Bitte beachten!

Füllen Sie bitte für jede Übung das beigefügte Deckblatt aus und heften Sie es an Ihre Aufgaben. Sie erleichtern uns damit unsere Listenführung und helfen mit, das Chaos, das wir am Ende des letzten Semesters mit den Punktelisten hatten, zu vermeiden.

Vielen Dank für Ihre Mitarbeit!

Sollte bei einer der ersten beiden Übungen das Deckblatt fehlen, gibt es nur die halbe Punktzahl, danach werden Übungen ohne ausgefülltes Deckblatt nicht mehr gewertet.

Mathematik für Informatiker II
Sommersemester 2001

Deckblatt zu Übung Nr.* _____

Name:* _____

Vorname:* _____

Matrikelnr.:*

Gruppe:*† _____

Bemerkung:*‡ _____

Erreichte Punkte:§

Aufgabe:						Summe	Korrektor
Punkte:							

*Bitte lesbar (in Druckschrift) ausfüllen!

†Bitte angeben: Tag, von-bis, Tutor; z. B. DI 09-11 Nelius

‡Hier z. B. Wechsel der Übungsgruppe angeben

§Wird vom Korrektor ausgefüllt

3. Übungsblatt

MATHEMATIK FÜR INFORMATIKER I (WS 2000/01)

Abgabe: Freitag, 11.5.2001 bis **11.00 Uhr !!!**

Abgabeort: s. Internet

Internet–Adresse der Vorlesung:

http://math–www.uni–paderborn.de/~chris/index10.html

Zur Information: **a)** Es soll wieder ein **Mail–Verteiler** für die einzelnen Übungsgruppen eingerichtet werden. Dazu muss sich jeder Teilnehmer anmelden. Also:

Mail an `majordomo@upb.de` mit dem Inhalt:

`subscribe mathe2u#` (Hierbei ist # wieder die Nr. der Übungsgruppe)

`end`

Es wird dann automatisch die email–Addresse eingetragen, von der die Anmeldung abgeschickt wurde.

b) Neue Übungsgruppe Nr. 22 : Di., 11–13 Uhr, N3.229 (Volker Winzenick). Wir wollen eine gleichmäßige Neuverteilung aller 3 Gruppen zu diesem Termin erreichen. Freiwillige aus den beiden Gruppen 7 (Nelius) und 20 (Mihailescu) können zunächst einmal am 8.5.2001 in diese neue Gruppe gehen.

---

12. Aufgabe: a) Die Abbildung $s : \mathrm{M}_n(K) \longrightarrow K$ sei definiert durch $s(A) := \sum_{i=1}^{n} a_{ii}$ für $A = (a_{ik})$, d.h. $s(A)$ ist die Summe der Hauptdiagonalelemente von A.

a) Beweise, daß s eine K–lineare Abbildung ist.

b) Bestimme die Dimension von Kern(s) (**Hinweis:** Benutze den Rangsatz). (4)

13. Aufgabe: Bestimme die Lösungsmenge des LGS's $Ax = b$ (über rr) in den folgenden Fällen mit Hilfe des Entzerrungsalgorithmus:

a) $A = \begin{pmatrix} 1 & 1 & 0 \\ 2 & 1 & -1 \\ 0 & 2 & 2 \\ 1 & 4 & 3 \end{pmatrix}$, $b = \begin{pmatrix} 0 \\ 1 \\ -2 \\ -3 \end{pmatrix}$ **b)** $A = \begin{pmatrix} -1 & 1 & 0 & 0 & 2 \\ -1 & 4 & 1 & -2 & 3 \\ 0 & 3 & 1 & -2 & 1 \\ 1 & -1 & 0 & 1 & 0 \end{pmatrix}$, $b = \begin{pmatrix} 1 \\ -3 \\ -4 \\ 3 \end{pmatrix}$ (5)

14. Aufgabe: U, V und W seien K–Vektorräume und $f : U \longrightarrow V$ und $g : V \longrightarrow W$ seien K–lineare Abbildungen. Beweise, daß die Hintereinanderausführung $g \circ f : U \longrightarrow W$ wieder eine K–lineare Abbildung ist. (3)

15. Aufgabe: Manchmal sollten Nachrichten geheim bleiben. Diese Geheimniskrämerei hat zur Folge, daß Nachrichten zum Senden kodiert und zum Lesen dekodiert werden. Sei $\mathcal{A}$ ein Alphabet, das zum Übertragen von den Nachrichten benutzt werden soll. Seien die Abbildung $f : \mathcal{A}^n \longrightarrow \mathcal{A}^n$ die Kodierung und die Abbildung $g : \mathcal{A}^n \longrightarrow \mathcal{A}^n$ die Dekodierung von Worten der Länge n in $\mathcal{A}$. Wenn f bijektiv ist, so läßt sich jede mit f kodierte Nachricht durch $g = f^{-1}$ dekodieren.

a) Wir betrachten nun ein spezielles Verfahren zur Kodierung von Nachrichten der Länge n. Dazu sei $\mathcal{A} = \mathbb{Z}_{29}$. Die Abbildung f sei durch $f(u) := A \cdot u$ für alle $u \in \mathbb{Z}_{29}^n$ und ein $A \in M_n(\mathbb{Z}_{29})$ gegeben. Welche Eigenschaft muß die Matrix A haben, damit f sich zum Kodieren eignet? (Hinweis: Aufgabe 11)

b) Wir ordnen nun den Buchstaben des lateinischen Alphabets $A, B, C, \ldots, Z$ die Elemente $0, 1, 2, \ldots, 25$ aus $\mathbb{Z}_{29}$ und Komma, Punkt und Leerzeichen die Elemente $26, 27, 28$ in der gegebenen Reihenfolge zu. Die Verschlüsselung erfolgt nun, indem wir zuerst die Buchstaben in die entsprechenden Elemente von $\mathbb{Z}_{29}$ umschreiben, die Botschaft in Blöcken zu 4 Elementen zerlegen, die Methode aus (a) mit der Matrix

$$A := \begin{pmatrix} 5 & 1 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & 6 & 1 \\ 0 & 0 & 0 & 6 \end{pmatrix} \in M_4(\mathbb{Z}_{29})$$

auf die Blöcke anwenden und danach die Elemente wieder in Buchstaben verwandeln.

i) Beschreibe die Dekodierung dieser Methode, dh. bestimme g.

ii) Entschlüssele die Nachricht

```
CAFNDLUXQNSR
```

(Hinweis: Beide Teile der Aufgabe können, was die Rechnung betrifft, in einem Schritt erledigt werden.) (6)

c*) (ohne Wertung) Benutze dieselbe Methode aus (b), um die mit der Matrix

$$A := \begin{pmatrix} 3 & 6 & 5 & 1 \\ 3 & 1 & 2 & 13 \\ 4 & 9 & 17 & 23 \\ 11 & 3 & 19 & 6 \end{pmatrix} \in M_4(\mathbb{Z}_{29})$$

verschlüsselte Botschaft

```
SMNLBUODM.H,SQCGPZTBTUPIOIHVY,NCBEHYEAAKPPG.QI YVISK
```

zu entschlüsseln. Es ist ein Zitat von Carl Friedrich Gauß.

(**Hinweis:** Verwende besser ein Computeralgebrasystem (Maple) für c*).

Deckblatt nicht vergessen!