Sets and Operations

- **Set**: well-defined collection of distinct obj. without any specific order
- The set itself is an object
- Def. by listing all emelements: $S = \{a_1, \dots a_n\}$
- Def. by restricting elements to a certain property by a predicate: $S = \{x \in A \mid P(x)\}$
- **Cardinality** $|A|$: # elements in A
- **Set equality**: $A = B :\Leftrightarrow \forall x\ (x \in A \to x \in B)$
  - To proof use: $A = B \Leftrightarrow (A \subseteq B) \wedge (B \subseteq A)$
- **Ordered pair**: $(a,b) := \{a, \{a,b\}\}$
- **Subset**: $A \subseteq B \Leftrightarrow \forall x\ (x \in A \to x \in B)$
  - Is transitive: $A \subseteq B \wedge B \subseteq C \to A \subseteq C$
- **Empty Set** $\emptyset$ or $\{\}$, contains 0 elements
  - Is subset of every set: $\forall A\ (\emptyset \subseteq A)$
- **Powerset** $P(A) := \{S \mid S \subseteq A\}$; set of all subsets of A
  - $|A| = k \Leftrightarrow |P(A)| = 2^k$
- **Union**: $A \cup B := \{x \mid x \in A \vee x \in B\}$
  - $\bigcup \mathcal{A} := \{x \mid \exists A \in \mathcal{A},\ x \in A\}$
- **Intersection**: $A \cap B := \{x \mid x \in A \wedge x \in B\}$
  - $\bigcap \mathcal{A} := \{x \mid \forall A \in \mathcal{A},\ x \in A\}$
- **Complement** $\bar{A} = \{x \mid x \notin A\}$
- **Difference**: $A \setminus B := \{x \in A \mid x \notin B\}$
- **Cartesian Product**: $A \times B := \{(a,b) \mid a \in A \wedge b \in B\}$
  - $|A \times B| = |A| \cdot |B|$
  - $\times_{i=1}^{k} A_i = \{(a_1, \dots a_k) \mid a_i \in A_i\}$
- **Russel's Paradoxon**: $R = \{A \mid A \notin A\}$
  - $R \in R \Rightarrow$ by def. $R \notin R$ ↯
  - $R \notin R \Rightarrow$ by def. $R \in R$ ↯
- Properties (also valid when $\cup, \cap$ are switched)
  - $A \cap A = A$ — Impotence
  - $A \cap B = B \cap A$ — Commutativity
  - $A \cap (B \cap C) = (A \cap B) \cap C$ — associativity
  - $A \cap (A \cup B) = A$ — Absorption
  - $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ — Dist.
  - $A \subseteq B \Leftrightarrow A \cap B = A$ — Consistency

Relation

- **Relation** $(a,b) \in \rho$ or $a \rho b$ from set A to B is a subset of $A \times B$
  - $A = B \Rightarrow \rho$ relation "on A"
- Representation:
  - **Boolean Mat.** M^ρ: $|A| \times |B|$
    $M^\rho_{a,b} = 1 \Leftrightarrow a \rho b$, else 0
  - **Directed graph** with $|A| + |B|$ vertices and edge (a,b) iff $a \rho b$
- Identity Relation $id_A = \{(a,a) \mid a \in A\}$
- operations (in addition to set ops)
  - **Inverse** $\hat{\rho} := \{(b,a) \mid (a,b) \in \rho\}$
    - $a \rho b \Leftrightarrow b \hat{\rho} a,\ \forall a,b$
  - **Composition** $\rho\delta := \{(a,c) \mid \exists b \in B\ a \rho b \wedge b \delta c\}$
    - $\widehat{\rho\delta} = \hat{\delta}\hat{\rho}$
  - **Transitive Closure** $\rho^* := \bigcup \rho^n$; $a \rho^* b$ iff $\exists$ path from a to b, $a \rho^k b$ iff $\exists$ path of length k from a to b
- **Reflexive**: $\forall a\ (a \rho a)$; each vertex has a loop
- **Irreflexive**: $\forall a\ (a \not\rho a)$; no loops
- **Symmetric**: $\forall a,b\ (a \rho b \Leftrightarrow b \rho a)$; symmetric about the diagonal
- **Antisymmetric**: $\forall a,b\ (a \rho b \wedge b \rho a) \to a = b$ no cycle of length 2
- **Transitive**: $\forall a,b,c\ (a \rho b \wedge b \rho c) \to a \rho c$
  - A transitive $\Leftrightarrow \rho^2 \subseteq \rho$
- **Equivalence Relation** is reflexive, symmetric and transitive
  - Intersection of two E.R. is a E.R.
- **Equivalence Class** $[a]_\theta := \{b \in A \mid b \theta a\}$
- **Partition** of A is a set of mutually disjoint $(S_i \cap S_j = \emptyset\ \forall_{ij})$ subsets of A that cover A $(\bigcup_i S_i = A)$
- **Quotient Set** $A/\theta := \{[a]_\theta \mid a \in A\}$ of set A by E.R. θ
  - A/θ is a partition of A
- **Partially Ordered Set (poset)** is a **partial order** (relation that is reflexive, antisymmetric and transitive) and a set A: $(A; \preceq)$
  - $a,b \in$ poset are **comparable** if $a \preceq b$ or $b \preceq a$, else **incomparable**
  - If any two elements are comparable, then A is **totally ordered** by $\preceq$
  - Poset is **well-ordered** if it is totally ordered and any non-empty subset has a least element.
  - $\forall$ subset of well-ordered poset is well-ordered
- b **covers** a, $a,b \in$ poset if $a \prec b$ and $\nexists\ c$ s.t. $a \prec c$ and $c \prec b$
- **Hasse Diagram** is a directed graph where vertices are all elements of poset and $\exists$ edge (a,b) iff b covers a
- **Lexicographic order** $\preceq_{lex}$ for $(A, \preceq), (B, \sqsubseteq)$ is relation on $A \times B$ and a poset:
  $(a_1, b_1) \preceq_{lex} (a_2, b_2) :\Leftrightarrow a_1 \prec a_2 \vee (a_1 = a_2 \wedge b_1 \sqsubseteq b_2)$
  - $(A, \preceq)(B, \sqsubseteq)$ totally ordered $\Rightarrow \preceq_{lex}$ is totally ordered
- For $(A, \preceq)$ and $S \subseteq A$:
  - $a \in S$ is **minimal** (**maximal**) elem. $\in S$ if $\nexists\ b \in S,\ b \prec a$ $(b \succ a)$
  - $a \in S$ is **least** (**greatest**) elem. $\in S$ if $\forall b \in S\ a \preceq b$ $(a \succeq b)$
  - $a \in A$ is **lower** (**upper**) **bound** of S if $\forall b \in S\ a \preceq b$ $(a \succeq b)$
  - $a \in A$ is **greatest lower** (**least upper**) **bound** of S is a is greatest (least) elem. of the set of all lower (upper) bounds of S.
    - $glb(S)$: greatest lower bound
    - $lub(S)$: least upper bound
- **Meet** of a,b is greatest lower bound $(a \wedge b)$
- **Join** of a,b is least upper bound $(a \vee b)$
- **Lattice** is poset, every pair has meet & join

