Mathematik *explorativ* - Sammlung der Sätze

Satz 1.1:

* $A \cap B \subseteq A \subseteq A \cup B$
* $A \setminus B \subseteq A$
* $A \Delta B = (A \cup B) \setminus (A \cap B)$
* $A \subseteq B$ ist gleichbedeutend mit $A \cap B = A$, dies wieder mit $A \cup B = B$

Satz 1.2: Für Mengen A, B, C gelten die *Kommutativgesetze*:
$A \cap B = B \cap A$; $A \cup B = B \cup A$; $A \Delta B = B \Delta A$
und auch die *Assoziativgesetze*
$(A \cap B) \cap C = A \cap (B \cap C)$; $A \cup (B \cup C) = (A \cup B) \cup C$; $A \Delta (B \Delta C) = (A \Delta B) \Delta C$
sowie die *Distributivgesetze*
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$; $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;
$A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$
die *Idempotenzgesetze*
$A \cup A = A$; $A \cap A = A$
und die *Verschmelzungsgesetze*
$A \cap (A \cup B) = A = A \cup (A \cap B)$

Satz 1.3: Seien A, B Teilmengen von U. Dann gilt

a) $A \cap CU(A) = \emptyset$; $A \cup CU(A) = U$

b) $CU(A \cap B) = CU(A) \cup CU(B)$; $CU(A \cup B) = CU(A) \cap CU(B)$ (Gesetze von De Morgan)

c) $CU(CU(A)) = A$.

Satz 1.4: Zu jedem $a \in \mathbb{Z}$ und $b \in \mathbb{N}$ gibt es eindeutig bestimmte ganze Zahlen q, r, sodass $a = b \cdot q + r$ mit $0 \leq r < b$.
Man nennt q den *Quotienten* und r den *Rest* der Division von a durch b.

Definition 1.11 / Satz:

$a^n = a \cdot a \cdot \ldots \cdot a$, (a tritt n mal als Faktor auf, $n \in \mathbb{N}_0$, mit $a^0 := 1$)
und es gilt $a^n \cdot a^m = a^{n+m}$

Als Verallgemeinerung zu $\frac{1}{a} = a^{-1}$ vereinbart man als Schreibweise für $\frac{1}{a^n}$ kurz a^{-n}.

Demnach gilt für $a \neq 0$ die Rechenregel $\frac{a^n}{a^m} = a^n \; a^{-m} = a^{n-m}$.

Satz 1.5: Die Zahl $\sqrt{2}$ ist keine rationale Zahl, $\sqrt{2}$ ist irrational.

Satz 1.6:

Sei $b \in \mathbb{N}$ mit $b \geq 2$. Dann lässt sich jede natürliche Zahl $a > 0$ eindeutig darstellen in der Gestalt

$$a = \sum_{i=0}^{n-1} a_i b^i \quad \text{mit } a_i \in \{0, 1, \ldots, b-1\} \text{ und } a_{n-1} \neq 0.$$

Satz 1.7: Die Dezimalbruchentwicklung des gekürzten Bruches (rationale Zahl) $\frac{u}{v}$, $u, v \in \mathbb{N}$, $v > 1$, besitzt genau dann eine endliche Dezimalbruchentwicklung, wenn im Nenner v nur die Primfaktoren 2 oder 5 vorkommen.

Satz 1.8: Ein gekürzter Bruch $\frac{u}{v}$ hat genau dann eine nicht periodische b-adische Darstellung, wenn alle Primfaktoren von v auch Primfaktoren von b sind.

Satz 1.9: Für die Variation mit Zurücklegen von k aus n Dingen gibt es n^k Möglichkeiten.

Satz 1.10:

(a) $\binom{n}{k} = \binom{n}{n-k}$

(b) $\binom{n}{0} = \binom{n}{n} = 1$ und $\binom{n}{1} = \binom{n}{n-1} = n$

Satz 1.11: f: A → B und g: C → D seien Funktionen.
f = g ⇔ (A = C und für alle a ∈ A: f(a) = g(a))

Satz 1.12: Seien f: A → B, g: B → C und h: C → D drei Funktionen. Dann gilt
h ∘ (g∘f) = (h∘g) ∘ f

Satz 1.13: Sei f: A → B bijektiv. Dann ist auch f^{-1}: B → A eine Funktion und ebenfalls bijektiv; es gelten folgende Regeln:
$f^{-1} \circ f = id_A$; $f \circ f^{-1} = id_B$; $(f^{-1})^{-1} = f$

Satz 1.14: Seien f: A → B und g: B → C bijektiv. Dann ist auch g∘f: A → C bijektiv und es gilt $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

Satz 1.15: Sei f eine Funktion von A nach B. Falls es eine Funktion g: B → A gibt mit $g \circ f = id_A$ und $f \circ g = id_B$, so ist f bijektiv und es gilt $g = f^{-1}$.

