ガロア理論とその発展

玉川安騎男

§0. はじめに

ガロア理論とは、Evariste Galois (1811-1832) によって創始された、代数方程式の解の置換に関する理論です。その基本定理は「体」と「群」という代数学の基本概念を用いて述べることができ、現在でも整数論の研究の中で最も基本的な道具の１つであり続けています。

この講義では、まず、ガロア理論の基本定理の感じをつかんでもらうことを目標にしたいと思います。次に、ガロア理論の古典的に有名な応用（ギリシャ数学３大難問のうちの角の３等分問題と立方体倍積問題の否定的解決、あるいは、５次以上の方程式の加減乗除とべき根のみを用いた解の公式の非存在の証明、など）の中から題材を選んで解説したいと思います。最後に、遠アーベル幾何など、現代の整数論・数論幾何におけるガロア理論の展開についても紹介したいと思います。

§1. 体

1.1. 数の体系

$$\mathbb{N} = \{ \text{自然数全体} \} = \{(0,)1, 2, \dots\}$$
$$\mathbb{Z} = \{ \text{整数全体} \} = \{0, \pm 1, \pm 2, \dots\}$$
$$\mathbb{Q} = \{ \text{有理数全体} \} = \{a/b \mid a, b \in \mathbb{Z}, b \neq 0\}$$
$$\mathbb{R} = \{ \text{実数全体} \}$$
$$\mathbb{C} = \{ \text{複素数全体} \} = \{a + b\sqrt{-1} \mid a, b \in \mathbb{R}\}$$

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。

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

$$
\begin{aligned}
&+ : K \times K \to K,\ (a,b) \mapsto a+b \\
&- : K \times K \to K,\ (a,b) \mapsto a-b \\
&\times : K \times K \to K,\ (a,b) \mapsto a \times b\ (= a \cdot b = ab) \\
&\div : K \times (K - \{0\}) \to K,\ (a,b) \mapsto a \div b\ (= a/b)
\end{aligned}
$$

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

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

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

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

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

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

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

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

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

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

$$1 \neq 0$$

このとき、K を体と言う。 □

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

例. p を素数とし、$\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ 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する。このとき、$\mathbb{F}_p$ は体となる。(除法の定義は省略。) □

1.3. 多項式

体 K と $n \in \mathbb{N}$ に対し、

$$K[x_1, \ldots, x_n] =$$
$$\{ \sum_{i_1, \ldots, i_n \geq 0} a_{i_1 \ldots i_n} x_1^{i_1} \cdots x_n^{i_n} \mid a_{i_1 \ldots i_n} \in K,\ \forall'(i_1, \ldots, i_n), a_{i_1 \ldots i_n} = 0\}$$

の元を、K 上の（変数 $x_1, \ldots, x_n$ に関する）n 変数多項式と呼びます。2つの多項式の和、差、積はまた多項式になります。

特に、$n = 1$ の場合、（x_1 を x と書いて）

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

となります。

1.4. 線形代数

多くの大学で初年次に実数体 $\mathbb{R}$（及び複素数体 $\mathbb{C}$）上の線形代数を勉強しますが、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

$$+ \colon V \times V \to V,\ (u, v) \mapsto u + v$$
$$- \colon V \times V \to V,\ (u, v) \mapsto u - v$$
$$\cdot \colon K \times V \to V,\ (a, u) \mapsto a \cdot u\ (= au)$$

と元 $o \in V$ が与えられており、次の性質を満たすとする。

$$(u + v) + w = u + (v + w)\ (u, v, w \in V)$$

$$u + v = v + u\ (u, v \in V)$$

$$u + o = u\ (u \in V)$$

$$(u - v) + v = u\ (u, v \in V)$$

$$a(u + v) = au + av,\ a(u - v) = au - av,\ a \cdot o = o\ (a \in K, u, v \in V)$$

$$(a + b)u = au + bu,\ (a - b)u = au - bu,\ 0 \cdot u = o\ (a, b \in K, u \in V)$$

$$(ab)u = a(bu),\ 1 \cdot u = u\ (a, b \in K, u \in V)$$

このとき、V を K 上のベクトル空間（または線形空間）と言う。 □

例. $V = \{o\}$ は K 上のベクトル空間となる。 □

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

例. $n \in \mathbb{N}$ に対し、

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

は K 上のベクトル空間となる。ここで、

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

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

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

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

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。 □

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

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

を考えます。

定義. φ が全射となるような $n \in \mathbb{N}$ 及び $v_1, \ldots, v_n$ が取れるとき、V は有限次元ベクトル空間であると言う。 □

