中心的単純環の理論と中心的斜体に関する種々の問題について

長谷川寿人

新潟大学大学院自然科学研究科博士前期課程
数理物質科学専攻

概要

本論文では，著者が修士のセミナーで学んできた中心的単純環の理論の紹介と，それにまつわる種々の問題と今後著者が取り組んでいきたい問題についてまとめたものである．

体論において，体 k が与えられたとき，その上の拡大体 (ここでは非可換なものも含める) がどのくらいあるのか分類することが，体 k を知る上で基本的な問題である．その中でも，とくに非可換な拡大体がどのくらいにあるのかに焦点を当て研究するのが中心的単純環の理論である．中心的単純環の理論の中で，とくにブラウアー群 $\mathrm{Br}(k)$ は，k 上の中心的斜体がどのくらいあるのかを表しており，k 上の非可換拡大がどのくらいあるかを知る上で非常に重要な対象となる．さらに，ブラウアー群は 2 次のコホモロジーとの対応がある．このことから，とくに数論的な体に対しては中心的単純環の理論と k 上の可換拡大についての理論である類体論を，同じコホモロジーという枠組みの中でみることが可能になる．

本論文は，主に修士のセミナーの発表に基づいている．とくに [斉藤], [渡部], [GS06], [Pie82] は内容をまとめる上でよく参考にさせてもらった．また，各節のはじめには，その節の内容をまとめる上でとくに参考にした文献を載せた．各文献の詳細は，本論文の最後の参考文献を参照してほしい．

本論文は 4 つの章からなる：

第 1 章では体上の多元環の定義と基本事項についてまとめた．

第 2 章では，本論文の主要な対象である中心的単純環についての理論についてまとめた．2.1 節では，はじめに中心的単純環の最も基本的な定理である Wedderburn の構造定理を示し，中心的単純環のテンソル積，係数拡大，逆多元環について述べた．その後に，中心的単純環の理論において重要である Skolem–Noether の定理と中心化定理の証明を行った．2.2 節では体の重要な不変量であるブラウアー群を導入し，中心的単純環の研究において重要な役割を果たす分解体や被約特性多項式の性質についてまとめた．この節の最後に，ブラウアー群の具体例をいくつか紹介した．2.3 節では，中心的単純環のなかでも非常に重要なクラスである巡回多元環と接合積についての理論を述べた．2.4 節では，

ブラウアー群とガロアコホモロジーとの関係について述べた．ここでの理論から，ブラウアー群をコホモロジー的観点からみることが可能になる．最後の 2.5 節では第 2 章で用いられた有限群のコホモロジーの定義を補足としてまとめた．

第 3 章では，中心的単純環の中でも，とくに四元数環と中心的斜体に焦点を当て，それらの理論を紹介した．まず，3.1 節は四元数環についての理論であり，はじめに四元数環の基本的な性質をまとめた．その後に，四元数環の同型や分解体に関する性質を述べた．最後に Albert の定理とよばれる，四元数環のテンソル積がいつ斜体になるかを判定するための定理を示した．この定理は，4.4 節において 4 次の中心的斜体で巡回多元環にならないような例を構成する上で非常に重要な役割を果たす．3.2 節は中心的斜体についての理論である．はじめに，一般の中心的単純環 A に対してインデックス $\mathrm{ind}(A)$ とピリオド $\mathrm{per}(A)$ と呼ばれる，ブラウアー類における重要な不変量を定義し，それに対して成り立つ性質をまとめた．それを用いて，中心的斜体の重要な性質であるプライマリー分解について紹介する．その後，次数がとくに 3 次, 4 次の中心的斜体に対して知られている結果を紹介した．ここでは，次数 3 の中心的斜体は必ず巡回多元環になることを紹介し，次数が 4 の中心的斜体は必ずしも巡回多元環にならないことを，3.1 節で準備した Albert の定理などを用いた反例の紹介を行った．

最後の第 4 章では，中心的単純環の研究における種々の問題と，著者の今後の研究課題について述べた．4.1 節では，中心的単純環の研究において未解決である問題をいくつか紹介し，それらに対し現在までに知られている結果をまとめた．4.2 節では，現在著者が興味を持ち取り組んでいる，中心的斜体の巡回性の問題と中心的斜体の同型問題について紹介し，今後それらの問題に対してどのように取り組んでいきたいかを述べた．

謝辞

指導教員である星明考先生には，研究室のセミナーにおいて丁寧に指導していただき，今後の研究に関して様々な助言をいただきました．また，本論文の作成する上でも，多くの有益な御意見をいただきました．深く感謝致します．

研究室の先輩の三浦正道氏には，学部の頃からセミナーをみていただき，先輩として様々なアドバイスをいただきました．ここに感謝を致します．研究室の同期の金井和貴氏は，私の疑問点に対し真摯に考え，時には深夜にまで議論を交わすこともありました．感謝の意を表します．同じ代数系の研究室である小島研究室の先輩の長峰孝典氏は，我々の修士のセミナーに参加してくださり，多くの数学的なアドバイスを頂きました．また，本論文を作成する上でも様々な相談にのっていただきました．心より感謝いたします．

最後に，私を支えてくださった多くの皆様へ，心から感謝の気持ちと御礼を申し上げます．

目次

記号 1

1 体上の多元環 2

1.1 体上の多元環 2

1.2 体上の多元環のテンソル積 5

2 中心的単純環とブラウアー群 7

2.1 中心的単純環の理論 7

2.1.1 Wedderburn の構造定理 7

2.1.2 体上の多元環のテンソル積の中心，単純性 9

2.1.3 多元環の係数拡大 11

2.1.4 逆多元環 A° 12

2.1.5 Skolem–Noether の定理 13

2.1.6 中心化定理 15

2.2 ブラウアー群と分解体 19

2.2.1 ブラウアー群 $\mathrm{Br}(k)$ 19

2.2.2 分解体 20

2.2.3 被約特性多項式 25

2.2.4 ブラウアー群の実例 30

2.3 巡回多元環と接合積 33

2.3.1 巡回多元環 $(K/k, \sigma, b)$ 33

2.3.2 接合積 $(K/k, G, \varphi)$ 35

2.4 ブラウアー群とガロアコホモロジー 39

2.5 補足：有限群のコホモロジーの定義 41

3 中心的単純環の具体例 44

3.1 四元数環の理論 44
3.1.1 基本事項 44
3.1.2 四元数環の同型 48
3.1.3 2 次体上での分解体 49
3.1.4 Albert の定理 51
3.2 中心的斜体の理論 53
3.2.1 インデックス $\mathrm{ind}(A)$ とピリオド $\mathrm{per}(A)$ 53
3.2.2 中心的斜体のプライマリー分解 57
3.2.3 次数 3 の中心的斜体 59
3.2.4 次数 4 の中心的斜体 60

4 種々の問題と今後の研究課題 62
4.1 種々の問題 62
4.1.1 中心的斜体に関する問題 62
4.1.2 インデックスとピリオドに関する問題 64
4.2 今後の研究課題 65
4.2.1 中心的斜体の巡回性の問題 65
4.2.2 中心的斜体の同型問題 66

記号

本稿で用いる記号や用語に関する注意をはじめに述べておく．

・$\mathbb{N}$ を自然数全体，$\mathbb{Z}$ を整数環，$\mathbb{Q}$ を有理数体，$\mathbb{R}$ を実数体，$\mathbb{C}$ を複素数体とする．

・$\mathbb{F}_q$ を位数 q の有限体とする．

・自然数 n, m に対し，$n \mid m$ で m が n の倍数であることを表す．

・環 R は，0 でない単位元を持つものと仮定する．

・環 R に対し，可逆元全体のなす群を $R^{\times}$ とする．

・単に体 k 上の線形空間といった場合，左 k 加群を指すものとする．右からのスカラー倍は定義していないことに注意する．

本論文では，今後，体は可換体を指すことにする．また，特に断らない限り k を体とし，$\overline{k}$ を k の代数閉包とする．

1　体上の多元環

1.1　体上の多元環

　本節では体 k 上の多元環の定義を行い，それに付随するいくつかの用語を準備する．また，今後扱う重要な多元環の例として，行列環や自己準同型写像のなす多元環についての事柄についても確認しておく．この節は，[斉藤], [渡部], [GS06] を参考にした．

定義　k 上の線形空間 A が k 上の**多元環** (k-algebra) であるとは, A が積の構造も持っており，

$$\text{任意の } \lambda \in k,\ x,\ y \in A \text{ に対し, } \lambda(xy) = (\lambda x)y = x(\lambda y)$$

が成り立つときをいう．k 上の多元環 D が**斜体** (k-division algebra) であるとは, D の 0 以外の元が逆元をもつときをいう．k 上の多元環 A の**次元** (dimension) は，A の k 上の線形空間としての次元とし，$[A:k]$ で表す．

例 1.1 (体 k 上の行列環) 体 k 上の n 次の正方行列 $\mathrm{M}_n(k)$ は，通常の和，スカラー倍，積に関して k 上の多元環になる．単位行列を E_n と表し，(i,j) 成分のみが 1 で他の成分が 0 である行列を $E_{i,j}$ で表す．$E_{i,j}$ を**行列単位**という．また，各行と各列に 1 が 1 つのみ入っている行列を**置換行列**という．

例 1.2 (多元環上の加群の自己準同型写像) A を k 上の多元環とし，左 A 加群を M とする．A の左 A 加群としての自己準同型写像全体 $\mathrm{End}_A(M)$ は，$f, g \in \mathrm{End}_A(M)$, $\lambda \in k$, $v \in V$ に対し，

$$(f+g)(v) = f(v) + g(v),\ (\lambda \cdot f)(v) = \lambda \cdot f(x),\ (f \cdot g)(v) = f(g(v))$$

と定めることにより，$\mathrm{End}_A(M)$ も k 上の多元環になる．

例 1.3 (四元数環) 体 k を標数 2 ではないものとする．a, $b \in k^\times$ に対し，k 上の 4 次元の k 上の多元環で，k 上の線形空間としての基底として $\{1, i, j, ij\}$ をもち，積に関しては

$i^2 = a$, $j^2 = b$, $ij = -ji$ みたすものを**四元数環** (quaternion algebra) といい，$\left(\frac{a,b}{k}\right)$ と表す．とくに，$k = \mathbb{R}$, $a = b = -1$ の場合は，Hamilton の四元数環であり，$\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$ と表す．

本論文では，以下 k 上の多元環といった場合，有限次元のものを指すことにする．

代数閉体 Ω 上には自身以外の斜体は存在しない．まず，このことをみてみよう．

命題 1.4 代数閉体 Ω 上の斜体は Ω のみである．

証明 Ω 上の斜体を D とする．任意に $a \in D$ をとる．すると，Ω の元と a によって生成される D の部分環 $\Omega[a]$ は体になる．すると，$\Omega[a]$ は Ω 上の有限次代数拡大になるから，a は Ω 上代数的である．すると，Ω が代数閉体であることから $a \in \Omega$ である．よって，$D = \Omega$ である． □

A を k 上の多元環とする．このとき，単純な左 A 加群の A 自己準同型写像のなす k 上の多元環は斜体になる．これは，Schur の補題と呼ばれるものの特別な場合である．本論文では，これを単に Schur の補題ということにする．

命題 1.5 (Schur の補題) A を k 上の多元環とする．このとき，単純な左 A 加群 M に対し，$\mathrm{End}_A(M)$ は k 上の斜体である．

証明 任意に 0 でない元 $f \in \mathrm{End}_A(M)$ をとる．$\mathrm{Ker}(f)$ は M の部分加群で，M が単純であることから $\mathrm{Ker}(f) = \{0\}$，よって f は単射である．また，$\mathrm{Im}(f)$ は M の部分加群で，M が単純であることから $\mathrm{Im}(f) = M$，よって f は全射である．よって，f は同型写像である．これより，f は逆写像をもつ．よって，$\mathrm{End}_A(M)$ は斜体である． □

定義 k 上の多元環 A の部分線形空間 $B \subset A$ が A の部分環であるとき，B は A の**部分多元環** (k-subalgebra) であるという．

定義 A, B を k 上の多元環とする．このとき, 写像 $f : A \to B$ が多元環の**準同型写像** (k-homomorphism) であるとは, f が線形写像であり，かつ環としての準同型写像であるときをいう．特に，多元環の準同型写像が全単射であるとき，多元環の**同型写像**

(k-isomomorphism) という．k 上の多元環 A, B に対し, 多元環の同型写像 f が存在するとき, A, B は多元環として k 上**同型** (k-isomorphic) であるといい, $A \simeq B$ とかく．

定義 A を k 上の多元環とし, A の部分集合を $S \subset A$ とする．このとき,

$$\mathrm{Z}_A(S) = \{a \in A \mid \text{任意の } s \in S \text{ に対し}, as = sa \}$$

とする．$\mathrm{Z}_A(S)$ は A の k 上の部分多元環である．とくに，$S = A$ のときは，単に $\mathrm{Z}(A)$ とかき A の**中心** (center) という．

定義 A を k 上の多元環とし，0 でない A の左イデアル $I \subset A$ とする．このとき，I に真に含まれる A の左イデアルが $\{0\}$ しかないとき, I を**極小左イデアル** (minimal left ideal) であるという．極小右イデアル (minimal right ideal) も同様に定義する．必ず $\{0\}$, A は A の両側イデアルになる．これを**自明な両側イデアル** (trivial two sided ideal) という．

D を k 上の斜体とする．D 上の行列環 $\mathrm{M}_n(D)$ の極小左イデアルについてみてみよう．このとき，$j = 1, \ldots, n$ に対し，j 列目のみに D の元がはいり，他の列には 0 のみしか入らない行列のなす集合を

$$I_j = \left\{ \begin{pmatrix} & \overset{j}{\check{a}_{1,j}} & \\ \text{\huge 0} & \vdots & \text{\huge 0} \\ & a_{n,j} & \end{pmatrix} \in \mathrm{M}_n(D) \,\middle|\, a_{i,j} \in D \right\} \simeq D^n$$

とする．この I_j $(j = 1, \ldots, n)$ は $\mathrm{M}_n(D)$ の左イデアルになる．このとき, 次が成り立つ．

命題 1.6 D 上の行列環 $\mathrm{M}_n(D)$ の極小左イデアルは I_j $(j = 1, \ldots, n)$ のいずれかである．

証明 $\mathrm{M}_n(D)$ の左イデアルの元は，$\mathrm{M}_n(D)$ の置換行列の左からの積に関して閉じていることから，いくつかの列に D の元がはいり，他の列は 0 のみしか入らない行列となる．よって，極小な左イデアルは，1 列のみにしか D の元が入らない行列からなるものであるから，$\mathrm{M}_n(D)$ の極小左イデアルは I_j $(j = 1, \ldots, n)$ のいずれかに等しい． □

本論文の主要な対象である中心的単純環は，次のようなものである．2.1 節において，中心的単純環の基本的な事項について確認する．

定義 A を k 上の多元環とする．A の中心 $\mathrm{Z}(A)$ が k であるとき，A は k **上中心的** (k-central) であるという．また，A が自明な両側イデアル以外の両側イデアルをもたないとき，A は**単純** (simple) であるという．k 上中心的であり，かつ単純である多元環を k 上の**中心的単純環** (k-central simple algebra) という．

中心的単純環の典型的な例として，中心的斜体上の行列環があげられる．このことについてみてみよう．

命題 1.7 D を k 上の斜体とする．このとき，D 上の n 次の行列環 $\mathrm{M}_n(D)$ は単純である．また，D が k 上中心的であれば，$\mathrm{M}_n(D)$ は中心的単純環である．

証明 I を 0 でない $\mathrm{M}_n(D)$ の両側イデアルとする．I の 0 でない行列 $M = (m_{i,j})_{1\leq i,j\leq n}$ をとり，$m_{s,t} \neq 0$ であるとする．すると，任意の $1 \leq r \leq n$ に対して，行列単位を用いて，

$$E_{r,r} = \frac{1}{m_{s,t}} E_{r,s} M E_{t,r} \in I$$

であるから，単位行列 $E_n = \sum_{r=1}^{n} E_{r,r}$ は I の元となる．よって，$\mathfrak{a} = \mathrm{M}_n(D)$ となり，$\mathrm{M}_n(D)$ は単純である．

また，D 上の行列環 $\mathrm{M}_n(D)$ の中心は $\mathrm{Z}(\mathrm{M}_n(D)) = \mathrm{Z}(D)$ である．よって，D が k 上中心的であれば，$\mathrm{Z}(\mathrm{M}_n(D)) = k$ となり，$\mathrm{M}_n(D)$ は k 上の中心的単純環となる． $\square$

上の命題から，とくに k 上の行列環 $\mathrm{M}_n(k)$ は中心的単純環である．行列環は中心的単純環のベースとなっている重要な対象である．

1.2 体上の多元環のテンソル積

この節では，k 上の線形空間に対するテンソル積において成り立つ性質を復習し，k 上の多元環のテンソル積の定義を行う．本節は，[斉藤] を参考にした．

まず，体 k 上の線形空間に対するテンソル積において成り立つ性質を復習しておこう．証明については [斉藤] を参照せよ．以下，特に基礎体 k が明らかなときは，テンソル積 $\otimes_k$ を単に $\otimes$ とかく．

命題 1.8 V_i $(i = 1, \ldots, n)$ を k 上の線形空間とし，$V = \otimes_{i=1}^n V_i$ とする．このとき，$(\otimes_{i=1}^n V_i) \otimes_k W \simeq \otimes_{i=1}^n (V_i \otimes W)$ が成り立つ．

命題 1.9 V, W を k 上の線形空間とし，$\{\alpha_1, \ldots, \alpha_n\}$ を V の基底とする．このとき，$V \otimes W$ の元は $\sum_{i=1}^n \alpha_i \otimes \beta_i (\beta_i \in W)$ と一意的にかける．

命題 1.10 U, V, W を k 上の線形空間とする．このとき，$V \otimes W \simeq W \otimes V$, $(U \otimes V) \otimes W \simeq U \otimes (V \otimes W)$ が成り立つ．

次に，k 上の多元環のテンソル積の定義をしよう．

定義 A, B を k 上の多元環とする．k 上の線形空間としてのテンソル積 $A \otimes B$ に対し，

$$(a \otimes b) \cdot (a' \otimes b') := (aa') \otimes (bb') \ (a, a' \in A,\ b, b' \in B)$$

により積を定めると，$A \otimes_k B$ は k 上の多元環になる．これを，k 上の多元環 A, B の k 上の**テンソル積** (tensor product) という．

命題 1.11 A を k 上の多元環とする．このとき，$\mathrm{M}_n(k) \otimes A \simeq \mathrm{M}_n(A)$ が成り立つ．とくに，$\mathrm{M}_n(k) \otimes \mathrm{M}_m(k) \simeq \mathrm{M}_{nm}(k)$ が成り立つ．

証明 k 上の多元環としての準同型写像 $\varphi : \mathrm{M}_n(k) \otimes_k A \to \mathrm{M}_n(A)$, $(\lambda_{i,j}) \otimes \alpha \mapsto (\alpha\lambda_{ij})$ を考えると，この写像は全射であり，k 上の次元を見ることで φ が同型であることがわかる．

また，特に，$A = \mathrm{M}_n(k)$ とすると，$\mathrm{M}_n(k) \otimes_k \mathrm{M}_m(k) \simeq \mathrm{M}_n(\mathrm{M}_m(k)) \simeq \mathrm{M}_{nm}(k)$ より，$\mathrm{M}_n(k) \otimes_k \mathrm{M}_m(k) \simeq \mathrm{M}_{nm}(k)$ が得られる． $\square$

2　中心的単純環とブラウアー群

2.1　中心的単純環の理論

本節では，本論文での主要な対象である中心的単純環に関する性質をみていく．とくに，重要な結果として，Wedderburn の構造定理 (2.1.1 節)，Skolem–Noether の定理 (2.1.5 節)，中心化定理 (2.1.6 節) が挙げられる．この節は，[斉藤], [渡部], [Cla], [Ten], [GS06] を参考にした．

2.1.1　Wedderburn の構造定理

命題 1.7 より，k 上の斜体 D 上の行列環 $\mathrm{M}_n(D)$ は k 上の単純多元環であることをみた．逆に，k 上の単純多元環は，ある k 上の斜体 D 上の行列環と同型になるというのが次の Wedderburn の構造定理である．これは，中心的単純環の理論において最も基本的な定理である．ここでの証明は [Ten] を参考にした．

定理 2.1 (Wedderburn の構造定理)　A を k 上の単純多元環とする．このとき，自然数 n と k 上の斜体 D が存在して，

$$A \simeq \mathrm{M}_n(D)$$

となる．さらに，上の斜体 D は同型を除き一意的に定まる．

証明　I を A の極小左イデアル，$D = \mathrm{End}_A(I)$ とする．Schur の補題 (命題 1.5) より，$D = \mathrm{End}_A(I)$ は斜体である．$d \in D$，$v \in I$ に対し，$d \cdot v = d(v)$ と作用させることで，I を D 上の線形空間とみなす．A が k 上有限次元であることから，I は D 上の線形空間として有限次元である．よって，ある自然数 n に対し，$I \simeq D^n$ となる．環の準同型写像 $\rho : A \to \mathrm{End}_D(I)$, $a \mapsto L_a$ と定める．ここで，$L_a : I \to I$, $L_a(x) = ax$ $(a \in A)$ である．k 上の多元環 A は単純であるから ρ は単射である．

次に，ρ は全射を示そう．それには，$\rho(A)$ が $\mathrm{End}_D(I)$ の左イデアルであることを示せば，$\rho(1) = \text{Ł}_1 = \mathrm{id}_I \in \rho(A)$ より，$\rho(A) = I$ となる．そのために，まず $\rho(I)$ が $\mathrm{End}_D(I)$

の左イデアルであることを示そう．任意の $w \in I$ に対し，$R_w : I \to I,\ x \mapsto xw$ は $D = \mathrm{End}_A(I)$ の元である．よって，任意の $v \in I$, $f \in \mathrm{End}_D(I)$ に対し，

$$(f \cdot \rho(v))(w) = f(L_v(w)) = f(vw) = f(R_w(v)) = R_w \circ f(v) = L_{f(v)}(w)\ (w \in I)$$

より，$f \cdot \rho(v) = L_{f(v)} = \rho(f(v)) \in \rho(I)$ となるから，$\rho(I)$ は $\mathrm{End}_D(I)$ の左イデアルである．次に，IA は A の両側イデアルであるから，A は単純より $IA = A$ である．これより，$\rho(A) = \rho(I)\rho(A)$ である．よって，$\rho(I)$ は左イデアルであるから，$\rho(A)$ も $\mathrm{End}_D(I)$ の左イデアルである．よって，ρ は全射である．以上より，ρ は同型写像であるから，$A \simeq \mathrm{End}_D(I) \simeq \mathrm{M}_n(D)$ である．

また，補題 1.6 から A の極小左イデアル I は

$$I \simeq I_1 = \left\{ \begin{pmatrix} a_{1,1} & & \\ \vdots & & \text{\huge 0} \\ a_{n,1} & & \end{pmatrix} \in \mathrm{M}_n(D) \;\middle|\; a_{i,1} \in D \right\}$$

である．多元環としての準同型写像 $\varphi : D \to \mathrm{End}_A(I_1),\ d \mapsto R_d$ を考える．ここで，$R_d : I \to I,\ R_d(a) = ad\ (d \in D)$ である．D が単純多元環であることから，φ は単射である．

次に，φ の全射性を示そう．任意に $f \in \mathrm{End}_A(I_1)$ をとり，

$$v = \begin{pmatrix} 1 & & \\ \vdots & & \text{\huge 0} \\ 1 & & \end{pmatrix} \in I_1$$

とおく．I_1 は極小左イデアルだから，左 $\mathrm{M}_n(D)$ 加群として単純である．よって，$\mathrm{M}_n(D)v = I_1$ である．任意の $a \in A \simeq \mathrm{M}_n(D)$ に対し，$f(av) = af(v)$ であることに注意すると，f は $f(v)$ によって決まる写像である．ここで，$a \in \mathrm{M}_n(D)$ として置換行列をとり，$f(av) = af(v)$ を考えると，ある $d \in D$ が存在して，$f(v) = vd = R_d(v)$ となる．よって，φ は全射となる．すると，φ は，D から $\mathrm{End}_A(I)$ への同型写像になる．よって，$D \simeq \mathrm{End}_A(I_1) \simeq \mathrm{End}_A(I)$ となる．これより，D は A とその極小左イデアル I により定まるから，D は同型を除き一意的に定まる． $\square$

