Diskrete Mathematik

Zusammenfassung HS2020 Robin Sieber

D2.1 Mathematical statement is either true or false, Proposition/Assertion/Claim

D2.2 True proposition: Theorem, Lemma, Corollary; Unknown: Conjecture, Assumption

D2.3 (Informal) Proof: Sequence of simple, easily verifiable, consecutive steps. Starts from a set of axioms and known facts. Each step applying a derivation rule. 3 Levels: Proof sketch (describe non-obvious ideas) Complete proof (state every applied rule/def.) Formal proof (phrased in a calculus)

D2.5 Negation $\neg A$; Conjunction $A \wedge B$; Disjunction $A \vee B$ Imp. $A \to B \equiv \neg A \vee B \equiv \neg B \to \neg A$

D2.6 Formula: correctly formed expression with symbols A, B, C and logical operators

D2.7 $F \equiv G$ (equivalent): truth values are equal for all truth assignments

L2.1 idempotence $A \wedge A \equiv A$, $A \vee A \equiv A$; commutativity $A \wedge B \equiv B \wedge A$, $A \vee B \equiv B \vee A$ associativity $(A \wedge B) \wedge C \equiv A \wedge (B \wedge C)$, $(A \vee B) \vee C \equiv A \vee (B \vee C)$, double negation $\neg\neg A \equiv A$ absorption $A \wedge (A \vee B) \equiv A$, $A \vee (A \wedge B) \equiv A$, dist. $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$ dist. $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$, de Morgan $\neg(A \wedge B) \equiv \neg A \vee \neg B$, $\neg(A \vee B) \equiv \neg A \wedge \neg B$

D2.8 A formula G is a logical consequence of F ($F \models G$) if for all truth assignments to the propositional symbols appearing in F or G, the truth value of G is 1 if the truth values of F is 1.

D2.9 F is called tautology or valid if it's true for all truth assignments ($\models F, \top$)

D2.10 F is called satisfiable if it's true for at least one truth assignment, unsatisfiable else ($\bot$).

L2.2,2.3 $F \equiv \top \Leftrightarrow \neg F \equiv \bot$; $F \to G \equiv \top \Leftrightarrow F \models G$

D2.11 A k-ary predicate P on U is a function $U^k \to \{0,1\}$

D2.12 Quantifiers $\forall x\, P(x)$ ($P(x)$ is true for all x in U); $\exists x\, P(x)$ (true for some x in U)

L2.4 For any F and G, if $F \models G$, then "F is valid $\Rightarrow$ G is valid" is true.

D2.13 Comp. of implications: If $S \Rightarrow T$ and $T \Rightarrow U$ both true, then $S \Rightarrow U$ also true.

L2.5 $(A \to B) \wedge (B \to C) \models A \to C$

D2.14 Direct proof: prove $S \Rightarrow T$ by assuming S and proving T under this assumption.

D2.15 Indirect proof: prove $S \Rightarrow T$ by assuming T false and proving S false (contraposition)

D2.16 Modus ponens: Find stmt. R; Prove R; Prove $R \Rightarrow S$ $[A \wedge (A \to B) \models B]$ (L2.7)

D2.17 Case distinction: Find finite list $R_1, \dots, R_k$ (cases); Prove one R_i true (case occurs); Prove $R_i \Rightarrow S$

L2.8 $(A_1 \vee \dots \vee A_k) \wedge (A_1 \to B) \wedge \dots \wedge (A_k \to B) \models B$ ($k=1 \equiv$ Modus ponens) (proof by induction)

D2.18 Contradiction: Find suitable T; Prove T false; Assume S false and prove T true ($\Rightarrow$ contradiction $\Rightarrow S$ must be true)

L2.9 $(\neg A \to B) \wedge \neg B \models A$

D2.19 Existence set X of parameters, for each $x \in X$ a stmt S_x. Prove at least one S_x true. Proof is constructive if it exhibits an a s.t. S_a true, else non-const.

D2.20 Pigeonhole set $|S| = n$, partitioned into $k < n$ sets, then one sets has $\lceil \frac{n}{k} \rceil$ elems.

D2.20 Counterexample set X of param., for each $x \in X$ stmt S_x. Find an a s.t. S_a is false

T2.11 Induction Basis step: Prove $P(0)$; Induction step: Prove for arb. n $P(n) \Rightarrow P(n+1)$

$P(0) \wedge \forall n (P(n) \to P(n+1)) \Rightarrow \forall n\, P(n)$ (for arb. n, not for ∞)

D3.1 Number of elements of a finite set is called cardinality, $|A|$

E3.2 $\{1,2,3\} = \{1,3,2,3\} = \{3,1,1,3\} = \{n \in \mathbb{N} \mid 0 < n < 4\}$ (order & multiple occurrences irrelevant → set description not unique)

D3.2 $A = B \overset{\text{def}}{\Leftrightarrow} \forall x (x \in A \leftrightarrow x \in B)$ Set is completely specified by its elements (No other property)

L3.1 For any a, b, $\{a\} = \{b\} \Rightarrow a = b$ (indirect proof)

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

D3.4 empty set $\phi, \{\}, \forall x (x \notin \phi)$. **L3.2** ϕ unique; **L3.3** $\forall A (\phi \subseteq A)$ (proof by contradict. Ass. $\phi \not\subseteq A$)

D3.5 power set $P(A)$ Set of all subsets of A $P(A) \overset{\text{def}}{=} \{S \mid S \subseteq A\}$; $|P(A)| = 2^{|A|}$

D3.6 union $A \cup B \overset{\text{def}}{=} \{x \mid x \in A \vee x \in B\}$; intersection $A \cap B \overset{\text{def}}{=} \{x \mid x \in A \wedge x \in B\}$

D3.7 complement $\bar{A} \overset{\text{def}}{=} \{x \in U \mid x \notin A\}$ (U = universe)

D3.8 difference $B \setminus A \overset{\text{def}}{=} \{x \mid x \in B \wedge x \notin A\}$ consist. $A \subseteq B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B$

T3.4 idem., commut., associat., distr., absorb. → L2.1; Proof: implication by law for logical operators

D3.9 cartesian product $A \times B = \{(a,b) \mid a \in A \wedge b \in B\}$ ordered pair $(a,b) = (c,d) \overset{\text{def}}{\Leftrightarrow} a = c \wedge b = d$ $|A \times B| = |A| \cdot |B|$; $\phi \times A = \phi$

D3.10 (binary) relation ρ from A to B is a subset of $A \times B$. If $A = B$, then ρ is a rel. on A $a \rho b \Leftrightarrow (a,b) \in \rho$; for any S, "$\subseteq$" is a rel. on $P(S)$; empty relation → $\rho = \phi$, complete relation → $\rho = A \times B$

D3.12 inverse $\hat{\rho} = \{(a,b) \mid (b,a) \in \rho\}$; $a \rho b \Leftrightarrow b \hat{\rho} a$; matrix representation → transposition

D3.13 composition $A \overset{\rho}{\to} B \overset{\sigma}{\to} C$, $\rho \circ \sigma \overset{\text{def}}{=} \{(a,c) \mid \exists b \in B ((a,b) \in \rho \wedge (b,c) \in \sigma)\}$ ($\rho \circ \sigma$)

L3.5 associativity $\rho \circ (\sigma \circ \phi) = (\rho \circ \sigma) \circ \phi$ (proof with D3.3)

L3.6 $\widehat{\rho\sigma} = \hat{\sigma}\hat{\rho}$; Proof: $\widehat{\rho\sigma} = \{(c,a) \mid a \rho\sigma c\} = \{(c,a) \mid \exists b \in B (a \rho b \wedge b \sigma c)\} = \{\dots \mid \exists b (c \hat{\sigma} b \wedge b \hat{\rho} a)\}$

D3.14 reflexive $a \rho a$ for all $a \in A$ ($\mathrm{id} \subseteq \rho$) **D3.15** irreflexive $\rho \cap \mathrm{id} = \phi$ (↳ matrix diagonal = 0)

D3.16 symmetric $a \rho b \Leftrightarrow b \rho a$ for all $a, b \in A$ ($\rho = \hat{\rho}$); matrix symmetric

D3.17 antisymmetric $(a \rho b \wedge b \rho a) \Rightarrow a = b$ for all $a, b \in A$ ($\rho \cap \hat{\rho} \subseteq \mathrm{id}$)

D3.18 transitive $(a \rho b \wedge b \rho c) \Rightarrow a \rho c$ for all $a, b, c \in A$; Graphendarstellung ↳ Abkürzung

L3.7 A relation is transitive if and only if $\rho^2 \subseteq \rho$ (prove "$\Leftrightarrow$" in both dir.)

