NTNU

Kunnskap for en bedre verden

Institutt for matematiske fag

Eksamensoppgave i
MA1202/MA6202 Lineær algebra med anvendelser

Faglig kontakt under eksamen: Kristian Gjøsteen

Tlf: 73 55 02 42

Eksamensdato: 31. mai 2019

Eksamenstid (fra–til): 09:00-13:00

Hjelpemiddelkode/Tillatte hjelpemidler: D: Ingen trykte eller håndskrevne hjelpemidler tillatt. Bestemt, enkel kalkulator tillatt.

Annen informasjon:

Målform/språk: bokmål

Antall sider: 4

Antall sider vedlegg: 0

Kontrollert av:

Informasjon om trykking av eksamensoppgave	
Originalen er:	
1-sidig ☐	**2-sidig** ☒
sort/hvit ☒	**farger** ☐
skal ha flervalgskjema ☐	

Dato Sign

Alle svar må begrunnes. Husk at du kan bruke resultater fra tidligere deloppgaver, selv om du ikke har klart å løse dem.

Oppgave 1 La

$$A = \begin{pmatrix} 1 & -6 & 9 \\ -1 & -2 & 6 \\ -1 & -1 & 4 \end{pmatrix} \qquad \beta_1 = \begin{pmatrix} -3 \\ -3 \\ -2 \end{pmatrix} \qquad \beta_2 = \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix} \qquad \beta_3 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

a) Vis at $\beta = \{\beta_1, \beta_2, \beta_3\}$ er en basis for $\mathbb{R}^3$.

b) La $L_A : \mathbb{R}^3 \to \mathbb{R}^3$ være gitt ved $L_A(x) = Ax$.

Finn $A_0 = [L_A]_\beta$. Forklar hvorfor A_0 er invertibel. Bruk dette til å forklare hvorfor matrisen A er invertibel.

c) La $F : \mathbb{R}^3 \to \mathbb{R}^4$ være en lineæravbildning. Vi får vite at

$$F(\beta_1) + 3F(\beta_2) - F(\beta_3) = 0.$$

Finnes det en lineæravbildning $G : \mathbb{R}^4 \to \mathbb{R}^3$ slik at $G \circ F$ er identiteten på $\mathbb{R}^3$?

Finnes det en lineæravbildning $G : \mathbb{R}^4 \to \mathbb{R}^3$ og et ikke-trivielt underrom U av $\mathbb{R}^3$ slik at $G \circ F$ er identiteten på U? Hvor høy dimensjon kan U ha?

Oppgave 2 La $V = P_2(\mathbb{R})$, dvs. polynomene av grad 2 eller mindre med reelle koeffisienter. Vi lar V ha den naturlige vektorromsstrukturen.

La $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{R}$ være gitt ved

$$\langle f(X), g(X) \rangle = \int_0^1 f(t)g(t)\mathrm{d}t.$$

a) Vis at $\langle \cdot, \cdot \rangle$ er et indreprodukt.

b) La $S = \{1, X, X^2\}$. Bruk Gram-Schmidt på S. Bruk svaret til å vise at S er en basis for V.

Oppgave 3 Gitt følgende data:

x	1	2	3	4
y	0.1	0.3	0.2	0.4

Bruk minste kvadraters metode til å finne en funksjon på formen $ax+b$ som «passer godt» til dataene.

Oppgave 4 La

$$M = \begin{pmatrix} 0.8 & 0 & 0.25 \\ 0.05 & 0.85 & 0.05 \\ 0.15 & 0.15 & 0.7 \end{pmatrix}.$$

a) Vis at $\lambda = 1$ er en egenverdi til matrisen. Finn en basis for egenrommet til $\lambda = 1$. Hva er $\lim_{n\to\infty} M^n$?

Datasystemer inneholder feil. Mange av disse feilene gjør ondsinnede angrep mot systemet mulig, dersom skurker får kunnskap om feilene.

