$ 次多項式になるので、最小多項式の定義から $\overline{F}$ の任意の元は F 上分離的である。特に、$F^{\mathrm{sep}} = \overline{F}$。一方で F の標数が正

の場合、一般には $F^{\mathrm{sep}} \neq \overline{F}$ であるが、実は自然な写像

$$\mathrm{Aut}_F(\overline{F}) \longrightarrow G_F$$

は群の同型写像である。

注意 2.1.2. 有限次 Galois 拡大 $F \subseteq E$ ($\subseteq F^{\mathrm{sep}}$) に対し、その正規性 (cf. 注意 1.17.1) から自然な群準同型写像

$$G_F \longrightarrow \mathrm{Gal}(E/F)$$

が存在する。そして、体同型の延長に関する基本的な事実（cf. 命題 1.21, (ii)) から全射になる。F^{sep} は E の分離閉包でもあり、この全射の核は G_E である。通常 G_F は単なる群としてではなく、部分群 $G_E \subseteq G_F$ たち（E は F の F^{sep} 内の有限次 Galois 拡大を走る) が $1 \in G_F$ の近傍の開基となるような位相 (Krull 位相) を入れて、位相群として扱う。こうしないと、無限次拡大に関する Galois 理論が正しく機能しないためである。定義から G_F は有限群の逆極限で書くことができるが、そういったものは副有限群という特別な種類の位相群である。本稿内で “開部分群” や “閉部分群” 等の位相群関連の用語を用いることもあるが、位相群的なことをご存知ない場合は、何か特別な種類の部分群を考えているというような認識でいただければと思う。

注意 2.1.3. 絶対 Galois 群 G_F が有限群になる状況 (下の計算例 1, 2 参照) はあまり存在せず、有限であれば実はその位数は 2 以下になる。位数が 2 の場合、F が実閉体と呼ばれる実数体の親戚のような体になることが知られている。

注意 2.1.4. 絶対 Galois 群 G_F の定義は F のみではなく代数閉包 $\overline{F}$ の選択に依存している。一方で、異なる代数閉包を選んで定義しても、代数閉包が同型を除いて一意的であることによって、二つの絶対 Galois 群の間には代数閉包の間の体の同型写像から誘導される群の同型写像が存在する。またこの群の同型写像は構成から内部自己同型の合成を除いて一意的に定まるものである（cf. 命題 2.3)。そのため、G_F は内部自己同型を除いて一意的に定まると表現される。代数閉包の選択は、適切な位相空間に対し基本群を定義する際の基点の選択と全く同質のものである。これらを抽象化することにより、Galois 圏やスキームに対するエタール基本群の理論等が SGA1([3]) で展開された。実際に、G_F は F に付随するアフィンスキーム Spec F 及びその基点 $*\colon \mathrm{Spec}\ F^{\mathrm{sep}} \to \mathrm{Spec}\ F$ から定まるエタール基本群 $\pi_1(\mathrm{Spec}\ F, *)$ である。遠アーベル幾何学を本格的に勉強する場合は、まずこういったエタール基本群等の理論の習得をお勧めしたい。

さて、絶対 Galois 群の定義をしたもののその構造や性質を調べるのは一般には非常に難しい。まずは、そこまで苦労なく調べられる例を紹介したい。

<u>計算例 1</u> F が代数閉体のとき、$G_F = \{1\}$。このことは定義から直ちに分かる。

<u>計算例 2</u> $G_{\mathbb{R}}$ は位数 2 の巡回群。実際、複素数体 $\mathbb{C} = \{a + b\sqrt{-1} \mid a, b \in \mathbb{R}\}$ は代数閉体で $\mathbb{R}$ の 2 次 Galois 拡大である。特に、生成元は複素共役である。

計算例 3 F が有限体（つまり、有限位数の体) のとき、

$$G_F \xrightarrow{\sim} \widehat{\mathbb{Z}} \overset{\text{def}}{=} \varprojlim_n \mathbb{Z}/n\mathbb{Z} \subseteq \prod_n \mathbb{Z}/n\mathbb{Z}$$

が成立する (n は全ての正の整数を走る)。また、$\prod_n \mathbb{Z}/n\mathbb{Z}$ は単に n ごとに $\mathbb{Z}/n\mathbb{Z}$ の元を取って並べたもの $(a_n)_n$ からなる集合で、$\varprojlim_n \mathbb{Z}/n\mathbb{Z}$ はその内、任意の正の整数 m, n に対し、自然な全射 $\mathbb{Z}/mn\mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$ で a_{mn} が a_n に移るという条件が成立するものからなる集合である。これらには、$\mathbb{Z}/n\mathbb{Z}$ の群構造から誘導される（単に成分ごとに足し算を考える）群構造が自然に入る。

計算のため、有限体に関するいくつかの性質を確認する。

命題 2.2. p を素数とし、F を標数 p の有限体とする。定義から自然な単射準同型 $\mathbb{F}_p \hookrightarrow F$ が存在するが、これによって $\mathbb{F}_p$ とその F 内での像を同一視する。このとき、次が成立する。

(i) $\mathbb{F}_p \subseteq F$ は有限次拡大である。また、F を含む $\mathbb{F}_p$ の代数閉包 $\overline{\mathbb{F}}_p$ を固定し、$n = [F : \mathbb{F}_p]$ と書けば、$F = \{x \in \overline{\mathbb{F}}_p \mid x^{p^n} = x\}$。

(ii) p 乗写像 $\phi_p \colon F \to F$ $(x \mapsto x^p)$ は体の同型写像。

(iii) $\mathbb{F}_p \subseteq F$ は有限次 Galois 拡大で、$\mathrm{Gal}(F/\mathbb{F}_p)$ は ϕ_p で生成される位数 $n = [F : \mathbb{F}_p]$ の巡回群。特に、ϕ_p を 1 に移す対応は同型写像 $\mathrm{Gal}(F/\mathbb{F}_p) \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z}$ を誘導する。

Proof. (i): F の位数が有限なので、$\mathbb{F}_p \subseteq F$ が有限次拡大であることは直ちに従う。また、F は $\mathbb{F}_p$ 上 n 次元のベクトル空間なので、その位数は p^n である。特に F の乗法群 $F^\times$ の位数が $p^n - 1$ なので、命題 1.10 を適用することで、任意の $x \in F^\times$ に対し、$x^{p^n-1} = 1$ が成立する。特に、$F \subseteq \{x \in \overline{\mathbb{F}}_p \mid x^{p^n} = x\}$。一方で、$F$ の位数が p^n かつ次数 p^n の多項式のある体内での根の数は p^n 以下であることから、この包含は等号となる。

(ii): ϕ_p が積構造を保つこと（つまり、$\phi_p(xy) = \phi_p(x)\phi_p(y)$) は直ちに従う。$\phi_p$ が加法構造を保つこと（つまり、$\phi_p(x+y) = \phi_p(x) + \phi_p(y)$) は二項定理と F 内では $p = 0$（F の標数は p) であることから従う。よって、ϕ_p は体の準同型写像であり、注意 1.5.1 から自動的に単射である。F は有限個の元からなるので、単射性は全射であることも意味する。

