6　代数拡大

6.1　代数的、超越的

K : 体、 $A : K-$ 代数とする。

定義 6.1. $x \in A$ が K 上代数的、代数的数 (algebraic)とは

$$^{\exists} f\ (\neq 0)\ \in K[X] : K \text{ 係数多項式 } s.t.\ f(x) = 0$$

となることで代数的でないときこれを超越的、超越的数 (transcendental)という。

命題 6.2. $x \in A$ に対して以下は同値

(1) $1, x, x^2, \cdots$ が K 上一次独立ではない

(2) $K[x]$ が有限次元

(3) x は K 上代数的

Proof. $3 \Rightarrow 1$

x が代数的なので、ある $f = \sum_{i=0}^{n} a_i X^i \in K[X]\ (0 \neq a_i \in K)$ において $f(x) = \sum_{i=0}^{n} a_i x^i = 0$ より $1, x, x^2, \cdots$ は一次独立ではない。

$1 \Rightarrow 3$

一次独立でないのである有限な m で $\sum_{i=0}^{m} a_i x^i = 0$ となる全ては 0 ではない $a_i \in K$ が存在するのでこれを $f = \sum_{i=0}^{m} a_i X^i$ とすれば $f \in K[X], f(x) = 0$ となるため x は K 上代数的である。

$2 \Leftrightarrow 3$

$x \in A$ に対し写像 $\phi : K[X] \longrightarrow A, X \longmapsto x$ は環準同型であり、$^{\exists} f \in K[X], \ker(\phi) = (f)$ となる。このとき x : 代数的 $\Leftrightarrow f \neq 0$ が定義より言える。したがって環準同型定理より $\mathrm{Im}\phi = K[x] \cong K[X]/(f)$ となる。そして $K[X]/(f)$ は $\deg(f) = n$ 以上の次数の多項式を割り算によりその次数以下にするから $K[X]/(f) = \{a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} | a_i \in K\}$ で表せるので $K[x]$ も同型より有限次元である。

とくに $1, x, \cdots, x^{n-1}$ は $n-1$ 次以下の $K[x]$ の元が一次結合で表わせ、一次独立であるから K 上の $K[x]$ における基底となる。

□

定義 6.3. x が K 上代数的数のとき $f(x) = 0$ となる $f(\neq 0) \in K[X]$ のうち次数が最小で monic (最高次の係数が 1) であるものを x の K における最小多項式 (minimal polynomial) という。$\deg(f)$ を x の次数ともいう。

$f \in K[X]$ に対して $f = gh \Rightarrow f = g$ または $f = h$ となるとき f を既約多項式という。

例 6.4. $a \in \mathbb{Q}$ で平方数でないものにおいて $\sqrt{a} \in \mathbb{C}$ の $\mathbb{Q}$ の最小多項式は $X^2 - a \in \mathbb{Q}[X]$ である。

e, π は $\mathbb{Q}$ 上超越的である。

定義 6.5. K : 可換環、 $A : K - alg$ のとき $x \in A$ が K 上整 (integral)とは

$$^{\exists} f\ (\neq 0)\ \in K[X] : K \text{ 係数 monic 多項式 } s.t.\ f(x) = 0$$

となること。

例 6.6. $\sqrt{2}, 1/\sqrt{2}$ は $X^2-2, X^2-1/2$ を考えれば $\mathbb{Q}$ 上整。

しかし、 $1/\sqrt{2}$ は $\mathbb{Z}$ 上で代数的であるが $2X^2-1 \in \mathbb{Z}[X]$ の根で monic にならないので $\mathbb{Z}$ 上整ではない。

命題 6.7. K : 体、 $A : K-alg$ で $x \in A$ が代数的、その最小多項式を $f \in K[X]$ とする。

このとき以下が成立。

(1) $g \in K[X]$ について $g(x)=0 \Leftrightarrow f|g$

(2) $K[X]/(f) \xrightarrow{\sim} K[x], X(\mod f) \longmapsto x$ とできてとくに $1, x, \cdots, x^{n-1}$ は $K[x]$ の基底 $(n = \deg f)$

(3) $x \in A^\times \Leftrightarrow f(0) \neq 0$ でありこのとき $x^{-1} \in K[x]$

Proof. (1)

Euclid の割り算から $g = q \cdot f + r$ となる $q, r \in K[X], \deg r < \deg f$ がある。$g(x)=0$ より $q(x)f(x)+r(x) = r(x) = 0$ となるが $\deg f$ の最小性から $r=0$ であるので $g = q \cdot f$ となるため $f|g$ である。

逆は $f|g \Rightarrow g = f \cdot (x$ の多項式) で $f(x)=0$ より従う。

(2)

