代数学概論III演習——一体のガロア理論

黒木 玄　(東北大学大学院理学研究科数学専攻)

2002年11月12日(火)

目 次

3　分離性と被約性 **36**

4　Galois 対応 **39**

5　方程式の Galois 群 **41**

6　Galois 理論の演習問題 **43**

7　お話: 数と函数の世界 **44**

3　分離性と被約性

二項係数は次のように定義される:

$$\binom{\alpha}{k} = \frac{\alpha(\alpha-1)\cdots(\alpha-n+1)}{k!} \quad (k = 0, 1, 2, \ldots).$$

ただし, $0! = 1$, $\binom{\alpha}{0} = 1$. $\alpha \in \mathbb{Z}_{\geq 0}$ のとき $k > \alpha$ ならば $\binom{\alpha}{k} = 0$.

[129] (一般化された二項定理)　$(1+x)^\alpha = \sum_{k=0}^{\infty} \binom{\alpha}{k} x^k$　$(|x| < 1,\ \alpha \in \mathbb{C})$. □

[130] p が素数で $k = 1, \ldots, p-1$ ならば $\binom{p}{k}$ は p で割り切れる. □

[131] p が素数で $e \in \mathbb{Z}_{\geq 0}$ で, a が p と素な自然数であるとき,

$$\binom{p^e a}{p^e} \equiv a \mod p.$$

(ヒント: $(1+x)^{p^e a} = (1+x^{p^e})^a) \mod p$ by **[130]**.) □

注意 3.1 **[131]** の結果は Sylow の定理の証明の中で使われた (cf. [Mo] p. 47).

[132] R は可換環であり, 素数 p について p 個の 1 の R における和が 0 になると仮定する. このとき, $R \to R$, $a \mapsto a^p$ は環の準同型である. □

[133] K は正標数 p の体であるとし, $q = p^e$, $e \in \mathbb{Z}_{\geq 0}$, $a \in K$ であるとする. K の代数閉包 $\overline{K}$ の元 α で $\alpha^q = a$ となるものをとる. このとき, $\overline{K}[x]$ の中で $x^q - a = (x-\alpha)^q$ が成立する. □

[134] k は正標数 p の体であるとし, $q = p^e$, $e \in \mathbb{Z}_{\geq 0}$ であるとし, k 上の 1 変数有理函数体 $K = k(t)$ を考える. このとき, $L = k(t^{1/q})$ は $x^q - t$ の根体でかつ最小分解体であり, L/K は純非分離拡大である. □

以下, 可換環 R において $f_1, \ldots, f_n$ から生成されるイデアルを $(f_1, \ldots, f_n)_R$ と書くことにする.

[135] K を体とし, $f \in K[x]$ とし, L は K の拡大体であるとする. このとき,

$$L \otimes_K \big(K[x]/(f)_{K[x]}\big) \cong L[x]/(f)_{L[x]}.$$

特に問題 **[134]** の状況において,

$$L \otimes_K L \cong L[x]/\big((x - t^{1/q})^q\big)_{L[x]}. \quad \square$$

定義 3.2 (被約 (reduced)) 可換環 R の元 a が巾零 (nilpotent) であるとは, ある $n = 1, 2, \ldots$ が存在して $a^n = 0$ が成立することである. R の巾零元の全体を $\sqrt{0} = \{\, a \in R \mid a \text{ は巾零} \,\}$ と書き, R の巾零根基 (nilpotent radical) と呼ぶ.

R が 0 以外の巾零元を持たない (すなわち $\sqrt{0} = 0$) とき, R は被約 (reduced) であるという. □

[136] 可換環 R の巾零根基は R のイデアルであり, $R/\mathfrak{a}$ が reduced になるような R のイデアル $\mathfrak{a}$ の中で最小である. □

[137] 整域は reduced である. A と B が reduced な可換環であるとき $A \times B$ もそうである. □

[138] $m = p_1^{e_1} \cdots p_n^{e_n}$ は自然数 m の素因数分解であるとする. すなわち, p_i は互いに異なる素数で, $e_1, \ldots, e_n$ は正の整数であるとする. このとき, $\mathbb{Z}/(m)$ が reduced であるための必要十分条件は $e_1 = \cdots = e_n = 1$ が成立していることである. (ヒント: $\mathbb{Z}/(m) \cong \mathbb{Z}/(p_1^{e_1}) \times \cdots \times \mathbb{Z}/(p_n^{e_n})$.) □

定義 3.3 (分離性 (separability)) A は体 K 上の可換代数 (すなわち K を含む可換環) であるとする. A が K 上分離的 (separable over K) であるとは, K の任意の拡大体 K' に対して, $K' \otimes_K A$ が reduced になることである[31]. □

[139] 以下を示せ:

(1) K 上の分離的可換代数の K 部分代数も分離的である.

