

< 実[双]行列の基底は群を成す >

実[双]行列（実-双対角対称行列のこと）の性質を継続して調べている。今回は、[（その143）](#)で導入した実[双]行列の基底が群を成すことがわかったので、それを示したい。

その前に、実[双]行列に関しこれまでに分かったことをまとめておきたい。

=====

(1) 実[双]行列は、掛け算に関して可換である。これは n 行 n 列の実[双]行列で成り立つ。

(2) 実[双]行列の集合は、掛け算に関してアーベル群（無限群）を成す。これは n 行 n 列の実[双]行列で成り立つ。

(3) n 行 n 列の実[双]行列は、 n 個の基底を持つ。

=====

まず実[双]行列は、例えば4次と5次では次の美しい対称的なものである（成分は実数）。この形を頭に入れていただきたい。

$$G4 = \begin{bmatrix} \alpha & 0 & 0 & \beta \\ 0 & a & b & 0 \\ 0 & b & a & 0 \\ \beta & 0 & 0 & \alpha \end{bmatrix} \quad G5 = \begin{bmatrix} \alpha & 0 & 0 & 0 & \beta \\ 0 & a & 0 & b & 0 \\ 0 & 0 & c & 0 & 0 \\ 0 & b & 0 & a & 0 \\ \beta & 0 & 0 & 0 & \alpha \end{bmatrix}$$

注記：実-双対角対称行列は、実対称行列の一種であり、右下方向と左下方向のそれぞれの対角線に対して対称で、且つそれぞれの対角線以外の成分は全て0となるものを言う。

実[双]行列は、単位行列（E）、零行列（O）もその仲間を含む。5 次の場合を示す。

$$E = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad O = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

さて今回、「実[双]行列の基底は群を成す」という事実を示す。[（その143）](#)での3次と4次で事例を使いながら任意の n 次元で成り立つことを示したい。

=====

< 実[双]行列の基底は群を成すことの証明 >

n 行 n 列の実[双]行列の基底が群を成すことを、3次と4次の例を土台に使いつつ証明する。なお、以下での“位数”とは、群の集合に含まれる元（要素）の数のことである。

< 3 次のケースを土台に >

次の 3 行 3 列の実[双]行列 G3 を考えよう。

$$G3 = \begin{bmatrix} a & 0 & b \\ 0 & c & 0 \\ b & 0 & a \end{bmatrix}$$

この G3 の基底 E_1, E_2, E_3 を次のように定義する。これらも実[双]行列である。

$$E_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, E_2 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}, E_3 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

G3 はこの三つの基底で次のように一意に表される。

$$G3 = aE_1 + bE_2 + cE_3 \quad \text{-----①}$$

これは次のように表せることから容易にわかる。

$$\begin{bmatrix} a & 0 & b \\ 0 & c & 0 \\ b & 0 & a \end{bmatrix} = a \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} + b \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} + c \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

これら三つの基底同士を掛け算した結果は ([その 1 4 3](#)) を参照いただきたい (略)。

実[双]行列は掛け算で可換であるから、基底の計算でも掛ける順番には無関係であることに注意したい。

①の G3 に対し、例えば、G3 の 3 回の掛け算 (3 乗) $G3^3$ を計算しよう。上記の基底の結果を用いて計算すると、普通の数のように計算でき、次となる。

$$G3^3 = (aE_1 + bE_2 + cE_3)^3 = (a^3 + 3ab^2)E_1 + (b^3 + 3a^2b)E_2 + c^3E_3 \quad \text{-----①-2}$$

$G3^3$ もやはり三つの基底で表される。この結果は、行列の形で計算した場合と一致する。

さて基底同士の掛け算の演算に関し、集合 $\{E_1, E_2\}$ は位数 2 の群を成し、集合 $\{E_3\}$ は位数 1 の群を成すことに気づく。[\(その 1 4 3\)](#) の結果を、次のように並べかえればそれがよりよく分かる。

$$E_1E_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = E_1$$

$$E_2E_2 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = E_1$$

$$E_1E_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} = E_2$$

$$E_3E_3 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} = E_3$$

まだわかりにくければ、 E_1 を e 、 E_3 も e という単位元的な表現に置き換えて、 $\{e, E_2\}$ と $\{e\}$ を考えれば、これらがそれぞれ位数 2 と位数 1 の群（アーベル群）を成すことが容易にわかる。すなわち、(1)閉集合性、(2)結合則、(3)単位元の存在、(4)逆元の存在、(5)可換性を全て満たしている。