(iii): (i) と (ii) から $\phi_p \in \mathrm{Aut}_{\mathbb{F}_p}(F)$ かつ ϕ_p^n は恒等写像。また、n より小さい正の整数 m に対し、ϕ_p^m は恒等写像にならない。（もしなれば、F の任意の元が p^m $(< p^n)$ 次の多項式 $X^{p^m} - X$ の根になってしまい、F の位数が p^n であることに矛盾する。）これらの観察から $\mathrm{Aut}_{\mathbb{F}_p}(F)$ は ϕ_p で生成される位数 n の巡回群を部分群として含む。一方で、注意 1.13.1 により $\mathrm{Aut}_{\mathbb{F}_p}(F)$ の位数は $n = [F : \mathbb{F}_p]$ 以下なので、証明が完了する。 □

代数拡大の定義から $\overline{\mathbb{F}}_p$ は $\mathbb{F}_p$ の ($\overline{\mathbb{F}}_p$ 内の）有限次拡大体の和集合なので、上の命題の (i) から

$$\overline{\mathbb{F}}_p = \bigcup_n \mathbb{F}_{p^n} \overset{\text{def}}{=} \{x \in \overline{\mathbb{F}}_p \mid x^{p^n} = x\}$$

である。（ただし、n は全ての正の整数を走る。）この観察と上の命題の (iii) から、

$$G_{\mathbb{F}_p} \xrightarrow{\sim} \varprojlim_n \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \xrightarrow{\sim} \varprojlim_n \mathbb{Z}/n\mathbb{Z}$$

が従う。(最初の同型写像は注意 2.1.2 内で述べられている、「有限群の逆極限で書くことができる」という部分に相当するものである。特に非自明な内容を含むものではないが、本稿では説明を省略する。講義ではもう少し説明を加える予定である。）G_F は自然な合成 (全射準同型写像)

$$\widehat{\mathbb{Z}} \xleftarrow{\sim} G_{\mathbb{F}_p} \twoheadrightarrow \mathrm{Gal}(F/\mathbb{F}_p) \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z}$$

の核と同型なので、それはまた $\widehat{\mathbb{Z}}$ と同型である。(演習問題)

計算例 3 によると、有限体の絶対 Galois 群はどれも同型であり体構造の情報などは一切保持していない (それどころか有限体の位数の情報すら保持していない）ことが分かる。

いくつかの計算を行ったが、最も基本的な体である有理数体 $\mathbb{Q}$ の絶対 Galois 群 $G_{\mathbb{Q}}$ を考えたくなる。一方で、$G_{\mathbb{Q}}$ は非常に重要かつ難しい対象で、この群の構造や（表現/外表現等の）性質を理解することは現代数論の目標の 1 つである。本稿で紹介する Neukirch-内田の定理は、一言で述べれば、数体（$\mathbb{Q}$ の有限次拡大体）の体構造はその絶対 Galois 群の群構造から決まってしまうというものである。特に、実質的に異なる二種類の演算を復元できてしまうほどに複雑な対象であることを示している。また、$G_{\mathbb{Q}}$ に関する有名な未解決問題の内、遠アーベル幾何学に深く関連するものを一つ挙げると、$G_{\mathbb{Q}}$ と Grothendieck-Teichmüller 群と呼ばれる組み合わせ論的に定義される群 GT の比較がある。

$$\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0, 1, \infty\}$$

($\overline{\mathbb{Q}}$ 上の射影直線引く 3 点 0, 1, ∞) というある非常に豊かな対称性を持つ幾何学的な対象のエタール基本群への $G_{\mathbb{Q}}$ の外作用を考えることで、

$$G_{\mathbb{Q}} \subseteq \mathrm{GT}$$

となることが示されているが、これらの群が一致するか否かという問題である。この問題についてはこれまで様々な観点から様々な研究がなされているが、組み合わせ論的遠アーベル幾何学という遠アーベル幾何学の一分野の進展に伴い最近でもいくつかの非自明な結果 ([7] 等) が得られている。説明は省略するが他にも $G_{\mathbb{Q}}$ 及びその閉部分群に関して、

- Galois の逆問題 — 任意の有限群は $G_{\mathbb{Q}}$ の (開正規部分群による）商として現れるか?
- Shafarevich 予想 — $\mathbb{Q}$ 上全ての 1 の冪根で生成される体の絶対 Galois 群は副有限群論的に自由か?

等様々な有名な未解決問題が存在する。

本節の最後に絶対 Galois 群を取る操作の関手性について説明する。

命題 2.3. F_1, F_2 を体、

$$\sigma\colon F_1 \hookrightarrow F_2$$

を体の準同型とする（注意 *1.5.1* から自動的に単射になる)。このとき、σ は G_{F_1} の内部自己同型の合成による差を除き群の準同型写像

$$G_{F_2} \longrightarrow G_{F_1}$$

を誘導する。

Proof. $\Omega_1 \subseteq F_2^{\mathrm{sep}}$ を $\sigma(F_1)$ 上代数的かつ分離的な F_2^{sep} の元全体からなる部分体とする。Ω_1 は $\sigma(F_1)$ の分離閉包になっていることに注意する。すると、定義から自然な準同型写像

$$G_{F_2} \longrightarrow G_{\sigma(F_1)} \overset{\mathrm{def}}{=} \mathrm{Gal}(\Omega_1/\sigma(F_1))$$

が存在する。また、命題 1.21 と分離的な元の定義から σ から誘導される体の同型写像 $F_1 \xrightarrow{\sim} \sigma(F_1)$ は延長 $\tilde{\sigma}\colon F_1^{\mathrm{sep}} \xrightarrow{\sim} \Omega_1$ を持つ。任意の $\tau \in G_{\sigma(F_1)}$ に対し、$\tilde{\sigma}^{-1} \circ \tau \circ \tilde{\sigma} \in G_{F_1}$ を与える対応によって群の同型写像

$$G_{\sigma(F_1)} \xrightarrow{\sim} G_{F_1}$$

を得る。構成は延長 $\tilde{\sigma}$ の取り方に依存しており、延長を取り換えれば、ある G_{F_1} の内部自己同型の分だけ差が生まれる（演習問題）。上の二つのディスプレイ内の準同型写像を合成することで G_{F_1} の内部自己同型の合成による差を除き準同型写像

$$G_{F_2} \longrightarrow G_{F_1}$$

を得る。 □

3 Kummer 理論

本節では、遠アーベル幾何学において乗法構造を復元する際にしばしば利用される Kummer 理論に関して簡単に説明を行う。§1 の有限体の場合のように乗法構造すら復元できない場合も多数存在するという事実から推測できる通り、実際には Kummer 理論を適用するだけで復元できるというような単純なものではない。一方で、Kummer 理論を眺めるだけでも、絶対 Galois 群の群構造と体の乗法群の群構造が関連する様子がある程度認識できる。

F を体とし、n を F の標数と互いに素な正の整数とする。$F^\times$ の任意の元 f に対し、その n 乗根は代数閉包の定義から $\overline{F}$ 内に存在する。さらに、n が F の標数と互いに素であることによって、そのような n 乗根たちは F^{sep} の元であることも確認できる。実際、$X^n - f$ が重根を持たないことを確認するには $X^n - f$ とその微分 nX^{n-1} が共通の根を持たないことを確認すればよいが、$n \neq 0$ という仮定から直ちに従う。f の n 乗根 $f^{\frac{1}{n}} \in F^{\mathrm{sep}}$ を選び、絶対 Galois 群 G_F の元 σ に対し、次のような対応

$$f \mapsto \frac{\sigma(f^{\frac{1}{n}})}{f^{\frac{1}{n}}} \in \mu_n(F^{\mathrm{sep}}) \overset{\mathrm{def}}{=} \{x \in F^{\mathrm{sep}} \mid x^n = 1\}$$

