Diskrete Mathematik für Informatiker

Zusammenfassung wichtiger Elemente der DMI

von Alexander Köster

Student der Universität Siegen, DMI 2016

Letzte Aktualisierung: 8. August 2017

Die DMI-Vorlesung der Universität Siegen ist ein „Sammelfach“ mathematischer Teilgebiete
mit Relevanz für die Informatik, die in einem Mathematik-Studium in mehreren Einzelfächern vermittelt wird,
u.a. Kombinatorik, Zahlentheorie (Arithmetik), Algebra, Lineare Algebra und Graphentheorie.

Dies stellt eine große Menge an vermitteltem Stoff dar
und ist daher eines der lern-anspruchvollsten Theoriefächer der Informatik.

Einzig für Lernzwecke erstellt.

Nicht geeignet als Klausurhilfe.
Das Erstellen einer eigenen Klausurhilfe führt zu einem besonders guten Lerneffekt.
Dieses Dokument sollte nur als Orientierung oder Vergleich dienen.
Jeder sollte seine Klausurhilfe individuell auf seinen Lernstand und seine eigenen Probleme anpassen,
gut bekannte Dinge auslassen und schlecht merkbare Dinge hinzufügen.
Dieses Dokument beinhaltet viel mehr, als für eine tatsächliche Klausur durchschnittlich benötigt wird.
Für einen guten Ansatz, welche Inhalte man braucht, sollte sich an der Probeklausur orientiert werden.

1 Mengenlehre

- $\bigcup_{i\in\mathbb{N}} A_i = A_1 \cup A_2 \cup ...$
- $\bigcap_{i\in\mathbb{N}} A_i = A_1 \cap A_2 \cap ...$
- $\prod_{i=0}^{n} A_i = A_1 \times A_2 \times ... \times A_n$
- **Potenzmenge** von Menge A:
  2^A | Die Menge aller Teilmengen
  Bsp.: $2^{\{1,2\}} = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$
- $\forall A : |A| \neq |2^A|$ (Cantor)
- **Kontinuumshypothese**:
  $\forall$ unendlichen $A \subseteq 2^{\mathbb{N}} : |A| = |\mathbb{N}| \vee |A| = \left|2^{\mathbb{N}}\right|$
- Mengen $A_1, A_2, ..., A_n$ **paarweise disjunkt**
  $\Leftrightarrow \forall i,j \in \{1,2,...,n\} : i \neq j \Rightarrow A_i \cap A_j = \emptyset$
  (*keine* gemeinsamen Elemente in mehr als einer der Mengen)
  - ▷ da gilt: $\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i|$
- $\forall$ endl. $A, B : |A \cup B| = |A| + |B| - |A \cap B|$
- endl. $A_1, A_2, ..., A_k : \left|\prod_{i=1}^{k} A_i\right| = \prod_{i=1}^{k} |A_i|$
- $\forall$ endl. $A : \left|A^k\right| = |A|^k$

2 Relationen $R \subseteq A \times B$

- **binär**: $R \subseteq A \times A$
- **Funktion**: $\forall a \in A : \exists_1 b \in B : aRb$
  Synonym: **Abbildung**, $f : A \to B,\ x \mapsto f(x)$
  Definitionsbereich / Wertebereich
- Relation kann Graph aus Graphentheorie sein
- B^A: Menge aller Funktionen $A \to B$
- $f(A')$ mit $A' \subseteq A$: **Bild** ($\mathrm{im}(f)$) – alle Ergebnisse, wenn man Werte aus A' einsetzt
- $f^{-1}(B')$ mit $B' \subseteq B$: **Urbild** – alle eingesetzten Werte, die B' erzeugen
- **surjektiv** (rechtstotal): alle Elemente im Zielbereich getroffen | $\forall b \in B : \exists a \in A : f(a) = b$
- **injektiv** (linkseindeutig): keine doppelten Treffer | $\forall a,b \in A : (f(a) = f(b) \Rightarrow a = b)$
  $\Leftrightarrow \forall a,b \in A : (a \neq b \Rightarrow f(a) \neq f(b))$
- Bijektion $\Rightarrow$ Mengen $|A| = |B|$
  Injektion $\Rightarrow |A| \leq |B|$
- **Verkettung**: $(f \circ g)(x) = \cancel{f(g(x))}\ \ g(f(x))$
- Eigenschaften von Relationen:
  Sei $R \subseteq A \times A;\ a,b,c \in A;\ aRb$
  - ▷ **reflexiv**: jedes Element zu sich selbst in Relation | $\forall a : aRa \Leftrightarrow \mathrm{id}_A \subseteq R$
  - ▷ **irreflexiv**: kein Element zu sich selbst in Relation | $\nexists a : aRa \Leftrightarrow \mathrm{id}_A \cap R = \emptyset$
  - ▷ **symmetrisch**: wenn aRb, auch bRa
    $\forall a,b : (aRb \Rightarrow bRa) \Leftrightarrow R^{-1} = R$
  - ▷ **antisymmetrisch**: kein einziges Element symmetrisch verknüpft |
    $\forall a,b : (aRb \wedge bRa \Rightarrow a = b)$
    $\Leftrightarrow R \cap R^{-1} \subseteq \mathrm{id}_A$
  - ▷ **transitiv**: alle „Umweg-Verknüpfungen“ |
    $\forall a,b,c : (aRb \wedge bRc \Rightarrow aRc)$
    $\Leftrightarrow R \circ R \subseteq R$
- Besondere Relationen:
  - ▷ **Partielle Ordnung**: reflexiv, antisymmetrisch, transitiv
  - ▷ **Lineare Ordnung**: Partielle Ordnung und jedes Element irgendwie in Relation |
    $\forall a,b \in A : aRb \vee bRa$ | Bsp.: $\leq$ auf $\mathbb{Z}$
  - ▷ **Äquivalenzrelation**: reflexiv, symmetrisch, transitiv | Bsp.: $=$ (Gleichheit)
- **Partition**: Aufteilen einer Menge in k Teilmengen | Bsp.: $\{1,2,3,4,5\} \to \{\{1,2\},\{3,4\},\{5\}\}$
- **Umkehrrelation**: R^{-1} ordnet jedem b das a zu, zu dem es in Relation steht
- **Transitive Hülle**: R^+ | Hinzufügen aller indirekt erreichbaren Paare | $R^+ = \bigcup_{n\in\mathbb{N}} R^n$
- **Reflexiv-transitive Hülle**: $R^* = R^+ \cup \mathrm{id}_A$
- $\forall$ binären Relationen ($R \subseteq A \times A$) gilt:
  - ▷ $R \circ \mathrm{id}_A = \mathrm{id}_A \circ R = R$
  - ▷ $(R \circ S) \circ T = R \circ (S \circ T)$
  - ▷ $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$
- Eigenschaften Verkettung etc.:
  - ▷ R Bijektion $\Rightarrow R^{-1}$ = Umkehrfunktion
  - ▷ f injektiv $\wedge$ g injektiv $\Rightarrow f \circ g$ injektiv
  - ▷ f surjektiv $\wedge$ g surjektiv $\Rightarrow f \circ g$ surjektiv
- Bool'sche Algebra $(B, \cdot, +, \bar{\ })$
  mit $|B| \geq 2$; $x,y,z \in B$, wenn:
  - ▷ $x + y = y + x$
  - ▷ $x + x = 1$
  - ▷ $x + 0 = x$
  - ▷ $x \cdot y = y \cdot x$
  - ▷ $x \cdot x = 0$
  - ▷ $x \cdot 1 = x$
  - ▷ $x + (y + z) = (x + y) + z$
  - ▷ $x + (y \cdot c) = (x + y) \cdot (x + y)$
  - ▷ $x(y + z) = (x + y) \cdot z$
  - ▷ $x(y + c) = (x \cdot y) + (x \cdot y)$

