連載講座

量子情報処理パラダイム
4. トポロジーと量子計算

八森　正泰，由良　文孝

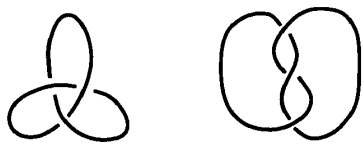
1. はじめに

この連載ではこれまで3回にわたって量子情報・量子計算の紹介が続けられてきているが，今回は少し休憩を入れて，ちょっと変わった方面の話：トポロジーと結び目理論の話をしてみたい．なぜ量子情報・量子計算の記事でそんな話が出てくるのか，と思われる方が多いのではないかと思われるが，まぁそれは置いておいて，早速トポロジーの話に入っていきたい．

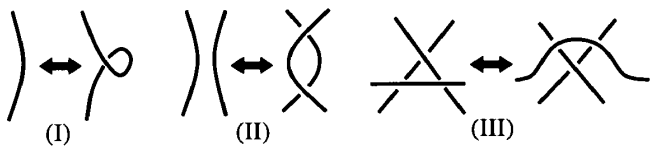
トポロジー（位相幾何学）というのは対象の形状を連続的な変形で不変な性質によって捉える分野である．つまり，ゴムでできた物体を伸ばしたり曲げたりしても同じものだと思う，ということで，例えば，三角形も円盤も同じものとして捉えるのである．正確には連続な全単射で逆写像も連続であるもの（同相写像）で移されるものは同じものと見なす，ということである．このような基本的な考え方や概念はトポロジーの教科書をどれでもよいから参照されるとよいだろう．今回の主役はその中でも低次元トポロジーでよく取り扱われる結び目の話である．

2. 結び目と不変量

結び目とは3次元空間の中にある閉じたひものことである（複数の閉じたひもからなるものは絡み目と呼ばれる）．これを空間中で連続的に変形して同じ形にできるものは同じものと考えるのであるが，この場合，同相性で考えてしまうとすべての結び目がただの輪っかと同じになってしまうので，正しく定義するためにはアンビエント・イソトピーなどを使うことになるのであるが，詳しいことは結び目理論の教科書を見てもらうこととして，ここでは実際にひもでつくった結び目を3次元空間中で切ったり張ったりせずに変形できるかどうか，というように考えてもらえば十分である．例えば次の絵の二つの結び目は実は同じ結び目である．



結び目の同値性に関する基本的な定理の一つがライデマイスターの定理である．この定理は異なる二つの射影が同じ結び目を表していることと下図の3種類の変形によって互いに移り合うことが同値である，ということを主張するものである．



ライデマイスター変形

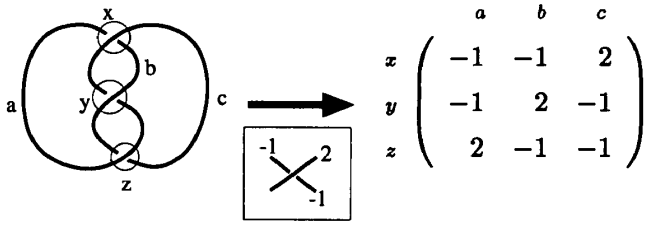
この結び目という対象は非常に単純なものなので，何も難しいことがありそうもないと思われるかも知れないが，「与えられた二つの結び目が同値かどうか」とか「結び目が自明（ほどける）かどうか」というのは実は結構難しい問題である．実際，与えられた二つの結び目が同値かどうかを判定するアルゴリズムが存在するかどうかという問題が肯定的に解かれたのはHemion (1979) [7]によってである（自明性の方は1961年にHakenによって解かれている）．計算量としては，結び目の自明性判定がNPに入るということが1997年にHass, Lagarias, Pippengerらによって示されている[6]が，同値性の方については未だにわかっていない．

結び目の同値性を示すのが難しい理由は，二つの結

はちもり　まさひろ
筑波大学 社会工学系
〒305-8573 つくば市天王台 1-1-1
ゆら　ふみたか
科学技術振興事業団 ERATO 今井量子計算機構プロジェクト
〒113-0033 東京都文京区本郷 5-28-3

