Proofs

D2.1: A *mathematical statement* is a statement that is true or false in an absolute, indesputable sense.

D (Composition of statements):

1. Negation: S is false.
2. And: S and T are both true.
3. Or: At least one of S and T is true.
4. Implication: If S is true, then T is true.

Proof Patters

Direct proof: To prove $S \implies T$ assume S and show T.

Indirect proof: To prove $S \implies T$ assume "T is false" and show "S is false".

Modus ponens: To prove S:

1. Find suitable R.
2. Prove R.
3. Prove $R \implies S$.

Case distinction: To prove S:

1. Find finite list $R_1, \ldots, R_k$ of statements.
2. Prove that at least one of the R_i is true.
3. Prove $R_i \implies S$ for $i = 1, \ldots, k$.

Proof by contradiction: To prove S:

1. Find suitable T.
2. Prove "T is false".
3. Assume "S is false" and prove T.

Pigeonhole principle (T2.10): If a set of n objects is partitioned into $k < n$ sets, at least one of these sets contains at least $\lceil \frac{n}{k} \rceil$ objects.

Proof by counterexample.

Proof by (strong) induction.

Sets, Relations, Functions

Introduction

D3.1: The number of elements in a finite set A is its cardinality $|A|$.

D (Russell's paradox): $R = \{A \mid A \notin A\}$.

Sets

D3.2: $A = B \overset{\text{def}}{\iff} \forall x(x \in A \leftrightarrow x \in B)$.

L3.1: $\{a\} = \{b\} \implies a = b$.

E3.1: $(a, b) \overset{\text{def}}{=} \{\{a\}, \{a, b\}\}$.

D3.3: $A \subseteq B \overset{\text{def}}{\iff} \forall x(x \in A \to x \in B)$.

L3.2: $A = B \iff (A \subseteq B) \wedge (B \subseteq A)$.

L3.3: $A \subseteq B \wedge B \subseteq C \implies A \subseteq C$.

D3.4: $A \overset{\cup}{\cap} B \overset{\text{def}}{=} \{x \mid x \in A \overset{\vee}{\wedge} x \in B\}$.

D3.5: $B \backslash A \overset{\text{def}}{=} \{x \in B \mid x \notin A\}$.

T3.4: For any sets A, B, C the following laws hold:

name	law
idempot.	$A \overset{\cup}{\cap} A = A$
commut.	$A \overset{\cup}{\cap} B = B \overset{\cup}{\cap} A$
assoc.	$A \overset{\cup}{\cap} (B \overset{\cup}{\cap} C) = (A \overset{\cup}{\cap} B) \overset{\cup}{\cap} C$
absorp.	$A \overset{\cup}{\cap} (A \overset{\cap}{\cup} B) = A$
distrib.	$A \overset{\cup}{\cap} (B \overset{\cap}{\cup} C) = (A \overset{\cup}{\cap} B) \overset{\cap}{\cup} (A \overset{\cup}{\cap} C)$
consist.	$A \subseteq B \iff$
	$A \cap B = A \iff A \cup B = B$

D3.6: The set A is called *empty* if $\forall x \neg(x \in A)$.

L3.5: There is only one empty set, denoted as $\varnothing$ or $\{\}$.

L3.6: $\forall A(\varnothing \subseteq A)$.

R (Construction of $\mathbb{N}$):

$\mathbf{0} \overset{\text{def}}{=} \varnothing$ $\mathbf{1} \overset{\text{def}}{=} \{\varnothing\}$ $\mathbf{2} \overset{\text{def}}{=} \{\varnothing, \{\varnothing\}\}$ $\mathbf{3} \overset{\text{def}}{=} \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$

The successor of $\mathbf{n}$ is defined as $s(\mathbf{n}) \overset{\text{def}}{=} \mathbf{n} \cup \{\mathbf{n}\}$.

An operation $+$ can be defined recursively as $\mathbf{m} + \mathbf{0} \overset{\text{def}}{=} \mathbf{m}$ and $\mathbf{m} + s(\mathbf{n}) \overset{\text{def}}{=} s(\mathbf{m} + \mathbf{n})$.

D3.7: $\mathcal{P}(A) \overset{\text{def}}{=} \{S \mid S \subseteq A\}$.

D3.8: $A \times B \overset{\text{def}}{=} \{(a, b) \mid a \in A \wedge b \in B\}$.

Relations

D3.9: A (binary) *relation* ρ from A to B is a subset of $A \times B$. We also write $a \rho b$ ($a \not\rho b$) instead of $(a, b) \in \rho$ ($(a, b) \notin \rho$).

D3.10: $\mathrm{id}_A = \{(a, a) \mid a \in A\}$.

Representations of ρ:

- $|A| \times |B|$ matrix M^ρ with $M^\rho_{a,b} = 1$ iff $a \rho b$.
- Directed graph with the vertices labeled with elements of A and B that contains an edge from a to b iff $a \rho b$.

D3.11: $\hat{\rho} \overset{\text{def}}{=} \{(b, a) \mid (a, b) \in \rho\}$.

D3.12: $\rho \circ \sigma \overset{\text{def}}{=} \{(a, c) \mid \exists b((a, b) \in \rho) \wedge (b, c) \in \sigma)\}$.

L3.7: $\rho \circ (\sigma \circ \phi) = (\rho \circ \sigma) \circ \phi$.

L3.8: $\widehat{\rho\sigma} = \hat{\sigma}\hat{\rho}$.

