Mathematik *explorativ* - Sammlung der Definitionen

Definition 1.1: (nach *Georg Cantor*, 1845-1918) Eine *Menge* ist eine Zusammenfassung verschiedener „Objekte unserer Anschauung oder unseres Denkens“ (welche die *Elemente* der Menge genannt werden) zu einem „Ganzen“. Falls x ein Element der Menge A ist, so bezeichnen wir dies mittels $x \in A$, andernfalls schreiben wir $x \notin A$.

Definition 1.2: Zwei Mengen A, B heißen gleich ($A = B$), falls jedes Element von A auch Element von B ist, und umgekehrt. Andernfalls schreibt man $A \neq B$.

Definition 1.3: Eine Menge A heißt *Teilmenge* einer Menge B, in Zeichen: $A \subseteq B$, falls jedes Element von A auch Element von B ist. Für $A \subseteq B$ und $A \neq B$ schreibt man auch $A \subset B$ (A heißt dann *echte Teilmenge* von B), statt $A \subseteq B$ schreibt man auch $B \supseteq A$ und sagt dann, B wäre eine *Obermenge* von A.

Definition 1.4: A, B, U seien Mengen mit $A \subseteq U$.

a) $A \cap B = \{x \mid x \in A \text{ und } x \in B\}$ heißt *Durchschnitt* von A und B. Gilt $A \cap B = \emptyset$, so heißen A und B *disjunkt*.

b) $A \cup B = \{x \mid x \in A \text{ oder } x \in B \text{ (oder beides)}\}$ heißt *Vereinigung* von A und B

c) $A \setminus B$ (manchmal auch: $A - B$) $= \{x \mid x \in A \text{ und } x \notin B\}$ heißt *Differenz* A minus B oder kurz „A ohne B“.

d) $A \Delta B = (A \setminus B) \cup (B \setminus A) = \{x \mid x \in A \text{ oder } x \in B \text{ (aber nicht beides)}\}$ heißt die *symmetrische Differenz* von A und B, gesprochen „A delta B“

e) $\mathbf{C}_U(A) = U \setminus A$ heißt *Komplement* von A in U (meist ist hier U eine übergeordnete Gesamtmenge, U heißt dann ein *Universum*).

Definition 1.5: I sei eine Menge und für jedes $i \in I$ sei A_i eine Menge.

$\bigcap_{i \in I} A_i = \{x \mid x \in A_i \text{ für alle } i \in I\}$

$\bigcup_{i \in I} A_i = \{x \mid x \in A_i \text{ für (mindestens) ein } i \in I\}$.

Definition 1.6: Seien A und B Mengen und $a \in A$, $b \in B$. Die Menge $\{a, \{a,b\}\}$, abgekürzt durch (a,b), heißt das *geordnete Paar* a,b. Weiters sei

$$A \times B = \{(a,b) \mid a \in A, b \in B\}.$$

$A \times B$ heißt das *(kartesische) Produkt* der Mengen A und B.

Für $A \times A$ schreibt man kurz A^2.

Manchmal, zB in der Graphentheorie, wo mit geordneten Paaren (a,b) eine „Kante“ vom Knoten a zu einem Knoten b gemeint ist, schreibt man auch <a,b> anstatt (a,b).

Man schreibt für $(A\times B)\times C$ oft auch kurz $A\times B\times C$. Die Notation $A^3, A^4, \ldots$ ist nun für Mengen definiert und jetzt kann man $\mathbb{R}^2$ mit der „Ebene“ und $\mathbb{R}^3$ mit dem „Raum“ unserer Anschauung identifizieren.

Ein Element $(a,b,c) \in A\times B\times C$ heißt auch *Tripel*,
ein $(a_1,a_2,\ldots,a_n) \in A_1\times A_2\times\ldots\times A_n$ (wofür man kurz $\bigtimes_{i=1}^{n} A_i$ schreibt) heißt kurz ein *n-Tupel*. A^1 wird mit A identifiziert.

Definition 1.7: A sei eine Menge. Die Menge aller Teilmengen von A heißt die *Potenzmenge* von A und wird mit $\mathrm{P}(A)$ oder 2^A abgekürzt.

Definition 1.8: Ein Nullteiler ist ein vom Nullelement verschiedenes Element a, für das es ein Element $b \neq 0$ gibt, sodass $ab = 0$. Ein Ring ohne Nullteiler heißt nullteilerfrei.

Z ist nullteilerfrei, denn sind $a, b \in Z$ und gilt $a \cdot b = 0$, so gilt entweder $a = 0$, oder $b = 0$, oder $a = b = 0$

Definition 1.9:

$$|n| = \begin{cases} n \text{ für } n \geq 0 \\ -n \text{ für } n < 0 \end{cases}$$

Definition 1.10: Die ganze Zahl $b \neq 0$ teilt die ganze Zahl a, kurz: b / a, wenn es eine ganze Zahl q gibt, sodass $a = b \cdot q$. Die Zahl b heißt dann *Teiler* von a und q heißt *komplementärer Teiler*. Wenn b die Zahl a nicht teilt, schreibt man $b \nmid a$.

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}.

Definition 1.12 ***(Zweierkomplement):***
Ist $a \in \mathbb{Z}$, so ist der Wert von a in einem Wort der Länge n mit $d_{n-1}\, d_{n-2} \ldots d_1, d_0, d_i \in \{0,1\}$ definiert als

$$a = -d_{n-1} \cdot 2^{n-1} + \sum_{i=0}^{n-2} d_i d^i$$

Definition 1.13: $n! = n \cdot (n-1) \cdot \ldots \cdot 1$ für $n \in \mathbb{N}$, man sagt dazu *n Fakultät*.

Definition 1.14: $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ ist der Binomialkoeffizient „n über k“.

Definition 1.15: Eine *Relation* R von einer Menge A in eine Menge B ist eine Teilmenge von A×B. Für (a,b) ∈ R schreiben wir auch aRb, für (a,b) ∉ R auch a $\not R$ b. Ist A = B, so sprechen wir von einer *Relation auf* A.
$R^{-1} := \{(b,a) \mid (a,b) \in R\}$ heißt die zu R *inverse Relation* (von B nach A).

Definition 1.16: Eine Relation R von A nach B heißt funktional oder auch eine Funktion, falls gilt: Für jedes a ∈ A gibt es genau ein b ∈ B, sodass (a,b) ∈ R.

Definition 1.17: R sei eine Relation auf einer Menge A.

a) R heißt *reflexiv*, falls für alle a ∈ A gilt: aRa
b) R heißt *symmetrisch*, falls für alle a,b ∈ A gilt: aRb ⇒ bRa
c) R heißt *antisymmetrisch*, falls für alle a,b ∈ A gilt: (aRb ∧ bRa) ⇒ a=b
d) R heißt *transitiv*, falls für alle a,b,c ∈ A gilt: (aRb ∧ bRc) ⇒ aRc

Definition 1.18: Eine reflexive, symmetrische und transitive Relation auf einer Menge A heißt eine Äquivalenzrelation. Eine reflexive, antisymmetrische und transitive Relation auf A heißt eine Ordnungsrelation.

Definition 1.19: Sei R eine funktionale Relation, also eine Funktion von A nach B. Dann heißt A der *Definitionsbereich* und B der *Bildbereich* von R. Das für jedes a ∈ A eindeutig bestimmte b ∈ B mit (a,b) ∈ R heißt der *Funktionswert* von a unter R, man schreibt dann b = R(a). Die vollständige Notation dieser Funktion mit diesen Begriffen ist nun:

$$R: A \to B,\ a \to R(a)$$

$R(A) := \{R(a) \mid a \in A\}$ heißt das *Bild* von A unter R. Statt „Funktion“ sagt man auch oft „*Abbildung*“.