2.1.2　体上の多元環のテンソル積の中心，単純性

1.2 節で多元環のテンソル積を定義した．ここでは，2 つの k 上の多元環のテンソル積の中心や単純性がどのようになるかについてみてみる．

まず，2 つの k 上の多元環のテンソル積の中心がどのようになるかをみてみよう．中心だけでなく，より一般的な場合を示す．

命題 2.2　A, B を k 上の多元環，R, S をそれぞれ A, B の部分多元環とする．このとき，

$$\mathrm{Z}_{A\otimes B}(R\otimes S)=\mathrm{Z}_A(R)\otimes \mathrm{Z}_B(S)$$

が成り立つ．

証明　$\mathrm{Z}_{A\otimes B}(R\otimes S)\supset \mathrm{Z}_A(R)\otimes \mathrm{Z}_B(S)$ は定義より従う．

任意に $x\in \mathrm{Z}_{A\otimes B}(R\otimes S)$ をとる．B の k 上の線形空間としての基底を $f_1,\dots,f_m$ $(m=[B:k])$ とすると，

$$x=\sum_{j=1}^{m} a_j\otimes f_j\ (a_j\in A)$$

とかける．このとき，x の取り方から，任意の $a\in R$ に対して，$(a\otimes 1_B)\cdot x=x\cdot(a\otimes 1_B)$ が成り立つ．ここで，$f_1,\dots,f_m$ が k 上一次独立であることに注意すると，，命題 1.9 より，$\sum_{j=1}^{m}(aa_j-a_ja)f_j=0$ であるから，任意の $j=1,\dots,m$ に対し，$aa_j=a_ja$ が成り立つ．これにより，$a_j\in \mathrm{Z}_A(R)$ となるから，$x\in \mathrm{Z}_A(R)\otimes B$ である．

次に，$\mathrm{Z}_A(R)$ の k 上の線形空間としての基底を $e_1,\dots,e_n$ $(n=[\mathrm{Z}_A(R):k])$ とすると，

$$x=\sum_{i=1}^{n} e_i\otimes b_i\ (b_i\in B)$$

とかける．ここで，$\mathrm{Z}_A(R)$ が A の k 上の部分多元環であることに注意しておこう．このとき，上と同様の計算によって，任意の $b\in S$ に対して，$bb_i=b_ib$ $(i=1,\dots,n)$ となるから，$b_i\in \mathrm{Z}_B(S)$ となる．これより，$x\in \mathrm{Z}_A(R)\otimes \mathrm{Z}_B(S)$ が得られる．　$\square$

特に，上の命題で $R=A, S=B$ とすると，2 つの k 上の多元環のテンソル積の中心が

どのようになるかがわかる．

系 2.3 $\mathrm{Z}(A\otimes B)=\mathrm{Z}(A)\otimes\mathrm{Z}(B)$．とくに，$A$，$B$ が k 上の中心的多元環ならば，$A\otimes B$ も k 上の中心的多元環である．

次に，2 つの k 上の多元環のテンソル積の単純性がどうなるのかをみてみよう．

命題 2.4 A を k 上の中心的多元環，B を k 上の多元環とする．このとき，以下は同値である．

(1) $A\otimes B$ が単純多元環である．

(2) A, B がともに単純多元環である．

証明 (1) $\Rightarrow$ (2) もし，A が非自明な両側イデアル I をもったとすると，$I\otimes B$ は $A\otimes B$ の非自明な両側イデアルとなり，(1) の仮定に反する．よって，A は単純である．B も同様に単純であることが分かる．

(2) $\Rightarrow$ (1) A, B が単純多元環であるとし，任意に $A\otimes B$ の 0 でない両側イデアル I をとる．まず，A, B がともに単純多元環であることから，$a\in A\setminus\{0\}, b\in B\setminus\{0\}$ に対して，$1_A\in AaA, 1_B\in BbB$ であることに注意する．

$x\in I$ に対し，

$$p(x)=\min\{n\in\mathbb{N}\mid x=\sum_{i=1}^{n}a_i\otimes b_i\ (a_i\in A,\ b_i\in B)\ \}$$

とし，$r=\min\{p(x)\mid x\in I\setminus\{0\}\}$ とおく．すると，$r=1$ であることを示そう．実際，$r>1$ と仮定すると，$x\in I$ で，

$$p(x)=r,\ x=\sum_{i=1}^{r}a_i\otimes b_i$$

となるものがある．ここで，最初の注意により $a_r=1$ としてよい．このとき，$p(x)=r$ であることから，$a_{r-1}, a_r(=1)$ は k 上一次独立である．すると，$a_{r-1}\notin k=\mathrm{Z}(A)$ であるから，$ca_{r-1}\neq a_{r-1}c$ となる元 $c\in A$ がとれる．このとき，$x'=(c\otimes 1_B)x-x(c\otimes 1_B)$ とすると，$x'=\sum_{i=1}^{r-1}(ca_i-a_ic)\otimes b_i$より，$x'\in I\setminus\{0\}$ で，$p(x')<r$ となり x のとり方

に矛盾する．よって，$r=1$ である．

すると，I の 0 でない元で $a\otimes b$ $(a\in A,\, b\in B)$ の形の元が含まれる．ここで，最初の注意により $1_A\otimes 1_B\in I$ とでき $I=A\otimes B$ となる．よって，$A\otimes B$ は単純多元環である． □

注意　命題 2.4 においては，A または B の少なくとも一方は中心的であるという仮定は外せない．実際，$\mathbb{C}$ を $\mathbb{R}$ 上の多元環とみなし，$T=\mathbb{C}\otimes\mathbb{C}$ とすると，$\mathbb{C}$ を $\mathbb{R}$ 上の単純多元環であるが，T は $\mathbb{R}$ 上単純多元環とはならない．このことをみるには，T が可換環であることから，もし T が単純であるとすると，体となることに注意する．$x=1\otimes i-i\otimes 1$, $y=1\otimes i+i\otimes 1\in T$ とすると，$1, i$ は $\mathbb{R}$ 上一次独立であるから，$x\neq 0, y\neq 0$ であるが，

$$xy=1\otimes i^2-i^2\otimes 1=1\otimes(-1)-(-1)\otimes 1=0$$

となる．よって，T は整域でないため，体とはならない．よって，T は単純多元環でない．

系 2.3 と命題 2.4 から次の定理が得られる．これは，今後定義するブラウアー群を定義する上で非常に重要となる事実である．

定理 2.5　A, B を k 上の中心的単純環とする．このとき，$A\otimes B$ も k 上の中心的単純環である．

2.1.3　多元環の係数拡大

K/k を体の拡大とする．k 上の多元環 A と K の k 上のテンソル積 $A\otimes K$ は K 上の多元環とみることができる．これにより，k 上の多元環の係数体を K に上げることができる．このとき，次が成り立つ．

命題 2.6　K/k を拡大体とする．このとき，A が k 上の中心的単純環ならば，$A\otimes K$ は K 上の中心的単純環となる．

証明　命題 2.4 より，$A\otimes K$ は単純多元環であり，命題 2.2 より，$\mathrm{Z}(A\otimes K)=\mathrm{Z}(A)\otimes \mathrm{Z}(K)=k\otimes K=K$ より，K 上の中心的である． □

中心的単純環の係数拡大に関する重要な性質として，k の中心的単純環を k の代数閉包 $\overline{k}$ まで係数拡大をすると必ず $\overline{k}$ 上の行列環と同型になることが挙げられる．この性質を述べているのが次の命題である．

命題 2.7 A を k 上の中心的単純環とする．このとき，$A \otimes \overline{k} \simeq \mathrm{M}_d(\overline{k})$ となる．

証明 $\Omega = \overline{k}$ とおく．A は k 上の中心的単純環であるから，命題 2.4 より $A \otimes \Omega$ は Ω 上の単純多元環になる．よって，Wedderburn の構造定理 (定理 2.1) と，命題 1.4 より，Ω 上に非自明な斜体 D が存在しないことから，ある自然数 d が存在して，$A \otimes \Omega \simeq \mathrm{M}_d(\Omega)$ となる． □

この命題により, 中心的単純環 A の k 上の次元は必ず平方数になることがわかる．実際，$\Omega = \overline{k}$ とすると, k 上の中心的単純環の次元は $[A : k] = [A \otimes \Omega : \Omega] = [\mathrm{M}_d(\Omega) : \Omega] = d^2$ となる．そこで，中心的単純環 A の次数を次のように定義する．

定義 A を k 上の中心的単純環とする．このとき，A の k 上の**次数** (degree) を $\deg A = \sqrt{[A : k]}$ で定める．

2.1.4 逆多元環 A°

ここで，少し一般の k 上の多元環 A の話に戻る．k 上の多元環 A に対し，A の逆多元環 A° と呼ばれる k 上の多元環を定義する．

定義 A を k 上の多元環とする. k 上の線形空間としての構造は A と同じだが，積 $\cdot$ が

$$a \cdot b = ba \ (a,\, b \in A)$$

で与えられる k 上の多元環を A の**逆多元環** (opposite algebra) といい，A° と表す.

逆多元環に関しては次の事実が重要である．この事実は，この後定義するブラウアー群においては，中心的単純環 A に対応するブラウアー群の元の逆元となるという事実に対応するものになっている．

命題 2.8 A を k 上の中心的多元環とし, $\deg(A) = n$ とする．このとき, $A \otimes A^{\circ} \simeq \mathrm{M}_{n^2}(k)$ である．

証明 多元環としての準同型写像 Φ を $\Phi : A \otimes A^{\circ} \to \mathrm{End}_k(A)$, $\sum_{i=1}^{m} a_i \otimes a_i' \mapsto \sum_{i=1}^{m} \varphi_{a_i, a_i'}$ と定める．ここで，$\varphi_{a,a'} : A \to A,\ x \mapsto axa'\ (a, a', x \in A)$ である．A が単純多元環であることから，A° も単純多元環である．すると，命題 2.4 により $A \otimes A^{\circ}$ も単純多元環であることがわかる．よって，Φ は零写像ではないから，Φ は単射である．また， $\mathrm{End}_k(A) \simeq \mathrm{M}_{n^2}(k)$ に注意すると，次元の関係から Φ が全単射になることがわかる．よって，$A \otimes A^{\circ} \simeq \mathrm{M}_{n^2}(k)$ である． □

2.1.5 Skolem–Noether の定理

行列環の理論でよく知られていることとして，k 上の行列環 $\mathrm{M}_n(k)$ の k 上の多元環としての自己同型写像は必ず内部自己同型写像，つまり $M \mapsto CMC^{-1}$ となる $C \in \mathrm{GL}_n(k)$ が存在して，それによって与えられるというものがある．この事実の一般化にあたるものが Skolem–Noether の定理である．

その証明の為に，補題を 2 つ示しておこう．

補題 2.9 A を k 上の単純多元環とし，M を有限生成左 A 加群，L を A の極小左イデアルとする．すると，M は L のいくつかの直和と同型である．すなわち，ある自然数 $s \in \mathbb{N}$ が存在して，

$$M \simeq \bigoplus_{i=1}^{s} L$$

である．

証明 Wedderburn の構造定理 (定理 2.1) より，$A \simeq \mathrm{M}_n(D)$ となる k 上の斜体 D が存在する．

A は左 L 加群として有限生成であるから，M も左 L 加群として有限生成である．よって，その最小の生成系を $\{m_1, \ldots, m_s\}$ とすれば，$M = \sum_{i=1}^{s} Lm_i$ となる．

ここで，左 A 加群としての全射準同型写像

$$\varphi : \bigoplus_{i=1}^{s} L \to M,\ (r_1, \ldots, r_s) \mapsto \sum_{i=1}^{s} r_i m_i$$

と定める．

単射となることを示そう．$\sum_{i=1}^{s} r_i m_i = 0$ $(r_i \in L)$ とする．ここで，ある j に対し $r_j \neq 0$ と仮定し，矛盾を導く．ここで，$j = 1$ としても一般性を失わない．$Ar_1 \subset L$ は 0 でない A の左イデアルであるから，L の極小性から $Ar_1 = L$ となる．すると，

$$Lm_1 = Ar_1 m_1 = A\left(-\sum_{i=2}^{s} r_i m_i\right) \subset \sum_{i=2}^{s} Lm_i$$

となることから，

$$M = \sum_{i=1}^{s} Lm_i = \sum_{i=2}^{s} Lm_i$$

となり，$\{m_1, \ldots, m_s\}$ が最小の個数の M の生成系であったことに矛盾する．よって，任意の j に対し $r_j = 0$ となり，φ は単射となる．

ゆえに，φ は同型写像になり，$M \simeq \bigoplus_{i=1}^{s} L$ が得られる． □

補題 2.10 A を k 上の単純多元環とし，M_1, M_2 を有限生成左 A 加群となる．このとき，以下は同値である．

(1) $[M_1 : k] = [M_2 : k]$ である．

(2) $M_1 \simeq M_2$ である．

証明 補題 2.9 より，L を A の極小イデアルとすると，$M_1 \simeq L^{m_1}, M_2 \simeq L^{m_2}$ となる．すると，$[M_1 : k] = [M_2 : k]$ であることは，$m_1 = m_2$ と同値であるから，$M_1 \simeq M_2$ と同値である． □

ここで本題である Skolem–Noether の定理は次の定理である．

定理 2.11 (Skolem–Noether の定理) A を k 上の中心的単純環，B は k 上の単純多元環とする．このとき，2 つの多元環としての準同型写像 $f, g : B \to A$ に対して，$u \in A^{\times}$ が存在して $g(b) = uf(b)u^{-1}$ $(b \in B^{\times})$ が成り立つ．

証明　$C = A \otimes B^\circ$ とする．$\tau_f : C \to \mathrm{End}_k(A)$，$\tau_f(a \otimes b)(x) = axf(b)$，$\tau_g : C \to \mathrm{End}_k(A)$，$\tau_g(a \otimes b)(x) = axg(b)$ により，A を左 C 加群とみなしたものをそれぞれ A_f，A_g とする．このとき，命題 2.4 より，C は k 上の単純多元環である．このとき，A_f と A_g の k 上の次数は等しいから，補題 2.10 より，左 C 加群としての同型写像 $\varphi : A_g \to A_f$ が存在する．$\varphi(1) = u \in A$ とすると，任意の $x \in A$ に対し

$$\varphi(x) = \varphi(x1) = \varphi(\tau_g(x \otimes 1)(1)) = \tau_f(x \otimes 1)(\varphi(1)) = xu$$

が成り立つ．φ は同型写像より，$u \in A^\times$ である．さらに任意の $b \in B$ に対し，

$$g(b)u = \varphi(g(b)) = \varphi(\tau_g(1 \otimes b)(1)) = \tau_f(1 \otimes b)(\varphi(1)) = uf(b)$$

より，$g(b) = uf(b)u^{-1}$ が成り立つ． □

例 2.12 ($\mathrm{M}_n(k)$ の自己準同型群) この定理を用いて，k 上の行列環 $\mathrm{M}_n(k)$ の k 自己同型写像は必ず内部自己同型となることを確認しよう．Skolem–Noether の定理における A，B をどちらも $\mathrm{M}_n(k)$，f を恒等写像とすることで，任意の $\mathrm{M}_n(k)$ の k 上の多元環としての自己同型写像 g に対し，$g(M) = CMC^{-1}$ となる $C \in \mathrm{M}_n(k)^\times = \mathrm{GL}_n(k)$ が存在する．このことから，Skolem–Noether の定理は行列環での自己同型写像に関する事実の一般化になっていることが確認できる．また，群の準同型写像 $\mathrm{GL}_n(k) \to \mathrm{Aut}(\mathrm{M}_n(k))$，$C \mapsto (M \mapsto CMC^{-1})$ は上のことから全射であり，この準同型写像の核は $\mathrm{M}_n(k)$ の中心，すなわち k のスカラー行列である．よって，$\mathrm{Aut}(\mathrm{M}_n(k)) = \mathrm{GL}_n(k)/k = \mathrm{PGL}_n(k)$ となることがわかる．

2.1.6　中心化定理

ここで示す中心化定理とは，中心的単純環 A と，その単純な部分多元環 B に対して，A の部分多元環 $\mathrm{Z}_A(B)$ がどのような部分多元環になっているのかを述べている定理である．この定理により，A の部分多元環の中で，部分多元環 $\mathrm{Z}_A(B)$ は比較的扱いやすい対象であることがわかる．

中心化定理の証明の前に 4 つ補題を準備しておこう．

補題 2.13 A を k 上の中心的多元環，B を A の部分多元環とする．A を $(a\otimes b)\cdot x = axb$ $(a,\ b,\ x\in A)$ によって，左 $A\otimes A^\circ$ 加群とみる．このとき，$\mathrm{End}_{A\otimes B^\circ}(A)\simeq \mathrm{Z}_A(B)$ である．

証明 命題 2.8 での多元環としての同型写像 $\Phi : A\otimes A^\circ \longrightarrow \mathrm{End}_k(A),\ \sum_{i=1}^m a_i\otimes b_i \mapsto \sum_{i=1}^m \varphi_{a_i,b_i}$ を考える．ここで，$\varphi_{a,b} : A\to A,\ x\mapsto axb\ (a,\ b\in A)$ である．$A\otimes B^\circ$ は $A\otimes A^\circ$ の部分環であるから，A は左 $A\otimes B^\circ$ 加群ともみれる．$f\in \mathrm{End}_k(A)$ に対し，$f\in \mathrm{End}_{A\otimes B^\circ}(A)$ であることは，任意の $a\in A,\ b\in B$ に対し $(f\circ\varphi_{a,b})(x) = f(axb) = f((a\otimes b)\cdot x) = (a\otimes b)\cdot f(x) = af(x)b = (\varphi_{a,b}\circ f)(x)\ (x\in A)$，すなわち，$f\circ\varphi_{a,b} = \varphi_{a,b}\circ f$ と同値である．よって，Φ から $\mathrm{Z}_{A\otimes A^\circ}(A\otimes B^\circ)\simeq \mathrm{End}_{A\otimes B^\circ}(A)$ を得る．ここで命題 2.4 より，$\mathrm{Z}_{A\otimes A^\circ}(A\otimes B^\circ)\simeq \mathrm{Z}_A(A)\otimes \mathrm{Z}_{A^\circ}(B^\circ)\simeq k\otimes \mathrm{Z}_{A^\circ}(B^\circ)\simeq \mathrm{Z}_A(B)$ より，$\mathrm{End}_{A\otimes B^\circ}(A)\simeq \mathrm{Z}_A(B)$ である． □

補題 2.14 A を k 上の多元環，M を左 A 加群とする．このとき，$\mathrm{End}_A(\bigoplus_{i=1}^n M)\simeq \mathrm{M}_n(\mathrm{End}_A(M))$ である．

証明 $\bigoplus_{i=1}^n M$ から M への自然な射影 $\pi_i : \bigoplus_{i=1}^n M\to M,\ \pi_i(r_1,\dots,r_n) = r_i$ と，M から $\bigoplus_{i=1}^n M$ への自然な埋め込み $\iota_j : M\to \bigoplus_{i=1}^n M,\ r\mapsto (0,\dots,0,\overset{j}{r},0,\cdots,0)$ とする．ここで，

$$\pi_i\circ\iota_j = \begin{cases} \mathrm{id}_M & (i=j) \\ 0 & (i\neq j) \end{cases}$$

に注意する．2 つの A 加群としての準同型写像 $\alpha,\ \beta$ を

$$\alpha : \mathrm{End}_A(\bigoplus_{i=1}^n M)\to \mathrm{M}_n(\mathrm{End}_A(M)),\ \alpha(\varphi) = (\pi_i\circ\varphi\circ\iota_j)_{1\le i,j\le n}$$

$$\beta : \mathrm{M}_n(\mathrm{End}_A(M))\to \mathrm{End}_A(\bigoplus_{i=1}^n M),\ \beta((\varphi_{i,j})_{1\le i,j\le n}) = \sum_{i=1}^n\sum_{j=1}^n \iota_i\circ\varphi_{i,j}\circ\pi_j$$

とすると，$\alpha,\ \beta$ は互いに逆写像になるから $\mathrm{End}_A(\bigoplus_{i=1}^n M)\simeq \mathrm{M}_n(\mathrm{End}_A(M))$ である． □

補題 2.15 A を k 上の単純多元環，M を有限生成左 A 加群とする．このとき，$[M : k]^2 = [A : k][\mathrm{End}_A(M) : k]$ である．

証明 L を A の極小左イデアルとする．Wedderburn の構造定理 (定理 2.1) とその証明から，$A \simeq \mathrm{M}_n(D)$ ($D \simeq \mathrm{End}_A(L)$)，$L \simeq D^n$ であり，補題 2.10 から自然数 $r \in \mathbb{N}$ が存在して，$M \simeq L^r$ であることに注意する．

補題 2.14 より，$\mathrm{End}_A(M) \simeq \mathrm{End}_A(L^r) \simeq \mathrm{M}_r(\mathrm{End}_A(L)) \simeq \mathrm{M}_r(D)$ を得る．これより，$[A : k][\mathrm{End}_A(M) : k] = [\mathrm{M}_n(D) : k][\mathrm{M}_r(D) : k] = r^2n^2[D : k]^2$ である．

一方，$[M : k] = [L^r : k] = r[L : k] = r[D^n : k] = rn[D : k]$ であることから $[M : k]^2 = [A : k][\mathrm{End}_A(M) : k]$ が得られる． □

補題 2.16 A, B を k 上の単純多元環とし，$A \simeq \mathrm{M}_n(D_A), A \simeq \mathrm{M}_m(D_B)$ (D_A, D_B は k 上の斜体) とする．このとき，以下は同値である．

(1) $D_A \simeq D_B$

(2) $A \otimes \mathrm{M}_s(k) \simeq B \otimes \mathrm{M}_t(k)$ となる自然数 $s, t \in \mathbb{N}$ が存在する．

証明 (1) $\Rightarrow$ (2) まず, $A \otimes \mathrm{M}_m(k) \simeq \mathrm{M}_n(D_A) \otimes \mathrm{M}_n(k) \simeq \mathrm{M}_{nm}(D_A \otimes k) \simeq \mathrm{M}_{nm}(k) \otimes D_A$ である．また，仮定より $D_A \sim D_B$ であることに注意すると，同様の計算により $B \otimes \mathrm{M}_n(k) \simeq \mathrm{M}_{nm}(k) \otimes D_B \simeq \mathrm{M}_{nm}(k) \otimes D_A$ である．よって，$A \otimes \mathrm{M}_m(k) \simeq B \otimes \mathrm{M}_n(k)$ より，命題の s, t はそれぞれ m, n としてとればよい．

(2) $\Rightarrow$ (1) $A \otimes \mathrm{M}_s(k) \simeq B \otimes \mathrm{M}_t(k)$ より，$\mathrm{M}_{ns}(D_A) \simeq \mathrm{M}_{mt}(D_B)$ である．すると，Wedderburn の構造定理 (定理 2.1) より $D_A \simeq D_B$ であるから，$A \sim B$ である． □

次の定理が，本題の中心化定理である．

定理 2.17 (中心化定理) A を k 上の中心的単純環，B を A の単純な部分多元環とする．このとき，以下が成り立つ．

(1) $\mathrm{Z}_A(B)$ は単純な部分多元環である．

(2) $[A : k] = [B : k][\mathrm{Z}_A(B) : k]$.

(3) $m = [B : k]$ とすると，$\mathrm{Z}_A(B) \otimes \mathrm{M}_m(k) \simeq A \otimes B^\circ$.

(4) $\mathrm{Z}(\mathrm{Z}_A(B)) = \mathrm{Z}(B)$.

(5) $\mathrm{Z}_A(\mathrm{Z}_A(B)) = B$.

