UNIVERSITETET I OSLO

Det matematisk-naturvitenskapelige fakultet

Eksamen i:	MAT3000 — Tall, rom og lineæritet.
Eksamensdag:	Torsdag 14. juni 2007.
Tid for eksamen:	14.30 – 17.30.
Oppgavesettet er på 3 sider.	
Vedlegg:	Ingen.
Tillatte hjelpemidler:	Ingen.

Kontroller at oppgavesettet er komplett
før du begynner å besvare spørsmålene.

Oppgave 1

La $f : \mathbb{Z}/(10) \to \mathbb{Z}/(10)$ og $g : \mathbb{Z}/(10) \to \mathbb{Z}(10)$ være definert ved

$$f(\overline{x}) = \overline{x}^3 \text{ og } g(\overline{x}) = \overline{3} \cdot \overline{x}^3, \quad \overline{x} \in \mathbb{Z}/(10).$$

a) Begrunn at f og g begge er bijeksjoner av $\mathbb{Z}/(10)$.

b) Du har kryptert en PIN-kode, som er et 4-sifret desimaltall $s_1s_2s_3s_4$, ved å beregne sekvensen $g(\overline{s_1}), g(\overline{s_2}), g(\overline{s_3}), g(\overline{s_4})$ i $\mathbb{Z}/(10)$.

Den krypterte sekvensen du beregnet er $\overline{2}, \overline{6}, \overline{9}, \overline{5}$. Hva er PIN-koden ?

Oppgave 2

La p være et primtall, $p \geq 3$.

a) La $\overline{a}, \overline{b} \in \mathbb{Z}/(p)$. Anta at $\overline{a}$ er en kvadratisk rest i $\mathbb{Z}/(p)$, mens $\overline{b}$ ikke er det. Vis at $\overline{ab}$ ikke er en kvadratisk rest i $\mathbb{Z}/(p)$.

b) Anta at $p \equiv 3 \pmod 4$ og at n er et naturlig tall som kan skrives på formen $n = x^2 + y^2$ der x og y er hele tall. Begrunn at $n \not\equiv kp \pmod{p^2}$ for alle $k \in \{1, \cdots, p-1\}$.

(Fortsettes side 2.)

Oppgave 3

La $V \neq \{0\}$ være et endelig dimensjonalt vektorrom over $\mathbb{K}$, der $\mathbb{K}$ betegner enten $\mathbb{R}$ eller $\mathbb{C}$. La T være en lineær avbildning fra V inn i V, m.a.o. la $T \in \mathcal{L}(V)$, og la $\mathcal{O} : V \to V$ betegne null-avbildningen (som avbilder alle vektorene i V på nullvektoren i V).

Anta at T er diagonaliserbar og at det fins et naturlig tall n slik at $T^n = \mathcal{O}$. Begrunn at $T = \mathcal{O}$.

Oppgave 4

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 matrisen $U^* A U$ er diagonal.

Oppgave 5

La V være et endelig dimensjonalt indreprodukt rom over $\mathbb{K}$, der $\mathbb{K}$ betegner enten $\mathbb{R}$ eller $\mathbb{C}$. Anta at $\dim(V) := n \geq 1$ og la $\mathcal{B}$ være en ortonormal basis for V. Vi definerer da et indreprodukt på $\mathcal{L}(V)$ ved

$$< S\,,\, T >' = \operatorname{tr}\left([S]_{\mathcal{B}}\,[T]_{\mathcal{B}}^{*}\right), \quad S, T \in \mathcal{L}(V),$$

der $\operatorname{tr} : M_{n\times n}(\mathbb{K}) \to \mathbb{K}$ betegner trase-avbildningen (så $\operatorname{tr}(A)$ er gitt ved summen av koeffisientene til A langs hoveddiagonalen).
Med andre ord, vi har at

$$< S\,,\, T >' = < [S]_{\mathcal{B}}\,,\, [T]_{\mathcal{B}} >, \quad S, T \in \mathcal{L}(V),$$

der $< \cdot\,,\, \cdot >$ betegner Frobenius indreproduktet på $M_{n\times n}(\mathbb{K})$.

La nå $\mathcal{C}$ være en annen ortonormal basis for V. Vis at

$$< S\,,\, T >' = \operatorname{tr}\left([S]_{\mathcal{C}}\,[T]_{\mathcal{C}}^{*}\right), \quad S, T \in \mathcal{L}(V).$$

(Fortsettes side 3.)

Oppgave 6

I denne oppgaven betrakter vi vektorrommet $V = M_{2\times 2}(\mathbb{K})$, der $\mathbb{K}$ betegner enten $\mathbb{R}$ eller $\mathbb{C}$.

Sett $E_{11} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $E_{21} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$, $E_{12} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, $E_{22} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$,

og la $\mathcal{B}$ være basisen for V gitt ved $\mathcal{B} = \{E_{11}, E_{21}, E_{12}, E_{22}\}$, ordnet i rekkefølgen som oppgitt her.

For hver $A \in V$ definerer vi en lineær avbildning $T_A \in \mathcal{L}(V)$ ved

$$T_A(A') = A\,A', \quad A' \in V.$$

a) Beregn matrisen $[T_A]_{\mathcal{B}}$ når $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in V$.

Vi betrakter nå V som et indreprodukt rom med hensyn på Frobenius indreproduktet. Som kjent er da $\mathcal{B}$ en ortonormal basis for V og vi kan derfor betrakte $\mathcal{L}(V)$ som et indreprodukt rom i henhold til oppgave 5 når vi utstyrer $\mathcal{L}(V)$ med indreproduktet $< \cdot, \cdot >'$.

b) Begrunn at $< T_A\,, T_B >' = 2 < A\,, B >$ når $A, B \in V$.

c) La W være underrommet av $\mathcal{L}(V)$ gitt ved $W = \{T_A \,|\, A \in V\}$. Angi dimensjonen til W og finn en ortonormal basis for W.

SLUTT