Functions

- **Function** $f: A \to B$ from domain A to codomain B is a relation of b with properties:
  - $\forall a \in A\ \exists b \in B\ a f b$ (totally def.)
  - $\forall a \in A\ \forall b, b' \in B\ (a f b \wedge a f b' \Rightarrow b = b')$ (well-def)
- Set of all functions $A \to B$ is B^A
- **Partial Func** is a func which is not totally-def.
- **Image**: $Im(f) = f(A) \subseteq B$
- **Preimage**: $f^{-1}(B') = \{a \in A \mid f(a) \in B'\}$, $B' \subseteq B$
- **Injective**: $a \neq b \Rightarrow f(a) \neq b\ \forall ab \in A$
- **Surjective**: $\forall b \in B\ \exists a \in A,\ b = f(a)$
- **Bijective**: injective and surjective
- **Inverse Function** f^{-1} of f exists if f is bijed.
- **Composition** of $f: A \to B$ and $g: B \to C$ is $g \circ f$ (gf), $(g \circ f)(x) := g(f(x))$
  - Is associative: $(h \circ g) \circ f = h \circ (g \circ f)$

Un-/Countable Sets

- A, B are **equinumerous** $(A \sim B)$ if $\exists$ bijection $A \to B$
  - $A \preceq B \wedge B \preceq A \Rightarrow A \sim B$
- B **dominates** A $(A \preccurlyeq B)$ if $A \sim C$ for some $C \subseteq B$
  - Rel. $\preceq$ is transitive
  - $A \subseteq B \Rightarrow A \preceq B$
- A is **countable** iff it is finite or $A \sim \mathbb{N}$
- $\{0,1\}^*$ of finite binary sequences is countable
- A and $A_i, i \in \mathbb{N}$ is countable
  - $\forall n \in \mathbb{N}\ A^n$ of n-tuples is countable
  - $\bigcup_{i \in \mathbb{N}} A_i$ is countable
  - A^* of finite sequences of A is countable
- $\{0,1\}^\infty$ semi-infinite bin. seq. is uncountable
  - Proof by cantor's diagonalization arg.

Division & Prime Factorisation

- a **divides** b $(a \mid b)$ iff $\exists c,\ b = ac$
  - a: divisor of b, b: multiple of a
    unique c (if $a \neq 0$): quotient
- $\forall a, d \neq 0 \in \mathbb{Z}\ \exists q, r \in \mathbb{Z}\ a = dq + r,\ 0 \leq r < |d|$
  - a: dividend, d: divisor, q: quotient, r: remainder $(R_d(a))$
- **greatest Common Divisor** d of any $a, b (\neq 0)$, if $d \mid a \wedge d \mid b \wedge \forall c ((c \mid a \wedge c \mid b) \to c \mid d)$
  - There are two GCD $(\pm d)$
  - $\gcd(a,b) = 1 \Leftrightarrow a, b$ are relative primes
  - $\gcd(a,b) = ua + vb\ \ \forall a,b\ \exists u,v$
  - $\gcd(m, n - qm) = \gcd(m, R_m(n)) = \gcd(m,n)$
  - $\gcd(a,b) = \prod_i p_i^{\min(e_i, f_i)}$
  - $\gcd(a,b) = ab / lcm(a,b)$
- **Ideal** generated by a, b is the set $(a,b) := \{ua + vb \mid u, v \in \mathbb{Z}\}$, $(a) := \{ua \mid u \in \mathbb{Z}\}$
  - $\forall a,b\ \exists d\ (a,b) = (d) \Rightarrow \gcd(a,b) = d$
- **Least Common Multiple** l of any a, b if $a \mid l \wedge b \mid l \wedge \forall m ((a \mid m \wedge b \mid m) \to l \mid m)$
  - $lcm(a,b) = \prod_i p_i^{\max(e_i, f_i)}$
  - $lcm(a,b) = ab / \gcd(a,b)$

Congruence & Mod Arithmetics

- **Congruence**: a congr. b mod m, $\forall abm \in \mathbb{Z}$
  $a \equiv_m b :\Leftrightarrow m \mid (a - b)$, $n \geq 1$
  - Is equivalence relation
  - $a \equiv_m b \wedge c \equiv_m d \Rightarrow a + c \equiv_m b + d \wedge ac \equiv_m bd$
  - $a_i \equiv_m b_i\ \ i \in 1 \dots k \Rightarrow f(a_1 \dots a_k) \equiv_m f(b_1 \dots b_k)$
- $\forall a, b, m \in \mathbb{Z}, m \geq 1$:
  - $a \equiv_m R_m(a)$
  - $a \equiv_m b \Leftrightarrow R_m(a) = R_m(b)$
  - $R_m(a + b) = R_m(R_m(a) + R_m(b))$
  - $R_m(ab) = R_m(R_m(a) \cdot R_m(b))$
- $R_9(a) = R_9(a_1 + \dots + a_n)$
- $R_{11}(a) = R_{11}(a_1 - a_2 + a_3 \dots a_n)$
  - a_i are digits of a, a_1 is rightmost dig.
- **Multiplicative Inverse** $x \in \mathbb{Z}_m$ is solution of $ax \equiv_m 1$ and exists iff $\gcd(a,m) = 1$
  - is unique
  - $x \equiv_m a^{-1}$
  - Find x by trying $x = 0 \dots m-1$ or extend. Euclidean algo.
- **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
- **Chinese Remainder Th.** (CRT): $m_1 \dots m_r$ are pairwise relative primes, $M = \prod_{i=1}^{r} m_i$
  $x \equiv_{m_1} a_1$, $\vdots$, $x \equiv_{m_r} a_r$ | $\forall a_1 \dots a_r,\ 0 \leq a_i < m_i,\ i \in 1..r$ has a unique sol. $0 \leq x < M$
  - Find x:
    - Calc $M_i = \frac{M}{m_i}$
    - Solve $M_i \alpha_i \equiv_{m_i} 1$
    - $x := (\sum_{i=1}^{r} a_i \alpha_i M_i) \% M$
    - $\forall n \in \mathbb{N}\ \ n \cdot M + x$ are solutions
- **Diffie-Hellman Public-Key**: Exchange a private key on an insecure channel

A	insec.	B	
x_A	p, g	x_B	$x \in \{0 \dots p-2\}$
$y_A = R_p(g^{x_A})$	$\longleftrightarrow$	$y_B = R_p(g^{x_B})$	
$k_{AB} = R_p(y_B^{x_A})$		$k_{BA} = R_p(y_A^{x_B})$	

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

- Group $\mathbb{Z}_p^*$ or any other cyclic group where computing x from y^x is hard

