

LOGIK

KAPITEL 6

D6.1 Beweissystem $\mathcal{T} = (S, P, \mathcal{I}, \phi)$

D6.2 Beweissystem korrekt: es gibt für keine falsche Aussage einen Beweis

D6.3 Beweissystem vollständig: es gilt für jede wahre Aussage einen Beweis

D6.4 Syntax: definiert Alphabet Λ mit Symbolen und welche Folgen aus Λ^* Formeln sind

D6.5 Semantik: definiert, welche Symbole frei sind

D6.8 Semantik: definiert Funktion σ , die einer Formel F und Interpretation \mathcal{A} einen Wahrheitswert zuweist: $\sigma(F, \mathcal{A}) = \mathcal{A}(F) = 0$ oder 1D6.6 Interpretation besteht aus Menge $\mathcal{Z} \subseteq \Lambda$ von Symbolen und Werten, die ihnen zugeordnet werden.

D6.7 Interpretation passend: weist jeder freien Variable einen Wert zu

D6.9 Interpretation Modell, falls $\mathcal{A}(F) = 1$. AFF

D6.10 Formel erfüllbar: es gibt ein Modell

D6.11 Tautologie: $\mathcal{A}(F) = 1$ für jede passende Int.D6.12 Logische Konsequenz: $F \models G$, wenn jedes Modell für F auch Modell für G istD6.13 F und G sind äquivalent, wenn für jede Interpretation \mathcal{A} gilt $\mathcal{A}(F) = \mathcal{A}(G)$ D6.15 Wenn F, G Formeln sind, dann auch $\neg F, (F \wedge G), (F \vee G)$ D6.16 $\mathcal{A}(\neg F) = 1 \iff \mathcal{A}(F) = 0$ $\mathcal{A}((F \wedge G)) = 1 \iff \mathcal{A}(F) = 1$ und $\mathcal{A}(G) = 1$ $\mathcal{A}((F \vee G)) = 1 \iff \mathcal{A}(F) = 1$ oder $\mathcal{A}(G) = 1$ L6.1 Für Formeln F, G, H gilt:

- 1) $F \wedge F \equiv F \vee F \equiv F$ (idempotence)
- 2) $F \wedge G \equiv G \wedge F, F \vee G \equiv G \vee F$ (comm.)
- 3) $(F \wedge G) \wedge H \equiv F \wedge (G \wedge H)$ (associativity)
- 4) $F \wedge (F \vee G) \equiv F \vee (F \wedge G) \equiv F$ (absorption)
- 5) $F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$ (1. dist.)
- 6) $F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$ (2. dist.)
- 7) $\neg \neg F \equiv F$ (double negation) (de Morgan)
- 8) $\neg(F \wedge G) \equiv \neg F \vee \neg G, \neg(F \vee G) \equiv \neg F \wedge \neg G$
- 9) $F \vee T \equiv T, F \wedge T \equiv F$ (tautology rules)
- 10) $F \vee \perp \equiv F, F \wedge \perp \equiv \perp$ (unsatisfiability)
- 11) $F \vee \neg F \equiv T, F \wedge \neg F \equiv \perp$

L6.2 F ist Tautologie $\iff \neg F$ ist unerfüllbar

L6.3 Folgende Aussagen sind äquivalent:

- 1) $\{F_1, F_2, \dots, F_k\} \models G$
- 2) $(F_1, F_2, \dots, F_k) \rightarrow G$ ist Tautologie
- 3) $\{F_1, F_2, \dots, F_k, G\}$ ist unerfüllbar

KALKÜLE

D6.17 Schlussregel: $\{F_1, \dots, F_k\} \vdash_R G$ $\hookrightarrow G$ wird aus Formelmenge mit Regel R geschl.

D6.19 Kalkül: endliche Menge von Schlussregeln

$$K = \{R_1, \dots, R_m\}$$

D6.21 Schlussregel R ist korrekt, falls

$$M \vdash_R F \Rightarrow M \models F$$

D6.22 K korrekt, falls $M \vdash_K F \Rightarrow M \models F$ Kalkül K vollständig, falls $M \models F \Rightarrow M \vdash_K F$ L6.4 Falls $\{F_1, \dots, F_k\} \vdash_K G$ für ein korrektes Kalkül gilt, $\models((F_1, \dots, F_k) \rightarrow G)$

AUSSAGENLOGIK

DEF 6.23 Syntax: • atomare Formeln sind Formeln, und Def. 6.15

DEF 6.24 Semantik: Interpretation passend, alle atomaren Formeln enthält (Def. 6.16)

DEF 6.25 Literal ist atom. Formel / Neg.

DEF 6.26 CNF (Konjunktive Normalform):

$$F = (L_{11} \vee \dots \vee L_{1m_1}) \wedge \dots \wedge (L_{n1} \vee \dots \vee L_{nm_n})$$

 \rightarrow Zeilen der Wertetabelle ausschliessen, Negation der Literale mit \vee getrennt

DEF 6.27 DNF (Disjunktive Normalform):

$$F = (L_{11} \wedge \dots \wedge L_{1m_1}) \vee \dots \vee (L_{n1} \wedge \dots \wedge L_{nm_n})$$

 \rightarrow Zeilen d. Wertetabelle mit \vee trennen

DEF 6.28 Klausel: Menge von Literalen

DEF 6.29 Die Klauselmenge einer Formel F in CNF ist die Menge

$$K(F) \stackrel{\text{def.}}{=} \{\{L_{11}, \dots, L_{1m_1}\}, \dots, \{L_{n1}, \dots, L_{nm_n}\}\}$$

