Logic (2,6): Propositional Logic

Proposition: Mathematical statement (true or false).
$A \to B \equiv \neg A \vee B$ (F for 1/0, T otherwise). $A \leftrightarrow B \equiv (A \to B) \wedge (B \to A) \equiv (A \wedge B) \vee (\neg A \wedge \neg B)$ [T for 0/0, 1/1]

$\wedge, \vee$ binds stronger than $\to, \leftrightarrow, \neg$ binds stronger than $\wedge, \vee$.

Equivalent: $F \equiv G$: Same truth values. **Logical consequence:** $F \models G$ G is 1 if F is 1 (but G can have more 1!). **Equivalences:**
6) $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$ 2) $A \wedge B \equiv B \wedge A$, $A \vee B \equiv B \vee A$
3) $(A \wedge B) \wedge C \equiv A \wedge (B \wedge C)$, $(A \vee B) \vee C \equiv A \vee (B \vee C)$ 7) $\neg\neg A \equiv A$
4) $A \wedge (A \vee B) \equiv A$, $A \vee (A \wedge B) \equiv A$ 5) $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$
1) $A \wedge A \equiv A$, $A \vee A \equiv A$ 8) $\neg(A \wedge B) \equiv \neg A \vee \neg B$, $\neg(A \vee B) \equiv \neg A \wedge \neg B$
9) $A \vee T \equiv T$, $A \wedge T \equiv T$ 10) $A \vee \bot \equiv A$, $A \wedge \bot \equiv \bot$ (rules are for
11) $F \vee \neg F \equiv T$, $F \wedge \neg F \equiv \bot$ any logic with these symbols)

Tautology / valid: True for all assignments of symbols ($\top$). **Satisfiable:** True for at least 1 assignment. ($F \equiv T \Leftrightarrow \neg F \equiv \bot$)
$F \to G$ is a tautology iff $F \models G$. **Syntax:** 1) Atomic formula is a formula. 2) For F, G, $\neg F$, $(F \wedge G)$, $(F \vee G)$ are form.
Literal: Atom. form. or negation of atom. form. **Conjunctive NF:** $F = (L_{11} \vee \dots \vee L_{1m_1}) \wedge \dots \wedge (L_{n1} \vee \dots \vee L_{nm_n})$. **Disjunctive NF:** $F = (L_{11} \wedge \dots \wedge L_{1m_1}) \vee \dots \vee (L_{n1} \wedge \dots \wedge L_{nm_n})$. DNF: Combine literals of rows = 1 ($\neg A_i$ if i-t is 0) with $\wedge$, comb. these with $\vee$.
CNF: Combine literals of rows = 0 (A_i if i-t is 0, $\neg A_i$ otherwise) with $\vee$, combine these with $\wedge$. **Predicate Logic:**
k-ary predicate is a function $U^k \to \{0,1\}$. E.g. unary prime(x): $x > 1 \wedge \forall_y \forall_z ((y_2 = x) \to ((y = 1) \vee (z = 1)))$. **Proposition formula:**
Formula with a single interpretation (e.g. $\exists_n (n > 5)$)

Syntax: 1) Variable symb.: x_i 2) Function symbol: $f_i^{(k)}$ k=args
3) Predicate symbol $P_i^{(k)}$ 4) Term t_i (vars or $f_i^{(k)}(t_1, \dots, t_k)$)
4) Formula: $P_i^{(k)}(t_1, \dots, t_k)$ is an atomic formula. $\neg F$, $(F \wedge G)$, $(F \vee G)$ are formulas and $\forall_x F$ and $\exists_x F$ are formulas.
Variable x in $\forall_x G$ or $\exists_x G$ is **bound**, **free** otherwise.
Closed formula: No free variables. **Substitution:**
$F[x/t]$ = Substituting every free occurence of x.

Interpretation: $A = (U, \phi, \psi, \xi)$ 1) U = Universe (non empty set) 2) ϕ assigns each function symbol a function 3) ψ assigns each pred. symbol a predicate. 4) ξ assigns each variable symbol a value of U.
Semantics: $A(t) = \xi(t)$ (var) or $A(t) = \phi(\epsilon)(A(t_1), \dots, A(t_k))$
$A((F \wedge G)) : A(F) = 1$ and $A(G) = 1$. $A(\neg F \vee G)$: $A(F) = 1$ or $A(G) = 1$.
$A(\neg F) : A(F) = 0$ | $F = P(t_1, \dots, t_k)$. $A(F) = \psi(P)(A(t_1), \dots, A(t_k))$.
$A(\forall_x G) = 1$ if $A_{x \to u}(G)$ for all $u \in U$. $A(\exists_x G)$ if $A_{x \to u}$ for some $u \in U$ (where $\xi(x) = u$). (x not free in Rules: H)