Algebra, Monoid & Group

- **Operation** is a function $S^n \to S$, $n \geq 0$ is the "arity"
  - $n = 0$: constant, $n = 1$: unary, $n = 2$: binary
- **Algebra** $\langle S; \Omega \rangle$, S is set and Ω is list of operations. S is the carrier of the alg.
- **(Left/Right) Neutral Elem.** $e \in S$, of algebra $\langle S; * \rangle$, $e * a = a * e = a$, $a \in S$
  - $\exists$ left and right $N.E \Rightarrow$ both are equal
- **Associative** op if $a * (b * c) = (a * b) * c$, $\forall abc$
- **Monoid** is algebra $\langle S; *, e \rangle$, $*$ is associative and e is neutral element.
- **(Left/Right) Inverse Element** $b \in S$ of a of algebra $\langle S; *, e \rangle$, $b * a = a * b = 0$
  - $\exists$ left and right I.E. $\Rightarrow$ both are equal
- **Group** $\langle G; *, \hat{\ }, e \rangle$ is algebra, where
  - G1: $*$ is associative
  - G2: e is neutral element
  - G3: $\hat{a}$ is inverse of a for all a
- **Commutative/Abelian** group or monoid $\langle G; * \rangle$ if $a * b = b * a\ \forall a, b \in G$
  - $|G| = p \in$ prime $\Rightarrow G$ is abelian
- For group $\langle G; *, \hat{\ }, e \rangle$, $\forall a, b, c \in G$:
  - $\hat{(\hat{a})} = a$
  - $\widehat{a * b} = \hat{b} * \hat{a}$
  - Left cancellation law: $a * b = a * c \Rightarrow b = c$
  - Right cancellation law: $b * a = c * a \Rightarrow b = c$
  - $a * x = b$ $(x * a = b)$ has a unique solution $\forall a, b$

Structure of Groups

- **Direct Product** of n groups $\langle G_1; *_1\rangle \dots \langle G_n, *_n\rangle$ is algebra $\langle G_1 \times \dots \times G_n; *\rangle$, $(a_1 \dots a_n) * (b_1 \dots b_n) = (a_1 *_1 b_1, \dots a_n *_n b_n)$
  - $\langle G_1 \times \dots G_n; *\rangle$ is group inv and neut. elem are component wise in the resp. groups.
- **Homomorphismus** structure preserving func. $\varphi: G \to H$ from group $\langle G; *, ^{-1}, e\rangle$ to $\langle H; \star, \tilde{}, e'\rangle$ if $\forall a,b$ $\varphi(a * b) = \varphi(a) \star \varphi(b)$

$$\begin{array}{ccc} G & \xrightarrow{*} & G \\ \downarrow \varphi & & \downarrow \varphi \\ H & \xrightarrow{\star} & H \end{array}$$

  - $\varphi(e) = e'$ and $\varphi(\hat{a}) = \widetilde{\varphi(a)}$
  - $\varphi(\hat{a}) = \widetilde{\varphi(a)}$
  - $\varphi(a^n) = \varphi(a)^n$
- **Isomorphismus** if homomorphismus ord bijective. G and H are isomorphic ($G \simeq H$)
  - inverse is isomorphism too
  - maps generators onto generators $\Rightarrow$ cyclic groups have same # generators
  - isomorphic to commutative group $\Rightarrow$ itself commutative
  - $\exists\, \varphi(n)$ isomorphisms between two cyclic groups of order $n > 0$
- $\langle \mathbb{Z}_n; +\rangle \simeq \langle \mathbb{Z}_p, +\rangle \times \langle \mathbb{Z}_q, +\rangle \Leftrightarrow n = p \cdot q$ and $\gcd(p,q) = 1$ (follows CRT)
- **Subgroup** $\langle H; *, ^{\wedge}, e\rangle$, H is a subset $H \subseteq G$ of group $\langle G; *, ^{\wedge}, e'\rangle$ if it is under all operations:
  - $a * b \in H \ \forall a,b \in H$
  - $e \in H$
  - $\hat{a} \in H \ \forall a \in H$
- $\{e\}$ and G are trivial subgroups of G

- **Order** $\mathrm{ord}(a)$, $a \in$ group G is the least $m \geq 1$ s.d. $a^m = e$. If $\nexists$ m, then $\mathrm{ord}(a) = \infty$
  - $\mathrm{ord}(e) = 1$
  - If $\mathrm{ord}(a) = 2 \Rightarrow a^{-1} = a$ is **self-inverse**
  - In a finite group G $\mathrm{ord}(a) \neq \infty \ \forall a \in G$
  - Order $|G|$ of a finite group G is # elements of G
  - Finite group G, $\forall m \in \mathbb{Z}$ $a^m = a^{R_{\mathrm{mod}(|G|)}(m)}$
  - $|G| =$ prime $\Rightarrow$ G is cyclic $\Rightarrow$ G is commutative
- For group G, and $a \in G$ the group generated by a is $\langle a\rangle := \{a^n \mid n \in \mathbb{Z}\}$
  - $\langle a\rangle$ is smallest subgroup of G containing element a
  - $\langle a\rangle = \{e, a, a^2 \dots a^{\mathrm{ord}(a)-1}\}$
- group $G = \langle a\rangle$ is called **cyclic** and a is the **generator** of it.
  - A group can have many generators
  - $\hat{a}$ is generator $\Rightarrow a^{-1}$ is generator
  - a cyclic group of $|G| = n$ is isomorphic to $\langle \mathbb{Z}_n; \oplus\rangle$ and hence abelian
  - all cyclic groups are commutative
  - All cyclic groups of same order are isomorphic.
  - $\mathbb{Z}_m \times \mathbb{Z}_n$ cyclic $\Leftrightarrow \gcd(m,n) = 1$
  - $\mathbb{Z}_p$, $p \in$ prime is cyclic
- **Lagrange**: For finite group G and subgroup H of G, the order of H divides the order of G: $|H| \mid |G|$
  - For finite group G, the order of any element divides the group order: $\mathrm{ord}(a) \mid |G| \ \forall a \in G$
  - For finite group G, $a^{|G|} = e \ \forall a \in G$
  - If $|G| =$ prime, G is cyclic and every $a \in G$ $a \neq e$ is a generator of A
- $\mathbb{Z}_m := \{0, \dots m-1\}$ is group with respect to add. mod m, but not mult. mod m, bc. not all elements have a multiplic. inv.
- $\mathbb{Z}_m^* := \{a \in \mathbb{Z}_m \mid \gcd(a,m) = 1\}$, fixed $\mathbb{Z}_m$ for mult. mod m.
  - $\langle \mathbb{Z}_m^*; \odot, ^{-1}, 1\rangle$ is a group
  - $\mathbb{Z}_m^*$ is cyclic iff $m = \{2, 4, p^e, 2p^e\}$, $p \in$ odd prime and $e \geq 1$
- **Euler Function** $\varphi: \mathbb{Z}^+ \to \mathbb{Z}^+$, $\varphi(m) := |\mathbb{Z}_m^*|$
  - $\mathbb{Z}_p^* = \{1, \dots p-1\} = \mathbb{Z}_p \setminus \{0\}$, $\varphi(p) = p - 1$ if $p \in$ prime
  - If prime factors of $m = \prod_{i=1}^{r} p_i^{e_i} \Rightarrow \varphi(m) = \prod_{i=1}^{r} (p_i - 1)\, p_i^{e_i - 1}$
- **Fermat/Euler**: $\forall a, m \geq 2$, $\gcd(a,m) = 1 \Rightarrow a^{\varphi(m)} \equiv_m 1$. $\forall p \in$ prime and $\forall a$, $b \nmid a$ $a^{p-1} \equiv_p 1$
  - Find inverse $\hat{a}$ of a if $\varphi(m)$ is known: $a\, a^{\varphi(m)-1} \equiv_m 1 \Rightarrow a^{\varphi(m)-1} = \hat{a}$

