

1 Operators

$$a|b :\Leftrightarrow \exists c \, b = ac \text{ for } a \neq 0$$
$$a \equiv_m b :\Leftrightarrow m|(a - b) \text{ i.e. } \exists r \in \mathbb{Z} \, a = b + rm$$

2 Propositions

Implication:	$A \rightarrow B :\Leftrightarrow \neg A \vee B$
Two-sided Implication:	$A \leftrightarrow B :\Leftrightarrow A \equiv B$
Associativity:	$(F \wedge G) \wedge H \equiv F \wedge (G \wedge H)$
Distributive Law:	$(A \wedge B) \vee C \equiv (A \vee C) \wedge (B \vee C)$ $(A \vee B) \wedge (C \vee D) \equiv (A \wedge C) \vee (A \wedge D) \vee (B \wedge C) \vee (B \wedge D)$
Idempotence:	$F \wedge F \equiv F$
Absorption:	$F \wedge (F \vee G) \equiv F$
de Morgan's Law:	$\neg(A \wedge B) \equiv (\neg A \vee \neg B)$

3 Proofs

To prove a sentence (either true or false) means to show that it's a tautology. The following **proof patterns** may be used.

3.0.1 Direct Proof of an Implication

Example: $F \rightarrow G$

A **direct proof of an implication** works by assuming F and then deriving G from F .

$$F \Rightarrow \dots \Rightarrow \dots \Rightarrow \dots \Rightarrow G$$

3.0.2 Indirect Proof of an Implication

Example: $F \rightarrow G$

An **indirect proof of an implication** proceeds by assuming $\neg G$ and deriving $\neg F$ under this assumption.

$$\neg G \Rightarrow \dots \Rightarrow \dots \Rightarrow \dots \Rightarrow \neg F$$

3.0.3 Composition of Implications

Example: $F \rightarrow G$ and $G \rightarrow H$

1. Prove the statement F
2. Prove the implications $F \Rightarrow G$ and $G \Rightarrow H$

3.0.4 Case Distinction

1. Define a complete list of cases
2. Prove the statement for each case separately

3.0.5 Proof by Contradiction

Assume that the sentence F is false and derive a false statement from it.

$$\neg F \Rightarrow \dots \Rightarrow \dots \Rightarrow \dots \Rightarrow \perp$$

3.0.6 Existence Proof

Example: $\exists x P(x)$

Either find a variable which satisfies the sentence (**constructive**) or proof the existence of such a variable without exhibiting it (**non-constructive**).

3.0.7 Proof by Counterexample

Example: $\neg \forall x P(x)$

Find a variable such that the sentence is wrong.

3.0.8 Proof by Induction

Example: $\forall n P(n)$

1. **Basis step:** Prove $P(0)$
2. Assume $P(n)$
3. **Induction step:** Prove $P(n+1)$

4 Predicate Logic

4.1 Rules

1. $\forall x P(x) \wedge \forall x Q(x) \Leftrightarrow \forall x (P(x) \wedge Q(x))$
2. $\exists x (P(x) \wedge Q(x)) \Rightarrow \exists x P(x) \wedge \exists x Q(x)$
3. $\neg \forall x P(x) \Leftrightarrow \exists x \neg P(x)$
4. $\neg \exists x P(x) \Leftrightarrow \forall x \neg P(x)$
5. $\exists y \forall x P(x, y) \Rightarrow \forall x \exists y P(x, y)$
6. $\forall x (\exists x P(x) \wedge P(x)) \vee P(\underline{x})$, where \underline{x} is free

5 Sets

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

$$A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$$

$$P(A) := \{S \mid S \subseteq A\}$$

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

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}, |A \times B| = |A| * |B|$$

$$\mathcal{P}(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}(\text{teilmenge}) |\mathcal{P}| = 2^{|A|}$$

$$\text{Ordered_sets} := (a, b) := \{\{a\}, \{a, b\}\}$$

A teilmenge of a set is the set itself, every element of the set and the null element.