Definition 1.20 und Beispiele:

a) Für jede Menge A ist $id_A: A \to A,\ a \to a$ eine Funktion, genannt die *identische Funktion* auf A.
b) $f: \mathbb{R} \to \mathbb{R},\ x \to x^2$ und $sin: \mathbb{R} \to \mathbb{R},\ x \to \sin(x)$ sind sogenannte „reelle“ Funktionen, also Funktionen, wobei Definitions- und Bildmenge Teilmengen der reellen Zahlen sind.
sin(x), die Sinusfunktion, ist ein Beispiel für die so genannten *trigonometrischen* Funktionen.
c) $w: \mathbb{N} \to \mathbb{R},\ x \to \pm\sqrt{x}$ ist keine Funktion, denn jede natürliche Zahl hat zwei Bilder. w heißt *Wurzelfunktion*.
d) $|\ |: \mathbb{R} \to \mathbb{R},\ x \to |x|$ ordnet jeder reellen Zahl ihren Absolutbetrag zu., | | heißt die *Betragsfunktion.*

Definition 1.21: f: $A \to B$ sei eine Funktion.

a) f heißt *injektiv*, falls gilt: Für alle $a_1, a_2 \in A$: $(f(a_1) = f(a_2) \Rightarrow a_1 = a_2)$, in Worten:
Jeder Funktionswert der Bildmenge wird maximal einmal durch ein Element der Definitionsmenge erreicht.

b) f heißt *surjektiv*, falls $f(A) = B$ ist, in Worten: Jeder Funktionswert der Bildmenge wird höchstens einmal durch ein Element der Definitionsmenge erreicht.

c) f ist *bijektiv*, falls f injektiv und surjektiv ist, in Worten: Jeder Funktionswert der Bildmenge wird genau einmal durch ein Element der Definitionsmenge erreicht.

Definition 1.22: Seien f: $A \to B$ und g: $B \to C$ Funktionen. Dann heißt $g \circ f$: $A \to C$, $a \to g(f(a))$ *die Hintereinanderausführung von g nach f,* man beachte hier die Reihenfolge!

Definition 2.1: Eine ganze Zahl $c \in \mathbb{Z}$ heißt *gemeinsamer Teiler* von $a, b \in \mathbb{Z}$, wenn c / a und c / b.

Definition 2.2: Es heißt $d = ggT(a,b)$ der *größte gemeinsame* Teiler von a und b, wenn
(i) d / a und d / b
(ii) für jeden gemeinsamen Teiler c von a und b gilt $c \leq d$.

Definition 2.3: Eine Zahl $u \in \mathbb{N}$ heißt *gemeinsames Vielfaches* von $a, b \in \mathbb{N}$, wenn a / u und b / u. Es heißt $v = kgV(a,b)$ das *kleinste gemeinsame Vielfache* von a und b, wenn
(i) a / v und b / v
(ii) für jedes gemeinsame Vielfache u von a und b gilt $u \geq v$.

Definition 2.4: Eine natürliche Zahl $p > 1$ heißt Primzahl, wenn sie außer 1 und p selbst keine weiteren (positiven) Teiler hat.

Definition 2.5: Seien $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}$.
Es heißt *„a kongruent b modulo m“,* wenn $m / (a–b)$.
Man schreibt $a \equiv b \bmod m$ oder auch $a \equiv_m b$. Die Zahl m ist der *Modul*.

Definition 2.6: Ein System $r_1, r_2, ..., r_m$ heißt *vollständiges Restsystem mod m*, wenn jede der Zahlen r_i genau einer Restklasse mod m angehört, d.h. wenn sie paarweise *inkongruent* sind: $r_i \not\equiv r_j \bmod m$ für $i \neq j$.

Definition 2.7: Die Eulersche φ-Funktion $\varphi(n)$ ist die Anzahl der zu n teilerfremden Zahlen aus $\{1,2,\ldots,n\}$.

Definition 2.8: Ist $ggT(a,m) = 1$, so heißt a *n-ter Potenzrest modulo m*, wenn es ein x gibt mit $x^n \equiv a \bmod m$.

Definition 2.9: Ist $ggT(a,m) = 1$ so heißt a *Quadratrest modulo m ,*wenn es ein $x \in \mathbb{Z}$ gibt, sodass $x^2 \equiv a \bmod m$. Gibt es so ein x nicht, heißt a *Nichtrest modulo m*.
Wir schreiben manchmal zur Vereinfachung *QR(m)* bzw. *NR(m).*

Definition 3.1: $c = a + b = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ a_2 + b_2 \end{pmatrix}$

Definition 3.2: Sind $\boldsymbol{a} = (a_1, a_2)$ und $\boldsymbol{b} = (b_1, b_2)$ zwei Vektoren, so definiert man ihr *Skalarprodukt* (oder: *Inneres Produkt*) $\boldsymbol{a} \cdot \boldsymbol{b} := a_1b_1 + a_2b_2$.

Definition 3.3: $\| \boldsymbol{v} \| := \sqrt{v \cdot v}$ heißt Norm oder Länge von $\boldsymbol{v}$

Definition 3.4: Unter dem skalaren Produkt $\boldsymbol{a} \cdot \boldsymbol{b}$ (kurz : $\boldsymbol{a}\,\boldsymbol{b}$) zweier Vektoren $\boldsymbol{a}$ und $\boldsymbol{b}$ der Längen $\| \boldsymbol{a} \|$ bzw. $\| \boldsymbol{b} \|$ versteht man $\boldsymbol{a} \cdot \boldsymbol{b} := \| \boldsymbol{a} \| \, \| \boldsymbol{b} \| \cos(\boldsymbol{a}, \boldsymbol{b})$

Definition 3.5: Die Vektoren $\boldsymbol{r}$ und $\boldsymbol{s}$ heißen linear abhängig, wenn es reelle Zahlen λ_1, λ_2 gibt, die nicht beide Null sind, sodass gilt

$$\lambda_1 \boldsymbol{r} + \lambda_2 \boldsymbol{s} = \boldsymbol{o}$$

Die Vektoren r und s heißen linear unabhängig, wenn die Beziehung $\lambda 1 r + \lambda 2 s = o$ nur für $\lambda 1 = \lambda 2 = 0$ gilt.

Definition 3.6: Das *vektorielle Produkt* von $\boldsymbol{a} = (a_1, a_2, a_3)$ und $\boldsymbol{b} = (b_1, b_2, b_3) \in \mathbb{R}^3$ ist der *Vektor* $\boldsymbol{a} \times \boldsymbol{b} = (a_2b_3 - b_3a_2, a_3b_1 - a_1b_3, a_1b_2 - a_2b_1) \in \mathbb{R}^3$

Definition 4.1: Eine *zweistellige Verknüpfung* auf einer Menge M ist eine Abbildung $\otimes : M \times M \to M$.

Definition 4.2: Die Verknüpfung $\otimes$ in der Menge M heißt *assoziativ*, wenn das *Assoziativgesetz* gilt:
Für alle $x, y, z \in M$ ist $(x \otimes y) \otimes z = x \otimes (y \otimes z)$.

Definition 4.3: Eine nicht-leere Menge M zusammen mit einer assoziativen Verknüpfung $\otimes$ heißt *Halbgruppe*.

Definition 4.4: Ist $(M, \otimes)$ eine Halbgruppe, so heißt $e \in M$ *neutrales Element*, wenn für jedes $x \in M$ gilt: $x \otimes e = e \otimes x = x$.

Definition 4.5: Eine Halbgruppe $(M, \otimes)$ heißt *Monoid*, wenn M ein *neutrales Element* enthält.

Definition 4.6: Eine Menge G mit der Verknüpfung $\otimes$ heißt *Gruppe*, wenn gilt

(i) das Assoziativgesetz: $(a \otimes b) \otimes c = a \otimes (b \otimes c)$ für alle $a,b,c \in G$

(ii) es gibt ein neutrales Element $e \in G$ mit $a \otimes e = e \otimes a = a$ für alle $a \in G$

(iii) zu jedem $a \in G$ gibt es ein *inverses* Element x, sodass $a \otimes x = x \otimes a = e$.

