1. Mengenlehre:

$\emptyset \subseteq M$, $\emptyset \notin M$, $A=\{1,\{2\}\} \to 1 \in A$, $\{1\} \subseteq A$, $\{2\} \in A$

$A \subseteq B :\Leftrightarrow \forall x (x \in A \to x \in B)$

$A=\{a,b\}$, Potenzmenge $P(A)=\{\emptyset,\{a\},\{b\},\{a,b\}\} = \{\{a\},\{b\}\}$

Def. 3.5: $P(A)=\{S \mid S \subseteq A\}$, $B=\emptyset$, $P(B)=\{\emptyset\}$, $\{\emptyset,\{\emptyset\}\}$, $P(P(B))=\{\emptyset,\ldots\}$

Def 3.6 + Theorem 3.4 + Lemmas:

$A \cap B := \{x \mid x \in A \wedge x \in B\}$ — $A \cup B := \{x \mid x \in A \vee x \in B\}$

$A \setminus B := \{x \mid x \in A \wedge x \notin B\}$ — $A \Delta B := \{x \mid x \in A \text{ XOR } x \in B\}$

$P(A)=2^A$: $x \in P(A) \Leftrightarrow x \subseteq A$ — $|P(A)| = 2^{|A|}$

$\bar{A} := \{x \mid x \in U \wedge x \notin A\}$ — $\bar{A} = U \setminus A$

Idempotenz	$A \cap A = A \cup A = A$
Kommutativität	$A \cap B = B \cap A$, $A \cup B = B \cup A$
Assoziativität	$A \cap (B \cap C) = (A \cap B) \cap C$ analog $\cup$
Absorption	$A \cap (A \cup B) = A = A \cup (A \cap B)$
Komplement	$A \cap \bar{A} = \emptyset$, $A \cup \bar{A} = U = I$
Konsistenz	$A \cap B = A \Leftrightarrow A \subseteq B \Leftrightarrow A \cup B = B$
Distributivität	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ analog $\cup, \cap$
Dominierender Wert	$X \cap \emptyset = \emptyset$, $X \cup I = I$ $I=U$
Neutraler Wert	$X \cap I = X$, $X \cup \emptyset = X$ $I=U$

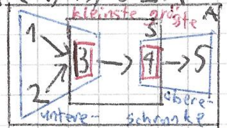
$(a,b) = \{\{a\},\{a,b\}\}$ Geordnetes Paar; falls $a=b \Rightarrow \{\{a\},\{a,a\}\} = \{\{a\}\}$

Poset: $P(M,R)$, M=Menge R=Relation z.B. $M=\mathbb{N}$, $R=\leq$ oder $|$

↳ falls alle Elemente vergleichbar: total geordnet

↳ $P(A,\preceq)$ b überdeckt a: $a \preceq b \wedge \nexists c\,(a \preceq c \wedge c \preceq b)$

$P(A,\preceq)$, $S \subseteq A$



$a \in S$ minimales Element v. S falls: $\neg\exists b\,(b \in S \wedge b \preceq a)$ 0 oder 1 mal

$a \in S$ kleinstes Element v. S falls: $a \preceq b \;\forall b \in S$ 0, 1 oder n mal

$a \in A$ untere Schranke v. S falls $a \preceq b \;\forall b \in S$, grösste untere Schranke $\neg\exists b \in A \mid a \preceq b \wedge b \preceq c \;\forall c \in S$

Gleichheit v. A und B: $\forall x \in A \to x \in B \wedge \forall x \in B \to x \in A$

Disjunkte Mengen: $\forall x \in A \to x \notin B \wedge \forall x \in B \to x \notin A$

Mengen gleichmächtig, falls elemente aus A eindeutig elementen aus B zugeordnet werden können. überabzählbar: $\mathbb{R}$, $P(\mathbb{N})$, $\{0,1\}^\infty$

↳ Abzählbarkeit: $A \sim \mathbb{N}$ oder $A \leq \mathbb{N}$, A, B abzählbar $\to A \times B$ abzählbar

$\mathbb{N} \times \mathbb{N}$ abzählbar, $\{0,1\}^*$ abzählbar, $\{0,1\}^\infty$ nicht abzählbar.

Peano Axiome: 1. $0 \in \mathbb{N}$, 2. nachfolger n' v. n ist ebenfalls in $\mathbb{N}$ 3. $n \in \mathbb{N} \to (n' \in \mathbb{N} \wedge n \neq 0)$, 4. genau einen Nachfolger $(n'=m') \to (n=m)$ 5. $0 \in X \wedge \forall n \in X (n \in X \to n' \in X) \to \mathbb{N} \subseteq X$ Induktionsaxiom

2. Relationen:

$1 \to_\rho^2$, $\rho=\{(1,2)\}$, $\rho^2=\{\}$; $\rho=\{(1,2),(2,2)\} = \rho^2 = \rho^n = \rho^*$

$A \rho \sigma C \Leftrightarrow a \rho \sigma c \Leftrightarrow \exists b\,(a \rho b \wedge b \sigma c)$ $a \in A, b \in B, c \in C$

Eigenschaft	Definition	Menge	Graph
reflexiv	$\forall a\; a \rho a$	$id \subseteq \rho$	
irreflexiv	$\forall a\; a \not\rho a \Leftrightarrow \forall a\; \neg(a \rho a)$	$id \cap \rho = \emptyset$	
symetrisch	$\forall a \forall b\; a \rho b \Leftrightarrow b \rho a$	$\rho = \hat{\rho}$	
antisymetrisch	$\forall a \forall b\; a \rho b \wedge b \rho a \to a=b$	$\rho \cap \hat{\rho} \subseteq id$	$a<b \to \emptyset$, $a \leq b \wedge a=b \to id$
transitiv	$\forall a \forall b \forall c\; a \rho b \wedge b \rho c \to a \rho c$	$\rho^2 \subseteq \rho$	

Reflexiv: $\leq, \geq, |$ in $\mathbb{Z}$, Irreflexiv: $<, >$

Symetrisch: $\equiv_m$ in $\mathbb{Z}$, Antisymetrisch: $\leq, \geq$, ($|$ in $\mathbb{N}$)

Transitiv: $\leq, \geq, <, >, |, \equiv_m$ in $\mathbb{Z}$, $=$

Transitive Hülle: $\rho^* := \bigcup_{n=1}^{\infty} \rho^n$ (Symetrisch = selbstinvers)

2. Relationen:

Komposition: $R \subseteq A \times B$, $Q \subseteq B \times C \to R \circ Q \subseteq A \times C$

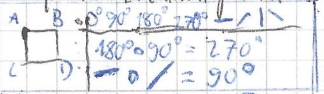
$(a,c) \in R \circ Q \leftrightarrow \exists b \in B: (a,b) \in R \wedge (b,c) \in Q$

Äquivalenzrelation: symetrisch, transitiv, reflexiv

Ordnungsrelation: reflexiv, antisymetrisch, transitiv

Partition: Disjunkte unterteilung in Untermengen $\bigcup_{i=1} A_i = A$

Äquivalenzrelation partitioniert Mengen in Äquivalenzklassen $[a] = \{b \mid b \sim a\}$



$180° \circ 90° = 270°$, $- \circ / = 90°$

Teilbarkeit: $a \mid b \Rightarrow \exists c\,(b = a \cdot c)$

eindeutig: $b = ac = ac'$, $c \neq c'$, $a \neq 0$

$ac + (a \cdot (-c)) = 0$, $ac + a(-c') = 0$, $a(c + (-c')) = 0$

Relation $f \subseteq A \times B$ funktional $(f: A \to B)$ falls: $0 \; e = c \; \xi$

$\forall a \in A \; \exists b \in B: (a,b) \in f$ $\quad ((a,b) \in f \wedge (a,b') \in f) \to b = b'$

Schreibweise: $(a,b) \in f$, $f(a) = b$, $f: a \to b$

f injektiv: $a \neq a' \to f(a) \neq f(a') \Leftrightarrow |A| \leq |B|$ — f bijektiv: f surjektiv $\wedge$ f injektiv

f surjektiv: $\forall b \; \exists a: f(a) = b \Leftrightarrow |A| \geq |B|$

$f: A \to B$, $g: B \to C \Rightarrow g \circ f = gf \Rightarrow (g \circ f)(a) = g(f(a))$

Brüche: $[(a,b)] \cdot [(c,d)] := [(ac, bd)]$ $(a,b) \sim (a',b') \to ab' = ba'$

Addition: $0 := \emptyset$, $1 := \{\emptyset\}$, $2 := \{\emptyset, \{\emptyset\}\}$ $\quad s(n+1) = s(n) \cup \{s(n)\}$

3. Modulo:

$a = dq + r$, $0 \leq r < |d|$

$a \equiv_m b \Leftrightarrow a - b = k \cdot m$, $k \in \mathbb{Z}$

$+, -, \cdot$: $(a+b) \bmod m = (a \bmod m + b \bmod m) \bmod m$

$a \cdot c \equiv_m b \cdot c$ und $\operatorname{ggT}(c,m) = 1$ $\to a \equiv_m b$

Speziell: $R_9(a^b) = R_9(a^{b \bmod \operatorname{ord}(b)})$

2: 1 falls ungerade, sonst 0

3: gleich quersumme mod 3

5: gleich letzter Ziffer mod 5

9: gleich quersumme mod 9

10: gleich letzter Ziffer

$p \nmid a \Rightarrow a^{p-1} \equiv_p 1$

S. v. Fermat (1): $a^p \equiv_p a \Leftrightarrow a^{p-1} \equiv_p 1$, $a \neq p$, p prime

(2): $R_p(a^b) = R_p(R_p(a)^{R_{p-1}(b)})$

$-1 \pmod x$ = selbstinvers; $5 \equiv_6 -1 \to 5 \cdot 5 \equiv_6 1$

$R_{10}(3^{160}) = R_{10}(3^{2 \cdot 80}) = R_{10}(9^{80}) = R_{10}(-1^{80}) = 1$

$R_8(3^{161}) = R_8(3 \cdot 3^{160}) = R_8(3 \cdot (3^4)^{40}) = R_8(3 \cdot 1^{40}) = 3$

$R_5(2007^{2007}) = R_5(2^{2007}) = R_5(2^3 \cdot 2^{2004}) = R_5(8 \cdot (2^4)^{501}) = R_5(3 \cdot 1) = 3$

$x \equiv_{22} a \to x \equiv_2 R_2(a) \wedge x \equiv_{11} R_{11}(a)$

$\mathbb{Z}_m = \{[0],[1],\ldots,[m-1]\}$ $a + b \in [a+b]$, $a \cdot b \in [a \cdot b]$ $a \dotplus b \equiv_m a + b$

$\forall a \in [a], \exists b \in [b]: a + b \in [0]$ Es existiert additive Inverse

$\exists x: [a] \cdot [x] = [1] \Leftrightarrow \operatorname{ggT}(a,m) = 1$ teilweise multiplikative Inverse

