

# Prüfungsrelevante Verfahren, Sätze und Rechenregeln

## 2 Diskrete Strukturen

### 2.1 Mengenlehre und Kombinatorik

- zwei Mengen  $A$  und  $B$  sind gleich wenn sie die selben Elemente haben, d.h. wenn  $A \subseteq B \wedge B \subseteq A$
- Beachte z.B. dass  $\{\{1, 2\}, 7\} \not\subseteq \mathbb{N}$
- Schnitt und Vereinigung sind kommutativ, assoziativ, distributiv in beide Richtungen; für Beweise kann es nützlich sein sich die Definitionen dieser Operationen in Erinnerung zu rufen;  $\overline{A \cup B} = \overline{A} \cap \overline{B}$ ,  $\overline{A \cap B} = \overline{A} \cup \overline{B}$
- $A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$  heißt **kartesisches Produkt** oder **Produktmenge**;  $|A \times B| = |A| \cdot |B|$
- **Potenzmenge**  $\mathcal{P}(A)$  ist die Menge aller (auch unechten) Teilmengen von  $A$ ,  $|\mathcal{P}(A)| = 2^{|A|}$ , es gilt stets  $\emptyset \in \mathcal{P}(A)$
- $\binom{n}{k} = \frac{n!}{k!(n-k)!}$
- **Handschlaglemma**: Anzahl der Teilnehmer einer Konferenz, die einer ungeraden Anzahl von Teilnehmern die Hand geben, ist immer gerade

### 2.2 Abbildungen

- für  $f : A \rightarrow B$ ,  $A' \subseteq A$  heißt  $f[A'] = \{f(a) \mid a \in A'\}$  Bild von  $A'$  unter  $f$
- **injektiv**:  $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$  ("für jedes  $b \in B$  existiert höchstens ein  $a \in A$  mit  $f(a) = b$ ")  
Beweise über Gegenbeispiel oder  $f(a_1) = f(a_2)$  setzen
- **surjektiv**:  $f[A] = B$  ("für jedes  $b \in B$  existiert mindestens ein  $a \in A$  mit  $f(a) = b$ ")  
Beweise über Gegenbeispiel oder Definitionsbereich der Umkehrfunktion untersuchen
- **bijektiv**: injektiv und surjektiv ("für jedes  $b \in B$  existiert genau ein  $a \in A$  mit  $f(a) = b$ ")
- für  $f$  *injektiv* (!!) definieren wir  $f^{-1} : f[A] \rightarrow A$ ,  $b \mapsto f^{-1}(b) = a$  mit  $f^{-1}(b) = a$  g.d.w.  $f(a) = b$
- für  $f : A \rightarrow B$ ,  $g : B \rightarrow C$  ist **Komposition**  $g \circ f : A \rightarrow C$ ,  $x \mapsto g(f(x))$  ( $\Rightarrow$  von rechts nach links ausführen!!)

### 2.3 Permutationen

- **Permutation** von  $X$  ist bijektive Abbildung von  $X$  nach  $X$ , für  $X = \{1, \dots, n\}$  ist  $S_n$  Menge aller Permutationen und  $\pi \in S_n$  mit  $\pi = \begin{pmatrix} 1 & \dots & n \\ \pi(1) & \dots & \pi(n) \end{pmatrix}$  und  $|S_n| = n!$
- **k-Zyklus** = k-Tupel der Form  $(a_1, \dots, a_k)$  mit  $\pi(a_k) = a_1, \pi(a_i) = a_{i+1}$ , jedes Element von  $S_n$  kann als Komposition elementfremder Zyklen notiert werden:  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} = (1, 2, 3) \circ (4, 5) = (123)(45)$
- bei elementfremden Zyklen ist Reihenfolge egal:  $(123)(45) = (45)(123)$ ; Elemente die auf sich selbst abgebildet werden heißen **Fixpunkte** und müssen nicht notiert werden:  $(123)(4) = (123)$ ; mit welchem Element im Zyklus angefangen wird ist Egal:  $(123)(45) = (312)(54)$
- **Transposition** = 2-Zyklus, jedes Element von  $S_n$  kann mit Transpositionen geschrieben werden als:  $(a_1, \dots, a_k) = (a_1 a_2)(a_2 a_3) \dots (a_{k-1} a_k)$  (nicht elementfremd  $\Rightarrow$  Reihenfolge wichtig!!)
- bei Komposition von Permutationen für jede Zahl von rechts nach links durchgehen:  $\underbrace{(123)}_{(2)} \underbrace{(35)}_{(1)} = \underbrace{(1235)}_{(3)}$   
5 wird in (1) auf 3 abgebildet, in (2) wird 3 auf 1 abgebildet, also  $5 \rightarrow 3 \rightarrow 1$  und damit  $5 \rightarrow 1$  in (3)