3 Kombinatorik

- **Fallende Faktorielle**: $n^{\underline{k}} = n \cdot (n-1) \cdot (n-2) \cdot ... \cdot (n-(k-1)) = \prod_{i=0}^{k-1} (n-i)$
- **Binomialkoeffizient**: $\binom{n}{k} = \binom{n}{n-k} = \frac{n!}{(n-k)!\cdot k!}$
- **Binomischer Lehrsatz**:
  $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$
  - ▷ Pascal'sches Dreieck
    $1 \to 11 \to 121 \to 1331 \to ...$

	mit Reihenf.	**ohne** Reihenf.
mit Zurückl.	n^k	$\binom{n+k-1}{k}$
ohne Zurückl.	$n^{\underline{k}}$	$\binom{n}{k}$

4 Graphentheorie

- $G = (V, E)$, ***V**ertex* = Knoten, ***E**dges* = Kanten
- Besondere Graphen:
  - ▷ K_n: **vollständiger Graph** – alle n Knoten mit allen verbunden
  - ▷ $K_{n,m}$: **vollständig bipartiter Graph** - alle n „linke“/„obere“ Knoten mit allen m „rechten“/„unteren“ Knoten verbunden | Bsp.: $K_{2,3}$:
  - ▷ C_n: **„Kreis“** – alle n Knoten ringförmig verbunden | Bsp.: C_5:
  - ▷ P_n: **Pfad** – alle n Knoten nacheinander (zweigloser Baum) | Bsp.: P_3:
  - ▷ **Baum**: Graph ohne echte Kreise
  - ▷ **Wald**: nicht zusammenhängende Bäume
- **Isomorph**: gleich bis auf Benennung der Kn.
- Eigenschaften:
  - ▷ **bipartit**: kann in 2 nur untereinander verbundene Mengen zerteilt werden
    - Graph mit ungerader Länge *nie* bip.
  - ▷ **planar**: kann ohne Überschneidungen von Kanten gezeichnet werden
    - genau dann, wenn Graph keinen K_5 oder $K_{3,3}$ enthält (Kuratowski)
  - ▷ **zusammenhängend**: keine „Inseln“
- **Nachbarschaft** eines Knotens a in G: $N_G(a) = \{...\}$ | direkt mit a verbundene Kn.
- **Grad** eines Knotens a: $d_G(a) = |N_G(a)|$
- **Weg** im Graphen G: $[k_1, k_2, ..., k_n]_G$
  führt nacheinander über die Knoten k_i
  - ▷ einfacher Weg: keine doppelten Knoten
- **induzierter Teilgraph**: $G[V']$
  Nur neue Knotenmenge $V' \subset V$, automatisch nicht mehr mögliche Kanten weglassen
- **Zusammenhangskomponente**: induz. TG, zusammenhängend, aber sobald man noch einen Knoten aus dem originalen G dazu nimmt, nicht mehr zusammenhängend
- **Linienzug** $L \subseteq \mathbb{R}^2$ $\quad f : [0,1] \to L$
  Stetige Bijektion (0-100%) („ohne Stift absetzen zeichnen können“)
- **Planare Einbettung** in den $\mathbb{R}^2$: Paar (r, l)
  - ▷ p ist Injektion und ordnet jedem Knoten einen eigenen Punkt im $\mathbb{R}^2$ zu
  - ▷ l ist Funktion und ordnet jeder Kante einen Linienzug zwischen den Knotenpunkten zu