Special properties of Relations

D3.13-D3.17, L3.9:

name	condition	set
reflexive	$a \rho a$	$\mathrm{id} \subseteq \rho$
symmetric	$a \rho b \iff b \rho a$	$\rho = \hat{\rho}$
antisym.	$a \rho b \wedge b \rho a \implies a = b$	$\rho \cap \hat{\rho} \subseteq \mathrm{id}$
transitive	$a \rho b \wedge b \rho c \implies a \rho c$	$\rho^2 \subseteq \rho$

D3.18: The *transitive closure* of a relation ρ on a set A is $\rho* = \bigcup_{n \in \mathbb{Z}^+} \rho^n$.

Equivalence relations

D3.19: An *equivalence relation* is a relation on a set A that is reflexive, symmetric, and transitive.

D3.20: For an equivalence relation θ on A and $a \in A$ the *equivalence class* of a is $[a]_\theta \overset{\text{def}}{=} \{b \in A \mid b \theta a\}$.

L3.10: The intersection of equivalence relations is an equivalence relation.

D3.21: A *partition* of a set A is a set of mutually disjoint subsets of A that cover A.

D3.22: The set of equivalence classes of an equivalence relation θ denoted by $A/\theta \overset{\text{def}}{=} \{[a]_\theta \mid a \in A\}$ is called the *quotient set* of A by θ or A *modulo* θ or A mod θ.

T3.11: The set A/θ is a partition of A.

Partial order relations

D3.23: A *partial order* on a set A is a relation $\preceq$ that is reflexive, antisymmetric, and transitive. Then $(A; \preceq)$ is called a *partially ordered set* or *poset*.

D: $a \prec b \overset{\text{def}}{\iff} a \preceq b \wedge a \neq b$.

D3.24: For a poset $(A; \preceq)$, two elements a, b are called *comparable* if $a \preceq b$ or $b \preceq a$; otherwise *incomparable*.

D3.25: If any two elements of a poset $(A; \preceq)$ are comparable, then A is called *totally ordered* by $\preceq$.

D3.26: In a poset $(A; \preceq)$ b is said to *cover* a if $a \prec b$ and there exists no c with $a \prec c$ and $c \prec b$.

D3.27: The *Hasse diagram* of a (finite) poset $(A; \preceq)$ is the directed graph whose vertices are labeled with the elements of A and where there is an edge from a to b iff b covers a.

D3.28: The *direct product* of posets $(A; \preceq)$ and $(B; \sqsubseteq)$ denoted $(A; \preceq) \times (B; \sqsubseteq)$ is $A \times B$ with the relation $\leqslant$ defined by $(a_1, b_1) \leqslant (a_2, b_2) \overset{\text{def}}{\iff} a_1 \preceq a_2 \wedge b_1 \sqsubseteq b_2$.

T3.12: $(A; \preceq) \times (B; \sqsubseteq)$ is a poset.

T3.13: For the posets $(A; \preceq)$ and $(B; \sqsubseteq)$, the relation $\leqslant_{\text{lex}}$ defined on $A \times B$ by $(a_1, b_1) \leqslant_{\text{lex}} (a_2, b_2) \overset{\text{def}}{\iff} a_1 \preceq a_2 \vee (a_1 = a_2 \wedge b_1 \sqsubseteq b_2)$.

D3.29: Let $(A; \preceq)$ be a poset and let $S \subseteq A$. Then:

1. $a \in A$ is a *minimal* (*maximal*) element of A iff there exists no $b \in A$ with $b \prec a$ ($b \succ a$).
2. $a \in A$ is the *least* (*greatest*) element of A iff $a \preceq b$ ($a \succeq b$) for all $b \in A$.
3. $a \in A$ is a *lower* (*upper*) *bound* of S iff $a \preceq b$ ($a \succeq b$) for all $b \in S$.
4. $a \in A$ is a *greatest lower bound* (*least upper bound*) of S iff a is the greatest (least) element of the set of all lower (upper) bounds of S.

D3.30: A poset $(A; \preceq)$ is *well-ordered* if it is totally ordered and if every non-empty subset of A has a least element.

D3.31: Let $(A; \preceq)$ be a poset. If a and b have a greatest lower bound, then it is called the *meet* of a and b, often denoted $a \wedge b$. If a and b have a least upper bound, then it is called the *join* of a and b, often denoted $a \vee b$.

D3.32: A poset $(A; \preceq)$ in which every pair of elements has a meet and join is called a *lattice*.

Functions

D3.33: A *function* $f\colon A \to B$ from a *domain* A to a *codomain* B is a relation from A to B with the special properties:

1. $\forall a \in A \exists b \in B a f b$,
2. $\forall a \in A \forall b, b' \in B (a f b \wedge a f b' \to b = b')$.

(f is totally defined and well-defined).

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

D3.35: A *partial function* $A \to B$ is a relation from A to B such that condition 2. in [D3.33] holds.

D3.36: For $f\colon A \to B$ and $S \subseteq A$, the *image* of S under f is $f(S) \overset{\text{def}}{=} \{f(s) \mid s \in S\}$.

D3.37: The subset $f(A)$ of B is called the *image* of f.

D3.38: For $T \subseteq B$, the *preimage* of T is $f^{-1}(T) \overset{\text{def}}{=} \{a \in A \mid f(a) \in T\}$.

D3.39: A function $f\colon A \to B$ is called:

1. *injective* if $a \neq a' \implies f(a) \neq f(a')$,
2. *surjective* if $f(A) = B$,
3. *bijective* if it is both injective and surjective.

D3.40: For a bijective function f the *inverse* is called the inverse function of f, denoted f^{-1}.

D3.41: The *composition* of functions $f\colon A \to B$, $g\colon B \to C$, denoted $g \circ f$, is defined by $(g \circ f)(a) = g(f(a))$.

L3.14: $(h \circ g) \circ f = h \circ (g \circ f)$.

Countability

D3.42: Let A, B be sets.

