

ガロアの逆問題と数論幾何

玉川安騎男

§0. はじめに

ガロアの逆問題とは、任意の有限群が有理数体上のガロア群として実現されるかという問題です。この問題は、19世紀末には既に研究が始まっていた数論の古典的難問題で、現在でも未解決です。この講義では、まず、ガロアの逆問題の定式化に必要な、群・体・ガロア理論についての基礎事項を解説します。次に、ヒルベルトの既約性定理について紹介し、ガロアの逆問題がどのように幾何の問題と結び付くかについて説明します。最後に、ガロアの逆問題へのいくつかの数論幾何的アプローチについて、その考え方の一端を紹介します。もし時間があれば、ガロア理論の別のタイプの逆問題と考えられる、遠アーベル幾何についても少しふれたいと思います。

§1. 体

1.1. 数の体系

$$\mathbb{N} = \{ \text{自然数全体} \} = \{1, 2, \dots\} \text{ (0を入れることも),}$$

$$\mathbb{Z} = \{ \text{整数全体} \} = \{0, \pm 1, \pm 2, \dots\},$$

$$\mathbb{Q} = \{ \text{有理数全体} \} = \{a/b \mid a, b \in \mathbb{Z}, b \neq 0\},$$

$$\mathbb{R} = \{ \text{実数全体} \},$$

$$\mathbb{C} = \{ \text{複素数全体} \} = \{a + b\sqrt{-1} \mid a, b \in \mathbb{R}\}.$$

このうち、 $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ は加法、減法、乗法、除法が (0 で割ることをのぞいて) 自由にできることに注意して下さい。 $\mathbb{N}$ は加法と乗法のみ、 $\mathbb{Z}$ は加法と減法と乗法のみ自由にできます。

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$ -TEX

1.2. 体とは

簡単に言うと、加減乗除が自由にできるような集合のことを体と呼びます。より正確に述べると、次のような定義になります。

定義. 集合 K 、写像

$$+ : K \times K \rightarrow K, (a, b) \mapsto a + b$$

$$- : K \times K \rightarrow K, (a, b) \mapsto a - b$$

$$\times : K \times K \rightarrow K, (a, b) \mapsto a \times b (= a \cdot b = ab)$$

$$\div : K \times (K - \{0\}) \rightarrow K, (a, b) \mapsto a \div b (= a/b)$$

および元 $0, 1 \in K$ が与えられており、次の性質を満たすとする。

$$(a + b) + c = a + (b + c) \quad (a, b, c \in K)$$

$$a + b = b + a \quad (a, b \in K)$$

$$a + 0 = a \quad (a \in K)$$

$$(a - b) + b = a \quad (a, b \in K)$$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad (a, b, c \in K)$$

$$a \cdot b = b \cdot a \quad (a, b \in K)$$

$$a \cdot 1 = a \quad (a \in K)$$

$$(a/b) \cdot b = a \quad (a \in K, b \in K - \{0\})$$

$$a \cdot (b + c) = ab + ac \quad (a, b, c \in K)$$

$$1 \neq 0$$

このとき、 K を体という。□

例. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ は体であり、それぞれ有理数体、実数体、複素数体という。□

例. p を素数とし、 $\mathbb{F}_p = \{0, 1, \dots, p-1\}$ とおく。 $a, b \in \mathbb{F}_p$ に対し、 $a+b, a-b, ab \in \mathbb{F}_p$ を、それぞれ通常の $a+b, a-b, ab \in \mathbb{Z}$ を p で割った余りとして定義し、 $a \in \mathbb{F}_p, b \in \mathbb{F}_p - \{0\}$ に対し、 a/b を、 $ab^{p-2} \in \mathbb{Z}$ を p で割った余りとして定義する。このとき、 $\mathbb{F}_p$ は体となる。(フェルマーの小定理に注意。) □

1.3. 多項式

体 K と $n \in \mathbb{N}$ に対し、

$$K[x_1, \dots, x_n] =$$

$$\left\{ \sum_{i_1, \dots, i_n \geq 0} a_{i_1 \dots i_n} x_1^{i_1} \cdots x_n^{i_n} \mid a_{i_1 \dots i_n} \in K, \forall' (i_1, \dots, i_n), a_{i_1 \dots i_n} = 0 \right\}$$

の元を、 K 上の(変数 $x_1, \dots, x_n$ に関する) n 変数多項式と呼びます。特に、 $n = 1$ の場合、(x_1 を x と書いて)

$$K[x] = \left\{ \sum_{i \geq 0} a_i x^i \mid a_i \in K, \forall i, a_i = 0 \right\}$$

となります。

2つの多項式の和、差、積はまた多項式になります。

$$f = \sum_{i_1, \dots, i_n \geq 0} a_{i_1 \dots i_n} x_1^{i_1} \cdots x_n^{i_n} \in K[x_1, \dots, x_n], f \neq 0 \text{ に対し、}$$

$$\deg(f) = \max\{i_1 + \cdots + i_n \mid a_{i_1 \dots i_n} \neq 0\}$$

を f の次数といいます。

次数 > 0 の多項式 $f \in K[x_1, \dots, x_n]$ は、ある次数 > 0 の多項式 $g, h \in K[x_1, \dots, x_n]$ に対して $f = gh$ と表されるとき可約、そうでないとき既約といいます。