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

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。 □

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。 □

例. $\dim_K(K^n) = n$。 □

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。 □

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がわかります。

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 を有限次拡大と言う。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。 □

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

次の定理は基本的ですが、応用上重要です。

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

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

$$K(\alpha_1, \ldots, \alpha_n) =$$
$$\{f(\alpha_1, \ldots, \alpha_n)/g(\alpha_1, \ldots, \alpha_n) \mid f, g \in K[x_1, \ldots, x_n],\ g(\alpha_1, \ldots, \alpha_n) \neq 0\}$$

とおくと、$K(\alpha_1, \ldots, \alpha_n)$ 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。

1.6. 体の自己同型

K_1, K_2 を体とします。全単射 $\sigma : K_1 \to K_2$ 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 $K \to K$ を K の自己同型と呼びます。$\mathrm{Aut}(K)$ 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 σ 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。$\mathrm{Aut}(L/K)$ 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 の上に演算 $G \times G \to G,\ (x, y) \mapsto x \circ y$ が与えられているとする。このとき、次の公理 I、II、III が満たされれば、G は群であるという。

I. 任意の $x, y, z \in G$ に対し、$(x \circ y) \circ z = x \circ (y \circ z)$
II. $e \in G$ があって、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、$\iota(x) \in G$ があって、$x \circ \iota(x) = \iota(x) \circ x = e$ □

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. II を満たす e はただ一つ定まる。e を G の単位元と言う。各 $x \in G$ に対し、III を満たす $\iota(x)$ はただ一つ定まる。$\iota(x)$ を x の逆元と言う。 □

注. 普通、群の演算は積で表し、$x \circ y$ を xy と記す。このときは、単位元 e を 1、x の逆元 $\iota(x)$ を x^{-1} と記す。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 $-x$ と記す。 □

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 $f : X \to X$ であって、（X の構造を保つ）逆射 $g : X \to X$（すなわち、$f \circ g = g \circ f = \mathrm{id}$）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 $\mathrm{Aut}(X)$ と記す時、$\mathrm{Aut}(X)$ 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 $\mathrm{id} : X \to X$ 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。

以上のことはとても抽象的に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、$\mathrm{Aut}(X)$ は全単射 $X \to X$ 全体の集合で、集合 X 上の対称群と呼ばれる。特に、$n \in \mathbb{N}$、$X = \{1, \ldots, n\}$ のとき、$\mathrm{Aut}(X)$ は n 次対称群と呼ばれ、S_n と記される。 □

例. X を体 K 上のベクトル空間とする。このとき、

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

は X 上の一般線形群と呼ばれ、$GL(X)$（あるいは $GL_K(X)$）と記される。特に、$X = K^n$ のとき、$\mathrm{Aut}(X)$ は n 次一般線形群と呼ばれ、$GL_n(K)$ と記される。 □

ガロア理論で重要なのは、次の例です。

例. (i) 体 K に対し、$\mathrm{Aut}(K)$ は群となり、K の自己同型群と呼ばれる。ここで、演算 $\circ$ は写像の合成により与えられ、単位元は K の恒等写像、逆元は逆写像によってそれぞれ与えられる。
(ii) 体の拡大 L/K に対し、$\mathrm{Aut}(L/K)$ は群となり、L の K 自己同型群と呼ばれる。ここで、演算 $\circ$ は写像の合成により与えられ、単位元は L の恒等写像、逆元は逆写像によってそれぞれ与えられる。 □

