Anhang: Lösungen zu ausgewählten Aufgaben

1.1.1 a) Ist $n = ab$ mit $a > 1$ und $b > 1$, so ist
$2^n - 1 = (2^a - 1)(1 + 2^a + \ldots + 2^{(b-1)a})$ eine echte Zerlegung.
b) Ist $n = pm$ mit ungerader Primzahl p, so gilt
$2^n + 1 = 1 - (-2^m)^p = (1 + 2^m)(1 + (-2^m) + \ldots + (-2^m)^{p-1})$.

1.3.3 a) Nach Aufgabe 1.3.2 gilt
$\sum_{j=0}^{m} j\binom{m}{j} = \sum_{j=1}^{m} m\binom{m-1}{j-1} = m(1+1)^{m-1} = m2^{m-1}$.
b) Es gibt $\binom{m}{j}$ Teilmengen K von M mit $|K| = j$. Jede enthält j Elemente. Also gilt $|\{(a, K) \mid a \in K \subseteq M, |K| = j\}| = \sum_{j=0}^{m} j\binom{m}{j}$. Andererseits gibt es m Elemente $a \in M$. Jede Menge K mit $a \in K \subseteq M$ wird eindeutig festgelegt durch $K \cap (M \setminus \{a\})$. Dies liefert 2^{m-1} Möglichkeiten für $K \cap (M \setminus \{a\})$.

2.1.3 a) Wegen $(ab)^2 = 1$ gilt $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$.
b) Sei $1 \neq g \in G$. Nach 2.1.10 ist $1 < |\langle g\rangle| \mid |G|$. Da $|G|$ eine Primzahl ist, folgt $\langle g\rangle = G$.
c) Für $|G| = 2, 3$ folgt aus b), daß G zyklisch ist. Sei $|G| = 4$. Gibt es ein $g \in G$ mit $\operatorname{Ord} g > 2$, so folgt mit 2.1.10 sofort $\langle g\rangle = G$. Anderenfalls gilt $g^2 = 1$ für alle $g \in G$. Somit ist G nach a) abelsch.

2.1.5 a) Ist U_1U_2 eine Untergruppe von G, so folgt für $u_j \in U_j$ $(j = 1, 2)$, daß $u_2^{-1}u_1^{-1} = (u_1u_2)^{-1} \in U_1U_2$, also $U_2U_1 = U_1U_2$. Sei nun $U_1U_2 = U_2U_1$. Sei $u_1, v_1 \in U_1$ und $u_2, v_2 \in U_2$. Dann gilt $u_2v_1 = v_1'u_2'$ mit $v_1' \in U_1, u_2' \in U_2$. Also ist $(u_1u_2)(v_1v_2) = u_1v_1'u_2'v_2 \in U_1U_2$. Für $u_j \in U_j$ $(j = 1, 2)$ gilt ferner $(u_1u_2)^{-1} = u_2^{-1}u_1^{-1} \in U_2U_1 = U_1U_2$. Dies zeigt, daß U_1U_2 eine Untergruppe von G ist.
b) Offenbar gilt $U_1U_2 = \cup_{g\in U_1} gU_2$. Ist $g_1U_2 = g_2U_2$ mit $g_j \in U_1$, so folgt $g_2^{-1}g_1 \in U_1 \cap U_2$. Ist $U_1 = \cup_j g_j(\mathrm{U}_1 \cap U_2)$ (disjunkt), so folgt $U_1U_2 = \cup_j g_jU_2$ (disjunkt). Daher ist $|U_1U_2| = |U_1 : U_1 \cap U_2||U_2| = |U_1||U_2|/|U_1 \cap U_2|$.
c) Sei $U_1 = \cup_{j\in J} g_j(U_1 \cap U_2)$ die Nebenklassenzerlegung von U_1 nach $U_1 \cap U_2$. Dann ist $U_1U_2 = \cup_{j\in J} g_jU_2$ disjunkt, daher $|J| \leq |G : U_2|$. Dies zeigt, daß $|U_1 : U_1 \cap U_2| \leq |G : U_2|$ und daher $|G : U_1 \cap U_2| = |G : U_1||U_1 : U_1 \cap U_2| \leq |G : U_1||G : U_2|$.
d) Ist G endlich und $G = U_1U_2$, so folgt mit b), dass $|G : U_1||G : U_2| = |G|^2/(|U_1||U_2|) = |G|/|U_1 \cap U_2| = |G : U_1 \cap U_2|$. Ist umgekehrt $|G|/|U_1 \cap U_2| = |G : U_1 \cap U_2| = |G : U_1||G : U_2| = |G|^2/(|U_1||U_2|)$, so folgt $|U_1U_2| = |U_1||U_2|/|U_1 \cap U_2| = |G|$, somit $G = U_1U_2$.

e) Wegen $|G:U_j| \mid |G:U_1\cap U_2|$ und der Teilerfremdheit von $|G:U_1|$ und $|G:U_2|$ folgt $|G:U_1||G:U_2| \mid |G:U_1\cap U_2|$. Andererseits gilt nach c), daß $|G:U_1\cap U_2| \le |G:U_1||G:U_2|$, also $|G:U_1\cap U_2| = |G:U_1||G:U_2|$.

2.2.2 Wegen $2 \mid n-1$ gilt $a^2 \equiv 1 \pmod 3$ für $3 \nmid a$, also $a^{n-1} \equiv 1 \pmod 3$. Wegen $n-1 \equiv 0 \pmod{10}$ und $a^{10} \equiv 1 \pmod{11}$ für $11 \nmid a$ folgt $a^{n-1} \equiv 1 \pmod{11}$. Ferner folgt aus $n-1 \equiv 0 \pmod{16}$ auch $a^{n-1} \equiv 1 \pmod{17}$ für $17 \nmid a$. Insgesamt ist $a^{n-1} \equiv 1 \pmod{3\cdot 11\cdot 17}$ für $\mathrm{ggT}(a, 3\cdot 11\cdot 17)$.

2.4.1 a) Es gilt
$2^n + (1+i)^n + (1-i)^n = \sum_{j=0}^n \binom{n}{j} + \sum_{j=0}^n \binom{n}{j}(-1)^j + \sum_{j=0}^n \binom{n}{j}(i^j + (-i)^j)$.
Für $2 \nmid j$ ist $i^j + (-i)^j = 0$. Für $j = 2k$ ist $i^j + (-i)^j = 2(-1)^k$. Somit bleibt $2^n + (1+i)^n + (1-i)^n = 4\sum_{4|j} \binom{n}{j}$.
Es gilt $1 \pm i = \sqrt{2}(\cos \pi/4 \pm i \sin \pi/4)$. Daher ist $(1+i)^n + (1-i)^n = 2(\sqrt{2})^n \cos(n\pi/4)$.
b) Die Behauptungen folgen aus

$$\cos(n\pi/4) = \begin{cases} 1 & \text{falls } n \equiv 0 \pmod 8 \\ 1/\sqrt{2} & \text{falls } n \equiv 1, 7 \pmod 8 \\ 0 & \text{falls } n \equiv 2, 6 \pmod 8 \\ -1/\sqrt{2} & \text{falls } n \equiv 3, 5 \pmod 8 \\ -1 & \text{falls } n \equiv 4 \pmod 8. \end{cases}$$

2.5.2 a) Ist $a = a^{-1}$, also $a^2 = 1$, so folgt $a = 1, -1$. Also ist $K^* = \{1, -1, a, a^{-1}, b, b^{-1}, \ldots\}$ und daher $\prod_{a\in K^*} = -1$.
b) Dies ist die Aussage in a), angewandt auf $K = \mathbb{Z}/p\mathbb{Z}$.
c) Wegen $(p+j)/2 \equiv -(p-j)/2 \pmod p$ folgt
$-1 \equiv (p-1)! \equiv (-1)^{(p-1)/2} (\frac{p-1}{2}!)^2 \pmod p$.

2.7.1 Sei $a + b\sqrt{p} + c\sqrt{q} = 0$ mit $a, b, c \in \mathbb{Q}$, nicht alle gleich 0. Wir können $a, b, c \in \mathbb{Z}$ annehmen. Dann ist $a^2 + 2ab\sqrt{p} + b^2 p = (a + b\sqrt{p})^2 = c^2 q$. Wegen $\sqrt{p} \notin \mathbb{Q}$ ist $ab = 0$. Ist $b = 0$, so ist $a^2 = c^2 q$, ein Widerspruch zu $\sqrt{q} \notin \mathbb{Q}$. Also ist $a = 0$, somit $b^2 p = c^2 q$. Wegen der eindeutigen Primfaktorzerlegung in $\mathbb{Z}$ geht dies nicht.

2.7.5 a) Aus $\dim V \ge \dim(U+W) = \dim U + \dim W - \dim(U\cap W)$ folgt $\dim(U\cap W) \ge \dim W + \dim U - \dim V = \dim W - 1$.
b) folgt aus a) durch Induktion nach k.
c) Sei $[w_1, \ldots, w_k]$ eine Basis von W und $[w_1, \ldots, w_k, v_1, \ldots, v_{n-k}]$ eine Basis von V. Wir setzen $U_j = \langle w_1, \ldots, w_k, v_1, \ldots, v_{j-1}, v_{j+1}, \ldots, v_{n-k}\rangle$. Dann ist offenbar $\dim U_j = n-1$ und $W = \cap_{j=1}^{n-k} U_j$.

2.7.6 a) Wegen $(U_1+U_2)+U_3 \geq U_1\cap U_3+U_2\cap U_3$ gilt
$\dim(U_1+U_2+U_3)=\dim(U_1+U_2)+\dim U_3-\dim((U_1+U_2)\cap U_3$
$\leq \dim U_1+\dim U_2-\dim U_1\cap U_2+\dim U_3-\dim(U_1\cap U_3+U_2\cap U_3)$
$=\dim U_1+\dim U_2+\dim U_3-\dim U_1\cap U_2-\dim U_1\cap U_3-\dim U_2\cap U_3+$
$\dim U_1\cap U_2\cap U_3$. Gleichheit gilt genau dann, wenn
$(U_1+U_2)\cap U_3=U_1\cap U_3+U_2\cap U_3$. Gilt die Gleichheit, so muß wegen $U_1+U_2+U_3=U_2+(U_1+U_3)=U_1+(U_2+U_3)$ auch $(U_1+U_3)\cap U_2=U_1\cap U_2+U_2\cap U_3$ und $(U_2+U_3)\cap U_1=U_1\cap U_2+U_1\cap U_3$ gelten.
b) Sei $U_j=\{(x_1,x_2,x_3)\mid x_j=0\}$ für $j=1,2,3$ und
$U_4=\{(x_1,x_2,x_3)\mid \sum_{j=1}^3 x_j=0\}$. Dann ist $\dim U_j=2$ und $V=\sum_{j=1}^4 U_j$. Offenbar gilt $\dim(U_i\cap U_j)=1$ für $i,j=1,2,3$. Ferner ist $U_1\cap U_4=\{(0,x_2,x_3)\mid x_2+x_3=0\}$, also $\dim(U_1\cap U_4)=1$. Man bestätigt leicht, daß $U_i\cap U_j\cap U_k=0$ für $1\leq i<j<k\leq 4$. Nun ist
$3=\dim(U_1+U_2+U_3+U_4)>\sum_{j=1}^4\dim U_j-\sum_{i<j}\dim(U_i\cap U_j)=8-6=2$.

2.7.7 Nach 2.6.8 gilt $\cup_{j=1}^m U_j\subset V$. Also gibt es ein $w\in V$ mit $w\notin\cup_{j=1}^m U_j$. Für $n-k=1$ folgt $V=U_j+\langle w\rangle$, und wir sind fertig. Gemäß Induktion nach $n-k$ gibt es zu den $U_j+\langle w\rangle$ ein gemeinsames Komplement W', also $(U_j+\langle w\rangle)+W'=V$ und $((U_j+\langle w\rangle)\cap W'=0$. Setzen wir $W=W'+\langle w\rangle$, so gilt $U_j+W=V$. Sei $u=aw+w'\in U_j\cap W$ mit $w'\in W'$. Dann ist $u-aw=w'\in(U_j+\langle w\rangle)\cap W'=0$. Dies zeigt $u=aw$, also $a=0$ wegen $w\notin U_j$. Somit ist $U_j\cap W=0$.

2.8.1 Das Polynom $x^2=p+(1-p)x$ hat die Nullstellen 1 und $-p$. Also ist $x_j=a+b(-1)^j$ mit geeigneten a,b. Aus $0<p<1$ folgt $\lim_{j\to\infty}x_j=a$. Aus $x_0=a+b$ und $x_1=a-pb$ folgt $a=(px_0+x_1)/(p+1)$, $b=(x_0-x_1)/(p+1)$. Also ist $\lim_{j\to\infty}x_j=(px_0+x_1)/(p+1)$.

2.8.2 a) Es gilt $f=(x-1)(x^2+\frac{2}{3}x+\frac{1}{3})=(x-1)(x-b_1)(x-b_2)$ mit $b_j=-1/3\pm\sqrt{2}i/3$. Somit ist $|b_j|^2=1/3$.
b) Wir erhalten $x_j=a_1+a_2b_1^j+a_3b_2^j$. Wegen $|b_j|<1$ folgt $\lim_{j\to\infty}x_j=a_1$.
c) Es folgt
$x_0+2x_1+3x_2=6a_1+a_2(1+2b_1+3b_1^2)+a_3(1+2b_2+3b_2^2)=a_1$, also $\lim_{j\to\infty}x_j=(x_0+2x_1+3x_2)/6$.

2.8.4 b) Wegen $a^3=1$ gilt $v_1=(1,1,1,1,1,\ldots)$, $v_2=(1,a,a^2,1,a,\ldots)$, $v_3=(1,a^2,a,1,a^2,\ldots)$, $v_4=(0,1,0,a^2,0,\ldots)$, $v_5=(0,1,0,a,0,\ldots)$. Offenbar genügt es zu zeigen, daß die hingeschriebenen Abschnitte linear unabhängig sind. Nach 2.8.2 c) sind v_1,v_2,v_3 linear unabhängig. Angenommen,
$xv_4+yv_5=(0,x+y,0,xa^2+ya,0,\ldots)=\sum_{j=1}^3 x_jv_j$. Dies verlangt $0=$

$x_1 + x_2 + x_3 = x_1 + x_2a^2 + x_3a = x_1 + x_2a + x_3a^2$. Wegen der linearen Unabhängigkeit von $(1,1,1), (1,a^2,a)$ und $(1,a,a^2)$ folgt $x_j = 0$ für $j = 1,2,3$. Dann bleibt $0 = x + y = xa^2 + ya$, also $x = y = 0$.
c) Wegen $\operatorname{Char} K = 2$ und $a^3 = 1$ gilt $(j+6)a^{j+6-1} = ja^{j-1}$.

3.1.4 Aus $A_U = 0$ folgt $U \leq \operatorname{Kern} A$ und aus $A_{V/U} = 0$ folgt $\operatorname{Bild} A \leq U$. Somit gilt $\operatorname{Bild} A \leq \operatorname{Kern} A$ und
$k = \dim \operatorname{Bild} A \leq \dim \operatorname{Kern} A = n - \dim \operatorname{Bild} A = n - k$.

3.2.4 In Kästchenaufteilung gilt $H_1 = \{\begin{pmatrix} * & * \\ 0 & 0 \end{pmatrix}\}$ und $H_2 = \{\begin{pmatrix} 0 & * \\ 0 & * \end{pmatrix}\}$, wobei das linke obere Kästchen vom Typ (m,m) ist. Dies zeigt $\dim H_1 = nm$ und $\dim H_2 = n(n-m)$. Aus $H_1 \cap H_2 = \{\begin{pmatrix} 0 & * \\ 0 & 0 \end{pmatrix}\}$ und $H_1 + H_2 = \{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\}$ folgt $\dim H_1 \cap H_2 = m(n-m)$ und $\dim(H_1 + H_2) = m^2 + n(n-m) = m^2 + n^2 - mn$.

3.3.2 a) Sei $AB = BA$. Nach Voraussetzung gibt es ein $g \in K[x]$ mit $Bv_0 = g(A)v_0$. Für $v = f(A)v_0$ folgt $Bv = Bf(A)v_0 = f(A)g(A)v_0 = g(A)f(A)v_0 = g(A)v$. Also ist $B = g(A) \in K[A]$.
b) Sei $[v_1, \ldots, v_n]$ die Standardbasis des K^n Wegen $Av_j = v_{j+1}$ $(j < n)$ gilt $K^n = K[A]v_1$ Mit a) folgt $\mathrm{C}(A) = K[A]$.
Dabei gilt $\sum_{j=0}^{n-1} a_j A^j = \begin{pmatrix} a_0 & a_1 & \ldots & a_{n-1} \\ a_1 & a_2 & \ldots & a_0 \\ \vdots & \vdots & & \vdots \\ a_{n-1} & a_0 & \ldots & a_{n-2} \end{pmatrix}$.
c) Hier gilt $Av_j = v_j + v_{j+1}$ für $j < n$, somit $K[A]v_1 = K^n$. Also ist
$\mathrm{C}(A) = K[A] = \{\begin{pmatrix} a_0 & 0 & 0 & \ldots & 0 \\ a_1 & a_0 & 0 & \ldots & 0 \\ \vdots & \vdots & & & \vdots \\ a_{n-1} & a_{n-2} & a_{n-3} & \ldots & a_0 \end{pmatrix}\}$.

3.3.3 a) Sei $A = (a_{ij}) \in \mathrm{C}(F)$. Der (i,j)-te Eintrag in AF ist $\sum_k a_{ik}$, der (i,j)-te Eintrag in FA ist $\sum_k a_{kj}$. Also ist $\sum_k a_{ik} = \sum_k a_{kj}$ für alle i,j.
b) Man kann a_{ij} für $i,j \leq n-1$ und a_{1n} vorgeben. Durch die Zeilensummen sind dann $a_{2n}, \ldots, a_{n-1\,n}$ festgelegt, und $a_{n1}, \ldots, a_{nn}$ durch die Spaltensummen. Somit gilt $\dim \mathrm{C}(F) = (n-1)^2 + 1$. c) $Ae = ce$ verlangt $\sum_{k=1}^{n} a_{ik} = c$ für alle i. Sei $v_j = (x_k) \in U$ mit $x_1 = 1$, $x_j = -1$ und $x_k = 0$ für $1 \neq k \neq j$.

Dann ist $Av_j = \begin{pmatrix} a_{11} - a_{1j} \\ \vdots \\ a_{n1} - a_{nj} \end{pmatrix}$. $Av_j \in U$ verlangt daher $\sum_k a_{k1} = \sum_k a_{kj}$. Ist $\sum_k a_{k1} = d$, so erhalten wir $nc = \sum_{k,j} a_{kj} = nd$, und wegen $\operatorname{Char} K \nmid n$ somit $c = d$.

