有理数体上の四元数環

2019 年度 代数学 5・整数論概論 II 講義ノート

渡部隆夫

内容 有理数体上の四元数環の分類を行う.

文献

1 J. W. S. Cassels, Rational Quadratic Forms, Dover, 1978.

2 P. Gille and T. Szamuely, Central Simple Algebras and Galois Cohomology, Second Ed. , Cambridge Univ. Press, 2017.

3 Y. Kitaoka, Arithmetic of Quadratic Forms, Cambridge Univ. Press, 1993.

4 G. Shimura, Arithmetic of Quadratic Forms, Springer, 2010.

5 J. Voight, Quaternion Algebras, `https://math.dartmouth.edu/~jvoight/quat.html`, 2018.

6 A. Weil, Basic Number Theory, Third Ed., Springer, 1974.

記号

$\mathbf{Z}$: 整数全体, $\mathbf{Q}$: 有理数全体, $\mathbf{R}$: 実数全体, $\mathbf{C}$: 複素数全体

R を環とするとき

$\mathrm{M}_{m,n}(R)$: R を成分にもつ (m,n) 行列の全体

$R^m = \mathrm{M}_{m,1}(R)$: R に成分をもつ m 次元列ベクトル全体

$\mathrm{M}_n(R) = \mathrm{M}_{n,n}(R)$: R に成分をもつ n 次正方行列全体

目 次

1　体の対合

Def　集合 R 上に 2 つの演算

$$(\text{和})\ R\times R\longrightarrow R:(a,b)\mapsto a+b \qquad (\text{積})\ R\times R\longrightarrow R:(a,b)\mapsto ab$$

が定義されていて, 以下をみたすときに R を **単位的環** または単に **環** (ring) という.

(R1) R は和についてアーベル群になる.

(R2) $^\forall a,b,c\in R$ について $a(bc)=(ab)c$.

(R3) $^\exists e\in R$ s.t. $^\forall a\in R$ について $ae=ea=a$.

(R4) $^\forall a,b,c\in R$ について, $a(b+c)=ab+ac,\quad (a+b)c=ac+bc$.

さらに積の交換法則 $ab=ba$, $(^\forall a,b\in R)$ が成り立つとき, R を **可換環** という.

Def　R を環とする. $0\neq a\in R$ が

$$^\exists x\in R\ \text{ s.t. }\ ax=xa=e$$

を満たすとき, a を **可逆元** または **単元** という. x を a の逆元といい, a^{-1} と表す. R の単元全体の集合を $R^\times$ と表し R の**単数群** (unit group) という.

例　R を可換環, $n\geq 2$ とするとき, $\mathrm{M}_n(R)$ は行列の和と積により非可換環になる.

$$a\in \mathrm{M}_n(R)^\times \iff a \text{ は逆行列 } a^{-1} \text{ をもち, かつ } a^{-1}\in \mathrm{M}_n(R) \iff \det a\in R^\times$$

$\mathrm{M}_n(R)^\times$ を $\mathrm{GL}_n(R)$ と表す.

Def　R が環で $R^\times=R-\{0\}$ を満たすとき, R を **斜体** (skew field) という. とくに R が可換環のときは **体** (field) という.

例
(1) $\mathbf{Q},\mathbf{R},\mathbf{C}$ は体. p を素数とするとき $\mathbf{F}_p=\mathbf{Z}/p\mathbf{Z}$ は体.
(2) $0\neq\xi\in\mathbf{C}$ で $\xi\notin\mathbf{Q},\xi^2\in\mathbf{Q}$ となる ξ を固定する. このとき

$$\mathbf{Q}(\xi)=\{a+b\xi\ :\ a,b\in\mathbf{Q}\}$$

は体である. $\xi\in\mathbf{R}$ $(\xi\notin\mathbf{R})$ のとき実 2 次体 (虚 2 次体) という.

以下 K を体, $\mathrm{ch}(K)\neq 2$ (すなわち $\mathbf{F}_2\not\subset K$) を仮定する.

Def　写像 $\rho : K \longrightarrow K$ が 2 条件

(I1) $\rho(a+b) = \rho(a) + \rho(b), \quad \rho(ab) = \rho(a)\rho(b) \qquad ({}^{\forall}a, b \in K)$

(I2) $\rho \neq \mathrm{id}_K$, $\rho^2 = \rho \circ \rho = \mathrm{id}_K$. ($\mathrm{id}_K$ は K の恒等写像.)

を満たすとき, K の対合 (involution) という. 対合は全単射で $\rho^{-1} = \rho$ である.

例
(1) 複素共役 $\mathbf{C} \longrightarrow \mathbf{C} : z \mapsto \bar{z}$ は対合である.
(2) $\xi \in \mathbf{C}$ を, $\xi \notin \mathbf{Q}$, $\xi^2 \in \mathbf{Q}$ とする. $\mathbf{Q}(\xi) = \{a + b\xi \ : \ a, b \in \mathbf{Q}\}$ に対し

$$\rho : \mathbf{Q}(\xi) \longrightarrow \mathbf{Q}(\xi) : a + b\xi \mapsto a - b\xi$$

は対合である.

Lemma 1

$\rho : K \longrightarrow K$ を対合として,

$$F = K^{\rho} = \{a \in K \ : \ \rho(a) = a\}$$

とする. このとき
(1) F は体である.
(2) K の元 $\xi \neq 0$ で $\rho(\xi) = -\xi$ となるものが存在し, K は $1, \xi$ を基底とする 2 次元 F ベクトル空間になる. また $\xi^2 \in F$ である.

証明 (1) は容易. (2) $\rho \neq \mathrm{id}_K$ だから $b \in K, b \notin F$ がとれる. $\xi = b - \rho(b) \neq 0$ とおけば $\rho(\xi) = -\xi$. 残りは容易. □

Def　$E \subset K$ を部分集合とする. E 自身が K の和と積により体になるとき, E を K の部分体という. このとき

$$E \times K \longrightarrow K : (\lambda, a) \mapsto \lambda a$$

をスカラー倍とみることにより, K は E 上のベクトル空間になる.

$$[K : E] = \dim_E K$$

とおいて, これを拡大次数とよぶ. とくに $n = [K : E] < \infty$ のとき, K を E の n 次拡大という. また F, E が共に K の部分体で, $F \subset E \subset K$ であるとき, E を F と K の中間体という. このとき

$$[K : F] = [K : E][E : F]$$

が成り立つ.

例
(1) $\mathbf{C}$ は $\mathbf{R}$ の 2 次拡大.
(2) $\mathbf{Q}(\xi)$ が $\mathbf{Q}$ の実または虚 2 次体ならば, $\mathbf{Q}(\xi)$ は $\mathbf{Q}$ の 2 次拡大
(3) $\rho : K \longrightarrow K$ が対合ならば, K は $F = K^\rho$ の 2 次拡大

Lemma 2

$E \subset K$ を部分体で $[K : E] = 2$ とする. このとき

$$^\exists\rho : K \longrightarrow K \text{ 対合 } s.t.\ K^\rho = E$$

このような ρ は一意である.

証明 $\xi \in K, \xi \notin E$ をとる. このとき $1, \xi$ は K の E 上の基底になる. したがって

$$\xi^2 = p + q\xi, \qquad (p, q \in E)$$

と書ける. ξ は 2 次方程式 $X^2 - pX - q = 0$ の一つの解であるから

$$X^2 - pX - q = (X - \xi)(X - \xi')$$

と分解され, $\xi' = -q\xi^{-1} \in K$ となる. そこで

$$\rho : K \longrightarrow K : \rho(a + b\xi) = a + b\xi'$$

と定義すれば, これは対合になる.
(一意性): ρ_1 がもう一つの対合で $K^{\rho_1} = E$ を満たすとする. $\rho_1(\xi) = \eta$ とおく. このとき

$$\eta^2 = \rho_1(\xi^2) = \rho_1(p + q\xi) = p + q\rho_1(\xi) = p + q\eta$$

だから, $\eta = \xi, \xi'$. $\eta = \xi$ ならば $\rho_1 = \mathrm{id}_K$ となってしまうので, $\eta = \xi'$. よって $\rho_1 = \rho$. □

例
(1) $\mathbf{Q}$ の部分体は $\mathbf{Q}$ 自身しかないので, $\mathbf{Q}$ は対合を持たない.
(2) 同様に $\mathbf{R}$, $\mathbf{F}_p$ も対合を持たない.
(3) $\mathbf{C}$ は無限個の対合をもつ.
(4) $0 \neq p, q \in \mathbf{Z}$ を異なる素数とする.

$$K = \{a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq} \ : \ a, b, c, d \in \mathbf{Q}\} \subset \mathbf{R}$$

とけば K は $\mathbf{Q}$ の拡大体で $[K : \mathbf{Q}] = 4$ である. K は 3 個の自明でない部分体をもつ.

$$F_1 = \mathbf{Q}(\sqrt{p}), \qquad F_2 = \mathbf{Q}(\sqrt{q}), \qquad F_3 = \mathbf{Q}(\sqrt{pq})$$

それぞれに対応する K の対合 ρ_1, ρ_2, ρ_3 があって $K^{\rho_i} = F_i$ を満たす.

2　四元数環

K を体, $\mathrm{ch}(K) \neq 2$ とする.
対合 $\rho : K \longrightarrow K$ を固定して, $F = K^{\rho}$ とする.

Def　$\beta \in F^{\times}$ を固定して, $\mathrm{M}_2(K)$ の部分集合 D を

$$D = D(K, \beta) = \left\{ \begin{pmatrix} a & b \\ \beta\rho(b) & \rho(a) \end{pmatrix} : a, b \in K \right\}$$

とおく. この D を四元数環 (quaternion algebra) という.

Lemma 3

$\rho(\xi) = -\xi$ となる $\xi \in K^{\times}$ を固定し, $\alpha = \xi^2 \in F^{\times}$ とおき, D の元

$$e_0 = I_2, \qquad e_1 = \begin{pmatrix} \xi & 0 \\ 0 & -\xi \end{pmatrix}, \qquad e_2 = \begin{pmatrix} 0 & 1 \\ \beta & 0 \end{pmatrix}, \qquad e_3 = e_1 e_2 = \begin{pmatrix} 0 & \xi \\ -\beta\xi & 0 \end{pmatrix}$$

をとる.
(1) D は e_0, e_1, e_2, e_3 を基底にもつ **4** 次元 F ベクトル空間である.
(2) D は行列の和と積により環になる. とくに e_0 は積の単位元で

$$e_1^2 = \alpha e_0, \quad e_2^2 = \beta e_0, \quad e_3^2 = -\alpha\beta e_0, \quad e_i e_j = -e_j e_i \ \ (i \neq j, i, j = 1, 2, 3)$$

(3) $a \in K$ に対し, 対応 $a \mapsto \mathrm{diag}(a, \rho(a)) \in D$ により $K \subset D$ とみなす. このとき

$$D = Ke_0 + Ke_2, \qquad ae_2 = e_2\rho(a) \ \ (^{\forall} a \in K)$$

であり, D は e_0, e_2 を基底にもつ **2** 次元 K ベクトル空間である.
(4) $X \in D$ について, $XY = YX \ \ ^{\forall} Y \in D \iff X = ae_0 \ \ a \in F$.

(証明は行列の計算により容易)

例
$K = \mathbf{C}$, $\rho(z) = \overline{z}$ とする. $F = \mathbf{R}$ である. $\xi = \sqrt{-1}$ にとれて, $\alpha = -1$. $\beta = -1$ とすると

$$\mathbf{H} = D(\mathbf{C}, -1) = \mathbf{R}e_0 + \mathbf{R}e_1 + \mathbf{R}e_2 + \mathbf{R}e_3, \qquad \begin{array}{c} e_3 = e_1 e_2, \ e_i^2 = e_2^2 = e_3^2 = -e_0 \\ e_i e_j = -e_j e_i \ \ (i \neq j, i, j = 1, 2, 3) \end{array}$$

をハミルトン四元数体という. $\mathbf{H}$ は斜体である. 実際

$$X = \begin{pmatrix} x & y \\ -\overline{y} & \overline{x} \end{pmatrix} \neq 0 \ \text{ に対し } \ X^{-1} = \frac{1}{|x|^2 + |y|^2} \begin{pmatrix} \overline{x} & -y \\ \overline{y} & x \end{pmatrix} \in D$$

3　多元環

Def　F を体として, V を F ベクトル空間とする. V に積

$$V \times V \longrightarrow V : (u, v) \mapsto uv$$

が定義されていて, 次を満たすとき V を F-多元環 (F-algebra) という.

(AL1) V は積の単位元 1_V をもち, 積とベクトル空間の和により環になる.

(AL2) $^\forall a, b \in F, {}^\forall u, v \in V$ に対し, $(au)(bv) = abuv$.

このとき $F \longrightarrow V : a \mapsto a1_V$ は単射なので, F と $F1_V$ を同一視して $F \subset V$ とみなす.

例
(1) $\mathrm{M}_n(F)$ は有限次元 F-多元環である.
(2) 1 変数多項式環 $F[X]$ は無限次元 F-多元環である.
(3) $D(K, \beta)$ は, $F = K^p$ とすると 4 次元 F-多元環である. K-多元環ではない.
(4) $V = Fu_0 + Fu_1 + Fu_2 + Fu_3$ を u_0, u_1, u_2, u_3 を基底にもつ 4 次元ベクトル空間とする. $0 \neq \alpha, \beta \in F$ を固定する. u_i の間の積を

- $u_0^2 = u_0, \quad u_0u_i = u_iu_0 \ \ (i = 1, 2, 3)$
- $u_1^2 = \alpha, \quad u_2^2 = \beta, \quad u_1u_2 = -u_2u_1 = u_3$
  (上の二つから, $u_3^2 = -\alpha\beta, \quad u_1u_3 = -u_3u_1 = \alpha u_2, \quad u_2u_3 = -u_3u_2 = -\beta u_1$)

により定義する. これから, V の任意の元の積を

$$\left(\sum_{i=0}^{3} a_iu_i\right)\left(\sum_{j=0}^{3} b_ju_j\right) = \sum_{i,j=0}^{3} a_ib_ju_iu_j \qquad (a_i, b_j \in F)$$

と定義することにより, V は F-多元環になる. $V = (\alpha, \beta)_F$ と表す.

Def　V と W を F-多元環とする. 写像 $f : V \longrightarrow W$ が,

- F-線形で $f(1_V) = 1_W$
- $f(uv) = f(u)f(v) \quad ({}^\forall u, v \in V)$

を満たすとき, f を (F-多元環の) 準同型写像という. さらに, 全単射であるとき, f を同型写像という. V と W の間に同型写像が存在するとき, V と W は (F-多元環として) 同型であるといい, $V \cong W$ と表す.

例

(1) $\mathbf{H} = D(\mathbf{C}, -1) = \mathbf{C}e_0 + \mathbf{C}e_2$ とする. $0 < \theta \in \mathbf{R}$ をとり

$$D(\mathbf{C}, -\theta) = \mathbf{C}e'_0 + \mathbf{C}e'_2, \qquad e'^2_2 = -\theta e'_0$$

とする. このとき, 写像

$$g : D(\mathbf{C}, -\theta) \longrightarrow D(\mathbf{C}, -1) : ae'_0 + be'_2 \mapsto ae_0 + b\sqrt{\theta}e_2$$

は $\mathbf{R}$ 線形同型写像で,

$$g(XY) = g(X)g(Y) \qquad ({}^\forall X, Y \in D(\mathbf{C}, -\theta))$$

が成り立つ. つまり $D(\mathbf{C}, -\theta) \cong D(\mathbf{C}, -1)$.

(2) $(\alpha, \beta)_F \cong (\beta, \alpha)_F$

(3) $\alpha, \beta, p, q \in F^\times$ とするとき $(\alpha, \beta)_F \cong (\alpha p^2, \beta q^2)_F$. (練習問題)

(4) 任意の $\alpha \in F^\times$ に対し $(\alpha, 1)_F \cong (1, \alpha)_F \cong \mathrm{M}_2(F)$. (練習問題)

(5) $D(K, \beta)$ で $F = K^\rho$, $K = F + F\xi$, $\rho(\xi) = -\xi$, $\xi^2 = \alpha \in F$ とする. このとき

$$D(K, \beta) \cong (\alpha, \beta)_F : e_i \longleftrightarrow u_i$$

(6) 逆に $(\alpha, \beta)_F$ に対し, $\xi = \sqrt{\alpha} \notin F$ とする. $K = F(\xi) = F + F\xi$ は体になり, $\rho(a + b\xi) = a - b\xi$ は K の対合で $K^\rho = F$. これにより

$$(\alpha, \beta)_F \cong D(K, \beta)$$

(7) (5), (6) により, $(\alpha, \beta)_F$ の全体は $D(K, \beta)$ の全体を含むとみてよい. $(\alpha, \beta)_F$ も四元数環という. (一般四元数環 (generalized quaternion) ということもある.)

