Lösungen:

16. **Permutationen** Es seien Permutationen σ, τ der Menge $\{1,2,3,4\}$ durch folgende Wertetabelle definiert:

n	1	2	3	4
$\sigma(n)$	4	3	2	1
$\tau(n)$	2	3	4	1

Man gebe in Zyklenschreibweise an: $\sigma, \tau, \sigma\tau, \tau\sigma, \sigma\sigma := \sigma^2, \tau\tau := \sigma^3$ und entsprechend die Potenzen $\sigma^3, \sigma^4, \tau^3, \tau^4$.

$\sigma = (14)(23), \tau = (1234), \sigma\tau = (13), \tau\sigma = (24)$

$\sigma^2 = (1), \sigma^3 = \sigma = (14)(23), \sigma^4 = (1)$

$\tau^2 = (13)(24), \tau^3 = (1432), \tau^4 = (1)$.

(Je 0.5 Punkte)

17. **Matrizenprodukt**

Für eine Matrix $A \in \mathbb{R}^{m\times n}$ sei ${}^tA \in \mathbb{R}^{n\times m}$ die an der Hauptdiagonalen gespiegelte Matrix, d.h., ist $A = (a_{ij})_{i=1,\ldots,m,\ j=1,\ldots,n}$, so ist ${}^tA = (\bar{a}_{ji})_{j=1,\ldots,n,\ i=1,\ldots,m}$ mit $\bar{a}_{ji} := a_{ij}$ für alle i, j.

Man zeige: Für $A \in \mathbb{R}^{l\times m}, B \in \mathbb{R}^{m\times n}$ gilt

$$ {}^t(AB) = {}^tB\ {}^tA $$

Beweis:

Seien $A = (a_{\lambda\mu})_{\lambda=1,\ldots,l,\mu=1,\ldots,m} \in \mathbb{R}^{l\times m}$, $B = (b_{\mu\nu})_{\mu=1,\ldots,m,\nu=1,\ldots,n} \in \mathbb{R}^{m\times n}$.

Dann $AB = (c_{\lambda\nu})_{\lambda=1,\ldots,l,\nu=1,\ldots,n} \in \mathbb{R}^{l\times n}$ mit $c_{\lambda\nu} = \sum_\mu a_{\lambda\mu}b_{\mu\nu}$.

${}^tB = (\bar{b}_{\nu\mu})_{\nu=1,\ldots,n,\mu=1,\ldots,m} \in \mathbb{R}^{n\times m}$ mit $\bar{b}_{\nu\mu} = b_{\mu\nu}$,

${}^tA = (\bar{a}_{\mu\lambda})_{\mu=1,\ldots,m,\lambda=1,\ldots,l} \in \mathbb{R}^{m\times l}$ mit $\bar{a}_{\mu\lambda} = a_{\lambda\mu}$,

${}^t(AB) = (\bar{c}_{\nu\lambda})_{\nu=1,\ldots,n,\lambda=1,\ldots,l} \in \mathbb{R}^{n\times l}$ mit $\bar{c}_{\nu\lambda} = c_{\lambda\nu} = \sum_\mu a_{\lambda\mu}b_{\mu\nu}$ für alle ν, λ.

${}^tB\ {}^tA = (d_{\nu\lambda})_{\nu=1,\ldots,n,\lambda=1,\ldots,l} \in \mathbb{R}^{n\times l}$ mit $d_{\nu\lambda} = \sum_\mu \bar{b}_{\nu\mu}\bar{a}_{\mu\lambda} = \sum_\mu b_{\mu\nu}a_{\lambda\mu} = \sum_\mu a_{\lambda\mu}b_{\mu\nu} = c_{\lambda\nu} = \bar{c}_{\nu\lambda}$ für alle ν, λ.

18. **Ringe**

Sei R ein Ring mit den neutralen Elementen 0 und 1. Man zeige für Elemente $a, b \in R$:

(a) $0a = a0 = 0$

$0 = 0 + 0 \Longrightarrow 0a = 0a + 0a$.

Addition des Elements $-(0a)$ liefert $0 = 0a - 0a = (0a + 0a) - 0a = 0a + (0a - 0a) = 0a + 0 = 0a$.

Ebenso wird gezeigt: $a0 = 0$.

(b) $-(ab) = (-a)b = a(-b)$

Zu zeigen ist: $ab + (-a)b = 0$ und $ab + a(-b) = 0$

Beweis: $ab + (-a)b = (a + (-a))b = 0b = 0$. Andere Aussage entsprechend.

(c) $(-a)(-b) = ab$
Beweis: $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$

(d) $-a = (-1)a$
Beweis: Zu zeigen ist: $a + (-1)a = 0$.
$a + (-1)a = (1 + (-1))a = 0a = 0$

(e) $0 = 1 \Longrightarrow R = \{0\}$
Beweis: Sei $a \in R$. Dann $a = 1a = 0a = 0$.

19. Endliche Körper

Für kleine natürliche Zahlen a, b kann an sich einfach von folgender Tatsache überzeugen: Sind a und b teilerfremd, so gibt es ganze Zahlen r, s mit $ra + sb = 1$. (Dies ist allgemein, also nicht nur für kleine Zahlen, richtig und kann mit Hilfe des Euklidischen Algorithmus bewiesen werden). Man zeige:

(a) Ist p eine Primzahl a eine natürliche Zahl mit $0 < a < p$, so gibt es
$x \in \{1, \ldots, p-1\}$ mit $a \odot x = 1$.
Dabei sei $\odot : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$ die Multiplikation in $\mathbb{Z}_p$, d.h. $a \odot x$ ist die eindeutig bestimmte Zahl in $\{0, \ldots, p-1\}$, die sich von ax um ein Vielfaches von p unterscheidet (also der Rest bei Division von ax durch p).

Da p prim ist, gibt es ganze Zahlen r, s mit $ra + sp = 1$.
Wähle $x \in \{1, \ldots, p-1\}$, das sich von r um ein Vielfaches von p unterscheidet, d.h. $x = r - qp$ it $g \in \mathbb{Q}$; x ist also der bei der Division von r durch p auftauchende Rest. Dann gilt:
$1 = ra + sp = xa + qpa + sp = xa + (qa + s)p$
xa unterscheidet sich demnach von 1 u ein ganzzahliges Vielfaches von p, d.h. $a \odot x = x \odot a = 1$.

(b) Für eine natürliche Zahl $m \geq 2$ gilt: Genau dann ist $\mathbb{Z}_m$ ein Körper, wenn m prim ist.

(c) Ist m prim, so hat nach der vorherigen Teilaufgabe jedes von 0 verschiedene Element von $\mathbb{Z}_m$ ein multiplikatives Inverses. Daher ist in diesem Fall $\mathbb{Z}_m$ ein Körper.
Ist m nicht prim, gibt es $a, b \in \{1, \ldots, p-1\}$ mit $ab = p$, d.h. $a \odot b = 0$. a und b können daher keine inversen Elemente besitzen. Denn wäre etwa $\bar{b}$ invers zu b so würde folgen: $0 = 0\bar{b} = ab\bar{a} = a$, im Widerspruch zu $a \in \{1, \ldots, p-1\}$.