3.3.6 a) Sei $\beta A = \alpha A^t$. Dann ist $\beta(A_1A_2) = \alpha(A_1A_2)^t = \alpha(A_2^tA_1^t) = \alpha(A_1^t)\alpha(A_2^t) = \beta(A_1)\beta(A_2)$. Nach 3.2.14 gibt es ein C mit $\beta(A) = C^{-1}AC$. Daher ist $\alpha(A) = C^{-1}A^tC$.
b) Ist $\alpha^2 = 1$, so gilt $A = C^{-1}(C^{-1}A^tC)^tC = C^{-1}C^tA(C^t)^{-1}C$ für alle A. Dies verlangt $C^{-1}C^t = aE$ mit $a \in K$. Wegen $C = C^{tt} = a^2C$ folgt $a = \pm 1$. Ist $A \in F$, so gilt $A = C^{-1}A^tC$. Für $C = C^t$ folgt $CA = (CA)^t$. Das zeigt $\dim F = n(n+1)/2$. Für $C^t = -C$ und $\operatorname{Char} K \neq 2$ ist hingegen $CA = -A^tC^t = -(CA)^t$, und daher $\dim F = n(n-1)/2$.

3.3.10 Offenbar ist $\mathcal{P}$ eine Untergruppe von $\mathrm{GL}(n,K)$ mit $|\mathcal{P}| = |K|^{\frac{n(n-1)}{2}} = p^{\frac{n(n-1)}{2}f}$. Wegen $|\mathrm{GL}(n,K)| = (p^{fn}-1)(p^{fn}-p^f)\dots(p^{fn}-p^{f(n-1)})$ ist $p^fp^{2f}\dots p^{(n-1)f} = p^{\frac{n(n-1)}{2}f}$ die höchste p-Potenz, welche $|\mathrm{GL}(n,k)|$ teilt. Daher gilt $p \nmid |\mathrm{GL}(n,k) : \mathcal{P}|$.

3.4.2 a) Aus $(b_{ij})(a_{jk}) = E$ folgt $\delta_{ik} = \sum_j b_{ij}a_{jk}$. Somit erhalten wir $1 = \sum_k \delta_{ik} = \sum_j b_{ij} \sum_k a_{jk} = \sum_j b_{ij}$.
b) Sei $(a_{ij})(b_{jk}) = E$ mit $A = (a_{ij})$ und $B = (b_{ij})$ stochastisch. Wegen $\sum_j a_{ij}b_{jk} = 0$ für $i \neq k$ folgt $a_{ij}b_{jk} = 0$ für alle j. Da B stochastisch ist, gibt es zu jedem j ein j' mit $b_{jj'} > 0$, und daher ist $a_{ij} = 0$ für $i \neq j'$. Die Spalten von A haben also die Gestalt $(0,\dots,0,a_{j'j},0,\dots,0)^t$. Da A regulär ist, ist $j \to j'$ injektiv, somit bijektiv. Da alle Zeilensummen von A gleich 1 sind, folgt $a_{j'j} = 1$. Also ist A eine Permutationsmatrix.

3.4.3 a) Ist $A = \begin{pmatrix} 1-p & p \\ q & 1-q \end{pmatrix}$, so folgt $\operatorname{Spur} A^2 = (1-p)^2 + (1-q)^2 + 2pq = 1 + (1-p-q)^2 \geq 1$.
b) Wir versuchen s und t so zu bestimmen, daß $\begin{pmatrix} 1-s & s \\ t & 1-t \end{pmatrix}^2 = \begin{pmatrix} (1-s)^2+st & s(2-s-t) \\ t(2-s-t) & (1-t)^2+st \end{pmatrix} = \begin{pmatrix} 1-p & p \\ q & 1-q \end{pmatrix}$. Dies verlangt u.a., daß $(s+t)(2-s-t) = p+q$. Setzen wir $s+t = u$, so ist $u(2-u) = p+q$, also $(1-u)^2 = 1-p-q \geq 0$. Wir wählen $u = 1-\sqrt{1-p-q}$, so daß $u \leq 1$. Schließlich bestimmen wir s und t

durch $s = p/(2-u)$, $t = q/(2-u)$. Dann gilt $s \geq 0$, $t \geq 0$ und $s+t = u \leq 1$. Also gelten $0 \leq s, t \leq 1$, und daher ist $\begin{pmatrix} 1-s & s \\ t & 1-t \end{pmatrix}$ stochastisch.

3.4.5 Der Zustand $i\,(0 \leq i \leq 6)$ liege vor, wenn Spieler 1 genau i Kärtchen hat. Die Übergangsmatrix ist

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1/6 & 0 & 5/6 & 0 & 0 & 0 & 0 \\ 0 & 2/6 & 0 & 4/6 & 0 & 0 & 0 \\ 0 & 0 & 3/6 & 0 & 3/6 & 0 & 0 \\ 0 & 0 & 0 & 4/6 & 0 & 2/6 & 0 \\ 0 & 0 & 0 & 0 & 5/6 & 0 & 1/6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Da die absorbierenden Zustände 0 und 6 von jedem Zustand aus erreichbar sind, hat $P = \lim_{k\to\infty} A^k$ die Gestalt

$$\begin{pmatrix} 1 & & 0 \\ s_1 & & 1-s_1 \\ \vdots & 0 & \vdots \\ s_5 & & 1-s_5 \\ 0 & & 1 \end{pmatrix}.$$

Dabei gilt offenbar $s_3 = \frac{1}{2}$ und $s_1 + s_5 = s_2 + s_4 = 1$. Aus $PA = P$ folgt $s_1 = \frac{1}{6} + \frac{5}{6}s_2, s_2 = \frac{2}{6}s_1 + \frac{4}{6}s_3 = \frac{2}{6}s_1 + \frac{2}{6}$. Dies liefert $s_1 = \frac{8}{13}, s_2 = \frac{7}{13}, s_4 = \frac{6}{13}, s_5 = \frac{5}{13}$. Im Besitz von nur einer Karte hat Spieler 1 immer noch die Wahrscheinlichkeit $1 - s_1 = \frac{5}{13}$, das Spiel zu gewinnen.

3.4.6 a) Man erhält

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & & \\ 0 & 1 & 0 & 0 & & \\ p & q & 0 & 0 & & \\ 0 & p & q & 0 & & \\ & & \ddots & & & \\ & & & p & q & 0 \end{pmatrix}.$$

Wegen $p > 0$ ist der Zustand 1 von jedem Zustand $3, \ldots, n$ aus erreichbar. Also existiert

$$P = \lim_{k\to\infty} A^k = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ a_3 & 1-a_3 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ a_n & 1-a_n & 0 & \ldots & 0 \end{pmatrix}.$$

b) Setzen wir $a_1 = 1, a_2 = 0$, so verlangt $P = AP$, daß $a_j = pa_{j-2} + qa_{j-1}$. Die Gleichung $s^2 = p + qs$ hat die Lösungen $s = 1, -p$. Daher ist $a_j = b + c(-p)^j$ mit $1 = b - cp$, $0 = b + cp^2$. Dies ergibt $b = p/(1+p), c = -1/(p(1+p))$. Also folgt $a_j = (p + (-p)^{j-1})/(1+p)$.

3.4.7 Da der absorbierende Zustand n wegen $r_1 \dots r_{n-1} > 0$ von jedem Zustand $1, 2, \dots, n-1$ aus erreichbar ist, gilt

$P = \lim_{k\to\infty} A^k = \begin{pmatrix} 1 & & 0 \\ s_1 & & 1 - s_1 \\ \vdots & 0 & \vdots \\ s_{n-1} & & 1 - s_{n-1} \\ 0 & & 1 \end{pmatrix}$. Aus $P = AP$ folgt

(1) $\quad s_1 = p_1 + q_1 s_1 + r_1 s_2,$

(i) $\quad s_i = p_i s_{i-1} + q_i s_i + r_i s_{i+1},$

(n-1) $\quad s_{n-1} = p_{n-1} s_{n-2} + q_{n-1} s_{n-1}.$

Daraus erhalten wir wegen $p_i + q_i + r_i = 1$

(1') $\quad u_1 - q_1 u_1 + p_1 \sum_{k=2}^{n-1} u_k = p_1,$

(i') $\quad r_i u_i = p_i u_{i-1},$

(n-1') $\quad r_{n-1} u_{n-1} = p_{n-1} u_{n-2}.$

Dies liefert $u_k = \frac{p_k p_{k-1} \dots p_2}{r_k r_{k-1} \dots r_2} u_1$ $(k = 2, \dots, n-1)$. Schließlich ist u_1 zu berechnen aus $u_1(1 - q_1 + p_1 \sum_{k=2}^{n-1} \frac{p_k p_{k-1} \dots p_2}{r_k r_{k-1} \dots r_2}) = p_1$.

3.5.3 a) Es gilt $0 = \operatorname{Bild} A^m \leq \operatorname{Bild}^{m-1} \leq \dots \leq \operatorname{Bild} A \leq V$. Da A^j auf $\operatorname{Bild} A^i / \operatorname{Bild} A^{i+1}$ die Nullabbildung bewirkt, folgt mit Aufgabe 3.5.1, daß $\operatorname{Spur} A^j = 0$ ist.

b) Sei $0 = a_0 E + a_1 A + \dots + a_k A^k$ minimal gewählt. Dann ist $0 = \operatorname{Spur} a_0 E = a_0 \dim V$. Wegen $\operatorname{Char} K = 0$ folgt $a_0 = 0$, somit $0 = A(a_1 E + \dots + a_k A^{k-1})$. Wegen $a_1 E + \dots + a_k A^{k-1} \neq 0$ ist A nicht regulär. Somit gilt $\operatorname{Kern} A > 0$. Aus $0 = \operatorname{Spur} A^j = \operatorname{Spur} A^j_{\operatorname{Kern} A} + \operatorname{Spur} A^j_{V/\operatorname{Kern} A} = \operatorname{Spur} A^j_{V/\operatorname{Kern} A}$ folgt vermöge Induktion nach $\dim V$ nun $A^{m-1}_{V/\operatorname{Kern} A} = 0$ für ein geeignetes m. Das zeigt $A^{m-1} V \leq \operatorname{Kern} A$, also $A^m = 0$.

3.6.2 a) Aus $P + Q = (P+Q)^2 = P^2 + PQ + QP + Q^2 = P + Q + PQ + QP$ folgt $PQ + QP = 0$. Daher ist $PQ = PQ^2 = -QPQ = Q^2 P = QP$, also $2PQ = 0$. Wegen $\operatorname{Char} \neq 2$ folgt $PQ = QP = 0$.

b) Ist $PQ = QP$, so folgt $PQ = (PQ)^2$. Wegen $PQv = QPv \in \operatorname{Bild} P \cap \operatorname{Bild} Q$ gilt $\operatorname{Bild} PQ \subseteq \operatorname{Bild} P \cap \operatorname{Bild} Q$. Sei umgekehrt $w = Qu = Pv \in \operatorname{Bild} P \cap \operatorname{Bild} Q$. Dann ist $w = Q^2 u = QPv = PQv \in \operatorname{Bild} PQ$. Somit gilt $\operatorname{Bild} PQ = \operatorname{Bild} P \cap \operatorname{Bild} Q$. Offenbar ist $\operatorname{Kern} P +$

$\operatorname{Kern} Q \leq \operatorname{Kern} PQ$. Sei $PQw = 0$. Dann ist $w = Qw + (w - Qw)$ mit $Qw \in \operatorname{Kern} P$ und $w - Qw \in \operatorname{Kern} Q$. Somit gilt $\operatorname{Kern} P + \operatorname{Kern} Q = \operatorname{Kern} PQ$.
c) Es gilt $R^2 = (P + Q - PQ)^2 = P^2 + Q^2 + (PQ)^2 + 2PQ - 2P^2Q - 2QPQ = P + Q + PQ - 2PQ = R$. Also ist R eine Projektion. Offenbar gilt $\operatorname{Kern} P \cap \operatorname{Kern} Q \subseteq \operatorname{Kern} R$. Ist $Rw = 0$, so folgt $0 = PRw = P^2w + PQw - PQw = P^2w = Pw$, also $w \in \operatorname{Kern} P$. Ebenso folgt $Qw = 0$. Somit ist $\operatorname{Kern} R = \operatorname{Kern} P \cap \operatorname{Kern} Q$. Aus $Rv = Pv + Q(v - Pv)$ folgt $\operatorname{Bild} R \subseteq \operatorname{Bild} P + \operatorname{Bild} Q$. Sei $v = Pv \in \operatorname{Bild} P$ und $w = Qw \in \operatorname{Bild} Q$. Dann ist $R(v + w) = Pv + Pw + Qv + Qw - PQv - PQw = v + Pw + Qv + w - QPv - Pw = v + w \in \operatorname{Bild} R$. Also ist $\operatorname{Bild} R = \operatorname{Bild} P + \operatorname{Bild} Q$.

3.6.4 a) und b) Offenbar ist A eine lineare Abbildung von V in $\oplus_{j=1}^m V/V_j$ mit $\operatorname{Kern} A = \cap_{j=1}^m V_j$. Es folgt $\dim V/\cap_{j=1}^m V_j = \dim V/\operatorname{Kern} A = \dim \operatorname{Bild} A \leq \dim \oplus_{j=1}^m V/V_j = \sum_{j=1}^m \dim V/V_j$.
c) Gleichheit gilt genau dann, wenn A surjektiv ist. Dies ist gleichwertig damit, daß zu jedem j und jedem $w \in V$ ein v existiert mit $(v+V_1, \ldots, v+V_m) = Av = (V_1, \ldots, w+V_j, \ldots, V_m)$. Dies verlangt $w-v \in V_j$ und $v \in \cap_{i \neq j} V_i$. Dann ist $w = (w - v) + v \in V_j + \cap_{i \neq j} V_j$. Also gilt $V = V_j + \cap_{i \neq j} V_i$ für alle j.

3.7.2 In $U = \{(k_1, \ldots, k_n) \mid \sum_{i=1}^n k_i = 0\} \leq K^n$ haben alle Vektoren gerades Gewicht. Nun gilt $C = (C \cap U) \cup (C \setminus (C \cap U))$. Alle Codeworte im Unterraum $C \cap U$ haben gerades und alle Codeworte in $C \setminus (C \cap U)$ haben ungerades Gewicht. Die Behauptung folgt wegen $|C \setminus (C \cap U)| = |C/C \cap U| = 0$, falls $C \leq U$, und $|C \setminus (C \cap U)| = |C|/2$ sonst, wegen $\dim C \cap U = \dim C - 1$.

3.7.5 a) Ist $v \notin C$, so existiert wegen der Perfektheit des Hamming-Codes (mit $e = 1$) ein $c \in C$ mit $\mathrm{d}(v, c) = 1$. Dann ist $v + C = v - c + C$, wobei $\mathrm{wt}(v - c) = \mathrm{d}(v, c) = 1$. Ist $u + C = u' + C$ mit $\mathrm{wt}(u) = \mathrm{wt}(u') = 1$, so gilt $u - u' \in C$. Wegen $\mathrm{wt}(u - u') \leq 2$ und da C die Minimaldistanz 3 hat, folgt $u = u'$.
b) Sei $v = c + e$ mit $c \in C$ und e vom Gewicht 1. Ist H eine Kontrollmatrix für C, so folgt $Hv^t = H(c + e)^t = He^t$, also $v - e \in \operatorname{Kern} H = C$, d.h. $v + C = e + C$. Somit ist e nach a) eindeutig bestimmt. Der Fehlervektor $e = ke_j$ $(k \in K)$, wobei $e_j = (0, \ldots, 0, 1, 0, \ldots, 0)$, läßt sich somit eindeutig aus $Hv^t = H(ke_j)^t$ bestimmen.

3.7.7 Es gilt $\sum_{c \in C} \mathrm{wt}(c) = \sum_{c \in C} |\{(c, f_i(c) \mid i = 1, \ldots, n,\ f_i(c) \neq 0\}| =$
$= \sum_{i=1}^n |\{(c, f_i(c)) \mid c \in C, f_i(c) \neq 0\}| = \sum_{i=1}^n (q^k - |\operatorname{Ker} f_i|) = n(q-1)q^{k-1}$.

3.8.3 Für $a = b = 0$ ist $\mathrm{r}(A) = 0$. Für $a = 0 \neq b$ oder $a \neq 0 = b$ ist offenbar $\mathrm{r}(A) = 3$. Sei also $ab \neq 0$. Durch elementare Umformungen erhalten wir

$$A \to \begin{pmatrix} 0 & a & 0 & 0 \\ b & 0 & a & a \\ b & b & -b & a-b \\ b & b & 0 & -b \end{pmatrix} \quad (s_3 \to s_3 - s_2, s_4 \to s_4 - s_2)$$

$$\to \begin{pmatrix} a & 0 & 0 & 0 \\ 0 & b & a & a \\ b & b & -b & a-b \\ b & b & 0 & -b \end{pmatrix} \quad (s_1 \leftrightarrow s_2)$$

$$\to \begin{pmatrix} a & 0 & 0 & 0 \\ 0 & b & a & a \\ 0 & 0 & -a-b & -b \\ 0 & 0 & -a & -a-b \end{pmatrix} \quad (z_3 \to z_3 - \tfrac{b}{a} z_1 - z_2, z_4 \to z_4 - \tfrac{b}{a} z_1 - z_2)$$

$$\to \begin{pmatrix} a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & -a-b & -b \\ 0 & 0 & -a & -a-b \end{pmatrix} \quad (s_3 \to s_3 - \tfrac{a}{b} s_2, s_4 \to s_4 - \tfrac{a}{b} s_2)$$

$$\to \begin{pmatrix} a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & -b & a \\ 0 & 0 & -a & -a-b \end{pmatrix} \quad (z_3 \to z_3 - z_4)$$

$$\to \begin{pmatrix} a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & -b & a \\ 0 & 0 & 0 & -(a^2+ab+b^2)/b \end{pmatrix} \quad (z_4 \to z_4 - \tfrac{a}{b} z_3).$$

Somit gilt

$$\mathrm{r}(A) = \begin{cases} 4 \text{ für } ab(a^2+ab+b^2) \neq 0 \\ 3 \text{ für } ab \neq 0 = a^2+ab+b^2. \end{cases}$$

3.8.4 Die Aussagen für $a = 0$ und $a = b$ sind trivial. Sei also $a(a-b) \neq 0$. Dann erhalten wir

$$A \to \begin{pmatrix} a-b & 0 & \dots & 0 & 0 \\ b & a & \dots & a & a \\ \vdots & \vdots & & \vdots & \vdots \\ b & b & \dots & b & a \end{pmatrix} \quad (z_1 \to z_1 - z_2)$$

$\to \begin{pmatrix} a-b & 0 & \dots & 0 & 0 \\ 0 & a & \dots & a & a \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & b & \dots & b & a \end{pmatrix}$ $(z_j \to z_j - \frac{b}{a-b} z_1)$. Die Teilmatrix vom Typ $(n-1, n-1)$ hat dieselbe Gestalt wie die Ausgangsmatrix, hat daher vermöge einer Induktionsannahme den Rang $n-1$.