1. A, B are *equinumerous*, denoted $A \sim B$, iff there exists a bijection $A \to B$.
2. B *dominates* A, denoted $A \preceq B$, if $A \sim C$ for some $C \subseteq B$, or equivalently, there exits an injection $A \to B$.

3. A is called *countable* iff $A \preceq \mathbb{N}$ and *uncountable* otherwise.

L3.15:

1. The relation $\sim$ is an equivalence relation.
2. The relation $\preceq$ is transitive.
3. $A \subseteq B \implies A \preceq B$.

T3.16: $A \preceq B \wedge B \preceq A \implies A \sim B$.

T3.17: A set A is countable iff it is finite or if $A \sim \mathbb{N}$.

T3.18: The set $\{0,1\}^* \overset{\text{def}}{=} \{\epsilon, 0, 1, 00, 01, 10, \ldots\}$ of finite sequences in countable.

T3.19: The set $\mathbb{N} \times \mathbb{N}$ is countable.

T3.22: Let A be a countable set.

1. For any $n \in \mathbb{N}$, the set A^n is countable.
2. The union of a countable list of of countable sets is countable.
3. The set A^* is countable.

D3.43: Let $\{0,1\}^\infty$ denote the set of semi-infinte binary sequences, or equivalently, of functions $\mathbb{N} \to \{0,1\}$.

T3.23: The set $\{0,1\}^\infty$ is uncountable.

D3.44: A function $f\colon \mathbb{N} \to \{0,1\}$ is called *computable* iff there is a program that, for every $n \in \mathbb{N}$, when given n as input, outputs $f(n)$.

C3.24: There are uncomputable functions $\mathbb{N} \to \{0,1\}$.

Number theory

Divisors and Division

D4.1: Divisibility.

T4.1 (Euclid): For all $a \in \mathbb{Z}$ and $d \neq 0$ there exist unique $q, r \in \mathbb{Z}$ satisfying $a = dq + r$ and $0 \leqslant r < |d|$.

D4.2: For $a, b \in \mathbb{Z}$ (not both 0) d is called a *greatest common divisor* of a and b if every common divisor of a and b divides d, i.e. if $d \mid a \wedge d \mid b \wedge \forall c((c \mid a \wedge c \mid b) \to c \mid d)$.

D4.3: For $a, b \in \mathbb{Z}$ (not both 0) one denotes the unique positive greatest common divisor by $\gcd(a,b)$ and calls it *the* greatest common divisor. If $\gcd(a,b) = 1$, then a and b are called *relatively prime*.

L4.2: For $m, n, q \in \mathbb{Z}$ we have $\gcd(m, n - qm) = \gcd(m,n)$.

D4.4: For $a, b \in \mathbb{Z}$, the *ideal generated by a and b* is $(a,b) \overset{\text{def}}{=} \{ua + vb \mid u, v \in \mathbb{Z}\}$.

L4.3: For $a, b \in \mathbb{Z}$ there exists $d \in \mathbb{Z}$ such that $(a,b) = (d)$.

L4.4: Let $a, b \in \mathbb{Z}$ (not both 0). If $(a,b) = (d)$ then d is a greatest common divisor of a and b.

D4.5: The *least common multiple* l of $a, b \in \mathbb{Z}^+$, denoted $l = \operatorname{lcm}(a,b)$, is the common multiple of a and b which divides every common multiple of a and b, i.e. $a \mid l \wedge b \mid l \wedge \forall m((a \mid m \wedge b \mid m) \to l \mid m)$.

Factorization into primes

D4.6: $p \in \mathbb{Z}_{>1}$ is called *prime* iff the only positive divisors of p are 1 and p. An $x \in \mathbb{Z}_{>1}$ that is not prime is called *composite*.

T4.6: Every positive integer can be written uniquely as the product of primes.

Expressing gcd and lcm

T: Let $a = \prod_i p_i^{e_i}$, $b = \prod_i p_i^{f_i}$. Then $\gcd(a,b) = \prod_i p_i^{\min(e_i, f_i)}$ and $\operatorname{lcm}(a,b) = \prod_i p_i^{\max(e_i, f_i)}$.

Congruences and modular arithmetic

D4.8: Let $a, b, m \in \mathbb{Z}$ with $m \geqslant 1$. $a \equiv_m b \overset{\text{def}}{\iff} m \mid (a - b)$.

L4.13: For $m \geqslant 1$, $\equiv_m$ is an equivalence relation on $\mathbb{Z}$.

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

L4.16: For any $a, b, m \in \mathbb{Z}$ with $m \geqslant 1$,

1. $a \equiv_m R_m(a)$,
2. $a \equiv_m b \iff R_m(a) = R_m(b)$.

L4.18: The congruence equation $ax \equiv_m 1$ has a (unique) solution $x \in \mathbb{Z}_m$ iff $\gcd(a,m) = 1$.

D4.9: If $\gcd(a,m) = 1$, the unique solution $x \in \mathbb{Z}_m$ to the congruence equation $ax \equiv_m 1$ is called the *multiplicative inverse of a modulo m*. One also uses the notation $x \equiv_m a^{-1}$.

T4.19: Let $m_1, \ldots, m_r$ be pairwise relatively prime integers and let $M = \prod_{i=1}^r m_i$. For every list $a_1, \ldots, a_r$ with $0 \leqslant a_i < m_i$ for $1 \leqslant i \leqslant r$, the system of congruence equations

$$x \equiv_{m_1} a_1$$
$$\cdots$$
$$x \equiv_{m_r} a_r$$

for x has a unique solution x satisfying $0 \leqslant x < M$.

Application: Diffie-Hellman key exchange

D (Diffie-Hellman): Let $p \in \mathbb{P}$ and g be public.

