BEVIS FOR CAYLEY–HAMILTON-TEOREMET

FORELESNING E12

TEOREM (CAYLEY – HAMILTON)

La $f: V \to V$ være en lineær operator på et endeligdimensjonalt vektorrom V og la $p(x)$ være det karakteristiske polynomet til f. Da er

$$\boxed{p(f) = 0}.$$

f - INVARIANTE ONDERRUIMTEN

$f : V \longrightarrow V$

DEFINISJON

Et underrom $U \subset V$ er invariant under f (a.k.a. f-invariant) hvis $\bar{v} \in U \Rightarrow f(\bar{v}) \in U$ (i.e. $f(U) \subset U$).

EKSEMPEL

La $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ være gitt ved $f(x,y) = (x+y, x+y)$.
Er underrommet

$$U = \{ (x,x) \mid x \in \mathbb{R} \} \subset \mathbb{R}^2$$

invariant under f? JA!

La $\bar{v} \in U$. Da er $\bar{v} = (x,x)$ for en $x \in \mathbb{R}$.
Det betyr $f(\bar{v}) = (x+x, x+x)$
$= (2x, 2x) \in U$.

$f: V \longrightarrow V$

DEFINISJON

Et underrom $U \subset V$ er invariant under f (a.k.a. f-invariant) hvis $\bar{u} \in U \Rightarrow f(\bar{u}) \in U$ (i.e. $f(U) \subset U$).

EKSEMPEL

La $f: \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ vare gitt ved $f(x,y) = (x+y, x+y)$.

Er underrommet

$$U = \{(x,x) \mid x \in \mathbb{R}\} \subset \mathbb{R}^2$$

invariant under f? JA!

Er underrommet

$$U' = \{(x,0) \mid x \in \mathbb{R}\} \subset \mathbb{R}^2$$

f-invariant? NEI!

$(1,0) \in U'$, men

$f(1,0) = (1,1) \notin U'$

$\square$

$f : V \to V$

DEFINISJON

Et underrom $U \subset V$ er invariant under f (a.k.a. f-invariant) hvis $\bar{u} \in U \Rightarrow f(\bar{u}) \in U$ (i.e. $f(U) \subset U$).

EKSEMPEL

La $D : \mathbb{R}[x] \to \mathbb{R}[x]$ være gitt ved derivasjon, $D(p) = p'$. Da er $\mathbb{R}[x]_{\leq n} \subset \mathbb{R}[x]$ et D-invariant underrom for hver $n \geq 0$.

$$p \in \mathbb{R}[x]_{\leq n} \Rightarrow \deg(p) \leq n$$

$$\Rightarrow \deg(D(p)) \leq n$$

$$\Rightarrow D(p) \in \mathbb{R}[x]_{\leq n}$$

$\square$

$f : V \to V$

KONSTRUKSJON / OBSERVASJON

La $\bar{0} \neq \bar{v} \in V$. Definér

$$U_{\bar{v}} = \operatorname{span}(\bar{v}, f(\bar{v}), f^2(\bar{v}), f^3(\bar{v}), \ldots) \subset V.$$

Da er $U_{\bar{v}}$

- et f-invariant underrom av V, og
- det minste f-invariante underrommet av V som inneholder $\bar{v}$.

Kommer som samarbeidsoppgave.

$f: V \to V$

HUSK

Hvis $\phi: X \to Y$ er en funksjon og $Z \subset X$ er en delmengde, så får vi en funksjon $\phi|_Z : Z \to Y$ gitt ved $\phi|_Z(s) = \phi(s)$ for hver $s \in Z$.

OBSERVASJON

Hvis $U \subset V$ er invariant under f, så får vi en lineær operator $f|_U$ på vektorrommet U, altså

$$f|_U : U \to U$$

gitt ved $f|_U(\bar{u}) = \underbrace{f(\bar{u})}_{\in U}$ for hver $\bar{u} \in U$. $\square$

$\in U$ fordi U er f-invariant!

LEMMATA

$f: V \to V$

LEMMA I

La V være endeligdimensjonalt og la $U \subset V$ være et f-invariant underrom. Da er det karakteristiske polynomet til $f|_U$ en faktor i det karakteristiske polynomet til f. Altså, $\text{charpol}(f|_U) \mid \text{charpol}(f)$.