↳ berechnung via EEA: $\operatorname{ggT}(a,m) = 1 \to ua + vm \to u = a^{-1} \bmod m$

$\mathbb{Z}_m^* = \{[a] \mid \operatorname{ggT}(a,m) = 1\}$, $|\mathbb{Z}_m^*| = \varphi(m) \to$ falls m prime: $p - 1$

$a \equiv_m b \Leftrightarrow a = tm + b \Leftrightarrow m \mid (b - a) \Leftrightarrow R_m(a) = R_m(b)$

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

Euler: $\operatorname{ggT}(a,n) = 1 \Rightarrow R_n(a^{\varphi(n)}) = 1$, $R_n(a^b) = R_n(a^{R_{\varphi(n)}(b)})$

Eulersche phi Funktion $\varphi(n)$: $a^e \equiv 2 \bmod m$

$\varphi(n) = \{x \in \mathbb{N} \mid 1 \leq x \leq n \wedge \operatorname{ggT}(x,m) = 1\}$, $\varphi(p) = p - 1$

p, q prime: $\varphi(p \cdot q) = (p-1) \cdot (q-1)$, $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n) \to \varphi(18) = \varphi(9) \cdot \varphi(2)$ teilerfremd

$\operatorname{ggT}(a,m) = 1 \to m \mid a^{\varphi(m)} - 1 \Leftrightarrow \operatorname{ggT}(a,m) = 1 \Rightarrow a^{\varphi(m)} \equiv_m 1$

$a \in \mathbb{N}$, s_a = Quersumme v. a $\quad R_9(a) = R_9(s_a)$ (Zahl 9)

$a = \sum a_i \cdot 10^i$, $s_a = \sum a_i$, $R_9(a) = R_9(\sum(a_i \cdot 10^i)) =$

$R_9(\sum R_9(a_i) \cdot \underbrace{R_9(10^i)}_{1}) = R_9(\sum R_9(a_i)) = R_9(\sum a_i) = R_9(s_a)$ $\square$

4. Erweiterter Euklidischer Algorithmus, EEA

$\operatorname{ggT}(a,b) = ua + vb$, $a = qb + r$

$s_1 = a$, $s_2 = b$, $u_1 = 1$, $u_2 = 0$, $v_1 = 0$, $v_2 = 1$

while $s_2 > 0$

$\quad q = s_1 \operatorname{div} s_2$, $r = s_1 - s_2 q$, $s_1 = s_2$, $s_2 = r$

$\quad t = u_2$, $u_2 = u_1 - q u_2$, $u_1 = t$

$\quad t = v_2$, $v_2 = v_1 - q v_2$, $v_1 = t$

$d = s_1$, $u = u_1$, $v = v_1$, $d = \operatorname{ggT}(a,b) = ua + vb$

s_1	s_2	u_1	u_2	v_1	v_2	q
327	28	1	0	0	1	11
28	19	0	1	1	-11	1
19	9	1	-1	-11	12	2
9	1	-1	3	12	-35	9
1	0	3	-28	-35	327	

$\operatorname{ggT}(327,28) = 1 = 3 \cdot 327 + (-35) \cdot 28 = u \cdot a + v \cdot b$

GGT: $d \mid a \wedge d \mid b \wedge \forall c\,((c \mid a \wedge c \mid b) \to c \mid d)$

$\operatorname{ggT}(a,b) = \operatorname{ggT}(b,a)$, $\operatorname{ggT}(ma, mb) = m \cdot \operatorname{ggT}(a,b)$

$\operatorname{ggT}(a,b) = \operatorname{ggT}(b, a \bmod b) = \operatorname{ggT}(b, a-b) = \operatorname{ggT}(a + mb, b)$

ggT = gcd, kgV = lcm

kgV: $a \mid l \wedge b \mid l \wedge \forall m\,((a \mid m \wedge b \mid m) \to l \mid m)$

$a = \prod p_i^{e_i}$, $b = \prod p_i^{f_i}$

$\operatorname{ggT}(a,b) = \prod p_i^{\min(f_i, e_i)}$, $\operatorname{kgV}(a,b) = \prod p_i^{\max(f_i, e_i)}$

$\operatorname{ggT}(a,b) \cdot \operatorname{kgV}(a,b) = ab$, a, b teilerfremd $\Leftrightarrow \operatorname{ggT}(a,b) = 1$

$a \mid b \wedge b \mid c \to a \mid c$ $\quad a \mid b \wedge b \mid a \to a = b \vee a = -b$

$a \mid b \wedge a \mid c \to a \mid (ub + vc)$ $\quad a \mid b \vee a \mid c \to a \mid bc$

$\forall a, d \in \mathbb{Z}, d \neq 0 \; \exists q, r \in \mathbb{Z} \to a = qd + r$ $\quad 0 \leq r < d$ $\quad R_d(a) = r$

$\mathbb{Z}_m^*$, $m = pq \to a \in \mathbb{Z}_m^* \to \operatorname{ggT}(a,m) = 1 \to \operatorname{ggT}(a,p) = 1 \wedge \operatorname{ggT}(a,q) = 1$

5. Primzahlen:

p prime $\Leftrightarrow \forall a > 0\,(a \mid p \to (a = 1 \vee a = p))$

$p \mid (ab) \to p \mid a \vee p \mid b$

Zahlen können in Primfaktoren zerlegt werden

Primtest nach Fermat: p prime $\to a^p \equiv_p 1$

Unendlich Primzahlen: Widerspruchsbeweis:

Sei p_n die höchste Primzahl dann $\prod_{i=1}^{n} p_i + 1 > p_n$ und nicht durch eine Primzahl $p_1 - p_n$ teilbar. Da alle Zahlen sich in Primfaktoren zerlegen lassen, wissen wir, dass es entweder selbst eine Primzahl ist, oder von einer Primzahl $> p_n$ geteilt wird ↯ $\square$

Pascalsche Dreieck

$\binom{0}{0}$

$\binom{1}{0}$ $\binom{1}{1}$

$\binom{2}{0}$ $\binom{2}{1}$ $\binom{2}{2}$

$\binom{3}{0}$ $\binom{3}{1}$ $\binom{3}{2}$ $\binom{3}{3}$

1

1 1

1 2 1

1 3 3 1

$3 + 3 = 6 = \binom{4}{2}$

6. Chinese Remainder Theorem

Wenn n Elemente auf m Mengen verteilt werden und n > m hat min. eine Menge mehr als 1 Element

Sei $m_1 \dots m_r$ paarweise teilerfremd ($ggT(m_i, m_j) = 1$) und x gesucht mit $x \equiv_{m_1} a_1, \dots, x \equiv_{m_r} a_r \Leftrightarrow x \equiv_M a$, $M = \prod m_i$

Berechnung: $a = R_M\left(\sum_{i=1}^{r} \left(a_i \cdot \frac{M}{m_i} \cdot \left(\frac{M}{m_i}\right)^{-1} (\text{mod } m_i)\right)\right)$

$M_i = \frac{M}{m_i}$, $y_i \Rightarrow M_i y_i \equiv_{m_i} 1$, $x = \sum a_i M_i y_i \pmod m$

Bsp. $x \equiv_5 1$, $x \equiv_6 2$, $x \equiv_7 3$

#i	a_i	m_i	M	M_i	y_i	X
1	1	5	$m_1 \cdot m_2 \cdot m_3$	$6 \cdot 7 = 42$	$42 y_1 \equiv_5 1 \Leftrightarrow 2 y_1 \equiv_5 1 \Leftrightarrow 6 y_1 \equiv_5 3 y_1 \equiv 3$	$x = 836$ (mod 210)
2	2	6	$= 5 \cdot 6 \cdot 7$	$5 \cdot 7 = 35$	$35 y_2 \equiv_6 1 \dots y_2 = 5$	
3	3	7	$= 210$	$5 \cdot 6 = 30$	$30 y_3 \equiv_7 1 \quad y_3 = 4$	$= 206$ (mod 210)

$\hookrightarrow x = 1 \cdot 42 \cdot 3 + 2 \cdot 35 \cdot 5 + 3 \cdot 30 \cdot 4 = \sum a_i M_i y_i \pmod m$

$m_1 \dots m_k$ paarweise teilerfremd (relative prime)

7. Crypto & Codes

Diffie-Hellmann $\langle g \rangle = G$ G $\vee$ g $\mathbb{Z}_p^*$

A: $x \in G$, g^x → B; B: $y \in G$, g^y → A; $k = (g^y)^x$, $k = (g^x)^y$

RSA: B: p, q prime, $n = p \cdot q$, e mit $ggT(e, (p-1)(q-1)) = 1$

pub(n, e) → A; m (Message), m < n, $c = R_n(m^e)$

EEA: $d = e^{-1} \pmod{(p-1)(q-1)}$, $m = R_n(c^d)$

Lagrange Interpolation: Polynom grad n ist mit ≥ n+1 stellen eindeutig bestimmt.

1) bestimme für jede Stelle a_j Polynom u_i, $u_i(a_j) = \begin{cases} 1, & i = j \\ 0, & \text{sonst} \end{cases}$

2) Interpoliere Polynom $p(x) = \sum y_i u_i(x)$ mit $u_i(x) = \prod_{j \neq i} \frac{x - a_j}{a_i - a_j}$ $a_j = x_0 \dots x_n$

Bsp. S = 1234, n = 6, k = 3, 1. k−1 randoms (166, 94)

$a_0 = 1234 = S$, $a_1 = 166$, $a_2 = 94$, $f(x) = 1234 + 166x + 94x^2$

$(x, f(x))_n$ Punkte: (1, 1494), (2, 1942), (3, 2578), (4, 3402), (5, 4414), (6, 5614)

$x = 2, 4, 5 \rightarrow u_0 = \frac{x - x_1}{x_0 - x_1} \cdot \frac{x - x_2}{x_0 - x_2} = \frac{x-4}{2-4} \cdot \frac{x-5}{2-5} = \frac{1}{6}x^2 - \frac{3}{2}x + \frac{10}{3}$

analog $u_1 = -\frac{1}{2}x^2 + \frac{7}{2}x - 5$, $u_2 = \frac{1}{3}x^2 - 2x + \frac{8}{3}$

$f(x) = \sum_{j=0}^{2} y_i u_i(x) \rightarrow f(x) = 1234 + 166x + 94x^2 \rightarrow f(0) = 1234 = S$

Bsp. k = 2, n = 4 in GF(5) $f(x) = a + bx$, $f(1) = 3$, $f(2) = 0$

$f(1) = a + b = 3$, $f(2) = a + 2b = 0 \rightarrow a = -2b$, $b = -3 \equiv 2$ $a = 6 \equiv 1$

Hamming-Codes/Distanz: $A = \{0, 1\}$, k = anzahl Zeichen

$k < n$ $E: A^k \rightarrow A^n$, $D: A^n \rightarrow A^k$

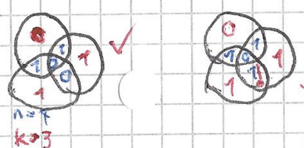
$E(a_0, \dots, a_{k-1}) = (c_0, \dots, c_{n-1})$, $Im(E) = Code$, $|Im(E)| = |A|^k$

$d = \min\{d_H(u, v) \mid u, v \in Code\}$ ≤ d−1 erkennen ≤ $\frac{d-1}{2}$ korrigieren

Länge $N = 2^k - 1$ k = 3, N = 7   n = N − k = 4

n-Bits = Daten, k-Bits = Kontrolle

Bsp.