証明の前に，この定理から何がわかるかについて述べておこう．まず，(1) から $\mathrm{Z}_A(B)$ が単純多元環であることがわかる．また，(2) により A の部分多元環 $\mathrm{Z}_A(B)$ の k 上の次数が A と B の次数からわかり，(4) により $\mathrm{Z}_A(B)$ の中心がわかる．特に，B が k 上中心的であれば，(1) と合わせることにより $\mathrm{Z}_A(B)$ も中心的単純環になることがわかる．

証明 $A \otimes B^\circ$ は k 上の単純多元環より，Wedderburn の構造定理（定理 2.1) から，ある自然数 $n \in \mathbb{N}$ と k 上の中心的斜体 D があって $A \otimes B^\circ \simeq \mathrm{M}_n(D)$ である．

(1) 補題 2.13 と補題 2.14 より，$\mathrm{Z}_A(B) \simeq \mathrm{End}_{A\otimes B^\circ}(A) \simeq \mathrm{M}_r(D)$ は単純多元環である．

(2) 補題 2.15 と (1) から，$[A:k]^2 = [A \otimes B^\circ : k][\mathrm{End}_{A\otimes B^\circ}(A) : k] = [A \otimes k][B \otimes k][\mathrm{Z}_A(B) : k]$ より，$[A : k] = [B : k][\mathrm{Z}_A(B) : k]$ である．

(3) $A \otimes B^\circ \simeq \mathrm{M}_n(D)$ で，(1) から $\mathrm{Z}_A(B) \simeq \mathrm{M}_r(D)$ であり，$n \geq r$ に注意すると，補題 2.16 より，$A \otimes B^\circ \simeq \mathrm{Z}_A(B) \otimes \mathrm{M}_m(k)$ $(m \in \mathbb{N})$ とおける．$[A \otimes B^\circ : k] = [A : k][B : k] = [B : k]^2[\mathrm{Z}_A(B) : k]$，$[\mathrm{Z}_A(B) \otimes \mathrm{M}_m(k) : k] = [\mathrm{Z}_A(B) : k]m^2$ であるから，$m = [B : k]$ を得る．

(4) $\mathrm{Z}(B) \subset \mathrm{Z}(\mathrm{Z}_A(B))$ はよい．命題 2.2 より，(3) の両辺の中心をとることで，$\mathrm{Z}(A \otimes B^\circ) \simeq \mathrm{Z}(A) \otimes \mathrm{Z}(B^\circ) \simeq \mathrm{Z}(B), \mathrm{Z}(\mathrm{Z}_A(B) \otimes \mathrm{M}_m(k)) = \mathrm{Z}(\mathrm{Z}_A(B)) \otimes \mathrm{Z}(\mathrm{M}_m(k)) \simeq \mathrm{Z}(\mathrm{Z}_A(B))$ であるから，$\mathrm{Z}(B) \subset \mathrm{Z}(\mathrm{Z}_A(B))$ と合わせて $\mathrm{Z}(B) = \mathrm{Z}(\mathrm{Z}_A(B))$ である．

(5) $B \subset \mathrm{Z}_A(\mathrm{Z}_A(B))$ はよい．(2) より，$[A : k] = [B : k][\mathrm{Z}_A(B) : k]$ であり，(1) で $\mathrm{Z}_A(B)$ は A の k 上の単純な部分多元環であるから，とくに $B = \mathrm{Z}_A(B)$ とすることで，$[A : k] = [\mathrm{Z}_A(B) : k][\mathrm{Z}_A(\mathrm{Z}_A(B)) : k]$ である．よって， $[B : k] = [\mathrm{Z}_A(\mathrm{Z}_A(B)) : k]$ であるから，$B \subset \mathrm{Z}_A(\mathrm{Z}_A(B))$ と合わせて $B = \mathrm{Z}_A(\mathrm{Z}_A(B))$ である． □

2.2　ブラウアー群と分解体

本節では，体 k に対する重要な不変量であるブラウアー群の定義を行う．その後，中心的単純環の研究において重要な役割を果たす分解体を定義すう．その後に，分解体の重要な性質である k 上の中心的単純環は，必ずある有限次のガロア拡大で分解するという事実を示す．その後，被約特性多項式の定義を行い，被約トレース，被約ノルムを導入し，最後にブラウアー群の実例を紹介する．この節は，[斉藤], [渡部], [Cla], [GS06], [FD93], [Dra83], [Pie82], [Ser79] 等を参考にした．

2.2.1　ブラウアー群 $\mathrm{Br}(k)$

まず，単純多元環に対してブラウアー同値を定義しよう．

定義　A, B を k 上の単純多元環とすると，Wedderburn の構造定理 (定理 2.1) より，

$$A \simeq \mathrm{M}_n(D_A),\ B \simeq \mathrm{M}_m(D_B)\ (n,\ m \in \mathbb{N},\ D_A,\ D_B \text{ は } k \text{ 上の斜体})$$

となる．このとき，2 つの k 上の単純多元環に，同値関係 $A \sim B$ を $D_A \simeq D_B$ によって定める．2 つの k 上の単純多元環が，この関係において同値であるとき**ブラウアー同値** (Brauer equivalent) であるという．

また，k 上の中心的単純環全体の集合をこの同値関係で類別した集合

$$\mathrm{Br}(k) = \{k \text{ 上の中心的単純環全体 }\}/\sim$$

と定め，各類を**ブラウアー同値類** (Brauer equivalent class) という．

定義から，ブラウアー同値類の代表元として，体 k 上の中心的斜体をとることができる．このことから，ブラウアー同値類は，k 上の中心的斜体がどのくらいあるかを表す量であり，k 上の非可換拡大を考える上で重要な不変量である．

ブラウアー同値に関する性質をいくつか挙げておこう．

命題 2.18 A, B を k 上の単純多元環とする．このとき，以下は同値である．

(1) $A \simeq B$ である．

(2) $A \sim B$ かつ $[A : k] = [B : k]$ である．

証明 (1) $\Rightarrow$ (2) Wedderburn の構造定理 (定理 2.1) よりわかる．

(2) $\Rightarrow$ (1) $A \simeq \mathrm{M}_n(D_A)$, $B \simeq \mathrm{M}_m(D_B)$ とする．$A \sim B$ より，$D_A \simeq D_B$ であるから，とくに $[D_A : k] = [D_B : k]$ である．すると，$[A : k] = [B : k]$ より，$n = m$ である．よって，$A \simeq B$ である．$\square$

また，ブラウアー同値の定義は次のように言い換えることもできる．

命題 2.19 A, B を k 上の単純多元環とする．このとき，以下は同値である．

(1) $A \sim B$ である．

(2) $A \otimes \mathrm{M}_s(k) \simeq B \otimes \mathrm{M}_t(k)$ となる自然数 $s, t \in \mathbb{N}$ が存在する．

証明 これは補題 2.16 で証明済みである．$\square$

ここで，体 k のブラウアー同値類に群の構造を定めよう．

$[A], [B] \in \mathrm{Br}(k)$ に対し，$[A] + [B] = [A \otimes B]$ として演算を定める．この演算が well-defined であることは，定理 2.5 と命題 2.19 を用いることでわかる．すると，$\mathrm{Br}(k)$ はこの演算に関し可換群の構造を持つ．このとき，単位元は $[k] = [\mathrm{M}_n(k)]$ であり, $[A]$ の逆元は，命題 2.8 より $[A^\circ]$ である．

定義 k のブラウアー同値類に $\mathrm{Br}(k)$ に上の演算を入れた可換群を，体 k の**ブラウアー群** (Brauer group) という．

2.2.2 分解体

次に，中心的単純環の分解体についてみていく．分解体とは，中心的単純環 A が行列環と同型になるような k 上の拡大体であり，中心的単純環の研究において重要な役割を果たす．命題 2.7 より，体 k の中心的単純環を代数閉包まで係数拡大すれば分解することはわ

かっている．ここでの目標は，k 上の中心的単純環は，ある**有限次のガロア拡大で分解する**という性質を導くことである．

まず，分解体の定義は次のとおりである．

定義 A を k 上の中心的単純環，K/k を体の拡大とする．$A \otimes_k K \simeq \mathrm{M}_n(K)$ となるとき，K は A の**分解体** (splitting field) であるという．また，このとき A は K 上**分解する** (A splits over K) という．

定義より，次のことがわかる．

命題 2.20 A, B を k 上の中心的単純環とし，$A \sim B$ とする．このとき，K が A の分解体であることと，K が B の分解体であることは同値である．

このことから，中心的単純環 A の分解体を調べるには，A とブラウアー同値な斜体 D の分解体を調べればよいことがわかる．

まず，中心的単純環の部分体に関する用語の定義をしておこう．

定義 A を k 上の中心的単純環で，$\deg(A) = n$ とする．このとき，拡大体 K/k で $K \subset A$ であるものを A の**部分体** (subfield) という．A の部分体の中で極大なものを**極大部分体** (maximal subfield) という．A の部分体 K で $[K : k] = n$ となるものを**強極大部分体** (strictly maximal subfield) という．

強極大部分体であれば極大部分体である．そのことは次の命題から従う．

命題 2.21 K を A の部分体とする．このとき，$[K : k] \mid \deg(A)$ である．

証明 $C = \mathrm{Z}_A(K)$ とする．$[C : K] = m^2$ とすると，中心化定理 (定理 2.17) の (2) より，$[A : k] = [K : k][C : k] = [K : k]^2 m^2$ であるから，$\deg(A) = [K : k]m$ である．よって，$[K : k] \mid \deg(A)$ である． $\square$

注意 中心的単純環は，必ず極大部分体はもつが，強極大部分体は必ずしも持つとは限らない．たとえば，$\mathbb{C}$ 上の行列環 $\mathrm{M}_n(\mathbb{C})$ は強極大部分体をもたない．しかし，このあとの

命題 2.23 により，中心的斜体は必ず強極大部分体をもつことがわかる．

中心的単純環とその極大部分体との関係に関して次の事実が成り立つ．

命題 2.22 A を k 上の中心的単純環，K を A の部分体とする．このとき，以下は同値である．

(1) $\mathrm{Z}_A(K) = K$ である．

(2) $\deg A = [K : k]$ である，すなわち K は強極大部分体である．

さらに，上の (1) もしくは (2) が成り立つとき，K は A の分解体である．

証明 中心化定理 (定理 2.17) の (2) より，$[A : k] = [\mathrm{Z}_A(K) : k][K : k]$ であり，$K \subset \mathrm{Z}_A(K)$ に注意すると，$\deg A = [K : k]$ は $[\mathrm{Z}_A(K) : k] = [K : k]$ と同値である．さらにこれは，$\mathrm{Z}_A(K) = K$ と同値であることから (1) と (2) の同値性が従う．

また，(1) (もしくは (2)) が成り立つとき，中心化定理の (3) より，$A \otimes K \simeq \mathrm{Z}_A(K) \otimes \mathrm{M}_m(k) \simeq \mathrm{M}_m(K)$ であるから，K は A の分解体である． □

とくに k 上の斜体の場合，上の命題は次のようになる．

命題 2.23 D を k 上の中心的斜体，K を D の部分体とする．このとき，以下は同値である．

(1) $\mathrm{Z}_D(K) = K$ である．

(2) $\deg D = [K : k]$ である，すなわち K は強極大部分体である．

(3) K は D の分解体である．

(4) K は D の極大部分体である．

とくに，中心的斜体は必ず強極大部分体をもつ．

証明 (1) $\Leftrightarrow$ (2)，(2) $\Rightarrow$ (3) は命題 2.22 よりわかる．

(3) $\Rightarrow$ (2) K を D の分解体とし，$[D : k] = d^2$ とおくと，$D \otimes K \simeq \mathrm{M}_d(K)$ である．V を単純な左 $D \otimes K$ 加群とすると，左 D 加群として $\mathrm{M}_d(K) \simeq \bigoplus_{i=1}^d V$ である．すると，$[K : k] = [K \otimes D : k] = [\mathrm{M}_d(K) : D] = [\bigoplus_{i=1}^d D_A \otimes K : D] = d[V : D]$ であるから，$d \mid [K : k]$ である．一方，中心化定理 (定理 2.17) の (2) から $d^2 = [D : k] =$

$[\mathrm{Z}_D(K):k][K:k]=[\mathrm{Z}_D(K):K][K:k]^2$．よって，$[K:k]^2 \mid d^2$ である．よって，$[K:k]^2=d^2=[D:k]$ である．

(1) $\Rightarrow$ (4) $K\subset M$ とすると，(1) の仮定から $M\subset \mathrm{Z}_D(K)=K$ より，$M=K$ である．

(4) $\Rightarrow$ (1) $K\subset \mathrm{Z}_D(K)$ はよい．一方，任意の $x\in \mathrm{Z}_D(K)$ に対し，K に x を添加した多元環 $K[x]$ は体になることに注意すると，$K\subset K[x]\subset D$ で (4) の仮定より，$K=K[x]$ であるから $x\in K$ である．よって，$\mathrm{Z}_D(L)\subset K$ である． □

さて，ここから目標である k 上の中心的単純環は，必ずある有限次ガロア拡大において分解するという性質を証明しよう．そのために，1 つ補題を示しておく．

補題 2.24 D を k 上の中心的斜体とする．このとき，ある D の部分体 K で K/k が分離的であるものが存在する．

証明 D の元だが k の元ではない元 $\alpha\in D\backslash k$ を任意にとる．k に α を添加した多元環 $k[\alpha]$ は k の代数拡大になる．$\mathrm{char}(k)=0$ なら，任意の拡大は分離的であるから $K=k[\alpha]$ とすればよい．$\mathrm{char}(k)=p(>0)$ とする．このとき，$k[\alpha]/k$ の中間体 L で，$k[\alpha]/L$ が純非分離拡大，L/k が分離拡大となるものが存在する．ここで，$L\supsetneq k$ であれば，$K=L$ とすれば証明が終わる．$L=k$ のとき，$k[\alpha]/k$ が α を k 上の純非分離拡大である．ここで，α を取りかえることで，k 上の純非分離拡大でない真の代数拡大をつくろう．$k[\alpha]/k$ が純非分離拡大より，α^{p^i} となる自然数 $i\in\mathbb{N}$ が存在する．そのような自然数 $i\in\mathbb{N}$ で最小のものをとり，$u=\alpha^{p^{i-1}}$ とおく．すると，i の最小から，$u\in D\backslash k$, $u^p=\alpha^{p^i}\in k$ である．k 上の多元環の自己準同型写像 $\sigma: D\to D,\ x\mapsto uxu^{-1}$ を考えると，u のとり方から $\sigma\neq \mathrm{id}_D$, $\sigma^p=\mathrm{id}_D$ である．ここで，$\tau=\sigma-\mathrm{id}_D$ とおくと，$\tau\neq 0$, $\tau^p=(\sigma-\mathrm{id}_D)^p=0$ である．そこで，$r=\max\{i\in\mathbb{N}\mid \tau^i\neq 0\}$ とおくと，$y\in D$ が存在して．$\tau^r(y)\neq 0$ である．$a=\tau^{r-1}(y)$, $b=\tau^r(y)$ とおけば，r の最大性によって，$\tau(a)=b\neq 0$, $\tau(b)=\tau^{r+1}(y)=0$ である．この τ によって，$\sigma(b^{-1}a)=b^{-1}\sigma(a)=b^{-1}(a+b)=b^{-1}a+1$ であるから，σ は $k[b^{-1}a]/k$ の非自明な k 上の自己同型写像になる．すなわち，$k[b^{-1}a]/k$ は純非分離でない代数拡大である． □

この補題を用いて，ここでの目標である次の定理を示そう．

定理 2.25 A を k 上の中心的単純環とすると，A は k 上のある有限次ガロア拡大体 K で分解する．

証明 命題 2.20 と命題 2.23 により，k 上の斜体 D に対して，k を含むような分離的な D の極大部分体が存在することを示せばよい．$n = [D : k]$ とおき，n に関する帰納法で示そう．$n = 1$ は明らかである．$n > 1$ のとき，補題 2.24 より，k を真に含むような分離的な D の部分体 L が存在することがわかる．$A = \mathrm{Z}_D(L)$ とすると，A は L 上の中心的斜体である．すると，中心化定理 (定理 2.17) の (2) から，$n = [D : k] = [A : k][L : k]$ である．いま，$[L : k] > 1$ より，$[A : L] < [A : k] < n$ が得られる．すると，帰納法の仮定から，L を含むような分離的な A の極大部分体 K が存在する．命題 2.23 より，$[A : L] = [K : L]^2$ である．すると，K は k 上分離的であり，$[D : k] = [A : k][L : k] = [A : K][L : k]^2 = [K : L]^2[L : k]^2 = [K : k]^2$ が得られるから，また命題 2.23 により，K は D の極大部分体である． $\square$

この節の最後に，中心的単純環 A が k の拡大体 K で分解するとき，K を強極大部分体としてもつような中心的単純環が A のブラウアー同値類の中にあることを示しておこう．この定理は，今後の証明中の議論においてしばしば用いられる．

定理 2.26 A を中心的単純環，K は A の分解体であるとする．このとき，次の (i), (ii) をみたす k 上の中心的単純環 B が同型を除いて一意的に存在する．

(i) $B \sim A$ である．

(ii) $K \subset B$ で，$\deg(B) = [K : k]$ である．すなわち，B は K を強極大部分体として含む．

証明 K/k を m 次拡大とする．K は A の分解体であるから，$A^\circ \otimes K \simeq \mathrm{M}_n(K)^\circ \simeq \mathrm{M}_n(K)$ であり，$\mathrm{M}_n(K) \simeq \mathrm{End}_K(K^n) \to \mathrm{End}_k(K) \simeq \mathrm{M}_{mn}(k)$ により，$A^\circ \otimes K$ を $R = \mathrm{M}_{mn}(k)$ の部分多元環とみる．さらに，$A^\circ \to A^\circ \otimes K$, $a \mapsto a \otimes 1$, $K \to A^\circ \otimes K$, $b \mapsto 1 \otimes b$ により，A°, K を自然に $A^\circ \otimes K$ の部分多元環とみる．

$B = \mathrm{Z}_R(A^\circ)$ とする．すると，中心化定理 (定理 2.17) の (1) より B は単純多元環であり，また中心化定理の (4) から $\mathrm{Z}(B) = \mathrm{Z}(A^\circ) = k$ であるから，B は k 上の中心的単

純環である．また，中心化定理の (3) より，$B \otimes \mathrm{M}_{n^2}(k) \simeq R \otimes A = \mathrm{M}_{mn}(k) \otimes A$ であるから，命題 2.19 より $A \sim B$ である．また，$L \subset B$ であり，中心化定理の (2) から $[R : k] = [A^\circ : k][B : k]$ より $(nm)^2 = n^2[B : k]$ であるから，$[B : k] = m^2 = [K : k]^2$ である．これより，この B が定理の条件をみたすものであるから，存在性は示された．

一意性は，もし定理の仮定をみたす k 上の中心的単純環 B, B' があったとすると，$B \sim A \sim B'$, $[B : k] = [K : k]^2 = [B' : k]$ であるから，命題 2.18 より $B \simeq B'$ であることが得られる． $\square$

2.2.3　被約特性多項式

この節では，中心的単純環の元に対して被約特性多項式と呼ばれる多項式を定義し，それを用いて被約トレース，被約ノルムの定義を行い，それらの基本的な性質をみる．その後に，一般の多元環に対して元のトレースやノルムを復習し，それと被約トレース，被約ノルムとの関係をみる．

定義　A を次数 n の中心的単純環とし，体の拡大 K を A の分解体とする．$A \otimes K$ から行列環 $\mathrm{M}_n(K)$ への k 上の多元環としての同型写像を $f : A \otimes K \to \mathrm{M}_n(K)$ とする．このとき，$a \in A$ に対し，$f(a \otimes 1)$ の特性多項式を $\mathrm{Prd}(a, x) = \det(xE_n - f(a \otimes 1))$ と表し，a の**被約特性多項式** (reduced characteristic polynomial) という．

しかし，この定義では分解体のとり方や，分解体まであげたときの行列環との同型写像のとり方に依存しているようにみえる．以下，そのとり方に依存しないことを示そう．

命題 2.27　A を k 上の中心的単純環とし, K を A の分解体とし, $f, g : A \otimes K \to \mathrm{M}_n(K)$ を K 上の多元環としての同型写像とする．このとき, $a \in A$ に対し, $\det(xE_n - f(a \otimes 1)) = \det(xE_n - g(a \otimes 1))$ である．

証明　Skolem–Noether の定理 (定理 2.11) より，$a \in A$ に対し，$g(a \otimes 1) = tf(a \otimes 1)t^{-1}$ となる $t \in \mathrm{GL}_n(K)$ $(n = \deg(A))$ が存在する．よって，$g(a \otimes 1)$ と $f(a \otimes 1)$ は $\mathrm{M}_n(K)$ で相似な行列だから，その特性多項式は一致する． $\square$

命題 2.28 A を k 上の中心的単純環とし，K, L を A の分解体とし，$f : A\otimes K \to \mathrm{M}_n(K)$ を K 上の多元環としての同型写像，$g : A \otimes L \to \mathrm{M}_n(L)$ を L 上の多元環としての同型写像とする．このとき，$a \in A$ に対し，$\det(xE_n - f(a \otimes 1)) = \det(xE_n - g(a \otimes 1))$ である．

証明 $k \subset K \subset L$ としてよい．$h : A \otimes L \xrightarrow{\sim} (A \otimes_k K) \otimes_K L \xrightarrow[f\otimes \mathrm{id}_L]{\sim} \mathrm{M}_n(K) \otimes_K L \xrightarrow{\sim} \mathrm{M}_n(L)$ とする．ここで, 1 つ目の同型写像は $A\otimes L \to (A\otimes_k K)\otimes_K L$, $a\otimes x \mapsto (a\otimes 1)\otimes x$ で与えられ，3 つ目の同型写像は $\mathrm{M}_n(K) \otimes_K L \to \mathrm{M}_n(L)$, $(\lambda_{i,j}) \otimes \alpha \mapsto (\alpha\lambda_{ij})$ で与えられるものである．このとき，$h(a \otimes 1) = f(a \otimes 1)$ であるから，任意の $a \in A$ に対し $h(a \otimes 1)$ と $f(a \otimes 1)$ の特性多項式は一致する．ここで，命題 2.27 より，分解体まであげたときの行列環との同型写像のとり方には依存しないから，$h(a \otimes 1)$ と $g(a \otimes 1)$ の特性多項式も等しく，よって，$f(a \otimes 1)$ と $g(a \otimes 1)$ の特性多項式は一致する． □

よって，命題 2.27 より，分解体まであげたときの行列環との同型写像のとり方に依存しないことがわかり，2.28 より，被約特性多項式は分解体のとり方に依らないことがわかった．さらに，次のことがわかる．

命題 2.29 A を k 上の中心的単純環とする．このとき，$\mathrm{Prd}(a, x) \in k[x]$ である．

証明 定理 2.25 より，A の分解体 K/k を有限次ガロア拡大であるようにとれる．$G = \mathrm{Gal}(K/k)$ とする．任意の $\sigma \in G$ をとる．このとき，${}^{\sigma}f : A \otimes K \to \mathrm{M}_n(K)$, $x \mapsto \sigma f \sigma^{-1}(x)$ とすると，これは K 上の多元環としての同型写像になる．すると，命題 2.27 より，分解体まであげたときの行列環との同型写像のとり方には依存しないから，任意の $a \in A$ に対し，$\mathrm{Prd}(a, x) = \det(xE_n - f(a \otimes 1)) = \det(xE_n - {}^{\sigma}f(a \otimes 1)) = \det(xE_n - \sigma f(\sigma^{-1}(a \otimes 1))) = \det(xE_n - \sigma f(a \otimes 1)) = \sigma(\det(xE_n - f(a \otimes 1))) = \sigma(\mathrm{Prd}(a, x))$ が成り立つ．よって，任意の $\sigma \in G$ で $\mathrm{Prd}(a, x)$ の係数は変わらないから，$\mathrm{Prd}(a, x) \in k[x]$ である． □

この命題から，被約特性多項式は k 上定義される多項式であることもわかった．

次に，いくつか被約特性多項式に関する基本的な性質をみていこう．中心的単純環の被

約特性多項式は，行列環の特性多項式の一般化になっている．このことを述べているのが次の命題である．

命題 2.30 $A = \mathrm{M}_n(k)$ とする．このとき，$a \in A$ の特性多項式と，被約特性多項式は一致する．

証明 $f : A \to \mathrm{M}_n(k)$ として恒等写像をとれば，$\mathrm{Prd}(a, x) = \det(xE_n - f(a)) = \det(xE_n - a)$ となり，$a \in \mathrm{M}_n(k) = A$ の特性多項式と一致する． □

