# 代数学概論III演習——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10月8日 (火)

## 目 次



## 3　体の拡大

**[57] (体のイデアルによる特徴付け)** 可換環 $R$ について, $R$ が体であることと, $R$ のイデアルが $0$ と $R$ しか存在しないことは同値である. □

**[58] (極大イデアルと体)** 可換環 $R$ とそのイデアル $\mathfrak{a}$ に対して, $R/\mathfrak{a}$ が体であることと, $\mathfrak{a}$ が $R$ の極大イデアルであることは同値である. □

**[59]** $R$ は可換環であり, $S$ はその部分環であるとする. $R$ の素イデアル $P$ に対して, $S\cap P$ は $S$ の素イデアルになる. しかし, $R$ の極大イデアル $\mathfrak{m}$ に対して, $S\cap\mathfrak{m}$ は $S$ の極大イデアルになるとは限らない. (ヒント: $R=\mathbb{C}(x)[y]$, $\mathfrak{m}=Ry$, $S=\mathbb{C}[x,y]$ が反例になっている.) □

**[60]** 体 $k$ 上の1変数多項式環 $k[x]$ は単項イデアル整域 (PID) である. □

**[61]** $R$ が PID のとき, $0\neq p\in R$ に対して以下の条件は互いに同値である:

(a) $p$ は $R$ の素元である.

(b) 単項イデアル $(p)$ は $R$ の素イデアルである.

(c) 単項イデアル $(p)$ は $R$ の極大イデアルである. □

可換環 $R$ 上の多項式環 $R[x_1,\dots,x_n]$ の $R$ に含まれない素元を $R$ 上の既約多項式と呼ぶ.

**[62] (根体)** $K$ は体であり, $f \in K[x]$ は $K$ 上の既約多項式であるとする. このとき, $L = K[x]/(f)$ は体になり, 自然な写像 $K \to L$, $a \mapsto a(1 \bmod f)$ による埋め込みによって, $K$ は $L$ の部分体とみなせる. さらに, ある $\theta \in L$ と $c \in K^\times$ が存在して, $f(\theta) = 0$, $L = K(\theta)$, $[K(\theta) : K] = \deg f$ が成立する. このような $L$ を既約多項式 $f$ の**根体**と呼ぶ. ($K(\theta) = \{\, f(\theta)/g(\theta) \mid f, g \in K[x],\ g(\theta) \neq 0 \,\}$.) □

**[63] (単拡大)** $L/K$ を体の拡大として, $0 \neq \theta \in L$ に対して, 環準同型

$$\phi : K[x] \to K(\theta), \quad f(x) \mapsto f(\theta)$$

を考える. このとき, 以下が成立する:

(1) $\operatorname{Ker}\phi = 0$ のとき, 同型 $K(x) \xrightarrow{\sim} K(\theta)$, $f(x) \mapsto f(\theta)$ が存在する. このとき, $\theta$ は $K$ 上**超越的 (transcendental)** であるという.

(2) $\operatorname{Ker}\phi \neq 0$ のとき, モニックな[19]既約多項式

$$f(x) = \operatorname{Irr}(\theta, K; x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in K[x]$$

で $\operatorname{Ker}\phi = (f)$ をみたすものが一意に存在し,

$$K[x]/(f) \to K(\theta), \quad g(x) \bmod f(x) \mapsto g(\theta)$$

は同型写像であり, $[K(\theta) : K] = \deg f = n$ が成立している. このとき, $\theta$ は $K$ 上**代数的 (algebraic)** であるといい, $n$ をその**次数 (degree)** と呼ぶ. □

**[64] (分母の有理化)** $L/K$ を体の拡大とし, $\theta \in L$ は $K$ 上次数 $n$ の代数的な元であるとする. このとき, $K(\theta)$ の任意の元 $a$ は,

$$a = c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1}, \quad c_0, c_1, \dots, c_{n-1} \in K$$

の形で一意に表わされる. □

上の問題がなぜ「分母の有理化」なのかについて考えてみよ.

**[65]** $\mathbb{Q}$ は標数 0 の任意の体の部分体とみなせる. □

**[66]** $p$ は素数であるとし, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ と置く. $\mathbb{F}_p$ は標数 $p$ で位数 $p$ の有限体であり, 標数 $p$ の任意の体の部分体とみなせる. □

$\mathbb{Q}$, $\mathbb{F}_p$ を素体と呼ぶ. 任意の体は素体の拡大体である.

**[67]** $\mathbb{C}$ は $\mathbb{R}$ の 2 次拡大であり, $\mathbb{C} = \mathbb{R}(\sqrt{-1})$. □

**[68]** $\mathbb{R}$ は $\mathbb{Q}$ の代数拡大ではない. □

[19]「モニックな」とは「最高次の係数が 1 の」という意味

[**69**] **(代数学の基本定理)** $\mathbb{C}$ は代数閉体である. (ヒント: 複素函数論やトポロジーを自由に用いて良い.) □

[**70**] $\overline{\mathbb{Q}} = \{\, \theta \in \mathbb{C} \mid \theta \text{ は } \mathbb{Q} \text{ 上代数的} \,\}$ とおくと, $\overline{\mathbb{Q}}$ は $\mathbb{Q}$ を含む $\mathbb{C}$ 内の最小の代数閉体である. (ヒント: [Mo] 第 V 章の系 2.3 (p. 186).) □

$\mathbb{Q}$ の有限次拡大体を**代数体 (algebraic number field)** もしくは**数体 (number field)** と呼ぶ.