1.4. 線形代数

多くの大学で初年次に実数体 $\mathbb{R}$ (および複素数体 $\mathbb{C}$) 上の線形代数を学びますが、その理論の基本的な部分は、一般の体の上でも成立します。特に、以下の定義と性質が最も基本的です。

定義. K を体とする。集合 V 、写像

$$\begin{aligned} +: V \times V &\rightarrow V, (u, v) \mapsto u + v \\ -: V \times V &\rightarrow V, (u, v) \mapsto u - v \\ \cdot: K \times V &\rightarrow V, (a, u) \mapsto a \cdot u (= au) \end{aligned}$$

と元 $o \in V$ が与えられており、次の性質を満たすとする。

$$\begin{aligned} (u + v) + w &= u + (v + w) \quad (u, v, w \in V) \\ u + v &= v + u \quad (u, v \in V) \\ u + o &= u \quad (u \in V) \\ (u - v) + v &= u \quad (u, v \in V) \\ a(u + v) &= au + av, \quad a \cdot o = o \quad (a \in K, u, v \in V) \\ (a + b)u &= au + bu, \quad 0 \cdot u = o \quad (a, b \in K, u \in V) \\ (ab)u &= a(bu), \quad 1 \cdot u = u \quad (a, b \in K, u \in V) \end{aligned}$$

このとき、 V を K 上のベクトル空間 (または線形空間) という。 $\square$

例. $V = \{o\}$ は K 上のベクトル空間となる。 $\square$

例. $V = K$ は K 上のベクトル空間となる ($o = 0$)。 $\square$

例. $n \in \mathbb{N}$ に対し、

$$V = K^n = \{(u_1, \dots, u_n) \mid u_1, \dots, u_n \in K\}$$

は K 上のベクトル空間となる。ここで、

$$(u_1, \dots, u_n) + (v_1, \dots, v_n) = (u_1 + v_1, \dots, u_n + v_n)$$

$$(u_1, \dots, u_n) - (v_1, \dots, v_n) = (u_1 - v_1, \dots, u_n - v_n)$$

$$a \cdot (u_1, \dots, u_n) = (au_1, \dots, au_n)$$

$$o = (0, \dots, 0)$$

K^1 は K と同一視できる。また、 K^0 は $\{o\}$ を表すものとする。 $\square$

V を体 K 上のベクトル空間とし、 $v_1, \dots, v_n$ を V の元とします。このとき、写像

$$\varphi = \varphi_{v_1, \dots, v_n} : K^n \rightarrow V, (a_1, \dots, a_n) \mapsto a_1 v_1 + \dots + a_n v_n$$

を考えます。

定義. φ が全射となるような $n \in \mathbb{N} \cup \{0\}$ および $v_1, \dots, v_n$ が取れるとき、 V は有限次元ベクトル空間であるという。 $\square$

定義. φ が全単射となるような $v_1, \dots, v_n$ を、 V の基底と呼ぶ。このとき、 n をこの基底の長さと呼ぶ。 $\square$

次の定理は基本的です。

定理. 有限次元ベクトル空間 V には常に基底が存在する。基底の長さは基底の取り方によらず V のみで定まる。 $\square$

定義. 有限次元ベクトル空間 V のある（したがって全ての）基底の長さを V の次元と呼び、 $\dim(V)$ あるいは $\dim_K(V)$ と表す。有限次元でないベクトル空間 V に対しては、 $\dim(V) = \infty$ とおく。 $\square$

例. $\dim_K(K^n) = n$ 。 $\square$

体 K 上の2つのベクトル空間 V, W の間に包含関係 $W \subset V$ があり、 V の $+$, $-$ および a 倍 ($a \in K$) を制限したものが W の $+$, $-$ および a 倍となっており、 V の o と W の o が一致するとき、「 W は V の部分 (ベクトル) 空間」と言います。

命題. V を体 K 上の有限次元ベクトル空間、 W をその部分ベクトル空間とする。このとき、

- (i) W は有限次元で、 $\dim_K(W) \leq \dim_K(V)$ 。
- (ii) $\dim_K(W) = \dim_K(V) \iff W = V$ 。 $\square$

1.5. 体の拡大

2つの体 K, L の間に包含関係 $K \subset L$ があり、 L の $+$, $-$, $\times$, $\div$ を制限したものが K の $+$, $-$, $\times$, $\div$ となっており、 K の $0, 1$ と L の $0, 1$ が一致するとき、「 K は L の部分体」「 L は K の拡大体」あるいは「 L/K は (体) の拡大」と言います。

例. $\mathbb{C}/\mathbb{Q}, \mathbb{R}/\mathbb{Q}, \mathbb{Q}/\mathbb{Q}, \mathbb{C}/\mathbb{R}, \mathbb{R}/\mathbb{R}, \mathbb{C}/\mathbb{C}$ は体の拡大。 $\square$

L/K を体の拡大とすると、 L は自然に K 上のベクトル空間となることからわかります。

定義. L が K 上のベクトル空間として有限次元のとき、 L/K を有限次拡大という。このとき、 $\dim_K(L)$ を L/K の次数と呼び、 $[L : K]$ と表す。有限次拡大でない拡大は無限次拡大と言い、 $[L : K] = \infty$ とおく。 $\square$