NOTASJON

Et polynom q er en faktor i et polynom p hvis det finnes et polynom s slik at $p = q \cdot s$. Dette noteres $q \mid p$.

EKSEMPEL

$(x+2) \mid (x^3 + 3x^2 + 3x + 2)$ siden $\underbrace{x^3 + 3x^2 + 3x + 2}_{p} = \underbrace{(x+2)}_{q} \cdot \underbrace{(x^2 + x + 1)}_{s}$. $\square$

$f: V \to V$

LEMMA I

La V være endeligdimensjonalt og la $U \subset V$ være et f-invariant underrom. Da er det karakteristiske polynomet til $f|_U$ en faktor i det karakteristiske polynomet til f. Altså, $\text{charpol}(f|_U) \mid \text{charpol}(f)$.

BEVIS

La $\gamma = \{\bar{v}_1, \dots, \bar{v}_k\}$ være en ordna basis for U og utvid til en ordna basis $\beta = \{\bar{v}_1, \dots, \bar{v}_k, \bar{v}_{k+1}, \dots, \bar{v}_n\}$ for V. La $B = [f]_\beta$ og $C = [f|_U]_\gamma$. Da er B på formen

$$B = \begin{pmatrix} C & ? \\ 0 & ? \end{pmatrix}$$

Null fordi $f(U) \subset U$

så $\text{charpol}(f|_U) = \det[C - x \cdot I_{k\times k}] \mid \det[B - x \cdot I_{n \times n}] = \text{charpol}(f)$. $\square$

$f: V \to V$

LEMMA II

La V være endeligdimensjonalt og la $\bar{0} \neq \bar{v} \in V$. Skriv $U = U_{\bar{v}}$ $(= \operatorname{span}(\bar{v}, f(\bar{v}), f^2(\bar{v}), f^3(\bar{v}), \ldots))$ og $\dim U = k$.

i) Mengden $\{\bar{v}, f(\bar{v}), f^2(\bar{v}), \ldots, f^{k-1}(\bar{v})\}$ er en basis for U.

ii) Hvis

$$a_0 \bar{v} + a_1 f(\bar{v}) + a_2 f^2(\bar{v}) + \ldots + a_{k-1} f^{k-1}(\bar{v}) + 1 f^k(\bar{v}) = \bar{0},$$

så er

$$\operatorname{charpol}(f|_U) = (-1)^k (a_0 + a_1 x + a_2 x^2 + \ldots + a_{k-1} x^{k-1} + 1 x^k)$$

LEMMA II

$f: V \to V$

La V være endeligdimensjonalt og la $\bar{o} \neq \bar{v} \in V$. Skriv $U = U_{\bar{v}}$ $(= \operatorname{span}(\bar{v}, f(\bar{v}), f^2(\bar{v}), f^3(\bar{v}), \dots))$ og $\dim U = k$.

i) Mengden $\{\bar{v}, f(\bar{v}), f^2(\bar{v}), \dots, f^{k-1}(\bar{v})\}$ er en basis for U.

BEVIS i

La $j \geq 0$ være det største tallet slik at

$$\beta = \{\bar{v}, f(\bar{v}), f^2(\bar{v}), \dots, f^{j-1}(\bar{v})\}$$

er lineært uavhengig. Det holder å vise at $U = \operatorname{span}(\beta)$.

Det er klart at $\operatorname{span}(\beta) \subset U$. Så siden $U = U_{\bar{v}}$ er det minste underrommet av V som er f-invariant og inneholder $\bar{v}$, holder det å vise at $\operatorname{span}(\beta)$ er f-invariant.

La $j \geq 0$ være det største tallet slik at

$$\beta = \{\bar{v}, f(\bar{v}), f^2(\bar{v}), \dots, f^{j-1}(\bar{v})\}$$

er lineært uavhengig. Det holder å vise at span (β) er f-invariant.

Merk at $f^j(\bar{v}) \in \mathrm{span}(\beta)$. Nå tar vi en vilkårlig $\bar{u} \in \mathrm{span}(\beta)$.