を考える。$\frac{\sigma(f^{\frac{1}{n}})}{f^{\frac{1}{n}}}$ が 1 の n 乗根であることは、等式 $\sigma(f^{\frac{1}{n}})^n = \sigma((f^{\frac{1}{n}})^n) = \sigma(f) = f = (f^{\frac{1}{n}})^n$ から従う。そしてこの対応は、乗法群 $F^\times$ から G_F と $\mu_n(F^{\mathrm{sep}})$ から定まるある群への群準同型写像

$$\kappa_F\colon F^\times \longrightarrow H^1(G_F, \mu_n(F^{\mathrm{sep}}))$$

を定める。(定義等は説明しないが、$H^1(G_F, \mu_n(F^{\mathrm{sep}}))$ は 1 次群コホモロジーと呼ばれる群で、$\mu_n(F^{\mathrm{sep}}) \subseteq F$ の場合には、単に副有限群 G_F から離散群 $\mu_n(F^{\mathrm{sep}})$ への連続準同型たちのなす群である。)　非自明な事実ではあるが、κ_F は全射でその核は $F^\times$ の n 乗元の成す群 $(F^\times)^n$ に一致することが知られている。特に、κ_F は同型

$$F^\times/(F^\times)^n \ \xrightarrow{\sim}\ H^1(G_F, \mu_n(F^{\mathrm{sep}}))$$

を誘導する。このことは 1 の冪根からなる群さえ復元できれば乗法群に近いものが構成できることを示している。遠アーベル幾何学では円分物を復元・管理することが非常に重要であるが、ここにその理由の一部が現れている。ただし、

- 1 の冪根からなる群の復元は多くの場合非自明で、有限体の場合は不可能なことが分かる。（有限体の場合は体の位数すら復元できない。）
- 1 の冪根からなる群の復元は、可能な場合でも $\mu_n(F^{\mathrm{sep}})$ そのものではなく、$\mu_n(F^{\mathrm{sep}})$ の同型物である。そのため遠アーベル幾何学では、これらを区別しその間の同型を管理する理論を展開する。（円分同期化の理論、及びそれを用いた Kummer 同型の構成。）
- 1 の冪根からなる群が復元できても構成できるのは、$\varprojlim_n F^\times/(F^\times)^n$ という群（の同型物）であって、一般には $F^\times$ とは大きく異なる。例えば、代数閉体の乗法群のように可除性の高い（冪乗の像が大きい）群だと非常に小さくなるし、有理数体の乗法群のように離散性の高い (整数のなす加法群 $\mathbb{Z}$ への全射をたくさん持つような）群だと非常に大きくなる。もちろん、大きくなる分には更なる議論で復元可能な余地があるが、あまりに小さくなってしまうと復元するのはほとんど不可能である。

本稿では説明しないが、実際に [11], §1（や [7]) ではこのような Kummer 理論的アプローチから非自明な遠アーベル幾何学的帰結を導いている。

4　局所体と大域体

本節では、数論的に重要なクラスの体である局所体や大域体を紹介する (詳しくは [9] や [13] 等をご参照ください)。既に登場している実数体 $\mathbb{R}$ や複素数体 $\mathbb{C}$ は局所体の、有理数体 $\mathbb{Q}$ は大域体の例である。局所体とは簡単に述べてしまえば、適切な意味での “距離”の概念が備わった体で、その距離に関して局所コンパクトなもののことである。後に説明するが、有理数体のような体は様々な種類の “距離”を備えており、それらに関する完備化という局所体を構成する操作が存在する。数論幾何学にはこういった距離たちのなす “集合/空間”を考える視点が存在し、そのような視点から有理数体のような体は大域的で、空間の “点”（つまり、一つの距離）に付随する体は局所的と呼ばれる。

定義 4.1. F を体とする。F 上の（階数 1 の乗法的）付値とは、写像

$$|\cdot|\colon F \longrightarrow \mathbb{R}_{\geq 0}$$

で次の三条件を満たすもののことである。

(i) $x \in F$ に対し、$x = 0$ であることと $|x| = 0$ であることは同値。
(ii) $|\cdot|$ は積と両立的。つまり、任意の $(x, y) \in F \times F$ に対し、$|xy| = |x||y|$ が成立。
(iii) $|\cdot|$ は三角不等式を満たす。つまり、任意の $(x, y) \in F \times F$ に対し、$|x + y| \leq |x| + |y|$ が成立。

F 上の二つの付値 $|\cdot|_1, |\cdot|_2$ が同値であるとは、ある正の実数が存在して $|\cdot|_1 = |\cdot|_2^s$ となることと定義する。

$\mathbb{Q}$ や $\mathbb{R}$ や $\mathbb{C}$ に対し通常の絶対値を考えると、上の性質を満たすのでそれぞれの体上の付値であることが確認できる。任意の体に対し、0 を 0 に 0 以外の元を 1 に送る写像を考えても付値になる。これは自明な付値と呼ばれる。

体 F 上に付値が与えられると、二元 x, y の間の距離をその差の付値 $|x - y|$ で定義することで F を距離空間とみなせる。定義 4.1 内の付値の同値性に関する条件は、距離空間としての位相が一致するという条件と同値になる。実はこの距離に関して、$\mathbb{Q}$ の通常の絶対値と $\mathbb{R}$ や $\mathbb{C}$ の通常の絶対値には Cauchy(コーシー) 列の収束性（完備性）に関する大きな違いが存在する。Cauchy 列とは無限列 $\{a_n\}_{n\in\mathbb{N}}$ で、任意の $\epsilon > 0$ に対し、ある $N \in \mathbb{N}$ が存在して、N より大きい任意の整数 m, n に対し、$|a_m - a_n| < \epsilon$ となるようなもののことであった。付値体（付値の備わった体）が完備であるとは、付随する距離に関してどんな Cauchy 列も収束するということである。完備かどうかは感覚的には「$\sqrt{2}$ は $\mathbb{Q}$ の元でいくらでも近似できるが $\mathbb{Q}$ の元ではない」といった現象が起きるか起きないかという違いである。そして、通常の絶対値に関して $\mathbb{Q}$ は完備でないが $\mathbb{R}$ や $\mathbb{C}$ は完備である。

定義 4.2. 非自明な付値を備えた付値体で、その距離空間としての位相が局所コンパクト（本稿では説明しないが、ある種の有限性に関する位相的性質）なものを局所体という。

ちょっとした位相に関する議論で局所体が完備になることが証明できる。$\mathbb{Q}$（に通常の絶対値を考えたもの）は完備ではないので局所体ではない。また、局所コンパクトの定義を知っていれば、$\mathbb{R}$ や $\mathbb{C}$（に通常の絶対値を考えたもの）が局所体であることは簡単に確認できる。