 \hookrightarrow Klausel ist Disjunktion von LiteralenDEF 6.30 Eine Klausel K folgt aus K_1, K_2 ,wenn es, ein Literal L gibt, sodass $L \in K_1$ und $\neg L \in K_2$: $K = (K_1 \setminus \{L\}) \cup (K_2 \setminus \{\neg L\})$

LEM 6.6 Das Resolutionskalkül ist korrekt.

$$K \vdash_{\text{res}} K \Rightarrow K \models K$$

THE 6.7 Eine Menge M von Formeln ist unerfüllbar $\iff K(M) \vdash_{\text{res}} \emptyset$ $\hookrightarrow M \models F$ beweisen: $K(M \cup \{\neg F\}) \vdash_{\text{res}} \emptyset$

$$\{F, G\} \vdash_{\text{res}} F \rightarrow G, \{F \rightarrow G\} \vdash_{\text{res}} G \rightarrow H, \{G \rightarrow H\} \vdash_{\text{res}} F \rightarrow H$$

$$\{(C \rightarrow B), A\} \vdash_{\text{res}} (C \rightarrow B) \rightarrow A \quad (1) \quad (F = (C \rightarrow B), G = A)$$

$$\{(B \rightarrow A), (C \rightarrow B)\} \vdash_{\text{res}} (B \rightarrow A) \rightarrow (C \rightarrow B) \quad (2) \quad (F = \dots, G = \dots)$$

$$\{(1), (2)\} \vdash_{\text{res}} C \rightarrow A \quad (F = (C \rightarrow B) \rightarrow A, G = \dots)$$

 $\hookrightarrow (C \rightarrow A)$ aus $\{A, B \rightarrow A, C \rightarrow B\}$ herleiten

PRÄDIKATENLOGIK

DEF 6.31 Syntax der Prädikatenlogik:

- x_i ist eine Variable
- $k=0$ Konstante
- $f_i^{(k)}$ ist eine k -stellige Funktion
- $P_i^{(k)}$ ist ein k -stelliges Prädikat
- Terme:
 - Variablen sind Terme
 - Funktion mit k Termen auch
- Formeln:
 - $P_i^{(k)}(t_1, \dots, t_k)$ ist atom. Formel
 - $\neg F, (F \wedge G), (F \vee G)$ sind Form.
 - $\forall x F$ und $\exists x F$ auch

DEF 6.32 $\forall x F / \exists x F$: x gebundene Variable

DEF 6.33 $F[x/t]$: freie Var. $x \rightarrow t$ ersetzen

DEF 6.34 Semantik; Interpretation ist

definiert als $A = (U, \emptyset, \Psi, \mathcal{E})$

- U ist Universum (nicht-leere Menge)
- \emptyset weist Funktionsymbolen eine Funktion zu
- Ψ weist Prädikatssymbolen ein Prädikat zu
- \mathcal{E} weist freien Variablen Wert aus U zu

DEF 6.35 Interpretation passend, wenn

Funktionen, Prädikate, freie Variablen def.

LEM 6.8 1) $\neg(\forall x F) \equiv \exists x \neg F$

2) $\neg(\exists x F) \equiv \forall x \neg F$

3) $(\forall x F) \wedge (\forall x G) \equiv \forall x (F \wedge G)$

4) $(\exists x F) \vee (\exists x G) \equiv \exists x (F \vee G)$

5) $\forall x \forall y F \equiv \forall y \forall x F$

6) $\exists x \exists y F \equiv \exists y \exists x F$

7) $(\forall x F) \wedge H \equiv \forall x (F \wedge H)$

8) $(\forall x F) \vee H \equiv \forall x (F \vee H)$

9) $(\exists x F) \wedge H \equiv \exists x (F \wedge H)$

10) $(\exists x F) \vee H \equiv \exists x (F \vee H)$

LEM 6.10 Wenn y nicht in G erscheint:

- $\forall x G \equiv \forall y (G[x/y])$
- $\exists x G \equiv \exists y (G[x/y])$

DEF 6.37 **Bereinigte Form**: keine Variable erscheint frei und gebunden

LEM 6.11 $\forall x F \models F[x/t]$

DEF 6.38 **Pränexform**: eine Formel mit allen Quantoren am Anfang

$\forall x \neg(F \vee G) \models \neg((\forall x F) \wedge (\forall x G))$ (A suitable)

$A(\forall x \neg(F \vee G)) = 1 \xrightarrow{\text{Sem. } \forall} A_{[x \rightarrow u]}(\neg(F \vee G)) = 1$ f.a. uell

$\xrightarrow{\text{Sem. } \forall} A_{[x \rightarrow u]}(F) = 0$ for all $u \in U$

$\xrightarrow{\text{Sem. } \forall} A_{[x \rightarrow u]}(G) = 0$ f.a. uell

Case 1: $A_{[x \rightarrow u]}(F) = 1$ for all uell. $\xrightarrow{\text{Ass.}} A_{[x \rightarrow u]}(G) = 0$ f.a. uell

$\xrightarrow{\text{Sem. } \forall} A(\forall x G) = 0 \xrightarrow{\text{Sem. } \wedge} A((\forall x F) \wedge (\forall x G)) = 0$

$\xrightarrow{\text{Sem. } \neg} A(\neg((\forall x F) \wedge (\forall x G))) = 1$ ■

Case 2: Otherwise, $A_{[x \rightarrow u]}(F) = 0$ for some $u \in U$

$\xrightarrow{\text{Sem. } \forall} A(\forall x F) = 0 \xrightarrow{\text{Sem. } \wedge} A((\forall x F) \wedge (\forall x G)) = 0$

$\xrightarrow{\text{Sem. } \neg} A(\neg((\forall x F) \wedge (\forall x G))) = 1$ ■

LOGIK

LEM 2.1 Siehe Lemma 6.2 1) - 8)

LEM 2.3 $F \rightarrow G$ ist Tautologie

$\iff F \models G$

LEM 2.4 Falls $F \models G$, dann gilt

F ist Tautologie $\Rightarrow G$ ist T

KAPITEL 2

PROOF PATTERNS

DEF 2.13 Implikation zusammensetzen

$S \Rightarrow T$ und $T \Rightarrow U$ beweisen. $S \Rightarrow U$

DEF 2.14 Direkter Beweis einer Impl.