[31] K' 上の可換代数 $K' \otimes_K A$ は次のようにして構成可能である. A の K 基底 $\{a_i\}$ を任意に取る. $\{a_i\}$ を基底に持つ K' 上のベクトル空間を $K' \otimes_K A$ と書く. $K' \otimes_K A$ の K 上の可換代数は K' 基底 a_i たちの積が与えられれば決まる. しかし, a_i たちの積は A における積として決まっている. よって, $K' \otimes_K A$ には自然に K' 上の可換代数の構造が入る.

(2) A は K 上分離的 $\iff$ K 上有限生成な A の任意の部分代数が K 上分離的.

(3) A は K 上分離的 $\iff$ K の任意の有限生成拡大体 K' に対して $K' \otimes_K A$ は reduced.

(4) A が K 上分離的ならば K の任意の拡大体 K' に対して $K' \otimes_K A$ は K' 上分離的である. □

[140] A が体 K の代数拡大体であるとき, 次の 2 つの条件は互いに同値である:

(a) A は 定義 3.3 の意味で分離的である.

(b) A は体論の意味で分離的である. すなわち, A の全ての元が重根を持たない K 係数多項式の根になる.

(ヒント: (a) $\implies$ (b). 対偶を示す. (b) でないならば, ある $a \in A$ と a を根に持つ既約多項式 $f \in K[x]$ で重根を持つものが存在する. A の部分代数 $K[a]$ は $K[x]/(f)_{K[x]}$ に同型である. f の最小分解体 K' に対して, $K' \otimes_K K[a] \cong K'[x]/(f)_{K'[x]}$. この右辺は reduced でない. よって, **[139]** (2) より, A は 定義 3.3 の意味で分離的ではない.
(b) $\implies$ (a). **[139]** (2) より, A は K の有限次分離拡大体であると仮定して良い. 有限次分離拡大体は単拡大であるという定理 (たとえば [Mo] 第 V 章の定理 4.9 (p. 201)) より, 重根を持たない既約多項式 $f \in K[x]$ が存在して, $A \cong K[x]/(f)_{K[x]}$. K の拡大体 K' に対して, $K' \otimes_K A \cong K'[x]/(f)_{K'[x]}$. f は重根を持たないので, この右辺は reduced である.) □

[141] 有限体の乗法群は巡回群である. □

[142] 体の有限次分離拡大体は単拡大である. □

[143] $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ である. (ヒント: $1/(\sqrt{2} + \sqrt{3})$ の分母を有理化してみよ.) $\sqrt{2} + \sqrt{3}$ の $\mathbb{Q}$ 上での最小多項式を求めよ. (ヒント: $\pm\sqrt{2} \pm \sqrt{3}$ ($\pm$ の組み合わせは 4 通りを考える) を根に持つ多項式を考えてみよ.) □

[144] $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3} - \sqrt{5})$ である. $\sqrt{3} - \sqrt{5}$ の $\mathbb{Q}$ 上での最小多項式を求めよ. □

[145] $K = \mathbb{C}(t)$ のとき, $K(\sqrt{t}, \sqrt{t+1}) = K(\sqrt{t} + \sqrt{t+1})$. □

[146] K は体であるとし, $f \in K[x]$ とする. f が 1 次以上で重根を持たなければ, $K[x]/(f)$ は reduced である. □

定義 3.4 (完全体 (perfect field)) 体 K が完全体 (perfect field) であるとは, K の任意の代数拡大が K 上分離的になることである. □

[147] K が正標数 p であるとき, 以下の条件は互いに同値である:

(a) K は完全体である.

(b) $K^{p^{-1}} = K$.

(c) $F_p : K \to K$, $a \mapsto a^p$ は全射である.

ここで, $K^{p^{-e}} = \{\theta \in \overline{K} \mid \theta^{p^e} \in K\}$. □

[148] 標数 0 の体は完全体である. □

[149] 有限体は完全体である. □

[150] k が正標数の体であるとき, k 上の 1 変数有理函数体 $K = k(t)$ は完全体ではない. (ヒント: 問題 **[134]**.) □

4 Galois 対応

体 L に対して, L の体としての自己同型全体のなす群を $\mathrm{Aut}\, L$ と書く. $\mathrm{Aut}\, L$ の部分群 G に対して,

$$L^G := \{\, x \in L \mid \sigma(x) = x \ \forall \sigma \in G \,\}$$

を G の不変体 (invariant field) と呼ぶ. 体の拡大 L/K に対して,

$$\mathrm{Aut}(L/K) := \{\, \sigma \in \mathrm{Aut}\, L \mid \sigma(x) = x \ \forall x \in K \,\}.$$

[151] 体 L の部分体 M, N に対して,

$$M \subset N \implies \mathrm{Aut}(L/M) \supset \mathrm{Aut}(L/N). \quad \square$$

[152] 体 L と $\mathrm{Aut}\, L$ の部分群 G に対して, $\mathrm{Aut}(L/L^G) \supset G$. □

[153] 体 L と L の部分体 K に対して, $L^{\mathrm{Aut}(L/K)} \supset K$. □

[154] **(正規拡大)** L/K は代数拡大であるとする. このとき, $\overline{L} = \overline{K}$ であり, 以下の条件は互いに同値である:

(a) L の任意の拡大体 M に対して, M の中間体で L と K 同型なものは L に限る.