D3.19 transitive closure of ρ on A: $\rho^* = \bigcup_{n \in \mathbb{N}_{\geq 1}} \rho^n$

D3.20 equivalence relation on A that is reflexive, symmetric and transitive

D3.21 equivalence class $[a]_\theta \overset{\text{def}}{=} \{b \in A \mid b \theta a\}$ where θ is a equiv. rel., $a \in A$

L3.8 intersection of 2 equiv. rel. is a equiv. rel. (e.g. $\equiv_3$ and $\equiv_5$ is $\equiv_{15}$)

D3.22 partition of a set A: Set of mutually disjoint subsets; $S_i \cap S_j = \phi$ $(i \neq j)$; $\bigcup_{i \in I} S_i = A$

D3.23 set of equiv. classes $A/\theta \overset{\text{def}}{=} \{[a]_\theta \mid a \in A\}$ "quotient set of A by θ", "A mod θ"

T3.9 A/θ is a partition of A. Proof: $a \theta b \Rightarrow [a] = [b]$ Proof: arb. $c \in [a] \Leftrightarrow c \theta a \Rightarrow c \theta b \Rightarrow c \in [b]$; $a \not\theta b \Rightarrow [a] \cap [b] = \phi$ Proof by contrad. $\to \exists c\ c \in [a] \cap [b]$, then transitivity

D3.24 partial order rel. on A reflexive, antisymmetric, transitive poset $(A; \leqslant)$

D3.25 For a poset $(A; \leqslant)$ a, b are comparable if $a \leqslant b \mid b \leqslant a$, else incomparable

D3.26 If any two elements of $(A; \leqslant)$ are comparable, A is totally/linearly ordered

D3.27 In a poset $(A; \leqslant)$ b covers a if $a < b$ and $\nexists c (a < c \wedge c < b)$ (between a and b)

D3.28 Hasse diagram of $(A; \leqslant)$ is the directed graph. Vertices = elements; edge if b covers a

T3.10 $(A; \leqslant), (B; \sqsubseteq)$: $(a_1, b_1) \leqslant (a_2, b_2) \overset{\text{def}}{\Leftrightarrow} a_1 \leqslant a_2 \wedge b_1 \sqsubseteq b_2$ ($\leqslant$ on $A \times B$ is a part. ord. rel.)

T3.11 $(A; \leqslant), (B; \sqsubseteq)$: $(a_1, b_1) \leqslant_{\text{lex}} (a_2, b_2) \Leftrightarrow a_1 < a_2 \vee (a_1 = a_2 \wedge b_1 \sqsubseteq b_2)$ ($\leqslant_{\text{lex}}$ is a part. ord.)

D3.29 $(A; \leqslant)$: a is a minimal (maximal) elem. of A if $\nexists b \in A$ with $b < a$ ($b > a$); a is a least (greatest) elem. of A if $a \leqslant b$ ($a \geqslant b$) for all $b \in A$ (might not exist)

$S \subseteq A$: lower (upper) bound of S if $a \leqslant b$ ($a \geqslant b$) for all $b \in S$; gr. lower bound (least upper bound) of S if a is the gr. (least) elem. of the set of all lower (upper) bounds of S.

D3.30 $(A; \leqslant)$ is well-ordered if it's totally ordered and every non-empty subset has a least elem. [finite ∧ totally ord. → well-ord.]

D3.31 $(A; \leqslant), a, b \in A$: meet: greatest lower bound of a and b, $a \wedge b$; join: least upper bound of a and b, $a \vee b$ (don't have to exist)

D3.32 $(A; \leqslant)$ where every pair of elems. has a meet and join is called a lattice

D3.33 function $f: A \to B$ is a rel. Ⓐ totally defined $\forall a \in A \exists b \in B\ a f b$ Ⓑ well-defined $\forall a \forall b, b' (a f b \wedge a f b' \to b = b')$

D3.34 set of all functions $A \to B$ denoted as B^A

D3.35 partial function cond. Ⓐ doesn't hold

D3.36 (Pre)image $\mathrm{Im}(f) = f(A) \overset{\text{def}}{=} \{f(a) \mid a \in A\}$; $\mathrm{Im}(f) \subseteq B$; preimage $f^{-1}(B) \overset{\text{def}}{=} \{a \in A \mid f(a) \in B\}$

D3.38 surjective $f(A) = B$ $\forall b \in B\ \exists a \in A\ b = f(a)$ injective $a \neq b \Rightarrow f(a) \neq f(b)$ bijective both

D3.40 inverse function f^{-1} exists for bijective functions (→ D3.12)

D3.41 composition of $f: A \to B$, $g: B \to C$, $c = g \circ f(a) = g(f(a))$ Andere Reihenfolge als bei "normalen" Relationen!

L3.12 Function composition is associative $(h \circ g) \circ f = h \circ (g \circ f)$ Proof: L3.5

D3.42 equinumerous, $A \sim B$, if there exists a bijection $A \leftrightarrow B$ if finite: $|A|=|B|$

A dominates B, $A \succcurlyeq B$, if $A \sim C$ for some $C \subseteq B$ or an injection $A \to B$

A is countable if $A \preccurlyeq \mathbb{N}$ and uncountable otherwise

L3.13 (i) $\preccurlyeq$ is transitive $A \preccurlyeq B \wedge B \preccurlyeq C \Rightarrow A \preccurlyeq C$ (ii) $A \subseteq B \Rightarrow A \preccurlyeq B$ Proof (i): comp. of injections Proof (ii): id is an injection

T3.14 $A \preccurlyeq B \wedge B \preccurlyeq A \Rightarrow A \sim B$ T3.15 No cardinality level between finite and countably inf.

T3.16 set of finite binary seq. $\{0,1\}^* = \{\underbrace{\varepsilon}_{\text{empty string}}, 0, 1, 00, 01, \dots\}$ is countable T3.17 $\mathbb{N}^2$ is countable

C3.18 $A \preccurlyeq \mathbb{N} \wedge B \preccurlyeq \mathbb{N} \Rightarrow A \times B \preccurlyeq \mathbb{N}$ C3.19 $\mathbb{Q}$ is countable

T3.20 A, A_i countable, $i, n \in \mathbb{N}$ (i) A^n countable (ii) $\bigcup_i A_i$ countable (iii) A^* countable (finite seq. of elems. of A)

D3.43 semi-infinite binary seq. $\{0,1\}^\infty$ T3.21 $\{0,1\}^\infty$ is uncountable Proof: Cantor diagonalization

D3.44 $f: \mathbb{N} \to \{0,1\}$ is computable if there is a program that outputs $f(n)$ for every n

C3.22 There are uncomputable functions $\mathbb{N} \to \{0,1\}$

Diffie/Hellman

Alice insecure Bob

Choose x_A $y_A = g^{x_A}$ $y_B = g^{x_B}$ Choose x_B

$y_B^{x_A} = k_{AB} = k_{BA} = y_A^{x_B}$

$= g^{x_A x_B}$

RSA

$n = p \cdot q$ (p, q prim) $\varphi(n) \overset{\text{hard}}{=} (p-1)(q-1)$ (easy) public secret

① Wähle p, q prim (gross)

② $n = p \cdot q$

③ $f = \varphi(n) = \varphi(p) \cdot \varphi(q) = (p-1)(q-1)$ (private key)

④ $e \in \mathbb{Z}_n^*$ (public key)

⑤ $d \equiv_f e^{-1} \iff e \cdot d \equiv_f 1$ (EEA)