Satz 2.1: Ist a = bq + r mit $0 \leq r < b$, dann ist ggT(a,b) = ggT(b,r).

Satz 2.2: kgV(a,b) · ggT(a,b) = a · b

Satz 2.3: Ist d = ggT(a,b), dann existieren Zahlen $x,y \in \mathbb{Z}$, sodass ax + by = d.

Satz 2.4: Sind $a,b,c \in \mathbb{Z}$ mit c ⁄ ab und ggT(a,c) = 1, so folgt
c / (abx + cby) und damit c ⁄ b.

Satz 2.5: Ist p prim und p ⁄ ab, so folgt (p ⁄ a oder p ⁄ b) oder (p ⁄ a und p ⁄ b): d.h. ist ein Produkt ab teilbar durch eine Primzahl p, so ist mindestens einer der Faktoren a,b durch p teilbar.

Satz 2.6: Jede natürliche Zahl $n \in \mathbb{N}$, n > 1, lässt sich in Primfaktoren zerlegen,

d.h. es gibt $k \in \mathbb{N}$, sodass $n = p_1 p_2 p_3 ... p_k$.
Diese Darstellung ist bis auf die Reihenfolge der Faktoren eindeutig.

Satz 2.7: Zwei Zahlen a, b sind genau dann relativ prim (d.h.: ggT(a,b) = 1), wenn jede Primzahl p, die in der Zerlegung von a vorkommt, nicht in der Zerlegung von b vorkommt und umgekehrt.

Satz 2.8: Es gibt unendlich viele Primzahlen.

Satz 2.9: Die lineare diophantische Gleichung $ax + by = c$ mit $a, b, c, x, y \in \mathbb{Z}$ ist genau dann lösbar, wenn für $d = ggT(a,b)$ gilt: $d \nmid c$.

Satz 2.10: $a \equiv b \bmod m$ genau dann, wenn die positiv kleinsten Reste von a und b bei der Division durch den Modul m übereinstimmen.

Satz 2.11: Sei $p(x) = c_n x^n + c_{n-1} x^{n-1} + ... c_1 x + c_0$ mit $c_i \in \mathbb{Z}$
Ist $a \equiv b \bmod m$, so ist $p(a) \equiv p(b) \bmod m$.

Satz 2.12: Ist $r_1, r_2, ..., r_m$ ein vollständiges Restsystem mod m und ist $ggT(a, m) = 1$ und $b \in \mathbb{Z}$, dann ist auch $ar_1 + b, ar_2 + b, ..., ar_m + b$ ein vollständiges Restsystem mod m.

Satz 2.13: Ist $ka \equiv kb \bmod m$ und $d = ggT(k,m)$, so gilt $a \equiv b \bmod \left(\frac{m}{d}\right)$.

Satz 2.14: Die Kongruenz $ax \equiv b \bmod m$ mit $x \in \mathbb{Z}$ ist dann und nur dann lösbar, wenn $d = ggT(a,m) \nmid b$. Ist die Kongruenz lösbar, so hat sie d verschiedene Lösungen.

Satz 2.15: Die Kongruenz $ax \equiv b \bmod m$ mit $ggT(a,m) = 1$ ist für jedes $b \in \mathbb{Z}$ durch eine und nur eine (d.h.:„genau eine“) Restklasse x mod m lösbar.

Satz 2.16: Sind die Moduln $m_1, m_2, ..., m_k$ paarweise relativ prim, dann ist das System $x \equiv c_i \bmod m_i$, $i = 1, 2,..., k$, stets lösbar und die Lösung ist modulo $M = m_1 m_2 ... m_k$ eindeutig.

Satz 2.17: Eine Zahl $a \in \mathbb{Z}$ ist genau dann quadratischer Rest mod 2^k, $k \geq 3$, wenn $a \equiv 1 \bmod 8$.

Satz 2.18: Es sei $m = p_1^{e_1} p_2^{e_2} ... p_s^{e_s}$ die Primzahlzerlegung von $m \geq 2$. Dann ist $a \in \mathbb{Z}$ genau dann ein quadratischer Rest mod m, wenn a ein QR($p_i^{e_i}$) für $i = 1,2,\ldots,s$ ist.

Satz 2.19: Ist mit $k \in \mathbb{N}$, $k \geq 1$ und $p > 2$, p prim, a ein QR (p^k), so ist a auch QR(p), und umgekehrt.

Satz 2.20: Die Zahlen $1^2, 2^2, \ldots ((p-1)/2)^2$ sind alle inkongruent mod p. Das heißt, mit $i^2 \equiv a \bmod p$, $i = 1,2,\ldots(p-1)/2$ erhält man $(p-1)/2$ Quadratreste.