例. $[\mathbb{Q} : \mathbb{Q}] = [\mathbb{R} : \mathbb{R}] = [\mathbb{C} : \mathbb{C}] = 1$ 、 $[\mathbb{C} : \mathbb{R}] = 2$ 、 $[\mathbb{C} : \mathbb{Q}] = [\mathbb{R} : \mathbb{Q}] = \infty$ 。 $\square$

定義. $\mathbb{Q}$ の有限次拡大体を代数体という。 $\square$

次の命題は基本的ですが、応用上重要です。

命題. $L/K, M/L$ を体の有限次拡大とする ($K \subset L \subset M$)。このとき、 M/K は有限次拡大で、 $[M : K] = [M : L][L : K]$ が成り立つ。 $\square$

L/K を体の拡大とし、 $\alpha_1, \dots, \alpha_n \in L$ とします。このとき、

$$K[\alpha_1, \dots, \alpha_n] = \{f(\alpha_1, \dots, \alpha_n) \mid f \in K[x_1, \dots, x_n]\}$$

$$K(\alpha_1, \dots, \alpha_n) = \{\beta/\gamma \mid \beta, \gamma \in K[\alpha_1, \dots, \alpha_n], \gamma \neq 0\}$$

とおくと、 $K(\alpha_1, \dots, \alpha_n)$ は L/K の中間拡大体 (すなわち、 L の部分体でかつ K の拡大体) となることがわかります。 $(K(\alpha_1, \dots, \alpha_n)$ を、 K に $\alpha_1, \dots, \alpha_n$ を添加した体といいます。) より詳しく言うと、

$$K \subset K[\alpha_1, \dots, \alpha_n] \subset K(\alpha_1, \dots, \alpha_n) \subset L$$

であり、(L の演算の制限により) $K(\alpha_1, \dots, \alpha_n)$ は体になりますが、 $K[\alpha_1, \dots, \alpha_n]$ は一般には体になりません。「環」にはなります。

1.6. 体の同型

K_1, K_2 を体とします。全単射 $\sigma: K_1 \rightarrow K_2$ において、 K_1 の $+, -, \times, \div, 0, 1$ と K_2 の $+, -, \times, \div, 0, 1$ が対応するとき、 σ を (K_1 から K_2 への) 同型と呼びます。特に、 K を体とするとき、同型 $K \rightarrow K$ を K の自己同型と呼びます。 $\text{Aut}(K)$ で、 K の自己同型全体のなす集合を表します。

L/K を体の拡大とします。 L の自己同型 $\sigma: L \rightarrow L$ で、任意の $a \in K$ に対し $\sigma(a) = a$ となるものを、 L の K 上の自己同型と呼びます。 $\text{Aut}(L/K)$ で、 L の K 上の自己同型全体のなす集合を表します。

§2. 群

2.1. 群とは

まず、群の厳密な定義を与えましょう。

定義. 集合 G 、写像

$$\begin{aligned} \circ: G \times G &\rightarrow G, (x, y) \mapsto x \circ y \\ \iota: G &\rightarrow G, x \mapsto \iota(x) \end{aligned}$$

および元 $e \in G$ が与えられており、次の公理 I、II、III を満たすとする。

I. 任意の $x, y, z \in G$ に対し、 $(x \circ y) \circ z = x \circ (y \circ z)$

II. 任意の $x \in G$ に対し、 $x \circ e = e \circ x = x$

III. 任意の $x \in G$ に対し、 $x \circ \iota(x) = \iota(x) \circ x = e$

このとき、 G は (あるいは、 $(G, \circ)$ は) 群であるという。□

定義. 上の定義で、更に

IV. 任意の $x, y \in G$ に対し、 $x \circ y = y \circ x$

が満たされるとき、 G をアーベル群 (または、可換群) という。□

注. e を G の単位元といい、 $\iota(x)$ を x の逆元といいます。□

注. 普通、群の演算は積で表し、 $x \circ y$ を xy と記します。このときは、単位元 e を 1 、 x の逆元 $\iota(x)$ を x^{-1} と記します。アーベル群については、演算を和で表し $x \circ y$ を $x + y$ と記すこともあり、このときは、単位元 e を 0 、 x の逆元 $\iota(x)$ を $-x$ と記します。□

例. K を体とするとき、 $(K, +)$ や $(K - \{0\}, \times)$ はアーベル群。 V を K 上のベクトル空間とするとき、 $(V, +)$ はアーベル群。□

例. $N \in \mathbb{N}$ とし、 $\mathbb{Z}/N\mathbb{Z} = \{0, 1, \dots, N-1\}$ とおく。 $a, b \in \mathbb{Z}/N\mathbb{Z}$ に対し、 $a+b, a-b, ab \in \mathbb{Z}/N\mathbb{Z}$ を、それぞれ通常の $a+b, a-b, ab \in \mathbb{Z}$ を N で割った余りとして定義する。また、 $\mathbb{Z}/N\mathbb{Z}$ の部分集合 $(\mathbb{Z}/N\mathbb{Z})^\times$ を

$$(\mathbb{Z}/N\mathbb{Z})^\times = \{a \in \mathbb{Z}/N\mathbb{Z} \mid (a, N) = 1\}$$

と定義する。このとき、 $(\mathbb{Z}/N\mathbb{Z}, +)$ はアーベル群で、 N 次巡回群と呼ばれる。また、 $((\mathbb{Z}/N\mathbb{Z})^\times, \cdot)$ もアーベル群。□