Encrypt: $c = R_n(m^e)$ Decrypt: $m = R_n(c^d) = R_n(m^{e \cdot d})$

EEA

$5x \equiv_{13} 1$

$\to 5 \equiv_{13} 18$

$\to 18 - 13 \cdot 1 = 5$

$13 - 5 \cdot 2 = 3$

$5 - 3 \cdot 1 = 2$

$3 - 2 \cdot 1 = 1$

$3 - (5 - 3 \cdot 1) \cdot 1 = 1$

$2 \cdot 3 - 5 \cdot 1 = 1$

$2 \cdot (13 - 5 \cdot 2) - 5 \cdot 1 = 1$

$2 \cdot 13 - 5 \cdot 5 = 1$

$2 \cdot 13 - 5 \cdot (18 - 13) = 1$

$(-3) \cdot 13 - 5 \cdot 18 = 1$

$\equiv 10 \cdot 13 + 8 \cdot 18 = 1 \mod$

$x \equiv 8$, $y \equiv 5$

D4.1 a divides b $(a|b)$ if $\exists c\,(b = ac)$ (a divisor, c quotient)

T4.1 For all $a, d \neq 0$, exist unique ints q, r s.t. $a = dq + r$ and $0 \leqslant r < |d|$; $r = R_d(a)$

D4.2 d is gcd of a, b if $d|a \wedge d|b \wedge \forall c((c|a \wedge c|b) \to c|d)$; $\mathbb{Z}: \pm d$ are gcds

D4.3 $\gcd(a,b) \geqslant 1$; a and b are relatively prime iff $\gcd(a,b) = 1$

L4.2 For any ints m, n, q, we have $\gcd(m, n - qm) = \gcd(m, n) = \gcd(m, R_m(n))$

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

L4.3/4.4 a, b not both 0, if $(a,b) = (d)$, $d = \gcd(a,b)$ C4.5 $\exists u, v\,(\gcd(a,b) = ua + vb)$

D4.5 l is lcm of a, b if $a|l \wedge b|l \wedge \forall m((a|m \wedge b|m) \to l|m)$ $\operatorname{lcm} \cdot \gcd = a \cdot b$

$a = \prod_i p_i^{e_i}$, $b = \prod_i p_i^{f_i}$; $\gcd = \prod_i p_i^{\min(e_i, f_i)}$ $\operatorname{lcm} = \prod_i p_i^{\max(e_i, f_i)}$

D4.6 positive int > 1 is prime if its only divisors are 1 and p, else they are called composites

T4.6 Every pos. int can be written uniquely as the product of primes

T4.8 $\sqrt{n}$ is irrational unless n is a square

L4.12 Every composite int n has a prime divisor $\leqslant \sqrt{n}$

L4.13 For any $m \geqslant 1$ $\equiv_m$ is an equiv. rel. on $\mathbb{Z}$. $\equiv_m$ has m equiv. classes $([0], [1], \dots [m-1])$

D4.8 modulo congruence $a, b, m \in \mathbb{Z}, m \geqslant 1$ $a \equiv_m b \overset{\text{def}}{\iff} m|(a-b)$ $a = b \Rightarrow a \equiv_m b$, $a \neq_m b \Rightarrow a \neq b$

L4.14 If $a \equiv_m b$ and $c \equiv_m d$, then $a + c \equiv_m b + d$ and $ac \equiv_m bd$

C4.15 $f(x_1, x_2, \dots, x_k)$ polynomial (deg $k-1$), int coeff. if $a_i \equiv_m b_i$ $\forall i$, then $f(a_1, \dots, a_k) \equiv_m f(b_1, \dots, b_k)$

L4.16 (i) $a \equiv_m R_m(a)$ (ii) $a \equiv_m b \iff R_m(a) = R_m(b)$

C4.17 $f(x_1, \dots, x_k)$ polynomial, int coeff., then $R_m(f(a_1, \dots, a_k)) = R_m(f(R_m(a_1), \dots, R_m(a_k)))$

E4.13 $R_{24}(7^{100}) = R_{24}((7^2)^{50}) = R_{24}(R_{24}(7^2)^{50}) = R_{24}(1^{50}) = 1$

E4.15 Check result by taking it modulo 11 (alternating cross sum)

L4.18 congruence equation $ax \equiv_m 1$ has a (unique) solution iff $\gcd(a,m) = 1$

D4.9 If $\gcd(a,m) = 1$, x in $ax \equiv_m 1$ is called multiplicative inverse $x \equiv_m a^{-1}$

T4.19 CRT $m_1, \dots, m_r$ rel. prime, $M = \prod_{i=1}^r m_i$, $a_1, \dots, a_r$ with $0 \leqslant a_i < m_i$, $1 \leqslant i \leqslant r$, $x \equiv_{m_1} a_1, \dots, x \equiv_{m_r} a_r$, $0 \leqslant x \leqslant M$ (unique)

① Calc. M, $M_i = M/m_i$ $\forall i$ ② Find N_i s.t. $M_i N_i \equiv_{m_i} 1$ $\forall i$ ③ $x = \sum_{i=1}^r a_i M_i \cdot N_i$

Ex. $2x^2 + 8 \equiv_{13} 6$, $x \equiv_{15} 2$

$\Rightarrow 2x^2 \equiv_{13} 11 \equiv_{13} 24 \Rightarrow x^2 \equiv_{13} 12$

$\to x = \pm 5 \Rightarrow x \equiv 8$, $x \equiv 5$

$x \equiv_{13} 5$ $x \equiv_{13} 8$

$x \equiv_{13} 2$ $x \equiv_{13} 2$

$M = 195 \to 15x_1 \equiv_{13} 1$ $13x_2 \equiv_{15} 1$

$\to x_1 = 2$ $x_2 = 2$

$\to x = 5 \cdot 15 \cdot 7 + 2 \cdot 13 \cdot 7 = 707 \equiv_{195} 122$

$x' = 8 \cdot 15 \cdot 7 + 2 \cdot 13 \cdot 7 = 47$

D5.1 operation func. $S^n \to S$, $n \geqslant 0$ "arity" of the operation n ($0 \to$ constant, $1 \to$ unary, $2 \to$ binary)

D5.2 algebra $\langle S; \Omega \rangle$ with carrier (set) S, $\Omega = (\omega_1, \dots, \omega_n)$ list of ops on S

D5.3 neutral element $e \in S$ s.t. $e * a = a * e = a$ for all $a \in S$ (LNE, RNE)

L5.1 $\langle S; * \rangle$ has at most one NE Proof: LNE: $e * e' = e'$, RNE: $e * e' = e$ $\Rightarrow e' = e$

D5.4 binary operation $*$ is associative if $a * (b * c) = (a * b) * c$ for all $a, b, c \in S$

D5.5 monoid is an algebra $\langle M; *, e \rangle$ where $*$ associative, e NE

D5.6 inverse element of a ($a, b \in S$), s.t. $\underbrace{b}_{\text{left inv.}} * a = a * \underbrace{b}_{\text{right inv.}} = e$

L5.2 Monoid $\langle M; *, e \rangle$, $a \in M$ can have at most one inverse Proof: b left inv., c right inv. $b = b * e = b * (a * c) = (b * a) * c = e * c = c$

D5.7 group $\langle G; *, \hat{}, e \rangle$ G1 $*$ associative G2 e is NE $a * e = e * a = a$ for all $a \in G$ G3 $\forall a \in G\, \exists \hat{a}$ $a * \hat{a} = \hat{a} * a = e$

D5.8 group/monoid is called abelian/commutative if $a * b = b * a$ for all $a, b \in G$

L5.3 (i) $\widehat{(\hat{a})} = a$ (ii) $\widehat{a * b} = \hat{b} * \hat{a}$ (iii) left cancellation law $a * b = a * c \Rightarrow b = c$ (iv) right cancellation law $b * a = c * a \Rightarrow b = c$

(v) $a * x = b$, $x * a = b$ have unique solutions x for any a and b.