(8) (3) ,(4), (5) より

$$D(K, \beta) \cong D(K, \beta q^2) \qquad ({}^\forall q \in F^\times), \qquad D(K, 1) \cong \mathrm{M}_2(F)$$

(9) $F = \mathbf{R}$ のとき (1), (3), (4), (8) より

$$D(\mathbf{C}, \beta) \cong \begin{cases} \mathrm{M}_2(\mathbf{R}) & (\beta > 0) \\ \mathbf{H} & (\beta < 0) \end{cases}, \qquad (\alpha, \beta)_{\mathbf{R}} \cong \begin{cases} \mathrm{M}_2(\mathbf{R}) & (\alpha > 0 \text{ または } \beta > 0) \\ \mathbf{H} & (\alpha < 0 \text{ かつ } \beta < 0) \end{cases}$$

(10) $F = \mathbf{C}$ のときは

$$(\alpha, \beta)_{\mathbf{C}} \cong \mathrm{M}_2(\mathbf{C}) \qquad ({}^\forall \alpha, \beta \in \mathbf{C}^\times)$$

4　四元数環のノルムとトレース

F を体, $\mathrm{ch}(F) \neq 2$ として

$$\alpha, \beta \in F^\times, \quad \xi = \sqrt{\alpha} \notin F, \quad K = F + F\xi, \quad K^\rho = F$$

とする. このとき

$$D(K, \beta) \cong (\alpha, \beta)_F = Fu_0 + Fu_1 + Fu_2 + Fu_3 \qquad (u_0 = 1,\ u_1^2 = \alpha,\ u_2^2 = \beta,\ u_3 = u_1u_2)$$

Def　$v = a_0u_0 + a_1u_1 + a_2u_2 + a_3u_3$ $(a_i \in F)$ に対し,

$$v^\iota = a_0u_0 - a_1u_1 - a_2u_2 - a_3u_3$$

を v の**共役**という. また

$$N(v) = vv^\iota = v^\iota v = a_0^2 - \alpha a_1^2 - \beta a_2^2 + \alpha\beta a_3^2 \in F$$

を v の**ノルム**,

$$T(v) = v + v^\iota = 2a_0 \in F$$

を v の**トレース**という.

注　$v \in D(K, \beta)$ とみて

$$v = \begin{pmatrix} s & t \\ \beta\rho(t) & \rho(s) \end{pmatrix}, \qquad s = a_0 + a_1\xi,\ t = a_2 + a_3\xi \in K$$

と表示した場合,

$$v^\iota = \begin{pmatrix} s & t \\ \beta\rho(t) & \rho(s) \end{pmatrix}^\iota = \begin{pmatrix} \rho(s) & -t \\ -\beta\rho(t) & s \end{pmatrix}$$

である. そして

$$N(v) = (\det v)I_2, \qquad T(v) = (s + \rho(s))I_2 = \mathrm{Tr}(v)I_2$$

となる.

Lemma 4

$\forall v, w \in (\alpha, \beta)_F$ に対し

(1) $(v^\iota)^\iota = v, \qquad (vw)^\iota = w^\iota v^\iota$

(2) $N(vw) = N(v)N(w)$

(3) v が単元 $\iff N(v) \neq 0$. このとき $v^{-1} = N(v)^{-1}v^\iota$ である.

証明 (1) は直接の計算. (2) は注 から明らか.
(3) v が単元ならば $v^{-1} \in (\alpha,\beta)_F$ が存在して, $vv^{-1} = 1$. よって $1 = N(1) = N(vv^{-1}) = N(v)N(v^{-1})$ から $N(v) \neq 0$. 逆に $N(v) \neq 0$ ならば $v^{-1} = N(v)^{-1}v^{\iota}$ である. □

定理 1

$D = (\alpha,\beta)_F$ に対し, 以下の 4 条件は互いに同値である.

(SQ1) $D \cong \mathrm{M}_2(F)$

(SQ2) D は斜体ではない

(SQ3) $0 \neq {}^{\exists}v \in D$ *s.t.* $N(v) = 0$

(SQ4) ${}^{\exists}z \in K = F(\sqrt{\alpha})$ *s.t.* $\beta = z\rho(z)$

とくに $D \ncong \mathrm{M}_2(F)$ である四元数環は斜体である.

証明 (SQ1) $\Longrightarrow$ (SQ2) は自明. (SQ2) $\Longrightarrow$ (SQ3) は Lemma 4 (3) から容易.
(SQ3) $\Longrightarrow$ (SQ4) : $N(v) = 0$ となる $v \neq 0$ を

$$v = a_0u_0 + a_1u_1 + a_2u_2 + a_3u_3$$

とする. もし $a_2 = a_3 = 0$ ならば $v \in K$ で $N(v) = v\rho(v) = 0$ となるから, $v = 0$ で矛盾. よって $a_2 \neq 0$ または $a_3 \neq 0$. このとき

$$0 = N(v) = a_0^2 - \alpha a_1^2 - \beta(a_2^2 - \alpha a_3^2), \qquad \beta = \frac{a_0^2 - \alpha a_1^2}{a_2^2 - \alpha a_3^2} = z\rho(z), \qquad z = \frac{a_0 + a_1\sqrt{\alpha}}{a_2 + a_3\sqrt{\alpha}}$$

(SQ4) $\Longrightarrow$ (SQ1) : $\beta = z\rho(z)$ とすると, $\beta^{-1} = z^{-1}\rho(z^{-1})$. そこで $z^{-1} = a + b\sqrt{\alpha}$ とする. $w_1 = au_2 + bu_3$ とおけば,

$$w_1^2 = \beta a^2 - \alpha\beta b^2 = \beta(a^2 - \alpha b^2) = \beta z^{-1}\rho(z^{-1}) = 1$$

また $w_1u_1 = -u_1w_1$. これから

$$w_2 = (1 + \alpha)u_1 + (1 - \alpha)w_1u_1$$

とおけば

$$w_1w_2 = (1 + \alpha)w_1u_1 + (1 - \alpha)u_1 = -w_2w_1 \quad \text{かつ} \quad w_2^2 = (1 + \alpha)^2\alpha - (1 - \alpha)^2\alpha = 4\alpha^2$$

これにより

$$D = Fu_0 + Fw_1 + Fw_2 + Fw_1w_2, \qquad w_1^2 = 1,\ \ w_2^2 = 4\alpha^2,\ \ w_1w_2 = -w_2w_1$$

だから

$$D \cong (1, 4\alpha^2)_F \cong \mathrm{M}_2(F)$$

□

5　回転群とハミルトン四元数体

$K = \mathbf{R}, \mathbf{C}$ とする. $X = (x_{ij}) \in \mathrm{M}_{m,n}(K)$ に対し

$$X^* = {}^t\overline{X} = \begin{cases} {}^tX & (K = \mathbf{R}) \\ {}^t\overline{X} = {}^t(\overline{x}_{ij}) & (K = \mathbf{C}) \end{cases}$$

と定める.

$$\mathrm{U}_n(K) = \{A \in \mathrm{GL}_n(K) \ : \ AA^* = I_n\} = \begin{cases} \mathrm{O}_n(\mathbf{R}) & (K = \mathbf{R}) \text{ 直交群} \\ \mathrm{U}_n(\mathbf{C}) & (K = \mathbf{C}) \text{ ユニタリ群} \end{cases}$$

$$\mathrm{SU}_n(K) = \{A \in \mathrm{U}_n(K) \ : \ \det A = 1\} = \begin{cases} \mathrm{SO}_n(\mathbf{R}) & (K = \mathbf{R}) \text{ 特殊直交群} \\ \mathrm{SU}_n(\mathbf{C}) & (K = \mathbf{C}) \text{ 特殊ユニタリ群} \end{cases}$$

とおく.

例　$A \in \mathrm{SO}_3(\mathbf{R})$ は必ず 1 を固有値にもつ. その長さ 1 の固有ベクトルを v_1 として, v_1 の直交補空間を E とすると

$$\mathbf{R}^3 = \mathbf{R}v_1 \oplus E$$

E の正規直交基 v_2, v_3 をその外積が $v_2 \times v_3 = v_1$ を満たすようにとる. この基底に関する A の行列表示は

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$$

となる. よって A は, 直線 $\mathbf{R}v_1$ の周りの角度 θ の回転になる.

ハミルトン四元数体

$$\mathbf{H} = (-1,-1)_{\mathbf{R}} = D(\mathbf{C}, -1) = \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \ : \ a, b \in \mathbf{C} \right\}$$

は斜体で, $\mathbf{H}^\times = \mathbf{H} - \{0\}$. 通常

$$\mathbf{H} = \mathbf{R}1 + \mathbf{R}i + \mathbf{R}j + \mathbf{R}k, \qquad i^2 = j^2 = -1, \ \ k = ij = -ij$$

と表す. $\mathbf{C} = \mathbf{R}1 + \mathbf{R}i$ から,

$$\mathbf{H} = \mathbf{C} + \mathbf{C}j, \qquad zj = j\overline{z} \ \ (\forall z \in \mathbf{C})$$

この表示で

$$u = a + bj = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \in \mathbf{H}, \quad N(u) = |a|^2 + |b|^2$$

Lemma 5

$\mathbf{H}^1 = \{u \in \mathbf{H} : N(u) = 1\}$ は $\mathbf{H}^\times$ の部分群で, $\mathbf{H}^1 = \mathbf{SU}_2(\mathbf{C})$ である.

証明

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SU}_2(\mathbf{C})$$

とすると

$$a\bar{a} + b\bar{b} = 1, \qquad \bar{a}c + \bar{b}d = 0, \qquad ad - bc = 1$$

から

$$\begin{pmatrix} a & -b \\ \bar{b} & \bar{a} \end{pmatrix}\begin{pmatrix} d \\ c \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{よって} \quad \begin{pmatrix} d \\ c \end{pmatrix} = \begin{pmatrix} \bar{a} & b \\ -\bar{b} & a \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \bar{a} \\ -\bar{b} \end{pmatrix}$$

□

$\mathbf{H}$ の部分空間

$$\mathbf{H}_0 = \{u \in \mathbf{H} : u^\iota = -u\} = \mathbf{R}i + \mathbf{R}j + \mathbf{R}k \cong \mathbf{R}^3 : xi + yj + zk \longleftrightarrow \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

をとる. $\mathbf{R}^3$ の標準内積により, $\mathbf{H}_0$ を内積空間とみる.

$$\|u\|^2 = (u, u) = N(u) \qquad (^\forall u \in \mathbf{H}_0)$$

である.

Prop 1

(1) $^\forall \alpha \in \mathbf{H}^1$, $^\forall u \in \mathbf{H}_0$ に対し, $\alpha u \alpha^{-1} \in \mathbf{H}_0$.
(2) $\alpha \in \mathbf{H}^1$ に対し, $T_\alpha : \mathbf{H}_0 \longrightarrow \mathbf{H}_0 : T_\alpha(u) = \alpha u \alpha^{-1}$ は $\mathbf{R}$ 線形で, $T_\alpha \in \mathbf{SO}_3(\mathbf{R})$.
(3) $T : \mathbf{H}^1 = \mathbf{SU}_2(\mathbf{C}) \longrightarrow \mathbf{SO}_3(\mathbf{R}) : \alpha \mapsto T_\alpha$ は全射準同型で $\mathbf{Ker}T = \{\pm 1\}$ である.

証明 (1) $\alpha \in \mathbf{H}^1$ だから $\alpha^{-1} = \alpha^\iota$. よって

$$u \in \mathbf{H}_0 \implies (\alpha u \alpha^{-1})^\iota = \alpha u^\iota \alpha^{-1} = \alpha(-u)\alpha^{-1} = -\alpha u \alpha^{-1}$$

となり, $\alpha u \alpha^{-1} \in \mathbf{H}_0$.
(2) T_α が線形であることは明らか.

$$\|T_\alpha(u)\| = N(\alpha u \alpha^{-1}) = N(\alpha)N(u)N(\alpha^{-1}) = N(u) = \|u\|$$

から $T_\alpha \in \mathrm{O}_3(\mathbf{R})$. $T_{\pm 1}$ は恒等写像なので, $\alpha \neq \pm 1$ として

$$\alpha = a + bi + cj + dk \qquad (a, b, c, d \in \mathbf{R})$$

とおく.

$$1 = N(\alpha) = a^2 + b^2 + c^2 + d^2$$

から $|a| < 1$. そこで $\theta = \cos^{-1} a \in (0, \pi)$ をとり

$$e_1 = \frac{bi + cj + dk}{\sin\theta} \in \mathbf{H}_0$$

とおけば

$$\alpha = \cos\theta + \sin\theta e_1$$

と書ける. 定義と $1 = \alpha\alpha^\iota = (\cos\theta + \sin\theta e_1)(\cos\theta - \sin\theta e_1)$ より

$$\|e_1\| = 1, \qquad e_1^2 = -1$$

である. $e_2 \in \mathbf{H}_0$ を

$$(e_1, e_2) = 0, \qquad \|e_2\| = 1$$

ととる. $e_2^\iota = -e_2$ だから

$$e_2^2 = -e_2 e_2^\iota = -\|e_2\|^2 = -1$$

で, さらに

$$(e_1 + e_2)^2 = -(e_1 + e_2)(e_1 + e_2)^\iota = -(e_1 + e_2, e_1 + e_2) = -(\|e_1\|^2 + \|e_2\|^2) = -2$$

他方

$$(e_1 + e_2)^2 = e_1^2 + e_1e_2 + e_2e_1 + e_2^2 = -2 + e_1e_2 + e_2e_1$$

よって

$$e_1e_2 = -e_2e_1$$

したがって $e_3 = e_1e_2$ とおけば

$$\mathbf{H}_0 = \mathbf{R}e_1 + \mathbf{R}e_2 + \mathbf{R}e_3, \qquad e_1^2 = e_2^2 = -1,\ e_3 = e_2e_1 = -e_2e_1$$

$\alpha = \cos\theta + \sin\theta e_1$, $\alpha^{-1} = \alpha^\iota = \cos\theta - \sin\theta e_1$ で, 基底 e_1, e_2, e_3 による T_α の行列表示を計算する.

$$\begin{aligned}
T_\alpha(e_1) &= N(\alpha)e_1 = e_1 \\
T_\alpha(e_2) &= (\cos\theta + \sin\theta e_1)e_2(\cos\theta - \sin\theta e_1) = \cos 2\theta e_2 + \sin 2\theta e_3 \\
T_\alpha(e_3) &= -\sin 2\theta e_2 + \cos 2\theta e_3
\end{aligned}$$

から

$$T_\alpha = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos 2\theta & -\sin 2\theta \\ 0 & \sin 2\theta & \cos 2\theta \end{pmatrix}$$

(3) T が準同型であることは容易. $T_\alpha = I_3$ とする. このとき

$$^\forall u \in \mathbf{H}_0, \quad \alpha u = u\alpha$$

だから, Lemma 3 (4) により, $\alpha = aI_2$, $(a \in F)$ となる. $N(\alpha) = a^2 = 1$ より $a = \pm 1$. よって $\mathrm{Ker}T = \{\pm I_2\}$. 全射であることを示す. $A \in \mathrm{SO}_3(\mathbf{R})$ に対し, $\mathbf{H}_0$ の正規直交基 e_1, e_2, e_3 を適当にとれば, この基底に関する A の行列表示が

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos 2\theta & -\sin 2\theta \\ 0 & \sin 2\theta & \cos 2\theta \end{pmatrix}$$

となるようにできる. このとき $\alpha = \cos\theta + \sin\theta e_1$ とすれば, $\alpha \in \mathbf{H}^1$ で, $T_\alpha = A$ である. □

6　単純環の構造定理

以下 R を単位的環とする.

Def　R の両側イデアル, すなわち

$$J \subset R \ \text{ s.t. } \begin{cases} a+b \in J & (\forall a, b \in J) \\ ax, xa \in J & (\forall a \in J,\ \forall x \in R) \end{cases}$$

であるような J が, $\{0\}$ と R 自身に限られるとき, R を**単純環** (simple ring) という.

Def　加群 M に対し, R のスカラー積

$$M \times R \longrightarrow M : (x, a) \mapsto xa$$

が定義されていて, 任意の $a, b \in R, x, y \in M$ で次が成り立つとき, M を**右 R 加群** (right R module) という.

(M1) $(x+y)a = xa + ya$

(M2) $x(a+b) = xa + xb$

(M3) $x(a \cdot b) = (xa)b$

(M4) $x1_R = x$

さらに, M の部分 R 加群が, $\{0\}$ と M 自身に限られるとき, M を単純という.

例
(1) D を斜体とすると, D は単純環である.

$$Z_D = \{x \in D \ :\ xy = yx \quad (\forall y \in D)\}$$

を D の中心という. Z_D は体になる. $F = Z_D$ とおけば, D を F ベクトル空間と見なすことにより, D は F-多元環になる.
(2) 体 F の行列環 $\mathrm{M}_n(F)$ は単純環である. (証明は下の Prop 2.)
(3) 四元数環 $(\alpha, \beta)_F$ は $\mathrm{M}_2(F)$ に同型であるか, そうでなければ斜体であるから, 単純環になる.

Prop 2

D を斜体として, $F = Z_D$ とする.
(1) D に成分をもつ行列環 $\mathbf{M}_n(D)$ は F-多元環であり, 単純環である.
(2) 任意の単純右 $\mathbf{M}_n(D)$ 加群は $\mathbf{M}_{1,n}(D)$ に同型である.

証明 (1) $\mathrm{M}_n(D)$ は行列の和と積で F-多元環になる. 各 $i,j=1,2,\cdots,n$ に対し

$$\boldsymbol{e}_{ij}=(i,j)\text{ 成分だけが }1\text{ で, それ以外の成分が }0\text{ である }(n,n)\text{ 行列}$$

とおけば.