**定義 3.1 ($A$ 上整)** $L$ は可換環であり, $A$ はその部分環であるとする. $\alpha \in L$ が $A$ 上**整 (integral)** であるとは, 0 でない $A$ 上のモニックな多項式 $f(x) \in A[x]$ で $f(\alpha) = 0$ を満たすものが存在することである[20]. □

[**71**] $L$ は可換環であり, $A$ はその部分環であるとする. $\alpha \in L$ に対して, $\alpha$ から $A$ 上生成される $R$ の部分環を $A[\alpha]$ と書く. このとき, $\alpha$ が $A$ 上整であるための必要十分条件は $A[\alpha]$ が $A$ 上の有限生成加群をなすことである[21] . □

[**72**] **(整閉包)** $L$ は可換環であり, $A$ はその部分環であるとする. このとき, $A$ 上整であるような $L$ の元全体は $L$ の部分環をなす. その部分環を $A$ の $L$ における整閉包 (integranl closure) と呼ぶ. (ヒント: 体の代数拡大に関する議論の類似.) □

$\mathbb{Z}$ 上整な複素数を**代数的整数 (algebraic integer)** と呼ぶ. 一般の代数的整数と $\mathbb{Z}$ の元を区別したい場合には $\mathbb{Z}$ の元を**有理整数 (rational integer)** と呼び, $\mathbb{Z}$ を有理整数環と呼ぶことがある. 代数体 $K$ における $\mathbb{Z}$ の整閉包を $\mathcal{O}_K$ と書き, 代数体 $K$ の**整数環 (integer ring)** と呼ぶ.

$\mathbb{Z}$ の素元としての素数と代数体 $K$ の整数環 $\mathcal{O}_K$ の素元としての素数を区別するために, $\mathbb{Z}$ の素数を**有理素数 (rational prime number)** と呼ぶことがある. おそらく, 有理素数という言葉をこの演習で多用することはないだろう. 何の断わりも無しに素数と言う場合には有理素数を意味するものとする.

[**73**] $\mathbb{Z}$ 上整な有理数は有理整数である. □

[**74**] $m$ は平方因子を含まない 0 以外の整数であるとする[22]. $K = \mathbb{Q}(\sqrt{m})$ の整数環は以下のようになる:

(1) $m \equiv 2, 3 \pmod 4$ ならば $\mathcal{O}_K = \{\, a + b\sqrt{m} \mid a, b \in \mathbb{Z} \,\}$.

(2) $m \equiv 1 \pmod 4$ ならば $\mathcal{O}_K = \{\, a + b\sqrt{m} \mid a, b \in \mathbb{Z}$ または $a, b \in \mathbb{Z} + 1/2 \,\}$.

ここで, $\mathbb{Z} + 1/2$ は整数に $1/2$ を足したもの全体の集合すなわち奇数を 2 で割ってできる数全体の集合である. たとえば, $(1 + \sqrt{5})/2 \in \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ だが, $(1 + \sqrt{-5})/2 \notin \mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$. (ヒント: [Taka1] 定理 5.1.)) □

[20] モニックな多項式 (最高次の係数が 1 の多項式) に取るところが重要である. $A$ が整域であり, $K$ がその商体で, $L$ が $K$ の拡大体であるとき, $\alpha \in L$ が $K$ 上代数的 (algebraic) であるための必要十分条件は 0 でないモニックとは限らない多項式 $f(x) \in A[x]$ で $f(\alpha) = 0$ を満たすものが存在することである. モニックであることを仮定するかしないかで integral と algebraic という概念が区別されることになる.

[21] $L$ が体であり, $K$ がその部分体のとき, $\alpha \in L$ に対して, $\alpha$ が $K$ 上代数的であるための必要十分条件は $K(\alpha)$ が $K$ 上の有限次元ベクトル空間をなすことである.

[22] $m$ は 2 以上の整数の二乗の形の約数を含まない整数であるということ.

**[75]** $\omega = \exp(2\pi\sqrt{-1}/3) = (-1+\sqrt{-3})/3$ と置き, $K = \mathbb{Q}(\sqrt[3]{2})$, $L = \mathbb{Q}(\omega\sqrt[3]{2})$, $M = \mathbb{Q}(\omega, \sqrt[3]{2})$ と置く. このとき,

(1) $K$ と $L$ は $x^3-2$ の $\mathbb{Q}$ 上での根体である.

(2) $KL = M$.

(3) $M$ は $x^3-2$ の最小分解体である. □

**[76]** $x^3-7$ の $\mathbb{Q}$ 上での最小分解体は $\mathbb{Q}(\sqrt[3]{7}, \omega)$ である. ここで, $\omega = \exp(2\pi\sqrt{-1}/3) = (-1+\sqrt{3})/2$. □

**[77]** 順次以下を示せ:

(1) $K = \mathbb{Q}(\sqrt[3]{5})$ と置くと $K$ は $\mathbb{Q}$ の 3 次拡大である.

(2) $\sqrt{-3}$ の $K$ 上の最小多項式は $x^2+3$ である.

(3) $K(\sqrt{-3}) = \mathbb{Q}(\sqrt[3]{5}, \sqrt{-3})$ は $K$ の 2 次拡大でかつ $\mathbb{Q}$ の 6 次拡大である.

(4) $\sqrt[3]{5}+\sqrt{-3}$ の $\mathbb{Q}$ 上での最小多項式は $x^6+9x^4-10x^3+27x^2+90x+52$ である. (ヒント: $\omega = \exp(2\pi\sqrt{-1}/3)$ と置く. $\{\sqrt[3]{5}, \omega\sqrt[3]{5}, \omega^2\sqrt[3]{5}\}$ の元と $\{\pm\sqrt{-3}\}$ の元の 6 通りの和を全て根に持つ多項式.)

(5) $\mathbb{Q}(\sqrt[3]{5}, \sqrt{-3}) = \mathbb{Q}(\sqrt[3]{5}+\sqrt{-3})$. □

**[78]** $p$ は素数であるとし, $\alpha = \sqrt[4]{p}$, $i = \sqrt{-1}$ と置く. このとき,

(1) $\mathbb{Q}(\alpha)$, $\mathbb{Q}(i\alpha)$ は $x^4-p$ の $\mathbb{Q}$ 上での根体である.

