Oblig 2 - MAT4000

Fredrik Meyer

1 Oppgave 1 - V07

La $f : \mathbb{Z}/(10) \to \mathbb{Z}/(10)$ og $g : \mathbb{Z}/(10) \to \mathbb{Z}/(10)$ være definert ved $f(x) = x^3$ og $g(x) = 3x^3$.

Oppgave 1.1 (a)**.** *f og g er bijeksjoner av* $\mathbb{Z}/(10)$.

Proof. Siden $10 = 2 \cdot 5$ og 2 og 5 er primtall, oppfyller f fra Setning 1.3 i Kryptografiheftet kravene for å være en bijeksjon.

La $h : \mathbb{Z}/(10) \to \mathbb{Z}/(10)$ være definert ved $h(x) = 3x$. Da er h en bijeksjon av $Z/(10)$ siden $(10, 3) = 1$. Siden $g = h \circ f$, og både h og f er bijeksjoner, må også g være det. □

Oppgave 1.2 (b)**.** *Du har kryptert en PIN-kode, som er et 4-sifret desimaltall,* $s_1s_2s_3s_4$*, ved å beregne sekvensen* $g(s_1), g(s_2), g(s_3), g(s_4)$ *i* $\mathbb{Z}/(10)$*. Den krypterte sekvensen er* $2, 6, 9, 5$*. Hva er PIN-koden?*

Proof. Vi må finne g^-1. Siden $g = h \circ f$, er $g^{-1} = f^{-1} \circ h^{-1}$. Vi finner disse hver for seg. For å finne h^{-1}, må vi løse ligningen $3x \equiv 1 \pmod{10}$. Vi kan bruke Euklids algoritme til å gjøre dette, men siden 10 er såpass lavt tall, ser vi raskt at 7 gjør jobben vi ønsker. Med andre ord er $3 \cdot 7 \equiv 21 \equiv 1 \pmod{10}$. Vi konkluderer med at $h^{-1}(x) = 7x$.

Vi ønsker å finne f^{-1}. Fra Setning 1.3 i Kryptografiheftet lar vi $M = (2 - 1)(5 - 1) = 4$, og løser likningen $3x = 1 \pmod{4}$. Igjen er 4 et så lavt tall at vi raskt ser at $x = 3$ er en løsning. Det følger fra Setning 1.3 at $f^{-1}(x) = x^3$.

Dermed er $g^{-1}(x) = f^{-1}(h^{-1}(x)) = f^{-1}(7x) = (7x)^3 = 3x^3$. Nå gjenstår

bare utregning:

$$\begin{aligned} g^{-1}(2) &= 3 \cdot 2^3 = 4 \\ g^{-1}(6) &= 3 \cdot 6^3 = 3^4 \cdot 2^3 \\ &= 81 \cdot 8 = 1 \cdot 8 = 8 \\ g^{-1}(9) &= 3 \cdot 9^3 = 3 \cdot 3^6 \\ &= 3^7 = 3^4 \cdot 3^3 = 1 \cdot 7 = 7 \\ g^{-1}(5) &= 3 \cdot 5^3 = 3 \cdot 5 = 5 \end{aligned}$$

Så PIN-koden er 4875. □

Oppgave 4 - V07

La $A = \begin{bmatrix} 2 & 1+i \\ 1-i & 3 \end{bmatrix} \in M_{2\times 2}(\mathbb{C})$. Begrunn at A er unitært diagonaliserbar og bestem en unitær $U \in M_{2\times 2}(\mathbb{C})$ som er slik at U^*AU er diagonal.

Proof. Vi legger merke til at $A^* = \begin{bmatrix} 2 & 1+i \\ 1-i & 3 \end{bmatrix} = A$. Da er spesielt A normal, siden $A^*A = AA^*$. En kvadratisk kompleks matrise er unitært diagonaliserbar hvis og bare hvis matrisen er normal, så det følger at A er unitært diagonaliserbar.

