Abstraktion = Simplifizierung ∧ Generalisierung
Diskrete Mathematik = Mathematik auf endlichen (bis $\aleph_0$) abzählbaren Strukturen.
Schokolade: $(x-1)+x(y-1)=xy-1=(y-1)+y(x-1)$
Falsche Beweise:
S = Es existiert größte Zahl n. T: n = 1 Beweisen ist nur $S \Rightarrow T$.

Beweissystem (Methode Korrektheit zu testen) $\Pi = (S, P, \tau, \phi)$
S: Menge der math. Aussagen. P: Menge von Beweisen.
Wahrheitsfunktion: Funktion $\tau: S \to \{0,1\}$ die jeder Aussage in S Wahrheitswert gibt
Verifizierfunktion: Funktion $\phi: S \times P \to \{0,1\}$ die sagt ob aus $S \Rightarrow P$.
Bsp.: c soll geheimer Schlüssel Diffie-Hellman (a, b sind private Schlüssel)
$\tau((a,b,c)) = 1 :\Leftrightarrow \exists x,y \in \mathbb{N}\ (a = g^x \wedge b = g^y \wedge c = g^{xy})$ $S = \mathbb{N}^3, P = \mathbb{N}$
$\phi((a,b,c),p) = 1 :\Leftrightarrow a = g^p \wedge c = b^p$
Vollständigkeit: Sei $(a,b,c) \in S$ mit $\tau((a,b,c)) = 1$. Dann gibt es ein $x,y \in \mathbb{N}$ mit $a = g^x, b = g^y$ und $c = g^{xy}$. Damit gilt auch $c = b^x$. Also ist x Beweis für (a,b,c).
Korrektheit: Sei (a,b,c) es mit $\tau((a,b,c)) = 0$. Dann gilt für alle $x,y \in \mathbb{N}$ mit $a = g^x$ und $b = g^y$, sodass $c \neq g^{xy}$. Somit gibt es kein x mit $a = g^x$ und $b^x = c$.
Vollständigkeit: $\forall s \in S\ \exists p \in P\ (\phi(s,p) = 1)$ Korr. $\forall s \in S\ \tau(s) = 1 \to \exists p\ \phi(s,p) = 1$

Syntax: Definiert welche Strings über Alphabet korrekte Formeln sind.
Domäne: Nicht-leere Klasse von Objekten unter betrachtet (Universum)
Semantik: Partielle Funktion $\sigma(F, \mathcal{A}) = \{0,1\}$. Jede Formel kriegt unter Interpretation Wert

Prädikatenlogik ($i \in \mathbb{N}$ Index, $k \in \mathbb{N}$ Anzahl Argumente
Syntax: (Objekt) Freie Variable/ Variable symbol: x_i (a,b...), Funk.symb. $f_i^{(k)}$
Falls k=0: Konstante, Prädikatsymbol: $P_i^{(k)}$, Term: Variable oder induktiv:
Term: Variable, oder induktiv falls $t_1, \dots, t_k$ Formeln $\Rightarrow f_i^{(k)}(t_1, \dots, t_k)$ ein Term.
Formel: Atomare Formel: $P_i^{(k)}(t_1, \dots, t_n)$ $\overset{k=0}{\text{Aussagen}}$ oder induktiv $\forall x_i F$ und $\exists x_i F$
Wenn F und G Formeln, dann sind auch $\neg F$, $(F \wedge G)$ und $(F \vee G)$ Formeln.

Aussagenlogik/semantik:
Eine Wahrheitsbelegung $\mathcal{A}: M \to \{0,1\}$, wo M atomare Formeln sind wird erweitert auf $\hat{M}$ mit Menge aller Formeln wie folgt:
$\mathcal{A}((F \wedge G)) = 1$ genau dann wenn $\mathcal{A}(F) = 1$ und $\mathcal{A}(G) = 1$, sonst 0
$\mathcal{A}(\neg F) = 1$ genau dann wenn $\mathcal{A}(F) = 0$.

Prädikatenlogik/Semantik: Struktur ist prädikatenlogische Interpretation
Struktur ist Tupel $\mathcal{A} = (U, \phi, \psi, \xi)$:
U nicht-leere Menge/Ans., dass Universum. $U^{\mathcal{A}} = \mathbb{N}$
ϕ definiert jede Funktion $f: U^k \to U$ $\phi^{\mathcal{A}} = \{f(x,y) = x+y, g(x) = x!\}$
ψ definiert jedes Prädikat $P: U^k \to \{0,1\}$ $\psi = \{P(x) = x \mid 2, Q(x,y) = x = y\}$
ξ definiert jede Variablensymbol $x_i \mapsto U$ $\xi = \{a = 3, b = 3.1415926\}$
or directly $f^{\mathcal{A}}(x,y) = x+y$, $a^{\mathcal{A}} = 3$
$\mathcal{A}(t) = \xi(t)$ $\mathcal{A}(f) = \phi(f)(\mathcal{A}(t_1), \dots, \mathcal{A}(t_n))$
$\mathcal{A}(P(t_1, \dots, t_n)) = \psi(P)(\mathcal{A}(t_1), \dots, \mathcal{A}(t_n))$
$\mathcal{A}(\underset{\exists}{\forall} x\ G) = \begin{cases} 1, & \text{falls } \mathcal{A}_{[x \to u]}(G) = 1 \text{ für alle } u \in U \ (\text{einz. } x) \\ 0, & \text{sonst} \end{cases}$

Substitution (falls $\forall$ & G) 6.8
$\forall x\ G \equiv \forall y\ G[x/y]$
$\exists x\ G \equiv \exists y\ G[x/y]$
$\mathcal{A}_{[x \to u]}(G) = \mathcal{A}_{[y \to u]}(G[x/y])$

Elimination (nur semantisch)
Falls F von der Form $\forall x\ G$
$\mathcal{A}(F)$ impliziert Struktur $\mathcal{A}_{[x \to u]}(G)$
Der einzige Unterschied, dass zus. $\xi(x) = u$

6.2
1) $F \wedge F \equiv F$ und $F \vee F \equiv F$ Idempotenz
2) $F \wedge G \equiv G \wedge F$ und $F \vee G \equiv G \vee F$ Kommutativität
3) $(F \wedge G) \wedge H \equiv F \wedge (G \wedge H)$ EQU ∨ Assoziativität
4) $F \wedge (F \vee G) \equiv F$ und $F \vee (F \wedge G) \equiv F$!!! Absorption
5) $F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$!!! Distr. ∧
6) $F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$!!! Distr. ∨
7) $\neg\neg F \equiv F$ Doppelnegation
8) $\neg(F \wedge G) \equiv \neg F \vee \neg G$ EQU ∨ De Morgan
9) $F \wedge \top \equiv F$ und $F \vee \top \equiv \top$!!! Tautologien
10) $F \wedge \bot \equiv \bot$ und $F \vee \bot \equiv F$!!! Unerfüllbar
11) $F \wedge \neg F \equiv \bot$ und $F \vee \neg F \equiv \top$!!!
Bsp. Beweis per Wahrheitstabelle und dem Satz:
Regel 8 folgt aus $\mathcal{A}(\neg(F \wedge G)) = 1$ genau dann wenn $\mathcal{A}(\neg F \vee G)$

6.6 F, G und H sind Formeln. In H darf x nicht frei vorkommen!

1,2) $\neg(\forall x\ F) \equiv \exists x\ \neg F$ EQU ∃
3,4) $(\forall x\ F) \wedge (\forall x\ G) \equiv \forall x (F \wedge G)$ EQU ∨
5,6) $\forall x \forall y\ F \equiv \forall y \forall x\ F$ EQU ∃
7) $\forall \wedge$ 8) $\forall \vee$ 9) $\exists \wedge$ 10) $\exists \vee$
$(\underset{\exists}{\forall} x\ F) \underset{\vee}{\wedge} H \equiv \underset{\exists}{\forall} x\ (F \underset{\vee}{\wedge} H)$ SUPEREQU

Teilbeweis $\{\forall x\ F, \forall y\ G\} \models F \wedge G$ $\boxed{\mathcal{A}(\forall x\ F) = 1 \Rightarrow \mathcal{A}_{[x \to u]}(F) = 1 \Rightarrow \mathcal{A}(F) = 1 \Rightarrow \mathcal{A}((F \wedge G)) = 1}$
6.7 In Subformeln anwenden!

6.10 $\neg \exists x \forall y (P(y,x) \Leftrightarrow \neg P(y,y))$ ist Tautologie
$\equiv \forall x \exists y (P(y,x) \Leftrightarrow P(y,y))$
Wenn y durch gebundene Variable x substituiert wird und $\forall x F(x,x)$ Tautologie, dann ist auch $\forall x \exists y\ F(x,y)$ Tautologie.

6.11 Russel: $\neg \exists R \forall S (S \in R \Leftrightarrow \neg(S \in S))$
Menge (R) aller Mengen, die sich selbst nicht enthalten.
6.13 $U^{\mathcal{A}}$: Menge aller Programme. $P^{\mathcal{A}}(y,x) = 1 :\Leftrightarrow$ Ausgabe von Programm x mit Eingabe y eine 1 ausgibt oder nichts. Nicht berechenbare Funktion $x: y \to \neg P(y,y)$
Programm, welches entscheidet ob Programm y mit Eingabe y 0 ausgibt (oder nicht hält)
Barbier U: Menge aller Männer, $P^{\mathcal{A}}(y,x) = 1 :\Leftrightarrow$ x rasiert y.

$A \Leftrightarrow B$. DNF: $(\neg A \wedge B) \vee (A \wedge \neg B) \to$ Jeder 1 Eintrag
CNF: $(A \vee B) \wedge (\neg A \vee \neg B) \to$ Das Resultat ist 0 und alle Werte verfälscht.
Klauselmenge (CNF): $\{\{A, B\}, \{\neg A, \neg B\}\}$

Klausel: Menge (und somit nur 0/1) von Literale (negierte atomare Formeln) verodert ∨
Klauselmenge: Menge von Klauseln verundet ∧

$F := A \Leftrightarrow B$ unerfüllbar: CNF $\vdash_{Res} \emptyset$ | Tautologie DNF negieren & De Morgan & Distrib.
$K_M \models F \Leftrightarrow K_M \cup \{F\} \vdash_{Res} \emptyset$ Res = {Res}
Resolution: $L \in K_1, \neg L \in K_2 : K = (K_1 - \{L\}) \cup (K_2 - \{\neg L\})$
Beweis korrekt: K_1 und K_2 müssen mind. je 1 korrekt haben. $\mathcal{A}(L) = 1 \Rightarrow K_2 - \{\neg L\}$ 1=1
Deswegen muss ein Klausel in K_2 wahr sein. Dieser Klausel ist auch in Vereinigung $\mathcal{A}(K) = 1$
Beweis endlich: 4^k Literalkombinationen. ~~Komplett~~: $M \models F \Rightarrow M \vdash_R F$

Definitionen
$A \to B :\equiv (\neg A \vee B)$
$A \leftrightarrow B :\equiv (A \wedge B) \vee (\neg A \wedge \neg B)$

Regeln:
$A \to B \equiv \neg B \to \neg A$
$\neg(A \leftrightarrow B) \equiv A \leftrightarrow \neg B$

Pränexnormalform: $\forall x \exists y \forall z\ F$ (zuerst bereinigen, Quantoren nach vorne)
Forcieren 3-Modell: $\forall x\ P(x,x) \wedge \exists a \exists b \exists c\ (\neg P(a,b) \wedge \neg P(a,c) \wedge \neg P(b,c))$
Forcieren ∞-Modell: $\forall x\ P(x, f(x)) \wedge \forall x \neg P(x,x) \wedge \forall x \forall y \forall z\ ((P(x,y) \wedge P(y,z)) \to P(x,z))$
f: reflexiv, P: transitiv aber nicht reflexiv. Falls Endlich Zyklus $\xRightarrow{\text{trans.}}$ reflexivität.