(2) $\mathbb{Q}(\alpha, i)$ は $x^4-p$ の最小分解体である. □

**[79]** $L = \mathbb{C}(t)$, $K = \mathbb{Q}(t^3)$ と置く. このとき $L$ は $K$ の 3 次拡大である. $x^3-t^3$ は $K$ 上既約であり, $L$ の中で $x$ の 1 次式の積に分解する. $x^3-t^3$ の $K$ 上での最小分解体を求めよ. □

**[80]** $p$ は素数であるとし, $f(x) = x^{p-1}+x^{p-2}+\cdots+1$, $\zeta = \exp(2\pi\sqrt{-1}/p)$ と置く. このとき, $\mathbb{Q}(\zeta)$ は $f(x)$ の $\mathbb{Q}$ 上での根体でかつ最小分解体である. □

**[81]** $\mathbb{Q}(\sqrt{5})\mathbb{Q}(\sqrt[3]{5}) = \mathbb{Q}(\sqrt[6]{5})$. □

**[82]** $\mathbb{C}$ 上の 1 変数有理函数体 $N = \mathbb{C}(t)$ の部分体 $K = \mathbb{C}(t^6)$, $L = \mathbb{C}(t^3)$, $M = \mathbb{C}(t^2)$ を考える. このとき, $L \cap M = K$, $LM = N$. □

# 4 一意分解整域

**定義 4.1 (Euclid 整域)** $R$ は整域であるとし, 写像 $N : R \to W = \{-\infty, 0, 1, 2, 3, \ldots\}$ で以下を満たすものが存在するとき, $R$ は **Euclid 整域 (Euclidean domain, Euclid 環)** であるという:

(a) 任意の $a \in R$ に対して, $\phi(a) = -\infty \iff a = 0$.

(b) 任意の $a, b \in R - \{0\}$ に対して $\phi(ab) \geq \phi(a)$.

(c) 任意の $a, b \in R$ に対して, $a \neq 0$ ならば, ある $q, r \in R$ で $b = qa + r$, $\phi(r) < \phi(b)$ をみたすものが存在する.

直観的に言えば Euclid 整域とは算数の割り算ができる環のことである. □

**例 4.2** $a \in \mathbb{Z} - \{0\}$ に対して $\phi(a) = |a|$ と定めれば $\mathbb{Z}$ は Euclid 整域であることがわかる. $K$ が体であるとき, $f \in K[x] - \{0\}$ に対して, $\phi(f) = \deg f$ と定めれば $K[x]$ が Euclid 整域であることがわかる. □

**[83]** Euclid 整域が PID であることを示せ. □

**[84]** Gauss の整数環 $\mathbb{Z}[\sqrt{-1}]$ は Euclid 整域であり, その単数の全体は $\{\pm 1, \pm\sqrt{-1}\}$ である. (ヒント: $\alpha \in \mathbb{Z}[\sqrt{-1}] - \{0\}$ に対して $\phi(\alpha) = |\alpha|^2$ と置けば良い. [Mo] 第 III 章の問題 4.7 (p. 88) により詳しいヒントがある. 詳しい解答は [Taka1] の定理 4.1 (p. 244) の証明にある.) □

**[85]** $\omega = \exp(2\pi\sqrt{-1}/3) = (-1 + \sqrt{-3})/2$ に対して, $\mathbb{Z}[\omega]$ は Euclid 整域であり, その単数の全体は $\{\pm 1, \pm\omega, \pm\omega^2\}$ である. (ヒント: Gauss の整数環の場合と同様に $\phi(\alpha) = |\alpha|^2$ と置けば良い. [Taka1] 第 4 章第 39 節の p. 257.) □

**[86] (非可換な Euclid 整域の例)** $K$ は $\mathbb{C}$ 上の有理型函数全体のなす体であるとする. $\mathbb{C}$ の座標を $x$ と書くことにする. $f \in K$ の $x$ に関する導函数を $f'$ と書き, $f$ の $k$ 階の導函数を $f^{(k)}$ と書くことにする. 函数 $a \in K$ を $K$ の元に乗じる写像 $a : K \to K$, $f \mapsto af$ と $x$ に関する微分 $\partial : K \to K$, $f \mapsto f'$ から生成される $\mathrm{End}_{\mathbb{C}}(K)$ の部分環を $\mathcal{D}$ と表わす. $\mathcal{D}$ を $K$ 係数の**線形上微分作用素環** と呼ぶ. このとき, 以下が成立している:

(1) $\mathcal{D}$ は両側 $(K, K)$ 加群である.

(2) $\mathcal{D}$ は左 $K$ 加群として $1, \partial, \partial^2, \ldots$ を基底に持つ. (ヒント: それらの $K$ 一次結合を $x^n$ に作用させてみれば一次独立性がわかる.)

(3) $\mathcal{D}$ の 0 でない元は $A = a_n\partial^n + a_{n-1}\partial^{n-1} + \cdots + a_0 \in \mathcal{D}$ $(a_i \in K)$, $a_n \neq 0$ の形に一意に表わされる. このとき, $A$ は $n$ 階であると言い, $\mathrm{ord}\, A = n$ と書く. $A = 0$ のときは $\mathrm{ord}\, A = -\infty$ であると約束しておく.

(4) $\mathcal{D}$ の積に関して次が成立している (Leibnitz 則):

$$\partial^n f = \sum_{k=0}^{n} \binom{n}{k} f^{(k)} \partial^{n-k} \quad (f \in K,\ n = 0, 1, 2, \ldots).$$

(5) 任意の $A, B \in \mathcal{D}$ に対して, $A \neq 0$ ならば, $Q, R \in \mathcal{D}$ で $B = QA + R$, $\operatorname{ord} R < \operatorname{ord} A$ となるものが一意に存在する.