また，行列環での Cayley–Hamilton の定理の一般化も次のように成り立つ．

命題 2.31 A を k 上の中心的単純環とし，$a \in A$ とする．このとき，$\mathrm{Prd}(a, a) = 0$ である．

証明 K を A の分解体とし，K 上の多元環としての同型写像 $f : A \otimes K \to \mathrm{M}_n(K)$ を 1 つとっておく．このとき，$\mathrm{Prd}(a, x) = x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0 \in k[x]$ は $f(a \otimes 1)$ の $\mathrm{M}_n(K)$ における特性多項式であるから，行列環での Cayley–Hamilton の定理より，$f((a^n + \alpha_{n-1}a^{n-1} + \cdots + \alpha_1 a + \alpha_0) \otimes 1) = f(a \otimes 1)^n + \alpha_{n-1} f(a \otimes 1)^{n-1} + \cdots + \alpha_1 f(a \times 1) + \alpha_0 = 0$ が得られる．$\mathrm{Prd}(a, a) = a^n + \alpha_{n-1}a^{n-1} + \cdots + \alpha_1 a + \alpha_0$ であり，f がとくに単射であることから $\mathrm{Prd}(a, a) \otimes 1 = 0$ が得られる．よって，$\mathrm{Prd}(a, a) = 0$ である． □

次に，被約特性多項式から，被約トレース，被約ノルムの定義を行う．

定義 A を k 上の中心的単純環とし，$a \in A$ とする．このときの被約特性多項式を $\mathrm{Prd}(a, x) = x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0 \in k[x]$ とする．このとき，$\mathrm{Trd}(a) = -\alpha_{n-1} \in k$ を a の**被約トレース** (reduced trace)，$\mathrm{Nrd}(a) = (-1)^n \alpha_0 \in k$ を a の **被約ノルム** (reduced norm) という．ここで，K を A の分解体とし，K 上の多元環としての同型写像 $f : A \otimes K \to \mathrm{M}_n(K)$ を 1 つとったとき，$\mathrm{Trd}(a) = \mathrm{Tr}(f(a \otimes 1))$，$\mathrm{Nrd}(a) = \det(f(a \otimes 1))$ であることに注意する．

被約ノルム，被約トレースは次の基本的な性質を満たす．

命題 2.32 A を k 上の中心的単純環とする．このとき，以下が成り立つ．

(1) $\mathrm{Trd}: A \to k$ は k 上の線形写像である．

(2) $\mathrm{Nrd}: A \to k$ は乗法的である，すなわち $\mathrm{Nrd}(ab) = \mathrm{Nrd}(a)\mathrm{Nrd}(b)$ $(a,\, b \in A)$ である．

(3) $a \in k$ に対して，$\mathrm{Trd}(a) = na$, $\mathrm{Nrd}(a) = a^n$ である．

(4) $\mathrm{Nrd}(a) \neq 0$ であることと，$a \in A^\times$ であることは同値である．とくに，$\mathrm{Nrd}: A^\times \to k^\times$ は群の準同型写像である．

(5) $a,\, b \in A$ に対し，$\mathrm{Trd}(ab) = \mathrm{Trd}(ba)$ が成り立つ．

証明 K を A の分解体とし，K 上の多元環としての同型写像 $f: A \otimes K \to \mathrm{M}_n(K)$ $(n = \deg(A))$ を 1 つとっておく．

(1), (2) は定義からわかる．

(3) $a \in k$ のとき，$\mathrm{Nrd}(a) = \det(f(a \otimes 1)) = \det(af(1 \otimes 1)) = \det(aE_n) = a^n$, $\mathrm{Trd}(a) = \mathrm{Tr}(f(a \otimes 1)) = \mathrm{Tr}(aE_n) = na$ より得られる．

(4) もし，$a \in A^\times$ なら，$ab = 1$ となる $b \in A^\times$ が存在するから，両辺で被約ノルムをとり，(2) の乗法性と，(3) より $\mathrm{Nrd}(1) = 1$ であることから，$\mathrm{Nrd}(a)\mathrm{Nrd}(b) = 1$ となり $\mathrm{Nrd}(a) \neq 0$ が得られる．

逆に，$\mathrm{Nrd}(a) \neq 0$ であれば，a の被約特性多項式 $\mathrm{Prd}(a, x) = x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0$ において $\alpha_0 = (-1)^n\mathrm{Nrd}(a) \neq 0$ である．ここで，命題 2.31 より，$\mathrm{Prd}(a, a) = a^n + \alpha_{n-1}a^{n-1} + \cdots + \alpha_1 a + \alpha_0 = 0$ であるから，

$$a\left(\frac{-1}{\alpha_0}\right)(a^{n-1} + \alpha_{n-1}a^{n-2} + \cdots + \alpha_1) = 1$$

あるから $a \in A^\times$ である．

(5) 一般に行列 $M,\, N \in M_n(K)$ に対し，$\mathrm{Tr}(MN) = \mathrm{Tr}(NM)$ であることから，a, $b \in A$ に対し，$\mathrm{Trd}(ab) = \mathrm{Tr}(f(ab \otimes 1)) = \mathrm{Tr}(f(a \otimes 1)f(b \otimes 1)) = \mathrm{Tr}(f(b \otimes 1)f(a \otimes 1)) = \mathrm{Tr}(f(ba \otimes 1)) = \mathrm{Trd}(ba)$ より得られる． □

このことから，とくに次のことがわかる．

系 2.33 A を k 上の中心的単純環とする．このとき，以下は同値である．

(1) A は k 上の中心的斜体である．

(2) 任意の $a \in A \setminus \{0\}$ に対し，$\mathrm{Nrd}(a) \neq 0$ である．

ここで，通常の k 上の多元環のトレース，ノルムと被約トレース，被約ノルムの関係についてみておこう．まず，k 上の多元環 A のトレース，ノルムがどのように定義されていたかを復習しておこう．k 上の多元環としての準同型写像 $\phi : A \to \mathrm{M}_n(k),\ a \mapsto L_a$ $(n = [A : k])$ とする．ここで，L_a は $A \to A,\ x \mapsto ax$ の表現行列である．このとき，行列 $\phi(a)$ のトレース，ノルムによって a のトレース $\mathrm{Tr}(a)$，ノルム $\mathrm{N}(a)$ が定義されていた．このとき，次の事実が成り立つ．これが Trd や Nrd が「被約」と呼ばれる由縁である．

命題 2.34 A を次数 n の k 上の中心的単純環とする．このとき，$a \in A$ に対し，$\mathrm{N}(a) = \mathrm{Nrd}(a)^n,\ \mathrm{Tr}(a) = n\mathrm{Trd}(a)$ が成り立つ．

証明 K を A の分解体とし，K 上の多元環としての同型写像 $f : A \otimes K \to \mathrm{M}_n(K)$ を 1 つとっておく．$\deg(A) = n$ より，$[A : k] = n^2$ に注意すると，上の k 上の多元環としての準同型写像は $\phi : A \to \mathrm{M}_{n^2}(K),\ a \mapsto L_a$ となる．ここで，$L_a : A \to A,\ x \mapsto ax$ $(a \in A)$ の表現行列である．ここで，k 上の多元環としての準同型写像を $g : A \otimes K \to \mathrm{M}_{n^2}(K),\ a \otimes \alpha \mapsto \alpha\phi(a)$ と定義する．

また，K 上の多元環としての準同型写像 $h : A \otimes K \to \mathrm{M}_{n^2}(K),\ s \mapsto \mathrm{diag}\underbrace{(f(s), \ldots, f(s))}_{n\text{ 個}}$ を考える．ここで，

$$\mathrm{diag}(f(s), \ldots, f(s)) = \begin{pmatrix} f(s) & 0 & 0 & \ldots & 0 \\ 0 & f(s) & 0 & \ldots & 0 \\ 0 & 0 & f(s) & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & f(s) \end{pmatrix} \in \mathrm{M}_{n^2}(K)$$

である．すると，Skolem–Noether の定理 (定理 2.11) より，任意の $t \in A \otimes K$ に対して $g(t) = uh(t)u^{-1}$ となる $u \in \mathrm{GL}_{n^2}(K)$ が存在する．よって，$a \in A$ に対し，$g(a \otimes 1)$ と

$h(a\otimes 1)$ は $\mathrm{M}_{n^2}(K)$ の行列として相似である．よって，特性多項式は一致する．

よって，$\phi(a)$ の特性多項式を $p(x)$ とおくと，$p(x)=\det(xE_{n^2}-\phi(a))=\det(xE_{n^2}-g(a\otimes 1))=\det(xE_{n^2}-h(a\otimes 1))=\det(xE_n-f(a\otimes 1))^n=\mathrm{Prd}(a,x)^n$ となる．これより，$\mathrm{N}(a)=\mathrm{Nrd}(a)^n$, $\mathrm{Tr}(a)=n\mathrm{Trd}(a)$ を得る． □

2.2.4 ブラウアー群の実例

ブラウアー群は，体 k に対する重要な不変量である．本節では，ブラウアー群の例をいくつかみていく．

まず，代数閉体上のブラウアー群はどうなるかをみてみよう．

命題 2.35 k を代数閉体とすると，$\mathrm{Br}(k)=\{0\}$ である．

証明 命題 1.4 より，代数閉体 k 上の斜体は k 自身だけであるから，k のブラウアー群は $\mathrm{Br}(k)=\{0\}$ である． □

次に，実数体 $\mathbb{R}$ のブラウアー群をみてみよう．

命題 2.36 $\mathbb{R}$ 上の中心的斜体は $\mathbb{R}$ または $\mathbb{H}$ と同型である．このことから，$\mathrm{Br}(\mathbb{R})\simeq\mathbb{Z}/2\mathbb{Z}$ である．

証明 D を $\mathbb{R}$ 上の中心的斜体とし，$\deg(D)>1$ とする．L を D の極大部分体とすると，$[L:\mathbb{R}]=2$ となり，$[D:\mathbb{R}]=4$ である．ここで，$L=\mathbb{C}$ としてよい．複素共役写像を $\tau:\mathbb{C}\to\mathbb{C},\ z\mapsto\overline{z}$ とすると，Skolem–Noether の定理 (定理 2.11) より，任意の $z\in\mathbb{C}$ に対し $\tau(z)=uzu^{-1}$ となるような $u\in D$ が存在する．$\tau^2=\mathrm{id}_{\mathbb{C}}$ より，任意の $z\in\mathbb{C}$ に対し $z=u^2zu^{-2}$ となる．これと命題 2.23 より，$u^2\in\mathrm{Z}_D(\mathbb{C})=\mathbb{C}$ であり，$\tau(u^2)=uu^2u^{-1}=u^2$ より，$u^2\in\mathbb{R}$ である．ここで，$u^2>0$ と仮定すると，$u^2=t^2$ となる $t\in\mathbb{R}$ が存在し，これより $u=\pm t\in\mathbb{R}$ となる．すると，τ は恒等写像となってしまうため矛盾する．よって，$u^2<0$ である．すると，$u^2=-t^2$ となる $t\in\mathbb{R}$ が存在する．そこで，$i=\sqrt{-1}$, $j=ut^{-1}$ とすると，$i^2=j^2=-1$, $ij=-ji$ である．ここで，$j=ut^{-1}\in\mathbb{C}$ だと，$u\in\mathbb{C}$ となり τ が恒等写像となり矛盾するため，$j\notin\mathbb{C}$ であること

に注意する．$[D:\mathbb{R}]=4$ であったから，上のことから $D\simeq\mathbb{H}$ が得られる． $\square$

次に，有限体 $\mathbb{F}_q$ のブラウアー群をみてみよう．そのために，群論的な補題を 1 つ示しておく．

補題 2.37 G を有限群とし，H を真の部分群とする．このとき，

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

である．

証明 G の H による正規化群を $\mathrm{N}(H)=\{g\in G \mid gHg^{-1}=H\}$ とする．すると，G の部分群で H と共役なものは $[G:\mathrm{N}(H)]$ 個である．すると，仮定から $|\cup_{g\in G}\, gHg^{-1}| \leq [G:\mathrm{N}(G)](|H|-1) \leq [G:H](|H|-1) = |G|-[G:H] < |G|-1$ であるから，$\cup_{g\in G} gHg^{-1} \subsetneq G$ である． $\square$

次の定理は Wedderburn の小定理としても知られる体論で有名な定理である．そこから，有限体のブラウアー群が自明群であることが従う．

命題 2.38 (Wedderburn の小定理) 有限体 $\mathbb{F}_q$ 上の斜体は $\mathbb{F}_q$ だけである．このことから，$\mathrm{Br}(\mathbb{F}_q)=\{0\}$ である．

証明 D を $\mathbb{F}_q$ 上の斜体とする．このとき，D の位数は有限であり，$K=\mathbb{Z}(D)$ は有限体であるから，$|K|=q'$ とおく．ここで，$\deg(D)>1$ と仮定する．D の 2 つの極大部分体を L_1, L_2 とすれば，命題 2.23 より $[L_1:K]=[L_2:K]=d$ より $|L_1|=|L_2|=q'^2$ である．位数が同じ有限体は同型であるから，$L_1\simeq L_2$ である．Skolem–Noether の定理 (定理 2.11) により，L_1 と L_2 は D において共役である．D の任意の元は，ある極大部分体に含まれることから，$D^\times=\cup_{d\in D^\times} dL_1^\times d^{-1}$ となり，補題 2.37 に反する．よって，$\deg(D)=1$ であるから，$D=\mathbb{F}_q$ である． $\square$

次に，C_1 体上のブラウアー群がどのようになるかみてみよう．まず，一般の負でない整数 $i\geq 0$ に対して C_i 体の定義を与える．

定義　体 k が C_i 体 (C_i-field) であるとは，自然数 $1 \leq n < m$ に対して，次数 n^i の m 変数斉次多項式 $f(x_1, \ldots, x_m) \in k[x_1, \ldots, x_m]$ が k 上で非自明な零点をもつときをいう．

C_i 体の例と基本的な性質を結果のみ紹介する．詳細は [Pie82, 19.2], [GS06, 6.2], [Ser79, Chapter X §7] などを参照せよ．

例 2.39 (C_i 体) (i) C_0 体は代数閉体である．

(ii) 有限体は C_1 体である (Chevalley の定理)．

(iii) k を代数閉体としたとき，k 上の超越次数 1 の拡大体は C_1 体である．(Tsen の定理)

命題 2.40　k を C_1 体とすると，k の任意の代数拡大体も C_1 体である．

C_1 体上のブラウアー群は次のようになる．

命題 2.41 k を C_1 体とすると，$\mathrm{Br}(k) = \{0\}$ である．

証明　D を k 上の中心的斜体，$\deg(D) = n$ とする．$\{v_1, \ldots, v_{n^2}\}$ を D の k 上の線形空間としての基底とし，$f(x_1, \ldots, x_{n^2}) = \mathrm{Nrd}(x_1 v_1 + \cdots + x_{n^2} v_{n^2}) \in k[x_1, \ldots, x_{n^2}]$ とする．すると，$f(x_1, \ldots, x_{n^2})$ は次数 n の n^2 変数斉次多項式となるから，$n > 1$ なら C_1 体の定義から $f(x_1, \ldots, x_{n^2})$ は k 上で非自明な零点をもつ．しかし，これは系 2.33 より D が斜体であることに矛盾する．よって，$n = 1$ であるから，$\mathrm{Br}(k) = \{0\}$ である．　□

最後に，p 進数体 $\mathbb{Q}_p$ と有理数体 $\mathbb{Q}$ 上のブラウアー群がどうなっているのかを紹介する．詳細は [Pie82, 17.10, 18.5] や [Ser79, Chapter XIII] を参照せよ．

まず，p 進数体 $\mathbb{Q}_p$ のブラウアー群は次のようになる．

命題 2.42　$\mathrm{Br}(\mathbb{Q}_p) \simeq \mathbb{Q}/\mathbb{Z}$ である．

次に，$\mathbb{Q}$ のブラウアー群をみてみよう．$\mathbb{Q}$ 上のブラウアー群に対し，完全系列

$$0 \to \mathrm{Br}(\mathbb{Q}) \xrightarrow{j} \bigoplus_i \mathrm{Br}(\mathbb{Q}_i) \xrightarrow{f} \mathbb{Q}/\mathbb{Z} \to 0$$

が存在する．ここで，$\mathbb{Q}_i$ は $\mathbb{Q}$ の完備化全てをわたり，j は標準的な埋め込み，$\mathrm{Br}(\mathbb{R})$ は $(1/2)\mathbb{Z}/\mathbb{Z}$ と同一視し，各素数 p に対し $\mathbb{Q}_p$ は $\mathbb{Q}/\mathbb{Z}$ と同一視することで，f は $f(\{x_i\}) = \sum_i x_i$ で定まる写像である．この完全系列から，$\mathbb{Q}$ のブラウアー群は次のようになる．

命題 2.43

$$\mathrm{Br}(\mathbb{Q}) \simeq \left\{ (a, x_p) \in (1/2)\mathbb{Z}/\mathbb{Z} \oplus \bigoplus_p \mathbb{Q}/\mathbb{Z} \;\middle|\; a \in (1/2)\mathbb{Z}/\mathbb{Z},\ x_p \in \mathbb{Q}/\mathbb{Z},\ a + \sum_p x_p = 0 \right\}$$

である．ここで，右辺の和は成分ごとの和である，

2.3 巡回多元環と接合積

本節では，中心的単純環の特別な例として巡回多元環，接合積の理論を紹介する．巡回多元環の特別な場合である四元数環に関しては深い理論があるが，それに関しては 3.1 節で解説することにする．この節は，[斉藤], [渡部], [FD93] を参考にした．

2.3.1 巡回多元環 $(K/k, \sigma, b)$

K/k を n 次巡回拡大とし，$G = \mathrm{Gal}(K/k) = \langle \sigma \rangle$，$b \in k^\times$ とする．このとき，K 上のベクトル空間

$$A = \sum_{i=0}^{n-1} K \cdot v^i \ (\{1, v, \ldots, v^{n-1}\} \text{ は } A \text{ の } K \text{ 上の基底})$$

に対し，積を $v \cdot \alpha = \sigma(\alpha) \cdot v \ (\alpha \in K)$, $v^n = b$ で定める．すると，A は k 上の多元環の構造をもち，さらに k 上の中心的単純環になる．これを**巡回多元環** (cyclic algebra) といい，$A = (K/k, \sigma, b)$ とかく．定義より，次元は $[A : k] = [K : k]^2 = n^2$ であるから，命題 2.22 より，とくに K は A の分解体となる．

例 2.44 (四元数環は巡回多元環) a, $b \in k^\times$ に対し，四元数環 $\left(\frac{a,b}{k}\right)$ は，$K = k(\sqrt{a})$, $\mathrm{Gal}(K/k) = \langle \sigma \rangle$ とすると，$\left(\frac{a,b}{k}\right) = (K/k, \sigma, b)$ である．

巡回多元環は次のように，極大部分体の言葉で特徴づけることができる．

命題 2.45 A を k 上中心的単純環とすると，以下は同値である．

(1) A が巡回多元環である．

(2) A が強極大部分体 K で K/k が巡回拡大であるものが存在する．

証明 (1) $\Rightarrow$ (2) は定義より従う．

(2) $\Rightarrow$ (1) $\mathrm{Gal}(K/k) = \langle\sigma\rangle$ とする．Skolem–Noether の定理 (定理 2.11) より，任意の $\alpha \in K$ に対して $\sigma(\alpha) = u\alpha u^{-1}$ となる $u \in A^\times$ が存在する． すると，任意の $\alpha \in K$ に対し，$u^n \alpha u^{-n} = \sigma^n(\alpha) = \alpha$ より，命題 2.22 に注意すると，$u^n \in \mathrm{Z}_A(K) = K$ となる．さらに，$\sigma(u^n) = u^n$ より，$u^n \in k$ である．ここで，$b = u^n$ とすると，k 上の多元環としての準同型写像 $(K/k, \sigma, b) \to A,\ \alpha v^i \mapsto \alpha u^i\ (\alpha \in K)$ を考えると，$(K/k, \sigma, b)$ が単純多元環であることと，k 上の次元の関係から，上の k 上の多元環としての準同型写像は同型写像になる． □

次の定理は，巡回拡大 K/k とそのガロア群の生成元 σ を上のようにとったとき，2 つの巡回多元環がいつ同型になるのかと，k でいつ分解しているのかを示す定理である．この結果は，後の接合積の場合に，より一般化された形で述べられる (定理 2.49)．

定理 2.46 K/k, σ は前の通りとし，b, $c \in k^\times$ とする．

(1) $(K/k, \sigma, b) \simeq (K/k, \sigma, c)$ であるための必要十分条件は $bc^{-1} \in \mathrm{N}_{K/k}(K^\times)$ である．

(2) $(K/k, \sigma, b) \simeq \mathrm{M}_n(k)$ であるための必要十分条件は $b \in \mathrm{N}_{K/k}(K^\times)$ である．

証明 $B = (K/k, \sigma, b) = \sum_{i=0}^{n-1} Kv^i$, $C = (K/k, \sigma, c) = \sum_{i=0}^{n-1} Kw^i$ とする．

(1) 十分性を示す．仮定から $\gamma \in K^\times$ が存在して，$bc^{-1} = \mathrm{N}_{K/k}(\gamma) = \gamma \cdot \gamma^\sigma \cdots \gamma^{\sigma^{n-1}}$ となる．ここで，k 上の多元環としての準同型写像 $B \to C,\ \alpha v^i \mapsto \alpha(\gamma w)^i\ (\alpha \in K)$ を考えると，これは B の単純性と次元の関係から k 上の同型写像になる．

次に必要性を示す．仮定から，k 上の同型写像 $\varphi : B \to C$ が存在する．Skolem–Noether の定理 (定理 2.11) より，$\varphi|_K = \mathrm{id}_K$ としても一般性を失わない．ここで，任意の $\alpha \in K$ に対し，$(\varphi(v) \cdot w^{-1}) \cdot \alpha = \varphi(v)\sigma^{-1}(\alpha)w^{-1} = \varphi(v\sigma^{-1}(\alpha))w^{-1} = \varphi(\alpha v)w^{-1} = \alpha\varphi(v)w^{-1}$ より，$\varphi(v)w^{-1} \in \mathrm{Z}_C(K) = K$ となる．よって，$\varphi(v) = \gamma w$ となる $\gamma \in K^\times$ が存在する．すると，$b = \varphi(b) = \varphi(v)^n = (\gamma w)^n = \mathrm{N}_{K/k}(\gamma)w^n = \mathrm{N}_{K/k}(\gamma)c$ より，

$bc^{-1} \in \mathrm{N}_{K/k}(K^{\times})$ が得られる．

(2) $B \simeq (K/k, \sigma, 1)$ であることは，(1) より $b \in \mathrm{N}_{K/k}(K^{\times})$ であることと同値である．よって，$(K/k, \sigma, 1) \simeq \mathrm{M}_n(k)$ を示せばよい．ここで，k 上の多元環としての準同型写像 $\varphi : (K/k, \sigma, 1) \to \mathrm{End}_k(K)$, $\alpha v^i \mapsto \alpha\sigma^i$ $(\alpha \in K)$ を考えると，これは同型写像になるから $(K/k, \sigma, 1) \simeq \mathrm{End}_k(K) \simeq \mathrm{M}_n(k)$ である． □

2.3.2 接合積 $(K/k, G, \varphi)$

以下，この節では有限群のコホモロジーの基本的な知識を仮定する．有限群のコホモロジーの定義については，2.5 節を参照せよ．

K/k を n 次ガロア拡大とし，$G = \mathrm{Gal}(K/k)$, 2 次のコサイクル $\varphi \in Z^2(G, K^{\times})$ をとる．このとき，K 上のベクトル空間

$$A = \sum_{\sigma \in G} K \cdot x_\sigma \ (\{x_\sigma \mid \sigma \in G\} \text{ は } A \text{ の } K \text{ 上の基底})$$

に対し，積を $x_\sigma \cdot \alpha = \sigma(\alpha) \cdot x_\sigma$ $(\alpha \in K)$, $x_\sigma \cdot x_\tau = \varphi(\sigma, \tau)x_{\sigma\tau}$ で定める．