S als wahr annehmen und T beweisen

DEF 2.15 Indirekter Beweis einer Impl.

T als falsch annehmen, S widerlegen

LEM 2.6 $\neg B \rightarrow \neg A \models A \rightarrow B$

DEF 2.16 Modus Ponens:

1) Eine Aussage R finden

2) R beweisen

3) Zeigen, dass $R \Rightarrow S$

zu beweisen

LEM 2.7 $A \wedge (A \rightarrow B) \models B$

Fallunterscheidung: versch. Fälle impl. S

L2.8 $(A_1 \vee \dots \vee A_k) \wedge (A_1 \rightarrow B) \wedge \dots \wedge (A_k \rightarrow B) \models B$

Bmk: $(\neg A \rightarrow B) \wedge (\neg A \rightarrow C) \wedge (\neg B \vee \neg C) \models A$

DEF 2.18 Widerspruchsbeweis

1) T formulieren

2) Zeigen, dass T falsch ist

3) Annehmen, dass S falsch ist, T bew.

LEM 2.9 $(\neg A \rightarrow B) \wedge \neg B \models A$

Bmk: $(A \vee B) \wedge \neg B \models A$

D2.19 Existenzbeweis: Wahre Int. angeben

THE 2.10 Tauberschlagprinzip (pigeonhole)

n Objekte in k Mengen aufteilen

\rightarrow mind eine Menge hat $\lceil \frac{n}{k} \rceil$ Elern.

DEF 2.20 Gegenbeispiel

Eine Interpretation falsche angeben

THE 2.11 Induktionsbeweis

$\underbrace{P(0)}_{\text{Ind. Anfang}} \wedge \underbrace{\forall n (P(n) \rightarrow P(n+1))}_{\text{Ind. Schritt}} \Rightarrow \forall n P(n)$

Ind. Anfang

Ind. Schritt

MENGEN

KAPITEL 3

DEF 3.1 Anz Elemente: Kardinalität, $|A|$ DEF 3.2 $A = B \Leftrightarrow \forall x (x \in A \Leftrightarrow x \in B)$ LEM 3.1 $\{a\} = \{b\} \Rightarrow a = b$ DEF 3.3 $A \subseteq B \Leftrightarrow \forall x (x \in A \rightarrow x \in B)$ $A = B \Leftrightarrow (A \subseteq B) \wedge (B \subseteq A)$ LEM 3.3 \emptyset is subset of any set $\forall A (\emptyset \subseteq A)$ DEF 3.5 Power Set von A $P(A) \stackrel{\text{def}}{=} \{S \mid S \subseteq A\}$
 $|P(A)| = 2^{|A|}$ DEF 3.6 $A \cup B \stackrel{\text{def}}{=} \{x \mid x \in A \vee x \in B\}$ (union) $A \cap B \stackrel{\text{def}}{=} \{x \mid x \in A \wedge x \in B\}$ (intersection)DEF 3.7 Komplement von A : $\bar{A} \stackrel{\text{def}}{=} \{x \in U \mid x \notin A\}$ DEF 3.8 Differenz von A, B : $B \setminus A \stackrel{\text{def}}{=} \{x \in B \mid x \notin A\}$ THE 3.4 $A \cap A = A$ Idempotence $A \cup A = A$ $A \cap B = B \cap A$

Commutativity

 $A \cup B = B \cup A$ $A \cap (B \cap C) = (A \cap B) \cap C$ Assoc. $A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (A \cup B) = A$ Absorption $A \cup (A \cap B) = A$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ Dist. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \subseteq B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B$

↳ Consistency

RELATIONEN

DEF 3.11 Identitätsrel. $\text{id}_A = \{(a, a) \mid a \in A\}$ DEF 3.12 Inverses einer Relation $\varphi: A \rightarrow B$ $\hat{\varphi}: B \rightarrow A \quad \hat{\varphi} \stackrel{\text{def}}{=} \{(b, a) \mid (a, b) \in \varphi\}$

DEF 3.13 Komposition von Relationen:

 $\varphi \circ \sigma \stackrel{\text{def}}{=} \{(a, c) \mid \exists b ((a, b) \in \varphi \wedge (b, c) \in \sigma)\}$

LEM 3.5 Komposition ist Assoziativ / idempotent

DEF 3.14 φ ist reflexiv: $a \varphi a$ für alle $a \in A$ D3.15 irreflexiv: $\forall a \forall a \varphi a \quad \varphi = \hat{\varphi}$ DEF 3.16 φ ist symmetrisch: $a \varphi b \Leftrightarrow b \varphi a$ DEF 3.17 φ ist antisymmetrisch: $a \varphi b \wedge b \varphi a \Rightarrow a = b \quad \text{pnp} \leq \text{id}$ DEF 3.18 φ ist transitiv: $a \varphi b \wedge b \varphi c \Rightarrow a \varphi c$ LEM 3.7 φ ist transitiv $\Leftrightarrow \varphi^2 \subseteq \varphi$ DEF 3.19 Transitive Hülle: $\varphi^* = \bigcup_{n \in \mathbb{N} \cup \{0\}} \varphi^n$
↳ "Erreichbarkeit"

ÄQUIVALENZRELATIONEN

D3.20 Äquivalenzrelation ist reflexiv, symmetrisch, transitiv

D3.21 Äquivalenzklasse $[a]_0 \stackrel{\text{def}}{=} \{b \in A \mid b \sim a\}$

L3.8 Intersection von Äquiv. rel. ist Äquiv. rel.