ところで、$\mathbb{Q}$ や $\mathbb{R}$ や $\mathbb{C}$ の通常の絶対値は、当たり前だが $\{|n| \mid n \in \mathbb{Z}\}$ という集合が有界でない（つまり、アルキメデス的）という性質を持っている。本節で次に紹介したいのは、$\mathbb{Q}$ には素数 p ごとに非アルキメデス的な付値 (p 進付値)

$$|\cdot|_p \colon \mathbb{Q} \longrightarrow \mathbb{R}_{\geq 0}$$

が定まることである。任意の $x \in \mathbb{Q}^\times$ に対し、一意的に定まる整数 m_x と p と互いに素な整数 a, b が存在して、$x = p^{m_x} \cdot \frac{b}{a}$ と書けることは簡単に確認できる。そして、

$$|0|_p \overset{\text{def}}{=} 0, \quad |x|_p \overset{\text{def}}{=} \frac{1}{p^{m_x}} \ (x \neq 0)$$

で写像 $|\cdot|_p$ を定義するとこれが付値であることが分かる。三角不等式に関しては強三角不等式と

呼ばれるより条件の強い不等式 $|x+y|_p \leq \max\{|x|_p, |y|_p\}$ が成立することも分かる。また、任意の整数 n に対し $|n|_p \leq 1$ が成立し、$\{|n| \mid n \in \mathbb{Z}\}$ が有界である。そのため、$|\cdot|_p$ は非アルキメデス的と呼ばれる。

これまで $\mathbb{Q}$ 上には通常の絶対値や p 進付値のような付値が存在することが分かったが、実は $\mathbb{Q}$ 上の任意の非自明な付値はこれらと同値であることが Ostrowski により証明されている。そのため、$\mathbb{Q}$ 上の付値の同値類の集合は素数の集合と通常の絶対値に対応する元からなる集合の和集合である。

続いて、完備化という付値体から完備な付値体を構成する操作を紹介したい。これによって、有理数体のような大域的な体から付値ごとに局所体を構成することが可能になる。（大域的な対象の研究を直接行うことは難しいので、現代の数論幾何ではそこから構成される局所的な対象をまず詳細に研究した後に、それを用いて大域的な対象に挑むという戦略が取られることが多い。）

定義 4.3. F を付値体とする。

$$\widehat{F}$$

を F の Cauchy 列の同値類で定義する。ただし、二つの Cauchy 列 $\{a_n\}_{n\in\mathbb{N}}, \{b_n\}_{n\in\mathbb{N}}$ が同値であるとは、任意の $\epsilon > 0$ に対し、ある正の整数 N が存在して、任意の $n > N$ に対し、$|a_n - b_n| < \epsilon$ となることで定義する。そして、$\widehat{F}$ 上の体構造を F から自然に誘導されるもので定義する。つまり、$\widehat{F}$ の二つの元に対し、それらの代表元 $\{f_n\}_{n\in\mathbb{N}}, \{g_n\}_{n\in\mathbb{N}}$ を取って、和や積を Cauchy 列 $\{f_n + g_n\}_{n\in\mathbb{N}}, \{f_n g_n\}_{n\in\mathbb{N}}$ の同値類で定義するというだけである。この定義が well-defined つまり、代表元の取り方に依らないことは三角不等式から直ちに従う。（演習問題）

さて、$\mathbb{R}$ の一つの構成の仕方は $\mathbb{Q}$ の通常の絶対値に関する完備化であった。この完備化を通常の絶対値ではなく、p 進付値 $|\cdot|_p$ に関して行えば全く別の体

$$\mathbb{Q}_p$$

が得られる。この体のことを p 進数体と呼ぶ。$\mathbb{Q}_p$ の元は形式的には

$$\sum_{i\geq m} a_i \cdot p^i \quad (a_i \in \{0, 1, \cdots, p-1\})$$

(m は整数）という無限和の形で書けるので、p 進数感が感じられるのではないだろうか。また、少し議論が必要ではあるが、$\mathbb{Q}_p$ の付値を $\mathbb{Q}_p$ の任意の有限次拡大体に自然に延長できて、その付値に関して完備で局所体であることが証明できる。このような体たちのことを p 進局所体という。

これまで紹介してきた局所体は全て標数 0 であったが、有限体上の一変数冪級数体といった正標数の局所体も存在する。大変非自明ではあるが、局所体は $\mathbb{R}$, $\mathbb{C}$, p 進局所体, 有限体上の一変数冪級数体のいずれかと同型であることが証明できる。

次に、大域体を紹介したい。体 F 上の一変数有理関数体

$$F(T)$$

とは、F 係数多項式 $f(T), g(T) \neq 0$ が存在して、$\frac{f(T)}{g(T)}$ と書けるような関数 (有理関数）たちのなす体のことである。そして、

定義 4.4. 大域体とは、$\mathbb{Q}$ の有限次拡大体または $\mathbb{F}_p$ 上の一変数有理関数体の有限次拡大体のことである。また、$\mathbb{Q}$ の有限次拡大体のことを数体という。特に、局所体とは大域体の付値による完備化から生じる体とも言い換えられる。

最後に、局所体や大域体に対する非常に深い理論である類体論をごく一部ではあるが紹介したい。類体論ではアーベル拡大と呼ばれる Galois 群が可換/アーベル群となるような特別な種類の Galois 拡大を扱う。類体論とは一言で述べれば、ある意味では体の外側の情報であるアーベル拡大の様子を体の乗法群的なデータの部分群たち（特に、内側の情報）で記述する理論である。このような理論はどのような体にも存在するものではなく、局所体や大域体のような数論的に特別な体にのみ存在するものである。遠アーベル幾何学の観点からは、類体論は局所体や大域体の乗法構造の復元において重要なものである。

まず、一般の有限次 Galois 拡大に対するノルムの概念を定義したい。(本当は Galois 性の仮定を必要とする概念ではない。)

定義 4.5. F を体、$F \subseteq E$ を有限次 Galois 拡大とする。任意の $x \in E^\times$ に対し、そのノルム $N_{E/F}(x) \in F^\times$ を x の F 上の共役の積

$$N_{E/F}(x) \overset{\text{def}}{=} \prod_{\sigma \in \mathrm{Gal}(E/F)} \sigma(x)$$

で定義する。ノルムの定義からどのような $\mathrm{Gal}(E/F)$ の元を作用させても不変なので、Galois 理論を適用することで $N_{E/F}(x)$ は F の元であることが確認できる。ノルムを取る操作が群準同型写像

$$N_{E/F} \colon E^\times \longrightarrow F^\times$$

を誘導することは簡単に確認できる。

例 4.6. $N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(a + b\sqrt{-1}) = (a + b\sqrt{-1})(a - b\sqrt{-1}) = a^2 + b^2.$

次に、体のアーベル拡大たちの親玉ともみなせる最大アーベル拡大の概念を定義する。

定義 4.7. F を体とし、F の代数閉包 $\overline{F}$ を固定する。このとき、F の最大アーベル拡大体

$$F^{\mathrm{ab}}$$

を F の $\overline{F}$ 内の有限次アーベル拡大体全ての和集合で定義する。（少し議論が必要だが、F^{ab} が実際に F のアーベル拡大体であることは確認できる。）また、絶対 Galois 群 G_F の元は F^{ab} の自己同型写像を誘導するので、命題 1.21, (ii) を適用すれば

$$G_F^{\mathrm{ab}} \overset{\text{def}}{=} \mathrm{Gal}(F^{\mathrm{ab}}/F)$$

を G_F の自然な商とみなすことができる。（本当は、G_F^{ab} は G_F の副有限群的最大アーベル商として副有限群論的に自然に構成できる。）

$\mathbb{R}$ や $\mathbb{F}_p$ の場合は、§2 の計算例 2, 3 によって、その代数閉包が最大アーベル拡大に一致することが分かる。さらに、代数閉包は 1 の冪根を全て添加して得られる体なので、最大アーベル拡大の構成までもが簡単に分かる体である。一方で、非アルキメデス的局所体や大域体の場合はこれらの例と違い、G_F^{ab} や F^{ab} のことについて理解することがはるかに難しい。(数体に関しては、F^{ab} をどのように構成するのかについて非常に特別な場合を除いてまだ知られていない。) この G_F^{ab}（つまり、アーベル拡大の様子）について、類体論の内容の一部を述べる。

