中心的単純多元環

渡部 隆夫

平成１７年度 (２００５年) 後期

1　代数系について (用語と記号のまとめ)

環, 体, 加群についての定義をまとめておく.

- **環**

  集合 R 上に 2 つの演算

  $$R \times R \to R : (a,b) \mapsto a+b, \qquad R \times R \to R : (a,b) \mapsto a \cdot b$$

  が定義されており, これらが次の四条件をみたすときに R を**環**という.

  (R1) R は加法 $+$ に関してアーベル群をなす.

  (R2) R は乗法 $\cdot$ に関して結合法則 $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ をみたす.

  (R3) R は分配法則

  $$a \cdot (b+c) = a \cdot b + a \cdot c, \qquad (a+b) \cdot c = a \cdot c + b \cdot c$$

  をみたす.

  (R4) R の加法に関する単位元を 0 と表すとき, R の元 $e \neq 0$ で, 任意の $a \in R$ について $e \cdot a = a \cdot e = a$ となるものが存在する.

  この e を R の**単位元**とよび, 1 または 1_R と表す. 加法に関する単位元は**零元**とよばれ 0 または 0_R と表す.

- **可換環**

  環 R が乗法に関して交換法則 $a \cdot b = b \cdot a$ をみたすとき, R を**可換環**という. また可換でない環を**非可換環**という.

- **中心**

  R を環とするとき, R の部分集合 Z_R を

  $$Z_R = \{a \in R \mid \text{任意の } b \in R \text{ で } a \cdot b = b \cdot a \text{ が成り立つ}\}$$

  で定義する. Z_R は R の**中心**とよばれる. Z_R は R の部分環である.

- **単数群**

  R を環とする. R の元 a に対して,

  $$a \cdot b = b \cdot a = 1_R$$

  をみたす $b \in R$ が存在するとき, a を**可逆元**という. またこの b を a^{-1} で表し, a の**逆元**という. R の可逆元全体の集合を $R^\times$ と表す. $R^\times$ は乗法に関して群を成す. この群を R の**単数群**という.

- **斜体**

  集合 K が次の二条件をみたすとき K を**斜体**という.

  (K1) K は環である.

  (K2) $K^\times = K - \{0\}$, 即ち K の零元以外の元は可逆元である.

さらに K が可換環ならば K は単に**体**とよばれる.

- **非可換体**

  斜体 K が非可換環であるとき, K は**非可換体**とよばれる.

- **多元環**

  K を体とする. 集合 A が環であり同時に K 上のベクトル空間でもあって, 任意の $\lambda \in K$, $a, b \in A$ について

$$(\lambda \cdot a) \cdot b = a \cdot (\lambda \cdot b) = \lambda \cdot (a \cdot b)$$

  が成り立つとき, A を K 上の**多元環**または K **多元環**という. A が K 多元環ならば, 写像

$$K \longrightarrow A : \lambda \mapsto \lambda 1_A$$

  は単射環準同型になる. この像 $K \cdot 1_A$ を K と同一視することにより, 以下では $K \subset A$ であるとする.

- **加群**

  R を環とし, M を加法 $+$ の定義されたアーベル群とする. 写像 (スカラー倍)

$$M \times R \longrightarrow M : (u, a) \mapsto ua \tag{1}$$

  が定義されており, 任意の $a, b \in R, u, v \in M$ で次が成り立つとき, M を**右** R **加群**であるという.

  (M1) $(u + v)a = ua + va$

  (M2) $u(a + b) = ua + ub$

  (M3) $u(a \cdot b) = (ua)b$

  (M4) $u1_R = u$

  同様に**左** R **加群**が定義される.

- **両側加群**

  R_1 と R_2 を環として, M が左 R_1 加群かつ右 R_2 加群であるとする. このとき, 任意の $a_1 \in R_1, a_2 \in R_2, u \in M$ で

$$(a_1 u)a_2 = a_1(u a_2)$$

  が成り立つならば, M は (R_1, R_2) **両側加群**であるという.

- **単純加群**

  R を環とする. 右または左 R 加群 M は, $\{0\}$ と M 自身以外に部分 R 加群をもたないとき, **単純**であるという

- **イデアル**

  環 R 自身を右 (左)R 加群とみなすとき, R の部分 R 加群を**右 (左) イデアル**という. 右かつ左イデアルを両側イデアルという.

- **単純環**

  環 R は, $\{0\}$ と R 自身以外に両側イデアルをもたないとき, **単純**であるという.

2　行列環

2.1　加群の自己準同型環

R を環とする.

定義　M を右 R 加群とするとき

$$\mathrm{End}_R(M) = \{f : M \longrightarrow M \mid f \text{ は } R \text{ 準同型 }\}$$

とする. $\mathrm{End}_R(M)$ には和と積が

$$(f+g)(u) = f(u) + g(u), \qquad (f \circ g)(u) = f(g(u)) \qquad (u \in M)$$

により定義される. この演算により, $\mathrm{End}_R(M)$ は環となる. この環を M の**自己準同型環**という.

写像

$$\mathrm{End}_R(M) \times M \longrightarrow M : (f, u) \mapsto f(u)$$

により, M は左 $\mathrm{End}_R(M)$ 加群になる. R 準同型写像の定義から, M は両側 $(\mathrm{End}_R(M), R)$ 加群になる.

定義　$\mathrm{End}_R(M)$ の単数群を $\mathrm{Aut}_R(M)$ で表し, M の**自己同型群**という.

$$\mathrm{Aut}_R(M) = \{f \in \mathrm{End}_R(M) \mid f \text{ は全単射 }\}$$

である.

定理 1 (Schur)　M が単純右 R 加群ならば, 環 $\mathrm{End}_R(M)$ は斜体である.

証明　$f \in \mathrm{End}_R(M)$, $f \neq 0$ とする. f は恒等的に 0 ではないから, $\mathrm{Ker}f \subsetneqq M$ かつ $\{0\} \subsetneqq \mathrm{Im}f$ である. M の単純性により, $\mathrm{Ker}f = \{0\}$ かつ $\mathrm{Im}f = M$ でなければならないから, f は全単射, 即ち $f \in \mathrm{Aut}_R(M)$ である.

2.2　行列環

一般に R を環として, m, n を自然数とするとき, $M_{m,n}(R)$ により R に成分をもつ $m \times n$ 行列全体の集合を表すことにする. とくに $m = n$ のときは, $M_{n,n}(R)$ を $M_n(R)$ と表す. $M_n(R)$ は通常の行列の加法と乗法により環となり, R に成分をもつ n **次行列環**とよばれる. 各 $i = 1, 2, \cdots, n$, $j = 1, 2, \cdots, n$ に対して, $\boldsymbol{e}_{ij}$ を (i, j) 成分だけが 1 で, それ以外の成分が 0 であるような $M_n(R)$ の元とする. この本では $\boldsymbol{e}_{ij}$ を $M_n(R)$ の**行列単位**とよぶことにする. 容易にわかるように $\boldsymbol{e}_{ij}$ は次の関係式をみたす.

$$\boldsymbol{e}_{ij} \cdot \boldsymbol{e}_{kl} = \begin{cases} \boldsymbol{e}_{il} & (j = k) \\ 0_{M_n(R)} & (j \neq k) \end{cases} \qquad (1 \leq i, j, k, l \leq n).$$

また $\boldsymbol{e}_{ij}$ で生成された左イデアル $M_n(R)\boldsymbol{e}_{ij}$ と右イデアル $\boldsymbol{e}_{ij}M_n(R)$ はそれぞれ

$$M_n(R)\boldsymbol{e}_{ij} = \left\{ \begin{pmatrix} 0 & \cdots & 0 & a_{1i} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & a_{ni} & 0 & \cdots & 0 \end{pmatrix} \mid j \text{ 列成分 } a_{1i}, \cdots, a_{ni} \in R \right\},$$

$$\boldsymbol{e}_{ij}M_n(R) = \left\{ \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \\ a_{j1} & \cdots & a_{jn} \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \mid i \text{ 行成分 } a_{j1}, \cdots, a_{jn} \in R \right\}$$

となる. 行列環 $M_n(R)$ は右自由 R 加群の自己準同型環と同一視できる. 列ベクトルの形で与えられる右自由 R 加群を

$$R^n = \left\{ \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \mid a_1, a_2, \cdots, a_n \in R \right\}$$

としよう. R^n の基底として

$$\boldsymbol{e}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \qquad \boldsymbol{e}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \qquad \cdots, \qquad \boldsymbol{e}_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

が取れる. 以下 $\boldsymbol{e}_1, \cdots, \boldsymbol{e}_n$ を R^n の標準基底とよぶことにする. $\mathrm{End}_R(R^n)$ の元 f に対し,

$$f(\boldsymbol{e}_j) = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{nj} \end{pmatrix}, \qquad (a_{1j}, a_{2j}, \cdots, a_{nj} \in R, \ \ j = 1, 2, \cdots, n)$$

とする. $M_n(R)$ の元 a_f を $a_f = (a_{ij})_{1 \le i,j \le n}$ により定義すれば,

$$f(u) = a_f \cdot u \qquad (u \in R^n)$$

が成り立つ. 写像 $f \mapsto a_f$ は, 環の同型 $\mathrm{End}_R(R^n) \cong M_n(R)$ を与える. 以下では, この対応により $\mathrm{End}_R(R^n)$ と $M_n(R)$ とを同一視しよう.

2.3 行列環の単純性

D を斜体とする.

命題 1 $M_n(D)$ は単純である.

証明　$\boldsymbol{e}_{ij}$, $(1 \le i, j \le n)$ を $M_n(D)$ の行列単位とする．I を $M_n(D)$ の $\{0_{M_n(D)}\}$ とは異なる両側イデアルとすれば, $0_{M_n(D)}$ とは異なる元 $a \in I$ がとれる．a の (k,l) 成分 a_{kl} が 0 ではないとする．このとき

$$(a_{kl}^{-1}\boldsymbol{e}_{ik}) \cdot a \cdot \boldsymbol{e}_{li} = \boldsymbol{e}_{ii}$$

が各 $i = 1, 2, \cdots, n$ で成り立つ．I は両側イデアルだから

$$1_{M_n(D)} = \boldsymbol{e}_{11} + \boldsymbol{e}_{22} + \cdots + \boldsymbol{e}_{nn} = \sum_{i=1}^{n} (a_{kl}^{-1}\boldsymbol{e}_{ik}) \cdot a \cdot \boldsymbol{e}_{li} \in I$$

となり, I は乗法の単位元を含む．したがって $I = M_n(D)$ となる．

命題 2 D^n は単純左 $M_n(D)$ 加群である．

証明　D^n の標準基底を $\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_n$ として, $M_n(D)$ の行列単位を $\{\boldsymbol{e}_{ij}\}_{1 \le i,j \le n}$ とする．D^n の 0 とは異なる元 $u = \boldsymbol{e}_1 a_1 + \cdots + \boldsymbol{e}_n a_n$, $(a_1, \cdots, a_n \in D)$ をとる．ある番号 j について $a_j \neq 0$ であるから, 各 $i = 1, 2, \cdots, n$ について, $a_j^{-1}\boldsymbol{e}_{ij}$ を左から u に掛ければ

$$a_j^{-1}\boldsymbol{e}_{ij} u = \boldsymbol{e}_i$$

となる．したがって, 基底 $\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_n$ は u で生成された部分 $M_n(D)$ 加群 $M_n(D)u$ に含まれる．よって $M_n(D)u = D^n$ が任意の $u \in D$, $u \neq 0$ で成り立つ．

命題 3 任意の単純左 $M_n(D)$ 加群は D^n に同型である．さらに任意の有限生成な左 $M_n(D)$ 加群は D^n の直和と同型になる．

証明　$M_n(D)$ の行列単位を $\{\boldsymbol{e}_{ij}\}_{1 \le i,j \le n}$ とすれば,

$$1_{M_n(D)} = \boldsymbol{e}_{11} + \boldsymbol{e}_{22} + \cdots + \boldsymbol{e}_{nn}$$

である．M を単純左 $M_n(D)$ 加群として, 0 とは異なる $u \in M$ をとる．このとき

$$u = 1_{M_n(D)} u = \boldsymbol{e}_{11} u + \boldsymbol{e}_{22} u + \cdots + \boldsymbol{e}_{nn} u$$

であるから, 少なくとも一つの i で $\boldsymbol{e}_{ii} u \neq 0$ でなければならない．$\boldsymbol{e}_{ii} u$ で生成された部分 $M_n(D)$ 加群を $M_n(D)\boldsymbol{e}_{ii} u$ とする．M の単純性から $M = M_n(D)\boldsymbol{e}_{ii} u$ である．また $M_n(D)\boldsymbol{e}_{ii}$ は左 $M_n(D)$ 加群として D^n と同型である．写像

$$M_n(D)\boldsymbol{e}_{ii} \longrightarrow M_n(D)e_{ii}u = M \,:\, a \mapsto au$$

は全射 $M_n(D)$ 準同型で, $M_n(D)\boldsymbol{e}_{ii} \cong D^n$ の単純性から単射である．したがって, これは左 $M_n(D)$ 加群の同型を与える．
次に M を有限生成な左 $M_n(D)$ 加群とする．$M_n(D)$ の部分環 $\{a 1_{M_n(D)} \mid a \in D\}$ を D と同一視することにより, M は左 D 加群とも見なせる．

$$M_n(D) = \sum_{1 \le i,j \le n} D\boldsymbol{e}_{ij}$$

であるから, M は左 D 加群としても有限生成である. よって M は有限次元左 D ベクトル空間となる. また M の任意の部分 $M_n(D)$ 加群は, ベクトル空間としての部分空間となる. さて, D 上の次元を考えることにより, M には, M 自身とは異なる極大な部分 $M_n(D)$ 加群が存在することがわかる. その一つを N としよう. $u \in M$ を $u \notin N$ であるようにとる. N の極大性から, 剰余加群 M/N は単純で, $M = N + M_n(D)u$ が成り立つ.

$$M_n(D)u = M_n(D)\boldsymbol{e}_{11}u + M_n(D)\boldsymbol{e}_{22}u + \cdots + M_n(D)\boldsymbol{e}_{nn}u$$

と分解すれば, 少なくとも一つの i で, $\{0\} \subsetneqq M_n(D)\boldsymbol{e}_{ii}u \not\subset N$ が成り立つ. このとき, 前半の証明と同じ議論から $D^n \cong M_n(D)\boldsymbol{e}_{ii}u$ が従い, とくに $M_n(D)\boldsymbol{e}_{ii}u$ は単純である. $M_n(D)\boldsymbol{e}_{ii}u \cap N$ は $M_n(D)\boldsymbol{e}_{ii}u$ の部分 $M_n(D)$ 加群で, $M_n(D)\boldsymbol{e}_{ii}u \not\subset N$ であったから $M_n(D)\boldsymbol{e}_{ii}u \cap N = \{0\}$ となる. また M/N は単純であるから $M = N + M_n(D)\boldsymbol{e}_{ii}u = N \oplus M_n(D)\boldsymbol{e}_{ii}u \cong N \oplus D^n$ となる. 後は D 上の次元に関する帰納法により結論を得る.