4.1.1 a) Offenbar gilt $N_1 \cap N_2 \trianglelefteq G$, und nach Teil c) ist $N_1 N_2$ eine Untergruppe von G. Für $g \in G$ und $n_j \in N_j$ $(j = 1, 2)$ gilt
$g^{-1} n_1 n_2 g = g^{-1} n_1 g g^{-1} n_2 g \in N_1 N_2$.
b) Für $n_j \in N_j$ $(j = 1, 2)$ ist
$n_1(n_2 n_1^{-1} n_2^{-1}) = (n_1 n_2 n_1^{-1}) n_2^{-1} \in N_1 \cap N_2 = \{1\}$, also $n_1 n_2 = n_2 n_1$.
c) Für $n \in N$ und $u \in U$ gilt $nu = uu^{-1}nu \in UN$, also $NU = UN$.

4.1.4 a) Es gilt $\mathcal{D} = \langle A, B \rangle$ mit $A^4 = B^2 = E$ und $B^{-1}AB = A^{-1}$. Daher ist $(A^j B)^2 = A^j B^{-1} A^j B = A^j A^{-j} = E$. Somit hat $\mathcal{D}$ fünf Elemente A^2, B, AB, A^2B, A^3B von der Ordnung 2 und zwei Elemente A, A^{-1} von der Ordnung 5. Ist $U < \mathcal{D}$ mit $|U| = 4$ und $U \neq \langle A \rangle$, so gilt $\mathcal{D} = U\langle A \rangle$, daher $8 = |U\langle A \rangle| = |U||\langle A \rangle|/|U \cap \langle A \rangle| = 16/|U \cap \langle A \rangle|$, also $|U \cap \langle A \rangle| = 2$. Dies zeigt $A^2 \in U$. Somit gibt es die Möglichkeiten $U_1 = \langle A^2, B \rangle = \{E, A^2, B, A^2B\}$ und $U_2 = \langle A^2, AB \rangle = \{E, A^2, AB, A^3B\}$.
b) Ist $|U| = 4$, so folgt mit Aufgabe 4.1.2, daß $U \lhd \mathcal{D}$. Wegen $B^{-1}A^2B = A^2$ gilt $\langle A^2 \rangle \lhd \mathcal{D}$. Aus $A^{-1}A^jBA = A^{j-1}A^{-1}B = A^{j-2}B \notin \langle A^jB \rangle$ folgt $\langle A^jB \rangle \not\trianglelefteq \mathcal{D}$ für $j = 0, 1, 2, 3$.
c) Es gilt $\langle B \rangle \lhd \langle A^2, B \rangle \lhd \mathcal{D}$, aber $\langle B \rangle \not\trianglelefteq \mathcal{D}$.

4.2.1 a) Es gilt $\tau_b^2 = \sigma^3 = \alpha^2 = \iota$, letzteres wegen $a^4 = a$.
b) Es gelten $\sigma^{-1}\tau_b\sigma = \tau_{a^{-1}b}$, $\alpha^{-1}\tau_b\alpha = \tau_{b^2}$ und $\alpha^{-1}\sigma\alpha = \sigma^2$. Dies zeigt $T \lhd \langle T, \sigma \rangle \lhd \langle T, \sigma, \alpha \rangle = S$.
c) Wir haben die Zyklenzerlegungen $\tau_b = (0, b)(c, c+b)$ mit $0 \neq c \neq b$, $\sigma = (0)(1, a, a^2)$ und $\alpha = (0)(1)(a, a^2)$. Somit ist $\operatorname{sgn} \tau_b = \operatorname{sgn} \sigma = 1$ und $\operatorname{sgn} \alpha = -1$.

4.2.3 a) Wegen $\begin{pmatrix} x \\ ax+b \end{pmatrix} \begin{pmatrix} x \\ a'x+b' \end{pmatrix} = \begin{pmatrix} x \\ aa'x+ab'+b \end{pmatrix}$
und $\begin{pmatrix} x \\ a^{-1}x - a^{-1}b \end{pmatrix} \begin{pmatrix} x \\ ax+b \end{pmatrix} = \iota$ ist U eine Gruppe.
b) Daß T ein Normalteiler ist, folgt aus
$\begin{pmatrix} x \\ ax+b \end{pmatrix}^{-1} \begin{pmatrix} x \\ x+c \end{pmatrix} \begin{pmatrix} x \\ ax+b \end{pmatrix} = \begin{pmatrix} x \\ x+a^{-1}c \end{pmatrix}$.

Die restlichen Aussagen unter b), c) und d) sind trivial.
c) $\begin{pmatrix} x \\ x+b \end{pmatrix}$ ist ein Produkt von p^{f-1} Zyklen der Länge p. Für $p > 2$ ist $\operatorname{sgn}\begin{pmatrix} x \\ x+b \end{pmatrix} = 1$, für $p = 2$ ist $\operatorname{sgn}\begin{pmatrix} x \\ x+b \end{pmatrix} = (-1)^{2^{f-1}} = 1$, falls $q > 2$. Ist $K^* = \langle a \rangle$, so ist $\begin{pmatrix} x \\ ax \end{pmatrix}$ ein Zykel der Länge $q-1$, daher $\operatorname{sgn}\begin{pmatrix} x \\ ax \end{pmatrix} = \begin{cases} 1 \text{ für } q = 2^f \\ -1 \text{ für } 2 \nmid q. \end{cases}$

4.3.3 Wir bezeichnen die jeweilige Matrix vom Typ (n,n) mit C_n. Entwicklung nach der ersten Zeile liefert
$$\det C_n = a \det \begin{pmatrix} & & 0 \\ & C_{n-2} & \vdots \\ 0 & \dots & 0\ a \end{pmatrix} + (-1)^{n-1} b \det \begin{pmatrix} 0 & & \\ \vdots & C_{n-2} & \\ b\ 0 & \dots & 0 \end{pmatrix}$$
$= (a^2 - b^2) \det C_{n-2}$. Man sieht leicht, daß $\det C_2 = a^2 - b^2$ und $\det C_3 = (a^2 - b^2)c$ ist. Durch Induktion nach n folgt die Behauptung.

4.5.4 a) folgt durch direkte Rechnung.
b) In $D^2 v_{i_1} \dots v_{i_p}$ taucht das Element $w = v_{i_1} \dots \not{v}_{i_k} \dots \not{v}_{i_l} \dots v_{i_p}$ (ohne v_{i_k} und v_{i_l} mit $i_k < i_l$) auf in $(-1)^{k-1} f(v_{i_k}) D(v_{i_1} \dots \not{v}_{i_k} \dots \dots v_{i_p})$ mit dem Beitrag $(-1)^{k-1+l-2} f(v_{i_k}) f(v_{i_l}) w$, aber auch in $(-1)^{l-1} f(v_{i_l}) D(v_{i_1} \dots \not{v}_{i_l} \dots v_{i_p})$ mit dem Beitrag $(-1)^{l-1+k-1} f(v_{i_l}) f(v_{i_k}) w$. Somit gilt $D^2 = 0$.

5.1.1 Durch Differenzieren von $(1+x)^n = \sum_{j=0}^n \binom{n}{j} x^j$ und Spezializierung $x = 1$ erhält man
$n 2^{n-1} = \sum_{j=0}^n j \binom{n}{j}$,
$n(n-1) 2^{n-2} = \sum_{j=0}^n j(j-1) \binom{n}{j}$,
$n(n-1)(n-2) 2^{n-3} = \sum_{j=0}^n j(j-1)(j-2) \binom{n}{j}$.
Daraus folgen leicht die Aussagen unter a), b), c).
d) Es gilt
$\sum_{j=0}^{2n-1} \binom{2n-1}{j} x^j = (1+x)^n n (1+x)^{n-1} \cdot \frac{1}{n} = \frac{1}{n} \sum_{k=0}^n \binom{n}{k} x^k \sum_{l=0}^n \binom{n}{l} l x^{l-1}$.
Vergleich der Kopeffizienten von x^{n-1} liefert
$n \binom{2n-1}{n-1} = \sum_{l=0}^n \binom{n}{n-l} \binom{n}{l} l = \sum_{l=0}^n \binom{n}{l}^2 l$. Man stellt leicht fest, daß $\binom{2n-1}{n-1} = \binom{2n}{n}/2$.

5.1.3 a) $\binom{x+y}{k}$ und $\sum_{j=0}^k \binom{x}{j} \binom{y}{k-j}$ sind Polynome in x und y, also $\binom{x+y}{k} = \sum_l f_l(x) y^l$ und $\sum_{j=0}^k \binom{x}{j} \binom{y}{k-j} = \sum_l g_l(x) y^l$ mit $f_j, g_j \in K[x]$. Nach der

Vorbemerkung gilt $\sum_l f_l(m)n^l = \sum_l g_l(m)n^l$ für alle $m, n \in \mathbb{N}$. Da die Polynome $\sum_l f_l(m)y^l$ und $\sum_l g_l(m)y^l$ an unendlich vielen Stellen übereinstimmen, folgt $f_l(m) = g_l(m)$ für alle $m \in \mathbb{N}$. Das zeigt $f_l(x) = g_l(x)$.
b) Wegen a) gilt
$(1+x)^\alpha(1+x)^\beta = \sum_j \binom{\alpha}{j}x^j \sum_k \binom{\beta}{k}x^k = \sum_l(\sum_{j+k=l}\binom{\alpha}{j}\binom{\beta}{k})x^l$
$= \sum_l \binom{\alpha+\beta}{l}x^l = (1+x)^{\alpha+\beta}$.
c) Nach b) ist $(1+x)^{-m} = \sum_{j=0}^\infty \binom{-m}{j}x^j$. Dabei ist
$\binom{-m}{j} = \frac{-m(-m-1)\ldots(-m-j+1)}{j!} = \frac{(-1)^j m(m+1)\ldots(m+j-1)}{j!} = (-1)^j\binom{m+j-1}{j}$.

5.1.5 Es gilt $y^j = ((y-1)+1)^j = \sum_{k=0}^j \binom{j}{k}(y-1)^k$
$= \sum_{k=0}^j \binom{j}{k}\sum_{i=0}^k \binom{k}{i}(-1)^{k-i}y^i = \sum_{i=0}^j(\sum_{k=0}^j(-1)^{k-i}\binom{j}{k}\binom{k}{i})y^i$.
Somit ist $\delta_{ij} = \sum_{k=0}^j(-1)^{k-i}\binom{j}{k}\binom{k}{i}$. Ist $A = (a_{ij})$ mit $a_{ij} = \binom{j}{i}$ und $B = (b_{ij})$ mit $b_{ij} = (-1)^{j-i}\binom{j}{i}$, so folgt $\sum_k b_{ik}a_{kj} = \sum_k(-1)^{k-i}\binom{k}{i}\binom{j}{k} = \delta_{ij}$, also $BA = E$.

5.2.2 b) Offenbar gilt $\mathcal{A}(\mathcal{N}) = e_\mathcal{N}R$.
c) Wegen $e_{\mathcal{N}_1}e_{\mathcal{N}_2} = e_{\mathcal{N}_1\cup\mathcal{N}_2}$ gilt $\mathcal{A}(\mathcal{N}_1)\mathcal{A}(\mathcal{N}_2) = \mathcal{A}(\mathcal{N}_1 \cup \mathcal{N}_2) = \mathcal{A}(\mathcal{N}_1) \cap \mathcal{A}(\mathcal{N}_2)$. Offenbar ist $\mathcal{A}(\mathcal{N}_1) + \mathcal{A}(\mathcal{N}_2) \subseteq \mathcal{A}(\mathcal{N}_1 \cap \mathcal{N}_2)$. Ist $\mathcal{N}'$ das Komplement von $\mathcal{N}$, so gilt $e_\mathcal{N} = 1 - e_{\mathcal{N}'}$. Es folgt $e_{\mathcal{N}_1\cap\mathcal{N}_2} = 1 - e_{(\mathcal{N}_1\cap\mathcal{N}_2)'} = 1 - e_{\mathcal{N}_1'}e_{\mathcal{N}_2'} = 1 - (1-e_{\mathcal{N}_1})(1-e_{\mathcal{N}_2}) = e_{\mathcal{N}_1}(1-e_{\mathcal{N}_2}) + e_{\mathcal{N}_2}$. Dies liefert $\mathcal{A}(\mathcal{N}_1 \cap \mathcal{N}_2) \subseteq e_{\mathcal{N}_1}(1-e_{\mathcal{N}_2})R + e_{\mathcal{N}_2}R \subseteq \mathcal{A}(\mathcal{N}_1) + \mathcal{A}(\mathcal{N}_2)$.
d) Sei $\mathcal{I}$ ein Ideal in R und $\mathcal{M} = \{j \mid f(j) = 0 \text{ für alle } f \in \mathcal{I}\}$. Dann gilt $\mathcal{I} \subseteq \mathcal{A}(\mathcal{M})$. Für jedes $i \notin \mathcal{M}$ existiert ein $f_i \in \mathcal{I}$ mit $f_i(i) \neq 0$. Ein Vielfaches g_i von f_i, welches auch in $\mathcal{I}$ liegt, hat dann die Eigenschaft $g_i(j) = \delta_{ij}$. Somit folgt $\sum_{i\notin\mathcal{M}} g_i = e_\mathcal{M} \in \mathcal{I}$ und daher $\mathcal{I} = e_\mathcal{M}R = \mathcal{A}(\mathcal{M})$.
e) Wegen $|T(f_1+f_2)| \leq |T(f_1)\cup T(f_2)| \leq |T(f_1)| + |T(f_2)|$ ist $\mathcal{B}$ ein Ideal in R. Angenommen, $\mathcal{B} = \mathcal{A}(\mathcal{M})$. Wegen $\mathcal{B} \subset R = \mathcal{A}(\emptyset)$ gilt $\emptyset \subset \mathcal{M}$. Ist $f_i(j) = \delta_{ij}$, so gilt $f_i \in \mathcal{B}$, aber $f_i \notin \mathcal{A}(\mathcal{M})$ für $i \in \mathcal{M}$.

5.3.3 a) Sind $a = \prod_i p_i^{a_i}, b = \prod_i p_i^{b_i}, c = \prod_i p_i^{c_i}$ die Primfaktorzerlegungen, so folgt aus $\max(a_i + b_i, a_i + c_i) = a_i + \max(b_i, c_i)$ sofort
$\mathrm{kgV}(ab, ac) \sim a\,\mathrm{kgV}(b, c)$. Für Hauptideale $\mathcal{A} = Ra, \mathcal{B} = Rb, \mathcal{C} = Rc$ heißt dies $\mathcal{AB} \cap \mathcal{AC} = \mathcal{A}(\mathcal{B} \cap \mathcal{C})$.
b) Ähnlich wie in a) folgt die Behauptung aus
$\min(a_i + b_i, a_i + c_i) = a_i + \min(b_i, c_i)$. Im Hauptidealring R entspricht dies der Relation $\mathcal{AB} + \mathcal{AC} = \mathcal{A}(\mathcal{B} + \mathcal{C})$, die in allen Ringen gilt.

5.3.4 a) Ist $Ra \cap Rb = Rk$, so folgt $Rac \cap Rbc = Rkc$. Also gilt
$\mathrm{kgV}(ac, bc) \sim c\,\mathrm{kgV}(a, b)$.

b) Sei $Rac \cap Rbc = Rd$ mit $d = r_1ac = r_2bc$. Wegen $c \mid d$ ist $d = ec$, somit $e = r_1a = r_2b \in Ra \cap Rb$. Ist $s_1a = s_2b \in Ra \cap Rb$, so folgt $s_1ac = s_2bc \in Rac \cap Rbc = Rd$. Wegen $d = ec$ erhalten wir $s_1a = s_2b = te \in Re$. Dies zeigt $Ra \cap Rb = Re$ und somit $\mathrm{kgV}(ac, bc) \sim d = ce \sim c \cdot \mathrm{kgV}(a, b)$.
c) Sei $Ra \cap Rb = Rk$. Wegen $ab \in Ra \cap Rb = Rk$ gilt $ab = dk$ mit $d \in R$. Wegen $b \mid k$ ist $k = br$, also $a = dr$. Somit ist $d \mid a$. Ebenso sieht man $d \mid b$. Mithin ist d ein gemeinsamer Teiler von a und b.
Sei nun s irgendein gemeinsamer Teiler von a und b, etwa $a = r_1s$ und $b = r_2s$. Nach Teil a) gilt $\mathrm{kgV}(a, b) = \mathrm{kgV}(r_1s, r_2s) \sim s \cdot \mathrm{kgV}(r_1, r_2)$, daher $k = sl$ mit $l \mid r_1r_2$, etwa $r_1r_2 = tl$. Es folgt $tls^2 = r_1r_2s^2 = ab = kd = sld$. Also ist $d = ts$, somit $s \mid d$. Daher ist $d = \frac{ab}{k}$ ein größter gemeinsamer Teiler von a und b. Dies zeigt $ab \sim \mathrm{kgV}(a, b)\,\mathrm{ggT}(a, b)$, falls $\mathrm{kgV}(a, b)$ existiert.

5.3.5 a) Man stellt leicht fest, daß $\mathrm{ggT}(ac, bc) \sim c \cdot \mathrm{ggT}(a, b)$. Sei d ein größter gemeinsamer Teiler von a und b. Wegen $a(bd^{-1}) = (ad^{-1})b \in Ra \cap Rb$ ist abd^{-1} ein gemeinsames Vielfaches von a und b.
Sei umgekehrt $a \mid k$ und $b \mid k$. Wegen $ab \mid kb$ und $ab \mid ka$ folgt
$ab \mid \mathrm{ggT}(ka, kb) \sim k \cdot \mathrm{ggT}(a, b) \sim kd$. Also gilt $\frac{ab}{d} \mid k$. Somit ist $\frac{ab}{d}$ ein kleinstes gemeinsames Vielfaches von a und b.
b) Ist $Ra + Rb = Rd$ ein Hauptideal, so ist d ein größter gemeinsamer Teiler von a und b. Nach a) existiert auch $\mathrm{kgV}(a, b)$. Also ist $Ra \cap Rb$ ein Hauptideal.