## 2.4 Beweis mittels vollständiger Induktion (Beispiel)

*Beweis.* Die Aussage  $A_n$  sei  $\sum_{k=0}^n q^k = \frac{1-q^{n+1}}{1-q}$  mit  $n \in \mathbb{N}, q \in \mathbb{R}, q \neq 1$ .

$$(IA): n_0 = 0: \sum_{k=0}^0 q^k = q^0 = 1 = \frac{1-q^{0+1}}{1-q} \quad \text{w.A.} \\ \Rightarrow \text{Es gilt } A_0$$

$$(IV): \forall \tilde{n} : n_0 \leq \tilde{n} \leq n : \sum_{k=0}^{\tilde{n}} q^k = \frac{1-q^{\tilde{n}+1}}{1-q}$$

$$(IS): \sum_{k=0}^{n+1} q^k = \sum_{k=0}^n q^k + q^{n+1} \stackrel{(IV)}{=} \frac{1-q^{n+1}}{1-q} + q^{n+1} = \frac{1-q^{n+1} + (1-q)q^{n+1}}{1-q} \\ = \frac{1-q^{n+1} + q^{n+1} - q^{n+2}}{1-q} = \frac{1-q^{(n+1)+1}}{1-q}$$

$\Rightarrow$  Damit ist die Behauptung für alle  $n \in \mathbb{N}$  vollständig bewiesen □

- "Die Aussage  $A_n$  sei..." nur in VL und AuD Skript, *evtl.* wird sonst aber z.Z.: erwartet; IV muss auch nicht unbedingt notiert werden
- alles nochmal mit  $(n+1)+1$  hinschreiben ist nicht nötig
- Varianten:  $A_n \Rightarrow A_{n+1}$  / aus  $A_n$  folgt  $A_{n+1}$  für alle  $n \in \mathbb{N}$   
w.A. / Folglich gilt  $A_n$  für alle  $n \in \mathbb{N}, n \geq n_0$
- Beachte dass oft auch nur für  $n \in \mathbb{N}, n \geq k$  bewiesen wird (kein  $\tilde{n}$ )!! und  $n_0 = 0$  nicht immer gelten muss

## 2.5 Zahlentheorie

- $n \in \mathbb{N}, n \geq 1$  kann *eindeutig* geschrieben werden als  $n = \prod_{i=1}^k p_i^{\alpha_i}$  ( $p_i$  prim,  $\alpha_i \in \mathbb{N}$ , "PFZ")  
 $\Rightarrow \# \text{Teiler von } n = \prod_i (\alpha_i + 1)$
- für  $a, b \in \mathbb{N}$  gilt  $a \mid b \Leftrightarrow \exists k : k \in \mathbb{N} \wedge ak = b$ ;  $a \mid b_1 \wedge a \mid b_2 \Rightarrow a \mid (b_1 + b_2) \wedge a \mid (b_1 - b_2)$
- für  $m, n \in \mathbb{Z}$  mit  $n > 0$  gilt  $\exists q, r : (q, r \in \mathbb{Z} \wedge m = nq + r \wedge 0 \leq r < n)$   
 $m \bmod n := r$ , für  $a \bmod n = b \bmod n$  schreibe  $a \equiv b \bmod n$
- **Homomorphieregel:**  $(a \bmod n + b \bmod n) \bmod n = (a + b) \bmod n$  (analog für  $\cdot$ )
- $\text{kgV}(m, 0) = \text{kgV}(0, n) = 0$ ;  $\text{ggT}(m, n) \cdot \text{kgV}(m, n) = m \cdot n$  ( $\Rightarrow$  kgV mit Euklid berechenbar)
- **Euklidischer Algorithmus:** immer weiter  $\text{ggT}(m, n) = \text{ggT}(n \bmod m, m)$  berechnen;  $\text{ggT}(m, n) = m$  falls  $m \mid n$ ;  $\text{ggT}(0, n) = n$ ;  $m, n$  teilerfremd  $\Leftrightarrow \text{ggT}(m, n) = 1$
- **Lemma von Bézout:**  $m, n \in \mathbb{N} \Rightarrow \exists a, b : a, b \in \mathbb{Z} \wedge \text{ggT}(m, n) = am + bn$
- **Erweiterter Euklidischer Algorithmus** am Beispiel ("EEA", keine offizielle Abkürzung):