(b) 任意の $\sigma \in \mathrm{Aut}(\overline{K}/K)$ に対して $\sigma L = L$.

(c) K 上既約な多項式 $f \in K[x]$ が L において根を持てば, f は L において 1 次式の積に分解される.

以上の同値な条件のどれかが成立しているとき, 代数拡大 L/K は正規拡大 (normal extension) であると言う. □

[155] K の代数拡大 L, M が共に K 上正規であるとき, $L \cap M$ と LM も K 上正規になる. □

[156] 代数拡大 L/K が正規であり, M がその中間体であるとき, M から $\overline{K}$ の中への K 同型[32] σ は, $\overline{\sigma}(L) = L$ を満たす $\overline{\sigma} \in \mathrm{Aut}(\overline{K}/K)$ に拡張される. □

[32] K の任意の元を固定する M から $\overline{K}$ への環準同型のこと. 常に単射になる.

[157] 有限次拡大 L/K が正規拡大になるための必要十分条件は, L がある多項式 $f \in K[x]$ の最小分解体になることである. □

[158] 任意の有限次拡大 L/K に対してある有限次正規拡大 M/K で $L \subset M$ をみたすものが存在する. □

定義 4.1 (Galois 拡大) 代数拡大 L/K が Galois 拡大であるとは正規かつ分離的であることである. L/K が Galois 拡大のとき, $\mathrm{Gal}(L/K) = \mathrm{Aut}(L/K)$ と置き, それを L/K の Galois 群と呼ぶ. □

[159] (E. Artin) L は体であるとし, G は $\mathrm{Aut}\, L$ の有限部分群であるとし, $K = L^G$ と置く. このとき, L/K は有限次 Galois 拡大であり, $\mathrm{Gal}(L/K) = G$ かつ $[L : K] = |G|$ となる[33]. □

[160] L/K が代数拡大であるとき,

$$L/K \text{ は Galois 拡大} \iff L^{\mathrm{Aut}(L/K)} = K. \quad \square$$

[161] (Galois の基本定理) L/K が体の有限次 Galois 拡大であるとき, L/K の中間体 M と $\mathrm{Gal}(L/K)$ の部分群 H が $H = \mathrm{Gal}(L/M)$, $M = L^H$ によって一対一に対応する. この対応を Galois 対応と呼ぶ. □

この節の以下の問題の解答において, この節の以上の問題の結果を自由に用いて構わない.

[162] Galois 対応は包含関係を逆転させる. □

[163] 体 L の部分体 M と $\sigma \in \mathrm{Aut}\, L$ に対して,

$$\mathrm{Aut}\left(L/\sigma(M)\right) = \sigma^{-1}\,\mathrm{Aut}(L/M)\sigma.$$

ここで, $\sigma(M) = \{\, \sigma(x) \mid x \in M \,\}$. □

[164] L/K が体の有限次 Galois 拡大であるとき, L に含まれる K の正規拡大 (よって Galois 拡大) と $\mathrm{Gal}(L/K)$ の正規部分群が Galois 対応によって一対一に対応する. さらに, L に含まれる K の正規拡大 M に対して, 制限写像

$$\mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K), \quad \sigma \mapsto \sigma|_M$$

は次の同型を誘導する:

$$\mathrm{Gal}(L/K)/\,\mathrm{Gal}(L/K) \xrightarrow{\sim} \mathrm{Gal}(M/K). \quad \square$$

定義 4.2 (Abel 拡大) L/K が Galois 拡大で $\mathrm{Gal}(L/K)$ が Abel 群であるとき, L/K は Abel 拡大であるという. □

[33] $|G|$ は有限群 G の位数 (元の個数) である.

