代数的整数論

2025 年 7 月 29 日

目次

ここで環とは零環でない単位的可換環とする.

1 代数体の整数環

Def 1.1

$\mathbb{Q}$ の有限次拡大体を**代数体**という. $[K:\mathbb{Q}]=d$ であるとき, K は d **次体**という.

代数体は $\overline{\mathbb{Q}}\subset\mathbb{C}$ の部分体と見做せる.

Def 1.2

A,B を環とする. 環準同型 $\varphi:A\to B$ によって B を A 代数と見做す.
$x\in B$ が A **上整**とは,

$$\exists a_1,\cdots,a_n\in A,\ x^n+\varphi(a_1)x^{n-1}+\cdots+\varphi(a_n)=0$$

B の任意の元が A 上整であるとき, B は A 上整であるという. 特に B が A の拡大環なら, B は A の**整拡大**であるという.

Remark 1.1. A 上整とは $\varphi(A)$ 係数の monic 多項式の根となる, ということである

Prop 1.1

$A\subset B$ を環拡大とする. $x\in B$ について次は同値

(1) x は A 上整
(2) $A[x]\subset C$ なる部分環 $C\subset B$ で, A 加群として有限生成なものが存在する.

Proof. (1)⇒(2) $x\in B$ は $f(T)=T^n+a_1T^{n-1}+\cdots+a_n\in A[T]$ の根とする. 準同型定理より全射準同型 $A[T]/(f(T))\to A[x]$ がある. $A[T]/(f(T))$ は有限生成加群なので $A[x]$ も有限生成加群. よって $C=A[x]$ とすればよい.
(2)⇒(1) 略 ■

Prop 1.2

$A\subset B\subset C$ を環拡大とする.

(1) B は有限生成 A 加群かつ C は有限生成 B 加群 $\Rightarrow$ C は有限生成 A 加群.
(2) $x\in C$ が A 上整 $\Rightarrow$ x は B 上整.
(3) C が A 上整 $\Rightarrow$ B は A 上整.
(4) $b_1,\cdots,b_n\in B$ が A 上整 $\Rightarrow$ $A[b_1,\cdots,b_n]$ は有限生成 A 加群.
特に $\{x\in B\mid x:A\text{上整}\}$ は B の部分環.

(5) C が B 上整かつ B が A 上整 $\Rightarrow$ C は A 上整.

Proof. (1) $\{b_1, \cdots, b_s\}$ を B の A 基底，$\{c_1, \cdots, c_t\}$ を C の B 基底とすると，$\{b_i c_j \mid 1 \leq i \leq s, 1 \leq j \leq t\}$ は C の A 基底となる．

(2) 自明

(3) (2) から自明

(4) $b_1, \cdots, b_n \in B$ は A 上整とする．

$$A_0 := A, A_1 := A[b_1], A_2 := A[b_1, b_2], \cdots, A_n := [b_1, \cdots, b_n]$$

とすると各 i に対し，b_i は A 上整なので (2) から A_{i-1} 上整．よって **Prop 1.1** より A_i は有限生成 A_{i-1} 加群である．(1) から A_n は有限生成 A 加群．

(5) $c \in C$ とすると，

$$\exists f(T) = T^n + b_1 T^{n-1} + \cdots + b_n \in B[T], f(c) = 0$$

$b_1, \cdots, b_n \in B$ は A 上整なので，$A[b_1, \cdots, b_n]$ は有限生成 A 加群．c は $A[b_1, \cdots, b_n]$ 上整なので $A[b_1, \cdots, b_n, c]$ は **Prop 1.1**(1)⇒(2) により $A[b_1, \cdots, b_n, c]$ は有限生成 $A[b_1, \cdots, b_n]$ 加群．よって (1) より $A[b_1, \cdots, b_n, c]$ は有限生成 A 加群．**Prop 1.1**(2)⇒(1) により c は A 上整．

■

Def 1.3

A を整域，$K = \mathrm{Frac}(A)$ とする．

$A \subset L$ なる体 L に対し，$B := \{x \in L \mid x : A\text{上整}\}$ を L の A における**整閉包**という．