6 Relations

6.1 Reflexive

Formula: $a \rho a$

Set: $id \subseteq \rho$

Matrix: Diagonal is all 1

Graph: Every vertex has a loop

Examples: $\leq, \geq, |, \equiv_m$ on \mathbb{Z}

6.2 Transitive

Formula: $a \rho b \wedge b \rho c \Rightarrow a \rho c$

Set: $\rho^2 \subseteq \rho$

Examples: $\leq, \geq, |, <, >, \equiv_m$ on \mathbb{Z}

6.3 Symmetric

Formula: $a \rho b \Leftrightarrow b \rho a$

Set: $\rho = \hat{\rho}$

Matrix: Matrix is symmetric

Graph: Undirected graph, possibly with loops

Examples: \equiv_m on \mathbb{Z}

6.4 Antisymmetric

Formula: $a \rho b \wedge b \rho a \Rightarrow a = b$

Set: $\rho \cap \hat{\rho} \subseteq id$

Graph: No cycle of length 2

Examples: \leq, \geq on \mathbb{Z} and $|$ on \mathbb{N}

6.4.1 Relations as Sets

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

$a (\rho \cup \sigma) b:$ Either $a \rho b$ or $a \sigma b$

$a (\rho \cap \sigma) b:$ $a \rho b$ and $a \sigma b$

The empty set \emptyset : symmetric and transitive

6.4.2 Transitive closure

$$p^* = \cup_{n=1}^{\infty} p^n \quad (1)$$

6.4.3 Equivalence Relation

Example: =

A relation that is reflexive, symmetric, and transitive.

The set of elements in A that equivalent to $a \in A$ according to the equivalence relation θ is called the **equivalence class** of a .

$$[a]_{\theta} := \{b \in A \mid b \theta a\}$$

The set A/θ of equivalence classes of θ on A is a **partition**.

If you are looking for a equivalence relation give the matrix with the above properties.

Hint:

$$a \theta b \Rightarrow [a] = [b]$$

$$a \not\theta b \Rightarrow [a] \cap [b] = \emptyset$$

6.5 Partial Order (Ordnungsrelation)

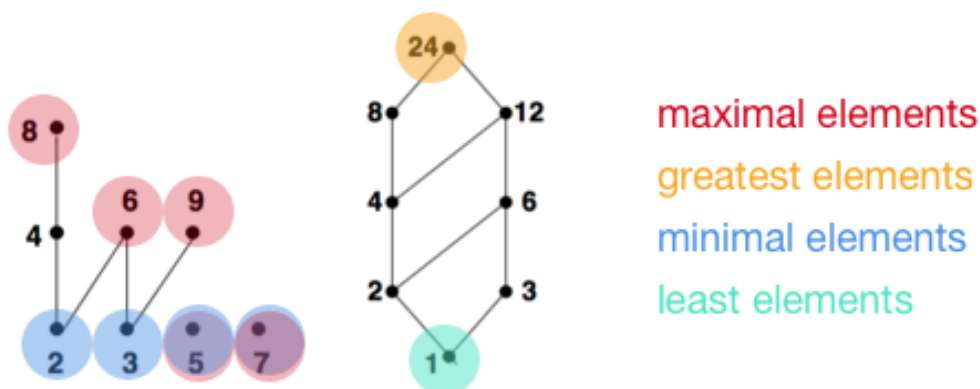
Example: \leq and \geq on \mathbb{Z}, \mathbb{Q} or \mathbb{R} , $=$ on \mathbb{N}

A relation that is reflexive, antisymmetric, and transitive.

If every two elements in a poset are comparable than the Set is **totally ordered**.

Special elements in a poset (A, \preceq) with a subset $S \subseteq A$:

minimal (maximal) element: $a \in S$ if there exists no $b \in S$ with $b \prec a$ ($b \succ a$)



Hasse Diagram of the Poset $(\{2, 3, 4, 5, 6, 7, 8, 9\}; |)$ and $(\{1, 2, 3, 4, 6, 8, 12, 24\}; |)$

least (greatest) element:

$a \in S$ if $a \leq b$ ($a \geq b$) for all $b \in S$

lower (upper) bound:

$a \in A$ if $a \leq b$ ($a \geq b$) for all $b \in S$

greatest lower (least upper) bound:

$a \in A$ if a is the greatest (least) element of the set of all lower (upper) bounds of S

6.6 Function

injective: no collisions. $\forall h_1, h_2 \in A \ h_1 \neq h_2 \Rightarrow f(h_1) \neq f(h_2)$.

surjective: every value in the codomain is taken on for some argument

bijective: one-to-one mapping (injective and surjective)

berinigter pranexform is when you write a formula with first all the quantifiers and then the formula.