[165] L/K が有限次 Abel 拡大であるとき, その任意の中間体は K の有限次 Abel 拡大になる. □

[166] (E. Artin) $\chi_1, \ldots, \chi_m$ を半群 S から体 K の乗法群 $K^\times$ への相異なる半群の準同型であるとする. このとき, $\alpha_1, \ldots, \alpha_m \in K$ が

$$\chi_1(s)\alpha_1 + \cdots + \chi_m(s)\alpha_m = 0 \quad (\forall s \in S)$$

をみたしているならば, $\alpha_1 = \cdots = \alpha_m = 0$. □

定義 4.3 (束 (lattice)) 順序集合 $(X, \leq)$ が束 (lattice) であるとは, それが最小限と最大限を持ち, 任意の $x, y \in X$ に対して, x と y の上限 $x \vee y$ と下限 $x \wedge y$ が X の中に存在することである. □

[167] 体の拡大 L/K に対して, その中間体 (intermediate field) 全体の集合を $\mathrm{Int}(L/K)$ と書くことにする. このとき, $(\mathrm{Int}(L/K), \subset)$ は束であり, $M, N \in \mathrm{Int}(L/K)$ に対して,

$$M \vee N = MN, \qquad M \wedge N = M \cap N. \quad \square$$

[168] 群 G に対して, その部分群全体の集合を $\mathrm{Sub}\, G$ と書くことにする. このとき, $(\mathrm{Sub}\, G, \subset)$ は束であり, $H, F \in \mathrm{Sub}\, G$ に対して,

$$H \vee F = \langle H, F \rangle, \qquad H \wedge F = H \cap F.$$

ここで, $\langle H, F \rangle$ は H と F から生成される G の部分群である. □

[169] 束のあいだ[34]の写像 $\phi : X \to Y$ が順序を逆転させる全単射であるとき, $x, x' \in X$ に対して, $\phi(x \vee x') = \phi(x) \wedge \phi(x')$ が成立する. 以上の結果を Galois 対応に適用すると, L/K が有限次 Galois 拡大であるとき, L/K の中間体 M, N に対して,

$$\mathrm{Gal}(L/MN) = \mathrm{Gal}(L/M) \cap \mathrm{Gal}(L/N),$$
$$\mathrm{Gal}(L/M \cap N) = \langle \mathrm{Gal}(L/M), \mathrm{Gal}(L/N) \rangle$$

であり,

$$L^{\langle H,F \rangle} = L^H \cap L^F, \quad L^{H \cap F} = L^H L^F. \quad \square$$

[170] L/K が体の拡大であるとき,

L/K は有限次 Galois 拡大 $\iff$ L は K 上のある分離的多項式の最小分解体. □

5 方程式の Galois 群

定義 5.1 (方程式の Galois 群) 体 K 上の分離的多項式 $f \in K[x]$ の最小分解体を L とするとき, $\mathrm{Gal}(L/K)$ を方程式 $f(x) = 0$ の Galois 群と呼ぶ. □

[34]「あいだ」を「間」と書くと「束の間」 (つかのま) になってしまう.

[171] L は体 K 上の分離的多項式 f の最小分解体であるとする. このとき, $\mathrm{Gal}(L/K)$ は f の根全体の集合の置換群の部分群とみなせる. □

この節の以下の問題の解答において **[171]** の結果を自由に用いて良い.

[172] L は $f(x)=x^3-5$ の $\mathbb{Q}$ 上での最小分解体であるとする. このとき, $L=\mathbb{Q}(\sqrt{-3},\sqrt[3]{5})$ であり, $\mathrm{Gal}(L/\mathbb{Q})\cong S_3$, $\mathrm{Gal}\left(L/\mathbb{Q}(\sqrt{-3})\right)$, $\mathrm{Gal}\left(\mathbb{Q}(\sqrt{-3})/\mathbb{Q}\right)\cong\mathbb{Z}/2\mathbb{Z}$. □

[173] L は $K=\mathbb{C}(t)$ のとき, $f(x)=x^3-t\in K[x]$ の K 上での最小分解体であるとする. このとき, $L=K(\sqrt[3]{t})$ であり, $\mathrm{Gal}(L/K)\cong\mathbb{Z}/3\mathbb{Z}$. □

[174] 体 k 上の n 変数有理函数体を $L=k(t_1,\dots,t_n)$ と書き, $t_1,\dots,t_n$ の基本対称式 $s_1,\dots,s_n$ を

$$\begin{aligned} f(x) &:= (x-t_1)\cdots(x-t_n) \\ &= x^n - s_1x^{n-1} + s_2x^{n-2} - \cdots + (-1)^{n-1}s_{n-1}x + (-1)^n s_n \end{aligned}$$

によって定める. すなわち,

$$s_k = \sum_{1\le i_1<\cdots<i_k\le n} t_{i_1}\cdots t_{i_k}.$$

L の部分体 K を $K=k(s_1,\dots,s_n)$ と定める. このとき, L は $f(x)\in K[x]$ の最小分解体となり, $\mathrm{Gal}(L/K)\cong S_n$ が成立する. □

[175] $\mathbb{C}$ が代数閉体であることを, 中間値の定理と純代数的な議論だけを用いて証明せよ. 複素函数論を用いてはいけない. (ヒント: [Mo] p. 211 の定理 5.9 の証明.) □

