数学IIシケプリ（対戸瀬教員用）

伊達直人

January 29, 2011

はじめに

これは戸瀬教員の講義を受けているみんなへのシケプリです。　このシケプリでは最小多項式、固有多項式、行列式、次元定理について解説、そして最後に過去問の解答解説をして線形代数全体のおさらいをします。というかするつもりです。時間的に全部はできない可能性があるので区切りのいいところで随時更新していきます。

1　最小多項式と固有多項式

1.1　最小多項式

まずは最小多項式についておさらいしましょう。講義は寝てたからおさらいじゃないよ、という人も読んでくださいね。

V を $\boldsymbol{K}$ 線形空間、f を V から V への線形写像とします。（$\boldsymbol{K}$ 線形空間の $\boldsymbol{K}$ とは体という数の集合を表します。講義では $\boldsymbol{K}$ を $\boldsymbol{R}$ や $\boldsymbol{C}$ と考えても良いということでしたね。わかりにくいという人は成分が実数（$\boldsymbol{R}$) や複素数（$\boldsymbol{C}$) のベクトルの集合がそれぞれ $\boldsymbol{R}$,$\boldsymbol{C}$ 線形空間と考えてください。）また f^n を f を n 個合成した写像とします。（n 回微分したものではありませんからご注意を。）$\boldsymbol{K}$ 係数多項式 $F(x)$ について x に f を代入したものは $F(f)$ です。（多項式は定義域が用意されている関数とは違いますから、基本的に和と積のできるものなら何でも代入していいのですね。因みに和と積のできる数の集合のことを「環」といいます。）$F(f) = 0$ を恒等的にみたす多項式 $F(\neq 0)$ のうち、次数が最小であるものを f の最小多項式とよび、通常 φ で表します。ここでは線形写像 f を代入して 0 になる多項式を考えましたが、一般的にある体 $\boldsymbol{K}$ の元 α について、代入して 0 になる次数最小の多項式を最小多項式

といいます。たとえば $\boldsymbol{R}$ の元 α の最小多項式は $F(X) = X - \alpha$ です。最小多項式は様々な性質を持ちます。

性質

f についての多項式 $G(f)$ が $G(f) = 0$ をみたすとき、$G(f)$ は必ず φ を因数に持ちます。つまり $G(f) = H(f) \cdot \varphi$ を満たす多項式 $H(f)$ が存在します。

証明

$\boldsymbol{K}$ 係数多項式の集合を $\boldsymbol{K}[X]$ とします。また $\boldsymbol{K}[X]$ の部分集合 I を $I = \{F(X) \in \boldsymbol{K}[X] \mid F(f) = 0\}$ とします。0 でない I の元で次数が最小のものを $D(X)$ としましょう。I の任意の元 $G(X)$ は $G(X) = D(X)H(X) + R(X)$ と表せます。（ただし $degD > degR$）$G(f) = D(f) = 0$ ですから、$R(f) = 0$ です。しかし $R(f) \neq 0$ とすると $D(X)$ の次数の最小性に反しますから、$R(X) = 0$ です。よって I の任意の元は $D(X)$ を因数に持つことが分かります。

$\boldsymbol{K}[X]$ は単項イデアル整域なんだよ？

この性質は先ほど紹介した「環」などの性質に起因していて、実際に講義でも戸瀬教員はこのことを解説していましたがいささか抽象的で分かりにくいのです。一応講義で解説された範囲内で以下に解説しますが、「環」などについて学ぶのは理学部でも一部の学科に限られるのでは読み飛ばしてもらっても全く構わないと思います。（自己責任で）

さて証明の際に作った部分集合 I のようなものをイデアルといいます。厳密には環 R の部分集合 I で、$r \in R, a, b \in I \Rightarrow \begin{cases} r \cdot a \in R \\ a - b \in R \end{cases}$ が成り立つものをイデアルといいます。また $\boldsymbol{K}[X]$ のイデアルのようにある元の $\boldsymbol{K}[X]$ 倍の元からのみ構成されるイデアルを単項イデアルといいます。環 R のすべてのイデアルが単項イデアルであるとき R を単項イデアル環といいます。$\boldsymbol{K}[X]$ は単項イデアル環ですね。さらに、環 R の任意の元 a, b が $a \cdot b = 0 \Rightarrow aorb = 0$ を満たすとき、R を整域といいます。$\boldsymbol{K}[X]$ は整域ですから、単項イデアル整域なのです。最小多項式の存在は $\boldsymbol{K}[X]$ が単項イデアル整域であることから保証されていたのですね。