すると，A は $1_A = \varphi(1,1)^{-1}x_1$ を単位元とする k 上の多元環の構造をもち，さらに k 上の中心的単純環になる．これを φ による**接合積** (crossed product) といい，$(K/k, G, \varphi)$ とかく．定義より，次元は $[(K/k, G, \varphi) : k] = [K : k]^2$ であるから，命題 2.22 より，とくに K は $(K/k, G, \varphi)$ の分解体となる．

前節で定義した巡回多元環は接合積となる．このことを示しておこう．

命題 2.47 巡回多元環は接合積である．

証明 K/k を n 次巡回拡大とし，$G = \mathrm{Gal}(K/k) = \langle\sigma\rangle$，$b \in k^{\times}$ とする．このとき，2 コチェイン $\varphi \in C^2(G, K^{\times})$ として

$$\varphi(\sigma^i, \sigma^j) = b^{[\frac{i+j}{n}] - [\frac{i}{n}] - [\frac{j}{n}]} \ ([\ ] \text{ はガウス記号 })$$

とすると，これは 2 コサイクルになる．すると，巡回多元環の定義における v を x_σ とすれば，$(K/k, G, \varphi) = (K/k, \sigma, b)$ である． □

次の命題から，接合積は極大部分体の言葉で特徴づけられる．命題 2.45 から，次のことからも，巡回多元環は接合積であることがわかる．

命題 2.48 A を k 上中心的単純環とすると，以下は同値である．

(1) A が接合積である．

(2) A が強極大部分体 K で，K/k がガロア拡大であるものが存在する．

証明 (1) $\Rightarrow$ (2) は定義より従う．

(2) $\Rightarrow$ (1) $G = \mathrm{Gal}(K/k)$ とする．Skolem–Noether の定理 (定理 2.11) より，それぞれの $\sigma \in G$ に対して，任意の $\alpha \in K$ に対して，$u_\sigma \alpha u_\sigma^{-1} = \sigma(\alpha)$ となる $u_\sigma \in A^\times$ がとれる．ここで $u_\sigma^{-1}\alpha = \sigma^{-1}(\alpha)u_\sigma^{-1}$ に注意すると，任意の $\alpha \in K$ に対し，$(u_\sigma u_\tau u_{\sigma\tau}^{-1})\alpha = \alpha(u_\sigma u_\tau u_{\sigma\tau}^{-1})$ が計算することでわかる．これより，仮定から $u_\sigma u_\tau u_{\sigma\tau}^{-1} \in (\mathrm{Z}_A(K))^\times = K^\times$ である．そこで，2 コチェイン $\varphi : G \times G \to K^\times$，$(\sigma, \tau) \mapsto u_\sigma u_\tau u_{\sigma\tau}^{-1}$ とすると，$\varphi \in Z^2(G, K^\times)$ であることが計算することでわかる．すると，k 上の多元環としての準同型写像 $\Phi : (K/k, G, \varphi) \to A$, $\alpha x_\sigma \mapsto \alpha u_\sigma$ とすると，接合積 $(K/k, G, \varphi)$ が単純であることから Φ は単射で，$n = [K : k]$ とすると，両辺の k 上の次元は n^2 であることから Φ は $(K/k, G, \varphi)$ と A の同型写像であるから $A \simeq (K/k, G, \varphi)$ である． □

次の定理は，ガロア拡大 K/k と 2 コサイクル $\varphi \in Z^2(G, K^\times)$ をとったとき，2 つの接合積がいつ同型になるのかと，k でいつ分解しているのかを示す定理である．この結果は，前の巡回多元環の場合 (定理 2.46) の一般化になっている．

定理 2.49 K/k, G は前の通りとし，$\varphi, \psi \in Z^2(G, K^\times)$ とする．このとき，以下が成り立つ．

(1) $(K/k, G, \varphi) \simeq (K/k, G, \psi)$ であるための必要十分条件は $[\varphi] = [\psi] \in H^2(G, K^\times)$ である．

(2) $(K/k, G, \varphi) \simeq \mathrm{M}_n(k)$ であるための必要十分条件は $[\varphi] = [1]$，すなわち $\varphi \in B^2(G, K^\times)$ である．

証明 $A = (K/k, G, \varphi) = \sum_{\sigma \in G} K x_\sigma$, $B = (K/k, G, \psi) = \sum_{\sigma \in G} K y_\sigma$ とおく．ここ

で，1 コチェイン $t: G \to K^\times$ に対し，それから定まる 2 コバウンダリーを $\hat{t}: G \times G \to K^\times$, $(\sigma,\tau) \mapsto t(\sigma)\sigma(t(\tau))t(\sigma\tau)^{-1}$ と書くことにする．

(1) 十分性を示す．$[\varphi] = [\psi]$ より，$\varphi = \hat{t}\psi$ となる $t \in C^1(G, K^\times)$ が存在する．すると，A が単純であることと，A, B の次元が等しいことから，k 上の多元環としての同型写像 $\Phi: A \to B$, $\alpha x_\sigma \mapsto \alpha t(\sigma) y_\sigma$ が得られる．

次に，必要性を示す．仮定から，k 上の多元環としての同型写像 $\Phi: A \to B$ が存在する．Skolem–Noether の定理 (定理 2.11) より，$\Phi|_K = \mathrm{id}_K$ としてよい．ここで，$\sigma \in G$ を 1 つ固定する．このとき $\Phi|_K = \mathrm{id}_K$ に注意すると，任意の $\alpha \in K$ に対し，$\Phi(x_\sigma)\alpha = \Phi(x_\sigma\alpha) = \Phi(\sigma(\alpha)x_\sigma) = \sigma(\alpha)\Phi(x_\sigma)$ より，$\Phi(x_\sigma)\alpha = \sigma(\alpha)\Phi(x_\sigma)$ である．ここで，上のことから，$\Phi(x_\sigma) = \sum_{\tau \in G} t_\tau y_\tau$ $(t_\tau \in K)$ とすると，$\sum_{\tau\in G} t_\tau \tau(\alpha) y_\tau = \Phi(x_\sigma)\alpha = \sigma(\alpha)\Phi(x_\sigma) = \sum_{\tau \in G} \sigma(\alpha) t_\tau y_\tau$ が得られる．これより，任意の $\tau \in G$, $\alpha \in K$ に対し，$t_\tau \tau(\alpha) = \sigma(\alpha) t_\tau$ が成り立つ．ここで，$\tau \neq \sigma$ に対しては，$\tau(\alpha) \neq \sigma(\alpha)$ となる $\alpha \in K$ が取れるから，$t_\tau = 0$ でなくてはならない．すると，$\Phi(x_\sigma) = t_\sigma y_\sigma$ とかける．このことにより，最初に固定した $\sigma \in G$ に対し，$K^\times$ の元 t_σ が定まる．

そこで，$t: G \to K^\times$, $\sigma \mapsto t_\sigma$ とする．すると，任意の $\sigma, \tau \in G$ に対して，$\Phi(x_\sigma x_\tau) = \Phi(x_\sigma)\Phi(x_\tau) = t(\sigma)\sigma(t(\tau))y_\sigma y_\tau = t(\sigma)\sigma(t(\tau))\psi(\sigma,\tau)y_{\sigma\tau}$ となる．一方で，$\Phi(x_\sigma x_\tau) = \Phi(\phi(\sigma,\tau)x_{\sigma\tau}) = \varphi(\sigma,\tau)t(\sigma\tau)y_{\sigma\tau}$ であるから，$t(\sigma)\sigma(t(\tau))\psi(\sigma,\tau) = \varphi(\sigma,\tau)t(\sigma\tau)$ が得られる．これから，任意の σ, $\tau \in G$ に対し，$\varphi(\sigma,\tau) = t(\sigma)\sigma(t(\tau))t(\sigma\tau)^{-1}\psi(\sigma,\tau) = \hat{t}(\sigma,\tau)\psi(\sigma,\tau)$ が成り立つから，$\varphi = \hat{t}\psi$，すなわち 2 次のコホモロジー $H^2(G, K^\times)$ の元として $[\varphi] = [\psi]$ が成り立つ．

(2) $(K/k, G, \phi) \simeq \mathrm{M}_n(k)$ であることは (1) より $(K/k, G, 1) \simeq \mathrm{M}_n(k)$ を示せばよい．$\mathrm{M}_n(k) \simeq \mathrm{End}_k(K)$ であることに注意すると，$(K/k, G, 1)$ は単純多元環で，$(K/k, G, 1)$, $\mathrm{End}_k K$ の k 上の次元は n^2 であるから，k 上の多元環としての準同型写像 $\Phi: (K/k, G, 1) \to \mathrm{End}_k K$, $\alpha \mapsto \alpha\sigma$ は同型写像になる．よって，$(K/k, G, 1) \simeq \mathrm{End}_k(K) \simeq \mathrm{M}_n(k)$ が得られる． □

この節の最後に，2 つの接合積のテンソル積の性質についてみておこう．この事実は次節の定理 2.52 の証明で重要である．

定理 2.50 $K/k, G$ は前の通りとし, $\varphi, \psi \in Z^2(G, K^\times)$ とする．このとき, $(K/k, G, \varphi) \otimes (K/k, G, \psi) \sim (K/k, G, \psi)$，すなわち，$(K/k, G, \varphi) \otimes (K/k, G, \psi)$ と $(K/k, G, \varphi\psi)$ はブラウアー同値である．

証明 $A = (K/k, G, \varphi) = \sum_{\sigma \in G} K x_\sigma$, $B = (K/k, G, \psi) = \sum_{\sigma \in G} K y_\sigma$, $C = (K/k, G, \varphi\psi) = \sum_{\sigma \in G} K z_\sigma$ とおく．A°, B は K 上の線形空間であるから，そのテンソル積 $V = A^\circ \otimes_K B$ とする．V に $A \otimes B$ の作用を右から，$a, a' \in A$, $b, b' \in B$ に対し，$(a' \otimes_K b') \cdot (a \otimes_k b) = a'a \otimes_K bb' = a \cdot a' \otimes_K bb'$ といれることにより，V は右 $A \otimes B$ 加群とみれる．さらに，V は C の作用を左から，$\alpha \in K$, $\sigma \in G$ に対し，$\alpha z_\sigma \cdot (a \otimes_K b) = \alpha x_\sigma a \otimes_K y_\sigma b$ といれることにより，V を左 C 加群ともみることができる．すると，V には両側 $(C, A \otimes B)$ 加群の構造がはいる．

ここで，k 上の多元環としての準同型写像 $\Phi : (A \otimes B)^\circ \to \mathrm{End}_C(V)$, $a \otimes b \mapsto \psi_{a,b}$ とおく．ここで，$\mathrm{End}_C(V)$ は左 C 加群としての自己準同型写像の集合であり， $\psi_{a,b}$ は $\psi_{a,b} : V \to V$, $v \mapsto v \cdot (a \otimes b)$ (左 $A \otimes B$ 加群の作用) $(a \in A, b \in B)$ と定める．命題 2.4 より $(A \otimes B)^\circ$ は単純であるから，Φ は単射である．あとは，両辺の k 上の次元を比較して等しいことを示せばよい．$(A \otimes B)^\circ$ の k 上の次元は n^4 である．

次に，$\mathrm{End}_C(V)$ の k 上の次元を考える．V は左 C 加群であるから k 上の線形空間でもある．$V = A \otimes_K B^\circ$ であったから，$[V : k] = [A : K][B : K][K : k] = n^3 = n[C : k]$ となる．すると，V は左 C 加群として，$V \simeq C^n$ であることがわかる．よって，補題 2.14 と $\mathrm{End}_C(C) \simeq C^\circ$ に注意すると，k 上の多元環としての同型として，$\mathrm{End}_C(V) \simeq \mathrm{End}_C(C^n) \simeq \mathrm{M}_n(\mathrm{End}_C(C)) \simeq \mathrm{M}_n(C^\circ) \simeq C^\circ \otimes \mathrm{M}_n(k)$ であることがわかる．すると，$[\mathrm{End}_C(V) : k] = n^2[C^\circ : k] = n^4$ となる．

よって, Φ は k 上の多元環としての同型写像となる．これより, $(A \otimes B)^\circ \simeq \mathrm{End}_C(V) \simeq C^\circ \otimes \mathrm{M}_n(k)$ が得られる．ここで，$(A \otimes B)^\circ \simeq A^\circ \otimes B^\circ$, $\mathrm{M}_n(k)^\circ \simeq \mathrm{M}_n(k)$ に注意すると，$A \otimes B \simeq C \otimes \mathrm{M}_n(k)$ が得られ，$A \otimes B \sim C$ を得る． □

命題 2.47 により，巡回多元環は接合積であるから，上の定理において，とくに A, B が巡回多元環の場合には次のようになる．

系 2.51 K/k を巡回拡大，そのガロア群の生成元 σ とし，$b,\ c \in k^{\times}$ とする．このとき，$(K/k,\sigma,b)\otimes(K/k,\sigma,c)\sim(K/k,\sigma,bc)$，すなわち，$(K/k,\sigma,b)\otimes(K/k,\sigma,c)$ と $(K/k,\sigma,bc)$ はブラウアー同値である．

2.4 ブラウアー群とガロアコホモロジー

本節では，相対ブラウアー群を定義し，ガロア群が G のガロア拡大 K/k に対し，相対ブラウアー群が 2 次のコホモロジー群 $H^2(G,K^{\times})$ と同型であることを示す．これにより，ブラウアー群をコホモロジー的観点からみることが可能になる．この節は，[渡部], [FD93], [Pie82] を参考にした．

まず，相対ブラウアー群の定義を行う．

定義 体の拡大 K/k に対して, 命題 2.20 より, 準同型写像 $\mathrm{Br}(k)\to\mathrm{Br}(K)$, $[A]\mapsto[A\otimes K]$ が定まる．この核を $\mathrm{Br}(K/k)$ と表し, **相対ブラウアー群** (relative Brauer group) という．

定義より，$\mathrm{Br}(K/k)=\{[A]\in\mathrm{Br}(k)\mid[A\otimes K]=[0]\}=\{[A]\in\mathrm{Br}(k)\mid A$ が K で分解する $\}$ である．定理 2.25 から，k 上の中心的単純環はある有限次ガロア拡大で分解するから，

$$\mathrm{Br}(k)=\bigcup_{K/k:\text{有限次ガロア拡大}}\mathrm{Br}(K/k)$$

である．

この節の主題である相対ブラウアー群とガロアコホモロジーには次のような関係がある．

定理 2.52 K/k をガロア拡大，$G=\mathrm{Gal}(K/k)$ とする．このとき，群の準同型写像 $\Phi:H^2(G,K^{\times})\to\mathrm{Br}(K/k)$, $[\varphi]\mapsto[(\varphi,K/k,G)]$ は同型写像である．

証明 まず，定理 2.50 より，$Z^2(G,K^{\times})\to\mathrm{Br}(K/k)$, $\varphi\mapsto[(K/k,G,\varphi)]$ は群の準同型写像となる．また，定理 2.49 より，この準同型写像の核は $B^2(G,K^{\times})$ である．よって，定理の中で定義された Φ は単射準同型写像であることがわかる．

あとは，Φ の全射性を示せばよい．命題 2.20 より，任意の K で分解する k 上の中心的斜体 D をとり，$\Phi(\varphi) = [D]$ となる $\varphi \in Z^2(G, K^\times)$ が存在することを示せばよい．ここで，$\deg(D) = d$ とおく．すると，$[D^\circ] = -[D] \in \mathrm{Br}(K/k)$ より $K \otimes D^\circ \simeq \mathrm{M}_d(K)$ となる．単純な左 $K \otimes D^\circ$ 加群を V とする．V は $\alpha \in K,\ x \in V,\ d \in D$ に対し，$\alpha \cdot x \cdot d = (\alpha \otimes d) \cdot x$ により，両側 (K, D) 加群ともみれる．V の右 D 加群としての k 上の次元を n とすると，$[V : k] = n[D : k] = nd^2$ であり，一方，$K \otimes D^\circ \simeq \mathrm{M}_d(K)$ より，$[V : k] = d[K : k]$ となる．よって，$[K : k] = nd$ であることがわかる．また，右 D 加群の自己準同型写像のなす k 上の多元環 $\mathrm{End}_D(V)$ は $\mathrm{M}_n(D)$ に同型であるから，$[\mathrm{End}_D(V) : k] = [\mathrm{M}_n(D) : k] = n^2[D : k] = n^2d^2 = [K : k]^2$ である．ここで，k 上の多元環の単射準同型写像 $K \to \mathrm{End}_D(V),\ \alpha \mapsto \alpha \cdot \mathrm{id}_V$ により，K は $\mathrm{End}_D(V)$ の部分体とみなせることに注意すると，$\mathrm{End}_D(V) \simeq \mathrm{M}_n(D)$ は，$\deg(\mathrm{M}_n(D)) = [K : k]$ となる部分体をもつから，命題 2.48 より $\mathrm{End}_D(V) \simeq \mathrm{M}_n(D)$ は接合積である．よって，$\mathrm{M}_n(D) \simeq (K/k, G, \varphi)$ となる $\varphi \in Z^2(G, K^\times)$ が存在して，$[D] = [\mathrm{M}_n(D)] = [(K/k, G, \varphi)] = \Phi(\varphi)$ となり，Φ の全射性が示される． $\square$

この定理から，ブラウアー群の各類の代表元として接合積をとることができることがわかる．よって，任意の中心的単純環は接合積とブラウアー同値である．

この定理を用いて，コホモロジーの観点からブラウアー群の実例を再度みてみよう．このとき，以下の事実に注意する．

命題 2.53 K/k を有限次の巡回拡大とし，$G = \mathrm{Gal}(K/k) = \langle \sigma \rangle$ とする．このとき，群の準同型写像 $k^\times / N_{K/k}(K^\times) \to \mathrm{Br}(K/k),\ [a] \mapsto [(K/k, \sigma, a)]$ は同型写像である．

証明 写像 $k^\times \to \mathrm{Br}(K/k),\ a \mapsto [(K/k, \sigma, a)]$ は系 2.51 と定理 2.26 より群の全射準同型写像となり，命題 2.46 の (2) より，この準同型写像の核は $N_{K/k}(K^\times)$ であることからわかる． $\square$

例 2.54 ($\mathbb{R}$ のブラウアー群) 命題 2.36 より $\mathbb{R}$ のブラウアー群は $\mathbb{Z}/2\mathbb{Z}$ と同型であった．これは，定理 2.52 より，$\mathrm{Br}(\mathbb{R}) = \mathrm{Br}(\mathbb{R}/\mathbb{R}) \cup \mathrm{Br}(\mathbb{C}/\mathbb{R})$ であり，命題 2.53 より，$\mathrm{Br}(\mathbb{C}/\mathbb{R}) \simeq \mathbb{R}^\times / N_{\mathbb{C}/\mathbb{R}}(\mathbb{C}^\times) \simeq \mathbb{Z}/2\mathbb{Z}$ であるから，$\mathrm{Br}(\mathbb{R}) \simeq \mathbb{Z}/2\mathbb{Z}$ がわかる．

例 2.55 ($\mathbb{F}_q$ のブラウアー群) 命題 2.38 より有限体 $\mathbb{F}_q$ のブラウアー群は自明群であった．これは，定理 2.52 より，$\mathrm{Br}(\mathbb{F}_q) = \cup_{n=1}^{\infty} \mathrm{Br}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ であり，命題 2.53 より，任意の $n \in \mathbb{N}$ に対し，有限体のノルム写像が全射であることに注意すると，$\mathrm{Br}(\mathbb{F}_{q^n}/\mathbb{F}_q) \simeq \mathbb{F}_q^{\times}/N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\mathbb{F}_{q^n}^{\times}) = \{0\}$ であることから，$\mathrm{Br}(\mathbb{R}) = \{0\}$ がわかる．

2.5 補足：有限群のコホモロジーの定義

本節では，本論文で用いた有限群のコホモロジーの定義について確認する．この節では [斉藤] を参考にした．以下，本節では G を有限群とする．

まず，G 加群の定義から行う．

定義 M を加群とする．このとき，M が **G 加群** (G-module) であるとは，M に G の作用が定義されていて，$x, y \in M$ に対し，$\sigma \cdot (x + y) = \sigma \cdot x + \sigma \cdot y$ が成り立つときをいう．以下，作用の $\cdot$ を省略してかく．

M を G 加群，$S \subset G$ を部分集合としたとき，

$$M^S = \{x \in M \mid \sigma x = x \ (\sigma \in S)\}$$

とすると，M^S は M の部分加群である．

また，$x \in M$ に対し，

$$\mathrm{N}_G(x) = \sum_{\sigma \in G} \sigma x$$

とおくと，$\mathrm{N}_G(x)$ は M^G の元であり，これにより加群の準同型写像 $\mathrm{N}_G : M \to M^G$ が定まる．これを**ノルム写像** (norm map) という．

次に，G 加群の準同型写像を定義しよう．

定義 M, N を G 加群とし，$f : M \to N$ を加群の準同型写像とする．このとき，f が **G 加群の準同型写像** (G-homomorphism) であるとは，任意の $\sigma \in G, x \in M$ に対し，$f(\sigma x) = \sigma f(x)$ が成り立つときをいう．

例 2.56 K/k をガロア拡大，$G = \mathrm{Gal}(K/k)$ とする．このとき，自然に $K^\times$ に G の作用が入り，それにより $K^\times$ を G 加群とみることができる．このとき，$K^\times$ の演算は積で入っていることに注意する．すると，G 加群のノルム写像は，$x \in K^\times$ に対し

$$\mathrm{N}_G(x) = \prod_{\sigma \in G} \sigma(x) = \mathrm{N}_{K/k}(x)$$

となり，体のノルム写像と一致する．

定義 M を G 加群とする．負でない整数 n に対し，

$$C^n(G, M) = \{\varphi : G^n \to M\}$$

とし，この元を n **コチェイン** (n-cochain) という．ここで，$C^0(G, M) = M$ と定める．

$C^n(G, M)$ は，$\varphi, \psi \in C^n(G, M)$, $\underline{\sigma} \in G^n$ に対し，$(\varphi + \psi)(\underline{\sigma}) = \varphi(\underline{\sigma}) + \psi(\underline{\sigma})$ により加法群になる．

ここで，$n \geq 0$ に対して，準同型写像 $d^n : C^n(G, M) \to C^{n+1}(G, M)$ を次のように定義する．

$$\begin{aligned} d^n(\varphi)(\sigma_1, \ldots, \sigma_{n+1}) &= \sigma_1 \varphi(\sigma_2, \ldots, \sigma_{n+1}) \\ &\quad + \sum_{i=1}^{n} (-1)^i \varphi(\sigma_1, \ldots, \sigma_{i-1}, \sigma_i \sigma_{i+1}, \sigma_{i+2}, \ldots, \sigma_{n+1}) \\ &\quad + (-1)^{n+1} \varphi(\sigma_1, \ldots, \sigma_n). \end{aligned}$$

ここで，$n = 0$ の場合は，$x \in C^0(G, M) = M$, $\sigma \in G$ に対して，$d^0(x)(\sigma) = \sigma(x) - x$ と定める．すると，計算することにより $d^{n+1} \circ d^n = 0$ となることがわかる．

ここで，$Z^n(G, M) = \mathrm{Ker}(d^n)$ $(n \geq 0)$, $B^n(G, M) = \mathrm{Im}(d^{n-1})$ $(n \geq 1)$ とおき，それらの元をそれぞれ n **コサイクル** (n-cocycle)，n **コバウンダリー** (n-coboundary) という．これらは，$C^n(G, M)$ の部分加群となる．すると，$d^{n+1} \circ d^n = 0$ より，$B^n(G, M) \subset Z^n(G, M)$ である．

これによって G 加群 M のコホモロジーが定義される．

定義　$H^0(G,M)=Z^0(G,M)$, $H^n(G,M)=Z^n(G,M)/B^n(G,M)$ $(n\geq 1)$ とし，これらを M の n 次の**コホモロジー群** (cohomology group) という．

実際に，本論文で用いられるのは n が 2 以下の場合である．この場合の n コサイクル，n コバウンダリーがどのようになっているかを具体的にみておこう．

例 2.57 (0 コサイクル) $Z^0(G,M)=H^0(G,M)=M^G$ である．

例 2.58 (1 コサイクル，1 コバウンダリー) $Z^1(G,M)$ の元は，写像 $\varphi:G\to M$ で

$$\sigma,\,\tau\in G \text{ に対し，} \varphi(\sigma\tau)=\sigma\varphi(\tau)+\varphi(\sigma)$$

