Diskrete Mathematik Zusammenfassung

Logik I (Kapitel 2)

Generell

Wahr (1) und Falsch (0)

A	B	$A\land B$	$A\lor B$	$A\to B$	$A\leftrightarrow B$
0	0	0	0	1	1
0	1	0	1	1	0
1	0	0	1	0	0
1	1	1	1	1	1

Negation: $\neg A$
Und (Konj.): $A \land B$
Oder (Disj.): $A \lor B$
Implikation: $A \to B = \neg A \lor B$

Doppelte Implikation: $A \leftrightarrow B = (A\to B) \land (B \to A)$
$\top$ ist Tautologie = immer 1, $\bot$ immer 0
F und G sind **äquivalent**, $F \Leftrightarrow G$
Erfüllbar, min. 1 wahrer Fall
Unerfüllbar, kein wahrer Fall
F nur Tautologie, falls $\neg F$ unerfüllbar ist
$F \Rightarrow G$: $F \to G$ ist Tautologie
k-tes Prädikat: P ist eine Funktion $U^k \to \{0,1\}$,
z.B. $\text{prime}(x) = \{1$ falls x prim, 0 sonst$\}$
$\forall$: Für alle...
$\exists$: Es existiert... } Quantore
Quantore können verschachtelt werden
$\forall x\, P(x) \land \forall x\, Q(x) = \forall x\, (P(x) \land Q(x))$
$\neg \forall x\, P(x) = \exists x\, \neg P(x)$
$\neg \exists x\, P(x) = \forall x\, \neg P(x)$
Modus Ponens: F, $F \to G$ wahr $\Rightarrow$ G Tautologie
Implikation ist transitiv: $F \to G \land G \to H \Rightarrow F \to H$

Beweistechniken

Direkter Beweis: $F \to G$, nehme F an und leite daraus G ab. (Beweist nur Implikation, nicht Wahrheitswert)
Indirekter Beweis: $F \to G$: nehme $\neg G$ an, beweise dann $\neg F$, d.h. Beweise $\neg G \to \neg F$. Ist $\neg G \to \neg F$ eine Tautologie, ist auch $F \to G$ Tautologie.
Beweis durch Fallenteschidung: Alle möglichen Fälle auflisten und einzeln beweisen.
Beweis durch Gegenannahme: Nehme an dass Aussage Falsch ist, Widerlege diese Annahme.
Existenzbeweis: Bei Aussage der Form $\exists x\, P(x)$, gebe ein Existierendes Element an so dass $P(x)$ wahr ist.
Gegenbeispiel: Bei Aussage der Form $\neg\forall x\, P(x)$ wird x gesucht so dass $\neg P(x)$ wahr ist.
Beweis durch Induktion:
1) Verankerung $P(0)$ beweisen
2) Unter Annahme dass $P(n)$ stimmt zeige $P(n+1)$.

Log. Konsequ.

Logische Konsequenz: $F \models G$: G ist logische Konsequenz von F, wenn für alle möglichen Wahrheitszuordnungen in den Symbolen in F und G der Wahrheitswert von G 1 ist wo der von F 1 ist.
Beispiel: $A \land B \models A \lor B$.

Schubfachprinzip:

Wenn eine Menge aus n Objekten in $k<n$ Mengen unterteilt wird, hat mindestens eine dieser Mengen $\lceil n/k \rceil$ Elemente.
Beispiel: Aus 100 Personen gibt es min. 9 Personen die im gleichen Monat Geburtstag haben.
$\to \lceil 100/9 \rceil = 12$ □

Logik II (Kapitel 6)

Beweissysteme

D6.1: **Beweissystem**: Quadrupel $\Pi = (S, P, \tau, \Phi)$
S: Aussagen, P: Beweise, τ: Wahrheitsfunktion $\tau: S \to \{0,1\}$ (Aussage wahr), Φ: Verifikationsfunktion $\Phi: S \times P \to \{0,1\}$ ($\Phi(s,p)$ wahr falls p gültiger Beweis für s.)
D6.2: **korrekt**: keine falsche Aussage hat einen Beweis: $\Phi(s,p)=1 \to \tau(s)=1$
D6.3: **komplett**: jede Aussage hat einen Beweis

Grundlagen

D6.4: **Syntax**: Grammatik der Aussage
D6.5: **Belegung**: Besondere Wahl der Werte in einer Fkt.
D6.6: **passend**: Belegung bei der alle Variabeln definiert sind.
D6.7: **Semantik**: Wahrheitsfunktion $\sigma(F, \mathcal{A}) \to \{0,1\}$ die jeder Formel F und jeder Belegung $\mathcal{A}$ passend für F einen Wert zuweist.
D6.8: **Modell** für F: $\mathcal{A} \models F$ ($\sigma(F,\mathcal{A})=1$), d.h. passende Belegung $\mathcal{A}$ wobei F wahr ist.
D6.9: **erfüllbar**: es gibt ein Modell für F, sonst heisst die Formel **unerfüllbar** ($\bot$)
$\sigma(F,\mathcal{A}) = \mathcal{A}(F)$: Wahrheitswert von F unter Belegung / Interpretation $\mathcal{A}$.
D6.10: **Tautologie / gültig**: wahr für alle Interpretationen.
L6.1: F ist Taut. genau wenn $\neg F$ $\bot$ ist.
D6.11: G ist **logische Konsequenz** von F ($F \models G$) falls jede passende Belegung für F und G sowohl ein Modell für F als auch für G ist.
D6.12: **Äquivalent**: $F \equiv G \Leftrightarrow F \models G \land G \models F$

Log. Kalkül

D6.14: **Schlussregel**: Regel zum Ableiten einer Formel G aus einer Menge an Formeln. Wir schreiben $\{F_1, \dots, F_n\} \vdash_R G$. Bsp.: $\{F \land G\} \vdash F$
D6.15: **Logisches Kalkül**: Endliche Menge von Schlussregeln: $K = \{R_1, \dots, R_n\}$
D6.16: **Herleitung**: Eine Formel G aus Menge M im Kalkül K durch Anwenden einer finiten Sequenz von Regeln aus K herleiten: $M \vdash_K G$
D6.17: **Korrekte Herleitung**: Regel R ist korrekt falls $M \vdash_R F \Rightarrow M \models F$ gilt.

D6.18: Herleitung ist **widerspruchsfrei** oder **korrekt**: $M \vdash_K F \Rightarrow M \models F$ und K ist **vollständig** falls $M \models F \Rightarrow M \vdash_K F$
L6.2: Wenn $F \vdash_K G$ für ein widerspruchfreies Kalkül, dann ist $\models (F \to G)$
D6.13: $\models F$: F ist **Tautologie**

D6.19: **Atomare Formel** der Form A_i, $i \in \mathbb{N}$. Eine **Formel** ist Kombination aus Atomaren Formeln, wobei diese auch Formeln sind.
D6.20: Für Menge M an Formeln, eine **Wahrheitsbelegung** ist eine Funktion $\mathcal{A}: M \to \{0,1\}$:
$\mathcal{A}((F \land G)) = 1$ genau wenn $\mathcal{A}(F) = 1 \land \mathcal{A}(G) = 1$
$\mathcal{A}((F \lor G)) = 1$ genau wenn $\mathcal{A}(F) = 1 \lor \mathcal{A}(G) = 1$
$\mathcal{A}(\neg F) = 1$ genau wenn $\mathcal{A}(F) = 0$.

