

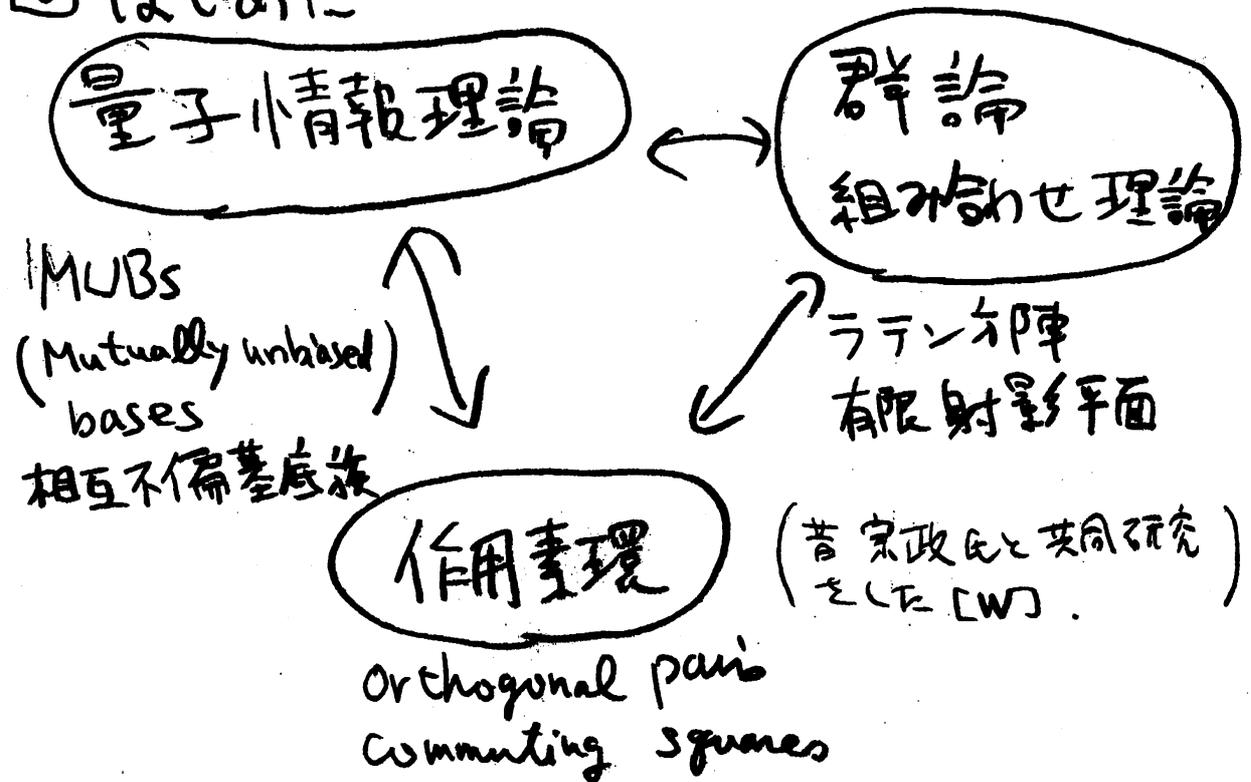
# Mutually unbiased bases, Latin squares and Orthogonal pairs