まず、局所体に対する類体論である局所類体論は次の通りである。

定理 4.8. F を局所体とする。このとき、相互写像と呼ばれる群準同型写像

$$r_F \colon F^\times \longrightarrow G_F^{\mathrm{ab}}$$

が存在して、次が成立する。

(i) 任意の有限次アーベル拡大 $F \subseteq E$ に対し、r_F と自然な商 $G_F^{\mathrm{ab}} \twoheadrightarrow \mathrm{Gal}(E/F)$ の合成は全射で、その核はノルム写像 $N_{E/F}$ の像に一致する。つまり、r_F は群の同型写像

$$F^\times/\mathrm{Im}(N_{E/F}) \ \xrightarrow{\sim}\ \mathrm{Gal}(E/F)$$

を誘導する。

(ii) r_F による逆像を取るという操作は、全単射

$$\{F \text{ の有限次アーベル拡大}\} \overset{\text{Galois 理論}}{=} \{G_F^{\mathrm{ab}} \text{の開部分群}\} \ \xrightarrow{\sim}\ \{F^\times \text{の指数有限開部分群}\}$$

を誘導する。

注意 4.8.1. F が非アルキメデス的局所体のとき r_F は単射になるが、アルキメデス的局所体のときは単射にならない。

注意 4.8.2. $\mathbb{R}$ や $\mathbb{C}$ のとき、有限次アーベル拡大は自明な拡大（1 次拡大) か $\mathbb{R} \subseteq \mathbb{C}$ しか存在しないので、上で何が行われているかの確認が容易である。

次に、大域体に対する類体論である大域類体論だが、局所類体論での体の乗法群の役割は、大域体の乗法群ではなくイデール類群という別の対象によって果たされる。これは大域体から発生する局所体の乗法群たちの積の適切な部分商だが、その定義のために体 F に対し、F 上の付値の同値類の集合を

$$\mathbb{V}(F)$$

と書くことにする。

定義 4.9. F を大域体とする。$v \in \mathbb{V}(F)$ に対し、F の v での完備化を F_v と書く。（F_v は局所体である。）このとき、F のイデール群

$$I_F \overset{\text{def}}{=} \prod_{v \in \mathbb{V}(F)}{}' F_v^\times \ \subseteq \ \prod_{v \in \mathbb{V}(F)} F_v^\times$$

を $F_v^\times$ たちの直積群の部分群で有限個の成分を除いて付値が 1 になるような元からなるものとする。また、自然な群準同型写像

$$F^\times \longrightarrow \prod_{v\in\mathbb{V}(F)} F_v^\times, \quad x \mapsto (x, x, \dots)$$

の像が I_F に入ることは簡単に確認できる。(慣れない方は $\mathbb{Q}$ の場合にでも考えていただければと思います。）そして、F のイデール類群

$$C_F$$

を I_F の $F^\times$ の像による商で定義する。

また、体の乗法群のときと同様にイデール類群に対してもノルム写像が定義できる。つまり、任意の有限次 Galois 拡大 $F \subseteq E$ に対し、ノルム写像

$$N_{C_E/C_F} : C_E \longrightarrow C_F$$

を共役元の積を取るという操作から誘導される準同型で定義する。イデール類群に入る位相については説明しないが、これらの記号の準備の下で大域類体論は次の通りである。

定理 4.10. F を大域体とする。このとき、相互写像と呼ばれる群準同型写像

$$r_F \colon C_F \longrightarrow G_F^{\mathrm{ab}}$$

が存在して、次が成立する。

(i) 任意の有限次アーベル拡大 $F \subseteq E$ に対し、r_F と自然な商 $G_F^{\mathrm{ab}} \twoheadrightarrow \mathrm{Gal}(E/F)$ の合成は全射で、その核はノルム写像 N_{C_E/C_F} の像に一致する。つまり、r_F は同型

$$C_F/\mathrm{Im}(N_{C_E/C_F}) \xrightarrow{\sim} \mathrm{Gal}(E/F)$$

を誘導する。

(ii) r_F による逆像を取るという操作は、全単射

$$\{F \text{ の有限次アーベル拡大}\} \overset{\text{Galois 理論}}{=} \{G_F^{\mathrm{ab}} \text{の開部分群}\} \xrightarrow{\sim} \{C_F \text{の指数有限開部分群}\}$$

を誘導する。

(iii) 任意の $v \in \mathbb{V}(F)$ に対し、r_{F_v} と r_F は両立的である。つまり、r_{F_v}, r_F と自然な準同型からなる図式

$$\begin{array}{ccc} F_v^\times & \xrightarrow{r_{F_v}} & G_{F_v}^{\mathrm{ab}} \\ \downarrow & & \downarrow \\ C_F & \xrightarrow{r_F} & G_F^{\mathrm{ab}} \end{array}$$

は可換である。ただし、右の縦の準同型は自然な体の準同型 $F \hookrightarrow F_v$ から誘導されるものである（アーベル商を考えているので内部自己同型による不定性は発生しないことに注意する)。

注意 4.10.1. F が正標数大域体のときは r_F は単射になるが、数体のときは単射にならない。

5 非アルキメデス的局所体や大域体に関連する復元定理の紹介

本節では、前節で紹介した非アルキメデス的局所体や大域体に対し、遠アーベル幾何学でどのようなことが知られているかについてその一部を紹介する。遠アーベル幾何学で考察する問題は、

体の情報の内どのような情報がその絶対 Galois 群の群構造から復元できるか

である。復元という言葉に関してその本来の言葉の意味を尊重するならば、望月新一氏による最近の単遠アーベル幾何学的観点（つまり、群論的な言葉で記述可能なアルゴリズムによって元の対象（の同型物）を構成する）を採用するのが理想的だが、入門的ノートの性質上、本稿では主張の理解しやすい双遠アーベル的観点を採用する。つまり、二つの体 F_1, F_2 に対し、その絶対 Galois 群の間の同型 $G_{F_1} \xrightarrow{\sim} G_{F_2}$ は F_1 や F_2 のどのような情報を保存するかという問題を考えることにし、保存されるとき復元されると表現することにする。その性質上、単遠アーベル幾何学的復元アルゴリズムを構成できれば、対応する双遠アーベル幾何学的問題は系として直ちに解決される。

さて、この復元問題に関して非アルキメデス的局所体と大域体で状況は大きく異なる。簡単に要約すれば、非アルキメデス的局所体では乗法群構造は復元できるが体構造までは復元できない一方で、大域体では体構造が完全に復元できることが知られている。より具体的な形で主張を述べると次の通りである。