2.2. 構造変換と群

少し抽象的な話になりますが、数学で群がどのように現れるかを簡単に説明したいと思います。 X を数学的構造を持った数学的対象とします。より正確に言うと、 X はある「圏」の「対象」ということになります。このとき、(X の構造を保つ)「射」 $f: X \rightarrow X$ であって、(X の構造を保つ) 逆射 $g: X \rightarrow X$ (すなわち、 $f \circ g = g \circ f = \text{id}$) が存在するものを、 X の自己同型射と呼びます。 X の自己同型射全体のなす集合を $\text{Aut}(X)$ と記すとき、 $\text{Aut}(X)$ は、射の合成 $\circ$ という演算により群になることがわかります。実際、群の公理の I は、射の合成の結合律から従い、II は、恒等射 $\text{id}: X \rightarrow X$ が単位元を与えることから従い、III は、各自己同型射に対し、逆射がその逆元を与えることから従います。

以上のことは抽象的で難しく感じられるかもしれませんが、以下のいくつかの例を見ていただければ感じがつかめるかと思います。

例. X を集合とする。このとき、全単射 $X \rightarrow X$ 全体の集合 $\text{Aut}(X)$ は (写像の合成を積として) 群となり、集合 X 上の対称群と呼ばれる。特に、 $n \in \mathbb{N}$ 、 $X = \{1, \dots, n\}$ のとき、 $\text{Aut}(X)$ は n 次対称群と呼ばれ、 S_n と記される。($n \geq 3$ のとき、 S_n は非アーベル群。) □

例. V を体 K 上のベクトル空間とする。このとき、

$$\text{Aut}(V) = \{f : V \rightarrow V \text{ 全単射} \mid f(u \pm v) = f(u) \pm f(v), f(o) = o, \\ f(au) = af(u) \ (u, v \in V, a \in K)\}$$

は(写像の合成を積として)群となり、 V 上の一般線形群と呼ばれ、 $GL(V)$ (あるいは $GL_K(V)$) と記される。特に、 $V = K^n$ のとき、 $\text{Aut}(V)$ は n 次一般線形群と呼ばれ、 $GL_n(K)$ と記される。 $GL_n(K)$ は、 K 係数 n 次正方行列で行列式が $\neq 0$ のものの全体が行列の積に関してなす群と同一視できる。 $(n \geq 2$ のとき、 $GL_n(K)$ は非アーベル群。) $\square$

例. G を群とする。このとき、

$$\text{Aut}(G) = \{f : G \rightarrow G \text{ 全単射} \mid f(x \circ y) = f(x) \circ f(y)\}$$

は(写像の合成を積として)群となり、 G の自己同型群と呼ばれる。 $\square$

ガロア理論で重要なのは、次の例です。

例. (i) 体 K に対し、 $\text{Aut}(K)$ は(写像の合成を積として)群となり、 K の自己同型群と呼ばれる。

(ii) 体の拡大 L/K に対し、 $\text{Aut}(L/K)$ は(写像の合成を積として)群となり、 L の K 自己同型群と呼ばれる。 $\square$

2.3. 部分群と商群

定義. 2つの群 G, H の間に包含関係 $H \subset G$ があり、 G の $\circ, \iota$ を制限したものが H の $\circ, \iota$ となっており、 G の e と H の e が一致するとき、「 H は G の部分群」という。 $\square$

定義. 群 G の部分群 H が、

$$y \in H, x \in G \implies x \circ y \circ \iota(x) \in H$$

を満たすとき、 H を G の正規部分群という。 $\square$

定義. G を群とし、 H をその部分群とする。このとき、 $x, y \in G$ に対し、 $\iota(x) \circ y \in H$ であることを $x \sim y$ で表すと、 $\sim$ は G の上の同値関係になる。すなわち、

$$x \sim x \text{ (反射律)}$$

$$x \sim y \implies y \sim x \text{ (対称律)}$$

$$x \sim y, y \sim z \implies x \sim z \text{ (推移律)}$$

さらに、 H が G の正規部分群のときは、

$$x \sim y, z \sim w \implies x \circ z \sim y \circ w$$

も満たされ、このとき、同値関係 $\sim$ による G の「商集合」は、 G の演算から誘導される演算によって群となる。この群を G/H で表し、 G の H による商群と呼ぶ。 $\square$

2.4. 群の位数

群 G の元の数 $|G|$ を G の位数と言ひ、 $|G|$ で表します。 $|G| < \infty$ のとき G は有限群であると言ひ、そうでないとき G は無限群であると言ひます。

例. $|S_n| = n!$. $\square$

次のラグランジュの定理は応用上重要です。

定理. G を有限群とし、 H を G の部分群とする。このとき、 $|H|$ は $|G|$ の約数。 $\square$

したがって、商 $|G|/|H|$ は自然数となりますが、これを H の G における指数と呼び、 $|G:H|$ と記します。

§3. ガロア理論

3.1. ガロア拡大

L/K を体の有限次拡大とします。

定理. 次の (i)(ii)(iii) は互いに同値。

(i) (最高次係数が 1 の) n 次多項式 $f(x) \in K[x]$ と相異なる n 個の元 $\alpha_1, \dots, \alpha_n \in L$ が存在して、 $L[x]$ において分解