Satz 2.21: Für $p > 2$ gibt es genau $(p-1)/2$ Quadratreste QR(p) und

(p-1)/2 Nichtreste NR(p).

Satz 2.22 *(Kriterium von Euler):*
Ist $a \in \mathbb{Z}$ prim zu $p > 2$, so ist a
QR(p) genau dann, wenn $a^{(p-1)/2} \equiv 1 \bmod p$,
NR(p) genau dann, wenn $a^{(p-1)/2} \equiv -1 \bmod p$.

Satz 2.23: Für Quadratreste QR(p) und Nichtreste NR(p) gelten für $p > 2$:
$QR(p) \cdot QR(p) = QR(p)$
$QR(p) \cdot NR(p) = NR(p)$
$NR(p) \cdot NR(p) = QR(p)$

Satz 2.24: 2 ist ein QR(p) für Primzahlen der Gestalt $p = 8k \pm 1$ und ein NR(p) für Primzahlen der Gestalt $p = 8k \pm 3$.

Satz 3.1: Das Skalarprodukt zweier Vektoren ist Null genau dann wenn wenigstens einer der beiden Vektoren der Nullvektor ist oder wenn die beiden Vektoren senkrecht aufeinander stehen.

Satz 3.2: Der Vektor $\boldsymbol{a} = (a,b)$ ist ein Normalvektor zur Geraden $g : ax + by - c = 0$.

Satz 3.3: Zwei Geraden $\boldsymbol{x} = \boldsymbol{p} + \lambda \boldsymbol{r}$ und $\boldsymbol{x} = \boldsymbol{q} + \mu \boldsymbol{s}$ sind genau dann parallel zueinander, wenn $r_1 s_2 - r_2 s_1 = 0$.

Satz 3.4: Zwei Vektoren $\boldsymbol{r}$ und $\boldsymbol{s}$ dann und nur dann linear abhängig, wenn sie parallel sind, also wenn gilt: $\boldsymbol{r} = \lambda \boldsymbol{s}$.

Satz 3.5: Das Vektorprodukt $\boldsymbol{a} \times \boldsymbol{b}$ ist dann und nur dann gleich dem Nullvektor $\boldsymbol{o}$, wenn die beiden Vektoren $\boldsymbol{a}$ und $\boldsymbol{b}$ linear abhängig sind.

Satz 3.6: Der Vektor $\boldsymbol{v} \times \boldsymbol{w}$ steht senkrecht auf $\boldsymbol{v}$ und $\boldsymbol{w}$.
Seine Länge ist dem Betrag nach gleich der Fläche des durch $\boldsymbol{v}$ und $\boldsymbol{w}$ gebildeten Parallelogramms.

Satz 3.7: Das Volumen V eines durch die (Orts)-Vektoren $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$ aufgespannten Parallelepipeds ist $V = |(\boldsymbol{a} \times \boldsymbol{b}) \cdot \boldsymbol{c}|$.

Satz 4.1: Die Menge aller Permutationen einer Menge M bildet bezüglich der Multiplikation von Permutationen eine Gruppe.
Man nennt sie *vollständige symmetrische Gruppe* S(M) auf M.

Satz 4.2: Die Anzahl der Permutationen einer Menge M mit m Elementen ist
$m! = m \cdot (m-1) \cdot \ldots \cdot 2 \cdot 1$ (genannt „m Fakultät“, auch „m Faktorielle“).

Satz 4.3: $(U, \otimes)$ mit $U \neq \{\}$ ist Untergruppe von $(G, \otimes)$, falls für alle $x, y \in U$ gilt:
$x \otimes y \in U$ und $x^{-1} \in U$.

Satz 4.4: Ist G eine endliche Gruppe, so ist die Ordnung ord (U) einer Untergruppe U ein Teiler der Ordnung ord (G) der Gruppe G.

Satz 4.5: Ist $(G, \otimes)$ eine *endliche* Gruppe mit dem neutralen Element e und der Ordnung $g = ord(G)$ und ist $x \in G$ beliebig, so gibt es eine positive ganze Zahl r, sodass $x^r = e$.

Satz 4.6: Alle zyklischen Gruppen sind abelsch.

Satz 4.7: Ist G eine Gruppe und $a \in G$ ein Element mit endlicher Ordnung k, dann erzeugt a eine zyklische Untergruppe U der Ordnung k, deren Elemente e, a, a^2, ..., a^{k-1} sind.

Satz 4.8: Für alle Elemente x einer Gruppe G mit der Ordnung $g = ord(G)$ gilt $x^g = e$, wobei e das neutrale Element von G ist.

Satz 4.9: Ist p prim und $x \in \mathbb{N}$ mit $p \nmid x$, dann gilt $x^{p-1} \equiv 1 \bmod p$.