単項イデアル整域は $\boldsymbol{K}[X]$ のほかにも整数の集合 $\boldsymbol{Z}$ などがあります。$\boldsymbol{K}[X]$ や $\boldsymbol{Z}$ のイデアルが単項イデアルであることを用いれば、任意の多項式 F, G について $F(X)H_1(X) + G(X)H_2(X) = 1$ を満たす多項式 H_1, H_2 が必ず存在することや任意の整数 a, b について $a \cdot d_1 + b \cdot d_2 = 1$ を満たす整数 d_1, d_2 が

必ず存在することが簡潔に、美しく示せてしまいます。興味がある人はやってみてはどうでしょう。

1.1.1 最小多項式と固有値

線形写像 f の固有値 a とは、$f(x) = ax$ をみたす 0 でない V の元 x が存在するような $\boldsymbol{K}$ の元でしたね。分かりにくいという人は具体的に考えてみましょう。線形写像 f が 3 次正方行列行列 A で表現されるとき、$A\vec{x} = a\vec{x}$ を満たす $\vec{x} \neq 0$ が存在するような a が A の固有値です。つまり A の固有多項式の解ですね。因みにこのときの $\vec{x}$ の集合を**固有空間**というのでした。(「線形写像の表現行列」が分からない人は 1.1.3 節で解説してありますので先にそちらを読んでもらっても構いません) 最小多項式は固有値についても次の性質を持ちます。

性質

a が f の固有値であることと $\varphi(a) = 0$ であることは同値である。

証明

$(\Rightarrow)$ a が f の固有値であるとき、$f(x) = ax$ より $f^n(x) = a^n x$ が成立。$\varphi(f) = m_n f^n + \cdots + m_1 f + m_0$ とすると、$m_i f^i = m_i a^i$ なのでこれを各 i について代入すれば $\varphi(f) = \varphi(a)$ がいえる。

$(\Leftarrow)$ $\varphi(a) = 0$ のとき、$\varphi(X)$ は因数に $(X - a)$ を持つ。つまり $\varphi(X) = (X - a) \cdot H(X)$ を満たす多項式 $H(X)$ が存在する。どんな 0 でない $x \in V$ についても $(f - a)(x) = f(x) - ax = 0$ が成立しないとすると、すべての x について $H(f)(x) = 0$ が成り立つ。しかし H の次数は φ よりも小さく、これは φ の次数の最小性に反する。よって $(f - a)(x) = f(x) - ax = 0$ をみたす 0 でない x が存在する。つまり a は f の固有値である。

ちょっと注意

$H(f)(x)$ などと分かりにくい箇所が多々あったかもしれません。この例で言えば $H(f)$ は多項式 $H(X)$ に線形写像 f を代入したものを $H(f)$ という線形写像と考えて、その写像の $x \in V$ での値を $H(f)(x)$ と表しているのです。多項式と写像を区別しながら読む必要がありますね。

1.1.2 最小多項式を求める

それでは線形空間Vの最小多項式を具体的に求めてみましょう。その前にいくつか準備があります。

線形空間の部分空間の最小多項式

$\boldsymbol{K}$ 線形空間 V がその部分空間 W_1 と W_2 の直和で表せるとします。（直和の意味が分からない人へ。簡単に言うと W_1 と W_2 が V の基底のようになっているということです。つまり任意の V の元がある W_1 の元と W_2 の元の線形結合で表されて、しかもその線形結合の組み合わせはは1通りしかない、ということ。式では $V = W_+ W_2$ と書きます。）このとき W_1 と W_2 に最小多項式 φ_1 と φ_2 が存在するとすると、V の最小多項式 φ は φ_1 と φ_2 の最小公倍式で表されます。一般に V が $W_1, W_2, \cdots, W_n$ の直和であるとき、Vの最小多項式は W_i たちの最小多項式の最小公倍式で表されます。（最小公倍式とは、ここでは φ_1 でも φ_2 でも割り切れる、次数が最小の多項式のことです。最小公倍数と同じ考え方ですね。）