3　単純環の構造定理

R を環として, I を $\{0\}$ とは異なる R の右イデアルとする. $A \subset R$, $B \subset R$ に対し

$$AB = \{\sum a_i b_i \mid a_i \in A,\ b_i \in B\}$$

とおく.

3.1　極小イデアル

定義　R の右イデアル J で, $\{0\} \subsetneqq J \subsetneqq I$ となるものが存在しないとき, I を**極小**であるという. これは I が右 R 加群として単純ということと同値である.

$\mathrm{End}_R(I)$: 右 R 加群としての I の自己準同型環

補題 1　I を極小右イデアルとする.

(1)　$x \in I$, $x \neq 0$ ならば, $I = xR$ である.

(2)　$x \in I$, $xI \neq \{0\}$ ならば, I の元 e で, $e^2 = e$ かつ $xe = x$ を満たすものが存在する.

証明　(1) $x \neq 0$ より, $\{0\} \subsetneqq xR \subset I$ である. I の極小性から $I = xR$ でなければならない.
(2) R 準同型写像 $\varphi : I \longrightarrow I$ を $\varphi(a) = xa$ により定義する. $\varphi \in \mathrm{End}_R(I)$ で, 定理 1 から $\varphi \in \mathrm{Aut}_R(I)$. $x \in I$ であるから, I の元 e で $\varphi(e) = x$ となるものが存在する. 即ち $xe = x$. よって $x(e^2 - e) = 0$ で, 単射性から $e^2 = e$ である.

一般に, R の 0 とは異なる元 e で $e^2 = e$ を満たすものを**べき等元**という. e がべき等元のとき, 集合 $eRe = \{eae \mid a \in R\}$ は, R の加法と乗法で閉じている. 即ち, 任意の $eae, ebe \in eRe$ について

$$eae + ebe = e(a+b)e \in eRe \qquad (eae)(ebe) = e(aeb)e \in eRe$$

である. さらに

$$e(eae) = eae = (eae)e$$

であるから, e が eRe の乗法の単位元となり, また $0_R \in eRe$ が零元となる. したがって eRe は環になる.

補題 2　$e \in R$ をべき等元として, e から生成された単項右イデアルを $I = eR$ とする. また右 R 加群としての I の自己準同型環を $\mathrm{End}_R(I)$ とする. $f \in \mathrm{End}_R(I)$ に対し, $\psi(f) = f(e)e$ とすれば, $\psi(f) \in eRe$ であり, これから定義される写像

$$\psi : \mathrm{End}_R(I) \longrightarrow eRe$$

は環の全射準同型写像になる. さらに I が極小ならば, ψ は同型写像になる.

証明　$f \in \mathrm{End}_R(I)$ とすると, $f(e) \in I = eR$ だから $f(e)e \in Ie = eRe$ である. ψ が準同型であることを示そう. $f, g \in \mathrm{End}_R(I)$ とする. まず

$$\psi(f+g) = (f+g)(e)e = (f(e)+g(e))e = f(e)e + g(e)e = \psi(f) + \psi(g)$$

が成り立つ．次に $f(e)=ea$, $g(e)=eb$ とするとき, f が R 準同型であることと $e^2=e$ から

$$
\begin{aligned}
\psi(f\circ g) &= (f\circ g)(e)e = f(g(e))e = f(eb)e = f(e)be = f(e^2)be = f(e)ebe \\
&= eaebe = (eae)(ebe) = \psi(f)\psi(g)
\end{aligned}
$$

が成り立つ．また $\mathbf{id}_I \in \mathrm{End}_R(I)$ を I の恒等写像とすれば, $\psi(id_I)=e^2=e$ である．よって ψ は環の準同型写像である．全射であることを示そう．任意に与えられた $c\in R$ に対して, $f_c\in\mathrm{End}_R(I)$ を $f_c(x)=ecx$ $(x\in I)$ により定義する．このとき $\psi(f_c)=ece$ となるから ψ は全射である．さて $\mathrm{Ker}\psi \subsetneqq \mathrm{End}_R(I)$ は両側イデアルである．I が極小ならば $\mathrm{End}_R(I)$ は斜体になるから, $\mathrm{Ker}\psi=\{0\}$ でなければならない．よって ψ は同型写像になる．

3.2 Wedderburn の構造定理

右イデアル I に対し, 右 R 加群としての I の自己準同型環を $S=\mathrm{End}_R(I)$ とおき, さらに左 S 加群としての I の自己準同型環を $T=\mathrm{End}_S(I)$ とおく．I は両側 (S,R) 加群および両側 (S,T) 加群の二つの構造をもつ．R の元 a に対し, $\iota_a\in T$ を

$$u\cdot\iota_a = ua \qquad (u\in I)$$

と定義する．対応 $a\mapsto\iota_a$ は環準同型 $\iota:R\longrightarrow T$ を与える．

補題 3 $a\in I$ ならば, 任意の $t\in T$ について $\iota_a t=\iota_{a\cdot t}$ が成り立つ．とくに ι による I の像 $\iota(I)$ は T の右イデアルである．

証明　I の元 b に対し, $s_b\in S$ を

$$s_b\cdot u = bu \qquad (u\in I)$$

により定義する．このとき, 任意の $t\in T$ と $a\in I$ に対して

$$(ba)\cdot t = (s_b\cdot a)\cdot t = s_b\cdot(a\cdot t) = b(a\cdot t)$$

であるから,

$$b\cdot(\iota_a t) = (b\cdot\iota_a)\cdot t = b\cdot\iota_{a\cdot t}$$

が任意の $b\in I$ で成り立つ．これから $\iota_a t=\iota_{a\cdot t}$ となる．

命題 4 R が単純環ならば, $\iota:R\longrightarrow T$ は同型写像である．

証明　R の単純性から, ι は単射であることが従う．ι が全射であることを示そう．ι の像を $\iota(R)$ と表す．$\iota_{1_R}=1_T\in\iota(R)$ であるから, $\iota(R)T\subset\iota(R)$ を示せばよい．I から生成された R の左イデアルを RI としよう．I は元々右イデアルであったから, RI は両側イデアルになる．R は単純であるから $R=RI$ が成り立つ．よって, $\iota(R)=\iota(R)\iota(I)$ となり, 前の補題から $\iota(I)T=\iota(I)$ であるから $\iota(R)T\subset\iota(R)$ が従う．

定理 2 R を単純環とする．このとき次の (1) と (2) は同値である．

(1) R は極小右イデアルをもつ.

(2) R は斜体 D 上の n 次行列環 $M_n(D)$ と同型になる.

証明　(1) を仮定しよう. I を極小な右イデアルとする. 右 R 加群として I は単純であるから, $\mathrm{End}_R(I)$ は斜体になる. そこで $D = \mathrm{End}_R(I)$ とおく. I が左 D ベクトル空間として有限次元であることを示そう. $J = \{a \in R \mid Ia = \{0\}\}$ とすると, J は R の両側イデアルになる. $J \subsetneq R$ であるから, R の単純性により $J = \{0\}$ である. とくに $II \neq \{0\}$ が成り立ち, 補題から I に含まれるべき等元 e が存在する. I の極小性から $I = eR$ で, D は $Ie = eRe$ と同型になる. よって Ie は D ベクトル空間として 1 次元である. $S = \{a \in R \mid \dim_D Ia < \infty\}$ とすれば, S は R の両側イデアルで, 上で見たように $e \in S$ であるから, $\{0\} \subsetneq S$ である. したがって R の単純性により $S = R$, とくに $1_R \in S$ で, $\dim_D I = n < \infty$ が成り立つ. これから同型 $R \cong \mathrm{End}_D(I) \cong M_n(D)$ を得る.

命題 5 D_1 と D_2 は斜体で $M_{n_1}(D_1) \cong M_{n_2}(D_2)$ ならば, $n_1 = n_2$ かつ $D_1 \cong D_2$ である.

証明　$R \cong M_{n_1}(D_1) \cong M_{n_2}(D_2)$ として, I を極小右イデアルとする. 定理 1 から $D = \mathrm{End}_R(I)$ は斜体である. $e_{11} \in M_{n_1}(D_1)$ を行列単位として, $I = e_{11}M_{n_1}(D_1)$ にとる. $e_{11} \in I$ はべき等元だから, 補題 2 から, $D \cong e_{11}Re_{11} \cong D_1$ となる. 同様に $D \cong D_2$ を得るから $D_1 \cong D_2$ である. また命題 3 から, $\dim_D I = n_1 = n_2$ である.

命題 6 R が単純環ならば Z_R は体である. とくに R は Z_R 上の多元環である

証明　$a \in Z_R$, $a \neq 0$ ならば, $Ra = aR$ であるから, Ra は両側イデアルとなる. 単純性から $Ra = R$ となり, a は逆元 $a^{-1} \in R$ をもつ. 任意の $b \in R$ について, $a \cdot b = b \cdot a$ であるから, $b \cdot a^{-1} = a^{-1} \cdot b$ が成り立つ. したがって $a^{-1} \in Z_R$ である.

命題 7 D を斜体とする. このとき $Z_{M_n(D)} = Z_D$ である.

4　中心的単純多元環

K を体とする.

4.1　中心的単純多元環

定義　K 上の多元環 R が次の 2 条件をみたすとき, **中心的単純多元環**という.

(CS1) R は K 上有限次元の単純環である.

(CS2) $Z_R = K$ である.

記述を簡単にするために, 次の記号を使う.

$$\begin{aligned}
\mathfrak{A}(K) &= K \text{ 多元環の集合} \\
\mathfrak{A}_s(K) &= K \text{ 上の有限次元単純多元環の集合} \\
\mathfrak{A}_{cs}(K) &= K \text{ 上の中心的単純多元環の集合} \\
\mathfrak{D}(K) &= K \text{ 上の有限次元中心的斜体の集合}
\end{aligned}$$

明らかに

$$\mathfrak{D}(K) \subset \mathfrak{A}_{cs}(K) \subset \mathfrak{A}_s(K) \subset \mathfrak{A}(K)$$

である. 次は構造定理と命題 7 の結論である.

定理 3 $R \in \mathfrak{A}_s(K)$ ならば, K 上有限次元の斜体 D が存在して $R \cong M_n(D)$ となる. とくに $R \in \mathfrak{A}_{cs}(K)$ ならば $D \in \mathfrak{D}(K)$ である.

定理 4 K が代数的閉体とする. このとき $\mathfrak{A}_s(K) = \mathfrak{A}_{cs}(K)$, $\mathfrak{D}(K) = \{K\}$ で, 任意の $A \in \mathfrak{A}_s(K)$ は行列環 $M_n(K)$ と同型になる.

証明　$A \in \mathfrak{A}_s(K)$ に対し, $K \subset Z_A$ である. Z_A/K は有限次拡大だから $K = Z_A$ で, $A \in \mathfrak{A}_{cs}(K)$ となる. よって $\mathfrak{A}_s(K) = \mathfrak{A}_{cs}(K)$ である. 定理 3 から, $A \cong M_n(D)$, $D \in \mathfrak{D}(K)$ となる. 任意の $a \in D$ に対し, $K \subset K(a) \subset D$ をとれば, $K(a)/K$ は有限次拡大になるから, $K = K(a)$ で, とくに $a \in K$. したがって $D = K$ で, $A \cong M_n(K)$ となる.

4.2　多元環のテンソル積

一般に $A, B \in \mathfrak{A}(K)$ に対し, A と B の K 上のテンソル積を $A \otimes B$ で表す. $A \otimes B \in \mathfrak{A}(K)$ である.

命題 8 $A, B \in \mathfrak{A}(K) \implies Z_{A\otimes B} = Z_A \otimes Z_B$.

証明　$\{b_i\}$ を B の K 上の基底とすると, $A \otimes B$ の元 x は

$$x = \sum_i x_i \otimes b_i, \qquad (x_i \in A)$$

と一意に書ける．$x \in Z_{A\otimes B}$ ならば, 任意の $a \in A$ について $(a \otimes 1)x = x(a \otimes 1)$, 即ち

$$\sum_i (ax_i) \otimes b_i = \sum_i (x_i a) \otimes b_i$$

が成り立つ．一意性から各 i について $ax_i = x_i a$ でなければならないから, 結局 $x_i \in Z_A$ である．したがって $Z_{A\otimes B} \subset Z_A \otimes B$ が言えた．次に $\{a_i\}$ を Z_A の K 上の基底とすれば, $Z_A \otimes B$ の元 y は

$$y = \sum_i a_i \otimes y_i, \qquad (y_i \in B)$$

と一意に書ける．もし $y \in Z_{A\otimes B}$ ならば上と同様に $y_i \in Z_B$ となり, よって $Z_{A\otimes B} \subset Z_A \otimes Z_B$ が言える．逆の包含関係 $Z_A \otimes Z_B \subset Z_{A\otimes B}$ は明らかである．

定理 5 $A \in \mathfrak{A}_{cs}(K)$, $B \in \mathfrak{A}(K)$ とする．$0 \neq I \subset A \otimes B$ が両側イデアルならば, I は $1_A \otimes b \neq 0$ という形の元を含む.

証明 A は単純環であるから, 任意の $0 \neq a \in A$ に対し, $x_1, x_1', x_2, x_2', \cdots, x_m, x_m' \in A$ で

$$\sum_{i=1}^{m} x_i a x_i' = 1_A \tag{2}$$

となるものが存在することに注意する．
$x \in I$ に対し

$$p(x) = \min\{j \mid x = a_1 \otimes b_1 + \cdots + a_j \otimes b_j, \quad a_i \in A, \ \ b_i \in B\}$$

とおき

$$p = \min\{p(x) \mid 0 \neq x \in I\}$$

とする．まず $p = 1$ を示す．$p > 1$ と仮定してみる．

$$x \in I, \quad p(x) = p, \ \ x = a_1 \otimes b_1 + \cdots + a_p \otimes b_p$$

をとる．上の注意から $a_p = 1_A$ としてよい．このとき, a_{p-1} と a_p は 一次独立．(そうでなければ $p(x) < p$ となり矛盾)．とくに $a_{p-1} \notin Z_A$, 従って

$$^{\exists}c \in A, \quad ca_{p-1} - a_{p-1}c \neq 0$$

よって

$$x' = (c \otimes 1)x - x(c \otimes 1) = (ca_1 - a_1 c) \otimes b_1 + \cdots + (ca_{p-1} - a_{p-1}c) \otimes b_{p-1} \neq 0$$

で $p(x') < p$ で矛盾. 故に $p = 1$．これから $0 \neq a \otimes b \in I$ がとれる．上の注意から

$$\sum_i (x_i \otimes 1)(a \otimes b)(x_i' \otimes 1) = 1_A \otimes b \in I$$

である.