RSA

- allows secure communication over an insecure channel
- **e-th root**: For finite group G and $e \in \mathbb{Z}$, $\gcd(|G|, e) = 1$. The func. $x \mapsto x^e$ is a bijection and the e-th root $y \in G$ is $x = y^d$, d is the multiplicative inverse of e mod $|G|$, i.e. $ed \equiv_{|G|} 1$
- $|G|$ is known $\Leftrightarrow$ d can be computed from $ed \equiv_{|G|} 1$. No method is known to compute d without knowing $|G|$
- **RSA**: Possible group $\mathbb{Z}_n^*$, $n = pq$, $p,q \in$ large prime. $|\mathbb{Z}_n^*| = (p-1)(q-1)$ can only be computed if p and q are known. Public encrypted message is $m \mapsto y = R_n(m^e)$ and secret decryption is $y \mapsto m = R_n(y^d)$, d is computed as $ed \equiv_{(p-1)(q-1)} 1$

A — Insec. chan — B

- gen. $p, q \in$ prime
- $n = p \cdot q$
- $f = (p-1)(q-1)$
- Select e
- $d \equiv_f e^{-1}$
- plaintext $m = R_n(y^d)$

$\xrightarrow{n,e}$

- plaintext $m \in \{1, \dots n-1\}$
- ciphertext $y = R_n(m^e)$

$\xrightarrow{y}$

Rings and Fields

- **Ring** $\langle R; +, -, 0, \cdot, 1\rangle$ is algebra with
  - i) $\langle R; +, -, 0\rangle$ is commutative group
  - ii) $\langle R; \cdot, 1\rangle$ is monoid
  - iii) right/left dist. law: $a(b+c) = ab + ac$ and $(b+c)a = ba + ca \ \forall a\, bc \in R$
- Commutative if mult. is com.: $ab = ba$
- $\langle R; +, -, 0, \cdot, 1\rangle$, $\forall a,b \in R$:
  - $0a = a0 = 0$
  - $(-a)b = -(ab)$
  - $(-a)(-b) = ab$
  - R non-trivial $\Rightarrow 1 \neq 0$
- In non-trivial ring $\nexists$ mult. inv. for 0
- **Characteristic** of a ring is $\mathrm{ord}(1)$ if $\mathrm{ord}(1) \neq \infty$, else it is def. as 0
- **Divisibility** is also valid for commutative rings
  - $a \mid b \wedge b \mid c \Rightarrow a \mid c$
  - $a \mid b \Rightarrow a \mid bc \ \forall c$
  - $a \mid b \wedge a \mid c \Rightarrow a \mid (b+c)$
- **GCD** is also valid for commutative rings
- **Zerodivisor** $a \in$ com. ring R, $a \neq 0$ if $ab = 0 \ \forall b \neq 0 \in R$
  - a zero div. $\Leftrightarrow \gcd(a, |G|) \neq 1$
- **Unit** $v^{-1} \in$ (com) ring R if u is invertable: $uv = vv^{-1} = 1 \ \forall v \in R$
  - Set of units of R is R^*
  - For ring R, R^* is a com. group

- **Integral Domain** is a nontrivial com. ring without zerodivisors: $\forall a,b$ $(ab = 0 \Rightarrow a = 0 \vee b = 0)$
  - In Integral Dom. if $a \mid b \Rightarrow b = ac$ for unique c
- **Polynomial** $a(x) = \sum_{i=0}^{d} a_i x^i$ over ring R, $d \geq 0$, $a_i \in R$. **Degree** $\deg(a(x))$ of $a(x)$ is greatest i for which $a_i \neq 0$. Def. $\deg(0) := -\infty$. $R[x]$ is set of all possible poly. over R.
  - Can be considered as a list of coefficients
  - $\forall\, a(x) = \sum_{i=0}^{d} a_i x^i$, $b(x) = \sum_{i=0}^{e} b_i x^i$
    - $a(x) + b(x) = \sum_{i=0}^{\max(d,e)} (a_i + b_i) x^i$
    - $a(x) \cdot b(x) = \sum_{i=0}^{d+e} \left(\sum_{k=0}^{i} a_k b_{i-k}\right) x^i$
      - $\deg(a(x)b(x)) \leq \deg(a(x)) + \deg(b(x))$
        - $=$ is valid if R is int. dom.
  - $\forall$ R, $R[x]$ is a ring
  - 0 is int. dom $\Rightarrow D[x]$ is int. dom.
  - Units of $D[x]$ are constant poly. that are units of D: $D[x]^* = D^*$
- **Field** is nontrivial com. ring F, every nonzero elem. is a unit: $F^* = F \setminus \{0\}$
  - ring F is field $\Leftrightarrow \langle F \setminus \{0\}; \cdot, ^{-1}, 1\rangle$ is abelian group
  - $\mathbb{Z}_p$ is field $\Leftrightarrow p \in$ prime
    - denoted as $GF(p)$
  - We can divide in fields!
  - Field is integral domain
  - $|F| = p^n$, $p \in$ prime $\forall n \in \mathbb{N}$
  - Mult. group of $GF(p)$ is cyclic
    - has $p-1$ elem. $\varphi(p-1)$ generators

Polynomials over a Field

- $b(x) \mid a(x) \Rightarrow v\,b(x) \mid a(x) \quad \forall v \in F \neq 0$
- $a(x) = b(x) \cdot c(x) \Rightarrow a(x) = v\,b(x) \cdot (v^{-1} c(x))$
- **Monic** is poly. $a(x)$ iff leading coefficient is 1
- **Irreducible** is poly $a(x) \in F[x]$, $\deg(a(x)) \geq 1$, if it is only divisible by constant polys. and constant multiples of $a(x)$
  - $\deg(a(x)) = 1 \Leftrightarrow a(x)$ is irreducible
  - Test irreducibility by checking all polys $b(x)$, $\deg(b(x)) \leq \deg(a(x))/2$ and which are monic
  - Irreducible polys:
    - $GF(2)[x]$: $x^2 + x$
    - $GF(3)[x]$: $x^3 + x + 1$, $x^3 + x^2 + 1$
    - $GF(9)[x]$: $\exists$ three such polys
- **GCD** is also valid for monic polys
- **Divisibility** is also valid for monic polys.
  - $R_{b(x)}\, a(x)$ denots the remainder poly

Polynomials as Functions

- poly. $a(x) \in R[x]$ ring can be interpreted as a function when we def. an evaluation of $a(x)$ at $\alpha \in R$: $R \to R$, $\alpha \to a(\alpha)$
- **Root** is $\alpha \in R$, $a(\alpha) = 0$ for $a(x) \in R[x]$
  - For field F, $\alpha \in F$ is root $\Leftrightarrow x - \alpha \mid a(x)$
  - Irreducible poly $a(x)$, $\deg(a(x)) \geq 2$ has no roots
  - Poly $a(x)$, $\deg(a(x)) \in \{2, 3\}$ is irreducible $\Leftrightarrow$ has no root
- $a(x) \in F[x]$, $\deg(a(x)) = d$ is uniquely def. by any $d+1$ values of $a(x)$ (**Interpolation**)