f 安定部分空間

線形空間 V の「基底」について再確認しておきましょう。「$e_1, e_2, \cdots, .e_n \in V$ が基底である」とは任意の V の元が $e_1, e_2, \cdots, .e_n$ の線形結合で表されて、しかも $e_1, e_2, \cdots, .e_n$ は線形独立（一次独立）であるということでした。$e_1, e_2, \cdots, .e_m$ は線形独立だけどこれらの線形結合だけじゃ表されない V の元もある、こともありますし逆に、V の元はすべて $e_1, e_2, \cdots, .e_m$ の線形結合で表されるけどこれらは線形結合じゃない、なんてこともあるわけです。これを踏まえておいてください。

V の元を1つとってきましょう。これを e とします。e を含む V の部分空間 W で、最小多項式をもつものを考えたいのです。どうして？　という疑問はとりあえず抱かないことにして下さい。W を、$e, f(e), f^2(e), \cdots, f^n(e)$ から生成される部分空間にとるとどうでしょう。（「$x_1, x_2, \cdots, x_m$ で生成される部分空間」とは $x_1, x_2, \cdots, x_m$ の線形結合で表されるものの集合のことです。）もし $f^{n+1}(e)$ が $e, f(e), f^2(e), \cdots, f^n(e)$ の線形結合で表されるとすると、$f^{n+1}(e)$ は $f(e)$ の多項式で表されます。（厳密には「ある多項式 $F(X)$ に $f(e)$ を代入した線形写像」ですが、この節では「多項式」と呼ぶことにします。直感的にも「X を $f(e)$ に置き換えたもの」として「多項式」の方がイメージしやすいので。）この多項式を $F_n(f)$ とすれば、「多項式」$f^{n+1} - F_n(f)$ という線形写像は0か e を必ず0に対応させせます。（$f(e)$ を f と略しました。）0に対応するのは0と e だけでしょうか。ちょっと考えてみると $e, f(e), f^2(e), \cdots, f^n(e)$ はそ

れぞれすべて 0 に対応しますね。f は線形写像で、$f(a+b)=f(a)+f(b)$ が成立しますから、$e, f(e), f^2(e), \cdots, f^n(e)$ の線形結合はすべて $f^(n+1)-F_n(f)$ に代入すると 0 となります。ということは、$e, f(e), f^2(e), \cdots, f^n(e)$ の線形結合で表される元の全体は W でしたから $f^{n+1}-F_n(f)$ は W において f の最小多項式ではないでしょうか。そう結論付けるのはちょっと早いかも知れません。なぜなら n を $n-1$ としても同様の議論ができて、$f^(n+1)-F_n(f)$ よりも次数の低い $f^(n)-F_{n-1}(f)$ ができてしまうからです。ではどの n で最小となるのでしょう。ここで、$e, f(e), f^2(e), \cdots, f^n(e)$ は線形独立だけど、$e, f(e), f^2(e), \cdots, f^{n+1}(e)$ は線形独立でないような n を考えてみます。するとどうでしょう、$f^{n+1}(e)$ は $e, f(e), f^2(e), \cdots, f^n(e)$ の線形結合で表されるのに、$f^n(e)$ は $e, f(e), f^2(e), \cdots, f^{n-1}(e)$ の線形結合では表されないのです。だから $f^{n+1}-F_n(f)$ は存在しても $f^(n)-F_{n-1}(f)$ は存在しないのです。これで $f^{n+1}-F_n(f)$ が $e, f(e), f^2(e), \cdots, f^n(e)$ を基底とする部分空間 W における f の最小多項式であることがいえました。この W を、**e の生成する f 安定部分空間**といいます。「安定」というのは"$f(W)\subset W$" が満たされていることから名付けられています。講義では「**f 不変**」とか行列を用いれば「**A 不変**」と言ってましたね。同じことです。