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

$J\subset M_n(D)$ を両側イデアルで $J\neq\{0\}$ とする. $0\neq a=(a_{ij})\in J$ がとれて, $a_{kl}\neq 0$ とする. このとき

$$(a_{kl}^{-1}\boldsymbol{e}_{ik})\cdot a\cdot\boldsymbol{e}_{li}=\boldsymbol{e}_{ii}\in J\qquad(i=1,2,\cdots,n)$$

より

$$I_n=\boldsymbol{e}_{11}+\boldsymbol{e}_{22}+\cdots+\boldsymbol{e}_{nn}\in J$$

よって $J=\mathrm{M}_n(D)$ となる.
(2) $\mathrm{M}_{1,n}(D)=\boldsymbol{e}_{11}D+\boldsymbol{e}_{12}D+\cdots+\boldsymbol{e}_{1n}D=\boldsymbol{e}_{11}\mathrm{M}_n(D)$ と同一視できる.

$$u=\boldsymbol{e}_{11}a_1+\cdots+\boldsymbol{e}_{1n}a_n\neq 0,\qquad(a_1,\cdots,a_n\in D)$$

を任意にとる. $^{\exists}\boldsymbol{e}_{1i}a_i\neq 0$. このとき

$$\boldsymbol{e}_{1j}=ua_i^{-1}\boldsymbol{e}_{ij}\in u\mathrm{M}_n(D)\quad(j=1,\cdots,n)\quad\text{よって}\quad u\mathrm{M}_n(D)=\mathrm{M}_{1,n}(D)$$

となり, $\mathrm{M}_{1,n}(D)$ は単純である.
M を任意の単純右 $\mathrm{M}_n(D)$ 加群として, $0\neq x\in M$ をとる. このとき

$$x=xI_n=x\boldsymbol{e}_{11}+x\boldsymbol{e}_{22}+\cdots+x\boldsymbol{e}_{nn}$$

から, $^{\exists}x\boldsymbol{e}_{ii}\neq 0$. M の単純性から $M=x\boldsymbol{e}_{ii}\mathrm{M}_n(D)$. $\boldsymbol{e}_{ii}\mathrm{M}_n(D)\cong\boldsymbol{e}_{11}\mathrm{M}_n(D)$ は単純右 $\mathrm{M}_n(D)$ 加群である. 写像

$$\boldsymbol{e}_{ii}\mathrm{M}_n(D)\longrightarrow xe_{ii}\mathrm{M}_n(D)=M:a\mapsto xa$$

は全射 $\mathrm{M}_n(D)$ 準同型で, $\boldsymbol{e}_{ii}\mathrm{M}_n(D)$ の単純性から単射である. □

Def $\{0\}\neq I\subset R$ を右イデアルとする. R の右イデアル J で, $\{0\}\subsetneq J\subsetneq I$ となるものが存在しないとき, I を**極小**であるという.

例 D を斜体として, $R=\mathrm{M}_n(D)$ とする. Prop 2 (2) から $J_i=e_{ii}R$ $(i=1,\cdots,n)$ は単純 R-加群であるから極小右イデアルになる. $J_1,J_2,\cdots,J_n$ で極小右イデアルは尽きる. R の任意の右イデアルは

$$J_{i_1}+J_{i_2}+\cdots+J_{i_k}\qquad(1\leq i_1<i_2<\cdots<i_k\leq n)$$

と表わせる.

右イデアル $I \subset R$ に対し

$$\mathrm{End}_R(I) = \left\{ f : I \longrightarrow I : \begin{array}{c} f(a+b) = f(a) + f(b) \ \ (a, b \in I) \\ f(ar) = f(a)r \ \ (a \in I,\ r \in R) \end{array} \right\}$$

とする. $\mathrm{End}_R(I)$ は和と積

$$(f_1 + f_2)(a) = f_1(a) + f_2(a), \quad (f_1 \circ f_2)(a) = f_1(f_2(a)) \qquad (f_1, f_2 \in \mathrm{End}_R(I),\ \ a \in I)$$

により, 環になる.

Lemma 6

極小右イデアル $\boldsymbol{I \subset R}$ が存在したとする.
(1) $\boldsymbol{0 \neq x \in I}$ ならば, $\boldsymbol{I = xR}$ である.
(2) $\boldsymbol{\mathrm{End}_R(I)}$ は斜体である.
(3) $\boldsymbol{x \in I, xI \neq \{0\}}$ ならば, $\boldsymbol{{}^{\exists}e \in I}$ *s.t.* $\boldsymbol{e^2 = e}$ かつ $\boldsymbol{xe = x}$.

証明 (1) $x \neq 0$ より, $\{0\} \subsetneq xR \subset I$. 極小性から $I = xR$.
(2) $0 \neq f \in \mathrm{End}_R(I)$ をとる. このとき $\mathrm{Ker}f \subsetneq I$ は右イデアルだから, 極小性により $\mathrm{Ker}f = \{0\}$. よって f は単射. また $\{0\} \neq \mathrm{Im}f \subset I$ も右イデアルだから, $\mathrm{Im}f = I$ で f は全射. f は全単射だから f^{-1} が存在する. $f^{-1} \in \mathrm{End}_R(I)$ は容易. よって $0 \neq {}^{\forall}f$ は単元だから $\mathrm{End}_R(I)$ は斜体である.
(3) $\varphi : I \longrightarrow I : \varphi(a) = xa$ とすると $\varphi \in \mathrm{End}_R(I)$. (2) から φ は全単射だから, ${}^{\exists}e \in I$ s.t. $\varphi(e) = x$. すなわち $xe = x$. よって $x(e^2 - e) = 0$ で, 単射性から $e^2 = e$ である. □

Def 環 R の元 $e \neq 0$ で $e^2 = e$ を満たすものを**べき等元**という. e がべき等元のとき, 集合 $eRe = \{eae \mid a \in R\}$ は, R の和と積で閉じている. つまり

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

さらに $e(eae) = eae = (eae)e$ から, e が積の単位元となり, eRe 自身が環になる.

Lemma 7

$\boldsymbol{e \in R}$ をべき等元として, $\boldsymbol{I = eR}$ を単項右イデアルとする. このとき $\boldsymbol{f \in \mathrm{End}_R(I)}$ に対し, $\boldsymbol{\psi(f) = f(e)e \in R}$ とすれば, $\boldsymbol{\psi(f) \in eRe}$ であり, 写像

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

は環の全射準同型写像になる. もし $\boldsymbol{I}$ が極小ならば, $\boldsymbol{\psi}$ は同型になる.

証明 $f \in \mathrm{End}_R(I)$ とすると, $f(e) \in I = eR$ だから $f(e)e \in Ie = eRe$ である.
(ψ は準同型) : $f, g \in \mathrm{End}_R(I)$ に対し

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

また $f(e) = ea$, $g(e) = eb$ とすると, $e^2 = e$ から

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

また $\mathrm{id}_I \in \mathrm{End}_R(I)$ を恒等写像とすれば, $\psi(\mathrm{id}_I) = e^2 = e$. よって ψ は環の準同型.
(全射性) : $c \in R$ に対し, $f_c \in \mathrm{End}_R(I)$ を $f_c(x) = ecx \quad (x \in I)$ と定義する. このとき $\psi(f_c) = ece$ から ψ は全射.
I が極小ならば $\mathrm{End}_R(I)$ は斜体. $\mathrm{Ker}\psi \subsetneq \mathrm{End}_R(I)$ は両側イデアルだから , $\mathrm{Ker}\psi = \{0\}$. よって ψ は単射でとくに同型になる. □

系 1

D_1 と D_2 は斜体で $\mathbf{M}_{n_1}(D_1) \cong \mathbf{M}_{n_2}(D_2)$ ならば, $n_1 = n_2$ かつ $D_1 \cong D_2$ である.

証明 ($n_1 = n_2$): $\mathrm{M}_{n_1}(D_1) \cong \mathrm{M}_{n_2}(D_2)$ の両辺の極小右イデアルの個数はそれぞれ n_1, n_2 でそれが一致しないといけないから, $n_1 = n_2$ となる.
($D_1 \cong D_2$): $n = n_1 = n_2$ とし, $R = \mathrm{M}_n(D_1) \cong \mathrm{M}_n(D_2)$ とおく. $I = e_{11}R$ とする. I は極小右イデアルで, Lemma 6 から $D = \mathrm{End}_R(I)$ は斜体である. $e_{11} \in I$ はべき等元だから, Lemma 7 から, $D \cong e_{11}Re_{11} \cong D_1$. 同様に $D \cong D_2$.

□

極小右イデアル $I \subset R$ が存在したとする. このとき $D = \mathrm{End}_R(I)$ は斜体である.

$$D \times I \longrightarrow I \ : \ \alpha * x = \alpha(x)$$

でスカラー倍を定義することにより, I は左 D ベクトル空間になる.

$$L = \mathrm{End}_D(I) = \{g \ : \ I \longrightarrow I \ : \ \text{左 } D\text{-線形写像}\}$$

とおく. $x \in I$, $g \in L$ のとき, g による x の像を $x \cdot g$ と表す. L は和と積

$$x \cdot (g_1 + g_2) = x \cdot g_1 + x \cdot g_2, \quad x \cdot (g_1 \circ g_2) = (x \cdot g_1) \cdot g_2 \qquad (g_1, g_2 \in L, \ \ x \in I)$$

により環になる. もし $\dim_D I = n < \infty$ ならば $L \cong \mathrm{M}_n(D)$ である.

Lemma 8

$a \in R$ に対し, 写像 $T_a : I \longrightarrow I$ を $x \cdot T_a = xa$ により定義すると, 次が成り立つ.
(1) $T_a \in L$
(2) 写像 $T : R \longrightarrow L : a \mapsto T_a$ は環準同型である.
(3) $T(I) \subset L$ は, L の右イデアルである.

証明 (1), (2) は容易.
(3) $b \in I$ に対し, $\beta_b \in D$ を

$$\beta_b * u = \beta_b(u) = bu \qquad (u \in I)$$

により定義する. このとき, $^\forall g \in L$, $^\forall x \in I$ に対して

$$(bx) \cdot g = (\beta_b * x) \cdot g = \beta_b * (x \cdot g) = b(x \cdot g)$$

だから

$$b \cdot (T_a \circ g) = (b \cdot T_a) \cdot g = (ba) \cdot g = b(a \cdot g) = b \cdot T_{a \cdot g} \qquad (^\forall b \in I)$$

これから $T_a \circ g = T_{a \cdot g}$. つまり $T(I) \circ g \subset T(I)$ ($^\forall g \in L$) で $T(I)$ は右イデアルになる.

□

定理 2 (Wedderburn)

V を有限次元 F-多元環とする. V が単純ならば, 斜体 D が存在し $V \cong \mathbf{M}_n(D)$ となる.
V から n は一意に定まり, D は同型を除いて一意に定まる.

証明 $\{0\} \neq I \subset V$ を右イデアルで, $\dim_F I$ が最小になるものとする. このとき I は極小右イデアルになる. $D = \mathrm{End}_V(I)$ は斜体であり, I は左 D ベクトル空間になる.

$$\dim_D I \leq \dim_F I \leq \dim_F V < \infty$$

Lemma 8 (2) より

$$T : V \longrightarrow \mathrm{End}_D(I) \cong \mathrm{M}_n(D)$$

は環準同型である.
(T は単射) : V は単純だから $\mathrm{Ker}T = \{0\}$ なので.
(T は全射) : $\mathrm{Im}T = T(V)$ に対し, $1_n \in T(V)$ だから, $T(V)\mathrm{M}_n(D) \subset T(V)$ を示せばよい. I から生成された V の左イデアルを VI とおく. I は右イデアルであったから, VI は両側イデアルになる. V の単純性から $V = VI$. よって, $T(V) = T(V)T(I)$ となり, Lemma 8 (3) から $T(I)\mathrm{M}_n(D) = T(I)$ だから $T(V)\mathrm{M}_n(D) \subset T(V)$ となる.
(一意性) は系 1 から従う. □

7　中心的単純多元環

F を体 ($\mathrm{ch}(F) = 2$ でもよい) とする.
A を F-多元環とする.

$$Z_A = \{a \in A \,:\, ax = xa \quad {}^\forall x \in A\}$$

を A の中心という. $F \subset Z_A$ である.

Lemma 9

A が単純ならば Z_A は体である. とくに Z_A は F の拡大体である.

証明 $a \in Z_A, a \neq 0$ ならば, $Aa = aA$ だから, Aa は両側イデアルとなる. 単純性から $Aa = A$ となり, a は逆元 $a^{-1} \in A$ をもつ. $a^{-1} \in Z_A$ は容易. □

Def　A が F 上有限次元の単純多元環 かつ $Z_A = F$ であるとき, A を F-中心的単純多元環 (F- central simple algebra, 略して F-c.s.) という.

例
(1) 四元数環 $(\alpha, \beta)_F$ は F-c.s. である. (Lemma 3 (4))
(2) F が代数的閉体 (たとえば $\mathbf{C}$) のとき, A が F-c.s. ならば $A \cong \mathrm{M}_n(F)$ である.

証明 定理 2 から, $A \cong \mathrm{M}_n(D)$. ここで D は斜体.

$$F = Z_A = Z_{M_n(D)} = Z_D$$

であるから F は D の中心. ${}^\forall a \in D$ に対し, $\dim_F F(a) \leq \dim_F D < \infty$ から, $F \subset F(a)$ は代数拡大になる. よって $F = F(a)$ で $a \in F$. つまり $D = F$. □

A, B を F-多元環 (有限次元でなくてもよい) とする.
A と B の F 上のテンソル積を $A \otimes B$ と表わす. これは次の性質をもつ.

(T1) $A \otimes B$ の任意の元は

$$x_1 \otimes y_1 + \cdots + x_k \otimes y_k \qquad (x_i \in A,\ y_i \in B,\ 1 \leq k \in \mathbf{Z})$$

と表わせる.

(T2) A の F 上の基底を $\{a_i\}$, B の F 上の基底を $\{b_j\}$ とすれば, $A \otimes B$ は $\{a_i \otimes b_j\}_{i,j}$ を基底にもつ F ベクトル空間である.

(T3) $^\forall x, x_1, x_2 \in A$, $^\forall y, y_1, y_2 \in B$, $^\forall \lambda \in F$ に対し,

$$(x_1 + x_2) \otimes y = x_1 \otimes y + x_2 \otimes y, \quad x \otimes (y_1 + y_2) = x \otimes y_1 + x \otimes y_2$$
$$\lambda(x \otimes y) = (\lambda x) \otimes y = x \otimes (\lambda y)$$
$$(x_1 \otimes y_1)(x_2 \otimes y_2) = (x_1 x_2) \otimes (y_1 y_2)$$

が成立. とくに $A \otimes B$ は F-多元環である.

Lemma 10

A, B を F-多元環とするとき, $Z_{A\otimes B} = Z_A \otimes Z_B$ である.

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

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

と一意に書ける. $x \in Z_{A\otimes B}$ ならば,

$$\forall a \in A, \ \ (a \otimes 1)x = x(a \otimes 1) \quad \text{つまり} \quad \sum_i (ax_i) \otimes b_i = \sum_i (x_i a) \otimes b_i$$

一意性から各 i について $ax_i = x_i a$. よって $x_i \in Z_A$. したがって $Z_{A\otimes B} \subset Z_A \otimes B$. 次に $\{a_i\}$ を Z_A の F 上の基底とすれば, $Z_A \otimes B$ の元 y は

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

と一意に書ける. もし $y \in Z_{A\otimes B}$ ならば上と同様に $y_i \in Z_B$ となり, よって $Z_{A\otimes B} \subset Z_A \otimes Z_B$ となる. □

Lemma 11

A を F-c.s. として, B を F-多元環とする. $0 \neq I \subset A \otimes B$ が両側イデアルならば, I は $1_A \otimes b \neq 0$ という形の元を含む.

証明 A は単純だから,

$$0 \neq {}^\forall a \in A, \ \ {}^\exists x_1, x_1', x_2, x_2', \cdots, x_m, x_m' \in A \ \text{ s.t. } \sum_{i=1}^m x_i a x_i' = 1_A$$

$x \in I$ に対し

$$p(x) = \min\{j \mid x \text{ は } x = a_1 \otimes b_1 + \cdots + a_j \otimes b_j, \ (a_i \in A, \ \ b_i \in B) \text{ と表示される}\}$$

とおき

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

とする. まず $p = 1$ を示す. $p > 1$ と仮定してみる.

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

をとる. 上の注意から $a_p = 1_A$ としてよい. このとき, a_{p-1} と a_p は F 上一次独立. (そうでなければ $p(x) < p$ となり矛盾). とくに $a_{p-1} \notin Z_A = F$. したがって

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

よって

$$x' = (c \otimes 1)x - x(c \otimes 1) = (ca_1 - a_1c) \otimes b_1 + \cdots + (ca_{p-1} - a_{p-1}c) \otimes b_{p-1} \neq 0$$

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

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

である. □

系 2

(1) $\boldsymbol{A}$ が $\boldsymbol{F}$-*c.s* で $\boldsymbol{B}$ が単純 $\boldsymbol{F}$-多元環ならば, $\boldsymbol{A \otimes B}$ は単純 $\boldsymbol{F}$-多元環である.
(2) $\boldsymbol{A, B}$ が共に $\boldsymbol{F}$-*c.s.* ならば $\boldsymbol{A \otimes B}$ も $\boldsymbol{F}$-*c.s* である.
(3) $\boldsymbol{A}$ が $\boldsymbol{F}$-多元環で $\boldsymbol{K}$ が $\boldsymbol{F}$ の拡大体のとき

$$\boldsymbol{A} \text{ が } \boldsymbol{F}\text{-c.s.} \iff \boldsymbol{A \otimes K} \text{ が } \boldsymbol{K}\text{-c.s.}$$

(4) $\boldsymbol{A}$ が $\boldsymbol{F}$-多元環で $\boldsymbol{\overline{F}}$ が $\boldsymbol{F}$ の代数閉包のとき

$$\boldsymbol{A} \text{ が } \boldsymbol{F}\text{-c.s.} \iff \boldsymbol{A \otimes \overline{F} \cong \mathbf{M}_n(\overline{F})}$$

(5) $\boldsymbol{A}$ が $\boldsymbol{F}$-*c.s.* ならば, $\boldsymbol{\dim_F A}$ は自然数の平方数になる.