$\{F_1, \dots, F_k\} \models G$ | Wenn A Modell für F, dann auch für G
$\Leftrightarrow (F_1 \wedge \dots \wedge F_k) \to G$ | Wenn A Modell für $F_1 \wedge F_2 \dots$, dann auch für G.
$\Leftrightarrow (F_1 \wedge \dots \wedge F_k \wedge \neg G)$ ist unerfüllbar | Wenn A Modell für F, dann nicht für $\neg G$
$F \wedge G \equiv G \Leftrightarrow \models F \wedge G \Leftrightarrow G$

Indirekter Beweis (Modus tollens) $\sqrt{x}$ rational $\Rightarrow$ x rational
$\neg B \to \neg A \equiv A \to B$ (falls $x > 0$) X irrational $\Rightarrow \sqrt{x}$ irrational
Modus Ponens $(x > 2 \wedge 2^{x-1} \equiv_x 1) \to x$ prim $\wedge\ 2^{300} \equiv_{300} 1 \Rightarrow 300 \wedge \in \mathbb{P}$
$A \wedge (A \to B) \models A \to B$
Fallunterscheidung: $3 \mid p \vee 3 \mid (p+2) \vee 3 \mid (p+4) \Rightarrow$ $R_3(p) = 0 \to 3 \mid p$, $R_3(p) = 1 \to 3 \mid (p+4)$, $R_3(p) = 2 \to 3 \mid (p+2)$
Schubfachprinzip: Teile n Elemente auf k Mengen.
Eine Menge hat mindestens Grösse $\lceil \frac{n}{k} \rceil$
Beweis: Angenommen alle $\lceil \frac{n}{k} \rceil - 1 \Rightarrow k \cdot (\lceil \frac{n}{k} \rceil - 1) < n$
Gegeben Sequenz n^2+1: (#/ bis i, # \ bis i). Können nicht gleich sein. Es gibt 1 bis max n^2 Paare mit Grösse n. Es gibt aber mind. n^2+1 unterschi. Paare. Also $\exists$ Sequenz $> n$.

Induktion: 1. Prove $P(0)$, 2. Prove $\forall n (P(n) \to P(n+1))$
(2. 1d) $P(0) \wedge \forall n (P(n) \to P(n+1)) \models \forall n\ P(n)$ $n \geq 0$
Proof: $\neg F = \neg(P(0) \wedge \forall n (P(n) \to P(n+1)) \to \forall n\ P(n))$ #
$\equiv P(0) \wedge \forall n (P(n) \to P(n+1)) \wedge \exists n \neg P(n) \equiv \bot$
$P(n)$ is non-empty and has a least element a for which $\neg P(a)$
Da $P(0) \wedge \neg P(a)$, $a > 0$. Aber $P(a-1)$ gilt, also gilt $P(a)$. $\bot \Rightarrow F \equiv \top$

Es gibt einen Affen für den gilt, dass falls dieser Affe eine Banane ist, alle Affen eine Banane essen.
$\exists x\ (P(x) \to \forall y\ P(y)) \equiv$ Det $\to \equiv$ $\neg\exists \to \forall \neg$ $\equiv \top$

Wahrheitstafel (ung. $2^{(2^n)}$) Prim: $(6k \pm 1)$ $3 \mid p \vee 3 \mid p+2 \vee 3 \mid p+4$
Es gibt unendlich Funktionen $\mathbb{N} \mapsto \mathbb{N}$ $g(x) = 1 + f(x)$
Widerspruchsfrei: Kein Beweis zwei falschen Aussagen. $\forall s \in S\ \forall p \in P\ (\phi(s,p) \to \tau(s))$
Vollständig: Jede korrekte Aussage hat Beweis $\forall s \in S\ \exists p \in P\ (\tau(s) \to \phi(s,p))$
Bsp.: Widerspruchsfrei: $\tau(s) = 1$ oder $\phi(s,p) = 0$ | Vollständig: $\tau(s) = 0$ oder $\phi(s,p) = 1$
Vollständig, aber nicht W: $K = \{R\}: \emptyset \vdash_R F$ | Sonst: $\{A \vee B\} \vdash_R B \vee A$
Immer korrekt: $\forall x (F \wedge G) \models (\forall x\ F) \wedge G$. Korrektes Kalkül: $M \vdash_R F \Rightarrow M \models F$
Vollständiges Kalkül: $M \models F \Rightarrow M \vdash_R F$

6.5 Formeln M sind unerfüllbar $\Leftrightarrow K(M) \vdash_{Res} \emptyset$ ($\Leftarrow$ folgt aus Korrektheit)
Induktion n=1: Nur A_1, dann nur $\{A_1, \neg A_1\} \vdash_{Res} \emptyset$ Gegeben Klauselmenge K
K_0 Klauseln wo gilt $A_{n+1} = 0$, alle Klauseln mit $\neg A_{n+1}$ wegnehmen und A_{n+1} entfernen.
Wenn A_{n+1} nicht in K_1 dann $K_0 \vdash_{Res} \emptyset \Rightarrow K \vdash_{Res} 0$. Wenn A_{n+1} in K_1 dann $K_0 \vdash_{Res} \emptyset \Rightarrow$
$K \vdash_{Res} \{\neg A_{n+1}\}$. Falls sonst! $K \vdash_{Res} \{A_{n+1}\} \wedge K \vdash_{Res} \{\neg A_{n+1}\} \Rightarrow K \vdash_{Res} \emptyset$

Semantikerweiterung: $\mathcal{A}((F \# G)) = 1 \Leftrightarrow \mathcal{A}(F) = 1$ oder $\mathcal{A}(G) = 1$
Syntaxerweiterung: F Formel und G Formel, dann auch $(F \# G)$ Formel.

$A := \{x \mid \Phi(x)\}$ $\quad \exists A \forall x (x \in A \leftrightarrow \Phi(x))$

Beweis: $a \in \{x \mid P(x)\}$ Zeige: $P(a)$ wahr

Beweis: $a \in \{x \in S \mid P(x)\}$ Zeige: 1. $a \in S$ 2. $P(a)$ wahr

$\emptyset := \forall x (x \notin \emptyset)$

$A \subseteq B$ $\quad \forall x (x \in A \to x \in B)$
$\forall x (x \notin B \to x \notin A)$

Beweis: $\{x \in \mathbb{Z} : 18 \mid x\} \subseteq \{x \in \mathbb{Z} : 6 \mid x\} \Leftrightarrow \forall x (x \in \{x \in \mathbb{Z} : 18 \mid x\} \to x \in \{x \in \mathbb{Z} : 6 \mid x\})$
Nehme an $a \in \{x \in \mathbb{Z} \mid 18 \mid x\} \Rightarrow a \in \mathbb{Z} \wedge \exists c (a = 18 \cdot c) \Rightarrow a \in \mathbb{Z} \wedge \exists c (a = 6 \cdot c)$

$A \nsubseteq B$ $\quad \forall x (x \in A \to x \in B \wedge \neg x \in A \leftrightarrow x \in B)$

$A = B$ $\quad (A \subseteq B \wedge B \subseteq A) \mid \forall x (x \in A \leftrightarrow x \in B)$
$A \neq B$ $\quad \exists x \neg (x \in A \leftrightarrow x \in B)$

$A \cap B$ $\quad \{x \mid x \in A \wedge x \in B\}$ Nehme an $a \in A \wedge a \in B$..
$A \cup B$ $\quad \{x \mid x \in A \vee x \in B\}$

$\bigcap \mathbb{Z}$ $\quad \{x \mid \forall A \in \mathbb{Z} (x \in A)\}$ Leere Menge/Relation $\emptyset$
$\bigcup \mathbb{Z}$ $\quad \{x \mid \exists A \in \mathbb{Z} (x \in A)\}$

$A - B, A \setminus B$ $\quad \{x \mid x \in A \wedge x \notin B\}$

$\{1\} \notin P(\{1\}) = \{\emptyset, \{1\}\}$
$\emptyset \subseteq P(\emptyset) = \{\emptyset\}$
$P(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$
$P(\{a,b\}) = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}$

$P(A)$ $\quad \{S \mid S \subseteq A\}$ $\quad |P(A)| = 2^{|A|}$

$\overline{A}$ $\quad \{x \mid x \in U \wedge x \notin A\}$

(a,b) $\quad \{\{a\}, \{a,b\}\}$

$(a,b) \in \rho \wedge (b,a) \in \rho \to (a,a) \in \rho^2 \wedge (b,b) \in \rho^2$
$(a,b) \in \rho \wedge (b,c) \in \rho \to (a,c) \in \rho^2$

$A \times B$ $\quad \{(a,b) \mid a \in A \wedge b \in B\}$
$X_{i=1}^{k} A_i$ $\quad \{(a_1, \dots, a_k) \mid a_i \in A_i$ für $1 \le i \le k\}$
A^n $\quad X_{i=1}^{k} A$

$A_n = P(A_{n-1})$

Subset regel $\quad \{a\} \subseteq A \Leftrightarrow a \in A$ $\quad$ 3.1 $\{a\} = \{b\} \Rightarrow a = b$

Powerset regeln $\quad a \in P(A) \Leftrightarrow a \subseteq A$ $\quad A \in P(A)$
$\{x\} \in P(A) \wedge \{y\} \in P(A) \Leftrightarrow \{x, y\} \in P(A)$

T3.4

Kommutativität $\quad A \cap B = B \cap A$ $\quad A \cup B = B \cup A$

Assoziativität $\quad (A \cap B) \cap C = A \cap (B \cap C)$ $\quad (A \cup B) \cup C = A \cup (B \cup C)$

Idempotenz $\quad A \cap A = A$ $\quad A \cup A = A$

Absorption $\quad A \cap (A \cup B) = A$ $\quad A \cup (A \cap B) = A$

Distributiv $\quad A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $\quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Komplementär $\quad A \cap \overline{A} = \emptyset$ $\quad A \cup A = U$

De Morgan $\quad \overline{A \cap B} = \overline{A} \cup \overline{B}$ $\quad \overline{A \cup B} = \overline{A} \cap \overline{B}$

Konsistenz $\quad A \subseteq B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B \overset{\text{endlich}}{\Leftrightarrow} |A \cap B| = |A|$

Kardinalität $\quad |A \times B| = |A| \cdot |B|$
$A \subseteq B \wedge A \subseteq C \Leftrightarrow A \subseteq B \cap C$

Russel: $R = \{A \mid A \notin A\}$ Denn: $R \in R \to R \notin R$, aber $R \notin R \to R \in R$

Trotzdem ok: $S = \{A \mid |A| \ge 7\}$

Def. 3.4 $\quad \forall x (x \notin \emptyset)$ $\quad \to \forall x \in \emptyset \to x \in A \equiv T$

3.2 $\forall A (\emptyset \subseteq A)$ $\quad$ 3.3 $\exists! \emptyset$
$\Leftrightarrow \forall A (\emptyset \in P(A))$ $\quad \emptyset \subseteq \emptyset' \wedge \emptyset' \subseteq \emptyset \to \emptyset = \emptyset'$

$A \subseteq B \Leftrightarrow P(A) \subseteq P(B)$ $\quad \forall x (x \in A \to x \in B) \Leftrightarrow \forall x (\{x\} \subseteq A \to \{x\} \subseteq B)$
$\Leftrightarrow \forall x (\{x\} \in P(A) \to \{x\} \in P(B)) \overset{DP}{\Leftrightarrow} \forall x (x \in A \to x \in B)$

$(A \times B) = (A \times C) \Rightarrow A \neq \emptyset \to B = C$ $\quad a \in A \wedge b \in B \Leftrightarrow a \in A \wedge b \in C \Leftrightarrow$
$\exists a (a \in A) \wedge b \in B \Leftrightarrow b \in C \Leftrightarrow a \in \emptyset \wedge B = C$

$A \times (B \cap C) = (A \times B) \cap (A \times C) \Leftrightarrow \{(x,y) \mid (x \in A) \wedge (y \in B \cap C)\} \Leftrightarrow \{(x,y) \mid x \in A \wedge y \in B \wedge y \in C\}$
$\Leftrightarrow \{(x,y) \mid x \in A \wedge x \in A \wedge y \in B \wedge y \in C\} \Leftrightarrow \{(x,y) \mid x \in A \wedge y \in B\} \cap \{(x,y) \mid x \in A \wedge y \in C\} = (A \times B) \cap (A \times C)$

$\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$

(A,B)-Relation $\rho \subseteq X_{i=1}^{k} A_i$ | Binär: $\rho \subseteq \underset{\text{Domän}}{A} \times \underset{\text{Codomän}}{B}$ | $2^{|A| \cdot |B|}$

$a \rho b :\Leftrightarrow (a,b) \in \rho$

Identitätsrelation $id_A = \{(a,a) \mid a \in A\}$ $\quad id_A = \overline{id_A}$