 $\hookrightarrow \equiv_3 \cap \equiv_5 = \equiv_{15}$

T3.9 Menge aller Äquivalenzklassen ist Partition

ORDNUNGSRELATIONEN

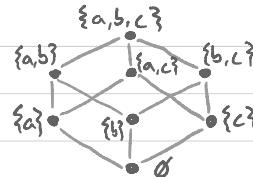
D3.24 Ordnungsrelation ist reflexiv, antisymmetrisch, transitiv. Poset $(A; \leq)$

Hasse Diagramm: Gerichteter Graph mit

Kante (a, b) falls "b überdeckt (\geq) a".Bsp. $(P(\{a, b, c\}), \leq)$:

D3.26 Total geordnet

Jede zwei Elemente sind vergleichbar

D3.30 • min/max Elemente: \exists kleineren/größeren• kleinstes / größtes Element: $a \leq b$ für alle $b \in A$ • untere / obere Schranke: $a \leq b$ für alle $b \in S$ • größte untere Schranke: $a \geq$ alle anderen SchrankenD3.32 • meet: größte untere Schranke von a, b • join: kleinste obere Schranke von a, b

D3.33 Lattice: jede 2 El. in Poset haben meet, join

FUNKTIONEN

D3.34 • $\forall a \in A \exists b \in B \quad a \text{fb}$ (Totally Defined)• $\forall a \in A \forall b, b' \in B \quad (a \text{fb} \wedge a \text{fb}' \rightarrow b = b')$

Partielle Funktion: nur 2. gilt (Well-Defined)

D3.35 Urbild $f^{-1}(T) \stackrel{\text{def}}{=} \{a \in A \mid f(a) \in T\}$ D3.40 • injektiv: $a \neq b \Rightarrow f(a) \neq f(b)$ • surjektiv: für jedes $b \in B$ existiert $a \in A, f(a) = b$

• bijektiv: injektiv und surjektiv

L3.12 Funktionen Assoz. $(h \circ g)af = h \circ (g \circ f)$

ABZÄHLBARKEIT

D3.43 1) $A \sim B$ gleich mächtig. (Bij. $A \rightarrow B$)2) $A \leq B$ B dominiert A (Inj. $A \rightarrow B$)3) A abzählbar: $A \leq \mathbb{N}$ (sonst überabzählbar)L3.13 1) \leq transitiv: $A \leq B \wedge B \leq C \Rightarrow A \leq C$ 2) $A \leq B \Rightarrow A \leq B$ T3.14 $A \leq B \wedge B \leq A \Rightarrow A \sim B$ T3.15 A ist abzählbar \Leftrightarrow endlich oder $A \sim \mathbb{N}$ T3.16 $\{0, 1\}^*$ (endliche bin. Sequenzen) ist abzählbarT3.17 $\mathbb{N} \times \mathbb{N} (= \mathbb{N}^2)$ ist abzählbarC3.18 $A \leq \mathbb{N} \wedge B \leq \mathbb{N} \Rightarrow A \times B \leq \mathbb{N}$

C3.19 Rationale Zahlen \mathbb{Q} abzählbarT3.20 Seien A, A_i für $i \in \mathbb{N}$ abzählbar(i) A^n für jedes $n \in \mathbb{N}$ ist abzählbar(ii) Union $\bigcup_{i \in \mathbb{N}} A_i$ ist abzählbar(iii) A^* ist abzählbarT3.21 $\{0, 1\}^{\infty}$ ist überabzählbar

↳ Beweis: Cantors Diagonalisierung

Überabzählbarkeit beweisen:

1) Diagonalisierung

2) B überabzählbar, Injektion $B \rightarrow A$ 3) $A \subseteq B$, B überabzählbar $B \setminus A$ überabzählbar $\Rightarrow A$ überabzählbar

ZAHLENTHEORIE KAPITEL 4

T4.1 Für alle $a \in \mathbb{Z}$ und $d \neq 0$ gibt es eindeutige q, r mit $a = dq + r$ und $0 \leq r < |d|$ D4.2 $\text{dla} \wedge \text{dlb} \wedge \forall c((cla \wedge clb) \rightarrow c|d)$

↳ d ist gcd von a und b

L4.2 $\text{gcd}(m, n \cdot qm) = \text{gcd}(m, R_m(n)) = \text{gcd}(m, n)$ D4.4 Ideal: $(a, b) := \{ua + vb \mid u, v \in \mathbb{Z}\}$ L4.3 Für $a, b \in \mathbb{Z}$ gibt es $d \in \mathbb{Z}$ mit $(a, b) = (d)$

↳ L4.4 d ist der gcd von a und b

L4.5 $\text{gcd}(a, b) = ua + vb$ mit $u, v \in \mathbb{Z}$ D4.5 $a \mid l \wedge b \mid l \wedge \forall m((alm \wedge blm) \rightarrow l|m)$