2.3. 部分群と商群

定義. 群 G の部分集合 H が

$$x, y \in H \Longrightarrow x \circ y \in H$$

$$e \in H$$

$$x \in H \Longrightarrow \iota(x) \in H$$

を満たすとき、H を G の部分群という。このとき、H は G の演算 $\circ$ を制限することによって群となる。 □

定義. 群 G の部分群 H が、

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

を満たすとき、H を G の正規部分群という。 □

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、

$$x \sim x \text{（反射律）}$$

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

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

さらに、H が G の正規部分群のときは、

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

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。 □

2.4. 群の位数

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

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 $|G|$ の約数である。 □

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 $\alpha_1, \ldots, \alpha_n \in L$ 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 $L = K(\alpha_1, \ldots, \alpha_n)$ が成り立つ。
(ii) L の任意の拡大体 M と任意の $\sigma \in \mathrm{Aut}(M/K)$ 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 $\sigma \in \mathrm{Aut}(M/K)$ が存在し、$\sigma(\alpha) \neq \alpha$。
(iii) $|\mathrm{Aut}(L/K)| = [L : K]$。 □

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 をガロア拡大と言う。この時、$\mathrm{Aut}(L/K)$ を $\mathrm{Gal}(L/K)$ と記し、L の K 上のガロア群と呼ぶ。 □

注. 上記の (i) の中の $\alpha_1, \ldots, \alpha_n$ が相異なるという条件、あるいは (ii) の中の $\sigma(\alpha) \neq \alpha$ という条件は、分離性の条件と呼ばれます。K が「完全体」(例えば、K が有理数体 $\mathbb{Q}$ の拡大体) のときは、これらの分離性の条件は省くことができます。 □

3.2. ガロア対応

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

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。 □

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。

$$\begin{array}{ccc} \{L/K \text{ の中間拡大体全体 }\} & \overset{1:1}{\simeq} & \{G \text{ の部分群全体 }\} \\ M & \mapsto & G(M) \\ L^H & \hookleftarrow & H \end{array}$$

(ii) L/M はガロア拡大で、$G(M) = \mathrm{Gal}(L/M)$ 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、$\mathrm{Gal}(M/K)$ は、商群 $G/G(M) = \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)$ と同一視される。 □

§**4.** ガロア理論の応用

4.1. 作図問題

体と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。講義でこのうちいくつかの解説をできればと思っています。

4.2. 代数方程式論

体と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。群論的準備を要する少し難しい応用が多いのですが、講義でこのうちいくつかの紹介をできればと思っています。

§5. ガロア理論の発展 — 無限次ガロア理論と遠アーベル幾何

5.1. 無限次ガロア理論

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 $\sigma \in \mathrm{Aut}(M/K)$ 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 $\sigma \in \mathrm{Aut}(M/K)$ が存在し、$\sigma(\alpha) \neq \alpha$。 □

上記の同値な条件のいずれか（したがって全て）が成立する時、L/K をガロア拡大と言い、このとき、$\mathrm{Aut}(L/K)$ を $\mathrm{Gal}(L/K)$ と記し、L の K 上のガロア群と呼びます。一般には $\mathrm{Gal}(L/K)$ 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」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。

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

$$M \qquad \mapsto \qquad G(M)$$

$$L^H \qquad \hookleftarrow \qquad H$$

5.2. 絶対ガロア群

任意の体 K に対して、K の最大ガロア拡大体 K^{sep} が（K 上の同型をのぞいて一意的に）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 が有理数体 $\mathbb{Q}$ の拡大体のとき）には、K^{sep} は K の「代数閉包」$\overline{K}$ と一致します。$G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ 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道具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、それ自身が整数論の重要な研究対象です。現代の整数論のかなりの部分は、$G_{\mathbb{Q}}$ のさまざまな観点からの研究とみなせると思います。

5.3. 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。

定義. $\mathbb{Q}$ の有限次拡大体を代数体と言う。 □

定理. K_1, K_2 を代数体とする。この時、

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

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と言うことができます。

5.4. スキームの基本群と遠アーベル幾何

前節で「絶対的ガロア理論」という遠アーベル幾何の精神について、例を挙げて説明しましたが、なぜ「幾何」なのか、なぜ「遠アーベル」なのか、ということについては説明しませんでした。以下これについて説明して本稿を終わりたいと思います。

体の一般化として、環という概念があります。体の定義の中で、除法（$\div$）に関する部分（及び $1 \neq 0$ という条件）を全て削除したものが環の定義になります。（正確には、これは「可換環」の定義ですが、ここでは可換環を単に環と呼ぶことにします。）つまり、環とは、加法、減法、乗法が自由にできるような集合のことを言います。体のほか、整数環 $\mathbb{Z}$ や多項式環 $K[x_1, \ldots, x_n]$、$K[x]$ などが環の例になります。

