FASIT MAT 3000/4000 VÅREN 2010.

Oppgave 1.

a) $f = E_{\overline{27}}$ i $\mathbb{Z}/(55)$. Vi har $55 = 5 \cdot 11$, så $M = 4 \cdot 10 = 40$.

Da er $(27, M) = (27, 40) = 1$ og f er en bijeksjon

b) Vi har $f^{-1} = E_{\overline{27}^{-1}}$ der $\overline{27}^{-1}$ regnes ut i $\mathbb{Z}/(40)$

$$27x \equiv 1 \equiv 81 \pmod{40}$$

$$x \equiv 3 \pmod{40}$$

$f^{-1}(\bar{x}) = \bar{x}^3$. Regner nå i $\mathbb{Z}/(55)$:

$$\bar{b}_1 = f^{-1}(\bar{5}) = \bar{5}^3 = \overline{125} = \overline{15} \quad (= O)$$

$$\bar{b}_2 = f^{-1}(\overline{24}) = \overline{24}^3 = \overline{576} \cdot \overline{24} = \overline{26} \cdot \overline{24} = \overline{624} = \overline{19} \quad (= S)$$

$$\bar{b}_3 = f^{-1}(\overline{23}) = \overline{23}^3 = \overline{529} \cdot \overline{23} = \overline{34} \cdot \overline{23} = \overline{782} = \overline{12} \quad (= L)$$

$$\bar{b}_4 = \bar{b}_1 \ (= O)$$

Beskjeden er OSLO.

Oppgave 2

Vi bruker Eulers kriterium med $p = 73$.

$$\bar{3}^{\frac{p-1}{2}} = \bar{3}^{36}$$

$\bar{3}^2 = \bar{9}$

$\bar{3}^4 = \overline{81} = \bar{8}$

$\bar{3}^8 = \overline{64} = -\bar{9}$

Vi observerer av dette at $\bar{3}^6 = -\bar{1}$, så $\bar{3}^{36} = (\bar{3}^6)^6 = (-\bar{1})^6 = \bar{1}$.
Altså er $\bar{3}$ en kvadratisk rest.

$5490 = 2 \cdot 3^2 \cdot 5 \cdot 61$. Eneste primtallsfaktor som er $\equiv 3 \pmod 4$ er 3 og den forekommer i en like potens. Altså er 5490 en kvadratsum.

Oppgave 3. Vi ser lett at

$$AA^* = A^*A = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$$

altså er A normal og dermed unitært diagonaliserbar.

Egenverdier: $\det(A-\lambda I) = \det\begin{bmatrix} 1-\lambda & 1 \\ -1 & 1-\lambda \end{bmatrix} = (1-\lambda)^2+1 = 0$

$$(1-\lambda)^2 = -1 \quad , \quad 1-\lambda = \pm i \quad , \quad \lambda = 1 \pm i.$$

Egenvektorer: $\lambda = 1+i$

$$-iz_1 + z_2 = 0 \quad , \quad \begin{bmatrix} z_1 \\ z_2 \end{bmatrix} = t\begin{bmatrix} 1 \\ i \end{bmatrix}$$

$$\vec{v}_1 = \begin{bmatrix} 1 \\ i \end{bmatrix} \quad , \quad \vec{u}_1 = \frac{\vec{v}_1}{\|\vec{v}_1\|} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ i \end{bmatrix}$$

$\lambda = 1-i$

$$iz_1 + z_2 = 0 \quad , \quad \begin{bmatrix} z_1 \\ z_2 \end{bmatrix} = t\begin{bmatrix} i \\ 1 \end{bmatrix}$$

$$\vec{v}_2 = \begin{bmatrix} i \\ 1 \end{bmatrix} \quad , \quad \vec{u}_2 = \frac{\vec{v}_2}{\|\vec{v}_2\|} = \frac{1}{\sqrt{2}}\begin{bmatrix} i \\ 1 \end{bmatrix}$$

$$U = [\vec{u}_1 \; \vec{u}_2] = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}$$

Oppgave 4

a) $\langle T(v+w), v+w\rangle - i\langle T(iv+w), iv+w\rangle + (i-1)\langle Tv, v\rangle + (i-1)\langle Tw, w\rangle$

$= \cancel{\langle Tv, v\rangle} + \langle Tv, w\rangle + \langle Tw, v\rangle + \cancel{\langle Tw, w\rangle} - i\big(\langle T(iv), iv\rangle + \langle T(iv), w\rangle + \langle Tw, iv\rangle + \langle Tw, w$

$+ i\langle Tv, v\rangle - \cancel{\langle Tv, v\rangle} + i\langle Tw, w\rangle - \cancel{\langle Tw, w\rangle}$