Finite Fields

- **Congruence** is also valid for poly. over F
- Mod $m(x)$ is equivalence relation on $F[x]$ and each equiv. class has a unique representation of degree $< \deg(m(x))$
- $F[x]_{m(x)} := \{a(x) \in F[x] \mid \deg(a(x)) < \deg(m(x))\}$, $m(x) \in F$
  - $|F[x]_{m(x)}| = q^{\deg(m(x))}$, F is finite field with q elements
  - $F[x]_{m(x)}$ is a ring with add. and mult mod $m(x)$
  - $\exists\, b(x) \in F[x]_{m(x)}$, $a(x)\, b(x) \equiv_{m(x)} 1 \Leftrightarrow \gcd(a(x), m(x)) = 1$. Sol. is unique
  - $F[x]^*_{m(x)} = \{a(x) \in F[x]_{m(x)} \mid \gcd(a(x), b(x)) = 1\}$
  - Ring $F[x]_{m(x)}$ is field $\Leftrightarrow m(x)$ is irreducible
- $\mathbb{R}[x]_{x^2+1}$ is isomorphic to $\mathbb{C}$
  - more generally: $\mathbb{R}[x]_{m(x)}$ is isomorphic to $\mathbb{C}$ $\forall\, m(x)$, $\deg(m(x)) = 2$

Error-Correcting Code

- Problem: 1. Data can be erased such that one notice that data is gone
- Problem: 2. Data may change without the notice of the user
- good error correcting can handle both
- **(n,k) encoding function** E for alphabet A is injective and maps information symbols to encoded symbols (codeword). $n > k$
  $E: A^k \to A^n$: $(a_0, \dots a_{k-1}) \mapsto (c_0, \dots c_{n-1})$
  - Codeword should be little bigger but not too large.
  - $C = \mathrm{Im}(E)$ often
- (n,k) error correcting code of alphabet A, $|A| = q$ is a subset of A^n with cardinality q^k
- alphabet is often $A = \{0,1\}$
- **Hamming distance** of two strings of equal length over finite alphabet A is # of positions at which to strings are different

- **Minimum distance** of an error-correcting code C is the minimum of the Hamming distance between any two codewords.
- **Decoding function** D for an (n,k)-encoded function is $D: A^n \to A^k$
  - Is t-error correcting for encoding func. E if $D((r_0, \dots r_{n-1})) = (a_0, \dots a_{k-1})$ for any $(a_0, \dots a_{k-1})$ and $(r_0, \dots r_{n-1})$ with Hamming distance at most t. Code C is t-error correcting if $\exists E$ and C with $C = \mathrm{Im}(E)$ where D is t-error correcting
- Code C with minimum distance d is t-error correcting $\Leftrightarrow d \geq 2t+1$
- $A = GF(q)$ and $\alpha_0, \dots \alpha_{n-1} \in A$. Encoding func $E((a_0, \dots a_{k-1})) = (a(\alpha_0), \dots a(\alpha_{n-1}))$, $a(x) = \sum_{i=0}^{k-1} a_i x^i$. This code has minimum distance $n-k+1$.

Logic Introduction

- Logic is framework for expressing math. statements and verifying proofs.
  - Tool for automatically gen. proofs.

Proof System

- **Proof System** $\pi = (S, P, T, \phi)$
  - **Statements** $S \subseteq \Sigma^*$ set of syntactic representation of math. statements
  - **Proofs** $P \subseteq \Sigma^*$ set of syntactic representations of proof strings.
  - **Truth func.** $T: S \to \{0,1\}$ assigns each statement $s \in S$ its truth value $T(s)$. Defines the symantics of $s \in S$.
  - **Verification Func** $\phi: S \times P \to \{0,1\}$ verifies if a proof $p \in P$ is a valid proof for statement $s \in S$: $\phi(s,p) = 1 \Leftrightarrow p$ is a valid proof for statement s.
  - We assume: $S = P = \{0,1\}^*$
- **Sound** is a proof system if no false statement has a proof: $\forall s \in S\ \exists p \in P$ s.t. $\phi(s,p) = 1 \Rightarrow T(s) = 1$
- **Complete** is a proof system if every true statement has a proof: $\forall s \in S\ T(s) = 1 \Rightarrow \exists p \in P\ \phi(s,p) = 1$
- Proof verification must be efficient, proof generation generally not
- Proof System is always restricted to a certain type of math. statement

Elementary General Concepts

- Try to create a proof system which can capture a large number of math. statements. It is never possible to capture all.
- **Derivation** is a step in a proof starting at some $s \in S$ formula.
- **Logic** is defined by syntax and semantics
- **Syntax** defines an alphabet Λ of allowed symbols and specifies which strings in Λ^* are formulas (syntactically correct)
- **Semantics** defines a func. which assigns to each formula $F = (f_1 \dots f_k) \in \Lambda^*$ a subset $I \subseteq \{1, \dots k\}$ of indices. If $i \in I$ then symbol f_i occures **free** in F.
- Symbols may occure free and non-free at the same time at different places.
- Free Symbols denote variables which need to be fixed
- **Interpretation** is a func. which assigns a certain set of symbols of Λ concrete values where each symbol has a certain domain
- **Universe** $\mathcal{U}$ defines the domain. Domains may be subsets of $\mathcal{U}$
- Interpretation is **suitable** for formula F if it assigns a value to all free symbols of F.
- **Semantic** defines a func. $\sigma(F, A) \in \{0,1\}$ assigning each formula and suitable interpretation A a truth-value.
  - Write $A(F)$ instead of $\sigma(F, A)$
- A **model** for F is a suitable interpretation A for which formula F is true ($A(F) = 1$); $A \models F$. For a set of formulas $\mathcal{M}$, a suitable interpretation for which all formulas of $\mathcal{M}$ are true is a model of $\mathcal{M}$: $A \models \mathcal{M}$. If A is not a model: $A \not\models \mathcal{M}$
- F ($/\mathcal{M}$) is **satisfiable** if there exists a model for F ($/\mathcal{M}$) and **unsatisfiable** otherwise ($\perp$)
- F is a **tautology/valid** if F is true for any suitable interpretation ($\top$)
  - $\models F$
- G is a **logical consequence** of F ($/\mathcal{M}$) if every interpretation suitable for F ($/\mathcal{M}$) and G, which is a model for F ($/\mathcal{M}$) is a model for G: $F \models G$ ($\mathcal{M} \models G$)
- F and G are **equivalent** ($F \equiv G$) if every interpretation suitable for both yields the same truth value.
  - $F \equiv G :\Leftrightarrow F \models G$ and $G \models F$
- Set of formula $\mathcal{M}$ may be interpreted as a conjunctive of all formulas since a interpretation for $\mathcal{M}$ must be a model for all formulas of $\mathcal{M}$.
- If F and G are formulas, then so are $\neg F$, $(F \wedge G)$ and $(F \vee G)$ (recursive def.)
- **Conjunction**: $(F \wedge G)$
- **Disjunction**: $(F \vee G)$
- Unneeded parentheses can be dropped
- Def. 6.16: For formula F, G and suitable interpretation A
  - $A((F \wedge G)) = 1 \Leftrightarrow A(F) = 1$ and $A(G) = 1$
  - $A((F \vee G)) = 1 \Leftrightarrow A(F) = 1$ or $A(G) = 1$
  - $A(\neg F) = 1 \Leftrightarrow A(F) = 0$
- For formula F, G, H:
  - $F \wedge F \equiv F \quad | \quad F \vee F \equiv F$
  - $F \wedge G \equiv G \wedge F \quad | \quad F \vee G \equiv G \vee F$
  - $(F \wedge G) \wedge H \equiv F \wedge (G \wedge H)$
    - $(F \vee G) \vee H \equiv F \vee (G \vee H)$
  - $F \wedge (F \vee G) \equiv F \quad | \quad F \vee (F \wedge G) \equiv F$
  - $F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$
    - $F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$
  - $\neg\neg F \equiv F$
  - $\neg(F \wedge G) \equiv \neg F \vee \neg G \quad | \quad \neg(F \vee G) \equiv \neg F \wedge \neg G$
  - $F \vee \top \equiv \top \quad | \quad F \wedge \top \equiv F$
  - $F \vee \perp \equiv F \quad | \quad F \wedge \perp \equiv \perp$
  - $F \vee \neg F \equiv \top \quad | \quad F \wedge \neg F \equiv \perp$
- F is taut. $\Leftrightarrow \neg$ is unsatisfiable
- F is unsatisf. $\Leftrightarrow \models (F \to \perp)$
- Equivalent statements
  - $\{F_1 \dots F_k\} \models G$
  - $(F_1 \wedge \dots \wedge F_k) \to G$ is tautology
  - $\{F_1 \dots F_k, \neg G\}$ is unsatisfiable
- **Theorem**: formula F, for which $T \models F$, T is a set of axioms

