

74\*) Compute the Jordan Canonical form of the matrix

$$A = \begin{pmatrix} 26 & 6 & 0 & 3 & -3 \\ -23 & -4 & 3 & -3 & 3 \\ -8 & -2 & -7 & -1 & -2 \\ -122 & -30 & 24 & -13 & 25 \\ 24 & 6 & 27 & 3 & 8 \end{pmatrix}.$$

You are given the information that  $\chi_A(x) = (x-2)^5$ . (You do **not** need to calculate a basis or a transforming matrix.)

75\*) Show that the matrices  $A = \begin{pmatrix} 0 & 1 \\ -4 & 4 \end{pmatrix}$  and  $B = \begin{pmatrix} -3 & 25 \\ -1 & 7 \end{pmatrix}$  are similar and find a matrix  $S$  such that  $S^{-1} \cdot A \cdot S = B$ . You are given the information that  $\chi_A(x) = \chi_B(x) = (x-2)^2$ . **Hint:** Find the Jordan Canonical form of  $A$  and  $B$ , as well as matrices  $P, Q$  such that  $P^{-1}AP$  is the Jordan form of  $A$  and  $Q^{-1}BQ$  is the Jordan form of  $B$ . Then  $S = PQ^{-1}$  has the desired property.

76\*) We know that two matrices that are similar have the same characteristic polynomial. But What about the converse? Are two matrices that have the same characteristic polynomial always similar? Justify your answer by giving a proof (if true) or a counterexample (if wrong).

**Hint:** Consider the Jordan Form.

77\*) **Making and breaking the HDCP copy protection** HDCP (High-definition copy protection) is a system built into newer big-screen TVs and HD-DVD players to prevent display on unauthorized devices. The system works as follows: Every system is assigned (by a central authority) a private key  $\underline{s}$  and a public key  $\underline{t}$ . If two devices  $a$  and  $b$  are connected they exchange their public keys. Then each device calculates the inner product of its private key with the other device's public key. (I.e.  $a$  calculates the inner product  $\langle \underline{s}_a, \underline{t}_b \rangle$ .) For both devices this inner product will result in the same number which then is used as the shared encryption key.

a) Let  $V$  be a vector space,  $U \leq V$  and  $W = U^\perp$ . (In reality  $V$  is 56-dimensional and  $U$  is 40 dimensional.) For each device the central authority picks up three random vectors  $\underline{u} \in U$ ,  $\underline{w} \in U^\perp$  and  $\underline{v} \in V$ . It then assigns this device the secret key  $\underline{s} = \underline{u} + \underline{v}$  and the public key  $\underline{t} = \underline{w} + \underline{v}$ . Show that under this scheme we have for every pair  $a, b$  of devices that  $\langle \underline{s}_a, \underline{t}_b \rangle = \langle \underline{s}_b, \underline{t}_a \rangle$ .

b) Suppose that  $U$  is of dimension  $d$ . Show that knowledge of  $d$  public keys can (likely, assuming that the vectors  $\underline{w}$  for these are linearly independent) be used to break the system.

The problems are all bonus problems. Solutions should be handed in to the departmental secretaries to put in my mail box or can be handed in at the start of the final. Old homework and midterms that have not been picked up will be destroyed after mid-May.

---

I will be out of town from April 28 to May 7. The last lectures and a review will be given by a colleague of mine. There will be extra office hours on April 27 from 2pm-4pm. I will not have office hours after that. You may visit the office hours of Dr. Achter (who teaches another section of M369) on Wednesday, May 3, 10am-11am or Thursday, May 4, 2pm-3pm in WB216 (next door to my office).

---

## About the Final

The final will be comprehensive. The material is the lectures I have given with the exception of: Schur's theorem (transform matrix in upper triangular form), Computation of SVD (which is too calculation intensive), Computation of transforming matrices for the Jordan Form. (I.e. the material up to homework problem 73)

There will be 8 problems, each of similar level as the midterm problems. What I care most about is that you know **how** to solve problems, not so much that you can type in numbers in a calculator. You are welcome to use a calculator though all problems will be set up that they can be done by hand.

The final will be on Monday, May 5 from 1:30-3:30 in the usual class room.

You are permitted to bring **one hand-written** (by yourself) sheet with notes. (Letter size. If you want double sided. No photocopies, reduction, other people's handwriting.) This sheet must carry your name, but does not need to be handed in. It can contain whatever you want.

I will endeavor to post grades as soon as available on WebCT. You will be able to pick up your graded exams in the front office.

1) Let  $A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \end{pmatrix}$ . Determine bases for  $CS(A)$ ,  $RS(A)$  and  $N(A)$ .

2) Let  $A = \begin{pmatrix} 4 & 0 \\ 3 & 1 \end{pmatrix}$ .

Show that  $A$  can be diagonalized and find a matrix  $S$  such that  $S^{-1}AS$  is diagonal.