Vi må finne egenvektorer for A. Vi finner først egenverdiene:

$$\det|A - \lambda I| = \begin{vmatrix} 2-\lambda & 1+i \\ 1-i & 3-\lambda \end{vmatrix} = \lambda^2 - 5\lambda + 4$$

Det følger at $\lambda_1 = 4$ og $\lambda_2 = 1$ er egenverdier for A. Vi finner egenvektorer:

$$\begin{bmatrix} -2 & 1+i \\ 1-i & -1 \end{bmatrix} \sim^{(1+i)II} \begin{bmatrix} -2 & 1+i \\ 2 & -1-i \end{bmatrix} \sim^{II+I} \begin{bmatrix} -2 & 1+i \\ 0 & 0 \end{bmatrix}$$

Så $\begin{bmatrix} 1 \\ \frac{1}{2} + \frac{1}{2}i \end{bmatrix}$ er en egenvektor for A. Vi normaliserer og setter $v_1 = \sqrt{\frac{2}{3}} \begin{bmatrix} 1 \\ \frac{1}{2} + \frac{1}{2}i \end{bmatrix}$. På samme måte finner vi v_2 og får at $v_2 = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 \\ -1-i \end{bmatrix}$. Vi setter $U = [v_1, v_2]$, og det følger at $A = UDU^*$ hvor $D = \text{diag}(4, 1)$. Dermed er $D = U^*AU$, og vi er ferdige. □

Oppgave 4 - V08

La V og W være vektorrom over $\mathbb{K}$, der $\mathbb{K} = \mathbb{C}$ eller $\mathbb{R}$. La $T : V \to W$ og $S : W \to V$ være lineæravbildninger. Anta at $ST = I$ der I er identitetsavbildningen $I : V \to V$. La $Q = TS$.

Oppgave 1.3. *Da er $W = R(T) \oplus N(S)$ og Q er projeksjonsavbildningen fra W på R(T) langs N(S).*

Proof. Ønsker å vise at $W = R(T) + N(S)$. La så $w \in W$. Da er $w = Q(w) + w - Q(w)$. Da er $Q(w) \in R(T)$: for $Q(w) = T(S(w))$, så det eksisterer en $w = S(w)$ slik at $T(w) = Q(w)$, og dermed er $Q(w) \in R(T)$. Vi har også at $w - Q(w) \in N(S)$:

$$\begin{aligned} S(w - Q(w)) &= S(w) - SQ(w) \\ &= S(w) - STS(w) \\ &= S(w) - SI(w) \\ &= S(w) - S(w) = 0 \end{aligned}$$

så $w - Q(w) \in N(S)$. Vi må vise at $R(T)$ og $N(S)$ er uavhengige underrom. Vi må vise at $R(T) \cap N(S) = \{0\}$. Så, anta $v \in R(T)$ $capN(S)$. Da er spesielt $S(v) = 0$ og det finnes en $v' \in V$ slik at $T(v') = v$. Men siden $ST = I$ er da $I(v') = ST(v') = S(v) = 0$. Siden identitetsavbildningen er 1-1, er dermed $v' = 0$. Men siden $T(v') = v$, er $v = T(v') = T(0) = 0$, så $v = 0$, som ønsket.

Anta nå $w_1 \in R(T)$ og $w_2 \in N(S)$. Da er $Q(w_1+w_2) = Q(w_1)+Q(w_2) = TS(w_1) + TS(w_2) = TS(w_1) + 0$. Siden $w_1 \in R(T)$, eksisterer en w_1' slik at $T(w_1') = w_1$. Dermed er $TS(w_1) = TST(w_1') = T(w_1') = w_1$, og dermed er $Q(w_1 + w_2) = w_1$, så Q er projeksjonsavbildningen fra W på R(T) langs N(S). □

Oppgave 1.4. *Anta videre at V og W er endeligdimensjonale. Da er* $\dim V \leq \dim W$ *og* $\dim N(s) = \dim W - \dim W$.