(6) 任意の $A, B \in \mathcal{D}$ に対して, $A \neq 0$ ならば, $Q, R \in \mathcal{D}$ で $B = AQ + R$, $\operatorname{ord} R < \operatorname{ord} A$ となるものが一意に存在する.

(7) $A = \partial + a$, $B = \partial^2 + b\partial + c$ のとき, $B = (\partial + b - a)A + c - a' - (b - a)a = A(\partial + b - a) + c - (b' - a') - a(b - a)$. □

**参考 4.3** [**86**] の線形上微分作用環 $\mathcal{D}$ は非可換な Euclid 整域と呼ぶべき性質を持っている. 左 $\mathcal{D}$ 加群は複素平面上の線形常微分方程式の抽象化である. たとえば, $P \in \mathcal{D}$ に対して, $M = \mathcal{D}/\mathcal{D}P$ は $Pu = 0$ という微分方程式に対応している. 実際, $u = 1 \bmod \mathcal{D}P \in M$ と置けば $Pu = 0$. そして, その方程式の函数空間 $\mathcal{F}$ (そこには $\mathcal{D}$ が作用しているとする) における解全体の空間は $\operatorname{Hom}_{\mathcal{D}}(M, \mathcal{F})$ と同一視できる. 実際, $\phi \in \operatorname{Hom}_{\mathcal{D}}(M, \mathcal{F})$ に対して, $f = \phi(u) \in \mathcal{F}$ と置けば $Pf =$ であり, 逆に $f \in \mathcal{F}$ が $Pf = 0$ を満たしていれば $\phi(Pu) = Pf$ によって $\phi \in \operatorname{Hom}_{\mathcal{D}}(M, \mathcal{F})$ を定めることができる.

現代においては線形微分方程式 (偏微分方程式を含む) を代数的に扱う方法が十分発達しており, $\mathcal{D}$ 加群の理論と呼ばれている. 非線形の場合を含む微分方程式一般を代数的に扱うべきだという哲学は佐藤哲学[23]と呼ばれている. □

[**87**] **(一意分解整域の定義)** 一意分解整域 (unique factorization domain, UFD) の定義を説明し, 証明抜きで UFD の例を 3 つ挙げよ. □

[**88**] PID が UFD であることを示せ[24]. □

[**89**] $R$ が整域ならば $R$ 上の 1 変数多項式環 $R[x]$ も整域であり, $R[x]$ の単元の全体は $R$ の単数[25] の全体に一致することを示せ. それでは, $R$ が整域とは限らない可換環でも同様の結果が成立するか? (ヒント: 成立しない. $a^2 = 0$ ならば $(1 + ax)(1 - ax) = 1$.) □

[**90**] **(0 を含む最大公約数と最小公倍数)** $\mathbb{Z}$ における $0, 9, 12$ の最大公約数と最小公倍数は何であるか? (ヒント: どんな数も 0 をかければ 0 になるので, 0 はあらゆる数の倍数であり, あらゆる数は 0 の約数である. 逆に, 単数[26] (たとえば 1) はあらゆる数の約数であり, あらゆる数は単数の倍数である. よって, 倍数関係で定義される前順序に関して, 0 は最大であり, 単数は最小である.) □

**定義 4.4 (原始多項式)** $R$ が UFD であるとき, 多項式

$$f = \sum a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n} \in R[x_1, \ldots, x_n]$$

の係数 $a_{i_1,\ldots,i_n} \in R$ の最大公約数が 1 になるとき, $f$ は $R$ 上の**原始多項式 (primitive polynomial)** であるという. □

---

[23] 佐藤幹夫の哲学. 英語では Sato philosophy. $\mathcal{D}$ 加群のアイデアも佐藤幹夫が提唱した.

[24] Euclid 整域 $\Longrightarrow$ PID $\Longrightarrow$ UFD である. 特に有理整数環 $\mathbb{Z}$, Gauss の整数環 $\mathbb{Z}[\sqrt{-1}]$ や体 $K$ 上の 1 変数多項式環 $K[x]$ は UFD である.

[25] $R$ は数で構成された環であるとは限らないので, 「単元倍」と言うべきかもしれないが, 気持ちの上では数なので単数倍と呼ぶことにした. 英語ではどちらも unit である.

[26] $\mathbb{Z}$ の単数は $\pm 1$ である.

**[91] (多項式の内容)** $R$ は UFD であり, $K$ はその商体であるとする. $K$ 係数の任意の多項式 $f \in K[x_1, \ldots, x_n]$ は $f = c \cdot f_0$ ($c \in K$, $f_0$ は $R$ 上の原始多項式) と書け, $c$ と $f_0$ は $f$ に対して $R$ の単数倍の違いを除いて一意に定まる. $f \in R[x_1, \ldots, x_n]$ ならば $I(f) \in R$ となる. このような $c$ の 1 つを選び $I(f)$ と書いて $f$ の内容 (content) と呼ぶ. (ヒント: [Mo] 第 III 章の補題 4.9 (p. 89) に 1 変数多項式の場合の証明がある. 我々は多変数の多項式を扱っているが全く同様である.) □

**[92]** $R$ は可換環であり, $I$ はそのイデアルとし, $\pi : R \to R/I$ は自然な全射環準同型であるとする. このとき, 写像 $\phi : R[x_1, \ldots, x_n] \to R/I[x_1, \ldots, x_n]$ を

$$\phi : \sum a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n} \mapsto \sum \pi(a_{i_1,\ldots,i_n}) x_1^{i_1} \cdots x_n^{i_n}$$

と定める. $\phi$ が全射環準同型であることを示せ. さらに, $\phi$ が自然な同型

$$R[x_1, \ldots, x_n]/IR[x_1, \ldots, x_n] \xrightarrow{\sim} R/I[x_1, \ldots, x_n]$$

を誘導することを示せ. □

**[93] (Gauss の補題)** $R$ は UFD であり, $K$ はその商体であるとすると以下が成立する:

(1) $R$ 上の原始多項式の積もまた原始多項式である.