Vi antar at det er tre muligheter for hvem som har kunnskap om disse feilene:

1. Ingen vet om noen feil. (Systemet er *trygt*.)
2. Skurker vet om en eller flere feil. (Systemet er *ekstremt sårbart*.)
3. Alle vet om en eller flere feil. (Systemet er *beskyttbart*.)

Hvis ingen vet om noen feil i én uke er det 5 % sannsynlighet for at skurkene finner en feil til neste uke. Det er 15 % sannsynlighet for at noen til neste uke finner en feil og offentliggjør den, uten at den blir rettet.

Når bare skurkene vet om feil i én uke er det 15 % sannsynlighet for at minst én feil blir alment kjent til uken etter.

Når en feil er alment kjent i én uke er det 25 % sannsynlighet for at alle kjente feil er rettet til uken etter (systemet er trygt). Det er 5 % sannsynlighet for at de alment kjente feilene er rettet, men at skurkene kjenner flere feil uken etter.

For et stort system er det rimelig å anta at det er så mange feil at det overstående holder i et lenger tidsrom, og vi kan dermed modellere dette som en Markovkjede.

b) Anta at systemet har vært lenge i drift. Gi et begrunnet anslag på hvor mange uker i gjennomsnitt du forventer at systemet er trygt i løpet av et år.

Oppgave 5 I denne oppgaven skal vi se på Lagrange-interpolasjon.

La $V = P_{t-1}(\mathbb{R})$. La S være en mengde med t distinkte reelle tall $x_1, x_2, \ldots, x_t$, ingen av dem 0. Definer

$$\phi_{i,S}(X) = \prod_{j=1, j\neq i}^{t} \frac{X - x_j}{x_i - x_j}.$$

a) Vis at for $x \in S$ har vi at

$$\phi_{i,S}(x) = \begin{cases} 1 & x = x_i, \\ 0 & x \in S \setminus \{x_i\}. \end{cases}$$

Vis at $\{\phi_{1,S}(X), \phi_{2,S}(X), \ldots, \phi_{t,S}(X)\}$ er en basis for V.

b) La g være et tall som ikke er 0 eller 1.

La $f(X) \in V$ og la tallene $y_1, y_2, \ldots, y_t$ være gitt ved $y_j = g^{f(x_j)}$ for $j = 1, 2, \ldots, t$.

Forklar hvordan du kan finne tall $\lambda_1, \lambda_2, \ldots, \lambda_t$ som er uavhengige av $f(X)$ slik at

$$\prod_{j=1}^{t} y_j^{\lambda_j} = g^{f(0)}.$$

Du kan bruke uten bevis at om $p(X)$ er et polynom av grad mindre enn t, og $p(X)$ har t nullpunkt, da er $p(X) = 0$.

Det følgende avsnittet er ikke relevant for å løse oppgaven, men beskriver kort en anvendelse av teorien i denne oppgaven. Teknikken som brukes her er veldig nyttig i kryptografi, der $f(0)$ kan være en hemmelig nøkkel, mens $f(x_j)$ er en «del» av den hemmelige nøkkelen. Lagrange-interpolasjon kan brukes til å rekonstruere den hemmelige nøkkelen fra delene. Formelen over gir et hint om hvordan vi kan bruke den hemmelige nøkkelen uten å avsløre delene.

Et **indreprodukt** $\langle \cdot, \cdot \rangle$ på et vektorrom V over en kropp $\mathbb{F}$ tilfredsstiller

1. $\langle v + w, z \rangle = \langle v, z \rangle + \langle w, z \rangle$ for alle $v, w, z \in V$;
2. $\langle av, z \rangle = a\langle v, z \rangle$ for alle $v, z \in V$ og $a \in \mathbb{F}$;
3. $\langle v, z \rangle = \overline{\langle z, v \rangle}$ for alle $v, z \in V$; og
4. $\langle v, v \rangle \geq 0$ for alle $v \in V$, med likhet hvis og bare hvis $v = 0$.