Definition 4.7: Es sei S eine Menge mit genau n Elementen. Diese seien mit 1, 2, ..., n bezeichnet. Eine *Permutation* dieser Elemente ist eine Umordnung in der Reihenfolge bei der Aufzählung.

Definition 4.8: Eine Teilmenge $U \subseteq G$ heißt *Untergruppe* von $(G, \otimes)$, wenn U bezüglich der Verknüpfung $\otimes$ selbst eine Gruppe ist.

Definition 4.9: Ist $(G, \otimes)$ eine Gruppe und $x \in G$, so heißt die kleinste natürliche Zahl r mit der Eigenschaft $x^r = e$ die *Ordnung* des Elementes x.

Definition 4.10: Eine Gruppe $(G, \otimes)$ heißt *zyklische Gruppe,* wenn es ein Element $a \in G$ gibt, sodass es für jedes $x \in G$ ein $k \in \mathbb{Z}$ gibt, sodass $x = a^k$.
Ein solches Element a heißt *Generator von G* oder *erzeugendes Element* oder *Erzeugende der zyklischen Gruppe.*

Definition 4.11: Ein Element $a \in G$ einer zyklischen Gruppe G heißt *Primitivwurzel*, wenn ord(a) = ord(G).

Definition 4.12: Sei $(G, \otimes)$ eine Gruppe, $U \subseteq G$ eine Untergruppe und $g \in G$. Dann heißt die Menge gU eine *Linksnebenklasse* (bzw. Ug: *Rechtsnebenklasse*) von G nach U.

Definition 4.13: Eine Untergruppe U einer Gruppe $(G, \otimes)$ heißt *Normalteiler* N, wenn die Linksnebenklassen und die Rechtsnebenklassen von G nach U übereinstimmen, wenn also gU = Ug für alle $g \in G$.

Definition 4.14: Sind G $(\oplus)$ und H $(\otimes)$ zwei Gruppen und ist $\varphi : G \to H$ eine bijektive Abbildung der Elemente von G auf die Elemente von H, mit

$$\varphi(a \oplus b) = \varphi(a) \otimes \varphi(b)$$

so heißt φ ein Gruppenisomorphismus.

Definition 4.15: Ein *Ring* ist eine nicht-leere Menge M in Verbindung mit zwei Operationen, Addition „+“ und Multiplikation „·“, sodass folgende Regeln gelten:

(1) wenn $x, y \in M$ dann $x + y \in M$ (Abgeschlossenheit bzgl. „+“)
(2) $x + y = y + x$ für alle $x, y \in M$ ((M,+) ist kommutativ)
(3) $(x + y) + z = x + (y + z)$ für alle $x, y, z \in M$ ((M,+) ist assoziativ)
(4) es gibt ein Element $0 \in M$, sodass $x + 0 = 0 + x$ für alle $x \in M$ („Nullelement“)
(5) für jedes $x \in M$ gibt es ein Element $-x \in M$, sodass $x + (-x) = 0 = (-x) + x$ (inverses Element existiert)
(6) wenn $x, y \in M$, dann $xy \in M$ (Abgeschlossenheit bzgl. „·“)
(7) $(xy) z = x (yz)$ für alle $x, y, z \in M$ ((M, ·) ist kommutativ)
(8) $x (y + z) = xy + xz$ und $(x + y) z = xz + yz$ für alle $x, y, z \in M$ (Distributivität)

Definition 4.16: Ein *Körper* ist ein Ring, für den folgende zusätzliche Regeln gelten:

(9) $xy = yx$ für alle $x, y \in M$
(10) es gibt ein „Einselement“ $e \in M$ (statt e schreibt man gelegentlich auch 1), sodass $xe = x = ex$ für alle $x \in M$
(11) für jedes $x \in M^* = M \setminus \{0\}$ gibt es ein *inverses* Element $x^{-1} \in M \setminus \{0\}$, sodass $xx^{-1} = x^{-1}x = e$.

Definition 4.17: Ist (M, +, ·) ein Ring, der bezüglich „·“ kommutativ ist, so heißt er *kommutativer Ring*. Ist zusätzlich (M \ {0}, ·) eine abelsche Gruppe, so heißt (M, +, ·) ein *Körper*.

Definition 4.18: Ein *Integritätsbereich* ist ein kommutativer Ring mit Einselement ohne Nullteiler.

Definition 4.19: Sei K ein Körper. Ein Ausdruck der Gestalt

$$p = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$$

mit $n \in \mathbb{N}_0$ und $a_i \in K$ für i = 0, 1, … n-1, n heißt *Polynom über* K.
Gilt $a_i = 0$ für i = 0, 1, ..., n, so heißt p das *Nullpolynom*.
Der *Grad* von p ist die höchste in p tatsächlich auftretende Potenz von x.

Definition 4.20: Sind p, q zwei Polynome über einem Körper K, so ist
$p + q = (a_n + b_n) x^n + (a_{n-1} + b_{n-1}) x^{n-1} + ... + (a_0 + b_0)$
man addiert also „komponentenweise“

Definition 4.21: Sind p, q zwei Polynome über einem Körper K, so ist
$p \cdot q = a_n b_m x^{n+m} + \ldots + (a_0 b_r + a_1 b_{r-1} + ... + a_{r-1} b_1 + a_r b_0) x^r + \ldots + a_0 b_0$

Definition 4.22: Ein Polynom p über dem Körper K heißt *reduzibel*, falls es Polynome $q, s \in K[x]$ mit Grad $Gd \geq 1$ gibt, sodass $p = q \cdot s$.
Andernfalls heißt p *irreduzibel*.

Definition 4.23: Ein Element $\alpha \in K$, für das gilt $p(\alpha) = a_n\alpha^n + a_{n-1} \alpha^{n-1} + ... + a_1\alpha + a_0 = 0$ heißt *Nullstelle* der Polynomfunktion p.

Definition 4.24: $GF(p^n) := \{ k_0 + k_1 x + \ldots + k_{n-1} x^{n-1} \mid k_i \in \mathbb{Z}_p \}$
heißt Galoisfeld der Ordnung p^n.

Definition 5.1: Es sei (K,+,·) =: K ein Körper mit neutralem Element 0 für die Addition und 1 für die Multiplikation. Eine abelsche Gruppe (V,+) heißt *Vektorraum über* K oder *linearer Raum*, falls eine Abbildung $K \times V \to V$, $(\lambda,v) \to \lambda v$ definiert ist, welche für alle $\lambda,\lambda' \in K$ und alle $v,v' \in V$ die Rechengesetze

a) $(\lambda+\lambda')v = \lambda v + \lambda' v$
b) $\lambda(v+v') = \lambda v + \lambda v'$
c) $\lambda(\lambda' v) = (\lambda\lambda')v$
d) $1v = v$

erfüllt.

Definition 5.2: Sei V ein Vektorraum über K. Eine Teilmenge $U \subseteq V$, welche bzgl. der auf U eingeschränkten Operationen selbst einen Vektorraum bildet, heißt ein *Unterraum* von V. Dieser Umstand wird dann mit $U \leq_K V$ bezeichnet.

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 ~.

Satz 5.4 und Definition:

a) Sei ~ 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*.

Definition 5.3: Sei V ein Vektorraum über dem Körper K, seien $v_1,\ldots,v_n \in V$ und $\lambda_1,\ldots,\lambda_n \in K\backslash\{0\}$. Dann heißt $\lambda_1 v_1 + \ldots + \lambda_n v_n$ eine *Linearkombination* der Vektoren $v_1,\ldots,v_n$. Ist $S = \{v_1,\ldots,v_n\}$, so heißt $L(S) := \{\lambda_1 v_1 + \ldots + \lambda_n v_n \mid \lambda_1,\ldots, \lambda_n \in K\}$ die *lineare Hülle* von S. Weiters definieren wir die lineare Hülle der leeren Menge, $L(\emptyset) := \{\mathbf{o}\}$.

