

## 5 体上の代数

### 5.1 $K$ -代数

**定義 5.1.** 環  $A$  の中心  $Z(A)$  とは任意の  $A$  の元と可換な  $A$  の元でありつまり  $Z(A) := \{x \in A \mid \forall a \in A, ax = xa\}$  となる集合でありこれは  $A$  の部分環を成す。

*Proof.* 部分環を成すことを示す。

結合則や分配則は  $A$  が環であることより保証される。 $\forall a \in A$  について単位元は定義より  $a1 = a = 1a, a0 = 0 = 0a$  より中心に含まれる。また、 $\forall x, y \in Z(A), a(x+y) = ax+ay = xa+ya = (x+y)a, a(xy) = (ax)y = (xa)y = x(ay) = x(ya) = (xy)a$  より加法乗法について閉じているから  $Z(A)$  は  $A$  の部分環である。  $\square$

**定義 5.2.**  $K$ -体とする。(可換環でもよい)

このとき  $K$ -代数 ( $K$ -algebra)  $A$  とは以下の同値な条件のうち一つを、すなわち全てを満たすような零環にならないものである。

(1). 単位的環であって環準同型  $\phi: K \rightarrow A$  が与えられており  $\text{Im}(\phi) \subset Z(A) = (A \text{ の中心})$  となるもの。  
 $K$  が体であれば  $\text{Im}(\phi) = K \subset Z(A) \subset A$  とみなすことができる

(2).  $K$ -加群であり環としての構造を持ち、積が任意の  $k \in K, x, y \in A$  にたいして  $k(xy) = (kx)y = x(ky)$  が成り立つような  $K$ -双線型となるもの。

とくに  $K$  倍できてそれが双線型であり  $K$  が体であれば  $K$ -ベクトル空間とみなすこともできる。そして  $[A:K] := \dim_K(A)$  を  $A$  の  $K$  上の次数という。

$K$ -代数  $A$  を  $K$ -alg,  $\phi: K \rightarrow A$  と書くときもある。

*Proof.* 両方共環であることは共通しているから  $\text{Im}(\phi) \subset Z(A)$  と  $K$ -加群であり積が上記のように成り立つことが同値であることを示せば良い。

まずスカラー乗法を  $\cdot: K \times A \rightarrow A, (k, a) \mapsto \phi(k)a$  と定めれば  $ka := \phi(k)a$  とすることで  $K$  によるスカラー乗法が定義でき、これにより  $K$ -加群の構造を持つことができる。

また、 $\text{Im}(\phi) \subset Z(A)$  より  $A$  の結合則から  $\forall a, b \in A, k(ab) = \phi(k)(ab) = (\phi(k)a)b = (ka)b = (a\phi(k))b = (ak)b = a(\phi(k)b) = a(kb)$  より成り立つ。双線型であることも環  $A$  の定義から明らか。

逆は環準同型  $\phi: K \rightarrow A$  を適切につくれば  $k(xy) = (kx)y = x(ky)$  より像は中心に含まれるので成り立つ。

$K$  が体のとき Note (??) から  $\phi$  が単射準同型より  $K = \text{Im}(\phi)$  と同一視できるため  $K$ -代数  $A$  は実際に  $K$  を部分環として含んでいる。  $\square$

**例 5.3.**  $K$  を体としたときその多変数多項式環  $A := K[X_1, \dots, X_n]$  は可換環で  $K$  係数より  $K$ -alg である。また、 $I$  を  $A$  のイデアルとしたときその剰余環  $K[X_1, \dots, X_n]/I$  も同様の理由で  $K$ -alg である。

$L_i/K$  を  $K$  のある体拡大とするとその拡大の直積  $A := L_1 \times \dots \times L_n$  はそれぞれの成分ごとに拡大体の演算によって  $L_i/K$  より  $a \in K$  倍を  $(a, \dots, a) \in K \times \dots \times K$  と同一視することで  $K$ -alg とみなせる。