系 1 $A \in \mathfrak{A}_{cs}(K)$, $B \in \mathfrak{A}_s(K) \implies A \otimes B \in \mathfrak{A}_s(K)$.

証明　$0 \neq I \subset A \otimes B$ を両側イデアルとすれば, $0 \neq 1_A \otimes b \in I$ が取れる. B も単純だから, $y_1, y_1', \cdots, y_n, y_n' \in B$ で

$$\sum_{i=1}^{n} y_i b y_i' = 1_B$$

となるものが取れる. したがって

$$\sum_{i=1}^{n} (1_A \otimes y_i)(1_A \otimes b)(1_A \otimes y_i') = 1_A \otimes 1_B \in I$$

である.

系 2 $A, B \in \mathfrak{A}_{cs}(K) \implies A \otimes B \in \mathfrak{A}_{cs}(K)$.

4.3　係数拡大

次は命題 8 と系 1 の結論である.

命題 9 L/K を拡大体とする. このとき $A \in \mathfrak{A}_{cs}(K)$ ならば $A \otimes L \in \mathfrak{A}_{cs}(L)$ である.

系 3 任意の $A \in \mathfrak{A}_{cs}(K)$ に対し, $\dim_K A$ は平方数である.

証明　$\overline{K}/K$ を K の代数閉包とする. 定理 4 から $A \otimes \overline{K} \cong M_n(\overline{K})$ となるから, $\dim_K A = n^2$ である.

定義　$A \in \mathfrak{A}_{cs}(K)$, $D \in \mathfrak{D}(K)$ で, $A \cong M_m(D)$ とする. $\deg A = \sqrt{\dim_K A}$ を A の**次数**, $\mathrm{ind} A = \sqrt{\dim_K D}$ を A の**指数**という.

4.4　反転多元環

定義　$A \in \mathfrak{A}(K)$ とする. A に新しい乗法 $\circ : A \times A \longrightarrow A$ を

$$a \circ b = ba \qquad (a, b \in A)$$

により定義する. この積 $\circ$ により A は K 上の多元環となる. これを A の**反転多元環**といい, A° により表す. $A \in \mathfrak{A}_{cs}(K) \iff A^\circ \in \mathfrak{A}_{cs}(K)$ である.

命題 10 $A \in \mathfrak{A}_{cs}(K)$, $\deg A = n$ とする. このとき多元環の同型 $A \otimes A^\circ \cong \mathrm{End}_K(A) \cong M_{n^2}(K)$ がある.

証明　証明. $a \in A$ と $b \in A^\circ$ に対して, $\psi_{a,b} \in \mathrm{End}_K(A)$ を $\psi_{a,b}(x) = axb$ $(x \in A)$ と定義する. これから写像

$$\psi : A \otimes A^\circ \to \mathrm{End}_K(A) \ : \ \sum_{i=1}^{m} a_i \otimes b_i \mapsto \sum_{i=1}^{m} \psi_{a_i,b_i}$$

が定義され, 容易に確かめられるように ψ は多元環の準同型になる. $A \otimes A^\circ$ は単純環だから ψ は単射である. 次元を比較することにより ψ は同型写像になることがわかる.

4.5　Brauer 群

定義　$A, B \in \mathfrak{A}_{cs}(K)$ に対し, ある $1 \leqq p, q \in \mathbf{Z}$ が存在して

$$A \otimes M_p(K) \cong B \otimes M_q(K)$$

となるとき, A と B は **Brauer 同値**であるといい, $A \sim B$ と表す. これは同値関係である. A を含む同値類を $[A]$ と表す. また

$$\mathrm{Br}(K) = \mathfrak{A}_{cs}(K)/\sim = \text{同値類全体の集合}$$

とおく.

命題 11　$D_1, D_2 \in \mathfrak{D}(K)$ とする. このとき

$$M_n(D_1) \sim M_m(D_2) \iff D_1 \sim D_2 \iff D_1 \cong D_2$$

である.

証明　これは命題５より従う.

命題 12　$A, B \in \mathfrak{A}_{cs}(K)$ に対し

$$A \cong B \iff A \sim B \ \text{かつ} \ \deg A = \deg B$$

命題 13　$\mathfrak{D}(K)/\cong$ を K 上有限次元の中心的斜体の同型類の集合とする. このとき写像

$$\mathfrak{D}(K)/\cong \longrightarrow \mathrm{Br}(K) \ : \ (D \text{ の同型類}) \mapsto [D]$$

は全単射である.

証明　これは定理３と命題１１による.

命題 14 Br(K) に積を

$$[A] \cdot [B] = [A \otimes B], \qquad (A, B \in \mathfrak{A}_{cs}(K))$$

により定義する．このとき

(1) この積は well-definied である.

(2) $[K]$ が単位元になる.

(3) $[A]$ の逆元は $[A]^{-1} = [A^{\circ}]$ である.

が成り立つ.

証明 証明は容易.

定義 上で与えられた積により Br(K) はアーベル群になる．これを K の **Brauer 群**という.

命題 15 L/K を拡大体とする．このとき写像

$$\mathrm{Br}(K) \longrightarrow \mathrm{Br}(L) \ : \ [A] \mapsto [A \otimes L]$$

は群の準同型である.

5 単純多元環の部分環と部分体

5.1 中心化定理

定義 $A \in \mathfrak{A}(K)$ で, X が A の部分集合であるとき, 集合

$$\{a \in A \mid 任意の\ x \in X\ について\ ax = xa\}$$

を X の A における**中心化**とよび $Z_A(X)$ と表す．明らかに $Z_A(X)$ は A の部分多元環になる．

定理 6 $A \in \mathfrak{A}_{cs}(K)$ で, B を A の単純部分多元環とする．このとき $Z_A(B)$ は単純部分多元環で

$$\dim A = \dim B \dim Z_A(B)$$

が成り立つ．

証明 同型写像 $\psi : A \otimes A^{\circ} \longrightarrow \mathrm{End}_K(A)$ により, A を左 $A \otimes A^{\circ}$ 加群とみなす．$B \otimes A^{\circ}$ は $A \otimes A^{\circ}$ の部分環であるから, A は左 $B \otimes A^{\circ}$ 加群ともみなせる．$f \in \mathrm{End}_K(A)$ に対し, $f \in \mathrm{End}_{B\otimes A^{\circ}}(A)$ であるためには

$$f \circ \psi_{b,a} = \psi_{b,a} \circ f \qquad (b \in B,\ \ a \in A^{\circ})$$

となることが必要十分である．したがって, ψ は同型

$$Z_{A\otimes A^{\circ}}(B \otimes A^{\circ}) \cong \mathrm{End}_{B\otimes A^{\circ}}(A)$$

を引き起こす．ここで

$$Z_{A\otimes A^{\circ}}(B \otimes A^{\circ}) \cong Z_A(B) \otimes Z_{A^{\circ}} \cong Z_A(B)$$

である． 仮定により $B \otimes A^{\circ}$ は単純環であるから, 極小左イデアル $I \subset B \otimes A^{\circ}$ が存在し, $D = \mathrm{End}_{B\otimes A^{\circ}}(I)$ は斜体で, I の右 D ベクトル空間としての次元を s とすると $B \otimes A^{\circ} \cong \mathrm{End}_D(I) \cong M_s(D)$ となる．また, 左 $B \otimes A^{\circ}$ 加群としての同型 $A \cong I^{\oplus k}$ が存在する．このとき

$$Z_A(B) \cong \mathrm{End}_{B\otimes A^{\circ}}(I^k) \cong M_k(D)$$

となり, $Z_A(B)$ は単純環になる．さらに

$$\dim Z_A(B) = k^2 \dim D, \quad \dim B \otimes A^{\circ} = s^2 \dim D, \quad \dim A = k \dim I = ks \dim D.$$

したがって $\dim B \dim C = \frac{s}{k} k^2 \dim D = \dim A$ である．

系 4 $A \in \mathfrak{A}_{cs}(K)$ で, B を A の中心的単純部分 K 多元環とするならば, K 多元環の同型 $A \cong B \otimes Z_A(B)$ がある．

証明 $Z_A(B)$ は中心的単純部分 K 多元環となる．したがって $B \otimes Z_A(B)$ も中心的単純 K 多元環である．写像

$$B \times Z_A(B) \to A : x \otimes y \mapsto xy$$

は同型 $B \otimes Z_A(B) \cong A$ を引き起こす．

5.2　極大部分体

$A \in \mathfrak{A}_{cs}(K)$ とする．

定義　拡大体 L/K で $L \subset A$ であるものを A の**部分体**という．A の部分体の中で極大のものを**極大部分体**という．

命題 16　$L \subset A$ を部分体とする．このとき

(1) $C = Z_A(L)$ とすれば, C は単純環で $Z_C = L$. 即ち $C \in \mathfrak{A}_{cs}(L)$ である．

(2) $\deg A = [L:K] \deg C$. とくに $[L:K] \mid \deg A$ である．

証明　(1) 定理６から C は単純部分多元環である．また定理６の証明で $B = L$ とすると, ある斜体 D が存在して

$$C = Z_A(L) \cong M_k(D), \qquad L \otimes A^\circ \cong M_s(D)$$

となる．$L \otimes A^\circ \in \mathfrak{A}_{cs}(L)$ だから $D \in \mathfrak{D}(L)$ である．よって $C \in \mathfrak{A}_{cs}(L)$ となる．
(2) $\dim_L C = m^2$ とすれば, 定理６から

$$\dim_K A = \dim_K L \dim_K C = [L:K]m^2[L:K] = [L:K]^2 m^2 .$$

よって $\deg A = [L:K]m$ である．

定義　部分体 $L \subset A$ で, $[L:K] = \deg(A)$ となるものを**強極大部分体**という．

強極大部分体は必ずしも存在するとは限らない．たとえば $M_n(\mathbf{C})$.

命題 17　$D \in \mathfrak{D}(K)$ とする．このとき $L \subset D$ が極大部分体ならば, L は強極大部分体である．とくに D は強極大部分体をもつ．

証明　$C = Z_D(L)$ とする．命題１６から, $L = Z_C \subset C \subset D$ である．$L \subsetneq C$ ならば, $c \in C$, $c \notin L$ が存在する．C は斜体だから, $L(c)$ は体となり L の極大性に反する．よって $L = C$ で, $\deg D = [L:K]$ が成り立つ

5.3　分解体

定義　$A \in \mathfrak{A}_{cs}(K)$, $\deg A = n$ とする．拡大体 L/K で

$$A \otimes L \cong M_n(L)$$

となるとき, この L を A の**分解体**という．

命題 18 $A \in \mathfrak{A}_{cs}(K)$, $D \in \mathfrak{D}(K)$ で, $A \sim D$ とする．このとき拡大 L/K について

$$L \text{ が } A \text{ の分解体} \iff L \text{ が } D \text{ の分解体}$$

命題 19 $D \in \mathfrak{D}(K)$ とする．有限次拡大 L/K が D の分解体ならば $\deg D \,|\, [L:K]$ である．

証明　$\deg D = d$ とすると, $D \otimes L \cong M_d(L)$ である．V を単純左 $D \otimes L$ 加群とする．$V \cong L^d$ だから, 左 D 加群として $M_d(L) \cong V^{\oplus d}$ である．よって

$$[L:K] = \dim_D D \otimes L = \dim_D M_d(L) = \dim_D V^{\oplus d} = d \dim_D V$$

であるから, $d|[L:K]$.

命題 20 $D \in \mathfrak{D}(K)$ で, $L \subset D$ を部分体とする．このとき

$$L \text{ が極大部分体} \iff L \text{ が強極大部分体} \iff L \text{ が } D \text{ の分解体}$$

である．

証明　$\deg D = d$ とする．
$(\Longleftarrow)$ 命題１６から $[L:K]|d$ で, 命題１９から $d|[L:K]$. したがって $[L:K] = d$.
$(\Longrightarrow)$ $[L:K] = d$ だから $\dim_L D = d$ である．D 自身を両側 (D, L) 加群とみる．これは準同型

$$\varphi \,:\, D \otimes L^\circ = D \otimes L \longrightarrow \mathrm{End}_L(D) = M_d(L)$$

を引き起こす．系１より $D \otimes L$ は単純だからこれは単射．次元が等しいから同型になる．

補題 4 $D \in \mathfrak{D}(K)$ で, D の任意の部分体が K 上純非分離拡大ならば $D = K$ である．

証明　$d = \deg D$ として, $L \subset D$ を極大部分体とする．このとき $[L:K] = d$ である．
($\mathrm{ch}(K) = 0$ のとき) $1 < d$ ならば L/K は分離拡大になるから仮定に矛盾．よって $d = 1$ で, $D = K$ である．
($\mathrm{ch}(K) = p > 0$ のとき) L/K は純非分離拡大だから $d = [L:K] = p^m$ となる．K の代数的閉包を $\overline{K}$ とすると, $D \otimes \overline{K} \cong M_d(\overline{K})$ である．自然な単射

$$D \hookrightarrow D \otimes \overline{K} \,:\, a \mapsto a \otimes 1$$

と合成して, K 多元環の準同型

$$\varphi \,:\, D \longrightarrow M_d(\overline{K})$$

がある．任意の $a \in D$ に対し, $K(a)/K$ は純非分離拡大だから

$$a^{p^k} = \lambda \in K$$

となる．ここで $p^k = [K(a):K]|d = p^m$. したがって, $M_d(\overline{K})$ の中で

$$(\varphi(a) - \lambda^{1/p^k} 1_d)^{p^k} = 0$$

である．とくに $\varphi(a) - \lambda^{1/p^k} 1_d$ はベキ零行列で, そのトレースをとれば

$$\mathrm{Tr}(\varphi(a)) - d\lambda^{1/p^k} = \mathrm{Tr}(\varphi(a) - \lambda^{1/p^k} 1_d) = 0.$$

もし $1 < d$ ならば, $p|d$ だから $d\lambda^{1/p^k} = 0$ で,

$$\mathrm{Tr}(\varphi(a)) = 0 \qquad (a \in D)$$

$M_d(L) = D \otimes \overline{K} = \varphi(D)\overline{K}$ だから, これは任意の $x \in M_d(\overline{K})$ で $\mathrm{Tr}(x) = 0$ を導き矛盾. よって $d = 1$ で, $D = K$ となる.