Satz 4.10: Ist G eine endliche Gruppe, deren Ordnung eine Primzahl ist, so hat G außer {e} und G selbst keine Untergruppen.

Satz 4.11: Sei U eine Untergruppe von $(G, \otimes)$. Dann gilt:

(1) Ist $a \in U \Rightarrow aU = U$.
(2) Je zwei Nebenklassen von G nach U sind disjunkt oder identisch.
(3) Alle Nebenklassen von G nach U sind gleichmächtig.

Satz von Lagrange 4.12:
Für jede Untergruppe U einer endlichen Gruppe G gilt $ord(G) = |G : U| \cdot ord(U)$.

Satz 4.13: $\mathbb{Z}_n$ ist dann und nur dann ein Körper, wenn n eine Primzahl p ist, d.h. $(\mathbb{Z}_p, +, \cdot)$ ist ein Körper.

Satz 4.14: Sind p, q zwei Polynome über einem Körper K und ist der Grad $Gd(q) \geq 0$, dann gibt es eindeutig bestimmte Polynome $s, r \in K[x]$ mit
$p = q \cdot s + r$ und $Gd(r) < Gd(q)$.

Satz 4.15: Ein Element $\alpha \in K$ ist dann und nur dann eine Nullstelle eines Polynoms p über dem Körper K, wenn $(x - \alpha)$ ein Teiler von p ist.

Satz 4.16: Ein Polynom vom Grad n über einem Körper K hat höchstens n Nullstellen, auch wenn man diese jeweils mit ihrer Vielfachheit zählt. Im Fall $K = \mathbb{C}$ gilt sogar die Gleichheit, mehr dazu in Kürze.

Satz 4.17: Jedes Polynom p(x) vom Grad $n \geq 1$ hat über dem Körper $\mathbb{C}$ genau n Nullstellen. *(Fundamentalsatz der Algebra).*

Satz 4.18: (a) Für jede Primzahl p und jedes $n \in \mathbb{N}$ gibt es (mindestens) ein normiertes irreduzibles normiertes Polynom. Das daraus resultierende Galoisfeld $GF(p^n)$ ist ein Körper mit p^n Elementen.

(b) Umgekehrt hat jeder endliche Körper K eine Primzahlpotenzordnung der Form p^n , wobei p eine Primzahl und $n \in \mathbb{N}$ ist. K ist dann zu $GF(p^n)$ isomorph.

(c) Wegen (b) gilt, dass je zwei endliche Körper mit gleich vielen Elementen isomorph (also identifizierbar) sind. Daher ist es auch egal, welches irreduzible Polynome gewählt wird.

(d) Die multiplikative Gruppe der Elemente ohne Null eines endlichen Körpers ist zyklisch (es sei wieder an Kapitel 4 erinnert), das bedeutet, dass es ein erzeugendes Element a gibt, sodass es für jedes $k \in K^* = K\backslash\{0\}$ ein $m \in \mathbb{N}$ gibt mit $k = a^m$.

Satz 5.1: In ${}_K V$ gilt

a) $\forall \lambda \in K: \ \lambda \mathbf{o} = \mathbf{o}$
b) $\forall v \in V: \ 0v = \mathbf{o}$
c) $\forall v \in V \ \forall \lambda \in K: \ (-\lambda)v = -(\lambda v) = \lambda(-v)$
d) Speziell gilt $(-1)v = -v$.
e) $\forall v,w \in V \ \exists! \ x \in V: \ v+x = w$ (nämlich $x = w+(-v) = w-v$).
f) $\forall v \in V \ \forall \lambda \in K: \ \lambda v = \mathbf{o} \Leftrightarrow (\lambda = 0 \vee v = \mathbf{o})$
g) $\forall v,w \in V \ \forall \lambda \in K: \ \lambda(v-w) = \lambda v - \lambda w$

Um Elemente $\in V$ von den Skalaren zu unterscheiden, schreibt man statt v,w,… oft **v**,**w**,… oder $\vec{v}$,$\vec{w}$,… oder gotische Buchstaben.

Satz 5.2 *(Unterraumkriterium):* Sei U eine nichtleere Teilmenge des Vektorraums ${}_K V$.

$$U \leq_K V \quad \Leftrightarrow \forall u,u' \in U \quad \forall \lambda \in K: \ u + u' \in U \wedge \lambda u \in U$$
$$\Leftrightarrow \forall u,u' \in U \quad \forall \lambda,\lambda' \in K: \ \lambda u + \lambda' u' \in U$$

Satz 5.3 und Definition: Die Menge $V/\sim = \{[v] \mid v \in V\}$ wird mit $\oplus$ und $\otimes$ dadurch zu einem Vektorraum über K, genannt *Faktorraum* von V nach $\sim$.