環の典型的な現れ方として、与えられた空間 X の上の（適当な条件を満たす）関数全体のなす環があります。この場合、関数の値の和、差、積を考えることにより、関数の和、差、積を定義します。（$1, 0$ は、それぞれ恒等的に値 $1, 0$ を取る関数として定義します。）

実は、任意の環はこのようにして得られることが知られています。より正確に言うと、与えられた環 R に対し、アフィンスキームと呼ばれるある種の空間 $\mathrm{Spec}(R)$ が定まり、R は空間 $\mathrm{Spec}(R)$ 上の正則関数全体のなす環と自然に同一視されます。更に、環を考えることとアフィンスキームを考えることは本質的に同等であることが知られています。

一般のスキームは、アフィンスキームをはり合わせることにより定義されます。１９５０年代後半にグロタンディークによって定義されたこのスキームは、代数多様体（$\approx$ 多項式で定義される図形）の概念を大きく一般化するもので、現在の代数幾何学・数論幾何学の基礎をなす概念です。

グロタンディーク自身により、体のガロア理論は、スキームのガロア理論へと一般化されました。この理論で体の絶対ガロア群に当たるものが、スキームの基本群です。絶対ガロア群は、与えられた体の（有限次分離）拡大体全体を統制する副有限位相群でしたが、基本群は、与えられたスキームの（有限エタール）被覆全体を統制する副有限位相群です。スキームの基本群は、通常の位相幾何（トポロジー）で扱う位相空間の基本群の代数的（ないし代数幾何的）な類似と見ることができます。

１９８０年代初頭、グロタンディークは、遠アーベル幾何という新し

い幾何を提唱しました。その基本的な発想の一つは、遠アーベルスキームと呼ばれるある種のスキームの幾何は、その（アーベル群から程遠い）基本群によって完全に決定されるだろう、というものです。

グロタンディークの提唱した形での遠アーベル幾何は、遠アーベルスキームの一般的な定義が見つかっていないなど、理論的にはまだまだ発展途上の状態ですが、既にいくつもの重要な結果が得られています。例えば、ノイキルヒ・内田の定理は、（グロタンディークが遠アーベル幾何を提唱する以前の結果ですが）遠アーベル幾何における一つの基本的な結果となっています。また、近年では、代数曲線やそのモジュライ空間の遠アーベル幾何の研究が、（本研究所を中心に）さまざまな角度から進められ、興味深い結果がいくつも得られています。

このように、１９世紀前半に生まれたガロア理論は、現代もなお強い生命力を持って進化しています。

ガロア理論とその発展 補足プリント

玉川安騎男

２００６年８月１日（火）

1.4. 線形代数（補足）

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 $+, -$ 及び a 倍（$a \in K$）を制限したものが W の $+, -$ 及び 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（補足）

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

$$
\begin{aligned}
&K[\alpha_1, \ldots, \alpha_n] = \\
&\{f(\alpha_1, \ldots, \alpha_n) \mid f \in K[x_1, \ldots, x_n]\} \\
&K(\alpha_1, \ldots, \alpha_n) = \\
&\{\beta/\gamma \mid \beta, \gamma \in K[\alpha_1, \ldots, \alpha_n],\ \gamma \neq 0\}
\end{aligned}
$$

とおくと、$K(\alpha_1, \ldots, \alpha_n)$ 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。（$K(\alpha_1, \ldots, \alpha_n)$ を、K に $\alpha_1, \ldots, \alpha_n$ を付加した体と呼びます。）より詳しく言うと、

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

となっていて、$K(\alpha_1,\dots,\alpha_n)$ は体ですが、$K[\alpha_1,\dots,\alpha_n]$ は一般には体にならず、「環」にしかなりません。

以下 $n=1$ のときを考えます（$\alpha=\alpha_1$）。

定義.
(i) $\varphi\in K[x]$, $\varphi\neq 0$ が存在して $\varphi(\alpha)=0$ となるとき、α は K 上代数的であると言う。
(ii) (i) の φ で、次数が最小のものを α の K 上の最小多項式と言う。 □