び目が同値であるかどうかを示す場合には（原理的には）実際に同じ形に変形する方法を示してあげればよいわけであるが，同値でないことを示すためには無限の可能性が考えられる（例えばライデマイスター変形の列は無限に考えられる）ため，同値でないことを保証する手段が簡単には見つからないためである．しかし，この非同値性を十分条件として簡単に示す道具は知られている．その一つが結び目の不変量という概念である．

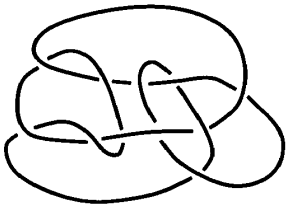
結び目の不変量というのは，各結び目に対して何らかの量を与え，同値な結び目に対しては同じ値になるようにしたものである．例えば結び目の判別式は不変量の一つである（文献[10]参照）．結び目の判別式を計算するには，まず，結び目の絵を書いたときの曲線分と交点のそれぞれにラベルを付け，接続行列で表現する．このときに，下図のように，交点で上側になっている1本の曲線分には2，下側になっている2本の曲線分には-1をあてる．



そして，行と列をそれぞれ一つずつ選んで削除し，残った行列の行列式を計算する．この行列式の絶対値が結び目の判別式である（0行0列の行列の判別式は1とする）．例えば上の例でz行c列を消去すると$\begin{pmatrix} -1 & -1 \\ -1 & 2 \end{pmatrix}$が得られるので，結び目の行列式は3ということになる．ここで，自明な結び目の行列式は1になるということから，上の結び目は自明でない（ほどけない）ということが分かるわけである．

この結び目の行列式が本当に結び目の不変量になっているということを確かめるには，この値が与えた結び目に対して（結び目の射影のとり方，削除する行と列の選び方によらずに）ユニークに定まることを確かめなければいけない．行と列の選び方で不変であることは簡単な線形代数の話であるが，射影のとり方によらないことを示す方には上記のライデマイスターの定理を使い，3種のライデマイスター変形において値が不変であることを示せばよい．もし興味があったら練習問題に証明してみていただきたい．

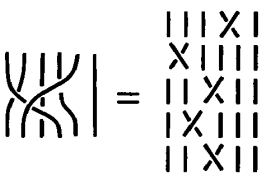
ただし，注意しておかなければいけないのは，不変量が異なるということは結び目の非同値性の十分条件ではあるが，必要十分条件ではないということである．例えば下の結び目は判別式が1であるが，自明な結び目ではない．



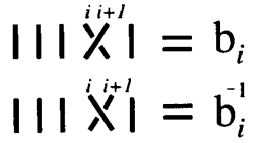
実は，結び目の不変量というのは種々知られているのであるが，結び目の同値性の必要十分条件を与えることができるような不変量はまだ知られておらず，そのような万能な不変量が存在するのか否かは未だに未解決である（前に触れたHakenやHemion達の同値性判定に関する結果はnormal surface theoryという全く異なる手法によって得られているのである）．とはいえ，結び目の不変量という概念が役に立たないというわけではなく，より多くの結び目の非同値性を示すことができる（同じ値を持つような同値な結び目の例の存在がまだ知られていないような）強力な不変量の登場や，多くの不変量を生成する仕組みによる統一的な議論，3次元多様体の不変量との関連などにより，結び目および3次元多様体の研究における議論の中心的な部分を占めているのである．

3. 組ひも群と結び目

前章では結び目を平面に射影した図を元に議論していたが，これとは別の結び目の表現方法に組ひもを用いたものがある．組ひもとは，下の左図のように，n本のひもが交差をしながら上から下に向かって垂れ下がっているもののことである．



このように組ひもが与えられると，上の右図のように，一つ一つの交点ごとに分解することができるのであるが，この一つ一つを



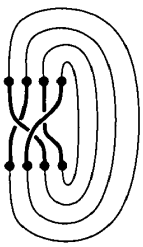
のように呼び，縦に連続する列を順に左から右へ並べて書くことにすると，上の例は $b_4b_1^{-1}b_3b_2b_3^{-1}$ ということになる．このように表記してみると，n 本からなる組ひもの全体が，組ひもを縦に並べてつなげるという操作を演算として群になっていることに気づくだろう(単位元は n 本のひもが交差なく平行に並んだ組ひも)．実際この群は $b_1, b_2, \cdots, b_{n-1}$ を生成元とし，