Satz 5.4 und Definition:

a) Sei $\sim$ eine verträgliche Äquivalenzrelation in ${}_K V$. Dann ist $\{v \in V \mid v \sim \mathbf{o}\} = [\mathbf{o}]$ ein Unterraum von V.

b) Sei U ein Unterraum von V und sei $\sim_U$ definiert durch $v \sim_U w \Leftrightarrow v - w \in U$. Die Äquivalenzklasse von $v \in V$ bzgl. $\sim_U$ ist dann durch $v + U := \{v + u \mid u \in U\}$ gegeben und heißt eine *lineare Mannigfaltigkeit*.

Satz 5.5: Die Lösungsmenge eines homogenen linearen Gleichungssystems ist ein Unterraum des K_n. Die Lösungsmenge eines beliebigen linearen Gleichungssystems ist eine lineare Mannigfaltigkeit, ihr „zugehöriger“ Unterraum ist der Lösungsraum des „homogenisierten“ Gleichungssystems.

Satz 5.6:

a) Für jedes $S \subseteq V$ ist $L(S)$ ein Unterraum von ${}_K V$.

b) $L(S)$ ist der (bzgl. $\subseteq$) kleinste Unterraum von V, der S umfasst.

c) $L(S)$ ist der Durchschnitt aller Unterräume von V, die S umfassen.

Satz 5.7: Für $S \subseteq V$ gilt: $S = L(S) \Leftrightarrow S \leq {}_K V$

Satz 5.8: Sei $S \subseteq V$. Dann sind folgende Bedingungen gleichwertig:

a) $\exists\, s \in S: L(S) = L(S \backslash \{s\})$

b) $\exists\, s \in S: s \in L(S \backslash \{s\})$

c) $\exists\, n \in \mathbb{N}\ \exists\, s_1,\ldots,s_n \in S\ \exists\, \lambda_1,\ldots,\lambda_n \in K:$
$(\lambda_1 s_1 + \ldots + \lambda_n s_n = \mathbf{o} \ \wedge\ \exists\, i \in \{1,\ldots,n\}:\ \lambda_i \neq 0)$

Satz 5.9: Seien $S,T \subseteq V$ mit $S \subseteq T$.

a) S ist linear abhängig $\Rightarrow$ T ist linear abhängig.

b) T ist linear unabhängig $\Rightarrow$ S ist linear unabhängig.

Satz** (Austauschsatz von Steinitz) **5.10:

Ist $B = (b_1,\ldots,b_n)$ eine Basis von ${}_K V$ und sind $c_1,\ldots,c_s$ (mit $s \leq n$) linear unabhängig, so gibt es $i_1,\ldots,i_{n-s} \in \{1,\ldots,n\}$, sodass $\{c_1,\ldots,c_s, b_{i_1},\ldots,b_{i_{n-s}}\}$ wieder eine Basis ist.
(Mit anderen Worten: Wir können s Elemente der Basis durch s andere ersetzen, sodass wir eine neue Basis erhalten.)

Satz 5.11 und Definition: Je zwei Basen eines endlichdimensionalen Vektorraums V haben gleich viele Elemente. Diese heißt die Dimension dimV von V.

Satz 5.12: $B = (b_1,\ldots,b_n)$ sei eine Basis von ${}_K V$. Dann lässt sich jedes $v \in V$ eindeutig als $v = \sum_{i \in I} \lambda_i b_i$ schreiben, d.h.:

$$\forall\, v \in V\ \ \forall\, i \in I\ \ \exists!\, \lambda_i \in K: \quad v = \sum_{i \in I} \lambda_i b_i\,.$$

Satz 6.1:

(a) ${}^m_n K$ ist ein Vektorraum über K

(b) Eine Basis von ${}_K({}^n_m K)$ ist $(E_{11},E_{12},\ldots,E_{1n}, E_{21},\ldots,E_{2n},\ldots,E_{m1},\ldots,E_{mn})$, wobei $E_{rs} := (e_{ij})$ durch
$e_{ij} = \begin{cases} 1 & (i,j) = (r,s) \\ 0 & \text{sonst} \end{cases}$ gegeben ist.

(c) $\dim_K({}^n_m K) = m \cdot n$. Neutrales Element in $({}^n_m K, +)$ ist die Nullmatrix; zu $A = (a_{ij})$ ist in $({}^n_m K, +)$ die Matrix $-A = (-a_{ij})$ invers.
Also haben ${}^n_m K$, ${}^m_n K$, K_{mn}, K^{mn} alle dieselbe Dimension.