命題 5.1. F_1, F_2 を非アルキメデス的局所体とし、

$$\sigma\colon G_{F_1} \xrightarrow{\sim} G_{F_2}$$

をその絶対 Galois 群の間の同型写像とする。そして、

$$\sigma^{\mathrm{ab}}\colon G_{F_1}^{\mathrm{ab}} \xrightarrow{\sim} G_{F_2}^{\mathrm{ab}}$$

を σ から自然に誘導される同型とする（定義 *4.7* 内の最後の部分を参照）。このとき、σ^{ab} は相互写像 $r_{F_1}\colon F_1^\times \hookrightarrow G_{F_1}^{\mathrm{ab}}$, $r_{F_2}\colon F_2^\times \hookrightarrow G_{F_2}^{\mathrm{ab}}$ の像たちの間に同型を誘導する。特に、σ は乗法群の間の同型

$$F_1^\times \xrightarrow{\sim} F_2^\times$$

を誘導する。

定理 5.2 (山形, Jarden-Ritter — cf. [18], [8])**.** 「体としては同型でないが、その絶対 Galois 群は同型である」ような p 進局所体 F_1, F_2 が存在する。特に、このような F_1, F_2 に対して、命題 *5.1* で構成された乗法群の間の同型写像は加法構造と両立的ではない。

定理 5.3 (Neukirch-内田 — cf. [14], [16], [17])**.** F_1, F_2 を大域体とし、

$$\sigma\colon G_{F_1} \xrightarrow{\sim} G_{F_2}$$

をその絶対 Galois 群の間の（副有限群としての）同型写像とする。このとき、σ は内部自己同型の合成による差を除いて、一意的な体同型写像

$$F_2 \xrightarrow{\sim} F_1$$

から生じる *(cf.* 命題 *2.3)*。

命題 5.1 によって、p 進局所体の絶対 Galois 群の群構造から体の乗法構造を復元できる。読者の中には最初から最大アーベル商の間の同型写像を考えたらどうか（つまり、σ^{ab} から出発したらどうか）という自然な疑問を持つ方もいるかもしれない。実は p 進局所体の乗法群の構造についてある程度理解していれば、それは $\widehat{\mathbb{Z}}$ 内で $\mathbb{Z}$ を特徴付けられるかという問題と同値であることが分かる。これは $\mathbb{Z}$ と $\widehat{\mathbb{Z}}$ の自己同型群のサイズが（大きく）異なることによって不可能である。命題 5.1 のレベルであれば深い結果という訳ではないが、$\widehat{\mathbb{Z}}$ のような副有限群の中で $\mathbb{Z}$ のような離散的な群を特徴づけるために非アーベル的な構造が使われるところは興味深い。一方で定理 5.2 は、p 進局所体の絶対 Galois 群の群構造からの体構造の復元問題に対する反例を与えている。非常に非自明な事実ではあるが、p 進局所体の絶対 Galois 群の群構造は（ごく例外的な場合を除けば）Jannsen-Wingberg により決定されており (cf. e.g., [14], Theorem 7.5.14)、反例の構成はそういった構造の決定（本当はそれより弱く、構造を決定する数値的データ）の研究に依存している。

また、正標数局所体の場合はその体としての同型類が係数体/剰余体によって完全に決まってしまうことにより、定理 5.2 の前半のような主張が成立しない。つまり、絶対 Galois 群が同型であれば（本当はより強くその最大アーベル商が同型であるというだけでも）体としても同型になる。しかし、局所類体論から誘導される命題 5.1 のような乗法群の間の同型写像は加法構造と両立的であるとは限らない。そのため、同じ非アルキメデス的局所体でありながら p 進局所体と正標数局所体では状況が少し異なる。

定理 5.3 は Neukirch-内田の定理として知られる大域体に対する体構造の復元定理で、遠アーベル幾何学では最も基礎的な定理の一つである。$F_1 = F_2 = \mathbb{Q}$ の場合でも大変非自明な事実であり、$\mathbb{Q}$ の自己同型写像が恒等写像しかないので、「$G_{\mathbb{Q}}$ の自己同型写像は自動的に内部自己同型になる」という主張と同値である。$G_{\mathbb{Q}}$ の元で具体的に書けるものは自明な元か複素共役ぐらいしか見当たらないことに注意すれば、この事実の非自明さを理解していただけるのではないだろうか。

非アルキメデス的局所体の場合には定理 5.3 のような主張はそのままでは成立しない。このことは定理 5.2 からも確認できるが、他にも、

- $\mathbb{Q}_p$ の体論的自己同型写像は恒等写像のみ（ちょっとした演習問題）
- $p \neq 2$ であれば、$G_{\mathbb{Q}_p}$ の自己同型写像で内部自己同型でないものが存在する（Jannsen-Wingberg による群構造の決定の応用）

という観察からも確認できる。その一方で、p 進局所体の場合は望月新一氏によって、分岐フィルトレーションと呼ばれる局所体の絶対 Galois 群のある部分群からなる集合を付加データとして考える形に修正すれば類似の主張が成立することが証明されている。（分岐理論の説明は本稿では行

わない。）　その後、V. Abrashkin 氏によって正標数局所体の場合にも類似の主張が成立することが示されている。つまり、

定理 5.4 (望月-Abrashkin — cf. [10], [1])**.** F_1, F_2 を非アルキメデス的局所体とし、

$$\sigma\colon G_{F_1} \xrightarrow{\sim} G_{F_2}$$

をその絶対 Galois 群の間の同型写像とする。σ が分岐フィルトレーションを保てば、σ は内部自己同型の合成による差を除いて、一意的な体同型写像

$$F_2 \xrightarrow{\sim} F_1$$

から生じる。

定理 5.4 は非常に興味深い定理である一方で、局所体の絶対 Galois 群の間の同型写像の住んでいる世界はどの程度体の同型写像の住んでいる世界と離れているかについては興味深い問題として残る。この方向に関してはいくつかの研究があるが (定理 5.2 はその出発点とみなせる)、非常に難しい問題で、例えば $\mathbb{Q}_2$ の絶対 Galois 群の自己同型で内部自己同型でないものが存在するかどうか（外部自己同型群が非自明かどうか）も知られていない。また、そもそもどの程度離れているかということを適切に定式化することでさえ非自明な問題である。

本節の残りの部分では、（非常に粗くではあるが）定理 5.3 の証明の流れを正標数大域体の場合に絞って説明したい。まず、付値に付随する分解群の概念を導入する。

定義 5.5. F を大域体とし、F_v を $v \in \mathbb{V}(F)$ での完備化とする。このとき、自然な体準同型

$$F \hookrightarrow F_v$$

は内部自己同型の合成を除いて定まる準同型

$$\phi_v\colon G_{F_v} \longrightarrow G_F$$

を誘導したことを思い出しておく。実はこの場合 ϕ_v は単射である。ϕ_v の (G_F 内で互いに共役な）代表元の像たちのことを v に付随する G_F の分解群という。

実は Brauer 群と呼ばれる群に関する高度に非自明な考察を行うことで、大域体の絶対 Galois 群の群構造からその分解群たちを復元することができる。そのため、

$$\sigma\colon G_{F_1} \xrightarrow{\sim} G_{F_2}$$

は全単射

$$\sigma_{\mathbb{V}}\colon \mathbb{V}(F_1) \xrightarrow{\sim} \mathbb{V}(F_2)$$

を誘導する。さらに、大域体 F に対し、制限直積

$$\prod_{v\in\mathbb{V}(F)}{}' G_{F_v}^{\mathrm{ab}} \subseteq \prod_{v\in\mathbb{V}(F)} G_{F_v}^{\mathrm{ab}}$$