0	1	1	1	0	0	1	0	1	0	1	0
k_1	k_2	n_3	k_4	n_5	n_6	n_7	k_8	n_9	n_{10}	n_{11}	n_{12}

fehler

$k_1 + n_3 + n_5 + n_7 + n_9 + n_{11}$ 1 ja, 1 nein

$k_2 + n_3 + n_6 + n_7 + n_{10} + n_{11}$ 2 ja, 2 nein

8. Algebra:

Halbgruppe: 1) Menge + Operation, 2) abgeschlossen, 3) assoziativ

Monoid: + neutrales Element

Gruppe: + inverses Element

Abelsche Gruppe: + kommutativ

Ring: 1) Menge + 2 Operationen, 2) ⟨R; +⟩ abelsche Gruppe, 3) ⟨R; ·⟩ Monoid, 4) Distributivität

Integritätsbereich: Kommutativer Ring (· ist kommutativ) ohne Nullteiler (0 ≠ 1) $\langle \mathbb{Z}_6; \oplus, \ominus, 0, \odot, 1 \rangle$ hat Nullteiler 1·6, 2·3, deshalb nur Ring!

↳ mult. inv. in endlich

Körper: Kommutativer Ring in dem jedes Element ≠ 0 Einheit ist

↳ $K^* = K \setminus \{0\}$

↳ multiplikativ inverses

↳ Endlicher Integritätsbereich

Körper = Integritätsbereich, aber alles ausser 0 invertirbar, jeder Körper ist auch Integritätsbereich!

Nullteiler: $a, b \neq 0$, $a \cdot b = 0$ $\mathbb{Z}^* = \{-1, 1\}$

Einheit: $\forall a \exists b$ $(a \cdot b) = (b \cdot a) = 1$

Assoziativität: $\forall a, b, c$ $(a * b) * c = a * (b * c)$

Neutralelement: $\forall a \exists b$: $a * b = b * a = e$

Inverseselement: $\exists e \forall g$ $g * e = e * g = g$

Kommutativ: $\forall a, b$ $a * b = b * a$ (abelsch)

Galoisfield: GF(p) endlicher Körper mit p Elementen, z.B. $\langle \mathbb{Z}_p; \oplus, \circledast \rangle$

Körper ⟨K; +, ·⟩   ⟨K; +⟩, ⟨K \ {0}; ·⟩ abelsche Grp.

Kommutivität in Ringen: $(1+1) \cdot (a+b)$ → $1(a+b) + 1(a+b)$ → $(1+1)a + (1+1) \cdot b$

$a + b + a + b = a + a + b + b \Rightarrow b + a = a + b$

Ordnung: $ord(G) = |G|$ = Anzahl Elemente in Grp.

$a \in \langle \mathbb{Z}_4; \oplus \rangle$: ord(a) := wie oft muss a ⊕ kombinieren damit e sonst ∞

$ord(\mathbb{Z}_4) = |\mathbb{Z}_4| = 4 = |\{0, 1, 2, 3\}|$

ord(0) := 1, ord(1) := 4, ord(2) := 2, ord(3) := 4

$ord(\mathbb{Z}_2 \times \mathbb{Z}_2) = |\mathbb{Z}_2 \times \mathbb{Z}_2| = 4 = |\{(0,0), (0,1), (1,0), (1,1)\}|$

ord((0,0)) := 1, ord((0,1)) := 2, ord((1,0)) := 2, ord((1,1)) := 2

$\mathbb{Z}_4 \not\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \Leftrightarrow (1, 4, 2, 4) \neq (1, 2, 2, 2)$

Generell: $\mathbb{Z}_n^* = \underbrace{\mathbb{Z}_{p_1}^*}_{k_1 \text{ mal}} \times \underbrace{\mathbb{Z}_{p_2}^*}_{k_2 \text{ mal}} \times \dots$ $\mathbb{Z}_n = \underbrace{\mathbb{Z}_{p_1}}_{k_1 \text{ mal}} \times \underbrace{\mathbb{Z}_{p_2}}_{k_2 \text{ mal}} \times \dots$

Untergruppe:

$H \subseteq G$, $H \neq \emptyset$, H Untergruppe v. G, falls ⟨G; ∗⟩ gruppe und ⟨H; ∗⟩ ebenfalls Gruppe $e \in G = e \in H$

$\forall a, b \in H \rightarrow (a * b) \in H$, $\forall a \in H \rightarrow a^{-1} \in H$

Theorem 5.8 Lagrange: $H \subseteq G \rightarrow |H|$ teilt $|G|$

Corollary 5.9: ord(a) teilt |G| $\forall a \in G$

$\langle a \rangle = \{e, a, a^2, \dots, a^{ord(a)-1}\}$ kleinste Untergruppe mit a

↳ $a^0 = e$, $a^1 = a$, $a^n = a \cdot a^{n-1}$, $a^n = (a^{-1})^{|n|}$, $ord(a) = |\langle a \rangle|$

$a^i * a^j = a^{R_{ord(a)}(i+j)}$, $(a^i)^{-1} = a^{ord(a)-i}$

Nebenklasse: UG: $a \in G$, $U \subseteq G$, Links/Rechts Nebenklasse:

LNK: $a \circ U = \{a \circ u \mid u \in U\}$ RNK: $U \circ a = \{u \circ a \mid u \in U\}$

Normalteiler: LNK = RNK ⇒ $a \circ N = N \circ a$ ~~falls G abelsch~~

Falls G abelsch, $U \subseteq G \rightarrow |G|$ teilt $|U| = 2$

Bsp. $\langle \mathbb{Z}_4; \oplus \rangle$ hat durch a = 3 eine Restklasse

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

e ∗ a = Normalteiler

isomorph

⊕	0	1
0	0	1
1	1	0

≅

∘	X	Y
X	X	Y
Y	Y	X

$GF_q = \mathbb{Z}_p$ ↳ Galois-Field

Zyklischegruppe:

G heisst zyklisch, falls $\exists g \in G$ ord(g) = |G|

↳ g heisst Generator v. G, $\langle g \rangle = G$

g Generator $\mathbb{Z}_n^*$ und $ggT(a, |G|) = 1$ dann g^a Generator

$\mathbb{Z}_p^*$ hat $\varphi(p-1)$, $\mathbb{Z}_n^*$ hat $\varphi(|\mathbb{Z}_n^*|)$ generatoren

|G| prime → G zyklisch → $\forall g \in G$, $g \neq e \rightarrow ord(g) = p$

Nach Lagrange 2: G endlich, $a \in G$: $a^{|G| \cdot k} = e$ $k \in \mathbb{N}$

$a^{k \cdot ord(a)} = (a^{ord(a)})^k = e^k = e$

$G \cong \langle \mathbb{Z}_{|G|}, \oplus \rangle$, untergruppen auch Zyklisch + abelsch

G besitzt $\varphi(|G|)$ generatoren

GF(2): $+ \equiv -$ $1 + 1 = 0$, $2 = 0$, $a = -a$

$(a+b)^2 = a^2 + b^2$ $(a^2 + 2ab + b^2 = a^2 + 0ab + b^2)$

Bsp. Untergruppen v. $\langle \mathbb{Z}_{12}; \oplus, \ominus, 0, \odot, 1 \rangle$:

{0}, {0, 6}, {0, 4, 8}, {0, 3, 6, 9}, {0, 2, 4, 6, 8, 10} + ⟨1⟩

Generator $\langle \mathbb{Z}_n; \oplus \rangle$ alle g mit GGT(n, g) = 1

falls ord(a) = 2 → selbstinvers, $a = a^{-1}$

$\langle \mathbb{Z}_n, \odot \rangle$ ist n−1 selbstinvers

Idea: $(a) := \{ua \mid u \in \mathbb{Z}\}$

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

Lemma 4.3: for $(a, b) = (d)$, $a, b \in \mathbb{Z}$, $\exists d \in \mathbb{Z}$

Sei d kleinste positive Zahl in $(a, b) \rightarrow (d) \subseteq (a, b)$

Sei $c \in (a, b)$ $\exists q, r$, $0 \leq r < d \rightarrow c = qd + r$ da c und $d \in (a, b)$

$r = c - qd$, da $0 \leq r < d$ und d kleinstes Element (a, b) muss r = 0 sein. → $c = qd \in (d) \rightarrow (a, b) \subseteq (d)$

$\langle \mathbb{Z}; +, \cdot \rangle$: $\langle 0 \rangle = \{0\}$, $\langle 1 \rangle = \mathbb{Z}$ $\langle 0 \rangle \leq I \leq \langle 1 \rangle$

$\langle n \rangle = n \cdot \mathbb{Z}$, $\langle 2, 3 \rangle = \{0, 2, 3, 2 \cdot k_1, 3 \cdot k_2, 2 \cdot k_1 + 3k_2\}$

$= \{2 \cdot k_1 + 3 \cdot k_2\} = \langle 1 \rangle = \mathbb{Z}$

Beispiele:

⟨ℕ; +⟩ Halbgruppe, kein Inverses

⟨ℕ; ·⟩ Halbgruppe, kein Inverses

⟨ℤ; +⟩ Gruppe

⟨ℤ; ·⟩ Halbgruppe, kein Inverses für 0

⟨ℤ; |⟩ | := Nichts, da nicht abgeschlossen

⟨ℚ; ·⟩ Halbgruppe, kein Inverses für 0 ⟨ℚ \ {0}; ·⟩ Gruppe

⟨ℚ; |⟩ Nichts, da nicht assoziativ

$\langle \mathbb{Z}_m; \oplus \rangle$ Abelsche Gruppe

ℤ, ℚ, ℝ, ℂ sind Integritätsbereiche, $\mathbb{Z}_m$ nur falls m prime

ℚ, ℝ, ℂ sind Körper, $\mathbb{Z}_m$ nur falls m prime

Falls D integritätsbereich, dann auch D[x]

Assoziativität v. +, · in ℕ, ℤ, ℚ, ℝ, ℂ, $\mathbb{Z}_m$ gegeben

7. Hamming:

$A = \{0, 1, 2\}$ $|A|^1 = 3$

(1, 3) codes: $C = \{(0, 0, 0), (0, 1, 2), (1, 2, 1)\}$

Gewicht

0	0	0		0	1	2	= 2
0	0	0		1	2	1	= 3
0	1	2		1	2	1	= 3
1	2	3		1	2	3	

Min Dist = 2

Parity-Bits: $2^n \rightarrow 1, 2, 4, \dots$ Daten: Rest

Parity-Check 2^i z abst. inkl. selbst.