九州大学・大学院数理学研究院 綿谷 安男

Kyushu University

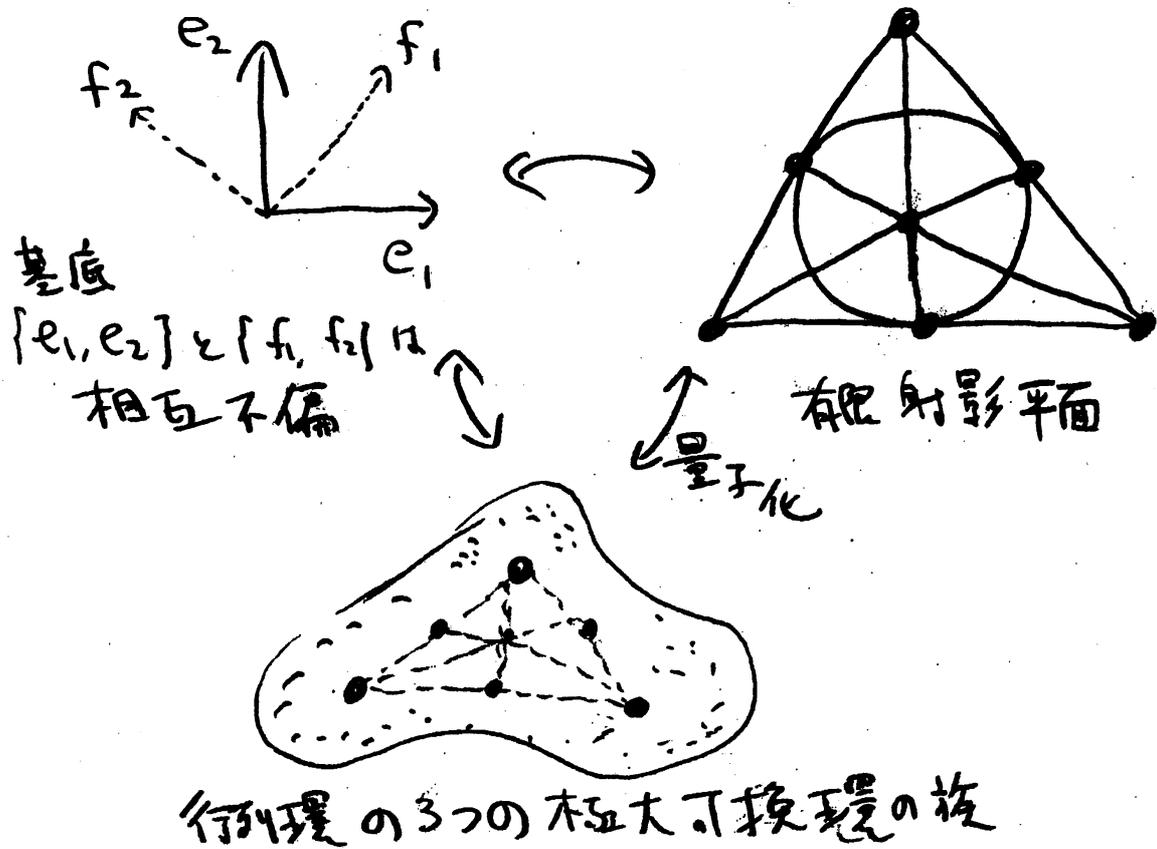
Watatani, Yasuo

① はじめに



このノートでは、上の図式にあてはるよう、  
3つの異なる分野、量子情報理論、作用素環  
群論・組み合わせ理論に関係があることを紹介する。

象徴的な対象を絵にしてみよ;



- ① 有限次元ヒルベルト空間の2つの基底が「相互不偏」である。
- ② 2つのララン方陣が「直交」する
- ③ 行列環  $M_n(\mathbb{C})$  の2つの極大可換環が  $\mathbb{C}I$  を除いて直交する (orthogonal pair である)。
- (よみんなよ似た概念で作用素環の commuting square の概念で統一できる。

# □ MUBs (Mutually Unbiased bases)

相互不偏基底族

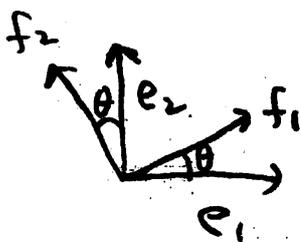
例)  $H = \mathbb{C}^2$  を 2次元のヒルベルト空間とする

$\mathcal{E} = \{e_1, e_2\}$  を標準基底とせよ。

つまり  $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ ,  $e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$  とする