7 Combinatorics

	with repetition	without repetition
ordered	n^k	$\frac{n!}{(n-k)!}$
	A passcode of length n with k different digits	How many ways can k places be awarded to n people
unordered	$\binom{n+k-1}{k}$	$\binom{n}{k} = \frac{n!}{k!(n-k)!}$
	Choose at most k scoops of ice cream from n different flavours	Select k from n objects

Hint: $\binom{n}{0} = \binom{n}{n} = 1$, $\binom{n}{1} = \binom{n}{n-1} = n$

7.1 Countability

same cardinality $A \sim B$:

There exists a bijection $A \rightarrow B$

B has at least the cardinality of A $A \preceq B$:

$A \sim C$ for some subset $C \subseteq B$

B dominates A $A \prec B$:

$A \preceq B \wedge A \not\sim B$

countable:

$A \preceq \mathbb{N}$

Hint:

The set $\{0, 1\}^* := \{0, 1, 00, 01, \dots\}$ of **finite binary sequences** is countable.

The set $\{0, 1\}^\infty$ is uncountable (Cantor's diagonalization argument).

The set A^n of **n -tuples** over A is countable.

The **union of a countable list** of countable sets is countable (can be considered as tuples).

\mathbb{N} , \mathbb{Z} und \mathbb{Q} are countable $\mathbb{P}(\mathbb{Z})$ ist überabzählbar (=not countable).

7.2 Inclusion/Exclusion Principle

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

7.3 Double counting principal

We want to count the subset of $A \times B$ (which is a relation). We can $a \in A$ the number m_a of $b \in B$ such that $(a, b) \in S$. Or the same for B (equal to the sum of ones in the matrix representation).

7.4 Pigeon hole principal

If a set of n objects is partitioned into $k < n$ sets, then at least one of these sets contains at least $\frac{n}{k}$ objects

7.5 Binomial Theorem

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

8 Graph Theory

8.1 Special Graphs

complete graph K_n	n vertices, $\frac{n(n-1)}{2}$ edges, (n) -regular (every vertex has the same degree n).
k regular graph	Each vertex has k neighbours.
complete bipartite graph $K_{m,n}$	$m + n$ vertices, mn edges, with two vertex subsets $ V_b = m$ and $ V_w = n$
tree:	undirected, connected graph with no cycles and $n - 1$ edges.
hypercube Q_d :	d -regular with 2^d vertices and $2^{d-1}d$ edges
mesh $M_{m,n}$:	mn vertices

8.2 Traversals

walk:	sequence of vertices such that consecutive vertices are connected
tour:	a walk with distinct edges
circuit:	a tour that ends where it started
Euler cycle:	a circuit that visits every node exactly once
Hamiltonian cycle:	a circuit that visits every vertex exactly once

8.3 Planar Graphs

For *connected, planar* graphs, the following equations hold:

$$r = |E| - |V| + 2 \text{ (number of regions)}$$

$$\sum_{v \in V} \deg(v) = 2|E| \text{ (sum of the degrees of the regions)}$$

if $|V| \geq 3 \Rightarrow |E| \leq 3|V| - 6$
 if $|V| \geq 3$ and bipartite $\Rightarrow |E| \leq 2|V| - 4$
 K_n is planar if and only if $n \leq 4$

Rules to prove **non-planarity**

- deletion of edges
- deletion of singleton vertices
- merging neighboring vertices

8.4 Isomorphism

Two graphs are **isomorphic** (denoted \cong) if there exists a bijection $\pi : V \mapsto V'$ such that

$$\{u, v\} \in E \Leftrightarrow \{\pi(u), \pi(v)\} \in E'$$

Hint: Look for cycles with vertices that have a distinct number of degrees. If the graph in question doesn't contain that specific cycle, it can't be isomorph.