Satz 6.2: Für $A,B \in {}^n_m K$ und $\lambda \in K$ gilt : $(A+B)^t = A^t + B^t$, $(\lambda A)^t = \lambda A^t$

Satz 6.3: Sei K ein Körper und seien m, n, p, q $\in \mathbb{N}$.

a) $\forall A \in K_m^n \ \forall B,C \in K_n^p$: $A\cdot(B+C) = A\cdot B + A\cdot C$ (1. Distributivgesetz)

b) $\forall A,B \in K_m^n \ \forall C \in K_n^p$: $(A+B)\cdot C = A\cdot C + B\cdot C$ (2. Distributivgesetz)

c) $\forall A \in K_m^n \ \forall B \in K_n^p \ \forall C \in K_p^q$: $(A\cdot B)\cdot C = A\cdot(B\cdot C)$ (Assoziativgesetz)

d) $\forall A \in K_m^n \ \forall B \in K_n^p \ \forall \lambda \in K$: $(\lambda A)\cdot B = \lambda(A\cdot B) = A\cdot(\lambda B)$

e) $\forall A \in K_m^n \ \forall B \in K_n^p$: $(A\cdot B)^t = B^t\cdot A^t$

f) $\forall A \in K_m^n$: $A\cdot E_n = E_m\cdot A = A$ (dabei seien E_n bzw. E_m die n×n- bzw. m×m-Einheitsmatrix).

Satz 6.4: Sei A x = b ein lineares Gleichungssystem mit regulärer Koeffizientenmatrix A. Dann hat dieses Systems genau eine Lösung, nämlich $x = A^{-1} b$

Satz 6.5: Ist $A \in K_n^n$ invertierbar, so ist auch A^t invertierbar und es gilt $(A^t)^{-1} = (A^{-1})^t$.

Satz 6.6: Seien $A \in K_n^n$ regulär und $a_1,\ldots,a_r \in K_n$. Dann gilt:
$a_1,\ldots,a_r$ sind linear unabhängig $\Leftrightarrow$ $A\cdot a_1,\ldots,A\cdot a_r$ sind linear unabhängig.

Satz 6.7: Sei $A\cdot x = b$ ein lineares Gleichungssystem mit $A \in K_m^n$.

a) Der Nullraum von A ist ein Unterraum von K_n.

b) Die Lösungsmenge $\{ x \in K_n \mid A\cdot x = b \}$ des Gleichungssystems $A\cdot x = b$ ist entweder leer oder eine lineare Mannigfaltigkeit; zugehöriger Unterraum ist der Nullraum von A.

Satz 7.1: Für alle A gilt: $\det(A) = \det(A^t)$.

Satz 7.2: Multipliziert man alle Elemente einer Zeile der Determinante mit $c \neq 0$, so multipliziert sich det(A) mit c: $\det(c \cdot A) = c \cdot \det(A)$.

Satz 7.3: Sind in A zwei Zeilen gleich oder ist eine Zeile $= \mathbf{o}$, so ist $\det(A) = 0$.

Satz 7.4: Addiert man zu einer Zeile ein Vielfaches einer anderen Zeile, so bleibt det(A) unverändert

Satz 7.5: Vertauscht man zwei Zeilen (Spalten) von A, so ändert det(A) sein Vorzeichen.

Satz 7.6:

Ist $A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \ddots & & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{pmatrix}$. Dann ist $\det(A) = a_{11}a_{22} \ldots a_{nn}$.

Satz 7.7: Für $A,B \in K_n^n$ gilt: $\det(A\cdot B) = \det(A)\det(B)$.

Satz 7.8: Ist A regulär, so gilt $\det(A^{-1}) = \dfrac{1}{\det(A)}$.

Satz 7.9 *(Laplace'scher Entwicklungssatz):*

a) „Entwicklung von det(A) nach der i-ten Spalte“. Für jedes fixe $i \in \{1,\ldots,n\}$ gilt:

$$\det(A) = \sum_{j=1}^{n} (-1)^{j+i} \; a_{ji} \det(A^{j,i})$$

b) „Entwicklung von det(A) nach der k-ten Zeile“. Für jedes fixe $k \in \{1,\ldots,n\}$ gilt

$$\det(A) = \sum_{j=1}^{n} (-1)^{k+j} \; a_{kj} \det(A^{k,j})$$

Satz 7.10 *(Cramer´sche Regel) (Gabriel Cramer, 1704-1752):*

Im Gleichungssystem $A \cdot x = b$ sei A regulär, $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ und für $i \in \{1,\ldots,n\}$ sei A_i diejenige Matrix, die sich aus A ergibt, indem man die i-te Spalte durch b ersetzt [vgl. folgendes Beispiel]. Dann gilt

$$x_i = \frac{\det(A_i)}{\det(A)}$$

Satz 7.11: Für $A \in K_n^n$ sind folgende Bedingungen paarweise äquivalent:

a) λ ist ein Eigenwert von A.

b) $\lambda E - A$ ist singulär.

c) $\det(A - \lambda E) = 0$ (Bemerkung: $\det(A - \lambda E)$ ist ein Polynom, genannt das *charakteristische Polynom* von A)

Satz 7.12: A und ihre transponierte A^T besitzen dieselben Eigenwerte.