z.B. 4: 4, 5, 6, 7, 12, 13, 14, 15, 20, 21, 22, 23, …

8. Algebra: (Fortsetzung) Beispiele:

Sei e, e' links & Rechtsneutral: $e * e' = e$ (rechtsneutral), $e * e' = e'$ (linksneutral) $\to e = e'$ □

Sei b, c links & Rechtsinverses v. $a \to a*b = b*a = e$, $a*c = c*a = e$

$b = b*e = b*(a*c) = (b*a)*c = e*c = c \to b = c$ □

Lemma 5.3: Grp: $\langle G; *, \hat{}, e\rangle$ $\forall a, b, c \in G$

$\hat{\hat{a}} = a$, $\widehat{a*b} = \hat{b} * \hat{a}$, left + right cancelation: $a*b = a*c \Rightarrow b = c$

$b*a = c*a \Rightarrow b = c$, $a*x = b$ und $x*a = b$ eindeutig

Homomorphismus & Isomorphismus:

Homomorphismus ist injektive Abbildung $\phi: G \to H$

Isomorphismus ist bijektive Abbildung $\psi: G \to H$

Gruppen $\langle G; *\rangle$, $\langle H; \square\rangle$, $\phi: G \to H$

$\langle G; *, \hat{}, e\rangle$, $\langle H; \square, \hat{}, e'\rangle$ ~~Lemma 5.5:~~

Definition: $\phi(a*b) = \phi(a) \square \phi(b)$

Lemma 5.5: $\phi(e) = e'$

$\phi(g) = \phi(g*e) = \phi(g) \square \phi(e) \to \phi(e) = e'$

$\phi(\hat{a}) = \widehat{\phi(a)}$

$e' = \phi(e) = \phi(g * \hat{g}) = \phi(g) \square \phi(\hat{g}) = \phi(g) \square \widehat{\phi(g)}$

Bsp. Isomorphismus: $\langle \mathbb{Z}_6; \oplus\rangle \times \langle \mathbb{Z}_{10}; \oplus\rangle \cong \langle \mathbb{Z}_2; \oplus\rangle \times \langle \mathbb{Z}_{30}; \oplus\rangle$

$\psi: \mathbb{Z}_6 \times \mathbb{Z}_{10} \to \mathbb{Z}_2 \times \mathbb{Z}_{30}$, $\psi((a, b)) = (a', b')$ $a' \equiv_2 a$, $b' \equiv_3 a$, $b' \equiv_{10} b$

$\langle \mathbb{Z}_2; \oplus\rangle \cong \langle \{True, False\}; XOR\rangle$

$\langle G; \circ\rangle, \langle K; *\rangle \to \langle G \times K; \sigma\rangle \Rightarrow (g, k) \sigma (g', k') = (g \circ g', k * k')$

Drehung/Spiegelung = Symetrie Gruppe mit $2n$ Elementen, n-Eck

$\langle \mathbb{Z}^*_{19}; \odot\rangle \cong \langle \mathbb{Z}_{18}; \oplus\rangle$ $\langle \mathbb{Z}^*_{15}; \odot\rangle \ncong S_\square \ncong \langle \mathbb{Z}_8; \oplus\rangle$

$G = \{e\}$

*	e
e	e

$G = \mathbb{Z}_2$, $* = \oplus$, $e = 0$, $a = 1$

*	e	a
e	e	a
a	a	e

$\langle \mathbb{Z}_4; \oplus\rangle \cong \langle \mathbb{Z}^*_5; \odot\rangle$

⊕	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$0 \mapsto 1$, $1 \mapsto 2$, $2 \mapsto 4$, $3 \mapsto 3$

⊙	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$2 \oplus 2 = 4 = 0$ $e = 1 = 16 = 4 \odot 4$

$|G| = 6 \Rightarrow \mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$ teilerfremd

$\mathbb{Z}^*_{20} \cong \mathbb{Z}^*_4 \times \mathbb{Z}^*_5 \cong \langle \mathbb{Z}_2; \oplus\rangle \times \langle \mathbb{Z}_4; \oplus\rangle$

$GF(9) = GF(3^2)$, $n = p^k$, $k \in \mathbb{N}$

Sind $|K_1| = |K_2|$ endlich

$\hookrightarrow K_1 \cong K_2$ isomorph

Polynome:

Polynome über $GF(2)$

+	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

•	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	x+1	1
x+1	0	x+1	1	x

$x, x+1$: irreduzibel

x^2, x^2+1: reduzibel

Teilbarkeit v. Polynomen: $a(x), b(x) \in K[x]$, $b \neq 0$,

$b(x) | a(x) :\Leftrightarrow \exists c(x) \in K[x] : b(x) \cdot c(x) = a(x)$

Reduzierbarkeit: $\deg(1)$ = irreduzibel (lineare Polynome)

$\deg(p(x)) > 1 : p(x) = s(x) \cdot t(x) \to (\deg(s) \vee \deg(t))$ $= 0$ oder 1

Grad 2, 3 genau dann, wenn keine Nullstelle

$F[x]_{m(x)} = \{a(x) \in F[x] \mid \deg(a(x)) < \deg(m(x))\}$

Polynom $\deg \geq 3$ <
- hat Nullstellen $\Rightarrow$ Reduzibel
- hat keine Nullstellen $\Rightarrow$ weiter abklären

Alle Polynome über Körper $F[x]$ bilden einen Ring

Sei $a(x)$ irreduzibel in $K = GF(p^n)$, dann $K[x]$ über $K \bmod a(x)$ ebenfalls Körper

Um $GF(p^d)$ aus $GF(p)$ zu konstruieren

1) alle Polynome a_i mit $\deg(a_i) < d$ in additions/multiplikations Tabelle
2) Wähle a irreduzibles Polynom grad d über $GF(p)$ und rechne Tabelle mod a

$\mathbb{Z}_2 = \{0, 1\}$, $\mathbb{Z}_2[x]_{x^3+x} = \{0, 1, x, x+1, x^2, x^2+x, x^2+x+1, x^2+1\}$

gibt es Nullteiler? Ja $(x)(x^2+1)$ und $(x+1)(x^2+x)$

Ist es Ring? Ja (abgeschlossen, neutralelement 0, 1, kommutativ, invers)

Rechnen: $x^2 \cdot x = x^3 = x^3 - (x^3 + x) = -x \equiv_2 x$

$\deg(a(x)) \geq 3 : a(x) = b(x) \cdot \underbrace{(3x + x)}_{0} + r(x) = r(x)$

$x^5 + x^3 + 1 / x^3 + x = x^2 \to x^5 + x^3 + 1 - (x^5 + x^3) = 1$

Wann ist $F[x]_{m(x)}$ ein Körper? Falls keine nullteiler $\to m(x)$ irreduzibel

$\mathbb{Z}_3[x]_{x^2+2x+2}$ Ring, Körper, Integritätsbereich da $\neq 0$ für $x \in \{0, 1, 2\}$

$\mathbb{Z}_3[x]_{x^2+2x+1}$ Ring da $= 0$ bei $x = 2$

Integritätsbereich $D \to D[x]$ ebenfalls Integritätsbereich

Anzahl Elemente: $|\mathbb{Z}_2[x]_{x^3+x}| = 8 = 2^3 = |\mathbb{Z}_2|^{\deg(x^3+x)}$

$|\mathbb{Z}_2[x]_{x^5+x^2+1}^*| = |\mathbb{Z}_2[x]_{x^5+x^2+1} \setminus \{0\}| = 2^5 - 1 = 31$

$\hookrightarrow$ da 31 prim, nach Lagrange Zyklisch $\to$ jedes Element Generator

Gesucht Körper mit 4 Elementen. $GF(2)[x]_{m(x)}$ ($\deg = 2$, irreduzibel)

Irreduzible Polynome in $GF(2)[x]$

deg 2: $x^2 + x + 1$, 3: $x^3 + x^2 + 1$, $x^3 + x + 1$, 4: $x^4 + x^3 + x^2 + x + 1$, $x^4 + x^3 + 1$, $x^4 + x + 1$

5: $x^5 + x^4 + [x^3 + [x^2 | x]\,|\,x^2 + x] + 1$, $x^5 + x^3 + [x^2 + x] + 1$, $x^5 + x^2 + 1$

$x^5 + x^4 + 1 = (x^3 + x + 1)(x^2 + x + 1)$

$\mathbb{Z}[x] : x^2 + 7x + 5$ $\psi: \mathbb{Z}[x] \to GF(2)[x]$ $x^2 + 7x + 5 \mapsto x^2 + x + 1$

da $x^2 + x + 1$ in $GF(2)[x]$ irreduzibel ist, ist $x^2 + 7x + 5$ irreduzibel

$\mathbb{R}[x]_{x^2+1} \approx \mathbb{C} : ax + b \approx ai + b$ $\mathbb{R}[x]_{x^2+1}(x^2) = -1$

$x^2 + 1$: irreduzibel in $\mathbb{R}$, $(x+i)(x-i)$ in $\mathbb{C} \to x^2 - i^2 = x^2 - (-1)$

9. Logik:

Verbände: $\langle M; \wedge, \vee\rangle$ falls $\langle M; \wedge\rangle$ und $\langle M; \vee\rangle$ abelsche Halbgruppen

$\hookrightarrow a = a \wedge (a \vee b) = a \vee (a \wedge b)$

Distributiver Verband:

$\hookrightarrow a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$, $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

Bolsche Algebra: Distributiver Verband mit neutral Element / invers

Lemma 6.1:

$F \wedge F \equiv F \vee F \equiv F$ $F \wedge G \equiv G \wedge F$ $F \vee G \equiv G \vee F$

$(F \wedge G) \wedge H \equiv F \wedge (G \wedge H)$, $(F \vee G) \vee H \equiv F \vee (G \vee H)$

$F \wedge (F \vee G) \equiv F \equiv F \vee (F \wedge G)$, $F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$

$F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$, $\neg(\neg F) \equiv F$, $F \vee \top \equiv \top$

$\neg(F \wedge G) \equiv \neg F \vee \neg G$, $\neg(F \vee G) \equiv \neg F \wedge \neg G$, $F \wedge \top \equiv F$

$F \vee \bot \equiv F$, $F \wedge \bot \equiv \bot$, $F \vee \neg F \equiv \top$, $\neg G \to \neg F \equiv F \to G$

$F \wedge \neg F \equiv \bot$ $F \to G \equiv \neg F \vee G$

$F \leftrightarrow G \equiv F = G \equiv (F \to G) \wedge (G \to F) \equiv (F \wedge G) \vee (\neg F \wedge \neg G)$

Lemma 6.6:

$\neg(\forall x\, F) \equiv \exists x\, \neg F$, $\neg(\exists x\, F) \equiv \forall x\, \neg F$, $(\forall x\, F) \wedge (\forall x\, G) \equiv \forall x (F \wedge G)$,

$(\exists x\, F) \vee (\exists x\, G) \equiv \exists x (F \vee G)$, $\forall x \forall y F \equiv \forall y \forall x F$, $\exists x \exists y F \equiv \exists y \exists x F$