1. $|E| + |E^-| = 2|E|$ ist gleich der Maximalen Anzahl kanten in Graph.
2. $\frac{|v|(|v|-1)}{2}$ ist gleich der Maximalen Anzahl kanten in Graph.

8.5 Trees

A tree is an undirected connected graph with no cycles. A forest is an undirected graph with no cycles. A leaf is a vertex with degree one. A tree has $n-1$ edges.

9 Number Theory

9.1 Division

Hint: Every non-zero integer is a divisor of 0. 1 and -1 are divisors of every integer.

9.2 Greatest Common Divisor

For integers a and b (not both 0), an integer d is called a $\gcd(a, b)$ if d divides both a and b and if every common divisor of a and b divides d .

$$d|a \text{ and } d|b \text{ and } c|a \wedge c|b \Rightarrow c|d$$

$$\gcd(a, b) :\Leftrightarrow \exists u, v \text{ } ua + vb$$

9.3 Chinese Remainder Theorem

$$\text{given} \quad z \equiv_{b_1} c_1$$

$$z \equiv_{b_2} c_2$$

$$z \equiv_{b_3} c_3$$

$$\text{then} \quad z = B_1x_1c_1 + B_2x_2c_2 + B_3x_3c_3$$

$$\text{where} \quad B_i = \frac{B}{b_i} \text{ with } B = b_1b_2b_3 \text{ and } B_ix_i \equiv_{b_i} 1$$

$$\text{To find different } z \text{ to satisfy certain constraints} \quad z' = z \pm n \cdot B, \quad n \in \mathbb{N}$$

9.4 Extended Euclidean Algorithm

$$\begin{array}{ll}\text{given} & x = \gcd(888, 54) \\ \text{then} & 888 = 54(16) + 24 \\ & 54 = 24(2) + \underline{6} \\ & 24 = 6(4) + 0 \\ \text{to find } 6 = u(888) + v(54): & 6 = 54 - 24(2) \\ & = 54 + 24(-2) \\ & = 54 + (888 - 54(16))(-2) \\ & = 54 + (888 + 54(-16))(-2) \\ & = 54 + 888(-2) + 54(32) \\ & = (-2)888 + (33)54\end{array}$$

9.5 Ideal

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

For $a, b \in \mathbb{Z}$ there exists $d \in \mathbb{Z}$ such that $(a, b) = (d)$. This implies that d is the **gcd** of a and b .

9.6 Least Common Multiple

$l = \text{lcm}(a, b)$ is the common multiple of a and b which divides every common multiple of a and b .

$$a \mid l' \text{ and } b \mid l' \Rightarrow l \mid l'$$

It follows:

$$\gcd(a, b) \cdot \text{lcm}(a, b) = ab$$

9.7 Modular Arithmetic

$$\begin{aligned}R_m(a + b) &= R_m(R_m(a) + R_m(b)) \\ R_m(ab) &= R_m(R_m(a) \cdot R_m(b)) \\ R_m(a^{bc}) &= R_m(R_m(a^b)^c)\end{aligned}$$

9.8 Multiplicative Inverses

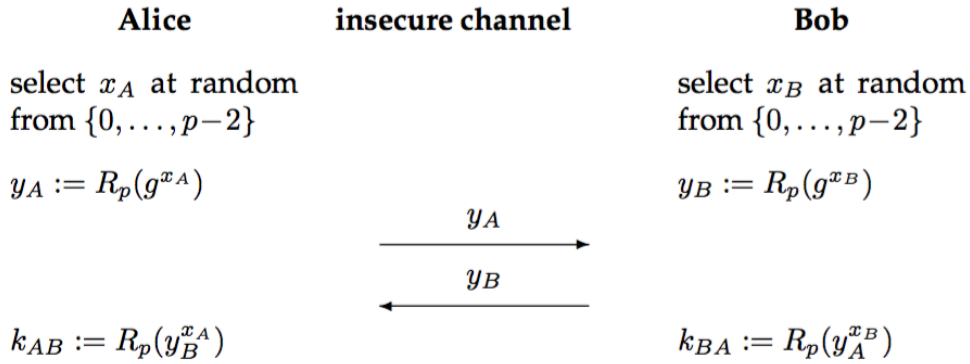
The **congruence equation** has a solution $x \in \mathbb{Z}_m$ if and only if $\gcd(a, m) = 1$. The solution is unique.