5.4.4 a) Sei $j \geq m + 1$ und $A^jv = 0$. Dann ist $A^{m+1}(A^{j-m-1}v) = 0$, somit $0 = A^m(A^{j-m-1}v) = A^{j-1}v = 0$. Wiederholung dieses Argumentes zeigt $\mathrm{Kern}\, A^j = \mathrm{Kern}\, A^m$ für alle $j > m$.
b) Die Aussage folgt aus $\dim \mathrm{Bild}\, A^j = \dim V - \dim \mathrm{Kern}\, A^j$.
c) Wegen $\mathrm{Bild}\, A^m = \mathrm{Bild}\, A^{2m}$ gibt es für $v \in V$ ein $w \in V$ mit $A^mv = A^{2m}w$. Dann ist $v = (v - A^mw) + A^mw$ mit $A^m(v - A^mw) = 0$. Daher gilt $V = \mathrm{Kern}\, A^m + \mathrm{Bild}\, A^m$. Ist $v = A^mu \in \mathrm{Kern}\, A^m \cap \mathrm{Bild}\, A^m$, so folgt $0 = A^mv = A^{2m}u$. Dies zeigt $u \in \mathrm{Kern}\, A^{2m} = \mathrm{Kern}\, A^m$, also $v = A^mu = 0$. Daher ist $\mathrm{Kern}\, A^m \cap \mathrm{Bild}\, A^m = 0$.

5.5.1 Man bestätigt leicht, daß $A^2 - nA + (2n-4)E =$

$$\begin{pmatrix} n-2 & 0 & 0 & \dots & 0 & 0 & 2-n \\ 0 & 2n-6 & -2 & \dots & -2 & -2 & 0 \\ 0 & -2 & 2n-6 & \dots & -2 & -2 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & -2 & -2 & \dots & -2 & 2n-6 & 0 \\ 2-n & 0 & 0 & \dots & 0 & 0 & n-2 \end{pmatrix},$$

woraus alle Aussagen folgen.

5.5.2 a) Durch $B(v+\operatorname{Kern} A^{m+1}) = Av+\operatorname{Kern} A^m$ wird eine offenbar wohldefinierte lineare Abbildung B von $\operatorname{Kern} A^{m+2}/\operatorname{Kern} A^{m+1}$ in $\operatorname{Kern} A^{m+1}/\operatorname{Kern} A^m$ definiert. Dabei ist $\operatorname{Kern} B = \operatorname{Kern} A^{m+1}$. Also folgt $\dim \operatorname{Kern} A^{m+2}/A^{m+1} = \dim \operatorname{Bild} B \leq \dim \operatorname{Kern} A^{m+1}/A^m$.
b) folgt unmittelbar aus a).

5.5.3 Wegen $A^m = \begin{pmatrix} B^m & 0 \\ mB^m & B^m \end{pmatrix}$ folgt $g(A) = \begin{pmatrix} g(B) & 0 \\ Bg'(B) & g(B) \end{pmatrix}$ für alle Polynome $g \in K[x]$. Somit ist $0 = m_A(A) = \begin{pmatrix} m_A(B) & 0 \\ Bm'_A(B) & m_A(B) \end{pmatrix}$.
Dies verlangt $m_B \mid m_A$ und $m_B \mid xm'_A$. Daher ist $b_i \leq a_i$. Ist $m_A = p_i^{a_i} s_i$, so wird auch verlangt, daß $p_i^{b_i} \mid xp_i^{a_i} s'_i + a_i x p_i^{a_i-1} p'_i s_i$. Wegen $\operatorname{Char} K = 0$ ist $p'_i \neq 0$ und wegen $\operatorname{Grad} p'_i < \operatorname{Grad} p_i$ gilt $p_i \nmid p'_i$. Also wird $a_i - 1 = b_i$ verlangt für $p_i \neq x$. Für $p_i = x$ reicht $a_i = b_i$.

5.5.5 a) Sei $[v_1, \ldots, v_n]$ eine Basis von V mit $Av_j = a_j v_j$. Sei $W < V$ mit $AW \leq W$ und $U \cap W = 0$, wobei W maximal bzgl. dieser Eigenschaften gewählt sei. Angenommen, $U + W < V$. Sei $v_j \notin U + W$. Daher gilt $W < \langle v_j \rangle + W$ und $A(\langle v_j \rangle + W) \leq \langle v_j \rangle + W$. Da W maximal ist, folgt $0 \neq U \cap (\langle v_j \rangle + W)$. Also gibt es ein $0 \neq u \in U$ und $w \in W$ mit $u = bv_j + w$. Wegen $U \cap W = 0$ ist $b \neq 0$, daher $bv_j = u - w \in U + W$. Dies ist ein Widerspruch. Also gilt $V = U \oplus W$.

5.6.1 a) Sei $Z_i = \langle z_i \rangle$. Wegen $\operatorname{ggT}(|Z_1|, |Z_2|) = 1$ gilt $Z_1 \cap Z_2 = \{1\}$. Sei $(z_1 z_2)^k = z_1^k z_2^k = 1$. Dann gilt $|Z_i| \mid k$, somit $|Z_1||Z_2| = \operatorname{kgV}(|Z_1|, |Z_2|) \mid k$. Dies zeigt $\operatorname{Ord} z_1 z_2 = |Z_1||Z_2|$. Somit ist $Z_1 Z_2$ zyklisch.
b) Sei $A/Z = \langle aZ \rangle$ und $Z = \langle z \rangle$. Dann gilt $a^{|A/Z|} = z^x \in Z$. Daher ist $(az^y)^{|A/Z|} = z^{x+y|A/Z|}$. Wegen $\operatorname{ggT}(|Z|, |A/Z|) = 1$ ist die Kongruenz $y|A/Z| \equiv -x \pmod{|Z|}$ lösbar. Dann gilt $(az^y)^{|A/Z|} = 1$, also insbesondere $Z \cap \langle az^y \rangle = E$. Somit ist $A = \langle z \rangle \times \langle az^y \rangle$ zyklisch nach a).

5.6.3 a) Für $p > 2$ zeigen wir durch Induktion nach k, daß $(1+px)^{rp^k} \equiv 1 + rp^{k+1}x \pmod{p^{k+2}}$. Für $k = 0$ ist die Aussage nach dem binomischen Lehrsatz richtig. Sei bereits $(1+px)^{rp^k} \equiv 1 + rp^{k+1}x + p^{k+2}f$ mit $f \in \mathbb{Z}[x]$ bewiesen. Da $\binom{p}{i}$ für $0 < i < p$ durch p teilbar ist, erhalten wir wegen $p(k+1) \geq k+3$ und $j(k+1) \geq k+3$ für $j \geq 2$ die Kongruenz $(1+px)^{rp^{k+1}} \equiv 1 + p^{k+2}(rx + pf) \equiv 1 + rp^{k+2}x \pmod{p^{k+3}}$. Durch Koeffizientenvergleich folgt $\binom{rp^k}{i} p^i \equiv 0 \pmod{p^{k+2}}$ für $i \geq 2$.
b) Aus $(1+2x)^{r2^k} = 1 + 2^{k+1}f$ folgt
$(1+2x)^{r2^{k+1}} = 1 + 2^{k+2}f + 2^{2k+2}f^2 \equiv 1 \pmod{2^{k+2}}$.

5.6.4 a) Für $ggT(m,b)=1$ ist φ mit
$\varphi(b+m\,\mathbb{Z}) = (b+p_1^{a_1}\,\mathbb{Z},\ldots,b+p_k^{a_k}\,\mathbb{Z})$ offenbar ein Monomorphismus von $E(\mathbb{Z}/m\,\mathbb{Z})$ in $E(\mathbb{Z}/p_1^{a_1}\,\mathbb{Z})\times\ldots\times E(\mathbb{Z}/p_k^{a_k}\,\mathbb{Z})$. Nach dem chinesischen Restsatz ist φ surjektiv.
b) Nach Aufgabe 5.6.3 ist $5^{2^{n-3}} = (1+4)^{2^{n-3}} \equiv 1+2^{n-1}\,(\mathrm{mod}\,2^n)$ und $5^{2^{n-2}} \equiv 1\,(\mathrm{mod}\,2^n)$. Wegen $|E(\mathbb{Z}/2^n\,\mathbb{Z})| = 2^{n-1}$ folgt
$E(\mathbb{Z}/2^n\,\mathbb{Z}) = \langle -1+2^n\,\mathbb{Z}\rangle \times \langle 5+2^n\,\mathbb{Z}\rangle$.
c) Nun ist ψ mit $\psi(a+p^n\,\mathbb{Z}) = a+p\,\mathbb{Z}$ ein Epimorphismus von $E(\mathbb{Z}/p^n\,\mathbb{Z})$ auf $E(\mathbb{Z}/p\,\mathbb{Z})$ mit $\mathrm{Kern}\,\psi = \{a+p^n\,\mathbb{Z} \mid a\equiv 1\,(\mathrm{mod}\,p)\}$. Mit Aufgabe 5.6.3 erhalten wir $(1+p)^{p^{n-2}} \equiv 1+p^{n-1}\,(\,\mathrm{mod}\,p^n)$ und $(1+p)^{p^{n-1}} \equiv 1\,(\,\mathrm{mod}\,p^n)$. Somit ist $\mathrm{Kern}\,\psi = \langle 1+p+p^n\,\mathbb{Z}\rangle$ zyklisch. Da $E(\mathbb{Z}/p\,\mathbb{Z})$ zyklisch ist, ist $E(\mathbb{Z}/p^n\,\mathbb{Z})$ nach Aufgabe 5.6.1 b) zyklisch.

5.7.3 b) Offenbar ist $W = \oplus_{j=1}^r W_j$ eine direkte Zerlegung als A-Moduln.
c) steht bereits in Aufgabe 5.5.3.
d) Es gilt $\mathrm{Kern}\,p(A) = \{\begin{pmatrix} v \\ v' \end{pmatrix} \mid p(B)v = 0 = Bp'(B)v + p(B)v'\}$. Dann ist $0 = p(B)(Bp'(B)v+p(B)v') = p(B)^2v'$. Zu $v'\in\mathrm{Kern}\,p(B)^2$ gibt es genau ein $v\in\mathrm{Kern}\,p(B)$ mit $Bp'(B)v+p(B)v' = 0$. Denn wegen $\mathrm{ggT}(xp',p)=1$ gibt es $f,g\in K[x]$ mit $1 = fxp'+gp$. Für $w\in\mathrm{Kern}\,p(B)$ folgt $w = f(B)Bp'(B)w$. Also ist $Bp'(B)$ auf $\mathrm{Kern}\,p(B)$ invertierbar. Somit ist
$\dim\mathrm{Kern}\,p(A) = \dim\mathrm{Kern}\,p(B)^2 = 2\dim\mathrm{Kern}\,p(B)$.
e) Nach d) hat A auf W_j zwei Jordankästchen, wobei eines davon nach Teil c) den Typ (p^{a_j+1},p^{a_j+1}) hat. Wegen $\dim W_j = p^{2a_j}$ hat das andere Jordankästchen den Typ (p^{a_j-1},p^{a_j-1}).

5.7.5 a) $\Rightarrow$ b) Dies haben wir bereits in Aufgabe 3.3.2 bewiesen.
b) $\Rightarrow$ c) Angenommen, $V = K[A]v_1\oplus K[A]v_2\oplus\ldots$ mit
$K[A]v_j \cong K[x]/p^{a_j}K[x]\,(j=1,2)$ und $a_1\geq a_2$. Wir definieren $B\in\mathrm{End}(V)$ durch $Bg(A)v_1 = g(A)v_2$ und $Bg(A)v_j = 0$ für $j\geq 2$. Dann ist B wohldefiniert und $AB=BA$, aber $B\notin K[A]$.
c) $\Rightarrow$ d) ist trivial, da nun $m_A = \prod_{j=1}^n p_j^{a_j} = f_A$.
d) $\Rightarrow$ a) Dies steht bereits in 5.5.7.

6.1.2 Offenbar sind $\|\,(x_i)\,\|_\infty \leq \|\,(x_i)\,\|_1 \leq\ n\,\|\,(x_i)\,\|_\infty$ und
$\|\,(x_i)\,\|_\infty \leq \|\,(x_i)\,\|_2 \leq \sqrt{n}\,\|\,(x_i)\,\|_\infty$ bestmögliche Abschätzungen. Aus $\sum_{i=1}^n |x_i|^2 \leq (\sum_{i=1}^n |x_i|)^2$ folgt $\|\,(x_i)\,\|_2 \leq \|\,(x_i)\,\|_1$. Die Schwarzsche Ungleichung liefert $(\sum_{i=1}^n |x_i|1)^2 \leq \sum_{i=1}^n |x_i|^2\cdot n$, also $\|\,(x_i)\,\|_1 \leq \sqrt{n}\,\|\,(x_i)\,\|_2$. Auch diese Abschätzungen sind bestmöglich.

6.2.4 Ist $\| A^k \| = \| A \|^k$ für alle k, so folgt mit 6.2.10, daß $\rho(A) = \lim_{k\to\infty} \sqrt[k]{\| A^k \|} = \| A \|$. Ist umgekehrt $\rho(A) = \| A \|$, so erhalten wir $\rho(A^k) = \rho(A)^k = \| A \|^k \geq \| A^k \| \geq \rho(A^k)$. Somit gilt $\| A \|^k = \| A^k \|$ für alle k.

6.2.6 Sei $S \in (\mathbb{C})_n$, so daß

$$S^{-1}AS = \begin{pmatrix} a_{11} & 0 & 0 & \dots & 0 \\ a_{21} & a_{22} & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{pmatrix}$$ Dreiecksgestalt hat. Dann ist

$\rho(A) = \max_j |a_{jj}|$. Ist T eine Diagonalmatrix mit den Diagonalelementen t_j, so hat $T^{-1}S^{-1}AST$ die Einträge $t_i^{-1}t_j a_{ij}$. Wir wählen $t_1 = 1$ und t_2 mit $|t_2^{-1}a_{21}| < \delta$. Dann t_3 so, daß $|t_3^{-1}a_{31}| < \delta$ und $|t_3^{-1}t_2 a_{32}| < \delta$. Schließlich sei $|t_n^{-1}t_j a_{nj}| < \delta$ für $j = 1, \dots, n-1$. Es folgt $\| T^{-1}S^{-1}AST \|_1 \leq \rho(A) + (n-1)\delta$. Man definiere also eine Algebrennorm $\| \cdot \|$ durch $\| B \| = \| T^{-1}S^{-1}BST \|_1$. Ist $(n-1)\delta < \varepsilon$, so ist $\| A \| \leq \rho(A) + \varepsilon$.

6.3.2 a) Sei $Av = av$ mit $|a| = 1$ und $v = (x_i)$. Dann ist $ax_i = \sum_{j=1}^n a_{ij}x_j$ und somit $|x_i| = |\sum_{j=1}^n a_{ij}x_j| \leq \sum_{j=1}^n a_{ij}|x_j|$. Wegen $A|v| = |v|$ gilt das Gleichheitszeichen. Somit haben wegen $a_{ij} > 0$ alle $x_j \neq 0$ die gleiche Richtung. Dies heißt $v = \varepsilon w$ mit $|\varepsilon| = 1$ und $w \geq 0$. Also ist $Aw = aw$. Wegen $A > 0$ und $w \geq 0$ folgt $0 < a \in \mathbb{R}$, also $|a| = 1$.
b) Wegen $A > 0$ ist $\rho(A)$ nach 6.3.4 e) ein einfacher Eigenwert. Sei $T^{-1}\rho(A)^{-1}AT = \begin{pmatrix} 1 & 0 \\ 0 & B \end{pmatrix}$. Wegen a) ist $\rho(B) < 1$. Damit folgt

$\lim_{k\to\infty} T^{-1}\rho(A)^{-k}A^kT = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

c) Sei $T = \begin{pmatrix} s_1 & \\ \vdots & * \\ s_n & \end{pmatrix}$ und $T^{-1} = \begin{pmatrix} t_1 & \dots & t_n \\ & * & \end{pmatrix}$. Setzen wir

$P = \lim_{k\to\infty} \rho(A)^{-k}A^k$, so gilt $P = T\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}T^{-1} = \begin{pmatrix} s_1t_1 & \dots & s_1t_n \\ \vdots & & \vdots \\ s_nt_1 & \dots & s_nt_n \end{pmatrix}$.

Wegen $Ay = \rho(A)y$ ist $0 < y = Py = \begin{pmatrix} s_1(t,y) \\ \vdots \\ s_n(t,y) \end{pmatrix}$, wenn wir $t = (t_i)$ setzen. Indem wir T um einen skalaren Faktor abändern, können wir $(t,y) = 1$ annehmen. Also ist $y_j = s_j$. Ferner ist

$(z_i) = (z_i)P = (t_1(y,z), \ldots, t_n(y,z)) = (t_i)$. Dies zeigt
$P = \begin{pmatrix} y_1z_1 & \ldots & y_1z_n \\ \vdots & & \vdots \\ y_nz_1 & \ldots & y_nz_n \end{pmatrix}$.

6.4.3 Aus $e^A = e^a e^N$ folgt $e^A - e^a E = NS$ mit regulärem $S = e^a(E + \frac{N}{2!} + \ldots)$. Wegen $NS = SN$ erhalten wir $(e^A - e^a E)^k = N^k S^k$. Wegen $N^{n-1} \neq 0 = N^n$ ist $(x - e^a)^n$ das Minimalpolynom von e^A.

6.5.3 Sei $V = \sum_{j=1}^n \mathbb{C}v_j$. Wir lassen A auf V operieren gemäß $Av_j = \sum_{k=1}^n a_{kj}v_k$ $(j = 1, \ldots, n)$. Sei $w_j = \sum_{k \in \mathcal{B}_j} v_k$ $(j = 1, \ldots, m)$. Wegen der Disjunktheit der $\mathcal{B}_j$ sind die w_j linear unabhängig. Es gilt $Aw_j = \sum_{k\in\mathcal{B}_j} Av_k = \sum_{l=1}^n \sum_{k\in\mathcal{B}_j} a_{lk}v_l = \sum_{r=1}^m \sum_{l\in\mathcal{B}_r} (\sum_{k\in\mathcal{B}_j} a_{lk})v_l = \sum_{r=1}^m b_{rj} \sum_{l\in\mathcal{B}_r} v_l = \sum_{r=1}^m b_{rj}w_r$. Ergänzen wir $w_1, \ldots, w_m$ zu einer Basis von V, so wird A eine Matrix der Gestalt $\begin{pmatrix} B & C \\ 0 & D \end{pmatrix}$ zugeordnet. Also ist $f_A = f_B f_D$.