$b_ib_j=b_jb_i \quad (|i-j|\geq 2)$

$b_ib_{i+1}b_i=b_{i+1}b_ib_{i+1}$

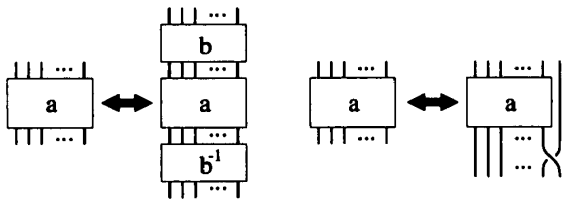
を関係式とする群であり，組ひも群 B_n と呼ばれている．

この組ひもという概念は結び目とよく似ているのであるが，実際非常に密接な関連がある．これを見るために，次の図のように組ひもの上下をつなげることを考えてみる．



すると，一つの組ひもを元にして結び目（または絡み目）を得ることができるのであるが，実は任意の結び目（または絡み目）を適当に変形すると必ずこの図のように組ひもの上下をつなげた形にすることができるということがAlexanderの定理として知られている．したがって，結び目（や絡み目）を考えるかわりに組ひもを考えてもよいということになるわけである．実際，与えられた結び目を与える組ひもはVogelのアルゴリズムなどによって簡単に得ることができる（例えば文献[12]参照）ので，計算の観点から見ても結び目を与えることと組ひもを与えることは等価であると考えてよいのである．

組ひもから結び目の不変量を考える場合に注意しないといけないのが，組ひもとして異なるものからも同じ結び目が生じることがあるということである．同値性に関しては，結び目に対してはライデマイスターの定理があったが，組ひもに対してはマルコフの定理というものがある．これは二つの組ひもが同じ結び目を与えることと，組ひもとしての同値変形および次の2種の変形で移り合うことが等価である，というものである．



マルコフ変形

(二つ目の変形では B_n と B_{n+1} の間の変形になっているが，これは B_n が B_{n+1} の中に埋め込まれているとして考えている) したがって，この2種の変形で不変であるような組ひもの不変量が結び目の不変量となるわけである．

4. 組ひも群の表現と結び目の不変量

さて前節で述べた組ひも群の表現を次のように作ってみる[8, 9]．少々唐突だが，次のテンパリーリーブ代数と呼ばれる代数 TL_n を定義しよう．生成元を $U_1, U_2, \cdots, U_{n-1}, \delta\in\mathbb{C}$ として，

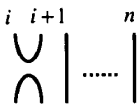
$U_i^2=\delta U_i$

$U_iU_{i+1}U_i=U_i \quad (1\leq i\leq n-2)$

$U_iU_{i-1}U_i=U_i \quad (2\leq i\leq n-1)$

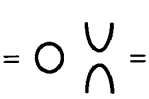
$U_iU_j=U_jU_i \quad (|i-j|\geq 2)$

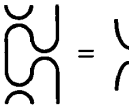
と定義される代数は次のような図形的な解釈を持つ．

$U_i =$ 

(1)

積演算は組ひも群と同じように縦につなげて並べ，曲がっている曲線は引っ張って伸ばすものとする．図形の中に閉じたループが現れた場合は，その寄与を複素数 δ をかけるものと見なす．

$U_i^2 =$  $= \delta U_i$

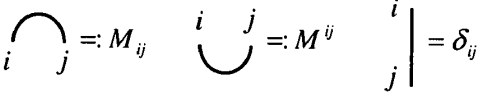
$U_iU_{i+1}U_i =$  $= U_i$

ここで上図の端点が，それぞれベクトル空間 V を表しているとすると，上端から下端へ $V^{\otimes n}\to V^{\otimes n}$ の写像と見なすことができる．簡単のため $V=\mathbb{C}^2$ とすると，この TL_n のテンソル積表現 ρ_n として例えば，

$$\rho_n:\ TL_n \ \to\ \mathrm{End}(V^{\otimes n})$$
$$U_i \ \mapsto\ id^{\otimes i-1}\otimes U\otimes id^{\otimes n-i-1}$$

$$id=\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad U=\left(\begin{array}{c|cc|c}0&0&0&0\\\hline 0&q&1&0\\0&1&q^{-1}&0\\\hline 0&0&0&0\end{array}\right) \tag{2}$$