$$ax \equiv_m 1$$

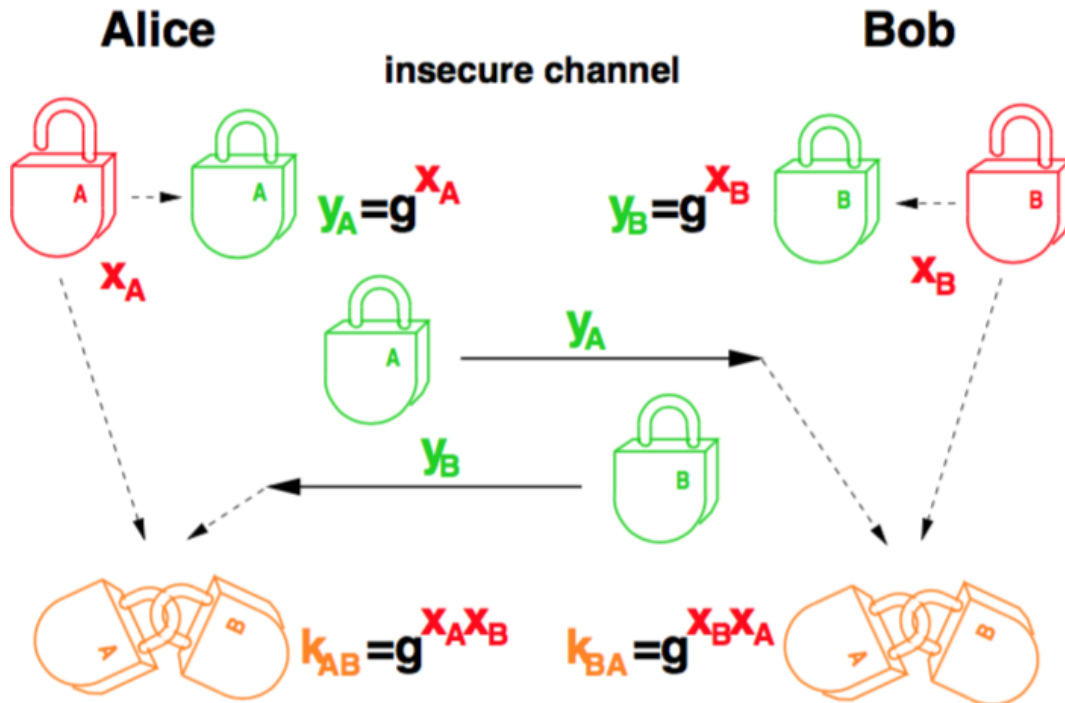
The x satisfying the equation is called the **multiplicative inverse of a modulo m** (a **Einheit of the Ring**) ($x \equiv_m a^{-1}$ or $x \equiv_m \frac{1}{a}$).

9.9 Diffie-Hellmann Key-Agreement Protocol

The Diffie-Hellmann protocol is based on the **discrete logarithm problem**. Basically, while $y = R_p(g^x)$ can be computed efficiently, it can't be solved for x .



$$k_{AB} \equiv_p y_B^{x_A} \equiv_p (g^{x_B})^{x_A} \equiv_p g^{x_A x_B} \equiv_p k_{BA}$$