↳ l ist least common multiple von a, b

T4.6 Jede pos. Ganzzahl kann eindeutig als

Produkt von Primzahlen dargestellt werden

 $\text{gcd}(a, b) = \prod_i p_i^{\min(e_i, f_i)}$ Produkt der Primfaktoren mit der kleineren/größeren $\text{lcm}(a, b) = \prod_i p_i^{\max(e_i, f_i)}$ Potenz (e: Potenzen von a, f: Potenzen von b) $\text{gcd}(a, b) \cdot \text{lcm}(a, b) = ab$ D4.8 $a \equiv_m b \stackrel{\text{def.}}{\iff} m \mid (a-b)$ (Modulare Kongruenz)L4.13 \equiv_m ist Äquivalenzrelation auf \mathbb{Z} ($m \geq 1$)L4.14 $a \equiv_m b$ und $c \equiv_m d \Rightarrow a+c \equiv_m b+d$ $a \cdot c \equiv_m b \cdot d$ L4.16 (i) $a \equiv_m R_m(a)$ $\left\{ \begin{array}{l} \\ m \geq 1 \end{array} \right.$ (ii) $a \equiv_m b \iff R_m(a) = R_m(b)$ L4.17 $R_m(f(a_1, \dots, a_k)) = R_m(f(R_m(a_1), \dots, R_m(a_k)))$ L4.18 $a \equiv_m 1$ hat Lösung $\iff \text{gcd}(a, m) = 1$

↳ x ist multiplikatives Inverses von a

ERW. EUKLID-ALGORITHMUS

i	a	b	q	r	x	y
1	31	26	1	5	-5	6
2	26	5	5	1	1	-5
3	5	1	5	0	0	1

multiplikat. ← Inverse
gcd(31, 26) ← Init

 $x_i = y_{i+1}$ $y_i = x_{i+1} - q_i \cdot y_{i+1}$

$$\text{gcd}(a, b) = x \cdot a + y \cdot b$$

$$R_m(a+b) = R_m(R_m(a) + R_m(b))$$

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

$$R_m(a^n) = R_m(R_m(a)^n)$$

$$R_m(a^{n+m}) = R_m(R_m(a)^n \cdot R_m(a)^m)$$

$$x \equiv_{a \cdot b} c \Rightarrow x \equiv_a c \wedge x \equiv_b c$$

$$x \equiv_a c \wedge x \equiv_b c \Rightarrow x \equiv_{\text{lcm}(a, b)} c$$

$$R_{63}(2^{2017}) = R_{63}(R_{63}(2^6)^{336} \cdot 2) = R_{63}(1^{336} \cdot 2) = \underline{\underline{2}}$$

$$R_{403}(2016^{42}) = R_{403}(R_{403}(2016)^{42}) = R_{403}(1^{42}) = \underline{\underline{1}}$$

$$R_g(6284) = R_g(6+2+8+4) = R_g(\underline{\underline{20}}) = 2 \quad (\text{Quersumme})$$

$$R_{11}(8725) = R_{11}(5-2+7-8) = R_{11}(2) = 2 \quad (+/- \text{ abwechseln})$$

CHINESISCHER RESTSATZ

$$\begin{array}{l} x \equiv_{m_1} a_1 \\ x \equiv_{m_2} a_2 \\ \vdots \\ x \equiv_{m_r} a_r \end{array} \left\{ \begin{array}{l} \text{hat eindeutige Lösung } x \\ \text{mit } 0 \leq x < M \quad (m_1, \dots, m_r \text{ paarweise teilerfremd}) \end{array} \right.$$
Beweis: Sei $M_i = M/m_i$ und $M_i \cdot N_i \equiv_{m_i} 1$ Daher $\sum_{i=1}^r a_i M_i N_i \equiv_{m_k} a_k$ für alle k.Daher $x = R_M \left(\sum_{i=1}^r a_i M_i N_i \right)$ Beispiel: $x \equiv_2 1 \quad M_1 = 65 \quad N_1 = 1$ $x \equiv_5 2 \quad M_2 = 26 \quad N_2 = 1$ $x \equiv_{13} 3 \quad M_3 = 10 \quad N_3 = 4$

$$\tilde{x} = 1 \cdot 65 \cdot 1 + 2 \cdot 26 \cdot 1 + 3 \cdot 10 \cdot 4 = 237$$

$$x = R_M(\tilde{x}) = R_{130}(237) = \underline{\underline{107}} \quad (\text{eindeutig in } \mathbb{Z}_{130})$$

DIFFIE-HELLMAN ($p = \text{Gruppengröße}$)Alice $y_A := R_p(g^{x_A}) \quad y_B := R_p(g^{x_B}) \quad \text{Bob}$

$$\xrightarrow{y_A} \xleftarrow{y_B}$$

$$k_{AB} := R_p(y_B^{x_A}) \quad k_{BA} := R_p(y_A^{x_B})$$

$$k_{AB} \stackrel{p}{=} y_B^{x_A} \stackrel{p}{=} (g^{x_B})^{x_A} \stackrel{p}{=} (g^{x_A})^{x_B} \stackrel{p}{=} k_{BA}$$

Private Keys x_A, x_B sind im Intervall $\{0, \dots, p-2\}$ p PrimzahlIrrationalität beweisen: • Ann. $\exists p, q: x = \frac{p}{q}$ Teilerfremdz.B. Sei $\sqrt{2} = \frac{p}{q}, \frac{p, q \in \mathbb{Z}}{\text{Teilerfremd}}$

$$\Rightarrow 2 \cdot q^2 = p^2 \quad \left| \begin{array}{l} p^2 \text{ gerade} \\ p \text{ gerade} \end{array} \right.$$

$$\left| \begin{array}{l} r = \frac{p}{2} \in \mathbb{Z} \\ r^2 = \frac{p^2}{4} \end{array} \right.$$

$$2 \cdot q^2 = 4 \cdot r^2 \quad \left| \begin{array}{l} q^2 \text{ gerade} \\ r^2 \text{ gerade} \end{array} \right.$$

$$q^2 = 2r^2 \quad \left| \begin{array}{l} 2 \mid q^2 \\ 2 \mid r^2 \end{array} \right.$$

$$\Rightarrow 2 \mid p \wedge 2 \mid q \quad \left| \begin{array}{l} p, q \text{ ungerade} \\ 2 \mid p \wedge 2 \mid q \end{array} \right.$$

$$\Rightarrow p = q = 0 \quad \left| \begin{array}{l} p, q \in \mathbb{Z} \\ p = q \end{array} \right.$$

$$R_{11}(2^{340}) = R_{11}(2^{R_{11}(3^{40})}) \quad \text{weil } 2, 11 \text{ teilerfremd}$$