証明 (1) は Lemma 11 から. (2) と (3) は (1) と Lemma 10 から. (4) は (3) と例 (2) から. (5) は (4) から. □

8　中心的単純多元環の自己同型群

F を体 ($\mathrm{ch}(F) = 2$ でもよい) とする.

Def　A を F-多元環として, A に新しい積 $\circ : A \times A \longrightarrow A$ を

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

により定義する. この積により A は F-多元環になる. これを A の**反転多元環**といい, A° により表す. A が F-c.s. $\Longleftrightarrow$ A° が F-c.s. である.

Lemma 12

A は F-c.s. で, $\dim_F A = n^2$ とする. A の F ベクトル空間としての線形写像全体を $\mathrm{End}_F(A) \cong \mathrm{M}_{n^2}(F)$ とする. このとき, 写像

$$\psi : A \otimes A^\circ \longrightarrow \mathrm{End}_F(A) : \psi(\sum_i a_i \otimes b_i)(v) = \sum_i a_i v b_i \qquad (v \in A)$$

は多元環の同型写像である.

証明　ψ はテンソル積の普遍性により well-defined で, 多元環の準同型であることは容易. $A \otimes A^\circ$ は単純だから ψ は単射. $\dim_F A \otimes A^\circ = \dim \mathrm{End}_F(A)$ だから ψ は同型写像になる. □

Def　A を F-c.s. とする. 単数 $a \in A^\times$ に対し,

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

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

$\mathrm{Aut}(A) = \{f : A \longrightarrow A :$ 多元環の同型写像 $\}$: A の自己同型群
$\mathrm{Inn}(A) = \{i_a \mid a \in A^\times\}$: A の内部自己同型群
とおく. $\mathrm{Inn}(A) \subset \mathrm{Aut}(A)$ は部分群で, 写像 $a \mapsto i_a$ により $A^\times / Z_A^\times \cong \mathrm{Inn}(A)$ である.

Prop 3

A が F-c.s. ならば $\mathrm{Aut}(A) = \mathrm{Inn}(A)$ である. すなわち,

$$^\forall f \in \mathrm{Aut}(A) \;\; ^\exists a \in A^\times \;\; s.t. \;\; f(x) = axa^{-1} \quad (x \in A)$$

証明 $\mathrm{Aut}(A) \subset \mathrm{End}_F(A)$ だから, Lemma 12 より

$$f(x) = \sum_i a_i x b_i \qquad (a_i \otimes b_i \in A \otimes A^\circ)$$

と書ける. ここで $\{a_i\}$ は A の基底としてよい. $f(xy) = f(x)f(y)$ より

$$0 = \sum_i a_i xy b_i - \sum_i a_i x b_i f(y) = \sum_i a_i x(yb_i - b_i f(y)), \qquad (^\forall x \in A)$$

したがって

$$\sum_i a_i \otimes (yb_i - b_i f(y)) = 0 \quad \text{よって} \quad yb_i - b_i f(y) = 0 \qquad (^\forall y \in A,\ ^\forall i)$$

これから

$$y(b_iA) = (yb_i)A = (b_i f(y))A \subset b_iA \ \text{ つまり } \ A(b_iA) \subset b_iA$$

となり b_iA は両側イデアルになる. 単純性から $b_iA = \{0\}$ または A. よって, $b_i = 0$ または $b_i \in A^\times$. $^\forall b_i = 0$ ならば $f = 0$ となってしまうから, $^\exists b_i \in A^\times$. このとき $f(y) = b_i y b_i^{-1}$ となる. □

Prop 3 より強く次が示せる.

定理 3 [Skolem-Noether]

A を F-c.s., B を有限次元単純 F-多元環とする. $f, g : B \longrightarrow A$ を共に自明でない多元環の準同型とする. このとき $i_a \in \mathrm{Inn}(A)$ で, $g = i_a \circ f$ となるものが存在する.

証明 次の限定版を示す. $A = D$ は斜体, $B = K$ が体. (応用ではこのケースのみ扱う.)
$R = K \otimes D$ とおけば R は K-c.s. である. D の R-スカラー倍を

$$D \times R \longrightarrow D : (x, \alpha \otimes y) \mapsto f(\alpha)xy$$

と定義して, D を 右 R-加群としたものを M_f と表す. 同様に M_g ができる. M_f, M_g は右 D-加群として単純だから, 右 R-加群としても単純. Prop 2 (2) より, 単純右 R-加群はすべて同型だから, 同型写像

$$\psi : M_f \longrightarrow M_g$$

がある. よって

$$\psi(f(\alpha)xy) = g(\alpha)\psi(x)y, \qquad (\alpha \in K,\ \ x, y \in D)$$

ψ は右 D 加群としての同型でもあるから, $\psi(1_D) = a \in D$ とおくと, $a \in D^\times$ で

$$\psi(1_D)f(\alpha) = \psi(f(\alpha)1_D) = g(\alpha)\psi(1_D) \quad \text{つまり} \quad af(\alpha) = g(\alpha)a$$

□

系 3

ch(F) ≠ 2 とする. A を F-多元環とするとき

$$A \text{ が四元数環} \iff A \text{ は 4 次元 } F\text{-c.s.}$$

証明 $\Longleftarrow$ を示す. 定理 2 から

$$A \cong \mathrm{M}_n(D), \qquad 4 = \dim_F A = n^2 \dim_F D$$

と書ける. これから, $n = 1, 2$ である.
$n = 2$ ならば $\dim_F D = 1$ から $F = D$. よって $A \cong \mathrm{M}_2(F) = (1,1)_F$.
$n = 1$ のとき. $A \cong D$ は斜体. $a \in A$, $a \notin F$ をとる. このとき $K = F(a)$ は F の拡大体で, A は自然に K ベクトル空間となるから

$$4 = \dim_F A = [K : F] \dim_K A$$

が成り立つ. $K \neq F$ だから, これが成り立つのは $[K : F] = 2$, $\dim_K A = 2$ のときに限る. よって K は 2 次拡大で, $K^\rho = F$ となる対合 ρ がある. そこで

$$f = \mathrm{id}_K : K \longrightarrow K \subset A, \qquad g = \rho : K \longrightarrow K \subset A$$

に定理 3 限定版を適用すれば,

$$^\exists b \in A^\times \text{ s.t. } \rho(x) = bxb^{-1} \qquad (x \in K)$$

明らかに $b \notin K$ で, $\dim_K A = 2$ だから

$$A = K + Kb, \qquad xb = b\rho(x) \qquad (x \in K)$$

$\beta = b^2 \in Z_A = F$ だから, $A \cong D(K, \beta)$ となる. □

系 4

ch(F) ≠ 2 として, K/F を 2 次拡大, $\alpha, \beta \in F^\times$ する. このとき

$$D(K, \alpha) \cong D(K, \beta) \iff {}^\exists z \in K^\times \ \textit{s.t.} \ \beta = z\rho(z)\alpha$$

証明 ($\Longleftarrow$)

$$D(K, \alpha) = K + Ku, \qquad u^2 = \alpha, \qquad au = u\rho(a) \quad ({}^\forall a \in K)$$

である. $z \in K^\times$ をとり $v = zw$ とおくと

$$D(K,\alpha) = K + Kv, \qquad v^2 = z\rho(z)\alpha, \qquad av = v\rho(a) \quad (^\forall a \in K)$$

だから

$$D(K,\alpha) \cong D(K, z\rho(z)\alpha)$$

($\Longrightarrow$)

$$D(K,\beta) = K + Kw, \qquad w^2 = \beta, \qquad aw = w\rho(a) \quad (^\forall a \in K)$$

として

$$\varphi : D(K,\alpha) \longrightarrow D(K,\beta) : \text{同型}$$

とする.

$$\mathrm{id}_K : K \longrightarrow D(K,\beta), \qquad \varphi : K \longrightarrow D(K,\beta)$$

に定理 3 限定版を適用すると,

$$^\exists y \in D(K,\beta) \ \text{ s.t. } \ \varphi(a) = yay^{-1} \quad (^\forall a \in K)$$

$t = y^{-1}\varphi(u)y \in D(K,\beta)$ とおく. このとき $a \in K$ に対し

$$at = ay^{-1}\varphi(u)y = y^{-1}\varphi(au)y = y^{-1}\varphi(u\rho(a))y = y^{-1}\varphi(u)yy^{-1}\varphi(\rho(a))y = t\rho(a)$$

これから

$$atw^{-1} = tw^{-1}a \quad (^\forall a \in K) \quad \text{つまり} \quad z = tw^{-1} \in K$$

で

$$t^2 = zwzw = z\rho(z)w^2 = z\rho(z)\beta$$

他方

$$t^2 = y^{-1}\varphi(u^2)y = y^{-1}\alpha y = \alpha$$

□

9　2 次形式

F は体で $\mathrm{ch}(F) \neq 2$ とする.

Def　V を有限次元 F ベクトル空間とする. 写像

$$Q : V \longrightarrow F$$

が次を満たすとき, Q を 2 次形式, (V, Q) を 2 次空間という.

(Q1) $Q(av) = a^2 Q(v) \quad (\forall a \in F, \ \forall v \in V)$

(Q2) $B : V \times V \longrightarrow F$ を $B(u, v) = 2^{-1}(Q(u+v) - Q(u) - Q(v))$ と定義すれば, B は双線形形式である.

(V, Q) を 2 次空間とする. V の基底 $e_1, \cdots, e_n$ を固定して, $V \cong F^n$ と同一視する. このとき

$$B(e_i, e_j) = b_{ij} \in F, \qquad T_Q = (b_{ij}) \in \mathrm{M}_n(F)$$

とおけば, ${}^t T_Q = T_Q$ であり

$$B(u, v) = {}^t u T_Q v, \qquad Q(v) = B(v, v) = {}^t v T_Q v$$

となる. T_Q を Q の Gram 行列という. $e'_1, \cdots, e'_n$ を V の別の基底として,

$$T'_Q = (b'_{ij}), \qquad b'_{ij} = B(e'_i, e'_j)$$

とすると

$$T'_Q = {}^t P T_Q P, \qquad P \in \mathrm{GL}_n(F) \ \text{ s.t. } \ (e'_1, \cdots, e'_n) = (e_1, \cdots, e_n)P$$

の関係がある. とくに $\det T_Q \in F$ は $(F^\times)^2 = \{a^2 : a \in F^\times\}$ を法として, 基底に依らずに決まる.

Def　2 次空間 (V, Q) に対し,

$$\delta(Q) = (-1)^{n(n-1)/2} \det T_Q \mod (F^\times)^2$$

を Q の**判別式** (discriminant) という. $\delta(Q) \neq 0$ のとき, (V, Q) は**非退化**という.

記号

(1) 2 次空間 (F^n, Q) が, 標準基底で $T_Q = \mathrm{diag}(\alpha_1, \cdots, \alpha_n)$ (対角行列) となるとき,

$$(F^n, Q) = \langle \alpha_1, \cdots, \alpha_n \rangle_F$$

と表わす.

(2) 2 次空間 (V,Q) と $\lambda \in F^\times$ に対し, $(V,\lambda Q)$ も 2 次空間である.
(3) $(V_1,Q_1),(V_2,Q_2)$ が 2 次空間のとき, $V = V_1 \oplus V_2$ として,

$$Q(v_1+v_2) = Q_1(v_1) + Q_2(v_2), \qquad v_1 \in V_1, v_2 \in V_2$$

とすると (V,Q) は 2 次空間になる, これを $(V_1,Q_1) \perp (V_2,Q_2)$ と表わす. V_1, V_2 の基底から V の基底をとれば, $T_Q = \mathrm{diag}(T_{Q_1}, T_{Q_2})$ となる.

Def (V,Q) を非退化 2 次空間とする.
(1) $v \in V$ が $Q(v) = 0$ のとき**等方ベクトル**といい, $Q(v) \neq 0$ のとき**非等方ベクトル**という.
(2) 部分空間 $W \subset V$ が 0 と異なる等方ベクトルを持つとき **等方的** であるという. 等方的でない部分空間を**非等方的**という.
(3) 部分空間 $W \subset V$ の元がすべて等方的であるとき, **全等方的**であるという.

例
(1) (F^{2n},Q) が, 標準基底 $e_1, e_2, \cdots, e_{2n}$ により

$$T_Q = \begin{pmatrix} 0_n & I_n \\ I_n & 0_n \end{pmatrix}$$

で定義された 2 次空間とすると, $W = Fe_1 + Fe_2 + \cdots + Fe_n$ は全等方的である. (F^{2n},Q) を双曲空間といい, H_{2n} と表す.
(2) (V,Q) を非退化 2 次空間, $W \subset V$ を部分空間とすると, 制限 $(W, Q|_W)$ も 2 次空間である.

$$W^\perp = \{v \in V \,:\, B(v,w) = 0 \ {}^\forall w \in W\}$$

を W の直交補空間という. 次は容易.

- $\dim W^\perp = \dim V - \dim W$
- $(W^\perp)^\perp = W$
- $V = W \oplus W^\perp \iff W \cap W^\perp = \{0\} \iff Q|_W$ が非退化
- W が全等方的 ($Q|_W = 0$) $\iff W \subset W^\perp$
- W が非等方的ならば $Q|_W$ は非退化

Lemma 13
(V,Q) を非退化 2 次空間とする. このとき

$$^\exists e_1, \cdots, e_n \ \ V \text{ の基底 } \ s.t. \ \ T_Q = \mathrm{diag}(\alpha_1, \cdots, \alpha_n)$$

(このような基底を直交基底という.)

証明 $n = \dim V$ についての帰納法. $Q(e_1) \neq 0$ となる $e_1 \in V$ をとる. $W = Fe_1$ は非等方的だから, $V = W \oplus W^\perp$ で, $(W^\perp, Q|_{W^\perp})$ は非退化 2 次空間になる. 帰納法の仮定から

$$^\exists e_2, \cdots, e_{n-1} \in W^\perp \text{ 基底 s.t. } T_{Q|_{W^\perp}} = \mathrm{diag}(\alpha_2, \cdots, \alpha_n)$$

このとき $e_1, e_2, \cdots, e_n$ をとればよい. □

Def $(V_1, Q_1), (V_2, Q_2)$ を 2 次空間とする. 写像

$$f : V_1 \longrightarrow V_2$$

が次を満たすとき, **等長写像** (isometry) という.

(IS1) f は線形写像である.

(IS2) $Q_2(f(v)) = Q_1(v)$ $(^\forall v \in V_1)$

さらに f が全単射のとき, 等長同型写像という. このとき (V_1, Q_1) と (V_2, Q_2) は同型であるといい, $(V_1, Q_1) \cong (V_2, Q_2)$ と表わす.

注 非退化 2 次空間の等長写像は必ず単射になるので, 等長写像が全射であれば等長同型写像になる.

例
(1) $(F^n, Q) \cong (F^n, Q') \iff {}^\exists P \in \mathrm{GL}_n(F)$ s.t. $T_{Q'} = {}^t P T_Q P$.
(2) $0 \neq {}^\forall \alpha \in F$ に対し, $\langle \alpha, -\alpha \rangle_F \cong H_2$. 実際

$$\begin{pmatrix} 1 & \alpha/2 \\ 1 & -\alpha/2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ \alpha/2 & -\alpha/2 \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & -\alpha \end{pmatrix}$$

(3) $0 \neq {}^\forall \alpha_1, \cdots, \alpha_n, \xi_1, \cdots, \xi_n \in F$ に対し

$$\langle \alpha_1, \cdots, \alpha_n \rangle_F \cong \langle \alpha_1 \xi_1^2, \cdots, \alpha_n \xi_n^2 \rangle_F$$

(4) $H_{2n} \cong H_2 \perp H_2 \perp \cdots \perp H_2$
(5) $F = \mathbf{C}$ のとき, $(\mathbf{C}^n, Q)$ が非退化ならば

$$(\mathbf{C}^n, Q) \cong \langle 1, \cdots, 1 \rangle_{\mathbf{C}} \cong \begin{cases} H_{2m} & (n = 2m) \\ H_{2m} \perp \langle 1 \rangle_{\mathbf{C}} & (n = 2m+1) \end{cases}$$

10 Wittの定理

F は体で $\mathrm{ch}(F) \neq 2$ とする.
(V, Q) が非退化2次空間, $\dim V = n$ のとき

$$O(V) = O(V, Q) = \{g : V \longrightarrow V : \text{等長写像}\} \cong \{g \in \mathrm{GL}_n(F) : {}^t g T_Q g = T_Q\}$$

を Q の直交群という.