(2) $f, g \in K[x_1, \ldots, x_n]$ に対して, $I(fg)$ と $I(f)I(g)$ は $R$ の単数倍を除いて等しい.

(ヒント: 問題 **[91]** より, (1) を示せば十分である. 以下 $A = R[x_1, \ldots, x_n]$ と置く. $f, g \in A$ について, $fg$ が原始的でないと仮定して, $f$ または $g$ が原始的でないことを示せば良い. $fg$ は原始的でないので $R$ のある素元 $p$ が存在して, $fg$ の全ての係数は $p$ で割り切れる. 問題 **[92]** を $I = (p)$ の場合に適用して, 全射環準同型 $\phi : A \to R/(p)[x_1, \ldots, x_n]$ を構成する. $h \in A$ の $\phi$ の像が 0 になることと, $h$ の全ての係数が $p$ で割り切れることは同値である. $0 = \phi(fg) = \phi(f)\phi(g)$ である. $p$ は素元であることより $R/(p)$ は整域なので, $R/(p)[x_1, \ldots, x_n]$ も整域になる. よって, $\phi(f)$ または $\phi(g)$ のどちらかが 0 になる. すなわち, $f$ または $g$ は原始的ではない.) □

**[94]** $R$ は UFD であり, $K$ はその商体であるとする. このとき, $f \in R[x_1, \ldots, x_n]$ が $R$ 上の既約多項式ならば $f$ は $K$ 上の既約多項式である. (ヒント: $f = gh \in R[x_1, \ldots, x_n]$, $g, h \in K[x_1, \ldots, x_n]$, $g, h \notin K$ という仮定のとで $f$ が $R$ 上既約でないことを示せば良い. **[93]** より, **[91]** の記号法のもとで必要ならば $R$ の単数倍をうまく調整すれば, $1 = I(f) = I(g)I(h)$, $f = f_0 = g_0 h_0$ が成立している. $g_0, h_0 \in R[x_1, \ldots, x_n]$, $g_0, h_0 \notin R$ なので $f$ は $R$ 上既約でないことがわかった.) □

**[95]** $R$ が UFD ならば $R$ 上の $n$ 変数多項式環 $R[x_1, \ldots, x_n]$ も UFD である. (ヒント: $n$ に関する帰納法より, 1 変数多項式環 $R[x]$ が UFD であることを示せば良い. **[91]** より, $R$ 係数の原始多項式が一意的に素元分解できることを示せば良い. 素元分解の一意性は **[88]** より $K[x]$ が UFD であることを使えばわかる.)

**[96]** $t^2$ と $t^3$ から $\mathbb{C}$ 上生成される $\mathbb{C}[t]$ の部分環を $\mathbb{C}[t^2, t^3]$ と表わす. $\mathbb{C}[t^2, t^3]$ は $1, t^2, t^3, t^4, \ldots$ を $\mathbb{C}$ 基底として持つ. $\mathbb{C}[t^2, t^3]$ は UFD ではない[27]. (ヒント: $t^6 = (t^2)^3 = (t^3)^2$ でかつ $t \notin \mathbb{C}[t^2, t^3]$.) □

**[97]** $R = \mathbb{C}[x, y, z]/(z^2 - xy)$ は整域だが UFD ではない[28]. □

**[98]** $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ は UFD ではない. (ヒント: $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.) □

**参考 4.5** 以上に続けて勉強するべきなのは Dedekind 整域 (Dedekind domain, Dedekind 環) の理論である. UFD は 0 でない各元が一意的に素元分解できるような整域のことであった. Dedekind 整域は 0 でないイデアルが素イデアルの積に一意的に分解できるような整域のことである. Dedekind 整域の最重要例は代数体の整数環である.

たとえば $\mathbb{Q}(\sqrt{-5})$ の整数環 $\mathbb{Z}[\sqrt{-5}]$ は UFD ではないが Dedekind 整域である ([Mo] 第 III 章の例 6.11, p. 102 でもその事実が注意されている). $\mathbb{Z}[\sqrt{-5}]$ のような環を詳しく研究するためには Dedekind 整域の理論が必要になる. そこまでたどりついた方は代数的整数論の入口に立っていることになる. 体の Galois 理論の最も重要な応用先は代数的整数論である. □

# 5 Eisenstein の判定法と既約多項式の例

体 $K$ 上の既約多項式 $f \in K[x]$ を与えるごとに, $K$ の有限次元拡大 $L = K[x]/(f)$ が得られる. それでは $f$ の既約性を判定するためにはどうすれば良いのだろうか. 次の Eisenstein の判定法が有名である.

**[99] (Eisenstein の判定法)** $R$ は UFD であり, $K$ はその商体であるとする. $R$ 上の原始多項式

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$$

がある素元 $p \in R$ について

$$p \nmid a_n, \quad p \mid a_i \quad (i = 0, \ldots, n-1), \quad p \nmid a_0$$

をみたしていれば $f$ は $R$ 上したがって $K$ 上既約である. □

以下の問題を解くときに, Eisenstein の判定法を自由に用いて良い.