1) $\neg(\forall_x F) \equiv \exists_x \neg F$ 2) $\neg(\exists_x F) \equiv \forall_x \neg F$ 5) $\forall_x \forall_y F \equiv \forall_y \forall_x F$
3) $(\forall_x F) \wedge (\forall_x G) \equiv \forall_x (F \wedge G)$ 4) $(\exists_x F) \vee (\exists_x G) \equiv \exists_x (F \vee G)$
6) $\exists_x \exists_y F \equiv \exists_y \exists_x F$ 7) $(\forall_x F) \wedge H \equiv \forall_x (F \wedge H)$ 8) $(\forall_x F) \vee H \equiv \forall_x (F \vee H)$
9) $(\exists_x F) \wedge H \equiv \exists_x (F \wedge H)$ 10) $(\exists_x F) \vee H \equiv \exists_x (F \vee H)$ **rectified:**
No variable bound / free and all vars distinct after quantifier.
Prenex: $Q_1 x_1 Q_2 x_2 \dots Q_n x_n G$ (Q_i: = Quantifiers, G: formula without quantifiers. Prenex form exists for every formula!
Theorem 6.11: $\neg\exists_x \forall_y (P(y,x) \leftrightarrow \neg P(y,y))$ E.g. Russell:
$\neg\exists_R \forall_S (S \in R \leftrightarrow S \notin S)$.

Proof system / Logic:

Proof system: Quadruple $\Pi = (\Sigma, P, \mathcal{T}, \Phi)$ with alphabet Σ
$S \subseteq \Sigma^*$ set of statements, $P \subseteq \Sigma^*$ set of proof strings.
Statement $s \in S$ is true or false, which is assigned by the truth function $\mathcal{T}: S \to \{0,1\}$ (truth value $\mathcal{T}(s)$)
$p \in P$ is a valid proof for a statement iff $\Phi(s,p) = 1$.
$\Phi: S \times P \to \{0,1\}$ is the verification function (efficient comp.)
Sound: No false statement has a proof. ($\Phi(s,p) = 1 \Rightarrow \mathcal{T}(s) = 1$)
Complete: Every true statement has a proof ($\mathcal{T}(s) = 1 \Rightarrow \Phi(s,p) = 1$)
Syntax: Alphabet Σ of allowed symbols and specifies which strings are formulas (syntactically correct).
Semantics: Defines a function which assigns to each formula $F = f_{i_1}, \dots, f_{i_k}$ a subset $I \subseteq \{1, \dots, k\}$ of the indices. If $i \in I$, a symbol occurs free in F. Also defines a function that assigns to each formula and values for each free symbols a truth value in $\{0,1\}$. **Interpretation:** Assigns to a certain set of symbols of Σ certain values. $\sigma(A, F)$ or $A(F)$ is the truth value of F under interpretation A. An interpretation is **suitable** if it assigns a value to all free symbols.
Model: Suitable interpretation for which F is true ($A(F) = 1$).
One also writes $A \models F$ or $A \models M$ if A is a model for a set M of formulas ($A \models F$ or $A \models M$ if not).
Satisfiable: There is a model (unsatisfiable / $\bot$ otherwise). ($\models (F \to \bot)$)
Tautology: True for every suitable interpretation. ($\models F$)
Logical consequence: $F \models G$. Every suitable interpretation for both F and G: Model for F is also a model for G.
Equivalent: Every suitable interpretation for both F and G yields same truth value for both ($F \models G$ and $G \models F$).

Calculus: **Derivation rule:** Rule for deriving a formula from a set of formulas (precondition). $\{F_1, \dots, F_k\} \vdash_R G$ or $\frac{F_1 \; F_2 \; \dots \; F_k}{G}$ if G can be derived from the set by rule R.
Calculus is a finite set of derivation rules.
Derivation of G from a set M is a finite sequence of applications of rules in K, leading to G.
$M \vdash_K G$ if there is a derivation of G from M in K.
Der. rule R is **correct** if $M \vdash_R F$ implies $M \models F$.
A calculus is **correct / sound**: If F can be derived from M, F is a logical consequence of M ($M \vdash_K F \Rightarrow M \models F$).
K is **complete**: If F is a logical consequence of M, it can also be derived ($M \models F \Rightarrow M \vdash_K F$).

Resolution calculus: **Clause:** Set of literals. Set of clauses associated to a formula in CNF is the set $\mathcal{K}(F)$. $F = (L_{11} \vee \dots \vee L_{1m_1}) \wedge \dots \wedge (L_{n1} \vee \dots \vee L_{nm_n})$
$\mathcal{K}(F) = \{\{L_{11}, \dots, L_{1m_1}\}, \dots, \{L_{n1}, \dots, L_{nm_n}\}\}$
Resolvent: If there is a literal L such that $L \in k_1, \neg L \in k_2$. Then $K = (k_1 \setminus \{L\}) \cup (k_2 \setminus \{\neg L\})$ (one res. per step!)
Resolution calculus is sound, if $K \vdash_{Res} k$ then $K \models k$.
Unsatisfiable: A set M of formulas is unsatisfiable iff $\mathcal{K}(M) \vdash_{Res} \emptyset$.

Proof patterns: **Direct proof of an implication:** $S \Rightarrow T$: Assume S, then prove T under this assumption. **Indirect proof of an implication:** $S \Rightarrow T$: Assume that T is false, prove that S is false under this assumption. **Composing implications:** If $S \Rightarrow T$ and $T \Rightarrow U$ is true, $S \Rightarrow U$ is too. **Modus ponens:** State R, prove R and $R \Rightarrow S$. **Case distinction:** State statements $R_1, \dots, R_k$ (cases). Prove that one must occur and $R_i \Rightarrow S$. **By contradiction:** Of S. State T, assume that S is false and proof that T is true from this assumption. Then prove that T is false.
Existence proof: $\exists_x P(x)$. Constructive if a is given, non-constructive otherwise. **By counterexample:** $\neg\forall_x P(x)$ by giving a for that $\neg P(a)$ is true. **By induction:** 1.) Prove P(0) 2.) Prove $\forall_n (P(n) \to P(n+1))$ **Pigeonhole:** If a set of n objects is partitioned into k cn sets, at least one contains at least $\lceil \frac{n}{k} \rceil$ objects.