Alice	insecure	Bob
select $x_A \in [p-2]$		select $x_B \in [p-2]$
$y_A := R_p(g^{x_A})$		$y_B := R_p(g^{x_B})$
	$\xrightarrow{y_A}$	
	$\xleftarrow{y_B}$	
$k_{AB} := R_p(y_B^{x_A})$		$k_{BA} := R_p(y_A^{x_B})$

$$k_{AB} \equiv_p k_{BA}$$

Algebra

Introduction

D5.1: An *operation* on a set S is a function $S^n \to S$, where $n \geqslant 0$ is called the *arity* of the operation.

D5.2: An *algebra* is a pair $\langle S; \Omega\rangle$ where S is a set (*carrier*) and Ω is a list of operations on S.

Monoids and groups

D5.3: A *left [right] neutral element* of an algebra $\langle S; *\rangle$ is an element $e \in S$ such tha $e * a = a$ $[a * e = a]$ for all $a \in S$.

L5.1: If $\langle S; *\rangle$ has both a left and right neutral element, then they are equal.

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

D5.5: A *monoid* is an algebra $\langle M; *, e\rangle$ where $*$ is associative and e is the neutral element.

D5.6: A *left [right] inverse element* of an element a in $\langle S; *, e\rangle$ is an element $b \in S$ such that $b * a = e$ $[a * b = e]$.

L5.2: In a monoid $\langle M; *, e\rangle$, if $a \in M$ has a left and right inverse, then they are equal.

D5.7: A *group* is an algebra $\langle G; *, \hat{\ }, e\rangle$ satisfying the following axioms:

1. $*$ is associative.
2. e is a neutral element.
3. Every $a \in G$ has an inverse element $\hat{a}$.

D5.8: A group $\langle G; *\rangle$ (or monoid) is called *commutative* if $a * b = b * a$ for all $a, b \in G$.

L5.3: For a group $\langle G; *, \hat{\ }, e\rangle$, we have for all $a, b, c \in G$:

1. $\hat{\hat{a}} = a$.
2. $\widehat{a * b} = \hat{b} * \hat{a}$.
3. Left cancellation: $a * b = a * c \implies b = c$.
4. Right cancellation: $b * a = c * a \implies b = c$.
5. The equation $a * x = b$ has a unique soultion x for any a, b.

The structure of groups

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

L5.4: $\langle G_1 \times \cdots \times G_n, \star\rangle$ is a group, where the neutral element and the inversion operation are component-wise in the respective groups.

D5.10: For groups $\langle G; *, \hat{\ }, e\rangle$ and $\langle H; \star, \tilde{\ }, e'\rangle$, a function $\psi\colon G \to H$ is called a *group homomorphism* iff for all a and b we have $\psi(a * b) = \psi(a) \star \psi(b)$. Iff ψ is a bijection from G to H, then it is called an *isomorphism*, and we write $A \simeq H$.

L5.5: A ψ in [D5.10] satisfies:

1. $\psi(e) = e'$,
2. $\psi(\hat{a}) = \widetilde{\psi(a)}$ for all a.

D5.11: $H \subseteq G$ of $\langle G; *, \hat{\ }, e\rangle$ is called a *subgoup* of G iff $\langle H; *, \hat{\ }, e\rangle$ is a group (closed).

D5.12: Let G be a group and $a \in G$. The *order* of a, denoted $\operatorname{ord}(a)$ is the least $m \geqslant 1$ such that $a^m = e$ if such an m exists, and ∞ otherwise.

D5.13: For a finite group G, $|G|$ is called the *order* of G.

D5.14: For a group G and $a \in G$ the *group generated by a* is $\langle a\rangle \overset{\text{def}}{=} \{a^n \mid n \in \mathbb{Z}\}$.

D5.15: A group $G = \langle g\rangle$ is called *cyclic* and g is called a *generator* of G.

T5.7: A cyclic group of order n is isomorphic to $\langle \mathbb{Z}_n; \oplus\rangle$.

T5.8 (Lagrange): Let G be a finite group and let H be a subgoup of G. Then $|H|$ divides $|G|$.

C5.10: Let G be a finite group. Then $a^{|G|} = e$ for every $a \in G$.

C5.11: Every group of prime order is cyclic, and every element except the neutral element is a generator.

D5.16: $\mathbb{Z}_m^* \overset{\text{def}}{=} \{a \in \mathbb{Z}_m \mid \gcd(a,m) = 1\}$.

D5.17 (Euler function): $\varphi(m) = |\mathbb{Z}_m^*|$.

L5.12: If the prime factorization of m is $m = \prod_{i=1}^r p_i^{e_i}$, then $\varphi(m) = \prod_{i=1}^r (p_i - 1) p_i^{e_i - 1}$.

T5.13: $\langle \mathbb{Z}_m^*; \odot, {}^{-1}, 1\rangle$ is a group.

C5.14 (Fermat, Euler): For all $m \geqslant 2$ and all a with $\gcd(a,m) = 1$ we have $a^{\varphi(m)} \equiv_m 1$. In particular, for $p \in \mathbb{P}$ and $p \nmid a$ we have $a^{p-1} \equiv_p 1$.

Application: RSA Public-key cryptography

T5.16: Let G be some finite group and let $e \in \mathbb{Z}$ be relatively prime to $|G|$. The function $x \mapsto x^e$ is a bijection and the unique e-th root of $y \in G$, namely $x \in G$ satisfying $x^e = y$ is $x = y^d$, where $ed \equiv_{|G|} 1$.