L6.2 Für Formeln F, G, H gilt:
Idempotenz: $F \land F \equiv F$ $\quad F \lor F \equiv F$
Kommutativität: $F \land G \equiv G \land F$ $\quad F \lor G \equiv G \lor F$
Assoziativität: $(F\land G) \land H \equiv F \land (G \land H)$ $\quad (F \lor G) \lor H \equiv F \lor (G \lor H)$
Absorption: $F \land (F \lor G) \equiv F$ $\quad F \lor (F \land G) \equiv F$
Distributiv: $F \land (G \lor H) \equiv (F \land G) \lor (F \land H)$
Distributiv: $F \lor (G \land H) \equiv (F \lor G) \land (F \lor H)$
Doppelte Neg.: $\neg(\neg F) \equiv F$
De Morgan: $\neg(F \land G) \equiv \neg F \lor \neg G$ $\quad \neg(F \lor G) \equiv \neg F \land \neg G$
Tautologie: $F \lor \top \equiv \top$ $\quad F \land \top \equiv F$
Unerfüllbar: $F \lor \bot \equiv F$ $\quad F \land \bot \equiv \bot$
$F \lor \neg F \equiv \top$ $\quad F \land \neg F \equiv \bot$

Aussagenlogik

D6.21: **Literal**: atomare Formel oder Negation davon
D6.22: **CNF (Konjunktive Normalform)**: Verunde alle oder-„Päckchen" an Literalen die 0 sind in der Wahrheitstabelle
D6.23: **DNF (Disjunktive Normalform)**: Verodere alle und-„Päckchen" an Literalen die 1 sind.
⇒ Bildung der Normalformen:
1) Lese / Fülle Wahrheitstabelle
2) Falls Ergebnis in Zeile = 0 → Bilde Klausel mit Invertierten Literalen, verodert. Verunde diese Klauseln → CNF
· Falls Ergebnis in Zeile = 1 → Bilde Klausel mit Literalen wie sie sind, verundet. Verodere diese Klauseln → DNF.
T6.3: Jede Formel ist äquiv. zu einer CNF & DNF
D6.24: **Klausel**: Menge an Literalen z.B. $\emptyset$, $\{A, \neg B, C\}$
D6.25: **K(F)**: Menge der Klauseln von F in CNF
D6.26: **K ist Resolvent** von Klauseln K_1, K_2 falls es ein Literal L gibt s.d. $L \in K_1$, $\neg L \in K_2$ und $K = (K_1 - \{L\}) \cup (K_2 - \{\neg L\})$
Bsp.: $\{A, \neg B, C\}$ und $\{\neg A, B\}$ haben Resolvente $\{\neg B, B, C\}$ und $\{A, \neg A, C\}$, aber nicht $\{C\}$ da Res. einzeln angewendet werden.

L6.5: **Resolutionskalkül** ist korrekt wenn $\mathcal{K} \vdash_{RES} K$ dann $\mathcal{K} \models K$

TC6.6: Eine Menge M an Formeln ist unerfüllbar g.d.w. $\mathcal{K}(M) \vdash_{RES} \emptyset$

Prädikatenlogik

D6.27: Prädikatenlogik:
- **Variablensymbol:** x_i, $i \in \mathbb{N}$
- **Funktionssymbol:** $f_i^{(k)}$, $i,k \in \mathbb{N}$, k = Anzahl Argumente
- **Prädikatensymbol:** $P_i^{(k)}$, $i,k \in \mathbb{N}$, k = Anzahl Arg. auf Präd.
- **Term:** Variable und $f_i^{(k)}(t_1,\dots,t_n)$ sind Terme
- **Formel:** $P_i^{(k)}(t_1,\dots,t_n)$ ist Formel
  - F, G Formeln → $\neg F$, $F \wedge G$, $F \vee G$ Formeln
  - $\forall x$: F, $\exists x$: F sind Formeln

D6.28: Variablen sind entweder **gebunden** oder **frei** → Eine V. ist durch einen Quantor im Term gebunden, sonst frei.
→ **Abgeschlossene Formel:** keine freien Variablen

D6.29: **F[x/t]:** jedes freie x wird durch t ersetzt.

D6.30: **Struktur:** Tupel $\mathcal{A} = (U, \phi, \psi, \xi)$
- U = Universum (z.B. $\mathbb{N}$)
- ϕ = weist jedem Fkt.symbol eine Fkt. zu: $\phi(f): U^k \to U$
- ψ = weist jedem Präd.symbol eine Fkt. zu: $\psi(P): U^k \to \{0,1\}$
- ξ = weist jedem Variablensymbol einen Wert aus U zu

D6.31: **Passende Struktur:** Passend für Formel F, falls alle Funktions- & Präd.symbole und freien Variablen von F defin.

D6.32: $\mathcal{A} = (U, \phi, \psi, \xi)$:
- Wert $\mathcal{A}(t)$: ist t Variable: $\mathcal{A}(t) = \xi(t)$
  ist $t = f(t_1,\dots,t_n)$: $\mathcal{A}(t) = \phi(f)(\mathcal{A}(t_1)\dots\mathcal{A}(t_n))$
- Wahrheitswert:
  - $\mathcal{A}((F \wedge G)) = 1$ g.d.w. $\mathcal{A}(F) = 1 \wedge \mathcal{A}(G) = 1$
  - $\mathcal{A}((F \vee G)) = 1$ g.d.w. $\mathcal{A}(F) = 1 \vee \mathcal{A}(G) = 1$
  - $\mathcal{A}(\neg F) = 1$ g.d.w. $\mathcal{A}(F) = 0$
  - $F = P(t_1 \dots t_n) \Rightarrow \mathcal{A}(F) = \psi(P)(\mathcal{A}(t_1) \dots \mathcal{A}(t_n))$

L6.7 Seien F, G, H Formeln (H ohne freie Variablen)

1) $\neg(\forall x F) \equiv \exists x \neg F$	6) $\exists x \exists y F \equiv \exists y \exists x F$
2) $\neg(\exists x F) \equiv \forall x \neg F$	7) $(\forall x F) \wedge H \equiv \forall x (F \wedge H)$
3) $(\forall x F) \wedge (\forall x G) \equiv \forall x (F \wedge G)$	8) $(\forall x F) \vee H \equiv \forall x (F \vee H)$
4) $(\exists x F) \vee (\exists x G) \equiv \exists x (F \vee G)$	9) $(\exists x F) \wedge H \equiv \exists x (F \wedge H)$
5) $\forall x \forall y F \equiv \forall y \forall x F$	10) $(\exists x F) \vee H \equiv \exists x (F \vee H)$

L6.8: Ersetzt man eine Teilformel G in F mit einer Äquivalenten H, so ist die resultierende Formel äquivalent zu F.

L6.9: Für G ohne y: $\forall x G \equiv \forall y G[x/y]$ $\quad \exists x G \equiv \exists y G[x/y]$

D6.33: **Pränexform:** Formel der Form $Q_1 x_1 Q_2 x_2 \dots Q_n x_n \, G$ wo Q_i Quantoren $(\forall, \exists)$ sind und G eine Quantoren-freie Formel ist.

T6.10: **bereinigt:** Variablen umbenennen s.d. keine Variable einmal als frei und als gebundene vorkommt.

T6.10: $\neg \exists x \, \forall y \, (P(y,x) \leftrightarrow \neg P(y,y))$

C6.11: **Russel:** Es gibt keine Menge die alle Mengen beinhaltet, die sich nicht selber beinhalten.

C6.12: Die Menge $\{0,1\}^\infty$ ist unabzählbar.