命題. $\alpha\in L$ が K 上代数的であるとし、φ をその最小多項式とする。$\psi\in K[x]$ に対し、次が成立する：
(i) $\psi(\alpha)=0$ ならば、ψ は φ で割りきれる。
(ii) $\psi(\alpha)\neq 0$ ならば、$\xi,\eta\in K[x]$ が存在して $\xi\varphi+\eta\psi=1$ が成り立つ。 □

定理. L/K を体の拡大とし、$\alpha\in L$ とする。
(i) L/K が有限次拡大ならば、α は K 上代数的である。
(ii) α が K 上代数的ならば、$K(\alpha)=K[\alpha]$ が成り立ち、$K(\alpha)/K$ は有限次拡大であり、その次数 $[K(\alpha):K]$ は α の K 上の最小多項式の次数に一致する。 □

4.1. 作図問題（補足）

作図問題の数学的定式化

平面 $\mathbb{R}^2=\{(a,b)\mid a,b\in\mathbb{R}\}$ の上の、有限個の点からなる集合 $\mathcal{P}_0$、有限個の直線からなる集合 $\mathcal{L}_0$、有限個の円からなる集合 $\mathcal{C}_0$ が与えられているとします。このとき、点 $Q\in\mathbb{R}$ が $(\mathcal{P}_0,\mathcal{L}_0,\mathcal{C}_0)$ から（初等的）作図可能とは、自然数 n と、各 $i=1,\dots,n$ に対して、$\mathbb{R}^2$ の上の有限個の点からなる集合 $\mathcal{P}_i$、有限個の直線からなる集合 $\mathcal{L}_i$、有限個の円からなる集合 $\mathcal{C}_i$ があって、次をみたすことを言います。

I. 各 $i=1,\dots,n$ に対し、次の (i)-(v) のいずれかが成り立つ。
(i) $\mathcal{P}_i=\mathcal{P}_{i-1}$, $\mathcal{L}_i=\mathcal{L}_{i-1}\cup\{\ell(P,P')\}$, $\mathcal{C}_i=\mathcal{C}_{i-1}$ $(\exists P,P'\in\mathcal{P}_{i-1},\ P\neq P')$。ここで、$\ell(P,P')$ は P,P' を通る（唯一の）直線。
(ii) $\mathcal{P}_i=\mathcal{P}_{i-1}$, $\mathcal{L}_i=\mathcal{L}_{i-1}$, $\mathcal{C}_i=\mathcal{C}_{i-1}\cup\{C(P,P')\}$ $(\exists P,P'\in\mathcal{P}_{i-1},\ P\neq P')$。ここで、$C(P,P')$ は P を中心とし P' を通る（唯一の）円。
(iii) $\mathcal{P}_i=\mathcal{P}_{i-1}\cup(\ell\cap\ell')$, $\mathcal{L}_i=\mathcal{L}_{i-1}$, $\mathcal{C}_i=\mathcal{C}_{i-1}$ $(\exists\ell,\ell'\in\mathcal{L}_{i-1},\ \ell\neq\ell')$。
(iv) $\mathcal{P}_i=\mathcal{P}_{i-1}\cup(\ell\cap C)$, $\mathcal{L}_i=\mathcal{L}_{i-1}$, $\mathcal{C}_i=\mathcal{C}_{i-1}$ $(\exists\ell\in\mathcal{L}_{i-1},C\in\mathcal{C}_{i-1})$。
(v) $\mathcal{P}_i=\mathcal{P}_{i-1}\cup(C\cap C')$, $\mathcal{L}_i=\mathcal{L}_{i-1}$, $\mathcal{C}_i=\mathcal{C}_{i-1}$ $(\exists C,C'\in\mathcal{C}_{i-1},\ C\neq C')$。
II. $Q\in\mathcal{P}_n$。

(上は点 Q の作図可能性でしたが、直線 m の作図可能性や円 D の作図可能性は、上の II を $m \in \mathcal{L}_n$ や $D \in \mathcal{C}_n$ にかえることにより定式化されます。)

例えば、立方体倍積問題は、$\mathcal{P}_0 = \{(0,0),(1,0)\}$, $\mathcal{L}_0 = \emptyset$, $\mathcal{C}_0 = \emptyset$ から $Q = (\sqrt[3]{2}, 0)$ が作図可能かという問題と言えます。