D (RSA):

Alice	insecure	Bob
generate $p, q \in \mathbb{P}$		
$m = pq$		
$\lambda = (p-1)(q-1)$		
select e		
$d \equiv_\lambda e^{-1}$	$\xrightarrow{n,e}$	$m \in [n-1]$
$m = R_n(c^d)$	$\xleftarrow{c}$	$c = R_n(m^e)$

Rings and fields

D5.18: 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 $a, b, c \in \mathbb{R}$.

A ring is called *commutative* if multiplication is commutative: $ab = ba$.

L5.17: For any ring $\langle R; +, -, 0, \cdot, 1\rangle$, and for all $a, b, \in \mathbb{R}$,

1. $0a = a0 = 0$.
2. $(-a)b = -(ab)$.
3. $(-a)(-b) = ab$.
4. If R is non-trivial, then $1 \neq 0$.

D5.19: The *characteristic* of a ring is the order of 1 in the additive group if it is finite, and 0 otherwise.

D5.20: An element u or a ring R is called a *unit* if u is invertible. The set of units of R is denoted by R^*.

L5.18: For a ring R, R^* is a group.

D5.21: For $a, b \in R$ we say that a *divides* b, denoted $a \mid b$, if there exists $c \in R$ such that $b = ac$. In the case, a is called a *divisor* of b and b is a *multiple* of a.

L5.19: In any commutative ring,

1. If $a \mid b$ and $b \mid c$ then $a \mid c$.
2. If $a \mid b$, then $a \mid bc$.
3. If $a \mid b$ and $a \mid c$, then $a \mid (b+c)$.

D5.22: gcd in R.

D5.23: An element $a \neq 0$ of a commutative ring R is called a *zerodivisor* if $ab = 0$ for some $b \neq 0$ in R.

D5.24: An *integral domain* D is a (nontrivial) commutative ring without zerodivisors: For all $a, b \in D$ we have $ab = 0 \implies a = 0 \vee b = 0$.

L5.20: In an integral domain, if $a \mid b$, then c with $b = ac$ is unique (and is denoted by $c = \frac{b}{a}$ or $c = b/a$ and called quotient).

D5.25: A *polynomial* $a(x)$ over a commutative ring R in the indeterminate x is a formal expression of the form $a(x) = a_d x^d + \cdots + a_1 x + a_0$ for some non-negative integer d, with $a_i \in R$. The *degree* of $a(x)$, denoted $\deg(a(x))$, is the greatest i for which $a_i \neq 0$. The special polynomial 0 is defined to have degree "minus infinity". Let $R[x]$ denote the set of polynomials (in x) over R.

T5.21: For any commutative ring R, $R[x]$ is a commutative ring.

L5.22: Let D be an integral domain. Then

1. $D[x]$ is an integral domain.
2. The degree of the product of two polynomials is the sum of their degrees.
3. The units of $D[x]$ are the constant polynomials that are units of D: $D[x]^* = D^*$.

D5.26: A field is a nontrivial commutative ring F in which every nonzero element is a unit, i.e., $F^* = F \backslash \{0\}$.

T5.23: $\mathbb{Z}_p$ is a field iff p is prime.

T5.24: A field is an integral domain.

Polynomials over a field

D5.27: A polynomial $a(x) \in F[x]$ is called *monic* if the leading coefficient is 1.

D5.28: A polynomial $a(x) \in F[x]$ with degree at least 1 is called *irreducible* if it is divisible only by constant polynomials and by constant multiples of $a(x)$.

D5.29: The monic polynomial $g(x)$ of largest degree such that $g(x) \mid a(x)$ and $g(x) \mid b(x)$ is called *the* greatest common divisor of $a(x)$ and $b(x)$, denoted $\gcd(a(x), b(x))$.

T5.25: Let F be a field. For $a(x)$ and $b(x) \neq 0$ in $F[x]$ there exist a unique $q(x)$ (the quotient) and a unique $r(x)$ (the remainder) such that $a(x) = b(x)q(x) + r(x)$ and $\deg(r(x)) < \deg(b(x))$.

Polynomials as functions

D5.33: Let $a(x) \in R[x]$. An element $\alpha \in R$ for which $a(\alpha) = 0$ is called a *root* of $a(x)$.

L5.29: For a field F, $\alpha \in F$ is a root of $a(x)$ iff $x - \alpha$ divides $a(x)$.

C5.30: A polynomial $a(x)$ of degree 2 or 3 over a field F is irreducible iff it has no root.

T5.31: For a field F, a nonzero polynomial $a(x) \in F[x]$ of degree d has at most d roots.

L5.32: A polynomial $a(x) \in F[x]$ of degree at most d is uniquely determined by any $d+1$ values of $a(x)$.

Finite fields

L5.33: Congruence modulo $m(x)$ is an equivalence relation on $F[x]$, and each equivalence class has a unique representation of degree less than $\deg(m(x))$.

D5.34: Let $m(x)$ be a polynomial of degree d over F. Then $F[x]_{m(x)} \overset{\text{def}}{=} \{a(x) \in F[x] \mid \deg(a(x)) < d\}$.

L5.34: Let F be a finite field with q elements and let $m(x)$ be a polynomial of degree d over F. Then $|F[x]_{m(x)}| = q^d$.

L5.35: $F[x]_{m(x)}$ is a ring with respect to addition and multiplication modulo $m(x)$.

L5.36: The congruence equation $a(x)b(x) \equiv_{m(x)} 1$ has a solution $b(x) \in F[x]_{m(x)}$ iff $\gcd(a(x), m(x)) = 1$. The solution is unique. In other words, $F[x]^*_{m(x)} = \{a(x) \in F[x]_{m(x)} \mid \gcd(a(x), b(x)) = 1\}$.

T5.37: The ring $F[x]_{m(x)}$ is a field iff $m(x)$ is irreducible.