  ($l : E \to 2^{\mathbb{R}^2}$, $\{x,y\} \in E \Rightarrow l(x,y)$ ist Linienzug mit Endpunkten $p(x)$ und $p(y)$, Linien überschneiden sich nicht, aber können gemeinsame Endpunkte haben)
  - ▷ G planar, wenn G planare Einbettung hat
  - ▷ Linien müssen nicht gerade sein
    - Jeder planare Graph kann geradlinig gezeichnet werden (Wagner & Fáry)
      Bsp.: K_4
  $l(x,y) = \{\alpha p(x) + (1-\alpha) p(y) \mid \alpha \in [0,1]\}$
- **Facette** $F \subseteq \mathbb{R}^2$: „Fläche“ zw. Kanten
  - ▷ jeder Graph hat min. eine Facette: die unendliche Facette „außenrum“
  - ▷ F max. Teilmenge
  - ▷ F zshgd. $\Rightarrow$ alle Punkte in F können durch Linienzüge verbunden sein
  - ▷ F disjunkt zu Linienzügen des Graphen
- **Eulers Formel**: $|V| + k = |E| + z + 1$
  k: Anzahl Facetten einer planaren Einbettung
  z: Anzahl Zusammenhangskomponenten
  - ▷ **Eulers Polyedersatz**: $e + f - k = 2$
    e: Anzahl Kanten, f: Anzahl Flächen, k: Anzahl Knoten
- **Unterteilung** eines Graphen G: H |
  Neue Knoten auf existierenden Kanten hinzufügen | Bsp.: G: $\to$ H:
- k-**Färbung**: Abbildung $c : V \to \{1, ..., k\}$
  Alle Knoten werden gefärbt, sodass keine benachbarten Knoten die gleiche Farbe haben ($\forall \{x,y\} \in E : c(x) \neq (y)$)
  - ▷ **Färbungszahl (chromat. Zahl)** $\chi(G)$: kleinste Zahl $k \geq 1$, sodass eine k-Färbung von G existiert
    - $\chi(K_n) = n$
    - $\chi(K_{n,m}) = 2$
    - $\chi(P_n) = 2$
    - $\chi(C_n) = \begin{cases} 2 & \text{falls } n \text{ gerade} \\ 3 & \text{falls } n \text{ ungerade} \end{cases}$
    - durch Finden dieser als Teilgraph kann man $\geq$ von $\chi(G)$ festlegen
- **Maximalgrad** $\Delta(G)$: der höchste Grad aller Knoten in G | $\Delta(G) = \max\{d_G(x) | x \in V\}$
  - ▷ $\forall$ endl. Gr.: $\chi(G) \leq \Delta(G) + 1$
- **Vierfarbensatz**: $\forall$ endl. planar. Gr.: $\chi(G) \leq 4$
- **Matchings** (Paarung) $M \subseteq E$: „Färben von *Kanten*“, sodass keine gemeinsamen Endpunkte im Matching sind | Bsp.: K_4 M
  - ▷ größtes Matching: $\forall M' : |M| \geq |M'|$
  - ▷ **perfekt**es Matching: alle Knoten von G von M berührt ($\forall x \in V : \exists e \in M : x \in e$)
  - ▷ **Matchingzahl** $\mu(G)$: Anzahl der Kanten im größten Matching von G
  - ▷ Knoten x ist M**-saturiert**, wenn x im Matching M berührt wird
  - ▷ M**-alternierender Weg**: einfacher Weg in G, sodass abwechselnd Kanten aus M und nicht aus M auf dem Weg liegen |
    $[v_1, v_2, ..., v_n]_G, \forall 1 \leq i \leq n-2 :$
    $\{v_i, v_{i+1}\} \in M \Rightarrow \{v_{i+1}, v_{i+2}\} \notin M$

- ▷ **M-erweiternder Weg**: M-alternierender Weg mit v_1 und v_n nicht M-saturiert (vergrößert M, falls noch nicht größtes)

- **Knotenüberdeckung** *(vertex cover)* $C \subseteq V$: C enthält von jeder Kante des Graphen min. einen der beiden Knoten ($\forall e \in E : e \cap C = \emptyset$)
  - ▷ **Überdeckungszahl** $\gamma(G)$: Anzahl Knoten in kleinster C von G
  - ▷ $\mu(G) \leq \gamma(G)$
  - ▷ bipartiter Graph: $\mu(G) = \gamma(G)$
  - ▷ $\forall$ endl. bip. $G = (A \cup B, E) : \exists M$ (perf. bzgl. A) von $G : \forall x \in A : M$-sat. $\Leftrightarrow \forall C \subseteq A : |N_G(C)| \geq |C|$
- $\mathrm{d_u}(G)$: Anzahl Knoten ungeraden Grades
- **Eulerpfad**: Weg in G, der jede Kante nur einmal besucht | $\exists \Leftrightarrow G$ zshgd. $\wedge\ \mathrm{d_u}(G) \in \{0, 2\}$
- **Eulerkreis**: Eulerpfad im Kreis (letzter Knoten = erster Knoten) | $\exists \Leftrightarrow G$ zshgd. $\wedge\ \mathrm{d_u}(G) = 0$
- **Hamiltonpfad**: Weg in G, sodass jeder Knoten nur einmal passiert wird
- **Hamiltonkreis**: Hamiltonpfad im Kreis (erster Kn. x_1 = letzter x_n), Bedingung: $\{x_1, x_n\} \in E$
  - ▷ Satz von Ore: G endl. zshgd.: $\forall x, y \in V : \{x, y\} \notin E \wedge x \neq y \Rightarrow \mathrm{d}_G(x) + \mathrm{d}_G(y) \geq n$ mit $n = |V| \Rightarrow$ Hamiltonkreis in G

