TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Mathematik • Institut für Algebra • Prof. Baumann, Jun.-Prof. Schneider

Einführung in die Mathematik für Informatiker INF–110–2

Zweite Modulprüfung am 07.08.2019

<table>
<tr><td colspan="3">Name, Vorname</td><td colspan="4">Matrikelnummer, Studiengang</td><td>Unterschrift</td></tr>
<tr><td colspan="3">................................</td><td colspan="4">..</td><td>...........</td></tr>
<tr><td>A1 (20 P)</td><td>A2 (20 P)</td><td>A3 (20 P)</td><td>A4 (20 P)</td><td>A5 (20 P)</td><td>Z6 (10 P)</td><td>$\sum$ (110 P)</td><td rowspan="2"></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Beachten Sie bitte folgende Hinweise:

- Der Rechenweg ist lückenlos anzugeben, Antworten sind zu begründen.

- Für jede Aufgabe ist ein Extrablatt zu verwenden und mit dem Namen zu beschriften.

Wir wünschen Ihnen viel Erfolg!

1. Durch $f\colon \mathbb{R}^4 \to \mathbb{R}^3, x \mapsto Ax$ mit $A := \begin{pmatrix} 1 & 0 & -3 & 0 \\ 0 & 2 & 0 & -2 \\ 1 & 2 & -1 & 0 \end{pmatrix}$ ist eine lineare Abbildung über $\mathbb{R}$ gegeben.

   (a) Berechnen Sie $\dim(\mathrm{Ker}(A))$ und $\dim(\mathrm{Im}(f))$.

   (b) Bestimmen Sie die Darstellungsmatrix A_{BC} bezüglich der (geordneten) Basen

   $$B = \left(\begin{pmatrix} 1\\1\\1\\1 \end{pmatrix}, \begin{pmatrix} 0\\1\\1\\1 \end{pmatrix}, \begin{pmatrix} 0\\0\\1\\1 \end{pmatrix}, \begin{pmatrix} 0\\0\\0\\1 \end{pmatrix} \right) \text{ und } C = \left(\begin{pmatrix} 1\\1\\1 \end{pmatrix}, \begin{pmatrix} 0\\1\\1 \end{pmatrix}, \begin{pmatrix} 0\\0\\1 \end{pmatrix} \right) \text{ des } \mathbb{R}^4 \text{ bzw. } \mathbb{R}^3.$$

   (c) Berechnen Sie unter Benutzung der Darstellungsmatrix A_{BC} das Bild des Vektors v mit Koordinatenvektor $V_B := (1,\ 0,\ 0,\ -1)^T$.

2. Es sei $a \in \mathbb{R}$ und $A := \begin{pmatrix} 3 & 1 & 1 \\ 4 & 0 & 1 \\ 4a & a & a-1 \end{pmatrix} \in \mathbb{R}^{3\times 3}$.

   (a) Zeigen Sie, dass $v := (1, 1, a)^T$ ein Eigenvektor der Matrix A ist. Geben Sie den zugehörigen Eigenwert an.

   (b) Berechnen Sie eine Basis des Eigenraums $\mathrm{Eig}_{-1}(A)$ von A zum Eigenwert -1, und geben Sie die Dimension von $\mathrm{Eig}_{-1}(A)$ an.

   (c) Berechnen Sie die Dimension und eine Basis des Orthogonalraums zu $\mathrm{Eig}_{-1}(A)$ (bezüglich des Standard-Skalarprodukts im $\mathbb{R}^3$).

   (d) Ergänzen Sie die Basis des Eigenraums $\mathrm{Eig}_{-1}(A)$ zu einer Basis des $\mathbb{R}^3$.

3. (a) Betrachtet wird für ein festes $m \in \mathbb{N}$, $m > 0$, die Abbildung

$$f_m \colon \mathbb{Z}_m \to \mathbb{Z}_m, \quad a \mapsto a^2 + 1 \pmod{m},$$

Untersuchen Sie, ob die Abbildungen f_5 und f_7 injektiv, surjektiv, oder gar bijektiv sind. Begründen Sie Ihre Entscheidungen!

(b) Gegeben sind die Relationen auf der Menge $\{0, 1, 2, 3, 4\}$:

$$R_1 := \big\{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2),(2,2),(3,3),(4,4)\big\},$$
$$R_2 := \big\{(0,0),(0,1),(0,2),(0,4),(1,1),(1,2),(1,4),(2,2),(4,4)\big\}.$$

(i) Geben Sie an, welche der Eigenschaften *reflexiv*, *symmetrisch*, *antisymmetrisch*, *transitiv* die Relationen R_1 bzw. R_2 besitzen.

(ii) Ist eine der Relationen eine Äquivalenzrelation? Falls ja, geben Sie die Äquivalenzklassen an.

(iii) Lässt sich eine der Relationen zu einer Ordnungsrelation erweitern? Falls ja, zeichnen Sie ein Ordnungsdiagramm der kleinsten solchen Ordnungserweiterung und bestimmen Sie die Ordnungsdimension.

4. Betrachtet wird das RSA-Kryptosystem mit dem öffentlichen Schlüssel $(n, e) := (65, 11)$.

(a) Begründen Sie, dass der angegebene Schlüssel tatsächlich ein RSA-Schlüssel ist.

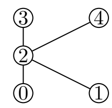
(b) Verschlüsseln Sie die Zahl $m := 2$ mittels des angegebenen Schlüssels.

(c) Berechnen Sie den geheimen Schlüssel (n, d).

(d) Führen Sie eine Probe durch, indem Sie die in (b) erhaltene Nachricht mit dem in (c) gefundenen geheimen Schlüssel entschlüsseln.

5. (a) Welcher Baum besitzt den Prüfer-Code $(1, 1, 0, 2, 2)$?

Bestimmen Sie den Prüfer-Code des nebenstehenden Baumes.



(b) Für eine natürliche Zahl $n > 1$ sei $[n] := \{1, 2, \ldots, n\}$. Betrachtet wird der Graph $G_n := (V_n, E_n)$ mit

$$V_n := \big\{A \subseteq [n] \mid |A| \in \{1, n-1\}\big\},$$
$$E_n := \big\{\{A, B\} \mid A, B \in V_n, A \neq B, A \subseteq B\big\}.$$

(i) Zeichnen Sie für die Graphen G_3 und G_4 jeweils ein Graphendiagramm.

(ii) Berechnen Sie die Anzahl der Knoten des Graphen G_n.

(iii) Begründen Sie, dass der Graph G_n regulär vom Grad $n - 1$ ist, und berechnen Sie die Anzahl der Kanten von G_n.

(iv) Zeigen Sie, dass der Graph G_n für alle $n > 1$ bipartit ist.

Zusatz 6. (a) Betrachtet werden zwei Gruppen $(G, \circ)$ und $(H, \bullet)$, deren neutrale Elemente mit e_G bzw. e_H bezeichnet werden, sowie ein Gruppenhomomorphismus $f \colon G \to H$. Zeigen Sie, dass der Kern von f, definiert durch $\mathrm{Ker}(f) = \{g \in G \mid f(g) = e_H\}$, eine Untergruppe von $(G, \circ)$ bildet.

(b) Im $\mathbb{R}^n$ mit dem Standard-Skalarprodukt sei eine Matrix $A \in \mathbb{R}^{n \times n}$ mit $A^T = A$ gegeben. Beweisen Sie: $\forall v, w \in \mathbb{R}^n : \quad Av_1 \bullet v_2 = v_1 \bullet Av_2$.