と取ることができる（$\delta=q+q^{-1}$）．さらに，式(1)の図形要素に対して，



$$M_{ij}=M^{ij}=\begin{pmatrix}0&q^{\frac{1}{2}}\\q^{-\frac{1}{2}}&0\end{pmatrix}$$

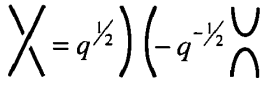
のように行列を対応させれば（ここで δ_{ij} はクロネッカーのデルタであり式(2)の id に対応する），$M^{ij}M_{kl}$ が式(2)で定義した行列 U の成分 $U_{kl,ij}$ に一致する．つまり，TL_n は行列 M と単位行列 id から構成できることがわかる．

さて，このテンパリーリーブ代数と組ひも群の図形表示はよく似ていると思われるだろう．実際，組ひも群の表現をテンパリーリーブ代数の上に作ることができるのである．次にそれを示そう．

$$\pi_n:\ B_n \ \to\ TL_n$$
$$b_i^{\pm 1} \ \mapsto\ id^{\otimes i-1}\otimes R^{\pm 1}\otimes id^{\otimes n-i-1}$$
$$R=q^{\frac{1}{2}}(id\otimes id)-q^{-\frac{1}{2}}U$$

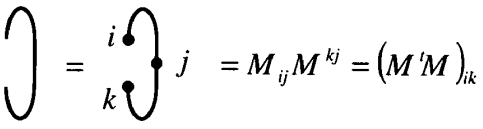
$$\rho_2(R)=\left(\begin{array}{c|cc|c}q^{\frac{1}{2}}&0&0&0\\\hline 0&0&-q^{-\frac{1}{2}}&0\\0&-q^{-\frac{1}{2}}&q^{\frac{1}{2}}-q^{-\frac{3}{2}}&0\\\hline 0&0&0&q^{\frac{1}{2}}\end{array}\right)$$

ここで $R^{\pm 1}$ は，i 番目と $i+1$ 番目のひものひねりを表す写像 $V^{\otimes 2}\to V^{\otimes 2}$ であり，



と描くことができる．この表現が組ひも群の関係式を満たすことは，例えば $b_ib_{i+1}b_i=b_{i+1}b_ib_{i+1}$ から得られる 8×8 行列を計算してみればよい（一般にこの R は R 行列と呼ばれ，量子群の対称性が背後にある[14]）．このようにして組ひも群を表す行列が得られた．

これらを用いて，前節と同じように組ひもの上下をつなげてみよう．詳しくは述べないが，組ひもの上下の端点どうしをつなぐ図形を



$$M^tM=\begin{pmatrix}q&0\\0&q^{-1}\end{pmatrix}=:\eta$$

と思うことにするとうまく組ひもが閉じて，前頁の図のように結び目（あるいは絡み目）が得られる．自由な端点のない結び目は，自由な添え字のなくなったテンソルに対応するからトレースを取って，

$$V(b)=q^{-3w(b)/2}\mathrm{tr}[\eta^{\otimes n}(\rho_n\circ\pi_n)(b)]$$

が得られる．ここで $w(b)$ は組ひも b を作る $\{b_i\}$ の数引く逆元 $\{b_i^{-1}\}$ の数で定義される整数である．

また，$\eta^{\otimes n}$ は n 本のひもの上下をそれぞれつなげることに対応している．この $V(b)$ が，組ひも $b\in B_n$ で表される結び目の不変量であり，ジョーンズ多項式と呼ばれるものである．マルコフ変形(I)で不変であることは $\eta^{\otimes 2}$ と R が可換であることからわかり，マルコフ変形(II)で不変となるように $w(b)$ の補正がついている（あるいはライデマイスター変形(I)）．

ところで一般に，有限群の行列表現はユニタリに取ることができる．組ひも群の場合はどうだろうか？次節で，より一般的な話題を紹介する．

5. 量子計算とモジュラー関手，トポロジー的量子場理論

さて，ここまで，「トポロジーと量子計算」というタイトルにも関わらず，延々と量子計算に関係なさそうな話をしてきたのであるが，ここで量子計算に話を結びつけることにしよう．連載第一回で簡単な紹介があったように，量子計算というのはおおざっぱにいうと，ユニタリ変換をするということが計算の過程となり，観測をすることによって計算結果を得るのである[5, 11]．ここで，群の表現が線形変換であったことを考えると，もしこの表現をユニタリに実現することができれば，量子計算におけるユニタリ変換を組ひも群の表現によって置き換えることにより，結び目が計