**[100]** $x^4 + 1$ は $\mathbb{Q}$ 上既約である. (ヒント: $x$ に $x + 1$ を代入して Eisenstein の判定法を適用せよ.) □

**[101]** 素数 $p$ に対して, $f(x) = (x^p - 1)/(x - 1) = x^{p-1} + x^{p-2} + \cdots + 1$ は $\mathbb{Q}$ 上既約である. (ヒント: $x$ に $x + 1$ を代入して Eisenstein の判定法を適用せよ.) □

[27] $\mathbb{C}[t]$ は PID なので UFD である. $C[t^2, t^3]$ は $x = t^2$, $y = t^3$ という対応によって $\mathbb{C}[x, y]/(y^2 - x^3)$ に同型である. $y^2 = x^3$ のグラフは原点でとがっている. その形状をカスプ (cusp) と呼ぶ. 実は可換環の UFD 性と可換環に対応する「図形」の非特異性のあいだには微妙な関係がある. たとえば, David Mumford の "The Red Book" citemumford の第 III 章の第 7 節, 特に p. 276 にある図を参照せよ.

[28] $\mathbb{R}^3$ の中で $z^2 = xy$ のグラフはどのような形をしているか?

**[102]** $x^n + px + p$ ($n \geq 2$, $p$ は素数) は $\mathbb{Q}$ 上既約である. □

**[103]** $p$ は素数であるとし, $a \in \mathbb{Z}$ は $p \mid a$, $p^2 \nmid a$ をみたしているとする. このとき, $x^n - a$ は $\mathbb{Q}$ 上既約である.

**[104]** $a$ が 3 上因子を含まない 2 以上の有理整数ならば $x^3 - a$ は $\mathbb{Q}$ 上既約である. □

**[105]** $k$ は任意の体であるとし, $K = k(t)$ と置く. $x^n + tx + x, x^n - t \in K[x]$ は $K$ 上既約である. (ヒント: $k(t)$ は $k[t]$ の商体であり, $t$ は $k[t]$ の素元である.) □

Eisenstein の判定法を使わない例も示しておこう.

**[106]** $f(x) = x^5 - x^3 - 2x^2 - 2x - 1$ は $\mathbb{Q}$ 上既約であることを示せ. (ヒント: [Taka2] 第 4 章第 24 節問題 2 (p. 130). $f(x)$ が既約でないとすると, 2 次式以下の整数係数の因子を持つ. その因子を $\phi(x) = ax^2 + bx + c$ と置き, $f(1) = 5$, $f(-1) = -1$ などの情報から有限個可能性に狭め, そのどれでも $f(x)$ が割り切れないことを示す. $f(x)$ が整数係数多項式の範囲内でこれ以上因数分解されないことを示すのは高校数学の範囲内の問題である.) □

**[107]** $K = \mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$ のとき, $f(x) = x^3 - x - 2 \in K[x]$ は $K$ 上既約である. (ヒント: $f$ は 3 次式なので既約でなければ 1 次式の因子を持つ. そのとき, ある $K$ の元 $a$ において $f(a) = 0$ となる. しかし, 実際に計算してみるとそうはならない.) □

# 6 線形無関連性

以下, $K$ は体であるとする.

**定義 6.1 ($K$ 代数)** $A$ は $K$ 上のベクトル空間であり, $K$ 上の双線形写像 $A \times A \to A$, $(a, b) \mapsto ab$ が与えられているとき, $A$ を $K$ 代数もしくは $K$ 上の代数 ($K$-algebra, algebra over $K$, $K$ 多元環) と呼び, $(a, b) \mapsto ab$ を積と呼ぶ.

$A$ は $K$ 代数であるとする.

$A$ の $K$ 部分空間 $B$ が積について閉じているとき, $B$ は $A$ の $K$ 部分代数 ($K$-subalgebra) であるという.

$A$ は $K$ 代数であるとする. $A$ の積が結合律 (associativity) をみたしているとき, すなわち $(ab)c = a(bc)$ $(a, b, c \in A)$ をみたしているとき, $A$ は結合的 (associative) であるという. $A$ の元 1 で $1a = a1 = a$ $(a \in A)$ をみたすものが存在するとき, $A$ は単位元を持つ (with unit) という. 結合的で 1 を持つ代数を単に $K$ 代数と呼ぶことも多い. □

**[108]** 上の定義のもとで, $L$ が体 $K$ の拡大体であれば, $L$ は結合的で 1 を持つ $K$ 代数であり, $K$ と $L$ の中間体は $L$ の $K$ 部分代数である. □

**[109]** $C_0(\mathbb{R}) = \{ f : \mathbb{R} \to \mathbb{C} \mid f$ は連続でかつ $x \to \pm\infty$ で $f(x) \to 0 \}$ と定めると, $\mathbb{C}_0(\mathbb{R})$ は $\mathbb{C}$ 上の結合的代数だが, 1 を持たない. □

**[110] (テンソル代数)** $K$ 上のベクトル空間 $V$ に対して, テンソル代数 $T(V) = \bigoplus_{i=0}^{\infty} V^{\otimes i}$ は結合的で 1 を持つ $K$ 代数である. □

**[111] (Lie 代数)** $K$ 代数 $A$ の積を $[a,b]$ と書くことにする. このとき, $[a,a]=0$, $[[a,b],c]=[a,[b,c]]-[b,[a,c]]$ (Jacobi 律) が成立しているならば, $A$ は Lie 代数であるといい, $[\ ,\ ]$ を Lie bracket と呼ぶ. 例えば, $M_n(K)$ に Lie bracket を $[A,B]=AB-BA$ と定めると $M_n(K)$ は Lie 代数をなす. □

**定義 6.2 (線形無関連性)** 体 $K$ 上の可換な代数 $\Omega$ の $K$ 部分代数 $A$, $B$ が $K$ 上線形無関連 (linearly disjoint) であるとは自然な $K$ 線形写像 $A\otimes_K B\to\Omega$, $\sum a_i\otimes b_i\mapsto\sum a_ib_i$ が単射になることである. □

**[112]** 体 $K$ 上の可換な代数 $\Omega$ の $K$ 部分代数 $A$, $B$ に関して以下の条件は互いに同値である:

(a) $A$ と $B$ は $K$ 上線形無関連である.