定理 4 [Witt]

(V, Q) を非退化2次空間として, V_1, V_2 は $Q|_{V_1}, Q|_{V_2}$ が非退化であるような V の部分空間とする. このとき

$$\boldsymbol{h : V_1 \longrightarrow V_2}$$

が等長同型ならば

$$\boldsymbol{{}^{\exists} g \in O(V) \ \ s.t. \ \ g|_{V_1} = h}$$

証明 $m = \dim V_1 = \dim V_2$ の帰納法で示す.
$m = 1$ のとき. $V_1 = Fx, V_2 = Fy = Fh(x)$ で, $Q(x) = Q(y) \neq 0$ である.

$$Q(x + y) + Q(x - y) = 4Q(x) \neq 0$$

だから, $Q(x + y) \neq 0$ または $Q(x - y) \neq 0$. $Q(x + y) \neq 0$ としてよい. $z = x + y$, $W = \{z\}^{\perp}$ として,

$$g : V = Fz \oplus W \longrightarrow V = Fz \oplus W : g(\alpha z + w) = \alpha z - w$$

と定義すると, $g \in O(V)$. $x - y \in W$ だから $g(x) = g((z + x - y)/2) = (z - x + y)/2 = y$. よって $g|_{V_1} = h$.
$m > 1$ とする. $x \in V_1, Q(x) \neq 0$ をとり,

$$y = h(x), \qquad W_1 = V_1 \cap \{x\}^{\perp}, \qquad W_2 = h(W_1)$$

とおけば

$$V_1 = Fx \oplus W_1, \qquad V_2 = Fy \oplus W_2$$

となる. $m = 1$ のケースから

$$^{\exists} g_1 \in O(V) \ \text{ s.t. } \ g_1(y) = x$$

このとき $g_1 W_2 = W_1' \subset \{x\}^{\perp}$ とおけば

$$W_1, W_1' \subset \{x\}^{\perp}, \qquad g_1 \circ h : (W_1, Q|_{W_1}) \cong (W_1', Q|_{W_1'}), \qquad \dim W_1 = m - 1$$

だから, 帰納法の仮定を $(\{x\}^\perp, Q|_{\{x\}^\perp})$ に適用して

$$^\exists g_2 \in O(\{x\}^\perp) \ \text{ s.t. } \ g_2|_{W_1} = g_1 \circ h$$

この g_2 は

$$g_2 : V = Fx \oplus \{x\}^\perp \longrightarrow Fx \oplus \{x\}^\perp : g_2(x) = x$$

と V に延長できて, $g_2 \in O(V)$ となる. したがって $g = g_1^{-1} \circ g_2 \in O(V)$ をとれば, $g|_{V_1} = h$ となる.

□

定理 5 [Witt 分解]

(V, Q) を非退化 2 次空間とする. このとき V の基底で次のようなものが存在する.

$$\boldsymbol{e_1, \cdots, e_m, f_1, \cdots, f_m, u_1, \cdots, u_r \qquad 2m + r = \dim V}$$

(1) $\boldsymbol{B(e_i, e_j) = B(f_i, f_j) = 0, \quad B(e_i, f_j) = \delta_{ij} \quad (^\forall i, j = 1, \cdots, m)}$
(2) $\boldsymbol{B(e_i, u_j) = B(f_i, u_j) = 0 \quad (^\forall i = 1, \cdots, m, \ ^\forall j = 1, \cdots, r)}$
(3) $\boldsymbol{V_0 = Fu_1 + \cdots Fu_r}$ **は非等方的**
とくに, $\boldsymbol{W = Fe_1 + \cdots + Fe_m}$**,** $\boldsymbol{W' = Ff_1 + \cdots + Ff_m}$ **とおけば,**

$$\boldsymbol{V = (W \oplus W') \oplus V_0} \qquad \begin{cases} \boldsymbol{W, W'} \text{ は全等方的で } \boldsymbol{(W \oplus W', Q|_{W \oplus W'}) \cong H_{2m}} \\ \boldsymbol{(W \oplus W') \perp V_0} \end{cases}$$

さらに $\boldsymbol{m}$ **は一意的に決まり, また** $\boldsymbol{(V_0, Q|_{V_0})}$ **は同型を除いて一意的である. (** $\boldsymbol{m}$ **を** $\boldsymbol{(V, Q)}$ **の** *Witt* **指数といい,** $\boldsymbol{V_0}$ **を非等方核という.)**

証明 (V, Q) が非等方的ならば $W = W' = \{0\}$, $V = V_0$ でよい.
(V, Q) を等方的とする. V は等方ベクトル $0 \neq e_1 \in V$ をもつ. B は非退化だから

$$^\exists x_1 \in V \ \text{ s.t. } \ B(e_1, x_1) = 1$$

そこで

$$f_1 = x_1 - 2^{-1}Q(x_1)e_1 \in V \ \text{ ととれば } \ B(e_1, f_1) = 1, \ \ Q(f_1) = 0$$

このとき $V_1 = Fe_1 + Ff_1$ とすれば $(V_1, Q|_{V_1}) \cong H_2$ で非退化, よって

$$V = V_1 \oplus V_1^\perp$$

と分解する. 以下 $V_1^\perp$ に同様なことを繰り返せば,

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_m \oplus V_0, \qquad \begin{cases} V_i = Fe_i + Ff_i, \ Q(e_i) = Q(f_i) = 0, \ B(e_i, f_i) = 1 \ \ (i \neq 0) \\ V_i \perp V_j \ \ (i \neq j) \\ V_0 \text{ は非等方的} \end{cases}$$

と分解する. $W = Fe_1 + \cdots + Fe_m, W' = Ff_1 + \cdots + Ff_m$ とおけば

$$W \oplus W' = V_1 \oplus \cdots \oplus V_m \cong H_2 \perp \cdots \perp H_2 \cong H_{2m}$$

(一意性) : V のもう一つの分解

$$V = (Y \oplus Y') \oplus X \qquad \begin{cases} Y, Y' \text{ は全等方的で } Y \oplus Y' \cong H_{2k} \\ X \text{ は非等方的で } (Y \oplus Y') \perp X \end{cases}$$

があったとする. $k < m$ と仮定すると

$$V = H_{2k} \oplus X = H_{2m} \oplus V_0 = H_{2k} \oplus H_{2(m-k)} \oplus V_0$$

であり, 定理 4 から

$$^\exists g \in O(V) \text{ s.t. } g|_{H_{2k}} = \mathrm{id}$$

である. このとき

$$X \cong g(X) = g(H_{2k}^\perp) = g(H_{2k})^\perp = H_{2(m-k)} \oplus V_0$$

となるから, X は $H_{2(m-k)}$ を含み非等方的であることに矛盾する. よって $m = k$ で $X \cong V_0$. □

例　$F = \mathbf{R}$ のとき, $(\mathbf{R}^n, Q)$ を非退化 2 次空間とすると

$$(\mathbf{R}^n, Q) \cong \langle 1, \cdots, 1, -1, \cdots, -1 \rangle_{\mathbf{R}} = \langle 1_p, -1_q \rangle_{\mathbf{R}}$$

$n = p + q = \dim V$ とすると $m = \min(p, q)$ が Witt 指数になる.

系 5

(V, Q) を非退化 2 次空間で $\dim V = 2$ とする.

$$\textbf{(V, Q) が等方的} \iff \textbf{$(V, Q) \cong H_2$} \iff \textbf{$\delta(Q) = [1]$}$$

証明　前半の同値性と後半 ($\Longrightarrow$) は容易. ($\Longleftarrow$): $(V, Q) \cong \langle \alpha, \beta \rangle_F$ とする. $\delta(Q) = [-\alpha\beta] = [1]$ だから

$$^\exists \xi \in F^\times \text{ s.t. } \beta = -\alpha^{-1}\xi^2 = -\alpha(\alpha^{-1}\xi)^2$$

よって

$$\langle \alpha, \beta \rangle_F = \langle \alpha, -\alpha(\alpha^{-1}\xi)^2 \rangle_F \cong \langle \alpha, -\alpha \rangle_F \cong H_2$$

□

記号　2 次空間 (V, Q) に対し,

$$V^* = V - \{0\}, \qquad Q(V^*) = \{Q(v) : v \in V^*\}$$

とおく.

系 6

(V, Q) を等方的な非退化 2 次空間とすれば, $Q(V^*) = F$ である.

証明　等方的だから, Witt 分解は $(V, Q) = H_{2m} \perp (V_0, Q|_{V_0})$, $m \geq 1$ となる. $^\forall\lambda \in F$ に対し

$$Q(e_1 + 2^{-1}\lambda f_1) = 2B(e_1, 2^{-1}\lambda f_1) + Q(e_1) + 4^{-1}\lambda^2 Q(f_1) = \lambda$$

だから, $F \subset Q(V^*)$ である. □

系 7

(V_1, Q_1) と (V_2, Q_2) を非退化 2 次空間とするとき

$$\textbf{$(V_1, Q_1) \perp (V_2, -Q_2)$ が等方的} \iff \textbf{$Q_1({V_1}^*) \cap Q_2({V_2}^*) \neq \emptyset$}$$

証明　($\Longrightarrow$) 仮定から $(0,0) \neq (v_1, v_2) \in V_1 \perp V_2$ で $Q_1(v_1) - Q_2(v_2) = 0$ が取れる. よって $Q_1(v_1) = Q_2(v_2)$
$Q_1(v_1) \neq 0$ のとき: $v_1 \neq 0, v_2 \neq 0$ だから, $Q_1(v_1) = Q_2(v_2) \in Q_1({V_1}^*) \cap Q_2({V_2}^*)$.
$Q_1(v_1) = 0$ かつ $v_1 \neq 0$ のとき: Q_1 は等方的だから, 系 6 から $Q_1({V_1}^*) = F$. よって $Q_1({V_1}^*) \cap Q_2({V_2}^*) = Q_2({V_2}^*) \neq \emptyset$
$v_1 = 0$ のとき: $v_2 \neq 0$ で $Q_2(v_2) = 0$ だから Q_2 が等方的で $Q_2({V_2}^*) = F$.
($\Longleftarrow$) $Q_1(v_1) = Q_2(v_2)$, $v_1 \in {V_1}^*$, $v_2 \in {V_2}^*$ が取れて, $Q_1(v_1) - Q_2(v_2) = 0$ となるから. □

11　低次元2次空間と四元数環

F は体で $\mathrm{ch}(F) \neq 2$ とする.

(1) 2 次元 2 次空間
K/F を拡大体で $[K:F]=2$ とすると, 対合 $\rho : K \longrightarrow K, K^{\rho} = F$ が一意にとれる. このとき

$$N_{K/F}(a) = a\rho(a) \qquad (a \in K)$$

を K/F のノルムという. $K = F + F\xi$, $\rho(\xi) = -\xi$ とすると

$$N_{K/F}(x+y\xi) = (x+y\xi)(x-y\xi) = x^2 - y^2\xi^2, \qquad (x, y \in F)$$

より, $(K, N_{K/F})$ は F 上 2 次元の 2 次空間となり

$$(K, N_{K/F}) \cong \langle 1, -\xi^2 \rangle_F$$

である. これをノルム形式という.

Prop 4

(V, Q) が非退化 2 次空間で $\dim V = 2$ とする. このとき

$$\delta(Q) \neq [1] \iff {}^{\exists}K/F,\ {}^{\exists}\lambda \in F^{\times}\ \ s.t.\ \ (V,Q) \cong (K, \lambda N_{K/F})$$

ここで K は $K = F(\sqrt{\delta(Q)})$ でよい.

証明 $(\Longrightarrow)$ $(V,Q) \cong \langle \alpha, \beta \rangle_F$ とすると

$$\delta(Q) = -\alpha\beta \notin (F^{\times})^2$$

$\xi = \sqrt{-\alpha^{-1}\beta}$ として, $K = F(\xi) = F(\alpha^2\xi) = F(\sqrt{\delta(Q)})$, $\lambda = \alpha$ とおけば

$$(K, \lambda N_{K/F}) \cong \lambda\langle 1, -\xi^2 \rangle_F = \langle \alpha, \beta \rangle_F \cong (V, Q)$$

$(\Longleftarrow)$ は容易. □

(2) 3 次元と 4 次元 2 次空間
$A = (\alpha, \beta)_F = Fe_0 + Fe_1 + Fe_2 + Fe_3$ を四元数環とし, $N(x) = xx^{\iota}$ をノルムとする.

$$A_0 = \{v \in A : v + v^{\iota} = 0\} = Fe_1 + Fe_2 + Fe_3, \qquad N_0 = N|_{A_0}$$

とおく. このとき (A, N), (A_0, N_0) は 2 次空間で, 基底 e_0, e_1, e_2, e_3 により

$$T_N = \mathrm{diag}(1, -\alpha, -\beta, \alpha\beta)$$

だから

$$(A,N) \cong \langle 1,-\alpha,-\beta,\alpha\beta\rangle_F, \qquad (A_0,N_0) \cong \langle -\alpha,-\beta,\alpha\beta\rangle_F$$

となる.

$$\delta(N) = [\alpha^2\beta^2] = [1], \qquad \delta(N_0) = [-\alpha^2\beta^2] = [-1]$$

である.

Prop 5

$A = (\alpha,\beta)_F, A' = (\alpha',\beta')_F$ を四元数環とし, N, N' をそのノルムとする.
(1) $A \cong \mathbf{M}_2(F) \iff N$ が等方的 $\iff N_0$ が等方的
(2) A が斜体 $\iff N$ が非等方的 $\iff N_0$ が非等方的
(3) $A \cong A' \iff (A,N) \cong (A',N') \iff (A_0,N_0) \cong (A_0{}',N_0{}')$

証明 (1) の最初は定理 1 から. N_0 が等方的 $\implies$ N が等方的 は明らか. 逆に N が等方的 とする. このとき $(A,N) \cong H_4$ だから, A は 2 次元の全等方的部分空間 W を含む. $\dim A_0 = 3$ だから $W \cap A_0 \neq \{0\}$. よって N_0 も等方的である. (2) は (1) の対偶である. (3) 練習問題. □

Prop 6

(V,Q) は非退化 2 次空間で, $\delta(Q) = [\delta]$ とする.
(1) $\dim V = 3$ のとき

$$^\exists A \text{ 四元数環 } s.t. \ (V,Q) \cong (A_0, -\delta N_0)$$

(2) $\dim V = 4$ かつ $\delta(Q) = [1]$ のとき

$$^\exists A \text{ 四元数環 } {}^\exists \lambda \in F^\times \ s.t. \ (V,Q) \cong (A, \lambda N)$$

証明 (1) $(V,Q) \cong \langle \alpha,\beta,\gamma\rangle_F$ とすると $\delta = -\alpha\beta\gamma$ である. $A = (-\beta\gamma, -\alpha\gamma)_F$ とすれば

$$(A_0, -\delta N_0) \cong \alpha\beta\gamma\langle\beta\gamma,\alpha\gamma,\alpha\beta\gamma^2\rangle_F = \langle\alpha\beta^2\gamma^2, \beta\alpha^2\gamma^2, \gamma(\alpha\beta\gamma)^2\rangle_F \cong \langle\alpha,\beta,\gamma\rangle_F$$

(2) $x \in V, Q(x) \neq 0$ をとり, $W = \{x\}^\perp$ とおけば $V = Fx \oplus W$. $(W, Q|_W)$ に (1) を用いれば

$$^\exists A \text{ s.t. } (W, Q|_W) \cong (A_0, \lambda N_0), \qquad \text{ここで } [-\lambda] = \delta(Q|_W)$$

$g : A_0 \longrightarrow W$ をこの等長同型写像とする. $\delta(Q) = [\lambda Q(x)] = [1]$ だから

$$^\exists \beta \in F^\times \text{ s.t. } Q(x) = \lambda\beta^2$$

そこで

$$f : A = Fe_0 + A_0 \longrightarrow V : f(ae_0 + y) = \beta^{-1}ax + g(y) \qquad (a \in F,\ y \in A_0)$$

と定義すれば

$$Q(f(ae_o + y)) = \beta^{-2}a^2Q(x) + Q(g(y)) = \lambda a^2 + \lambda N_0(y) = \lambda N(ae_0 + y)$$

となるから, $(V, Q) \cong (A, \lambda N)$ である. □

12　p 進体の 2 次拡大

p 進体について, 以下で必要となる事柄をまとめておく. 素数 p を固定する. $0 \neq {}^{\forall}n \in \mathbf{Z}$ に対し, $n = p^k n'$, $p \nmid n'$, のとき

$$|n|_p = p^{-k}$$

と定義し, さらに

$${}^{\forall}n/m \in \mathbf{Q},\ \ |n/m|_p = |n|_p |m|_p^{-1}, \qquad |0|_p = 0$$

により

$$|\cdot|_p : \mathbf{Q} \longrightarrow \mathbf{R}$$

を定義する. このとき

$$d_p : \mathbf{Q} \times \mathbf{Q} \longrightarrow \mathbf{R} : d_p(x, y) = |x - y|_p$$

は距離になる.

$$R_p = \{\{a_i\}_{i=1}^{\infty} : \mathbf{Q} \text{ の } d_p \text{ に関するコーシー列 }\}$$

として, R_p に和と積を

$$\{a_i\} + \{b_i\} = \{a_i + b_i\}, \quad \{a_i\} \cdot \{b_i\} = \{a_i b_i\}$$

と定義すれば R_p は可換環になる. さらに

$$I_p = \{\{a_i\} \in R_p : \lim a_i = 0\}$$

とすると, I_p は極大イデアルになる. よって R_p/I_p は体. これを

$$\mathbf{Q}_p = R_p/I_p$$

と表わし, p 進体という.

$$\mathbf{Q} \longrightarrow \mathbf{Q}_p : r \mapsto \{r, r, r, r, \cdots\} + I_p$$

により $\mathbf{Q} \subset \mathbf{Q}_p$ とみなす. $\mathbf{Q}_p$ は $\mathbf{Q}$ の d_p に関する完備化である. $|\cdot|_p$ は

$$a = \{a_i\} + I_p \in \mathbf{Q}_p,\ \ |a|_p = \lim |a_i|_p$$

により $\mathbf{Q}_p$ に延長できる.

$$\mathbf{Z}_p = \mathbf{Z} \text{ の } \mathbf{Q}_p \text{ における閉包}$$

とけば, $\mathbf{Z}_p$ は開かつコンパクトな部分環で

$$\mathbf{Z}_p = \{a \in \mathbf{Q}_p : |a|_p \leq 1\}$$

となる. $p\mathbf{Z}_p = \{a \in \mathbf{Z}_p : |a|_p < 1\}$ は $\mathbf{Z}_p$ の唯一つの素イデアルである.