Definition 5.4: Die Vektoren $v_1,v_2,\ldots,v_n$ eines Vektorraums ${}_K V$ heißen *linear unabhängig*, falls für $\lambda_1,\ldots,\lambda_n \in K$ gilt:

$$\lambda_1 v_1 + \ldots + \lambda_n v_n = \mathbf{o} \Rightarrow \lambda_1 = \ldots = \lambda_n = 0$$

Andernfalls heißt sie *linear abhängig*.

Definition 5.5: Eine Familie $B = (b_1,\ldots,b_n) \subseteq {}_K V$ heißt eine *Basis* von ${}_K V$, falls gilt:

a) B ist linear unabhängig

b) $L(B) = V$

Achtung! Es ist wichtig, hier für B den Begriff „Familie“ und nicht „Menge“ zu fordern, die Reihenfolge der Elemente ist also nicht egal. Mehr dazu in Kürze beim Thema „Koordinaten“

Definition 5.6 und Beispiel:

a) $(e_1, e_2,..., e_n) := ((1,0,\ldots,0),(0,1,0,\ldots,0),\ldots,(0,\ldots,0,1))$ heißt die *kanonische Basis* des $\mathbb{R}^n$ (kanonisch soll heißen „natürlich“) Im $\mathbb{R}^3$ etwa lässt sich jeder Vektor (x, y, z) als x (1,0,0) + y (1,1,0) + z (0,0,1) darstellen, daher ist ((1,0,0), (0,1,0), (0,0,1)) eine Basis des $\mathbb{R}^3$.

b) Für jedes $c \in \mathbb{R}$ ist ((1,0),(c,1)) eine Basis des ${}_{\mathbb{R}}\mathbb{R}^2$. Jedes Paar $(x,y) \in \mathbb{R}^2$ lässt sich eindeutig als $(x - y\,c)\,(1,0) + b\,(c,1)$ darstellen, zum Beispiel für B = ((1,0), (2,1)) gilt: $(3,5) = (3 - 5\cdot 2) \cdot (1,0) + 5 \cdot (2,1) = -7 \cdot (1,0) + 5 \cdot (2,1) = (-7,0) + (10,5) = (3,5)$!

c) $\{1, \mathrm{i}\}$ ist eine Basis von ${}_{\mathbb{R}}\mathbb{C}$. Jede komplexe Zahl $x + \mathrm{i}\, y$ lässt sich eindeutig als $x \cdot 1 + y \cdot \mathrm{i}$ schreiben.

d) Analog lässt sich zeigen, dass ((1,1,1),(1,1,0),(1,0,0)) eine weitere Basis für ${}_K K^3$ (für jeden Körper K) ist.

e) $(1, x, x^2, \ldots, x^n)$ ist die kanonische Basis des ${}_{\mathbb{R}}P_n(\mathbb{R})$.

Definition 5.7: Seien B und v wie vorher. Dann heißen die λ_i *Koordinaten* von v und wir definieren $(v)_B := (\lambda_1, \ldots, \lambda_n)$ also die Koordinaten von v bezüglich der Basis B.

Definition 6.1: M sei eine Menge und m,n seien in $\mathbb{N}$.

(a) Eine m×n-Matrix über M ist eine durch $\{1,\ldots,m\} \times \{1,\ldots,n\}$ indizierte Familie

$$A = (a_{(i,j)})_{(i,j) \in \{1,\ldots,m\}\times\{1,\ldots,n\}}$$

von Elementen aus M, die man etwas kürzer als

$$A = (a_{ij})_{1 \le i \le m,\ 1 \le j \le n}$$

oder noch kürzer als (a_{ij}) anschreibt. Eine andere Schreibweise ist

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}.$$

Dabei sei $Z_i := (a_{i1},a_{i2},\ldots,a_{in})$ die i-te *Zeile* und $S_j := \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}$

die j-te *Spalte* von A.

M_m^n bezeichnet die Menge aller m×n-Matrizen über M.

(b) Eine n×n-Matrix bezeichnet man als *quadratische Matrix*,

(c) In einer quadratischen Matrix $A = (a_{ij}) \in M_n^n$ bezeichnet man die Folge $(a_{11},a_{22},\ldots,a_{nn})$ als *Hauptdiagonale* von A, so ist etwa für obiges a die Hauptdiagonale gleich (1, –1, 2)

(d) Die zu $A = (a_{ij})_{1 \le i \le m,\ 1 \le j \le n} \in M_m^n$ *transponierte Matrix* ist durch $A^t := (a_{ji})_{1 \le j \le n,1 \le i \le m} \in M_n^m$ gegeben.

(e) Wenn beide Matrizen dieselbe „Dimension“ – also dieselbe Anzahl von Zeilen bzw. Spalten – haben und an jeder Komponente a_{ij} gleich sind, betrachtet man die Matrizen als gleich:
Sei also $A = (a_{ij}) \in M_m^n$, $B = (b_{rs}) \in M_p^q$, dann gilt:

$$A = B \Leftrightarrow (m = p \wedge n = q \wedge \forall\, (i,j) \in \{1,\ldots,m\} \times \{1,\ldots,n\} : a_{ij} = b_{ij})$$

Definition 6.2:

(a) $O := \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \in K_m^n$ heißt die *Nullmatrix* von K_m^n und

$E := \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \in K_n^n$ die *Einheitsmatrix* des K_n^n.

Die Zeilen einer Matrix $A \in K_m^n$ sind (Zeilen-)Vektoren $\in K^n$, die Spalten sind (Spalten-) Vektoren aus K_m. Weiters gilt $K_m^1 = K_m$ und $K_1^n = K^n$ (aber $K_1^1 \neq K$).

(b) Matrizen der Form $A = (a_{ij})$ mit $a_{ij} = 0$ für $i > j$ heißen *obere*, solche mit $a_{ij} = 0$ für $i<j$ *untere Dreiecksmatrizen*.

(c) Ist $a_{ij} = 0$ für $i \neq j$, so heißt $A \in K_n^n$ eine *Diagonalmatrix* und wird auch statt $A = \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & a_{22} & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{pmatrix}$ als $\mathrm{diag}(a_{11},a_{22},\ldots,a_{nn})$ geschrieben, so

Definition 6.3: Seien a,b Elemente einer beliebigen nicht-leeren Menge.

$$\delta_{a,b} := \begin{cases} 1 & \text{für } a = b \\ 0 & \text{sonst} \end{cases}$$

δ heißt das *Kronecker-Symbol* (nach *Leopold Kronecker*, 1823-1891). Beispielsweise ist $E = (\delta_{ij})$, also die Matrix, deren Einträge genau für $i = j$ den Wert 1 haben, ansonsten 0.

Definition 6.4: Es seien $A = (a_{ij})$ und $B = (b_{ij})$ Matrizen aus K_m^n und es sei $\lambda \in K$.
$A+B := (a_{ij} + b_{ij})$; $\lambda A := (\lambda a_{ij})$

Definition 6.5: Für $a = (a_1,\ldots,a_n) \in K^n$, $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in K_n$ und $\lambda \in K$ sei

$$a \cdot x := a_1x_1 + a_2x_2 + \ldots a_nx_n,$$

also das aus Kapitel 3 bekannte Skalarprodukt zweier Vektoren.