D5.9 direct product of n groups $\langle G_1; *_1 \rangle, \dots, \langle G_n; *_n \rangle$ is the algebra $\langle G_1 \times \cdots \times G_n; * \rangle$, component-wise operation $(a_1, \dots, a_n) * (b_1, \dots, b_n) = (a_1 *_1 b_1, \dots, a_n *_n b_n)$

L5.4 $\langle G_1 \times \cdots \times G_n; * \rangle$ is a group. NE and inverse are component-wise

D5.10 group homomorphism $\phi: \langle G; *, \hat{}, e \rangle \to \langle H; \star, \tilde{}, e' \rangle$ if $\phi(a * b) = \phi(a) \star \phi(b)$ isomorphism if ϕ is bijective $G \cong H$

L5.5 group homomorphism $\phi: G \to H$ (i) $\phi(e) = e'$ (ii) $\phi(\hat{a}) = \widetilde{\phi(a)}$ PW: $\phi(a^n) = \phi(a)^n$

D5.11 $H \subseteq G$ of group G is a subgroup if $\langle H; *, \hat{}, e \rangle$ is a group and (1) $a * b \in H$, $\forall a, b \in H$ (2) $e \in H$ (3) $\hat{a} \in H$ for all $a \in H$

D5.12 order of $a \in G$, $\operatorname{ord}(a)$ is the least $m \geqslant 1$ s.t. $a^m = e$, if not possible $\operatorname{ord}(a) = \infty$ $\operatorname{ord}(a) = 1$

L5.6 In a finite group, every element has finite order Proof: G finite $\Rightarrow \exists r, s$ $a^r = a^s = b$, $r < s$ $a^{s-r} = a^s \cdot a^{-r} = b \cdot b^{-1} = e$

D5.13 For a finite group G, $|G|$ is the order of G (element count)

D5.14 group generated by $a \in G$ $\langle a \rangle \overset{\text{def.}}{=} \{a^n \mid n \in \mathbb{Z}\} \overset{\text{def.}}{=}$ smallest subgroup containing a $\{e, a, a^2, \dots, a^{\operatorname{ord}(a)-1}\}$

D5.15 group $G = \langle g \rangle$ generated by g is cyclic and g is a generator of G If g is gen., then g^{-1} too

T5.7 A cyclic group of order n is isomorphic to $\langle \mathbb{Z}_n; \oplus \rangle$, hence abelian Proof: Bijection $\mathbb{Z}_n \to G$ $i \mapsto g^i$ $i \oplus j \mapsto g^i * g^j = g^j * g^i$

T5.8 (Lagrange) G finite, H subgroup of G, then $|H|$ divides $|G|$

C5.9 Finite group G, $\operatorname{ord}(a)$ divides $|G|$ for every $a \in G$ Proof: $\langle a \rangle$ is a subgroup $\to$ T5.8

C5.10 Finite group G, $a^{|G|} = e$ for every $a \in G$ Proof: $a^{|G|} = a^{k \cdot \operatorname{ord}(a)} = (a^{\operatorname{ord}(a)})^k = e^k = e$

C5.11 Every group of prime order is cyclic ($\to$ abelian), every elmt. except NE is a gen. Proof: $a \neq e$ must have order $p \Rightarrow$ cyclic

D5.16 $\mathbb{Z}_m^* \overset{\text{def}}{=} \{a \in \mathbb{Z}_m \mid \gcd(a,m)=1\}$ D5.17 Euler function $\varphi: \mathbb{Z}^+ \to \mathbb{Z}^+$ $\varphi(m) = |\mathbb{Z}_m^*|$

L5.12 $\varphi(m) = \prod (p_i-1)p_i^{e_i-1}$ $m = 2\cdot2\cdot3\cdot5\cdot5\cdot17$ $\varphi(m) = 1\cdot2\cdot2\cdot4\cdot5\cdot16$ $\varphi(m\cdot n) = \varphi(m)\cdot\varphi(n)$ $\varphi(p) = p-1$ (prime)

T5.13 $\langle \mathbb{Z}_m^*; \odot, ^{-1}, 1\rangle$ is a group Proof: associativity inherited, $1 \in \mathbb{Z}_m^*$; closure under $\odot$: if $\gcd(a,m)=1$ and $\gcd(b,m)=1$, then $\gcd(ab,m)=1$ too

C5.14 (Fermat/Euler) For all $m \geq 2$ and all a s.t. $\gcd(a,m)=1$: $a^{\varphi(m)} \equiv_m 1$;
and for every prime p and every a not divisible by p: $a^{p-1} \equiv_p 1$
Proof: Follows from Cor. 5.10 for $\mathbb{Z}_m^*$

T5.15 $\mathbb{Z}_m^*$ is cyclic $\Leftrightarrow$ $m = 2, 4, p^e, 2p^e$ (p: odd prime, $e \geq 1$)

T5.16 G finite mult. group $x \mapsto x^e$ bijection, unique e-th root of $y \in G$ is x: $x^e = y$,
$e \in \mathbb{Z}$, $\gcd(e,|G|)=1$ where $x = y^d$ with $e\cdot d \equiv_{|G|} 1$ Proof: $ed = k\cdot|G|+1 \Rightarrow (x^e)^d = (x^{|G|})^k \cdot x = e^k x = x$

D5.18 Ring $\langle R; +, -, 0, \cdot, 1\rangle$ (+: Ass, NE, Com; ·: Ass, NE; -: NE)
(i) $\langle R; +, -, 0\rangle$ is a commutative group Ring is commut. if mult. is commut.
(ii) $\langle R; \cdot, 1\rangle$ is a monoid
(iii) left + right dist. law $a(b+c) = (ab)+(ac)$; $(b+c)a = (ba)+(ca)$ $\forall a,b,c \in R$

L5.19
(i) $0a = a0 = 0$ Proof: $0 = -(a0)+a0 = -(a0)+a(0+0) = -(a0)+a0+a0 = 0+a0 = a0$, same for $0a=0$
(ii) $(-a)b = -ab$ Proof: too hard
(iii) $(-a)(-b) = ab$
(iv) If R non-trivial ($|R|>1$), then $1 \neq 0$ Proof: Ass. $1=0$ ($a \neq 0$) $\overset{a0=0}{\Rightarrow} a1 = a \overset{(i)}{(\text{def. NE})}$ $\Rightarrow$ contradiction

D5.19 characteristic of a ring: order of 1 in the additive group if finite, otherwise by def. 0 (!)

D5.20 (commutative!) $a,b \in R$, $a \neq 0$: a divides b ($a|b$) if exists $c \in R$ s.t. $b = ac$ (a divisor of b, b multiple of a)

L5.18 (i) $a|b$ and $b|c$, then $a|c$ (transitivity) (iii) $a|b$ and $a|c$, then $a|(b+c)$
(ii) If $a|b$, then $a|bc$ for all c ↳ Proof: $b = ax$, $c = ay$ $\Rightarrow b+c = ax+ay = a(x+y)$

D5.21 $a,b,d \in R$: d is greatest common divisor if $d|a \wedge d|b \wedge \forall c((c|a)\wedge(c|b) \to c|d)$

D5.22 $a \neq 0 \in R$ is a zerodivisor if $ab = 0$ for some $b \neq 0 \in R$

D5.23 $u \in R$ is a unit if u is invertible ($uv = vu = 1$ for some $v \in R$) set of units in R, den. R^*

L5.19 For a ring R, R^* is a multiplicative group. Proof: Abgeschlossenheit zeigen: $u,v \in R^* \to uv \in R^*$
$\to \exists (uv)^{-1} = v^{-1}u^{-1} \in R$, associativity inherited

D5.24 Integral domain is a non-trivial comm. ring without zerodivisors: $\forall a \forall b (ab = 0 \to a = 0 \vee b = 0)$

E5.11 m prime $\Rightarrow \mathbb{Z}_m$ is ID; If $m = ab$, then a,b are zerodivisors in $\mathbb{Z}_m$.