Logical Calculi

- **Calculus** is set of rules
  - There are many different ones
  - Always a trade-off between simplicity and versatility.
- **Hilbert-style calculi**: Syntactic objects that are manipulated are formulas
- **Derivation Rule**: rule for deriving a formula from a set of formulas: $\{F_1 \dots F_k\} \vdash_R G$: G can be derived from the set $\{F_1 \dots F_k\}$ by rule R
  - Derivation rules involves place-holders for formulas

  1) Select subset $\mathcal{M}' \subseteq \mathcal{M}$
  2) Replace placeholders of R by formulas of $\mathcal{M}'$ and derive G
  3) add G to the set $\mathcal{M}$
- A **Calculus** $\mathcal{K}$ is a finite set of derivation rules $\mathcal{K} = \{R_1 \dots R_m\}$
- A **derivation** of formula G from set $\mathcal{M}$ of formulas in a calculus $\mathcal{K}$ is a finite sequence of applications of rules in $\mathcal{K}$, leading to G. If there is a derivation of G from $\mathcal{M}$ in calculus $\mathcal{K}$, we write $\mathcal{M} \vdash_{\mathcal{K}} G$
- A derivation rule R is **correct** if for every set $\mathcal{M}$ of formulas and every formula F, $\mathcal{M} \vdash_R F \Rightarrow \mathcal{M} \models F$
- A calculus $\mathcal{K}$ is **sound/correct** if for every set $\mathcal{M}$ of formulas and every formula F, $\mathcal{M} \vdash_{\mathcal{K}} F \Rightarrow \mathcal{M} \models F$
- A calculus is **complete** if for every $\mathcal{M}$ and F, $\mathcal{M} \models F \Rightarrow \mathcal{M} \vdash_{\mathcal{K}} F$
- Calculus is sound and complete: $\mathcal{M} \vdash_{\mathcal{K}} F \Leftrightarrow \mathcal{M} \models F$
- $F \vdash_{\mathcal{K}} G$ for sound $\mathcal{K} \Rightarrow \models (F \to G)$
- $\{F_1 \dots F_k\} \vdash G \Rightarrow \models ((F_1 \wedge \dots \wedge F_k) \to G)$
- Logic Calculy does not completely constitute a proof system since the syntax does not include a way to express how placeholders are instantiated.

Propositional Logic

- **Syntax**: An **atomic formula** is of the form A_i, $i \in \mathbb{N}$.
  A formula is defined recursively:
  - An atomic formula is a formula
  - F, G are formulas $\Rightarrow \neg F, (F \wedge G), (F \vee G)$ are formulas
  - Corresponds to a tree with atomic formulas as leaves and operators as nodes.
- **Semantics**: **Truth assignment** $\alpha: Z \to \{0,1\}$ assigns truth values to set Z of atomic formulas. α is suitable if it assigns truth values to all atomic formulas appearing in Z. The semantics is defined as $A(A_i) = \alpha(A_i)$ and def. 6.16.
  - Truth assignment is usually denoted as A instead of α
- **Literal** is an atomic formula or its negation
- Formula F is in **Conjunctive Normal Form (CNF)** if it is a conjunction of disjunctive literals: $F = (L_{11} \vee \dots \vee L_{1m_1}) \wedge \dots \wedge (L_{n1} \vee \dots L_{nm_n})$
  - Every row evaluating to 1 in the truth table, take disjunction of A_i if $A_i = 1$, otherwise $\neg A_i$. Conjunction of all these disjunctions is CNF
- Formula F is in **Disjunctive Normal Form (DNF)** if it is a disjunction of conjunction literals: $F = (L_{11} \wedge \dots \wedge L_{1m}) \vee \dots \vee (L_{n1} \wedge \dots L_{nm_n})$
  - Every row evaluating to 0 in the truth table, take disjunction of A_i if $A_i = 0$, otherwise $\neg A_i$. Disjunction of all these conjunctions is DNF
- $\exists$ a DNF and CNF for every F
- F in DNF $\Leftrightarrow \neg F$ in CNF
- gen. CNF/DNF by rearranging F using basic equivalence of prop. logic
- **Resolution** is a calculus where sets of clauses are used as syntactic objects.
  - $F \in \mathcal{M}$ must be in CNF
  - We may prove:
    - $\mathcal{M}$ is unsatisfiable
    - F is tautology ($\neg F$ is unsatisfiable)
    - $\mathcal{M} \models F$ ($\mathcal{M} \cup \{\neg F\}$ is unsatisf.)
    - F is valid ($\neg F$ is unsatisfiable)
- **Clause**: Set of literals
- Set of clauses $\mathcal{K}(F) = \{\{L_{11} \dots L_{1m_1}\}, \dots, \{L_{n1} \dots L_{nm_n}\}\}$ of F in CNF. The set of clauses of $\mathcal{M} = \{F_1, \dots F_k\}$ is the union $\mathcal{K}(\mathcal{M}) := \bigcup_{i=1}^{k} \mathcal{K}(F_i)$
- $\mathcal{K}(F)$ is only satisfied if it contains some literals evaluating to true. $\mathcal{K}(\mathcal{M})$ is only satisfied if every clause is satisfied.
- $\mathcal{M} = \{F_1 \dots F_k\}$ is satisfied iff $\bigwedge_{i=1}^{k} F_i$ is satisfied
- Empty clause $\emptyset$ corresponds to an unsatisfiable formula and the empty clause set to a tautology
- Clause K is a **resolvent** of clause K_1 and K_2 if there exists clause L, $L \in K_1$ and $\neg L \in K_2$ and $K = (K_1 \setminus \{L\}) \cup (K_2 \setminus \{\neg L\})$
- **Resolution Step**, takes $K_1 \in \mathcal{K}$ and $K_2 \in \mathcal{K}$, computes resolvent K and adds K to $\mathcal{K}$. We may write $\{K_1, K_2\} \vdash_{res} K$, where $R_{res} = \{res\}$ is one single rule: $\mathcal{K} \vdash_{R_{res}} K$
- Resolution calculus is sound: $\mathcal{K} \vdash_{res} K \Rightarrow \mathcal{K} \models K$
- Set $\mathcal{M}$ of formulas is unsatisfiable iff $\mathcal{K}(\mathcal{M}) \vdash_{res} \emptyset$