Satz 7.13: Seien A und B $n \times n$ Matrizen. Dann besitzen die Matrizen AB und BA dieselben Eigenwerte.

Satz 7.14: Ist λ ein Eigenwert der regulären Matrix A, dann ist ein λ^{-1} Eigenwert von ihrer Inversen A^{-1}.

Satz 7.15: Ist λ ein Eigenwert der Matrix A, dann ist λ^k Eigenwert von A^k.

Satz 7.16: Die Determinante einer $n \times n$ Matrix A ist gleich dem Produkt der Eigenwerte λ_i von A:

$$\det(A) = \prod_{i=1}^{n} \lambda_i$$

Satz 7.17: Die Summe der Eigenwerte λ_i einer Matrix A ist gleich der Summe der Diagonalelemente (der „*Spur*“) von A:

$$\sum_{i=1}^{n} \lambda_i = \sum_{i=1}^{n} a_{ii}$$

Satz 8.1: $$\sum_{x \in V(X)} d(x) = 2 \left| E(X) \right|$$

Satz 8.2: Jede Kantenfolge von x_1 nach x_n enthält einen Weg von x_1 nach x_n.

Satz 8.3: Sind $x \neq y$ zwei Knoten des Graphen X und $K(x) \cap K(y) \neq \emptyset$, so ist $K(x) = K(y)$.

Satz 8.4: Zwei Blöcke eines Graphen X haben höchstens einen gemeinsamen Knoten und dieser ist Artikulation von X.

Satz 8.5: Ein Knoten x ist Artikulation von X genau dann, wenn x in mindestens zwei Blöcken liegt.

Satz 8.6: Jede Kante und jeder Kreis von X liegen in genau einem Block von X.

Satz 8.7: Sei X ein zusammenhängender Graph und $e \in E(X)$. Dann sind die folgenden Aussagen äquivalent:

(i) e ist eine Brücke von X
(ii) e liegt auf keinem Kreis von X
(iii) Es gibt Knoten x und y von X, so dass e auf jedem Weg von x nach y liegt.

Satz 8.8: Ist X ein Graph mit $n = |V(X)|$ und $m = |E(X)|$, dann sind folgende Aussagen äquivalent:

(i) X ist ein Baum.
(ii) Je zwei Knoten in X sind durch genau einen Weg in X verbunden.
(iii) X ist zusammenhängend und jede Kante von X ist eine Brücke.
(iv) X ist zusammenhängend und $m = n-1$.
(v) X besitzt keinen Kreis und $m = n-1$.
(vi) X besitzt keinen Kreis. Verbindet man aber zwei Knoten von V(X), die nicht in X verbunden sind, durch eine Kante, so erhält man einen Graphen mit genau einem Kreis.

Satz 8.9: Ein g.Graph X ist stark zusammenhängend, genau dann, wenn X zusammenhängend ist und jede Kante $e \in E(X)$ auf einem g.Kreis in X liegt.

Satz 8.10: Ein Teilgraph T eines zusammenhängenden Graphen X ist genau dann ein spannender Baum von X, wenn folgende zwei Bedingungen erfüllt sind:

(i) T enthält keinen Kreis,
(ii) fügt man zu T eine Kante $e \in \{E(X) - E(T)\}$ hinzu, so enthält T genau einen Kreis.

Satz 8.11: Ist $X = (V(X), E(X))$ ein vollständiger Graph und sind die den Kanten $e \in E(X)$ zugeordneten Zahlen g(e) paarweise verschieden, dann hat das Problem des Minimalgerüstes eine eindeutige Lösung.

Satz 8.12: Ein binärer Baum B mit n Knoten hat
- mindestens die Höhe $h = \log_2(n+1) - 1$,
- höchstens $b = 2^h$ Blätter

bzw.
ein binärer Baum B der Höhe h hat höchstens $n = 2^{h+1} - 1$ Knoten.

Satz 8.13: Es gilt $q^{n-2} \leq F(n) \leq q^{n-1}$ für $n \geq 1$

Satz 8.14: Der Fibonaccibaum F_{h+1} der Höhe h hat F(h+3) – 1 Knoten.