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$$

が成立し、しかも $L = K(\alpha_1, \dots, \alpha_n)$ が成り立つ。

(ii) L の任意の拡大体 M と任意の $\sigma \in \text{Aut}(M/K)$ に対し、 $\sigma(L) = L$ 。また、任意の $\alpha \in L - K$ に対し、 L のある拡大体 M とある $\sigma \in \text{Aut}(M/K)$ が存在し、 $\sigma(\alpha) \neq \alpha$ 。

(iii) $|\text{Aut}(L/K)| = [L : K]$ 。 $\square$

定義. 上記の同値な条件のいずれか(したがって全て)が成立するとき、 L/K をガロア拡大という。このとき、 $\text{Aut}(L/K)$ を $\text{Gal}(L/K)$ と記し、 L の K 上のガロア群と呼ぶ。 $\square$

注. 上の定義の (i) の中の $\alpha_1, \dots, \alpha_n$ が相異なるという条件や (ii) の中の $\sigma(\alpha) \neq \alpha$ となる σ が存在するという条件は、分離性と呼ばれます。 K が「完全体」のとき(例えば、 K が $\mathbb{Q}$ の拡大体のとき)は、この分離性の条件は省くことができます。 $\square$

注. 上の定義の (i) において、 $L = K(\alpha_1, \dots, \alpha_n)$ を f の K 上の最小分解体といい、 $\text{Gal}(L/K) = \text{Gal}(K(\alpha_1, \dots, \alpha_n)/K)$ を方程式 $f = 0$ の(あるいは多項式 f の) K 上のガロア群といいます。 f の K 上の最小分解体や K 上のガロア群は、同型をのぞいて K と f のみから決まります。 $\square$

例. K を $\mathbb{C}$ の部分体とする。 $a \in K$ に対し、 $K(\sqrt{a})$ はガロア拡大。 $\square$

例. $N \in \mathbb{N}$ に対し $\zeta_N = e^{\frac{2\pi i}{N}} = \cos \frac{2\pi}{N} + i \sin \frac{2\pi}{N}$ とおく ($i \in \mathbb{C}$ は虚数単位)。このとき、 $\mathbb{Q}(\zeta_N)/\mathbb{Q}$ はガロア拡大。また、 $\mathbb{Q}(\cos \frac{2\pi}{N})/\mathbb{Q}$ や $\mathbb{Q}(\sin \frac{2\pi}{N})/\mathbb{Q}$ もガロア拡大。 $\square$

例. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ はガロア拡大でない。 $\square$

例. $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ と $\mathbb{Q}(\sqrt{2}, \sqrt{1+\sqrt{2}})/\mathbb{Q}(\sqrt{2})$ はともにガロア拡大だが、 $\mathbb{Q}(\sqrt{2}, \sqrt{1+\sqrt{2}})/\mathbb{Q}$ はガロア拡大でない。 $\square$

3.2. ガロア対応

L/K を有限次ガロア拡大とし、 $G = \text{Gal}(L/K)$ とおきます。 G は有限群となります ($|G| = [L : K]$)。

定義.

(i) G の部分群 H に対し、

$$L^H = \{\alpha \in L \mid \forall \sigma \in H, \sigma(\alpha) = \alpha\}$$

とおく。

(ii) L/K の中間拡大体 M ($K \subset M \subset L$) に対し、

$$G(M) = \{\sigma \in G \mid \forall \alpha \in M, \sigma(\alpha) = \alpha\}$$

とおく。 $\square$

上の定義で、(i) では L^H が L/K の中間拡大体となること、(ii) では $G(M)$ は G の部分群となることが、それぞれ容易に示せます。

次の定理がガロア理論の基本定理です。

定理.

(i) ガロア対応と呼ばれる次の一対一対応がある。

$$\{L/K \text{ の中間拡大体全体} \} \stackrel{1:1}{\cong} \{G \text{ の部分群全体} \}$$

$$M \mapsto G(M)$$

$$L^H \longleftarrow H$$

(ii) L/M は (常に) ガロア拡大で、 $G(M) = \text{Gal}(L/M)$ が成立する。また、 M/K がガロア拡大であることと $G(M)$ が G の正規部分群であることは同値である。この場合、 $\text{Gal}(M/K)$ は、商群 $G/G(M) = \text{Gal}(L/K)/\text{Gal}(L/M)$ と同一視される。

(iii) 次の等式が成立する。

$$[L : M] = |G(M)| = |\text{Gal}(L/M)|$$

$$[M : K] = |G : G(M)| = |\text{Gal}(L/K) : \text{Gal}(L/M)| \quad \square$$

3.3. ガロア理論の古典的応用

ガロア理論の作図問題への応用として、

- ・立方体倍積問題の否定的解決
- ・角の3等分問題の否定的解決
- ・正多角形の作図問題

などがあります。また、ガロア理論の代数方程式論への応用として、

- ・代数学の基本定理の証明
- ・円分多項式の既約性の証明
- ・4次以下の方程式の解法
- ・5次以上の方程式の加減乗除とべき根のみを用いた解法の非存在の証明

などがあります。

3.4. ガロアの逆問題

上で見たように、ガロア拡大 $L/\mathbb{Q}$ に対し、ガロア群 $\text{Gal}(L/\mathbb{Q})$ として有限群を得ることができます。逆に、次のような問題が考えられます。