A の K における整閉包が A となるとき，A を**整閉整域**または**正規環**という．

Remark 1.2. **Prop 1.2**(4) より，L の A における整閉包は L の部分環になる．

Remark 1.3. 環での整，整拡大，整閉包は体での代数的，代数拡大，代数閉包に対応する．

Def 1.4

$\mathbb{Z}$ 上整な複素数を**代数的整数**という．$\mathbb{C}$ の $\mathbb{Z}$ における整閉包（代数的整数の全体）を**代数的整数環**といい，Ω で表す．$K \subset \mathbb{C}$ が代数体のとき，K における $\mathbb{Z}$ の整閉包を $\mathcal{O}_K$ とかき，K の**整数環**という．つまり $\mathcal{O}_K = K \cap \Omega$ である．

Prop 1.3

B は整域，$A \subset B$ は部分環，B は A 上整とする．このとき，

$$A \text{ が体} \Leftrightarrow B \text{ が体}$$

Proof. (⇒) $x \in B \backslash \{0\}$ とすると,

$$\exists a_1, \cdots, a_n \in A, x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

$a_n = 0$ なら $x(x^{n-1} + a_1 x^{n-2} + \cdots + a_{n-1}) = 0$ なので $x^{n-1} + a_1 x^{n-2} + \cdots + a_{n-1} = 0$. これを繰り返して $a_n \neq 0$ と仮定してよい．このとき,

$$x(x^{n-1} + a_1 x^{n-2} + \cdots + a_{n-1}) = -a_n \in A^\times$$
$$\therefore x^{-1} = -a_n^{-1}(x^{n-1} + a_1 x^{n-2} + \cdots + a_{n-1}) \in B$$

よって $B \backslash \{0\} \subset B^\times$ なので B は体.
(⇐) $x \in A \backslash \{0\}$ とすると，$A \subset B$ で生成される B は体なので $x^{-1} \in B$ である．よって

$$\exists a_1, \cdots, a_n \in A, x^{-n} + a_1 x^{-(n-1)} + \cdots + a_n = 0$$

両辺に x^n をかけると $1 + a_1 x + \cdots + a_n^n = 0$ なので $-1 = x(a_1 + \cdots + a_1 x^{n-1})$ を得る.

$$\therefore x^{-1} = -(a_1 + \cdots + a_1 x^{n-1}) \in A$$

よって $A \backslash \{0\} \subset A^\times$ なので A は体. ■

Lem 1.1
A, B は整域，$S \subset A$ は積閉集合とする.

$$A \subset B \text{ が整拡大} \Rightarrow S^{-1}A \subset S^{-1}B \text{ も整拡大}$$

Proof. $S^{-1}B$ は環として B と $\{s^{-1} \mid s \in S\}$ で生成される．$\{s^{-1} \mid s \in S\} \subset S^{-1}A$ なので, $S^{-1}B$ は $S^{-1}A$ 上整である. ■

Prop 1.4
A を整域, $K = \mathrm{Frac}(A)$, L/K を有限次体拡大, B を A の L における整閉包, $S \subset A$ を積閉集合とする．このとき，$S^{-1}A$ の L における整閉包は $S^{-1}B$ である.
よって，A が正規環 $\Rightarrow$ $S^{-1}A$ も正規環．また $\mathrm{Frac}(B) = L$.

Proof. **Lem 1.1** より $S^{-1}B$ は $S^{-1}A$ 上整である．$x \in L$ が $S^{-1}A$ 上整であれば,

$$\exists a_1, \cdots, a_n \in A, \exists s_1, \cdots, s_n \in S, x^n + \frac{a_1}{s_1} x^{n-1} + \cdots + \frac{a_n}{s_n} = 0$$

$s := s_1 \cdots s_n, b_i := s a_i / s_i$ とおけば，$x^n + (b_1 x^{n-1} + \cdots + b_n)/s = 0$ となる．両辺に s^n をかけて,

$$(sx)^n + b_1 (sx)^{n-1} + s b_2 (sx)^{n-2} + \cdots + s^{n-1} b_n = 0$$

を得る．よって sx は A 上整．よって $sx \in B, x \in S^{-1}B$．A が正規環なら K における A の整閉包は A なので，$S^{-1}A$ の K における整閉包は $S^{-1}A$.