Definition 6.6: Seien $A = (a_{ij}) = \begin{pmatrix} Z_1 \\ \vdots \\ Z_n \end{pmatrix}_{Matrix} \in K_m^n$ (also eine Matrix gegeben durch ihre Zeilenvektoren) und $B = (b_{kr}) = (S_1,\ldots,S_p)_{matrix} \in K_n^p$ (gegeben durch die Spaltenvektoren). Dann sei $A \cdot B := (c_{ir}) \in K_m^p$ mit $c_{ir} = Z_i \cdot S_r$.

Definition 6.7: Ein *lineares Gleichungssystem* über einem Körper K von m Gleichungen in n Unbekannten ist eine m×(n+1)-Matrix über K, also in der Schreibweise des Gleichungssystems zu Beginn dieses Kapitels:

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & b_m \end{pmatrix} \in K_m^{n+1}$$

Die m×n-Matrix $A = \begin{pmatrix} a_{11} & \cdots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & b_m \end{pmatrix} \in K_m^n$

heißt die *Koeffizientenmatrix* des Gleichungssystems.

Definition 6.8: Gibt es zu $A \in K_n^n$ ein $B \in K_n^n$ mit $AB = BA = E$, so nennt man A auch *regulär*, andernfalls *nicht-regulär* oder auch *singulär*. Die Matrix B heißt die zu A *inverse Matrix* und wird mit A^{-1} bezeichnet.

Definition 6.9: Der *Nullraum* einer Matrix $A \in K_m^n$ ist die Lösungsmenge des linearen Gleichungssystems $A \cdot x = \mathbf{o}$.

Definition 7.1: Für A sei $A^{i,k}$:= die Matrix, die man aus A erhält, indem man die i-te Zeile und k-te Spalte streicht

Definition 7.2: Die Determinante det(A) ist eine Abbildung von der Menge aller quadratischen Matrizen über einem Ring nach diesem Ring, die nach den Regeln (a)- (d) berechnet wird.
Im für uns wichtigsten Fall, dass der Ring gleich dem Körper der reellen Zahlen ist, d.h. die Matrixelemente a_{ik} aus $\mathbb{R}$ sind, ist demnach det(A):
$\mathbb{R}^{n^n} \to \mathbb{R}$

Definition 7.3: Eine *Fehlstelle* in einer Permutation π ist ein Paar (π(i),π(j)) mit i < j, aber π(i) > π(j). Hat π f Fehlstellen, so heißt sign(π) := $(-1)^f$ die *Signatur* von π.

Definition 7.4: Sei A = eine n x n Matrix mit den Elementen a_{ik} aus einem Körper K.
Für $A = (a_{ik})_{1 \le i,\, k \le n}$ definiert man
$\det A = \det(a_{ik}) = \sum_{\pi \in S_n} \text{sign}\,(\pi)\; a_{1,\pi(1)}, a_{2,\pi(2)} \ldots a_{n,\pi(n)}$
als die *Determinante* von A.

Definition 7.5: Gilt für $A \in K^n_n$, $\boldsymbol{x} \in K^n$, $\lambda \in K$, mit $\boldsymbol{x} \neq \boldsymbol{o}$, die Gleichung $A \cdot \boldsymbol{x} = \lambda \boldsymbol{x}$, so heißt $\boldsymbol{x}$ ein *Eigenvektor* von A zum *Eigenwert* λ, der größte Eigenwert von A heißt *dominanter* Eigenwert. Die Beziehung $A \cdot \boldsymbol{x} = \lambda \boldsymbol{x}$ wird oft als $(\lambda E - A) = \boldsymbol{o}$ geschrieben.

Definition 7.6: Reelle Zahlen $\lambda \in \mathbb{R}$, für die das homogene lineare Gleichungssystem mit seiner n x n Koeffizientenmatrix $A - \lambda E$ nichttriviale Lösungen hat, heißen Eigenwerte der Matrix A.

Definition 8.1: Ein *ungerichteter Graph* X besteht aus einer Menge V = V(X), den *Knoten* von X, und einer Menge E = E(X) von ungeordneten Paaren e = [x,y] verschiedener Elemente aus V, den *Kanten* von X.

Definition 8.2: Gegeben seien zwei Graphen $X_1 = (V1,E1)$ und $X_2 = (V2,E2)$. Eine bijektive Abbildung f von V_1 und V_2 heißt ein Isomorphismus von X_1 auf X_2, wenn gilt: $[x,y] \in E_1$ genau dann, wenn $[f(x),f(y)] \in E_2$ ist. Gibt es einen Isomorphismus von X_1 auf X_2, so nennt man X_1 und X_2 isomorph, symbolisch $X_1 \cong X_2$.

Definition 8.3: Ein Graph $X_1 = (V_1,E_1)$ heißt Teilgraph von X = (V,E), wenn $V_1 \subseteq V$ und $E_1 \subseteq E$ ist. Ein Teilgraph von X ist spannender Teilgraph von X, wenn $V_1 = V$ ist. Enthält E_1 alle Kanten aus E, deren Endpunkte in V_1 liegen, so sagt man, dass X_1 von $V_1 \subseteq V$ in X aufgespannt wird oder dass X_1 ein gesättigter Teilgraph von X ist.

Definition 8.4: Eine Kantenfolge von x_1 nach x_n in einem Graphen X ist eine endliche Folge von Kanten$[x_1,x_2],[x_2,x_3],...,[x_{i-1},x_i],[x_i,x_{i+1}],...,[x_{n-1},x_n]$, so dass je zwei aufeinanderfolgende Kanten einen Endpunkt gemeinsam haben.

Definition 8.5: Ein *Kantenzug* ist eine Kantenfolge, in der alle Kanten voneinander verschieden sind. Ein *Weg* W ist eine offene Kantenfolge, in der alle Knoten verschieden sind. Einen Knoten x fassen wir ebenfalls als Weg auf.

Definition 8.6: Ein *Kreis* ist ein geschlossener Kantenzug, bei dem die Knoten $x_1,x_2,...x_{n-1}$ alle verschieden sind.

Definition 8.7: Ein Graph heißt *zusammenhängend*, wenn je zwei seiner Knoten durch einen Weg verbunden sind.

Definition 8.8: Die *Komponente K(x) des Knotens x* ist die Menge aller Knoten y, die mit x durch einen Weg verbunden sind: $K(x) = \{y : \exists\, W\ (x,y)\}$.

Definition 8.9: Die von den K(x) aufgespannten Teilgraphen heißen *Komponenten von X.*

Definition 8.10: Ist X ein Graph und $A \subset V(X)$, so erhält man durch Streichen von A in X, symbolisch X-A, folgenden Graphen:
$V(X-A) = V(X)-A$
$E(X-A) = \{[x,y] \mid [x,y] \in E(X), x \notin A \text{ und } y \notin A\}$.

Definition 8.11: Ein Knoten $x \in V(x)$ heißt *Artikulation* von X oder *Zerfällungsknoten*, wenn $X - \{x\}$ mehr Komponenten besitzt als X.

Definition 8.12: Ein Teilgraph X_1 von X heißt *Block* von X, wenn er ein gesättigter und zusammenhängender Teilgraph ist, keine Artikulation enthält und maximal ist, d.h., wenn kein Teilgraph X_2 mit $V(X_2) \supset V(X_1)$ diese Eigenschaft besitzt.

Definition 8.13: Ist $F \subset E(X)$, so ist der Graph $X - [F]$ definiert auf V(X) durch die Kanten aus $E(X) - F$.

Definition 8.14: Eine Kante $e \in E(X)$ heißt *Brücke* von X, wenn $X - [e]$ mehr Komponenten besitzt als X.

Definition 8.15: Ein zusammenhängender ungerichteter Graph ohne Kreis heißt *Baum*. Ist jede Komponente eines Graphen X ein Baum, so heißt X ein *Wald*.

Definition 8.16: Ist X = (V(X),E(X)) ein zusammenhängender Graph und T ein Teilgraph von X, dann heißt der Graph T = (V(T),E(T)) ein *spannender Baum* oder *Gerüst* von X, wenn V(T) = V(X) *und* T ein Baum ist.