$(\forall x\, F) \wedge H \equiv \forall x (F \wedge H)$, $(\forall x\, F) \vee H \equiv \forall x (F \vee H)$,

$(\exists x\, F) \wedge H \equiv \exists x (F \wedge H)$, $(\exists x\, F) \vee H \equiv \exists x (F \vee H)$

Erfüllbar: In Wahrheitstabelle min. 1x Wahr

Tautologie: In Wahrheitstabelle immer Wahr

Unerfüllbar: In Wahrheitstabelle nie Wahr

F ist Tautologie, falls $\neg F$ unerfüllbar

$F \to G$ ist Tautologie, falls $F \models G$

$F \equiv G :\Leftrightarrow F \models G \wedge G \models F$ F Tautologie: $\models F$

F unerfüllbar: $\models (F \to \bot)$ $\models : \Leftrightarrow \Rightarrow$

Beweissysteme:

S Menge von Math. Aussagen (Formeln) $s \in S : \{True, False\}$

P Menge von Beweisen

τ Wahrheitsfunktion $\tau : S \to \{0, 1\}$

ρ Funktion $\rho : S \times P \to \{0, 1\}$, $\rho(s, p) = 1 \to$ Gültiger Beweis

$\Pi = (S, P, \tau, \rho)$ ist Beweissystem

Korrekt: keine falsche Aussage hat Beweis

$\forall s \in S (\exists p \in P\ \rho(s, p) = 1 \to \tau(s) = 1)$

vollständig: jede Korrekte Aussage hat Beweis

$\forall s \in S (\tau(s) = 1 \to \exists p \in P\ \rho(s, p) = 1)$

Bsp. $\tau(s) = 0$, $\rho(s, p) = 1$ Vollständig

$\tau(s) = 0$, $\rho(s, p) = 0$ Vollständig, Korrekt

In einer Betrachtung heissen $s \in S$ Formeln. Syntax def. Alphabet und bestimmt welche Folgen v. Symbolen Korrekt

Logik ist durch Syntax und Semantik definiert.

Interpretation ist Bestimmte Wahl v. Werten für Formeln

Interpretation passend: min alle benötigten Variabeln definiert.

Semantik σ weisst jeder Formel und passender Interpretation einen Wahrheitswert $\{True, False\}$ zu.

$\hookrightarrow$ Oft $A(F)$ anstelle v. $\sigma(F, A)$, A = Interpretation

Syntax: wenn F, G Formel, dann $F \wedge G$ auch Formel

Semantik: $A(F \wedge G) = 1 \to A(F) = 1$ und $A(G) = 1$

Modell: Passende Interpretation, welche Formeln wahr macht

$\hookrightarrow A \models F$, falls $A \models F\ \forall F \in M \to A \models M$

Hilbert-Style Calculi:

$\{F_1, \dots, F_k\} \vdash_R G$ auch: $\frac{F_1 \dots F_k}{G}$

z.B. $\{F \wedge G\} \vdash F$, $\{F \wedge G\} \vdash G$, $\{F, G\} \vdash F \wedge G$

$M \vdash_R F :\Leftrightarrow M \models F$, $F \vdash_R G \Leftrightarrow \models (F \to G)$

Schlussregeln: Regeln um Formel aus Menge v. Formeln herzuleiten. $\to \{F_1, \dots, F_k\} \vdash_R G$

Logisches Kalkül: Endliche Menge v. Schlussregeln

$\hookrightarrow K : \{R_1, \dots, R_m\}$

Atomare Formeln:

- A_i, $i \in \mathbb{N}$: $F, G, F_1, F_2, \dots$
- Wenn F, G Formeln, dann auch $F \wedge G$, $F \vee G$, $\neg F$,

Hilbert-Style Calculi: (Fortsetzung)

$\{F \vee G, F \to H, G \to H\} \vdash H$, $\{F \vee G, \neg G\} \vdash F$

Prädikatenlogik:

x_i, $i \in \mathbb{N}$ ist Variabel
$f_i^{(k)}$ $i \in \mathbb{N}$ ist Funktion mit k Parametern
$f_i^{(0)}$ ist Konstante.
$P_i^{(k)}$, $i \in \mathbb{N}$ ist Prädikat mit k Parametern
term: Variabeln oder $f_i^{(k)}(t_1, \dots, t_k)$, falls $t_1 - t_k$ Terme
Formel: F, G, falls F, G Formel auch $\neg F$, $F \wedge G$, $F \vee G$, $\forall x_i F$, $\exists x_i F$
falls $t_1 - t_k$ Term $P_i^{(k)}(t_1, \dots, t_k) \to$ atomare Formel

$A = (U, \Phi, \Psi, \mathcal{E})$
U = Universum nicht leer $\leftrightarrow U^A$
Φ = Funktionen $\Phi(f): U^k \to U$ $\leftrightarrow f^A$
Ψ = Prädikate $\Psi(P): U^k \to \{0,1\}$ $\leftrightarrow P^A$
$\mathcal{E}$ = Variabeln $\mathcal{E}(x): x \in U$ $\leftrightarrow x^A$

Bsp: $F = \forall x (P(x) \vee P(f(x, a)))$
Passend: $U^A = \mathbb{N}$, $a^A = 3$, $f^A(x,y) = x + y$, $P^A(x) = 1$ falls x gerade

Gleichwertige Aussagen:

1) $\{F_1, \dots, F_k\} \models G$
2) $(F_1 \wedge \dots \wedge F_k) \to G$ Tautologie
3) $\{F_1, \dots, F_k, \neg G\}$ unerfüllbar

Sei A passende Interpretation für $F_1, \dots, F_k, G$:
1) Falls A Modell für $\{F_1, \dots, F_k\}$ dann auch für G
2) Tautologie, da jedes Model für $F_1, \dots, F_k$ auch für G
3) Falls A Modell für $F_1, \dots, F_k$, dann nicht für $\cancel{\neg} G$

CNF & DNF

Disjunktive Normalform: $(A \wedge B) \vee (A \wedge \neg B) \vee (\neg A \wedge \neg B)$
Konjunktive Normalform: $(A \vee B) \wedge (A \vee \neg B) \wedge (\neg A \wedge \neg B)$

Bsp.

	A	B	F
1	0	0	0
2	0	1	1
3	1	0	1
4	1	1	0

DNF: $(\overset{2}{\neg A \wedge B}) \vee (\overset{3}{A \wedge \neg B})$

CNF: $\neg(\overset{1}{\neg A \wedge \neg B}) \wedge \neg(\overset{4}{A \wedge B}) \equiv (A \vee B) \wedge (\neg A \vee \neg B)$
$\equiv (\underset{1}{A \vee B}) \wedge (\underset{4}{\neg A \vee \neg B})$

10. Kombinatorik

Anzahl k-Tupel aus n: n^k
Anzahl geordneter k-Tupel mit verschiedenen Elementen $\frac{n!}{k!}$
Anzahl Permutationen v. n: $n!$
Anzahl Teilmengen von n mit k Elementen: $\binom{n}{k}$
Anzahl von k Kompositionen in n Summanden $\binom{k-1}{n-1}$
Anzahl Zerlegungen v. k in n Summanden $\binom{n+k-1}{k}$

	Ohne Wiederholung/Zurücklegen	Mit
Permutation $(a,b) \neq (b,a)$	$n!$	$\frac{n!}{\text{Einzelne Mengen}!} = \frac{n!}{P_1! \cdot P_2! \cdots}$
Variation $(a,b) \neq (b,a)$	$\lvert A \rvert^k = n^k$	$\leftrightarrow \binom{n}{k} \cdot k! = \frac{n!}{(n-k)!}$
Kombination $\{a,b\} = \{b,a\}$	$\binom{n}{k} = \frac{n!}{(n-k)! \cdot k!}$	$\left(\!\binom{n}{k}\!\right) = \binom{n+k-1}{k} = \frac{(n+k-1)!}{(n-1)! \cdot k!}$

	beliebig viel	max 1 pro n	min 1 pro n
k unterschiedliche, n unterschiedliche	n^k	$\frac{n!}{(n-k)!} = k! \binom{n}{k}$	$n! \, S_{k,n}$
k gleiche Bälle, n unterschiedliche	$\binom{k+n-1}{k}$	$\binom{n}{k}$	$\binom{k-1}{n-1}$
k unterscheidbare, n gleiche Fächer	$S_{k,0} + S_{k,1} + \dots + S_{k,n}$	1 für $k \leq n$, 0 für $k > n$	$S_{k,n}$
k gleiche Bälle, n gleiche Fächer	$P_{k,0} + \dots + P_{k,n} = P_{k+n,n}$	1 für $k \leq n$, 0 für $k > n$	$P_{k,n}$

$S_{n,k} = \frac{1}{k!} \sum_{j=0}^{k} \left((-1)^{k-j} \binom{k}{j} j^n\right)$ $P_{n,k} = P_{n-k,k} + P_{n-1,k-1}$ $P_{1,1} = 1$, $n \geq k$

Inklusion: $\{a,b,c,d,e\}$ wieviele Wörter Länge 4 die $\{a,b,c\}$ enthalten? W = Menge Wörter L = 4, $W_a = W \setminus \{a\}, \dots$
$\lvert W_a' \cap W_b' \cap W_c' \rvert = \lvert W \rvert - \lvert W_a \rvert - \lvert W_b \rvert - \lvert W_c \rvert + \lvert W_a \cap W_b \rvert + \lvert W_b \cap W_c \rvert + \lvert W_a \cap C \rvert - \lvert W_a \cap W_b \cap W_c \rvert$
$= 5^4 - 4^4 - 4^4 - 4^4 + 3^4 + 3^4 + 3^4 - 2^4 = 84$

Binominalkoeffizient/Binomischer Lehrsatz:

$\binom{n}{k} = \frac{n!}{(n-k)! \cdot k!} = \frac{n \cdot (n-1) \cdot \ldots \cdot (n-k+1)}{k!} = \binom{n}{n-k} = \binom{n-1}{k-1} + \binom{n-1}{k}$
$= \binom{n+1}{k} - \binom{n}{k-1}$ $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$ $k > n \to 0$
$\binom{n}{0} = 1 = \binom{n}{n}$ $\binom{n}{1} = n = \binom{n}{n-1}$ $\binom{n}{k} = \frac{n}{k} \cdot \binom{n-1}{k-1} \Leftrightarrow k \cdot \binom{n}{k} = n \cdot \binom{n-1}{k-1}$
$\sum_{k=0}^{n} \binom{n}{k} = 2^n$ Binomialkoeffizient: $\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} = (x+y)^n$