をみたすもの全体のなす加群である．

$B^1(G,M)$ の元は，写像 $\varphi:G\to M$ で，任意の $\sigma\in G$ に対して $\varphi(\sigma)=\sigma(x)-x$ となる $x\in M$ が存在するようなもの全体のなす加群である．

例 2.59 (2 コサイクル，2 コバウンダリー) $Z^2(G,M)$ の元は，写像 $\varphi:G\times G\to M$ で

$$\sigma,\,\tau,\,\rho\in G \text{ に対し，} \sigma\varphi(\tau\rho)+\varphi(\sigma,\tau\rho)=\varphi(\sigma\tau,\rho)+\varphi(\sigma,\tau)$$

をみたすもの全体のなす加群である．

$B^2(G,M)$ の元は，写像 $\varphi:G\times G\to M$ で，任意の $\sigma,\,\tau\in G$ に対して $\varphi(\sigma,\tau)=\sigma\lambda(\tau)-\lambda(\sigma\tau)+\lambda(\sigma)$ となる $\lambda\in C^1(G,M)$ が存在するようなもの全体のなす加群である．本論文では，この λ から定まる 2 コサイクルを $\hat{\lambda}$ とかいていた．

3　中心的単純環の具体例

3.1　四元数環の理論

本節では，k 上の多元環の例 1.3 であげた四元数環についての理論について解説する．この節は，[GS06], [Lam05], [斉藤] を参考にした．以下，体 k の標数は 2 でないとする．

3.1.1　基本事項

四元数環の定義について，再度復習しておこう．

定義　体 k を標数 2 ではないものとする．$a,\, b \in k^\times$ に対し，k 上の 4 次元の k 上の多元環で，k 上の基底として $\{1, i, j, ij\}$ をもち，積に関しては $i^2 = a,\, j^2 = b,\, ij = -ji$ みたすものを**四元数環** (quaternion algebra) といい，$\left(\frac{a,b}{k}\right)$ と表す．

四元数環は $k^\times/k^{\times 2}$ によって決まる．これが次の命題である．

命題 3.1　$a,\, b \in k^\times$ とする．このとき，$u,\, v \in k^\times$ に対して，$\left(\frac{u^2a,v^2b}{k}\right) \simeq \left(\frac{a,b}{k}\right)$ である．

証明　$\left(\frac{a,b}{k}\right)$ の k 上の基底を $\{1, i, j, ij\}$ と，よって，k 上の多元環としての準同型写像を

$$\left(\frac{a,b}{k}\right) \to \left(\frac{au^2, bv^2}{k}\right),\ i \mapsto ui, j \mapsto vj$$

と定めれば，$(ui)^2 = u^2a,\, (vj)^2 = v^2b,\, (ui)(vj) = -(vj)(ui)$ より，$\{1, ui, vj, (ui)(vj)\}$ は $\left(\frac{au^2,bv^2}{k}\right)$ の k 上の基底はとなる．よって，上の準同型写像は同型写像である．　$\square$

四元数環に関する基本的な用語についての定義を行っておく．

定義　四元数環 $\left(\frac{a,b}{k}\right)$ の元 $q = x + yi + zj + wij,\, (x, y, z, w \in k)$ に対し，$\overline{q} = x - yi - zj - wij$ を q の**共役** (conjugate) という．

この共役に関し，定義から次が成り立つ．

(i) 任意の $q_1,\, q_2 \in \left(\frac{a,b}{k}\right)$ に対し，$\overline{q_1 + q_2} = \overline{q_1} + \overline{q_2}$ が成り立つ．

(ii) 任意の $q_1, q_2 \in \left(\frac{a,b}{k}\right)$ に対し，$\overline{q_1 q_2} = \overline{q_2}\,\overline{q_1}$ が成り立つ．

(iii) 任意の $q \in \left(\frac{a,b}{k}\right)$ に対し，$\overline{\overline{q}} = q$ が成り立つ．

定義　四元数環 $Q = \left(\frac{a,b}{k}\right)$ の元 q に対し，$\mathrm{N}(q) = q\overline{q}$ と定め，$\mathrm{N}_Q(q)$ を四元数環 $\left(\frac{a,b}{k}\right)$ での q の**ノルム** (norm) という．対象としている四元数環が明らかな場合は，$\mathrm{N}_Q(q)$ を単に $\mathrm{N}(q)$ とかく．

四元数環 Q の元 $q = x + yi + zj + wij$, $(x, y, z, w \in k)$ に対し，$\mathrm{N}(q) = x^2 - ay^2 - bz^2 + abw^2$ であるから，ノルム $\mathrm{N}(q)$ は k の元であることがわかる．

この四元数環のノルムに関し，定義から次が成り立つ．

(i) 任意の $q_1, q_2 \in \left(\frac{a,b}{k}\right)$ に対し，上の共役の性質に注意すると，$\mathrm{N}(q_1 q_2) = \mathrm{N}(q_1)\mathrm{N}(q_2)$ が成り立つ．

(ii) 四元数環の元 $q \in \left(\frac{a,b}{k}\right)$ に対し，q が可逆元であるであることと，$\mathrm{N}(q) \neq 0$ であることは同値である．とくに，四元数環 $\left(\frac{a,b}{k}\right)$ が斜体であることと，任意の $q \in \left(\frac{a,b}{k}\right)$ に対し $\mathrm{N}(q) \neq 0$ であることは同値である．

定義　四元数環 $\left(\frac{a,b}{k}\right)$ の元 $q = x + yi + zj + wij$, $(x, y, z, w \in k)$ に対し，$x = 0$ のとき，q を**純四元数** (pure quaternion) という．

定義より，$q \in \left(\frac{a,b}{k}\right)$ が純四元数であることと，q が $q^2 \in k$, $q \notin k$ であることは同値である．任意の四元数環 $\left(\frac{a,b}{k}\right)$ の元 q は $q = q_1 + q_2$ ($q_1 \in k$, q_2 は純四元数) とかける．このとき，q の共役は，$\overline{q} = q_1 - q_2$ となり，純四元数 q_2 に対し，そのノルムは $\mathrm{N}(q_2) = -q_2^2$ であることがわかる．

次に，四元数環が k で分解することと同値な条件をみる．そのために 1 つ補題を示しておく．

補題 3.2　$b \in k^{\times}$ に対し，$\left(\frac{1,b}{k}\right) \simeq \mathrm{M}_2(k)$ である．すなわち，$\left(\frac{1,b}{k}\right)$ は k で分解する．

証明　$\left(\frac{1,b}{k}\right)$ の k 上の基底を $\{1, i, j, ij\}$ とする．k 上の多元環としての準同型写像を

$$\left(\frac{1,b}{k}\right) \to \mathrm{M}_2(k),\ i \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, j \mapsto \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}$$

と定めれば，これは k 上の多元環としての同型写像である．□

命題 3.3　$a, b \in k^\times$ とする．このとき，以下は同値である．

(1) $\left(\frac{a,b}{k}\right)$ が k で分解する．

(2) $\left(\frac{a,b}{k}\right)$ が斜体ではない．

(3) $\left(\frac{a,b}{k}\right)$ の 0 でない元 q で，$\mathrm{N}(q) = 0$ となるものが存在する．

(4) $b \in \mathrm{N}_{k(\sqrt{a})/k}(k(\sqrt{a}))$ である．

(4)′ $a \in \mathrm{N}_{k(\sqrt{b})/k}(k(\sqrt{b}))$ である．

(5) x, y, z の 2 次形式 $ax^2 + by^2 = z^2$ が k 上で非自明な解 (x_0, y_0, z_0) をもつ．

とくに，四元数環は分解するか，斜体になるかのいずれかである．

証明　(1) ⇒ (2) 仮定より $\left(\frac{a,b}{k}\right) \simeq \mathrm{M}_2(k)$ であるから，斜体ではない．

(2) ⇒ (3) 上で述べたことから，四元数環 $\left(\frac{a,b}{k}\right)$ が斜体であることと，任意の $q \in \left(\frac{a,b}{k}\right)$ に対し $\mathrm{N}(q) \neq 0$ であることは同値であるから，この対偶をとればよい．

(3) ⇒ (4) もし，$a \in k^{\times 2}$ なら $\mathrm{N}_{k(\sqrt{a})/k}(k(\sqrt{a})) = k$ よりよい．そこで，$a \notin k^{\times 2}$ のときを考える．$K = k(\sqrt{a})$ とする．仮定から，$\left(\frac{a,b}{k}\right)$ の 0 でない元 $q = x+yi+zj+wij$ (x, y, z, $w \in k$) で，$\mathrm{N}(q) = 0$ となるものが存在する．ここで $\mathrm{N}(q) = x^2-ay^2-bz^2+abw^2 = 0$ より，$a \notin k^{\times 2}$ に注意すると，$x^2-ay^2 = b(z^2-aw^2) = b(z+\sqrt{a}w)(z-\sqrt{a}w) \neq 0$ となり，$z+\sqrt{a}w \neq 0$ である．よって，$\mathrm{N}_{K/k}((x+\sqrt{a}y)/(z+\sqrt{a}w)) = (x^2-ay^2)/(z^2-aw^2) = b$ となる．

(3) ⇒ (4)′ これは，(3) ⇒ (4) の議論で a, b を入れ替えればよい．

(4) ⇒ (1) 仮定から，$b \in \mathrm{N}_{k(\sqrt{a})/k}(k(\sqrt{a}))$ であるから，$b^{-1} \in \mathrm{N}_{k(\sqrt{a})/k}(k(\sqrt{a}))$ である．よって，$b^{-1} = r^2 - as^2$ (r, $s \in k$) とかける．そこで，k 上の多元環としての準同型

写像

$$\left(\frac{a,b}{k}\right) \to \left(\frac{1,4a^2}{k}\right),\ i \mapsto u = ri + sij, j \mapsto v = (1+a)i + (1-a)ui$$

とすると, 計算することにより $u^2 = 1, v^2 = 4a^2, uv = -vu$ が得られるから, $\{1, u, v, uv\}$ は $\left(\frac{1,4a^2}{k}\right)$ の k 上の基底となり，上の準同型写像は同型写像である．すると，補題 3.2 より $\left(\frac{1,4a^2}{k}\right)$ は分解するから，$\left(\frac{a,b}{k}\right)$ も分解する．

(4)$'$ ⇒ (1) これは，(4) ⇒ (1) の議論で a, b を入れ替えればよい．

(4) ⇒ (5) 仮定より $b \in \mathrm{N}_{k(\sqrt{a})/k}(k(\sqrt{a}))$ であるから，$b = r^2 - as^2$ $(r,\ s \in k)$ とかける．これより，$(s, 1, r)$ が $ax^2 + by^2 = z^2$ の非自明な解となる．

(5) ⇒ (4) $a \notin k^{\times 2}$ としてよい．$ax^2 + by^2 = z^2$ の非自明な解を (x_0, y_0, z_0) とする．$y_0 = 0$ のとき，$a \in k^{\times 2}$ となり a のとり方に反する．$y_0 \neq 0$ であれば $b = (z_0/x_0)^2 - a(x_0/y_0)^2 \in \mathrm{N}_{k(\sqrt{a})/k}(k(\sqrt{a}))$ となりよい． □

命題 3.3 を使ったいくつかの例をみてみよう．

例 3.4 ($\mathbb{Q}$ 上斜体となる四元数環 1) $k = \mathbb{Q}$ とする．命題 3.3 の (6) より，a, $b \in \mathbb{Q}$ のとき，$a < 0$, $b < 0$ ならば $ax^2 + by^2 = z^2$ は非自明解をもちないから，$\left(\frac{a,b}{\mathbb{Q}}\right)$ は斜体である．

例 3.5 ($\mathbb{Q}$ 上斜体となる四元数環 2) $k = \mathbb{Q}$ とする．このとき，$\left(\frac{5,-3}{\mathbb{Q}}\right)$ は斜体になることを示そう．そのためには，命題 3.3 の (6) より，$5x^2 - 3y^2 = z^2$ は自明解しかもたないことを示せばよい．もし非自明解をもったとすると，$3 \nmid x$ であり，$5x^2 - 3y^2 = z^2$ を mod3 でみると，$5x^2 \equiv z^2 \pmod 3$ となり，5 が mod 3 で平方剰余になる．しかし，平方剰余記号を計算すると $\left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$ より，これは矛盾する．よって，$5x^2 - 3y^2 = z^2$ は自明解しかもたない．ゆえに，$\left(\frac{5,-3}{\mathbb{Q}}\right)$ は斜体になる．

例 3.6 ($\mathbb{Q}$ 上分解する四元数環) $k = \mathbb{Q}$ とする．命題 3.3 の (6) より，$3x^2 - 2y^2 = z^2$ は非自明解 $(1, 1, 1)$ をもつから，$\left(\frac{3,-2}{\mathbb{Q}}\right)$ は分解する．

例 3.7 ($\mathbb{F}_q$ 上の四元数環) $k = \mathbb{F}_q$ (q は奇素数のべき) とする．このとき，a, $b \in \mathbb{F}_q$ の

とき $\left(\frac{a,b}{\mathbb{F}_q}\right)$ は分解することを示そう．$\mathbb{F}_q^\times$ は位数 $q-1$ の巡回群であるから $\mathbb{F}_q$ の平方数は $1+(q-1)/2$ 個である．ここで，$\{ax^2 \mid x \in \mathbb{F}_q\}$ と $\{1-by^2 \mid y \in \mathbb{F}_q\}$ はどちらも $1+(q-1)/2$ 個の元をもつから，鳩の巣原理からかならずどちらにも属する元が存在する．すると，$ax_0^2 = 1-by_0^2$ となる x_0, $y_0 \in F_q$ が存在するから，命題 3.3 の (6) より，$ax^2+by^2=z^2$ は非自明解 $(x_0, y_0, 1)$ をもつ．よって，$\left(\frac{a,b}{\mathbb{F}_q}\right)$ は分解する．

例 3.8 ($k(t)$ 上の四元数環) a, $b \in k^\times$ とし，$k(t)$ を 1 変数有理関数体とする．このとき，$\left(\frac{a,b}{k}\right)$ が分解することと，$\left(\frac{a,b}{k(t)}\right)$ が分解することが同値であることを示そう．$\left(\frac{a,b}{k}\right)$ が分解すれば，$\left(\frac{a,b}{k}\right) \otimes k(t) \simeq \left(\frac{a,b}{k(t)}\right)$ も分解する．逆に，$\left(\frac{a,b}{k(t)}\right)$ が分解すれば，命題 3.3 の (6) より，$ax^2+by^2=z^2$ は $k(t)$ 上で非自明解 $(x(t), y(t), z(t))$ $(x(t),\, y(t),\, z(t) \in k(t))$ が存在する．ここで，$x(t)$, $y(t)$, $z(t)$ は $k[t]$ の元で，少なくとも 1 つは定数項が 0 でないものと仮定してよい．すると，$t=0$ を代入することにより，$ax^2+by^2=z^2$ は k 上で非自明解 $(x(0), y(0), z(0))$ $(x(0),\, y(0),\, z(0) \in k)$ が存在する．よって，命題 3.3 の (6) より $\left(\frac{a,b}{k}\right)$ が分解する．

これを繰り返し用いることで，$k(t_1, \ldots, t_n)$ を n 変数有理関数体とすると，$\left(\frac{a,b}{k}\right)$ が分解することと，$\left(\frac{a,b}{k(t_1,\ldots,t_n)}\right)$ が分解することが同値であることがわかる．

3.1.2 四元数環の同型

この節では，四元数環の同型に関する命題をみてみよう．

命題 3.9 $a, b \in k^\times$ とする．このとき，次が成り立つ．

(1) u, $v \in k^\times$ に対して，$\left(\frac{u^2a,v^2b}{k}\right) \simeq \left(\frac{a,b}{k}\right)$ である．

(2) $\left(\frac{b,a}{k}\right) \simeq \left(\frac{a,b}{k}\right)$ である．

(3) $\left(\frac{1,b}{k}\right) \simeq \left(\frac{a,1}{k}\right) \simeq \mathrm{M}_2(k)$, つまり $\left(\frac{1,b}{k}\right)$, $\left(\frac{a,1}{k}\right)$ は k で分解する．

(4) x, $y \in k$ に対し，$x^2-ay^2 \neq 0$ であれば，$\left(\frac{a,b(x^2-ay^2)}{k}\right) \simeq \left(\frac{a,b}{k}\right)$ である．

(5) $\left(\frac{a,-ab}{k}\right) \simeq \left(\frac{a,(1-a)b}{k}\right) \simeq \left(\frac{a,b}{k}\right)$ である．

(6) $a \neq 1$ のとき，$\left(\frac{a,-a}{k}\right) \simeq \left(\frac{a,1-a}{k}\right) \simeq \mathrm{M}_2(k)$，つまり $\left(\frac{a,-a}{k}\right)$, $\left(\frac{a,1-a}{k}\right)$ は k で分解する．

証明 (1) これは命題 3.1 よりよい．

(2) $\left(\frac{1,b}{k}\right)$ の k 上の基底を $\{1, i, j, ij\}$ とする．すると，k 上の多元環としての準同型写像 $\left(\frac{a,b}{k}\right) \to \left(\frac{b,a}{k}\right)$，$i \mapsto j, j \mapsto i$ は同型写像である．

(3) $\left(\frac{1,b}{k}\right) \simeq \mathrm{M}_2(k)$ は補題 3.2 よりよい．また，$\left(\frac{a,1}{k}\right) \simeq \mathrm{M}_2(k)$ は (2) よりよい．

(4) $c = x^2 - ay^2$ とおくと，k 上の多元環としての準同型写像 $\left(\frac{a,b}{k}\right) \to \left(\frac{a,bc}{k}\right)$，$i \mapsto u = i, j \mapsto v = (x + yi)j$ とすると，$u^2 = a$, $v^2 = bc$, $uv = -vu$ が得られるから，$\{1, u, v, uv\}$ は $\left(\frac{a,bc}{k}\right)$ の k 上の基底となり，上の準同型写像は同型写像である．

(5) 上の (4) において，$x = 0, y = 1$ とすることにより $\left(\frac{a,-ab}{k}\right) \simeq \left(\frac{a,b}{k}\right)$ が得られる．また，(4) において，$x = y = 1$ とすることにより $\left(\frac{a,(1-a)b}{k}\right) \simeq \left(\frac{a,b}{k}\right)$ が得られる．

(6) 上の (5) において，$b = 1$ とすることにより (3) から，$\left(\frac{a,-a}{k}\right) \simeq \left(\frac{a,1-a}{k}\right) \simeq \left(\frac{a,1}{k}\right) \simeq \mathrm{M}_2(k)$ が得られる． □

命題 3.9 を用いた例をいくつかみてみよう．

例 3.10 ($\mathbb{Q}$ 上の四元数環の同型) $k = \mathbb{Q}$ とする．例 3.4 より $\left(\frac{-1,-1}{\mathbb{Q}}\right)$ と $\left(\frac{-2,-3}{\mathbb{Q}}\right)$ は $\mathbb{Q}$ 上の斜体である．命題 3.9 の (2) と (5) より，$\left(\frac{-1,-1}{\mathbb{Q}}\right) \simeq \left(\frac{-1,-2}{\mathbb{Q}}\right) \simeq \left(\frac{-2,-1}{\mathbb{Q}}\right) \simeq \left(\frac{-2,-3}{\mathbb{Q}}\right)$ である．

例 3.11 $a \in k^\times$ とする．このとき，$\left(\frac{a,a}{k}\right) \simeq \left(\frac{a,-1}{k}\right)$ である．実際，命題 3.9 の (1) と (5) より，$\left(\frac{a,a}{k}\right) \simeq \left(\frac{a,-a^2}{k}\right) \simeq \left(\frac{a,-1}{k}\right)$ である．

3.1.3 2 次体上での分解体

四元数環は次数 2 の中心的単純環である．実は，この事実の逆が成り立ち，次数 2 の k 上の中心的単純環は四元数環に限る．この事実を示すために 1 つ補題を示しておく．

補題 3.12 D を次数 2 の k 上の斜体とする．このとき，D が極大部分体として $k(\sqrt{a})$ $(a \in k)$ をもてば，$D \simeq \left(\frac{a,b}{k}\right)$ となる $b \in k$ が存在する．

証明 $q = \sqrt{a} \in D$ とおく．$q \notin k = \mathrm{Z}(D)$ より，$\varphi : D \to D$, $x \mapsto q^{-1}xq$ は D の k 上の多元環としての自己同型写像であり，$\varphi^2 = \mathrm{id}_D$ である．これより，φ は k 上の線形写

像の固有値として -1 をもつ．よって，$\varphi(r) = -r$ となるような $r \in D$ が存在する．すると，$qr = -rq$ が成り立つ．これより，$b = r^2$ とすると，D の k 上の多元環としての準同型写像 $\psi : D \to \left(\frac{a,b}{k}\right)$，$x \mapsto r^{-2}xr^2$ により，$\psi(q) = q$, $\psi(r) = r$ であり，$q^2 = a$, $r^2 = b$, $qr = -rq$ である．よって，ψ は同型写像であり，$D \simeq \left(\frac{a,b}{k}\right)$ が成り立つ． □

定理 3.13 A を次数 2 の k 上の中心的単純環とする．このとき，$a, b \in k^\times$ が存在して，$A \simeq \left(\frac{a,b}{k}\right)$ となる．

証明 Wedderburn の構造定理 (定理 2.1) より $A \simeq \mathrm{M}_n(D)$ (D は k 上の斜体) となる．$\deg(A) = 2$ より，$n = 1$, $\deg(D) = 2$ または，$n = 2$, $\deg(D) = 1$ である．後者の場合は，$D = k$ となるから，命題 3.9 の (3) から，$A \simeq \mathrm{M}_2(k) \simeq \left(\frac{1,1}{k}\right)$ となるからよい．よって，前者の場合を考えればよい．このとき，$A \simeq D$ より，A は k 上の斜体である．$a \in A \setminus k$ をとり，$f_a \in k[x]$ を a の k 上での最小多項式とする．すると，k 上の多元環としての埋め込み $k(a) \simeq k[x]/(f_a) \hookrightarrow A,\ g(x) \mapsto g(a)$ により $k(a)$ を A の部分体とみると，$a \notin k$ より $[k(a) : k] = 2$ である．よって，補題 3.12 より $A \simeq \left(\frac{a,b}{k}\right)$ となる $b \in k^\times$ が存在する． □

これにより，次数 2 の k 上の中心的単純環は四元数環になることがわかった．

次に，2 次体 $K = k(\sqrt{c})$ が与えられたとき，四元数環が K で分解する条件をみてみよう．

命題 3.14 $a, b \in k^\times$, $c \in k^\times \setminus (k^\times)^2$ とし，$Q = \left(\frac{a,b}{k}\right)$, $K = k(\sqrt{c})$ とする．このとき，以下は同値である．

(1) Q は K で分解する．

(2) $Q \simeq \left(\frac{c,d}{k}\right)$ となる $d \in k^\times$ が存在する．

(3) K は k 上の多元環として Q に埋め込みがある．

証明 (2) $\Rightarrow$ (1) 仮定より，命題 3.9 の (1), (3) に注意すると，$Q \otimes K \simeq \left(\frac{c,d}{K}\right) \simeq \left(\frac{(\sqrt{c})^2,d}{K}\right) \simeq \left(\frac{1,d}{K}\right) \simeq \mathrm{M}_2(K)$ より，Q は K で分解する．

(3) $\Rightarrow$ (2) もし，Q が k で分解していたら，命題 3.9 の (3) より $Q \simeq \mathrm{M}_2(k) \simeq \left(\frac{c,1}{k}\right)$ と

なるから $d=1$ ととればよい．また，Q が k で分解していなかったら，命題 3.3 より Q は k 上の斜体であるから，補題 3.12 と仮定から $Q \simeq \left(\frac{c,d}{k}\right)$ となる $d \in k^{\times}$ が存在する．

(1) $\Rightarrow$ (3) 仮定より K は Q の分解体であるから，定理 2.26 より $Q \sim B$ であり，K を強極大部分体として含むような k 上の中心的単純環 B が存在する．このとき，$[B:k] = \deg(B)^2 = 4 = \deg(Q)^2 = [Q:k]$ であるから，命題 2.18 より $B \simeq Q$ となる．この同型写像によって，K は Q に埋め込まれる． □