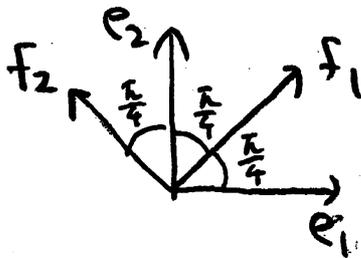
$\mathcal{F} = \{f_1, f_2\}$  を他の基底とする。

$\mathcal{E}$  と  $\mathcal{F}$  が「互いに偏よっていない」を以下に定義したい。



$f_1$  は  $e_1$  には近いが  $e_2$  には遠いのをこねてはダメ。

そこで  $\theta = \frac{\pi}{4}$  に変えてみる:  $f_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ ,  $f_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 \\ 1 \end{pmatrix}$



$$\begin{aligned} |(e_1, f_1)| &= \frac{1}{\sqrt{2}}, & |(e_1, f_2)| &= \frac{1}{\sqrt{2}} \\ |(e_2, f_1)| &= \frac{1}{\sqrt{2}}, & |(e_2, f_2)| &= \frac{1}{\sqrt{2}} \end{aligned}$$

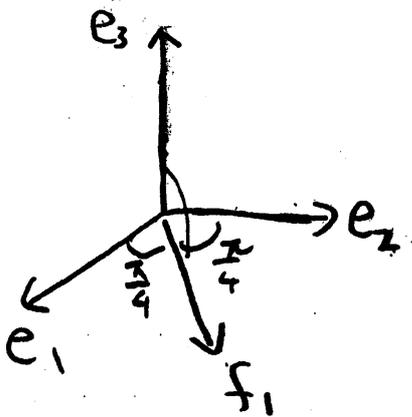
そこで  $\mathcal{E}$  と  $\mathcal{F}$  が相互不偏 といふ  $|(\mathcal{E}_i, \mathcal{F}_j)| = \frac{1}{\sqrt{2}}$  とする。

例)  $H = \mathbb{C}^3$

$\mathcal{E} = \{e_1, e_2, e_3\}$  を標準基底とせよ。

つまり  $e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ ,  $e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ ,  $e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$  とする

$\mathcal{F} = \{f_1, f_2, f_3\}$  を他の基底とする。



$$f_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \text{ とおいてやる}$$

$f_1$  は  $e_1$  と  $e_2$  とは同じ距離  
 (13) だけ、 $f_1$  と  $e_3$  はそれより  
 ずっと離れている。

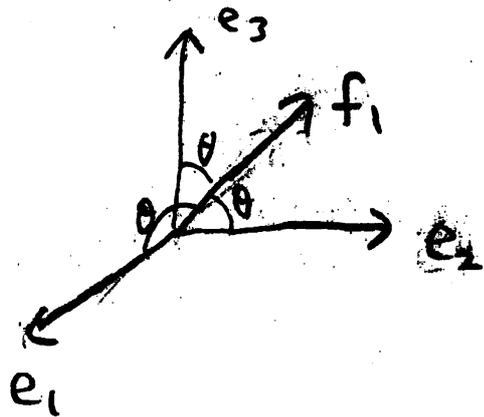
$$(e_1 | f_1) = \frac{1}{\sqrt{2}}, \quad (e_2 | f_1) = \frac{1}{\sqrt{2}}$$

$$(e_3 | f_1) = 0 \quad \text{垂直}$$

$f_1$  が  $e_1, e_2, e_3$  の3つと偏りなく離れているようにする  
 にはどうしたらいいか?

$$f_1 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

かよせられた。



$$\left. \begin{aligned} |(e_1 | f_1)| &= \frac{1}{\sqrt{3}} \\ |(e_2 | f_1)| &= \frac{1}{\sqrt{3}} \\ |(e_3 | f_1)| &= \frac{1}{\sqrt{3}} \end{aligned} \right\} \leftarrow \text{偏りなく離れている}$$

残りの  $f_2$  と  $f_3$  も  $e_1, e_2, e_3$  の3つと偏りなく離れている  
 ようにしたい。  $\omega$  を1の原始3乗根の1つとして

$$f_2 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ \omega \\ \omega^2 \end{pmatrix}, \quad f_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ \omega^2 \\ \omega \end{pmatrix} \text{ とおくと } |(e_i | f_j)| = \frac{1}{\sqrt{3}}$$