定理 7 任意の $D \in \mathfrak{D}(K)$ に対し, 極大部分体 $L \subset D$ で, L/K が分離拡大となるものが存在する.

証明

$$L = K \text{ 上分離的な } D \text{ の部分体の中で極大のもの}$$

とおく．$C = Z_D(L)$ とすれば, 命題１６より $C \in \mathfrak{D}(L)$ である．$L \subsetneqq C$ ならば, 分離拡大 $L \subsetneqq L' \subset C$ が存在し, L'/K も分離拡大になるから, L の極大性に矛盾する．よって $L = C$, 即ち $L = Z_D(L)$ となり, L は極大部分体になる.

系 5 任意の $A \in \mathfrak{A}_{cs}(K)$ は, K 上ガロア拡大であるような分解体をもつ.

6 Skolem-Noether の定理

6.1 Skolem-Noether の定理

補題 5 $R \in \mathfrak{A}_s(K)$ として, M_1 と M_2 を有限生成左 R 加群とする. このとき

$$\dim_K M_1 = \dim_K M_2 \iff M_1 \cong M_2$$

である.

証明 定理 3 と命題 3 より, M_1, M_2 は単純 R 加群 N の有限個の直和に同型である. $M_1 \cong N^k$, $M_2 \cong N^\ell$ とすると

$$\dim_K M_1 = \dim_K M_2 \iff k = \ell \iff M_1 \cong M_2$$

となる.

定義 $A \in \mathfrak{A}_{cs}(K)$ とする. 単数 $a \in A^\times$ に対し,

$$i_a : A \longrightarrow A : i_a(x) = axa^{-1} \qquad (x \in A)$$

とおく. i_a は K 多元環の自己同型写像である. この形の写像を**内部自己同型**という.

内部自己同型の全体 $\mathrm{Inn}(A) = \{i_a \mid a \in A^\times\}$ は群になる. これを**内部自己同型群**という. 写像 $a \mapsto i_a$ は群の同型 $A^\times / Z_A^\times \cong \mathrm{Inn}(A)$ を与える.

定理 8 (Skolem-Noether) $A \in \mathfrak{A}_{cs}(K)$, $R \in \mathfrak{A}_s(K)$ で, $f, g : R \longrightarrow A$ は K 多元環の自明でない準同型とする. このとき $i_a \in \mathrm{Inn}(A)$ で, $g = i_a \circ f$ となるものが存在する.

証明 $D \in \mathfrak{D}(K)$ で, $A \cong M_n(D) = \mathrm{End}_D(D^n)$ となるものがとれる. D° を D の反転多元環とする. このとき $V = D^n$ (右 D 加群) は

$$(A \otimes D^\circ) \times V \longrightarrow V : (a \otimes d, v) \mapsto avd$$

により左 $A \otimes D^\circ$ 加群と見なせる. 写像 $f : R \longrightarrow A$ により V を左 $R \otimes D^\circ$ 加群と見たものを V_f と表す. 即ち

$$V_f = V, \quad (R \otimes D^\circ) \times V_f \longrightarrow V_f : (\alpha \otimes d, v) \mapsto f(\alpha)vd$$

である. 同様に写像 $g : R \longrightarrow A$ により V を左 $R \otimes D^\circ$ 加群と見たものを V_g で表す. 定理 4 から $R \otimes D^\circ \in \mathfrak{A}_s(K)$ である. $\dim_K V_f = \dim_K V = \dim_K V_g$ だから, 補題 8 により左 $R \otimes D^\circ$ 加群として $V_f \cong V_g$ となる. 即ち同型写像

$$\varphi : V_f \longrightarrow V_g, \quad \varphi(f(\alpha)vd) = g(\alpha)\varphi(v)d \qquad (\alpha \in R,\ d \in D,\ v \in V)$$

が存在する. これは右 D 加群としての同型でもあるから $\varphi \in \mathrm{Aut}_D(V) \cong A^\times$ である. 対応する $A^\times$ の元を a とすれば

$$a \cdot f(\alpha)v = \varphi(f(\alpha)v) = g(\alpha)\varphi(v) = g(\alpha)a \cdot v$$

が任意の $v \in V$ で成り立つ. よって $g(\alpha) = af(\alpha)a^{-1} = i_a \circ f(\alpha)$ が任意の $\alpha \in R$ で成り立つから, $g = i_a \circ f$ である.

系 6 $A \in \mathfrak{A}_{cs}(K)$ で, R は A の単純部分多元環とする. 任意の自明でない準同型 $f : R \longrightarrow A$ に対し, $i_a \in \mathrm{Inn}(A)$ で $f = i_a|_R$ となるものが存在する.

6.2 実数体の Brauer 群

定理 9 (Frobenius) $D \in \mathfrak{D}(\mathbf{R}) \implies D \cong \mathbf{H}$.

証明 $1 < \deg D$ とする. $L \subset D$ を極大部分体とする. $1 < d = [L : \mathbf{R}] = 2$ となる. $L = \mathbf{C}$ としてよい.

$$\tau : \mathbf{C} \longrightarrow \mathbf{C} : \alpha + \beta\sqrt{-1} \mapsto \alpha - \beta\sqrt{-1}$$

とする. Skolem-Noether の定理から, ある $i_a \in \mathrm{Inn}(D)$ で, $i_a|_{\mathbf{C}} = \tau$ となるものが存在する.

$$a(\alpha + \beta\sqrt{-1})a^{-1} = \alpha - \beta\sqrt{-1}\,.$$

とくに $i_{a^2}|_{\mathbf{C}}$ は恒等写像だから, $a^2 \in Z_D(\mathbf{C}) = \mathbf{C}$. さらに

$$\tau(a^2) = aa^2a^{-1} = a^2$$

から $a^2 \in \mathbf{R}$ となる. $a^2 > 0$ ならば $a^2 = t^2$ $(t \in \mathbf{R})$ で, $a = \pm t$ となり, $i_a|_{\mathbf{C}} \neq \tau$ で矛盾. したがって $a^2 < 0$ で, $a^2 = -t^2$ とおける.

$$\boldsymbol{i} = \sqrt{-1}, \quad \boldsymbol{j} = at^{-1}, \quad \boldsymbol{k} = \boldsymbol{ij}$$

とおけば,

$$\boldsymbol{i}^2 = \boldsymbol{j}^2 = \boldsymbol{k}^2 = \boldsymbol{ijk} = -1$$

で, $\dim_{\mathbf{R}} D = 4$ から $D = \mathbf{R}1 + \mathbf{R}\boldsymbol{i} + \mathbf{R}\boldsymbol{j} + \mathbf{R}\boldsymbol{k}$ となり, $D \cong \mathbf{H}$ を得る.

系 7 $\mathrm{Br}(\mathbf{R}) \cong \{\pm 1\}$.

6.3 有限体の Brauer 群

補題 6 G は有限群で, $H \subsetneqq G$ は部分群とする. このとき

$$\bigcup_{g \in G} gHg^{-1} \subsetneqq G$$

である.

証明 $[G : H] = n > 1$, $|H| = h$ とすると $|G| = nh$. G/H の代表元を $g_1, \cdots, g_n$ とすると

$$\bigcup_{g \in G} gHg^{-1} = \bigcup_{i=1}^{n} g_iHg_i^{-1}$$

よって

$$\Bigl|\bigcup_{g \in G} gHg^{-1}\Bigr| \leqq \sum_{i=1} |g_iHg_i^{-1}| - (n-1) = nh - (n-1) < nh = |G|$$

定理 10 (Wedderburn) 有限非可換体は存在しない.

証明 D を有限非可換体とする. $K = Z_D$ は有限体である. $q = |K|$, $\deg D = d > 1$ とする. D の二つの極大部分体を L_1, L_2 とすれば, $[L_1 : K] = [L_2 : K] = d$ で $|L_1| = |L_2| = q^d$ である. 位数が同じ有限体は同型だから $L_1 \cong L_2$. Skolem-Noether の定理により, この同型は D の内部自己同型に延長される. とくに L_1 と L_2 は共役になる. したがって D の任意の極大部分体は互いに共役である. D の任意の元は, ある極大部分体に含まれるから, 結局

$$D^\times = \bigcup_{a \in D} a L_1^\times a^{-1}$$

となるが, 補題１０により, これは矛盾である.

系 8 K が有限体ならば $\mathrm{Br}(K) = 0$.

7　中心的単純多元環の構成例

7.1　巡回多元環

K は体とする. L/K を n 次巡回拡大として, そのガロア群を $\Gamma_{L/K} =< \sigma >$ とする.

定義　$a \in K^\times$ を固定し, x は不定元とする. x のべき $1 = x^0, x, x^2, \cdots, x^{n-1}$ で生成された L 上の n 次元ベクトル空間

$$V = L1 + Lx + \cdots + Lx^{n-1}$$

に積を次の関係で定義する.

$$(\alpha x^i)(\beta x^j) = \begin{cases} (\alpha\sigma^i(\beta))x^{i+j} & (i+j < n) \\ (a\alpha\sigma^i(\beta))x^{i+j-n} & (i+j \geqq n) \end{cases} \qquad (0 \leqq i, j \leqq n-1.\ \ \alpha, \beta \in L).$$

これは次の二つの関係式と同値である.

(CY1) $x^n = a$.

(CY2) $x\alpha = \sigma(\alpha)x$ $(\alpha \in L)$.

この積により V は K 多元環となる. これを**巡回多元環**といい, $V = (L/K, \sigma, a)$ と表す.

命題 21 $(L/K, \sigma, a) \in \mathfrak{A}_{cs}(K)$ である.

証明は後でより一般の接合積の場合に与える.

命題 22 L が $A \in \mathfrak{A}_{cs}(K)$ の強極大部分体ならば, 次の三条件をみたす要素 $u \in A^\times$ が存在する.

(CY0) $1, u, \cdots, u^{n-1}$ は L 上 A の基底である.

(CY1) $u^n \in K^\times$.

(CY2) $u\alpha u^{-1} = \sigma(\alpha)$ $(\alpha \in L)$.

とくに $A \cong (L/K, \sigma, u^n)$ である.

証明　Skolem-Noether の定理から, $\sigma : L \longrightarrow L$ はある $i_u \in \mathrm{Inn}(A)$ に拡張される. 即ち

$$u\alpha u^{-1} = \sigma(\alpha) \qquad (\alpha \in L).$$

これから

$$u^n\alpha u^{-n} = \sigma^n(\alpha) = \alpha \qquad (\alpha \in L).$$

したがって $u^n \in Z_A(L) = L$ で, さらに

$$\sigma(u^n) = uu^nu^{-1} = u^n$$

から $u^n \in K^\times$ である. $1, u, \cdots, u^{n-1}$ が L 上一次独立になることは容易にわかる. $\dim_L A = n$ だから, これらは A の基底になる.

系 9 $A \in \mathfrak{A}_{cs}(K)$ に対し, A が巡回多元環であるためには, A が K 上巡回拡大であるような強極大部分体をもつことが必要十分である.

定理 11 **(1)** n と k が互いに素ならば $(L/K, \sigma, a) \cong (L/K, \sigma^k, a^k)$.

(2) $(L/K, \sigma, a) \cong (L/K, \sigma, b) \iff ab^{-1} \in \mathrm{Nr}_{L/K}(L^\times)$.

(3) $(L/K, \sigma, a) \cong M_n(K) \iff a \in \mathrm{Nr}_{L/K}(L^\times)$.

証明 (1) $(L/K, \sigma^k, a^k) = L1 + Ly + \cdots + Ly^{n-1}$ とする. 写像

$$\varphi : (L/K, \sigma^k, a^k) \longrightarrow (L/K, \sigma, a) : \begin{cases} \varphi(\alpha) = \alpha \ \ (\alpha \in L) \\ \varphi(y) = x^k \end{cases}$$

は同型になる.
(2) $A = (L/K, \sigma, a)$, $B = (L/K, \sigma, b)$ とおき

$$B = L1 + Ly + \cdots + Ly^{n-1}$$

とする.
$(\Longleftarrow)$ $ab^{-1} = \delta \cdot \delta^\sigma \cdot \cdots \cdot \delta^{\sigma^{n-1}}$ とする.

$$\varphi : A \longrightarrow B : \begin{cases} \varphi(\alpha) = \alpha \ \ (\alpha \in L) \\ \varphi(x) = \delta y \end{cases}$$

は同型になる.
$(\Longrightarrow)$ $\varphi : A \longrightarrow B$ を同型写像とする. 必要ならば $\mathrm{Inn}(B)$ の元と合成することにより, $\varphi|_L = \mathbf{id}$ としてよい. $i_x \in \mathrm{Inn}(A)$, $i_y \in \mathrm{Inn}(B)$ とすると, $i_{\varphi(x)}|_L = i_y|_L = \sigma$. したがって $\varphi(x)y^{-1} \in Z_B(L) = L$ となるから, ある $\delta \in L^\times$ により $\varphi(x) = \delta y$ と書ける. よって

$$a = \varphi(a) = \varphi(x^n) = (\delta y)^n = \mathrm{Nr}_{L/K}(\delta) y^n = \mathrm{Nr}_{L/K}(\delta) b$$

となる.
(3) (2) より $(L/K, \sigma, a) \cong (L/K, \sigma, 1) \iff a \in \mathrm{Nr}_{L/K}(L^\times)$ であるから, $(L/K, \sigma, 1) \cong M_n(K)$ を示せばよい. $M_n(K) \cong \mathrm{End}_K(L)$ である. 写像

$$\varphi : (L/K, \sigma, 1) \longrightarrow \mathrm{End}_K(L) : \begin{cases} \varphi(\alpha) = \alpha \text{ 倍写像 } \ (\alpha \in L) \\ \varphi(x) = \sigma \end{cases}$$

は同型になる.

命題 23 任意の $a, b \in K^\times$ について

$$(L/K, \sigma, a) \otimes (L/K, \sigma, b) \sim (L/K, \sigma, ab)$$

である.

証明 証明は後で一般の接合積の場合に与える.