問題. 任意の有限群 G が与えられたとき、ガロア拡大 $L/\mathbb{Q}$ でガロア群 $\text{Gal}(L/\mathbb{Q})$ が G と同型になるものが存在するか? $\square$

この問題こそが、本講義のタイトルにあるガロアの逆問題です。(逆ガロア問題ともいいます。) この問題は見かけは非常に単純ですが、実はたいへんな難問題で、現在までさまざまな研究がなされて部分的な結果はいろいろ得られていますが、一般には未解決問題となっています。

ガロアの逆問題に関するさまざまな結果やアプローチは、5節で紹介します。

§4. ヒルベルトの既約性定理

命題. K を体とするとき、次の (i)(ii) は同値。

(i) 任意の $m, r, n \in \mathbb{N}$ と m 個の $(r+n)$ 変数既約多項式 $f_1, \dots, f_m \in K[t_1, \dots, t_r, x_1, \dots, x_n]$ に対し、無限個の $(a_1, \dots, a_r) \in K^r$ が存在し、任意の $i = 1, \dots, m$ に対して $f_i(a_1, \dots, a_r, x_1, \dots, x_n) \in K[x_1, \dots, x_n]$ は既約。

(ii) 任意の 2 変数既約多項式 $f \in K[t, x]$ に対し、 $a \in K$ が存在し、 $f(a, x) \in K[x]$ は既約。 $\square$

定義. 上記の同値な条件のいずれか（したがって全て）が成立するとき、 K はヒルベルト体であるという。 $\square$

次の、ヒルベルトの既約性定理が基本的です。

定理. 任意の代数体（特に $\mathbb{Q}$ ）はヒルベルト体である。 $\square$

この定理と次の命題が、ガロアの逆問題への応用の鍵となります。

命題. K をヒルベルト体とする。 $f \in K[t_1, \dots, t_r, x] \subset K(t_1, \dots, t_r)[x]$ とし、 f の $K(t_1, \dots, t_r)$ 上のガロア群を G とする。このとき、無限個の $(a_1, \dots, a_r) \in K^r$ が存在し、 $f(a_1, \dots, a_r, x) \in K[x]$ の K 上のガロア群は G と同型になる。 $\square$

§5. ガロアの逆問題へのアプローチ

G を有限群とします。ガロア拡大 L/K でガロア群 $\text{Gal}(L/K)$ が G と同型になるものが存在するとき、 G は K 上実現可能、といいます。ガロアの逆問題は、任意の有限群が $\mathbb{Q}$ 上実現可能か、と言い換えることができます。

5.1. 円分体と算術級数定理

命題. $N \in \mathbb{N}$ に対し、 $\text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \simeq (\mathbb{Z}/N\mathbb{Z})^\times$ 。

略証. 群準同型 $\text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \rightarrow (\mathbb{Z}/N\mathbb{Z})^\times$ の構成とその単射性の証明は簡単。全射性は「(第 N) 円分多項式」の既約性と同値で、その既約性の証明はいくつかあるが、ガロア理論と「フロベニウス元」を用いるものやガロア理論と「惰性群」を用いるものが代表的。□

定理 (算術級数定理). $n \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, n) = 1$ とする。このとき、素数 p で $p \equiv a \pmod{n}$ となるものが無限個存在する。□

定理. 任意の有限アーベル群 G は $\mathbb{Q}$ 上実現可能。□

略証. 「アーベル群の基本定理」により、 $G \simeq (\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_r\mathbb{Z})$ となる ($r, n_1, \dots, n_r \in \mathbb{N}$)。算術級数定理より、相異なる素数 $p_1, \dots, p_r$ であって $p_i \equiv 1 \pmod{n_i}$ となるものが存在する。 $N = p_1 \cdots p_r$ とおくと、 $\text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \simeq (\mathbb{Z}/N\mathbb{Z})^\times \simeq (\mathbb{Z}/p_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r\mathbb{Z})^\times$ となるので、右辺の部分群 $((\mathbb{Z}/p_1\mathbb{Z})^\times)^{n_1} \times \cdots \times ((\mathbb{Z}/p_r\mathbb{Z})^\times)^{n_r}$ に対応する $\mathbb{Q}(\zeta_N)/\mathbb{Q}$ の中間拡大体 L をとれば、 $\text{Gal}(L/\mathbb{Q}) \simeq G$ となることがわかる。□

5.2. 類体論

類体論は、与えられた代数体のアーベル拡大 (= ガロア拡大でガロア群がアーベル群のもの) を完全に記述する、整数論における非常に強力な理論です。類体論を繰り返し帰納的に用いることで、次の結果が証明できることが知られています。

定理 (シャファレヴィッチ). 任意の有限可解群は $\mathbb{Q}$ 上実現可能。□

ここで、群の可解性は次のように定義されます。

定義. G を群とする。 G の正規部分群の列

$$G = H_0 \supset H_1 \supset \cdots \supset H_n = \{e\}$$

が存在して、任意の $i = 1, \dots, n$ に対して商群 H_{i-1}/H_i がアーベル群となるとき、 G は可解群であるという。□

5.3. ネーターの問題

G を S_n の部分群とします。 G は、体 $\mathbb{L} = \mathbb{Q}(x_1, \dots, x_n)$ に次のように「作用」します： $f = g/h$ ($g, h \in \mathbb{Q}[x_1, \dots, x_n], h \neq 0$) と $\sigma \in G$ に対し、

$$\sigma(f) = g(x_{\sigma^{-1}(1)}, \dots, x_{\sigma^{-1}(n)})/h(x_{\sigma^{-1}(1)}, \dots, x_{\sigma^{-1}(n)})$$