Inverse: $\rho : A \to B$ $\quad \hat{\rho} : B \to A$ $\quad a \rho b :\Leftrightarrow b \hat{\rho} a$

3.6 $\widehat{\rho\sigma} = \hat{\sigma}\hat{\rho}$

Komposition: $a \rho \circ \sigma c :\Leftrightarrow \exists b \in B (a \rho b \wedge b \sigma c)$

3.5 Assoziativ: $\rho \circ (\sigma \circ \tau) = (\rho \circ \sigma) \circ \tau$ $\quad$ Beweis: $p(\sigma\tau)$ $\exists b (a \rho b \wedge b \sigma \tau d) \Rightarrow \dots$

N-ary Komposition: $\rho^n = \underbrace{\rho \circ \rho \dots \rho}_{n}$

Transitive Hülle $\rho^* = \bigcup_{n=1}^{\infty} \rho^n$ $\quad$ (Pfad von a zu b: $\exists c_1 \dots c_n (a \rho c_1 \wedge \dots \wedge c_n \rho b)$)

3.7 ρ transitiv $\Leftrightarrow \rho^2 \subseteq \rho$ $\quad$ Beweis: $\Rightarrow (a,c) \in \rho^2 \wedge \rho^2 \subseteq \rho \Rightarrow (a,c) \in \rho$
$\Leftarrow (a,b), (b,c) \in \rho \wedge (b,c) \in \rho$
$\Rightarrow a \rho^2 b :\Leftrightarrow \exists c (a \rho b \wedge b \rho c) \Rightarrow a \rho c$

Transitiv: $\forall a \forall b (a \rho b \wedge b \rho c) \to a \rho c$ $\quad =, \le, \ge, <, >, |, \equiv_m$, Ahnl.
$\rho^2 \subseteq \rho$

Reflexiv: $\forall a (a \rho a) \Leftrightarrow id_A \subseteq \rho$ $\quad =, \le, \ge, |$ (über $\mathbb{Z}$)

Irreflexiv: $\forall a (a \not\rho a) \Leftrightarrow id_A \cap \rho = \emptyset$ $\quad diag(M) = 0$ $\quad <, >, \neq,$

Symmetrisch: $\forall a \forall b (a \rho b \leftrightarrow b \rho a) \Leftrightarrow \rho = \hat{\rho}$ $\quad =, \neq, \equiv_m$, verbeinahtet

Antisymmetrisch: $\forall a \forall b (a \rho b \wedge b \rho a) \to a = b$ $\quad =, \le, \ge, <, >, |$ (über $\mathbb{N}$) Sonst $\to a = a$

$\rho \cap \hat{\rho} \subseteq id_A$

alles bis auf irreflexiv

$\emptyset$: alles bis auf reflexiv

ρ antisym. $\wedge \sigma$ antisym. $\Rightarrow \sigma \circ \rho$ antisym.
$(\sigma \circ \rho) \cap (\sigma \circ \rho)^{-1} \subseteq \rho(\sigma \circ \rho)^{-1} \subseteq \rho \cap \rho^{-1} \subseteq id$

Komplette Relation

Äquivalenz

$< :\Leftrightarrow \ge$ $\quad \| \quad \le \Leftrightarrow \ge$ (Achtung reflexiv bei Inverse!)

$a \mid b :\Leftrightarrow \exists k \in \mathbb{Z} (a = k \cdot b)$ $\quad \| \quad \rho^{-1} \cap \rho \Leftrightarrow id_A$ $\quad <\cap> \Leftrightarrow \emptyset$

$a \equiv_m b :\Leftrightarrow \exists k (a - b = k \cdot m)$ $\quad \| \quad \equiv_m \cap \equiv_n \Leftrightarrow \equiv_{kgv(m,n)}$ $\quad <\cup> \Leftrightarrow \overline{id}$

$3 < 4 = 3$ aber $4 < 4 = 4$ $\quad$ Komplement

Äquivalenzrelation ($\equiv$) reflexiv, transitiv & symmetrisch ($\equiv_m$ auf $\mathbb{Z}$)

Äquivalenzklasse: $[a]_\rho := \{b \in A \mid \overset{\text{sym.}}{b \rho a}\}$ $\quad [1]_{\equiv_3} = \{\dots, -5, -2, 1, 4, 7, \dots\}$

Quotientklasse: $A/\rho = A \text{ mod } \rho = \{[a]_\rho \mid a \in A\} \rightsquigarrow$ 3.9 ist Partition

Partition: $A = \bigcup_{i \in I} S_i = A \wedge S_a \cap S_b = \emptyset$ (falls $a \neq b$)
Klasse $S = \{S_1, \dots, S_n\}$

3.8 ρ, σ Äquivalenzrelationen $\Rightarrow \rho \cap \sigma$ Äquivalenzrelation

3.9 Quotientenklasse = Partition. $\quad$ Kevin: $\rho = \rho^2 \Rightarrow$ reicht nur symmetrisch

1. $a \ominus b \Rightarrow [a] = [b]$: $c \in [a] \Rightarrow c \ominus a \Rightarrow c \ominus b \Rightarrow c \in [b]$ $\quad$ transitiv & symmetrisch
2. $a \not\ominus b \Rightarrow [a] \cap [b] = \emptyset$: Kontadiktion $c \in [a] \cap [b] \Rightarrow c \ominus a \wedge c \ominus b \Rightarrow a \ominus b \Rightarrow \perp$

Rationale Zahlen: $(a,b) \sim (c,d) :\Leftrightarrow ad = bc$ wo $(a,b) \in (\mathbb{Z} \times (\mathbb{Z} - \{0\}))^2$
Reflexiv: $ab = ba$ Symm.: $ad = bc \Leftrightarrow cb = da$ Trans. $(a,b) \sim (c,d) \wedge (c,d) \sim (e,f) \Rightarrow (a,b) \sim (e,f)$
Trans. Beweis: $ad = bc \wedge cf = de \Rightarrow adcf = bcde \Rightarrow acf = bce \wedge d \neq 0$. Falls $c \neq 0 \Rightarrow af = be$
Falls $c = 0 \Rightarrow a = 0$ (weil $d \neq 0 \wedge ad = bc$) $\wedge e = 0$ (weil $d \neq 0 \wedge cf = de$) $\Rightarrow af = be$
$\mathbb{Q} = \mathbb{Z} \times (\mathbb{Z} - \{0\}) / \sim$

Partielle Ordnung: reflexiv, antisymmetrisch, transitiv $(A; \preceq)$, $\preceq \subseteq A^2$
z.B.: $\le, \ge, | \subseteq \mathbb{N}^2$, $(P(S); \subseteq)$, $a \sqsupseteq b$ wenn a überdeckt b.

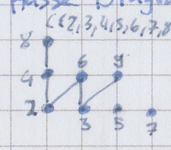
Vergleichbar: $\quad a \preceq b \vee b \preceq a$ $\quad$ Total geordnet falls alle vergleichbar $\to \le, \ge$ & reflexiv!

Wohlgeordnet: Total geordnet $\wedge$ jede Teilmenge hat ein kleinstes Element.
z.B.: $(\mathbb{Z}; \le)$
Nicht $(P(A); \subseteq)$ und $(\mathbb{N}, |)$ $\quad$ ↳ gilt immer für endliche total geord. Bsp.

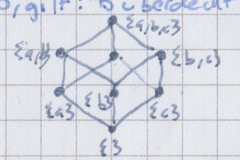
$a \prec b :\Leftrightarrow a \preceq b \wedge a \neq b$ $\quad$ Wenn $a \preceq b$ transitiv $\Rightarrow a \prec b$ transitiv

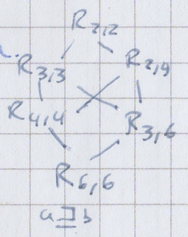
$\Rightarrow (a \overset{1}{\preceq} b \wedge a \overset{2}{\neq} b \wedge b \overset{3}{\preceq} c \wedge b \overset{4}{\neq} c) \to a \overset{5}{\preceq} c \wedge a \overset{6}{\neq} c$ $\quad$ 5: Durch 1,3 und transitiv.
6: $a = c \Rightarrow c \preceq b \wedge b \preceq c \Rightarrow \perp \Rightarrow a \neq c$ $\square$

Hasse Diagramm: Wenn $a \prec b$, gilt: b überdeckt a.



min: 2,3,5,7
max: 8,6,9,5,7
glb(8,6,2) = 2
lub(7,3) = 6





!: unik

Minimal: $\neg \exists a (a \prec m)$ $\quad$ Maximal: $\neg \exists a (m \prec a)$

! Unterstes: $\forall a (u \preceq a)$ $\quad$ Oberstes: $\forall a (a \preceq o)$

Untere Schranke: $\forall s \in S (u \preceq s)$ $\quad$ Obere Schranke: $\forall s \in S (s \preceq o)$ $\quad$ Erlaubt: $o \in S$.

! Grösste untere Schranke: $glb(S) = \max$ $\quad$ Tiefste obere Schranke: $lub(S) = \min$

$(\mathbb{N}; |)$ $glb(\{a,b,c\}) = gcd(a, gcd(b,c))$ $\in (\mathbb{N}; |)$ $lub(S) = lcm(s_1, lcm(s_2, s_3))$

$(P(A); \subseteq)$ $glb(\{a,b\}) = a \cap b$ $\quad (P(A); \subseteq)$ $lub(\{a,b\}) = a \cup b$

$\downarrow$ meet (infimum) = glb von Grösse 2. $\quad \uparrow$ join (supremum) = lub von Grösse 2.

Verband = Poset, bei dem jedes Element paar ein meet und join hat.
Bsp.: $(P(A); \subseteq)$, $(\mathbb{N}, |)$ aber nicht immer $(A; |)$

Ordnungsrelation: $(A; \preceq)$ und $(B; \sqsubseteq)$ formt: $(A \times B; \le)$
$(a_1, b_1) \le (a_2, b_2) :\Leftrightarrow a_1 \preceq a_2 \wedge b_1 \sqsubseteq b_2$

Lexikographische Ordnungsrelation:
$(a_1, b_1) \le_{lex} (a_2, b_2) :\Leftrightarrow a_1 \prec a_2 \vee (a_1 = a_2 \wedge b_1 \sqsubseteq b_2)$

Antisym.
$(a_1 \overset{1}{\prec} a_2 \vee (a_1 \overset{2}{=} a_2 \wedge b_1 \sqsubseteq b_2)) \wedge (a_2 \overset{3}{\prec} a_1 \vee (a_2 = a_1 \overset{4}{\wedge} b_2 \sqsubseteq b_1)) \to (a_1, b_1) = (a_2, b_2)$

1 3 kann nicht wahr sein.
1 4 $a_1 \neq a_2 \wedge a_1 = a_2 \to \perp$ ditto
2 3 $a_1 \neq a_2 \wedge a_1 = a_2 \to \perp$ ditto
2 4 $a_1 = a_2$ folgt von 2 und $b_1 \sqsubseteq b_2 \wedge b_2 \sqsubseteq b_1 \to b_1 = b_2$

Reflex. $a_1 \prec a_1 \vee (a_1 = a_1 \wedge b_1 \sqsubseteq b_2) \Rightarrow T$

$\forall x\ \neg elt(x,x)$

$gelt(x,y) :\Leftrightarrow \exists z\,(elt(x,z) \wedge elt(z,y))$

$geschw(x,y) :\Leftrightarrow x \neq y \wedge \exists z\,(elt(z,x) \wedge elt(z,y))$

$onkel(x,y) :\Leftrightarrow \delta(x) \wedge (\exists z\,(elt(z,x) \wedge gelt(z,y))) \wedge \neg elt(x,y)$

$vorfahr(x,y) :\Leftrightarrow elt(x,y) \vee gelt(x,y)$ ABER rekursive: $\forall x \forall y\ vorfahr(x,y) \Leftrightarrow ((elt(x,y) \to vorfahr(x,y)) \wedge (vorfahr(x,y) \wedge vorfahr(y,z) \to vorfahr(x,z)) \wedge \forall x\ \neg vorfahr(x,x))$

$vorfahr(x,y) :\Leftrightarrow \exists z\,(vorfahr(z,x) \wedge vorfahr(z,y)) \wedge x \neq y$

Funktion $(f: A \to B) \subseteq A \times B$ A: Definitionsbereich B: Wertebereich / Bild bereich