を有限個の付値を除いた非アルキメデス的付値 $v \in \mathbb{V}(F)$ では惰性群と呼ばれる分岐理論的に特別な $G^{\mathrm{ab}}_{F_v}$ の部分群に入っている元たちのなす部分群とする。（惰性群は G_{F_v} の群構造から復元可能であることが遠アーベル幾何学の研究によって知られている。）このとき、σ は $\sigma_{\mathbb{V}}$ と両立的な可換図式

$$\begin{array}{ccc} \prod'_{v_1 \in \mathbb{V}(F_1)} G^{\mathrm{ab}}_{(F_1)_{v_1}} & \xrightarrow{\sim} & \prod'_{v_2 \in \mathbb{V}(F_2)} G^{\mathrm{ab}}_{(F_2)_{v_2}} \\ \downarrow & & \downarrow \\ G^{\mathrm{ab}}_{F_1} & \xrightarrow{\sim} & G^{\mathrm{ab}}_{F_2} \end{array}$$

を誘導することが分かる。また、正標数大域体 F に対し類体論 (及び注意 4.10.1) を適用することで、合成写像

$$\prod_{v \in \mathbb{V}(F)}' F_v^{\times} \xrightarrow{\prod' r_{F_v}} \prod_{v \in \mathbb{V}(F)}' G^{\mathrm{ab}}_{F_v} \longrightarrow G^{\mathrm{ab}}_{F}$$

の核は $F^{\times}$ に一致することに注意する。つまり、F_1 や F_2 が正標数の大域体であれば全ての付値が非アルキメデス的なので、この注意と命題 5.1 及び上の可換図式から σ は乗法群の同型写像

$$\sigma_f \colon F_1^{\times} \xrightarrow{\sim} F_2^{\times}$$

を誘導することが分かる。さらに、本稿では紹介していない非アルキメデス的局所体に対する遠アーベル幾何学の研究から、各付値 $v_1 \in \mathbb{V}(F_1)$ に対して、

- 任意の $x \in F_1^{\times}$ に対し
$$v_1(x) \;=\; \sigma_{\mathbb{V}}(v_1)(\sigma_f(x))$$
が成立すること、及び、
- σ_f は群の同型写像
$$\{1 + x_1 \mid x_1 \in F_1,\ v_1(x_1) < 1\} \xrightarrow{\sim} \{1 + x_2 \mid x_2 \in F_2,\ \sigma_{\mathbb{V}}(v_1)(x_2) < 1\}$$
を誘導すること

も分かる。実はこの条件さえあれば、内田の補題と呼ばれる巧妙な技術によって、σ_f が誘導する全単射

$$F_1 \;=\; F_1^{\times} \cup \{0\} \xrightarrow{\sim} F_2^{\times} \cup \{0\} \;=\; F_2$$

が加法構造を保つことを証明できる。内田の補題は正標数大域体のみに適用可能な技術ではなく、一般の体上の代数曲線の関数体に対しても適用可能なものである。証明するには代数曲線論に関する説明が必要になるので本稿では行わない。一方で、星裕一郎氏による 2014 年の公開講座の原稿で複素数体上の射影直線の関数体に対する内田の補題を代数幾何の用語を使わない形で説明されているので、興味のある読者はご覧いただければと思う。そこまで長い証明でもないので、代数曲線論の基本的なことをある程度ご存知の方は、原論文や [11], Propositions 1.2, 1.3 を読むのにそこまでの苦労はないと思われる。また、星裕一郎氏により内田の補題の数体類似も得られて

いる ([4])。ただし、数体に対してはアルキメデス的素点に関する部分の問題によって上で説明した方法では乗法群の復元ができない。数体の場合の Neukirch-内田の定理は Neukirch による分解群の復元は使用されるものの、それ以降の議論は全く別の議論で証明される。

内田の補題を証明しない代わりに、そのような主張が成立する簡単な例として内田の補題の有理数体 $\mathbb{Q}$ 版（星裕一郎氏の結果の非常に特別な場合）を説明したい。素数 p に対し、有理数が "p で何回割れるか" で定義される群準同型写像

$$v_p \colon \mathbb{Q}^\times \longrightarrow \mathbb{Z}$$

（つまり 0 でない有理数 x に対し、$v_p(x)$ は p と互いに素な整数 a, b を用いて $x = p^m \cdot \frac{b}{a}$ と書いた時の整数 m) と

$$U_p \overset{\text{def}}{=} \left\{ 1 + p \cdot \frac{b}{a} \mid a, b \in \mathbb{Z},\ a \text{ は } p \text{ と互いに素な非零整数} \right\}$$

という $\mathbb{Q}^\times$ の部分群を考える。v_p は加法付値と呼ばれるもので、簡単に確認できる通り p 進 (乗法) 付値とは

$$|-|_p \ = \ \frac{1}{p^{v_p(-)}}$$

という関係にある。素数の集合を $\mathfrak{Primes}$ と書くとき次が成立する。

命題 5.6.

$$\sigma \colon \mathbb{Q}^\times \ \xrightarrow{\sim}\ \mathbb{Q}^\times$$

を有理数体の乗法群の間の自己同型写像とする。そして、全単射

$$\sigma_{\mathbb{V}} \colon \mathfrak{Primes} \ \xrightarrow{\sim}\ \mathfrak{Primes}$$

で、二条件

(a) 任意の $x \in \mathbb{Q}^\times$, $p \in \mathfrak{Primes}$ に対し、$v_p(x) = v_{\sigma_{\mathbb{V}}(p)}(\sigma(x))$
(b) 任意の $p \in \mathfrak{Primes}$ に対し、$\sigma(U_p) = U_{\sigma_{\mathbb{V}}(p)}$

を満たすものが存在することを仮定する。このとき σ は恒等写像である。特に、σ は自明な体の自己同型写像を誘導する。

Proof. 任意の $p \in \mathfrak{Primes}$ に対し、

$$\mathbb{Z}_{(p)}^\times \overset{\text{def}}{=} \{x \in \mathbb{Q}^\times \mid v_p(x) \ = \ 0\}$$

という $\mathbb{Q}^\times$ の部分群を考える。任意の $\mathbb{Z}_{(p)}^\times$ の元 x に対し、一意的に定まる $a \in \{1, \ldots, p-1\}$ と $b \in U_p$ が存在して $x = ab$ と書ける。そして、対応 $x \mapsto a$ は群の同型写像 $\mathbb{Z}_{(p)}^\times / U_p \xrightarrow{\sim} \mathbb{F}_p^\times$ を誘導する。つまり、条件 (a), (b) から σ は群の同型写像

$$\mathbb{F}_p^\times \ \xrightarrow{\sim}\ \mathbb{F}_{\sigma_{\mathbb{V}}(p)}^\times$$