以上の2つはもともと可換な構造の上であったのでそのまま中心に埋め込めたが  $A = M_n(K)$  とした行列

環は非可換でありこのときは以降のように定めることで非可換な  $K\text{-alg}$  になる。すなわち、

$$K \longrightarrow A$$

$$a \longmapsto \begin{pmatrix} a & & \\ & \ddots & \\ & & a \end{pmatrix}$$

となる環準同型でこの像は単位行列の定数倍なので  $A$  の中心に入るため  $K\text{-alg}$  になる。

以下では  $K$ -代数は断らない限り全て可換であるとする。

**定義 5.4.**  $K\text{-alg}, \phi: K \longrightarrow A, \psi: K \longrightarrow B$  があるとする。このとき  $K$ -代数の準同型  $\varphi: A \longrightarrow B$  とは環準同型であって  $K\text{-alg}$  としての構造と可換なもの、つまり  $\psi = \varphi \circ \phi$  となるもののこと。

これと同値なものとして  $\varphi$  が  $K$ -加群の準同型写像であることという定義でも良い。

*Proof.* 同値性を示す。

$\psi = \varphi \circ \phi$  となっていて  $\forall x, y \in A, \varphi(xy) = \varphi(x)\varphi(y), \varphi(x+y) = \varphi(x) + \varphi(y)$  が環準同型であることより成り立つ。 $k \in K$  について  $K\text{-alg}$  のスカラー倍の定義から  $\phi(k) \cdot 1 = k \in A, \psi(k) \cdot 1 = k \in B$  とみなせる。このとき  $\varphi(k) = \varphi(\phi(k) \cdot 1) = \varphi \circ \phi(k) \cdot \varphi(1) = \varphi \circ \phi(k) = \psi(k) = \psi(k) \cdot 1 = k$  より  $K$  の元について不変となる。

□

## 5.2 元の添加

**定義 5.5.**  $L/K$ : 体の拡大、 $S: L$  の部分集合のとき、 $K(S) := (S$  を含む最小の  $K$  の拡大体  $\subset L)$  と定義し、これを  $K$  上  $S$  で生成される部分体という。 $S = \{a_1, \dots, a_n\}$  なら  $K(S) = K(a_1, \dots, a_n)$  と書く。

$S, T$  と 2 つの  $L$  の部分集合があるときその 2 つのを含む最小の  $K$  の拡大体は集合  $S \cup T$  を含むと考えれば良いので  $K(S \cup T) = K(S)(T) = K(T)(S)$  となりこれを  $K(S, T)$  と書く。

**定義 5.6.**  $L/K$  が有限生成とは  $L = K(S)$  となる有限集合  $S \subset L$  が存在すること。

特に一元集合で生成されるとき  $L/K$  は 単生、単元生成 (monogenic) という。

**Rem 5.7.** 有限次拡大  $\Rightarrow$  有限生成

*Proof.*  $[L:K] = n$  とするとき  $L$  の  $K$  上の基底を  $\{w_1, \dots, w_n\}$  とする。 $K(w_1, \dots, w_n)$  はこの基底を含む体なので  $K$  上の線形結合も含むことを考えればこれは  $L$  と一致するから有限生成。 □

ここで逆は成り立たない。 $K(X), X$ : 変数とするとこれは有理関数体で単生だが  $1, X, \dots, X^n, \dots$  が全て異なるので  $K$  の無限次拡大となるような反例があるためである。

## 5.3 体の合成

**定義 5.8.**  $M_1/K, M_2/K$ : 体の拡大としたときこの 2 つの 合成、合成体、合成拡大 (a composite extension) とは三組  $(L, u_1, u_2)$  で

1.  $L$  は  $K$  の拡大体。

2.  $u_i : M_i \longrightarrow L$  は  $K$  の拡大の準同型で  $L$  は  $u_1(M_1) \cup u_2(M_2)$  により生成される。

となるようなもののことである。したがって写像のとり方の自由性から  $M_1/K, M_2/K$  に対しこれらの合成はいくつもありえる。