6.5.4 a) Nun ist $\mathcal{B}_1 = \{1, \ldots, n\}$ und $\mathcal{B}_2 = \{n+1\}$ eine für A zulässige Partition. Das führt zu $B = \begin{pmatrix} 2/3 & 1/3 \\ 1 & 0 \end{pmatrix}$ mit $f_B = (x-1)(x+1/3)$.
b) Ist n gerade, so ist auch $\mathcal{B}_1 = \{1, 3, \ldots, n-1\}$, $\mathcal{B}_2 = \{2, 4, \ldots, n\}$ und $\mathcal{B}_3 = \{n+1\}$ zulässig. Das liefert $B = \begin{pmatrix} 0 & 2/3 & 1/3 \\ 2/3 & 0 & 1/3 \\ 1/2 & 1/2 & 0 \end{pmatrix}$ mit $f_B = (x-1)(x+1/3)(x+2/3)$.
c) Ist $3 \mid n$, so ist $\mathcal{B}_1 = \{1, 4, \ldots, n-2\}$, $\mathcal{B}_2 = \{2, 5, \ldots, n-1\}$, $\mathcal{B}_3 = \{3, 6, \ldots, n\}$ und $\mathcal{B}_4 = \{n+1\}$ zulässig. Dies führt zu $B = \begin{pmatrix} 0 & 1/3 & 1/3 & 1/3 \\ 1/3 & 0 & 1/3 & 1/3 \\ 1/3 & 1/3 & 0 & 1/3 \\ 1/3 & 1/3 & 1/3 & 0 \end{pmatrix} = 1/3F - 1/3E$ mit $F = \begin{pmatrix} 1 & \ldots & 1 \\ \vdots & & \vdots \\ 1 & \ldots & 1 \end{pmatrix}$. Da F die Eigenwerte $0, 0, 0, 4$ hat, folgt $f_B = (x-1)(x+1/3)^3$.
d) Für $n = 6$ hat A nach b) und c) die Eigenwerte $1, -1/3, -1/3, -1/3, -2/3$. Sind a, b die fehlenden Eigenwerte von A, so gilt $0 = \operatorname{Spur} A = -2/3 + a + b$ und $2 = \operatorname{Spur} A^2 = 1 + 7/9 + a^2 + b^2$. Dies führt zu $a = b = 1/3$. Somit hat A die Eigenwerte $1, -1/3, -1/3, -1/3, -2/3, 1/3, 1/3$.

6.5.6 a) Man erhält $B = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1/4 & 1/4 & 1/2 \end{pmatrix}$ mit $f_B = (x-1)(x^2-x/2-1/4)$. Somit hat B die Eigenwerte $1, (1+\sqrt{5})/4, (1-\sqrt{5})/4$. Da 1 ein zweifacher Eigenwert von A ist, erhalten wir für die fehlenden Eigenwerte a, b von A die Gleichungen $2+1/2 = \operatorname{Spur} A = 2+1/2+a+b$ und $3+1/4 = \operatorname{Spur} A^2 = 2+3/4+a^2+b^2$. Dies liefert $a = 1/2, b = -1/2$. Also hat A die Eigenwerte $1, 1, 1/2, -1/2, (1+\sqrt{5})/4, (1-\sqrt{5})/4$.

b) Im Prozeß aus 3.4.9 b) erhielten wir die Übergangsmatrix $A = \begin{pmatrix} E & 0 \\ C & B \end{pmatrix}$ mit

$B = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1/2 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 1/2 \end{pmatrix} = \begin{pmatrix} 0 & E \\ U & V \end{pmatrix}$. Da xE mit U vertauschbar ist, folgt mit 4.3.10 a), daß $f_B = \det(x(xE-V)-U) = \det \begin{pmatrix} x^2-1/2 & -x/2 \\ 0 & x^2-x/2 \end{pmatrix} = (x^2-1/2)x(x-1/2)$. Somit hat B die Eigenwerte $0, 1/2, 1/\sqrt{2}, -1/\sqrt{2}$. Daher hat A die Eigenwerte $1, 1, 0, 1/2, 1/\sqrt{2}, -1/\sqrt{2}$. Der die Konvergenzgeschwindigkeit des Prozesses bestimmende Eigenwert ist $(1+\sqrt{5})/4$ im Fall a) und $1/\sqrt{2}$ im Fall b). Wegen $(1+\sqrt{5})/4 > 1/\sqrt{2}$ konvergiert der Prozeß in b) mit Selektion schneller als der unter a).

6.5.7 a) Für $\pi, \tau \in \pi_i U$ haben wir $\sum_{\rho \in \pi_j U} a_{\pi,\rho} = \sum_{\rho \in \pi_j U} a_{\tau,\rho}$ für alle $i, j = 1, \ldots, k$ nachzuweisen. Nun ist
$\sum_{\rho \in \pi_j U} a_{\pi,\rho} = \sum_{\rho \in \pi_j U} p(\rho\pi^{-1}) = \sum_{\sigma \in \pi_j U\pi^{-1}} p(\sigma)$ und entsprechend
$\sum_{\rho \in \pi_j U} a_{\tau,\rho} = \sum_{\sigma \in \pi_j U\tau^{-1}} p(\sigma)$. Wegen $\pi, \tau \in \pi_i U$ gilt $\pi U = \pi_i U = \tau U$. Daraus folgt $U\pi^{-1} = U\tau^{-1}$, und daher $\pi_j U\pi^{-1} = \pi_j U\tau^{-1}$. Dies liefert $\sum_{\rho \in \pi_j U} a_{\pi,\rho} = \sum_{\rho \in \pi_j U} a_{\tau,\rho}$.
b) Man erhält $b_{11} = \sum_{\sigma \in \mathrm{A}_m} a_{\iota,\sigma} = \sum_{\sigma \in \mathrm{A}_m} p(\sigma) = b_{22}$ und
$b_{12} = \sum_{\sigma \notin \mathrm{A}_m} a_{\iota,\sigma} = \sum_{\sigma \notin \mathrm{A}_m} p(\sigma) = b_{21}$. Somit hat $B = (b_{ij})$ die Eigenwerte 1 und es gilt
$b_{11} + b_{22} - 1 = 2\sum_{\sigma \in \mathrm{A}_m} p(\sigma) - \sum_{\sigma \in \mathrm{S}_m} p(\sigma) = \sum_{\sigma \in \mathrm{S}_m} p(\sigma)\operatorname{sgn}(\sigma)$.

6.5.8 Die Berechnung von $a_{\sigma,\tau} = p(\tau\sigma^{-1})$ liefert die angegebene Übergangsmatrix. a) Wegen $\mathrm{r}(A) = 3$ hat A die Eigenwerte $1, 0, 0, 0, a, b$. Dabei gelten $1 + a + b = \operatorname{Spur} A = 0$ und $1 + a^2 + b^2 = \operatorname{Spur} A^2 = 1 + 1/2$. Dies leifert $a = b = -1/2$.

b) Die Komponenten der Partition zu U sind
$U = \{\iota, (12)\}, (13)U = \{(13), (123)\}, (23)U = \{(23), (132)\}$. Damit erhält man $B = \begin{pmatrix} 1/2 & 1/2 & 0 \\ 0 & 0 & 1 \\ 1/2 & 1/2 & 0 \end{pmatrix}$. Somit hat B die Eigenwerte $1, 0$ und $\operatorname{Spur} B - 1 = -1/2$.

6.5.9 Es gilt $a_{j,j+1} = \frac{n-j}{n}p$ und $a_{j,j-1} = \frac{j}{n}q$, sowie $a_{jj} = \frac{j}{n}p + \frac{n-j}{n}q$. Wegen $a_{jj} > 0$ folgt mit 6.5.10, daß $z = c(1, n\frac{p}{q}, \binom{n}{2}\frac{p^2}{q^2}, \ldots, \binom{n}{n-1}\frac{p^{n-1}}{q^{n-1}}, \frac{p^n}{q^n})$.

7.1.1 a) Die Wohldefiniertheit von $[\cdot, \cdot]$ verlangt $(v_1 + w_1, v_2 + w_2) = (v_1, v_2)$ für alle $v_j \in V$ und alle $w_j \in W$. Dies bedeutet $W \leq V^\perp$.
b) Ist $0 = [v_1 + W, v_2 + W] = (v_1, v_2)$ für alle $v_2 \in V$, so gilt $v_1 \in V^\perp$. Die Regularität von $[\cdot, \cdot]$ erzwingt dann $V^\perp = W$.

7.1.3 Offenbar gilt $(AB, C) = \operatorname{Spur} ABC = (A, BC)$. Sei $(A, B) = 0$ für alle $B \in (K)_n$ Dann ist $0 = \operatorname{Spur} AE_{ij} = \operatorname{Spur} \sum_{k,l=1}^n a_{kl}E_{kl}E_{ij} = \operatorname{Spur} \sum_{k=1}^n a_{ki}E_{kj} = \sum_{k=1}^n a_{ki}\delta_{kj} = a_{ji}$. Also gilt $A = 0$. Somit ist $(\cdot, \cdot)$ regulär.

7.1.4 a) Es gilt $U^\perp = \langle w \rangle$ mit $(w, w) = 0$. Dann ist $\langle w \rangle^\perp = U^{\perp\perp} = U$. Sei w, w' ein hyperbolisches Paar. Wegen $(w, w') = 1$ gilt $w' \notin \langle w \rangle^\perp = U$, somit $V = U \oplus \langle w' \rangle$. Da A eine Isometrie ist, folgt für alle $u \in U$, daß $0 = (u, w') - (Au, Aw') = (u, w' - Aw')$. Das zeigt $Aw' - w' \in U^\perp = \langle w \rangle$, also $Aw' = w' - cw$ mit $c \in K$. Für alle $v = u + aw'$ (mit $u \in U, a \in K$) folgt $Av = u + aw' - acw = v + c(v, w)w$. Ist umgekehrt $(w, w) = 0$, so gilt $(v_1 + c(v_1, w)w, v_2 + c(v_2, w)w) = (v_1, v_2) + c(v_2, w)(v_1, w) + c(v_1, w)(w, v_2) = (v_1, v_2)$. Somit ist die Abbildung $Av = v + c(v, w)w$ eine Isometrie.
b) Sei U regulär und $\operatorname{Char} K \neq 2$. Dann ist $V = U \perp \langle w \rangle$ mit $U^\perp = \langle w \rangle$. Aus $AU = U$ folgt $AU^\perp = U^\perp$, somit $Aw = aw$ mit $a \in K^*$. Da $U^\perp$ regulär ist, ist $(w, w) \neq 0$. Daher ist $0 \neq (w, w) = (Aw, Aw) = (aw, aw) = a^2(w, w)$. Wegen $A \neq E$ ist $a = -1$. Also ist $Au = u$ für alle $u \in U$ und $Aw = -w$. Dies zeigt $Av = v - \frac{2(v,w)}{(w,w)}w$ für alle $v \in V$.
c) Sei nun U nicht regulär. Dann ist $U^\perp = \langle w \rangle \leq U$, also $(w, w) = 0$. Sei w, w' ein hyperbolisches Paar, also $w' \notin \langle w \rangle^\perp = U$. Somit gilt $V = U \oplus \langle w' \rangle$. Für alle $u \in U$ ist $0 = (u, w') - (Au, Aw') = (u, w' - Aw')$. Dies heißt $Aw' - w' = cw \in U^\perp = \langle w \rangle$. Wegen $(w, w') = (w', w) = 1$ gilt auch $0 = (w', w') = (Aw', Aw') = 2c(w, w') = 2c$. Wegen $\operatorname{Char} K \neq 2$ folgt $c = 0$, entgegen der Annahme $A \neq E$.

d) Da U regulär ist, gilt $V = U \perp U^\perp = U \perp \langle w\rangle$ mit $(w,w) \neq 0$. Wegen $Gw \in U^\perp$ ist $Gw = aw$ mit $a \in K$. Dabei gilt $0 \neq (w,w) = (Gw, Gw) = a(\alpha a)(w,w)$. Daher ist $Gw = aw$ mit $a(\alpha a) = 1$. Man sieht leicht, daß jede solche Abbildung eine Isometrie ist.
e) Nun gilt wie vorher $U = \langle w\rangle^\perp$ mit $(w,w) = 0$, also $w \in U$. Sei wieder w, w' ein hyperbolisches Paar. Wie oben folgt $V = U \oplus \langle w'\rangle$ und $Aw' - w' = cw \in U^\perp$. Dabei gilt $0 = (w',w') = (Aw', Aw') = (cw + w', cw + w') = c(w,w') + (\alpha c)(w',w) = c + \alpha c$. Dann ist $Av = v + c(v,w)w$ für alle $v \in V$. Ist umgekehrt $0 = (w,w) = c + \alpha c$, so gilt für alle $v_j \in V$, daß $(v_1 + c(v_1,w)w, v_2 + c(v_2,w)) = (v_1,v_2) + \alpha(c(v_2,w))(v_1,w) + c(v_1,w)(w,v_2) = (v_1,v_2) + (v_1,w)(w,v_2)(\alpha c + c) = (v_1,v_2)$. Somit wird durch $Av = v + c(v,w)w$ eine Isometrie definiert.

7.3.3 a) Seien $W_1 = \langle w_1, \ldots, w_m\rangle$ und $W_2 = \langle w_1', \ldots, w_m'\rangle$ isotrope Unterräume von V. Nach 7.3.4 gibt es isotrope Unterräume $W_1' = \langle u_1, \ldots, u_m\rangle$ und $W_2' = \langle u_1', \ldots, u_m'\rangle$ mit $V = W_1 \oplus W_1' = W_2 \oplus W_2'$ und $(w_i, u_j) = (w_i', u_j') = \delta_{ij}$. Durch $Gw_i = w_i'$, $Gw_i' = w_i$, $Gu_i = u_i'$ und $Gu_i' = u_i$ für $i = 1, \ldots, m$ wird dann ein $G \in \mathrm{O}(V)$ mit $GW_1 = W_2$ definiert.
b) Sei $V = W_1 \oplus W_1'$ wie in a). Sei $G \in \mathrm{O}(V)$ mit $Gw_i = \sum_{j=1}^m a_{ij} w_j$ und $Gu_k = \sum_{l=1}^m (c_{kl} w_l + b_{kl} u_l)$. Es folgt $\delta_{jk} = (w_j, u_k) = (Gw_j, Gu_k) = (\sum_{j=1}^m a_{ij} w_j, \sum_{l=1}^m (c_{kl} w_l + b_{kl} u_l)) = \sum_{j=1}^m a_{ij} b_{kj}$. Schreiben wir die Matrix zu G in der Gestalt $\begin{pmatrix} A & 0 \\ C & B \end{pmatrix}$, so gilt also $AB^t = E$, und somit $\det \begin{pmatrix} A & 0 \\ C & B \end{pmatrix} = \det A \det B^t = 1$.
c) folgt unmittelbar aus b).
d) Da W_j isotrop ist, gilt $W_j \leq W_j^\perp$. Wegen $\dim W_j^\perp = 2m - \dim W_j = \dim W_j$ folgt $W_j^\perp = W_j$. Daher ist $(W_1 + W_2)^\perp = W_1^\perp \cap W_2^\perp = W_1 \cap W_2$. Sei $\dim(W_1 \cap W_2) = m - r$. Dann ist $\dim(W_1 + W_2) = \dim W_1 + \dim W_2 - \dim(W_1 \cap W_2) = 2m - (m-r) = m + r$. Sei $W_1 + W_2 = (W_1 \cap W_2) \perp U$ mit regulärem U und $\dim U = 2r$. Wegen $W_j = (W_1 \cap W_2) \perp (W_j \cap U)$ hat U isotrope Unterräume $W_j \cap U$ der Dimension r. Wegen $\dim U = 2r$ ist $\operatorname{ind} U = r$. Dabei gilt $(W_1 \cap U) \cap (W_2 \cap U) = (W_1 \cap W_2) \cap U = 0$, daher $U = (W_1 \cap U) \oplus (W_2 \cap U)$. Sei $W_1 \cap U = \langle w_1, \ldots, w_r\rangle$. Dann gibt es $v_j \in U$ mit $(w_i, v_j) = \delta_{ij}$. Ist $v_j = s_j + w_j'$ mit $s_j \in W_1 \cap U$ und $w_j' \in W_2 \cap U$, so folgt $(w_i, w_j') = \delta_{ij}$. Somit gilt $U = \langle w_1, w_1'\rangle \perp \ldots \perp \langle w_r, w_r'\rangle$. Sei $V = V_0 \perp U$. Wir definieren eine Isometrie G von V durch $G_{V_0} = E$, $Gw_i = w_i'$, $Gw_i' = w_i$. Dann gilt $\det G = (-1)^r$. Wegen $W_1 \cap W_2 \leq U^\perp = V_0$ ist $GW_1 = (W_1 \cap W_2) \perp \langle w_1', \ldots, w_r'\rangle = W_2$. Es folgt $\dim(W_1 \cap W_2) = m - r \equiv \begin{cases} m \pmod 2 & \text{falls } G \in \mathrm{SO}(V) \\ m - 1 \pmod 2 & \text{falls } G \notin \mathrm{SO}(V). \end{cases}$

e) Sei $0 \neq v \in V$ mit $(v,v) = 0$. Dann gibt es einen isotropen Unterraum U von V mit $v \in U$ und $\dim U = 2$. Somit gilt $V = \langle w_1, w_1' \rangle \perp \langle w_2, w_2' \rangle$ mit hyperbolischen Paaren w_1, w_1' und w_2, w_2' und $w_1 = v$. Sei $w \notin \langle w_1 \rangle$. Genau dann ist $\langle w_1, w \rangle$ isotrop, wenn $(w_1, w) = (w, w) = 0$. Daß heißt einmal $w \in \langle w_1 \rangle^\perp = \langle w_1, w_2, w_2' \rangle$. Ist $w = a_1 w_1 + a_2 w_2 + a_3 w_2'$, so ist ferner $0 = (w,w) = 2a_2 a_3$, also $a_2 = 0$ oder $a_3 = 0$. Somit liegt $v = w_1$ nur in den isotropen Unterräumen $\langle w_1, w_2 \rangle$ und $\langle w_1, w_2' \rangle$. Wegen $\dim(\langle w_1, w_2 \rangle \cap \langle w_1, w_2' \rangle) = 1$ liegen $\langle w_1, w_2 \rangle$ und $\langle w_1, w_2' \rangle$ nach d) in verschiedenen Bahnen von $\mathrm{SO}(V)$. Die restlichen Aussagen folgen sofort aus Teil d).

7.3.5 Sei W ein maximaler isotroper Unterraum von V mit $U \leq W$. Dann ist $\dim W = \operatorname{ind} V$. Wegen $W \leq U^\perp$ ist W/U ein bzgl. $[\cdot,\cdot]$ isotroper Unterraum von $U^\perp/U$. Dies zeigt $\operatorname{ind} U^\perp/U \geq \dim W/U = \operatorname{ind} V - \operatorname{ind} U$. Sei umgekehrt W'/U ein maximaler bzgl. $[\cdot,\cdot]$ isotroper Unterraum von $U^\perp/U$. Dann ist W' isotrop bzgl. $(\cdot,\cdot)$, und es folgt
$\operatorname{ind} U^\perp/U = \dim W'/U = \dim W' - \dim U \leq \operatorname{ind} V - \dim U$. Somit gilt $\operatorname{ind} U^\perp/U = \operatorname{ind} V - \dim U$.