(b) $b_1,\dots,b_n\in B$ が $K$ 上一次独立ならばそれらは $A$ 上でも一次独立である[29].

(c) $a_1,\dots,a_n\in A$ が $K$ 上一次独立ならばそれらは $B$ 上でも一次独立である. □

**[113]** 体の拡大 $\Omega/K$ の中間体 $L$, $M$ について以下の 2 つの条件は互いに同値である[30]:

(b) $b_1,\dots,b_n\in M$ が $K$ 上一次独立ならばそれらは $L$ 上でも一次独立である.

(c) $a_1,\dots,a_n\in L$ が $K$ 上一次独立ならばそれらは $M$ 上でも一次独立である.

(ヒント: 逆も同様なので (b) $\Longrightarrow$ (c) のみを示せばよい. (b) を仮定し, $a_1,\dots,a_n\in L$ は $K$ 上一次独立であり, $b_1,\dots,b_n\in M$, $a_1b_1+\cdots+a_nb_n=0$ と仮定する. 適当に順序を変更して, $\{b_1,\dots,b_k\}$ は $K$ 上一次独立な $\{b_1,\dots,b_n\}$ の極大部分集合にできる. そのとき, $b_i=\sum_{j=1}^k c_{ij}b_j$ $(c_{ij}\in K,\ i=1,\dots,n)$ と書ける. $0=\sum_i a_ib_i=\sum_j(\sum_i a_ic_{ij})b_j$. (b) を仮定したので $\sum_i a_ic_{ij}=0$ $(j=1,\dots,k)$. $a_1,\dots,a_n$ は $K$ 上一次独立と仮定したのですべての $c_{ij}$ は 0 になる. よって, $b_i=\sum_j c_{ij}b_j=0$ $(i=1,\dots,n)$. □

**参考 6.3** **[112]** の結果より, **[113]** の条件 (b), (c) は定義 6.2 の意味で $L$, $M$ が $K$ 上線形無関連であることと同値である. 代数学の入門的な教科書の多くは $L$, $M$ が $K$ 上線形無関連であることの定義として **[113]** の条件 (b), (c) を採用している. □

**[114]** 体の拡大 $\Omega/K$ を考える. このとき, 以下が成立する:

(1) $\Omega$ の $K$ 部分代数は整域であり, その商体は自然に $\Omega/K$ の中間体とみなせる.

(2) $\Omega$ の $K$ 部分代数 $A$, $B$ を取り, それらの商体をそれぞれ $L$, $M$ と書く. このとき, $A$ と $B$ が $K$ 上線形無関連ならば $L$ と $M$ もそうである. □

**[115]** $L$, $M$, $N$ は体の拡大 $\Omega/K$ の中間体であり, $M\subset N$ であるとする. このとき, 次の 2 つの条件は互いに同値である:

(a) $L$ と $N$ は $K$ 上線形無関連である.

[29] $b_1,\dots,b_n\in B$ が $A$ 上一次独立であるとは, 任意の $a_1,\dots,a_n\in A$ に対して, $a_1b_1+\cdots+a_nb_n=0$ ならば $b_1=\cdots=b_n=0$ となること.

[30] $\Omega/K$ の典型例としては $\mathbb{C}/\mathbb{Q}$ を考えよ.

(b) $L$ と $M$ は $K$ 上線形無関連であり, 合成体 $LM$ と $N$ は $M$ 上線形無関連である.

(ヒント: まず問題の意味を理解するために [Mo] の p. 181, p. 184, などにあるような図を描いてみよ. **[112]** を見よ. **[114]** を使う.) □

**[116]** 体の拡大 $\Omega/K$ の中間体 $L$, $M$ について, $[L:K] < \infty$ ならば次の 2 つの条件は互いに同値である:

(a) $L$ と $M$ は $K$ 上線形無関連である.

(b) $[LM:M] = [L:K]$. □

**[117]** 体の有限次拡大 $M/K$ の中間体 $L$ について $[M:K] = [M:L][L:K]$. □

**[118]** 体の拡大 $\Omega/K$ の中間体 $L$, $M$ について以下が成立する:

(1) $[LM:K] < \infty \iff [L:K] < \infty$ かつ $[M:K] < \infty$.

(2) $[LM:K] < \infty$ のとき, $[LM:K]$ は $[L:K]$ と $[M:K]$ の倍数であり, $[LM:K] \leq [L:K][M:K]$.

(3) $[LM:K] < \infty$ のとき, $[L:K]$ と $[M:K]$ が互いに素ならば, $[LM:K] = [L:K][M:K]$ かつ $L$ と $M$ は $K$ 上線形無関連である. □

**[119]** 体の拡大 $\Omega/K$ の中間体 $L$, $M$ が $K$ 上線形無関連ならば $L \cap M = K$. □

**[120]** 体の拡大 $\mathbb{C}/\mathbb{Q}$ の中間体 $L = \mathbb{Q}(\sqrt[3]{5})$, $M = \mathbb{Q}(\omega\sqrt[3]{5})$ $(\omega = \exp(2\pi\sqrt{-1}/3))$, $N = \mathbb{Q}(\sqrt{-3})$ とおく. 以下が成立することを示せ:

(1) $L$ と $N$ は $\mathbb{Q}$ 上線形無関連である.

(2) $LM = LN$ でかつ, $L$ と $M$ は $\mathbb{Q}$ 上線形無関連ではない.

(3) $L \cap M = \mathbb{Q}$.