Sets, relations, functions (3):

Sets: $A = B :\Leftrightarrow \forall x\,(x \in A \leftrightarrow x \in B)$. $A \subseteq B :\Leftrightarrow (A \subseteq B) \wedge (B \subseteq A)$

Subset: Every elem. of A is $\in B$: $A \subseteq B :\Leftrightarrow \forall x\,(x \in A \to x \in B)$

$A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$. **Power set:** Set of all subsets of A. $\mathcal{P}(A) := \{S \mid S \subseteq A\}$ (2^A). **Cardinality** for set with k elem.: 2^k

E.g. $\mathcal{P}(\{a,b,c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$

Union: $A \cup B := \{x \mid x \in A \vee x \in B\}$ **Intersection:** $A \cap B := \{x \mid x \in A \wedge x \in B\}$ **Laws:** Id) $A \cap A = A$, $A \cup A = A$

Co) $A \cap B = B \cap A$, $A \cup B = B \cup A$ Ab) $A \cap (A \cup B) = A$, $A \cup (A \cap B) = A$

As) $A \cap (B \cap C) = (A \cap B) \cap C$, $A \cup (B \cup C) = (A \cup B) \cup C$ **Distributivity:**

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Co) $A \subseteq B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B$ **Cartesian product:** $A \times B$

First component from A, second from B: $A \times B = \{(a,b) \mid a \in A \wedge b \in B\}$

$|A \times B| = |A| \cdot |B|$ (for finite sets) **Relations:**

Relation ρ is a subset of $A \times B$. If $A = B$, relation is on A.

$(a,b) \in \rho$ or $a \rho b$. **Inverse relation** $\hat{\rho}$ from B to A: $\forall a \in A \forall b \in B\,(a \rho b \Leftrightarrow b \hat{\rho} a)$ [Matrix: Transpose. Graph: inv. edges]

Composition: ρ: A to B, σ: B to C. $\rho\sigma$ or $\rho \circ \sigma$ A to C:

$a \rho\sigma c :\Leftrightarrow \exists b \in B\,(a \rho b \wedge b \sigma c)$. $\rho^n = \underbrace{\rho \circ \rho \circ \rho \circ \ldots \circ \rho}_{n\text{-times}}$

Composition is assoc. $\rho(\sigma\emptyset) = (\rho\sigma)\emptyset$. $\hat{\rho}\hat{\sigma} = \widehat{\sigma\rho}$ **Reflexive:**

$\forall a\,(a \rho a)$ [$\mathrm{id} \subseteq \rho$] **Irreflexive:** $\forall a\,(a \not\rho a)$ [$\rho \cap \mathrm{id} = \emptyset$]

Symmetric: $\forall a \forall b\,(a \rho b \Leftrightarrow b \rho a)$ [$\rho = \hat{\rho}$] **Antisymmetric:**

$\forall a \forall b\,((a \rho b \wedge b \rho a) \to a = b)$ [$\rho \cap \hat{\rho} = \mathrm{id}$] **Transitive:**

$\forall a \forall b \forall c\,(a \rho b \wedge b \rho c) \to a \rho c$. **Transitive closure:**

$\rho^* = \bigcup_{n \geq 0} \rho^n$ [Graph: Reachable] **Equivalence relation:**

Relation on set A that is reflexive, symmetric, transitive.

Intersection of 2 equiv. relations is an equiv. relation.

Equiv. class: Set of elements that are equiv. to a:

$[a]_\theta := \{b \in A \mid b \theta a\}$. Set of equiv. classes of an equiv. relation is the **quotient set** of A or A mod θ (A/θ)

$A/\theta := \{[a]_\theta \mid a \in A\}$. It is a partition of A!

Partial order: Reflexive, antisymmetric and transitive relation.

Set with $\preceq$ is called partially ordered set (poset).

$a \prec b :\Leftrightarrow a \preceq b \wedge a \neq b$. **Totally ordered** by $\preceq$: All elements of $(A, \preceq)$ are comparable. **Well-ordered:** Totally ordered and every non-empty subset has ≥ 1 elem. (every finite totally ordered poset) **Covering:** An elem. b covers a if $a \prec b$ and no c with $a \prec c$ and $c \prec b$.

Hasse diagram: Directed graph with elems as vertices. Edge from a to b if a covers b. E.g. (rotated 90°):

$\{\{1,2,3,4,6,8,12,24\}\mid|\}$ 

Lexicographic order:

$(a_1, b_2) \leq_{Lex} (a_2, b_2) :\Leftrightarrow a_1 \prec a_2 \vee (a_1 = a_2 \wedge b_1 \preceq b_2)$ [for $(A, \preceq), (B, \sqsubseteq)$]

For $(A, \preceq)$ and some subset $S \subseteq A$: **Minimum / maximum** ($a \in S$) of S if there is no $b \in S$ with $b \prec a$ ($b \succ a$).