算過程を表すというように考えられるのではないか，ということになるわけである．

前節で紹介した組ひも群の表現に関連した概念にモジュラー関手というものがあり，これは組ひも群の表現を拡張した概念と見ることができるのであるが，ごく最近，Freedman, Kitaev, Larsen, Wang といった研究者たちがこのモジュラー関手が量子計算と等価であることを示している．モジュラー関手というのは少しややこしい概念であるが，簡単に紹介したい．まず，穴が n 個あいた2次元球面（または $n-1$ 個の穴の空いた円盤で外側を n 番目の穴と解釈してもよい）の各境界にラベルをラベル集合 $\mathcal{L}=\{1,2,\cdots,\}$ からつけたものおよびそれらの和集合を対象とし，その穴あき球面間の自己同相写像を射とするカテゴリーを考える．ここで，ラベル $\mathcal{L}$ には involution $\hat{}$（$\hat{\hat{a}}=a$ を満たす演算子）で $\hat{1}=1$ であるものが定義されているとする．これに対して，このカテゴリーからベクトル空間と線形写像のカテゴリーへの関手で次のような性質を満たすものがモジュラー関手である．

- 互いに交わりのない要素に対して，

$$F(\quad)=F(\quad)\otimes F(\quad).$$

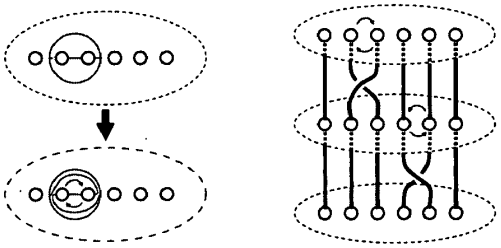
- $F(\quad)=\oplus_{x\in\mathcal{L}}F(\quad)$.
- Y の向きづけを逆にし，すべてのラベルに$\hat{}$を作用させたものを Y^*とすると，$F(Y^*)=(F(Y))^*$.
- $F(\emptyset)\simeq\mathbb{C}$.

$$\bullet\ F(\quad)\simeq\begin{cases}\mathbb{C} & \text{if } a=1\\ 0, & \text{if } a\neq 1.\end{cases}$$

$$\bullet\ F(\quad)\simeq\begin{cases}\mathbb{C} & \text{if } a=\hat{b}\\ 0, & \text{if } a\neq\hat{b}.\end{cases}$$

- システム全体を $F(\quad)$, $F(\quad)$, $F(\quad)$ の適当な基底によって $\mathbb{Q}$ 上代数的に記述することができる．

この関手 F において自己同相写像もベクトル空間の射に写されるので，自己同相写像 $X\xrightarrow{f}Y$ は対応するベクトル空間の線形変換 $F(X)\xrightarrow{F(f)}F(Y)$ に対応する．ここで，穴あき円盤の境界に与えるラベルをすべて同じラベル1にしてしまうと，この穴あき円盤の（イソトピーを除いて考えた）自己同相写像は下図左側に示したような「デーン・ツイスト」を繰返し適用したものとして表すことができ（文献[1]参照），これは下図右側のような解釈によって組ひも群と同型となるのである．



このとき，モジュラー関手では自己同相写像の合成はベクトル空間の線形写像の合成に写されることを考えると，ちょうど組ひも群の表現になっていることがわかるだろう．

この節の冒頭で，（ユニタリな）組ひもの表現は量子計算と見ることができる，ということを書いたが，Freedman, Kitaev, Larsen, Wang らは文献[2]と文献[4]によってユニタリなモジュラー関手が量子計算と等価であることを示している（文献[3]も参照）．「等価である」というのは量子計算における BQP というクラスを念頭においての話で，任意のユニタリなモジュラー関手に対して穴あき円盤の自己同相写像に対応する線形写像を量子ゲートの列で近似することができ，逆に，任意の量子ゲートをあるユニタリなモジュラー関手における自己同相写像の列によって近似することができる，ということである．量子計算をユニタリなモジュラー関手で模擬する方のアイディアは，1の5乗根上の Chern-Simons 理論（ラベルセットは $\{1,2,3,4\}$）において $\quad$ が2次元のベクトル空間と対応することに着目し，これを n 個含む大きい穴あき球面の中に n qubit のシステム $\mathbb{C}^2\otimes\mathbb{C}^2\otimes\cdots\otimes\mathbb{C}^2$ を埋め込み，この部分空間上のユニタリ変換を全体のユニタリ変換で表現することが可能であることを示すという手法を用いている．