Definition 8.17: Ein *gerichteter Graph X* (kurz: *g.Graph*) besteht aus einer Menge V = V(X), den Knoten von X, und einer Menge E = E(X) von geordneten Paaren <x,y> verschiedener Elemente aus V, den Kanten von X.

Definition 8.18: $d^+(x) = \{ \mid <x,y> \mid <x,y> \in E(X) \mid \}$
$d^-(x) = \{ \mid <y,x> \mid <y,x> \in E(X) \mid \}$

Definition 8.19: Unter dem *Grad* d(x) eines Knotens $x \in V(X)$ versteht man $d(x) = d^+(x) + d^-(x)$.

Definition 8.20: Ein g.Graph X heißt *stark zusammenhängend*, wenn je zwei Knoten x,y durch einen g.Weg W(x,y) verbunden sind.

Definition 8.21: Eine *starke Komponente* eines g.Graphen X ist ein maximaler, stark zusammenhängender Teilgraph von X.

Definition 8.22: Ein g.Graph X heißt *azyklisch*, wenn er keine g.Kreise enthält.

Definition 8.23: Eine *Arboreszenz* A ist ein azyklischer Graph A, in dem genau für ein $x_0 \in V(A)$ gilt $d^-(x_0) = 0$ und für alle übrigen Knoten $d^-(x) = 1$.

Definition 8.24: Ist X = (V(X), E(X)) ein zusammenhängender ungerichteter Graph und T ein Teilgraph von X, dann heißt der Graph T = (V(T), E(T)) ein *spannender Baum* oder *Gerüst* von X, wenn V(T) = V(X) und T ein Baum ist.

Definition 8.25: Man spricht von einem *bewerteten Graphen* X =(V(X),E(X)), wenn eine Abbildung $g: E(X) \rightarrow S$ definiert ist, wobei S eine (für anfallende Rechenoperationen) „geeignete“ algebraische Struktur ist.

Definition 8.26: Ist X = (V(X), E(X)) ein bewerteter Graph mit g:E(X)-> $\mathbb{R}$, so heißt T = (V(T), E(T)) ein *Minimalgerüst* von X, wenn

(i) T ein Gerüst von X und

(ii) $\sum_{e \in E(T)} g(e)$ = Minimum ist.

Definition 8.27: Ist X = (V(X), E(X)) ein bewerteter Graph X, so heißt

$$g(X) = \sum_{e \in E(X)} g(e)$$

die Länge des Graphen X.

Definition 8.28: Ein binärer Baum ist entweder ein leerer Baum oder besteht aus einer Wurzel r, die „links“ und „rechts“ je einen Sohn hat, die jeweils wieder binäre Bäume sind.

Definition 8.29: Unter der *Höhe* h(B) eines binären Baumes versteht man die Länge (= Anzahl der Kanten) des längsten Weges W(r,b) von der Wurzel r bis zu einem Blatt b.

Definition 8.30: Sei B ein nichtleerer binärer Baum und w : V(B) → K eine bijektive Abbildung von V(B) auf eine Schlüsselmenge K.
B heißt *Suchbaum*, wenn für jeden Knoten x, der kein Blatt ist, gilt
w(y) < w(x), für alle y aus dem linken Unterbaum von y, und
w(y) > w(x), für alle y aus dem rechten Unterbaum von y ist.

Definition 8.31: Die *Fibonaccizahlen* sind F(0) = 0, F(1) = 1 und
F(n+1) = F(n) + F(n-1) für n ≥ 1.

Definition 8.32:
- Der leere Baum ist der Fibonaccibaum F_0.
- Ein einzelner Knoten ist der Fibonaccibaum F_1 der Höhe h = 0.
- Ein Baum bestehend aus der Wurzel w und der Kante [w,b] zu einem Blatt b ist der Fibonaccibaum F_2 der Höhe h=1.
- Sind F_h und F_{h-1} zwei Fibonacci Bäume der Höhen h–1 bzw. h–2, so erhält man den Fibonaccibaum F_{h+1} der Höhe h, in dem man einen neuen Wurzelknoten mit jeweils einem F_h (links) und F_{h-1} (rechts) als Unterbäume kombiniert:

  „ $F_{h+1} = <F_h, w, F_{h-1}>$“
- Keine anderen Bäume sind Fibonaccibäume

Definition 8.33: Ein binärer Baum T heißt *ausgeglichen* oder *balanziert* (engl.: balanced tree), wenn für die Balance b(x) jedes Knotens x gilt: $| b(x) | \leq 1$; d.h., wenn sich die Höhen der beiden Unterbäume T_l, T_r mit der Wurzel x um höchstens 1 unterscheiden.

Definition 8.34: Ein B-Baum oder B(k,h) Baum liegt vor, wenn gilt:
- alle Blätter b haben denselben Abstand h zur Wurzel r
- die Wurzel ist entweder ein Blatt oder hat *mindestens* 2 Söhne
- jeder von der Wurzel verschiedene innere Knoten x hat *wenigstens* k+1 Söhne
- jeder Knoten hat *höchstens* 2k + 1 Söhne
- der leere Baum ist ein B(k,h) Baum

Definition 8.35: Ein ungerichteter Graph X = (V(X), E(X)) heißt vollständig, wenn je zwei verschiedene Knoten $x,y \in V(X)$ mit einer Kante verbunden sind (d.h.: adjazent sind).

Definition 8.36: Der zu X *komplementäre Graph* $\overline{X}$, das Komplement zu X, ist der Graph mit

$$V(\overline{X}) = V(X)$$
$$E(\overline{X}) = \{[x,y] \mid x \neq y, x,y \in V(X), [x,y] \notin E(X)\}$$

Definition 8.37: Eine *k-Clique* Q_k in einem Graphen X ist ein vollständiger Teilgraph Q_k davon mit k Knoten.

Definition 8.38: Eine *Knotenüberdeckung* in X = (V(X), E(X)) ist eine Teilmenge $W \subseteq V(X)$, wenn jede Kante aus E(X) in einem $x \in W$ inzidiert.

Definition 8.39: Eine *Eulertour* in X = (V(X), E(X)) ist ein geschlossener Kantenzug, der jede Kante von X genau einmal enthält.
Gibt es in X eine Eulertour, so heißt X *eulersch* oder *Euler-Graph*.

Definition 8.40: Gibt es im Graphen X einen geschlossenen Kantenzug (Kreis) C, der jeden Knoten $x \in V(X)$ *genau einmal* enthält, so heißt C eine *Hamilton´sche Linie* und der Graph *Hamilton´scher Graph.*

Definition 8.41: Ein Graph X heist *planar* oder *plättbar*, wenn man ihn so in der Ebene zeichnen (einbetten) kann, dass sich keine zwei Kanten überkreuzen.

Definition 8.42: Eine Transition heißt *aktiviert* oder *schaltbereit*, falls sich auf jeder Eingangsstelle mindestens eine Marke befindet.
Schaltbereite Transitionen können zu einem beliebigen Zeitpunkt schalten (*feuern*).

Definition 8.43: Beim Schalten einer Transition wird aus deren Eingangsstellen je eine Marke abgezogen und *jeder* Ausgangsstelle je eine Marke hinzugefügt. Eine anschauliche Interpretation des Schaltens ist z.B. ein Produktionsablauf. Eine Transition produziert das den Ressourcen (Marken) der Eingangsstellen ein oder mehrere neue Produkte, die dann die als Marken auf den Ausgangsstellen dargestellt werden. Das Schalten (Produzieren) kann nur stattfinden, wenn alle benötigten Bauteile auf den Eingangsstellen vorhanden sind, wenn also jede Eingangstelle mindestens mit einem Token markiert ist.