[176] K は体であるとし, $f\in K[x]$ は K 上分離的であり, L は f の最小分解体であるとする. $f=gh$, $g,h\in K[x]$ であり, M, N はそれぞれ L に含まれる g, h の分解体であるとする. このとき, $M\cap N=K$ であれば, 同型

$$\mathrm{Gal}(L/K)\cong\mathrm{Gal}(M/K)\times\mathrm{Gal}(N/K)$$

が成立する. □

注意 5.2 **[176]** の状況のもとで, $[MN:M]=[N:K]$ が成立することがすぐにわかるので, **[116]** より M と N は K 上線形無関連である. □

[177] $g(x)=x^2+3$, $h(x)=x^3-1$ と定める. このとき, $\mathbb{C}$ に含まれる g の分解体と h の最小分解体は等しい. □

[178] L/K が有限次 Galois 拡大であるとき, L/K の中間体 M, N に対して,

$$[MN:L]=[\mathrm{Gal}(L/K):\mathrm{Gal}(L/M)\cap\mathrm{Gal}(L/N)].$$ □

[179] L/K は有限次 Galois 拡大であり, M, N はその中間体で, $[M:N]=2^a$, $[N:K]=2^b$ であっても, $[MN:K]$ が 2 の巾になるとは限らないことを示せ. (**[178]** を使う. S_4 の部分群 H, H' を $H=\{\,\sigma\in S_4\mid\sigma(4)=4\,\}$, $H'=\{\,\sigma\in S_4\mid\sigma(1)=1\,\}$ と定めると, $[S_4:H]=[S_4:H']=4$ であるが, $[S_4:H\cap H']=12$ である. よって, $\mathrm{Gal}(L/K)=S_4$ であれば **[178]** を用いて反例を構成できる.) □

[180] (判別式 (discriminant)) K は体であるとし, $f \in K[x]$ の最小分解体を L と書く. このとき, f は $L[x]$ において,

$$f(x) = a(x-\alpha_1)\cdots(x-\alpha_n) \quad (\alpha_i \in L,\ a \in K^\times)$$

と分解する. f の判別式 $D(f)$ を次のように定義する:

$$D(f) := \prod_{1\le i<j\le n} (\alpha_i - \alpha_j)^2.$$

このとき, $D(f) \in K[x]$. □

注意 5.3 $D(f)$ は $\alpha_1, \ldots, \alpha_n$ の差積 (difference product) の 2 乗に等しい. □

[181] $f(x) = ax^2 + bx + c$ $(a \neq 0)$ のとき, $D(f) = \dfrac{b^2 - 4ac}{a^2}$. □

[182] $f(x) = x^3 + ax + b$ のとき, $D(f) = -4a^3 - 27b^2$. □

[183] $f(x) = x^4 + ax^2 + bx + c$ のとき,

$$D(f) = 16a^4c - 4a^3b^2 - 128a^2c^2 + 144ab^2c - 27b^4 + 256c^3.$$ □

[184] K は体であるとし, $f \in K[x]$ は分離的であり, L はその最小分解体であるとすると以下の 2 つの条件は互いに同値である:

(a) f は K 上の既約多項式である.

(b) $\mathrm{Gal}(L/K)$ は f の根全体に推移的に作用する.

(ヒント: (a) $\Longrightarrow$ (b). f が K 上既約であるとき, f の任意の根 α, β に対して, K 同型 $K(\alpha) \cong K(\beta)$ が存在する. この同型は L の同型に拡張可能である.
(b) $\Longrightarrow$ (a). f が K 上既約でないとき, $f = gh$, $(g, h \in K[x], \deg g, \deg h \geq 1)$ と分解する. 任意の $\sigma \in \mathrm{Gal}(L/K)$ は g の根を g の根に, h の根を h の根にうつす. f は分離的なので g と h は共通根を持たないので, $\mathrm{Gal}(L/K)$ の f の根全体への作用は推移的ではない.) □

6 Galois 理論の演習問題

[185] $\mathbb{R}$ の代数拡大は $\mathbb{R}$ と $\mathbb{C}$ 以外に存在しない. $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$ である. □

[186] (有限体の性質のまとめ) p は素数であるとし, $e = 1, 2, \ldots$, $q = p^e$ とする.

(1) 位数 q の有限体 $\mathbb{F}_q$ が同型を除いて唯一存在する.

(2) $\{\, a \in \overline{\mathbb{F}_q} \mid a^{q^m} = a \,\}$ は位数 q^m の有限体である. それを $\mathbb{F}_{q^m}$ と書く.

(3) $\mathbb{F}_{q^m}$ は分離多項式 $x^q - x \in \mathbb{F}_q[x]$ の最小分解体である.

(4) $\mathbb{F}_{q^m}/\mathbb{F}_q$ は m 次の Galois 拡大であり, $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) = \langle F \rangle \cong \mathbb{Z}/m\mathbb{Z}$. ここで, $F : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$ は $F(a) = a^q$ と定義された Frobenius 写像である.