Application: Error-Correcting Codes

D5.35: An $(n,\, k)$-*encoding function* E for some alphabet $\mathcal{A}$ is an injective function that maps a list $a_0, \ldots, a_{k-1} \in \mathcal{A}^k$ of k symbols to a list of $c_0, \ldots, c_{n-1} \in \mathcal{A}^n$ of $n > k$ (encoded) symbols in $\mathcal{A}$ called *codeword*.

D5.36: An $(n,\, k)$-*error-correcting code* over the alphabet $\mathcal{A}$ with $|\mathcal{A}| = q$ is a subset of $\mathcal{A}^n$ of cardinality q^k.

D5.37: The *Hamming distance* between two strings of equal length over a finite alphabet $\mathcal{A}$ is the number of positions at which the two strings differ.

D5.38: The *minimum distance* of an error-correcting code $\mathcal{C}$, denoted $d_{\min(\mathcal{C})}$, is the minimum of the Hamming distance between any two codewords.

D5.39: A *decoding function* D for an $(n,\, k)$-encoding function is a function $D\colon \mathcal{A}^n \to \mathcal{A}^k$.

D5.40: A decoding function D is *t-error correcting* for the encoding function E if for any $(a_0, \ldots, a_{k-1})$ we have $D((r_0, \ldots, r_{n-1})) = (a_0, \ldots, a_{k-1})$ for any $(r_0, \ldots, r_{n-1})$ with Hamming distance at most t from $E((a_0, \ldots, a_{k-1}))$. A code $\mathcal{C}$ is *t-error correcting* if there exist E and D with $\mathcal{C} = \operatorname{Im}(E)$ where D is t-error correcting.

T5.41: A code $\mathcal{C}$ with minimum distance d is t-error-correcting iff $d \geqslant 2t+1$.

T5.42: Let $\mathcal{A} = \mathrm{GF}(q)$ and let $\alpha_0, \ldots, \alpha_{n-1}$ be arbitrary distinct elements of $GF(q)$. Consider the encoding function $E((a_0, \ldots, a_{k-1})) = (a(\alpha_0), \ldots, a(\alpha_{n-1}))$, where $a(x)$ is the polynomial $a(x) = a_{k-1}x^{k-1} + \cdots + a_1 x + a_0$. This code has a minimum distance of $n - k + 1$.

Logic

Proof systems

A *proof system* is a quadruple $\Pi = (\mathcal{S}, \mathcal{P}, \tau, \phi)$, where

1. $\mathcal{S}, \mathcal{P} \subseteq \Sigma^*$,
2. $\tau\colon \mathcal{S} \to \{0,1\}$,
3. $\tau\colon \mathcal{S} \times \mathcal{P} \to \{0,1\}$,

W.l.o.g. we consider $\mathcal{P} = \mathcal{S} = \{0,1\}^*$.

D6.2: Π is *sound* iff for all $s \in \mathcal{S}$ for which there exists $p \in \mathcal{P}$ with $\phi(s,p) = 1$ we have $\tau(s) = 1$.

D6.3: Π is *complete* iff for all $s \in \mathcal{S}$ with $\tau(s) = 1$ there exists $p \in \mathcal{P}$ with $\phi(s,p) = 1$.

Elementary general concepts in logic

D6.4: The *syntax* of a logic defines an alphabet Λ and specifies which strings in Λ^* are formulas.

D6.5: The *semantics* of a logic defines a function *free* which assigns to each formula $F = (f_1, \ldots, f_k) \in \Lambda^*$ a subset *free*$(F) \subseteq [k]$ of the indices. If $i \in$ *free*(F), then the symbol f_i is said to occur *free* in F.

D6.6: An *interpretation* consists of a set $\mathcal{Z} \subseteq \Lambda$, a domain for each symbol in $\mathcal{Z}$, and a function that assigns that assigns to each symbol in $\mathcal{Z}$ a value in its associated domain.

D6.7: An interpretation is *suitable* for a formula F if it assigns a value to all symbols $\beta \in \Lambda$ occurring free in F.

D6.8: The *semantics* of a logic also defines a function σ assigning to each formula F and each interpretation $\mathcal{A}$ suitable for F, a truth value $\sigma(F, \mathcal{A})$ in $\{0,1\}$. One often writes $\mathcal{A}(F)$ instead of $\sigma(F, \mathcal{A})$ and calls $\mathcal{A}(F)$ the *truth value of F under the interpretation $\mathcal{A}$*.

D6.9: A (suitable) interpretation $\mathcal{A}$ for which the formula F is true is called a *model* for F and one writes $\mathcal{A} \models F$.

D6.10: F is called *satisfiable* iff there exists a model for F, and *unsatisfiable* (denoted $\bot$) otherwise.

D6.11: F is called a *tautology* (denoted $\top$) iff it is true for every suitable interpretation.

D6.12: A formula G is a *logical consequence* of a formula F, denoted $F \models G$, if every interpretation suitable for both F and G, which is a model for F is also a model for G.

D6.13 (Equivalence): $F \equiv G \overset{\text{def}}{\iff} F \models G$ and $G \models F$.

D6.14: If F is a tautology we write $\models F$.

D5.15: If F, G are formulas then also $\neg F$, $F(F \wedge G)$, and $(F \vee G)$ are formulas.