Least / greatest ($a \in S$) of S if $a \preceq b$ ($a \succeq b$) for all $b \in S$.

Lower / upper bound ($a \in A$) of S if $a \preceq b$ ($a \succeq b$) for all $b \in S$.

Greatest lower bound / least upper bound ($a \in A$) of S if a is the greatest / least elem. of all lower / upper bounds.

Meet: If a and b ($\{a,b\} \subseteq A$) have a greatest lower bound, it is the meet of them (denoted $a \wedge b$). **Join:** If they have a least upper bound, it's the join ($a \vee b$). **Lattice:** A poset where every pair of elem. has a meet / join.

Functions: $f: A \to B$ from a domain to a codomain is a relation with properties: 1) $\forall a \in A\ \exists b \in B\ a\,f\,b$ (totally defined) 2) $\forall a \in A \forall b, b' \in B\ a\,f\,b \wedge a\,f\,b' \to b = b'$ (well-def.)

Set of all functions $A \to B$ is denoted B^A. **Partial function:** Only condition 2. **Equal:** Two functions are equal if they are equal as relations. **Image** of a subset S of A: $f(S) := \{f(a) \mid a \in S\}$. Subset $f(A)$ of B is called **image / range** of f (denoted $\mathrm{Im}(f)$). **Inverse image:** $T \subseteq B$ $f^{-1}(T) := \{a \in A \mid f(a) \in T\}$ **Properties:**

1) injective if $a \neq b \Rightarrow f(a) \neq f(b)$ (no „collisions")

2) surjective (onto) if for every $b \in B$, $b = f(a)$ for some $a \in A$

3) bijective (one-to-one) if injective and surjective.

Composition of a function $f: A \to B$ and $g: B \to C$ ($g \circ f : A \to C$): $(g \circ f)(a) = g(f(a))$. Function comp. is assoc., $(h \circ g) \circ f = h \circ (f \circ g)$.

Countability: Cardinality: 1) Two sets have the same cardinality ($A \approx B$) if there is a bijection $A \to B$.

2) Cardinality of B is at least card. of A ($A \preceq B$) if $A \approx C$ for some subset $C \subseteq B$. Equivalent to the existance of an injection $A \to B$. 3) **Countable:** $A \preceq \mathbb{N}$, uncountable otherwise. **Transitive:** $A \preceq B \wedge B \preceq C \Rightarrow A \preceq C$.

$A \subseteq B \Rightarrow A \preceq B$ **Countable:** A set is countable iff it is finite or $A \approx \mathbb{N}$ **Rules:** For countable sets:

1) Set A^n of n-tuples over A is countable.

2) Union of a countable list of countable sets is countable. 3) The set A^* of finite sequences of elements from A is countable. **Examples:** 1) The set $\{0,1\}^*$ is countable (put 1 in front, convert)

2) Cartesian product of two countable sets is countable (enumerate pairs: (0,0), (1,0), (0,1), (2,0), (1,1), (0,2), ...)

3) Rational numbers are countable (pair of two numbers, same proof). 4) $\{0,1\}^\infty$ is uncountable (Cantor's diagonalization argument).

Number theory (4)

Euclid: For all integers $a, d \neq 0$ there exist unique ints: $a = dq + r$ and $0 \leq r < |d|$ **Greatest common divisor:** For ints a and b ($\neq 0$), int d is called gcd if it divides a and b and every common divisor of a, b divides d: $d \mid a \wedge d \mid b \wedge \forall c\,((c \mid a \wedge c \mid b) \to c \mid d)$. The unique positive gcd is called the gcd. **Relatively prime:** $\gcd(a,b) = 1$. **Division:** $a \mid b \Leftrightarrow \exists c\,(b = ac)$ **Gcd-rule:** $\gcd(m, n - qm) = \gcd(m, n)$ **Ideal:** $(a,b) := \{ua + vb \mid u, v \in \mathbb{Z}\}$

$(a) := \{ua \mid u \in \mathbb{Z}\}$. For $a, b \in \mathbb{Z}$ there exists $(a,b) = (d)$ and d is the gcd. Also there is $u, v \in \mathbb{Z}$ so that: $\gcd(a,b) = ua + vb$. **Euclid's extended gcd algorithm:**

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

while $s_2 > 0$ **do**; $q = s_1$ div s_2; $r = s_1 - q s_2$; $s_1 = s_2$; $s_2 = r$; $t = u_2$; $u_2 = u_1 - q u_2$; $u_1 = t$; $t = v_2$; $v_2 = v_1 - q v_2$; $v_1 = t$;

end; $d = s_1$; $u = u_1$; $v = v_1$; **Irrationality of roots:**

$\sqrt{n}$ is irrational unless $n = c^2$ for $c \in \mathbb{Z}$ (unique p.factors)

Least common multiple: $\mathrm{lcm}(a,b) = a \mid l \wedge b \mid l \wedge \forall m\,((a \mid m \wedge b \mid m) \to l \mid m)$. $a = \prod_i p_i^{e_i}$, $b = \prod_i p_i^{f_i}$ Then:

$\gcd(a,b) = \prod_i p_i^{\min(e_i, f_i)}$ $\mathrm{lcm}(a,b) = \prod_i p_i^{\max(e_i, f_i)}$. $\gcd \cdot \mathrm{lcm} = ab$