(5) $\overline{\mathbb{F}_q}$ に含まれる $\mathbb{F}_q$ の m 次拡大は $\mathbb{F}_{q^m}$ に等しい.

(6) k は m の約数であるとする. F^k で固定される $\mathbb{F}_{q^m}$ の元の全体を $(\mathbb{F}_{q^m})^{F^k}$ と書くと, $(\mathbb{F}_{q^m})^{F^k} = \mathbb{F}_{q^k}$.

以上のように有限体の有限次拡大の様子は非常によくわかる. □

参考 6.1 $\mathbb{R}$ や $\mathbb{F}_q$ の有限次拡大の様子は完全によくわかる. しかし, $\mathbb{Q}$ に関する同じ問題は数論におけるおそるべき難問である. □

[187] $\mathbb{Q}(\sqrt{2}+\sqrt{3})/\mathbb{Q}$ が Galois 拡大であることを示し, $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}+\sqrt{3})/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$ を証明し, その非自明な中間体の全体は $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{6})$ である. □

[188] $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})/\mathbb{Q}$ は 6 次の Galois 拡大であり, で $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})/\mathbb{Q}) \cong S_3$. (ヒント: $\omega = \exp(2\pi\sqrt{-1}/3)$ と置くと $\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$.) □

[189] 4 次の対称群 S_4 の (1234), (24) から生成される部分群を D_4 と書くと, D_4 の位数が 8 になることを示せ[35]. $K = \mathbb{Q}(\sqrt[4]{2}, \sqrt{-1})$ が $\mathbb{Q}$ 上の既約多項式 $x^4 - 2 \in \mathbb{Q}[x]$ の最小分解体であることを示し, $\mathrm{Gal}(K/\mathbb{Q}) \cong D_4$ であることを示せ. □

[190] K は 1 の原始 n 乗根 ζ を含む体とする. このとき, n は K の標数 p で割り切れない. □

[191] (Kummer 拡大の特殊な場合) K は 1 の原始 n 乗根 ζ を含む体とする. $1 \neq a \in K$ とし, r は a^r が K の元の n になるような最小の正の整数であるとする. このとき, $x^n - a$ の根の 1 つを α とすると, $K(\alpha)$ は $x^n - a$ の最小分解体であり, $\mathrm{Gal}(K(\alpha)/K) \cong \mathbb{Z}/r\mathbb{Z}$ が成立する. □

7 お話: 数と函数の世界

「数や函数にはどのようなものがあるだろうか?」という問題は, 皆によって基本的な数学の問題であったはずである.

小学生のときに $1, 2, 3, \ldots$ という自然数について習い, さらに 0 やマイナスの数 $-1, -2, -3, \ldots$ についても習うことになる. 分数や小数について習い (有理数の存在を知る), ついには円周率 $\pi = 3.141592653\cdots$ のようなおそろしい数についても習うことになる. そして, $\sqrt{2}$ が無理数であることを中学か高校あたりで習い, 有理数と実数の世界の違いについて知ったはずである. そして, 複素数についても習うことになる. 実係数の 2 次方程式は実数の範囲内では必ずしも解けないが, 数の体系を複素数まで拡張すればいつでも解けるのである. この事実は一般の n 次方程式まで拡張される (代数学の基本定理). 我々は今現在, 有

[35] D_4 は **[43]** で定義した $n = 4$ の場合の二面体群 (dihedral group) と $a = (1234)$, $b = (24)$ によって同一視できる. 一般に, $a = (12\cdots n)$ とし, b を 1 を固定し $2, \ldots, n$ に関しては k と $n+2-k$ を交換する置換とみなすことによって, D_n は S_n の部分群とみなせる.

理数係数の一般の n 次方程式の根を $\mathbb{Q}$ に付け加えた数の体系を体の Galois 理論の題材として扱っているのである.

これと同様のストーリーを函数についても述べることができる. 小学校の高学年のときに, 二つの数が互いに関係していることの重要性を習ったはずである. そして, そのグラフを描くことの重要性を知ったはず. そして, 中学校では文字式について習うことになる. 一番簡単なのは $ax+b$ の型の一次函数である. そして, ax^2+bx+c という二次函数についても習うことになる. 一般に多項式分の多項式の形の函数は有理函数と呼ばれている. 有理函数は函数の世界における有理数の類似物である. 有理函数でない函数 (すなわち無理函数) の例として, $\sqrt{x}$ のような函数が存在する. これは $\sqrt{2}$ のような無理数の函数の世界における類似物である. 高校に入ると, $\cos x$ や $\sin x$ のような三角函数についても習うことになる. 三角函数は e^x や $\log x$ と同じく超越函数である. 超越函数は函数の世界における超越数 (たとえば π, e など) の類似物である. そして, 大学ではさらに難しい函数を習うことになる.