D6.16:

$$\mathcal{A}((F \wedge G)) = 1 \iff \mathcal{A}(F) = 1 \text{ and } \mathcal{A}(G) = 1$$
$$\mathcal{A}((F \vee G)) = 1 \iff \mathcal{A}(F) = 1 \text{ or } \mathcal{A}(G) = 1$$
$$\mathcal{A}(\neg F) = 1 \iff \mathcal{A}(F) = 0$$

L6.1: For any formulas F, G and H we have

name	law
idempot.	$F \overset{\vee}{\wedge} F \equiv F$
commut.	$F \overset{\vee}{\wedge} G = G \overset{\vee}{\wedge} F$
assoc.	$F \overset{\vee}{\wedge} (G \overset{\vee}{\wedge} H) = (F \overset{\vee}{\wedge} G) \overset{\vee}{\wedge} H$
absorp.	$F \overset{\vee}{\wedge} (F \overset{\wedge}{\vee} G) = F$
distrib.	$F \overset{\vee}{\wedge} (G \overset{\wedge}{\vee} H) = (F \overset{\vee}{\wedge} G) \overset{\wedge}{\vee} (F \overset{\vee}{\wedge} H)$
double neg.	$\neg\neg F \equiv F$
deMorgan	$\neg(F \overset{\vee}{\wedge} G) \equiv \neg F \overset{\wedge}{\vee} \neg G$
taut.	$F \vee \top \equiv \top$ and $F \wedge \top \equiv F$
unsat.	$F \vee \bot \equiv F$ and $F \wedge \bot \equiv \bot$
	$F \vee \neg F \equiv \top$ and $F \wedge \neg F \equiv \bot$

L6.2: F is a tautology iff $\neg F$ is unsatisfiable.

L6.3: The following statements are equivalent:

1. $\{F_1, \ldots, F_k\} \models G$,
2. $(F_1 \wedge \ldots \wedge F_k) \to G$ is a tautology,
3. $\{F_1, \ldots, F_k, \neg G\}$ is unsatisfiable.

Logical calculi

D.17: A *derivation rule* R is a relation from the power set of the set of formulas to the set of formulas and the symbol $\vdash_R$ is the relation symbol.

D6.18: The *application of a derivation rule* R to a set M of formulas means

1. Select $N \subseteq M$ such that $N \vdash_R G$.
2. Replace M with $M \cup \{G\}$.

D6.19: A (logical) *calculus* K is a finite set of derivation rules $K = \{R_1, \ldots, R_m\}$.

D6.20: A *derivation* of a formula G from a set M of formulas in a calculus K is a finite sequence of applications of rules in K, leading to G. We write $M \vdash_K G$.

D6.21: R is *correct* iff $M \vdash_R F \implies M \models F$.

D6.22: K is *sound* iff $M \vdash_K F \implies M \models F$.
K is *complete* iff $M \models F \implies M \vdash_K F$.

Propositional logic

D6.23 (Syntax): An *atomic formula* is a symbol of the form A_i. A *formula* is defined as follows:

1. An atomic formula is a formula.
2. See [D6.15].

D6.24 (Semantics): Each atomic formula is assigned a truth value. Then see [D6.16].

D6.25: A *literal* is an atomic formula or the negation of an atomic formula.

D6.26: A formula F is in *conjunctive normal form* (CNF) iff it is of the form $F = (A \vee \cdots \vee B) \wedge \cdots \wedge (Y \vee \cdots \vee Z)$.

D6.27: A formula F is in *disjunctive normal form* (DNF) iff it is of the form $F = (A \wedge \cdots \wedge B) \vee \cdots \vee (Y \wedge \cdots \wedge Z)$.

T6.4: Every formula is equivalent to a formula in CNF and a formula in DNF.

D6.28: A *clause* is a set of literals.

D6.29: The set of clauses associated to a formula in CNF (see [D6.26]) is $\mathcal{K}(F) \overset{\text{def}}{=} \{\{A, \ldots, B\}, \ldots, \{Y, \ldots, Z\}\}$.

D6.30: The clause K is a *resolvent* of clause K_1 and K_2 if there is a literal L such that $L \in K_1$, $\neg L \in K_2$, and $K = (K_1 \backslash \{L\}) \cup (K_2 \backslash \{\neg L\})$.

D (Resolution calculus): Let K_1, K_2, K as in [D6.30]. Then the *resolution rule* is $\{K_1, K_2\} \vdash_{\text{res}} K$ and the *reolution calculus* is $\text{Res} = \{\text{res}\}$.

L6.5: The resolution calculus is sound.

T6.6: A set M of formulas is unsat. iff $\mathcal{K}(M) \vdash_{\text{Res}} \emptyset$.

Predicate logic

D6.31 (syntax of predicate logic):

1. *variable*: x_i
2. *function*: $f_i^{(k)}$
3. *predicate*: $P_i^{(k)}$
4. *term*: Variables are terms and if $t_1, \ldots, t_k$ are terms, then $f_i^{(k)}(t_1, \ldots, t_k)$ is a term.
5. *formula*:
   - If $t_1, \ldots, t_k$ are terms, then $P_i^{(k)}(t_1, \ldots, t_k)$ is an *atomic* formula.
   - If F and G are formulas, then $\neg F$, $(F \wedge G)$, $(F \vee G)$ are formulas.
   - If F is a formula then $\forall x_i F$ and $\exists x_i F$ are formulas.

D6.32: Every occurence of a variable in a formula is either *bound* or *free*. Iff a variable x occurs in a (sub-)formula of the form $\forall x G$ or $\exists x G$ then it is bound. A formula is *closed* if it contains no free variables.

D6.33: For a formula F, a variable x and term t, $F[x/t]$ denotes the formula obtained from F by substituting every free occurence of x by t.

D6.34: An *interpretation* is a tuple $\mathcal{A} = (U, \phi, \psi, \xi)$ where

- U is a non-empty *universe*,
- ϕ is a function assigning to each function symbol a function, $\phi(f^{(k)}) : U^k \to U$,
- ψ is a function assigning to each predicate symbol a function, $\phi(P^{(k)}) : U^k \to \{0, 1\}$,
- ξ is a function assigning to each variable symbol a value, $\phi(x) \in U$.