Proof. Siden $W = R(T) \oplus N(S)$, er $\dim W = \dim R(T) + \dim N(S)$, så $\dim N(S) = \dim W - \dim R(T)$. Ved dimensjonsteoremet følger det at $\dim N(S) = \dim W - \dim V + \dim N(T)$. Det holder å vise at $\dim N(T) = 0$. Anta så $v \in N(T)$. Da er $T(v) = 0$, og det følger at $I(v) = ST(v) = S(0) = 0$, så $I(v) = 0$. Men I er 1-1, så $v = 0$. Det følger at $\dim N(T) = 0$. Dermed er $\dim N(S) = \dim W - \dim V$. Ulikheten følger direkte fra likheten. □

Oppgave 4 - V09

La V være et endeligdimensjonalt vektorrom over $\mathbb{C}$, $V \neq \{0\}$, og la $T \in L(V)$. Betrakt følgende to utsagn:

1) T er diagonaliserbar.
2) Det eksisterer en basis B for V slik at $[T]_B$ er normal.

Oppgave 1.5. 1) $\Rightarrow$ 2

Proof. Anta T er diagonaliserbar, og la C være en eller annen basis for V. Da er $[T]_C$ similær med en diagonalmatrise. Men dette er det samme som at det finnes en basis B slik at $[T]_C$ er diagonal. Siden diagonalmatriser kommuterer og er sin egen transponert, og derfor er normale, er vi ferdige. □

Oppgave 1.6. 2) $\Rightarrow$ 1)

Proof. En matrise N er unitært diagonaliserbar hvis og bare hvis den er normal. Det følger at det eksisterer en U slik at $U[T]_B U^{-}1$ er diagonal. □

Oppgave 6 - V09

La V være et endeligdimensjonalt vektorrom (over $\mathbb{R}$ eller $\mathbb{C}$). La $T \in L(V)$ og anta $R(T) = R(T^2)$. Begrunn at $N(T) = N(T^2)$. Begrunn deretter at $V = R(T) \oplus N(T)$.

Proof. Vi begrunner først at $N(T) = N(T^2)$. Siden V er endeligdimensjonalt, kan vi bruke dimensjonsteoremet, og vi får

$$\dim N(T) + \dim R(T) = \dim V = \dim N(T^2) + \dim R(T^2)$$

Siden $R(T) = R(T^2)$, følger det at $\dim N(T) = \dim N(T^2)$. Da er $N(T)$ er et underrom av $N(T^2)$: for la $u, v \in N(T)$. Da er $T(T(au + bv)) = T(aT(u) + bT(v)) = T(0 + 0)) = 0$. Men siden de har samme dimensjon, må de være like. Dermed $N(T) = N(T^2)$.

Så til begrunnelsen for at $V = R(T) \oplus N(T)$. Vi viser først at enhver $v \in V$ kan skrives som en sum av en vektor fra $R(T)$ og en fra $N(T)$. For siden $R(T) = R(T^2)$, eksisterer det for alle $v \in V$ en w slik at $T(v) = T^2(w)$. Dermed er $T(v - T(w)) = T(v) - T^2(w) = T(v) - T(v) = 0$, så $v - T(w) \in N(T)$. La nå $v \in V$. Fra ligningen $(v - T(w)) + T(w)$ følger det at $V = R(T) + N(T)$.

Vi må vise at underrommene er uavhengige. Så, anta at $v \in R(T) \cap N(T)$. Da eksisterer en v' slik at $T(v') = v$ og $T(v) = 0$. Det følger at $T^2(v') = T(T(v')) = T(v) = 0$, så $v' \in N(T^2)$. Men siden $N(T) = N(T^2)$, er også $v = T(v') = 0$. Dermed må $R(T) \cap N(T) = \{0\}$, og underrommene er uavhengige. $\square$