C6.13: Es gibt unberechenbare Fkt. $\mathbb{N} \to \{0,1\}$

Beispiele zu Logik:

1) Finde alle Modelle für $(C \to (A \vee B)) \to (A \wedge B)$
Lsg: Mache Wahrheitstabelle, nimm die wahren Belegungen

2) Kalkül, das vollständig, aber nicht korrekt [I] und eines das korrekt aber nicht vollständig ist:
I) K mit Regel $\{F\} \vdash_R T$
II) K mit Regel $\{F \vee \neg F\} \vdash_R T$

3) Gib eine Prädikatenlogische Formel F mit Identität an, in der ein zweistell. Fkt.symbol f vorkommt, s.d. für jedes Modell $\mathcal{A}$ von F gilt, dass $\langle U_\mathcal{A}; f^\mathcal{A} \rangle$ ein Monoid ist:
Lsg: $F := \exists e \, \forall x \, (f(x,e) = e \wedge f(e,x) = x) \wedge \forall x \forall y \forall z \, (f(f(x,y),z) = f(x, f(y,z)))$

4) Erweitere die Aussagenlogik um das Symbol $\oplus$ (Exklusives oder):
Syntax: Für alle Formeln F und G ist auch $(F \oplus G)$ eine F.
Semantik: $\mathcal{A}((F \oplus G)) = 1$ g.d.w. $\mathcal{A}(F) = 1$ oder $\mathcal{A}(G) = 1$, aber nicht beides!

5) Sei $F := \forall x \exists y \, (P(x,y) \wedge \neg P(f(x),y) \wedge Q(y,z))$. Finde eine Struktur, die (I) Passend und Modell, (II) passend und kein Modell, (III) nicht passend zu F ist.
I) $U^\mathcal{A} = \mathbb{R}^+$, $f^\mathcal{A}(x) = 2x$, $P^\mathcal{A}(x,y) = 1 \Leftrightarrow x \leq x$, $Q^\mathcal{A}(x,y) = 1$, $z^\mathcal{A} = 1$
II) $U^\mathcal{A} = \mathbb{R}^+$, $f^\mathcal{A}(x) = x$, $P^\mathcal{A}(x,y) = 0$, $Q^\mathcal{A}(x,y) = 0$, $z^\mathcal{A} = 1$, denn für alle x,y ist $Q^\mathcal{A}(x,y) = 0$
III) $U^\mathcal{A} = \mathbb{R}^+$, $z^\mathcal{A} = 1337$, denn für alle x,y gilt $Q^\mathcal{A}(x,y) = 0$ (unvollständig)

Mengen, Relationen, Funktionen (Kapitel 3)

Mengen

D3.1: $A = B \Leftrightarrow \forall x (x \in A \leftrightarrow x \in B)$

D3.2: **Kardinalität $|A|$:** Anzahl Elemente in A

D3.3: $A \subseteq B :\Leftrightarrow \forall x (x \in A \to x \in B)$
↳ $A = B \Leftrightarrow (A \subseteq B) \wedge (B \subseteq A)$

D3.4: $\forall x (x \in \emptyset) \Leftrightarrow \forall x \, \neg(x \in \emptyset)$ **Leere Menge**
↳ L3.2: $\forall A \, (\emptyset \subseteq A)$

D3.5: **Potenzmenge $P(A)$** oder 2^A: $P(A) := \{S \mid S \subseteq A\}$ immer mit $\emptyset$. $|A| = k$, $|P(A)| = 2^k$

D3.6: **$A \cup B$:** Vereinigung, $\{x \mid x \in A \vee x \in B\}$
$A \cap B$: Schnittmenge, $\{x \mid x \in A \wedge x \in B\}$

D3.7: **$\bar{A}$, A^c:** Komplement von A, $\{x \in U \mid x \notin A\}$

D3.8: **$A \setminus B$:** A ohne B, $\{x \in A \mid x \notin B\}$

Idempotenz:	$A \cap A = A$	$A \cup A = A$
Kommutativität:	$A \cap B = B \cap A$	$A \cup B = B \cup A$
Assoziativität:	$A \cap (B \cap C) = (A \cap B) \cap C$	$A \cup (B \cup C) = (A \cup B) \cup C$
Absorption:	$A \cap (A \cup B) = A$	$A \cup (A \cap B) = A$
Distributiv:	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
Kompaktheit:	$A \cap \bar{A} = \emptyset$	$A \cup \bar{A} = U$

Ausgeglichenheit: $A \subseteq B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B$

D3.9: **Karthesisches Produkt** $A \times B = \{(a,b) \mid a \in A, b \in B\}$, Bsp.: $A \times \emptyset = \emptyset$, $|A \times \emptyset| = 0$

Relationen

D3.10: **Relation** ρ von A nach B ist Teilmenge von $A \times B$.

D3.11: $id_A = \{(a,a) \mid a \in A\}$

D3.12: **Inverse** einer Relation $a \rho b \Leftrightarrow b \hat{\rho} a$

D3.13: **Komposition:** $a \rho\sigma c :\Leftrightarrow \exists b \in B : (a \rho b \wedge b \sigma c)$
↳ Inverse: $\widehat{\rho\sigma} = \hat{\sigma}\hat{\rho}$

D3.14: **reflexiv:** $a \rho a \;\; \forall a \in A$, $id \subseteq \rho$

D3.15: **irreflexiv:** $a \not\rho a \;\; \forall a \in A$, $id \cap \rho = \emptyset$

D3.16: **symmetrisch:** $\rho = \hat{\rho}$, $a \rho b \Leftrightarrow b \rho a$

D3.17: **antisymmetrisch:** $\rho \cap \hat{\rho} \subseteq id$, $a \rho b \wedge b \rho a \Rightarrow a = b$

D3.18: **transitiv:** $a \rho b \wedge b \rho c \Rightarrow a \rho c$
↳ transitiv falls $\rho^2 \subseteq \rho$

D3.19: **Transitiver Abschluss:** $\rho^* := \bigcup_{n=1}^{\infty} \rho^n$

Äquivalenzrelationen

D3.20: **Äquivalenzrelation:** reflexiv, symmetrisch, transitiv

D3.21: **Äquivalenzklasse** von a: $[a]_\rho := \{b \in A \mid b \rho a\}$, d.h. Elemente die äquivalent zu a sind.

D3.22: **Zerlegung** von A: Unterteilung in disjunkte Teilmengen, die zusammen A bedecken.

D3.23: **Quotientenmenge:** Menge der Äquivalenzklassen von A: $A/\theta = \{[a]_\theta \mid a \in A\}$, A mod θ

Partielle Ordnung

D3.24: **Partielle Ordnung:** reflexiv, antisymmetrisch, transitiv
↳ **Poset:** $(A; \preceq)$ Menge mit part. Ordnung $\preceq$ auf A
↳ $a \prec b \Leftrightarrow a \preceq b \wedge a \neq b$

D3.25: **Vergleichbar:** $a \preceq b \wedge b \preceq a$, sonst unvergleichbar

D3.26: **total geordnet:** zwei bel. El. von $(A; \preceq)$ sind vergleichb.

D3.27: **wohlgeordnet:** total geordnet + jede Teilmenge hat kleinstes Element.

D3.28: **überdecken:** $a \prec b \wedge \neg \exists c (a \prec c \wedge c \prec b)$

D3.29: **Hasse-Diagramm:** gerichteter Graph von $(A; \preceq)$, Knoten = Elemente, a mit b verbunden falls b a überdeckt.

D3.30:
1) $a \in S \subseteq A$ **minimales/maximales Element** von S: $\nexists b \in S: b \prec a \;/\; a \prec b$
2) $a \in S$ **kleinstes/grösstes Element** von S: $\forall b \in S: a \preceq b \;/\; b \preceq a$
3) $a \in A$: **untere/obere Schranke** von S: $\forall b \in S: a \preceq b \;/\; b \preceq a$
4) $a \in A$: **grösste untere/kleinste obere Schranke** von S: wenn a grösstes/kleinstes Element von Menge aller unteren/oberen Schranken von S ist.

D3.31: Meet of a and b $(a \wedge b)$: a und b haben eine grösste untere Schranke
Join of a and b: $(a \vee b)$: a und b haben eine kleinste obere Schranke.

D3.32: Verband: alle Paare von El. haben meet & join.