7.2 表象

n は $\mathrm{ch}(K)$ と素な自然数として, μ_n を K の代数閉包の中の 1 の n 乗根の群とする. 以下ここでは $\mu_n \subset K$ であると仮定する. 1 の原始 n 乗根 $\zeta \in K$ を一つ固定しておく. いま L/K を n 次巡回拡大とすれば, Kummer 拡大の理論から, ある $a \in K^\times$ が存在して, $L = K(\sqrt[n]{a})$ となり, 写像

$$\Gamma_{L/K} \longrightarrow \mu_n \,:\, \sigma \mapsto \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}$$

は同型になる. そこで $\Gamma_{L/K}$ の生成元 σ を

$$\frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} = \zeta$$

となるようにとる. $b \in K^\times$ に対し, 巡回代数 $(L/K, \sigma, b)$ は

$$(L/K, \sigma, b) = L1 + Ly + \cdots + Ly^{n-1} \qquad \begin{cases} (\mathrm{CY1})\ y^n = b \\ (\mathrm{CY2})\ y\alpha = \sigma(\alpha)y \quad (\alpha \in L) \end{cases}$$

で決まる. $x = \sqrt[n]{a}$ とおけば

$$L = K1 + Kx + \cdots + Kx^{n-1}, \quad x^n = a\,.$$

で, 条件 (CY2) は $\alpha = x$ で成り立てばよい. 即ち

$$y\alpha = \sigma(\alpha)y \quad (\alpha \in L) \iff yx = \sigma(x)y = \zeta xy$$

である. これから $(L/K, \sigma, b)$ は

$$(L/K, \sigma, b) = \sum_{0 \leqq i,j \leqq n-1} Kx^i y^j \qquad \begin{cases} x^n = a \\ y^n = b \\ yx = \zeta xy \end{cases}$$

で定義される代数である. この定義を任意の $a \in K^\times$ で考えることにより次の定義を得る.

定義　$\mu_n \subset K$ として, 原始 n 乗根 $\zeta \in \mu_n$ を固定する. このとき $a, b \in K^\times$ に対し, 関係

$$\sum_{0 \leqq i,j \leqq n-1} Kx^i y^j \qquad \begin{cases} x^n = a \\ y^n = b \\ yx = \zeta xy \end{cases}$$

で定義される K 多元環を**表象**とよび $(a, b)_n$, 詳しくは $\left(\dfrac{a, b}{K, \zeta}\right)$ と表す.

命題 24　$(a, b)_n \in \mathfrak{A}_{cs}(K)$ である.

証明　$A = (a, b)_n$, $K(x) = K1 + Kx + \cdots + Kx^{n-1}$ とおく. $K(x) \subset A$ は部分代数で, 一般に体になるとは限らない. A の任意の元は

$$u = f_0(x)1 + f_1(x)y + \cdots + f_{n-1}(x)y^{n-1}, \quad f_j(x) = c_{0j}1 + c_{1j}x + \cdots + c_{n-1j}x^{n-1} \in K(x)$$

とかける.
(中心性) $u \in Z_A$ とする. $yu = uy$ から

$$c_{ij} = c_{ij}\zeta^i \qquad (0 \leqq i, j \leqq n-1)$$

を得る. これから $i \neq 0$ ならば $c_{ij} = 0$. したがって

$$u = c_{00}1 + c_{01}y + \cdots + c_{0n-1}y^{n-1}$$

となる. また $xu = ux$ から同様に $c_{01} = \cdots = c_{0n-1} = 0$ が従うから, $u = c_{00} \in K$ である. したがって $Z_A = K$ となる.
(単純性) $0 \neq I \subset A$ を両側イデアルとする.

$$\ell = \min\{\deg_y u \mid u \in I\}, \quad I_\ell = \{u \in I \mid \deg_y u = \ell\} \subset I$$

とし, さらに

$$k = \min\{\deg f(x) \mid f(x) \in M\}, \quad M = \{\text{ すべての } u \in I_\ell \text{ の } y^\ell \text{ 係数部分 }\} \subset K(x)$$

とおく. このときある $u \in I_\ell$ で

$$u = f(x)y^\ell + v + f_0(x)1, \qquad \deg f(x) = k,\ \ 1 \leqq \deg_y v \leqq \ell - 1,\ \ f_0(x) \in K(x)$$

となるものがある.

$$f(x) = c_0 + c_1x + \cdots + c_kx^k$$

とおく. いま $1 \leqq k$ と仮定してみる. このとき

$$I_\ell \ni u - yuy^{-1} = (f(x) - f(\zeta x))y^\ell + \cdots$$

で, $f(x) - f(\zeta x) \in M$ は定数項が 0 であるから

$$I \ni x^{-1}(u - yuy^{-1}) = x^{-1}(f(x) - f(\zeta x))y^\ell + \cdots, \quad \deg x^{-1}(f(x) - f(\zeta x)) = k - 1$$

となり, k の最小性に矛盾する. したがって $k = 0$, $f(x) = c_0 \in K^\times$ で

$$u = c_0y^\ell + v + f_0(x) \in I_\ell$$

となる. 次に $1 \leqq \ell$ と仮定してみる. このとき $f_0(x) = 0$ ならば, $uy^{-1} \in I$ で, $\deg_y uy^{-1} = \ell - 1$ となり ℓ の最小性に矛盾するから, $f_0(x) \neq 0$ である. しかし

$$I \ni u - \zeta^\ell xux^{-1} = v - \zeta^\ell xvx^{-1} + (1 - \zeta^\ell)f_0(x) \neq 0$$

で $\deg_y(u - \zeta^\ell xux^{-1}) \leqq \ell - 1$ となり, やはり ℓ の最小性に矛盾する. したがって $\ell = 0$ で, I は $u = c_0 \in K^\times$ を含むから $I = A$ となる.

補題 7 一般に $A \in \mathfrak{A}_{cs}(K)$, $\deg A = n$ に対し,

$$A \cong M_n(K) \iff A \text{ は部分多元環として } K^n = K \oplus \cdots \oplus K \text{ を含む.}$$

証明　($\Longrightarrow$) は明らか. ($\Longleftarrow$) を示す. K^n はベキ単元 $\boldsymbol{e}_1, \cdots, \boldsymbol{e}_n$ で

$$\boldsymbol{e}_1 + \cdots + \boldsymbol{e}_n = 1, \qquad \boldsymbol{e}_i \boldsymbol{e}_j = \delta_{ij} \boldsymbol{e}_j$$

をみたすものを含む. これから A は左 A 加群として

$$A = \boldsymbol{e}_1 A \oplus \cdots \oplus \boldsymbol{e}_n A$$

と分解する. $A = M_m(D)$, $D \in \mathfrak{D}(K)$ とすると, D^m が単純左 A 加群だから, $m \geqq n$ でなければならない. $m \geqq \deg A = n$ であるから, $m = n$ で $D = K$ となる.

定理 12 d が n の約数とする. このとき任意の $a, b \in K^\times$ に対し

$$\left(\frac{a^d, b}{K, \zeta}\right) \cong \left(\frac{a, b}{K, \zeta^d}\right) \otimes M_d(K)$$

である. とくに $(a^n, b)_n \cong M_n(K)$ である.

証明　$n = dm$ とする. ζ^d は 1 の原始 m 乗根である. $A = (a^d, b)_n = \sum K x^i y^j$ とする. 部分多元環 $K(x) = K1 + Kx + \cdots + Kx^{n-1}$ を考えれば, 中国式剰余定理から K 多元環の同型

$$K(x) \cong K[X]/(X^n - a^d) \cong \bigoplus_{i=0}^{d-1} K[X]/(X^m - a\zeta^{im})$$

がある. 右辺の要素で

$$(\zeta^{-i} X \mod (X^m - a\zeta^{im}))_{i=0,1,\cdots,d-1}$$

に対応する $K(x)$ の要素を z とする. このとき

$$z^m = a, \qquad y^d z y^{-d} = \zeta z$$

が成り立つ. したがって z と $w = y^d$ で生成された部分多元環は

$$B = \sum_{0 \leqq i,j \leqq m-1} K z^i w^j \cong \left(\frac{a, b}{K, \zeta^d}\right)$$

となる. $B \in \mathfrak{A}_{cs}(K)$ であるから, 中心化定理により

$$A \cong B \otimes Z_A(B)$$

となる. 容易にわかるように $x^m \in Z_A(B)$ であるから, $t = x^m$ で生成された部分多元環は

$$Z_A(B) \supset K(t) = K1 + Kt + \cdots + Kt^{d-1} \cong K[X]/(X^d - a^d) \cong K^d$$

となる. $\deg Z_A(B) = d$ だから, 補題１１により $Z_A(B) \cong M_d(K)$ となる.

系 10 $a, b \in K^\times$ として, L を多項式 $X^n - a = 0$ の分解体で $m = [L : K]$ とする. $\sigma \in \Gamma_{L/K}$ を $\sigma(\sqrt[n]{a}) = \zeta^{n/m}\sqrt[n]{a}$ となるようにとれば,

$$(a, b)_n \cong (L/K, \sigma, b) \otimes M_{n/q}(K)$$

である. とくに

$$(a, b)_n \cong M_n(K) \iff b \in \mathrm{Nr}_{L/K}(L^\times).$$

証明 ガロア理論から $c = (\sqrt[n]{a})^m \in K^\times$ で, $L = K(\sqrt[m]{c})$ である. $a = c^{n/m}$ だから

$$(a, b)_n \cong \left(\frac{c, b}{K, \zeta^{n/m}}\right) \otimes M_{n/m}(K), \qquad \left(\frac{c, b}{K, \zeta^{n/m}}\right) \cong (L/K, \sigma, b)$$

となる. また, 定理１２から

$$(a, b)_n \cong M_n(K) \iff (L/K, \sigma, b) \cong M_m(K) \iff b \in \mathrm{Nr}_{L/K}(L^\times)$$

が成り立つ.

定理 13 $a, b, c \in K^\times$ とする.

(1) $(a, b)_n \cong (b^{-1}, a)_n$

(2) $(a, b)_n \otimes (a, c)_n \sim (a, bc)_n$, $(a, b)_n \otimes (c, b)_n \sim (ac, b)_n$.

(3) $(a, 1-a)_n \cong M_n(K)$.

証明 (1) $(a, b)_n = \sum Kx^iy^j$, $(b^{-1}, a)_n) = \sum Kz^iw^j$ とする. このとき写像

$$\varphi : (a, b)_n \longrightarrow (b^{-1}, a)_n : \varphi(x) = w, \ \ \varphi(y) = w^{-1}$$

は同型を与える.
(2) L を $X^n - a = 0$ の分解体とすれば, 系１０と命題２３から

$$(a, b)_n \otimes (a, c)_n \sim (L/K, \sigma, b) \otimes (L/K, \sigma, c) \sim (L/K, \sigma, bc) \sim (a, bc)_n$$

となる.
(3) $(a, 1-a)_n = \sum Kx^iy^j$ とする. $z = x + y$ とおけば

$$z^n = (x+y)^n = x^n + y^n = a + 1 - a = 1$$

が成り立つ. これから $K(z) = K1 + Kz + \cdots + Kz^{n-1} \cong K^n$ となるから, 補題７により $(a, 1-a)_n \cong M_n(K)$ である.

7.3 四元数環

K は体とする.

定義 $A \in \mathfrak{A}_{cs}(K)$ が $\deg A = 2$ であるとき, **四元数環**という. さらに A が斜体ならば **四元数体**という.

補題 8 $A \in \mathfrak{A}_{cs}(K)$ を四元数環とする.

(1) A が斜体でなければ, $A \cong M_2(K)$ である.

(2) A が斜体ならば A は巡回多元環である.

証明 (1) A が斜体でなければ, $\mathrm{ind}A < \deg A = 2$ だから $A \cong M_2(K)$ である.
(2) A が斜体ならば, A は K 上分離的な極大部分体 L を含む. $[L : K] = \deg A = 2$ であるから, L/K は巡回拡大になる. 系 9 から A は巡回多元環になる.

四元数体を $A = (L/K, \sigma, b)$ と表す.
$\mathrm{ch}(K) \neq 2$ ならば, $L = K(\sqrt{a})$ と書けるから

$$A = (a,b)_2 = K1 + Kx + Ky + Kxy, \quad x^2 = a,\ \ y^2 = b,\ \ yx = -xy$$

と表示できる.
$\mathrm{ch}(K) = 2$ ならば, L は $X^2 + X + a = 0$ の分解体で, 命題 2 2 から

$$A = K1 + Kx + Ky + Kxy, \quad x^2 + x = a,\ \ y^2 = b,\ \ yxy^{-1} = x + 1$$

と表示できる.

8　接合積

8.1　Noether 因子団とコホモロジー

$A \in \mathfrak{A}_{cs}(K)$ として, 次の条件を考えよう.

(CP) A は K 上ガロア拡大であるような強極大部分体 L をもつ.

L/K のガロア群を $\Gamma = \Gamma_{L/K}$ とする. 各 $\sigma \in \Gamma$ に Skolem-Noether の定理を適用すれば, ある $u_\sigma \in A^\times$ で $\sigma = i_{u_\sigma}|_L$ となるものが存在する. このとき

$$\xi_{\sigma,\tau} = u_\sigma u_\tau u_{\sigma\tau}^{-1} \in Z_A(L)^\times = L^\times \qquad (\sigma, \tau \in \Gamma)$$

である. $u_\sigma u_\tau = \xi_{\sigma,\tau} u_{\sigma\tau}$ を使って $(u_\sigma u_\tau)u_\rho = u_\sigma(u_\tau u_\rho)$ を計算すると

$$\xi_{\sigma,\tau}\xi_{\sigma\tau,\rho} = \xi_{\sigma,\tau\rho}\sigma(\xi_{\tau,\rho}) \qquad (\sigma, \tau, \rho \in \Gamma)$$

をえる. A の部分多元環

$$B = \sum_{\sigma\in\Gamma} L u_\sigma$$

を考えると, $\{u_\sigma\}_{\sigma\in\Gamma}$ が L 上 1 次独立であることは容易に示せるから, $\dim_K B = [L:K]^2 = \dim_K A$ となり, 結局 A は

$$A = \sum_{\sigma\in\Gamma} L u_\sigma, \qquad \begin{cases} u_\sigma \alpha u_\sigma^{-1} = \sigma(\alpha) & (\alpha \in L) \\ u_\sigma u_\tau = \xi_{\sigma,\tau} u_{\sigma\tau} \end{cases}$$

と表示されることがわかる.

定義　一般に L/K を有限次ガロア拡大として, $\Gamma = \Gamma_{L/K}$ をガロア群とする. 写像

$$\xi : \Gamma \times \Gamma \longrightarrow L^\times : (\sigma, \tau) \mapsto \xi_{\sigma,\tau}$$

が次の条件をみたすとき, ξ を **Noether 因子団**または **2 コサイクル**という.

(NF) $\xi_{\sigma,\tau}\xi_{\sigma\tau,\rho} = \xi_{\sigma,\tau\rho}\sigma(\xi_{\tau,\rho}) \qquad (\sigma, \tau, \rho \in \Gamma)$.

Noether 因子団の全体を $Z^2(\Gamma, L^\times)$ で表す.