Predicate Logic

- Extension of propositional Logic
- Syntax
  - Variable Symbol: of form x_i, $i \in \mathbb{N}$
  - Function Symbol: of form $f_i^{(k)}$, $i,k \in \mathbb{N}$
  - Predicate Symbol: of form $P_i^{(k)}$, $i,k \in \mathbb{N}$
  - Term: def. inductively: variable is a term and if $t_1 \dots t_k$ are terms, then $f_i^{(k)}(t_1 \dots t_k)$ are terms
  - Formula: def. inductively:
    - $\forall i,k$ if $t_1 \dots t_k$ are terms, then $P_i^{(k)}(t_1 \dots t_k)$ is a formula, called atomic formula
    - If F and G are formula, then $\neg F$, $(F \wedge G)$, $(F \vee G)$ are formulas
    - If F is formula, then $\forall_i$, $\forall x_i F$ and $\exists x_i F$ are formulas
  - Universal quantifier: $\forall$
  - Existential quantifier: $\exists$
  - Formula correspond to trees where the leaves correspond to terms and inner nodes to operations
- Variables are either bond or free. If it occures in a (sub)formula of a quantifier, then it is bond, else it is free.
- F is closed if it contains no free vars.
- Same variable may occure free in one place and bond in another place
  - In a tree, all variables with a quantifier in the path to the root are bond
- $F[x/t]$ is the formula obtained from formula F by substituting all free vars.
- Interpretation / structure is a table $A = (U, \Phi, \Psi, S)$
  - U: non-empty set universe
  - Φ: function which assigns each function symbol a function: $\Phi(f): U^k \to U$
  - Ψ: function which assigns each predicate symbol a function: $\Psi(P): U^k \to \{0,1\}$
  - S: function which assigns each variable symbol a value in U.
  - write f^A instead of $\Phi(f)$, P^A instead of $\Psi(P)$ and x^A instead of $S(x)$ and U^A to make the interpretation clear.
- Interpretation A is suitable for formula F if it defines all function, predicate and freely occuring variable symbols.
- Semantics for an interpretation $A = (U, \Phi, \Psi, S)$
  - Value $A(t)$ for a term is def. recursively:
    - If t is a variable, then $A(t) = S(t)$
    - If t is of the form $f(t_1 \dots t_k)$, $t_i \in 1..k$ are terms and $f^{(k)}$ is a function, then $A(t) = \Phi(f) = (A(t_1) \dots A(t_k))$
  - Truth value of formula F is def. inductively by def. 6.16 and
    - If F is of the form $F = P(t_1 \dots t_k)$, $t_i \in 1..k$ are terms and $P^{(k)}$ is predicate then $A(F) = \Psi(P)(A(t_1) \dots A(t_k))$
    - If F is of the form $\forall x G$ or $\exists x G$ then let $A_{[x \to u]}$ for $u \in U$ be the same struct as A except that $S(x)$ is overwritten by u ($S(x) = u$):
      - $A(\forall x G) = \begin{cases} 1 & \text{if } A_{[x \to u]}(G) = 1 \ \forall u \in U \\ 0 & \text{else} \end{cases}$
      - $A(\exists x G) = \begin{cases} 1 & \text{if } A_{[x \to u]}(G) = 1 \ \forall u \in U \\ 0 & \text{else} \end{cases}$
  - This defines function $\sigma(F, A)$
- Equality symbol "=" is not allowed
- For all formula F, G, H, x does not occure free in x:
  - $\neg(\forall x F) \equiv \exists x \neg F$
  - $\neg(\exists x F) \equiv \forall x \neg F$
  - $(\forall x F) \wedge (\forall x G) \equiv \forall x (F \wedge G)$
  - $(\exists x F) \vee (\exists x G) \equiv \exists x (F \vee G)$
  - $\forall x, \forall y F \equiv \forall y, \forall x F$
  - $\exists x \exists y F \equiv \exists y \exists x F$
  - $(\forall x F) \wedge H \equiv \forall x (F \wedge H)$
  - $(\forall x F) \vee H \equiv \forall x (F \vee H)$
  - $(\exists x F) \wedge H \equiv \exists x (F \wedge H)$
  - $(\exists x F) \vee H \equiv \exists x (F \vee H)$
- Replacing a sub-formula G of a formula F with an equivalent formula H, it remains equivalent to F.
- Bound Substitution: Names of bond variables do not carry any semantical meaning, we may replace them. For G where y does not occure:
  - $\forall x G \equiv \forall y G[x/y]$
  - $\exists x G \equiv \exists y G[x/y]$
- Rectified Form is a formula where no variable occures as free and as bond. Every formula can be transformed into this form.
- Universal elimination: For any formula F and any term t one can derive from formula $\forall x F$ the formula $F[x/t]$: $\forall x F \models F[x/t]$
- Prenex Form: is a formula of the form $Q_1 x_1 Q_2 x_2 \dots Q_n x_n$, Q_i are quantifier and G is a formula free of quantifiers
  - $\exists$ Prenex form for all formulas
  - Transform formula into rectified form and then into prenex form
- $\neg \exists x \forall y (P(y,x) \leftrightarrow \neg P(y,y))$ is true for any suitable interpretation

Mathematical Statements

- Mathematical statement, assertion, claim, proposition is either true or false
- True proposition is:
  - Theorem: great importance
  - Lemma: intermediate result
  - Corrolary: consequence of theorem/lemma
- Conjecture is a proposition which is not known to be true or false

Introduction to Logic

- Implication: $A \to B$: $\neg A \vee B$
- Two-sided implication: $A \leftrightarrow B$: $(A \to B) \wedge (B \to A)$: $(A \wedge B) \vee (\neg A \wedge \neg B)$
- Logical consequence: $F \models G$, always when formula F is true, G is true

Proof Patterns

- Composition of Implication
  - $(A \to B) \wedge (B \to C) \models A \to C$
- Direct proof of an implication
  - $A \to B$
- Indirect proof of an implication
  - $\neg B \to \neg A \equiv A \to B$
- Modus Ponens: 1. find a suitable statement R. 2. Prove R. 3. Prove $R \Rightarrow S$
  - $A \wedge (A \to B) \models B$
- Case Distinction: 1. find list of math. statements $R_1 \dots R_k$. 2. Prove that one case R_i must be true. 3. Prove $R_i \Rightarrow S$, $i = 1 \dots k$
  - $(A_1 \vee \dots \vee A_k) \wedge (A_1 \to B) \wedge \dots \wedge (A_k \to B) \models B$
- Proof by Contradiction: 1 Find a suitable math. statement T. 2: prove T is false. 3: assume S is false, prove that T is false.
  - Often provide the proofs in other direction: assume S false, show that some T, which is obviously true, is wrong under this assumption
  - $(\neg A \to B) \wedge \neg B \models A$
- Existance Proof
  - $\exists x \in U$, $P(x) = 1$
  - Constructive if $\exists x$, else non-constr.
- Existence Proof via Pigeonhole Principle: Set of n objects is distributed into $k < n$ buckets. Then there is at least one bucket containing $\lceil \frac{n}{k} \rceil$ objects.
- Proof by Counterexample: Show that a statement $S(x)$ is false by providing an $x \in U$ s.t. $S(x) = 0$.
- Proof by induction: prove statement of the form $\forall n S(n)$
  - Base Case: Show statements holds for an trivial case
  - Inductive Hypothesis: State hypothesis
  - Inductive Step: assume $S(n)$ and prove that $S(n+1)$ is true
  - $S(0) \wedge \forall n (S(n) \to S(n+1)) \models \forall n S(n)$

Some Rules e/c.