Funktionen

D3.33: Funktion: $f: A \to B$ mit: $(B^A$ = alle $A \to B)$

1) total definiert: $\forall a \in A \; \exists b \in B: afb$
2) wohldefiniert: $\forall a \in A \; \exists b, b' \in B: afb \wedge afb' \Rightarrow b = b'$

D3.34: partielle Funktion: $A \times B$, nur 2) ist wahr

D3.38: Bild von $A = \{f(a)\} \subseteq B$, $\to \operatorname{Im}(f)$

D3.40: Injektiv: $a \neq b \Rightarrow f(a) \neq f(b)$
Surjektiv: jedes $b \in B$ wird min. 1x getroffen
Bijektiv: injektiv & surjektiv, invertierbar f^{-1}

D3.42: Verkettung: von $f: A \to B$, $g: B \to C = g \circ f$ / gf
$(g \circ f)(a) = g(f(a))$

L3.12: Verkettung ist assoziativ: $(h \circ g) \circ f = h \circ (g \circ f)$

Beispiele zu Mengen, Relationen, Funktionen

1) Beweise $A \subseteq B \Leftrightarrow P(A) \subseteq P(B)$

„$\Rightarrow$": Sei $A \subseteq B$. Wir müssen nun zeigen dass $S \in P(A)$ auch $S \in P(B)$ ist. Mit def. 3.5 folgt: $S \subseteq A \subseteq B$, da $A \subseteq B$ und $\subseteq$ trans. Somit ist S auch ein Element aus $P(B)$. Dies gilt für alle $S \subseteq P(A)$: $A \subseteq B \Rightarrow P(A) \subseteq P(B)$

„$\Leftarrow$": Sei $P(A) \subseteq P(B)$. Weil $A \in P(A)$ und $P(A) \subseteq P(B)$, so muss auch $A \in P(B)$ gelten. Somit ist $A \subseteq B$. □

2) Sei $\leq$ eine bel. Ordnungsrelation. Zeige: $< := \leq \wedge \neq$ ist transitiv.

Lsg: z.z.: $\forall x,y,z\, ((x \leq y \wedge x \neq y \wedge y \leq z \wedge y \neq z) \to (x \leq z \wedge x \neq z))$.
Aus 1. Klammer folgt wegen trans. von $\leq$: $x \leq z$.
Aus $x \neq y \wedge y \neq z$ folgt aber $x \neq z$ nicht! Also müssen wir zeigen, dass $x \leq y \wedge x \neq y \wedge y \leq z \wedge y \neq z$ auch $x \neq z$ impliziert. Annahme: Implikation gilt nicht:
$\exists x,y,z\, (x \leq y \wedge x \neq y \wedge y \leq z \wedge y \neq z \wedge x = z)$. Aus $x \leq y \wedge y \leq z \wedge x = z$ folgt aber $x \leq y \wedge y \leq x$.
Wegen Antisymmetrie von $\leq$ folgt aber $x = y$
$\to$ Widerspruch zu $x \neq y$ □

3) Seien A, B, C Mengen mit $A \neq \emptyset$ und $A \times B = A \times C$. Zeige dass $B = C$ gilt.

Lsg.: Sei $B \neq C$. Dann gibt es ein $x \in B$ und $x \notin C$. Betrachte nun (a, x). von $A \times B$. Dies existiert da $A \neq \emptyset$. Nach Annahme ist aber $x \notin C$ und somit $(a, x) \notin A \times C \to A \times B \neq A \times C$
$\to$ Widerspruch! □

4) Sei A eine bel. Menge und $f: A \to P(A)$ eine Fkt. Zeige: f ist nicht surjektiv.

Lsg: Wir betrachten $M_f := \{a \in A \mid a \notin f(a)\}$ und zeigen, dass die Menge von der Fkt. nicht angenommen wird, was der Aussage widerspricht, dass f nicht surjektiv ist. Sei $f: A \to P(A)$. Angenommen es gibt ein $a \in A$ mit $f(a) = M_f$. Dann gilt $a \in M_f \Leftrightarrow a \notin f(a) = M_f$, ein Widerspruch zu unserer Annahme, womit es kein $a \in A$ mit $f(a) = M_f$ geben kann und M_f somit nicht im Bild von f ist. f ist also nicht surjektiv.

5) Seien A, B Mengen, $f: A \to B$ injektiv und $g: B \to A$ surjektiv. Zeige $\emptyset: A^A \to B^B$, $h \mapsto f \circ h \circ g$ ist injektiv.

Lsg: Wir müssen zeigen dass $\forall h_1, h_2 \in A^A: h_2 \neq h_1 \Rightarrow \emptyset(h_1) \neq \emptyset(h_2)$. Seien $h_1, h_2 \in A^A$ mit $h_1 \neq h_2$, d.h. $\exists a \in A: h_1(a) \neq h_2(a)$. Sei a_0 ein solches Element mit $h_1(a_0) \neq h_2(a_0)$. Sei ausserdem $b \in B$ mit $g(b) = a_0$. Dieses b existiert immer durch surj. von g. Wir haben also $h_1(g(b)) \neq h_2(g(b))$. Durch die Inj. von f folgt weiter $f(h_1(g(b))) \neq f(h_2(g(b))) \Leftrightarrow f \circ h_1 \circ g \neq f \circ h_2 \circ g \neq \emptyset(h_2)$ □

6) Seien X, Y bel. Mengen und $f: X \to Y$ eine Funktion. Zeige: Für alle Mengen $A, B \subseteq X$ gilt: $f(A \cap B) = f(A) \cap f(B)$ $\Leftrightarrow$ f ist injektiv.

Lsg.: Wir zeigen zuerst: Für alle Mengen A und $B \subseteq X$ gilt $f(A \cap B) = f(A) \cap f(B) \Rightarrow f$ ist injektiv:
Die Beh. muss insbesondere für $A \cap B = \emptyset$ mit $A \neq \emptyset$ und $B = \emptyset$ gelten. Für die Injektion von f müssen wir zeigen dass $a \neq b \Rightarrow f(a) \neq f(b)$ gilt. Mit $A \cap B = \emptyset$ folgt $a \neq b$. Mit $A \cap B = \emptyset$ ist auch $f(A \cap B) = \emptyset$ und damit gem. Annahme auch $f(A) \cap f(B) = \emptyset$. Für $f(a) \in f(A)$, $f(b) \in f(B)$ muss also wegen $f(A \cap B) = \emptyset$ gelten $f(a) \neq f(b)$ wie gewünscht.

Wir zeigen nun noch „$\Leftarrow$":
Dafür zeigen wir zuerst $f(A \cap B) \subseteq f(A) \cap f(B)$ für $A, B \subseteq X$. Falls $f(A \cap B) = \emptyset$ gilt $f(A \cap B) \subseteq f(A) \cap f(B)$ trivialerweise. Falls $f(A \cap B) \neq \emptyset$ sei $c \in f(A \cap B)$. Es gilt $c = f(a) = f(b)$ für ein $a \in A$, $b \in B$. Da f nach Annahme injektiv ist, folgt $f(a) = f(b) \Rightarrow a = b$, und damit $a \in A \wedge a \in B$ $\Rightarrow a \in A \cap B \Rightarrow f(a) \in f(A \cap B) \Rightarrow c \in f(A \cap B)$ wie gewünscht. Da wir nun beide Richtungen $f(A \cap B) \subseteq f(A) \cap f(B)$ und $f(A) \cap f(B) \subseteq f(A \cap B)$ gezeigt haben, gilt die Gleichheit $f(A \cap B) = f(A) \cap f(B)$
□

Zahlentheorie (Kapitel 4)

Division & GGT

D4.1: $a \mid b$, $a = 0$, a teilt b, $\Leftrightarrow \exists c: b = a \cdot c$
a: Teiler (Divisor), b: Vielfaches von a,
c: Quotient

T4.1: (Euklid): Für $a, d \neq 0$ gibt es einzigartige q, r so dass $a = dq + r$, $0 \leq r < |d|$
r ist der Rest, auch $R_d(a)$ oder a mod d genannt.