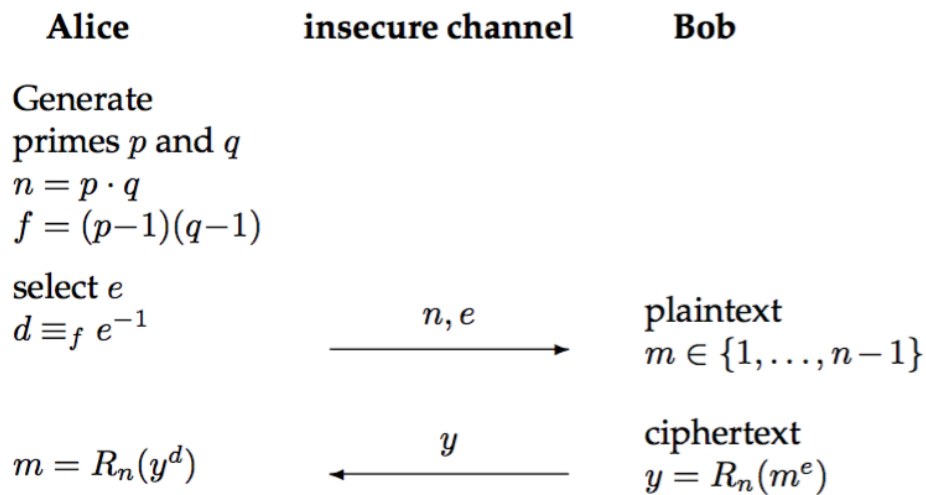
9.10 RSA

A finite group needs G needs to be chosen. Usually, the group \mathbb{Z}_n^* where $n = pq$ is the product of two secret prime numbers. Then d is equal to

$$d \equiv_{|G|} e^{-1} \equiv_{(p-1)(q-1)} e^{-1}$$

where d is the **private key** and the tuple (n, e) is the **public key**.

Hint: It's not possible to calculate d without knowing G 's order.



10 Algebra

10.1 Special Properties

Some special properties of an algebra $\langle S; *, e \rangle$ are

neutral element:	$e \in S$ such that $e * a = a * e = a$
associativity:	$*$ is associative if $a * (b * c) = (a * b) * c$ for all $a, b, c \in S$
inverse element:	b is the inverse of a if $b * a = a * b = e$
commutative/abelian:	$a * b = b * a$ for all $a, b \in S$

The **neutral** and **inverse element** can have a left and right version. E.g. $e * a = a$ is the left neutral element. However, there is *always only one* neutral/inverse element.

10.2 Special Algebras

	Notation	Axioms	Examples
Semigroup	$\langle S; * \rangle$	$*$ is associative	
Monoid	$\langle M; *, e \rangle$	$*$ is associative	
		e is the neutral element	
Group	$\langle G; *, \hat{\cdot}, e \rangle$	$*$ is associative	$\langle \mathbb{Z}; +, -, 0 \rangle,$ $\langle \mathbb{Q} - \{0\}; \cdot, ^{-1}, 1 \rangle,$ $\langle \mathbb{R}; +, -, 0 \rangle$
		e is the neutral element	
		every $a \in G$ has an inverse element	
Ring	$\langle R; +, -, 0, \cdot, 1 \rangle$	$\langle R; +, -, 0 \rangle$ is a commutative group	$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ (commutative)
		$\langle R; \cdot, 1 \rangle$ is a monoid	
		$a(b + c) = ab + ac$ and $(b + c)a = ba + ca$ for all $a, b, c \in R$	
Integral Domain (korper)		commutative	$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
		no zerodividers $ab = 0 \Rightarrow a = 0 \vee b = 0$	
Field	$GF(p) \equiv \mathbb{Z}_p$	$\langle F - \{0\}; \cdot, ^{-1}, 1 \rangle$ is a commutative ring	$\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$
		every nonzero element is a unit (has an inverse)	

Hint: In order to prove a specific algebra, prove its axioms and that the set is closed in correspondence to its operations, a ring R^* means the ring that only contains units.

10.3 Groups

10.3.1 Direct Product

The **direct product of n groups** $\langle G_1; *_1 \rangle, \dots, \langle G_n; *_n \rangle$ is the group

$$\langle G_1 \times \dots \times G_n, \star \rangle$$

where the operation \star is component-wise:

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

10.3.2 Homomorphism

A function ψ from a group $\langle G; *, \hat{\cdot}, e \rangle$ to a group $\langle H; \star, \hat{\cdot}, e' \rangle$ is a group homomorphism if, for all a and b

$$\psi(a * b) = \psi(a) \star \psi(b)$$

Furthermore, ψ is an **isomorphism** if it's a bijection.