7.3.6 Ist $\dim V$ ungerade, so hat G trivialerweise einen reellen Eigenwert. Sei also $\dim V = n$ gerade und $\operatorname{ind} V = m$ ungerade. Nach 5.4.20 gibt es ein $U \leq V$ mit $GU = U$ und $1 \leq \dim U \leq 2$. Wegen $GU = U$ ist auch $GU^\perp = U^\perp$ und $G(U \cap U^\perp) = U \cap U^\perp$. Ist $\dim U = 1$ oder $\dim(U \cap U^\perp) = 1$, so sind wir fertig. Sei also $\dim U = 2$ und $U \cap U^\perp = 0$ oder $U \leq U^\perp$.
Fall 1: Sei $U \leq U^\perp$. Durch $[w_1 + U, w_2 + U] = (w_1, w_2)$ für $w_j \in U^\perp$ wird nach Aufgabe 7.1.1 wegen $U^{\perp\perp} = U$ auf $U^\perp/U$ ein reguläres Skalarprodukt definiert, und wegen Aufgabe 7.3.5 gilt $\operatorname{ind} U^\perp/U = \operatorname{ind} V - \dim U = m - 2 \not\equiv 0 \,(\mathrm{mod}\, 2)$. Dann ist $\overline{G}$ mit $\overline{G}(w + U) = Gw + U$ eine Isometrie von $U^\perp/U$. Gemäß Induktionsannahme hat $\overline{G}$ einen reellen Eigenwert. Nach dem Kästchensatz ist $f_{\overline{G}}$ ein Teiler von f_G. Also hat auch G einen reellen Eigenwert.
Fall 2: Sei $U \cap U^\perp = 0$, somit $V = U \perp U^\perp$. Ist U eine hyperbolische Ebene mit hyperbolischem Paar u_1, u_2, so sind wegen $(x_1 u_1 + x_2 u_2, x_1 u_1 + x_2 u_2) = 2x_1 x_2$ nur die Vielfachen von u_1 und u_2 isotrop. Also gilt $Gu_1 = au_1$ und $Gu_2 = a^{-1}u_2$ oder $Gu_1 = au_2$ und $Gu_2 = a^{-1}u_1$. Im ersten Fall ist a ein reeller Eigenwert von G, im zweiten ist $G(u_1 + au_2) = u_1 + au_2$. Sei weiterhin U von der Signatur $(1,1)$ oder $(-1,-1)$. Sei $(1, \ldots, 1, -1, \ldots, -1)$ mit r Einsen und s Minus-Einsen die Signatur von V. Dann ist $n = r + s$ gerade und $m = \operatorname{ind} V = \min(r,s)$. Also sind r und s ungerade. Hat U die Signatur $(1,1)$, so hat $U^\perp$ die Signatur $(r-2, s)$. Dann ist $\operatorname{ind} U^\perp$ ungerade. Hat U

die Signatur $(-1,-1)$, so ist $\operatorname{ind} U^\perp = \min(r, s-2)$ ebenfalls ungerade. Per Induktion hat G auf $\mathrm{U}^\perp$ einen reellen Eigenwert.

7.4.1 Seien $c, c' \in C$. Aus $\mathrm{wt}(c+c') = \mathrm{wt}(c) + \mathrm{wt}(c') - 2|\,\mathrm{T}(c) \cap \mathrm{T}(c')|$ folgt wegen der 4-Dividierbarkeit von C, daß $2 \mid |\,\mathrm{T}(c) \cap \mathrm{T}(c')|$. Also ist $(c, c') = |\,\mathrm{T}(c) \cap \mathrm{T}(c')|1 = 0$.

7.4.4 a) Mit 7.4.13 erhalten wir
$0 \le A_{n-k+2} = \binom{n}{k-2}(q^2 - 1 - (n-k+2)(q-1)) =$
$\binom{n}{k-2}(q-1)(q+1-(n-k+2))$, woraus die Behauptung unmittelbar folgt.
b) Wegen 7.4.10 ist auch $C^\perp$ ein MDS-Code. Da $\dim C^\perp = n-k \ge n-(n-2) = 2$ ist, folgt aus a) nun $q \ge n-(n-k)+1 = k+1$.

7.4.6 Für $w \in K^n$ hängt $\sum_{\substack{v \in K^n \\ \mathrm{wt}(v)=j}} (-1)^{(v,w)}$ offenbar nur von $\mathrm{wt}(w)$ ab, und ist gleich $K_j^n(i)$, falls $\mathrm{wt}(w) = i$ ist. Seien $w_i \in K^n$ mit $\mathrm{wt}(w_i) = i$ für $i = 0, \ldots, n$. Es folgt
$0 \le \sum_{\substack{v \in K^n \\ \mathrm{wt}(v)=j}} \left(\sum_{c \in C} (-1)^{(v,c)}\right)^2 = \sum_{\substack{v \in K^n \\ \mathrm{wt}(v)=j}} \sum_{c,c' \in C} (-1)^{(v,c+c')}$
$= \sum_{c,c' \in C} \sum_{\substack{v \in K^n \\ \mathrm{wt}(v)=j}} (-1)^{(v,c+c')} = \sum_{i=0}^n \sum_{\substack{c,c' \in C \\ \mathrm{d}(c,c')=i}} \sum_{\substack{v \in K^n \\ \mathrm{wt}(v)=j}} (-1)^{(v,c+c')}$
$= \sum_{i=0}^n D_i \sum_{\substack{v \in K^n \\ \mathrm{wt}(v)=j}} (-1)^{(v,w_i)} = \sum_{i=0}^n D_i K_j^n(i)$.

7.5.2 Ist $(Sw, w) = -(w,w) < 0$, so gilt $Sw \sim w$, also $S \in L^+$. Ist hingegen $(Sw, w) = -(w,w) > 0$, so gilt $Sw \not\sim w$, also $S \notin L^+$.

8.2.1 a) Sei $\dim V = 2$ und seien a_1, a_2 die Eigenwerte von A mit $|a_1| \le |a_2| = \rho(A)$. Wir wählen eine Orthonormalbasis von V derart, daß A die Dreiecksmatrix $\begin{pmatrix} a_1 & 0 \\ b & a_2 \end{pmatrix}$ zugeordnet ist. Dann ist
$\begin{pmatrix} a_1 & 0 \\ b & a_2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} a_1 x_1 \\ b x_1 + a_2 x_2 \end{pmatrix}$. Wegen $|a_1| = \rho(A) = \| A \|$ zeigt dies $|a_1 x_1|^2 + |b x_1 + a_2 x_2|^2 \le \| A \|^2 (|x_1|^2 + |x_2|^2) = |a_1|^2(|x_1|^2 + |x_2|^2)$. Also folgt $|b x_1 + a_2 x_2|^2 \le |a_1|^2 |x_2|^2$ für alle x_1, x_2. Dies erzwingt $b = 0$, und A ist normal.
b) Sei B eine nichtnormale Matrix vom Typ (m,m) mit $m \ge 2$. Ferner sei $a \in \mathbb{C}$ mit $\| B \| \le |a|$. Sei schließlich $A = \begin{pmatrix} a & 0 \\ 0 & B \end{pmatrix}$. Dann ist A nicht normal. Für $v = \begin{pmatrix} x \\ w \end{pmatrix}$ folgt $Av = \begin{pmatrix} ax \\ Bw \end{pmatrix}$, also $\| Av \|^2 = |ax|^2 + (Bw, Bw) \le |ax|^2 + \| B \|^2 (w,w) \le |a|^2(|x|^2 + (w,w)) = |a|^2 (v,v)$.

Wegen $\rho(B) \leq \| B \| \leq |a|$ folgt $\rho(A) = |a|$, also $\| Av \|^2 \leq \rho(A)^2 \| v \|^2$. Dies zeigt $\| A \| = \rho(A)$.

8.2.2 a) Wir bilden die hermiteschen Abbildungen $H = AA^* = A^*A$. Wegen $H^2 = A^{*2}A^2$ ist $0 = (H^2v, v) = (Hv, Hv)$, somit $A^*Av = Hv = 0$. Daher ist $0 = (A^*Av, v) = (Av, Av)$, somit $Av = 0$.
b) Offenbar ist $g(A)$ normal. Ist $g(A)^2 = 0$, so folgt mit a), daß $g(A) = 0$ ist.
c) Sei $h = (x-a)^2k$ mit $h(A) = 0$. Setzen wir $g = (x-a)k$, so gilt $g(A)^2 = 0$, nach b) also auch $g(A) = 0$. Daher hat m_A keine mehrfache Nullstelle. Also ist A nach 5.5.3 diagonalisierbar.

8.2.3 a) Nach 5.4.20 existiert ein Unterraum V_1 von V mit $AV_1 \leq V_1$ und $1 \leq \dim V_1 \leq 2$. Nach 8.2.6 gilt $AV_1^\perp \leq V_1^\perp$, und die Einschränkung von A auf $V_1^\perp$ ist wieder normal. Also folgt die Behauptung durch Induktion nach $\dim V$.
b) Sei $\dim V_j = 2$ und sei $[v_{j_1}, v_{j_2}]$ irgendeine Orthonormalbasis von V_j. Sei $Av_{j_1} = av_{j_1} + bv_{j_2}, Av_{j_2} = cv_{j_1} + dv_{j_2}$. Nach 8.2.2 ist dann
$A^*v_{j_1} = av_{j_1} + cv_{j_2}, A^*v_{j_2} = bv_{j_1} + dv_{j_2}$. Wegen $AA^* = A^*A$ folgt
$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.
Dies führt zu $b^2 = c^2$ und $ac + bd = ab + cd$.
Fall 1: Sei $b = -c$. Da V_j bzgl. A unzerlegbar ist, ist $b \neq 0$. Somit folgt $b(-a + d) = b(a - d)$, also $a = d$.
Fall 2: Sei $b = c$. Dann hat
$\det(xE - \begin{pmatrix} a & b \\ b & d \end{pmatrix}) = (x - \frac{a+d}{2})^2 - (\frac{(a-d)^2}{4} + b^2)$ reelle Nullstellen. Somit enthält V_j einen Eigenvektor v'_{j_1} von A zu einem reellen Eigenwert. Da die Einschränkung von A auf V_j normal ist, folgt $V_j = \langle v'_{j_1} \rangle \perp \langle v'_{j_2} \rangle$ mit $A\langle v'_{j_2} \rangle \leq \langle v'_{j_2} \rangle$, entgegen der Unzerlegbarkeit von V_j.

8.2.4 Ist $A^* = f(A)$ mit einem Polynom f, so gilt $A^*A = AA^*$. Sei zuerst $K = \mathbb{C}$. Nach 8.2.7 gibt es eine Orthonormalbasis $[v_1, \ldots, v_n]$ von V mit $Av_j = a_jv_j$. Wegen 8.2.2 ist $A^*v_j = \overline{a_j}v_j$. Wir wählen $f \in \mathbb{C}[x]$ vermöge Interpolation (siehe 5.2.11) so, daß $f(a_j) = \overline{a_j}$ für $j = 1, \ldots, n$. Dann ist $A^* = f(A)$.
Sei nun $K = \mathbb{R}$. Nach Aufgabe 8.2.3 gehört zu A bzgl. einer geeigneten Orthonormalbasis von V eine Matrix der Gestalt $A_0 = \begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_r \end{pmatrix}$,

wobei entweder $A_j = (a_j)$ oder $A_k = \begin{pmatrix} a_k & b_k \\ -b_k & a_k \end{pmatrix}$ mit $b_k \neq 0$ gilt. Dabei ist $A_0^t = \begin{pmatrix} A_1^t & & \\ & \ddots & \\ & & A_r^t \end{pmatrix}$. Wir suchen ein Polynom f mit $f(A_j) = A_j^t$. Für $A_j = (a_j)$ verlangt dies $f \equiv a_j \,(\mathrm{mod}\,(x - a_j))$. Für $A_k = \begin{pmatrix} a_k & b_k \\ -b_k & a_k \end{pmatrix}$ gilt $A_k^t = -A_k + 2a_k E$. Für diese k fordern wir also $f \equiv -x + 2a_k \,(\mathrm{mod}\, f_k)$, wobei $f_k = (x - a_k)^2 + b_k^2$ das wegen $b_k \neq 0$ in $\mathbb{R}[x]$ irreduzible charakteristische Polynom von A_k ist. Die Polynome $x - a_j, (x - a_k)^2 + b_k$ sind teilerfremd oder gleich. Nach dem chinesischen Restsatz 5.2.10 können wir daher die simultanen Kongruenzen $f \equiv a_j \,(\mathrm{mod}\,(x - a_j))$ und $f \equiv -x + 2a_k \,(\mathrm{mod}\, (x - a_k)^2 + b_k^2)$ für die benötigten j und k lösen. Daher folgt $f(A_0) = \begin{pmatrix} f(A_1) & & \\ & \ddots & \\ & & f(A_r) \end{pmatrix} = \begin{pmatrix} A_1^t & & \\ & \ddots & \\ & & A_r^t \end{pmatrix} = A_0^t$.

8.2.8 Sei $[v_1, \ldots, v_n]$ eine Orthonormalbasis von V mit $Av_j = a_j v_j$. Sei ferner $(A+B)v = cv$ mit $v = \sum_{j=1}^n x_j v_j$. Dann ist $Bv = \sum_{j=1}^n x_j(c - a_j)v_j$. Dies liefert
$\sum_{j=1}^n |x_j|^2 |c - a_j|^2 = (Bv, Bv) \leq \| B \|^2 (v, v) = \| B \|^2 \sum_{j=1}^n |x_j|^2$. Daher gibt es ein j mit $|c - a_j| \leq \| B \|$.

8.3.2 a) Es gilt $P = \lim_{k\to\infty} P_k$ mit
$\| P_k \| = \| \frac{1}{k} \sum_{j=0}^{k-1} A^j \| \leq \frac{1}{k} \sum_{j=0}^{k-1} \| A \|^j \leq 1$. Also ist $\| P \| \leq 1$, und somit $P = P^*$ nach 8.3.7. Mit 6.2.8 folgt
$V = \mathrm{Bild}\, P \perp \mathrm{Kern}\, P = \mathrm{Kern}(A - E) \perp \mathrm{Bild}(A - E)$.
b) Wegen $\| A^* \| = \| A \| \leq 1$ gilt auch $P = P^* = \lim_{k\to\infty} \sum_{j=0}^{k-1} \frac{1}{k} A^{*j}$ und daher $\mathrm{Kern}(A - E) = \mathrm{Kern}(A^* - E)$, $\mathrm{Bild}(A^* - E) = \mathrm{Bild}(A - E)$.

8.3.3 a) Es gilt $(A_{u,w}v, z) = ((v, u)w, z) = (v, u)(w, z)$ und $(v, A_{w,u}z) = (v, (z, w)u) = \overline{(z, w)}(v, u)$, somit $A_{u,w}^* = A_{w,u}$.
b) Für $v \in \langle u \rangle^\perp$ ist $A_{u,w}v = 0$. Sei $w = w' + su$ mit $w' \in \langle u \rangle^\perp$. Dann ist $A_{u,w}u = (u, u)w = (u, u)(w' + su)$. Dabei ist $(w, u) = s(u, u)$. Also gilt $A_{u,w}u = w'' + (w, u)u$ mit $w'' \in \langle u \rangle^\perp$. Daher hat $A_{u,w}$ die Eigenwerte $0, \ldots, 0, (w, u)$.
c) Es gilt
$(A_{u,w}v, A_{u,w}v) = ((v, u)w, (v, u)w) = |(v, u)|^2 (w, w) \leq \| v \|^2 \| u \|^2 \| w \|^2$.

Dies zeigt $\| A_{u,w} \| \leq \| u \| \| w \|$. Dabei ist $(A_{u,w}u, A_{u,w}u) = (u,u)^2(w,w)$, somit $\| A_{u,w}u \| = \| u \|^2 \| w \|$. Also ist $\| A_{u,w} \| = \| u \| \| w \|$.
d) Wir haben $A^*_{u,w}A_{u,w}v = A_{w,u}(v,u)w = (v,u)(w,w)u$ und $A_{u,w}A^*_{u,w}v = A_{u,w}(v,w)u = (v,w)(u,u)w$. Die Normalität von $A_{u,w}$ fordert insbesondere für $v = u$, daß $(u,u)(w,w)u = (u,w)(u,u)w$. Somit ist $u = aw$ mit $a \in \mathbb{C}$. Ist $u = aw$, so folgt andererseits $(v,u)(w,w)u = \overline{a}(v,w)(w,w)au = (v,w)(u,u)w$. Somit ist $A^*_{u,w}A_{u,w} = A_{u,w}A^*_{u,w}$. Genau dann ist A hermitesch, wenn außerdem der Eigenwert $(w,u) = \overline{a}(w,w)$ reell ist, wenn also a reell ist.

8.3.5 Seien $b_1 \geq \ldots \geq b_n$ die Eigenwerte von A^*A. Nach 8.3.15 ist $\| A \|^2 = b_1 \leq b_1 + \ldots + b_n = \| A \|_2^2$.
a) Sei zuerst $\| A \|^2 = \| A \|_2^2$. Wegen $b_j \geq 0$ ist dann $b_2 = \ldots = b_n = 0$. Da die hermitesche Abbildung A^*A diagonalisierbar ist, folgt
$\dim \operatorname{Kern} A^*A \geq n-1$. Für $v \in \operatorname{Kern} A^*A$ gilt $(Av, Av) = (v, A^*Av) = 0$. Daher ist $\dim \operatorname{Kern} A \geq \dim \operatorname{Kern} A^*A \geq n-1$ und $\mathrm{r}(A) \leq 1$.
Sei umgekehrt $\mathrm{r}(A) \leq 1$. Sei $[w_1, \ldots, w_n]$ eine Orthonormalbasis von V mit $\langle w_1, \ldots, w_{n-1} \rangle \leq \operatorname{Kern} A$. Dann ist $Aw_j = 0$ für $j \leq n-1$. Sei
$Aw_n = \sum_{k=1}^n b_{kn} w_k$. Es folgt $\| A \|_2^2 =$
$\operatorname{Spur} A^*A = \sum_{k=1}^n |b_{kn}|^2 = (Aw_n, Aw_n) \leq \| A \|^2 \, (w_n, w_n) = \| A \|^2$, also $\| A \| = \| A \|_2$.
b) Ist $\| A \|^2 = \frac{1}{n} \| A \|_2^2$, so gilt $b_1 = \ldots = b_n$. Also hat A^*A den n-fachen Eigenwert b_1. Daher folgt $A^*A = b_1 E$. Ist $0 = b_1 = \| A \|^2$, so ist $A = 0$. Dann ist unsere Behauptung mit $c = 0$ erfüllt. Ist $b_1 = c^2 > 0$ mit $0 < c \in \mathbb{R}$, so ist $U = c^{-1}A$ wegen $U^*U = c^{-2}A^*A = E$ unitär.
Sei umgekehrt $A = cU$ mit $0 \leq c \in \mathbb{R}$ und unitärem U. Dann ist
$\| A \| = |c| \, \| U \| = |c|$. Ferner ist $\| A \|_2^2 = |c|^2 \, \| U \|_2^2 = |c|^2 \operatorname{Spur} U^*U = |c|^2 \operatorname{Spur} E = \| A \|^2 \, n$. In diesem Fall gilt also $\| A \| = \frac{1}{\sqrt{n}} \| A \|_2$.