Congruent modulo: $a \equiv_m b :\Leftrightarrow m \mid (a - b)$. For $m \geq 1$, $\equiv_m$ is an equiv. relation on $\mathbb{Z}$. If $a \equiv_m b$ and $c \equiv_m d$: $a + c \equiv_m b + d$, $ac \equiv_m bd$. **For polynoms:** If $q_i \equiv_m b_i$ for $1 \leq i \leq k$, then $f(a_1, \ldots, a_k) \equiv_m f(b_1, \ldots, b_k)$. **Rules:** 1) $a \equiv_m R_m(a)$ 2) $a \equiv_m b \Leftrightarrow R_m(a) = R_m(b)$ 3) $R_m(a+b) = R_m(R_m(a) + R_m(b))$

4) $R_m(ab) = R_m(R_m(a) \cdot R_m(b))$ **Tricks:** $R_9(n)$: Adding decimal digits of n, computing R_9 of this sum. $R_{11}(n)$: Same, but with alternating sign (+/-/+/-). **Multiplicative inverse:** $ax \equiv_m 1$ has a solution $x \in \mathbb{Z}_m$ iff $\gcd(a,m) = 1$. The solution is called multiplicative inverse and one also writes $x \equiv_m a^{-1}$ or $x \equiv_m 1/a$.

Chinese remainder theorem: $m_1, m_2, \dots, m_r$ pairwise rel. prime integers and $M = \prod_{i=1}^{r} m_i$. The system $x \equiv_m a_1, x \equiv_m a_2, \dots, x \equiv_m a_r$ has a unique solution $0 \le x < M$. Let $M_i = M/m_i$ and $N_i M_i \equiv_{m_i} 1$. Then $x = R_M(\sum_{i=1}^{r} a_i M_i N_i)$

Diffie Hellmann: $K_{AB} \equiv_p \gamma_B^{X_A} \equiv_p (g^{X_B})^{X_A} \equiv_p g^{X_A X_B} \equiv_p K_{BA}$

Alice: Random X_A from $\{0, \dots, p-2\}$ Bob: Random X_B from $\{0, \dots, p-2\}$

$\gamma_A := R_p(g^{X_A})$ → X_A → $\gamma_B := R_p(g^{X_B})$

$K_{AB} := R_p(\gamma_B^{X_A})$ ← γ_B ← $K_{BA} := R_p(\gamma_A^{X_B})$

p, g are public params, γ_A / γ_B public keys, X_A / X_B private keys and $K_{AB} = K_{BA}$ the message/key for further crypt.

Algebra (5)

Operation: On a set S: function $S^n \to S$.

Algebra: Pair $(S; \Omega)$ where S is the set (carrier) and $\Omega = (\omega_1, \dots, \omega_n)$ a list of operations on S. E.g. $\langle \mathbb{Z}; +, -, 0, ; 1 \rangle$ or $\langle \mathbb{Z}_n; \oplus \rangle$ and $\langle \mathbb{Z}_n; \odot \rangle$.

Neutral element: A left/right neutral element of an algebra is an element $e \in S$ so that $e * a = a$ / $a * e = a$. If $\langle S; * \rangle$ has a left and right neutral element, they are equal. **Associativity:** Binary operation $*$ on a set S is assoc if for all $a, b, c \in S$: $a * (b * c) = (a * b) * c$.

Monoid: Algebra $\langle M; *, e \rangle$ where $*$ is assoc. and e the neutral element. E.g. $\langle \mathbb{Z}; +, 0 \rangle$, $\langle \mathbb{Z}; \cdot, 1 \rangle$, $\langle \mathbb{Q}; +, 0 \rangle$ $\langle \mathbb{Q}; \cdot, 1 \rangle$, $\langle \mathbb{R}; +, 0 \rangle$, $\langle \mathbb{R}; \cdot, 1 \rangle$, $\langle \mathbb{Z}_n; \oplus, 0 \rangle$, $\langle \mathbb{Z}_n; \odot, 1 \rangle$.

Inverse element: Left/right inverse of an element in an algebra: $b \in S$ so that $b * a = e$ / $a * b = e$. If a in a monoid has a left/right inverse, they are equal.

Group: $\langle G; * \rangle$ with these axioms: 1) $*$ is assoc 2) There is a neutral element $e \in S$ so that $a * e = e * a = a$ for all $a \in G$. 3) Every $a \in G$ has an inverse elem. $\hat{a}$ i.e. $a * \hat{a} = \hat{a} * a = e$. **Commutative / Abelian:** A group/monoid is called comm. if $a * b = b * a$ $\forall a, b \in G$.