A group homomorphism satisfies:

$$\begin{aligned} \psi(e) &= e' \\ \psi(\hat{a}) &= \widehat{\psi(a)} \end{aligned}$$

10.4 Subgroup

A subset $H \subseteq G$ of a group $\langle G; *, \hat{\cdot}, e \rangle$ is called a subgroup if $\langle H; *, \hat{\cdot}, e \rangle$ is *closed* with respect to all operations.

$$a * b \in H \text{ for all } a, b \in H$$

$$e \in H$$

$$\hat{a} \in H \text{ for all } a \in H$$

The smallest subgroup of a group G containing the element $g \in G$ is the **group generated** by g :

$$\langle g \rangle := \{g^n | n \in \mathbb{Z}\}$$

where the resulting group is called **cyclic**.

Hint: The order of a subgroup of a finite group divides its enclosing group's order i.e. $|H|$ divides $|G|$. A subgroup of size two contains e and an element a , a has to be its own inverse: $aa=e$. A subgroup with a prime order is cyclic and therefore isomorphic to \mathbb{Z}_n, \oplus and because of \oplus is also kommutativ.

10.4.1 Cyclic Group

A **cyclic group** of order n is isomorphic with $\langle \mathbb{Z}_n; \oplus \rangle$.

Hint: Every group of prime order is cyclic, and in such a group every element except the neutral element is a generator.

Hint: \mathbb{Z}_p^* is cyclic if and only if $m = 2$, $m = 4$, $m = p^e$ or $m = 2p^e$, where p is a prime and $e \geq 1$

10.4.2 Order

of a finite group: $|G|$ is the order of G

of an element of G : The order of $a \in G$ is the least $m \geq 1$ such that $a^m = e$ if such an m exists, and $ord(a) = \infty$ otherwise.

Hint: $ord(e) = 1$. If $ord(a) = 2$, then $a^{-1} = a$.

10.5 Group \mathbb{Z}_m^* and Euler's Function

$\langle \mathbb{Z}_m^*; \odot, ^{-1}, 1 \rangle$ is a group with the set

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

The **Euler function** is defined as follows:

$$\varphi(m) = |\mathbb{Z}_m^*| = (p-1)(q-1) \text{ with } n = pq$$

where p and q are prime.

Hint: If p is a prime, then $\mathbb{Z}_p^* = \{1, \dots, p-1\} = \mathbb{Z}_p - \{0\}$

Fermat, euler

$$a^{\varphi(m)} \equiv_m 1 \tag{2}$$

for every prime p and every a not divisible by p

$$a^{p-1} \equiv_p 1 \tag{3}$$

10.6 Polynomials over Fields

$R[x]$ denotes a **polynomial ring**, a set of polynomials over R .

A polynomial is called **monic**, if its first coefficient is 1.

The polynomial $a(x) \in F[x]$ is called **irreducible** if it is divisible only by constants and by constant multiples of $a(x)$. Moreover, $\alpha \in F$ is a **root** $\Leftrightarrow (x - \alpha)$ divides $a(x)$.

Hint: Every polynomial of degree 2 except $x^2 + x + 1$ is reducible. Every irreducible polynomial of degree ≥ 2 has no roots.

Example: Polynomial Division on $GF(2)$:

$$\begin{array}{r} (x^4 + x + 1) : (x^2 + x + 1) = x + 2 \\ \underline{-(x^3 + 2x)} \\ -2x^2 - 2x + 5 \\ \underline{-(2x^2 + 4)} \\ -2x + 1 \end{array}$$

Example: Polynomial Interpolation

$$\begin{array}{ll} \text{given} & a(x) \text{ with } a(3) = 2, a(4) = 6, a(5) = 7 \\ \text{then} & a(x) = 2 \frac{(x-4)(x-5)}{(3-4)(3-5)} + 6 \frac{(x-3)(x-5)}{(4-3)(4-5)} + 7 \frac{(x-3)(x-4)}{(5-3)(5-4)} \end{array}$$

10.6.1 Finite fields

There exists a finite field with q elements if and only if q is a power of a prime. The prime is called the **characteristic** of the field. Moreover, any two finite fields of the same size q are isomorphic.

10.7 Error-Correcting Codes

A **(k,n)-error-correcting code** \mathcal{C} over the alphabet \mathcal{A} with $|\mathcal{A}| = q$ is a subset of cardinality q^k of \mathcal{A}^n i.e. one element is of length n , with q^k different elements.