最小多項式を求めましょう

以上のことを用いれば次のようにして行列の最小多項式を求めることができます。

問題　次の行列の最小多項式を求めましょう

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

解答　e_1, e_2, e_3, e_4 を標準基底（第 i 成分が 1 でそれ以外が 0 のベクトルからなる基底）とする。$Ae_1 = e_1 + e_4, A^2e_1 = e_1 + 2e_4 = 2Ae_1 - e_1 \in < e_1, Ae_1 >$ だから、e_1 によって生成される A 安定部分空間 W_{e_1} は $< e_1, Ae_1 > = < e_1, e_4 >$ であり、W_{e_1} での A の最小多項式 φ_{e_1} は $X^2 - 2X + 1$ である。

　$Ae_2 = e_3, A^2e_2 = e_4, A^3e_2 = e_4 = A^2e_2 \in < e_2, Ae_2, A^2e_2 >$ だから、e_2 によって生成される A 安定部分空間 W_{e_2} は $< e_2, Ae_2, A^2e_2 > = < e_2, e_3, e_4 >$ であり、W_{e_2} での A の最小多項式 φ_{e_2} は $X^3 - X^2$ である。

$\boldsymbol{K}^4 = W_{e_1} + W_{e_2}$ だから、A の最小多項式は、$\varphi_{e_1} = X^2 - 2X + 1$ と $\varphi_{e_2} = X^3 - X^2$ の最小公倍式 $X^2(X-1)^2$ である。

1.1.3 線形写像の表現行列

ここで本題とはズレますが線形写像の表現行列について解説します。そんなのもう分かってるよ！　なんて人は読み飛ばしてください。

ここまで線形写像と行列を区別して扱ってきましたが、正直 2 つが同じにしか見えないという人は危ないです。そもそも $\boldsymbol{K}$ 線形空間とは（厳密でなくいえば）元同士の足し算や $\boldsymbol{K}$ 倍について閉じている集合のことでした。そして線形写像とは線形空間の元を線形空間に対応させる写像で、"$f(a+b) = f(a) + f(b)$" を満たすもののことでした。これだけ見ると、線形写像が行列とどう関係あるの？　と疑問に思うかも知れません。実は $m \times n$ 行列は R^n から R^m への線形写像なのです。というよりも成分を $m \times n$ 個ならべたものが線形写像になるように行列の和や積を定義したのです。だから線形写像と行列には切っても切れない縁があるのですね。しかもどんな線形写像も行列で表すことができるのです。

V を $\boldsymbol{K}$ 線形空間、$e_1, e_2, \cdots, .e_n$ を V の基底とします。このとき V の任意の元は $x = a_1e_1 + \cdots + a_ne_n$ と表されますが、この $x \in V$ と $(a_1, a_2, \cdots, a_n)^t \in \boldsymbol{R^n}$ には 1 対 1 対応がありますね。だから V と $\boldsymbol{R}$ を同一視してよいのです。もうひとつ $\boldsymbol{K}$ 線形空間を考えましょう。これを W とします。そして V から W への線形写像を f とします。先ほどの x を f で W に飛ばしましょう。$f(x) = f(a_1e_1) + f(a_2e_2) + \cdots f(a_ne_n) = a_1f(e_1) + a_2f(e_2) + \cdots a_nf(e_n) = b_1h_1 + b_2h_2 + \cdots b_mh_m$（ただし $h_1, h_2, \cdots, h_m$ は W の基底）このときも $f(x) \in W$ と $(b_1, b_2, \cdots, b_m)^t \in \boldsymbol{R^m}$ に 1 対 1 対応を考えることができます。線形写像 f の表現行列とは $A(a_1, a_2, \cdots, a_n)^t = (b_1, b_2, \cdots, b_m)^t$ をみたす A のことです。

話を整理しましょう。f は $V \longrightarrow W$ の線形写像でした。そして V, W はそれぞれ $\boldsymbol{R^n}, \boldsymbol{R^m}$ と同一視できるのでした。V や W では通常行列の計算ができませんが $\boldsymbol{R^n}$ や $\boldsymbol{R^m}$ では行列の計算ができます。そこで V と W のある基底 $< e_1, e_2, \cdots, .e_n >, < h_1, h_2, \cdots, h_m >$ を取って、その基底により $\boldsymbol{R^n}, \boldsymbol{R^m}$ の元となった V, W の元がどのような行列で関係付けられているのか、ということを解説したのです。このときの行列 A を f の $< e_1, e_2, \cdots, .e_n >, < h_1, h_2, \cdots, h_m >$ に関する表現行列といいます。具体的な計算は以上のことを押さえていればできるでしょうから、演習の問題などを解いてみてください。