$\mathbb{K} = \mathbb{L}^G = \{f \in \mathbb{L} \mid \forall \sigma \in G, \sigma(f) = f\}$ とおきます。

命題. $\mathbb{L}/\mathbb{K}$ はガロア拡大で、 $\text{Gal}(\mathbb{L}/\mathbb{K}) \simeq G$ 。 $\square$

系. $\mathbb{K} \simeq \mathbb{Q}(t_1, \dots, t_n)$ と仮定する。このとき、 G は $\mathbb{Q}$ 上実現可能。

略証. ヒルベルトの既約性定理。 $\square$

問題 (ネーターの問題). どのような $G (\subset S_n)$ に対して $\mathbb{K} \simeq \mathbb{Q}(t_1, \dots, t_n)$ となるか? $\square$

例. $G = \mathbb{Z}/8\mathbb{Z}$ のとき、 $\mathbb{K} \simeq \mathbb{Q}(t_1, \dots, t_n)$ とならない。 $\square$

定理. $G = S_n$ は、 $\mathbb{Q}$ 上実現可能。

略証. $k = 1, \dots, n$ に対し、 $x_1, \dots, x_n$ の k 次基本対称式

$$s_k = \sum_{1 \leq i_1 < \dots < i_k \leq n} x_{i_1} \dots x_{i_k}$$

を考えると、 $\mathbb{K} = \mathbb{Q}(s_1, \dots, s_n) \simeq \mathbb{Q}(t_1, \dots, t_n)$ がわかる。 $\square$

5.4. 正則逆ガロア問題と剛性

ヒルベルトの既約性定理により、有限群 G が $\mathbb{Q}(t)$ 上実現可能であれば、 G は $\mathbb{Q}$ 上実現可能です。「 G が $\mathbb{Q}(t)$ 上実現可能」より少し強い問題として、次を考えます。

定義. K を体とし、 G を有限群とする。ガロア拡大 $\mathbb{L}/K(t)$ であって $\mathbb{L}/K$ が正則拡大であり、ガロア群 $\text{Gal}(\mathbb{L}/K(t))$ が G と同型になるものが存在するとき、 G は K 上正則的に実現可能、という。但し、 $\mathbb{L}/K$ が正則拡大とは、 $\mathbb{L}/K$ の有限次中間拡大が K 自身に限ることをいう。 $\square$

問題 (正則逆ガロア問題). 任意の有限群は $\mathbb{Q}$ 上正則的に実現可能か? $\square$

命題. 正則逆ガロア問題が肯定的ならばガロアの逆問題も肯定的。より強く、有限群 G が $\mathbb{Q}$ 上正則的に実現可能ならば、 $\mathbb{Q}$ の無限個のガロア拡大 $L_1, L_2, \dots$ で互いに同型でないものが存在して、任意の $i = 1, 2, \dots$ に対して $\text{Gal}(L_i/\mathbb{Q}) \simeq G$ となる。

略証. ヒルベルトの既約性定理。 $\square$

したがって、正則逆ガロア問題は、元のガロアの逆問題よりも難しい問題ということになりますが、実際には、正則逆ガロア問題では幾何を用いることができるようになるため、元のガロアの逆問題ではできなかった数論幾何的アプローチができるようになります。

より正確に言うと、一般に、

$\mathbb{Q}(t)$ 上の (正則的) G ガロア拡大

$\rightsquigarrow$ $\mathbb{C}(t)$ 上の (正則的) G ガロア拡大

$\rightsquigarrow$ 「射影直線」 $\mathbb{P}_{\mathbb{C}}^1$ の代数的 G ガロア分岐被覆

$\rightsquigarrow$ 球面 S^2 の位相的 G ガロア分岐被覆

$\rightsquigarrow$ 有限個の点を抜いた球面の「基本群」から G への全射準同型

となっています。ここで、(1) は拡大の「基底変換」(体論)、(2) は「代数曲線」の一般論(代数幾何)、(3) はいわゆる「GAGA」(鍵は「リーマンの存在定理」)、(4) は基本群の一般論(位相幾何)です。

n 点抜き球面の基本群は階数 $n-1$ の「自由群」となることが知られていますので、 n を十分大きく取れば、いつでも G への全射準同型が存在します。問題は、(1) の逆(拡大の「基底降下」)が一般には言えないことですが、 $\mathbb{C}(t)$ 上の (正則的) G ガロア拡大 ($\approx$ 有限個の点を抜いた球面の基本群から G への全射準同型) をうまく選ぶと、「剛性」の手法によって (1) の逆がたどれる場合があります。次の定理は、この剛性の手法を用いて証明されます。

定理. 26 個の「散在型有限単純群」のうち、マシュー群 M_{23} を除く 25 個は $\mathbb{Q}$ 上 (正則的に) 実現可能。

5.5. フルビッツ空間

ある条件を満たす幾何的対象(「代数多様体」やその間の「射」など)の分類空間(パラメータ空間)を「モジュライ空間」と言います。モジュライ空間は、しばしばそれ自身が代数多様体(に近いもの)になります。