を誘導する。両辺の位数を考えれば $p = \sigma_{\mathbb{V}}(p)$ だと分かるので、$\sigma_{\mathbb{V}}$ は恒等写像。そうすると条件 (a) と素因数分解の一意性から、任意の $x \in \mathbb{Q}^{\times}$ に対し、

$$\sigma(x) \ \in \ \{\pm x\}$$

だと分かる。特に平方数は σ で動かない。次に m を 3 以上の素数 l を素因数に持つ整数とする。条件 (b) から $\sigma(U_l) = U_l$ なので、$\sigma(1+m) = -(1+m)$ となることはない。よって、そのような m に対し $\sigma(1+m) = 1+m$ である。また、任意の -1 ではない整数 n に対し $3+4n$ は必ず 3 以上の素数を素因数に持つ。したがって、4 は平方数なので、

$$\sigma(1+n) \ = \ \sigma\left(\frac{1+(3+4n)}{4}\right) \ = \ \frac{\sigma(1+(3+4n))}{\sigma(4)} \ = \ \frac{4+4n}{4} \ = \ 1+n$$

以上によって全ての 0 でない整数は σ で動かないことが分かった。σ は群準同型写像なので、このことは σ が恒等写像であることを意味する。 □

上の証明内で使用した、

$$x \ \in \ \{\pm 1\} \iff v_p(x) \ = \ 0 \ (\forall p \in \mathfrak{Primes})$$

という性質はかなり特殊な数体（一般には素数ではなく一般の付値（や素イデアル）に関して議論することになる）に対しての性質である。そして、単数と呼ばれる右側の条件を満たす x が少ないことによって上のような比較的簡単な証明で済んでいることに注意したい。一般の数体の場合、単数のなす群が大きくなるのでもっと難しい議論が必要になる。一方で、全体から見れば単数のなす群はそこまで大きくない (例えば、Dirichlet の単数定理により有限生成である）ことによって内田の補題のような主張が成立するとも考えられる。どの程度小さければ、このような現象が発生するのかは興味深い問題である。

以上で証明の流れの説明を終えるが、Neukirch-内田の定理は既に単遠アーベル幾何学版が存在していることも述べておきたい。つまり、大域体の絶対 Galois 群の位相群構造から純群論的な手続きによって元の大域体の体構造を記述することが可能だということである。正標数大域体の場合は（整理は必要だが）基本的には内田氏による元の証明がそのような手続きを与えており、澤田晃一郎氏により [15] で単遠アーベル幾何学的整理に基づいた解説がなされている。数体の場合は内田氏による証明が単遠アーベル幾何学的ではないという事情があったが、星裕一郎氏により [5] でそのような手続きが与えられている。

補足

多くの結果が存在するので具体的には紹介しないが、前節で紹介した遠アーベル幾何学的定理は既に様々な形での一般化が行われている。一方で、それでもまだよく分からないことだらけであるという印象を筆者は持っている。体構造への対称性のなす群からのアプローチに興味を持ち、遠アーベル幾何学を勉強（さらには研究）する方が増えれば、この分野の一研究者として幸いで

ある。また、本稿で紹介した定理の多くは、実は A. Grothendieck が有名な「G. Faltings への手紙」([2]) で遠アーベル幾何学という分野を創始する以前の結果である。§2 内の注意でも言及したエタール基本群という概念を用いれば、体に限らずより広範な幾何学的対象に対して類似の結果の成否を問うことができる。[2] では主に素体 ($\mathbb{Q}$ や $\mathbb{F}_p$) 上有限生成な体上の双曲的曲線という幾何学的対象に対しての様々な基本的な（いわゆる Grothendieck 予想を含む）予想が提示されている。（そしてこういった対象のエタール基本群は非可換度が高く、「遠アーベル」というのはその状況を反映した用語である。特に中心が自明であるという性質は技術的にもいたるところで適用することになる性質である。）これらについて興味を持たれた方（で代数幾何学に関してある程度の基礎知識をお持ちの方）は、例えば、中村博昭氏、玉川安騎男氏、望月新一氏による [12] のような入門的な解説をご一読いただきたい。また、[12] に書かれている結果は 1990 年代までに得られていた結果なので、より最近 (2010 年代まで) の結果がある程度まとめられている星裕一郎氏による文献 [6] も挙げておく。

参考文献

[1] V. Abrashkin, Modified proof of a local analogue of the Grothendieck conjecture, *Journal Theorie des Nombres de Bordeaux* **22** (2010), pp. 1–50.

[2] A. Grothendieck, *Letter to G. Faltings* (June 1983) in Lochak, L. Schneps, *Geometric Galois Actions; 1. Around Grothendieck's Esquisse d'un Programme*, *London Math. Soc. Lect. Note Ser.* **242**, Cambridge Univ. Press (1997).

[3] A. Grothendieck and M. Raynaud, *Revêtements étales et groupe fondamental* (SGA1), *Lecture Notes in Math.* **224** (1971), Springer-Verlag.

[4] Y. Hoshi, On the field-theoreticity of homomorphisms between the multiplicative groups of number fields, *Publ. Res. Inst. Math. Sci.* **50** (2014), pp. 269–285.

[5] Y. Hoshi, Mono-anabelian reconstruction of number fields, *RIMS Kôkyûroku Bessatsu* B**76** (2019), pp. 1–77.

[6] 星裕一郎, 「遠アーベル幾何学の進展」, 数学 **74** (2022), pp. 1–30.

[7] Y. Hoshi, S. Mochizuki, and S. Tsujimura, Combinatorial construction of the absolute Galois group of the field of rational numbers, RIMS Preprint **1935** (December 2020). 最新版は `https://www.kurims.kyoto-u.ac.jp/~motizuki/` から利用可能。

[8] M. Jarden, J. Ritter, On the characterization of local fields by their absolute Galois groups, *J. Number Theory* **11** (1979), pp. 1–13.

[9] 加藤和也, 黒川信重, 齋藤毅, 「数論 I — Fermat の夢と類体論」, 岩波書店 (2005).

[10] S. Mochizuki, A version of the Grothendieck conjecture for p-adic local fields, *Internat. J. Math.* **8** (1997), pp. 499–506.

[11] S. Mochizuki, Topics in absolute anabelian geometry III: Global reconstruction algorithms, *J. Math. Sci. Univ. Tokyo* **22** (2015), pp. 939–1156.

[12] 中村博昭, 玉川安騎男, 望月新一, 「代数曲線の基本群に関する Grothendieck 予想」, 数学 **50** (1998), pp. 113–129.

[13] J. Neukirch, *Algebraic number theory*, *Grundlehren der Mathematischen Wissenschaften* **322**, Springer-Verlag (1999). (邦訳： J. ノイキルヒ,「代数的整数論」, シュプリンガージャパン)

[14] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, *Grundlehren der Mathematischen Wissenschaften* **323**, Springer-Verlag (2000).

[15] K. Sawada, Algorithmic approach to Uchida's theorem for one-dimensional function fields over finite fields, Inter-universal Teichmüller theory summit 2016, *RIMS Kôkyûroku Bessatsu* B**84** (2021), pp. 1–21.

[16] K. Uchida, Isomorphisms of Galois groups, *J. Math. Soc. Japan* **28** (1976), pp. 617–620.

[17] K. Uchida, Isomorphisms of Galois groups of algebraic function fields, *Ann. Math.* **106** (1977), pp. 589–598.

[18] S. Yamagata, A counterexample for the local analogy of a theorem by Iwasawa and Uchida, *Proc. Japan Acad.* **52** (1976), pp. 276–278.