また、角の 3 等分問題は、与えられた $0 \leq \theta < 2\pi$ に対し、$\mathcal{P}_0 = \{(0,0),(1,0),(\cos\theta, \sin\theta)\}$, $\mathcal{L}_0 = \emptyset$, $\mathcal{C}_0 = \emptyset$ から $Q = (\cos\frac{\theta}{3}, \sin\frac{\theta}{3})$ が作図可能かという問題と言えます。

最後に、正 N 角形の作図問題は、$\mathcal{P}_0 = \{(0,0),(1,0)\}$, $\mathcal{L}_0 = \emptyset$, $\mathcal{C}_0 = \emptyset$ から $Q = (\cos\frac{2\pi}{N}, \sin\frac{2\pi}{N})$ が作図可能かという問題と言えます。

体論との関係

さて、$Q \in \mathbb{R}$ が与えられた $(\mathcal{P}_0, \mathcal{L}_0, \mathcal{C}_0)$ から作図可能であるとし、上の条件をみたすような $(\mathcal{P}_i, \mathcal{L}_i, \mathcal{C}_i)$ $(i = 1, \ldots, n)$ を取ります。ここで、

$$K_i = \mathbb{Q}(\mathcal{P}_i, \mathcal{L}_i, \mathcal{C}_i)$$

とおきます。この意味は、K_i は、$\mathbb{Q}$ に、$\mathcal{P}_i$ に属する全ての点 (a,b) に対する a, b、$\mathcal{L}_i$ に属する全ての直線 $y = ax + b$ に対する a, b 及び $x = a$ に対する a、$\mathcal{C}_i$ に属する全ての円 $(x-a)^2 + (y-b)^2 = c$ に対する a, b, c、を全部付加した体ということです。定義により、

$$\mathbb{Q} \subset K_0 \subset K_1 \subset \cdots \subset K_n \subset \mathbb{R}$$

となります。

命題. $[K_i : K_{i-1}] = 1$ または 2 $(i = 1, \ldots, n)$。 □

系. $[K_n : K_0] = 2^r$。 □

ガロア理論とその発展 補足プリント（その２）

玉川安騎男

２００６年８月２日（水）

4.1. 作図問題（補足）（続き）

作図可能性の定式化についての疑問点

疑問１．相異なる点 P, P', R が与えられたとき、R を中心として半径 $|\overrightarrow{PP'}|$ の円を描く操作は許さないのか？

解答１．１．許してもよい。なぜならば、この操作を許しても先の命題（$[K_i : K_{i-1}] = 1$ または 2）が成立するから。（あるいは、より一般に、先の命題が成立するような操作は何でも許してよい。） □

解答１．２．許しても許さなくても同じことになる。つまり、操作 (i)-(v) を組み合わせることにより、この操作は実行可能である。（ユークリッド「原論」に書いてあるそうです。長岡亮介「数学の歴史」pp.31-33 参照。） □

疑問２．「不定の補助点」を取ることは許さないのか？

例．点 P と直線 ℓ が与えられたとき、P を通り ℓ と垂直な直線は作図可能か？ □

例．円 C が与えられたとき、C の中心点は作図可能か？ □

解答２．１．許さなくてよい。実際、立方体倍積問題、角の 3 等分問題、正多角形の作図問題などにおいては、点があらかじめ２つ以上与えられ

ており、十分いろいろな点が作図可能であるので、それ以上の操作は許さなくてもよい。 □

$\mathbb{R}^2$ の上の、有限個の点からなる集合 $\mathcal{P}_0$、有限個の直線からなる集合 $\mathcal{L}_0$、有限個の円からなる集合 $\mathcal{C}_0$ が与えられたとき、操作 (i)-(v) のほかに、平面、(既に作図された) 直線、あるいは (既に作図された) 円のある「領域」(= 空でない「開集合」) 内の補助点を取るという操作を認め、これらの操作を有限回組み合わせることにより、点 Q が得られたとします。(各「領域」は、こちらで自由に設定してよいものとします。) ここで、(平面、直線、または円の) ある領域内の補助点を取るという操作が何回かでてきますが、それぞれの領域内に別の補助点を取ったとしても、それらの取り方によらず最終的に同じ点 Q が得られる場合、点 Q は $(\mathcal{P}_0, \mathcal{L}_0, \mathcal{C}_0)$ から弱作図可能であると言うことにします。(以上の厳密な定式化は、少し煩雑なので省略します。)