Group rules: 1) $\hat{(\hat{a})} = a$. 2) $\widehat{a * b} = \hat{b} * \hat{a}$ 3) Left cancel. law: $a * b = a * c \Rightarrow b = c$ 4) Right cancel. law: $b * a = c * a \Rightarrow b = c$. 5) The equations $a * x = b$ / $x * a = b$ have a unique solution x for any a and b. **Direct product:** The direct product of n groups $\langle G_1; *_1 \rangle, \dots, \langle G_n; *_n \rangle$ is the algebra $\langle G_1 \times \dots \times G_n; \bullet \rangle$ where $\bullet$ is component-wise: $(a_1, \dots, a_n) \bullet (b_1, \dots, b_n) = (a_1 *_1 b_1, \dots, a_n *_n b_n)$. $\langle G_1 \times \dots \times G_n; \bullet \rangle$ is a group where the neutral element / inversion is component-wise in the respective group. **Group homomorphism:** A function ψ from a group $\langle G; *, \hat{}, e \rangle$ to a group $\langle H; \bullet, \hat{}, e' \rangle$ where $\forall a, b: \psi(a * b) = \psi(a) \bullet \psi(b)$. If ψ is a bijection from G to H, it is an **isomorphism.** A group homomorphism satisfies: 1) $\psi(e) = e'$ 2) $\psi(\hat{a}) = \widehat{\psi(a)}$. Example: Group $\langle \mathbb{Z}_6; \oplus \rangle \times \langle \mathbb{Z}_{10}; \oplus \rangle$ is isomorphic to $\langle \mathbb{Z}_2; \oplus \rangle \times \langle \mathbb{Z}_{30}; \oplus \rangle$. $\psi((a, b)) = (a', b')$ where $a' \equiv_2 a$, $b' \equiv_3 a$, $b' \equiv_5 b$.

Subgroup: A subset $H \subseteq G$ of a group $\langle G; *, \hat{}, e \rangle$ is called a subgroup if $\langle H; *, \hat{}, e \rangle$ is a group, which requires: 1) $a * b \in H$ $\forall a, b \in H$ 2) $e \in H$ 3) $\hat{a} \in H$ $\forall a \in H$.

Order: The order of a group element $a \in G$ ($\text{ord}(a)$) is the least $m \ge 1$ so that $a^m = e$. If no m exists, $\text{ord}(a) = \infty$. E.g.: $\text{ord}(6) = 10$ in $\langle \mathbb{Z}_{20}; \oplus, \ominus, 0 \rangle$. $a^0 = e$, $a^n = a \cdot a^{n-1}$ for $n \ge 1$ and $a^n = (a^{-1})^{|n|}$ for $n \le -1$. For all m, n: $a^m \cdot a^n = a^{m+n}$, $(a^m)^n = a^{mn}$.

Finite groups: $|G|$ is called the order of a finite group G.

Cyclic groups: A cyclic group $G = \langle g \rangle$ is generated by a generator g with: $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\} = \{e, g, g^2, \dots, g^{\text{ord}(g)-1}\}$. We have: $g^m = g^{R_{\text{ord}(g)}(m)}$. E.g. $\langle \mathbb{Z}_n, \oplus \rangle$ (where all g with $\gcd(n, g) = 1$ are generators) or $\langle \mathbb{Z}, +, -, 0 \rangle$ as an infinite one.

Isomorphism: A cyclic group of order n is isomorphic to $\langle \mathbb{Z}_n, \oplus \rangle$ (and therefore abelian) Proof: Bijection $\mathbb{Z}_n \to G$: $i \to g^i$ ($i \oplus j \mapsto g^{i+j} = g^i * g^j$).

Lagrange: Let G be a finite group and H a subgroup of G. Then $|H|$ divides $|G|$. Three consequences: 1) For a finite Group G, the order of every element divides the group order ($\text{ord}(a)$ divides $|G|$) 2) $a^{|G|} = e$ for every $a \in G$ ($a^{|G|} = a^{k \cdot \text{ord}(a)} = (a^{\text{ord}(a)})^k = e^k = e$ 3) Every group of prime order is cyclic ($\text{ord}(a) = 1$ v $\text{ord}(a) = p$).

$\mathbb{Z}_n^*$: $\mathbb{Z}_n$ with $\odot$ is only a group if we exclude elems with no multiplicative inverse. $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$

Euler function: Cardinality of $\mathbb{Z}_n^*$. $\varphi(n) = |\mathbb{Z}_n^*|$. $\varphi(p) = p - 1$. If $n = \prod_{i=1}^{r} p_i^{e_i}$, then: $\varphi(n) = \prod_{i=1}^{r} (p_i - 1) p_i^{e_i - 1}$

Fermat, Euler: For all $m \ge 2$ and a with $\gcd(a, n) = 1$: $a^{\varphi(n)} \equiv_n 1$. Therefore for every prime and a not divisible by p: $a^{p-1} \equiv_p 1$

$\mathbb{Z}_n^*$ cyclic: $\mathbb{Z}_n^*$ is cyclic iff $n = 2, n = 4, n = p^e, n = 2p^e$ (where p is an odd prime and $e \ge 1$.

RSA: Following theorem is needed for RSA: G some finite group, e with $\gcd(e, |G|) = 1$. The e-th root of $y \in G$, namely $x \in G$ satisfying $x^e = y$ can be computed by $x = y^d$ where d is the multiplicative inverse of e mod $|G|$, i.e. $ed \equiv_{|G|} 1$. Proof: $(y^d)^e = y^{de} = y^{k \cdot |G| + 1} = (y^{|G|})^k \cdot y = y$.

RSA-Encryption:

Alice: Generate primes p, q. $n = p \cdot q$. $f = (p-1)(q-1)$ select e. $d \equiv_f e^{-1}$

Bob: message $m \in \{1, \dots, n-1\}$ → n, e → $m = R_n(m^e)$

Alice: ← y ← $y = R_n(m^d)$

Alice's public key: (n, e), secret key: d

Ring: A ring $\langle R; +, -, 0, \cdot, 1 \rangle$ is an algebra for which: 1) $\langle R; +, -, 0 \rangle$ is a commutative group. 2) $\langle R; \cdot, 1 \rangle$ is a monoid 3) $a(b+c) = (ab) + (ac)$ and $(b+c)a = (ba) + (ca)$ for all $a, b, c \in R$ (left and right distributive law). A ring is commutative if multiplication is comm. ($ab = ba$).