$\{E_1, E_2\}$ については集合 $\{1, -1\}$ が、 $\{E_3\}$ については集合 $\{1\}$ が掛け算に関して群を成すのとまったく同じである。別の表現を用いれば、集合 $\{E_1, E_2\}$ で一つの独立国を成し、集合 $\{E_3\}$ で一つの独立国を成している。

よって、3 次の場合は、基底の集合 $\{E_1, E_2\}$ が位数 2 の群を成し、基底の集合 $\{E_3\}$ は位数 1 の群を成すことが分かった。⇒位数 2 の群 1 個、位数 1 の群 1 個。

このことは任意の奇数次（ n 次）に拡張できる。3 次の場合も含めて示す。

1 次($n=1$)の場合、1 次(1 行 1 列)の基底 E_1 に関し、集合 $\{E_1\}$ が位数 1 の群を成す。⇒位数 1 の群 1 個。

3 次($n=3$)の場合、3 次の基底 E_1, E_2, E_3 に関し、集合 $\{E_1, E_2\}$ が位数 2 の群を成し、集合 $\{E_3\}$ が位数 1 の群を成す。⇒位数 2 の群 1 個、位数 1 の群 1 個。

5 次($n=5$)の場合、5 次の基底 E_1, E_2, E_3, E_4, E_5 に関し、集合 $\{E_1, E_2\}$ と $\{E_3, E_4\}$ がそれぞれ位数 2 の群を成し、集合 $\{E_5\}$ が位数 1 の群を成す。⇒位数 2 の群 2 個、位数 1 の群 1 個。

...

このように、延々と単純な規則で、各階層での基底の集合に対応する群ができていく。例えば、5 次($n=5$)では、三階層でのそれぞれの基底集合に対応する群がある。

結局、奇数次（ n 次）では、位数 2 の群が $(n-1)/2$ 個、位数 1 の群が 1 個できる。

＜4 次のケースを土台に＞

4 行 4 列の実[双]行列 G_4 を考えよう。

$$G_4 = \begin{bmatrix} a & 0 & 0 & b \\ 0 & A & B & 0 \\ 0 & B & A & 0 \\ b & 0 & 0 & a \end{bmatrix}$$

この G_4 の基底 E_1, E_2, E_3, E_4 を次のように定義する。これらも実[双]行列である。

$$E_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad E_2 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}, \quad E_3 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad E_4 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

すると、 G_4 はこの四つの基底で次のように一意に表される。

$$G_4 = aE_1 + bE_2 + AE_3 + BE_4 \quad \text{-----②}$$

これは次のようにできることから容易にわかる。

$$\begin{bmatrix} a & 0 & 0 & b \\ 0 & A & B & 0 \\ 0 & B & A & 0 \\ b & 0 & 0 & a \end{bmatrix} = a \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} + b \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} + A \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} + B \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

これら四つの基底同士を掛け算した結果は（[その 1 4 3](#)）を参照いただきたい（略）。

実[双]行列は掛け算で可換であるから、基底の計算も掛ける順番には無関係であることに注意したい。

②の G4 に対し、例えば G4 の 3 回の掛け算（3 乗） $G4^3$ を計算しよう。上記の基底を用いて計算すると、普通の数のように計算でき、次となる。

$$G4^3 = (aE_1 + bE_2 + AE_3 + BE_4)^3 = (a^3 + 3ab^2)E_1 + (b^3 + 3a^2b)E_2 + (A^3 + 3AB^2)E_3 + (B^3 + 3A^2B)E_4 \text{ ---②-2}$$

$G4^3$ もやはり四つの基底で表現された。この結果は行列の形で計算した場合と一致する。

さて、上記の基底同士での掛け算の演算から、集合 $\{E_1, E_2\}$ は位数 2 の群を成し、集合 $\{E_3, E_4\}$ も位数 2 の群を成すことに気づく。次のように並べかえれば、それがよりよく分かる。（[その 1 4 3](#)）から、上記集合内の基底同士の掛け算の結果を抜粋する。

$$E_1E_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = E_1$$

$$E_2E_2 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = E_1$$

$$E_1E_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} = E_2$$

$$E_3E_3 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = E_3$$

$$E_4E_4 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = E_3$$

$$E_3E_4 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = E_4$$

まだわかりにくければ、3 次の場合と同様に、 E_1 を e 、 E_3 も e という単位元的な表現に置き換えれば、集合 $\{e, E_2\}$ も集合 $\{e, E_4\}$ も 位数 2 の群（アーベル群）を成すことが容易にわかるだろう。すなわち (1) 閉集合性、(2) 結合則、(3) 単位元の存在、(4) 逆元の存在、(5) 可換性を全て満たしている。