D4.2: ggT: $d \mid a$, $d \mid b$ und $c \mid a \wedge c \mid b \Rightarrow c \mid d$

D4.3: ggT ist eindeutig. $ggT(a, b) = 1 \Leftrightarrow$ a,b sind teilerfremd.

L4.2: $ggT(n, m - qn) = ggT(m, n)$

D4.4: Ideal: $(a, b) := \{ua + vb \mid u, v \in \mathbb{Z}\}$
$(a) := \{ua \mid u \in \mathbb{Z}\}$

L4.3: Für $a, b \in \mathbb{Z}$ gibt es $d \in \mathbb{Z}$, s.d. $(a, b) = (d)$

L4.4: Falls $(a, b) = (d)$, dann $ggT(a, b) \neq 0$.

K4.5: $ggT(a, b) = ua + vb$, $a, b \neq 0$.

Euklids erweiterter Algorithmus: $(a \geq b)$
berechnet $ggT(a, b)$ sowie s, t so dass
$ggT(a, b) = s \cdot a + t \cdot b$:

a	b	q	u	s	v	t
0	99	0	0	1	1	0
99	78	1	1	0	0	1

$ggT(a, b)$
$=$
$ggT(b, a \bmod b)$

I) Initialisiere mit $a = 0$, $b = a$ und $s, v = 1$

II) Berechnung der nächsten Zeile:
- $a = q \cdot b + r$ (mit neuem a, b)
- $a_{neu} = b$
- $b_{neu} = r$
- $u_{neu} = s$
- $v_{neu} = t$
- $s_{neu} = u - q \cdot s$
- $t_{neu} = v - q \cdot t$

III) So lange machen bis $b = 0$, a ist dann der ggT.

Primfaktorzerlegung

D4.5: Primzahl: $p > 1$ und nur $1 \mid p \wedge p \mid p$
$\hookrightarrow$ sonst zusammengesetzte Zahl.

L4.7: $p \mid (x_1 \cdot x_2 \cdot \ldots \cdot x_n) \Rightarrow p \mid x_i$ für $i \in \{1, \ldots, n\}$

T4.8: Alle Zahlen $\in \mathbb{Z}$ können als Primfaktorzerlegung geschrieben werden.

T4.9: $\sqrt{n}$ irrational ausser $\exists c\; n = c^2$

D4.6: kgV: $a \mid l$, $b \mid l$, $l > 0$ und $a \mid l' \wedge b \mid l'$ $\Rightarrow l \mid l'$, $ggT(a, b) \cdot kgV(a, b) = a \cdot b$

D4.8: $a \equiv_m b$: $m \mid (a - b)$, a ist kongruent zu b mod m, d.h. a und b haben den gleichen Rest bei Division durch m.

L4.14: $m \geq 1$: $\equiv_m$ ist Äquivalenzrelation

L4.15: $f(x_1, \ldots, x_k)$ Polynom mit k Variablen. $m \geq 1$, falls $a_i \equiv_m b_i$ gilt $f(a_1, \ldots, a_k) \equiv_m f(b_1, \ldots, b_k)$

L4.17: i) $a \equiv_m R_m(a)$

ii) $a \equiv_m b \Leftrightarrow R_m(a) = R_m(b)$

L4.18 i) $R_m(a+b) = R_m(R_m(a) + R_m(b))$

ii) $R_m(a \cdot b) = R_m(R_m(a) \cdot R_m(b))$

↳ $R_9(n) \rightarrow$ addiere Dezimalstellen, mod 9

↳ $R_{11}(n) \rightarrow$ addiere Dezimalstellen mit alternierenden VZ

L4.19: $ax \equiv_m 1$ hat Lsg falls $ggT(a, m) = 1$

D4.9: $ax \equiv_m 1$ ist **multiplikative Inverse**: $x \equiv_m a^{-1}$

Chinesischer Restsatz (CRT):

Seien $m_1, m_2, \dots, m_r$ paarweise teilerfremde Zahlen. Sei $M = m_1 \cdot m_2 \cdot \ldots \cdot m_r$. Für jede Liste $a_1, \dots, a_r$ mit $0 \leq a_i < m_i$ hat das System

$x \equiv_{m_1} a_1$

$x \equiv_{m_2} a_2$ $M_i = M/m_i$

$\vdots$ $M_i N_i \equiv_{m_i} 1$ Falls i, sonst $M_i N_i \equiv_{m_k} 0$ $i \neq k$

$x \equiv_{m_r} a_r$

genau 1 Lösung mit $0 \leq x < M$.

$\Rightarrow x = R_M(a_1 M_1 N_1 + a_2 M_2 N_2 + \ldots + a_r M_r N_r)$

Diffie - Hellman - Protokoll

Primzahl p und Generator g in $\mathbb{Z}^*_p$ gegeben.

wähle x_A zufällig aus $\{0, \dots, p-2\}$	wähle x_B zufällig aus $\{0, \dots, p-2\}$
$y_A := R_p(g^{x_A})$	$y_B := R_p(g^{x_B})$
$k_{AB} := R_p(y_B^{x_A})$	$k_{BA} := R_p(y_A^{x_B})$

Secret Key $k_{AB} \equiv_p y_B^{x_A} \equiv_p (g^{x_B})^{x_A} \equiv_p g^{x_A x_B} \equiv_p k_{BA}$

Beispiele zu Zahlen Theorie:

1) Berechne 7^{100} mod 24:
$R_{24}(7^{100}) = R_{24}((7^2)^{50}) = R_{24}(R_{24}(7^2)^{50}) = R_{24}(1^{50}) = 1$

2) Berechne $R_{990}(5^{222}) \Rightarrow$ Benutze CRT & $990 = 9 \cdot 10 \cdot 11$

Lsg: Wir suchen: $x \equiv_9 R_9((5^{6})^{8} \cdot 5^2) = R_9(1 \cdot 5^2) = 7$

$x \equiv_{10} R_{10}((5^{222}) \cdot 1) = 5$

$x \equiv_{11} R_{11}((5^{22})^{10} \cdot 5^2) = R_{11}(1 \cdot 5^2) = 3$

$\rightarrow$ CRT: $R_{990}(7 \cdot 110 \cdot 5 + 5 \cdot 99 \cdot 9 + 3 \cdot 90 \cdot 6) = R_{990}(9925) = \underline{\underline{25}}$

3) Sei $m, n \in \mathbb{N}$, mit $m > n$, $n \nmid m^2$ (← teilt nicht), $ggT(m, n) = 1$. Zeige $mn \nmid m(m+n)$.

Lsg: $n \nmid m^2 \wedge ggT(m, n) = 1 \Rightarrow n \nmid m \Rightarrow \neg \exists k: kn = m$
$\Rightarrow \neg \exists k: kn = m + n \Rightarrow n \nmid (m+n) \Rightarrow mn \nmid m(m+n)$ □

4) Beweise: $a | b \Rightarrow \forall c: a | bc$

Lsg.: $a | b \Rightarrow \exists d: b = ad \Rightarrow bc = a(dc) \Rightarrow a | bc$ □

5) Beweise: $a | b \wedge a | c \Rightarrow a | (b+c)$

Lsg: $a | b \Rightarrow \exists d: b = ad$ und $a | c \Rightarrow \exists e: c = ae$.
Nun gilt $b + c = ad + ae = a(d+e)$ und daher $a | (b+c)$ □

6) Beweise: $a | b \wedge c | \frac{b}{a} \Rightarrow c | b \wedge a | \frac{b}{c}$

Lsg: $c | \frac{b}{a} \Rightarrow \exists e: \frac{b}{a} = ec \Rightarrow b = eca \Rightarrow \exists_m: b = mc$
$\Rightarrow c | b \Rightarrow \exists m: \frac{b}{a} = cm \Rightarrow \exists m: b = cma \Rightarrow$
$\frac{b}{c} = ma \Rightarrow a | \frac{b}{c}$ □

7) Beweise: Es gilt unendlich viele Primzahlen.

