

Lineare Algebra für Informatiker und Statistiker

Aufgabe 21 (4 Punkte)

Gegeben seien die reellen Matrizen

$$A_1 := \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & -1 \end{pmatrix}, \quad A_2 := \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \quad A_3 := \begin{pmatrix} -1 & 2 & 3 \end{pmatrix}.$$

Bestimmen Sie, so weit möglich, die Matrizenprodukte $A_i \cdot A_j$, $i, j = 1, 2, 3$.

Aufgabe 22 (4 Punkte)

Sei K ein Körper, $m, n, r, s \in \mathbb{N}$. Zeigen Sie:

- (a) Für $A \in K^{m \times n}$ und $B, C \in K^{n \times r}$ gilt

$$A \cdot (B + C) = A \cdot B + A \cdot C.$$

- (b) Für $A \in K^{m \times n}$, $B \in K^{n \times r}$ und $C \in K^{r \times s}$ gilt

$$(A \cdot B) \cdot C = A \cdot (B \cdot C).$$

Aufgabe 23 (4 Punkte)

- (a) Sei $(K, +, \cdot)$ ein Körper, (L, \oplus, \odot) eine Menge mit zwei Verknüpfungen und $\varphi : K \rightarrow L$ sei eine bijektive Abbildung mit den Eigenschaften

$$\varphi(a + b) = \varphi(a) \oplus \varphi(b) \quad (a, b \in K) \tag{1}$$

$$\varphi(a \cdot b) = \varphi(a) \odot \varphi(b) \quad (a, b \in K) \tag{2}$$

Zeigen Sie: L ist ein Körper.

Bemerkung: Sofern K und L Körper sind, heißt eine Abbildung $\varphi : K \rightarrow L$ Körperhomomorphismus, wenn sie (1), (2) und $\varphi(1) = 1$ erfüllt. Ein bijektiver Körperhomomorphismus wird als Körperisomorphismus bezeichnet. In diesem Fall nennt man K und L zueinander isomorphe Körper.

- (b) Zeigen Sie, dass $L := \left\{ \begin{pmatrix} x & -y \\ y & x \end{pmatrix} : x, y \in \mathbb{R} \right\}$ mit der Matrizenaddition

und -multiplikation ein zu \mathbb{C} isomorpher Körper ist.

Hinweis: Betrachten Sie die Abbildung $\varphi : \mathbb{C} \rightarrow L$, $x + iy \mapsto \begin{pmatrix} x & -y \\ y & x \end{pmatrix}$ (mit $x, y \in \mathbb{R}$).

- (c) Geben Sie das multiplikative Inverse zu $\begin{pmatrix} x & -y \\ y & x \end{pmatrix}$ für $(x, y) \in \mathbb{R}^2 \setminus \{0\}$ an.

Bitte wenden!

Aufgabe 24 (4 Punkte)

Die endlichen Körper $GF(2^k)$, $k \in \mathbb{N}$ können folgendermaßen konstruiert werden (ohne Beweis): Man nimmt $(\mathbb{Z}_2^k, +)$ als additive Gruppe und benutzt eine andere Multiplikation $*$ als die im Ring $(\mathbb{Z}_2^k, +, \cdot)$ sonst übliche. Unter dieser Multiplikation wird $(\mathbb{Z}_2^k \setminus \{0\}, *)$ zu einer zyklischen Gruppe mit dem neutralen Element $e = (\bar{0}, \dots, \bar{0}, \bar{1})$. Die Multiplikation kann so gewählt werden, dass $a := (\bar{0}, \dots, \bar{0}, \bar{1}, \bar{0})$ diese zyklische Gruppe erzeugt und $a^2 = (\bar{0}, \dots, \bar{0}, \bar{1}, \bar{0}, \bar{0}), \dots, a^{k-1} = (\bar{1}, \bar{0}, \dots, \bar{0})$ gilt. Eine weitere Eigenschaft ist, dass a^k sich als Summe (nicht notwendig aller) a^0, a^1, \dots, a^{k-1} schreiben lässt.

- (a) Im Körper $GF(2^3)$ gibt es eine Multiplikation $*$ mit der speziellen Eigenschaft $a^3 = a + e$. Benutzen Sie diese Eigenschaft und die obigen Informationen, um $a^0, a^1, \dots, a^7 \in \mathbb{Z}_2^3$ zu bestimmen.

- (b) Berechnen Sie $(\bar{1}, \bar{1}, \bar{0}) * (\bar{0}, \bar{1}, \bar{1})$ und $\frac{(\bar{1}, \bar{0}, \bar{0})}{(\bar{1}, \bar{1}, \bar{1})}$.

Bemerkung: In Anwendungen, z.B. der Fehlerkorrektur für CDs, DSL und DVB-T, kommt oft der endliche Körper $GF(2^8)$ mit der Multiplikation, die $a^8 = a^4 + a^3 + a^2 + e$ erfüllt, zum Einsatz.

Abgabe einzeln oder zu zweit: Dienstag, 2.12.2008 bis 12⁰⁰ Uhr,
Übungskasten vor der Bibliothek im 1. Stock