Abschätzungen:
Binomialkoeffizient: $\left(\frac{n}{k}\right)^k \leq \binom{n}{k} \leq \left(\frac{en}{k}\right)^k$
Aritmetisches Mittel: $\frac{1}{n} \sum_{i=1}^{n} x_i \leq \sqrt{\frac{1}{n} \sum_{i=1}^{n} x_i^2}$ Quadratisches Mittel
Fakultätsfunktion: $n^{n/2} \leq n! \leq \left(\frac{n+1}{2}\right)^n$
~~Stirlingformel: n! ≈~~
Vandermonde: $\binom{f}{k} = \sum_{t=0}^{k} \binom{r}{t} \binom{n-r}{k-t}$

11. Sonstiges:

Identität und Inverses:

$id = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$ Inverses: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 5 & 2 \end{pmatrix}$
Permutation ist selbstinvers, falls: $\pi \circ \pi = id$
Komposition: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$

Relationen und Mengen:

$(a^b)^c \neq a^{(b^c)}$ ^ nicht assoziativ
$\emptyset \subseteq A$ (every set) Proof by contradiction:
$\emptyset \not\subseteq A \to x \in \emptyset \wedge x \notin A \to \lvert \emptyset \rvert > 0$ ↯
$\emptyset$ eindeutig: $\emptyset, \emptyset'$ da $\emptyset$ leer $\to \emptyset \subseteq \emptyset'$
da $\emptyset'$ leer $\to \emptyset' \subseteq \emptyset$ $\to \emptyset = \emptyset'$
$A = \{\{\emptyset\}\}$, $B = \{\{\emptyset\}, \{\emptyset, \emptyset\}\}$, $C = \{\emptyset, \{\emptyset\}\}$
$D = \{\emptyset, \{\emptyset, \{\emptyset\}\}\}$ $A = B \subseteq C \in D$

Zahlentheorie:

ab ist quadratisch, falls a und b quadratisch:
$a \cdot b = (u \cdot u) \cdot (v \cdot v) = (u \cdot v) \cdot (u \cdot v) = (uv)^2$
$\sqrt{x}$ rational $\to$ x rational, $\sqrt{x} = m/n \Rightarrow x = m^2/n^2$
n nicht durch 5 teilbar, n^4 um 1 grösser als vielfaches v. 5
$n = 5k + c$, $0 \leq k$, $1 \leq c \leq 4$, $n^4 = (5k+c)^4$ wobei c^4 übrig bleibt.
$1^4 \equiv_5 2^4 \equiv_5 3^4 \equiv_5 4^4 \equiv_5 1$ □ (Fallunterscheidung)
$\sqrt{2}$ irrational: Wiederspruch: Sei $\sqrt{2}$ rational:
$\sqrt{2} = \frac{m}{n} \to (\sqrt{2})^2 = \frac{m^2}{n^2} = 2 \to m^2 = 2n^2$
↳ m^2 gerade $\to$ m gerade $\to m = 2k \to m^2 = 2n^2 = 4k^2$
↳ $n^2 = 2k^2 \to$ n gerade. Da m, n gerade
↳ $ggT(m,n) = 2x$, $x \geq 1$ ↯ m, n müssen relativ prim
Falls a gerade auch a^2 gerade: $a = 2n$
↳ $a^2 = a \cdot a = 2n \cdot 2n = 2 \cdot (2n^2)$
Falls a^2 ungerade auch a ungerade: $a^2 = (2k+1)^2$
↳ $a^2 = 2(2k^2 + 2k) + 1 = a \cdot a = (2k+1)(2k+1)$
Induktion: $\sum 2^i = 2^{n+1} - 1$: $P(0) = 1 = 2^0 = 2^{0+1} - 1 = 2 - 1 = 1$
Schritt: $\sum^{n+1} 2^i = \sum^{n} 2^i + 2^{n+1} = (2^{n+1} - 1) + 2^{n+1} = 2^{(n+1)+1} - 1$
$x^3 + x^2 = y^4 + y + 1$? Nein, da links immer gerade, links ungerade
$a = b \Rightarrow a \equiv_m b$, $a \equiv_m b \Rightarrow a \neq b$, $a \equiv_m b$, $c \equiv_m d$; $a + c \equiv_m b + d$
$\to m \mid (a-b) \wedge m \mid (c-d) \Rightarrow m \mid ((a-b) + (c-d)) \Rightarrow (a-b) + (c-d) = (a+c) - (b+d)$
$a \equiv_m b \Leftrightarrow R_m(a) = R_m(b)$
$ax \equiv_m 1$ hat lösung, falls $ggT(a,m) = 1$, EEA $\to x = u$
x eindeutig: sei x und y lösung: $ax - ay \equiv_m 0$
↳ $m \mid a(x-y)$, da $ggT(m,a) = 1$, $\to m \mid (x-y)$
↳ $R_m(x) = R_m(y)$. Deshalb $R_m(x)$ einzige Lösung
Ungerade + Ungerade = Gerade: $(2n+1) + (2m+1) = 2(m+n+1)$
Falls n Prime, darf n nicht durch $p < \sqrt{n}$ geteilt werden

eorie:

rzerlegung (Existenz)

plikativ neutral

mzahl gemäss Definition

iederspruch Beweis: Angenommen es gibt Zahlen faktor Zerlegung, n, kleinste davon, $n \geq 1$. Da n noch prim, besitzt n nicht triviale Teiler $\exists a, b: a \cdot b = n$. a und b müssen beide in Primzahlen zerlegbar, da n kleinste legbare. $a = \prod p_a$, $b = \prod p_b \to n = a \cdot b = \prod p_a \cdot \prod p_b$ ↯

torzerlegung (Eindeutigkeit) n = kleinste Zahl mit mehreren: mmen $n = p \cdot a = q \cdot b$, p, q prime, $a \neq b$. Lemma v. Euklid: p ein Produkt → dann teilt p auch einen Faktor. da q r muss p, b teilen. p taucht also in beiden Zerlegungen Dann muss auch n/p mehrere Zerlegungen haben ↯

weissysteme:

ekter Beweis: $S \Rightarrow T$, S angenommen, T nachweisen

irekter Beweis: T Falsch $\Rightarrow$ S Falsch

eweisschritt: $(S \Rightarrow U, U \Rightarrow T) \Rightarrow (S \Rightarrow T)$

eweis mit Modus-Einteilung: S unter Verwendung R mit $R \Rightarrow S$

eweis durch Fallunterscheidung: $R_i \Rightarrow S$ $(i \in \{1, \dots, k\})$

iederspruchsbeweis: T führt an, setzt S falsch voraus, Annahme T wahr ↳ beweis T falsch.

xistenzbeweis: $\exists x\, P(x)$ für best. Universum und Prädikat P

eweis mittels Gegenbeispiel: $\neg \forall x\, P(x) \equiv \exists x\, \neg P(x)$

Relationsbeweise:

omposition v. Relationen: $a \rho\sigma c \Leftrightarrow \exists b: (a \rho b \wedge b \sigma c)$

$\rho(\sigma\square) = (\rho\sigma)\square$: $\rho(\sigma\square) \subseteq (\rho\sigma)\square$ (und umgekehrt.)

e: $a \rho b \wedge b \sigma c \wedge c \square d \to a \rho(\sigma\square) d$

ansitivität: $\forall a, b, c: (a \rho b \wedge b \rho c) \to (a \rho c)$

) Falls $a \rho b$ und $b \rho c$, dann $a \rho^2 c \to a \rho c$, da $\rho^2 \subseteq \rho$

) Sei ρ transitiv und $a \rho^2 b$ für einige a, b z. Z.: $a \rho b$. Per Definition $a\rho^2 b \to \exists c: a \rho c \rho b$, Transitivität ~~besagt: a ρ b~~ impliziert: $a \rho b$ □

hinese Remainder Theorem:

ls ein Set $|M| = n$ in k Partitionen, $k < n$ geteilt wird, t min. 1 Set $\lceil n/k \rceil$ Elemente.

eweis durch Wiederspruch: angenommen alle Sets haben ax $\lceil n/k \rceil - 1$ Elemente, dann gibt es max $k(\lceil n/k \rceil - 1)$ lemente, was weniger als n ist, da

$(\lceil n/k \rceil) < (n+1)k = n+k$ Theorem 2.9

evt. $< (\frac{n}{k} + 1)k = n + k$

sei $\rho = |$ (teilt): $\left.\begin{array}{l} a|b \to ax = b. \\ b|c \to by = c. \end{array}\right\} \to a\underbrace{x y}_{z} = c \to az = c$ ↳ $a|c$

rsicht: ist $n^2 - n + 41$ prime? Scheinbar ja, aber $n = 41 \Rightarrow 41^2 - 41 + 41$, 41^2 nicht prime.

$A \cup B) = (A \cup C) \not\Rightarrow B = C$. C könnte = $A \cup B$ sein!

$= \{1, 2\}$, $B = \{3, 4\}$, $C = \{1, 2, 3, 4\}$, $A \cup B = A \cup C = \{1, 2, 3, 4\} = C$

Nullteiler in $\langle \mathbb{Z}_n; \odot \rangle$:

z.B. $\mathbb{Z}_{10}$: PFZ: $10 = 2 \cdot 5$

ggT(a,n) > 1: ↳ [2], [5] sowie vielfache < 10: [4], [6], [8]

ggT(a,n) = 1: ↳ Einheiten: [1], [3], [7], [9] alle nicht nullteiler ausser 0 ↘ Gruppe: $\mathbb{Z}_n^*$

Lemma v. Euklid (L4.7)

Falls n prime ∧ $n | (x_1 \cdot x_2 \cdot \ldots \cdot x_k) \to n | x_i$, $i \in \{1, \dots, k\}$

Induktion: m = 1 ✓, $k \to k+1$: $n | (x_1 \cdot \ldots \cdot x_n \cdot x_{k+1})$, sei

$y = (x_1 \cdot \ldots \cdot x_k)$, $p | y x_{k+1}$

falls $p | y$: $p | x_i$, $i \in \{1, k\}$

falls $p \nmid y$: $ggT(p, y) = 1 \to (up + vy) = 1 \to$

$x_{k+1} = (up + vy) x_{k+1} = (u x_{k+1}) p + v (y x_{k+1})$

$\to p | x_{k+1}$

Gaps between Primes:

Können beliebig gross sein: für jedes $k \in \mathbb{N}$ existiert $n \in \mathbb{N}$ $\to \{n, n+1, \dots, n+k-1\}$ hat keinen Prim

Sei $n = (k+1)! + 2$, $2 \leq l \leq k+1$, l teilt $(k+1)! = n - 2$

$\to$ l teilt $(k+1)! + l = n - 2 + l$, weshalb $\{n, \dots, n+k-1\}$ nicht prime.