5 Ramseytheorie

- $\binom{A}{2}$: Menge aller 2-elem. Teilmengen von A
  - ▷ $\left|\binom{A}{n}\right| = \binom{|A|}{n}$
- $[n] = \{1, 2, \ldots, n\}$ *(hier)*
- **Färbung von Mengen**: $c : \binom{A}{2} \to [r]$ | r: Anzahl Farben
- ... *(Nicht im Detail aufgeführt, da für die 2016-Klausur nicht erforderlich)*

6 Algebraische Strukturen

6.1 Monoide & Gruppen

- n-stellige Operation auf Menge A: $f : A^n \to A$ (Abbildung)
  - ▷ 2-stellige Operation: $f : A \times A \to A$
- **Monoid**: $(A, \circ)$
  A: beliebige Menge
  $\circ : A \times A \to A$: 2-stellige Operation auf A
  $\circ$ ist assoziativ | $(a \circ b) \circ c = a \circ (b \circ c)$
  $\exists$ neutrales El. e | $\forall a \in A : a \circ e = e \circ a = a$
- **Gruppe**: $(A, \circ)$
  Monoid, für das zusätzlich gilt:
  Jedes Element hat ein inverses Element
  $\forall a \in A : \exists \overline{a} \in A : a \circ \overline{a} = \overline{a} \circ a = e$
- kommutatives M.: $\forall a, b \in A : a \circ b = b \circ a$
  - ▷ kommutative Gruppe = **abelsch**
- **Zyklische Gruppe**: $(G, \circ) = \langle g \rangle$
  $\exists g \in G : G = \{g^n | n \in \mathbb{Z}\}$ ← $g \circ g \circ \ldots \circ g$, n-mal
  - ▷ immer kommutativ $(g^m \circ g^n = g^{m+n} = g^n \circ g^m)$
- $\forall a \in G$ (endl. Gruppe) : $a^{|G|} = 1$
- **Ordnung** von a in G: $\mathrm{ord}(a)$
  Kleinste Zahl $k > 0$ mit $a^k = 1$
  - ▷ Sei $\mathbb{G} = (G, \circ)$ endl. Gruppe.
    $\forall a \in G, k \geq 0 : a^k = 1 \Leftrightarrow \mathrm{ord}(a) | k$
  - ▷ Sei $\mathbb{G} = (G, \circ)$ endl. abelsche Gruppe.
    $\forall a, b \in G : \mathrm{ggT}(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$
    $\Rightarrow \mathrm{ord}(a \circ b) = \mathrm{ord}(a) \cdot \mathrm{ord}(b)$
  - ▷ Sei $\mathbb{G}$ endl. abelsche Gruppe.
    $k = \max\{\mathrm{ord}(a) | a \in G\}$
    $\Rightarrow \forall b \in G : b^k = 1$
- Menge aller **Permutationen** auf A: S_A
  - ▷ symmetrische Gruppe auf A: $(S_A, \circ)$
  - ▷ **symmetrische Gruppe** auf n Elementen: $S_n = S_{\{1,2,\ldots,n\}}$
    - hat $n!$ Elemente
    - für $n \geq 3$ *nicht* kommutativ
  - ▷ Permutationen = Änderung der Reihenfolge | **Bsp.:** $S_3 \ni \sigma = \left(\overleftrightarrow{1, 2, 3}\right)$
    El. von Pos. 1 geht an Pos. 2, 2 an 3, 3 an 1
    Anwendung: $\sigma(a, b, c) = (c, b, a)$
  - ▷ mehrfach: $\sigma(1, 2, 3) = (3, 2, 1)$
  - ▷ $S_3 = \{\mathrm{id}, (1,2), (2,3), (1,3), (1,2,3), (1,3,2)\}$
- Ganzzahlige Division mit Rest:
  $x \mod n$: Rest, $x \operatorname{div} n$: Quotient ohne Rest
  Bsp.: $7 : 2 = 3\ \mathrm{R}\ 1$ ($7 \operatorname{div} 2 = 3$, $7 \mod 3 = 1$)
  - ▷ **Kongruenz** (mod-Schreibweise):
    $x \mod n = m \mod n \Leftrightarrow x \equiv_n m$