3) Determine the least-squares approximation by a linear function (i.e. a polynomial of the form  $a + bx$  for the following data set:

$$(0, 35), (1, 20), (2, 15), (3, 10)$$

4) a) Let  $V$  be a vector space with inner product  $\langle \cdot, \cdot \rangle$  and  $\underline{\mathbf{w}} \in V$  a particular vector. Show: The map  $L: V \rightarrow \mathbb{R}$  defined by setting  $L(\underline{\mathbf{v}}) = \langle \underline{\mathbf{w}}, \underline{\mathbf{v}} \rangle$  is linear.

b) Let  $V = \text{Span}(1, x, x^2)$  with inner product  $\langle \underline{\mathbf{f}}, \underline{\mathbf{g}} \rangle = \int_0^1 f(x)g(x) dx$  and  $\underline{\mathbf{w}} = 1 + x \in V$ . Determine  $\langle 1, \underline{\mathbf{w}} \rangle$ ,  $\langle x, \underline{\mathbf{w}} \rangle$  and  $\langle x^2, \underline{\mathbf{w}} \rangle$ .

c) For  $V$  and  $\underline{\mathbf{w}}$  as defined in b) define  $L: V \rightarrow \mathbb{R}$  by  $L(\underline{\mathbf{v}}) = \langle \underline{\mathbf{w}}, \underline{\mathbf{v}} \rangle$ . (By part a)  $L$  is linear.) Determine  ${}_S [L]_{\mathcal{B}}$ , where  $\mathcal{S} = (1)$  is the standard basis of  $\mathbb{R}$  and  $\mathcal{B} = (1, x, x^2)$ .

5) Let  $V$  be a vector space with inner product  $\langle \cdot, \cdot \rangle$  and  $\{\underline{\mathbf{u}}_1, \dots, \underline{\mathbf{u}}_k\}$  a set of  $k$  vectors such that  $\langle \underline{\mathbf{b}}_i, \underline{\mathbf{b}}_j \rangle = \delta_{i,j} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$ . Show, using the definition of linear independence, that the set  $\{\underline{\mathbf{u}}_1, \dots, \underline{\mathbf{u}}_k\}$  is linear independent.

6) Let  $V = \mathbb{R}^n$  with standard inner product  $\langle \underline{\mathbf{x}}, \underline{\mathbf{y}} \rangle = \underline{\mathbf{x}}^T \underline{\mathbf{y}}$  and let  $A \in \mathbb{R}^{n \times n}$  symmetric. Let  $\lambda \neq \mu$  be two different eigenvalues of  $A$ . Show that the eigenspaces of  $A$  for  $\lambda$  and  $\mu$  are mutually orthogonal, i.e. that any eigenvector for  $\lambda$  is orthogonal to any eigenvector for  $\mu$ . (Hint: Let  $\underline{\mathbf{x}}$  be an eigenvector for  $\lambda$  and  $\underline{\mathbf{y}}$  an eigenvector for  $\mu$  and show that  $\langle A\underline{\mathbf{x}}, \underline{\mathbf{y}} \rangle = \langle \underline{\mathbf{x}}, A\underline{\mathbf{y}} \rangle$ .) **(15 points)**

7) Let  $V$  be a vector space with inner product  $\langle \cdot, \cdot \rangle$  and  $U \leq V$ . Prove, that  $U^\perp \leq V$ . (You may want to use the definition that  $U^\perp = \{\underline{\mathbf{v}} \in V \mid \langle \underline{\mathbf{u}}, \underline{\mathbf{v}} \rangle = 0 \ \forall \underline{\mathbf{u}} \in U\}$ .)

8) Suppose that  $A, B, C \in \mathbb{F}^{n \times n}$  are matrices.

a) Show that  $\text{CS}(BC) \leq \text{CS}(B)$  and that  $\text{RS}(AB) \leq \text{RS}(B)$ .

b) Show that if  $C$  is invertible then  $\text{CS}(BC) = \text{CS}(B)$ . (Use that  $B = BC \cdot C^{-1}$  and a))

c) Show that  $\text{rank}(ABC) \leq \text{rank}(B)$  in general, and that  $\text{rank}(ABC) = \text{rank}(B)$  if  $A$  and  $C$  are invertible.

9) Determine the Jordan Canonical Form of the following matrices. (You do not need to determine the transforming matrix  $S$ .) Explain your reasoning.

$$A = \begin{pmatrix} 7 & 3 & 1 & -1 \\ 3 & 7 & 1 & -1 \\ 1 & 1 & 7 & -3 \\ -1 & -1 & -3 & 7 \end{pmatrix} \quad B = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 1 & 3 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}$$

$$\chi_A(x) = (x-12)(x-8)(x-4)^2 \quad \chi_B(x) = (x-2)^2(x-3)^2$$

**Note:** Avoid unnecessary work, think before calculating bases of eigenspaces!

10) Let  $\mathcal{B} = ((1, 1, -4)^T, (2, 2, 1)^T, (1, -1, 0)^T)$ .

a) Show that the vectors in  $\mathcal{B}$  are mutually orthogonal with respect to the standard inner product.

- b) Is  $\mathcal{B}$  a basis of  $\mathbb{R}^3$ ? (Hint: you can deduce this from a) without any new calculation)  
c) Compute the projection of  $\underline{\mathbf{v}} = (1, 1, 1)^T$  onto  $\text{Span}(\mathcal{B})$ .  
d) Compute the coefficient vector  $(\underline{\mathbf{v}})_{\mathcal{B}}$ .

**11)** Give an example of a matrix  $A$  with characteristic polynomial  $(x - 3)^2 \cdot (x + 5)^3$  such that both eigenvalues have geometric multiplicity one.

**12)** Let  $V = \text{Span}(1, x^2, x^3)$  with inner product  $\langle f, g \rangle = \int_0^1 f(t)g(t) dt$ . Compute an orthonormal basis of  $V$ .

**13)** Let

$$A = \begin{pmatrix} 1 & -18 & 0 \\ 0 & 4 & 0 \\ -8 & -13 & 9 \end{pmatrix}.$$

Find two (different) matrices  $R$ , such that  $R^2 = A$ .

**Hint:** Diagonalize  $A$

In addition, you might want to review the homework problems and the problems given as midterm samples over the semester.