Mathematik für Informatiker II

Prof. Dr. Benjamin Doerr
MPI für Informatik

M.Sc. Kai Hagenburg
MIA Group

Sommersemester 2010
Universität des Saarlandes

Hausübung Blatt 5
Ausgabe: 14. Mai 2010 **Abgabe:** 21. Mai 2010 vor der Vorlesung

Aufgabe 1 (1+2+3=6 Punkte)

Beweisen Sie folgende Aussagen aus Satz 34.5:

a) Die lineare Abbildung $f : U \to V$ ist genau dann injektiv, wenn Ker $(f) = \{0\}$ ist.

b) Ist $f : U \to V$ linear, so ist Ker (f) ein Unterraum von U und Im (f) ein Unterraum von V.

c) Seien U, V K-Vektorräume und $f : U \to V$ lineare Abbildung. Dann gilt

$$\dim U = \dim \text{Ker}\,(f) + \dim \text{Im}\,(f).$$

Aufgabe 2 (6 Punkte)

Beweisen Sie folgende Behauptung: Ein System $S = \{v_1, \ldots, v_r\}$ ist linear unabhängig genau dann, wenn für alle $k = 1, \ldots, r$ gilt:

$$v_k \notin \text{span}(v_1, \ldots, v_{k-1})$$

(dabei ist $\text{span}(\emptyset) = \{0\}$)?

Aufgabe 3 (3+3=6 Punkte)

a) Der Vektor $v \in \mathbb{R}^3$ habe bezüglich der Standardbasis die Koordinaten $x = (3, 5, 8)$. Bestimmen Sie den Koordinatenvektor $\eta \in \mathbb{R}^3$ von v bezüglich der Basis

$$v_1 = \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix}, \qquad v_2 = \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}, \qquad v_3 = \begin{pmatrix} 3 \\ 1 \\ 1 \end{pmatrix}$$

b) Der Vektor $w \in \mathbb{C}^3$ habe bezüglich der Standardbasis die Koordinaten $z = (2, 1 + 2\mathrm{i}, 2 - \mathrm{i})$. Bestimmen Sie den Koordinatenvektor $\varphi \in \mathbb{C}^3$ von w bezüglich der Basis

$$w_1 = \begin{pmatrix} 1 \\ 0 \\ \mathrm{i} \end{pmatrix}, \qquad w_2 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \qquad w_3 = \begin{pmatrix} 1 \\ \mathrm{i} \\ 1 \end{pmatrix}$$

Aufgabe 4 (6 Punkte)

Ein einfaches Verfahren zur Erzeugung von Pseudozufallszahlenfolgen ist die Verwendung von sogenannten linear rückgekoppelten Schieberegistern (linear feedback shift register - LFSR), die u.a. für einige kryptografische Verfahren eingesetzt werden. Hierbei wird eine beliebige Folge als initialen Wert genommen (normalerweise geheim) und die Resultate des Schieberegisters werden dann als Zufallszahlen verwendet. In dieser Aufgabe behandeln wir die mathematischen Eigenschaften eines solchen Registers.

Sei $\mathbb{K}$ ein Körper und $V = W = \mathbb{K}^n$. Seien $c_1, \ldots, c_n \in \mathbb{K}$ fest gewählte Koordinaten. Wir betrachten die Abbildung $f : \mathbb{K} \to \mathbb{K}$, gegeben durch

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{n-1} \\ x_n \end{pmatrix} \mapsto f\left(\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{n-1} \\ x_n \end{pmatrix}\right) = \begin{pmatrix} x_2 \\ x_3 \\ \vdots \\ x_n \\ c_1x_1 + c_2x_2 + \ldots + c_nx_n \end{pmatrix}.$$

Offenbar ist f linear. Zeigen Sie: f ist genau dann bijektiv, wenn $c_1 \neq 0$ ist. Welche Folgen hat dies für kryptografische Verfahren?