Satz 8.15: Ist T ein ausgeglichener Baum mit n Knoten, dann gilt
$\log_2(n+1) - 1 \leq h(T) \leq 1{,}4404 \cdot \log_2(n+2) - 1{,}328$

Satz 8.16: Die Anzahl der Knoten in einem B(k,h) Baum ist *mindestens*
$$1 + 2\,\frac{(k+1)^h - 1}{k}$$

Satz 8.17: Die Anzahl der Knoten in einem B(k,h) Baum ist *höchstens*
$$\frac{(2k+1)^{h+1} - 1}{2k}$$

Satz 8.18: Sind X = (V(X), E(X)) und sein komplementärer Graph $\overline{X} = (V(X), \overline{E(X)})$ gegeben, dann spannt $Q(S) \subseteq V(X)$ in X genau dann eine Clique auf (induziert sie), wenn $V(X) \setminus Q(S)$ in $\overline{X}$ eine Knotenüberdeckung ist.

Satz 8.19: Ein zusammenhängender Graph X ist genau dann ein Euler-Graph, wenn jeder seiner Knoten geraden Grad hat.

Satz 8.20: Ist X (V(X), E(X)) zusammenhängend und eben, dann gilt
$|E(X)| - |V(X)| + 2 = g$ = Anzahl der Gebiete.

Satz 8.21: Ist X = (V(X), E(X)) mit $|V(X)| \geq 3$ planar, dann ist $|E(X)| \leq 3\,|V(X)| - 6$.

Satz 8.22: $\sum_{x \in aV(N)} \Phi(x) = 0$ und $\varphi(q) = -\,\varphi(s)$.

Satz 8.23 *(Max- Flow-Min-Cut Theorem)**:***
Der maximale Wert eines Flusses φ von der Quelle q zur Senke s ist gleich der minimalen Kapazität eines Schnittes.

Satz 8.24: Ein Matching M im Graphen X = (V(X),E(X)) ist genau dann maximal, wenn es bezüglich M keinen erweiternden Weg W gibt.

Satz 8.25: Ein Graph X ist genau dann paar, wenn er keine oder nur Kreise mit gerader Länge enthält.

Satz 10.1: Ist $d = d_{min}(C)$, so kann C bis zu d–1 Fehler erkennen und bis zu $\left\lfloor \frac{d-1}{2} \right\rfloor$ Fehler richtig decodieren.

Satz 10.2: Sei C ein (n,k)-Code mit Kontrollmatrix A.
a) $d_{min}(C)$ = das kleinste Gewicht eines Codeworts $\neq 0$.
b) $d_{min}(C) = rg(A) + 1$.

Satz 10.3:

a) $rg(A) = 2$, also $d_{min}(A) = 3$.

b) Ein Hamming-Code kann also alle Einfachfehler korrigieren und alle Doppelfehler erkennen.

c) Ist bei der Übertragung von x in y genau ein Fehler passiert, dann war er an der i-ten Stelle, wobei i die Binärzahl von $A \cdot y^t$ ist. (vgl. folgendes Beispiel)

Satz 10.4 *(ohne Beweis)**:***

Der so entstehende RS(n,k)-Code hat eine Minimaldistanz von q–k, kann also bis zu $\left\lfloor \frac{q-k}{2} \right\rfloor$ Fehler richtig decodieren.

Satz 11.1: Die lineare Kongruenzmethode (x_0, a, c, m) hat die maximale Periodenlänge m dann und nur dann, wenn

(i) ggT(c,m) = 1

(ii) a-1 ein Vielfaches von p für jeden primen Teiler von m ist

(iii) a-1 ein Vielfaches von 4 ist, falls m ein Vielfaches von 4 ist.

Satz 11.2: In einer Folge $x_{i+1} = a\ x_i \bmod m$ wird eine maximale Periode μ erreicht, wenn

(i) $ggT(x_0,m) = 1$ und

(ii) a primitives Element modulo m ist.

Für $m = 2^j$ gilt dann: $\mu(2) = 1$, $\mu(4) = 2$ und $\mu(2^j) = 2^{j-2}$ für $j \geq 3$.

Satz 11.3: Ist $m = 2^j$ mit $j \geq 4$, so ist a ein primitives Element modulo m dann und nur dann, wenn entweder $a \bmod 8 = 3$ oder $a \bmod 8 = 5$ ist.

Satz 11.4: Eine Matrix $A \in \mathbb{R}^{n \times n}$ ist genau dann diagonalisierbar, wenn sich mit n Eigenvektoren von A eine Basis von $\mathbb{R}_n$ bilden lässt. Im dreidimensionalen Fall bedeutet dies etwa, dass es drei linear unabhängige Eigenvektoren von A gibt. Diese n Eigenvektoren bilden dann die Spalten von C und damit erhält man $A = C \cdot D \cdot C^{-1}$.

Satz 11.5: Besitzt eine Matrix $A \in \mathbb{R}^{n \times n}$ n verschiedene Eigenwerte, so ist sie diagonalisierbar.

Satz 11.6: Es ist $R(E–dA) = D$ lösbar, wenn $0 < d < 1$ gilt.