GRUPPEN

KAPITEL 5

D5.5 Monoid: Algebra $\langle M; *, e \rangle$ • $*$ ist assoziativ (Def. 5.4) Def. 5.3• e ist neutrales Element ($e * a = a * e = a$) Def. 5.3L5.1 Links-NE = Rechts-NE (Nur ein NE in Algebra)D5.7 Gruppenaxiome $\langle G; *, \hat{ }, e \rangle$ G1) $*$ ist assoziativG2) e ist NE: $a * e = e * a = a \quad \forall a \in G$ G3) Jedes $a \in G$ hat Inverses \hat{a} ($a * \hat{a} = e$)D5.8 Falls $*$ kommutativ: Abelsche GruppeL5.3 (i) $(\hat{a}) = a$ (ii) $\hat{a * b} = \hat{b} * \hat{a}$ (iii) Left cancellation: $a * b = a * c \Rightarrow b = c$ (iv) Right cancellation: $b * a = c * a \Rightarrow b = c$ (v) $a * x = b$ hat eindeutige Lösung

D5.10 Gruppen Homomorphismus

 $\langle G; *, \hat{ }, e \rangle \quad \psi: G \rightarrow H$ $\langle H; \circ, \hat{ }, e' \rangle \quad \psi(a * b) = \psi(a) \circ \psi(b)$ Falls ψ bijektiv: Isomorphismus, $G \cong H$ L5.5 $\psi: G \rightarrow H$ erfüllt (i) $\psi(e) = e'$ Gruppen Homomorph. (ii) $\psi(\hat{a}) = \hat{\psi(a)}$ für alle $a \in G$ D5.11 $H \leq G$ ist Untergruppe $\langle H; *, \hat{ }, e \rangle$:1) $a * b \in H$ für alle $a, b \in H$ (abgeschlossen)2) $e \in H$ 3) $\hat{a} \in H$ für alle $a \in H$ Triviale Untergruppen: $\{e\}$, G selberD5.12 Ordnung: $\text{ord}(a) = m$ mit $a^m = e$ L5.6 In endlicher Gruppe: $\text{ord}(a)$ endlich $\forall a$ D5.13 $|G|$ ist Ordnung der Gruppe G Zyklische Gruppe: $\langle a \rangle = \{a^n \mid a \in \mathbb{Z}\}$ $a^m = a^{\text{ord}(a)(m)}$ $G = \langle g \rangle$ GeneratorT5.7 Zyklische Gruppe der Ordnung n ist isomorph zu $\langle \mathbb{Z}_n; + \rangle$ (\rightarrow abelsch) \hookrightarrow Generatoren von $\langle \mathbb{Z}_n; + \rangle$: $\text{gcd}(n, g) = 1$ T5.8 Lagrange: Die Ordnung jeder Untergruppe H teilt die Gruppenordnung von G .
 $\Rightarrow |H| \text{ teilt } |G|$ L5.9 $\text{ord}(a)$ teilt $|G|$ für jedes $a \in G$ L5.10 $a^{|G|} = e$ für jedes $a \in G$ L5.11 Jede Gruppe mit $|G|$ prim ist zyklischD5.16 $\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m \mid \text{gcd}(a, m) = 1\}$ L5.12 $\varphi(m) = |\mathbb{Z}_m^*| = \prod_{i=1}^r (p_i - 1) \cdot p_i^{e_i-1} \rightarrow$ Potenz
($\varphi(m) = m \cdot \prod_{i=1}^r \left(\frac{p_i - 1}{p_i}\right)$) i -ter PrimfaktorL5.14 Fermat/Euler Für $m \geq 2$ und alle a mit $\text{gcd}(m, a) = 1$ gilt $a^{\varphi(m)} \equiv_m 1$.Außerdem, wenn $p \nmid a$: $a^{p-1} \equiv_p 1$ T5.15 \mathbb{Z}_m^* ist zyklisch $\Leftrightarrow m=2, m=4$,
 p ist Primz. $\geq 2 \rightarrow m=p^e, m=2p^e$

RSA

T5.16 Sei G endliche Gruppe, $\text{gcd}(e, |G|) = 1$ Die Funktion $x \mapsto x^e$ ist Bijektion, $y = x^e$.Also ist $x = y^e$, e ist mult. Inverses von d : $ed \equiv_G 1$ (Beweis: $(x^e)^d = x^{ed} = x^{k \cdot |G| + 1} = x^{k \cdot |G|} \cdot x = x$) \uparrow Ist $|G|$ bekannt, wird d einfach berechnetAlice (zufällige Primz. p, q , zufälliges e) Bob $n = p \cdot q$ Gruppengrösse public key $f = (p-1)(q-1)$ $d \equiv_f e^{-1}$ $m = R_n(y^d)$ private key $y = R_n(m^e)$ Ciphertext \hookrightarrow Berechnung: $ed \equiv_f 1$