3.1.4 Albert の定理

この節では，2 つの四元数環のテンソル積ついて考察する．

命題 3.15 $a, b, b' \in k^{\times}$ に対して，$\left(\frac{a,b}{k}\right) \otimes \left(\frac{a,b'}{k}\right) \simeq \left(\frac{a,bb'}{k}\right) \otimes \mathrm{M}_2(k)$ である．

証明 例 2.44 より $\left(\frac{a,b}{k}\right) = (k(\sqrt{a})/k, \sigma, b), \left(\frac{a,b'}{k}\right) = (k(\sqrt{a})/k, \sigma, b')$ であるから，系 2.51 より，$\left(\frac{a,b}{k}\right) \otimes \left(\frac{a,b'}{k}\right) = (k(\sqrt{a})/k, \sigma, b) \otimes (k(\sqrt{a})/k, \sigma, b') \sim (k(\sqrt{a})/k, \sigma, bb') = \left(\frac{a,bb'}{k}\right)$ である．よって，両辺の次数をみることで，$\left(\frac{a,b}{k}\right) \otimes \left(\frac{a,b'}{k}\right) \simeq \left(\frac{a,bb'}{k}\right) \otimes \mathrm{M}_2(k)$ を得る． □

この命題から，とくに次のことがわかる．

系 3.16 $a, b \in k^{\times}$ に対して，$\left(\frac{a,b}{k}\right) \otimes \left(\frac{a,b}{k}\right) \simeq \mathrm{M}_4(k)$ である．

証明 上の命題と命題 3.9 より，$\left(\frac{a,b}{k}\right) \otimes \left(\frac{a,b}{k}\right) \simeq \left(\frac{a,b^2}{k}\right) \otimes \mathrm{M}_2(k) \simeq \left(\frac{a,1}{k}\right) \otimes \mathrm{M}_2(k) \simeq \mathrm{M}_2(k) \otimes \mathrm{M}_2(k) \simeq \mathrm{M}_4(k)$ より得られる． □

四元数環 $Q = \left(\frac{a,b}{k}\right)$ に対し，Q に対応する 2 次形式を $\Phi(x_1, x_2, x_3) = -ax_1^2 - bx_2^2 + abx_3^2$ と定める．これは，Q の純四元数 $q = x_1 i + x_2 j + x_3 ij$ $(x_i \in k)$ のノルムから定まる 2 次形式である．

定義 $Q_1 = \left(\frac{a,b}{k}\right)$, $Q_2 = \left(\frac{c,d}{k}\right)$ を四元数環とし，$A = Q_1 \otimes Q_2$ とし，Q_i に対応する 2 次形式を Φ_i とする．このとき，2 次形式 $\phi(x_1, x_2, x_3, y_1, y_2, y_3) = \Phi_1(x_1, x_2, x_3) - \Phi_2(y_1, y_2, y_3) = -ax_1^2 - bx_2^2 + abx_3^2 + cy_1^2 + dy_2^2 - cdy_3^2$ を A の **Albert form** という．

この Albert form を用いることで，2 つの四元数環のテンソル積が斜体になるかどうかが判定できる．それが，次の Albert の定理である．

定理 3.17 (Albert の定理) Q_1, Q_2 を四元数環とし，$A = Q_1 \otimes Q_2$ とする．このとき，次は同値である．

(1) A は斜体でない．

(2) $Q_1 \simeq \left(\frac{a,b}{k}\right)$, $Q_2 \simeq \left(\frac{a,b'}{k}\right)$ となるような $a, b, b' \in k^\times$ が存在する．

(3) A の Albert form ϕ とすると，$\phi(x_1, x_2, x_3, y_1, y_2, y_3) = 0$ が非自明な解を持つ．

証明 Q_1 の k 上の基底を $\{1, i, j, ij\}$，Q_2 の k 上の基底を $\{1, u, v, uv\}$ とし，Q_i のノルムを N_i とかくことにする．

(2) $\Rightarrow$ (3) 仮定から，$q_i^2 = \mathrm{N}_i(q_i) = a$ となる純四元数 $q_i \in Q_i \setminus \{0\}$ が存在する．すると，$q_1 = x_1 i + x_2 j + x_3 ij$, $q_2 = y_1 u + y_2 v + y_3 uv$ とすると，$\phi(x_1, x_2, x_3, y_1, y_2, y_3) = \Phi_1(x_1, x_2, x_3) - \Phi_2(y_1, y_2, y_3) = \mathrm{N}_1(q_1) - \mathrm{N}_2(q_2) = 0$ となる．

(3) $\Rightarrow$ (1) 仮定から，$\phi(x_1, x_2, x_3, y_1, y_2, y_3) = 0$ となるような $(x_1, x_2, x_3, y_1, y_2, y_3) \neq (0, \dots, 0)$ が存在する．$q_1 = x_1 i + x_2 j + x_3 ij \in Q_1$, $q_2 = y_1 u + y_2 v + y_3 uv \in Q_2$ とすると，q_1, q_2 は A の中で可換であるから，$\phi(x_1, x_2, x_3, y_1, y_2, y_3) = \mathrm{N}_1(q_1) - \mathrm{N}_2(q_2) = -q_1^2 + q_2^2 = (q_1 - q_2)(q_1 + q_2) = 0$ となり，$q_1 - q_2 \neq 0$, $q_1 + q_2 \neq 0$ であるから，A は斜体にならない．

(1) $\Rightarrow$ (2) 対偶を示す．(2) が成り立たないとすると，Q_1, Q_2 はどちらも斜体になる．ここで，任意の Q_i の k 上 2 次の部分体 K_i $(i = 1, 2)$ に対して，K_1 は Q_1 を分解するが Q_2 を分解しない，K_2 は Q_2 を分解するが Q_1 を分解しないことに注意する．すると，$Q_1 \otimes K_2, Q_2 \otimes K_1$ は K_i 上の斜体になる．そこで，任意の $\alpha \in A \setminus \{0\}$ に対して $\beta\alpha = 1$ となる $\beta \in A$ が存在することを示せば，A が斜体であることが示される．

任意の $\alpha \in A \setminus \{0\}$ をとる．$K_2 = k(v)$ とすると，$\alpha = \beta_1 + \beta_2 v + (\beta_3 + \beta_4 v)uv$ $(\beta_i \in Q_1)$ とかける．ここで，$\beta_3 + \beta_4 v = 0$ なら，$\alpha = \beta_1 + \beta_2 v \in Q_1 \otimes K_2$ で $\in Q_1 \otimes K_2$ は斜体であるから，$\beta\alpha = 1$ となる $\beta \in Q_1 \otimes K_2 \subset A$ が存在して証明が終わる．

$\beta_3 + \beta_4 v \neq 0$ なら，α に $\beta_3 + \beta_4 v \in Q_1 \otimes K_2$ の逆元を左からかけることにより，

$\alpha=\beta_1+\beta_2 v+uv$ の場合に帰着される．

ここで，β_1, $\beta_2\in A$ が可換であれば，$k(\beta_1,\beta_2)$ は Q_1 の部分体となるから k または k 上の 2 次拡大 $K\subset Q_1$ になる．したがって，α は Q_2 または $Q_2\otimes K$ となり，どちらも斜体であるから $\beta\alpha=1$ となる $\beta\in A$ が存在して証明が終わる．

一方，β_1, $\beta_2\in A$ が可換でなければ，$\lambda=\beta_1-\beta_2 v-uv\in A$ とすると，$\lambda\alpha=(\beta_1-\beta_2 v-uv)(\beta_1+\beta_2 v+uv)=(\beta_1^2-\beta_2^2 v^2-(uv)^2)+(\beta_1\beta_2-\beta_2\beta_1)v\in Q_1\otimes K_2$ となる．よって，$Q_1\otimes K_2$ が斜体であることから $\beta'(\lambda\alpha)=1$ となる $\beta'\in A$ が存在するから，$\beta=\beta'\lambda\in A$ とすればよい． □

例 3.18 $k=\mathbb{Q}$ とする．例 3.4，例 3.5 より，$\left(\frac{-1,-1}{\mathbb{Q}}\right)$, $\left(\frac{5,-3}{\mathbb{Q}}\right)$ は斜体である．このとき，$A=\left(\frac{-1,-1}{\mathbb{Q}}\right)\otimes\left(\frac{5,-3}{\mathbb{Q}}\right)$ とすると，A の Albert form は $\phi(x_1,x_2,x_3,x_4,x_5,x_6)=x_1^2+x_2^2+x_3^2+5x_4^2-3x_5^2+15x_6^2$ で $\phi(x_1,x_2,x_3,x_4,x_5,x_6)=0$ は $(1,1,1,0,1,0)$ を非自明解にもつから，A は斜体ではない．

3.2 中心的斜体の理論

本節では，中心的斜体に焦点を当て，それに対して成り立つ性質を見ていく．中心的斜体の基本的な性質としては，プライマリー分解とよばれる分解ができることが挙げられる．このことにより，さまざまな中心的斜体の性質は，次数が素数べきのものごとに対してみていけばよいことがわかる．本節の最後に，次数 3 と次数 4 の中心的斜体が巡回多元環について詳しくみていく．ここで，3.2.1 節に関しては，一般の中心的単純環に対して成り立つものであることに注意しておく．この節は，[渡部], [Pie82] を参考にした．

3.2.1 インデックス $\mathrm{ind}(A)$ とピリオド $\mathrm{per}(A)$

この節では，中心的単純環に対し，インデックスとピリオドという概念を導入する．これは，ブラウアー同値類で不変であるため，ブラウアー群の元に対する重要な不変量となっている．これらの不変量に対する基本的な性質をみていく．

まず，インデックスとピリオドの定義をしよう．

定義　A を k 上の中心的単純環とする．すると，Wedderburn の構造定理 (定理 2.1) より $A \simeq \mathrm{M}_n(D)$ となる k 上の斜体 D が存在する．このとき A の**インデックス** (index) を $\mathrm{ind}(A) = \deg(D)$ と定義する．また，A の**ピリオド** (period) を A のブラウアー同値類 $[A] \in \mathrm{Br}(k)$ のブラウアー群の元としての位数と定義し，$\mathrm{per}(A)$ と表す．

定義より，この 2 つの量はブラウアー同値類の不変量となることがわかる．まず，インデックスに関して成り立つ性質をみてみよう．

命題 3.19　A を k 上の中心的単純環とする．このとき，以下が成り立つ．

(1) $\mathrm{ind}(A) \mid \deg(A)$ である．とくに，$\mathrm{ind}(A) = \deg(A)$ であることと A が k 上の斜体になることは同値である．

(2) K を A の分解体とすると，$\mathrm{ind}(A) \mid [K : k]$ である．

(3) A の部分体 K で，A の分解体であり，かつ $[K : k] = \mathrm{ind}(A)$ となるものが存在する．

(4) K/k を体の有限次拡大とすると，$\mathrm{ind}(A \otimes K) \mid \mathrm{ind}(A) \mid [K : k]\,\mathrm{ind}(A \otimes K)$ である．

証明　(1) $A \simeq \mathrm{M}_n(D)$ (D は k 上の斜体) とすると，$\deg(A) = n\deg(D) = n\,\mathrm{ind}(A)$ より $\mathrm{ind}(A) \mid \deg(A)$ である．また，$\mathrm{ind}(A) = \deg(A)$ であることは $n = 1$ であることと同値であり，これは $A \simeq D$，すなわち A が k 上の斜体になることと同値である．

(2) 定理 2.26 によって，K を極大部分体にもつような A とブラウアー同値な k 上の中心的単純環 B が存在する．このとき，$B \simeq \mathrm{M}_n(D)$ (D は k 上の斜体) とすると，$A \sim D$ であり，$[K : k] = \deg(B) = n\deg(D) = n\ \mathrm{ind}(A)$ より，$\mathrm{ind}(A) \mid [K : k]$ である．

(3) Wedderburn の構造定理 (定理 2.1) より $A \simeq \mathrm{M}_n(D) \simeq D \otimes \mathrm{M}_k$ (D は k 上の斜体) となる．すると，命題 2.23 より，D の極大部分体 K は D の分解体であるから A の分解体でもあり，かつ強極大部分体でもあるから $[K : k] = \deg(D) = \mathrm{ind}(A)$ である．よって，K を上の同型写像で引き戻したものが求める A の部分体である．

(4) A を k 上の中心的斜体と仮定してよい．すると, (1) から $\mathrm{ind}(A \otimes K) \mid \deg(A \otimes K) = \deg(A) = \mathrm{ind}(A)$ である．また，(3) より，$A \otimes K$ の部分体 L で，$A \otimes K$ の分解体であ

り，かつ $[L:K]=\operatorname{ind}(A\otimes K)$ となるものが存在する．すると，L は A の分解体でもあるから (2) より，$\operatorname{ind}(A)\mid[L:k]=[L:K][K:k]=[K:k]\operatorname{ind}(A\otimes K)$ である． □

この命題から，中心的斜体 D を係数拡大したときに，それがまた斜体となるかどうかの判定法が得られる．

系 3.20 D を k 上の中心的斜体とし，K/k を体の有限次拡大で $[K:k]$ が $\deg(D)$ の素因子であるものとする．このとき，以下は同値である．

(1) K は D の部分体と同型である．

(2) $D\otimes K$ は斜体でない．

(3) $\deg(D)=[K:k]\operatorname{ind}(D\otimes K)$ である．

証明 (1) $\Rightarrow$ (2) 仮定より $K\subset D$ としてよい．K を含むような D の極大部分体を L とする．すると，L は D の分解体であるから，$D\otimes K$ の分解体にもなる．すると，$\operatorname{ind}(D\otimes K)\leq[L:K]<[L:k]=\deg(D)=\deg(D\otimes K)$ であるから，命題 3.19 の (1) より $D\otimes K$ は斜体でない．

(2) $\Rightarrow$ (3) $D\otimes K$ は斜体でないから $\operatorname{ind}(D\otimes K)<\deg(D\otimes K)=\deg(D)$ である．すると，命題 3.19 の (4) から，$\deg(D)\mid[K:k]\operatorname{ind}(D\otimes K)$ より $[K:k]\operatorname{ind}(D\otimes K)=m_1\deg(D)$ となる $m_1\in\mathbb{N}$ が存在する．一方，$\operatorname{ind}(D\otimes K)\mid\operatorname{ind}(D)=\deg(D)$ より，$\deg(D)=m_2\operatorname{ind}(D\otimes K)$ となる $m_2\in\mathbb{N}$ が存在する．すると，$[K:k]\operatorname{ind}(D\otimes K)=m_1\deg(D)=m_1m_2\operatorname{ind}(D\otimes K)$ より，$[K:k]=m_1m_2$ が得られる．ここで，$[K:k]$ が素数であり，$\operatorname{ind}(D\otimes K)<\deg(D)$ より $m_2>1$ であることに注意すると $m_1=1$ である．よって，$\deg(D)=[K:k]\operatorname{ind}(D\otimes K)$ が得られる．

(3) $\Rightarrow$ (1) 命題 3.19 の (3) から，$D\otimes K$ の部分体 L で，$D\otimes K$ の分解体であり，かつ $[L:K]=\operatorname{ind}(D\otimes K)$ となるものが存在する．L は $D\otimes K$ の分解体であるから，D の分解体であり，仮定から $\deg(D)=[K:k]\operatorname{ind}(D\otimes K)=[L:k]$ である．よって，定理 2.26 から，k 上の中心的単純環 B で，$B\sim D$ であり，かつ L を極大部分体にもつものが存在する．すると，$\deg(B)=[E:k]=\deg(D)$ であるから，$B\sim D$ とあわせて命題 2.18 から $B\simeq D$ である．この同型により，K は D の部分体と同型である． □

次に，インデックスとピリオドの間にはどのような関係があるかをみてみる．

命題 3.21 A を k 上の中心的単純環とする．このとき, $m = \mathrm{ind}(A)$ とおくと, $m[A] = [0]$ となる．これより，$\mathrm{per}(A) \mid \mathrm{ind}(A)$ となる．

証明 A の分解体 K で，K/k が有限次ガロア拡大となるものをとる．$G = \mathrm{Gal}(K/k)$ とする．すると，定理 2.52 より，$[A] = [(K/k, G, \varphi)]$ となる $\varphi \in Z^2(G, K^\times)$ が存在する．定理 2.50 より，$m[A] = [(K/k, G, \varphi^m)]$ となるから，$\varphi^m \in B^2(G, K^\times)$ を示せばよい．

$B = (K/k, G, \varphi)$ とすると，$B \simeq \mathrm{M}_r(D)$ となる k 上の斜体 D が存在する．$V = D^r$ とすると，自然に V は左 B 加群とみなせる．一方，$K \subset B$ より，V は K 上の線形空間である．ここで，$[A] = [B] = [D]$ に注意すると，$\mathrm{ind}(D) = \mathrm{ind}(A) = m$ であるから $[K : k] = \deg(K/k, G, \varphi) = \deg(\mathrm{M}_r(D)) = rm$ となる．これより，$[V : K] = [V : k]/[K : k] = [D^r : k]/[K : k] = rm^2/rm = m$ となる．ここで，V の K 上の線形空間としての基底を $\{v_1, \ldots, v_m\}$ とする．すると，任意の $b \in B$ に対し，

$$b \begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix} = \begin{pmatrix} b_{11} & \ldots & b_{1m} \\ \vdots & \ddots & \vdots \\ b_{m1} & \ldots & b_{mm} \end{pmatrix} \begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix}$$

となる行列 $(b_{ij}) \in M_m(K)$ が存在する．これにより，各 $b \in B$ に対し，行列 $(b_{ij}) \in M_m(K)$ を対応させる．

$B = (K/k, G, \varphi) = \sum_{\sigma \in G} K x_\sigma$ とし，x_σ に対応する行列を X_σ とする．任意に σ, $\tau \in G$ をとる．すると，$x_\sigma x_\tau = \varphi(\sigma, \tau) x_{\sigma\tau}$ より，$\varphi(\sigma, \tau) X_{\sigma\tau} = \sigma(X_\tau) X_\sigma$ が得られる．よって，両辺の行列式をとると，$\varphi(\sigma, \tau)^m \det(X_\sigma) = \sigma(\det(X_\tau)) \det(X_\sigma)$ となるから，$\varphi(\sigma, \tau)^m = \sigma(\det(X_\tau)) \det(X_\sigma) \det(X_\sigma)^{-1}$ となる．そこで，1 コチェイン $t : G \to K^\times$ を，$t(\sigma) = \det(X_\sigma)$ とすれば，$\varphi(\sigma, \tau)^m = \sigma(t(\tau)) t(\sigma) (t(\sigma\tau))^{-1} = \hat{t}(\sigma, \tau)$ となる．よって，$\varphi^m = \hat{t} \in B^2(G, K^\times)$ である． □

このことから，ブラウアー群の元の位数はどれも有限であることがわかる．このことから，次の系が得られる．

系 3.22 $\mathrm{Br}(A)$ はねじれアーベル群になる．

また，インデックスとピリオドの素因子の間には次のような事実が成り立つ．

命題 3.23 A を k 上の中心的単純環とする．このとき，p を $\mathrm{ind}(A)$ の素因子の 1 つとすると，p は $\mathrm{per}(A)$ の素因子にもなる．

証明 命題 3.21 の証明と同様に，$[A]=[(K/k,G,\varphi)]$, $(K/k,G,\varphi)\simeq \mathrm{M}_r(D)$ (D は k 上の斜体) とする．$d=\mathrm{ind}(A)=\deg(D)$ とし，d の素因子の 1 つを p とする．$|G|=[K:k]=\deg(\mathrm{M}_n(D))=rd$ より，$p \mid |G|$ を得る．

ここで，G_p を G の p シロー部分群とする．$K_p=K^{G_p}$ とすると，$[K_p:k]=|G_p|=p^e$ ($e\in\mathbb{N}$) となる．$p\nmid [K^p:k]$ であるから，命題 3.19 の (2) より，K_p は D の分解体ではない．よって，K_p は A の分解体でもない．よって，$\mathrm{per}(A\otimes K_p)\neq 1$ である．

一方で，命題 3.19 の (2) より $[A\otimes K_p]\in \mathrm{Br}(K/K_p)$ より $\mathrm{ind}(A\otimes K_p)\mid [K:K_p]=p^e$ であることがわかる．よって，命題 3.21 より，$\exp(A\otimes K_p)\mid p^e$ であり，$\mathrm{per}(A\otimes K_p)\neq 1$ であるから $p\mid \mathrm{per}(A\otimes K_p)$ である．ここで，制限写像 $\mathrm{res}_{K_p/k}:\mathrm{Br}(k)\to \mathrm{Br}(K_p)$, $[A]\mapsto [A\otimes K_p]$ を考えると，元の位数は $\mathrm{per}(A\otimes K_p)\mid \mathrm{per}(A)$ より $p\mid \mathrm{per}(A)$ である． □

3.2.2 中心的斜体のプライマリー分解

中心的斜体は，素数べきごとの中心的斜体のテンソル積に同型を除いて一意的に分解される．これを，中心的斜体のプライマリー分解という．この節では，この中心的斜体のプライマリー分解の証明を行う．そのために，1 つ補題を用意しておく．

補題 3.24 D_1, D_2 を k 上の中心的斜体で $\deg(D_1)$, $\deg(D_2)$ は互いに素であるとする．このとき，$D_1\otimes D_2$ も k 上の中心的斜体になる．

証明 $d_1=\deg(D_1)$, $d_2=\deg(D_2)$ とし，$D_1\otimes D_2\simeq \mathrm{M}_n(D)$ (D は k 上の斜体) とする．k 上の斜体 D_3 を $[D_3]=[D_1^\circ]+[D]$ となるものとすると，$D_1^\circ\otimes D\simeq \mathrm{M}_r(D_3)$ となる．すると，命題 2.8 より，$\mathrm{M}_{d_1^2}(D_2)\simeq \mathrm{M}_{d_1^2}(k)\otimes D_2\simeq (D_1^\circ\otimes D_1)\otimes D_2\simeq D_1^\circ\otimes \mathrm{M}_n(D)\simeq \mathrm{M}_{nr}(D_3)$ となる．よって，$d_1^2=nr$ より $n\mid d_1^2$ である．

一方，k 上の斜体 D_4 を $[D_4]=[D_2^\circ]+[D]$ となるものとすると， $D_2^\circ\otimes D\simeq \mathrm{M}_{r'}(D_4)$ となる．すると，上と同様の計算により，$n\mid d_2^2$ である．

よって，d_1 と d_2 は互いに素であるから，$n=1$ であるから $D_1\otimes D_2\simeq D$ となり，$D_1\otimes D_2$ は斜体となる． □

定理 3.25 (中心的斜体のプライマリー分解) D を k 上の中心的斜体，$d=\deg(D)$ とし，d の素因数分解を $d=p_1^{e_1}\dots p_g^{e_g}$ とする．このとき，g 個の中心的斜体 $D_1,\dots,D_g$ が存在して，

$$D\simeq D_1\otimes\cdots\otimes D_g\ (\deg(D_i)=p_i^{e_i})$$

となる．また，上の $D_1,\dots,D_g$ は同型を除き一意的に定まる．

証明 $d=d_1d_2$, d_1, d_2 は互いに素としたとき，k 上の斜体 D_1, D_2 で $D\simeq D_1\otimes D_2$, $\deg(D_1)=d_1$, $\deg(D_2)=d_2$ となるものが同型を除いて一意であることを示せばよい．

d_1, d_2 が互いに素より，$d_1q_1+d_2q_2=1$ となる $q_1,q_2\in\mathbb{Z}$ が存在する．ここで，k 上の斜体 D_1, D_2 を，$d_2q_2[D]=[D_1]$, $d_1q_1[D]=[D_2]$ となるようなものとしてとる．すると，$[D_1\otimes D_2]=[D_1]+[D_2]=(d_1q_1+d_2q_2)[D]=[D]$ で，$\mathrm{ind}(D)=\deg(D)=d$ であるから，命題 3.21 より，$d_1[D_1]=d_1d_2q_2[D]=dq_2[D]=[0]$ である．よって，$\mathrm{per}(D_1)\mid d_1$ である．同様の計算により，$d_2[D_2]=[0]$ より，$\mathrm{per}(D_2)\mid d_2$ である．よって，d_1, d_2 が互いに素より，$\mathrm{per}(D_1)$, $\mathrm{per}(D_2)$ も互いに素である．すると，命題 3.23 より，$\mathrm{ind}(D_1)=\deg(D_1)$, $\mathrm{ind}(D_2)=\deg(D_2)$ も互いに素である．よって，補題 3.24 より $D_1\otimes D_2$ は k 上の斜体であるから，$[D_1\otimes D_2]=[D]$ より $D_1\otimes D_2\simeq D$ であるから存在性は示された．