1. $\forall a \in A\ \exists b \in B\ a f b$ (total definiert)
2. $\forall a \in A\ \forall b, b' \in B\ a f b \wedge a f b' \to b = b'$ (wohldefiniert / partielle Funktion)

Die Menge aller Funktionen wird geschrieben: B^A, $|B^A| = |B|^{|A|}$

Bild von S: $f(S) := \{f(a) \mid a \in S\}$

Bild $= Im(A) := f(A)$

Urbild von T: $f^{-1}(T) := \{a \in A \mid f(a) \in T\}$ $\to$ $x \in f^{-1}(A) \wedge f$ bijektiv $\Rightarrow f(x) \in A$

$S = f^{-1}(T)$ $f(S) = T$

$f: A \to B$, $f^{-1}(f(A')) \subseteq A' \Rightarrow f$ injektiv. Nutz: $a \in A' \wedge a \in A - A'$

i) injektiv: $a \neq b \Rightarrow f(a) \neq f(b)$ oder $\forall a, a' \in A\ (f(a) = f(a')) \to a = a'$

ii) surjektiv: $\forall b \in B\ \exists a \in A\ (f(a) = b)$ $\forall a \forall A\ f(a) \in f(A) \to a \in A$

iii) bijektiv = surjektiv $\wedge$ injektiv

f injektiv $\wedge\ |A| = |B| \Rightarrow f$ bijektiv

$A \to B$ injektiv $\Leftrightarrow B \to A$ surjektiv

Abzählbarkeit

$A \sim B :\Leftrightarrow |A| = |B| \Leftrightarrow \exists$ bijektive Funktion: $A \to B$ (equipotent)

$A \preceq B :\Leftrightarrow |A| \leq |B| \Leftrightarrow \exists C\,(C \subseteq B \wedge A \sim C) \Leftrightarrow \exists$ injektive Funktion: $A \to B$

$A \prec B :\Leftrightarrow |A| < |B| \Leftrightarrow A \preceq B \wedge \neg(A \sim B)$

A abzählbar $\Leftrightarrow A \preceq \mathbb{N}$

Schröder-Bernstein: $A \preceq B \wedge B \preceq A \Rightarrow A \sim B$

$A \subseteq B \Rightarrow A \preceq B$

$\preceq$ transitiv: $A \preceq B \wedge B \preceq C \Rightarrow A \preceq C$

Beweis: Es gibt Injektion $A \to B$ und Injektion $B \to C$, dann auch Injektion $A \to C$.

$\mathbb{R} \sim [-1,3]$: $r \mapsto \begin{cases} r+2 & \text{wenn } r > -1 \wedge r < 1 \\ \frac{1}{r} & \text{sonst} \end{cases}$ Umgekehrt $\mathbb{R} \preceq [-1,3] \wedge [-1,3] \preceq \mathbb{R} \to \mathbb{R} \sim$ (immer injektiv)

$\mathbb{N} \to \mathbb{Z}$ $n \mapsto (-1)^n \lceil \frac{n}{2} \rceil$ $\mathbb{Z} \to \mathbb{N}$: $z \mapsto z^2 + 1$ ($+1$ nachher falls $z < 0$)

$\mathbb{N} \to \mathbb{O}$: $2n+1$

$\mathbb{N} \times \mathbb{N} \to \mathbb{N}$: $\pi(x,y) = \frac{1}{2}(x+y-2)(x+y-1) + y$ $\to (1,1), (1,2), \ldots$ 3.16

$\mathbb{N}_0 \to \mathbb{N}_0 \times \mathbb{N}_0$: $n \mapsto (k,m)$: $k + m = t - 1$ | t, k kleinste Zahl sodass: $\binom{t+1}{2} > n$

$\mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$: $\pi_0(x,y) = \frac{1}{2}(x+y)(x+y+1) + y$ $\to (0,0), (1,0), (0,1), (1,1)$

3.14 A abzählbar $\Leftrightarrow A \sim \mathbb{N} \vee |A| \in \mathbb{N}$

Es existiert also Bijektion $f: A \to C \subseteq \mathbb{N}$. Für eine unendliche Menge C, kann das kleinste Element c_0 ausgesucht werden und $g(c_0) = 0$ definieren. Dies wiederholt man mit $C - \{c_0\} \ldots$ $g \circ f$ Bijektion zu $\mathbb{N}$

Zählbar:

$\{0,1\}^* := \{\varepsilon, 0, 1, 01, \ldots\}$

Beweis: 1 am Anfang & dann binäre Repräsent.

$f: A \to \mathbb{N}$ $g: B \to \mathbb{N}$ $A \times B$ A^n $\bigcup_{i \in \mathbb{N}} A_i$ $A_i \preceq \mathbb{N}$ $A^* = \bigcup_{i=0}^{\infty} A^i$

$(a,b) \mapsto \pi(f(a), g(b))$ $A_3' = A_3 - \{A_1' \cup A_2' \cup A_3\}$

$(a_1, \ldots, a_n) \mapsto \prod_{i=1}^{n} p_i^{f(a_i)}$ $\to$ Tabelle!

$\mathbb{R}$, $P(\mathbb{N})$, $\{0,1\}^\infty$, $\mathbb{R} - \mathbb{N}$, $[0,1)$ B, falls $\mathbb{R} \preceq B$

N-te Bit B_{ii} xoren! $\alpha: B_{00} B_{11} \ldots$ existiert nicht!

Zahlentheorie

$a|b :\Leftrightarrow \exists e\,(b = e \cdot a)$ Teiler: $\{a : a|b\}$ Vielfaches: $\{b : a|b\}$

1. $a|b \Rightarrow \forall k\ a|k \cdot b$
2. $c|a \wedge c|b \Rightarrow c|(a \pm b)$
3. $c|a \wedge c|b \Rightarrow c|(a \cdot b)$ ($\Leftarrow$ $\gcd(a,b)=1$)
4. $a|b \wedge b|c \Rightarrow a|c$

(*) $c|(a \pm \cancel{c \cdot b}) \wedge c|b \Rightarrow c|a$

$f: A \to \mathbb{Z}$ $\exists \alpha$ injektiv von $\bigcup_{i \in \mathbb{N}}$

Euklidd. Division $\left(\frac{a}{b} = q + r \cdot \frac{1}{b}\right)$ $\forall a \forall b \neq 0\ \exists q\ \exists r: (a = b \cdot q + r) \wedge 0 \leq r < |d|$

$r := R_b(a)$ $-\frac{26}{3} = 3 \cdot (-9) + 1$

$Idea(a) := \{u \cdot a \mid u \in \mathbb{Z}\}$, $(a,b) := \{u \cdot a + v \cdot b \mid u, v \in \mathbb{Z}\}$ Für $\mathbb{Z}$ ±

$GGT(a,b) = d :\Leftrightarrow d|a \wedge d|b \wedge \forall c\,((c|a \wedge c|b) \to c|d)$

4.4 $(a,b) = (d) \Rightarrow d = \gcd(a,b)$ Annahme c ist $\gcd(a,b) \Rightarrow c|a \wedge c|b$ $\forall u \forall v\ c|(u \cdot a + v \cdot b) \overset{4.3}{\Rightarrow} c|d$. Dies ist Def. von gcd.

$(1) \in (a,b) \Rightarrow (1) = (a,b)$ $\Leftrightarrow$ prim

4.2 $\gcd(m - qn) = \gcd(m,n)$ 4.3 $\forall a,b \in \mathbb{Z}\ \exists d\ (a,b) = (d) = (\gcd(a,b))$ wenn $u \cdot a + v \cdot b = 1$?

$LCM(a,b) = d :\Leftrightarrow a|l \wedge b|l \wedge \forall m((a|m \wedge b|m) \to l|m)$

$\gcd(a,b) \cdot lcm(a,b) = a \cdot b$

Primfaktor: $a = \prod_i p_i^{e_i}$ $b = \prod_i p_i^{e_i}$ $\gcd(a,b) = \prod_i p_i^{\min(e_i,f_i)}$ (gemeinsam) $lcm(a,b) = \prod_i p_i^{\max(e_i,f_i)}$ (gemeinsam)

s_n	$s(z=r)$	q	u_1	u_2	v_1	v_2	
a	b	–	1	0	0	1	nach Initialisierung
b	Rest $\left(\frac{a}{b}\right)$	$\lfloor \frac{a}{b} \rfloor$	0	$u_1 - q \cdot u_2$	1	$v_2 - q \cdot v_2$	nach Schleifendurchgang 1.
⋮	⋮	⋮	⋮	⋮	⋮	⋮	
gcd(a,b)	0	*	u	~	v	~	nach letztem Schleifendurchgang

Primzahl: $prime(p) :\Leftrightarrow \forall a \forall b\,(p|(a \cdot b) \to p|a \vee p|b)$

Irrationalität $\sqrt{n}$: $\sqrt{n} = \frac{a}{b} \Rightarrow a = nb$ Wenn n keine Quadratzahl ist, hat es mind. ein Primfaktor mit ungeradem Grad. $\Leftarrow$ 2 gerade # Primfaktoren und $n \cdot b^2$ nicht.

$\sqrt[n]{m}$: $\frac{a}{b}$, wo a & b teilerfremd, sonst ok.

$m \cdot b^n = a^n$ Es gilt $\wedge|$ # Primfaktoren von a^n und b^n. Sonst: $m = \frac{a^n}{b^n}$ Summanden ≠ #Ef.

Nur noch zu Bew.: $n \nmid$ # Primfaktoren m

Irrationalität $\log_2(3) = \frac{a}{b} \Rightarrow 2^{\frac{a}{b}} = 3 \Rightarrow 2^a = 3^b$ $\to$ ABER: Ungleiche Primfaktoren

$x^n + x - 1 = y^2 \rightsquigarrow R_3(\text{links}) = 2 \wedge R_3(\text{rechts}) \in \{0,1\}$

$x^n + y^n = z$: $n = 2$ hat Lösung $n > 3$ nicht.

Binomialsatz: $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$

$ax + by = \gcd(a,b) \Rightarrow x = u, y = v$ (or solve)

$x = x_0 + \frac{b}{\gcd(a,b)} \cdot t$ $y = y_0 - \frac{a}{\gcd(a,b)} \cdot t$; $t \in \mathbb{Z}$

4.3 Proof:

$(a,b) \neq \emptyset$ $d > 0$

S: d das kleinste Element $\in (a,b)$

$(d) \subseteq (a,b)$ offensichtlich

$c \in (a,b) \wedge c = dq + r$

Da $c \in (a,b) \wedge d \in (a,b)$ ist auch $r \in (a,b)$. Da d kleinstes El., $r = 0$.