$i, j = 1, 2, 3$  とできる。これで相互に偏りなく離れた。

**Def**  $H = \mathbb{C}^n$ :  $n$ 次元  $\mathbb{C}$  線形空間

$\mathcal{E} = \{e_1, e_2, \dots, e_n\}$  : a basis

$\mathcal{F} = \{f_1, f_2, \dots, f_n\}$  : a basis

$\mathcal{E}$  と  $\mathcal{F}$  が mutually unbiased (相互不偏)

$$\stackrel{\text{def}}{\Leftrightarrow} \forall i, \forall j \quad |\langle e_i, f_j \rangle| = \frac{1}{\sqrt{n}}$$

**Def**  $H = \mathbb{C}^n$  の MUBs (Mutually Unbiased bases)

(相互不偏基底族) の中で最大のものの個数を

$N_{\text{MUB}}(n)$  とおこう

**例 1**  $N_{\text{MUB}}(2) = 3$

$H = \mathbb{C}^2$  上の 3 つの基底  $\mathcal{E}, \mathcal{F}, \mathcal{G}$  をとればよい

$\mathcal{E} = \{e_1, e_2\}, \mathcal{F} = \{f_1, f_2\}, \mathcal{G} = \{g_1, g_2\}$

$$e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, f_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, f_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}, g_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, g_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix}$$

**例 2**  $q = p^k$ : 素数  $p$  の中  $\Rightarrow N_{\text{MUB}}(q) = q + 1$

$H = \mathbb{C}^q$  上の  $\omega \neq 1$  の原始  $q$  乗根とする

$$a, b \in \mathbb{F}_q \text{ 互いに相異なる, } v_{a,b} := \frac{1}{\sqrt{q}} \left( \omega^{ax^2 + bx} \right)_{x \in \mathbb{F}_q} \in \mathbb{C}^q$$

$\mathcal{E}_a := \{v_{a,b} \in H \mid b \in \mathbb{F}_q\}$  は basis

$\Rightarrow \{\mathcal{E}_a \mid a \in \mathbb{F}_q\} \cup \{\text{標準基底}\}$  が MUBs  $q+1$  個

**問題**  $N_{\text{MUB}}(n) = n+1 \Rightarrow n$  は素数中か?

は未解決の問題です。

$N_{\text{MUB}}(2) = 3, N_{\text{MUB}}(3) = 4, N_{\text{MUB}}(4) = 5$  ですか。

$N_{\text{MUB}}(6)$  を求めることは、まだ未解決です。

$N_{\text{MUB}}(8) \geq 3$  しかわかっていない。

## ② 組み合わせ・群論

極大相互不偏基底の数  $N_{\text{MUB}}(n)$  と大変類似したことは組み合わせ論でよく知られています。

**問題**  $n$  を素数中とした時、位数  $n$  の有限射影平面が存在します。その逆です。

位数  $n$  の有限射影平面が存在  $\Rightarrow n$  は素数中か?  
は未解決の問題です。

また位数  $n$  の有限射影平面の存在

$\Leftrightarrow$  位数  $n$  のラテン方阵で互いに直交するものの  
極大右ものの個数  $N_{\text{MOLS}}(n) = n-1$

はよく知られています。

$\langle$  相互不偏基底と直交ラテン方阵は類似がある  $\rangle$

**Def)**  $A = (a_{ij})_{ij}$  が位数  $n$  の ラテン方陣

$\Leftrightarrow$   $A$  は 各成分  $a_{ij}$  が  $\{1, 2, \dots, n\}$  を与える  $n \times n$  行列で、  
どの行とどの列にも  $\{1, 2, \dots, n\}$  が 2回以上現れない。

**Def)** 2つのラテン方陣  $A = (a_{ij})_{ij}$  と  $B = (b_{ij})_{ij}$  が 直交する

$\Leftrightarrow \{(a_{ij}, b_{ij}) \mid i=1, \dots, n, j=1, \dots, n\}$  は すべて  
異なり対になっている。

**例)**  $A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}$ ,  $B = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix}$  は 位数3の  
ラテン方陣

$$(a_{ij}, b_{ij})_{ij} = \begin{pmatrix} (1,1), (2,2), (3,3) \\ (2,3), (3,1), (1,2) \\ (3,2), (1,3), (2,1) \end{pmatrix}$$