補題 9　任意の $\xi \in Z^2(\Gamma, L^\times)$ に対し

$$\xi_{e,\sigma} = \xi_{e,e}, \quad \xi_{\sigma,e} = \sigma(\xi_{e,e}), \qquad (\sigma \in \Gamma)$$

である.

証明　(NF) で, $\sigma = \tau = e$ とすれば, $\xi_{e,e}\xi_{e,\rho} = \xi_{e,\rho}^2$ となるから, $\xi_{e,e} = \xi_{e,\rho}$ である. また $\tau = \rho = e$ とすれば, $\xi_{\sigma,e}^2 = \xi_{\sigma,e}\sigma(\xi_{e,e})$ となるから, $\xi_{\sigma,e} = \sigma(\xi_{e,e})$ である.

補題 10 $\xi, \eta \in Z^2(\Gamma, L^\times)$ として, その積

$$\xi \cdot \eta : \Gamma \times \Gamma \longrightarrow L^\times$$

を

$$(\xi \cdot \eta)_{\sigma,\tau} = \xi_{\sigma,\tau} \cdot \eta_{\sigma,\tau}, \qquad (\sigma, \tau \in \Gamma)$$

により定義すれば, $\xi \cdot \eta \in Z^2(\Gamma, L^\times)$ で, $Z^2(\Gamma, L^\times)$ はこの積でアーベル群になる. 単位元 $\mathbf{1}$ は $\mathbf{1}_{\sigma,\tau} = 1$ $(\sigma, \tau \in \Gamma)$ で定まる 2 コサイクルである.

定義 写像 $t : \Gamma \longrightarrow L^\times$ から, 写像

$$\widehat{t} : \Gamma \times \Gamma \longrightarrow L^\times$$

を

$$\widehat{t}_{\sigma,\tau} = t_\sigma \sigma(t_\tau) t_{\sigma\tau}^{-1}, \qquad (\sigma, \tau \in \Gamma)$$

で定義すれば, $\widehat{t}$ は 2 コサイクルになる. この形の 2 コサイクルを**コバウンダリー**という. コバウンダリー全体を $B^2(\Gamma, L^\times)$ と表す.

補題 11 $B^2(\Gamma, L^\times)$ は $Z^2(\Gamma, L^\times)$ の部分群である.

定義 剰余群 $Z^2(\Gamma, L^\times)/B^2(\Gamma, L^\times)$ を, Γ の $L^\times$ 係数の**2ーコホモロジー群**といい, $H^2(\Gamma, L^\times)$ と書く. $\xi \in Z^2(\Gamma, L^\times)$ が属するコホモロジー類を $[\xi]$ で表し, 単位元を $[\mathbf{1}]$ で表す.

8.2 接合積

L/K をガロア拡大で, $\Gamma = \Gamma_{L/K}$ をそのガロア群とする.

定義 $V = \sum_{\sigma\in\Gamma} L x_\sigma$ を不定元 $\{x_\sigma\}_{\sigma\in\Gamma}$ で生成された L 上のベクトル空間とする. $\xi \in Z^2(\Gamma, L^\times)$ が与えられたとき, V に積を

(CP1) $x_\sigma \alpha = \sigma(\alpha) x_\sigma$, $(\alpha \in L, \sigma \in \Gamma)$.

(CP2) $x_\sigma x_\tau = \xi_{\sigma,\tau} x_{\sigma\tau}$, $(\sigma, \tau \in \Gamma)$.

により定義する. この積により V は $\xi_{e,e}^{-1} x_e$ を単位元にもつ K 多元環になる. この多元環を L と Γ の ξ による**接合積**といい, (L, Γ, ξ) と表す. またこの形の多元環を**接合積多元環**とよぶ.

命題 25 $(L, \Gamma, \xi) \in \mathfrak{A}_{cs}(K)$ で, L は (L, Γ, ξ) の強極大部分体である.

証明 $A=(L,\Gamma,\xi)$ とする.
(中心性) Z_A の元を
$$z=\sum_{\sigma\in\Gamma}a_\sigma x_\sigma$$
とする. 任意の $\alpha\in L$ について, $\alpha z=z\alpha$ だから
$$\alpha a_\sigma=\sigma(\alpha)a_\sigma, \qquad (\sigma\in\Gamma)$$
となる. $\sigma\neq e$ ならば $\sigma(\alpha)\neq\alpha$ となる $\alpha\in L$ が存在するから, $a_\sigma=0$. よって $z=a_e x_e$ で, さらに $zx_\sigma=x_\sigma z$ から
$$\sigma(a_e)\xi_{\sigma,e}=a_e\xi_{e,\sigma}\,.$$
補題 9 から
$$\sigma(a_e\xi_{e,e})=a_e\xi_{e,e}$$
となり, $a_e\xi_{e,e}\in K$ がわかる. よって $z=a_e x_e=a_e\xi_{e,e}1_A\in K$ となる.
(単純性) $I\subsetneqq A$ を両側イデアルとする. $\pi: A\longrightarrow A/I$ を自然な準同型とする. $\pi|_L: L\longrightarrow A/I$ は単射であるから, $L\subset A/I$ としてよい. $\overline{x}_\sigma=\pi(x_\sigma)$ とおく. このとき
$$\overline{x}_\sigma\alpha=\sigma(\alpha)\overline{x}_\sigma \qquad (\alpha\in L,\ \sigma\in\Gamma)$$
が成り立つ. $\{\overline{x}_\sigma\}_{\sigma\in\Gamma}$ は L 上 1 次独立である. 実際, 部分集合 $J\subset\Gamma$ を $\{\overline{x}_\sigma\}_{\sigma\in J}$ が一次独立になるようなものでかつこの性質で極大なものとする. $J\subsetneqq\Gamma$ ならば, $\tau\notin J$ がとれて
$$\overline{x}_\tau=\sum_{\sigma\in J}a_\sigma\overline{x}_\sigma$$
と書ける. 任意の $\alpha\in L$ で
$$\tau(\alpha)\overline{x}_\tau=\overline{x}_\tau\alpha=\sum_{\sigma\in J}a_\sigma\overline{x}_\sigma\alpha=\sum_{\sigma\in J}a_\sigma\sigma(\alpha)\overline{x}_\sigma$$
だから
$$0=\sum_{\sigma\in J}a_\sigma(\tau(\alpha)-\sigma(\alpha))\overline{x}_\sigma$$
となる. $\{\overline{x}_\sigma\}_{\sigma\in J}$ は一次独立だから
$$a_\sigma(\tau(\alpha)-\sigma(\alpha))=0\,.$$
ある $\sigma\in J$ では $a_\sigma\neq 0$ だから, 結局
$$\tau(\alpha)=\sigma(\alpha), \qquad (\alpha\in L)$$
で, $\tau=\sigma\in J$ となり矛盾である. よって $J=\Gamma$ である. したがって $\dim_L A/I=\dim_L A=[L:K]$ が成り立つから, $I=0$ である.

系 11 $A\in\mathfrak{A}_{cs}(K)$ が接合積多元環であるためには, A が K 上ガロア拡大であるような強極大部分体をもつことが必要十分である.

定理 14 $\xi, \eta \in Z^2(\Gamma, L^\times)$ のとき

$$(L, \Gamma, \xi) \cong (L, \Gamma, \eta) \iff [\xi] = [\eta]\,.$$

証明 $A = (L, \Gamma, \xi) = \sum Lx_\sigma$, $B = (L, \Gamma, \eta) = \sum Ly_\sigma$ とおく.
$(\Longrightarrow)$ 同型写像を

$$\varphi : A \longrightarrow B$$

とする. Skolem-Noether の定理により $\varphi|_L = \mathbf{id}$ としてよい. このとき

$$\varphi(x_\sigma)\alpha = \sigma(\alpha)\varphi(x_\sigma), \qquad (\alpha \in L)$$

である.

$$\varphi(x_\sigma) = \sum_{\tau \in \Gamma} c_\tau y_\tau$$

として, 上の関係式を使えば

$$\varphi(x_\sigma) = c_\sigma y_\sigma$$

となることがわかる. このとき

$$\varphi(x_\sigma x_\tau) = c_\sigma y_\sigma c_\tau y_\tau = c_\sigma \sigma(c_\tau) y_\sigma y_\tau = c_\sigma \sigma(c_\tau) \eta_{\sigma,\tau} y_{\sigma\tau}$$

で, 他方

$$\varphi(x_\sigma x_\tau) = \varphi(\xi_{\sigma,\tau} x_{\sigma\tau}) = \xi_{\sigma,\tau} c_{\sigma\tau} y_{\sigma\tau}$$

である. したがって

$$\xi_{\sigma,\tau} = \widehat{c}_{\sigma,\tau} \eta_{\sigma,\tau}$$

が成り立ち, $[\xi] = [\eta]$ をえる.
$(\Longleftarrow)$ $[\xi] = [\eta]$ とすると, ある $c : \Gamma \longrightarrow L^\times$ で $\xi = \widehat{c} \cdot \eta$ となるものが存在する. 写像 $\varphi : A \longrightarrow B$ を

$$\varphi(\sum a_\sigma x_\sigma) = \sum a_\sigma c_\sigma y_\sigma$$

と定義すれば, これは同型写像になる.

定理 15 $(L, \Gamma, \mathbf{1}) \cong M_n(K)$ である.

証明 $(L, \Gamma, \mathbf{1}) = \sum Lx_\sigma$ とする. 写像

$$\varphi : (L, \Gamma, \mathbf{1}) \longrightarrow \mathrm{End}_K(L) : \begin{cases} \varphi(\alpha) = \alpha \text{ 倍写像 } (\alpha \in L) \\ \varphi(x_\sigma) = \sigma \ \ (\sigma \in \Gamma) \end{cases}$$

は同型写像である.

系 12 $(L, \Gamma, \xi) \cong M_n(K) \iff [\xi] = [\mathbf{1}]$.

定理 16 任意の $\xi, \eta \in Z^2(\Gamma, L^\times)$ で

$$(L, \Gamma, \xi) \otimes (L, \Gamma, \eta) \sim (L, \Gamma, \xi \cdot \eta)\,.$$

証明

$$A=(L,\Gamma,\xi)=\sum Lx_\sigma,\quad B=(L,\Gamma,\eta)=\sum Ly_\sigma,\quad C=(L,\Gamma,\xi\cdot\eta)=\sum Lz_\sigma$$

とする．A, B を左 L 加群と見る．このとき A° は右 L 加群になるから, L 加群としてのテンソル積

$$V=A^\circ\otimes_L B$$

ができる．V は自然に両側 (A°,B) 加群になるから, 右 $A\otimes B$ 加群と見なせる．即ち

$$(a'\otimes_L b')(a\otimes b)=a'a\otimes_L b'b=a\circ a'\otimes_L b'b,\qquad (a,a'\in A,\ b,b'\in B)$$

C の V への作用を

$$C\times V\longrightarrow V\ :\ \alpha z_\sigma(a\otimes_L b)=a\circ(\alpha x_\sigma)\otimes_L y_\sigma b=\alpha x_\sigma a\otimes_L y_\sigma b$$

で定義する．これは

$$\begin{aligned}\alpha z_\sigma\cdot\beta z_\tau(a\otimes_L b) &= \alpha z_\sigma(\beta x_\tau a\otimes_L y_\tau b)\\ &= (\alpha x_\sigma\beta x_\tau a)\otimes_L (y_\sigma y_\tau b)\\ &= (\alpha\sigma(\beta)\xi_{\sigma,\tau}x_{\sigma\tau}a)\otimes_L(\eta_{\sigma,\tau}y_{\sigma\tau}b)\\ &= (\alpha\sigma(\beta)\xi_{\sigma,\tau}\eta_{\sigma,\tau}z_{\sigma\tau})(a\otimes_L b)\\ &= (\alpha z_\sigma\beta z_\tau)(a\otimes_L b)\end{aligned}$$

をみたすから, V は左 C 加群の構造をもつ．したがって V は両側 $(C,A\otimes B)$ 加群となり, K 多元環の準同型

$$(A\otimes B)^\circ\longrightarrow \mathrm{End}_C(V)$$

がある．$(A\otimes B)^\circ$ は単純環だから, これは単射になる．

$$\dim_K V=[L:K]\dim_L A\dim_L B=n^3=n\dim_K C$$

であるから, C 加群として $V\cong C^n$ である．したがって

$$\mathrm{End}_C(V)\cong\mathrm{End}_C(C^n)\cong M_n(\mathrm{End}_C(C))\cong M_n(C^\circ)\cong C^\circ\otimes M_n(K)\,.$$

次元を計算すると

$$\dim_K\mathrm{End}_C(V)=n^2\dim_K C=n^4=\dim_K(A\otimes B)$$

となるから

$$(A\otimes B)^\circ\cong\mathrm{End}_C(V)\cong C^\circ\otimes M_n(K)\,.$$

ゆえに $A\otimes B\sim C$ をえる．

8.3 接合積としての巡回多元環

L/K を n 次巡回拡大として, $\Gamma = \Gamma_{L/K} =< \sigma >$ とする.

命題 26 $a \in K^\times$ として, $(L/K, \sigma, a)$ を巡回多元環とする. このとき

$$\xi_{\sigma^i, \sigma^j} = \begin{cases} 1 & (i+j < n) \\ a & (i+j \geqq n) \end{cases}$$

で定義された ξ は２コサイクルで, $(L/K, \sigma, a) \cong (L, \Gamma, \xi)$ である.

証明 $(L/K, \sigma, a)$ は L を強極大部分体にもつから, 接合積多元環になる. $(L/K, \sigma, a) = \sum Lx_\sigma$ として, Noether 因子団を計算すると上の ξ になる.

命題 27 任意の $\xi \in Z^2(\Gamma, L^\times)$ に対し, 接合積 (L, Γ, ξ) は巡回多元環である.

命題２１, 命題２３はそれぞれ命題２５, 定理１７から従う.

9 Brauer 群の構造

9.1 同型定理

任意の拡大 L/K に対し, 命題１５から, 写像

$$\mathrm{Br}(K) \longrightarrow \mathrm{Br}(L) : [A] \mapsto [A \otimes L]$$

は準同型であった. その核を $\mathrm{Br}(L/K)$ と表す. 即ち

$$\mathrm{Br}(L/K) = \{[A] \in \mathrm{Br}(A) \mid [A \otimes L] = [1]\}$$

である.

命題 28 $\mathrm{Br}(K) = \displaystyle\bigcup_{L/K:\text{ガロア拡大}} \mathrm{Br}(L/K)$ である.

証明 系５より, 任意の $A \in \mathfrak{A}_{cs}(K)$ は K 上ガロア拡大であるような分解体をもつ.

定理 17 任意のガロア拡大 L/K に対し, 写像

$$H^2(\Gamma, L^\times) \longrightarrow \mathrm{Br}(L/K) : [\xi] \mapsto [(L, \Gamma, \xi)]$$

は群の同型写像である.