このとき、次の定理が成立し、解答２．１が正当化できます。

定理. $\mathcal{P}_0$ に点が２つ以上含まれていると仮定する。このとき、点 Q が作図可能であることと弱作図可能であることは同値である。 □

この定理の証明のポイントは、次の命題にあります。

命題. $\mathcal{P}_0$ に点が２つ以上含まれていると仮定する。このとき、
(i) 作図可能な点全体は $\mathbb{R}^2$ 内で稠密である。
(ii) 直線 ℓ が作図可能なとき、ℓ 上の作図可能な点全体は ℓ 内で稠密である。
(iii) 円 C が作図可能なとき、C 上の作図可能な点全体は C 内で稠密である。 □

<u>立方体倍積問題の作図不可能性</u>

この場合 $K_0 = \mathbb{Q}$ であり、もし作図可能であると仮定すると $\sqrt[3]{2} \in K_n$ となり、$\mathbb{Q}(\sqrt[3]{2}) \subset K_n$ となるはずです。ところが、

命題. $x^3 - 2$ は $\sqrt[3]{2}$ の $\mathbb{Q}$ 上の最小多項式である。 □

系. $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$。 □

により、$3 = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \mid [K_n : \mathbb{Q}] = 2^r$ となり、矛盾します。したがって、立方体倍積問題は作図不可能です。

角の 3 等分問題の作図不可能性

この場合 $K_0 = \mathbb{Q}(\cos\theta, \sin\theta)$ であり、もし作図可能であると仮定すると、特に $\cos\frac{\theta}{3} \in K_n$ となり、$\mathbb{Q}(\cos\frac{\theta}{3}) \subset K_n$ となるはずです。

今、例えば $(\cos\theta_0, \sin\theta_0) = \left(\frac{3}{5}, \frac{4}{5}\right)$ となる θ_0 が与えられたとしましょう。このとき、$K_0 = \mathbb{Q}$ となります。ところが、

命題. $4x^3 - 3x - \frac{3}{5}$ は $\cos\frac{\theta_0}{3}$ の $\mathbb{Q}$ 上の最小多項式である。 □

系. $[\mathbb{Q}(\cos\frac{\theta_0}{3}) : \mathbb{Q}] = 3$。 □

により、$3 = [\mathbb{Q}(\cos\frac{\theta_0}{3}) : \mathbb{Q}] \mid [K_n : \mathbb{Q}] = 2^r$ となり、矛盾します。したがって、角の 3 等分問題は、一般には作図不可能です。

正 N 角形の作図問題

この場合 $K_0 = \mathbb{Q}$ であり、もし作図可能であると仮定すると、特に $\cos\frac{2\pi}{N} \in K_n$ となり、$\mathbb{Q}(\cos\frac{2\pi}{N}) \subset K_n$ となるはずです。ところが、ガロア理論の力を借りると、

命題. $[\mathbb{Q}(\cos\frac{2\pi}{N}) : \mathbb{Q}] = \frac{\varphi(N)}{2}$。 □

が証明できます。但し、φ はオイラーの関数で、$N = p_1^{n_1} \cdots p_r^{n_r}$（$p_1, \ldots, p_r$ は相異なる素数、$n_i > 0$）に対し、$\varphi(N) = (p_1^{n_1} - p_1^{n_1-1}) \cdots (p_r^{n_r} - p_r^{n_r-1})$ となります。これより、

$$\text{正 } N \text{ 角形が作図可能} \implies N = 2^m p_1 \cdots p_r,\ m \geq 0,\ p_1, \ldots, p_r \text{ は相異なるフェルマ素数 } (p_i = 2^{s_i} + 1,\ s_i > 0)$$