1.1.4　最小多項式と対角化

線形写像の対角化

$\boldsymbol{K}$ 線形空間 V から V への線形写像 f は V の基底の取り方によっては対角行列で表すことができます。このことを線形写像の対角化といいます。（すべての線形写像が化できるわけではない）線形写像 f が対角化可能である条件は f の最小多項式を用いることで述べることができるのです。

次の条件は同値です

(1) 線形写像 f は対角化可能

(2) V の基底 $x_1, x_2, \cdots, x_n$ で、各 x_i が f の固有ベクトルであるものが存在する

(3) $a_1, a_2, \cdots, a_r$ を f の固有値のすべてであるとして、f の最小多項式 φ が $\varphi = (X - a_1)(X - a_2) \cdots (X - a_r)$ である

(4) $V = V_{a_1} + V_{a_2} + \cdots + V_{a_r}$

(5) $V = V_{a_1} \oplus V_{a_2} \oplus \cdots \oplus V_{a_r}$

1.2　固有多項式

固有多項式は夏学期から **2** 次や **3** 次のものを具体的に求めているので特に込み入った説明は要らないでしょう。しかし行列の固有多項式と線形写像の固有多項式を区別することに注意が必要です。

正方行列 A について $det(\lambda I - A)$ を A の固有多項式といい、通常 $\Phi_A(\lambda)$ と表します。正方行列 A, B について $A = P^{-1}BP$ をみたす正則行列 P が存在するとき、A と B が共役であるといいますが、以下のようにして共役な行列の固有多項式は等しいことが分かります。

$$\begin{aligned}
\Phi_A &= det(\lambda I - A) \\
&= det(\lambda P^{-1} I P - P^{-1} B P) \\
&= det(P^{-1}(\lambda I - B)P) \\
&= det(P^{-1}) det(\lambda I - B) det(P) \\
&= det(\lambda I - B) \\
&= \Phi_B
\end{aligned}$$

一般に線形写像fの表現行列は基底のとり方によって異なりますが、それらの行列はすべて互いに共役です。つまり線形写像 f について固有多項式が唯一つ決まるのです。これを f の固有多項式といい、通常 Φ_f と表します。

1.2.1 固有多項式と固有値

a が線形写像 f の固有値であることと $\Phi_f(a)=0$ とは同値です

証明

$\Phi_f(a)=0$ と $det(f-a)=0$ は同値です。$det(f-a)=0$ は逆行列が存在しないことと同値ですから、これは $f-a$ が単射でないことと同値です。これは $Ker(f-a)\neq 0$ と同値ですから a が固有値であることと同値であることが分かります。

最小多項式 φ は固有多項式 Φ を割り切ります。

この証明にはいくつか補題が必要です。補題の証明は各自挑戦してみて下さい。

補題 1　V の f 安定部分空間 W の f の固有多項式 $\Phi_{|_W}$ は V での f の固有多項式 Φ を割り切る。
　証明略

補題 2　e の生成する f 安定部分空間の最小多項式と固有多項式は等しい。
　証明略

証明

$V=W_1+W_2+\cdots+W_n$ とすると f の最小多項式 φ は $\varphi_{W_1},\cdots,\varphi_{W_n}$ の最小公倍式であり、$\varphi_{W_1},\cdots,\varphi_{W_n}$ はそれぞれ $\Phi_{W_1},\cdots,\Phi_{W_n}$ を割り切るので $\Phi_{W_1},\cdots,\Phi_{W_n}$ を因数に持つ f の固有多項式 Φ は φ で割り切れる。

1.3 行列式

講義では行列式について説明するのに置換やその符号について時間をかなり費やしていたため、一見紆余屈折しているようで混乱してしまった人もいるかも知れません。いったんこの章で整理してみましょう。また行列式に密接に関連する写像について復習して証明問題に備えます。