Modulo

$a \equiv_m b :\Leftrightarrow m|(a-b) \Leftrightarrow \exists k\ a = k \cdot m + b$

4.14 $\equiv_m$ ist Äquivalenzrelation: Reflexiv: $m|0 \Rightarrow m|(a-a) \Rightarrow a \equiv_m a$

Sym: $\exists k\,(a = k \cdot m + b) \Leftrightarrow \exists q\,(b = q \cdot m + a)$. Trans: $m|(a-b) \wedge m|(b-c) \Rightarrow m|(a - \cancel{b} + \cancel{b} - c)$

$\hookrightarrow$ (0): $a \equiv_m b \wedge b \equiv_m c \Rightarrow a \equiv_m c$

i. $a \not\equiv_m b \Rightarrow a \neq b$

ii. $a \equiv_m b \Rightarrow p \cdot a \equiv_m p \cdot b$

iii. $p \cdot a \equiv_m p \cdot b \wedge \gcd(p,m) = 1 \Rightarrow a \equiv_m b$

iv. $a \equiv_m b \wedge c \equiv_m d \Rightarrow a + c \equiv_m b + d$ Proof: $m|(a-b) + (c-d) \Rightarrow m|(a+c) - (b+d)$

v. $a \equiv_m b \wedge c \equiv_m d \Rightarrow a \cdot c \equiv_m b \cdot d$ Proof: 1. $m|(a-b) \Leftrightarrow a = mc_1 + b$ 2. $m|(c-d) \Leftrightarrow c = mc_2 + d$

$ac = (mc_1 + b)(mc_2 + d) = m(mc_1c_2 + c_1b + c_2d) + bd$

$ac - bd = m(\ldots) + bd - bd$

$\langle \ldots \rangle \in \mathbb{Z} \Rightarrow |(\ldots)| \cdot m \equiv_m$

v2 $a \equiv_m b \Rightarrow a^n \equiv_m b^n$

vi. $f(a_1, \ldots, a_k)$ Multivariatpolynom; z.B. $f(x,y) = a_{21}x^2y^2 + a_{10}x \cdot y^2 + a_0a_0$

$a_i \equiv_m b_i$ (und $m \geq 1$) $\Rightarrow f(a_1, \ldots, a_k) \equiv_m f(b_1, \ldots, b_k)$

0. Jede Zahl: $\forall a\ a = k \cdot m + R_m(a)$

4.17i: $\forall a\ a \equiv_m R_m(a)$ Direkt von 0. $a - R_m(a) = k \cdot m \Rightarrow a \equiv_m R_m(a)$

4.17ii: $a \equiv_m b \Leftrightarrow R_m(a) \equiv_m R_m(b)$

$R_m(a \pm b) = R_m[R_m(a) \pm R_m(b)]$

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

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

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

$R_m(a) \in [a]_{\equiv_m}$

$a + b \equiv_m R_m(a) + R_m(b)$

$R_m(a+b) \equiv_m R_m(R_m(a) + R_m(b))$

$a = k \cdot m + R_m(a) \wedge b = q \cdot m + R_m(b)$

$R_m(a \cdot b) = R_m[k \cdot q \cdot m^2 + k \cdot m \cdot R_m(b) + q \cdot m \cdot R_m(a) + R_m(a) \cdot R_m(b)] = R_m(R_m(a) \cdot R_m(b))$

$R_m(a^{-1}) = (R_m(a))^{-1}$

$\gcd(n,m) = 1 \wedge a \equiv_{mn} b \Leftrightarrow a \equiv_n b \wedge a \equiv_n b$

$\Leftarrow x_m = a - b = y_n \Rightarrow m|y_n \overset{\gcd}{\Rightarrow} m|y \Rightarrow a - b = y_n = z_{nm}$

Fast Modulo 1: $R_{19}(7^{11}) \overset{\text{Binär Exp.}}{=} R_{19}(7^{8+2+1}) = R_{19}[R_{19}(7^8) \cdot R_{19}(7^2) \cdot R_{19}(7^1)]$

1 2 4 8

$7, 14, \overset{14 \cdot 14 = 196}{6}, 17$

Lineare Kongruenz $ax \equiv_m b$

Nur Lösung wenn $\gcd(a,m) | b$. Es gibt $\gcd(a,m)$ Äquivalenzlösungen.

Alle Lösungen: $x_i = x_0 + \frac{m}{\gcd(a,m)} \cdot i$ $[x_i]_m$ Lösung.

Multiplikative Inverse $ax \equiv_m 1$ Alternativ nach S. 38

4.19 hat NUR eine Lösung falls $\gcd(a,m) = 1$, sonst keine. Unik!

$\gcd(a,m) = ua + v \cdot m$; $a^{-1} = x = R_m(u)$ minimale Lösung unik in $[0,m)$

Proof: $ua = v \cdot m + 1$

($\Rightarrow$) $\gcd(a,m)|a \wedge \gcd(a,m)|m \Rightarrow \gcd(a,m)|(ax - vm) \Rightarrow \gcd(a,m)|1 \Rightarrow \gcd(a,m) = 1$

($\Leftarrow$) $\gcd(a,m) = 1 \Rightarrow xa + v \cdot m = 1 \Rightarrow x \cdot a \equiv_m 1 \Rightarrow R_m(x) \cdot a \equiv_m 1 \in \mathbb{Z}$

Unik: $ax - ax' \equiv_m 0 \Rightarrow m|a(x - x') \overset{\gcd}{\Rightarrow} m|(x - x') \Rightarrow R_m(x) = R_m(x') \Rightarrow [0,m)$ □

$\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m \mid \gcd(a,m) = 1\}$

Chinesischer Restsatz

Unik $[0, M[$ $\quad x' - x'' \equiv_{m_i} 0 \ (\forall i)$

$m_i \mid (x' - x'') \ \forall i$

$\mathrm{lcm}(m_1, \dots, m_n) = M \mid x' - x''$

$x' \equiv_M x''$

$X \equiv m_1 \ a_1$

$\vdots$

$X \equiv m_n \ a_n$

$$x = R_M\left[M_1 \cdot a_1 \cdot X_1 + \dots + M_n a_n X_n\right]$$

$x + M \cdot k$ andere Lösungen.

$M = \prod m_i$ $\quad$ Geht wenn $\gcd(m_i, m_j) = 1 \ (i \neq j)$

$M_i = \frac{M}{m_i}$ $\quad$ 1. $\gcd(M_i, m_i) = 1$

$M_i \cdot X_i \equiv_{m_i} 1$ $\quad$ 2. $M_i \cdot X_i \equiv_{m_j} 0 \ (i \neq j)$

3. $\sum_{i=1}^{r} a_i M_i X_i \equiv_{m_k} a_k$

1: $X \equiv_3 4 \Rightarrow X \equiv_3 1$ $\quad M = 3 \cdot 4 \cdot 5 = 60$

2: $X \equiv_4 2$ $\quad x = R_{60}\left(\frac{60}{3} \cdot 1 \cdot X_1 + \frac{60}{4} \cdot 2 \cdot X_2 + \frac{60}{5} \cdot 3 \cdot X_3\right)$

3: $X \equiv_5 3$

$X_1: 15 \cdot X_2 \equiv_4 1 \Rightarrow X_2 = 3.$

$X_3: 12 \cdot X_3 \equiv_5 1 \Rightarrow X_3 = 3$ $\quad$ können gleich sein.

Trick: Wegen (3) endet auf 3 oder 8. Wegen (2) ist die letzte Zahl gerade.
Kandidaten: 8, 18, 28, 38, 48, 58.
1 erfüllen nur 28, 58. Wegen 58 ist einzige durch 4 teilbare Zahl.

Falls nicht erfüllt: $m = ab$, $n = ac$, $a = \gcd(m, n)$

~~$X \equiv_6 0$~~ $\Rightarrow$ ~~$X \equiv_3 0$~~

$X \equiv_8 2$ $\quad$ ~~$X \equiv_2 0$~~ implizierte

$X \equiv_9 6$ $\quad$ implizierte

Nur Implikationspfeile! Widersprüche stimmen

Nur eine Lösung zwischen $[0, 72 = 8 \cdot 9)$

Diffie-Hellmann

Wähle p und $q \in \langle \mathbb{Z}_p^*, \odot \rangle$

Einfach: $x \to R_p(g^x)$

Diskretes Logarithmus Problem:

Schwer: $R_p(g^x) \to x$

$y_A = R_p(g^{x_A})$

$y_B = R_p(g^{x_B})$

$k_{AB} = R_p(y_B^{x_A}) = R_p(g^{x_B \cdot x_A}) = R_p(y_A^{x_B})$

Wähle G und Generator $g \in G$

$\langle \mathbb{Z}_n, \oplus \rangle$ z.B. $g = 2$, $n = 5$

Einfach: $x \to g^x$ (hier: $x \to g \cdot x$)

(schwer): $g^x \to x$ (hier: $g \cdot x \to x$)

$y_A = R_n(g \cdot x_A)$

$y_B = R_n(g \cdot x_B)$

$k_{AB} = R_n(y_B \cdot x_A) = R_n(g \cdot x_A \cdot x_B)$

$= R_n(g \cdot x_A(a \cdot g) \cdot x_B)$ $\quad : R_n(a \cdot g) = 1$ geeignet

$= R_n(R_n(g \cdot x_A) \cdot R_n(a \cdot g \cdot x_B))$

$= R_n(R_n(g \cdot x_A) \cdot R_n(a) \cdot R_n(g \cdot x_B))$

RSA über endliche Gruppe G

$e \in \mathbb{Z}$, sodass $\gcd(|G|, e) = 1$ $\quad$ Ziel: $m^e = y$ = encrypted msg

$m = y^d$, wobei d inv. e: $ed \equiv_{|G|} 1$

Beweis: $(y^d)^e = y^{de} = y^{k \cdot |G| + 1} = (y^{|G|})^k \cdot y = y$

$\mathbb{Z}_n^*$, wobei $n = p \cdot q$ und $|\mathbb{Z}_n^*| = \varphi(n) = (p-1) \cdot (q-1)$

Encryption: $m \to y = R_n(m^e)$ $\quad$ | $\quad$ Decryption: $y \to m = R_n(y^d)$ $\quad$ NP-hard finding n-th root

$ed \equiv_{(p-1)(q-1)} 1 \Rightarrow$ Mult. Inverse: $\gcd(e, \varphi(n)) = d \cdot e + f \cdot \varphi(n)$

Algebra

Ein Operator ist eine (geschlossene) Funktion $w: S^n \to S$; $n \geq 0$ Arität

$\langle S; w_1, \dots, w_n \rangle$ ist algebraische Struktur mit Trägermenge S.

Geschlossenheit

(G0) $\forall (a, b) \in G \ (a \circ b \in G)$ $\quad$ Magma:

Assoziativität

(G1) $(a \circ b) \circ c = a \circ (b \circ c)$ $\quad$ Halbgruppe:

Neutrale element = Links- & Rechtsinvers

(G2) $\exists e \ (e \circ a = a = a \circ e)$ $\quad$ Monoid:

Inverse element = Links- & Rechtsinvers

(G3) $\forall a \ \exists \hat{a} \ (a \circ \hat{a} = e = \hat{a} \circ a)$ Gruppe:

Beispiel linksneutral / rechtsinvers: $\langle \mathbb{R} \setminus \{0\}; |a| \cdot b \rangle$

~~Assoz~~ $\quad$ Komm: $\frac{a+b}{2}$

Linksneutral = Rechtsneutral $\quad e_L \overset{G2}{=} e_L \circ e_R \overset{G2}{=} e_R$

Eindeutigkeit Neutrale $\quad e \overset{G2}{=} e \circ e' \overset{G2}{=} e'$

Rechtsinvers $\Rightarrow$ Linksinvers: $\quad \hat{a} \circ a \overset{G2}{=} (\hat{a} \circ a) \circ e \overset{G3}{=} (\hat{a} \circ a) \circ (\hat{a} \circ \hat{\hat{a}})$

$\overset{G1}{=} \hat{a} \circ ((a \circ \hat{a}) \circ \hat{\hat{a}}) \overset{G2}{=} \hat{a} \circ (e \circ \hat{\hat{a}}) \overset{G2}{=} \hat{a} \circ \hat{\hat{a}} \overset{G3}{=} e$

Eindeutigkeit Invers: $\hat{a} \overset{G2}{=} \hat{a} \circ e \overset{G3}{=} \hat{a} \circ (a \circ a^{-1}) \overset{G1}{=} (\hat{a} \circ a) \circ a^{-1} \overset{G3}{=} e \circ a^{-1} \overset{G2}{=} a^{-1}$

Rechtsneutral $\Rightarrow$ linksneutral: $\quad e \circ a \overset{G3}{=} (a \circ \hat{a}) \circ a \overset{G1}{=} a \circ (\hat{a} \circ a) \overset{G3}{=} a \circ e \overset{G2}{=} a$

Falls Inverse existiert:

Umpotenz $\Rightarrow$ Neutral $\quad a \cdot a = a \Leftrightarrow a \cdot a \cdot a^{-1} = a \cdot a^{-1} \Leftrightarrow a = e$

Ring / Multiplikativer Monoid $\quad x \cdot x = e \Leftrightarrow x^2 - 1 = 0 \Leftrightarrow (x-1)(x+1) = 0$

$\Leftrightarrow x \in \{-1, 1\}$

(5.3i) $\hat{\hat{a}} = a$ $\quad a \overset{G2}{=} e \circ a \overset{G3}{=} (\hat{\hat{a}} \circ \hat{a}) \circ a \overset{G1}{=} \hat{\hat{a}} \circ (\hat{a} \circ a) \overset{G3}{=} \hat{\hat{a}} \circ e \overset{G2}{=} \hat{\hat{a}}$

(5.3ii) $\widehat{a \circ b} = \hat{b} \circ \hat{a}$ $\quad \widehat{a \circ b} \overset{G2}{=} (\widehat{a \circ b}) \circ e \overset{G3}{=} (\widehat{a \circ b}) \circ (a \circ \hat{a})$