Lemma 14

(1) $\forall a \in \mathbf{Q}_p$ は, $k = -\log_p |a|_p \in \mathbf{Z}$ とすると次の表示をもつ.

$$a = \sum_{i=k}^{\infty} a_i p^i \qquad a_i \in \{0, 1, \cdots, p-1\}$$

(2) $\mathbf{Z} \subset \mathbf{Z}_p$ により, $\mathbf{Z}/p\mathbf{Z} \cong \mathbf{Z}_p/p\mathbf{Z}_p$ である.
(3) $\mathbf{Z}_p^{\times} = \{a \in \mathbf{Z}_p \ : \ |a|_p = 1\} = \mathbf{Z}_p - p\mathbf{Z}_p$
(4) $\mathbf{Q}_p^{\times} = p^{\mathbf{Z}} \cdot \mathbf{Z}_p^{\times} = \{p^k u \ : \ k \in \mathbf{Z}, \ u \in \mathbf{Z}_p^{\times}\}$
(5) $\mathbf{Z}_p$, $\mathbf{Z}_p^{\times}$ は開かつコンパクトな集合である. とくに $\mathbf{Q}_p$ は局所コンパクト位相体で, $\mathbf{Q}_p^{\times}$ は局所コンパクト位相群である.

(証明は容易)

$a \in \mathbf{Z}_p$ を

$$a = \sum_{i=0}^{\infty} a_i p^i$$

とすると,

$$a \equiv a_0 \mod p \quad \text{すなわち} \quad \overline{a} = \overline{a}_0 \in \mathbf{F}_p$$

である. そこで

$$\chi_p(a) = \begin{cases} 1 & (\overline{a} \in (\mathbf{F}_p{}^{\times})^2) \\ -1 & (\overline{a} \notin (\mathbf{F}_p{}^{\times})^2) \\ 0 & (\overline{a} = 0) \end{cases}$$

と定義する. $a \in \mathbf{Z}_p^{\times}$ ならば $\overline{a} \neq 0$ だから

$$\chi_p : \mathbf{Z}_p^{\times} \longrightarrow \{\pm 1\}$$

であり, これは準同型写像になる.

Lemma 15

(1) $p \neq 2$ のとき, $\ker \chi_p = (\mathbf{Z}_p^{\times})^2$ である. よって $\mathbf{Z}_p^{\times}/(\mathbf{Z}_p^{\times})^2$ は位数 **2** である. その代表系を $\{1, \epsilon\}$ とすると, $\mathbf{Q}_p^{\times}/(\mathbf{Q}_p^{\times})^2 = \{[1], [\epsilon], [p], [\epsilon p]\}$ である.
(2) $p = 2$ のとき $(\mathbf{Z}_2^{\times})^2 = \{a \in \mathbf{Z}_2^{\times} \ : \ a \equiv 1 \mod 8\}$ が成り立つ. とくに $\mathbf{Z}_2^{\times}/(\mathbf{Z}_2^{\times})^2$ は位数 **4** で,$\{\pm 1, \pm 3\}$ がその代表系になる. また $\mathbf{Q}_2^{\times}/(\mathbf{Q}_2^{\times})^2 = \{\pm[1], \pm[3], \pm[2], \pm[6]\}$ である.

(証明は略)

$[1] \neq [\alpha] \in \mathbf{Q}_p^{\times}/(\mathbf{Q}_p^{\times})^2$ として, $\xi = \sqrt{\alpha}$ とおき

$$K = \mathbf{Q}_p(\xi) = \{a + b\xi \ : \ a, b \in \mathbf{Q}_p\} \cong \mathbf{Q}_p[X]/(X^2 - \alpha)$$

とすれば $K/\mathbf{Q}_p$ は 2 次拡大となる. よって

$$^{\exists}\rho : K \longrightarrow K \text{ 対合 s.t. } K^{\rho} = \mathbf{Q}_p$$

$x \in K$ に対し

$$N_{K/\mathbf{Q}_p}(x) = x\rho(x) \in \mathbf{Q}_p$$

をノルムという.

$$N_{K/\mathbf{Q}_p} : K^{\times} \longrightarrow \mathbf{Q}_p^{\times}$$

は群の準同型写像になる. そこで

$$|\cdot|_K : K \longrightarrow \mathbf{R} : |x|_K = |N_{K/\mathbf{Q}_p}(x)|_p^{1/2}$$

と定義すれば, 距離 $d_K(x, y) = |x - y|_K$ により K は完備距離空間になる.

$$O_K = \{x \in K : |x|_K \leq 1\}, \qquad P_K := \{x \in K : |x|_K < 1\}$$

とおけば, 次が成り立つ.

(1) O_K は P_K をただ一つの素イデアルにもつ整域である.

(2) $O_K \cap \mathbf{Q}_p = \mathbf{Z}_p$, $P_K \cap \mathbf{Q}_p = p\mathbf{Z}_p$, $\mathbf{F}_p = \mathbf{Z}_p/p\mathbf{Z}_p \subset O_K/P_K$ である.

(3) $\pi = \pi_K \in P_K - {P_K}^2$ を一つ固定する. このとき $P_K = \pi O_K$ で, O_K/P_K の代表系 $\{c_1, \cdots, c_n\}$ を固定すれば, K の任意の元 x は

$$x = \sum_{i=k}^{\infty} c_i \pi^i,$$

と一意に表示できる.

(4) $O_K^{\times} = O_K - P_K$, $K^{\times} = \pi^{\mathbf{Z}} \cdot O_K^{\times}$

(5) O_K, $O_K^{\times}$ は開かつコンパクトで, K は局所コンパクト体, $K^{\times}$ は局所コンパクト群である.

$|\mathbf{Q}_p^{\times}|_K = |\mathbf{Q}_p^{\times}|_p$ だから

$$|\mathbf{Q}_p^{\times}|_p \subset |K^{\times}|_K = \{|x|_K : x \in K^{\times}\}$$

そこで

$$e = e_K = [|K^{\times}|_K : |\mathbf{Q}_p^{\times}|_p]$$

とおく. また, O_K/P_K は $\mathbf{F}_p$ の拡大体だから, 拡大次数を

$$f = f_K = [O_K/P_K : \mathbf{F}_p]$$

とおく.

Def e を $K/\mathbf{Q}_p$ の分岐指数, f を $K/\mathbf{Q}_p$ の不分岐次数という. また $e=1$ のとき $K/\mathbf{Q}_p$ を不分岐拡大といい, $e>1$ のとき $K/\mathbf{Q}_p$ を分岐拡大という.

Prop 7

$\boldsymbol{K=\mathbf{Q}_p(\sqrt{\alpha})/\mathbf{Q}_p}$ を **2** 次拡大とする.
(1) $\boldsymbol{ef=[K:\mathbf{Q}_p]}$ である. よって $\boldsymbol{e=1, f=2}$ または $\boldsymbol{e=2, f=1}$ である.
(2) $\boldsymbol{\mathbf{Q}_p}$ の不分岐拡大は一意に定まる.

$$\boldsymbol{e=1 \iff [\alpha]=[\epsilon]\in \mathbf{Z}_p^{\times}/(\mathbf{Z}_p^{\times})^2}$$

ただし $\boldsymbol{p=2}$ のとき, $\boldsymbol{[\epsilon]=[-3]}$ とする.
(3) $\boldsymbol{K/\mathbf{Q}_p}$ が不分岐ならば $\boldsymbol{N_{K/\mathbf{Q}_p}(O_K^{\times})=\mathbf{Z}_p^{\times}}$ である.

(証明は略)

13 Minkowski-Hasse 不変量

以下, p は素数 または $p=\infty$ として, $p=\infty$ のとき $\mathbf{Q}_\infty=\mathbf{R}$ と定める.

Def $\alpha,\beta\in\mathbf{Q}_p^\times$ に対して

$$h_p(\alpha,\beta)=\begin{cases}1 & (\langle\alpha,\beta,-1\rangle_{\mathbf{Q}_p}\ \text{が等方的})\\ -1 & (\langle\alpha,\beta,-1\rangle_{\mathbf{Q}_p}\ \text{が非等方的})\end{cases}$$

と定義する. h_p を **Hilbert のノルム剰余記号**という.

Prop 8

$\alpha,\beta,\gamma\in\mathbf{Q}_p^\times$ に対し, 次が成り立つ.
(1) $h_p(\alpha,\beta)=h_p(\beta,\alpha)$
(2) $h_p(\alpha,\beta\gamma^2)=h_p(\alpha,\beta)$, とくに $h_p(\alpha,\gamma^2)=h_p(\alpha,1)=1$
(3) $h_p(\alpha,\beta\gamma)=h_p(\alpha,\beta)h_p(\alpha,\gamma)$
(4) $h_p(\alpha,-\alpha)=1$ とくに $h_p(\alpha,\alpha)=h_p(\alpha,-1)$
(5) $h_p(\alpha,1-\alpha)=1$ $(\alpha\neq 1)$
(6) $h_p(\alpha,\beta)=1\ {}^\forall\beta\in\mathbf{Q}_p^\times \iff \alpha\in(\mathbf{Q}_p^\times)^2$
(7) $2\neq p<\infty$ で $\alpha,\beta\in\mathbf{Z}_p^\times$ のとき,

$$h_p(\alpha,\beta)=1,\qquad h_p(\alpha,p)=\chi_p(\alpha)=\begin{cases}1 & (\alpha \mod p\in(\mathbf{F}_p^\times)^2)\\ -1 & (\alpha \mod p\notin(\mathbf{F}_p^\times)^2)\end{cases}$$

(8) $p=2$ で $\alpha,\beta\in\mathbf{Z}_2^\times$ のとき

$$h_2(\alpha,\beta)=1 \iff \alpha\equiv 1 \mod 4 \text{ または } \beta\equiv 1 \mod 4$$
$$h_2(\alpha,2)=1 \iff \alpha\equiv\pm 1 \mod 8$$

(9) $p=\infty$ のとき

$$h_\infty(\alpha,\beta)=-1 \iff \alpha<0,\ \beta<0$$

証明 定義から

$$h_p(\alpha,\beta)=1 \iff \alpha x^2+\beta y^2=z^2 \text{ が } \mathbf{Q}_p \text{ で非自明解 } (x,y,z)\neq(0,0,0) \text{ をもつ}$$

であるから, (1), (2), (4), (5), (9) は明らか. とくに (2) から

$$h_p:\mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^2\times\mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^2\longrightarrow\{\pm1\}$$

である. よって h_p は $\mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^2$ の代表系での値で完全に決まる.

(7) $2 \neq p < \infty$ のとき, $\mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^2 = \{[1], [\epsilon], [p], [\epsilon p]\}$ である.
(case 1) $\alpha, \beta \in \mathbf{Z}_p^\times$ ならば, $[\alpha], [\beta] \in \{[1], [\epsilon]\}$ で

$$h_p(\alpha, \beta) = h_p(1, 1),\ h_p(1, \epsilon),\ h_p(\epsilon, \epsilon)$$

の 3 通り. $h_p(1,1) = h_p(1,\epsilon) = 1$ は明らか. $h_p(\epsilon, \epsilon)$ を決めるために

$$\epsilon x^2 + \epsilon y^2 = z^2$$

の非自明解を調べる. $K = \mathbf{Q}_p(\sqrt{\epsilon})$ は不分岐 2 次拡大で, Prop 7 から $N_{K/\mathbf{Q}_p}(O_K^\times) = \mathbf{Z}_p^\times$ であった. $\epsilon \in \mathbf{Z}_p^\times$ だから

$$^\exists a + b\sqrt{\epsilon} \in K^\times \ \text{ s.t. } \ N_{K/\mathbf{Q}_p}(a + b\sqrt{\epsilon}) = a^2 - b^2\epsilon = \epsilon$$

よって非自明解 $(x, y, z) = (1, b, a)$ が存在するので $h_p(\epsilon, \epsilon) = 1$ である.
(case 2) $h(\epsilon, p)$ を求める. もし $h_p(\epsilon, p) = 1$ ならば, $\epsilon x^2 + py^2 = z^2$ は非自明解 $(x, y, z) = (a, b, c)$ をもつ. $a, b, c, \in \mathbf{Z}_p$ としてよい. $a = 0$ ならば, $p \in (\mathbf{Q}_p^\times)^2$ で矛盾するから, $a \neq 0$. このとき $\overline{\epsilon a}^2 = \overline{c}^2$ より, $\overline{\epsilon} \in (\mathbf{F}_p{}^\times)^2$ で $\chi_p(\epsilon) = 1$. Lemma 15 から $\epsilon \in (\mathbf{Z}_p^\times)^2$ で ϵ の取り方に矛盾する. よって $h_p(\epsilon, p) = -1$.
(case 3) $h_p(\epsilon, \epsilon p)$ を求める.

$$\epsilon x^2 + \epsilon p y^2 = z^2 \iff x^2 + py^2 = \epsilon(\epsilon^{-1}z)^2$$

非自明解 $(x, y, z) = (a, b, c)$ があったとする. $a, b, c, \in \mathbf{Z}_p$ で $\epsilon p \notin (\mathbf{Q}_p^\times)^2$ だから $a \neq 0$ としてよい. $\mod p$ をとれば $\chi_p(\epsilon) = 1$ で矛盾する. よって

$$h_p(\epsilon, \epsilon p) = h_p(\epsilon, -p) = -1$$

(case 4) $h_p(p, \epsilon p)$ を決める.

$$px^2 + \epsilon p y^2 = z^2 \iff x^2 + \epsilon y^2 = p(p^{-1}z)^2$$

だから

$$h_p(p, \epsilon p) = h_p(p, -\epsilon) = \begin{cases} 1 & ([-\epsilon] = [1]) \\ -1 & ([-\epsilon] = [\epsilon]) \end{cases} = \begin{cases} 1 & (\chi_p(-1) = -1) \\ -1 & (\chi_p(-1) = 1) \end{cases}$$

同様に $h_p(p, p)$ も計算できて, $\mathbf{Q}_p^\times \times \mathbf{Q}_p^\times$ 上の h_p の値が完全に決まる.
(8) も同様に個別に値を計算する.
(3) と (6) は (7) と (8) の計算結果の結論である. □

系 8

$\boldsymbol{\alpha \in \mathbf{Q}_p^\times}$ に対し,

$$\boldsymbol{h_{p,\alpha} : \mathbf{Q}_p^\times \longrightarrow \{\pm 1\} : h_{p,\alpha}(\lambda) = h_p(\alpha, \lambda)}$$

は準同型写像である. また $\boldsymbol{h_{p,\alpha}}$ が全射 $\boldsymbol{\iff \alpha \notin (\mathbf{Q}_p^\times)^2}$

Prop 9

$\alpha_1, \cdots, \alpha_n, \beta_1, \cdots, \beta_n \in \mathbf{Q}_p^\times$ に対し

$$\langle \alpha_1, \cdots, \alpha_n \rangle_{\mathbf{Q}_p} \cong \langle \beta_1, \cdots, \beta_n \rangle_{\mathbf{Q}_p} \implies \prod_{1 \le i < j \le n} h_p(\alpha_i, \alpha_j) = \prod_{1 \le i < j \le n} h_p(\beta_i, \beta_j)$$

である.