1.3.1 行列式の定義

n 次正方行列 A の行列式 $det(A)$ を次のように定義します。

$$det(A) = \sum_{\sigma \in \mathcal{S}} sgn(\sigma) a_{\sigma(1)1} a_{\sigma(2)2} \cdots a_{\sigma(n)n} \qquad A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$$

1 つ 1 つの記号を整理していきましょう。$\sigma \in \mathcal{S}$ の σ は 1 から n までの自然数の並び替えについてすべて、という意味です。$\mathcal{S}$ は σ 全体の集合のことで $n!$ 個の元を持ちます。$sgn(\sigma)$ は σ の符号のことですね。σ が偶置換であれば 1, 奇置換であれば-1 です。簡単に言えば上の式の意味は「A の各列から 1 つずつ成分を取ってきてすべて掛け合わせ、その符号を取ってきた成分（例えば第 i 成分）たちの sgn とする」ということです。

1.3.2 多重線形性と交代性を持つ写像

行列式は多重線形性と交代性を持つ写像と深い関わりがあります。そしてこのことが行列式についての証明問題では大きく生きてくるのです。まずはこれらの性質について復習します。

多重線形性

$a_1, a_2, \cdots, a_n$ を変数とする写像 d が次を満たすとき、d は多重線形性を持つという。

$$d(a_1, , \cdots, sa_i + tb_i, \cdots, a_n) = s \cdot d(a_1, , \cdots, a_i, \cdots, a_n) + t \cdot d(a_1, , \cdots, b_i, \cdots, a_n)$$

つまりどの変数についても線形性があるということです。行列式はこの性質をもっていますね。

交代性

$a_1, a_2, \cdots, a_n$ を変数とする写像 d が次を満たすとき、d は交代性を持つという。

$$d(a_1, , \cdots, a_i, \cdots, a_j, \cdots, a_n) = -d(a_1, , \cdots, a_j, \cdots, a_i \cdots, a_n)$$

この性質も行列式は持っています。

命題

n 個の n 次元ベクトル $\vec{a_1}, \vec{a_2}, \cdots, \vec{a_n}$ を変数とする写像 d が多重線形性と交代性を有するとき、次式が成り立つ。

$$d(A) = d(I_n) \cdot det(A) \qquad\qquad A = (\vec{a_1}\vec{a_2} \cdots \vec{a_n})$$

証明

$\boldsymbol{R^n}$ の標準基底を $\vec{e_1}, \vec{e_2}, \cdots, \vec{e_n}$ とする。$\vec{a_1}, \vec{a_2}, \cdots, \vec{a_n}$ をそれぞれ標準基底で表すと、$\vec{a_1} = \sum_{k=1}^{n} a_{k1}\vec{e_k}, \cdots, \vec{a_i} = \sum_{k=1}^{n} a_{ki}\vec{e_i}, \cdots$ である。よって $d(A) = d(\sum_{k=1}^{n} a_{k1}\vec{e_k}, \cdots, \sum_{k=1}^{n} a_{ki}\vec{e_i}, \cdots)$ を多重線形性によって展開すると交代性により $d(\cdots, e_i, \cdots, e_i, \cdots) = 0$ などが成り立つので、結局残る項は d が $\vec{e_1}, \vec{e_2}, \cdots, \vec{e_n}$ をそれぞれ 1 つずつすべて変数に持つ場合で、これらを 1 から順に並び替えると d の符号はその sgn である。

よって $d(A) = d(I_n) \sum_{\sigma \in \mathcal{S}} sgn(\sigma) a_{\sigma(1)1} a_{\sigma(2)2} \cdots a_{\sigma(n)n} = d(I_n) \cdot det(A)$

この写像を用いて次のような等式を示せます。

$$det \begin{pmatrix} A & C \\ O & B \end{pmatrix} = det(A) \cdot det(B)$$

解答　写像 d を $d : A \longrightarrow det \begin{pmatrix} A & C \\ O & B \end{pmatrix}$ と定義すると、d は A の列ベクトルについて多重線形性と交代性を持つ。よって $d(A) = d(I_n) \cdot det(A) = det \begin{pmatrix} I_n & C \\ O & B \end{pmatrix} \cdot det(A) = det(B) \cdot det(A)$ これで示せた。