(ヒント: (1) は **[119]** の (3) を使う. (2) は **[116]** を使う. (3) は **[117]** を使う.) □

**[121]** 体の拡大 $\mathbb{C}/\mathbb{Q}$ の中間体 $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ は $\mathbb{Q}$ 上線形無関連である. (ヒント: $1$, $\sqrt{2}$ が $\mathbb{Q}(\sqrt{3})$ 上一次独立であることを示せば良い.) □

**[122]** $m, n \in \mathbb{Z} - \{0, 1\}$ とし, $K = \mathbb{Q}(\sqrt{m})$, $L = \mathbb{Q}(\sqrt{n})$ と置く. もしも $K \neq L$ ならば $K$ と $L$ は $\mathbb{Q}$ 上線形無関連である. □

**[123]** 体の拡大 $L/K$ と $K$ 上の 1 変数有理函数体 $L(x)$ を考える. このとき, $L(x)/K$ の中間体 $L$, $K(x)$ は $K$ 上線形無関連である. □

**[124]** $\mathbb{C}$ 上の 1 変数有理函数体 $K = \mathbb{C}(t)$ の代数的閉包を $\Omega = \overline{K}$ と書く. $\Omega/K$ の中間体 $K(\sqrt{t})$, $K(\sqrt{t-1})$ は $K$ 上線形無関連である. (ヒント: **[121]** とこの問題は似ている.) □

# 7 楕円函数体

**[125]** $X$ は $\mathbb{C}$ の連結開部分集合であるとする. $X$ 上の有理型函数の定義を説明し, $X$ 上の有理型函数全体が自然に体をなすことを証明せよ. □

**[126]** $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cap \{\infty\}$ (複素射影直線) 上の有理型函数とは $C$ 上の有理型函数 $f(z)$ で $g(w) = f(1/w)$ が $w = 0$ の近傍で有理型になるもののことである. $\mathbb{P}^1(\mathbb{C})$ 上の有理型函数の全体は $\mathbb{C}$ 上の 1 変数有理函数体 $\mathbb{C}(z)$ に一致することを示せ. □

**[127] (複素有理函数体)** $\omega_1, \omega_2 \in \mathbb{C}$ は $\mathbb{R}$ 上一次独立であるとする. このとき, $\mathbb{C}$ 上の有理型函数 $f(u)$ が周期 $\omega_1, \omega_2$ を持つ楕円函数 (elliptic function) であるとは, $f(u+\omega_i) = f(u)$ $(i = 1, 2)$ が成立することである. 固定された周期を持つ楕円函数の全体が体をなすことを証明せよ. 楕円函数の全体のなす体を楕円函数体と呼ぶ. □

**[128] (Weierstrass の $\wp$ 函数)** $\omega_1, \omega_2 \in \mathbb{C}$ は $\mathbb{R}$ 上一次独立であるとし, $\Gamma = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, $\Gamma' = \Gamma - \{0\}$ と置く. 次の式によって周期 $\omega_1$, $\omega_2$ を持つ楕円函数 $\wp(u)$ を構成可能なことを示せ:

$$\wp(u) = \frac{1}{u^2} + \sum_{\omega \in \Gamma'} \left( \frac{1}{(u-\omega)^2} - \frac{1}{\omega^2} \right).$$

これを Weierstrass の $\wp$ 函数と呼ぶ. □

**参考 7.1** $K$ を周期 $\omega_1$, $\omega_2$ を持つ楕円函数全体のなす体とすると, $K$ は $\wp$ とその導函数 $\wp'$ から $\mathbb{C}$ 上生成されることが知られている. すなわち $K = \mathbb{C}(\wp, \wp')$. さらに, Weierstrass の $\wp$ 函数は次の形の微分方程式を満たしている:

$$\wp'(u)^2 = 4\wp(u)^3 - g_2\wp(u) - g_3.$$

ここで, $g_2$, $g_3$ は周期 $\omega_1$, $\omega_2$ で決まるある定数である. よって, $(x, y) = (\wp(u), \wp'(u))$ は $\mathbb{C} - \Gamma$ による複素曲線

$$\{\, (x, y) \in \mathbb{C}^2 \mid y^2 = 4x^3 - g_2 x - g_3 \,\}$$

の parametrization を与える. この曲線を複素楕円曲線 (elliptic curve) と呼ぶ. 楕円函数体 $K$ は $\mathbb{C}(x)$ に $y = \sqrt{x^3 - g_2 x - g_3}$ を添加して得らえる $\mathbb{C}(x)$ の 2 次拡大体に一致する. 楕円函数と楕円曲線の理論は基本的でかつ重要である. 楕円函数論の教科書には [Take], [U] などがある.

さらに難しい複素曲線と複素函数を扱う理論に代数函数論がある. その別の名はコンパクト Riemann 面の理論である. 代数函数論は 19 世紀数学の花形の 1 つである. 興味のある方は岩澤健吉著『代数函数論』 [I] を読んで欲しい. 代数函数論では代数的な Galois 理論 (代数函数体の有限次拡大の理論) と幾何学的な Galois 理論 (コンパクト Riemann 面の分岐被覆の理論) が統一されることになる.

代数函数体 (algebraic function field) と代数体 (algebraic number field) の理論はよく似ている. 楕円函数体は有理函数体の次に簡単な代数函数体である. 上の記号における $\sqrt{x^3 - g_2 x - g_3}$ という無理函数は $\sqrt{2}$ のような無理数の類似物である. 体の Galois 理論を理解するとき, 純代数的な議論が納得できな人は代数函数体の場合について考えると納得できる場合が増えるかもしれない. □

# つづく.

# 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

[Taka1] 高木貞治: 初等整数論講義, 共立出版, 第 2 版 1971, 2000

[Taka2] 高木貞治: 代数学講義, 共立出版, 改定新版 1965, 1999

[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