命題 (6.2) の (2) より従う。

(3)

$\Rightarrow$

$f = X^n + a_{n-1}X^{n-2} + \cdots + a_1 X + a_0$ とする。$x \in A^\times$ より $f(x)=0$ から

$$-\frac{a_0}{x} = -(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1)$$

であり $\deg f$ の最小性からこの右辺は $\neq 0$ なので $-a_0/x \neq 0 \Rightarrow a_0 \neq 0$ より $f(0) = a_0 \neq 0$ となる。

$\Leftarrow$

$f(0) = a_0 \neq 0$ とすると $a_0 \in K^\times$ より

$$1 = x \cdot \frac{-(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1)}{a_0}$$

となりこの $-(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1)/a_0$ は $K[x]$ の元であり x の逆元 x^{-1} になるので $x \in A^\times$ と $x^{-1} \in K[x]$ が言えた。 □

6.2 代数拡大

定義 6.8. 体の拡大 L/K が代数的 (algebraic)とは $^\forall x \in L$ が K 上代数的であること。

超越的 (transcendental)とは代数的でないこと

Rem 6.9. L/K : 有限次拡大 $\Rightarrow$ L が代数的

Proof. $^\forall x \in L$ に対して $1, x, x^2, \cdots, x^n, \cdots$ を考えると $[L:K]$ が有限よりこれは K 上一次独立でないからある有限な n で $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$ となるような全てが 0 ではない $a_0, \ldots, a_{n-1} \in K$ が存在する。よって $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$ とすればこれは x を根にもつ $f \in K[X]$ より x は代数的でしたがって L は代数的。 □

一般に逆は成り立たない。

例 6.10. $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \cdots)/\mathbb{Q}$ は代数的だが有限次ではない。

Fact 6.11. 後に示す $x \in K$ の最小多項式 f に対して $[K(x):K] = \deg_K f$ を認めれば $[\mathbb{Q}(\sqrt{p_1}, \cdots, \sqrt{p_n}) : \mathbb{Q}] = 2^n$ が示される。上記の例ではこれを用いれば有限次ではないことがわかる。

補題 6.12. $A : K - alg$ で整域とする。このとき $x \in A$ が K 上代数的ならば x は $K[x]$ で可逆。

Proof. x の最小多項式を f とすると命題 (6.7) の (2) より $K[x] \xrightarrow{\sim} K[X]/(f)$ である。$x \in A$ より $K[x] \subset A$ より $K[x]$ も整域だから $K[X]/(f)$ も整域。したがって (f) は素イデアルなので f は既約多項式より $f(0) \neq 0$ である。これより命題 (6.7) の (3) から $x \in A^\times, x^{-1} \in K[x]$ となる。 □

命題 6.13. L/K において次は同値。

(1) L/K は代数的

(2) L/K の任意の部分 $K - alg$ は体。

Proof. (1) $\Rightarrow$ (2)

任意の部分 $K - alg, A$ をとる。これは $A \subset L$ より整域であるので補題 (6.12) より $^\forall x \in A \subset L$ に対して L/K が代数的で x が代数的なので x は $K[x] \subset A$ で可逆。したがって A は体。

(2) $\Rightarrow$ (1)

L の任意の元 x をとる。このとき $K[x]$ は $K - alg$ より仮定から体なので $x^{-1} \in K[x]$ をもつ。よってある n 次多項式で $x^{-1} = a_n x^n + \cdots + a_1 x + a_0$ と書ける。$1 = x \cdot x^{-1} = a_n x^{n+1} + \cdots a_0 x$ で $a_n \in K^\times$ より $f = X^{n-1} + \cdots a_0/a_n X - 1/a_n$ とすればこれは $f \in K[X]$ で $f(x) = 0$ となるから x は K 上代数的。よって L/K は代数的。 □

命題 6.14. L/K において $x \in L$ が K 上代数的ならばその最小多項式を f として $K[x] = K(x) \cong K[X]/(f)$ であり、$[K(x):K] = \deg_K(x)$ となる。

Proof. 命題 (6.13) と (6.7) より $K[x]$ は体であり $K[x] \cong K[X]/(f)$ で $\dim_K K[x] = n = \deg f$ が成り立つ。よって体 $K(x) = \{q(x) | q(X) \in K[X]\}$ の定義より $K(x) = K[x]$ となる。そして $\dim_K K[x] = \dim_K K(x) = [K(x):K] = n = \deg_K f$ である。 □