Lsg. Sei P die Menge aller Primzahlen endlich. Sei $m = \prod_{p \in P}(p) + 1$. m ist eine Primzahl, da keine Primzahl in m als Faktor vorkommt, sonst würde dieser Faktor 1 teilen. Dann war aber m zu Beginn nicht in P und P war somit nicht vollständig. Also gibt es unendlich viele PZ. □

8) Seien $a, b, u, v \in \mathbb{Z} - \{0\}$ mit $au + bv = 1$. Zeige $ggT(a, b) = 1$.

Lsg.: Aus der Definition des ggT folgt $ggT(a,b) | a$ und $ggT(a,b) | b$, d.h. es existieren $c, d \in \mathbb{Z}$ mit $a = c \cdot ggT(a,b)$ und $b = d \cdot ggT(a,b)$. Daraus folgt $1 = ua + vb = (uc + vd) \cdot ggT(a,b)$ also $ggT(a,b) | 1$. Da 1 aber der einzige positive teiler von 1 ist, ist somit $ggT(a,b) = 1$ □

9) Irrationalität beweisen: $\sqrt[a]{b}$

Lsg: Annahme $\sqrt[a]{b} \in \mathbb{Q}$, dies bedeutet, es gibt ein $p, q \in \mathbb{Z}$, so dass $\sqrt[a]{b} = \frac{p}{q} \Rightarrow b = (\frac{p}{q})^n$, was $q^n + q^n = p^n$, was aber dem grossen Fermatschen Satz widerspricht!

↳ $a^n + b^n = c^n$ ist für $n > 2$ unlösbar.

Grosse Fermatsche Satz: $a^n + b^n = c^n$
ist für positive ganze Zahlen a, b, c, n mit $n > 2$ unlösbar

Algebra (Kapitel 5)

D5.2: **Algebra**: $\langle S; \Omega \rangle$, S: Trägermenge, Ω: Liste von Operationen auf S.

Monoide & Gruppen

D5.3: **Links [rechts] neutrales Element**: $e \in S$, s.d. $e * a = a$ $[a * e = a]$ $\forall a \in S$. $\Rightarrow e * a = a * e = a$
$\rightarrow$ **neutrales Element**

↳ L5.1: $\langle S; * \rangle$ hat höchstens ein NE.

D5.4: Binäre Operation $*$ auf S ist assioziativ wenn $a * (b * c) = (a * b) * c$

D5.5: **Halbgruppe**: $\langle S; * \rangle$ mit $*$ assi. $\langle \mathbb{Z}; + \rangle$

D5.6: **Monoid**: $\langle S; *, e \rangle$ $*$ ass, e ist NE: $\langle \mathbb{Z}; +, 0 \rangle$

D5.7: **Links [rechts] inverses Element** von a aus $\langle S; *, e \rangle$ ist $b \in S$, s.d. $b * a = e$ $[a * b = e]$
$\rightarrow b * a = a * b = e \Rightarrow$ **inverses Element von a.**

↳ L7.2: $\langle S; *, e \rangle$ hat höchstens ein IE.

D5.8: **Gruppe** $\langle G; * \rangle$:

G1) $*$ ist assioziativ $\langle \mathbb{Z}; +, -, 0 \rangle$

G2) Es gibt ein NE $e \in G$

G3) Jedes $a \in G$ hat IE $\hat{a}$, also $a * \hat{a} = \hat{a} * a = e$

D5.9: **kommutativ / abelsch**: $a * b = b * a$ $\forall a, b \in G$

L5.3: i) $\hat{\hat{a}} = a$ iv) rechts lö.: $b * a = c * a \Rightarrow b = c$

ii) $\widehat{a * b} = \hat{b} * \hat{a}$ v) $a * x = b \Rightarrow x$ ist eindeutig

iii) Links löschen: $a * b = a * c \Rightarrow b = c$

Struktur von Gruppen

D5.10: **Direktes Produkt** aus n Gruppen $\langle G_1; *_1 \rangle, \dots, \langle G_n; *_n \rangle$ ist die Algebra $\langle G_1 \times \ldots G_n; \star \rangle$ mit komponenterweiser Operation $\star$

L5.11: In obiger Algebra sind auch NE und IE komp.w.

D5.11: Eine **Funktion** ψ von $\langle G; *, \hat{}, e \rangle$ nach $\langle H; \star, \sim, e' \rangle$ ist ein **Gruppenhomomorphismus**, falls $\forall a, b$ $\psi(a, b) = \psi(a) \star \psi(b)$. Ist ψ bijektiv, handelt es sich um einen **Isomorphismus**.

D5.13: **Teilmenge** H von $\langle G; *, \hat{}, e \rangle$ ist eine **Teilgruppe** von G, falls $\langle H; *, \hat{}, e \rangle$ geschlossen ist:
i) $a * b \in H$ $\forall a, b \in H$ ii) $e \in H$ iii) $\forall a \in H$: $\hat{a} \in H$

D5.14: **Ordnung** von a: $ord(a) = m$ $(m \geq 1, a^m = e)$, gibt es kein solches $m \Rightarrow ord(a) = \infty$

D5.15: **Ordnung** für Finite Gruppen: $|G|$

D5.16: Teilgruppe $\langle a \rangle := \{a^n | n \in \mathbb{Z}\}$ **generierte Gruppe**

D5.17: $G = \langle g \rangle$ generiert von $g \in G$ ist **zyklisch mit Generator** g.

T5.7: Eine zykl. Gruppe mit Ordnung n ist isomorph zu $\langle \mathbb{Z}_n; \oplus \rangle$, also abelsch.

T5.8: H ist Teilgruppe von $G \Rightarrow |H|$ teilt $|G|$

K5.9: $Ord(a)$ teilt $|G|$ $\forall a \in G$

K5.10: Sei G finit: $a^{|G|} = e$ $\forall a \in G$

K5.11: $|G|$ ist prim $\Rightarrow G$ ist zyklisch und alle Elemente sind Generatoren.

Struktur von Gruppen

D5.18 $\mathbb{Z}_m^* := \{a \in \mathbb{Z}_m \mid ggT(a,m) = 1\}$
z.B. $\mathbb{Z}_{16}^* = \{1, 2, 4, 8, 11, 13, 15\}$

D5.19 **Eulerfunktion** $\varphi(m) = |\mathbb{Z}_m^*|$ (anz. Elemente)

T5.13: $\langle \mathbb{Z}_m^*; \odot, ^{-1}, 1 \rangle$ ist eine Gruppe

K5.14: (Euler, Fermat): für $m \geq 2$ und a mit $ggT(m,a) = 1$ gilt: $a^{\varphi(m)} \equiv_m 1$, bzw. p = prim $\Rightarrow a^{p-1} \equiv_p 1$

T5.15: $\mathbb{Z}_m^*$ ist zyklisch für $m = 2, 4, p^x, 2p^x$ ($p \in$ Prim, $x \geq 1$)

T5.16: Sei G finit und $e \in \mathbb{Z}$ ein geg. Exponent teilerfremd zu $|G|$. Die e-te Wurzel von $y \in G$ (so dass $x^e = y$) kann durch $x = y^d$ berechnet werden, wobei d das mult. Inv. von e mod $|G|$ ist: $ed \equiv_{|G|} 1$.