とすべて異なり対が現れるので  $A$  と  $B$  は直交する

**Def)** 位数  $n$  のラテン方陣の中で互いに直交する  
族の中で最大のものの個数を

$N_{\text{MOLS}}(n)$  と表す。

**例)**  $N_{\text{MOLS}}(2) = 1$ ,  $N_{\text{MOLS}}(3) = 2$ ,  $N_{\text{MOLS}}(4) = 3$

$N_{\text{MOLS}}(5) = 4$ ,  $N_{\text{MOLS}}(6) = 1$ ,  $N_{\text{MOLS}}(7) = 6$

$N_{\text{MOLS}}(8) = 7$ ,  $N_{\text{MOLS}}(9) = 8$ ,  $N_{\text{MOLS}}(10) \geq 2$

量子情報理論	組み合わせ理論
ヒルベルト空間の基底	ラテン方阵
次元	位数
相互不偏	直交
$N_{\text{MUB}}(n)$ : 相互不偏な基底の数が最大の個数	$N_{\text{MOLS}}(n)$ : 互いに直交するラテン方阵の数が最大の個数
$n \geq 2$ $\Rightarrow 3 \leq N_{\text{MUB}}(n) \leq n+1$	$n \geq 2$ $\Rightarrow 1 \leq N_{\text{MOLS}}(n) \leq n-1$
$n$ が素数の中 $\Rightarrow N_{\text{MUB}}(n) = n+1$ 逆は予想で未解決	$n$ が素数の中 $\Rightarrow N_{\text{MOLS}}(n) = n-1$ 逆は予想で未解決
$n$ が素数の中の時の例の構成は有限体を用いる	$n$ が素数の中の時の例の構成は有限体を用いる
$n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r} \geq 2$ と素因数分解されている $\Rightarrow N_{\text{MUB}}(n)$ $\geq \min \{ p_i^{e_i} + 1 \mid i=1, 2, \dots, r \}$	$n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r} \geq 2$ と素因数分解されている $\Rightarrow N_{\text{MOLS}}(n)$ $\geq \min \{ p_i^{e_i} - 1 \mid i=1, 2, \dots, r \}$
$n$ が偶数で決定は難	$n$ が偶数で決定は難

相互不偏基底族については最近の review [B] とここにも、という文献をみてもらう。群論を用いた構成とその限界については [ACW] がよい。  $N_{\text{HUB}}(n)$  と  $N_{\text{MOLS}}(n)$  との間の関係式については次が知られている。

**Theorem** (Wojan - Beth) [WB]

$$N_{\text{HUB}}(k^2) \geq N_{\text{MOLS}}(k) + 2$$

### ③ 作用素環による統一

相互不偏基底 と 直交打ラテン平方の話は類似があるというだけでなく作用素環論における Jones の 部分因子環理論 [J] において使われた commuting square の概念を使うと統一的に扱える。

ヒルベルト空間  $H$  上の有界作用素全体  $B(H)$  は  $*$ 環になるが、弱作用素位相で閉じた部分  $*$ 環を von Neumann 環、作用素  $l_1$  位相で閉じた部分  $*$ 環を  $C^*$ 環と称する。以下では finite trace  $\tau: M \rightarrow \mathbb{C}$  を von Neumann 環  $M$  を主に与える。  $M$  に内積を  $(T|S) = \tau(S^*T)$  によって  $\text{Hilbert}$  空間化 ( $\hookrightarrow L^2(M, \tau)$ ) とす。

**Def**  $A, B, C \subseteq M$  の \*subalg とす

$$A \subset M$$

$$U \quad U$$

$$C \subset B$$

$\Rightarrow$  Wronsky square とす

$$\stackrel{\text{def}}{\Leftrightarrow} \begin{cases} C = A \cap B \\ L^2(A) \perp L^2(B) \text{ は } L^2(C) \text{ と } \perp \text{ になる } \end{cases}$$

$\Rightarrow (L^2(A) \cap L^2(C))^\perp \perp (L^2(B) \cap L^2(C))^\perp$

特に  $C = \{0\}$  とすれば  $A$  と  $B$  は orthogonal pair とす (P).