系 6.15. L/K : 有限次拡大は $L = K(a_1, \ldots, a_r), (a_i \in L)$ の形で $K \subset K(a_1) \subset \cdots \subset K(a_1, \ldots, a_r) = L$ と体の拡大の列ができる。

a_i の $K(a_1, \ldots, a_{i-1})$ 上の拡大次数を n_i とし最小多項式を $f_i \in K(a_1, \ldots, a_{i-1})[X]$ とすると $[L:K] = n_1 \cdots n_r$ で $\{a_1^{\nu_1} \cdots a_r^{\nu_r} | 0 \leq \nu_i \leq n_i\}$ は L の K 上の基底となる。

$$L \cong \left(\left(\left(\frac{K[X_1]}{(f_1)} \right) [X_2]/(f_2) \right) \cdots \right) [X_r]/(f_r)$$

が成り立つ。

Proof. 命題 (6.14) を繰り返し用いれば良い。 □

補題 6.16. K 上代数的数 x, y に関して、$x+y, xy, x-y$ も代数的であり、y が 0 で無いのなら x/y も代数的である。

Proof. $x+y, xy, x-y, xy \in K(x,y)$ であり、x, y の最小多項式をそれぞれ f, g とするとともに有限次。したがって $K(x,y) = K(x)(y)$ は拡大次数が最小多項式の次数と等しいことから有限次拡大である。よって K

上の代数拡大であるのでそこに含まれる元は K 上代数的。 □

命題 6.17. $L/M/K$ を拡大の列とするとき以下が成り立つ。

$$L/K \text{ が代数的} \Leftrightarrow L/M, M/K \text{ がともに代数的}$$

Proof. $(\Rightarrow)$ は $M \supset K$ より明らか。

$(\Leftarrow)$

$^{\forall}x \in L$ が K 上代数的であることを示す。x は M 上代数的なので $^{\exists}f = \sum_{i=0}^{n} a_i X^i \in M[X], f(x) = 0$ となる。また、 $a_i \in M$ よりこれは K 上代数的であるので命題 (6.14) で L を M と、 x を a_i とみれば $K' = K[a_0, \ldots, a_n]$ は体で $K(a_0, \ldots, a_n)$ と等しい。したがって K の有限次拡大であり $f \in K'[X]$ で x は K' 上代数的である。同様に命題 (6.14) から $K'[x] \cong K'[X]/(f)$ となる。ここでこの右辺は命題 (6.7) の (2) から $\dim_{K'} K'[X]/(f) = n$ なので左辺は K' 上有限次拡大。そして K' は K 上有限次拡大であったので $K'[x]$ は K 上有限次拡大。したがって Rem(6.9) より $K'[x]/K = K[a_1, \ldots, a_n, x]/K$ は代数拡大なので $x \in K'[x] \subset L$ は K 上代数的。 □

命題 6.18. $M_1/K, M_2/K$: 代数拡大 $\Rightarrow$ 任意の合成拡大 (L, u_1, u_2) は K 上代数的

Proof. $^{\forall}x \in M_1$ は K 上代数的より最小多項式 $f = \sum_{i=0}^{n} a_i X^i, f(x) = 0$ が存在する。そして u_1 は $K-$準同型より $0 = u_1(f(x)) = u_1(\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} u_1(a_i) u_1(x)^i = \sum_{i=0}^{n} a_i u_1(x)^i = f(u_1(x))$ となるから $u_1(x)$ は K 上代数的になる。u_2 も同様に考えると $u_1(M_1), u_2(M_2)$ は K 上代数的である。補題 (6.16) よりこの集合間の四則演算は全て代数的なので $L = K(u_1(M_1), u_2(M_2))$ は代数的である。 □

命題 6.19. $M_1/K, M_2/K$:

定義 6.20. L/K : 拡大とする。

K の L の中での相対的代数閉包 (relative algebraic closure) M とは

$$M := \{x \in L | x \text{ は } K \text{ 上代数的 }\}$$

となるもの。これを $\overline{K}$ と書くこともある。

また、 K が L の中で (相対的に) 閉じているとは $K = M$ となること。

命題 6.21. 上の定義における相対的代数閉包 M は体。

Proof. 補題 (6.16) より和と積について M は閉じている。

$K(x) \subset M$ であり、 $K(x)$ は x を含む最小の L の部分体より $x^{-1}, -x \in K(x) \subset M$ なので逆元も存在する。 □

例 6.22. K の $K(X)$ (X は変数) の中での相対的代数閉包は X は変数なのでそれが含まれると K 上代数的でなくなるため K である。

$\mathbb{R}$ の $\mathbb{C}$ の中での相対的代数閉包は $\mathbb{C}$ と一致するが $\mathbb{Q}$ の $\mathbb{C}$ の中での相対的代数閉包 $\overline{\mathbb{Q}}$ は $\mathbb{C}$ と一致しない。