$= \langle Tv, w\rangle + \langle Tw, v\rangle - i\big(\cancel{\langle Tv, v\rangle} + i\langle Tv, w\rangle - i\langle Tw, v\rangle + \cancel{\langle Tw, w\rangle}\big)$

$+ \cancel{i\langle Tv, v\rangle} + \cancel{i\langle Tw, w\rangle}$

$= \langle Tv, w\rangle + \langle Tw, v\rangle - i^2\langle Tv, w\rangle + i^2\langle Tw, v\rangle = 2\langle Tv, w\rangle.$

b) Alle uttrykkene på venstre side i 4a) er på formen $\langle Tv, v\rangle$. Altså er venstre side 0, dvs.

$$\langle Tv, w\rangle = 0 \quad \text{for alle } v, w \in V.$$

Men da må $Tv = \vec{0}$ (ellers, la bare $w = Tv$).

c) For alle $v \in V$ har vi da

$\langle TT^*v, v\rangle = \langle T^*v, T^*v\rangle = \|T^*v\|^2 = \|Tv\|^2 = \langle Tv, Tv\rangle$

$= \langle T^*Tv, v\rangle$. Altså er $\langle TT^*v, v\rangle = \langle T^*Tv, v\rangle$

dvs.

$$\langle (TT^* - T^*T)v, v\rangle = 0 \quad \text{for alle } v \in V.$$

Men da er $TT^* - T^*T = 0$, dvs. $TT^* = T^*T$ og T er normal.

Oppgave 5

a) $\phi : W_1 \times W_2 \to V$ definert ved $\phi(w_1, w_2) = w_1 - w_2$

er lineær, $N(\phi) = \{(w_1, w_2) \mid w_1 = w_2\}$

$$= \{(w, w) \in W_1 \times W_2 \mid w \in W_1 \cap W_2\} \cong W_1 \cap W_2$$

(isomorf). Dimensjonsteoremet gir

$$m_1 + m_2 = \dim(W_1 \times W_2) = \dim N(\phi) + \dim R(\phi)$$

$$= \dim(W_1 \cap W_2) + \dim R(\phi) \leq \dim(W_1 \cap W_2) + n$$

$$\Rightarrow \dim(W_1 \cap W_2) \geq m_1 + m_2 - n.$$

b). Velg $v_1 \neq 0$ i V_1 og anta at vi induktivt har funnet $v_j \in V_j$ slik at $\{v_1, \dots, v_j\}$ er en ortogonal basis for V_j for $j = 1, \dots, k$. $(k < n)$

Da er $\dim V_k^\perp = n - k$, siden $V = V_k \oplus V_k^\perp$ og dermed er

$$\dim(V_{k+1} \cap V_k^\perp) \geq (k+1) + (n-k) - n = 1$$

altså kan vi finne $v_{k+1} \in V_{k+1} \cap V_k^\perp$, $v_{k+1} \neq 0$.

Da er $\{v_1, \dots, v_{k+1}\}$ ortogonal og derfor lineært uavhengig, dvs en basis for V_{k+1}. La $\mathcal{B} = \{v_1, \dots, v_n\}$. $\mathcal{B}$ er ortogonal basis for $V = V_n$ og siden $T(v_k) \in V_k$, er $T(v_k)$ en lineær kombinasjon av $\{v_1, \dots, v_k\}$, altså er $[T]_{\mathcal{B}}$ øvre triangulær.

Oppgave 6 Kan anta $n > 2$ siden $n = 2$ er et primtall. Da er $\bar{a} \cdot \bar{a}^{n-1} = \bar{1}$, dvs. $\bar{a}$ har invers i $\mathbb{Z}/(n)$ og vi kan ta alle heltallige potenser $\bar{a}^m$, $m \in \mathbb{Z}$. De er også forskjellige fra $\bar{0}$, siden $\bar{a}^m \cdot \bar{a}^{-m} = \bar{1}$.

Påstår at $\bar{a}, \bar{a}^2, \dots, \bar{a}^{n-1} \in \mathbb{Z}/(n)^* = \mathbb{Z}/(n) \setminus \{\bar{0}\}$ alle er forskjellige, for hvis $\bar{a}^k = \bar{a}^l$ med $1 \leq k < l \leq n-1$ og $m = l - k$, så er $0 < m < n-1$ og $\bar{a}^m = \bar{1}$.

Men $\mathbb{Z}/(n)^*$ består av $n-1$ restklasser, som altså er $\bar{a}, \dots, \bar{a}^{n-1}$. Dette betyr at alle restklasser i $\mathbb{Z}/(n)^*$ har en multiplikativ invers. n kan da ikke være sammensatt, $n = qr$ der $q, r > 1$, siden $\bar{q}$ og $\bar{r}$ da begge er nulldivisorer i $\mathbb{Z}/(n)$.