Da er

$$\bar{u} = a_0 \bar{v} + a_1 f(\bar{v}) + a_2 f^2(\bar{v}) + \dots + a_{j-1} f^{j-1}(\bar{v}), \quad a_i \in F$$

og derfor blir

$$f(\bar{u}) = f\left(a_0 \bar{v} + a_1 f(\bar{v}) + a_2 f^2(\bar{v}) + \dots + a_{j-1} f^{j-1}(\bar{v})\right)$$

$$= \underbrace{a_0 f(\bar{v}) + a_1 f^2(\bar{v}) + \dots + a_{j-2} f^{j-1}(\bar{v})}_{\in \mathrm{span}(\beta)} + \underbrace{a_{j-1} f^j(\bar{v})}_{\in \mathrm{span}(\beta)} \in \mathrm{span}(\beta).$$

Dette viser at span (β) er f-invariant.

LEMMA II

$f : V \to V$

La V være endeligdimensjonalt og la $\bar{0} \neq \bar{v} \in V$. Skriv $U = U_{\bar{v}}$ $(= \text{span}(\bar{v}, f(\bar{v}), f^2(\bar{v}), f^3(\bar{v}), \dots))$ og $\dim U = k$.

ii) Hvis $a_0 \bar{v} + a_1 f(\bar{v}) + a_2 f^2(\bar{v}) + \dots + a_{k-1} f^{k-1}(\bar{v}) + 1 f^k(\bar{v}) = \bar{0}$,
så er $\text{charpol}(f|_U) = (-1)^k (a_0 + a_1 x + a_2 x^2 + \dots + a_{k-1} x^{k-1} + 1 x^k)$.

BEVIS ii

Vi vet at $\text{charpol}(f|_U) = \text{charpol}\,[f|_U]_\beta$ hvor β er en vilkårlig ordna basis for U. Vi bruker
$\beta = \{\bar{v}, f(\bar{v}), f^2(\bar{v}), \dots, f^{k-1}(\bar{v})\}$ fra i). Anta at
$a_0 \bar{v} + a_1 f(\bar{v}) + a_2 f^2(\bar{v}) + \dots + a_{k-1} f^{k-1}(\bar{v}) + 1 f^k(\bar{v}) = \bar{0}$. Da blir

$$[f|_U]_\beta = \begin{bmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \dots & 0 & -a_{k-2} \\ 0 & 0 & \dots & 1 & -a_{k-1} \end{bmatrix}$$

med $\text{charpol}\,[f|_U]_\beta = (-1)^k (a_0 + a_1 x + a_2 x^2 + \dots + a_{k-1} x^{k-1} + 1 x^k)$. $\square$

BEVIS FOR

CAYLEY – HAMILTON-TEOREMET

TEOREM (CAYLEY – HAMILTON)

La $f: V \to V$ være en linear operator på et endeligdimensjonalt vektorrom V og la $p(x)$ være det karakteristiske polynomet til f. Da er

$$\boxed{p(f) = 0}.$$

BEVIS

Vi må vise at $\boxed{p(f)(\bar{v}) = \bar{0} \quad \forall \ \bar{v} \in V}$. Dette er opplagt for $\bar{v} = \bar{0}$, så anta at $\bar{v} \neq \bar{0}$. Se på $U = U_{\bar{v}}$ som i BEVIS for LEMMA II. Ved i) finnes $a_0, \dots, a_{k-1} \in F$ slik at

$$a_0 \bar{v} + a_1 f(\bar{v}) + a_2 f^2(\bar{v}) + \dots + a_{k-1} f^{k-1}(\bar{v}) = -f^k(\bar{v}) \qquad (*)$$

og dermed gir ii) at

$$\operatorname{charpol}(f|_U) = q(x) = (-1)^k (a_0 + a_1 x + a_2 x^2 + \dots + a_{k-1} x^{k-1} + x^k) \ (**).$$

$(*)$ og $(**)$ gir til sammen

$$\boxed{q(f)(\bar{v})} = (-1)^k (a_0 \bar{v} + a_1 f(\bar{v}) + a_2 f^2(\bar{v}) + \dots + a_{k-1} f^{k-1}(\bar{v}) + f^k(\bar{v})) \boxed{= \bar{0}}.$$

Ved LEMMA I er q en faktor i $p = \mathrm{charpol}(f)$, altså $p = q \cdot s$ for et polynom s. Det følger at $p(f)(\bar{v}) = \bar{0} \quad \forall \ \bar{v} \in V$. $\square$