RSA-Schlüsseltausch

$\Rightarrow |\mathbb{Z}_n^*| = \varphi(n) = (p-1)(q-1)$

Generiere Primzahlen p, q

$n = p \cdot q$
$f = (p-1) \cdot (q-1)$

Wähle e:
$d \equiv_f e^{-1}$

$\xrightarrow{n, e}$

Plaintext $m \in \{1, \dots, n-1\}$

$\xleftarrow{y}$

Ciphertext $y = R_n(m^e)$

$m = R_n(y^d)$

Ringe & Körper

D5.20: Ring $\langle R; +, -, 0, \circ, 1 \rangle$ ist eine Algebra wo:
i) $\langle R; +, -, 0 \rangle$ ist eine kommutative Gruppe
ii) $\langle R; \circ, 1 \rangle$ ist ein Monoid
iii) $a(b+c) = ab + ac$ und $(b+c)a = ba + ca$
$\Rightarrow$ Kommutativ falls es Multiplikation ist.

Triviale Ring: Ring mit 1 Element (und oft $1 = 0$)

D5.21: **Charakteristik** eines Ringes ist die Ordnung von 1 in Additiver Gruppe, falls finit, sonst 0.
$\mathbb{Z}_m \rightarrow m$, $\mathbb{Z} \rightarrow 0$

D5.23: **Nullteiler:** $a \neq 0$ so dass $\exists b \neq 0: ab = 0$

D5.24: **Einheit** $u \in R$ heisst Einheit falls u invertierbar ist ($uv = 1 = vu$, $v = u^{-1}$)
$\Rightarrow$ Menge an Einheiten $= R^*$

L5.19: R^* ist multiplikative Gruppe

D5.25: **Integritätsbereich:** non-triviale Ring ohne Nullteiler: $ab = 0 \Rightarrow a = 0 \vee b = 0$.

D5.27: **Polynom:** $a(x) = a_d x^d + \dots + a_1 x + a_0 = \sum_{i=0}^{d} a_i x^i$
deg(a(x)): Grad, grösstes i
R[x] sind Polynome im Vari. x über Ring R

T5.21: $R[x]$ ist ein Ring.

L5.22: i) Ist D ein Integritätsber. so auch $D[x]$
ii) Einh. von $D[x]$ sind konst. Polynome die Einh. von D sind. $D[x]^* = D^*$

D5.27: **Körper:** nontriviale kommutativer Ring F, in welchem jedes non-zero Element eine Einheit ist
$\Rightarrow F^* = F - \{0\}$

T5.23: $\mathbb{Z}_p$ ist ein Körper g.d.w. p prim ist.

T5.24: Ein Körper ist ein Integritätsbereich

T5.25: Ein finiter Integritätsbereich ist ein Körper

Polynome über Körper

D.5.28: **Monisch / Normiert:** führender Koeff. ist 1

D5.29: **Irreduzibel:** $deg(a(x)) \geq 1$ nur durch konstante Polynome teilbar.

D5.31: Sei $a(x) \in R[x]$: Für ein $\alpha \in R$, so dass $a(\alpha) = 0 \Rightarrow \alpha$ ist **Nullstelle**

L5.29: α ist NS g.d.w. $(x - \alpha) \mid a(x)$

K5.30: Ein Polynom vom Grad 2,3 ist irreduzibel g.d.w. es keine Nullstelle hat.

K5.31: Für IB D hat ein non-zero Polynom mit Grad d höchstens d Nullstellen.

L5.32: Ein Polynom mit Grad d ist eindeutig bestimmt von $d+1$ Werten von $a(x)$

Finite Körper

D5.36: $F[x]_{m(x)}$: $F[x]$ modulo $m(x)$
$\Rightarrow \{a(x) \in F[x] \mid deg(a(x)) < d\}$

L5.34: $|F[x]_{m(x)}| := q^d$ q: Element von F, d: Grad von $m(x)$

L5.35: $F[x]_{m(x)}$ ist ein Ring mit Addition und Multiplikation modulo $m(x)$

T5.37: $F[x]_{m(x)}$ ist ein Körper g.d.w. $m(x)$ irreduzibel

GF(p): Körper mit p Elementen (statt $\mathbb{Z}_p$)

Error-Correcting Codes

D5.37: Ein **(k, n) - Fehlerkorrigierender Code** C über dem Alphabet A mit $|A| = q$ ist eine Teilmenge der Kardinalität q^k von A^k.

D5.38: **Hamming-Distanz:** zwischen 2 Bitstrings, ist die Anzahl Positionen wo sich die Strings unterscheiden.

D5.39: **Minimale Distanz** eines Codes C ist die minim. Hamming Distanz zwischen 2 bel. Strings.

D5.40: **Dekodier-Funktion:** Für (k,n)-Code ist Fkt: $D: A^n \rightarrow A^k$

T5.41: Ein Code C mit minim. Distanz d kann t Fehler korrigieren, falls $d \geq 2t + 1$

Beispiele zu Algebra (Kapitel 5)

1) Wieviele NT hat $\langle \mathbb{Z}_m; \oplus, \odot \rangle$? $\rightarrow m - \varphi(m) - 1$

2) Dividiere $x^5 + 6x^2 + 5$ durch $5x^2 + 2x + 1$ über $\mathbb{Z}_7$.
$\rightarrow$ Mult. Inverses von 5: $3 \cdot 5 \equiv_7 1 \Rightarrow 3$ ist 1. Koeff.

$\Rightarrow (x^5 + 7x^4 + 7x^3 + 6x^2 + 7x + 5) : (5x^2 + 2x + 1) = 3x^3 + 3x^2 + x + 3$

$$
\begin{array}{l}
-(x^5 + 6x^4 + 3x^3) \\
\hline
x^4 + 4x^3 + 6x^2 \\
-(x^4 + 6x^3 + 3x^2) \\
\hline
5x^3 + 3x^2 + 7x \\
-(5x^3 + 2x^2 + x) \\
\hline
x^2 + 6x + 5 \\
-(x^2 + 6x + 3) \\
\hline
\text{Rest: } 2
\end{array}
$$

$\rightarrow$ Aufpassen wegen modulo 7!

3) Sei G eine Gruppe. Zeige / Widerlege: Für alle Untergruppen $H_1, H_2 \leq G$ von G ist auch $H_1 \cup H_2$ eine Untergruppe von G.
Lsg: Betrachte $G = \langle \mathbb{Z}_6; \oplus \rangle$, $H_1 = \{0, 3\}$, $H_2 = \{0, 2, 4\}$
$\{2, 3\} \subseteq H_1 \cup H_2$ aber $2 + 3 = 5 \notin H_1 \cup H_2$. Damit ist die Vereinigung nicht abgeschlossen und somit keine Untergruppe.

4) Zeige / Widerlege: Für alle endlichen zyklischen Gruppen $G_1 = \langle g_1 \rangle$ und $G_2 = \langle g_2 \rangle$ gilt $G_1 \times G_2 = \langle (g_1, g_2) \rangle$
Lsg: Die Behauptung ist falsch. Beweis: Betrachte $G_1 = G_2 = \langle \mathbb{Z}_3^*, + \rangle = \langle 1 \rangle$. Nun bedeutet dies aber $\langle (g_1, g_2) \rangle = \{(g_1^n, g_2^n) \mid n \in \mathbb{Z}\}$. Damit ist bsp. $(0, 1)$ nicht enthalten. Da es aber ein Element von $G_1 \times G_2$ ist, ist die Beh. falsch.

5) Sei F ein endlicher Körper. Zeige dass ein nichtkonstantes Polynom $a(x) \in F[x]$ existiert, das keine NS in F hat.
Lsg.: Sei $|F| = n$. Wir konstruieren also $a(x) = (x + a_n)(x + a_{n-1}) \dots (x + a_1) + 1$ mit a_i in F und $a_i \neq a_j$. Mit L5.32 folgt, dass $a(x)$ keine NS hat.