このモジュラー関手よりも一般的な概念がトポロジー的量子場理論[13]で，これは（向きづけられた）n 次元多様体を対象とし，つまり，二つの多様体を互いに共通部分を持たない和集合として境界に持つ $n+1$ 次元多様体（コボルディズム，または，同境）を射とするカテゴリーに対して，ベクトル空間のカテゴリーへの関手である種の条件を満たすようなもののことであるが，モジュラー関手は大抵の場合にトポロジー的量子場理論に拡張できることが知られている．こうし

て，トポロジー的量子場理論と量子計算を結びつけることができることになるわけであるが，こうしたトポロジー的量子場理論やそれに類した構造をうまく量子計算と対応づけることにより，量子計算の裏にある深い構造を記述することができるのではないか，という夢が広がるのである．

6. おわりに

以上，結び目の量子不変量およびトポロジー的量子場理論といったトポロジーの話題に量子計算が関係しているという話を簡単に紹介してみたが，いかがだっただろうか？　この方面の研究はまだ始まったばかりであり，これを用いて新しいアルゴリズムが構成されたり量子計算機を実現されたりというところまで至ってはいない．したがって，「数学者のおもちゃ」と思う方面もあるだろう．が，一方，量子計算という枠組の持つ奥行きの深さを感じて頂けた方も中にはいるのではないかと思う．量子計算というと，素因数分解が早くできるなど安全な暗号通信ができるとかいうような（量子計算・量子通信が実現した暁に得られるであろう）実用面のありがたさだけが取り上げられがちであるが，実用的に利用価値があるというだけでは面白い研究対象とはなり得ないのである（実用性のある研究と面白い研究は別の概念である）．誌面の分量上および筆者の能力の関係上ごく簡単な紹介しかできなかったが，今回の短い紹介記事によって（内容はよくわからなくても）量子計算という分野の深みの一端をほんの少しでもかいま見て頂ければ成功であるとしたい．もし，少しも面白さが伝わらなかったとすると，筆者の文章力に問題があるのかもしれないので，文末の参考文献リストに直接当たってみていただければ幸いである．

参考文献

[1] J. S. Birman, *Braids, links, and mapping class groups*, Princeton, (1974).

[2] M. H. Freedman, A. Kitaev and Z. Wang, Simulation of topological field theories by quantum computers, preprint, (2000), http://www.arXiv.org/abs/quant-ph/0001071/

[3] M. H. Freedman, A. Kitaev, M. J. Larsen and Z. Wang, Topological Quantum Computation, preprint, (2001), http://www.arXiv.org/abs/quant-ph/0101025/

[4] M. H. Freedman, M. J. Larsen and Z. Wang, A modular functor which is universal for quantum computation, preprint, (2000), http://www.arXiv.org/abs/quant-ph/0001108/

[5] J. Gruska, *Quantum Computing*, McGrawhill, (1999).

[6] J. Hass, J. C. Lagarias and N. Pippenger, The computational complexity of knot and link problems, J. ACM, **46** (1999), 185-211.

[7] G. Hemion, On the classification of homeomorphisms of 2-manifolds and the classification of 3-manifolds, Acta Math., **142** (1979), 123-155.

[8] L. H. Kauffman, *Knots and Physics*, World Scientific, (1991).

[9] L. H. Kauffman, Quantum Computing and the Jones Polynomial, preprint, (2001), http://www.arXiv.org/abs/quant-ph/0105255/

[10] C. Livingston, *Knot Theory*, Mathematical Association of America, (1993).

[11] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge, (2000).

[12] V. V. Prasolov and A. B. Sossinsky, *Knots, Links, Braids and 3-Manifolds : An Introduction to the New Invariants in Low-Dimensional Topology* American Mathematical Society, (1997).

[13] V. G. Turaev, *Quantum Invariants of Knots and 3-Manifolds*, de Gruyter, (1994).

[14] 神保道夫，量子群とヤンバクスター方程式，シュプリンガーフェアラーク東京，(1990).