「数や函数の世界がどのような様子をしているか?」という問題, もしくは「数や函数の世界ではどのような面白いことが起こっているか?」という問題は現代の数学研究においても基本的な問題である.

基本的な数の世界は, 有理整数 $0, \pm1, \pm2, \ldots$ の世界から出発して, 商体を作る操作と代数方程式の根を付け加える操作と完備化する操作の繰り返しによって構成される数の世界である.

たとえば, $\mathbb{Z}$ の商体 $\mathbb{Q}$ を考え, その絶対値 $|\ |$ に関する完備化を構成すると実数体 $\mathbb{R}$ ができる. $\mathbb{R}$ の非自明な代数拡大体は $\mathbb{C}$ しか存在しない. これが $\mathbb{Z} \to \mathbb{Q} \to \mathbb{R} \to \mathbb{C}$ という経路である.

$\mathbb{Q}$ の完備化は $\mathbb{R}$ 以外にも存在する. $\mathbb{Q}$ の $\mathbb{R}$ 以外の完備化は各素数 p ごとに存在し, $\mathbb{Q}_p$ と表わされ, p 進数体と呼ばれている. 集合として, $\mathbb{Q}_p$ を次のように表わすことができる:

$$\mathbb{Q}_p = \{\, a_N p^N + a_{N+1}p^{N+1} + a_{N+2}p^{N+2} \mid N \in \mathbb{Z},\ a_i = 0, 1, \ldots, p-1 \,\}.$$

N は負の整数でも良いことに注意せよ. すなわち, $\mathbb{Q}_p$ は $0, 1, \ldots, p-1$ を係数に持つ p の Laurent 級数 (p 進級数) 全体の集合であるとみなせる. 任意の有理函数が局所的に Laurent 級数展開できるのと同じように, 任意の有理数も p 進級数に展開できる. たとえば,

$$1 + p + p^2 + p^3 + \cdots = \frac{1}{1-p} \qquad \text{in } \mathbb{Q}_p.$$

素数 p の絶対値は必ず 1 より大きいという先入観を捨てなければいけない. $\mathbb{Q}_p$ の中で p は絶対値が 1 より小さな数とみなされるのである. $\mathbb{Q}_p$ では実数体 $\mathbb{R}$ の世界と同じようなことがかなりできる. たとえば, $\mathbb{R}$ と同様に $\mathbb{Q}_p$ は局所コンパクトになり, $\mathbb{R}$ 上の Lebesgue 積分論と同様の積分論が $\mathbb{Q}_p$ 上でも可能である.

さらに, $\mathbb{Q}$ に有理数係数の代数方程式の根 α を付け加えれば $K = \mathbb{Q}(\alpha)$ という $\mathbb{Q}$ の有限次代数拡大体が得られる. $\mathbb{Q}$ に有理数係数の全ての代数方程式の根を付け加えれば $\overline{\mathbb{Q}}$ という代数閉体が得られる. $\overline{\mathbb{Q}}$ に含まれる数は代数的数と呼ばれ, $\overline{\mathbb{Q}}$ に含まれない数は超越数と呼ばれている.

上で用いた操作に, さらに素イデアルによる剰余環を構成する操作と文字を付け加える操作を追加すれば, 数の世界が函数の世界に拡張されることになる.

たとえば, 素数 p から生成される $\mathbb{Z}$ の素イデアル $\mathbb{Z}p$ で割った $\mathbb{Z}$ の剰余環 $\mathbb{F}_p$ は位数 p の有限体である. 有限体の n 次代数拡大は位数 p^n の有限体 $\mathbb{F}_{p^n}$ である. 標数 p の有限体はこのようなもので尽きている.

位数 q の有限体 $k = \mathbb{F}_q$ に文字 t を付け加えた多項式環 $k[t]$ を考え, その商体を考えると, 有限体上の (1 変数) 有理函数体 $k(t)$ である. この時点で数の世界から函数の世界に突入することになるのだが, 有限体上の有理函数体は有限体から出発したのでかなり離散的な性質を持っており, 有理数体と非常に似た性質を持っている.

有理数体を実数体や p 進数体に完備化するのと同じように $K = k(t)$ を $c \in k$ と ∞ において完備化することができる:

$$K_c = \{\, a_N(t-c)^N + a_{N+1}(t-c)^{N+1} + a_{N+2}(t-c)^{N+2} \mid N \in \mathbb{Z},\ a_i \in k \,\},$$
$$K_\infty = \{\, a_N t^{-N} + a_{N+1}t^{-N-1} + a_{N+2}t^{-N-2} \mid N \in \mathbb{Z},\ a_i \in k \,\}.$$

$\mathbb{Q}_p$ と K_c は非常に似ている.