証明 定理１７より

$$Z^2(\Gamma, L^\times) \longrightarrow \mathrm{Br}(K) : \xi \mapsto [(L, \Gamma, \xi)]$$

は準同型で, 系１２によりその核は $B^2(\Gamma, L^\times)$ である. したがって単射準同型

$$H^2(\Gamma, L^\times) \longrightarrow \mathrm{Br}(K)$$

がある. 像が $\mathrm{Br}(L/K)$ に含まれることは容易である. 逆に $D \in \mathfrak{D}(K)$ で $[D] \in \mathrm{Br}(L/K)$ とする. $\deg D = d$ とすれば, $[D^\circ] = [D]^{-1} \in \mathrm{Br}(L/K)$ だから

$$L \otimes D^\circ \cong M_d(L)$$

である. $V \cong L^d$ を単純左 $L \otimes D^\circ$ 加群とする. V は両側 (L, D) 加群になる. 右 D 加群としての V の階数を n とすれば

$$\dim_K V = d[L : K] = n \dim_K D = nd^2$$

である. また $\mathrm{End}_D(V) \cong M_n(D)$ だから

$$\dim_K \mathrm{End}_D(V) = \dim_K M_n(D) = d^2n^2 = (dn)^2 = [L : K]^2 .$$

写像

$$L \longrightarrow \mathrm{End}_D(V) : \alpha \mapsto \alpha\text{ 倍写像}$$

は単射だから, $L \subset \mathrm{End}_D(V)$ と見なすことができ, L は $\mathrm{End}_D(V)$ の強極大部分体となる. 系１１から, $\mathrm{End}_D(V) \cong (L, \Gamma, \xi)$ となる $\xi \in Z^2(\Gamma, L^\times)$ が存在する. このとき

$$[D] = [M_n(D)] = [\mathrm{End}_D(V)] = [(L, \Gamma, \xi)]$$

となる.

9.2 ベキ指数

定義 $A \in \mathfrak{A}_{cs}(K)$ に対し, $[A] \in \mathrm{Br}(K)$ の位数を A の**ベキ指数**とよび, $\exp(A)$ で表す.

命題 29 $m = \mathrm{ind}(A)$ ならば $[A]^m = [1]$ である. とくに $\exp(A)|\mathrm{ind}(A)$.

証明 L/K をガロア拡大で $[A] \in \mathrm{Br}(L/K)$ となるものとする. 定理１８より $[A] = [(L, \Gamma, \xi)]$ とする. $[A]^m = [(L, \Gamma, \xi^m)]$ だから, $\xi^m \in B^2(\Gamma, L^\times)$ を示せばよい. $B = (L, \Gamma, \xi) \cong M_r(D)$, $D \in \mathfrak{D}(K)$ として, $V = D^r$ を左 B 加群とする. $L \subset B$ だから, V は左 L ベクトル空間になる.

$$[L : K] = \deg(L, \Gamma, \xi) = \deg M_r(D) = rm$$

$$\dim_K V = r \dim_K D = rm^2 = \dim_L V [L : K] = \dim_L V rm$$

だから

$$\dim_L V = m$$

である. V の L 上の基底を $v_1, \cdots, v_m$ として, $b \in B$ に対し

$$bv_i = b_{i1}v_1 + \cdots + b_{in}v_n$$

により $m \times m$ 行列 $(b_{ij}) \in M_m(L)$ を対応させる.

$$B = \sum L x_\sigma$$

として, x_σ に対応する行列を X_σ と表せば

$$\xi_{\sigma,\tau} X_{\sigma\tau} = \sigma(X_\tau) X_\sigma$$

が成り立つ. 両辺の行列式を取れば

$$\xi^m_{\sigma,\tau} \det(X_{\sigma\tau}) = \sigma(\det(X_\tau)) \det(X_\sigma)$$

となるから $\xi^m \in B^2(\Gamma, L^\times)$ である.

系 13 $\mathrm{Br}(K)$ はねじれアーベル群である.

命題 30 p が $\mathrm{ind}(A)$ の素因数ならば, p は $\exp(A)$ の素因数でもある.

証明 前と同様に $[A] = [(L, \Gamma, \xi)], (L, \Gamma, \xi) \cong M_r(D)$ とする. $d = \mathrm{ind}(A) = \deg(D)$ とおく.

$$|\Gamma| = [L : K] = (\deg M_r(D)) = dr$$

だから $p||\Gamma|$. そこで Γ の p-Sylow 群を Γ_p とする. $L_p = L^{\Gamma_p}$ とおけば

$$[L : L_p] = |\Gamma_p|\,.$$

$p \not| [L_p : K]$ だから, 命題１９により L_p は D の分解体にはならない. よって A の分解体にもならない. したがって $\exp(A \otimes L_p) \neq 1$. 他方 $[A \otimes L_p] \in \mathrm{Br}(L/L_p)$ だから, 命題１９より $\mathrm{ind}(A \otimes L_p)|[L : L_p] = |\Gamma_p|$. 命題２９より $\exp(A \otimes L_p)|\mathrm{ind}(A \otimes L_p)$ だから $p|\exp(A \otimes L_p)$ となる. $\exp(A \otimes L_p)|\exp(A)$ だから $p|\exp(A)$ である.

9.3　斜体のプライマリー分解

補題 12 $D_1, D_2 \in \mathfrak{D}(K)$ で, $\deg(D_1)$ と $\deg(D_2)$ が互いに素ならば $D_1 \otimes D_2$ も斜体である.

証明　$d_1 = \deg(D_1), d_2 = \deg(D_2)$ とおく. $D_1 \otimes D_2 \cong M_n(D)$, $D \in \mathfrak{D}(K)$ とする. $n = 1$ を示せばよい. $D_3 \in \mathfrak{D}(K)$ を $D_1^\circ \otimes D \cong M_r(D_3)$ となるものとすると,

$$\begin{aligned} M_{d_1^2}(D_2) &\cong M_{d_1^2}(K) \otimes D_2 \cong D_1^\circ \otimes D_1 \otimes D_2 \cong D_1^\circ \otimes M_n(D) \\ &\cong M_{nr}(D_3) \end{aligned}$$

だから, $D_2 \cong D_3$ かつ $d_1^2 = nr$. よって $n | d_1^2$. 同様に $n | d_2^2$ となるから仮定により $n = 1$ である.

定理 18 $D \in \mathfrak{D}(K)$ として, $d = \deg(D)$ の素因数分解を $d = p_1^{e_1} p_2^{e_2} \cdots p_\ell^{e_\ell}$ とする. このとき $D_1, \cdots, D_\ell \in \mathfrak{D}(K)$ で

$$D \cong D_1 \otimes D_2 \otimes \cdots \otimes D_\ell, \qquad \deg(D_i) = p_i^{e_i}, \ \ i = 1, 2, \cdots \ell$$

となるものが存在する. また $D_1, \cdots, D_\ell$ は同型を除いて一意に定まる.

証明　$d = d_1 d_2$, d_1 と d_2 は互いに素, とするとき, $D_1, D_2 \in \mathfrak{D}(K)$ で

$$D \cong D_1 \otimes D_2, \qquad \deg(D_1) = d_1, \ \deg(D_2) = d_2$$

となるものが, 同型を除いて一意に存在することを示せばよい. $q_1, q_2 \in \mathbf{Z}$ を

$$d_1 q_1 + d_2 q_2 = 1$$

となるようにとる. $\mathrm{Br}(K)$ の中で, $[D]^{d_2 q_2} = [D_1]$, $[D]^{d_1 q_1} = [D_2]$ となるように $D_1, D_2 \in \mathfrak{D}(K)$ をとる. D_1, D_2 は同型を除いて一意に決まる. このとき

$$[D_1 \otimes D_2] = [D]^{d_2 q_2 + d_1 q_1} = [D]$$

である. $\deg(D) = \mathrm{ind}(D) = d$ だから, 命題２９により

$$[D_1]^{d_1} = [D]^{d_1 d_2 q_2} = [D]^{d q_2} = [1].$$

よって $\exp(D_1) | d_1$. 同様に $\exp(D_2) | d_2$. d_1 と d_2 は互いに素だから $\exp(D_1)$ と $\exp(D_2)$ も互いに素である. また命題３０により $\mathrm{ind}(D_1) = \deg(D_1)$ と $\mathrm{ind}(D_2) = \deg(D_2)$ も互いに素になる. よって補題１６により $D_1 \otimes D_2$ も斜体になり, $[D] = [D_1 \otimes D_2]$ だから $D \cong D_1 \otimes D_2$ となる.

9.4　非接合積斜体の存在

定理１８から, 任意の斜体は接合積と Brauer 同値になる. これは次の問題を引き起こす.

問 1 任意の斜体は接合積と同型になるか？

この問については, 次が知られている.

定理 19 (Wedderburn, Albert, Dickson) $D \in \mathfrak{D}(K)$ で, $\deg D \in \{2,3,4,6,12\}$ ならば D は接合積である.

定理 20 (Frobenius, Hasse, Tsen, Wedderburn, Witt) K が次の体の一つであるとする.

- $\mathbf{C}$, $\mathbf{C}(t)$, $\mathbf{C}((t))$.
- $\mathbf{R}$, $\mathbf{R}(t)$, $\mathbf{R}((t))$.
- 局所体.
- 大域体 (有限次代数体または有限体上の１変数代数関数体).
- 有限体.
- 局所体上の１変数形式的ベキ級数体

このとき任意の $D \in \mathfrak{D}(K)$ は接合積である.

しかし一般には, 否定的である.

定理 21 (Brussel) K を $\mathbf{Q}$ 上の１変数有理関数体 $\mathbf{Q}(t)$ または $\mathbf{Q}$ 上の１変数ベキ級数体 $\mathbf{Q}((t))$ とする. このとき $\mathfrak{D}(K)$ の元で, 接合積と同型にならないものがある.

関連する問題として

問 2 $D \in \mathfrak{D}(K)$ で $\deg D = p$ が素数ならば, D は巡回代数になるか？

がある. $p = 2, 3$ の場合は定理１９により成り立つ. $p = 5$ の場合は未解決である.

定義　斜体 $D \in \mathfrak{D}(K)$ は, $D \cong D_1 \otimes D_2$ となる $K \neq D_1, K \neq D_2 \in \mathfrak{D}(K)$ が存在するとき decomposable であるといい, そうでないとき indecomposable であるという.

定理１８から, D が indecomposable ならば, $\deg(D)$ は素数のべきである. 逆に, 素数 p とそのべき $p^e \leqq p^d$ が与えられたとき, $\exp(D) = p^e$, $\deg(D) = p^d$ となる indecomposable な斜体が存在するかどうかについては次が知られている.

定理 22 (Albert, Jacob) $(p^e, p^d) \neq (2, 4)$ ならば, ある体 K において indecomposable な斜体 $D \in \mathfrak{D}(K)$ で $\exp(D) = p^e$, $\deg(D) = p^d$ となるものが存在する. 他方, 任意の体において, $\exp(D) = 2$, $\deg(D) = 4$ となる斜体は, 二つの四元数体のテンソル積である.

10 Merkurjev-Suslin の定理

10.1 Milnor K 群

K の乗法群 $K^\times$ と同型な加法群を $\mathbf{K}_1(K)$ とおく. 同型写像を

$$\ell : K^\times \longrightarrow \mathbf{K}_1(K) : a \mapsto \ell(a)$$

とする.

$$\ell(1) = 0, \quad \ell(a^n) = n\ell(a), \quad \ell(ab) = \ell(a) + \ell(b) \qquad (n \in \mathbf{Z},\ a, b \in K^\times)$$

である. $\mathbf{K}_1(K)$ は $\mathbf{Z}$ 加群だから, テンソル代数 $\mathbf{TK}_1(K)$ ができる. 即ち

$$\mathbf{TK}_1(K) = \bigoplus_{n=0}^{\infty} \mathbf{T}^n\mathbf{K}_1(K), \qquad \mathbf{T}^0\mathbf{K}_1(K) = \mathbf{Z},\ \ \mathbf{T}^n\mathbf{K}_1(K) = \mathbf{K}_1(K) \otimes_{\mathbf{Z}} \cdots \otimes_{\mathbf{Z}} \mathbf{K}_1(K).$$

$\mathbf{TK}_1(K)$ の中で

$$J = \{\ell(a) \otimes \ell(1-a) \mid a \in K^\times,\ a \neq 1\} \text{ で生成された両側イデアル}$$

とおき, 剰余加群 $\mathbf{TK}_1(K)/J$ を考える.

$$\pi : \mathbf{TK}_1(K) \longrightarrow \mathbf{TK}_1(K)/J$$

を自然な写像として,

$$\mathbf{K}_n(K) = \pi(\mathbf{T}^n K_1(K)), \quad \{a_1, \cdots, a_n\} = \pi(\ell(a_1) \otimes \cdots \otimes \ell(a_n))$$

と表す.

$$\mathbf{TK}_1(K)/J = \bigoplus_{n=0}^{\infty} \mathbf{K}_n(K)$$

と書ける.

定義 $\mathbf{K}_n(K)$ を K の **Milnor K 群**という.

とくに $\mathbf{K}_2(K)$ を詳しく見ると, 定義から

(M1) $\{ab, c\} = \{a, c\} + \{b, c\}$, $\{a, bc\} = \{a, b\} + \{a, c\}$.

(M2) $\{a, 1-a\} = 0$, $(a \neq 1)$.

(M3) $\{a, 1\} = \{1, a\} = 0$, $\{a, b^{-1}\} = -\{a, b\}$.

である.

命題 31 任意の $a, b \in K^\times$ についてさらに次が成り立つ.

(M4) $\{a, -a\} = 0$.

(M5) $\{a, b\} = -\{b, a\}$.

10.2 Merkurjev-Suslin の定理

自然数 n を固定して

$$\mathrm{Br}(K)_n = \{[A] \in \mathrm{Br}(K) \mid [A]^n = [1]\}$$

とおく.

定理 23 (Merkurjev-Suslin) $(n, \mathrm{ch}(K)) = 1$ で, $\mu_n \subset K$ と仮定する. 1 の原始 n 乗根 $\zeta \in \mu_n$ を固定する. このとき写像

$$\mathbf{K}_2(K) \longrightarrow \mathrm{Br}(K) : \{a, b\} \mapsto (a, b)_n = \left(\frac{a, b}{K, \zeta}\right)$$

は well-definied で, その核は $n\mathbf{K}_2(K)$, 像は $\mathrm{Br}(K)_n$ となる. 即ち同型

$$\mathbf{K}_2(K)/n\mathbf{K}_2(K) \cong \mathrm{Br}(K)_n$$

を導く.