L5.20 ID: if $a|b$, then c s.t. $b = ac$ is unique ($c = b/a$ is called quotient) Proof: $b = ac = ac'$, $a \neq 0$
$0 = b+(-b) = a(c+(-c))$

D5.25 polynomial over a ring $R[x]$ $a(x) = \sum_{i=0}^{d} a_i x^i$ $a_i \in R$, $d \geq 0$ $\deg(a(x))$ greatest i with $a_i \neq 0$, $\deg(0) = -\infty$

T5.21 For any ring R, $R[x]$ is a ring. Proof: Check D5.18 → (i) by def. of +, inheritance from R
(ii) NE + associativity (iii) dist. law from R

L5.22 If D is an ID, then so is $D[x]$; units of $D[x]$ are const. polynomials that are units of D
$D[x]^* = D^*$

D5.26 A field is a non-trivial comm. ring, every non-zero element is a unit $\langle F\setminus\{0\}; \cdot, ^{-1}, 1\rangle$ ab. group
$F^* = F\setminus\{0\}$

T5.23 $\mathbb{Z}_p$ is a field if and only if p is prime. $GF(p) = \mathbb{Z}_p$ Proof: $\mathbb{Z}_p^* = \mathbb{Z}_p\setminus\{0\}$ is a mult group iff p prime

T5.24 A field is an integral domain. Proof by contradict.: arb. $u \in F$ is not a zerodiv. Ass. $uv = 0$
$v = 1v = (u^{-1}u)v \overset{\text{Ass.}}{=} u^{-1}0 = 0$ $\Rightarrow u$ is not a zerodiv.

D5.28 $a(x) \in F[x]$, $\deg \geq 1$ is irreducible (≈ prime) if it is divisible by only (const polynomials, const. multiples of $a(x)$)
↳ deg 2, 3, 4 criterias → PVW Script, DM script p. 113

D5.29 monic polynomial $g(x)$ of largest deg. $g(x)|a(x) \wedge g(x)|b(x)$ is the gcd($a(x)$,$b(x)$)

T5.25 $a(x)$ and $b(x) \neq 0 \in F$, these exists a unique monic $q(x)$ (quotient) and unique $r(x)$ (rem.) s.t. $a(x) = b(x)\cdot q(x) + r(x)$, $\deg(r(x)) < \deg(b(x))$. Proof existence + uniqueness (hard)

D5.30 ID: $p \in D\setminus\{0\}$, not a unit. If $p = ab$, then either a or b is a unit.

D5.33 $a(x) \in R[x]$. $\alpha \in R$ s.t. $a(\alpha) = 0$ is called root of $a(x)$. (Nullstelle)

L5.28 $\alpha \in F$ is a root of $a(x) \Leftrightarrow (x-a)$ divides $a(x)$ Proof $\Rightarrow$: Ass. α root $\Rightarrow a(x) = (x-\alpha)q(x)+r$ $\Rightarrow r = a(\alpha)-(\alpha-\alpha) = 0$
$\Leftarrow$: Ass. $(x-\alpha)|a(x) \Rightarrow a(x) = (x-\alpha)q(x)$

C5.29 $a(x)$, deg $= 2$ or 3 over F is reducible iff it has no roots.

D5.31 If α is a root of $a(x)$, then its multiplicity is the highest power of $(x-\alpha)$ dividing $a(x)$

T5.30 non-zero polynomial $a(x) \in F[x]$ of deg d has at most d roots (incl. multiplicities)

L5.31 polynomial interpolation $a(x) \in F[x]$ of deg at most n is uniquely determined by any $n+1$ values of $a(x)$, i.e. by $a(\alpha_1), \dots, a(\alpha_{n+1})$ for distinct $\alpha_1, \dots, \alpha_{n+1} \in F$
$a(x) = \sum_{i=1}^{n+1} a(\alpha_i)\, u_i(x)$; $u_i(x) = \frac{(x-\alpha_1)\cdots(x-\alpha_{i-1})(x-\alpha_{i+1})\cdots(x-\alpha_{n+1})}{(\alpha_i-\alpha_1)\cdots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\cdots(\alpha_i-\alpha_{n+1})}$

L5.32 Congruence mod $m(x)$ is an equiv.rel. on $F[x]$, each equiv. class has an element of deg $< \deg(m(x))$

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

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

L5.34 $F[x]_{m(x)}$ is a ring with add./mult. mod $m(x)$.

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

T5.36 The ring $F[x]_{m(x)}$ is a field iff $m(x)$ is irreducible $F[x]^*_{m(x)} = F[x]_{m(x)}\setminus\{0\}$

D5.36 (n,k)-encoding function, inj. func E, maps list $(a_0, \dots, a_{k-1}) \in A^k$ to a list $(c_0, \dots, c_{n-1}) \in A^n$ of $n > k$ encoded symbols (codeword)

D5.37 (n,k)-error-correcting code over $|A| = q$ is a subset of A^n ($A = \{0,1\}$)

D5.38 Hamming distance number of positions at which two strings of same length differ

D5.39 minimum distance smallest Hamming dist. between any two codewords

D5.40 decoding function $D: A^n \to A^k$ decode into the most plausible information

D5.41 D is t-error correcting if $D((c_0, \dots c_{n-1})) = (a_0, \dots, a_{k-1})$ and with Hamming dist. at most t

T5.40 A code C with min. dist. d is t-error correcting if and only if $d \geq 2t+1$

T5.41 $A = GF(q)$, $\alpha_0, \dots, \alpha_{n-1} \in GF(q)$; $E((a_0, \dots, a_{k-1})) = (a(\alpha_0), \dots, a(\alpha_{n-1}))$

$a(x) = a_{k-1}x^{k-1} + \dots + a_1 x + a_0$ Code C has minimal distance $n-k+1$

D6.1 A proof system (stmts. / proofs / truth func. / verification func.) $\Pi = (S, P, \tau, \phi)$ $\tau: S \to \{0,1\}$ $\phi: S \times P \to \{0,1\}$; usually $S = P = \{0,1\}^*$

D6.2 proof system Π is sound if no false statement has a proof: $\phi(s,p) = 1 \to \tau(s) = 1$

D6.3 proof system Π is complete if every true statement has a proof: $\tau(s) = 1 \to \phi(s,p) = 1$

Logic is defined by the syntax and the semantics. Formulas are a basic concept in any logic.

D6.4 syntax of a logic defines alphabet Λ (allowed symbols) and specifies which strings $\in \Lambda^*$ are formulas (syntact. correct)

D6.5 semantics of a logic defines a func. "free" which assigns to each formula $F = (f_1, \dots, f_k) \in \Lambda^*$ a subset free(F) $\subset \{1, \dots, k\}$ of the indices. If $i \in$ free(F), then f_i occurs free in F. $A \wedge B$ f_2 f_3

D6.6 interpretation $\mathcal{A}$: set $\mathfrak{D} \subseteq \Lambda$, domain (possible values) for each symbol in $\mathfrak{D}$; function that assigns to each symbol in $\mathfrak{D}$ a value in its domain

D6.7 interpretation is suitable for a formula F if it assigns a value to all symbols free in F

D6.8 $\sigma(F, \mathcal{A}) = \mathcal{A}(F) \to \{0,1\}$, truth value of F under the suitable interpretation $\mathcal{A}$.

D6.9 suitable interpretation $\mathcal{A}$ for which F is true is called model for F $\mathcal{A} \models F$ or set of formulas $\mathcal{A} \models M$

D6.10 F (or set M) is satisfiable if a model exists, unsatisfiable ($\perp$) otherwise.

D6.11 F is a tautology / valid ($\top$) if it is true for every suitable interpretation

D6.12 G is a logical consequence of F, $F \models G$, if every model for F is a model for G too.

D6.13 equivalent $F \equiv G \overset{\text{def.}}{\Leftrightarrow} F \models G$ and $G \models F$ D6.14 $\models F$ means F is a tautology

D6.15 Syntax: If F and G are formulas, then $\neg F$, $(F \wedge G)$ and $(F \vee G)$ are formulas too.