Ringe

D5.18 Ring $\langle R; +, -, 0, \cdot, 1 \rangle$ (i) $\langle R; +, -, 0 \rangle$ ist kommutative Gruppe(ii) $\langle R; \cdot, 1 \rangle$ ist Monoid(iii) $a(b+c) = (ab) + (ac)$ (L/R Distributivgesetz) \hookrightarrow Wenn $ab = ba$: Ring ist kommutativL5.17 Für $\langle R; +, -, 0, \cdot, 1 \rangle$ und alle $a, b \in R$ gilt:(i) $0a = a0 = 0$ (iii) $(-a)(-b) = ab$ (ii) $(-a)b = - (ab)$ (iv) $1 \neq 0$ falls R nicht trivial

L5.18 In einem kommutativen Ring gilt

(i) $ab \wedge b c \rightarrow a c$ (i ist transitiv)(ii) Wenn ab , dann $a \mid (b \cdot c)$ für alle c (iii) $ab \wedge a c \rightarrow a \mid (b+c)$ D5.22 Einheit: invertierbares Element (R^* enthält Einheiten von R)L5.19 In einem Ring R ist R^* eine mult. GruppeD5.24 Integritätsbereich: $\forall a \forall b (ab = 0 \rightarrow a = 0 \vee b = 0)$ \hookrightarrow hat keine Nullteiler, z.B. \mathbb{Z}

KÖRPER (jedes El. mult. Inverses)

D5.26 Körper ist kommutativer Ring, in dem jedes Element eine Einheit ist (+ kommutativ, nicht-trivial)T5.23 \mathbb{Z}_p ist Körper $\Leftrightarrow p$ ist PrimzahlGF(n) \rightarrow irgendein Körper mit n Elementen \hookrightarrow geht nur, falls $n = p^d$, p prim, $d \geq 1$ T5.38 Körper F mit q Elementen existiert $\hookrightarrow q$ ist Potenz einer Primzahl

Körper mit gleicher Grösse sind isomorph

T5.24 Körper ist I.B. (hat keine Nullteiler)

 \hookrightarrow ein endlicher I.B. ist ein Körper

POLYNOME

T5.21 R Ring $\Rightarrow R[x]$ Ring

L5.22 (i) D Integritätsbereich $\Rightarrow D[x]$ I.B.

(ii) Einheiten von $D[x]$ sind die Konstanten Polynome, die Einheiten von D sind $(D[x]^* = D^*)$
 F Körper $\Rightarrow F[x]$ Ring oder I.B.

D5.27 Monisch: erster Koeffizient = 1

D5.28 Irreduzibel: nur durch Konstante

Polynome und Vielfache von sich teilbar

D5.29 $\gcd(a(x), b(x))$ ist $g(x)$ ^{monisch} ^{größerer Rang}

T5.25 $a(x) = b(x) \cdot q(x) + r(x)$
^{eindeutig} \uparrow \uparrow $\deg(r(x)) < \deg(b(x))$

Faktorisierung von Polynomen

$\deg = 1$: irreduzibel

$\deg = 2$ oder 3 : irreduzibel v Nullstelle

$\deg = 4$: irreduzibel v Nullstelle v irreduz. Faktor $\deg = 2$

allg.: irreduzibel v irreduz. Faktor mit $\deg \leq \frac{d}{2}$

L5.28 $a \in F$ ist Nullstelle von $a(x) \Leftrightarrow (x-a) \mid a(x)$

Nullstelle \Leftrightarrow Faktor mit Grad 1

L5.29 $a(x)$ mit $\deg = 2$ oder 3 ist irreduzibel

$\Leftrightarrow a(x)$ hat keine Nullstelle

T5.30 $a(x) \in F[x]$ hat max. $\deg(a(x))$ Nullstellen

L5.31 Lagrange Interpolation: $a(x) \in F[x]$ ist mit $\deg(a(x))+1$ Auswertungen eindeutig best.

$$a(x) = \sum_{i=1}^m \beta_i u_i(x)$$

$$u_i = \frac{(x-\alpha_1) \cdots (x-\alpha_{i-1})(x-\alpha_{i+1}) \cdots (x-\alpha_{d+1})}{(\alpha_i-\alpha_1) \cdots (\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1}) \cdots (\alpha_i-\alpha_{d+1})}$$

$$|F^*| = |F| - 1$$

ENDLICHE KÖRPER

D5.35 $F[x]_{m(x)} \stackrel{\text{def.}}{=} \{a(x) \in F[x] \mid \deg(a(x)) < d\}$

L5.33 $|F[x]_{m(x)}| = q^d$ ($q = |F|$, $d = \deg(m(x))$)

L5.35 $F[x]_{m(x)}^* = \{a(x) \in F[x]_{m(x)} \mid \gcd(a, m) = 1\}$

T5.36 $F[x]_{m(x)}$ ist Körper $\Leftrightarrow m(x)$ irreduzibel
 \hookrightarrow Sonst Ring (L5.34)

ERROR-CORRECTING CODES

D5.36 (n, k) -encoding function E für ein

Alphabet A ist injektiv, erstellt Codewörter:

$$E: A^k \rightarrow A^n: (a_0, \dots, a_{k-1}) \mapsto E(a_0, \dots, a_k) = (c_0, \dots, c_{n-1})$$

D5.37 (n, k) -error-correcting code C für A , $|A|=q$
 ist eine Untermenge von A^n mit Kardinalität q^k

D5.38 Hamming Distanz: Anzahl unterschiedlicher Positionen von zwei Strings

D5.39 Minimal Distanz: $d_{\min}(C)$ ist die minimale Hamming Distanz zu zwei beliebigen Codewörtern