G を有限群とするとき、射影直線の代数的 G ガロア分岐被覆のモジュライ空間 $H(G)$ は代数多様体(の可算非交和)となり、フルビッツ空間と呼ばれます。このとき、おおざっぱに言うと、

射影直線の代数的 G ガロア被覆で $\mathbb{Q}$ 上に降下するもの

(つまり、 $\mathbb{Q}(t)$ の正則的 G ガロア拡大を定めるもの)

$\rightsquigarrow H(G)$ の $\mathbb{Q}$ 有理点 (座標が全て $\mathbb{Q}$ に入る点)

となりますので、 G が $\mathbb{Q}$ 上正則的に実現可能であることを示すことは、 $H(G)$ の $\mathbb{Q}$ 有理点が存在することを示すことと同値になり、正則逆ガロア問題は原理的にディオファントス幾何（不定方程式論）の問題に帰着されます。

$\mathbb{Q}$ 上では、この手法で正則的实现可能な新しい有限群 G が見付かった例はまだないのではないかと思います。有限体上の正則逆ガロア問題の研究などでこの手法は力を発揮しています。

§6. 遠アーベル幾何

6.1. 無限次ガロア理論

簡単のため K を $\mathbb{Q}$ の拡大体とします。 L/K を体の（有限次とは限らない）拡大とします。

定理. 次の (i)(ii) は同値。

(i) L/K の中間拡大 M/K で有限次ガロア拡大になるものを考えると、そのような M 全ての（集合としての）合併は L に一致する。

(ii) L の任意の拡大体 M と任意の $\sigma \in \text{Aut}(M/K)$ に対し、 $\sigma(L) = L$ 。 $\square$

上記の同値な条件のいずれか（したがって両方）が成立するとき、 L/K をガロア拡大と言い、このとき、 $\text{Aut}(L/K)$ を $\text{Gal}(L/K)$ と記し、 L の K 上のガロア群と呼びます。 L/K が有限次拡大でないときは $\text{Gal}(L/K)$ は有限群になりませんが、「副有限群」という特別な種類の群になり、「位相空間」の構造が入って「位相群」となることがわかります。この場合も、次のようなガロア対応が存在します。

$$\{L/K \text{ の中間拡大体全体} \} \simeq \{G \text{ の「閉」部分群全体} \}$$

$$M \quad \mapsto \quad G(M)$$

$$L^H \quad \longleftarrow \quad H$$

6.2. 絶対ガロア群

任意の体 K に対して、 K の最大ガロア拡大 K^{sep} が（同型を除いて一意的に）存在し、任意のガロア拡大 L/K は、 K^{sep}/K の中間拡大とみなすことができます。 K^{sep} は K の「分離閉包」（あるいは「分離的代数閉包」）として定義され、 K が完全体のとき（例えば K が $\mathbb{Q}$ の拡大体のとき）には、 K^{sep} は K の「代数閉包」 $\bar{K}$ と一致します。 $G_K = \text{Gal}(K^{\text{sep}}/K)$ を

K の絶対ガロア群と言います。これは、体 K から決まる重要な群で、 K のさまざまな情報を含んでおり、今日の整数論・数論幾何学における最も基本的な研究対象の一つとなっています。

特に、有理数体の絶対ガロア群 $G_{\mathbb{Q}}$ は、整数論の重要な研究対象です。現代の整数論のかかなりの部分は、さまざまな観点からの $G_{\mathbb{Q}}$ の研究である、とすら言えると思います。

6.3. ノイキルヒ・内田の定理

ガロア理論の基本定理は、ガロア対応により、体の拡大の様子が群の言葉で完全に記述できることを示しています。しかし、そこに現れる体は、あくまで固定された一つの体の拡大体ばかりです。

遠アーベル幾何の精神は、一種の絶対的なガロア理論であり、ある種の体に対しては、体そのものの様子を群の言葉で完全に記述できるだろうという考えです。特に、一つの体だけでなく、二つの異なる体の上のガロア群の群論的な比較という問題を含みます。

次のノイキルヒ・内田の定理（の弱形）は、遠アーベル幾何の典型的な例を与えています。

定理. K_1, K_2 を代数体とする。このとき、

$$K_1 \simeq K_2 \text{ (体として同型)} \iff G_{K_1} \simeq G_{K_2} \text{ (位相群として同型)} \quad \square$$

通常の $\mathbb{Q}$ 上の（無限次）ガロア理論の帰結として出るのは、

$$K_1 \simeq K_2 \iff G_{K_1} \text{ と } G_{K_2} \text{ が } G_{\mathbb{Q}} \text{ 内で互いに共役}$$

であり、 G_{K_1}, G_{K_2} はあくまで $G_{\mathbb{Q}}$ の部分群としてしか見ていません。その意味で、あくまで $\mathbb{Q}$ 上の相対的なガロア理論であると言えます。一方、ノイキルヒ・内田の定理では、 G_{K_1}, G_{K_2} を抽象的な（位相）群として扱っており、 $G_{\mathbb{Q}}$ の部分群として見ているわけではありません。この意味で「絶対的なガロア理論」を考えていることになります。

ノイキルヒ・内田の定理（あるいはより一般に（体の）遠アーベル幾何）は、体 K の絶対ガロア群 G_K から K 自身を復元する問題と考えることができ、その意味で、（絶対的な）ガロア理論のある種の逆問題を考えている、ということができます。