D6.16 $\mathcal{A}((F \wedge G)) = 1$ iff: $\mathcal{A}(F) = 1$ and $\mathcal{A}(G) = 1$; $\mathcal{A}((F \vee G)) = 1$ iff: $\mathcal{A}(F) = 1$ or $\mathcal{A}(G) = 1$; $\mathcal{A}(\neg F) = 1$ iff: $\mathcal{A}(F) = 0$

L6.1 For any formulas F, G, H: $F \barwedge F \equiv F$; $F \barwedge G \equiv G \barwedge F$; $(F \barwedge G) \barwedge H \equiv F \barwedge (G \barwedge H)$
$F \barwedge (F \hat{\vee} G) \equiv F$; $F \barwedge (G \hat{\vee} H) \equiv (F \barwedge G) \hat{\vee} (F \barwedge H)$; $\neg\neg F \equiv F$; $\neg(F \barwedge G) \equiv \neg F \hat{\vee} \neg G$
$F \vee \top \equiv \top$, $F \wedge \top \equiv F$, $F \vee \perp \equiv F$, $F \wedge \perp \equiv \perp$, $F \wedge \neg F \equiv \perp$, $F \vee \neg F \equiv \top$ Proof: from D6.16

L6.2 F is a tautology iff $\neg F$ is unsatisfiable L6.3 The following statements are equivalent:
(1) $\{F_1, F_2, \dots, F_k\} \models G$ (2) $(F_1 \wedge F_2 \wedge \dots \wedge F_k) \to G$ is tauct. (3) $\{F_1, F_2, \dots, F_k, \neg G\}$ is unsatisfiable

D6.17 derivation rule $\{F_1, F_2, \dots, F_k\} \vdash_R G$ (G is derived by rule R)

D6.18 logical calculus K is a finite set of derivation rules $K = \{R_1, R_2, \dots, R_m\}$

D6.20 derivation of G from a set M in a calc. is a finite seq. of applications of rules leading to G.
$M_0 := M$, $M_i := M_{i-1} \cup \{G_i\}$ ($N \vdash_{R_j} G_i$; $N \subseteq M_{i-1}$), $M \vdash_K G$

D6.21 derivation rule R is correct if $M \vdash_R F \Rightarrow M \models F$

D6.22 calculus is sound/correct if $M \vdash_K F \Rightarrow M \models F$; complete $M \models F \Rightarrow M \vdash_K F$
calculus sound & complete $M \vdash_K F \Leftrightarrow M \models F$

L6.4 If $F \vdash_K G$ holds for a sound calc., then $\models (F \to G)$. $\{F_1, \dots, F_k\} \vdash G \Rightarrow \models ((F_1 \wedge \dots \wedge F_k) \to G)$

→D6.15

D6.23 syntax: atomic formula is of form A_i ($i \in \mathbb{N}$). An atomic formula is a formula

D6.24 semantics: $\mathcal{Z}$ set of atomic formulas, $\mathcal{A}$ (truth ass.) $\mathcal{A}: \mathcal{Z} \to \{0,1\}$. $\mathcal{A}(F) = \mathcal{A}(A_i)$ (→D6.16)

D6.25 Literal is an atomic formula or the negation of an atomic formula.

D6.26 F is in conjunctive normal form (CNF) if $F = (L_{11} \vee \cdots \vee L_{1m_1}) \wedge \cdots \wedge (L_{n1} \vee \cdots \vee L_{nm_n})$ (Literal)

D6.27 F is in disjunctive normal form (DNF) if $F = (L_{11} \wedge \cdots \wedge L_{1m_1}) \vee \cdots \vee (L_{n1} \wedge \cdots \wedge L_{nm_n})$

T6.5 Every formula has equivalent formulas in CNF and DNF. Proof by existence using truth tables

D6.28 A clause is a set of literals D6.29 $F = (L_{11} \vee \cdots \vee L_{1n}) \wedge \cdots \wedge (L_{m1} \vee \cdots \vee L_{mn}) \Rightarrow K(F) = \{\{L_{11}, \dots L_{1n}\}, \dots\}$

D6.30 clause K is resolvent of clauses K_1, K_2 if there is a literal $L \in K_1, \neg L \in K_2$ and $K = (K_1 \setminus \{L\}) \cup (K_2 \setminus \{\neg L\})$

L6.6 The resolution calculus is sound, if $K \vdash_{Res} K$ then $K \models K$. Proof: Show $\{K_1, K_2\} \vdash_{Res} \Rightarrow \{-\} \models K$

Let $\mathcal{A}$ be an arb. inst. D6.30 If $\mathcal{A}(L) = 1$, then $\mathcal{A}$ makes at least one Literal in $K_2 \setminus \{\neg L\}$ true (¬L false)
If $\mathcal{A}(L) = 0$, then $\mathcal{A}$ makes at least one Literal in $K_1 \setminus \{L\}$ true (L false)
⇒ at least one Literal in K is true ⇒ $\mathcal{A}$ model

T6.7 set M of formulas is unsatisfiable if and only if $K(M) \vdash_{Res} \emptyset$

D6.31 syntax pred. logic: A variable symbol is of the form x_i with $i \in \mathbb{N}$. A func. symbol is of the form $f_i^{(k)}$ with $i,k \in \mathbb{N}$ (k=#args, k=0 → const.). A predicate symbol is of the form $P_i^{(k)}$ $i,k \in \mathbb{N}$ where k denotes #args. A term is defined inductively: variable is a term, if $t_1, \dots, t_k$ are terms, then $f_i^{(k)}(t_1, \dots, t_k)$ is a term. A formula is defined inductively: If $t_1, \dots, t_k$ are terms, then $P_i^{(k)}(t_1, \dots, t_k)$ is formula, called atomic formula. If F, G formulas, then $\neg F$, $(F \vee G)$, $(F \wedge G)$ are forms. If F is a formula, then, for any i, $\forall x_i F$ and $\exists x_i F$ are formulas.

D6.32 Every occurrence of a var. in any F is either free or bound. F closed if it has no free vars.

D6.33 For form F, var x, term t, $F[x/t]$ denotes F obtained by substituting every free x by t

D6.34 Interpretation/structure $\mathcal{A} = (U, \phi, \psi, \xi)$, U universe, assignments ϕ functions, ψ predicates, ξ vars

D6.35 $\mathcal{A}$ is suitable for F if it defines all functions, predicates and free variables

D3.36 semantics: value under interpretation: value $\mathcal{A}(t)$ of term t is defined recursively:

· If t variable, then $\mathcal{A}(t) = \xi(t)$. · If $t = f(t_1, \dots, t_k)$, then $\mathcal{A}(t) = \phi(f)(\mathcal{A}(t_1), \dots, \mathcal{A}(t_k))$

truth value of formula: by D6.16 and if $F = P(t_1, \dots, t_k)$, then $\mathcal{A}(F) = \psi(P)(\mathcal{A}(t_1), \dots, \mathcal{A}(t_k))$

If F of form $\forall x G$ or $\exists x G$, then let $\mathcal{A}_{[x \to u]}$ for $u \in U$ be the same struct as $\mathcal{A}$ except $\xi(x)$ is overwritten by u ($\xi(x) = u$)

$\mathcal{A}(\exists x G) = \begin{cases} 1 & \text{if } \mathcal{A}_{[x \to u]}(G) = 1 \text{ for all } u \in U \text{ (some)} \\ 0 & \text{else} \end{cases}$

L6.8

$\neg(\forall x F) \equiv \exists x \neg F$	$\neg(\exists x F) \equiv \forall x \neg F$	$(\forall x F) \wedge (\forall x G) \equiv \forall x (F \wedge G)$	$(\exists x F) \vee (\exists x G) \equiv \exists x (G \vee F)$
$\forall x \forall y F \equiv \forall y \forall x F$	$\exists x \exists y F \equiv \exists y \exists x F$	$(\forall x F) \overset{x}{\wedge} H \equiv \forall x (F \overset{x}{\wedge} H)$ (x nicht frei in H)	$(\exists x F) \overset{x}{\wedge} H \equiv \exists x (F \overset{x}{\wedge} H)$
$\exists x (F \wedge G) \models \exists x F \wedge \exists x G$		$\exists y \forall x F \models \forall x \exists y F$	$(\exists x F) \vee G \models \exists x (F \wedge G)$
$\forall x F \vee \forall x G \models \forall x (F \vee G)$			

L6.9 If a sub-formula G of F is replaced by an equiv. formula, the result is equiv to F

L6.10 bound substitution $\forall x G \equiv \forall y G[x/y]$ $\exists x G \equiv \exists y G[x/y]$ (y may not occur in G)

D6.37 formula is rectified if no variable occurs both free and bound. Every formula can be rectified

L6.11 universal instantiation any formula F, any term t $\forall x F \models F[x/t]$

D6.38 prenex form: quantifiers $\forall/\exists$, G free of quantifiers $Q_1 x_1 Q_2 x_2 \dots Q_n x_n G$

T6.12 For every formula, there is an equivalent formula in prenex form. Proof: existence rectify + L6.8

T6.13 $\neg \exists x \forall y (P(y,x) \leftrightarrow \neg P(y,y)) \equiv \top$

C6.14 Exists no set that contains all sets S that do not contain themselves ($\{S \mid S \notin S\}$ is not a set)

C6.15 $\{0,1\}^\infty$ is uncountable C6.16 There are uncomputable functions $\mathbb{N} \to \{0,1\}$

C6.17 $f: \mathbb{N} \to \{0,1\}$ assigning to each $y \in \mathbb{N}$ the complement of what prog. y outputs on inp. y is unc.