証明 (概略) (V, Q) を非退化 2 次空間とする. V の二つの直交基底の組, $E = (e_1, \cdots, e_n)$ と $E' = (e_1', \cdots, e_n')$ が link するということを

$$E \sim E' \iff {}^\exists i_0, j_0 \quad \text{s.t.} \quad e_{i_0} = e_{j_0}'$$

により定義する. $\dim V \ge 3$ ならば V の任意の直交基底 E, E' に対し,

$${}^\exists E_1, \cdots, E_k \ \ V \text{ の直交基底の列 s.t. } E \sim E_1 \sim E_2 \sim \cdots \sim E_k \sim E'$$

が成り立つ.
基底 E で $(V,Q) \cong \langle \alpha_1, \cdots, \alpha_n \rangle_{\mathbf{Q}_p}$, E' で $(V,Q) \cong \langle \beta_1, \cdots, \beta_n \rangle_{\mathbf{Q}_p}$ とする.

$$\prod_{1 \le i < j \le n} h_p(\alpha_i, \alpha_j) = \prod_{1 \le i < j \le n} h_p(\beta_i, \beta_j) \tag{13.1}$$

を n の帰納法で示す. $n = 2$ のとき, $\langle \alpha_1, \alpha_2 \rangle_{\mathbf{Q}_p} \cong \langle \beta_1, \beta_2 \rangle_{\mathbf{Q}_p}$ ならば, $\langle \alpha_1, \alpha_2, -1 \rangle_{\mathbf{Q}_p} \cong \langle \beta_1, \beta_2, -1 \rangle_{\mathbf{Q}_p}$ だから, 定義により $h_p(\alpha_1, \alpha_2) = h_p(\beta_1, \beta_2)$ となる. 以下 $n \ge 3$ とする.
(case 1) E' が E の置換のとき: このとき, $\beta_1, \cdots, \beta_n$ は $\alpha_1, \cdots, \alpha_n$ の置換である. 互換で $\beta_k = \alpha_{k+1}, \beta_{k+1} = \alpha_k, \beta_i = \alpha_i \ \ (i \ne k, k+1)$ の場合を示せば十分. $k, k+1$ を含む項は

$$\left(\prod_{i<k} h_p(\alpha_i, \alpha_k) h_p(\alpha_i, \alpha_{k+1}) \right) h_p(\alpha_k, \alpha_{k+1}) \left(\prod_{k+1<j} h_p(\alpha_k, \alpha_j) h_p(\alpha_{k+1}, \alpha_j) \right)$$
$$= \left(\prod_{i<k} h_p(\beta_i, \beta_{k+1}) h_p(\beta_i, \beta_k) \right) h_p(\beta_{k+1}, \beta_k) \left(\prod_{k+1<j} h_p(\beta_{k+1}, \beta_j) h_p(\beta_k, \beta_j) \right)$$

となるから, (13.1) が成り立つ.
(case 2) $E \sim E'$ のとき: (case 1) から, $e_1 = e_1'$ の場合に帰着する. このとき $\alpha_1 = \beta_1$.

$$(V,Q) \cong \langle \alpha_1 \rangle_{\mathbf{Q}_p} \perp \langle \alpha_2, \cdots, \alpha_n \rangle_{\mathbf{Q}_p} \cong \langle \alpha_1 \rangle_{\mathbf{Q}_p} \perp \langle \beta_2, \cdots, \beta_n \rangle_{\mathbf{Q}_p}$$

より, Witt の定理から

$$\langle \alpha_2, \cdots, \alpha_n \rangle_{\mathbf{Q}_p} \cong \langle \beta_2, \cdots, \beta_n \rangle_{\mathbf{Q}_p}$$

帰納法の仮定から

$$\prod_{2 \le i < j \le n} h_p(\alpha_i, \alpha_j) = \prod_{2 \le 1 < j \le n} h_p(\beta_i, \beta_j)$$

残りの項は

$$\begin{aligned} h_p(\alpha_1,\alpha_2)\cdots h_p(\alpha_1,\alpha_n) &= h_p(\alpha_1,\alpha_2\cdots\alpha_n) = h_p(\alpha_1,\alpha_1^{-1})h_p(\alpha_1,\alpha_1\alpha_2\cdots\alpha_n) \\ &= h_p(\alpha_1,\alpha_1^{-1})h_p(\alpha_1,(-1)^{n(n-1)/2}\delta(Q)) \\ &= h_p(\beta_1,\beta_1^{-1})h_p(\beta_1,(-1)^{n(n-1)/2}\delta(Q)) \end{aligned}$$

となるので, (13.1) が成り立つ. □

Def 非退化 2 次空間 (V,Q) に対し, $(V,Q)\cong\langle\alpha_1,\cdots,\alpha_n\rangle_{\mathbf{Q}_p}$ であるとき

$$\chi_p((V,Q)) = \chi_p(Q) = \prod_{1\le i<j\le n} h_p(\alpha_i,\alpha_j)$$

とおき, これを (V,Q) の **Minkowski-Hasse 不変量**という. Prop 9 より, $\chi_p(Q)$ は Q の対角化の仕方に依存しない.

Lemma 16

p を素数, $(V,Q),(V_1,Q_1),(V_2,Q_2)$ を非退化 2 次空間とし, $\lambda\in\mathbf{Q}_p^\times$ とする.
(1) $\chi_p(\lambda Q) = h_p(\lambda,-1)^{n(n-1)/2}h_p(\lambda,\det T_Q)^{n-1}\chi_p(Q)$　ただし $n=\dim V$.
(2) $\chi_p(Q_1\perp Q_2) = \chi_p(Q_1)\chi_p(Q_2)h_p(\det T_{Q_1},\det T_{Q_2})$

証明 (1) $(V,Q)\cong\langle\alpha_1,\cdots,\alpha_n\rangle_{\mathbf{Q}_p}$ とすると

$$\begin{aligned} \chi_p(\lambda Q) &= \prod_{1\le i<j\le n} h_p(\lambda\alpha_i,\lambda\alpha_j) = \prod_{1\le i<j\le n} h_p(\lambda,\lambda)h_p(\lambda,\alpha_i)h_p(\lambda,\alpha_j)h_p(\alpha_i,\alpha_j) \\ &= h_p(\lambda,\lambda)^{n(n-1)/2}h_p(\lambda,\alpha_1)^{n-1}h_p(\lambda,\alpha_2)^{n-1}\cdots h_p(\lambda,\alpha_n)^{n-1}\chi_p(Q) \\ &= h_p(\lambda,-1)^{n(n-1)/2}h_p(\lambda,\det T_Q)^{n-1}\chi_p(Q) \end{aligned}$$

(2) $(V_1,Q_1)=\langle\alpha_1,\cdots,\alpha_m\rangle_{\mathbf{Q}_p}$, $(V_2,Q_2)\cong\langle\beta_1,\cdots,\beta_n\rangle_{\mathbf{Q}_p}$ とすると

$$\begin{aligned} \chi_p(Q) &= \prod_{1\le i<j\le m} h_p(\alpha_i,\alpha_j)\prod_{1\le i<j\le n} h_p(\beta_i,\beta_j)\prod_{\substack{1\le i\le m\\1\le j\le n}} h_p(\alpha_i,\beta_j) \\ &= \chi_p(Q_1)\chi_p(Q_2)h_p(\alpha_1\cdots\alpha_m,\beta_1\cdots\beta_n) \end{aligned}$$

□

14　p 進体上の 2 次形式

以下では p を素数, (V,Q) を $\mathbf{Q}_p$ 上の非退化 2 次空間とする. $Q(V^*)$ は

$$Q(V^*) = \bigsqcup_i \lambda_i (\mathbf{Q}_p^\times)^2$$

と $(\mathbf{Q}_p^\times)^2$ を法とする有限個の類の和集合になることに注意する.

Lemma 17

$\dim V = 2$ のとき, $\lambda \in \mathbf{Q}_p^\times$ に対し

$$\boldsymbol{\lambda \in Q(V^*) \iff \chi_p(Q) = h_p(\lambda, \delta(Q))}$$

証明 $(V,Q) \cong H_2$ ならば, $Q(V^*) = \mathbf{Q}_p$, $\chi_p(Q) = h_p(1,-1) = 1$, $\delta(Q) = [1]$ だから,

$$^\forall\lambda \text{ に対し } \ \lambda \in Q(V^*), \ \ \chi_p(Q) = h_p(\lambda, \delta(Q))$$

となる.
以下 $(V,Q) \cong \langle \alpha, \beta \rangle_{\mathbf{Q}_p} \ncong H_2$ とする.

$$\lambda \in Q(V^*) \iff \lambda^{-1} = \lambda\lambda^{-2} \in Q(V^*) \iff 0 \neq {}^\exists \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbf{Q}_p^2 \ \text{ s.t. } \ \alpha x^2 + \beta y^2 = \lambda^{-1}$$

$$\iff 0 \neq {}^\exists \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbf{Q}_p^3 \ \text{ s.t. } \ \lambda\alpha x^2 + \lambda\beta y^2 = z^2 \iff h_p(\lambda\alpha, \lambda\beta) = 1$$

である. ($z = 0$ なら $(V,Q) \ncong H_2$ に矛盾するので $z \neq 0$ となることに注意.) ここで

$$h_p(\lambda\alpha, \lambda\beta) = h_p(\lambda,\lambda) h_p(\lambda, \alpha\beta) h_p(\alpha,\beta) = h_p(\lambda,-1) h_p(\lambda,\alpha\beta)\chi_p(Q) = h_p(\lambda, \delta(Q))\chi_p(Q)$$

だから, 主張が示せた. □

Prop 10

$\dim V = 3$ のとき

$$\boldsymbol{(V,Q) \text{ が等方的} \iff \chi_p(Q) = h_p(-1, \delta(Q))}$$

証明 $(V,Q) \cong \langle \alpha_1, \alpha_2, \alpha_3 \rangle_{\mathbf{Q}_p}$ とする.

$$\begin{aligned}
(V,Q) \text{ が等方的} &\iff \alpha_1 x^2 + \alpha_2 y^2 + \alpha_3 z^2 = 0 \text{ が非自明解をもつ} \\
&\iff (-\alpha_1/\alpha_3)x^2 + (-\alpha_2/\alpha_3)y^2 = z^2 \text{ が非自明解をもつ} \\
&\iff h_p(-\alpha_1/\alpha_3, -\alpha_2/\alpha_3) = 1 \\
&\iff h_p(-\alpha_1\alpha_3, -\alpha_2\alpha_3) = 1 \\
&\iff h_p(-\alpha_1\alpha_3, \alpha_2) h_p(-\alpha_1\alpha_3, -\alpha_3) = 1 \\
&\iff h_p(-\alpha_1\alpha_3, \alpha_2) h_p(-\alpha_1, -\alpha_3) = 1 \quad (h_p(\alpha_3, -\alpha_3) = 1)
\end{aligned}$$

他方

$$\begin{aligned}
\chi_p(Q) h_p(-1, \delta(Q)) &= h_p(\alpha_1, \alpha_2) h_p(\alpha_1, \alpha_3) h_p(\alpha_2, \alpha_3) h_p(-1, -\alpha_1\alpha_2\alpha_3) \\
&= h_p(\alpha_1, \alpha_2) h_p(\alpha_1, \alpha_3) h_p(\alpha_2, \alpha_3) h_p(-1, -\alpha_1) h_p(-1, \alpha_2) h_p(-1, \alpha_3) \\
&= h_p(-\alpha_1, \alpha_2) h_p(-\alpha_1, \alpha_3) h_p(\alpha_2, \alpha_3) h_p(-1, -\alpha_1) \\
&= h_p(-\alpha_1, \alpha_2) h_p(-\alpha_1, -\alpha_3) h_p(\alpha_3, \alpha_2) \\
&= h_p(-\alpha_1\alpha_3, \alpha_2) h_p(-\alpha_1, -\alpha_3)
\end{aligned}$$

よって

$$(V,Q) \text{ が等方的} \iff \chi_p(Q) h_p(-1, \delta(Q)) = 1 \iff \chi_p(Q) = h_p(-1, \delta(Q))$$

□

系 9

四元数環 $\boldsymbol{A = (\alpha, \beta)_{\mathbf{Q}_p}}$ に対し

$$\boldsymbol{(A,N) \text{ が等方的} \iff h_p(\alpha,\beta) = 1 \iff \chi_p(N) = h_p(-1,-1) = \begin{cases} 1 & (p \neq 2) \\ -1 & (p = 2) \end{cases}}$$

証明 Prop 5 より

$$(A,N) \text{ が等方的} \iff (A,N) \cong (\mathrm{M}_2(\mathbf{Q}_p), \det) \cong H_4 \iff (A_0, N_0) \text{ が等方的}$$

$(A_0, N_0) \cong \langle -\alpha, -\beta, \alpha\beta \rangle_{\mathbf{Q}_p}$ から

$$\chi_p(N) = \chi_p(N_0) = h_p(-\alpha, -\beta) h_p(-\alpha, \alpha\beta) h_p(-\beta, \alpha\beta) = h_p(-1,-1) h_p(\alpha, \beta)$$

Prop 10 から

$$(A_0, N_0) \text{ が等方的} \iff h_p(-1,-1) h_p(\alpha,\beta) = h_p(-1, -\alpha^2\beta^2) \iff h_p(\alpha,\beta) = 1$$

□

Prop 11

$\dim V = 4$ のとき

$$\textbf{(}V, Q\textbf{) が非等方的} \iff \delta(Q) = [1] \text{ かつ } \chi_p(Q) = -h_p(-1,-1)$$

証明 ($\Longleftarrow$) $\delta(Q) = [1]$ だから, Prop 6 より

$$^{\exists}A = (\alpha, \beta)_{\mathbf{Q}_p}, \quad ^{\exists}\lambda \in \mathbf{Q}_p^{\times} \text{ s.t. } (V, Q) \cong (A, \lambda N)$$

Lemma 16 (1) より $\chi_p(Q) = \chi_p(\lambda N) = \chi_p(N)$ となるから, $\chi_p(N) = -h_p(-1,-1)$ で, 系 9 から (A, N) は非等方的, よって (V, Q) も非等方的である.

($\Longrightarrow$) $(V, Q) \cong \langle \alpha_1, \alpha_2, \alpha_3, \alpha_4 \rangle_{\mathbf{Q}_p}$ とする.

$$(V_1, Q_1) = \langle \alpha_1, \alpha_2 \rangle_{\mathbf{Q}_p}, \qquad (V_2, Q_2) = \langle -\alpha_3, -\alpha_4 \rangle_{\mathbf{Q}_p}$$

とおけば

$$(V, Q) = (V_1, Q_1) \perp (V_2, -Q_2)$$

系 7 から

$$(V, Q) \text{ が非等方的} \iff Q_1(V_1{}^*) \cap Q_2(V_2{}^*) = \emptyset$$

このとき $(V_i, Q_i) \ncong H_2$ $(i = 1, 2)$ である. (そうでなければ, $Q_1(V_1^*) = \mathbf{Q}_p$ または $Q_2(V_2^*) = \mathbf{Q}_p$ となり $Q_1(V_1{}^*) \cap Q_2(V_2{}^*) = \emptyset$ に矛盾.) よって, $\delta(Q_i) \neq [1]$, つまり

$$[-\alpha_1\alpha_2] \neq [1], \qquad [-\alpha_3\alpha_4] \neq [1]$$

したがって, 系 8 から

$$h_{p,-\alpha_1\alpha_2},\ h_{p,-\alpha_3\alpha_4} : \mathbf{Q}_p^{\times} \longrightarrow \{\pm 1\}$$

は全射である. Lemma 17 から

$$0 \neq \lambda \in Q_1(V_1{}^*) \iff h_p(\lambda, -\alpha_1\alpha_2) = h_p(\alpha_1, \alpha_2) \iff \lambda \in h^{-1}_{p,-\alpha_1\alpha_2}(h_p(\alpha_1, \alpha_2))$$

よって

$$\mathbf{Q}_p^{\times} = h^{-1}_{p,-\alpha_1\alpha_2}(h_p(\alpha_1, \alpha_2)) \sqcup h^{-1}_{p,-\alpha_1\alpha_2}(-h_p(\alpha_1, \alpha_2))$$

同様に

$$\mathbf{Q}_p^{\times} = h^{-1}_{p,-\alpha_3\alpha_4}(h_p(-\alpha_3, -\alpha_4)) \sqcup h^{-1}_{p,-\alpha_3\alpha_4}(-h_p(-\alpha_3, -\alpha_4))$$

$Q_1(V_1{}^*) \cap Q_2(V_2{}^*) = \emptyset$ ならば

$$h^{-1}_{p,-\alpha_1\alpha_2}(h_p(\alpha_1, \alpha_2)) = h^{-1}_{p,-\alpha_3\alpha_4}(-h_p(-\alpha_3, -\alpha_4)), \qquad h^{-1}_{p,-\alpha_1\alpha_2}(-h_p(\alpha_1, \alpha_2)) = h^{-1}_{p,-\alpha_3\alpha_4}(h_p(-\alpha_3, -\alpha_4))$$

でなければならない. 1 を含む方は核だから,

$$h_p(\alpha_1, \alpha_2) = -h_p(-\alpha_3, -\alpha_4)$$

これからまた

$$h_{p,-\alpha_1\alpha_2} = h_{p,-\alpha_3\alpha_4}, \quad \text{つまり} \quad h_{p,\alpha_1\alpha_2\alpha_3\alpha_4} \equiv 1$$

となるから, $\delta(Q) = [\alpha_1\alpha_2\alpha_3\alpha_4] = [1]$ である. 前半の証明と同様に, 系 9 から $\delta(Q) = -h_p(-1,-1)$ となる. □

系 10

$\dim V = 3$ のとき, $\mathbf{Q}_p^\times = \delta(Q)(\mathbf{Q}_p^\times)^2 \cup (Q(V^*) - \{0\})$ である.

証明 $(Q(V^*) - \{0\}) \neq \mathbf{Q}_p^\times$ とすると, $^\exists\lambda \notin (Q(V^*) - \{0\})$. このとき

$$Q(V^*) \cap \lambda(\mathbf{Q}_p^\times)^2 = \emptyset \quad \text{系 7 から} \quad (V', Q') = (V, Q) \perp \langle -\lambda \rangle_{\mathbf{Q}_p} \text{ は非等方的}$$

よって

$$\delta(Q') = \lambda\delta(Q) = [1]$$

つまり

$$\lambda \notin (Q(V^*) - \{0\}) \implies \lambda \in \delta(Q)(\mathbf{Q}_p^\times)^2$$

□

定理 6

$\dim V \geq 5$ ならば, (V, Q) は等方的である. とくに $Q(V^*) = \mathbf{Q}_p$ である.

証明 $\dim V = 5$ で示せばよい. $(V, Q) \cong \langle \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5 \rangle_{\mathbf{Q}_p}$ とする.

$$(V_1, Q_1) = \langle \alpha_1, \alpha_2, \alpha_3 \rangle_{\mathbf{Q}_p}, \qquad (V_2, Q_2) = \langle -\alpha_4, -\alpha_5 \rangle_{\mathbf{Q}_p}$$

とおく. $\mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^2$ の類の個数は 4 $(p \neq 2)$ または 8 $(p = 2)$ であるが, Lmma 17 より $Q_2({V_2}^*)/(\mathbf{Q}_p^\times)^2$ はちょうど半数の類を含み, 系 10 から $Q_1({V_1}^*)/(\mathbf{Q}_p^\times)^2$ は半数より多くの類を含む. これから

$$Q_1({V_1}^*) \cap Q_2({V_2}^*) \neq \emptyset$$

よって 系 7 から $(V_1Q_1) \perp (V_2, -Q_2) \cong (V, Q)$ は等方的である. □

系 11

$\dim V = 4$ ならば $Q(V^*) \cup \{0\} = \mathbf{Q}_p$ である.