系 14 $(n, \mathrm{ch}(K)) = 1$ かつ $\mu_n \subset K$ とする. $A \in \mathfrak{A}_{cs}(K)$ が $\exp(A)|n$ をみたすならば, ある $a_1, b_1, \cdots, a_r, b_r \in K^\times$ で

$$A \sim (a_1, b_1)_n \otimes \cdots \otimes (a_r, b_r)_n$$

となるものが存在する.

系 15 $\mathrm{ch}(K) \neq 2$ とする. $A \in \mathfrak{A}_{cs}(K)$, $\exp(A) = 2$ ならば, ある $a_1, b_1, \cdots, a_r, b_r \in K^\times$ で

$$A \sim (a_1, b_1)_2 \otimes \cdots \otimes (a_r, b_r)_2$$

となるものが存在する.

11 局所体の Brauer 群

11.1 斜体の付値

D を斜体とする．D の付値について結果をまとめておく．

- **付値**

  写像 $v : D \longrightarrow \mathbf{R}$ が次の 3 条件をみたすとき v を**非アルキメデス付値**という．

  (VA1) $v(x) \geqq 0, \ \ (x \in D)$ で, $v(x) = 0$ となるのは $x = 0$ のときに限る．
  (VA2) $v(xy) = v(x)v(y), \quad (x, y \in D)$.
  (VA3) $v(x + y) \leqq \max(v(x), v(y)), \quad (x, y \in D)$.

  以下, 自明な付値 $v(x) = 1, \ \ (x \in D^{\times})$ は除く．

- **付値環**

  v を D の非アルキメデス付値とするとき, 集合

  $$O_v = \{x \in D \mid v(x) \leqq 1\}$$

  は部分環になる．これを v の**付値環**という．O_v の単数群は

  $$O_v^{\times} = \{x \in D \mid v(x) = 1\}$$

  である．

- **付値イデアル, 剰余体**

  O_v の中で,

  $$P_v = \{x \in O_v \mid v(x) < 1\}$$

  は極大両側イデアルになる．これを**付値イデアル**といい, O_v/P_v を v の**剰余体**という．

- **付値による位相と完備化**

  非アルキメデス付値 v から, D 上の距離 δ_v が $\delta_v(x, y) = v(x - y), \ (x, y \in D)$ により定義される．これにより D は距離空間になる．δ_v による D の完備化を D_v と表す．D_v は斜体になり, v は D_v に自然に延長される．$D = D_v$ のとき v を**完備な付値**という．

- **付値の同値**

  v と w を D の非アルキメデス付値とする．ある実数 $r > 0$ が存在して, $w = v^r$ の関係があるとき, v と w は同値であるといい, $v \sim w$ と書く．次の同値性がある．

  $$v \sim w \iff O_v \subset O_w \iff P_v \subset P_w \iff (D, \delta_v) \text{ と } (D, \delta_w) \text{ は同相}$$

- **離散付値, 素元**

  $v(D^{\times})$ が $\mathbf{R}^{\times}$ の巡回部分群になるとき v を**離散付値**という．このとき $\varpi \in O_v$ で, $v(D^{\times}) = \{v(\varpi)^n \mid n \in \mathbf{Z}\}$ となるものが存在する．この ϖ を O_v の素元という．

- **局所コンパクト性**

  非アルキメデス付値 v について次の同値な条件がある．

  D は局所コンパクト $\iff$ O_v はコンパクト $\iff$ v は完備離散で, O_v/P_v は有限体

- **局所斜体**

  非アルキメデス付値 v をもつ斜体 D で局所コンパクトなものを**局所斜体**(D が体ならば**局所体**) という．このとき付値環を O_D, 極大両側イデアルを P_D で表し, 剰余体を $\mathfrak{f}_D = O_D/P_D$ で表す.

- **局所体の拡大**

  K を非アルキメデス付値 v をもつ局所体として, $K \subset D$ を K 上有限次元の斜体とする．このとき v は D の非アルキメデス付値 w に一意に拡張され, D も局所斜体となる．$e(D/K) = [w(D^\times) : v(K^\times)]$ を**分岐指数**といい, $f(D/K) = [\mathfrak{f}_D : \mathfrak{f}_K]$ を**相対次数**という．関係

  $$[D : K] = e(D/K)f(D/K)$$

  がある.

- **不分岐拡大**

  K を非アルキメデス付値 v をもつ局所体として, L/K を有限次拡大とする．L も局所体である．$e(L/K) = 1$ であるとき, L/K を**不分岐拡大**という．任意の自然数 n に対して, 不分岐拡大 K_n/K で, $[K_n : K] = n$ となるものが同型を除いてただ一つだけ存在する．$q = [O_v : P_v]$ とするとき, $K_n = K(\mu_{q^n-1})$ である．K_n/K は巡回拡大である.

- **Frobenius 自己同型**

  K を局所体として, K_n/K のガロア群を $\Gamma_{K_n/K}$ とし, 剰余体の拡大 $\mathfrak{f}_{K_n}/\mathfrak{f}_K$ のガロア群を $\Gamma_{\mathfrak{f}_{K_n}/\mathfrak{f}_K}$ とする．このとき写像

  $$\Gamma_{K_n/K} \longrightarrow \Gamma_{\mathfrak{f}_{K_n}/\mathfrak{f}_K} \ : \sigma \mapsto \sigma|_{O_{K_n}}$$

  は同型を引き起こす．$\mathfrak{f}_K \cong \mathbf{F}_q$, $\mathfrak{f}_{K_n} \cong \mathbf{F}_{q^n}$ とすると, $\Gamma_{\mathfrak{f}_{K_n}/\mathfrak{f}_K}$ は

  $$\overline{\sigma} \ : \mathfrak{f}_{K_n} \longrightarrow \mathfrak{f}_{K_n} \ : x \mapsto x^q$$

  で生成される巡回群である．そこで $\overline{\sigma}$ に対応する $\Gamma_{K_n/K}$ の元を σ_n と表し, これを K_n/K の **Frobenius 自己同型**という.

11.2 局所体の Brauer 群

定理 24 K を局所体として, $D \in \mathfrak{D}(K)$, $\deg D = d$ とする．このとき D は d 次不分岐拡大 K_d/K を部分体として含み

$$e(D/K) = f(D/K) = [K_d, K]$$

が成り立つ．とくに $K_d \subset D$ は極大部分体となり, D は巡回代数になる.

定理 25 K を局所体として, $\varpi \in K$ を素元とする．このとき写像

$$\theta_K \ : \mathbf{Q}/\mathbf{Z} \longrightarrow \mathrm{Br}(K) \ : \frac{m}{n} \mod \mathbf{Z} \mapsto [(K_n/K, \sigma_n, \varpi^m)]$$

は同型写像である.

12　代数体の Brauer 群

12.1　素点

$K/\mathbf{Q}$ を有限次拡大とする．

- **有限素点**

  K の非アルキメデス付値の同値類の集合を $V_{K,f}$ で表す．$V_{K,f}$ の要素を**有限素点**という．以下 $V_{K,f}$ の要素とそれを代表する非アルキメデス付値 v を同一視する．各 $v \in V_{K,f}$ に対し, K_v を K の距離 δ_v に関する完備化とする．K_v は局所体である．定理２２から, 同型

  $$\theta_v : \mathrm{Br}(K_v) \longrightarrow \mathbf{Q}/\mathbf{Z}$$

  がある．

- **無限素点**

  K から $\mathbf{C}$ の中への同型写像全体を $\mathrm{Hom}(K,\mathbf{C})$ とする．$\mathrm{Hom}(K,\mathbf{C})$ に同値関係 $\sim$ を

  $$\varphi \sim \psi \iff \varphi(x) = \overline{\psi(x)} \quad (x \in K)$$

  で定義して, 同値類全体の集合を $V_{K,\infty}$ と表す．$V_{K,\infty}$ の要素を K の**無限素点**という．同値類 $w \in V_{K,\infty}$ に対し, w の代表を $\psi_w \in \mathrm{Hom}(K,\mathbf{C})$ と表す．また

  $$K_w = \psi_w(K) \text{ の } \mathbf{C} \text{ の中での閉包}$$

  とおく．これは代表 ψ_w の取り方に関係なく定まり, $K_w = \mathbf{R}$ または $K_w = \mathbf{C}$ である．$K_w = \mathbf{R}$ のとき w を**実素点**といい, $K_w = \mathbf{C}$ のとき w を**複素素点**という．実素点全体の集合を $V_{K,1}$ で表し, 複素素点全体の集合を $V_{K,2}$ で表す．このとき

  $$[K:\mathbf{Q}] = \sharp(V_{K,1}) + 2\sharp(V_{K,2})$$

  が成り立つ．$w \in V_{K,1}$ ならば, 系７より写像

  $$\theta_w : \mathrm{Br}(K_w) = \mathrm{Br}(\mathbf{R}) \longrightarrow \frac{1}{2}\mathbf{Z}/\mathbf{Z} : \theta_w([A]) = \begin{cases} 1/2 + \mathbf{Z} & ([A] = [\mathbf{H}]) \\ 0 + \mathbf{Z} & ([A] = [1]) \end{cases}$$

  は同型になる．

- **素点**

  $V_K = V_{K,\infty} \cup V_{K,f}$ とおく．V_K の要素を K の**素点**という．

12.2　代数体上の中心的単純多元環

以下 $K/\mathbf{Q}$ を有限次拡大とする．任意の $A \in \mathfrak{A}_{cs}(K)$ と任意の $v \in V_K$ に対し

$$A_v = A \otimes_K K_v$$

とおく．

$$([A_v])_{v \in V_K} \in \prod_{v \in V_K} \mathrm{Br}(K_v)$$

で, 写像

$$\mathrm{Br}(K) \longrightarrow \prod_{v\in V_K} \mathrm{Br}(K_v) \,:\, [A] \mapsto ([A_v])_{v\in V_K}$$

は準同型になる.

定理 26 (Albert-Hasse-Brauer-Noether) $A \in \mathfrak{A}_{cs}(K)$, $\deg A = n$ とする.

(1) 有限個の素点を除いたほとんどすべての $v \in V_K$ で, $A_v \cong M_n(K_v)$ となる. とくに

$$([A_v])_{v\in V_K} \in \bigoplus_{v\in V_K} \mathrm{Br}(K_v).$$

(2) すべての $v \in V_K$ で $A_v \cong M_n(K_v)$ となるための必要十分条件は $A \cong M_n(K)$ となることである. 即ち写像

$$\mathrm{Br}(K) \longrightarrow \bigoplus_{v\in V_K} \mathrm{Br}(K_v)$$

は単射である.

(3) 次の完全系列がある.

$$1 \longrightarrow \mathrm{Br}(K) \longrightarrow \bigoplus_{v\in V_K} \mathrm{Br}(K_v) \xrightarrow{\sum \theta_v} \mathbf{Q}/\mathbf{Z} \longrightarrow 1$$

したがって

$$\mathrm{Br}(K) \cong \left\{ (\alpha_v) \in \bigoplus_{v\in V_K} \mathbf{Q}/\mathbf{Z} \;\middle|\; \sum_{v\in V_K} \alpha_v = 0,\ \ \alpha_w \in \frac{1}{2}\mathbf{Z}/\mathbf{Z}\ \ (w \in V_{K,1}),\ \ \alpha_w = 0\ \ (w \in V_{K,2}) \right\}.$$

定理 27 任意の $A \in \mathfrak{A}_{cs}(K)$ は巡回代数で $\mathrm{ind}(A) = \exp(A)$ が成り立つ.

13 Hausdorff-Banach-Tarski Paradox への応用

14 単純多元環の対合

15 Brauer-Severi 多様体

整数論特論 参考書

この講義の主題は中心的単純多元環の構造とその分類であるが, 残念ながらこのデーマについての日本語の教科書は Bourbaki の邦訳 (数学原論 代数６) または van der Waerden の邦訳 (現代代数学 III) 以外にほとんどない. 従って洋書が大部分である. まず, 非可換環論を含む結合的環 (associative ring) の一般論に関する教科書としては,

[1] Rowen, Ring Theory I & II, Academic Press, 1988

または

[2] Pierce, Associative Algebras, Springer Verlag, 1982

がある. [1] は詳細な専門書であり, この分野に関する結果はほとんど網羅されている. [2] は教科的で, [1] よりも読みやすい. この講義の Wedderburn の構造定理の証明, 巡回代数, 表象代数, 接合積は [1] を, また極大部分体や強極大部分体, 分解体の扱いは [2] を参考にしている. 少し古いが

[3] Herstein, Noncommutative Rings, The Mathematical Association of America, 1968

も読みやすい本である. 非可換代数や非可換体, Brauer 群に話題を限定した本として,

[4] Draxl, Skew Fields, Cambridge University Press, 1983

[5] Farb & Dennis, Noncommutative Algebra, Springer Verlag, 1993

[6] Jacobson, Finite-Dimensional Division Algebras over Fields, Springer Verlag, 1996

[7] Kersten, Brauergruppen von Körpern, Vieweg, 1990

がある. 局所体や代数体など特定の体上の Brauer 群の構造については, 結果だけならば上記 [1],[2],[4],[5] でも見られるが, 証明は

[8] Deuring, Algebren, Springer Verlag, 1968

[9] Albert, Structure of Algebras, American Mathematical Society, 1961

[10] Weil, Basic Number Theory, Springer Verlag, 1973

等に書かれている. 最近の非可換体論に関する結果と問題については

[11] Saltman, Lectures on Division Algebras, American Mathematical Society, 1999.

[12] Platonov & Yanchevskii, Finite-Dimensional Division Algebras, in Algebra IX, Encyclopaedia of Mathematical Sciences, Springer Verlag, 1996.

を見よ. [12] はサーベイである. 整数論的な興味からは, 代数体上の非可換体の整環 (order) の構造が取り上げられる. 整環の一般論については

[13] Reiner, Maximal Orders (2nd ed.), Clarendon Press, 2003

が標準的な教科書である. とくに四元数体の整環を詳細に調べたものとして

[14] Vignéra, Arithmétique des Algèbres de Quaternions, Springer Verlag, 1980

がある. Eichler の近似定理やゼータ関数については

[15] 清水英男, 近似定理, ヘッケ環, ゼータ関数, 東大数学教室セミナリーノート 21, 1968

を見よ. 代数体上の斜体の整環の単数群を調べたものとして

[16] Kleinert, Units in Skew Fields, Birkhäuser, 2000

がある. 他に, 中心的単純多元環上の対合 (involution), 代数群との関連については

[17] Knus, Merkurjev, Rost & Tignol, The Book of Involutions, American Mathematical Society, 1998

に詳しい.