Examples: $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ are comm. rings. $\langle \mathbb{Z}_n, \oplus, \ominus, \odot, 0, 1 \rangle$ is a comm. ring. **Rules:** 1) $0_R \cdot a = a \cdot 0 = 0$ 2) $(-a)b = -ab$ 3) $(-a)(-b) = ab$ 4) If R is non-trivial (more than one elem.), then $1 \neq 0$. **Characteristics:** Order of 1 in the additive group if it is finite, otherwise 0. E.g. $\mathbb{Z}$ has char. 0 and $\langle \mathbb{Z}_n, \oplus, \ominus, 0, \odot, 1 \rangle$ n. **Divisors:** For $a, b \in R$ with $a \neq 0$ $a | b$ (a divides b) if there is $c \in R$ such that $b = ac$. $1 \neq 1$ are divisors of every element and every non-zero element is divisor of 0. **Rules:** 1) If $a | b$ and $b | c$, then $a | c$. 2) If $a | b$ then $a | bc$ for all c. 3) If $a | b$ and $a | c$ then $a | (b+c)$. **Unit:** Element of a comm. ring that is invertible, i.e. $uv = vu = 1$ for some $v \in R$ ($v = u^{-1}$). Set of units is denoted R^*. E.g. $\mathbb{Z}^* = \{-1, 1\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$. **Integral domain:** A nontrivial ($1 \neq 0$) comm. ring without zerodivides. Vakbl $ab = 0 \to a = 0 \vee b = 0$). E.g. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$. $\mathbb{Z}_n$ only if n is prime. In an integral domain, if $a | b$ then c with $b = ac$ is unique.

Polynomial ring: A polynomial over a ring R is an expression of the form: $a(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_1 x + a_0 = \sum_{i=0}^{d} a_i x^i$ with $a_i \in R$. $\deg(a(x))$ is the greatest i so that $a_i \neq 0$. The poly 0 has degree „minus infinity". $R[x]$ is the set of polys over R. $R[x]$ is a ring for any ring R! If D is an integral domain, so is $D[x]$ (with same units as D, as constant polynoms). **Field:** Nontrivial commutative ring in which every nonzero element is a unit i.e. $F^* = F \setminus \{0\}$. This means that a ring F is a field iff $\langle F \setminus \{0\}; \cdot, ^{-1}, 1 \rangle$ is a comm. group. Examples: $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are fields, $\mathbb{Z}$ and $R[x]$ (for any ring R) are not. (F has no zero divisors!)

$\mathbb{Z}_p$ is a field iff p is prime. The field with p elements is denoted $GF(p)$ (Galois field). A field is an integral domain and a finite integral domain is a field.

Polynomials over a field: A polynomial $a(x) \in F[x]$ is called monic if the leading coefficient is 1. A poly $a(x) \in F[x]$ with degree at least 1 is irreducible if it is divisible by constant polys and multiples of $a(x)$. For $a(x)$ and $b(x)$ a poly is called gcd if $d(x) | a(x) \wedge d(x) | b(x)$ and every common divisor of $a(x)$ and $b(x)$ divides $d(x)$. The monic polynomial is called the gcd. E.g.: $GF(7)[x], a(x) = x^3 + 4x^2 + 5x + 2, b(x) = x^3 + 6x^2 + 4x + 6$. $\gcd(a(x), b(x)) \stackrel{!}{=} x^3 + 3x + 2$. **Division:** $a(x), b(x) \in F[x]$ there exists unique $q(x)$ and $r(x)$ such that: $a(x) = b(x) \cdot q(x) + r(x)$ and $\deg(r(x)) < \deg(b(x))$. **Polynomials as functions:** An element $\alpha \in R$ so that $a(\alpha) = 0$ is called a root of $a(x)$. For a field F, $\alpha \in F$ is a root of $a(x)$ iff $(x - \alpha)$ divides $a(x)$. A polynomial $a(x)$ of degree 2 or 3 over a field is irreducible iff it has no roots. The multiplicity of a root is the highest power of $(x - \alpha)$ dividing $a(x)$. A nonzero polynomial of degree d has at most d roots, counting multiplicities.

Polynomial interpolation: A polynomial of degree d is uniquely determined by any $d+1$ values of $a(x)$. It can be interpolated as follows: $a(x) = \sum_{i=1}^{d+1} B_i \cdot u_i \cdot c_i$.

Where $B_i = a(\alpha_i)$ $(i = 1 \ldots d+1)$ and $u_i := \frac{(x-\alpha_1)\ldots(x-\alpha_{i-1})(x-\alpha_{i+1})\ldots(x-\alpha_{d+1})}{(\alpha_i-\alpha_1)\ldots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\ldots(\alpha_i-\alpha_{d+1})}$

Finite fields: Besides $GF(p)$, there are other finite fields.