次に一意性を示そう．$D\simeq D_1\otimes D_2\simeq D_1'\otimes D_2'$ $(\deg(D_1)=\deg(D_1')=d_1, \deg(D_2)=\deg(D_2')=d_2)$ とする．上と同様に，$d_1q_1+d_2q_2=1$ となる $q_1,q_2\in\mathbb{Z}$ をとっておく．すると，$[D_1\otimes D_2]=[D_1'\otimes D_2']$ より，$[D_1]+[D_2]=[D_1']+[D_2']$ である．両辺を d_1 倍すると，$d_1[D_1]=d_1[D_1']=[0]$ より，$d_1[D_2]=d_1[D_2']$ を得る．この両辺を q_1 倍すると，$d_1q_1=1-d_2q_2$, $d_2[D_2]=d_2[D_2']=[0]$ に注意することで，$[D_2]=[D_2']$ を得る．よって，$D_2\simeq D_2'$ である．このことから，$D_1\simeq D_1'$ を得て一意性が示される． □

3.2.3　次数 3 の中心的斜体

一般に，次数 3 の中心的斜体は巡回多元環になることが知られている．この節では，この事実について Haile [Hai89] による証明を紹介する．その際に用いられる事実として，中心的斜体の巡回性を判定するための基本的な定理の 1 つである Albert の巡回性判定法がある．証明は [Alb39, Theorem 11.4] を参照せよ．

定理 3.26 (Albert の巡回性判定法)　D を k 上の素数次 p の中心的斜体とする．このとき，D が巡回多元環であることと，$d \in D \setminus k$ の元で $d^p \in k$ となるものが存在することは同値である．

この定理を用いて，k 上の次数 3 の中心的斜体は巡回多元環になることを示そう．

命題 3.27 ([Hai89, Proposition])　D を k 上の次数 n の中心的斜体とし，K をその極大部分体とする．このとき次が成り立つ．

(1) $d \in D^\times$ の元で，任意の $k \in K$ に対して $\mathrm{Trd}(kd) = 0$ となるものが存在する．

(2) d を (1) をみたすものとする．このとき，K の次元 $n-1$ の部分空間 V で，任意の $v \in V \setminus \{0\}$ に対して $\mathrm{Trd}(v^{-1}d) = \mathrm{Trd}(d^{-1}v) = 0$ となるものが存在する．

とくに，D の $n-1$ 次元部分空間 W で，任意の $w \in W \setminus \{0\}$ に対して $\mathrm{Trd}(w) = \mathrm{Trd}(w^{-1}) = 0$ となるものが存在する．

証明　(1) k 上の線形写像 $U : D \to K^*,\ d \mapsto U(d)$ とする．ここで，$U(d)(k) = \mathrm{Trd}(kd)$ ($d \in D$) である．ここで，$[D : k] > [K : k] = [K^* : k]$ より，$\mathrm{Ker}(U) \setminus \{0\} \neq$ より，$d \in \mathrm{Ker}(U) \setminus \{0\}$ をとればよい．

(2) $d \in D$ を (1) の条件を満たすものとする．k 上の線形写像 $S : K \to k,\ k \mapsto \mathrm{Trd}(d^{-1}k)$ とする．ここで，$v \in \mathrm{Ker}(S) \setminus \{0\}$ とすると，d のとり方から $\mathrm{Trd}(v^{-1}d) = 0$ であり，$v \in \mathrm{Ker}(S)$ より，$\mathrm{Trd}(d^{-1}v) = 0$ となる．$[\mathrm{Ker}(S) : k] \geq n-1$ より，V として $\mathrm{Ker}(S)$ の k 上の $n-1$ 次元部分空間をとればよい．

とくに，$W = d^{-1}V$ とすると，任意の $w \in W$ に対して $\mathrm{Trd}(w) = \mathrm{Trd}(w^{-1}) = 0$ である．　□

これより，3 次の中心的斜体に対して次のことが成り立つ．

命題 3.28 ([Hai89, Corollary 2]) D を k 上の次数 3 の中心的斜体とする．このとき，$d \in D \setminus k$ の元で $d^3 \in k$ となるものが存在する．

証明 命題 3.27 より，D の $n-1$ 次元部分空間 W で，任意の $w \in W \setminus \{0\}$ に対して $\mathrm{Trd}(w) = \mathrm{Trd}(w^{-1}) = 0$ となるものが存在する．$d \in W \setminus k$ をとると，$d \in D^\times$ で $\mathrm{Trd}_D(d) = \mathrm{Trd}_D(d^{-1}) = 0$ となる．この d の k 上の最小多項式は $x^3 - \alpha$ $(\alpha \in k^\times)$ とかけるから，$d^3 \in k$ である． □

Albert の巡回性判定法 (定理 3.26) と命題 3.28 から，次数 3 の中心的斜体は巡回多元環になることがわかった．

3.2.4 次数 4 の中心的斜体

次数が 2 の中心的斜体は四元数環であるから巡回多元環である．また，3.2.3 節より，次数 3 の中心的斜体は巡回多元環になることがわかる．しかし，次数 4 の中心的斜体は一般に巡回多元環になるとは限らないことが知られている．この節では，次数 4 の巡回多元環にならない中心的斜体の例を紹介する．

$k = \mathbb{Q}(u, v)$ を $\mathbb{Q}$ 上の 2 変数有理関数体，$D_1 = \left(\frac{u,-1}{k}\right)$, $D_2 = \left(\frac{-u,v}{k}\right)$, $A = D_1 \otimes D_2$ とする．このとき，A は巡回多元環にならない中心的斜体になる．このことをみてみよう．次のことに注意する．

(a) -1 が k の平方和でかけないとする．このとき，K/k が 4 次巡回拡大ならば，$-1 \notin K^2$ である．

(b) K/k を 4 次巡回拡大とし，$-1 \notin K^2$ とする．このとき，K/k の唯一の 2 次部分体 L とすると，$L \simeq k(\sqrt{s^2 + t^2})$ となる $s, t \in k$ が存在する．

(c) $p = r_1 + \cdots + r_n^2$, $q = s_1^2 + \cdots + r_m^2$ $(r_i, s_i \in Q[u, v] \setminus \{0\})$ とする．このとき，$p \neq 0$, $p \pm uq \neq 0$ であり，$\deg_u(p)$, $\deg_v(p)$, $\deg_v(p \pm uq)$ はどれも偶数である．

(d) $L = k(\sqrt{r^2 + s^2})$ $(r, s \in \mathbb{Q}[u, v])$ で，$r^2 + s^2 \notin k^2$ であれば，$A \otimes L$ は斜体である．

証明 (a), (b), (c) の詳細は [Pie82, 15.7] を参照せよ．ここでは，(d) の証明をする．

Φ_1, Φ_2 をそれぞれ D_1, D_2 に対応する 2 次形式とする．すると，A の Albert form は $\phi(x_1, x_2, x_3, x_4, x_5, x_6) = \Phi_1(x_1, x_2, x_3) - \Phi_2(x_4, x_5, x_6) = -ux_1^2 + x_2^2 - ux_3^2 - ux_4^2 + x_5^2 + uvx_6^2$ となる．

このとき，$A \otimes L$ が斜体であることを示すには，Albert の定理 (定理 3.17) より $\boldsymbol{a} = (a_1, \ldots, a_6)$, $\boldsymbol{b} = (b_1, \ldots, b_6) \in \mathbb{Q}(u, v)^6$ で $\phi(\boldsymbol{a} + \sqrt{r^2+s^2}\boldsymbol{b}) = 0$ ならば，$\boldsymbol{a} = \boldsymbol{b} = (0, \ldots, 0)$ であることを示せばよい．ここで，ϕ は 2 次形式であるから a_i, $b_i \in \mathbb{Q}[u, v]$ としてよい．

$$B(\boldsymbol{a}, \boldsymbol{b}) = \frac{\phi(\boldsymbol{a} + \sqrt{r^2+s^2}\boldsymbol{b}) - \phi(\boldsymbol{a}) - (r^2+s^2)\phi(\boldsymbol{b})}{2\sqrt{r^2+s^2}}$$

とすると，$r^2 + s^2 \notin k^2$ より，$\phi(\boldsymbol{a} + \sqrt{r^2+s^2}\boldsymbol{b}) = \phi(\boldsymbol{a}) + (r^2+s^2)\phi(\boldsymbol{b}) + 2B(\boldsymbol{a}, \boldsymbol{b})\sqrt{r^2+s^2} = 0$ であるから，$\phi(\boldsymbol{a}) + (r^2+s^2)\phi(\boldsymbol{b}) = 0$ である．よって，$up_1^2 - p_2^2 + up_3^2 = -up_4^2 + p_5^2 + uvp_6^2$ $(p_i = a_i^2 + (rb_i)^2 + (rb_i)^2)$ となる．

もし，この両辺が 0 であれば，$p_2 = u(p_1^2 + p_3^2)$ より，両辺の u の次数を比較すると (c) から左辺は偶数，右辺は奇数になる．よって，$p_1 = p_2 = p_3 = 0$ となる．また，$up_4 = v(p_5 + up_6)$ より，両辺の v の次数を比較すると (c) から左辺は偶数，右辺は奇数になる．よって，$p_4 = p_5 = p_6 = 0$ となる．よって，$p_1 = p_2 = p_3 = p_4 = p_5 = p_6 = 0$ となる．

一方，そうでなければ，$v(p_5 + up_6) = u(p_1 + p_3 + p_4) - p_2$ であるから，両辺の v の次数を比較すると (c) から左辺は奇数，右辺は偶数になる．よって，$p_5 = p_6 = 0$ である．すると，$p_2 = u(p_1 + p_3 + p_4)$ より，両辺の u の次数を比較すると (c) から左辺は偶数，右辺は奇数になるから，$p_1 = p_2 = p_3 = p_4 = 0$ となるから，この場合も $p_1 = p_2 = p_3 = p_4 = p_5 = p_6 = 0$ となる．

すると，r, s は 0 ではないから，$a_i = 0$, $b_i = 0$ となる．よって，$\boldsymbol{a} = \boldsymbol{b} = (0, \ldots, 0)$ が得られる．よって，(d) が示された． $\square$

すると，命題 3.19 の (1) と上の (d) から $\mathrm{ind}(A \otimes L) = \deg(A \otimes L) = 4$ であり，$\mathrm{ind}(A) \mid \deg(A) = 4$ である．よって，命題 3.19 の (4) と合わせると，$\mathrm{ind}(A \times L) = 4 \mid \mathrm{ind}(A) \mid \deg(A) = 4$ であるから，$\mathrm{ind}(A) = \deg(A) = 4$ となる．よって命題 3.19 の (1)

から A は斜体である．

次に，A が巡回多元環でないことを証明しよう．

もし，A が巡回多元環であれば，A の極大部分体 K で K/k が 4 次巡回拡大であるものが存在する．すると，上の (a), (b) から，K/k の 2 次部分体 L は $k(\sqrt{r^2+s^2})$ (r, $s \in \mathbb{Q}[u,v]$) と同型である．すると，系 3.20 より，$A \otimes L$ は斜体ではない．しかし，これは (d) に矛盾する．よって，A が巡回多元環でない．

よって，A は巡回多元環にならない中心的斜体となっていることがわかった．

4　種々の問題と今後の研究課題

4.1　種々の問題

本節では中心的単純環におけるいくつかの問題についての紹介を行う．この節の内容は [渡部], [ABGV11] を参考にした．

4.1.1　中心的斜体に関する問題

この節では中心的斜体に関する問題と，それについて知られている結果について紹介する．定理 2.52 より，任意の k 上の中心的斜体は接合積とブラウアー同値になることがわかる．そこで，自然に次のような問題が生じる．

問題 1　任意の k 上の中心的斜体は接合積になるか？

この問題について知られている結果をまとめておく．

(i) $\deg(D) = 2$ の場合は，定義より D は巡回多元環であるから，接合積である．

(ii) $\deg(D) = 3$ の場合は，3.2.3 節で巡回多元環になることがわかっているから，接合積である．

ここで，1 つ巡回多元環に関する一般的な結果を紹介しておく．証明に関しては [Pie82, 15.3] を参照せよ．

命題 4.1　D を k 上の中心的斜体とし，$D \simeq D_1 \otimes \cdots \otimes D_g$ を中心的斜体のプライマリー

分解 (定理 3.25) とする．このとき，D が巡回多元環であることと，各 D_i $(i=1,\ldots,g)$ が巡回多元環であることは同値である．

すると，この命題から $\deg(D)=6$ の場合も巡回多元環であることがわかり，接合積になる．

(iii) $\deg(D)=4$ の場合は，3.2.4 節で一般に巡回多元環にはならないことを示したが，任意の次数 4 の中心的斜体が接合積になることが [Alb39] により得られている．

また，接合積に関して次のことが知られている．詳細は [ABGV11, Section 0] を参照せよ．

命題 4.2 A を k 上の中心的単純環とする．このとき，A が接合積であれば，$\mathrm{M}_n(A)$ も接合積である．また，A が巡回多元環であれば，$\mathrm{M}_n(A)$ も巡回多元環である．

すると，次数が 3, 4 の中心的斜体は接合積であることと，定理 2.50 に注意すると，上の命題から $\deg(D)=12$ の場合も接合積であることがわかる．

よって，次の結果がわかる．

定理 4.3 D を k 上の中心的斜体としたとき，$\deg(D)=2,3,4,6,12$ であれば，D は接合積である．

しかし，Amitsur [Ami72] により，問題 1 が否定的であるような例がはじめて構成された．

問題 1 に関連する問題として，次の問題が挙げられる．

問題 2 任意の次数 n の k 上の中心的斜体は巡回多元環になるか？

上で述べたように，$n=2,3$ の場合はこの問題は肯定的であるが，$n=4$ のときは否定的である．しかし，$n\geq 5$ の場合は一般に現在未解決である．この問題に関しては著者も興味をもっている．この問題に関するさらなる詳細は 4.2 節を参照せよ．

次に，中心的斜体の分解に関する問題を挙げる．

定義 D を k 上の中心的斜体とする．このとき，D が**分解可能** (decomposable) であると

は，$D \simeq D_1 \otimes D_2$ となる k 上の斜体 $D_1 \neq k$, $D_2 \neq k$ が存在するときをいう．

中心的斜体のプライマリー分解 (定理 3.25) により，D が分解可能でないとすると，$\mathrm{Deg}(D)$ は素数のべきでなくてはならない．そこで，次のような問題が生じる．

問題 3 p を素数としたとき，次数が p^n の分解可能でない中心的斜体は存在するか？

この問題関しては，次の結果が知られている．

定理 4.4 ([Alb32]) D を k 上の中心的斜体とし，$\mathrm{per}(D) = 2$, $\deg(D) = 4$ とする．このとき，分解可能である．

定理 4.5 ([Jac91]) D を k 上の中心的斜体で $\mathrm{per}(D) = p$, $\deg(D) = p^n$ (ただし，$p = 2$, $n = 2$ を除く) で分解可能でないものが存在する．

4.1.2 インデックスとピリオドに関する問題

この節ではインデックスとピリオドに関する問題と，それについて知られている結果について紹介する．A を k 上の中心的単純環としたとき，インデックスとピリオドの基本的な性質として，命題 3.21 から $\mathrm{per}(A) \mid \mathrm{ind}(A)$ であり，命題 3.23 より，$\mathrm{per}(A)$ と $\mathrm{ind}(A)$ は同じ素因子をもつという事実があった．これから，ブラウアー次元というものが定義される．定義は以下の通りである．

定義 体 k に対し，**ブラウアー次元** (Brauer dimension) を $\mathrm{Br.dim}(k) = \min\{n \in \mathbb{Z} \mid$ 任意の k 上の中心的単純環 A に対し $\mathrm{ind}(A) \mid \mathrm{per}(A)^n$ が成り立つ $\}$ と定義する．最小値が存在しないとき，$\mathrm{Br.dim}(k) = \infty$ と定める．

定義からわかることとして $\mathrm{Br}(k) = \{0\}$ であれば，$\mathrm{Br.dim}(k) = 0$ である．また，$\mathrm{Br.dim}(k) = 1$ であることは，任意の k 上の中心的単純環 A に対し，$\mathrm{ind}(A) = \mathrm{per}(A)$ であることは同値である．すると，ブラウアー次元に対して次のような問題が生じる．

問題 4 体 k に対し，$\mathrm{Br.dim}(k)$ を決定せよ．

この問題については，次のことが知られている．

定理 4.6 体 k が代数体であれば，$\mathrm{Br.dim}(k) = 1$ である．

この結果は Albert-Brauer-Hasse-Noether の定理から得られることが知られている．詳細は，[Pie82, 18.5, 18.6] を参照せよ．

定理 4.7 ([Jon04]) 体 k が代数閉体上有限生成である超越次数 2 の拡大体であれば，$\mathrm{Br.dim}(k) = 1$ である．

定理 4.8 ([Lie15]) 体 k が有限体上の超越次数 2 の拡大体であれば，$\mathrm{Br.dim}(k) = 2$ である．

4.2 今後の研究課題

本節では，特に著者が現在興味を持っている問題についての紹介と，今度の展望について述べる．

4.2.1 中心的斜体の巡回性の問題

著者が興味を持っている問題の 1 つとして，上で挙げた問題 2 が挙げられる．問題を再掲しておく．

問題 2 (再掲, p. 63) 任意の次数 n 次の k 上の中心的斜体は巡回多元環にになるか？

この問題に対する有名な結果として，Rowen と Saltman [RS82] により次の結果が得られている．

定理 4.9 ([RS82, Theorem 1]) n を奇数とし，$k \ni \zeta_n$ (ζ_n は 1 の原始 n 乗根) とし，D を k 上の中心的斜体とする．このとき，D が，ガロア群が二面体群 D_n のガロア拡大で分解していれば，D は巡回多元環である．

この定理の証明の方針を簡単に紹介する．仮定より基礎体 k は 1 の n 乗根を含んでい

るから，n 乗して初めて k にはいるような D の元 $x \in D \setminus k$ が存在することが示せれば，クンマー理論により D の部分体 $k(x)$ は k 上の n 次巡回拡大である．よって，命題 2.45 より D は巡回拡大になることがわかる．

今後の研究課題として，この定理 4.9 の基礎体 k が 1 の n 乗根を含んでいるという仮定を緩められないかという問題について考えている．

F として 1 のべき根をまったく含まない体とし $k' = F(\zeta_n + \zeta_n^{-1})$ とすると，$[F(\zeta_n) : F(\zeta_n + \zeta_n^{-1})] = 2$ となる．定理 4.9 では，基礎体が $k = F(\zeta_n)$ 上で考えているとみることができる．最終目標としては基礎体 k を 1 のべき根をまったく含まない体 F まで下げたいと考えている．その最初の段階として，基礎体 k を 2 次下の体である k' に下げた体において定理 4.9 と同様の結果が得られないかを考察している．

4.2.2　中心的斜体の同型問題

体 k のブラウアー群の各類の代表元として，k 上の中心的斜体をとることができた．すると，2 つの次数 n の中心的斜体 D_1, D_2 が与えられてとき，命題 2.18 より，それらが k 上の多元環として同型であることと，それらが k 上のブラウアー群の元として同じ類に属することが同値であることがわかる．すると，ブラウアー群の元を考察する上で，自然に次の問題を考えることができる．

問題 5　*次数 n の k 上の中心的斜体 D_1, D_2 が与えられてとき，D_1 と D_2 が同型かどうかを D_1, D_2 の情報を使って判定できるか？*

そこで，一般に n の k 上の中心的斜体 D に対して，命題 2.23 より，D の部分体 K に対して，K が D の極大部分体であることと，K が D の分解体であることは同値である．すると，D の極大部分体 K は D の部分体の中での分解体となるから，K は D の構造に関する情報をもっていることが予想できる．そこで，著者は次の予想が成り立つのではないかと考えた．

予想　*次数 n の k 上の中心的斜体 D_1, D_2 が与えられてとき，D_1 と D_2 が同型であることと，D_1, D_2 が同じ極大部分体の族をもつことが同値である．*

D_1 と D_2 が同型であることと，D_1, D_2 が同じ極大部分体の族をもつことはよい．そこで，問題は D_1, D_2 が同じ極大部分体の族をもてば，D_1 と D_2 が同型であることがいえるかである．この予想に関して知られている結果をまとめておく．

(i) $n = 2$ の場合，体 k が代数体であるときは肯定的であることが，Albert-Brauer-Hasse-Noether の定理から得られることが知られている．しかし，一般の体 k に対しては否定的であることが知られている．

(ii) $n \geq 3$ の場合は，体 k が代数体であっても否定的であることが知られている．

これらの結果の詳細は [CRR15] を参照せよ．

そこで，この予想が成り立たない原因の 1 つとして，D を n (> 1) 次の k 上の中心的斜体とすると，D の逆多元環 D° は D と同じ極大部分体の族をもつことが挙げられる．このことから，もし予想が肯定的だとすると，$D \simeq D^\circ$ であり，このことから，とくに D° と D はブラウアー同値であるから $[D] = [D^\circ]$ でなくてはならず，これより $2[D] = [0]$ である．よって，予想が肯定的であるとすると $\mathrm{per}(D) = 2$ でなくてはならないことがわかる．

このことから，今後の研究課題として $\mathrm{per}(D) = 2$ の k 上の中心的斜体に対して，上で挙げた予想が成り立つのかどうかを研究していきたい．

参考文献

[斉藤] 斉藤秀司，整数論，共立出版，1997.

[渡部] 渡部隆夫，中心的単純多元環．以下より入手可能．
http://www.math.sci.osaka-u.ac.jp/~twatanabe/algebra.pdf

[Alb32] A. A. Albert, *Normal division algebras of degree four over an algebraic field*, Trans. Amer. Math. Soc. **34** (1932) 363–372.

[Alb39] A. A. Albert, *Structure of algebras*, American Mathematical Society, 1939.

[Ami72] S. A. Amitsur, *On central division algebras*, Israel J. Math. **12** (1972) 408–420.

[ABGV11] A. Auel, E. Brussel, S. Garibaldi, U. Vishne, *Open problems on central simple algebras*, Transform. Groups **16** (2011) 219–264.

[CRR15] V. I. Chernousov, A. S. Rapinchuk, I. A. Rapinchuk, *Division algebras with the same maximal subfields*, Russian Math. Surveys **70** (2015) 83–112.

[Cla] P. L. Clark, *Noncommutative algebra.* 以下より入手可能．
http://math.uga.edu/~pete/noncommutativealgebra.pdf

[Dra83] P. K. Draxl, *Skew fields*, Cambridge University Press, 1983.

[FD93] B. Farb, R. K. Dennis, *Noncommutative algebra*, Springer-Verlag, 1993.

[GS06] P. Gille, T. Szamuely, *Central simple algebra and Galois cohomology*, Cambridge University Press, 2006.

[Hai89] D. Haile, *A useful proposition for division algebras of small degree*, Proc. Amer. Math. Soc. **106** (1989) 317–319.

[Jac91] B. Jacob, *Indecomposable division algebras of prime exponent*, J. Reine Angew. Math. **413** (1991) 181–197.

[Jon04] A. J. de Jong, *The period-index problem for the Brauer group of an algebraic surface*, Duke Math. J. **123** (2004) 71–94.

[Lam05] T. Y. Lam, *Introduction to quadratic forms over fields*, American Mathematical Socirty, 2005.

[Lie15] M. Lieblich, *The period-index problem for fields of transcendence degree* 2, Ann. of Math. (2) **182** (2015) 391–427.

[Pie82] R. S. Pierce, *Associative algebras*, Springer-Verlag, 1982.

[RS82] L. H. Rowen, D. J. Saltman, *Dihedral algebras are cyclic*, Proc. Amer. Math. Soc. **84** (1982) 162–164.

[Ser79] J-P. Serre, *Local fields*, Springer-Verlag, 1979.

[Ten] E. Tengan, *Central simple algebras and the Brauer group.* 以下より入手可能. http: //conteudo.icmc.usp.br/pessoas/etengan/algebra/arquivos/cft.pdf