$S = A\backslash\{0\}$ とすれば，$S^{-1}A = K$ である．L は K 上整なので $S^{-1}B = L$．よって $\mathrm{Frac}(B) = L$. ■

Prop 1.5
A, B は整域，$A \subset B$ は整拡大とする．

(1) $\forall \mathfrak{p} \in \mathrm{Spec}(A), \exists \mathfrak{P} \in \mathrm{Spec}(B), \mathfrak{P} \cap A = \mathfrak{p}$
(2) $\mathfrak{P} \subset B$ が極大イデアル $\Rightarrow$ $\mathfrak{P} \cap A$ も極大イデアル

Proof. (1) $S := A\backslash\mathfrak{p}$ とすると，**Lem 1.1** より $S^{-1}B$ は $A_\mathfrak{p} = S^{-1}A$ の整拡大．局所化 $S^{-1}B$ は零環でないので $S^{-1}B$ には極大イデアル $\mathfrak{m}$ が存在する．$\mathfrak{m} \cap A_\mathfrak{p}$ は $A_\mathfrak{p}$ の真のイデアルであるから $A_\mathfrak{p}/(\mathfrak{m} \cap A_\mathfrak{p})$ は零環でなく，$S^{-1}B/\mathfrak{m}$ の部分環と見做せる．$S^{-1}B$ の元は $A_\mathfrak{p}$ 係数の monic 多項式の根であるから，$\mathfrak{m}, \mathfrak{m} \cap A_\mathfrak{p}$ を法として考えれば，$S^{-1}B/\mathfrak{m}$ は $A_\mathfrak{p}/(\mathfrak{m} \cap A_\mathfrak{p})$ 上整であることがわかる．$S^{-1}B/\mathfrak{m}$ は体なので **Prop 1.3** より $A_\mathfrak{p}/(\mathfrak{m} \cap A_\mathfrak{p})$ も体．よって $\mathfrak{m} \cap A_\mathfrak{p}$ は $A_\mathfrak{p}$ の極大イデアルである．$(A_\mathfrak{p}, \mathfrak{p}A_\mathfrak{p})$ は局所環なので $\mathfrak{m} \cap A_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$ である．$\mathfrak{P} := \mathfrak{m} \cap B$ とすると，$\mathfrak{m}$ は素イデアルなので $\mathfrak{P}$ も B の素イデアルである．**Prop ??**(2) により，

$$\mathfrak{P} \cap A = \mathfrak{m} \cap B \cap A = \mathfrak{m} \cap A = \mathfrak{m} \cap A_\mathfrak{p} \cap = \mathfrak{p}A_\mathfrak{p} \cap A = \mathfrak{p}$$

(2) $\mathfrak{p} := \mathfrak{P} \cap A$ とする．B の元は A 係数の monic 多項式の根であるから，$\mathfrak{P}, \mathfrak{p}$ を法として考えれば，$B/\mathfrak{P}$ は $A_\mathfrak{p}$ 上整であることがわかる．$B/\mathfrak{P}$ が体なので $A_\mathfrak{p}$ も体である．よって $\mathfrak{p}$ も極大イデアルである．

■

Example 1.1. $\mathbb{Z} \subset \mathbb{Z}[i]$ は整拡大である. $\mathfrak{p} = 3\mathbb{Z} \in \mathrm{Spec}(\mathbb{Z})$ に対し, $\mathfrak{P} = 3\mathbb{Z}[i] \in \mathrm{Spec}(\mathbb{Z}[i])$ とすれば $\mathfrak{P} \cap \mathbb{Z} = 3\mathbb{Z}$

Def 1.5
$A \subset B$ が環拡大で，$\mathfrak{P} \in \mathrm{Spec}(B)$，$\mathfrak{p} = \mathfrak{P} \cap A$ であるとき，$\mathfrak{P}$ は $\mathfrak{p}$ **の上にある素イデアル**であるという．