The ring $F[x]_{m(x)}$: Congruence modulo $m(x)$ is an equiv. rel. on $F[x]$ and each equiv. class has a unique representation of degree less than $m(x)$. E.g. $5x^3 - 2x + 7 \equiv_{3x+2} 8x^2 + 1 \equiv_{3x+2} -\frac{16}{5}x + 7$. $F[x]_{m(x)} := \{a(x) \in F[x] \mid \deg_F(a(x)) < d\}$ $|F[x]_{m(x)}| = q^d$ ($d = \deg_F(m(x))$) and $q =$ nr. of elements of field F). $F[x]_{m(x)}$ is a ring with respect to addition and multiplication modulo $m(x)$. The congruence equation $a(x)b(x) \equiv_{m(x)} 1$ has a solution iff $\gcd(a(x), b(x)) = 1$. Therefore the ring $F[x]_{m(x)}$ is a field iff $m(x)$ is irreducible. $\mathbb{R}[x]_{m(x)}$ is isomorphic to $\mathbb{C}$ for all irreducible polynom of degree 2 over $\mathbb{R}$.

Error-Correcting codes: The encoding function takes a list of k information symbols and encodes it into a list of $n > k$ symbols in A (codeword). The set C of codewords is called an error-correcting code. $C = \text{Im}(E) = \{E(a_0, \ldots, a_{k-1}) \mid a_0 \ldots a_{k-1} \in A^k\}$

$A(n, k)$-error correcting code C over the alphabet A with $|A| = q$ is a subset of A^n with cardinality q^k. **Hamming distance:** Number of positions at which two strings (equal length) differ. **Minimum distance** of an ECC is the minimum of the Hamming distance between any two keywords. Example: $(5,2)$-code over $A = \{0,1\}$: $\{(0,0,0,0,0), (1,1,1,0,0), (0,0,1,1,1), (1,1,0,1,1)\}$

A code C with minimum distance d can correct t errors iff $d \geq 2t+1$. **Polynomial encoding:** $A = GF(q)$ and $\alpha_0, \ldots, \alpha_{n-1}$ arbitrary distinct elements from $GF(q)$. Encoding function: $E(a_0, \ldots, a_{n-1}) = (a(\alpha_0), \ldots, a(\alpha_{n-1}))$ where $a(x)$ is the polynomial: $a(x) := a_{n-1}x^{k-1} + \ldots + a_1 x + a_0$. The code has min. distance $n - k + 1$.

Appendix

Formulas / Statement about formulas: $F \not\equiv G$ or $F \equiv G$ are statements about formulas. "F is a tautology" is also a statement about the formula F. **Example of a calculus:**

Sound, but not complete: $K = \{R_1\}$ where $\{F\} \vdash_{R_1} F$

Complete, but not sound: $K = \{R_2\}$ where $\vdash_{R_2} F$ **Set of formulas:** A set M of formulas can be interpreted as the conjunction (AND) of all formulas in M. **Necessary / sufficient conditions:**

Necessary: A condition A is necessary for a condition B if the falsity of A guarantees the falsity of B. E.g.: A student must hand in the paper ($=A$) to get a 6 ($=B$).

Sufficient: A condition A is sufficient for a condition B if the truth of A guarantees the truth of B. **Examples of formula interpretations:** For the formula $G := \forall x \exists y (P(x,y) \wedge \neg P(f(x), y) \wedge Q(y, z))$ give a structure:

suitable and a model for G: $U^A = \mathbb{R}^+$; $f^A(x) = 2x$; $P^A(x,y) = 1 \iff x \leq y$; $Q^A(y,y) = 1$; $z^A = 1$

suitable but not a model for G: $U^A = \mathbb{R}^+$; $f^A(x) = x$; $P^A(x,y) = 0$; $Q^A(y,y) = 0$; $z^A = 1$; Not suitable for G: $U^A = \mathbb{R}^+$; $z^A = 42$;

Power sets example: $P(\emptyset) = \{\emptyset\}$, $P(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$

Set cardinality: $|\emptyset| = 0$, $|\{\emptyset\}| = 1$, $|\{\emptyset, \{\emptyset\}\}| = 2$ **Cartesian product:** $A \times \emptyset = \emptyset$ **Set difference:** $A \setminus B := \{x \in A \mid x \notin B\}$

Example relation composition: For the relation $p = \{(1,4), (2,1), (2,3), (4,2)\}$, determine p^3 and p^* (using matrix representation). $p^3 = \{(1,1), (1,3), (2,2), (4,4)\}$

$$M^{p^*} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

Ordered pair with sets: $(a,b) := \{\{a\}, \{a, b\}\}$

$\mathbb{Z}_m$ zerodivisors: A special property of $\mathbb{Z}_m$ is that each non-zero element is either a unit (the set $\mathbb{Z}_m^*$) or a zerodivisor (not relatively prime to m). **Irreducible polynomials:** A polynomial $a(x)$ over a field F is irreducible iff it has no roots. A polynomial of degree 4 is either irreducible, has a factor of degree 1 or has an irreducible factor of degree 2. **Finite fields / Galois field:** There exist a finite field with q elements iff q is a power of a prime. The multiplicative group of every finite field is cyclic, has $q-1$ elements and $\varphi(q-1)$ generators. Finite fields with p^d elements are $GF(p)[x]_{m(x)}$ where $m(x)$ is an irreducible polynomial of degree d. **Euler Phi function values:**

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