Definition 8.44: Eine Transition ist schaltbereit, falls sich in allen Eingangsstellen mindestens so viele Marken befinden, wie die Transition an Kosten verursacht und wenn zugleich die Ausgangsstellen genügend Kapazität zur Aufnahme der neuen Marken haben.

Definition 8.45: Beim Schalten einer Transition werden aus deren Eingangsstellen den Kantengewichten entsprechend Marken weggenommen und den Ausgangsstellen den Kantengewichten entsprechend viele Marken hinzugefügt.

Definition 8.46: Ein Petrinetz ist ein 6-Tupel (S, T, F, K, W, M_o), wobei

(1) S: eine nicht leere Menge von Stellen (Plätzen) $S = \{s_1, s_2, ..., s_n\}$

(2) T: eine nicht leere Menge von Transitionen $T = \{t_1, t_2, ..., t_m\}$

(3) $S \cap T = \varnothing$

(4) F: eine nicht leere Menge von Kanten: $F \subseteq (S \times T) \cup (T \times S)$ d.h. es führen nur Kanten von Stellen zu Transitionen und von Transitionen zu Stellen. F heißt *Flussrelation*.

(5) $K: S \rightarrow \mathbb{N} \cup \{\infty\}$. K heißt *Kapazitätsfunktion*.

(6) $W: F \rightarrow \mathbb{N}$. W ist die Kostenfunktion für die Kanten

(7) M_o ist die Startmarkierung, eine aktuelle Markierung M nennt man *Zustand des Petrinetzes*, mit M(s) bezeichnet man die Anzahl der Markierungen auf der Stelle $s \in S$.

Definition 8.47: Die Eingangsstellen (*Vorbereich*) zu einer Transition t sind
${}_*t = \{s \in S \mid (s,t) \in F\}$, die Ausgangsstellen (*Nachbereich*) sind
$t_* = \{s \in S \mid (s,t) \in F\}$.

Definition 8.48: Ein *ganzzahliger Fluss* Φ auf einem Transportnetz N ist eine Abbildung φ von E(N) in die Menge der ganzen Zahlen $\mathbb{Z}$.
Man nennt $\varphi(e)$ den Fluss durch die Kante $e \in E(N)$.
Ist $\varphi(<x,y>) = \varphi(e) > 0$, so fließt φ in die Richtung von
$e = <x,y> \in E(N)$ mit $x,y \in V(N)$
Ist $\varphi(e) < 0$, so fließt φ gegen die Richtung von e.

Definition 8.49: Mit $A \subset V(N)$ ist $\Phi(A) = \Phi^+(A) - \Phi^-(A)$ erklärt, wobei
$\Phi^+(A) = \Sigma\, \varphi(e)$, $e<x,y>$, $x \in A$, $y \in V(N) - A$
$\Phi\text{-}(A) = \Sigma\, \varphi(e)$, $e<x,y>$, $x \in A$, $y \in V(N) - A$

Definition 8.50: Ein Knoten $q \in v(N)$ mit $d^-(q) = 0$, $d^+(q) > 0$ heißt *Quelle* und $\Phi(q) = \Phi^+(q)$ ihre *Ergiebigkeit*. Ein Knoten $s \in V(N)$ mit d– (s) > 0 und $d^+(s) = 0$ heißt *Senke* und $\Phi(s) = \Phi^-(s)$ ihr *Verbrauch*. Besitzt ein Fluss φ von q nach s genau eine Quelle und genau eine Senke, so heißt φ ein *Fluss von q nach s* und $\Phi(q)$ der *Wert von* φ.

Definition 8.51: Ein *Transportnetz N mit Kapazitäten* ist ein endlicher gerichteter Graph N = (V(N), E(N)) mit:

(i) Es gibt genau einen Knoten q mit $d^+(q) > 0$ und $d^-(q) = 0$. Er heißt *Quelle* von N.

(ii) Es gibt genau einen Knoten s, mit $d^-(s) > 0$ und $d^+(s) = 0$. Er heißt *Senke* von N.

(iii) Auf den Kanten von N ist ein positiver ganzzahliger Fluss φ erklärt: $\varphi: E(N) \rightarrow \mathbb{N}_0$.

(iv) Für alle von der Quelle und der Senke verschiedenen Knoten $x \in V(N), x \neq q, s$ gilt

$$\sum_{\substack{y \in V(N) \\ <y,x> \in E(N)}} \varphi(<y,x>) = \sum_{\substack{y \in V(N) \\ <x,y> \in E(N)}} \varphi(<x,y>)$$

(v) Jeder Kante $e \in e(N)$ ist eine nichtnegative ganze Zahl c(e) als ihre *Kapazität* zugeordnet.

(vi) Für jeden Fluss φ gilt

$$0 \leq \varphi(e) \leq c(e) \quad \forall\, e \in E(N).$$

Definition 8.52: Ein *Schnitt* (V_1,V_2) (engl.: cut) in einem Transportnetz N mit der Quelle q und der Senke s ist eine Partition von V(N) der Art, dass $q \in V_1, s \in V_2$ mit $V_1 \cap V_2 = \varnothing$ und $V_1 \cup V_2 = N$.

Definition 8.53: Die *Kapazität* $c(V_1,V_2)$ eines Schnittes (V_1,V_2) ist die Summe der Kapazitäten aller Kanten, die von V_1 nach V_2 führen:

$$c(V_1,V_2) = \Sigma\, c(<x,y>),\ x \in V_1,\ y \in V_2.$$

Definition 8.54: Sei X = (V(X), E(X)) ein ungerichteter Graph. Eine Teilmenge $M \subseteq E(X)$ heißt Matching in X, wenn keine zwei Kanten $e_i, e_j \in E(X)$ adjazent sind. Ein Knoten $a \in V(X)$ heißt bezüglich M gesättigt, wenn eine Kante $[a,x] \in M$ existiert, also a mit einer Kante $e \in M$ inzidiert. Andernfalls nennt man a ungesättigt bezüglich M.

Definition 8.55: Ein Matching M mit größtmöglicher Anzahl von Kanten heißt *maximales Matching*. Ein Matching M heißt *perfekt*, wenn es keine ungesättigten Knoten bezüglich M gibt.

Definition 8.56: Ein Weg W[a,b] in X heißt *alternierend* bezüglich M oder M-alternierend, wenn in W abwechseln Kanten $e \in M$ und Kanten $e \notin M$ aufeinander folgen. Ein solcher Weg W[a,b] heißt *erweiternd*, wenn a,b bezüglich M ungesättigt sind.

Definition 8.57: Ein Graph X = (V(X), E(X)) heißt paarer (oder bipartiter) Graph, wenn $V(X) = V_1 \cup V_2$ mit $V_1 \cap V_2 = \varnothing$ und mit $e = [x,y] \in E(X)$ folgt, dass $x \in V_1$ und $y \in V_2$.

Definition 9.1: Ein Alphabet A ist eine endliche Menge von Zeichen.

Definition 9.2: Ein Wort *über* einem Alphabet A besteht aus einer endlichen Folge von Symbolen *aus* A. Das leere Wort wird dargestellt durch ε und ist eine leere Folge von Symbolen und ein Wort über jedem beliebigen Alphabet A. Die Länge eines Wortes w ist bestimmt durch die Anzahl der Symbole in w. Deshalb gilt $| \varepsilon | = 0$.

Definition 9.3: A* bezeichnet die Menge aller Wörter über A.

Definition 9.4: Eine Sprache L (über einem Alphabet A) besteht aus einer Menge von Wörtern über A. Somit ist L über A eine Teilmenge von A*.