  $\forall x, y, n \in \mathbb{Z}, n \geq 2$:
  - ▷ $((x \mod n) + (y \mod n)) \mod n = (x + y) \mod n$
  - ▷ $((x \mod n) \cdot (y \mod n)) \mod n = (x \cdot y) \mod n$
  - ▷ $x_1 \equiv_n x_2 \wedge x_2 \equiv_n y_2 \Rightarrow x_1 + x_2 \equiv_n y_1 + y_2 \wedge x_1 \cdot x_2 \equiv_n y_1 \cdot y_2$
  - ▷ $x^2 \mod n = (x \mod n)^2 \mod n$
- $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ (alle $\mathbb{N}$ bis $n-1$)
- $a +_n b = (a + b) \mod n$
  $a \cdot_n b = (a \cdot b) \mod n$
- **Homomorphismus**
  von $\mathbb{G}_1 = (G_1, \circ_1)$ nach $\mathbb{G}_2 = (G_2, \circ_2)$:
  Abbildung $f : G_1 \to G_2$,
  $\forall a, b \in G_1 : h(a \circ_1 b) = h(a) \circ_2 h(b)$
- **Isomorphismus**: bijektiver Homomorphismus
- **Untergruppe** $U \trianglelefteq \mathbb{G} = (G, \circ)$
  - ▷ $U \subseteq G, U \neq \emptyset$
  - ▷ $\forall a \in U : a^{-1} \in U$ (Inverse alle da)
    $\forall a, b \in U : a \circ b \in U$ (abgeschlossen)
  - ▷ Gruppe $\mathbb{H} \leq \mathbb{G}$, wenn in $\mathbb{G}$ eine Untergruppe U existiert, die isomorph zu $\mathbb{H}$ ist
    Bsp.: $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$
- Nebenklassen einer Untergruppe U:
  - ▷ **Linksnebenklassen**: $L \subseteq \mathbb{G}, L = a \circ U = \{a \circ u | u \in U\} = aU$ $(a \in \mathbb{G})$
  - ▷ **Rechtsnebenklassen**: $R \subseteq \mathbb{G}, R = U \circ a = \{u \circ a | u \in U\} = Ua$ $(a \in \mathbb{G})$
  - ▷ Bei abelschen Gruppen: $L = R$
  - ▷ $\forall L, R : |L| = |R| = |U|$
  - ▷ $aU = bU \Leftrightarrow a^{-1}b \in U$
    $Ua = Ub \Leftrightarrow ab^{-1} \in U$
  - ▷ verschiedene NK sind immer disjunkt.
  - ▷ $|U| \,|\, |G|$ (Lagrange),
    $\frac{|G|}{|U|}$ = Anzahl LNK/RNKs = **Index** $[\mathbb{G} : U]$
- Multiplikation von Teilmengen AB *(hier)*: alle Elemente von A je verknüpft mit allen Elementen aus B ($\mathbb{G} = (G, \circ)$, $A, B \subseteq G, AB = A \circ B = \{a \circ b | a \in A, b \in B\} \subseteq G$)
- **Normalteiler** $U \subseteq G$
  wenn $\forall g \in G : \forall u \in U : g^{-1}ug \in U$
  - ▷ auch genannt: „U ist unter Konjugation mit beliebigen Elementen aus G abgeschlossen“
  - ▷ G/U = Menge aller LNK von U
  - ▷ $g_1U \circ g_2U = (g_1g_2)U \in G/U$
  - ▷ $(G/U, \circ)$ wieder Gruppe („Quotient von $\mathbb{G}$ bzgl. U“)
- Seien $\mathbb{G} = (G, \circ)$, $\mathbb{H} = (H, \circ)$ Gruppen, $\varphi : G \to H$ Homomorphismus.
  - ▷ **Kern**: $\ker(\varphi) = \{g \in G | \varphi(g) = e_{\mathbb{H}}\}$
  - ▷ **Bild**: $\mathrm{im}(\varphi) = \{\varphi(g) | g \in G\}$
  - ▷ $\ker\varphi$ ist Normalteiler von $\mathbb{G}$
  - ▷ $\mathrm{im}\,\varphi$ ist Untergruppe von $\mathbb{H}$
  - ▷ $\mathbb{G}/\ker\varphi$ ist isomorph zu $\mathrm{im}\,\varphi$ (1. IsoG)

6.2 Ringe & Körper

- **Ring** $(A, \oplus, \otimes)$
  - ▷ $(A, \oplus)$ abelsche Gruppe, Neutralel.: 0
  - ▷ $(A, \otimes)$ Monoid, Neutralel: 1
  - ▷ Distributivgesetz gilt
    $\forall a, b, c : a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$
    $\forall a, b, c : (b \oplus c) \otimes a = (b \otimes a) \oplus (c \otimes a)$
  - ▷ wenn $(A, \otimes)$ kommutativ: „komm. Ring“
- **Körper** $(A, \oplus, \otimes)$
  - ▷ $(A, \oplus)$ abelsche Gruppe
  - ▷ $(A \setminus \{0\}, \otimes)$ abelsche Gruppe
  - ▷ Distributivgesetz gilt
  - ▷ $\forall$ Körper : $1 \neq 0$
- Konventionen:
  - ▷ Ring: Inverses von $a \in (A, \oplus) \widehat{=} -a$
  - ▷ Körper: Inverses von $a \in (A, \otimes) \widehat{=} a^{-1}$
  - ▷ Ring: $a \otimes b = ab$
- Eigenschaften von Körpern:
  - ▷ $\forall a \in K : a \otimes 0 = 0 \otimes a = 0$
  - ▷ $\forall a, b \in K : ab = 0 \Rightarrow (a = 0 \vee b = 0)$ „Nullteilerfreiheit“
  - ▷ $\forall a \in K : -a = (-1) \otimes a$
  - ▷ $(K, +, \cdot)$ endl. $\Rightarrow (K \setminus \{0\}, \cdot)$ zyklisch Erzeuger „primitives Element“ genannt
- **Ringhomomorphismus** $\varphi : \mathbb{Z} \to K, n \in \mathbb{Z}$

$$\varphi(n) = \begin{cases} 1 \oplus 1 \oplus \ldots \oplus 1 (n \text{ mal}) & \text{wenn } n > 0 \\ 0 & \text{wenn } n = 0 \\ -\varphi(-n) & \text{wenn } n < 0 \end{cases}$$