$\overset{G2}{=} (\widehat{a \circ b}) \circ (a \circ (e \circ \hat{a})) \overset{G3}{=} (a \circ b) \circ (a \circ ((b \circ \hat{b}) \circ \hat{a}))$

$\overset{2 \times G1}{=} ((\widehat{a \circ b}) \circ (a \circ b)) \circ (\hat{b} \circ \hat{a}) \overset{G3}{=} e \circ (\hat{b} \circ \hat{a}) \overset{G2}{=} \hat{b} \circ \hat{a}$

(5.3iii) $a \circ b = a \circ c \Leftrightarrow b = c$ $\quad (b \circ a) \hat{a} = (c a) \hat{a}$

$\Leftrightarrow b(a \hat{a}) = c(a \hat{a})$

(5.3iv) $b \circ a = c \circ a \Leftrightarrow a = c$ $\quad \Leftrightarrow be = ce$

$\Leftrightarrow b = c$

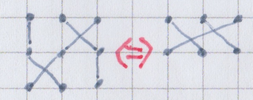
(5.3v) $a \circ x = b \vee x \circ a = b \Rightarrow b$ eine Lösung

$\circ$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Permutation S_n

Neutr. (1,2,3)

$(1,3,2) \circ (2,1,3) = (2,3,1)$



Gruppen:

$\langle \mathbb{R}^{m \times n}; \cdot \rangle$

$\langle \mathbb{Z}_m; \oplus, -a, 0 \rangle$

$\langle \mathbb{Z}_m^*; \odot, -1, 1 \rangle$

$\langle \mathbb{R}[x]; + \rangle$

$\langle \mathbb{R} \setminus \{0\}; \cdot \rangle$

S_n

Rotation:

Rotation ∘ Rotation = Rotation

Rotation ∘ Spiegelung = Spiegelung

Spiegelung ∘ Spiegelung = Rotation

Monoide:

String concatenation

$\langle \mathbb{R}; \cdot \rangle$ 0 hat kein Inverses.

$\{0, 1\}^*$

$\langle \mathbb{N} \setminus \{0\}; \cdot \rangle$ $\mathbb{Z}$ $\frac{1}{2}$ fehlt

Halbgruppe: $\begin{array}{c|ccc} \circ & 1 & 2 & 3 \\ \hline 1 & 1 & 2 & 3 \\ 2 & 1 & 2 & 3 \\ 3 & 1 & 2 & 3 \end{array}$ $\perp$

leere Trägermenge

Magma: $\begin{array}{c|ccc} \circ & 0 & 1 & 2 \\ \hline 0 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 2 & 0 & 0 & 2 \end{array}$

Direktes Produkt (direkte Gruppe)

$\langle \times_{i=1}^{n} G_i; * \rangle$

$(a_1, \dots, a_n) * (b_1, \dots, b_n) = (a_1 *_1 b_1, \dots, a_n *_n b_n)$

Neutr. $\langle e_1, e_2, \dots \rangle$ $\quad$ Inv. $\langle \hat{a}_1, \hat{a}_2, \dots, \hat{a}_n \rangle$

$\gcd(m, n) = 1 \Rightarrow \mathbb{Z}_{mn}^* \cong \mathbb{Z}_m^* \times \mathbb{Z}_n^*$ da teilerfremd!

Homomorphismen

$\langle G; \circ, ^{-1}, e_G \rangle$ $\quad \langle H; *, ^{\wedge}, e_H \rangle$

$\varphi(a \circ b) = \varphi(a) * \varphi(b)$ $\quad$ Allgemein: $\mathbb{Z}_{12,6} \mapsto \mathbb{Z}_{20} \times \mathbb{Z}_2$ $\quad \mathbb{Z} \to \mathbb{Z}_3$, $a \mapsto R_3(a)$

(5.5i) $\varphi(e_G) = e_H$ $\quad \varphi(e_G) = \varphi(e_G \circ e_G) = \varphi(e_G) * \varphi(e_G)$

$a * a = a \Rightarrow a = e_H$ $\quad$ Nicht erforderlich!

(5.5ii) $\varphi(\hat{a}) = \widehat{\varphi(a)}$ $\quad \varphi(a) * \varphi(\hat{a}) = \varphi(a \circ \hat{a}) = \varphi(e_G) = e_H$

Isomorphism: $\forall h \in H \ \exists! g \in G \ (\varphi(g) = h)$

Proving:

(i) Infinite cyclic $\cong \langle \mathbb{Z}; + \rangle$

$\vdash x: \mathbb{R} \setminus \{0\} \mapsto \mathbb{R}^+$

$\log(x \cdot y) \mapsto \log(x) + \log(y)$

Mit Inverse

$e^x \cdot e^y = e^{x+y}$

(ii) $\gcd(m, n) = 1 \Leftrightarrow \mathbb{Z}_{m \cdot n} \cong \mathbb{Z}_m \times \mathbb{Z}_n$

$\varphi(a, b) = \begin{cases} a \equiv_m x \\ a \equiv_n x \end{cases}$ $\quad 1 \equiv_m x$, $1 \equiv_n x$ only 1 solution

(iii) $\gcd(m, n) = 1 \Leftrightarrow \mathbb{Z}_{m \cdot n}^* \cong \mathbb{Z}_m^* \times \mathbb{Z}_n^*$

$f(x) = (R_m(x), R_n(x))$

(iv) $\mathrm{ord}(G) = n \wedge$ zyklisch $\Leftrightarrow G \cong \langle \mathbb{Z}_n, \oplus \rangle$

(v) n prim $\cong \langle \mathbb{Z}_n \setminus \{0\}; \cdot \rangle$ $\quad \mathbb{Z}_{p^k}$ & $\mathbb{Z}_{2^k}$ $\quad \mathbb{Z}_m \times \mathbb{Z}_n$

$\hookrightarrow \langle a \rangle = \{a^0, \dots, a^{n-1}\}$

$|\langle a \rangle| = n$, also gibt (Element mit größter Ordnung $\mathrm{lcm}(m, n)$)

Disproving:

(i) Not same order

(ii) One commutative, other not

(iii) # Selbstinversen

$\varphi: i \to g^i$, da $i \oplus j \to g^{i \oplus j} = g^i \cdot g^j$

Untergruppe $H \subseteq G$ $(G;\circ,{}^{-1},e) \leq (H;\circ,{}^{-1},e)$

Triviale $\{e\}$ und G

(i) $a \circ b \in H$ (reicht für endliche Gruppen, sonst zeige Neutr. & Inv.)

Disprove: Neutr. Element muss vorhanden sein.

Multiplikative Notation: $a^0 = e$ ($n=0$); $a^n = a \cdot a^{-1}$ ($n>0$); $a^n = (a^{-1})^{|n|}$ ($n<0$)

Ordnung & Begriffe $\mathrm{ord}(G) = |G|$, $\mathrm{ord}(a) = \min_{m \geq 1} a^m = e$, sonst ∞ nur bei ∞-Group

Endliche Gruppen: $a^m = a^{R_{\mathrm{ord}(a)}(m)}$

$\langle a \rangle := \{a^n \mid n \in \mathbb{Z}\}$ ist immer Untergruppe von G.

$\langle g \rangle = G$, dann ist g Generator und G zyklisch.

5.8 Lagrange $H \subseteq G \Rightarrow |H|$ teilt $|G|$

↳ 5.9 $\mathrm{ord}(a) \mid G$

↳ 5.10 $a^{|G|} = e$. Beweis: $a^{|G|} = a^{k \cdot \mathrm{ord}(a)} = (a^{\mathrm{ord}(a)})^k = e^k = e$

↳ 5.11 Jede Gruppe $|G|$ prim ist zyklisch. Beweis: $\langle a \rangle \mid p \Rightarrow \mathrm{ord}(a) = 1 \Rightarrow a = e$, $\mathrm{ord}(a) = p$

Technik Generator: Finden mit $g^{|G|-1} \neq e$ und dann:

g^k Generator $\Leftrightarrow \gcd(k, \mathrm{ord}(G)) = 1$

$\mathbb{Z}_m^* := \{a \in \mathbb{Z}_m \mid \gcd(a,m) = 1\}$ z.B. $\mathbb{Z}_{15}^* = \{1,2,4,7,8,11,13,14\}$

$\varphi(m) = \mathrm{ord}(\mathbb{Z}_m^*)$; $m = \prod_{i=1}^{r} p_i^{e_i} \Rightarrow \varphi(m) = \prod_{i=1}^{r} (p_i - 1) p_i^{e_i - 1}$

5.14 $m \geq 2 \wedge \gcd(a,m) = 1 \Rightarrow a^{\varphi(m)} \equiv_m 1$

5.15 $\boxed{\mathbb{Z}_m^*}$ zyklisch $\Leftrightarrow m = 2, m = 4, m = p^e, m = 2p^e$ $e \geq 1$, $p \geq 3$ prim

Ring $\langle R; +, -, 0, \cdot, 1 \rangle$

Bsp.: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$; $\langle \mathbb{Z}_m; \oplus, \ominus, 0, \odot, 1 \rangle$

(Ri) $\langle R; +, -, 0 \rangle$ kommutative Gruppe. $(1+1)(x+y) = ((1+1)x + (1+1)y = -x+y$; $1(x+y)+1(x+y) = \ldots y+x$

(Rii) $\langle R; \cdot, 1 \rangle$ Monoid (Ass./Neutr.)

(Riii) $a \cdot (b+c) = a \cdot b + a \cdot c \wedge (b+c) \cdot a = b \cdot a + c \cdot a$ $(\forall a,b,c \in R)$

Kommutativer Ring $\Leftrightarrow a \cdot b = b \cdot a$

5.17

(i) $0 \cdot a = a \cdot 0 = 0$ | $0 \overset{G3}{=} -(a \cdot 0) + (a \cdot 0) \overset{G2}{=} -(a \cdot 0) + a \cdot (0+0) \overset{dist.}{=} -(a \cdot 0) + (a \cdot 0 + a \cdot 0) \overset{G1}{=} (-(a \cdot 0) + a \cdot 0) + a \cdot 0 \overset{G3}{=} 0 + a \cdot 0 \overset{G2}{=} a \cdot 0$

(*) $-a = (-1) \cdot a = a \cdot (-1)$ | $(-1)a + a = (-1) \cdot a + 1 \cdot a \overset{dist.}{=} ((-1)+1) \cdot a = 0 \cdot a \overset{5.17i}{=} 0 \overset{\text{eind. Inv.}}{\Rightarrow} -a = (-1)a$

(ii) $(-a)b = -ab = a(-b)$ | $(-a)b + ab \overset{dist.}{=} (-a+a)b = 0b = 0 \overset{5.17i}{\Rightarrow} (-a)b = -ab$

(iii) $(-a)(-b) = ab$ | $(-a)(-b) + (-ab) \overset{ii}{=} (-a)(-b) + (-a)b = (-a)(-b+b) = (-a)0 = 0 \overset{\text{Eind. Inverse}}{\Rightarrow} (-a)(-b) = ab$

(iv) $1 \neq 0$ | $a = a \cdot 1 = a \cdot 0 = 0$

ausser triv. Ring $\forall a (a = 0)$

Endlich 0, Nullteiler oder Einheit: Injektive Funktion: $x \mapsto ax$

Nichtinjektiv: $\exists b \exists c\, (b \neq c) \wedge ab = ac \Rightarrow a(b-c) = 0 \Rightarrow a$ Nullteiler. $\exists b (ab = 1)$

Charakteristik $k(R) := \mathrm{ord}(1)$ in Gruppe (additive) $\langle R; +, -, 0 \rangle$

ABER für $|R| = \infty$, z.B. charakteristik $(\mathbb{Z}) = 0$.

Charakteristik $\langle \mathbb{Z}_m; \oplus, \ominus, 0, \odot, 1 \rangle = m$

Teiler $a \mid b \Leftrightarrow \exists c\, (b = a \cdot c)$ ← Muss KOMMUTATIV sein! a Teiler, b Vielfaches

(i) $a \mid b \wedge b \mid c \Rightarrow a \mid c$ (trans.)

(ii) $\forall c\; a \mid b \rightarrow a \mid c \cdot b$

(iii) $a \mid b \wedge a \mid c \Rightarrow a \mid (b \pm c)$

↑S.18

Nullteiler

kommutativ!

kom. Ring $a \neq 0$ Nullteiler $\Leftrightarrow \exists b \neq 0\; a \cdot b = 0$

bei $\mathbb{Z}_n$ sind Faktoren (und dessen mult.) Nullteiler.