D6.35: An interpretation $\mathcal{A}$ is *suitable* for a formula F iff it defines all function symbols, predicate symbols and freely occurring variables of F.

D6.36 (semantics): For an interpretation $\mathcal{A} = (U, \phi, \psi, \xi)$, we define the value (in U) of terms and the truth value of formulas as follows:

1. The value $\mathcal{A}(t)$ of a term t is defined recursively:
   - If $t = x_i$, then $\mathcal{A}(t) = \xi(x_i)$.
   - If $t = f(t_1, \ldots, t_k)$, then $\mathcal{A}(t) = \phi(f)(\mathcal{A}(t_1), \ldots, \mathcal{A}(t_k))$.
2. The truth value of a formula F is defined recursively:
   - See [D6.16].
   - If $F = P(t_1, \ldots, t_k)$, then $\mathcal{A}(F) = \psi(P)(\mathcal{A}(t_1), \ldots, \mathcal{A}(t_k))$.
   - $\mathcal{A}(\forall x G) = \begin{cases} 1 & \mathcal{A}_{[x \to u]}(G) = 1 \text{ for all } u \in U \\ 0 & \text{otherwise .} \end{cases}$
   - $\mathcal{A}(\exists x G) = \begin{cases} 1 & \mathcal{A}_{[x \to u]}(G) = 1 \text{ for some } u \in U \\ 0 & \text{otherwise .} \end{cases}$

L6.7: For any formulas F, G, H, where x does not occur free in H, we have

1. $\neg(\forall x F) \equiv \exists x \neg F$;
2. $\neg(\exists x F) \equiv \forall x \neg F$;
3. $(\forall x F) \wedge (\forall x G) \equiv \forall x (F \wedge G)$;
4. $(\exists x F) \vee (\exists x G) \equiv \exists x (F \vee G)$;
5. $\forall x \forall y F \equiv \forall y \forall x F$;
6. $\exists x \exists y F \equiv \exists y \exists x F$;
7. $(\forall x F) \wedge H \equiv \forall x (F \wedge H)$;
8. $(\forall x F) \vee H \equiv \forall x (F \vee H)$;
9. $(\exists x F) \wedge H \equiv \exists x (F \wedge H)$;
10. $(\exists x F) \vee H \equiv \exists x (F \vee H)$.

L6.8: If one replaces a sub-formula G of a formula F by an equivalent (to G) formula H, then the resulting formula is equivalent to F.

L6.9: For a formula G in which y does not occur, we have:

1. $\forall x G \equiv \forall y G[x/y]$,
2. $\exists x G \equiv \exists y G[x/y]$.

D6.37: A formula in which no variable occurs both as a bound and as a free variable and in which all variables appearing after the quantifies are distinct is said to be in *rectified* form.

D6.38: A formula of the form $Q_1 x_1 \cdots Q_n x_n G$, where Q_i are arbitrary quantifiers and G is a formula free of quantifiers is said to be in *prenex form*.

T6.10: For every formula there is an equivalent formula in prenex form.

L6.11: For any formula F and any term t we have $\forall x F \models F[x/t]$.

T6.12: $\neg \exists x \forall y (P(y, x) \leftrightarrow \neg P(y, y))$.

Lookup

Factorizations

$2023 = 7 \cdot 17^2 \quad 2024 = 2^3 \cdot 11 \cdot 23 \quad 2025 = 3^4 \cdot 5^2$

Small primes

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997, 1009, 1013, 1019, 1021, 1031, 1033, 1039, 1049, 1051, 1061, 1063, 1069, 1087, 1091, 1093, 1097, 1103, 1109, 1117, 1123, 1129, 1151, 1153, 1163, 1171, 1181, 1187, 1193, 1201, 1213, 1217, 1223, 1229, 1231, 1237, 1249, 1259, 1277, 1279, 1283, 1289, 1291, 1297, 1301, 1303, 1307, 1319, 1321

Small groups

$\lvert G \rvert$	abelian	non-abelian
1	Z_1	
2	Z_2	
3	Z_3	
4	Z_4, Z_2^2	
5	Z_5	
6	Z_6	D_6
7	Z_7	
8	$Z_8, Z_4 \times Z_2, Z_2^3$	D_8, Q_8
9	Z_9, Z_3^2	
10	Z_{10}	D_{10}

Euler function

x	φ	x	φ	x	φ	x	φ
1	1	21	12	41	40	61	60
2	1	22	10	42	12	62	30
3	2	23	22	43	42	63	36
4	2	24	8	44	20	64	32
5	4	25	20	45	24	65	48
6	2	26	12	46	22	66	20
7	6	27	18	47	46	67	66
8	4	28	12	48	16	68	32
9	6	29	28	49	42	69	44
10	4	30	8	50	20	70	24
11	10	31	30	51	32	71	70
12	4	32	16	52	24	72	24
13	12	33	20	53	52	73	72
14	6	34	16	54	18	74	36
15	8	35	24	55	40	75	40
16	8	36	12	56	24	76	36
17	16	37	36	57	36	77	60
18	6	38	18	58	28	78	24
19	18	39	24	59	58	79	78
20	8	40	16	60	16	80	32

Appendix

Notation

R: The word *iff* stands for "if and only if".

D: Let $n \in \mathbb{Z}^+$. Then $[n] := \{1, \ldots, n\}$.

Symbols

A	Algorithm
C	Corollary
D	Definition
E	Example
F	Fact
L	Lemma
O	Observation
P	Proposition
R	Remark
T	Theorem