  - ▷ $\varphi(m) \oplus \varphi(n) = \varphi(m + n)$
  - ▷ $\varphi(m) \otimes \varphi(n) = \varphi(m \cdot n)$
- **Charakteristik** $\mathrm{char}(\mathbb{K})$ des Körpers $\mathbb{K}$
  - ▷ wenn $\varphi(n) = 1 \oplus 1 \oplus \ldots \oplus 1$ (n mal) $\neq 0$ $\forall n \geq 1 \Rightarrow \mathrm{char}\,\mathbb{K} = 0$
  - ▷ wenn $\exists n \geq 1$ mit $\varphi(n) = 0$ $\Rightarrow \mathrm{char}\,\mathbb{K} = \min\{n | \text{mit d. Eigensch.}\}$
  - ▷ wenn $\mathrm{char}\,\mathbb{K} \neq 0 \Rightarrow \mathrm{char}\,\mathbb{K}$ prim
- $(\mathbb{Z}_n, +_n, \cdot_n)$ ist Körper, genau wenn n prim

6.3 Polynome

- **Polynom** über $\mathbb{K}$ vom Grad $n \geq 0$:
  $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0$
  mit $a_i \in \mathbb{K}$ und $(a_n \neq 0 \vee n = 0)$
- $\mathbb{K}[x]$: Menge aller Polynome über $\mathbb{K}$
- $p(x)$ sei ein bestimmtes Polynom, $\mathrm{grad}(p(x)) = n$ für Grad von $p(x)$
- Polynome mit Grad 0 sind Elemente von $\mathbb{K}$
- $\mathbb{K}[X] \subseteq \mathbb{K}$
- $(\mathbb{K}, +, \cdot)$ kommutativer Ring („**Polynomring**“)
  - ▷ Polynome kann man addieren und multiplizieren
- Auswerten: Abbildung $v_k : \mathbb{K}[x] \to \mathbb{K}$
  mit $v_k(a_n x^n + \ldots + a_0) = a_n k^n + \ldots + a_0$
  - ▷ $v_k(p(x))$ auch einfach $p(k)$
  - ▷ v_k ist ein Ringhomomorphismus
- **Polynomdivision**: analog schr. Division in $\mathbb{Z}$
  $\forall a(x), b(x) \in \mathbb{K}[x] : \exists q(x), r(x) \in \mathbb{K}[x] :$
  $a(x) = b(x) \cdot q(x) + r(x)$
  - ▷ $q(x) = a(x) \operatorname{div} b(x)$
  - ▷ $r(x) = a(x) \mod b(x)$
  - ▷ Modulo-Rechenregeln genau wie $\mathbb{Z}$
  - ▷ Teilbarkeit wie üblich ($\exists q(x) \ldots$)
  - ▷ $\forall a(x) \in \mathbb{K}[x], k \in \mathbb{K}$:
    $a(x) | k \cdot a(x) \wedge k \cdot a(x) | a(x)$
- **Nullstellen**: $k \in \mathbb{K}$ ist Nullstelle von $a(x) \in \mathbb{K}[x]$, wenn $a(x) = 0$
  - ▷ wenn k Nullstelle, $\exists b(x) \in \mathbb{K}[x]$:
    $a(x) = (x - k) \cdot b(x)$

- ▷ $a(x)$ hat max. $\text{grad}(a(x))$ viele Nullst.
- ▷ $\mathbb{K}$ ist „algebraisch abgeschlossen“ wenn *jedes* Polynom ≥ 1 Nullst. hat (**Bsp.:** Körper der Menge $\mathbb{C}$)
- ▷ mehrfache Nullstelle:
  $\exists b(x): a(x) = (x-k)^2 \cdot b(x)$
  k ist mehrfache Nullst. von $a(x)$, genau dann wenn k *keine* Nullst. von $a'(x)$

- **Ableitung** $a'(x) \in \mathbb{K}[x]$
  - ▷ übliche Ableitungsregeln gelten:
    $a(x) = \sum_{i=0}^{n} a_i x^i \Rightarrow a'(x) = \sum_{i=0}^{n} i \cdot a_i x^{i-1}$
  - ▷ Summenregel gilt: $a(x) = p(x) + q(x)$
    $\Rightarrow a'(x) = p'(x) + q'(x)$
  - ▷ Produktregel gilt: $a(x) = u(x) \cdot v(x)$
    $\Rightarrow a'(x) = u'(x) \cdot v(x) + u(x) \cdot v'(x)$
- **Irreduzibles Polynom** $p(x) \in \mathbb{K}[x] (\neq 0)$, wenn $\forall a(x), b(x) \in \mathbb{K}[x] : p(x) = a(x) \cdot b(x) \Rightarrow \text{grad}(a(x)) = 0 \wedge \text{grad}(b(x)) = 0$
  - ▷ sozusagen „Primzahlen in $\mathbb{K}[x]$“
- Es gibt $\text{ggT}(a(x), b(x))$ analog $\mathbb{Z}$ (auch mit erw. Euklidischen Algorithmus)
- „Äquivalent“ des Restklassenrings: $\mathbb{K}[x]_{q(x)} = \left(\mathbb{K}[x]_n, +_{q(x)}, \cdot_{q(x)}\right)$
  - ▷ $q(x) \in \mathbb{K}[x], n = \text{grad}(q(x)) > 0$
  - ▷ $\mathbb{K}[x]_n = \{a(x) \in \mathbb{K}[x] \mid \text{grad}(a(x) < n)\}$
  - ▷ $a(x) +_{q(x)} b(x) = (a(x) + b(x)) \bmod q(x)$
  - ▷ ist kommutativer Ring
  - ▷ ist Körper genau wenn $q(x)$ irreduzibel
  - ▷ ist Erw.-Körper von $\mathbb{K}$ ($\mathbb{K}[x]_{q(x)} \supseteq \mathbb{K}$)
- **Zerfällungskörper**: $\forall a(x) \in \mathbb{K}[x] : \exists \mathbb{K}' \supseteq \mathbb{K}$, sodass $a(x)$ über $\mathbb{K}'$ in Linearfaktoren zerfällt (**Bsp.:** im Körper mit $\mathbb{C}$)
- Sei $p \in P$, $\mathbb{K} = (K, +, \cdot)$, $\text{char}(\mathbb{K}) = p$, $q = p^r$ $(r > 0)$
  - ▷ $x^q - x$ hat keine mehrfachen Nullst. in $\mathbb{K}$
  - ▷ $\{k \in K \mid k^q - k = 0 \text{ in } \mathbb{K}\}$ = Menge aller Nullst.: Teilkörper von $\mathbb{K}$
  - ▷ $\exists_1$ Körper mit q Elementen (außer Isomorphie) genannt $\text{GF}(x)$