	$\overbrace{m}^{1008}$	$\overbrace{n}^{499}$	$-q_i$		$\overbrace{m}^{1008}$	$\overbrace{n}^{499}$	$-q_i$
1008	1	0		1008	1	0	
499	0	1		499	0	1	
$1008 \bmod 499 = 10$	1	$0 + 1 \cdot (-q_i) = -2$	$1008 = 499 \cdot 2 + 10 \Rightarrow -q_i = -2$	$\Rightarrow$	10	1	-2
$499 \bmod 10 = 9$	-49	$1 + (-2)(-q_i) = 99$	-49		9	-49	99
$10 \bmod 9 = 1$	50	$-2 + 99(-q_i) = -101$	-1		1	50	-101
$9 \bmod 1 = 0$							

in  $m$  Spalte wird analog zu  $n$  Spalte gerechnet, das ganze bis in der linken Spalte 0 stehen würde

$$\Rightarrow \text{ggT}(1008, 499) = 1 = 50 \cdot 1008 - 101 \cdot 499 \quad (\text{Bézout Koeffizienten } a = 50, b = -101)$$

- **chinesischer Restsatz:** Seien  $0 < n_1, \dots, n_k \in \mathbb{N}$  teilerfremd und seien  $a_1, \dots, a_k \in \mathbb{Z}$ . Dann existiert genau ein  $x \in \{0, 1, \dots, \prod_{i=1}^k n_i - 1\}$  mit  $x \equiv a_i \bmod n_i$  für alle  $i = 1, \dots, k$
- für  $k = 2$ : Seien  $0 < m, n \in \mathbb{N}$  teilerfremd und seien  $a_1, a_2 \in \mathbb{N}$ . Dann existiert genau ein  $x \in \{0, 1, \dots, mn - 1\}$  mit  $x \equiv a_1 \bmod m \wedge x \equiv a_2 \bmod n$ ; anschaulich heißt das, dass ein  $m \times n$  Spielbrett eindeutig wie in VL durchnummeriert werden kann wenn  $\text{ggT}(m, n) = 1$

## 2.6 Gruppentheorie

- Gruppe  $(G, \circ)$  (auch  $(G; \circ, ^{-1}, e)$ ; dann Definition einfach anders formulieren) besteht aus Menge  $G$  und innerer Verknüpfung  $\circ : G \times G \rightarrow G$  so dass:  $\circ$  assoziativ, es existiert **neutrales Element**  $e$  ( $a \circ e = a = e \circ a$  für alle  $a \in G$ ), es existiert **Inverses**  $a^{-1}$  zu jedem  $a \in G$  ( $a \circ a^{-1} = e = a^{-1} \circ a$ )
- Gruppe heißt **abelsch**/kommutativ, falls  $\circ$  kommutativ ist
- $\mathbb{Z}_n = \{0, \dots, n-1\}$  bildet mit Addition mod  $n$  eine Gruppe; Symmetrien eines Quadrates ("D<sub>4</sub>"/"D<sub>8</sub>")/Dreiecks etc. bilden ebenfalls eine Gruppe (Komposition führt zu Drehungen, Spiegelungen und Identitätsabbildung)
- Nullteiler** mod  $n$  sind  $a \in \mathbb{Z}_n \setminus \{0\}$  für die  $b \in \mathbb{Z}_n \setminus \{0\}$  existiert mit  $a \cdot b \equiv 0 \pmod{n}$   
**Einheiten** mod  $n$  sind  $a \in \mathbb{Z}_n$  für die  $b \in \mathbb{Z}_n$  existiert mit  $a \cdot b \equiv 1 \pmod{n}$ ; 1 ist immer eine Einheit  
 $m$  ist Einheit mod  $n \Leftrightarrow m$  ist kein Nullteiler mod  $n \Leftrightarrow \text{ggT}(m, n) = 1$
- Die Menge der Einheiten mod  $n$  heißt  $\mathbb{Z}_n^*$  und bildet eine Gruppe mit Multiplikation mod  $n$ ; es gilt mit PFZ dass  $\phi(n) := |\mathbb{Z}_n^*| = \prod_{i=1}^k (p_i^{\alpha_i} - p_i^{\alpha_i-1}) = \#$  zu  $n$  teilerfremde Zahlen
- multiplikative Gruppe ist **zyklisch** falls  $g \in G$  existiert mit  $G = \{g^j \mid j \in \mathbb{Z}\}$  (Potenzrechengesetze ähnlich wie in  $\mathbb{N}$ , für additive Gruppen schreibe  $G = \{jg \mid j \in \mathbb{Z}\}$ ); Erzeuger sind  $g \in G, |G| = n$  so dass  $G = \{g^j \mid j \in \mathbb{Z}_n\}$ ; Erzeuger von  $\mathbb{Z}_n$  sind genau die Elemente von  $\mathbb{Z}_n^* \Rightarrow \# \text{ Erzeuger} = \phi(n)$
- für  $p$  prim ist  $(\mathbb{Z}_p^*, \cdot \text{ mod } n)$  zyklisch;  $\# \text{ Erzeuger} = \phi(p-1)$ ; diese Erzeuger heißen **Primitivwurzeln**
- Isomorph**=Strukturgleich ("man kann Elemente einfach umbenennen"), jede zyklische Gruppe ist isomorph entweder zu  $(\mathbb{Z}, +)$  oder einem  $(\mathbb{Z}_n, + \text{ mod } n)$ ; als Beweis das zwei Gruppen nicht isomorph sind genügt z.B. " $G_1$  ist zyklisch,  $G_2$  nicht"
- $U \subseteq G$  heißt **Untergruppe** von  $G$  falls  $e \in U$ ;  $a \circ b \in U$  für alle  $a, b \in U$ ;  $a^{-1} \in U$  für alle  $a \in U$
- $\langle g \rangle := \{g^i \mid i \in \mathbb{Z}\}$  ist **von  $g$  erzeugte Untergruppe**
- $g \circ U = \{g \circ u \mid u \in U\}$  ist eine **(Links-)Nebenklasse** ("LNK") von  $U$ ,  $|g \circ U| = |U|$ , 2 LNK sind entweder gleich oder disjunkt  $\Rightarrow$  jedes  $g \in G$  liegt in genau einer LNK (nämlich  $g \circ U$ )
- Satz von Lagrange:**  $|G| = |G : U| \cdot |U|$  ( $|G : U| = \# \text{ LNK von } U \text{ in } G = \text{Index von } U \text{ in } G$ )  
 $|G|$  heißt Ordnung von  $G$ ,  $o(g) := |\langle g \rangle|$  Ordnung von  $g$
- Satz von Euler-Fermat:** Seien  $n \in \mathbb{N}, a \in \mathbb{Z}$  mit  $\text{ggT}(a, n) = 1$ . Dann gilt  $a^{\phi(n)} \equiv 1 \pmod{n}$
- für Beweise bieten sich oft Verknüpfungstafeln an, folgende Methoden helfen beim effizient rechnen:

## 2.7 Effizient potenzieren mod $n$

- andere Form von Euler-Fermat:  $a^m \equiv a^{m \bmod \phi(n)} \pmod{n}$ , gilt aber auch nur für  $\text{ggT}(a, n) = 1$  !!
- einfach die Zahlen Stück für Stück mit mod zerlegen

## 2.8 Kryptographie

- für  $p$  prim und  $g$  Primitivwurzel von  $\mathbb{Z}_p^*$  ist der **diskrete Logarithmus** von  $x \in \mathbb{Z}_p^*$  zur Basis  $g$  die Zahl  $m \in \{0, \dots, p-2\}$  mit  $g^m \equiv x \pmod{p}$  ( $m = \log_g(x)$ );  $m$  kann nicht effizient berechnet werden,  $x$  aus  $g^m$  schon
- Diffie-Hellman-Merkle:**
  - Alice und Bob einigen sich auf Primzahl  $p$  und Primitivwurzel  $g$  von  $\mathbb{Z}_p^*$
  - Alice wählt geheime Zufallszahl  $a$  und berechnet  $a' = g^a \pmod{p}$ ; Bob analog:  $b' = g^b \pmod{p}$
  - beide teilen sich  $a'$  und  $b'$  mit und berechnen das Geheimnis  $c = g^{ab} \pmod{p} = (a')^b \pmod{p} = (b')^a \pmod{p}$

Um damit Nachricht  $m \leq c$  zu verschlüsseln:

- schreibe  $m$  und  $c$  binär als  $m = m_1 \dots m_l, c = c_1 \dots c_k$
- Alice verschickt  $v_1 = m_1 + c_1 \pmod{2}, \dots, v_l = m_l + c_l \pmod{2}$ ; Bob berechnet  $m_i = v_i + c_i \pmod{2}$

### • RSA:

- Bob wählt zufällig 2 Primzahlen  $p, q$  und berechnet  $n := pq$
- Bob wählt zufällig  $d \in \mathbb{Z}_{\phi(n)}^*$  und berechnet  $i, h \in \mathbb{Z}$  mit  $i \cdot d + h \cdot \phi(n) = \text{ggT}(d, \phi(n)) = 1$  (EEA)
- $n$  und  $i$  sind öffentliche Schlüssel und werden an Alice weitergegeben,  $d$  ist privater Schlüssel
- Alice schickt  $c = m^i \pmod{n}$  an Bob mit Nachricht  $m$  ( $0 \leq m < n$ )
- Bob berechnet  $m = c^d \pmod{n}$

**2.9    Ungerichtete Graphen**

**2.10    Gerichtete Graphen**

**2.11    Aussagenlogik**

**2.12    Relationen**