これは集合 $\{1, -1\}$ が掛け算に関して群を成すのとまったく同じである。別の表現を用いれば、集合 $\{E_1, E_2\}$ で一つの独立国を成し、また集合 $\{E_3, E_4\}$ で一つの独立国を成している。

よって、4 次の場合は、集合 $\{E_1, E_2\}$, $\{E_3, E_4\}$ が位数 2 の群を成すことが分かった。⇒位数 2 の群 2 個。

このことは任意の偶数次 (n 次) に拡張できる。上記 4 次も含めて、次となる。

2 次 ($n=2$) の場合、2 次 (2 行 2 列) の基底 E_1, E_2 に関し、集合 $\{E_1, E_2\}$ は位数 2 の群を成す。⇒位数 2 の群 1 個。

4 次 ($n=4$) の場合、4 次の基底 E_1, E_2, E_3, E_4 に関し、集合 $\{E_1, E_2\}$ と $\{E_3, E_4\}$ はそれぞれ位数 2 の群を成す。⇒位数 2 の群 2 個。

6 次 ($n=6$) の場合、6 次の基底 $E_1, E_2, E_3, E_4, E_5, E_6$ に関し、集合 $\{E_1, E_2\}$ と $\{E_3, E_4\}$ と $\{E_5, E_6\}$ はそれぞれ位数 2 の群を成す。⇒位数 2 の群 3 個。

...

このように延々と単純な規則で、各階層での基底集合に対応する群ができていく。例えば、6 次 ($n=6$) では、三階層でのそれぞれの基底集合に対応する群がある。

結局、偶数次 (n 次) では、位数 2 の群が $n/2$ 個できる。

以上より、任意の n 行 n 列の実[双]行列の (各階層の) 基底の集合は群を成すことが分かった。
(証明終わり)

=====

このように n 行 n 列の実[双]行列では、各階層での基底の集合がそれぞれ独立国を成し、それぞれが群を形成している。

この事実を見てもわかるように、実[双]行列は n が大きくなってもその構造は単純であり、偶数次では 2 行 2 列の実[双]行列の構造がひたすら繰り返されていくだけである。奇数次もほとんど同じだが、中心の 1 行 1 列の行列 (数) が一つ余計についてくる。

n 行 n 列の実[双]行列はフラクタル的な構造をしている。ロシアのマトリョーシカ人形のようなものと言ってよい。

最後に、分かってきたこと、予想、アイデアなど思いつくまま書いておく。

■計算により、実[双]行列の集合は体を成すと分かってきた。なんと、群よりもっと制約が厳しい体を成しているのである！ まだ 2 次の場合しか計算していないが、任意の n 次で成り立つはずである。後日示したい。

■ (その142) で、次の問いを發した。

「今回、証明したように、実-双対角対称行列は無限群のアーベル群となった。行列の無限群で且つアーベル群となるものは他にないのだろうか？」

これが気になっていたのだが、2次元回転行列(直交行列の一種)の集合が無限群 且つアーベル群を成すと分かった。 $SO(2)$ と表現される有名な行列群である。

ただしアーベル群であるのは $SO(n)$ の $n=2$ のときだけで、3次元以上の $SO(n)$ は非アーベル群(非可換群)となるようである。参考:「現代数学の流れ2」(岩波書店、青本・加藤・上野・高橋・神保・難波 著)p.107

実[双]行列の集合は、任意の n 行 n 列でアーベル群(可換群)を成す。やはり実[双]行列は特別である。

■ ゼータの源流は、次のフーリエ級数である。

フーリエ級数

$$(\pi-x)/2 = \sin x/1 + \sin 2x/2 + \sin 3x/3 + \sin 4x/4 + \cdots \quad (0 < x < 2\pi)$$

に $\int_{(0 \sim x)} e^{(ax)}$ を作用させ x にある数を代入すると、ゼータの香りの漂う公式が得られる。(aは任意の実数)

http://www5b.biglobe.ne.jp/sugi_m/page212.htm

この小さなフーリエ級数が、 $L(\chi, s)$ ゼータという大アマゾンの源流である。香り公式と部分分数展開式が実質的に同値であると気づいたのは1年半前である。 $\Rightarrow$ (その14)。

三角関数の対称性が一次の $L(\chi, s)$ ゼータの豊かさを生み出している。2次の保型形式(楕円曲線)ゼータの豊かさは、モデューラ関数の対称性がもたらしていると思われる。

2020.2.1 杉岡幹生