6) Sei $\langle G; \cdot, ^{-1}, 1 \rangle$ eine Gruppe mit $\forall x \in G$: $x \cdot x = 1$. Zeige: G ist kommutativ.
Lsg: Seien $x, y \in G$. $xy = 1xy1 = (yy)xy(xx) = y(yx)(yx)x = y1x = yx$ $\square$

7) Berechne $\varphi(77)$: $\varphi(77) \overset{PFZ}{=} \varphi(7 \cdot 11) = (7-1)(11-1) = 60$

8) Berechne $\varphi(60)$: $\varphi(60) \overset{PFZ}{=} \varphi(2^2 \cdot 3 \cdot 5) = 2^1 \cdot (2-1) \cdot 3^0 (3-1) \cdot 5^0 (5-1) = 2 \cdot 2 \cdot 4 = 16$

Generell: $\varphi(p) = (p-1)$ falls p prim. Bei PFZ: $\varphi(m) = \varphi(a^n \cdot b^k) = a^{n-1}(a-1) \cdot b^{k-1}(b-1)$ etc.

9) Sei G eine Gruppe mit 35 Elementen und H eine Untergruppe von G mit $G \neq H$. Zeige: H ist kommutativ.

Lsg: Wir wissen, dass für eine Untergruppe H von G mit $|H| = m$, $|G| = n$ gilt $m \mid n$. Da $H \neq G$ bleiben so nur $n = \{1, 5, 7\}$. Für $n = 1$ ist H trivialerweise komm., da das eine Element das Neutralelement sein muss. Da 5 und 7 prim sind, ist H zyklisch und damit isomorph zu $\langle \mathbb{Z}_m; \oplus \rangle$. Die Komm. von H folgt somit aus der Komm. von $\oplus$.

10) Sei R ein kommutativer Ring mit min. 2 Elementen und $r \in R$. Zeige: $r \in R^* \Leftrightarrow \forall s \in R\ \exists t \in R: s = rt$.

Lsg: „$\Rightarrow$": Sei $r \in R^*$. Nach Definition von R^* ist r eine Einheit und somit invertierbar, d.h. $\exists u \in R: ru = 1$. Für ein $s \in R$ beliebig gilt damit $s = 1 \cdot s = rus$, und wir haben mit $t = us$ ein $t \in R$ gefunden mit $s = rt$.

„$\Leftarrow$": Sei $s = 1$. Nach Annahme $\forall s \in R\ \exists t \in R: s = rt$ gibt es also ein $t \in R$ mit $rt = 1$. t ist gerade die Definition eines Inversen zu r und r damit eine Einheit $\rightarrow r \in R^*$. □

11) Seien H_1 und H_2 Untergruppen von G. Zeige: $H_1 \cup H_2$ ist g.d. Untergruppe, wenn $H_1 \subseteq H_2$ oder $H_2 \subseteq H_1$ ist.

Lsg. Wenn $H_1 \subseteq H_2$ oder $H_2 \subseteq H_1$, dann ist $H_1 \cup H_2 = H_2$ oder $H_2 \cup H_1 = H_1$, und somit eine UG von G. Z.z. ist die Umkehrung. Nehmen wir an, dass diese Aussage nicht gilt, d.h. es gibt ein $a \in H_1 \setminus H_2$ und $b \in H_2 \setminus H_1$. Da nach Annahme $H_1 \cup H_2$ eine Gruppe bzgl. der Gruppenoper. $\diamond$ bildet, gibt es wegen Abgeschlossenh. $c = a \diamond b \in H_1 \cup H_2$. Das El. kann aber nicht in H_1 liegen da sonst $b = \hat{a} \diamond c \in H_1$ wäre, analog da sonst $a = c \diamond \hat{b} \in H_2$ wäre. Somit ist $c \notin H_1 \cup H_2$ und $H_1 \cup H_2$ nicht abgeschlossen.

12) $(2,5)$-Code über $A = \{0,1\}$: $\{(0,0,0,0,0), (1,1,1,0,0), (0,0,1,1,1), (1,1,0,1,1)\}$. Minimale Distanz ist 3.

Algorithmen & Berechnungshilfen

kleinstes gemeinsames Vielfaches kgV:

1) Primfaktorzerlegung
2) Man nimmt alle Primfakt., die in min. einer der Zahlen vorkommt, mit der jeweils höchsten Potenz.
3) Multipliziere diese $\rightarrow$ kgV.

Beispiel: $144 = 2^4 \cdot 3^2$, $160 = 2^5 \cdot 5^1$, $175 = 5^2 \cdot 7^1$

$\Rightarrow \text{kgV}(144, 160, 175) = 2^5 \cdot 3^2 \cdot 5^2 \cdot 7^1 = 50'400$

Grösster gemeinsamer Teiler ggT:

1) PFZ
2) alle Faktoren, die in allen Zerlegungen vorkommen, mit kleinster Potenz.
3) Multipliziere diese $\rightarrow$ ggT

Beispiel: $3528 = 2^3 \cdot 3^2 \cdot 7^2$, $3780 = 2^2 \cdot 3^3 \cdot 5^1 \cdot 7^1$

$\Rightarrow \text{ggT}(3528, 3780) = 2^3 \cdot 3^2 \cdot 7^1 = 252$

R_m - Rechnung:

1) $R_m(a^n) = R_m(a^{R_e(n)})$ wobei $n = qe + R_e(n)$ gilt.

Bsp: $R_{11}(4^{2015}) = R_{11}(4^{R_{10}(2015)}) = R_{11}(4^5) = R_{11}(2^{10}) = 1$

Chinesische Restsatz:

- System von Kongr. $x \equiv a_i \bmod m_i$, $i = 1 \dots n$
- $M_i = M / m_i$, M_i und m_i sind teilerfremd
- $M = m_1 \cdot m_2 \cdot \ldots \cdot m_n$
- Finde $r_i \cdot m_i + s_i \cdot M_i = 1$ mit Euklid $i = 1 \dots n$
- setze $e_i = s_i \cdot M_i$ mit
  $e_i \equiv 1 \bmod m_i$
  $e_i \equiv 0 \bmod m_j$, $j \neq i$
- Die Zahl x ist dann eine Lösung der Kongruenz:

$$x = \sum_{i=1}^{n} a_i e_i$$

Allgemeiner Fall für nicht-teilerfremde Moduln:

- Eine Lsg. existiert genau dann, wenn für alle $i \neq j$ gilt: $a_i \equiv a_j \bmod \text{ggT}(m_i, m_j)$. Alle Lsg sind dann kongruent modulo dem kgV der m_i.

Beispiel:

$$\left.\begin{array}{l} x \equiv 1 \bmod 2 \\ x \equiv 1 \bmod 3 \\ x \equiv 1 \bmod 4 \\ x \equiv 1 \bmod 5 \\ x \equiv 1 \bmod 6 \end{array}\right] - x \equiv 1 \bmod \text{kgV}(2,3,4,5,6)$$

$x \equiv 0 \bmod 7$

$\rightarrow$ $x \equiv 1 \bmod 60$
$x \equiv 0 \bmod 7$

$\rightarrow$ Neues System per einfachem CRS lösbar.

R_m - Rechnung:

- 2: Rest = 1 falls letzte Ziffer ungerade, 0 sonst
- 3: Rest der Quersumme (rekursiv angewendet)
- 5: Rest der letzten Ziffer durch 5
- 9: Addiere Dezimalstellen, mod 9
- 10: Letzte Ziffer
- 11: Addiere Dezimalstellen mit alternierendem VZ.

$$R_m(a^b) = R_m[R_m(a)^b]$$

$$R_m(a^b) = R_m(a^{R_{m-1}(b)}) \text{ falls } m \text{ prim}$$

Assoziativ: $a \circ (b \circ c) = (a \circ b) \circ c$
Kommutativ: $a \circ b = b \circ a$
Transitiv: $a \circ b \wedge b \circ c \Rightarrow a \circ c$