Hint: Usually, $\mathcal{A} = \{0, 1\}$ with $q = 2$ is being considered

The **Hamming distance** between two codewords is the number of positions at which the two codewords differ.

The **minimum distance** of an error-correcting code \mathcal{C} is the minimal Hamming distance between any two codewords.

A code \mathcal{C} with minimum distance d can correct t errors if and only if $d \geq 2t + 1$.

11 Logic

11.1 Proof System

A **proof system** is a quadruple $\Pi = (\mathcal{S}, \mathcal{P}, \tau, \phi)$ with the following components:

set of statements \mathcal{S} : every $s \in \mathcal{S}$ is either *true* or *false*
set of proofs \mathcal{P} : e.g. strings over some alphabet
truth function τ : defines the meaning (*semantics*) of objects in \mathcal{S}
verification function ϕ : $\phi(s, p) = 1$ means that p is a valid proof for the statement s

The proof system $\Pi = (\mathcal{S}, \mathcal{P}, \tau, \phi)$ is

sound if no false statement has a proof
 $\phi(s, p) = 1 \Rightarrow \tau(s) = 1$
complete if every true statement has a proof
 $\tau(s) = 1 \Rightarrow \exists p \in (\mathcal{P}) \phi(s, p) = 1$

11.2 Syntax and Semantics

	Description	Notation
Syntax	alphabet of allowed symbols and which strings are valid	
Interpretation	an assignment to all variable, predicate, function and constant symbols	$\mathcal{A}(A) = \{0, 1\}$
Semantics	a function σ assigning to each formula F and each suitable interpretation \mathcal{A} a truth value	$\sigma(F, \mathcal{A}) = \{0, 1\}, \mathcal{A}(F)$
Model	an interpretation \mathcal{A} for which F is true	$\mathcal{A} \models F$

Hint: $F \models G$ means that every model for F is also a model for G .

11.2.1 Structure

A **structure** is a tuple $\mathcal{A} = (U, \phi, \psi, \xi)$ with the following components:

universe U : nonempty set
function ϕ : assigns to each function symbol a function $U^k \mapsto U$
function ψ : assigns to each predicate symbol a function $U^k \mapsto \{0, 1\}$
function ξ : assigns to each variable symbol a value in U

11.3 Calculi

A **derivation rule** is a rule for deriving a formula from a set of formulas. G can be derived from the set $\{F_1, \dots, F_k\}$ by rule R :

$$\{F_1, \dots, F_k\} \vdash_R G$$

A **calculus K** is a finite set of derivation rules $K = \{R_1, \dots, R_m\}$. It is

sound/correct if and only if every derivation rule is correct
complete if F is a logical consequence of M , then F can be derived from M using K

11.4 Normal Forms

11.4.1 Conjunctive Normal Form (CNF)

$$F = (L_{11} \vee \dots \vee L_{1m_1}) \wedge \dots \wedge (L_{n1} \vee \dots \vee L_{nm_n})$$

11.4.2 Disjunctive Normal Form (DNF)

$$F = (L_{11} \wedge \dots \wedge L_{1m_1}) \vee \dots \vee (L_{n1} \wedge \dots \wedge L_{nm_n})$$

Hint: Every formula is equivalent to a formula in **CNF** and **DNF**.

11.5 Resolution Calculus

Given a Formula F in *CNF*, one can transform it into a set of clauses:

$$\mathcal{K}(F) = \{\{L_{11}, \dots, L_{1m_1}\}, \dots, \{L_{n1}, \dots, L_{nm_n}\}\}$$

A clause K is then a **resolvent** of clauses K_1 and K_2 if there is a literal L such that $L \in K_1$ and $\neg L \in K_2$

$$K = (K_1 - \{L\}) \cup (K_2 - \{\neg L\})$$

This derivation is denoted as follows:

$$\{K_1, K_2\} \vdash_{res} K$$

Hint: A set M of formulas is unsatisfiable if and only if $\mathcal{K}(M) \vdash_{res} \emptyset$

11.5.1 Prenex Form

In order to bring a formula into prenex form

1. Resolve all name collisions
2. Pull the quantifiers to the front by inverting them every time they surpass a \neg .