Ch2

$H = F \overset{\leftrightarrow}{\to} G$ (new formula); $F \overset{=}{\models} G$ (strict. abl. formulas, cf. L2.3); $A \overset{\Leftrightarrow}{\Rightarrow} B$ (strict abl. strats)

Pigeonhole: $k\left(\left\lceil \frac{n}{k} \right\rceil - 1\right) < k\left(\left(\frac{n}{k} + 1\right) - 1\right) = k\left(\frac{n}{k}\right) = n$

Ch3

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

$A \overset{=}{\subseteq} B \Leftrightarrow \mathcal{P}(A) \overset{=}{\subseteq} \mathcal{P}(B)$ Proof: ($\Rightarrow$): $S \in \mathcal{P}(A)$ arb. D3.5 → $S \subseteq A \Rightarrow S \subseteq B$

($\Leftarrow$): A,B arb. $\mathcal{P}(A) \subseteq \mathcal{P}(B)$: $A \in \mathcal{P}(A) \Rightarrow A \in \mathcal{P}(B)$ D3.5 → $A \subseteq B$

$\forall A \; A \in \mathcal{P}(A)$ ✓ $\forall A \; A \subseteq \mathcal{P}(A)$ ×

$\mathcal{A}$ set of sets $\cup\mathcal{A} = \{x \mid x \in A \text{ for some } A \in \mathcal{A}\}$

cart. prod. not associative! $\cap\mathcal{A} = \{x \mid x \in A \text{ for all } A \in \mathcal{A}\}$

$\bigtimes_{i=1}^{k} A_i = \{(a_1, \dots, a_k) \mid a_i \in A_i \text{ for } 1 \le i \le k\}$

relations: symmetric → matrix symmetric, reflexive → diagonal full

irreflexive → diagonal empty, antisymmetrisch → komplementär zur Diagonalen. asymmetrisch = irreflexiv + antisymmetrisch

x is half-sibling of y: $(ic \circ ip) \setminus (ic \circ im \cap ic \circ if)$ (all siblings; siblings with same mother and father)

σ, ρ antisym. $\Rightarrow \sigma \cap \rho$ antisym.

Prove: If A countable, C uncountable ⇒ C\A uncountable. (C\A)∪A = C∪A

Assume C\A uncountable ⇒ $C \subseteq (C \setminus A) \cup A$ ⇒ C\A (count.) ∪ A (count.) ⇒ count.

⇒ contradiction: C by def. uncountable

Ch3

Prove $A \setminus (B \cap C) = (A \setminus B) \cup (A \cap C)$. Let $x \in A \setminus (B \cap C)$ arb.

→ $x \in A \wedge x \notin (B \cap C)$ (Def \) $\equiv x \in A \wedge \neg(x \in B \wedge x \notin C)$ (Def \) $\equiv x \in A \wedge (x \notin B \vee x \in C)$

$\equiv (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C)$ (dist. law) $\equiv x \in (A \setminus B) \cup (A \cap C)$ (Def. ∪,∩)

Prove total order → show that any two elements are comparable (e.g. case dist.)

Prove $A = \bigcup_{i=1}^{n} A_i$ countable: A_i countable for $i \in \mathbb{N}$. for $i \in \mathbb{N}$, there exists a injective function $f_i: A_i \to \mathbb{N}$. Let p_i be the i-th prime number.

⇒ $F: \bigcup_{i=1}^{n} A_i \to \mathbb{N}$, $F(a_i) = p_i^{f_i(a_i)}$ for $a_i \in A_i$. F injective because of uniqueness prime factorization

Ch4

Fermat's little theorem $a^{p-1} \equiv_p 1$ (→C.5.14)

CRT: $x \equiv_{10} 6 \rightleftarrows x \equiv_2 0$, $x \equiv_{15} 11 \rightleftarrows x \equiv_5 1$ Lösung muss bei beiden Gleichungen gleich sein, sonst existiert keine.

Prove: $a|bc$ and $\gcd(a,b) = 1 \Rightarrow a|c$ $(a,b,c \in \mathbb{Z} \setminus \{0\})$: $\gcd = 1 \Rightarrow ua + vb = 1$

$uac + vbc = c$. $a|uac \wedge a|vbc$ (ass.) $\Rightarrow a|uac + vbc \Leftrightarrow a|c$

$R_{11}(2^{340}) = R_{11}(2^{R_{20}(340)}) = R_{11}(2^{R_{10}(320)}) = R_{11}(2^{(-1)^{20}}) = 2$

Find and prove: isomorphism $\psi: \langle \mathbb{Z}_{12}; \oplus \rangle \to \langle \mathbb{Z}_3; \oplus \rangle \times \langle \mathbb{Z}_4; \oplus \rangle$

→ $\psi(x) = (R_3(a), R_4(a))$. Surj: $\psi(x) = (a,b) \Rightarrow (a,b) = (R_3(x), R_4(x))$

$\Rightarrow x \equiv_3 a \wedge x \equiv_4 a \Rightarrow$ unique sol in $\mathbb{Z}_{12}$ by CRT.

Inj: $\psi(a) = \psi(b) \Leftrightarrow (R_3(a), R_4(a)) = (R_3(b), R_4(b)) \Rightarrow a \equiv_3 b \wedge a \equiv_4 b \Rightarrow a \equiv_{12} b \Rightarrow a = b$

Homomorphism: $\psi(x \oplus_{12} y) = (R_3(x \oplus_{12} y), R_4(x \oplus_{12} y)) = (R_3(x) \oplus_3 R_3(y), R_4(x) \oplus_4 R_4(y))$

$= (R_3(x), R_4(x)) \oplus_{12} (R_3(y), R_4(y)) = \psi(x) \oplus_{12} \psi(y)$

Ch.5

Show $f: G \to G : x \mapsto ax$ is bijective.

inj: Assume $f(x)=f(x') \Leftrightarrow a*x = a*x'$. Then: $x = 1*x = (\hat{a}*a)x = \hat{a}*(a*x)$

$\overset{(ass.)}{=} \hat{a}*(a*x') = (\hat{a}*a)*x' = x'$.

surj: $\forall b \in G \exists c$ $(b=f(c))$. Define $c = \hat{a}*b$, then $f(c) = a*c = a*\hat{a}*b = b$

$|G|=77 \Rightarrow$ subgroups have order 7, 11 $\Rightarrow$ prime $\to$ cyclic $\to$ abelian

$a*b = a*c \Rightarrow b=c$ Proof: $b = e*b = (\hat{a}*a)*b = \hat{a}*(a*b) \overset{ass.}{=} \hat{a}*(a*c) = \dots = c$

Prove $(\hat{a}) = a$: $\hat{a}*\hat{a} = e = a*\hat{a}$ $\to$ cancellation law

Left inv = right inv: $\hat{a}*a \overset{LI}{=} (\hat{a}*a)*e = (\hat{a}*a)*(\hat{a}*\hat{\hat{a}}) = \hat{a}*((a*\hat{a})*\hat{\hat{a}})$