8.3.9 a) Sei $[v_1, \ldots, v_n]$ eine Orthogonalbasis von V mit $Av_j = a_j v_j$. Wegen $A \geq 0$ gilt $0 \leq a_j \in \mathbb{R}$ nach 8.3.14. Seien $0 \leq b_j \in \mathbb{R}$ mit $b_j^m = a_j$. Wir definieren B durch $Bv_j = b_j v_j$. Dann ist $B \geq 0$ und $B^m = A$. Ist $f \in \mathbb{R}[x]$ mit $f(a_j) = b_j$ $(j = 1, \ldots, n)$, so gilt $B = f(A)$.
Zum Beweis der Eindeutigkeit von B gehen wir wie folgt vor: Seien $a_1, \ldots, a_r$ die verschiedenen Eigenwerte von A. Setzen wir $V_j = \operatorname{Kern}(A - a_j E)$, so folgt $V = V_1 \perp \ldots \perp V_r$. Sei nun $H \geq 0$ mit $H^m = A$. Wegen $HA = AH$ gilt für $v_j \in V_j$ dann $AHv_j = HAv_j = a_j Hv_j$. Dies zeigt $HV_j \leq V_j$. Da die Einschränkung von H auf V_j hermitesch ist, gibt es eine Orthonormalbasis $[v_{j_1}, \ldots, v_{j_{n_j}}]$ von V_j mit $Hv_{j_k} = h_{j_k} v_{j_k}$. Wegen $H \geq 0$ gilt dabei $0 \leq h_{j_k} \in \mathbb{R}$. Ferner ist wegen $H^m = A$ auch $h_{j_k}^m = a_j$ $(k = 1, \ldots, n_j)$. Dies

erzwingt $h_{j_k} = b_j$, also $H = B$.
b) Wegen $B = f(A)$ folgt aus $AC = CA$ auch $BC = CB$.

8.3.12 a) Wegen $P_j = P_j^*$ ist $\| P_j \| \leq 1$, also $\| P_1P_2 \| \leq \| P_1 \| \| P_2 \| \leq 1$. Zum Beweis der Existenz von $\lim_{k\to\infty}(P_1P_2)^k$ muß man nach 6.2.12 nur zeigen, daß P_1P_2 keinen von 1 verschiedenen Eigenwert vom Betrag 1 hat. Sei also $P_1P_2v = av$ mit $|a| = 1$ und $v \neq 0$. Wegen $\| P_j \| \leq 1$ gilt dann $\| P_2v \| \geq \| P_1P_2v \| = |a| \| v \| = \| v \| \geq \| P_2v \|$. Also ist $\| P_2v \| = \| v \|$, somit $v \in \operatorname{Bild} P_2$. Aus $\| v \| = \| P_1P_2v \| = \| P_1v \|$ folgt ebenso $v \in \operatorname{Bild} P_1$, und daher $P_1P_2v = v$. Nun ist $P = \lim_{k\to\infty}(P_1P_2)^k$ eine Projektion mit $\| P \| \leq 1$. Daher ist $P = P^*$. Ist $v \in \operatorname{Bild} P_1 \cap \operatorname{Bild} P_2$, so ist $P_1P_2v = v$, also $Pv = v$. Sei umgekehrt $Pv = v$. Dann ist $v = Pv = P_1P_2Pv = P_1P_2v$. Wie oben folgt $v = P_1v = P_2v$. Insgesamt zeigt dies $\operatorname{Bild} P = \operatorname{Bild} P_1 \cap \operatorname{Bild} P_2$. Wegen $P^* = P$ folgt schließlich
$\operatorname{Kern} P = (\operatorname{Bild} P)^\perp = (\operatorname{Bild} P_1)^\perp + (\operatorname{Bild} P_2)^\perp = \operatorname{Kern} P_1 + \operatorname{Kern} P_2$.
b) Wegen $\| \frac{1}{2}(P_1+P_2) \| \leq 1$ haben wir abermals nur zu zeigen, daß 1 der einzige Eigenwert von $\frac{1}{2}(P_1 + P_2)$ vom Betrag 1 ist. Sei also $\frac{1}{2}(P_1 + P_2)v = av$ mit $|a| = 1$ und $v \neq 0$. Dann ist $\frac{1}{2}[(P_1, v) + (P_2v, v)] = a(v, v)$. Wegen $0 \leq (P_jv, v) \in \mathbb{R}$ folgt $a = 1$. Somit existiert $Q = \lim_{k\to\infty}(\frac{1}{2}(P_1 + P_2))^k$, und es gilt $Q^2 = Q = Q^*$. Für $v \in \operatorname{Bild} P_1 \cap P_2$ gilt $P_1v = P_2v = v$, also $Qv = v$.
Sei umgekehrt $Qv = v$. Dann ist $v = Qv = \frac{1}{2}(P_1+P_2)Qv = \frac{1}{2}(P_1+P_2)v$. Aus $2(v, v) = (P_1, v) + (P_2v, v)$ und $0 \leq (P_jv, v) \leq (v, v)$ folgt $(P_jv, v) = (v, v)$, also $P_jv = v$. Somit ist $\operatorname{Bild} Q = \operatorname{Bild} P_1 \cap \operatorname{Bild} P_2$. Wegen $Q^* = Q$ folgt wie in a), daß $\operatorname{Kern} Q = \operatorname{Kern} P_1 + \operatorname{Kern} P_2$. Somit ist
$\lim_{k\to\infty}(\frac{1}{2}(P_1 + P_2))^k = P = \lim_{k\to\infty}(P_1P_2)^k$.

8.3.13 Sei $P^2 = P$ und $0 \neq P \neq E$. Sei $[v_1, \ldots, v_n]$ eine Orthonormalbasis von V mit $\operatorname{Bild} P = \langle v_1, \ldots, v_m \rangle$. Zu P gehört dann die (m, m)-Matrix $\begin{pmatrix} E & A \\ 0 & 0 \end{pmatrix}$.Zu PP^* gehört daher die Matrix $\begin{pmatrix} E & A \\ 0 & 0 \end{pmatrix}\begin{pmatrix} E & 0 \\ \overline{A}^t & 0 \end{pmatrix} = \begin{pmatrix} E + A\overline{A}^t & 0 \\ 0 & 0 \end{pmatrix}$. Ist a der größte Eigenwert von $A\overline{A}^t$, so ist $1 + a$ der größte Eigenwert von PP^*. Also folgt $\| P \|^2 = 1 + a$. (Ist insbesondere $A \neq 0$, also $P \neq P^*$, so folgt $\| P \| > 1$.) Zu $(E - P)^*(E - P)$ gehört die Matrix $\begin{pmatrix} 0 & 0 \\ -\overline{A}^t & E \end{pmatrix}\begin{pmatrix} 0 & -A \\ 0 & E \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & E + \overline{A}^tA \end{pmatrix}$. Nach 5.4.6 haben $A\overline{A}^t$ und $\overline{A}^tA$ dieselben Eigenwerte, abgesehen von der 0. Somit ist a auch der größte Eigenwert von $\overline{A}^tA$, womit $\| E - P \|^2 = 1 + a = \| P \|^2$ folgt.

8.4.1 Seien $c_1, \ldots, c_n$ die Eigenwerte von AB. Nach 5.4.6 sind dies auch die Eigenwerte von BA. Dann gilt
$\sum_{j=1}^{n} |c_j|^2 = \| AB \|_2^2$ (nach 8.4.5 c), da AB normal)
$= \mathrm{Spur}(AB)^*(AB)$
$= \mathrm{Spur}(B^*A^*AB)$
$= \mathrm{Spur}(B^*AA^*B)$ (da A normal)
$= \mathrm{Spur}(A^*BB^*A)$
$= \mathrm{Spur}(A^*B^*BA)$ (da B normal)
$= \mathrm{Spur}(BA)^*(BA) = \| BA \|_2^2$.
Nach 8.4.5 c) ist daher BA normal.

8.5.3 b) Sei T die Diagonalmatrix mit Diagonaleinträgen t_j, wobei $t_1 = 1$ und t_j rekursiv durch $(t_{j+1}t_j^{-1})^2 b_j = c_j$ definiert sei. Dann hat $T^{-1}AT$ die behauptete Gestalt.
c) Wir können annehmen, daß A reell symmetrsich ist. Ist $A(x_j) = d(x_j)$, so gilt
$a_1x_1 + b_1x_2 = dx_1, c_1x_1 + a_2x_2 + b_2x_3 = dx_2, \ldots, c_{n-1}x_{n-1} + a_nx_n = dx_n$.
Ist $x_1 \neq 0$ vorgegeben, so lassen sich wegen $b_j > 0$ die Werte $x_2, \ldots, x_n$ rekursiv bestimmen. Also ist $\dim \mathrm{Kern}(A - cE) \leq 1$. Da A reell symmetrisch ist, hat jeder Eigenwert von A die Vielfachheit 1.

9.1.2 Sei T orthogonal mit
$T^{-1}AT = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\varphi & \sin\varphi \\ 0 & -\sin\varphi & \cos\varphi \end{pmatrix}$. Dann folgt $\| A - E \|_2^2 = \| T^{-1}AT - E \|_2^2$
$= 2((1 - \cos\varphi)^2 + \sin^2\varphi) = 4(1 - \cos\varphi) = 8\sin^2\frac{\varphi}{2}$.

9.1.7 Ist $(v, v) = (w, w)$, so gilt $(v - w, v + w) = 0$, nach Voraussetzung also $(A(v - w), A(v + w)) = 0$, und somit $(Av, Av) = (Aw, Aw)$. Daher ist $(Av, Av)/(v, v)$ unabhängig von $v \neq 0$. Somit gilt $(Av, Av) = b^2(v, v)$ mit $b > 0$. Dann ist $b^{-1}A$ orthogonal.

9.2.1 Ist $Av = u \times v$ mit $u \neq 0$, so gilt $\mathrm{Kern}\, A = \langle u \rangle$. Wegen
$\mathrm{Bild}\, A \leq \langle u \rangle^\perp$ und $\dim \mathrm{Bild}\, A = 2$ folgt $\mathrm{Bild}\, A = \langle u \rangle^\perp$. Nach 9.2.7 d) gilt $A^2v = u \times (u \times v) = -(u, u)v + (u, v)u$. Es folgt $A(A^2 + (u, u)E) = 0$. Wegen $A \neq 0$ und $A^2 \neq -(u, u)E$ liefert dies $m_A = f_A = x(x^2 + (u, u))$. Aus $(Av, w) = (v, -u \times w)$ erhalten wir $A^* = -A$.

9.2.2 a) Nach 9.2.7 d) gilt $Av = (u \times v) \times w = (u, w)v - (v, w)u$. Wegen $Au = 0$ folgt $A(A - (u, w)E) = 0$. Da $0 \neq A \neq (u, w)E$ ist, folgt $m_A = x(x - (u, w))$.

b) Ist $(u,w)=0$, so folgt $m_A=x^2$, also $f_A=x^3$. Dann ist $Av=-(v,w)u$, somit $\operatorname{Bild} A=\langle u\rangle$ und $\operatorname{Kern} A=\langle w\rangle^\perp$. Wegen $m_A=x^2$ ist A nicht diagonalisierbar, erst recht nicht normal.
c) Sei $(u,w)\neq 0$. Wegen $m_A=x(x-(u,w))$ ist A diagonalisierbar. Ist $Av=0$, so folgt $u\times v\in\langle u\rangle^\perp\cap\langle w\rangle=0$. Also gilt $\operatorname{Kern} A=\langle u\rangle$ und somit $f_A=x(x-(u,w))^2$. Wegen $\dim\operatorname{Bild} A=2$ und $\operatorname{Bild} A\leq\langle w\rangle^\perp$ erhalten wir $\operatorname{Bild} A=\langle w\rangle^\perp$. Es gilt $(v,A^*z)=(Av,z)=(v,(w\times z)\times u)$. Somit ist $A^*z=(w\times z)\times u$. Für $\langle u\rangle=\langle w\rangle$ ist also $A^*=A$. Sei A normal, also $(u,w)\neq 0$ und $\langle u\rangle^\perp=(\operatorname{Kern} A)^\perp=\operatorname{Bild} A=\langle w\rangle^\perp$. Dann ist $\langle u\rangle=\langle w\rangle$.

9.2.5 a) Wegen der Jacobi-Identität gilt
$D(v_1\times v_2)=(v_1\times v_2)\times w=-(v_2\times w)\times v_1-(w\times v_1)\times v_2=$
$v_1\times(v_2\times w)+(v_1\times w)\times v_2=v_1\times Dv_2+Dv_1\times v_2$.
b) Sei $[e_1,e_2,e_3]$ eine Orthonormalbasis von V mit $e_1\times e_2=e_3, e_2\times e_3=e_1, e_3\times e_1=e_2$. Sei D eine Derivation und $De_j=\sum_{j=1}^3 a_{jk}e_k$. Aus $De_1=De_2\times e_3+e_2\times De_3$ folgt $a_{12}=-a_{21}$ und $a_{11}=a_{22}+a_{33}$. Analog erhält man $a_{23}=-a_{32}, a_{22}=a_{33}+a_{11}, a_{31}=-a_{13}, a_{33}=a_{11}+a_{22}$. Dies liefert $a_{11}=a_{22}=a_{33}=0$. Also ist D eine schiefsymmetrische Matrix zugeordnet. Ist S der $\mathbb{R}$-Vektorraum aller Derivationen auf V, so folgt $\dim S\leq 3$. Andererseits liefert $w\mapsto D_w$ mit $D_wv=v\times w$ einen Monomorphismus von V in S. Also hat jede Derivation die Gestalt D_w.

9.3.3 Nach 9.3.2 d) gilt $a^2-S(a)a+e_0=0$. Wegen $a\neq\pm e_0$ ist $x^2-S(a)x+1$ irreduzibel. Daher ist $m_A=x^2-S(a)x+1$. Da nach 5.5.8 jeder irreduzible Teiler von f_A auch ein Teiler von m_A ist, folgt $f_A=(x^2-S(a)x+1)^2$. Da A keinen Eigenwert ±1 hat, hat die Normalform von $\rho(a,e_0)$ die Gestalt $\begin{pmatrix} D(\varphi) & 0\\ 0 & D(\varphi)\end{pmatrix}$, denn φ ist durch $S(a)$ festgelegt. Aus $4a_0=\operatorname{Spur}\rho(a,e_0)=2\operatorname{Spur}D(\varphi)=4\cos\varphi$ folgt $\cos\varphi=a_0$.

Literatur

[1] E. Artin. Geometric Algebra, Wiley-Interscience, 1988.

[2] M. Aigner und G.M. Ziegler. Proofs from THE BOOK. Springer Verlag, 3rd edition, 2004.

[3] H.D. Ebbinghaus, H. Hermes, F. Hirzebruch, M. Köcher, K. Mainzer, K. Neukirch, J. Prestel und R. Remmert. Zahlen. Springer Verlag, 3. verb. Aufl., 1992.

[4] M. Eigen. Stufen des Lebens. Piper, 1987.

[5] H.W. Golan and W. Lempken. An easy linear algebra approach to the eigenvalues of the Bernoulli-Laplace model of diffusion. Archiv Math. 64 (1995), 150-153.

[6] J.E. Goodman and J.O'Rourke, editors. Handbook of Discrete and Computational Geometry. CRC Press, 1997.

[7] G.H. Hardy and E.M. Wright. An Introduction to the Theory of Numbers. Oxford Science Publications, Fifth Edition, 1994.

[8] B. Huppert. Angewandte Lineare Algebra. DeGruyter, 1990.

[9] M. Köcher. Lineare Algebra und analytische Geometrie. 2. Auflage, Springer, 1985.

[10] M. von Laue. Relativitätstheorie. 1. Band, Vieweg Verlag, 5. Aufl., 1951.

[11] G. Pickert. Projektive Ebenen. Springer, 1955.

[12] P. Ribenboim. Fermat's Last Theorem for Amateurs. Springer, 1999.

[13] R.P. Stanley. Enumerative Combinatorics. Vol. 2, Cambridge University Press, 2001.

[14] A.E. Taylor. Introduction to Functional Analysis. John Wiley, 1958.

[15] S. Wagon. The Banach-Tarski Paradox. Cambridge University Press, 1994.

[16] B. Walsh. The scarcity of crossproducts in euclidian spaces. Amer. Math. Monthly 74 (1967), 188-194.

[17] W. Willems. Codierungstheorie. DeGruyter, 1999.