**例**  $M = M_n(\mathbb{C})$  :  $n \times n$  行列全体

$H = \mathbb{C}^n$  の basis  $\mathcal{E} = \{e_1, e_2, \dots, e_n\}$  に對し

$\mathbb{C}e_i$  への projection を  $P_i$  とおき,  $P_i(x) = (x|e_i)e_i$ .

$A(\mathcal{E}) := \left\{ \sum_{i=1}^n \lambda_i P_i \mid \lambda_i \in \mathbb{C} \right\}$  は  $M_n(\mathbb{C})$  の極大可換環に成り,

逆に  $M_n(\mathbb{C})$  のどの極大可換環も

$H$  のある basis  $\mathcal{E}$  に対して  $A(\mathcal{E})$  の形に成る。

例として  $\mathcal{E}$  が標準基底ならば  $A(\mathcal{E})$  は対角行列全体の成る環である。この意味で

$$\{\mathbb{C}^n \text{ の基底} \} \xrightarrow{1:1} \{M_n(\mathbb{C}) \text{ の極大可換環} \}$$

**Proposition**  $H = \mathbb{C}^n$  上の basis  $\mathcal{E} = \{e_1, \dots, e_n\}$  と  
 $\mathcal{F} = \{f_1, \dots, f_n\}$  をとる (3).  $M_n(\mathbb{C})$  上には正則化  
 した  $\tau$  have  $\tau: M_n(\mathbb{C}) \rightarrow \mathbb{C}$  が存在する?

この時  $\tau$  は同値:

① 基底  $\mathcal{E}$  と  $\mathcal{F}$  は相互不偏

② 極大可換環  $A(\mathcal{E})$  と  $A(\mathcal{F})$  は orthogonal pair  
 in  $(M_n(\mathbb{C}), \cdot)$  通常の積

**例**  $A = (a_{ij})_{ij}$  を  $n$  次のラティス陣とす。これを  $\tau$  が  $\tau$ -  
 積  $\circ$  した  $(M_n(\mathbb{C}), \circ)$  の元とす。

$$P_k(i, j) = \begin{cases} 1 & (a_{ij} = k) \\ 0 & (a_{ij} \neq k) \end{cases} \quad \text{とおく}$$

$P_k$  は  $(M_n(\mathbb{C}), \circ)$  の projection に互い,

$A = 1P_1 + 2P_2 + 3P_3 + \dots + nP_n$  はスベクトル分解

より  $\mathcal{B}(A) = \{ \sum_{k=1}^n \lambda_k P_k \mid \lambda_k \in \mathbb{C} \}$  とおくと  $\mathcal{B}(A)$  は

$(M_n(\mathbb{C}), \circ)$  の可換部分環。

**Proposition** 上  $\tau$   $(M_n(\mathbb{C}), \circ)$  上には  $\tau(A) = \frac{1}{n^2} \sum_{i,j=1}^n a_{ij} \tau$

have とおける。  $A$  と  $B$  をラティス陣とす  $\tau$  は同値

① ラティス陣  $A$  と  $B$  は互いに

② 可換環  $\mathcal{B}(A)$  と  $\mathcal{B}(B)$  は orthogonal pair である

**注**  $\tau$  は  $M_n(\mathbb{C})$  上の通常の積  $\cdot$  と  $\tau$  が  $\tau$ -積  $\circ$  の違いだ。

## «References»

- [ACW] M. Aschbacher, A. Childs, P. Wojan, The limitation of nice mutually unbiased bases, *Upper J Algebr. Comb.*
- [J]. V. Jones, Index for subfactors, *Invent. Math.* 66 (1983), 1-25.
- [B]. I. Bengtson, Three ways to look at mutually unbiased bases, arXiv: quant-ph/0610216, (2006)
- [P]. S. Popa, Orthogonal pairs of  $\ast$  subalgebras in finite von Neumann algebras, *J. Operatn. Theory*, 9 (1983), 253-268
- [W] Y. Watatani, Latin squares, commuting squares and intermediate subfactors, "Subfactors" (1994) 85-104,
- [WB] P. Wojan and T. Beth, New construction of mutually unbiased bases in square dimensions *Quantum, Inform. Comput.* 5 (2005), 93-101.