D5.40 Decoding Function $D: A^n \rightarrow A^k$

T5.40 Code C mit Min. Distanz d ist t -error correcting $\Leftrightarrow d \geq 2t + 1$

T5.41 Sei $A = GF(q)$ und $\alpha_0, \dots, \alpha_{n-1} \in GF(q)$

Sei $E(a_0, \dots, a_{n-1}) = (a(\alpha_0), \dots, a(\alpha_{n-1}))$, wobei $a(x) = a_{k-1}x^{k-1} + \dots + a_1x + a_0$

\hookrightarrow Dieser Code hat Minimaldistanz $n-k+1$

Beweis: jede zykl. Gruppe ist kommutativ

z.B: $a * b = b * a$. Seien a, b bel., $a = g^i, b = g^j$

$$a * b = g^i * g^j = \underbrace{g * \dots * g}_{i \text{ Mal}} * \underbrace{g * \dots * g}_{j \text{ Mal}} = b * a$$

IRREDUZIBLE POLYNOME

$GF(2)[x]_{10, 11, 111, 1011, 11011, 10011, 11001, 11111, 100101, 101001, 101111, 110111, 111011, 111101, 1000011, 1001001, 1010111, 1011011, 110001, 1100111, 110101, 1110011, 1110101}$

$GF(3)[x]_{10, 11, 12, 101, 112, 122, 1021, 1022, 1102, 1112, 1121, 1201, 1211, 1222, 10012, 10022, 10102, 10111, 10121, 10202, 11002, 11021, 11101, 11111, 11122, 11222, 12002, 12011, 12101, 12112, 12121, 12212}$

$GF(4)[x]_{10, 11, 12, 13, 112, 113, 121, 122, 131, 133, 1002, 1003, 1011, 1021, 1031, 1101, 1112, 1113, 1123, 1132, 1201, 1213, 1222, 1232, 1233, 1301, 1312, 1322, 1323, 1333}$

$GF(5)[x]_{10, 11, 12, 13, 14, 102, 103, 111, 112, 123, 124, 133, 134, 141, 142, 1011, 1014, 1021, 1024, 1032, 1033, 1042, 1043, 1101, 1102, 1113, 1114, 1131, 1134, 1141, 1143, 1201, 1203, 1213, 1214, 1222, 1223, 1242, 1244, 1302, 1304, 1311, 1312, 1322, 1323, 1341, 1343, 1403, 1404, 1411, 1412, 1431, 1434, 1442, 1444}$

$GF(7)[x]_{10, 11, 12, 13, 14, 15, 16, 101, 102, 104, 113, 114, 116, 122, 123, 125, 131, 135, 136, 141, 145, 146, 152, 153, 155, 163, 164, 166}$

wobei: $1412 = x^3 + 4x^2 + x + 2$

Gruppen (1: e auch LNE, 2: $\widehat{a * b} = \widehat{b} * \widehat{a}$, 3: $a * b = a * c \Rightarrow b = c$)

$$1) e * a = (a * \widehat{a}) * \widehat{a} = a * (\widehat{a} * \widehat{a}) = a * e = \widehat{a}$$

$$2) (a * b) * (\widehat{b} * \widehat{a}) = a * (b * (\widehat{b} * \widehat{a})) = a * ((b * \widehat{b}) * \widehat{a}) = \widehat{a} = e$$

$$3) \text{For all } a, b, c \in G: a * b = a * c \Rightarrow \widehat{a} * (a * b) = \widehat{a} * (a * c) \Rightarrow (\widehat{a} * a) * b = (\widehat{a} * a) * c \Rightarrow e * b = e * c \Rightarrow b = c$$

f: $\mathbb{Z}_{mn}^* \rightarrow \mathbb{Z}_n^* \times \mathbb{Z}_m^*$, $f(x) = (R_n(x), R_m(x))$ Isomorph.

1) f is function. We show $f(x) \in \mathbb{Z}_n^* \times \mathbb{Z}_m^*$ for all $x \in \mathbb{Z}_{mn}^*$

Let x . $\gcd(x, mn) = 1$. Let $d = \gcd(x, n)$.

Then, $d \mid x$ and $d \mid n \Rightarrow d \mid x$ and $d \mid nm \Rightarrow d \mid \gcd(x, nm)$

$\Rightarrow d = 1$. Therefore, $\gcd(R_n(x), n) = 1 \Rightarrow R_n(x) \in \mathbb{Z}_n^*$

2) f is surjective. Take $(a, b) \in \mathbb{Z}_n^* \times \mathbb{Z}_m^*$. Since $\gcd(m, n) = 1$

and CRT, there is unique $x \in \mathbb{Z}_{mn}$ w/ $(R_n(x), R_m(x)) = (a, b)$

Contradiction: let $d = \gcd(x, mn) > 1$. Let $p \mid d$. $\in \mathbb{Z}_n^*$

Then, $p \mid x$ and $p \mid n$. Therefore, $p \mid \gcd(x, n) = \gcd(R_n(x), n) = 1$

3) f injective. Above x unique in $\mathbb{Z}_{mn} \Rightarrow$ unique \mathbb{Z}_{mn}^*

4) f homomorphism. $f(a \cdot_{\text{num}} b) = (R_n(a \cdot_{\text{num}} b), R_m(a \cdot_{\text{num}} b))$

$$= (R_n(R_{nm}(ab)), R_m(R_{nm}(ab))) = (R_n(ab), R_m(ab))$$

$$= (R_n(R_n(a) \cdot R_n(b)), R_m(R_m(a) \cdot R_m(b))) = (R_n(a) \cdot_{\text{num}} R_n(b), \dots)$$

$$= (R_n(a), R_n(a)) * (R_n(b), R_m(b)) = f(a) * f(b)$$