6.4 Vektoren

- Sei $\mathbb{K} = (K, +, \cdot)$ endl. Körper dann $\exists p \in P, r \geq 1 : |K| = p^r$
- **Vektorraum** über Körper $\mathbb{K}$: Tripel $\mathbb{V} = (V, \oplus, \odot)$
  - ▷ $(V, \oplus)$ abelsche Gruppe
  - ▷ $\otimes : K \times K \to V$ ist Abbildung **„Skalarmultiplikation“**
    - $\forall a, b \in K, v \in V : a \odot (b \otimes v) = (a \times b) \otimes v$
    - $\forall a \in K, u, v \in V : a \odot (u \oplus v) = (a \odot u) \otimes (a \odot v)$
    - $\forall a, b \in K, v \in V : (a + b) \odot v = (a \odot v) \oplus (b \odot v)$
    - $\forall v \in V : 1 \odot v = v$
- **Lineare Unabhängigkeit** von $U \subseteq V$: $\forall a_1, a_2, ..., a_n \in K$; paarweise verschiedene $v_1, v_2, ..., v_n \in U : a_1 v_1 \oplus a_2 v_2 \oplus ... \oplus a_n v_n = 0_{\mathbb{V}} \Rightarrow a_1 = a_2 = ... = a_n = 0_{\mathbb{K}}$
  - ▷ **Basis** von $\mathbb{V}$: linear unabhängige Teilmenge $B \subseteq V$, $\forall v \in V : \exists a_1, ..., a_n \in K; v_1, ..., v_n \in B : a_1 v_1 \oplus a_2 v_2 \oplus ... \oplus a_n v_n$
    - jeder $\mathbb{V}$ hat eine Basis
    - alle Basen haben die gleiche Kardinalität $\dim \mathbb{V}$
    - $\dim \mathbb{V} = n < \infty \wedge \{v_1, ..., v_n\}$ Basis von $\mathbb{V} \Rightarrow$ jeder $v \in \mathbb{V}$ hat eine eindeutige Darstellung $v = a_1 v_1 \oplus a_2 v_2 \oplus ... \oplus a_n v_n$, man kann v mit Tupel $(a_1, a_2, ..., a_n)$ identifizieren
    - $\mathbb{V}$ endl.-dimensional, $\mathbb{K}$ endl. $\Rightarrow |\mathbb{V}| = |\mathbb{K}|^{\dim \mathbb{V}}$

7 Zahlentheorie

- $a|b$: „a **teilt** b“
- $\text{ggT}(a,b)$: **größter gemeinsamer Teiler**
  $= \max\{k \in \mathbb{N} | (k|a) \wedge (k|b)\}$
  $= p_k^{\min\{e_{ka}, e_{kb}\}} ... p_1^{\min\{e_{1a}, e_{1b}\}}$ einer PFZ
  - ▷ $\text{ggT}(0,0)$ nicht definiert
- **Primzahlen**: $P = \{p \in \mathbb{N} \setminus \{0,1\} |$
  $\forall n \in \mathbb{N} \setminus \{0\} : (n|p) \Rightarrow n = 1 \vee n = p\}$
- $p \in P, a, b \in \mathbb{Z}, p|(a \cdot b) \Rightarrow p|a \vee p|b$ (Euklid)
- **Fundamentalsatz der Arithmetik**: Jede Zahl $n \in \mathbb{N}$ lässt sich eindeutig als Produkt von Primzahlen darstellen (**Primfaktorzerlegung**)
- $\forall \lambda \in \mathbb{Z} : t|m \wedge t|n \Rightarrow t|(n + \lambda m)$
- $\forall \lambda \in \mathbb{Z} : \text{ggT}(m,n) = \text{ggT}(m, n + \lambda m)$
  - ▷ $\text{ggT}(m,n) = \text{ggT}(m, n \mod m)$
    (Grundlage des Euklidischen Algorithmus')
- **Erweiterter Euklidischer Algorithmus**

m	n	$n \text{ div } m$	$n \bmod m$	x	y
22	222	2	2		
⋮	⋮	⋮	⋮		
2		2		⊙ ⊕	1
2	2	2	0	1	0

ggT ← fertig!