$= \hat{a}*(e*\hat{\hat{a}}) = \hat{a}*\hat{\hat{a}} \overset{RI}{=} e$

Homomorph.: $\phi(a^{-1}) = \phi(\tilde{a}^{-1}) \cdot e_H = \phi(\tilde{a}^{-1})(\phi(a)\cdot\widehat{\phi(a)}) = \phi(\tilde{a}^{-1}*a)\cdot\widehat{\phi(a)} = \phi(e)\cdot\widehat{\phi(a)} = e'\cdot\widehat{\phi(a)}$

Solve $3036^m \equiv_{7105} 1$ $\quad 3036 = 2^3\cdot 3\cdot 11\cdot 23$, $7105 = 5\cdot 7^2\cdot 29$ $\Rightarrow gcd = 1$ $\quad m = \varphi(7105)$

Find roots of $xy^2+y+x+1 \in GF(2)[x]_{x^2+x+1}[y]$ $\to$ try all elements for y; $\to$ 1, x are zerodivisors

Find inverse of $x+2$ in $GF(3)_{x^2+2x+2}$

$(x^2+2x+2)+1 : (2x+2) = 2x+2 \to x+1$, $-(x^2+x)$, $\times$, $-(x+1)$, 2

inverse $a(x)\cdot inv(x) = k\cdot m(x)+1$

0	1	2
x	x+1	x+2
2x	2x+1	2x+2

Ring $\langle R; +, -, 0, \cdot, 1\rangle$ s.t. $a\cdot a = a$.

Prove $a+a=0$:
$(a+a) = (a+a)\cdot(a+a)$
$a+a = aa+aa+aa+aa$
$a+a = a+a+a+a$
$0 = a+a$

Prove R commutative:
$(a+b) = (a+b)^2 = a^2+ab+ba+b^2$
$0 = ab+ba$
$(-ab) = ba$
$ab = ba$

Is there a subgroup of order 9 of $GF(81)^*$? No, $|GF(81)^*| = 80$ $\to 9 \nmid 80$

$|\mathbb{Z}_n \times \mathbb{Z}_m| = lcm(n,m)$

zerodivs in $\mathbb{Z}_m = m - \varphi(m) - 1$ (gilt nicht für fields)

Monoids $\langle \mathbb{Z}; +, 0\rangle, \langle \mathbb{Q}; \cdot, 1\rangle, \langle \mathbb{Z}_m; \oplus, 0\rangle, \langle \mathbb{Z}_m; \odot, 1\rangle$

Groups $\langle \mathbb{Z}; +, -, 0\rangle, \langle \mathbb{Q}\setminus\{0\}; \cdot, ^{-1}, 1\rangle, \langle \mathbb{Z}_m; \oplus, \ominus, 0\rangle, R^*$ (for Ring R)

Rings $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, R[x]$

ID $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_{prime}, D[x]$

Field $\mathbb{Q}, \mathbb{R}, \mathbb{C}, GF(p) = \mathbb{Z}_p, GF(p)[x]_{m(x)}$

Ch.6

Prove $(\exists x F) \vee G \models \exists x (F \vee G)$: Let $\mathcal{A}$ be a suitable interpretation such that $\mathcal{A}((\exists x F)\vee G) = 1$. By the semantics of $\vee$, we have $\mathcal{A}(\exists x F) = 1$ or $\mathcal{A}(G) = 1$.

Using def. of $\exists$: $\mathcal{A}_{[x\to u]}(F) = 1$ for some u or $\mathcal{A}(G) = 1$. $\Rightarrow$ case distinction:

① $\mathcal{A}_{[x\to u]}(F) = 1$ for some u: $\Rightarrow \mathcal{A}_{[x\to u]}(F\vee G) = 1$ for some u $(F \models F\vee G)$

$\Rightarrow \mathcal{A}(\exists x (F\vee G)) = 1$ ② $\mathcal{A}(G) = 1$: $\Rightarrow \mathcal{A}_{[x\to u]}(G) = 1$ for $u = x^{\mathcal{A}}$

$\Rightarrow \mathcal{A}_{[x\to u]}(G) = 1$ for some u $\Rightarrow \mathcal{A}_{[x\to u]}(F\vee G) = 1$ for some u $(F \models F\vee G) \Rightarrow \mathcal{A}(\exists x (F\vee G)) = 1$

Derivation rules: $\neg\neg F \vdash F$, $F \wedge G \vdash G \wedge F$, $\neg(F\vee G) \vdash \neg F \wedge \neg G$, $F \wedge G \vdash F$

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

A	B	$B \wedge (\neg B \to A)$
0	0	0
0	1	1
1	0	0
1	1	1

DNF $(\neg A \wedge B) \vee (A \wedge B)$

CNF $(A \vee B) \wedge (\neg A \vee B)$

Equiv. rel: $F_1 = \forall x P(x,x)$ $\quad F_2 = \forall x \forall y (P(x,y) \to P(y,x))$

$F_3 = \forall x \forall y \forall z (P(x,y) \wedge P(y,z) \to P(x,z))$ $\quad \{F_1, F_2, F_3\} \models G$

Monoid $\forall x \forall y \forall z ((f(x,e) = f(e,x) = x) \wedge (f(x, f(y,z)) = f(f(x,y),z)))$

Group $\exists e \forall x (\forall y \forall z (f(x,f(y,z)) = f(f(x,y),z)) \wedge f(x,e) = x \wedge (\exists y (f(x,y) = f(y,x) = e))$

$\{F_1, F_2\}$ satisfiable $\not\Leftrightarrow$ F_1 satisfiable and F_2 satisfiable

! Never rename free variables

Irreducible polynomials: $GF(2)[x]$: 111, 1011, 10011, 10001, 10111

$GF(3)[x]$: 101, 122, 1021, 1121, 10121, 11222 $\quad GF(4)[x]$: 112, 131, 1101, 1213

$GF(5)[x]$: 102, 103, 111, 112, 123, 124, 1024, 1102, 1141, 1444 $\quad GF(7)[x]$: 102, 113, 122, 146

$1021 = x^3+2x+1$

Lemma: $\forall x \exists y (P(x,f(x)) \vee \neg P(x,y))$ is tautology

$(\equiv \forall x (P(x,f(x)) \vee \exists y \neg P(x,y)))$

Proof: Let $\mathcal{A}$ be an arbitrary suitable interpretation.

To show: $\mathcal{A}(\cdot) = 1 \Leftrightarrow \mathcal{A}_{[x\to u]}(P(x,f(x)) \vee \exists y \neg P(x,y))$ for all u in U.

$\Leftrightarrow \mathcal{A}_{[x\to u]}(P(x,f(x)) = 1$ or $\mathcal{A}_{[x\to u]}(\exists y \neg P(x,y)) = 1)$ for all u in U.

case distinction for a fixed u:

① $P^{\mathcal{A}}(u, f^{\mathcal{A}}(u)) = 1 \Rightarrow \mathcal{A}_{[x\to u]}(P(x,f(x))) = 1$.

② $P^{\mathcal{A}}(u, f^{\mathcal{A}}(u)) = 0 \Rightarrow \mathcal{A}_{[x\to u][y\to v]}(\neg P(x,y)) = 1$ for a v

$\overset{v=f(u)}{\Leftrightarrow} \neg P^{\mathcal{A}}(u, f(u)) = 1$

NAND

$\neg F = F$ NAND F

$F \wedge G = (F$ NAND $F)$ NAND $(G$ NAND $G)$

$F \vee G = (F$ NAND $G)$ NAND $(F$ NAND $G)$

Lagrange interpolation (→ L5.31): $f(0) = 1$, $f(1) = 3$, $f(3) = 2 \Rightarrow deg = 2$

$u_0 = \frac{(x-1)(x-3)}{(0-1)(0-3)}$, $u_1 = \frac{(x-0)(x-3)}{(1-0)(1-3)}$, $u_2 = \frac{(x-0)(x-1)}{(3-0)(3-1)}$

$\Rightarrow a(x) = 1\cdot u_0(x) + 3\cdot u_1(x) + 2\cdot u_2(x)$