Definition 9.5: Ein endlicher Automat EA = (S, I, Σ, t, F) besteht aus:

(i) einer endlichen Menge von Zuständen S
(S = states, oft auch mit Z oder Q bezeichnet)
(ii) einer Menge von Anfangszuständen $I \subset S$
(iii) einer (endlichen) Eingabe, dem Alphabet Σ
(iv) einer Menge von Endzuständen $F \subseteq S$
und
(v) einer Übergangsrelation $t \subseteq S \times \Sigma \times S$

Definition 9.6: Ein deterministischer endlicher Automat DEA ist ein 5-Tupel $(S, s_o, \Sigma, \delta, F)$, wobei im Vergleich zum EA folgendes verlangt wird:

(i) es gibt genau einen Anfangszustand $s_o \in S$
(ii) anstatt einer *Übergangsrelation* t wird eine *Übergangsfunktion* $\delta : S \times \Sigma \rightarrow S$ eingesetzt.

Definition 9.7: Ein deterministischer endlicher Ein/Ausgabe Automat E/A_DEA = $(S, s_o, \Sigma, \delta, \Theta, \theta, F)$ besteht aus:

(i) einer endlichen Menge von Zuständen S
(ii) genau einem Anfangszustand s_o
(iii) einem Eingabealphabet Σ
(iv) einer Zustandsüberführungsfunktion $\delta : S \times \Sigma \rightarrow S$
(v) einem Ausgabealphabet Θ
(vi) einer Ausgabefunktion $\theta : S \times \Sigma \rightarrow \Theta$
(vii) einer Menge von Endzuständen $F \subseteq S$

Definition 9.8: Die Folge $s, \delta'(s, a_1), \delta'(s, a_1,a_2), ..., \delta'(s, a_1,a_2.....a_n)$ heißt *Zustandstrajektorie* von s unter $w = a_1a_2.....a_n$.

Definition 9.9: Die von einem DEA = $(S, s_0, \Sigma, \delta, F)$ akzeptierte Sprache L(DEA) ist $\{ w \in \Sigma^* \mid \delta' (s_0, w) \in F \}$.

Definition 10.1: Ein Code ist eine Abbildung von Zeichen eines Alphabetes A in Wörter über einem Alphabet B.
Wir erinnern daran, dass Wörter durch Aneinanderreihen (Konkatenation) von Zeichen *aus* dem Alphabet A entstehen und A* als Menge aller Wörter *über* A mit dem leeren Wort ε das *freie Monoid* oder *Wortmonoid* über dem Alphabet A genannt wird.

Definition 10.2: Ein *Einfachfehler* liegt vor, wenn in einem übertragenen Wort genau ein Bit fehlerhaft übertragen wird. Man spricht von einem *Doppelfehler* bzw. *n-fach Fehler*, wenn genau zwei bzw. n Bits fehlerhaft sind.

Definition 10.3: Wird eine Folge von n Bits hintereinander falsch übertragen, so spricht man von einem *Fehler-Burst* der Länge n.

Definition 10.4: Ein (linearer) *Code* über dem Körper $K = \mathbb{Z}_p$ ist der *Nullraum* $C = \{c \in K^n \mid A \cdot c^t = \mathbf{o}\}$ einer Matrix $A \in K^{n}_{n-k}$, also alle Spaltenvektoren, die mit A multipliziert den Nullvektor ergeben.
A heißt dann eine *Kontrollmatrix* von C und C heißt ein *linearer (n,k)-Code*. Elemente aus C heißen *Codewörter*. Für p = 2 spricht man von *binären Codes*.

Definition 10.5: Seien $x = (x_1,\ldots,x_n)$, $y = (y_1,\ldots,y_n) \in (\mathbb{Z}_2)^n$. Die *Hamming-Distanz* d(x,y) ist die Zahl der Stellen, an denen sich x und y unterscheiden.

Definition 10.6: Die kleinste Hamming-Distanz zwischen je zwei (verschiedenen) Codewörtern aus C heißt die *Minimaldistanz* von C und wird mit $d_{min}(C)$ bezeichnet.

Definition 10.7:

a) $d(x,0) =: w(x)$ heißt das *Hamming-Gewicht* von x.

b) Sei A eine m×n-Matrix. Dann sei rg(A) das größte r, sodass je r Spalten von A linear unabhängig sind.

Definition 10.8: Falls A aus allen s^t mit $s \in (\mathbb{Z}_2)^n$, $s \neq \mathbf{o}$, besteht, also falls alle möglichen n-stelligen Binärzahlen spaltenweise vorkommen, so heißt A bzw. der dadurch definierte Code ein *Hamming-Code*; es handelt sich dann um einen $(2^n-1, 2^n-1-n)$-Code.

Definition 10.9: Beschreibt die Kontrollmatrix A einen Hamming-Code, so kann man durch Anhängen einer „Nullspalte“ und Darüberschieben einer „Einerzeile“ den *erweiterten Hamming-Code* $\overline{A}$ erhalten.

Definition 10.10: Sei C ein (n,k)-Code mit Minimaldistanz $d_{min}(C) =: d$.

a) $\frac{k}{n}$ heißt die *Informationsrate* von C, sie gibt die Anzahl der „relevanten Bits“ pro Codewort an.

b) $\frac{d}{n}$ heißt die *Korrekturrate* von C.

Sowohl $\frac{k}{n}$ als auch $\frac{d}{n}$ sind Zahlen zwischen 0 und 1. Je größer, desto besser ist der Code.

Definition 10.11: Ein zyklischer Code ist ein Code, für den gilt:
$c_0 \ldots c_{n-1}$ ist Codewort $\Rightarrow c_{n-1}\, c_1 \ldots c_{n-2}$ ist Codewort.

Definition 10.12: Ein *Reed-Solomon Code* mit k Informationsstellen der Länge q–1>k über GF(q), kurz ein RS(n,k)-Code entsteht auf folgende Weise:

1. Man wählt ein erzeugendes Element a der multiplikativen Gruppe von GF(q). Es ist dann $a^{q-1} = 1$.

2. Die zu codierenden Wörter seien Folgen $(w_0,w_1,\ldots,w_{k-1})$ der Länge k mit Komponenten $w_i \in GF(q)$.

3. Zur Codierung schreibt man eine solche Folge $(w_0,\ldots,w_{k-1})$ als Polynom
   $w_0 + w_1x + \ldots + w_{k-1}x^{k-1} =: w(x)$
   und codiert es zu
   $(w(1),w(a),\ldots,w(a^{q-2}))$
   und erhält eine codierte Folge der Länge q-1, die verschickt wird.

4. Der Empfänger erhält also q-1 Werte für eine – ihm unbekannte – Polynomfunktion w(x) vom Grad k < q-1. Da für die Interpolation zum Berechnen von w(x) schon k Werte ausreichen würden, kann man aus der Redundanz das ursprüngliche Polynom w(x) auch bei einigen fehlerhaften Werten den $w(a^i)$ berechnen.

Definition 11.1: Die Adjazenzmatrix $A(X) = \{a_{ij}\}$ eines Graphen X = (V(X), E(X)) mit n Knoten ist eine $n \times n$ Matrix A mit den Elementen $a_{ij} = 1$, wenn x_i und x_j adjazent sind, $a_{ij} = 0$ sonst.

Definition 11.2: Eine zu m relativ prime Zahl a mod m heißt *primitives Element modulo m*, wenn ihre Ordnung ord(a) maximal ist.

Definition 11.3: Eine Folge $H = \{k_1, k_2, \ldots, k_n\}$ von n Schlüsseln $k_i \in \mathbb{N}$ heißt Halde, wenn folgende Beziehung gilt:
$k_i \geq k_{i\ DIV\ 2}$ für $2 \leq i \leq n$

Definition 11.4: Eine Matrix $A \in \mathbb{R}^{n\times n}$ heißt *diagonalisierbar*, wenn es eine Matrix $C \in \mathbb{R}^{n\times n}$ gibt, sodass $D = C^{-1}\cdot A\cdot C$ und D eine Diagonalmatrix ist.
In diesem Fall gilt dann natürlich $A = C\cdot D\cdot C^{-1}$