が従います。

実は、ガロア理論の力を借りると、逆も成立することが証明できます。

ガロア理論とその発展 補足プリント（その３）

玉川安騎男

２００６年８月３日（木）

3.1. ガロア拡大（補足）

ガロア拡大の例

例. $a \in \mathbb{Q}$ に対し、$\mathbb{Q}(\sqrt{a})/\mathbb{Q}$ はガロア拡大。 □

例. $N \in \mathbb{N}$ に対し $\zeta_N = e^{\frac{2\pi\sqrt{-1}}{N}}$ とおく。（ζ_N は「1 の原始 N 乗根」である。）このとき、$\mathbb{Q}(\zeta_N)/\mathbb{Q}$ はガロア拡大。また、$\mathbb{Q}(\cos\frac{2\pi}{N})/\mathbb{Q}$ もガロア拡大。更に、$\mathbb{Q}(\zeta_N)/\mathbb{Q}(\cos\frac{2\pi}{N})$ もガロア拡大。 □

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

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

4.2. 代数方程式論（補足）

代数学の基本定理

定義. K を体とする。任意の $f \in K[x],\ \deg(f) > 0$ に対して方程式 $f(x) = 0$ が K 内に解を持つとき、K を代数閉体という。 □

定理. 複素数体 $\mathbb{C}$ は代数閉体である。 □

この定理の証明は位相幾何的なもの、複素関数論的なもの、などいろいろ知られていますが、この講義では、ガロア理論を用いた群論的な証明を紹介します。出発点は、次の２つの（高校数学の範囲内で証明が理解できる）命題です。

命題. $\mathbb{R}$ 上の任意の奇数次方程式は $\mathbb{R}$ 内に解を持つ。

証明. 中間値の定理を用いる。 □

命題. $\mathbb{C}$ 上の任意の 2 次方程式は $\mathbb{C}$ 内に解を持つ。

証明. 解の公式を用いる。 □

あとは、有限群論における次の重要な定理（シローの定理の一般化）を用います。

定理. G を有限群、p を素数、r を自然数とする。このとき、$p^r \mid |G|$ ならば、G の部分群 H で $H = p^r$ となるものが存在する。 □

代数方程式の加減乗除とべき根のみを用いた解法

K を体、$f \in K[x]$ とし、簡単のため f の最高次係数は 1 とします。このとき、K の有限次拡大体 L で、$\alpha_1, \ldots, \alpha_n \in L$ が存在し、$L[x]$ において分解

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

が成立し、しかも $L = K(\alpha_1, \ldots, \alpha_n)$ が成り立つようなものが、（本質的に一意的に）存在します。（L を f の K 上の最小分解体と呼びます。）K が完全体ならば、L/K はガロア拡大になるので、$G = \mathrm{Gal}(L/K)$ とおき、方程式 $f(x) = 0$ の K 上のガロア群と呼びます。このとき、次が成立します。

定理. 次の (i)(ii) は同値。
(i) f の根 $\alpha_1, \ldots, \alpha_n$ が、K の元から加減乗除とべき根（累乗根）を取ることを有限回繰り返して得られる。
(ii) G は可解群。 □

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 $i = 1, \ldots, n$ に対して商群 H_{i-1}/H_i がアーベル群となるとき、G は可解群であると言う。 □

n 次方程式のガロア群は n 次対称群 S_n の部分群とみなせます。上の定理と次の有限群論における命題が、方程式の加減乗除とべき根による解法の理論における鍵となります。

命題. (i) $n \leq 4$ のとき、S_n は可解群である。(したがって、S_n の任意の部分群も可解群である。)
(ii) $n \geq 5$ のとき、S_n は非可解群である。 □

命題の (i) により、4 次以下の方程式は加減乗除とべき根のみを用いて解けることがわかります。一方、$n \geq 5$ のとき、$\mathbb{Q}$ 上の n 次方程式でガロア群が S_n に一致するものが構成できます。命題の (ii) により、このような方程式は加減乗除とべき根のみを用いては解けないことがわかります。

ガロアの逆問題

上で見たように、方程式が与えられると、そのガロア群を考えることができます。逆に、次のような問題が考えられます。

問題. 有限群 G が与えられたとき、$\mathbb{Q}$ 上の方程式で、その $\mathbb{Q}$ 上のガロア群が G (と同型) になるものが存在するか? □

この問題は、ガロアの逆問題と呼ばれます。見かけは単純ですが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。