Multiplikativ Inverses:

$ax \equiv_m 1$ hat lösung $x \in \mathbb{Z}_m$, falls $ggT(a, m) = 1$

$ax = km + 1$, da $ggT(a, m)$ sowohl a als auch m teilt, teilt er auch $ax - km$. $ax - km = 1 \to ggT(a, m) = 1$

$\to$ falls $ggT(a, m) > 1 \to$ keine Lösung!

gemäss Lemma 4.4 $\to \exists u, v: ua + vm = ggT(a, m) = 1$

$vm \equiv_m 0 \to ua \equiv_m 1 \to x = u$ ist Lösung in $\mathbb{Z}$

$\to R_m(u)$ ist Lösung in $\mathbb{Z}_m$ eindeutig (siehe Modulo)

Zyklische Gruppen:

Eine Zyklische Gruppe der Ordnung n ist isomorph zu $\langle \mathbb{Z}_n; \oplus \rangle$ und dadurch abelsch

↳ Sei $G = \langle g \rangle$ zyklisch, order n, mit e als neutral

↳ bijektion $\mathbb{Z}_n \to G: i \mapsto g^i$ ist Gruppen isomorphismus, da $i \oplus j \mapsto g^{i+j} = g^i * g^j$, $\ominus i \mapsto g^{-i}$, $0 \mapsto e$

Sei G eine eine endliche Gruppe, $\to a^{|G|} = e$ $\forall a \in G$ (endlich ≠ zyklisch)

↳ $|G| = k \cdot ord(a) \to a^{|G|} = a^{k \cdot ord(a)} = (a^{ord(a)})^k = e^k = e$

Jede |Gruppe| = prime ist zyklisch, jedes $a \in G$ ist $\langle a \rangle$ ausser e

↳ $|G| = p$ $\forall a \in G$ $ord(a) \,|\, |G|$ $\begin{cases} ord(a) = 1 \to a = e \\ ord(a) = p \to \langle a \rangle = G \end{cases}$

Urbild:

$A = \{1, 2, 3, 4\}$, $B = \{a, b, c, d\}$ $f: A \to B$

$1 \mapsto a$

$2 \mapsto a$

$3 \mapsto b$

$4 \mapsto d$

$f = \{(1, a), (2, a), (3, b), (4, d)\}$

Theorem 5.15

$\mathbb{Z}_m^*$ ist zyklisch für $m = 2$, $m = 4$, $m = p^e$, $m = 2p^e$

p = ungerade prime, $e \geq 1$

z.B. $\mathbb{Z}_{19}^* = \langle 2 \rangle$: 2, 4, 8, 16, 13, 7, 14, 9, 18, 17, 15, 11, 3, 6, 12, 5, 10, 1

$G = \langle 2 \rangle, \langle 3 \rangle, \langle 10 \rangle, \langle 13 \rangle, \langle 14 \rangle, \langle 15 \rangle$

Quiz: 4 | pwacker | 5

Potenzmenge, P(A): $A = \{\emptyset, \{\emptyset\}, \{\emptyset, \emptyset\}\} = \{\emptyset, \{\emptyset\}\}$

$P(A) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$

Kardinalität, A, B beliebig:

$|B \cup (A \times \emptyset)| = |B|$, $|(A \times \emptyset)| = 0$

$|A \cap (B \cap \overline{B})| = 0$, $|(B \cap \overline{B})| = 0$

Fibonacci: $f_1 = 1$, $f_2 = 1$, $f_n = f_{n-1} + f_{n-2}$, $n > 2$

z.Z. $n > 0$: $f_{n+2} = 1 + \sum_{i=1}^{n} f_i$

Induktion: $n = 1$: $f_3 = f_2 + f_1 = 1 + f_1 = 2$ ✓

Schritt: $f_{(n+1)+2} = f_{n+3} \stackrel{IA}{=} (1 + \sum_{i=1}^{n} f_i) + f_{n+1} = 1 + \sum_{i=1}^{n+1} f_i$

Quiz 5:

A, B, C, beliebige Mengen:

$A \cup B = A \cup C \Rightarrow B = C$ Falsch z.B. $C = A \cup B$

$A \cap B = A \cap C \Rightarrow B = C$ Falsch: $A = \{1\}$, $B = \{2\}$, $C = \{3\}$

$(A \cup B) - (A \cap B) = (A \cup C) - (A \cap C) \Rightarrow B = C$ Wahr

$A \times B = B \times A$ Falsch

ρ relation auf A, $|A| > 0$

falls ρ nicht reflexiv → ρ irreflexiv Falsch

falls ρ irreflexiv → ρ nicht reflexiv Wahr

falls ρ symetrisch → ρ nicht antisymetrisch Falsch

falls ρ antisymetrisch → ρ nicht symetrisch Wahr

Quiz 6:

Def äquivalenz-Relation: reflexiv, symetrisch, transitiv

Def partionelle Ordnung: reflexiv, antisymetrisch, transitiv

$A = \{2, 3, 4, 5, 6, 7, 8\}$, $\rho = (|\cup \dagger)$, ρ = Äquivalenzrelation

Äquivalenzklassen: $\{2, 3, 4, 6, 8\}$, $\{5\}$, $\{7\}$

Quiz 7:

ggT(15, 18), kgV(15, 18): $15 = 2^0 \cdot 3^1 \cdot 5^1$, $18 = 2^1 \cdot 3^2 \cdot 5^0$

ggT: $2^0 \cdot 3^1 \cdot 5^0 = 3$, kgV: $2^1 \cdot 3^2 \cdot 5^1 = 90$ oder EEA für ggT und $kgV(a, b) = \frac{a \cdot b}{ggT(a, b)}$

$ggT(15, 18) = 15u + 18v \to$ EEA/Raten: $u = -1$, $v = 1$

$R_m(a+b) \neq R_m(a) + R_m(b)$ teilweise, nicht immer.

Sei $m = 9$, $a = 3$, $b = 4$: $R_9(3+4) = R_9(7) = 7 = 3 + 4 = R_9(3) + R_9(4)$ ✓

Sei $m = 2$, $a = b = 1$: $R_2(1+1) = R_2(2) = 0 \neq 2 = 1 + 1 = R_2(1) + R_2(1)$

$n^3 + 2n$ durch 3 teilbar für alle n? Ja!

$R_3(n) = 0$: $R_3(n^3 + 2n) = R_3(0^3 + 2 \cdot 0) = R_3(0) = 0$ ✓

$R_3(n) = 1$: $R_3(n^3 + 2n) = R_3(1^3 + 2 \cdot 1) = R_3(1 + 2) = R_3(3) = 0$ ✓

$R_3(n) = 2$: $R_3(n^3 + 2n) = R_3(2^3 + 2 \cdot 2) = R_3(8 + 4) = R_3(12) = 0$ ✓

In allen Fällen $R_3(n^3 + 2n) = 0 \to n^3 + 2n$ durch 3 teilbar

Quiz 8: Gruppe, Monoid, weder noch?

$\langle \mathbb{R}; \cdot \rangle$: Monoid

$\langle \mathbb{N} \setminus \{0\}; | \rangle$: Weder noch

$\langle P(\mathbb{N}); \cap \rangle$: Monoid

$\langle \mathbb{Q} \setminus \{0\}; \cdot \rangle$: Gruppe + Monoid

$\langle S, * \rangle$, e, e' neutral z.Z. $e = e'$: $e \stackrel{e' \text{Ne}}{=} e * e' \stackrel{e \text{Ne}}{=} e'$

$\langle S, *, e \rangle$, b, c inverse v. a:

$b \stackrel{e \text{Ne}}{=} b * e \stackrel{c \text{inv}}{=} b * (a * c) \stackrel{\text{associativ}}{=} (b * a) * c \stackrel{b \text{ inverse}}{=} e * c \stackrel{e \text{Ne}}{=} c$

$b = c$, a hat nur 1 Inverses!

$\mathbb{N}$ = Natürliche Zahlen, $\mathbb{Z}$ = Ganze Zahlen

$\mathbb{Q}$ = Rationale Zahlen, $\mathbb{R}$ = Reelle Zahlen

Quiz 9:

Anzahl Generatoren in Zyklischer Gruppe: $\varphi(n)$, $|G|=n$

Jede echte Untergruppe v. $|G|=25$ kommutativ: Ja

RSA: Sei (n,e) public Key, m Nachricht, y Cryptotext. Prüfen ob y Crypto von m, ohne Kentniss v. d: m mit (n,e) verschlüsseln und mit m vergleichen.

Wieviele Ringe $\langle R;+,0,\cdot,1\rangle$ mit $0\neq 1$ gibt es (bis auf Isomorphie)

↳ 1. Ringe mit Charakteristik 0: z.B. $\mathbb{Z}$
Ring mit Charakteristik 10: z.B. $\mathbb{Z}_{10}$

Quiz 10: Ring, Integritätsbereich, Körper?

$R[x]$ für Ring $R=\langle \mathbb{Z}_6;\oplus,\ominus,0,\odot,1\rangle$: Ring

$D[x]$ für Integritätsbereich $D=\langle \mathbb{Z};+,-,0,\cdot,1\rangle$: Ring, Integritätsbereich

$F[x]$ für Körper $F=\langle \mathbb{Z}_7;\oplus,\ominus,0,\odot,1\rangle$: Ring, Integritätsbereich

Teiler von $a(x)=2x+1$ im Ring $\mathbb{Z}_3[x]$: $1, 2, x+2, 2x+1$

Reduzibel/Irreduzibel v. Polynome über $\mathbb{Z}_3$:
x^2+x+2 irreduzibel, x^2+x+1 reduzibel, x^3+2x^2+1 irreduzibel
$x^4+2x^3+2x^2+2$ reduzibel

Quiz 11:

Gibt es Körper mit 2016 Elementen? Nein

Ring, Integritätsbereich, Körper?
$\mathbb{Z}_3[x]_{x^2+2x+2}$ für Körper $\langle \mathbb{Z}_3;\oplus,\ominus,0,\odot,1\rangle$
↳ Ring, Integritätsbereich, Körper
$\mathbb{Z}_3[x]_{x^2+2x+1}$ für Körper $\langle \mathbb{Z}_3;\oplus,\ominus,0,\odot,1\rangle$: Ring

Beweisen, dass Multiplikative Gruppe des Körpers $\mathbb{Z}_2[x]_{x^5+x^2+1}$ zyklisch ist, und finden sie Generator:
Ordnung Multiplikative Gruppe: $2^5-1=31$ (31 prim) → Korollar 5.11 → Gruppe zyklisch und jedes Element (ausser e / 1) ist Generator, z.B. $\langle x\rangle$

Quiz 12:

Beweissystem $\Pi=(S,P,\tau,\phi)$, $\tau: S\to\{0,1\}$, $\phi: S\times P\to\{0,1\}$
$\tau(s)=0$, $\phi(s,p)=1$ $\forall s\in S, \forall p\in P$: vollständig
$\tau(s)=0$, $\phi(s,p)=0$ $\forall s\in S, \forall p\in P$: vollständig & korrekt

Interpretation, $M=\{A\vee B, \neg A\wedge C\}$
$\mathcal{A}=\{A=0, B=1, C=1\}$ passend, nicht Modell
$\mathcal{A}=\{A=0, B=1, D=1\}$ weder passend, noch Modell
$\mathcal{A}=\{A=0, B=1, C=1, D=0\}$ passend und Modell

$A\vee B\vee C$ CNF: $(A\vee B\vee C)$ DNF: $(A)\vee(B)\vee(C)$ CNF ≡ DNF

Quiz 13:

$F:=\forall x((\exists y\, P(x,y))\wedge\neg P(x,y))\equiv\forall x((\exists y\, P(x,y))\wedge\neg P(x,z))$
z.B. $U=\mathbb{N}$, $P(x,y):=x<y$, $z=0$

$(\forall x F)\wedge G\models\forall x(F\wedge G)$: Falsch
$\forall x(F\wedge G)\models(\forall x F)\wedge G$: Wahr

z.B. Formel: $F=P(x)$, $G=Q(x)$ (Struktur: $U=\mathbb{N}$, $P(x)=(x\geq 0)$, $Q(x)=$ x is Prime und $x=2$

$\forall y(\exists z\, P(x,y,z)\wedge\forall x\,\neg Q(x))$ in bereinigte Pränexform (x: freie Variabel)
z.B. $\forall y\exists z\forall t(P(x,y,z)\wedge\neg Q(t))$

$GF(9)\cong GF(3)[x]_{x^2+1}$

Gültige Formel := Tautologie
Def 6.10

Mock-Exam:

Inverse v. 5 in $\mathbb{Z}_{17}^*$ ~~additiv: 12~~, multiplikativ: 7 (0 kommt nicht vor)

Anzahl Nullteiler von Ring $\langle\mathbb{Z}_{36};\oplus,\odot\rangle$: 23
↳ $|\langle\mathbb{Z}_{36};\oplus,\odot\rangle|=36\to 36-\varphi(36)-1$, $\varphi(36)$ = Einheiten, -1 = "Nullelement" ($0\cdot a=0$)

$\mathbb{R}$ überabzählbar nach Cantors 2. Diagonalargument

$P(M)\geq M$, falls $|M|$ unendlich → $P(M)$ überabzählbar.

$\sum_{i=1}^{n} i^2=\frac{n(n+1)(2n+1)}{6}$ IH: IV: Es gilt für $n=1$ ($n\to n+1$)
IS: $\sum_{i=1}^{n+1} i^2=\sum_{i=1}^{n} i^2+(n+1)^2=\frac{n(n+1)(2n+1)+6(n+1)(n+1)}{6}=\frac{(n+1)(n(2n+1)+6(n+1))}{6}$
$=\frac{(n+1)(2n^2+7n+6)}{6}=\frac{(n+1)((n+1)+1)(2(n+1)+1)}{6}$ □

$(A,\simeq)$ äquivalenzrelation, $(B,\preceq)$ partitielle Ordnung
$\leqslant$ Relation auf $A\times B$: $(a,b)\leqslant(a',b')\Leftrightarrow(a\simeq a')\wedge(b\preceq b')$
$\leqslant$ Reflexiv, da äquivalenz und po beide reflexiv. $(a,b)\in A\times B$: $(a,b)\leqslant(a,b)\Leftrightarrow a\simeq a\wedge b\preceq b$
$\leqslant$ Transitiv da $(a,b),(a',b'),(a'',b'')$: $(a,b)\leqslant(a',b')\leqslant(a'',b'')\to(a,b)\leqslant(a'',b'')\Leftrightarrow(a,b)\leqslant(a',b')\wedge(a',b')\leqslant(a'',b'')$
Def: $a\simeq c\wedge c\simeq e\Rightarrow a\simeq e$ (ist trans)
Def: $b\preceq b'\wedge b'\preceq b''\Rightarrow b\preceq b''$ (ist trans)
$\}\to(a,b)\leqslant(a'',b'')$
$\leqslant$ nicht antisymmetrisch da $a\in A$, $\exists\varepsilon\neq 0$ mit $a+\varepsilon\in A\to(a\simeq a+\varepsilon)\wedge(a+\varepsilon\simeq a)$
→ nicht antisymmetrisch

$A\subseteq B\Leftrightarrow P(A)\subseteq P(B)$: $(\Rightarrow)$ $U\subseteq A\xrightarrow{\text{da trans}} U\subseteq B\to U\in P(B)$
$\forall U(U\in P(A)\to U\in P(B))\xrightarrow{\text{Def}} P(A)\subseteq P(B)$, $U\subseteq A\xrightarrow{\text{def}} U\in P(A)$ damit folgt
$(\Leftarrow)$ Es gilt $A\in P(A)\Rightarrow A\in P(B)\xrightarrow{\text{Def}} A\subseteq B$

$R_{990}(5^{7^{22}})$: CRT: $x\equiv_2 a_1$ $R_2(5^{7^{22}})=1$
$x\equiv_5 a_2$ $R_5(5^{7^{22}})=0$
$x\equiv_9 a_3$ $R_9(5^{7^{22}})=R_9((5^{90})^{8}\cdot 5^2)=7$
$x\equiv_{11} a_4$ z.z. v. Fermat: $ggT(a,p)=1$: $a^{p}\equiv_p a\Leftrightarrow a^{p-1}\equiv_p 1$
$R_{11}(5^{7^{22}})=R_{11}((5^{72})^{10}\cdot 5^2)=3$
$a=5^{90}$, $p=9$ $R_9(5^{90})=1$
↳ $x=25$

$m,n\in\mathbb{N}$, $m>n$, $n\nmid m^2$, $gcd(m,n)=1$ z.Z. $mn\nmid m(m+n)$
$n\nmid m^2\wedge gcd(m,n)=1\to m>1\wedge n\nmid m\to\nexists k: m=kn\to\nexists k: m+n=kn$
$\Rightarrow n\nmid(m+n)\Rightarrow mn\nmid m(m+n)$ □

$a|b\to\forall c: a|bc$ $a|b\Rightarrow\exists k: b=ak$, $a|bc\Rightarrow\exists l: bc=al=akc=bc$ ($\exists k: akc=bc\to\exists m: bc=am$)
$a|b\wedge c|\frac{b}{a}\Rightarrow c|b\wedge a|\frac{b}{c}$ $c|\frac{b}{a}\to\exists k: ck=\frac{b}{a}\to\exists k: cka=b\to\exists m: cm=b\Rightarrow c|b$
$\to\exists m: cm=\frac{b}{a}\to\exists m: cma=b\to\exists m: ma=\frac{b}{c}\to a|\frac{b}{c}$ □

$3|(n^3-n)$ für alle n: $\Leftrightarrow n^3-n\equiv_3 0$, $n\in\{0,1,2\}$

Rechnen in GF(11):
$2+23=25\equiv_{11}3$, $2-23=-21\equiv_{11}-10\equiv_{11}1$
$10/3\equiv_{11}10\cdot$ inverses v. $3\equiv 10\cdot 4\equiv_{11}40\equiv_{11}7$

Prädikatenlogische Formel F mit Identität in der $f^{(2)}$ vorkommt, jedes Modell $\mathcal{A}$ von F gilt $\langle U^{\mathcal{A}}; f^{(2)\mathcal{A}}\rangle$ ist Gruppe.
↳ Gruppenaxiome formalisiert: Assoziativ, Neutral, Inverses
$\forall x\forall y\forall z(f(f(x,y),z)=f(x,f(y,z)))\wedge$
$\exists e\forall x((f(x,e)=f(e,x)=x)\wedge\exists y(f(x,y)=f(y,x)=e))$

$F=\neg((\forall x P(x,g(x)))\vee(\exists x\forall y(Q(x,f(z))\to\exists z R(y,z))))$

Freie Variabeln: z

Bereinigte Form: $\neg((\forall x P(x,g(x)))\vee\exists a\forall b(Q(a,f(z))\to\exists c R(y,c)))$

Pränex Form: $\exists x\exists a\forall b\forall c(\neg P(x,g(x))\wedge Q(a,f(z))\wedge\neg R(y,c))$

| pwacker |

$a\cdot x\equiv_m 1$ hat exakt 1 Lösung, falls $ggT(a,m)=1$

$\sqrt[42]{5}\in\mathbb{Q}$: Gegenannahme $\sqrt[42]{5}=\frac{a}{b}$, $ggT(a,b)=1$
nun gilt: $a^{42}=5b^{42}\to b|a^{42}$, $\forall$ primfaktoren von b
$p|a^{42}\to p|a$. Da $ggT(a,b)=1\to b=1\to a^{42}=5$
existiert nicht in $\mathbb{Q}\to\sqrt[42]{5}$ irrational ↯

$ab|c\Rightarrow a|c\wedge b|c$

Faktorisierung über $\mathbb{Z}_m$: 1) Finde NS von m
2) Finde inverses von NS, klammere $(x+inv)$ aus
3) Setze $(x+inv)(ax^2+bx+c)$, rechne aus
4) Berechne Koeffizient.

Resolutionskalkül: Formel in CNF bringen
nach $\wedge$ trennen: $F=(A\vee B)\wedge(C\vee\neg B)\to P=\{A,B\}$, $Q=\{C,\neg B\}$
$R=\{A,C\}$ $B,\neg B$ heben sich auf.
A, C möglich → Formel erfüllbar.
Falls $\neg F$ unerfüllbar: $\top$
Falls F unerfüllbar: $\bot$

Wie oft muss multiplikativ neutrales (1) addiert werden
Charakteristik: Körper/Ring: um additives (0) zu erhalten

n	φ(n)																
n	φ(n)	22	10	43	42	64	32	85	64	Prime:			283	421	547	673	82
2	1	23	22	44	20	65	48	86	42	2	73	179	293	431	557	677	82
3	2	24	8	45	24	66	20	87	56	3	79	181	307	433	563	683	82
4	2	25	20	46	22	67	66	88	40	5	83	191	311	439	569	691	83
5	4	26	12	47	46	68	32	89	88	7	89	193	313	443	571	701	85
6	2	27	18	48	16	69	44	90	24	11	97	197	317	449	577	709	85
7	6	28	12	49	42	70	24	91	72	13	101	199	331	457	587	719	859
8	4	29	28	50	20	71	70	92	44	17	103	211	337	461	593	727	863
9	6	30	8	51	32	72	24	93	60	19	107	223	347	463	599	733	877
10	4	31	30	52	24	73	72	94	46	23	109	227	349	467	601	739	881
11	10	32	16	53	52	74	36	95	72	29	113	229	353	479	607	743	883
12	4	33	20	54	18	75	40	96	32	31	127	233	359	487	613	751	887
13	12	34	16	55	40	76	36	97	96	37	131	239	367	491	617	757	907
14	6	35	24	56	24	77	60	98	42	41	137	241	373	499	619	761	91
15	8	36	12	57	36	78	24	99	60	43	139	251	379	503	631	769	91
16	8	37	36	58	28	79	78	100	40	47	149	257	383	509	641	773	92
17	16	38	18	59	58	80	32	101	100	53	151	263	389	521	643	787	93
18	6	39	24	60	16	81	54	102	32	59	157	269	397	523	647	797	94
19	18	40	16	61	60	82	40	103	102	61	163	271	401		653	809	94
20	8	41	40	62	30	83	82	104	48	67	167	277	409		659	811	95
21	12	42	12	63	36	84	24	105	48	71	173	281	419	541	661	821	96