$x_i = -x_{i-1} \cdot (n \text{ div } m)_i + y_{i-1}$

- $\text{ggT}(a,n) = \text{ggT}(b,n) = 1 \Rightarrow \text{ggT}(a,b) = 1$
- $\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n \mid \text{ggT}(x,n) = 1\} \subseteq \{1, ..., n-1\}$, $n \geq 2$: „Alle zu n teilerfremden Zahlen bis n“
- **Eulersche** φ**-Funktion**: $\varphi(n) = \left|\mathbb{Z}_n^*\right|, n \geq 2$
  - ▷ $p \in P : \varphi(p) = p - 1$
  - ▷ Für $p, q \in P$ mit $p \neq q$:
    $\varphi(p \cdot q) = (p-1)(q-1)$
  - ▷ $\forall n \geq 2, a \in \mathbb{Z}_n^* : a^{\varphi(n)} \equiv_n 1$ (Euler)
    - $\mathbb{G} = (G, \circ)$ endl. Gruppe (Neutr.e. 1) und $|G| = n \Rightarrow \forall a \in G : a^n = 1$
- $\forall n \geq 2 : n \in P \Leftrightarrow \forall a \in \mathbb{Z}_n \setminus \{0\} : a^{n-1} \equiv_n 1$ (Kleiner Satz von Fermat)
- **Chinesischer Restsatz**:
  Seien $m_1, m_2, ..., m_k \geq 2$, $\text{ggT}(m_i, m_j) = 1$ wenn $i \neq j$. Sei $M = m_1 \cdot m_2 \cdot ... \cdot m_k$. Dann:
  $\mu : \mathbb{Z}_M \to \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times ... \times \mathbb{Z}_{m_k}$ bijektiv
  $\mu(x) = (x \mod m_1, ..., x \mod m_k)$

  Bsp.: Finde $x \in \mathbb{Z}_{210}$
  $\to M = m_1 \cdot m_2 \cdot m_3 = 210$
  $x \mod 3 = 1$ (1) $M_1 = \frac{M}{m_1} = 70$
  $x \mod 7 = 3$ (2) $M_2 = \frac{M}{m_2} = 30$
  $x \mod \underset{m_i}{10} = \underset{a_i}{5}$ (3) $M_3 = \frac{M}{m_3} = 21$

  - ▷ Finde $x_i N_i$ mit $x_i \cdot m_i + N_i \cdot M_i = 1$
  - ▷ Lösung: $x = \sum_{i=1}^{3} a_i N_i M_i \mod 210$
  - ▷ *Eukl. Alg.*: gesucht N_i (x_i ist unwichtig!)
    $m_i \mid M_i \mid M_i \text{ div } m_i \mid M_i \bmod m_i \mid x_i \mid N_i$

7.1 RSA-Verschlüsselung

- Idee: Empfänger E erzeigt einen Schlüssel c und einen Entschlüsselungsschlüssel d, c wird an Sender S geschickt.
- E wählt 2 große Primzahlen p, q.
  - ▷ berechnet: $n = p \cdot q$ (öffentlich, also c), $\varphi(n) = (p-1)(q-1)$ (geheim, also d)
  - ▷ bestimme zufällig $k \in \mathbb{N}$, sodass $\text{ggT}(k, \varphi(n)) = 1$ (öffentlich) und $l \in \mathbb{N}$, sodass $k \cdot l \equiv_{\varphi(n)} 1$ (geheim)
- Nachricht ist Zahl $x \in \mathbb{Z}_n$
  - ▷ Codierung: $x \mapsto x^k \mod n$
  - ▷ Decodierung: $y \mapsto y^l \mod n \left(\left(x^k\right)^l \equiv_n x\right)$
- Euklidischer Algorithmus liefert x, y mit $k \cdot x + \varphi \cdot y = 1$, $k \cdot x \mod \varphi(n) = 1 \to l = x \mod \varphi(n)$:
  $k \mid \varphi(n) \mid \varphi \text{ div } k \mid \varphi \bmod k \mid x \mid y$
- „Brechen“ durch diskretes Wurzelziehen

7.2 Fibonacci-Zahlen

- $F_0 = 0, F_1 = 1, F_{n+2} = F_{n+1} + F_n \quad \forall n > 0$
- Betrachte $x^2 = x + 1$.
  Lösungen: $\phi = \frac{1+\sqrt{5}}{2} \approx 1{,}618$ $\psi = \frac{1-\sqrt{5}}{2} - \phi \approx -0{,}618$
  - ▷ $\phi^{n+2} = \phi^{n+1} + \phi^n \wedge \psi^{n+2} = \psi^{n+1} + \psi^n$
  - ▷ $\forall n \geq 0 : F_n = \frac{1}{\sqrt{5}}\left(\phi^n - \psi^n\right) = \left[\frac{\phi^n}{\sqrt{5}}\right]$
    (runden, $0{,}5$ abrunden)
  - ▷ Laufzeit eukl. Alg. $(n, m) = k$ Aufrufe, $m \geq F_k \wedge n \geq F_{k+1}$

8 Kodierungstheorie

- **Hamming-Distanz**:
  Anzahl unterschiedlicher Stellen
- (k,n)-Code: $f : \Sigma^k \to \Sigma^n$
- t-fehlerekennende Codes: $\forall u, v \in \Sigma^k : u \neq v \Rightarrow \text{d}_\text{H}(f(u), f(v)) \geq t + 1$
- t-fehlerkorrigierend: $\forall u, v \in \Sigma^k : u \neq v \Rightarrow \text{d}_\text{H}(f(u), f(v)) \geq 2t + 1$
- **Reed-Solomon-Codes**: $\text{RS}_{s,k,t} : \text{GF}(2^s)^k \to \text{GF}(2^s)^{2t+k}$ $(k, 2t+k)$-Code, $\cdot s$ für Bits
- ... *(Nicht im Detail aufgeführt, da für die 2016-Klausur nicht erforderlich)*