Namensverzeichnis

Abel, N. H., 22, 191
Adleman L., 39

Banach, S., 315
Bessel, F. W., 441
Bézout, E., 41
Bruck, R. H., 171

Cantor, G., 1, 11, 63
Cardano, G., 191
Carmichael, R. D., 38
Cartan, E. J., 513
Catalan, E. C., 25, 242
Cauchy, A. L., 315
Cayley, A., 44, 193, 272, 526
Clifford, W. K., 531
Cohen, P., 11
Courant, R., 477
Cramer, G., 204

Dedekind, R., 5, 56, 249, 264
del Ferro, S., 191
Delsarte, P., 417
de Moivre, A., 47
de Morgan, A., 7

Eckmann, B., 526
Ehrenfest, P., 368
Einstein, A., 32, 432
Euklid, 11, 41, 498
Euler, L., 2, 28, 36, 63, 265, 507

Feit, W., 192
Fermat, P., 2, 36, 264
Ferrari, L., 191
Fisher Sir, R. A., 170
Fizeau, H., 432
Fontana, N. (genannt Tartaglia), 191
Fourier, J. B., 440
Fresnel, A. J., 433
Frobenius, F. G., 49, 338, 526

Galois, E., 192
Gauß, K. F., 3, 43, 266
Gelfand, I. M., 529
Gelfond, A. O., 63
Gershgorin, S. A., 355
Golan, H. W., 367
Golay, M. J. E., 161, 406, 411
Gram, J. P., 374
Graßmann, H. G., 220

Haar, A., 529
Hamilton, W. R., 272, 523
Hamming, R. W., 148, 150, 153, 154, 163
Hausdorff, F., 508
Heisenberg, W., 137, 326, 467
Helmholtz, H. L. F., 507
Hensel, K., 215
Hermite, C., 63, 447, 459
Hilbert, D., 11, 438
Hölder, L. O., 326
Hooke, R., 176
Hurwitz, A., 44, 526

Jacobi, C. G., 109
Janko, Z., 171
Jordan, M. E. C., 305, 307

Killing, W. K., 513
Kimura, 238, 346
Klein, F. Ch., 191, 543
Krawtchouk, M. P., 410
Kronecker, L., 93, 218
Kummer, E. E., 265

Lagrange, J. L., 27, 146, 226, 248
Laplace, P. S., 227
Lebesgue, H., 439, 467
Legendre, A. M., 447
Lempken, W., 367
Leont'ev, V. K., 150
Lie, M. S., 510
Lindemann von, C. L. F., 63
Liouville, J., 63
Lorentz, H. A., 418, 431, 433

MacWilliams, F. J., 408, 411
Mathieu, C. L., 407
Markoff, A. A., 75, 117
Maschke, H., 144, 446
Mazur, S., 529
Mersenne, M., 3
Michelson, A. A., 429
Minkowski, H., 313, 418, 429
Möbius, A. , F., 264
Montgomery, 265
Moran, P. A. P., 132
Muller, D. E., 160

Nakayama, T., 301
Newton Sir, I., 176, 483
Noether, E., 97

Perron, O., 338
Pisano, L. (genannt Fibonacci), 74
Plotkin, M., 159
Pólya, G., 366
Pontryagin, L. S., 529
Prüfer, E. P. H., 249
Pythagoras von Samos, 440

Reed, I. S., 157, 160
Riesz, F., 321
Rivest, R. L., 39
Ryser, R. J., 171

Schmidt, E., 439
Schneider, T., 63
Schur, I., 481
Schwarz, H. A., 314, 372
Shamir, A., 39
Singelton, R. C., 152
Skolem, T., 97
Solomon, G., 157
Steinitz, E., 65
Stirling, J., 18
Sun Zi, 246
Sylow, P. L. M., 27, 116
Sylvester, J. J., 397

Taylor, B., 114
Thompson, J. G., 192
Tietäväinen, A., 150

Uchida, 265

Vandermonde, A. T., 208
von Laue, M., 435
von Neumann, J., 438

Wedderburn, J., 34, 245
Wielandt, H., 326, 339, 482
Wiles, A., 265
Wilson, J., 52
Witt, E., 34, 393, 394

Zinov'ev, V. A., 150
Zorn, M., 66, 295

Index

$\operatorname{sgn}\pi$, 189
$a \sim b$, 253
$(K)_n$, 100
$(K)_{m,n}$, 100
$A > B$, 337
$A \geq 0$, 469
$A \geq B$, 337
$A > 0$, 469
A^t, 108
$B(V)$, 323
$E(V)$, 319
$K[A]$, 286
K^n, 53
$M^\perp$, 378
R-Homomorphismus, 293
$\mathrm{End}_K(V)$, 83
$\mathrm{GL}(V)$, 94, 213, 216
Gol(23), 407
Gol(24), 407
$\mathrm{O}(V)$, 385
$\mathrm{SL}(V)$, 205, 213, 216
SO(3), 523
SO(4), 523
$\mathrm{SO}(V)$, 385
SU(2), 529
$\mathrm{SU}(V)$, 401
$\operatorname{Sp} A$, 136
$\mathrm{T}(M)$, 298
$\mathrm{U}(V)$, 385
$\mathbb{Z}_n$, 35
$\det A$, 194
$\equiv$, 246
$\mathrm{Hom}_K(V,W)$, 83
ind, 395
$\mu(n)$, 264
$\| A \|$, 323
$\| v \|$, 312
π-Rotation, 505
$\mathrm{r}(A)$, 97, 108
$\varphi(n)$, 28
$a \mid b$, 253
Ähnlichkeit, 426
Äquivalenz-
    klasse, 6
    relation, 6, 26

Abbildung, 8
    adjungierte, 449
    bijektive, 9, 19
    Bild, 9
    hermitesche, 459, 461
    identische, 8
    injektive, 9, 16, 19
    invertierbare, 11
    lineare, 83
    monomiale, 158
    normale, 452, 455
    orthogonale, 498
    surjektive, 9, 18, 19
    symmetrische, 466
    unitäre, 456
    Urbild , 9
Ableitung eines Polynoms, 237
Achse, 503
    n-zählige, 535
Adjungierte, 449
Adjunkte, 202
Algebra, 93, 102
    graduierte, 224

Graßmann, 220
Algebren-
automorphismus, 96
homomorphismus, 96, 233
isomorphismus, 96, 103
Algebrennorm, 323
allgemeiner binomischer Satz, 241
allgemeiner Kongruenzsatz, 444
anisotrop, 392
Antiautomorphismus, 115, 524
Anzahl isotroper Vektoren, 401
Assoziativgesetze, 4, 8, 22
Austauschsatz von Steinitz, 65
Auswahlsatz, 10, 260
Automorphismus, 94, 104
Automorphismus von Gruppen, 182

Bézout-Koeffizienten, 41
Banach-
algebra, 323
raum, 315
Basis
Orientierung, 214
Basis eines Vektorraums, 63, 66
Binomialkoeffizienten, 13
binomischer Lehrsatz, 14

cartesisches Produkt, 5, 16
Cauchy-Folge, 315
Cauchy-Multiplikation, 240
Cayleysche Oktaven, 44, 526
Charakteristik, 36
charakteristisches Polynom, 268
Chinesischer Restsatz, 31, 246
Clifford-Algebra, 531
Code
äquivalenter, 159
binärer, 148
binärer erweiterter Golay-, 407, 411
binärer Golay-, 407
dualer, 404
Erzeugermatrix, 153
Hamming-, 154
ISBN-, 55
Kontrollmatrix, 153
linearer, 148
Minimaldistanz, 148
Paritätscheck-, 55
perfekter, 150
Redundanz, 148
Reed-Muller-, 160
Reed-Solomon-, 157
selbstdualer, 404
Simplex-, 163
ternärer, 148
ternärer erweiterter Golay-, 416
ternärer Golay-, 161
Wiederholungs-, 147
Codewort
Gewicht, 149
Cosinussatz, 499
erster, 520
Cramersche Regel, 204

de Morgansche Regeln, 7
Dedekind-Identität, 5, 56
Dedekindring, 249, 264
Derivation, 522
innere, 522
Determinante, 186, 194
Charakterisierung der, 215
Kästchensatz, 200
Multiplikationssatz, 198
Vandermondesche, 208
diagonalisierbar, 283
Diedergruppe, 115, 535
Dimension, 66
direkte Summe, 140, 295
Diskriminante, 374
Distributivgesetze, 4, 33
Division mit Rest, 41, 232, 253
doppelte Abzählung, 20
Drehung, 503
Dreiecksgestalt, 278
Dreiecksungleichung, 43, 121, 149, 312
Durchschnitt, 4

Ehrenfest-Diffusion, 368
Eigenvektor, 268
Eigenwert, 268
Eigenwertabschätzungen, 477
einfach zusammenhängend, 531
Einheit, 253
Einheiten, 33
Einheitengruppe, 253
Einheitskugel, 319
Einheitswurzeln, 46
Einparameteruntergruppe, 510
Einsteinsche Addition der Geschwindigkeiten, 432
Einsteinsches Additionsgesetz, 32
elementare Umformung, 165
Elementarmatrizen, 165
endlich erzeugbar, 294
Endomorphismus, 83
  Determinante, 205
  diagonalisierbarer, 283
  invertierbarer, 94
  Projektion, 140
  regulärer, 94
  singulärer, 94
  Spektralradius, 330
Epimorphismus, 83, 87, 182, 243, 294
Ergodensatz, 328
Erzeugendensystem, 59
Erzeugnis
  in einem Vektorraum, 59
  in einer Gruppe, 28
Euklidischer Algorithmus, 41, 79
euklidischer Ring, 253, 266
euklidischer Vektorraum, 498
Eulersche Funktion, 28, 29, 36, 39, 210
Eulersche Winkel, 507

faires Mischen, 364
Faktormodul, 293
Faktorraum, 80, 84
Fakultät, 13
Fermatsche Vermutung, 264
formale Potenzreihe, 240
Fresnelschen Mitführungskoeffizienten, 433
Frobenius-Automorphismus, 49
Fundamentalsatz der Algebra, 43

Galileische Fallbewegung, 488
Gaußscher Ring, 266
Gewichtspolynom, 405
Gitter, 503
gleichmächtig, 11
Gleichzeitigkeit, 434
Golay-Code
  binärer, 407
  binärer erweiterter, 407, 411
  ternärer, 161
  ternärer erweiterter, 416
Google, 342
größter gemeinsamer Teiler, 254
Grad, 231
Gramsche Matrix, 374
Graph
  stochastische Matrix, 358
Graßmann-Algebra, 220
Grenzwert, 314
Gruppe, 21
  abelsche, 22
  alternierende, 190
  Automorphismus, 182
  Dieder-, 115
  endliche, 22
  freie, 508
  Homomorphiesatz, 184
  Homomorphismus, 182
  inverses Element, 23
  Kürzungsregeln, 25
  Kleinsche Vierer-, 191
  kommutative, 22
  Lorentz-, 418
  Mathieu-, 407
  monomiale, 158
  neutrales Element, 23
  normale Unter-, 183
  Normalteiler, 183

orthogonale, 385
spezielle orthogonale, 385
symmetrische, 187
symplektische, 384
unitäre, 385
Unter-, 26
verallgemeinerte Quaternionen-, 116
zyklische, 29

Halbgruppe, 22
Hamming-
Abstand, 148
Schranke, 150
Hauptachsen, 463
Hauptideal, 244
Hauptidealring, 253
Hauptminor
r-ter, 472
Hausdorffsches Paradoxon, 508
Heisenberg-Gleichung, 137, 326
Heisenbergsche Unschärferelation, 467
Hilbertraum, 436, 438
Homomorphiesatz, 86, 244
Homomorphismus, 83, 182, 243
beschränkter, 318
Bild, 83, 183
Kern, 83, 183
Rang, 97
stetiger, 318
hyperbolische Ebene, 391
hyperbolischer Raum, 392
hyperbolisches Paar, 391
Hyperebene, 82
Hyperfläche, 463

Ideal, 243
Prim-, 257
Identität von Lagrange, 226
Index, 395, 398, 403
Inklusions-Exklusions-Prinzip, 16
Intergritätsbereich, 253
Inverse, 11, 103, 111, 204
Involution, 27
irreduzibel, 253
Isometrie, 158, 335, 376, 400
Isomorphismus, 84, 87, 95, 101, 182, 243, 294
isotrop, 388

Jacobi-Identität, 512
Jordan-Kästchen, 307

Kästchenmultiplikation, 110
Körper, 33
algebraisch abgeschlosser , 236
Charakteristik, 36
endlicher, 49, 67
lokal kompakt, 529
multiplikative Gruppe, 236
Kausalitätssatz, 486
Kette, 295
induktive, 295
kleinstes gemeinsames Vielfaches, 254
Komplement
in Mengen, 5
in Vektorräumen, 64
komplexe Zahlen, 42
Absolutbetrag, 43
Imaginärteil, 43
konjugiert , 43
Realteil, 43
komplexer Zahlkörper, 42
Komponente
freie, 484
gebundene, 484
Kompositum, 8
Kontinuumhypothese, 11
Kontraktion, 323
konvex, 322
Kronecker
-Produkt, 218
symbol, 93
Kugelpackungsgleichung, 150

Längenkontraktion, 433
Lagrangesches Interpolationspolynom, 248
Laplacescher Entwicklungssatz, 227

Lichtkegel, 418
Lichtvektoren, 418
Liealgebra, 510, 512
linear
    abhängig, 59
    unabhängig, 59
lineare Schwingungen, 483
lineares Gleichungssystem, 173
    homogenes, 173, 205
    inhomogenes, 173
    Lösungsalgorithmus, 174
Linksideal, 294
lokaler Körper, 529
Lorentz-
    Transformationen, 418, 431
    Translation, 421
Lorentzgruppe, 418

Möbius-Funktion, 264
MacWilliams-Identitäten, 411
Markoff-Prozeß, 117
Martingal, 130
Matrix, 100
    Übergangs-, 117
    Adjunkte, 202
    charakteristisches Polynom, 268
    Determinante, 194
    diagonalisierbare, 283
    Dreiecks-, 109, 194
    Elementar-, 165
    Gramsche, 374
    hermitesch, 459
    invertierbare, 103
    irreduzible, 337
    irreduzible stochastische, 358
    Jacobi-, 109, 131, 364, 368
    nichtnegative, 337
    normale, 457
    Permutations-, 110
    reduzible, 337
    reguläre, 103
    singuläre, 103
    Spaltenrang, 106
    Spur, 136
    stochastische, 118
    stochstische, 355
    symmetrische, 110
    transponierte, 108, 307
    unitäre, 442, 457
    Zeilenrang, 106
Maximalbedingung, 258
mechanisches System, 176, 177
Menge, 1
    abzählbare, 11
    Durchschnitt, 4
    endliche, 11
    konvexe, 322
    leere, 4
    Potenz-, 4
    symmetrische, 322
    Teil-, 3
    unendliche, 11
    Unter-, 3
    Vereinigung, 4
Mesonen, 434
Metrik, 148
metrischer Raum, 314
Minimalpolynom, 283
Minkowskiraum, 373, 375, 418, 430
Modul, 293
    endlich erzeugbarer, 294
    freier, 296
    projektiver, 297
    torsionsfreier, 298
Moivresche Formeln, 47
Monomorphismus, 84, 87, 182, 243, 294

Norm
    eines Quaternions, 524
    Vektorraum-, 312
Normalteiler, 183
normierter Vektorraum, 312
Nullstelle, 235
    m-fache, 235

Oktaeder, 538
Orthogonalbasis, 388
orthogonale

Abbildung, 498
Vektoren, 378
Orthogonalität, 371
Orthonormalbasis, 389, 390

Parallelogrammgleichung, 437, 438
Partition, 5
Permutation, 187
Signum, 188
Plotkin-Konstruktion, 159
Polya's Urnenmodell, 366
Polynom, 231
Grad, 231
Hermite-, 447
Krawtchouk, 410
Legendre-, 447
Minimal-, 283
normiertes, 231
Nullstelle, 235
total zerfallend, 236
Polynomring, 231, 262
Potenzmenge, 4, 12, 15
Potenzreihen, 240
Potenzreihenring, 266
Prüferring, 249, 265
Primelement, 257
Primfaktorzerlegung, 257
Primideal, 257
Primzahlen
Fermatsche, 2
Mersennesche, 3
Prinzip der doppelten Abzählung, 20
Produktionsplanung, 335
Projektion, 140
projektive Ebene, 68, 171
Public-Key-Verfahren, 39

quadratische Form, 463
Quaternionen, 34, 523

Rang, 97, 108
Spalten-, 106
Zeilen-, 106
Rang eines freien Moduls, 296
redundante Bits, 147
reguläres n-Eck, 3
Rekursionsfolge
Periode einer, 76
Rekursionsgleichung, 72
Relation, 6
Ring, 33
kgV-, 257
Einheiten, 33
euklidischer, 253
Hauptideal-, 253
Homomorphismus, 243
Integritätsbereich, 253
kommutativer, 33
RSA-Verfahren, 39, 77

Satz
von Cayley-Hamilton, 272
von Fisher, 170
von Frobenius, 526
von Gelfand-Mazur, 529
von Hensel, 215
von Lagrange, 27
von MacWilliams, 408
von Maschke, 144, 446
von Perron-Frobenius, 338
von Pontryagin, 529
von Skolem-Noether, 97
von Sylow, 27
von Wedderburn, 34, 245
Schieberegister, 77
Schiefkörper, 33, 34
der Quaternionen, 116
Schranke
Hamming-, 150
Singleton-, 152, 163
Schubfachprinzip, 58
Schwerpunkt, 487
Signatur, 397
Signum, 188
simultane Diagonalisierbarkeit, 290
simultane Dreiecksgestalt, 280
Sinussatz, 520
Skalarprodukt, 371
α-, 371

definites, 372
klassisches, 385
orthosymmetrisches, 378
regulares, 375
schiefsymmetrisches, 384
semidefinites, 372
singuläres, 375
symplektisches, 384
unitäres, 385
Spektralradius, 330
stochastischer Matrizen, 356
Spektralzerlegung, 465
spezielle lineare Gruppe, 205
Spezielle Relativitätstheorie, 429
sphärische Trigonometrie, 519
Spiegelung, 504
orthogonale, 386
unitäre, 386
Spur, 136
stochastische Matrix, 118
doppelt, 363
stochastischer Prozeß, 117
Übergangsmatrix, 117
absorbierender Zustand, 122, 126, 131
Ehrenfest-Diffusion, 368
Elementarprozeß, 117
Farbenblindheit, 123
Gambler's ruin, 129
gerichteter Graph, 126
Irrfahrten, 127, 361
Mischen von Spielkarten, 362
Modell von Kimura, 238, 346
Modell von Moran, 132
Pólya's Urnenmodell, 366
Random walk, 127
Zustand, 117
Streckung, 88, 213
Stromchiffren, 76
Suchmaschinen, 341
Sylowgruppe, 116

Teilmenge
abgeschlossene, 314
offene, 314
Tetraeder, 538, 542
Torsionselement, 298
torsionsfrei, 298
Toto-Elferwette, 162
Träger einer Funktion, 252
Trägheitssatz von Sylvester, 397
Transposition, 187
Transvektion, 88, 165, 213
symplektische, 386
unitäre, 387

Ungleichung
Höldersche, 326
Minkowskische, 313
Schwarzsche, 372
Untergruppe, 26
Index einer, 26, 27
Untermodul, 293
Unterraum, 54
$\mathcal{A}$-invarianter, 143
isotroper, 388, 391

Vandermondesche Determinante, 208
Vektor, 53
isotroper, 388
Null-, 53
raumartiger, 418
zeitartiger, 418
vektorielles Produkt, 510
Vektorraum, 53
anisotroper, 392, 397
Basis, 63
Dimension, 66
endlich erzeugbarer, 59
euklidischer, 498
Faktorraum, 80
Hilbert-, 436
Index, 395
kompletter, 315
normierter, 312
Nullraum, 54
regulärer, 375
singulärer, 375
symplektischer, 384

unitärer, 385
Unterraum, 54
vollständiger, 315
verallgemeinerter Produktsatz, 226
Vereinigung von Mengen, 4, 17
Vielfachheit
eines Eigenwertes, 270
Volumenfunktion, 196
Charakterisierung der, 198

Weltpunkt, 429
winkeltreu, 499

Zahlen
algebraische, 63
Carmichael-, 38
Catalan-, 25, 242
Fibonacci-, 74, 79
ganz-rationale, 2
komplexe, 42
natürliche, 2
rationale, 2
reelle, 2
Stirling-, 18
teilerfremde, 28
transzendente, 63
Zeitdilatation, 433
Zerlegung
orthogonale, 388
Zornsches Lemma, 295
zulässige Partition, 368
Zykel, 187
Zyklenzerlegung, 188