有理数体 $\mathbb{Q}$ の有限次拡大体を代数体と呼ぶのと同じように, 体 k 上の有理函数体 $k(t)$ の有限次拡大体を体 k 上の代数函数体と呼ぶ. もしも体 k が有限体ならば体 k 上の代数函数体は代数体と非常に似た性質を持つことが知られている.

複素函数論と密接に関係しているのは $k = \mathbb{C}$ の場合である. $\mathbb{C}$ 上の有理函数体 $\mathbb{C}(t)$ は複素射影直線上の有理型函数全体のなす体と同一視できる. さらに, $t^3 + at + b$ が重根を持たないような $a, b \in \mathbb{C}$ に対して, 楕円函数体 $\mathbb{C}(t, \sqrt{t^3 + at + b})$ は楕円曲線上の有理型函数全体のなす体と同一視できる ([Take], [U]). 一般に, $\mathbb{C}$ 上の代数函数体はあるコンパクト Riemann 面上の有理型函数全体のなす体と同一視でき, 逆にコンパクト Riemann 面上の有理型函数全体のなす体はある代数函数体と同一視できる. これによって, 複素代数函数体の理論とコンパクト Riemann 面の理論は完全に同値になることがわかる ([I]). 数学全体においてこの地点は, 函数の理論と多様体の理論が完璧に接しているポイントとして極めて重要である. 他の理論もこの地点で生まれたアイデアの何らかの意味での一般化になっていることが多い. この地点では体の Galois 理論 (代数) と分岐被覆の Galois 理論 (位相幾何) が完全に対応している. 三角函数や楕円函数のような函数はこの世界に自然に現われる.

我々はまだ数と函数の世界のほんの入口しか覗いてないのだが, そのほんの入口ですでにかなり難しい世界に突入してしまっている. 入口付近がおそろしく難解だというのが数の世界の特徴である. たとえば, 「素数がどれだけたくさんあるか?」という古くからある問題について立てられた皆が正しいと信じている予想 (Riemann 予想) はまだ解けていない. しかし, その有限体上の代数函数体上での類似物は Grothrndieck と Deligne によって高次元の場合に拡張された予想 (Weil 予想) がすでに解けている. そして, 非常に非自明なことを考えれば, 複素数体上でも Weil 予想の類似を考えることができ, それも解けている (斉藤盛彦の混合 Hodge 加群の理論). 元来の有理整数の世界に関する Riemann 予想はおそるべき難問である.

上においては函数の世界を 1 変数函数の場合に限って説明したのであるが, 一般に n 変数函数の世界を考えることもできる. 1 変数函数は幾何的には 1 次元の多様体上の函数とみなすことができるのだが, n 変数函数は n 次元多様体上の函数とみなすことができる.

さらに, 代数方程式を解くという操作以外にも, 微分方程式を解くという操作を世界を拡大するために考えることもできる. 初等函数の世界から出発して, 既知の函数を係数として持つ線形微分方程式の解もまた既知と考えることによって到達できない函数で性質

がよくわかるものにはどのようなものがあるのか, のような問題を考えることもできる. Pailevé 方程式の解はそのような函数の実例である.

以上においては, あえて「数と函数」という見方に沿って話を進めたが, そのような見方は数学的見方のほんの一部に過ぎない. 他にも様々な視点が存在し, 色々面白いことがわかっており, わかっていること以上に謎が残されているのである.

しかし, この節の最初に述べたように, $0, \pm 1, \pm 2, \ldots$ に関する算数で習ったときの経験を忘れてはいけないと思う. 我々は子どものときにたくさんの計算によって, 整数の算数の世界で何が起こっているかを感覚的に非常によく知っている. たとえば, あとで倍数や約数と言葉を習ったとき, それが大体どのようなものであるかについて割り算の経験によってよく知っていたはずである. より抽象的な数学を理解するときにも, そのような経験が重要だという経験は役に立つ. たとえば,「体の拡大」という言葉を習ったときに, 簡単な体の拡大にはどのようなものがあるかをよく知ってないと結局のところ「体の拡大」が何であるかをまったく理解できずに終わってしまうのだ. そして, どんなにたくさん計算しても, その結果を単なる計算のバラバラの集積だと感じているうちは, その世界を理解したという感覚にはなれないだろう. たくさんの計算例と抽象的な理論をすべて統合的に理解するところに到達するように努力すべきなのである.

つづく予定であるが果たしてどうなるか?

参考文献

[I] 岩澤健吉: 代数函数論, 岩波書店, 1952, 1989

[Mo] 森田康夫: 代数概論, 数学選書 9, 裳華房, 1987

[Take] 竹内端三: 楕圓函數論, 岩波全書, 1936, 1996

[U] 梅村浩: 楕円函数論——楕円曲線の解析学, 東京大学出版会, 2000