証明 $\alpha \in \mathbf{Q}_p^\times$ に対し, $(V,Q) \perp \langle -\alpha \rangle_{\mathbf{Q}_p}$ は等方的だから, $Q(V^*) \cap \alpha(\mathbf{Q}_p^\times)^2 \neq \emptyset$. つまり $\alpha \in Q(V^*)$. よって $\mathbf{Q}_p^\times \subset Q(V^*)$ である. □

定理 7

$(V_1, Q_1), (V_2, Q_2)$ を $\mathbf{Q}_p$ 上の非退化 2 次形式とするとき

$$\boldsymbol{(V_1, Q_1) \cong (V_2, Q_2) \iff \dim V_1 = \dim V_2, \quad \delta(Q_1) = \delta(Q_2), \quad \chi_p(Q_1) = \chi_p(Q_2)}$$

証明 ($\Longleftarrow$) を示せばよい. $\dim V_1 = \dim V_2 = n$ の帰納法で示す.
$n = 1$ のとき: $(Q_1, V_1) \cong \langle \delta(Q_1) \rangle_{\mathbf{Q}_p} = \langle \delta(Q_2) \rangle_{\mathbf{Q}_p} \cong (V_2, Q_2)$.
$n \geq 2$ のとき: $Q_1(V_1^*) \cap Q_2(V_2^*) \neq \emptyset$ である. 実際, $n = 2$ のときは, Lemma 17 から $Q_1(V_1^*) = Q_2(V_2^*)$ である. また $n \geq 3$ のときは, $(V,Q) = (V_1, Q_1) \perp (V_2, -Q_2)$ は $\dim V \geq 5$ だから, 定理 6 により等方的になる. よって $Q_1(V_1^*) \cap Q_2(V_2^*) \neq \emptyset$ である. $0 \neq \alpha \in Q_1(V_1^*) \cap Q_2(V_2^*)$ をとれば,

$$(V_1, Q_1) = \langle \alpha \rangle_{\mathbf{Q}_p} \perp (V_1', Q_1'), \qquad (V_2, Q_2) = \langle \alpha \rangle_{\mathbf{Q}_p} \perp (V_2', Q_2')$$

と分解する. このとき

$$\dim V_1' = \dim V_2' = n - 1, \qquad \delta(Q_1') = \delta(Q_2'), \qquad \chi_p(Q_1') = \chi_p(Q_2')$$

だから, 帰納法の仮定により $(V_1', Q_1') \cong (V_2', Q_2')$. □

系 12

$\epsilon \in \mathbf{Z}_p^\times$ は $h_p(\epsilon, p) = -1$ を満たすとする.
(1) $\mathbf{Q}_p$ 上の非退化 4 次元非等方的 2 次空間は, 同型を除いてただ一つしかなく, それは

$$\boldsymbol{\langle 1, -\epsilon, -p, \epsilon p \rangle_{\mathbf{Q}_p}}$$

に同型である.
(2) $\mathbf{Q}_p$ 上の四元数体は, 同型を除いてただ一つしかなく, それは

$$\boldsymbol{D(K, p) = (\epsilon, p)_{\mathbf{Q}_p}}$$

に同型である. ここで $K/\mathbf{Q}_p$ は不分岐 2 次拡大とする.

15　有理数体上の四元数環

Prop 12

$\alpha, \beta \in \mathbf{Q}^\times$ に対し, 有限個の p を除いて $h_p(\alpha, \beta) = 1$ である. また

$$\prod_{p \leq \infty} h_p(\alpha, \beta) = 1$$

である.

証明 $h_p(\alpha, \beta) = h_p(\alpha(\mathbf{Q}^\times)^2, \beta(\mathbf{Q}^\times)^2)$ だから, $\alpha, \beta \in \mathbf{Z}$ としてよい. $p \nmid \alpha\beta$ かつ $p \neq 2, \infty$ ならば, $\alpha, \beta \in \mathbf{Z}_p^\times$ だから, このような p で $h_p(\alpha, \beta) = 1$.

$$\alpha = q_1 \cdots q_s, \qquad \beta = r_1 \cdots r_t \qquad (q_i, r_i \text{ は -1 または素数})$$

とすると

$$\prod_{p \leq \infty} h_p(\alpha, \beta) = \prod_{i,j} \prod_{p \leq \infty} h_p(q_i, r_j)$$

となる.

(case 1) $q_i = q, r_j = r$ が奇素数のとき

$$h_p(q, r) = \begin{cases} 1 & (p \neq 2, q, r) \\ (-1)^{(q-1)(r-1)/4} & (p = 2) \\ \chi_q(r) & (p = q) \\ \chi_r(q) & (p = r) \end{cases}$$

平方剰余の相互法則から

$$\prod_{p \leq \infty} h_p(q, r) = 1$$

となる.

以下同じように (case 2) $q_i = q$ が奇素数, $r_j = 2$　(case 3) $q_i = r_j = 2$　(case 4) $q_i = q$ が奇素数, $r_j = -1$　(case 5) $q_i = 2, r_j = -1$,　(case 6) $q_i = r_j = -1$ を個別に計算する.　□

$\alpha, \beta \in \mathbf{Q}^\times$ として, $A = (\alpha, \beta)_{\mathbf{Q}}$ を四元数環とする. このとき $p \leq \infty$ に対し

$$A_p = A \otimes \mathbf{Q}_p = (\alpha, \beta)_{\mathbf{Q}_p}$$

は系 2 から $\mathbf{Q}_p$ 上の四元数環になり,

$$A_p \cong \mathrm{M}_2(\mathbf{Q}_p) \iff h_p(\alpha, \beta) = 1$$

である.

系 13

A を $\mathbf{Q}$ 上の四元数環とするとき, 有限個の p を除いて $A_p \cong \mathbf{M}_2(\mathbf{Q}_p)$ であり, A_p が斜体となる $p \leq \infty$ は偶数個である.

Def A を $\mathbf{Q}$ 上の四元数環とするとき, A_p が斜体となる素数 p の積を $d(A)$ とおき, A の判別式という. (A_p が斜体となる p が存在しない場合は $d(A) = 1$ と定める.) また $A_\infty \cong \mathrm{M}_2(\mathbf{R})$ のとき, A は indefinite であるといい, $A_\infty \cong \mathbf{H}$ のとき A は definite であるという.

$$A \text{ が definite} \iff d(A) \text{ の素因数の個数は奇数}$$

である.

定理 8 (Minkowski - Hasse)

(V, Q) を $\mathbf{Q}$ 上の非退化 2 次空間として, 各 $p \leq \infty$ に対し, $V_p = V \otimes \mathbf{Q}_p$ とする. Q の V_p への自然な拡張を Q_p と表わす. このとき

$$(V, Q) \text{ が等方的} \iff \text{任意の } p \leq \infty \text{ で } (V_p, Q_p) \text{ が等方的}$$

証明 ($\Longrightarrow$) は明らか.
($\Longleftarrow$) $\dim V = 2$ のとき:

$$(V, Q) \cong \lambda\langle a, -1\rangle_{\mathbf{Q}}, \qquad (\lambda \in \mathbf{Q}^\times,\ a \in \mathbf{Z})$$

と書ける.

$$(V, Q) \text{ が等方的} \iff \delta(Q) = [1]$$

から, $\delta(Q) = [a] = [1]$ を示せばよい. (V_∞, Q_∞) が等方的だから, $a > 0$ である. a の素因数分解を $a = p_1^{e_1} \cdots p_r^{e_r}$ とする.

$$(V_{p_i}, Q_{p_i}) \text{ が等方的} \implies p_i^{e_i} \in (\mathbf{Q}_{p_i}^\times)^2 \iff e_i \in 2\mathbf{Z}$$

よって $a \in (\mathbf{Q}^\times)^2$ となる.
$\dim V = 3$ の場合: (V_∞, Q_∞) が等方的だから

$$(V, Q) \cong \lambda\langle a, b, -1\rangle_{\mathbf{Q}} \qquad (\lambda \in \mathbf{Q}^\times,\ 0 < a \leq |b| \in \mathbf{Z} \text{ square free})$$

と書ける. $k = a + |b|$ の帰納法で示す.

$k=2$ のとき: $a=|b|=1$ だから $x^2 \pm y^2 - z^2 = 0$ は非自明解 $(1,0,1)$ をもつので (V,Q) は等方的である.

$k \geq 3$ のとき: $a=1$ のときは上と同様だから, $2 \leq a \leq |b|$ とする. よって $K = \mathbf{Q}(\sqrt{a})$ は $\mathbf{Q}$ の 2 次拡大で

$$ax^2 + by^2 - z^2 = 0 \iff b = \left(\frac{z}{y} + \frac{x}{y}\sqrt{a}\right)\left(\frac{z}{y} - \frac{x}{y}\sqrt{a}\right) = N_{K/\mathbf{Q}}\left(\frac{z}{y} + \frac{x}{y}\sqrt{a}\right)$$

から $b \in N_{K/\mathbf{Q}}(K^\times)$ を示せばよい.

(claim 1) $a \mod b$ は $\mathbf{Z}/b\mathbf{Z}$ で平方数である.

$|b| = p_1 \cdots p_r$ とすると, Chinese Remainder Theorem から

$$\mathbf{Z}/b\mathbf{Z} \cong \prod_{i=1}^{r} \mathbf{Z}/p_i\mathbf{Z}$$

よって, 各 $p = p_i$ で $a \mod p$ が平方数であることを示せばよい. $p|a$ のときは明らかだから $p \nmid a$ とする. $\langle a,b,-1\rangle_{\mathbf{Q}_p}$ が等方的だから

$$0 \neq {}^\exists(x,y,z) \in \mathbf{Z}_p^3 \quad \text{s.t.} \quad ax^2 + by^2 - z^2 = 0$$

x,y,z の一つは $\mathbf{Z}_p^\times$ の元としてよい. b は square free だから $p^2 \nmid b$. もし $p \mid x$ ならば $p \mid z$ であり, $p^2 \mid x^2, p^2 \mid z^2$ だから $p \mid y$ となり矛盾. よって $p \nmid x$, つまり $x \in \mathbf{Z}_p^\times$. このとき

$$a \equiv (z/x)^2 \mod p$$

(claim 1) から

$$0 \neq {}^\exists c \in \mathbf{Z} \quad \text{s.t.} \quad a \equiv c^2 \mod b$$

よって

$${}^\exists d \in \mathbf{Z} \quad \text{s.t.} \quad c^2 = a + bd$$

c は $|c| \leq |b|/2$ にとれる. このとき

$$|d| = \frac{|c^2 - a|}{|b|} \leq \frac{|c|^2}{|b|} + \frac{|a|}{|b|} \leq \frac{|b|}{4} + 1 < |b|$$

$$bd = c^2 - a = (c - \sqrt{a})(c + \sqrt{a}) = N_{K/\mathbf{Q}}(c + \sqrt{a}) \qquad \text{つまり} \quad bd \in N_{K/\mathbf{Q}}(K^\times)$$

$N_{K/\mathbf{Q}}(K^\times) \subset \mathbf{Q}^\times$ は部分群だから

$$b \in N_{K/\mathbf{Q}}(K^\times) \iff d \in N_{K/\mathbf{Q}}(K^\times)$$

$\mathbf{Q}_p$ で同様に考えれば,

$$\langle a,b,-1\rangle_{\mathbf{Q}_p} \text{が等方的} \iff \langle a,d,-1\rangle_{\mathbf{Q}_p} \text{が等方的}$$

であるから, 仮定により $\langle a, d, -1\rangle_{\mathbf{Q}_p}$ は等方的になる. $|d| < |b|$ だから, 帰納法の仮定により $d \in N_{K/\mathbf{Q}}(K^\times)$ よって $b \in N_{K/\mathbf{Q}}(K^\times)$.
$n = \dim V \geq 4$ のとき: $(V, Q) \cong \langle a_1, a_2, \cdots, a_n\rangle_{\mathbf{Q}}$ として

$$(V_1, Q_1) = \langle a_1, a_2\rangle_{\mathbf{Q}}, \qquad (V_2, Q_2) = \langle -a_3, \cdots, -a_n\rangle_{\mathbf{Q}}$$

とおき

$$(V, Q) \cong (V_1 Q_1) \perp (V_2, -Q_2) \text{ が等方的} \iff Q_1(V_1^*) \cap Q_2(V_2^*) \neq \emptyset$$

を使う. 以下略. (四元数環への応用 (以下の定理 9) には 3 次元までよい.) □

系 14

(V, Q) を $\mathbf{Q}$ 上の非退化 2 次空間とするとき, $a \in \mathbf{Q}^\times$ に対し

$$a \in Q(V^*) \iff a \in Q_p(V_p{}^*) \quad (^\forall p \leq \infty)$$

証明 $a \in Q(V^*) \iff (V, Q) \perp \langle -a\rangle_{\mathbf{Q}}$ が等方的, だから, $(V, Q) \perp \langle -a\rangle_{\mathbf{Q}}$ に定理を適用すればよい. □

系 15

$(V, Q), (W, R)$ を $\mathbf{Q}$ 上の非退化 2 次空間とするとき

$$(V, Q) \cong (W, R) \iff (V_p, Q_p) \cong (W_p, R_p) \quad (^\forall p \leq \infty)$$

証明 ($\Longleftarrow$) を $\dim V$ の帰納法で示す. $\dim V = 1$ のときは, 前の系である. $\dim V \geq 2$ として, $0 \neq a \in Q(V^*)$ をとる.

$$a \in Q_p(V_p{}^*) = R_p(W_p{}^*)$$

だから, 前の系により, $a \in R(W^*)$. そこで

$$V = \langle a\rangle_{\mathbf{Q}} \perp V', \qquad W = \langle a\rangle_{\mathbf{Q}} \perp W'$$

とする. $V_p \cong W_p, \langle a\rangle_{\mathbf{Q}_p}$ に Witt の定理を使えば

$$(V_p{}', Q_p|_{V_p{}'}) \cong (W_p{}', R_p|_{W_p{}'}) \qquad (^\forall p \leq \infty)$$

だから, 帰納法の仮定により, $(V', Q|_{V'}) \cong (W', R|_{W'})$. よって $(V, Q) \cong (W, R)$ となる. □

定理 9

A, A' を $\mathbf{Q}$ 上の四元数環とする.

$$A \cong A' \iff A_p \cong A_p' \quad (^\forall p \leq \infty) \iff d(A) = d(A')$$

証明 最初の ($\Longleftrightarrow$) を示す.

$$\begin{aligned} A_p \cong A_p' \quad (^\forall p \leq \infty) &\iff ((A_p)_0, N_0) \cong ((A_p')_0, N_0') \quad (^\forall p \leq \infty) \\ &\iff (A_0, N_0) \cong (A_0', N_0') \quad (3 \text{ 次元の Hasse-Minkowski の定理}) \\ &\iff A \cong A' \end{aligned}$$

残りは明らか. □

定理 10

$\mathbf{1 \leq N \in Z}$ を *square free* とする. このとき

$$^\exists A \quad \mathbf{Q} \text{ 上の四元数環} \quad s.t. \quad d(A) = N$$

証明 $N = p_1 \cdots p_k$ として, $\epsilon = (-1)^k$ とおく. Dirichlet の算術級数定理
「a, b を互いに素な自然数とするとき, 等比級数 $\{a + mb\}_{m=1}^{\infty}$ は無限に多くの素数を含む」
を次の a, b に適用する.

$$b = \begin{cases} 8N & (2 \nmid N) \\ 4N & (2 \mid N) \end{cases} \quad \text{よって} \quad \mathbf{Z}/b\mathbf{Z} \cong \mathbf{Z}/8\mathbf{Z} \times \prod_{p_i \neq 2} \mathbf{Z}/p_i\mathbf{Z}$$

として,

$$a \equiv \begin{cases} \epsilon \mod 8 & (2 \nmid N) \\ 5\epsilon \mod 8 & (2 \mid N) \end{cases} \text{ かつ } \quad \chi_{p_i}(a) = -\chi_{p_i}(\epsilon) \quad (2 \neq {}^\forall p_i)$$

このとき, 次を満たす素数 q がとれる.

$$\epsilon q \equiv \begin{cases} 1 \mod 8 & (2 \nmid N) \\ 5 \mod 8 & (2 \mid N) \end{cases} \text{ かつ } \quad \chi_{p_i}(\epsilon q) = -1 \quad (2 \neq {}^\forall p_i)$$

これから

$$A = (\epsilon N, \epsilon q)_{\mathbf{Q}}$$

と定める.

$$k \text{ が奇数} \iff \epsilon = -1 \iff A_\infty = \mathbf{H} \iff d(A) \text{ の素因数は奇数個}$$

明らかに

$$p \nmid 2Nq \implies h_p(\epsilon N, \epsilon q) = 1 \iff A_p = \mathrm{M}_2(\mathbf{Q}_p) \implies p \nmid d(A)$$

よって

$$d(A) \mid 2Nq$$

$p = p_i \neq 2$ ならば

$$h_p(\epsilon N, \epsilon q) = h_p(p, \epsilon q) = \chi_p(\epsilon q) = -1 \implies A_p \text{ は斜体} \implies p \mid d(A)$$

また

$$h_2(\epsilon N, \epsilon q) = \begin{cases} 1 & (2 \nmid N) \\ -1 & (2 \mid N) \end{cases} \quad \text{つまり} \quad 2 \mid N \iff 2 \mid d(A)$$

よって

$$N \mid d(A) \quad \text{かつ} \quad d(A) \mid Nq$$

N と $d(A)$ の素因数の個数の偶奇は一致するから, $d(A) = N$ である. □

以上から, 次の 1 対 1 対応を得る.

$$\{\mathbf{Q} \text{ 上の四元数環の同型類}\} \longleftrightarrow \{\text{square free な自然数}\}$$