

本にあるように A の最小多項式を $\phi_A(x)$ とすれば、 $f(A) = 0$ となるスカラ係数の多項式 $f(x)$ はすべて、 $\phi_A(x)$ で割り切れることを示す。

代数学の話として、 $h(x)$ の x の次数が $\phi_A(x)$ の次数より小さいとして、

$$f(x) = g(x)\phi_A(x) + h(x) \quad (1)$$

と表される。(https://ja.wikipedia.org/wiki/除法の原理#多項式に対する除法の原理 参照のこと。) 本にあるように、A を $f(x)$ に代入して、 $f(A) = 0$ になること、最小多項式の定義より、 $\phi_A(A) = 0$ に、注意すると、

$$0 = f(A) = g(A)\phi_A(A) + h(A) = h(A) \quad (2)$$

よって、 $h(A) = 0$ になる。しかし、 $h(x)$ が x の多項式であれば、 $\phi_A(x)$ より次数が小さい、 $h(x)$ が、 $h(x) = 0$ となるため、最小多項式の定義に反する。そのため、 $h(x)$ は恒等的に 0 になる。(つまり $h(x) = 0$) なお、この議論では、右から割り切れる、左から割り切れるについて考慮していないが、P.144 の問 3 の最後の部分のように、スカラ係数の多項式の場合は、右から割った場合と、左から割った場合の商は一致する。

上記の議論より、 $\phi_A(x)$ の次数は一意に決まる。

同じ次数の $\phi_A(x) = 0, \phi_A'(x) = 0$ が存在するとする。その場合、上記の議論の $f(x)$ を $\phi_A(x)$ と考えることができ、

$$\phi_A'(x) = g(x)\phi_A(x) \quad (3)$$

となる。次数を比較すると $g(x)$ は定数になるが、P.144 にあるように、最高次数の係数が 1 になっているので、実数倍の任意性はない。そのため、

$$\phi_A'(x) = \phi_A(x) \quad (4)$$

となり、 $\phi_A(x)$ と異なる、 $\phi_A'(x)$ は存在せず、 $\phi_A(x)$ は一意になる。

次に”A の最小多項式 $\phi_A(x)$ の根は (重複度を無視すれば) 固有値と一致する”ことの別証について確認する。

まず、行列係数の多項式にするということを考えると、 c_i を $c_i E$ とすることが考えられる。この際、スカラとしては

$$\phi_A(x) = \sum_{i=0}^n c_i x^{n-i} \quad (5)$$

が

$$\sum_{i=0}^n c_i E x^{n-i} = \left(\sum_{i=0}^n c_i x^{n-i} \right) E = \phi_A(x) E \quad (6)$$

となり、等式を満たす。これは行列 X を変数としても、 X と E や $c_i E$ は常に X と可換なので、

$$\phi_A(X) E = \phi_A(X) = \sum_{i=0}^n c_i X^{n-i} = \sum_{i=0}^n c_i E X^{n-i} = \sum_{i=0}^n c_i X^{n-i} E = \left(\sum_{i=0}^n (c_i E) X^{n-i} \right) \quad (7)$$

となり、等式を満たす。

つまり、行列係数の多項式にするには、

$$\phi_A(x) E = \sum_{i=0}^n c_i E x^{n-i} \quad (8)$$

とすればよく、これは、スカラ x でも行列 $X(x)$ (とも書いたりする) でも常時成立する。

さて、最小多項式の定義より、 $\phi_A(A) = 0$ (行列の 0) になることはわかっている。その結果、(8) の左辺も 0 となる。

ここで (1) と同じように、P.145 の左辺を $(xE - A)$ で割ったときの剰余を考える。つまり、ひとまず、(1) で $g(x)$ に相当する何かしらの行列 $B^*(x)$ を利用して、

$$\phi_A(x)E = (xE - A)B^*(x) + H(x) \quad (9)$$

とかける。ここで、 $H(x)$ は $(xE - A)$ より x の次数が小さくなる。つまり、 x について、0 次となり、定数の行列 $H(x) = H$ となる。

(11) に A を代入すると、

$$\phi_A(A)E = H = 0 \quad (10)$$

となり、 $H = 0$ (行列) が求まる。

つまり、

$$\phi_A(x)E = (xE - A)B^*(x) \quad (11)$$

となり、 $\phi_A(x)E$ は $(xE - A)$ で割り切れる。

と、前回の会のときに思ったが、よく考えると x はスカラでないと話が進まない気がする。そうした場合、 $B^*(x) = \sum_{i=0}^{n-1} B_i^* x^i$ として、

$$\phi_A(x)E = (xE - A)B^*(x) + H = (xE - A)\left(\sum_{i=0}^{n-1} B_i^* x^i\right) + H \quad (12)$$

となり、係数を比較すると、まず、 $c_n E = B_{n-1}$ になる。

また、 $1 \leq i \leq n-1$ に対して、 $c_i E = -AB_i + B_{i-1}$ になる。これを考えると、 $0 \leq i \leq n-1$ で $B_i = \sum_{j=i+1}^n c_j A^{j-i-1}$

すると、 $c_0 E = -\sum_{j=1}^n c_j A^j + H$ となり、

$$H = \sum_{j=0}^n c_j A^j = \phi_A(A) = 0 \quad (13)$$

となる。よって、

$$\phi_A(x)E = (xE - A)B^*(x) \quad (14)$$

と割り切れる。

本にあるようにこの式の両辺の行列式を取れば、左辺は、

$$|\phi_A(x)E| = \phi_A(x)^n \quad (15)$$

右辺は P.140 の (2) を利用して、

$$|(xE - A)B^*(x)| = |(xE - A)| |B^*(x)| = f_A(x) |B^*(x)| \quad (16)$$

よって、本にあるように、

$$\phi_A(x)^n = f_A(x) |B^*(x)| \quad (17)$$

となり、スカラの多項式 $\phi_A(x)^n$ はスカラの多項式 $f_A(x)$ で割り切れる。 ($|B^*(x)|$ もスカラの多項式になっており、これらから、 $\phi_A(x)^n$ が最も、 x の次数が高いことがわかる。)

なお、P.140 の (4) の上の部分を考えると、

$$f_A(x) = \prod (x - a_i)^{s_i} \quad (18)$$

となる。 a_i の重複度を s_i とする。 $s_i \geq 1$ であり、重複度を含めて固有値は n 個なので、 $\sum s_i = n$ 。よって、 $s_i \leq n$ となる。

多項式が割り切れるためには割られる側の多項式は割る多項式の因数をすべて持つ必要がある。 $\phi_A(x)^n$ は n 乗されているので、同じ因数を n 個以上持っており、 $f_A(x)$ は n 個の因数しか持たないので、 $\phi_A(x)$ は $f_A(x)$ に含まれる因数をすべて持つ必要があるが、少なくとも 1 個だけ持てば良い。

上記より、”A の最小多項式 $\phi_A(x)$ の根は (重複度を無視すれば) 固有値と一致する”が言える。