Einheit

kom. Ring u Einheit $\Leftrightarrow \exists v\, (u \cdot v = 1 = v \cdot u)$

= invertierbar

Einheitmenge $(\mathbb{Z}) = \mathbb{Z}^* = \{-1, 1\}$; $\mathbb{R}^* = \mathbb{R} - \{0\}$

Einheitmenge $(\mathbb{Z}_m) = \mathbb{Z}_m^*$ Gaussz. Zahlen: $1, i, -1, -i$

5.19 $\langle R^*; \cdot, 1, {}^{-1} \rangle$ Multiplikative Gruppe

Beweis: $u \cdot v \in R^*$, also hat $u \cdot v$ Inverse. Rest folgt von mult. Monoid.

Integritätsbereich

Kommutativer nichttrivialer Ring

$\forall a \forall b\, (a \cdot b = 0 \rightarrow a = 0 \vee b = 0)$

hat keine Nullteiler!

z.B.: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ und ($\mathbb{Z}_p$ wo p prim!) NICHT $\mathbb{Z}_m$

5.20 Quotient ist unik: $a \mid b \Rightarrow \frac{b}{a} = c$

Proof: $b = a \cdot c = a \cdot c' \Rightarrow ac - ac' \overset{dist.}{=} a \cdot (c - c') = 0$. $P\, a \neq 0$: $c = c'$

Polynomringe

$a(x) = a_d \cdot x^d + a_{d-1} \cdot x^{d-1} + \ldots + a_1 \cdot x + a_0 = \sum_{i=0}^{d} a_i \cdot x^i \in R[x]$

$\mathrm{Grad}(a(x)) = d$

$a(x) + b(x) = \sum_{i=0}^{\max(d,d')} (a_i + b_i) \cdot x^i$ + Neutr. Elem. $(\forall i)\, a_i = 0$; + Inv. Elem $a_i = \widehat{a_i}$

$a(x) \cdot b(x) = \sum_{i=0}^{d+d'} \left(\sum_{k=0}^{i} a_k \cdot b_{i-k} \right) \cdot x^i$ • Neutr. Element $(\forall i)\, a_i = 1$

5.21 R Ring $\Rightarrow R[x]$ Ring

Assoziativität Mult. Monoid: $(a(x)b(x))c(x) = \sum_{i=0}^{d+d'+d''} \left(\sum_{j=0}^{i} \left(\sum_{k+l=j} a_k b_l \right) c_{i-j} \right) x^i = \sum \ldots$

5.22 i) D Integritätsbereich $\Rightarrow D[x]$ Integritätsbereich (easy)

ii) $D^* = D[x]^* \rightsquigarrow$ also nur Polynome 0-ten Grades!

⊗ $\deg(a(x)b(x)) = \deg(a(x)) + \deg(b(x))$ Wenn Ring $a_n \cdot b_n \neq 0$

Körper

nicht-trivialer kommutativer Ring, wo jedes (nichtnull) Element invertierbar ist

(bzw. Einheit ist) (also $F^* = F - \{0\}$) $\Leftrightarrow \langle F - \{0\}; \cdot, {}^{-1}, 1 \rangle$ abelsch ist!

Endliche Körper unik $\mathrm{ord}(p^n)$, wo n prim. Sonst $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ in endlichen zyklisch.

5.23 $\mathrm{ord}(F) = p$ prim $\Leftrightarrow F = \mathbb{Z}_p = GF(p)$

(i) Polynomring $R[x]$ und $\mathbb{Z}$ sind keine Körper ⊗

5.24 F Körper $\Rightarrow F$ Integritätsbereich. Einheit $\neq$ Nullteiler: $u \cdot v = 0$; $v = 1 \cdot v = u^{-1} u v = u^{-1} 0 = 0$ ↯

5.25 F Integritätsbereich $\wedge F$ endlich $\Rightarrow F$ Körper

Assume: $d \in D - \{0\} \wedge d$ keine Einheit $\Rightarrow (d) := \{d \cdot a \mid a \in D\}$, dann $1 \notin (d)$ und $|(d)| < |D|$

Also $\exists a \exists b\; a \neq b \wedge d \cdot a = d \cdot b$ (Schubfach). $d \cdot (a-b) = 0$ und $a - b \neq 0$ ↯

$GF(p^l)$ ist Unterkörper von $GF(p^d) \Leftrightarrow l \mid d$

LGS

⇝ Schreibweise: $\mathbb{Z}_{10}$ $(-10, 0, 10, 20, \ldots)$

$$\left[\begin{array}{ccc|c} 10 & 2 & 5 & 1 \\ 7 & 4 & 6 & 2 \\ 3 & 6 & 9 & 4 \end{array}\right] \quad \oplus 10$$

Eingang	0	1	2	3	4	5	6	7	8	9	10
⊙	x	1	6	4	3	9	2	8	7	5	10
⊖	0	10	9	8	7	6	5	4	3	2	1

$$\begin{array}{c} \left[\begin{array}{ccc|c} 1 & 9 & 6 & 10 \\ 7 & 4 & 6 & 2 \\ 3 & 6 & 9 & 4 \end{array}\right] \\ \ominus 7 \quad \ominus 3 \end{array} \sim \left[\begin{array}{ccc|c} 1 & 9 & 6 & 10 \\ 0 & 1 & 2 & 7 \\ 0 & 7 & 8 & 9 \end{array}\right]$$

$2te - 7 \times erste = 2te + 3 \times erste$

$$\left[\begin{array}{ccc|c} 1 & 9 & 0 & 3 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 3 \end{array}\right] \ominus 9 = 2 \rightsquigarrow \left[\begin{array}{ccc|c} 1 & 0 & 0 & 5 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 3 \end{array}\right]$$

Polynomring über Körper

Monisches Polynom: $:\equiv 1$ als vorderster Koeffizient

$b(x) \mid a(x) \Rightarrow \forall_{c \neq 0}\, b(x) \mid a(x)$ // Nullteiler!!

Irreduzierbar $a(x) \in F[x]$ heisst irreduzierbar $\Leftrightarrow$

$\forall b(x)\; b(x) \mid a(x) \rightarrow b(x)$ constant oder Vielfaches von $a(x)$.

Technik für irreduzierbar: Alle monische Polynome $\leq \lfloor \frac{d}{2} \rfloor$

z.B. $x^2 + 2$ irreduzierbar $GF(5)$ $x + \alpha$ testen.

$GF(p) :\equiv$ endlicher (unik) Körper von Grösse p prim $:\equiv \mathbb{Z}_p$

$GF(p)[x] :\equiv \mathbb{Z}_p[x]$

Reduzierbar in $GF(p)[x] \rightsquigarrow$ Nullteiler für $[1,3]$

$a(x) = x^4 + 2x^3 + 2x^2 + 2$ in $GF(3)[x]$

$[1,3]$ $[2,2]$

Teste 2: $x^4 + 2x^3 + 2x^2 + 2$ $(x^2 + ax + b)(x^2 + cx + d)$

2 | 2

1 | 4

2 | 8

1 | 16

$1 + 2 \cdot 2 + 2 \cdot 1 + 2 = 0$

Auskesten!

$(x-2) \Leftrightarrow (x+1) \mid a(x)$

Quotient: $\exists!\, q(x), r(x)$ $(a(x) = b(x) \cdot q(x) + r(x)$

$r(x) = R_{b(x)}(a(x))$ $\deg(r(x)) < \deg(b(x))$

$GCD(3x^3 + 4x^2 + 3x + 4,\; 3x^3 + 4x^2 + 3)$ in $GF(5)[x]$

$3x^3 + 4x^2 + 3x + 4 : 3x^3 + 4x^2 + 3 = 1\; R\; 3x + 1$

$\ominus 3x^2 \ominus 4x^2$ $\ominus 3$

$0x^2 + 0x^2 + 3x + 1$

$3x^3 + 4x^2 + 3 : 3x + 1 = 1x^2 + 1x + 3\; R\; 0$ ($3 = 2$)

$\ominus 3x^3 \ominus x^2$

$3x^2 + 3$

$\ominus 3x^2 \ominus x$

$4x + 3$

$\ominus 4x \ominus 3$

0

$3x + 1$ ist ein GCD, aber monisch: $2 \cdot (3x+1) = x + 2$

(*) $R[x]^* = \{a_0 + a_1 x + \ldots + a_n x \mid a_0 \in R^* \wedge \forall i \exists n\, a_i^n = 0\}$

$GF(p)[x]^*$ = Konstante Polynome mit $a_0 \in GF(p)^*$

Polynome als Funktionen (nicht unbedingt Körper)

Evaluationsfunktion: $\alpha \mapsto a(\alpha)$; $a(x) \in R[x]$

Wurzel $:\equiv \alpha \in R$, wo $a(\alpha)=0$ ↳ für $F[x]$

(5.29) $\alpha \in$ Körper $\Leftrightarrow (x-\alpha) \mid a(x)$ $\quad a(x)=(x-\alpha)\cdot q(x)+r(x)$

($\Rightarrow$) Annahme α Wurzel: $\deg(r(x)) < 1 = \deg(x-\alpha) \Rightarrow r$ constant.
$x=\alpha \Rightarrow r = a(\alpha)-(\alpha-\alpha)q(\alpha) = 0-0\cdot q(\alpha) = \underline{0}$

($\Leftarrow$) Annahme: $(x-\alpha) \mid a(x) \Rightarrow a(x)=(x-\alpha)\cdot q(x) \overset{x=\alpha}{\Rightarrow} a(\alpha)=(\alpha-\alpha)\cdot q(\alpha)=0$

$\Rightarrow$ In $F[x]$ (F Körper) irreduzibles Polynom Grad $\geq 2 \Rightarrow$ keine Wurzel
↳ 5.30 Falls Polynom $\in F[x]$ Grad $2,3$ ^ keine Wurzel $\Rightarrow$ irred.

Vielfachheit (alg.) $=$ multiplicity$(\alpha) :\equiv \max_n (x-\alpha)^n \mid a(x)$

(5.31) Nicht-null Polynom von Integritätsbereich von Grad d hat höchst. d Wurzel.
Beweis: Nicht-null Polynom von Grad d hat keine Wurzel: $a(x)=(x-\alpha)^t q(x)$
$q(x)$ darf nur $d-t$ Wurzeln haben (B). $a(x)=(B-\alpha)^t q(B)$
Aber $a(x)$ muss Grad d haben, also $\xrightarrow{\neq 0} d = t + \underline{(d-t)}$ i.H. auf $q(x)$

Polynominterpolation (jedes Pol. von Grad d kann durch $d+1$ Werte berech. werden)

Gegeben:
$B_i := a(\alpha_i)$. $\quad a(x)=\sum_{i=1}^{d+1} B_i \cdot U_i(x)$ → nach Lagrange

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

Beweis: $U_i(\alpha_i)=1$ und $U_i(\alpha_j)=0$. $i \neq j$ Uniqueness: $a(x)$ hat Grad d. Es hat also max. d Nullstellen (ausser es ist 0)!
$a(x)-a'(x)$ hat $d+1$ Nullstellen: $a(x)-a'(x)=0 \Rightarrow$ ...

$a(x)=(x-2)^2 b(x)$ über $GF(7)[x]$:
$a(4)=3=(\underbrace{4-2}_{a\cdot 2})^2 b(4) \Rightarrow \underline{b(4)=6}$ $\quad \underline{b(3)=2}$ $\quad \underline{b(6)=6}$ → B_3

$$U_1(x)=\frac{(x-3)(x-6)}{(4-3)(4-6)} = \frac{x^2-9x+18}{-2=5} = (x^2+5x+4)(3=\hat{5}) = 3x^2+x+5$$

$F[x]_{m(x)} :\equiv \{a(x) \in F[x] \mid \deg(a(x)) < d\}$
$a(x) \equiv_{m(x)} b(x) :\Leftrightarrow m(x) \mid (a(x)-b(x))$ $\cdot \Leftrightarrow m(x) \mid (a(x)-b(x))$
neutr. 0 inv. $-a(x)$

5.34 $\mathrm{ord}(F)=q \Rightarrow |F[x]_{m(x)}| = q^d$ $\quad$ entweder 0, Nullteiler oder Einheit.

5.36 $a(x)\,b(x) \equiv_{m(x)} 1$ ⇝ $b(x)$ ist eind! Bzw.:
$F[x]^*_{m(x)} = \{a(x) \in F[x]_{m(x)} \mid \gcd(a(x), m(x)) = 1\}$
→ ineffizient, raten!
$m(x)$ irreduzibel $\Rightarrow F[x]^*_{m(x)} = F[x]_{m(x)} - \{0\}$
Z.B. $m(x)=x^2+1$: Inverse von x: $x\cdot(ax+b)=t(x^2+1)$ $\quad$ $x\cdot(ax+b)=t(x^2+1)$
$a=t$, $b=0$, $0=2t=1$ ↳ da Grad 1! $\Rightarrow x\cdot x \equiv_{m(x)} 1$
Brute-force!

5.38 $F[x]_{m(x)}$ Körper $\Leftrightarrow m(x)$ irreduzibel

$\mathbb{R}[x]_{m(x)} \cong \mathbb{R}[x]_{x^2+1} \cong \mathbb{C}$ (→ Kgr. rel.)

$GF(p^d) \cong GF(p)[x]_{m(x)}$, wo $m(x)$ irred. und Grad d hat!
$m(x)$ finden, versuche x^n+ax+b

Fast multiplikativ inverse $\quad a x \equiv_m 1$
wegen 5.14 $\gcd(a,m)=1 \Rightarrow a^{\varphi(m)} \equiv_m 1 \Rightarrow a^{\varphi(m)+1} \equiv_m a^{-1}$ Falls m prim a^{m-2}
Key fast: $R_{11}(5^{772}) \Rightarrow \varphi(11)=10$ $R_{11}(5^{10})=1 \Rightarrow R_{11}((5^{10})^{77}\cdot 5^2) = \underline{3}$

(k,n)-error collecting codes

$R_{33}(a^b) < \begin{cases} x \equiv_5 R_5(a^b) \\ x \equiv_7 R_7(a^b) \end{cases}$

$\mathcal{A}$ = alphabet, k = Grösse der verschl. Nachrit. n = Grösse der unverschl.

Kodierung: $E: \mathcal{A}^k \mapsto \mathcal{A}^n$
Dekodierung $D: \mathcal{A}^n \mapsto \mathcal{A}^k$
Hamming Distanz $:\equiv$ # unterschi. Elemente in einer Sequenz.

$|A| = q$, und somit q^k Codewörter

d = Max. Abstand zwischen 2 Codewörter $E(a_i)$ und $E(a_j)$

Reed-Solomon Codes

$\mathcal{A}^k = (a_1, a_2, \ldots, a_{k-1})$, $a_i \in F[x]$, bzw. $GF(p^q)[x]$
Eine Dekodierfunktion kann t Fehler beheben $\Leftrightarrow 2\cdot t+1 \leq d$

(5.42) $E((a_0, a_1, \ldots, a_{k-1})) = (a(\alpha_0), \ldots, a(\alpha_{n-1}))$,
$a(x) := a_{k-1}x^{k-1} + \cdots + a_1 x + a_0$

Minimale Distanz $d = n-k+1$
Und somit $t \leq \frac{n-k}{2}$.
Beweis $a(x)$ und $a'(x)$ können nicht an k Stellen gleich sein, sonst wäre $a(x)=a'(x)$.
Also unterscheiden sie sich an mind. $n-(k-1)=n-k+1$.
If a polynomial has hamming distance $\leq \frac{n-k}{2}$ of the other prime polynomial it's a keyword!

$f: P(A) \to P(A)$ $\quad \{a,b\} \mapsto \{a,b\}$ $\quad f(A \cap B)$ Gegenb. $\{1,2\} \cap \{1,3\}$
$f(x) \in f(A \cup B) \overset{x}{\Rightarrow} \exists x \in A \cup B \overset{inj}{\Rightarrow} x \in A \cap B$
$f(x) \in f(A \cap B) \overset{n}{\Rightarrow} x \in A \cap B$ Gegenb.: $\{1\},\{2\}$, $1 \mapsto 1$, $2 \mapsto 1$

Technik $a(x) \in F^*[x]_n \Leftrightarrow a_0 \neq 0$
Es muss gelten $\gcd(a(x), x^n)=1$
Notwendig: $a_0=0 \Rightarrow x \mid a(x) \wedge x \mid x^n$
Hinreichend: Teiler von x^n: $x^{n-1}, \ldots x, 1$
Also wenn $a_0 \neq 0$, gilt $\gcd(a(x), x^n)=1$

Technik Nullteiler $F[x]_{m(x)}$. Rechne: $m(x)/a(x) = q(x) + r(x)$
Falls $r(x)=0$, dann $\vee a(x)$ & $\vee q(x)$ Nullteiler
wobei $0 < \deg(a(x)) < \deg(m(x))$

$(a=5^k \cdot b \wedge b = 5^q \cdot a) \Rightarrow a = 5^{k+q} \cdot a \Rightarrow 1 = 5^{k+q} \Rightarrow k+q=0 \overset{k,q \in \mathbb{N}}{\Rightarrow} a=b$

- $x^{q-1}=1$, wo $x \in F$. Also $F^* = F - \{0\}$, $\langle a \rangle$ Untergruppe, $\mathrm{ord}(A) \mid q-1$ □
- $p(x) = xy^2+y+(x+1) \in GF(2)[x]_{x^2+x+1}[y]$. Nullteiler testen: $y \in \{0,1,x,x+1\}$
- $\varphi: G_1 \to G_2$ $\quad f(G_1)$ Untergruppen von G_2
  - $\mathrm{ord}(f(G_1))$ teilt $\mathrm{ord}(G_1)$
  - $f^{-1}(\{e\})$ Untergruppe G_1
  - $\mathrm{ord}(f(G_1))$ teilt G_2 & G_1

$\Rightarrow$ (Closure: $\varphi(a_1)=a_2$, $\varphi(a_1 \cdot b_1) \in f(G_1)$
$= \varphi(a_1)\cdot\varphi(b_1) = a_2 \cdot b_2 \in f(G_1)$

$\mathbb{Z}_m \to \mathbb{Z}_n$ $\quad$ Untergruppen von $\mathbb{Z}_n$ und $\mathbb{Z}_m$
$m=9$, $n=12$ $\quad \{0,3,6\} \mapsto \{0,4,8\}$ $\quad \{0,3,6\} \mapsto 0$, $\{1,4,7\} \mapsto 1$, $\{2,5,8\} \mapsto 2$
Kleinste Grösse Def. n

f Injektiv: $f: V \to W$
$f^{-1}(A \cap B) \overset{\text{Def. n}}{=} \{x \in V \mid f(x) \in A \cap B\} = \{x \in V \mid f(x) \in A \wedge f(x) \in B\}$
$\overset{\text{Def. n}}{=} \{x \in V \mid f(x) \in A\} \cap \{x \in V \mid f(x) \in B\} = f^{-1}(A) \cap f^{-1}(B)$

$\mathbb{Z}_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Zyklisch
Abelisch

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Abelian
Nicht-zyklisch
$\{e3\}, \{e,a\}, \{e,b\}, \{e,c\}$

Zyklisch $\Rightarrow$ abelsch: $a=g^m$, $b=g^n \Rightarrow a\cdot b = g^m \cdot g^n = g^{m+n} = g^{n+m} = b \cdot a$ $\quad R_n(i+j)$
Caley table cyclic group: $1, g, g^2, \ldots g^{i+j} = g$

$S_3 \cong D_3$ $\quad \mathbb{Z}_6$

	123	213	132	321	231	312
123	123	213	132	321	231	312
213	213	123	231	312	132	321
132	132	312	123	231	321	213
321	321	231	312	123	213	132
231	231	321	213	132	312	123
312	312	132	321	213	123	231

nicht zyklisch, nicht abelsch

312^n rotat. Ung.
$321 \cdot 312^n$ Ung.
$\mathrm{ord}(S_n)=n!$

$|G|=8$: $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $S_\square$

φ	0	1	2	3	4	5	6	7	8	9
0+		1	1	2	2	4	2	6	4	6
10+	4	10	4	12	6	8	8	16	6	18
20+	8	12	10	22	8	20	12	18	12	28
30+	8	30	16	20	16	24	12	36	18	24
40+	16	40	12	42	20	24	22	46	16	42
50+	20	32	24	52	18	40	24	36	28	58
60+	16	60	30	36	32	48	20	66	32	44
70+	24	70	24	72	36	40	36	60	24	78
80+	32	54	40	82	24	64	42	56	40	88
90+	24	72	44	60	46	72	32	96	42	60

$2016 = 1024+512+256+128+64+32$
$\varphi(2016) = 576, 1152, 1728, 2304, 2880, 3456, 4032, 4608, 5184, \ldots$

$R_{11}(5^{772}) = R_{11}((5^{10})^{77} \cdot 5^2) = \underline{3}$

$\exists b\, \forall a \in \mathbb{N}$ $210^a \equiv_b 1$

$R_{209}(210^a) = R_{209}(R_{209}(210)^a) = 1^a$

$|\langle \mathbb{Z}_m; \odot \rangle| = \varphi(m)$

$5 \cdot x \equiv_{11} 6 \Rightarrow 5 \cdot 6^{-1} x \equiv_{11} 1$
$\Rightarrow 10 x \equiv_{11} 1$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
2	1																					
3	1	2																				
5	1	3	2	4																		
7	1	4	5	2	3	6																
11	1	6	4	3	9	2	8	7	5	10												
13	1	7	9	10	8	11	2	5	3	4	6	12										
17	1	9	6	13	7	3	5	15	2	12	14	10	4	11	8	16						
19	1	10	13	5	4	6	11	12	17	2	7	8	3	15	14	6	9	18				
23	1	12	8	6	14	4	10	3	18	7	21	2	16	5	20	13	19	9	17	15	11	22

Anzahl irr. Polyn. $\Phi = |F|$ → $\frac{\Phi^p - \Phi}{p}$

$GF(3)[x]$: $2, x+1, x+2, 2x, x^2+1, x^2+x+2, x^2+2x+2, 2x^2, x^3+2x+1, 2x^3, 2x^\alpha$

4	1	x	3						
6	1	x	x	x	5				
8	1	x	3	x	5	x	7		
9	1	5	x	7	2	x	4	8	
10	1	x	7	x	x	x	3	x	9
12	1	x	x	x	5	x	7	x	x	x	11

$GF(2^3)[x] \overset{\text{nonirr.}}{=} x+\alpha$, x^2+x+2, 113, 121, 122, 131, 133

$GF(5)[x] \overset{\text{nonirr.}}{=} x+\alpha$, x^2+2, 103, 111, 112, 123, 124, (x^3+x+1)

14:3, 18:5, 19:2, 22:7, 25:13, 26:7, 27:2

$\mathbb{Z}_6 \times \mathbb{Z}_{10} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{10} \cong \mathbb{Z}_2 \times \mathbb{Z}_{30}$ $\quad \{\{t_1, t_4\}, \{t_2, t_4\}\}$ $\{t_1, t_4\}$

Cantor Theorem: $f: A \to P(A)$ nichtsurjektiv $\Leftrightarrow Z_f := \{x \in A \mid x \notin f(x)\}$ nicht im Bild!

$R^A(m,b) :\Leftrightarrow m \in f(b)$ $\quad U^A = A$; $\exists b \in A\, (\forall m \in A\, (m \in f(b) \Leftrightarrow m \notin f(b))$

Def. $\Leftrightarrow \exists b \in A\, (\forall m \in A\, (m \in f(b) \to m \notin f(b)) \wedge \forall k \in A\, (k \notin f(b) \to k \in f(b))$

$\overset{\text{Def. } Z_f \text{ und } f(b)}{\Leftrightarrow} \exists b \in A\, (\forall m \in A\, m \in Z_f \wedge \forall k \in A\, k \in f(b)) \overset{\text{Def. } \subseteq}{\Leftrightarrow} \exists b \in A\, (f(b) \subseteq Z_f \wedge (Z_f \subseteq f(b))$

$\Leftrightarrow \exists b \in A\, (Z_f = f(b)) \Leftrightarrow Z_f \in P(A)$ aber nicht $Z_f \in f(A)$. Wenn keine surjektive Funktion existiert $f: A \to P(A)$, dann keine injektive.