- $\forall x P(x) \wedge \forall x Q(x) \equiv \forall x (P(x) \wedge Q(x))$
- $\exists x (P(x) \wedge Q(x)) \models \exists x P(x) \wedge \exists x Q(x)$
- $\neg \forall x P(x) \equiv \exists x \neg P(x)$
- $\neg \exists x P(x) \equiv \forall x \neg P(x)$
- $\exists y \forall x P(x,y) \models \forall x \exists y P(x,y)$

- $A \setminus \emptyset = A$
- $P(\emptyset) = \{\emptyset\}$
- $|P(\emptyset)| = 1$
- $|\emptyset| = 0$
- $|\mathbb{Z}_n| - |\mathbb{Z}_n^*| - 1 = \#$ zero dividers of $\mathbb{Z}_n$
- $\gcd(f(x), g(x))$ is meet of both

- $|\mathbb{Z}_n| = n$
- $|GF(n)^*| = n-1$
- correct & not complete calculus: $K = \emptyset$
- $F \vee G \equiv \neg F \to G$
- $F \wedge G \equiv \neg(F \to \neg G)$

- Fields: $\mathbb{Z}_p$, $\mathbb{R}[x]_{x^2+2}$

- Not Fields: $\mathbb{Z}_3 \times \mathbb{Z}_3$, $\mathbb{Z}_{81}$
- $\mathbb{Z}[x]$: ring, int. domain

Potenzen

- 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024,
- 3, 9, 27, 81, 243, 729, 2187, 6561,
- 4, 16, 64, 256, 1024, 4096, 16384
- 5, 25, 125, 625, 3125, 15625, 78125
- 6, 36, 216, 1296, 7776, 46656
- 7, 49, 343, 2401, 16807, 117649
- 8, 64, 512, 4096, 32768, 262144
- 9, 81, 729, 6561, 59049, 531441,
- 11, 121, 1331, 14641, 161051
- 12, 144, 1728, 20736, 248832
- 13, 169, 2197, 28561
- 14, 196, 2744
- 15, 225, 3375

General

- $a^1 = a$
- $a^0 = 1$
- $a^{-n} = 1/a^n$
- $a^{1/n} = \sqrt[n]{a}$
- $a^m a^n = a^{m+n}$
- $a^m / a^n = a^{m-n}$
- $(a^m)^n = a^{mn}$
- $a a^n = a^{n+1}$
- $y = \lg_b x \Leftrightarrow b^y = x$
- $\lg(uv) = \lg u + \lg v$
- $\lg(u/v) = \lg u - \lg v$
- $\lg(1/v) = -\lg v$
- $\lg(u^r) = r \lg u$
- $\lg_a x = \lg_b x / \lg_b a$

- Irreducible polynoms
  - deg. 3, $\mathbb{Z}_3[x]$
    - x^3+2x^2+2x+2
    - x^3+2x^2+x+1
    - x^3+2x^2+1
    - x^3+x^2+2x+1
    - x^3+x^2+x+2
    - x^3+x^2+2
    - x^3+2x+2
    - x^3+2x+1
  - GF(2)
    - 1: x, $x+1$
    - 2: x^2+x+1
    - 3: x^3+x^2+1, x^3+x+1
    - 4: x^4+x^3+1, $x^4+x^3+x^2+x+1$, x^4+x+1
    - 5: $x^5+x^4+x^3+x^2+1$, $x^5+x^4+x^3+x+1$
      x^5+x^3+1, $x^5+x^3+x^2+x+1$,
      x^5+x^2+1, $x^5+x^4+x^2+x+1$

10 osel

order

- Proof $\forall A,\ A = \bigcup P(A)$
  - $A \subseteq \bigcup P(A)$
    - Let $x \in A$
      $\Rightarrow \exists S \subseteq A \wedge x \in S$
      $\Rightarrow S \in P(A) \wedge x \in S$
      $\Rightarrow x \in \bigcup P(A)$
  - $\bigcup P(A) \subseteq A$
    - Let $x \in \bigcup P(A)$
      $\Rightarrow \exists S \in P(A) \wedge x \in S$
      $\Rightarrow S \subseteq A \wedge x \in S$
      $\Rightarrow x \in A$
  - $A = \bigcup P(A)$

- Cantors diagonalization argument
  - By contradiction: assum you can list all sequences (find a bijection)
  - Take the diagonal and invert all digits
  - This new number cannot be in the list ↯

- Euclidean Algorithm: $\gcd(966, 1081)$
  - $1081 / 966 = 1,\ R\ 115$
    $966 / 115 = 8,\ R\ 46$
    $115 / 46 = 2,\ R\ 23$
    $46 / 23 = 2,\ R\ 0$
    $\Rightarrow \gcd(966, 1081) = 23$

- $R_{63}(100^{1207})$
  - find $R_7(100^{1207}) = 2$
    $R_9(100^{1207}) = 1$
  - $\gcd(7,9) = 1 \Rightarrow$ crt
  - $x \equiv_9 1,\ m_1 = 7 : 9\alpha_1 \equiv_9 1$
    $x \equiv_7 2,\ m_2 = 9 : 7\alpha_2 \equiv_7 1$
  - $\alpha_1 = \alpha_2 = 4$
  - $x = R_{63}(1 \cdot 7 \cdot 4 + 2 \cdot 9 \cdot 4) = 37$

- List all elements of $GF(3)[x]^*_{x^2+2x+1}$
  - $x^2 + 2x + 1 = (x+1)(x+1)$
    $\Rightarrow (x+1)$ and $(2x+2)$ are not in the mult. group
  - $\{1, 2, x, 2x, x+2, 2x+1\}$

- Find a gen. for $GF(3)[x]^*_{x^2+2x+1}$
  - $|GF(3)[x]^*_{x^2+2x+1}| = 6$
    $\Rightarrow$ order of elements must be $\{1, 2, 3, 6\}$
    $\Rightarrow x$ is gen.

- List all elements of $GF(3)[x]_{x^2+2x+1}$
  - $\{0, 1, 2, x, 2x, x+1, x+2, 2x+1, 2x+2\}$

- $\mathrm{ord}(a \cdot b) = \mathrm{ord}(b \cdot a)$
  $\Rightarrow (a \cdot b)^n = e$
  $\Rightarrow b(a \cdot b)^n a = b \cdot a$
  $\Rightarrow b \cdot a \cdot (b \cdot a)^n = b \cdot a$
  $\Rightarrow \hat{a}\hat{b}\, b \cdot a \cdot (b \cdot a)^n = \hat{a}\hat{b}\, b a$
  $\Rightarrow (b \cdot a)^n = e$

- $2x^2 + 8 \equiv_{13} 6$ to CRT Form
  - $2x^2 \equiv_{13} 6 - 8 \equiv -2 \equiv 11 \equiv 11 + 13 \equiv 24$
  - $x^2 \equiv_{13} 24/2 \equiv 12 \equiv 12 + 13 \equiv 25$
  - $x \equiv_{13} \pm\sqrt{5} \equiv \sqrt{5} \equiv -\sqrt{5} \equiv 8$

- $\exists x\ \forall y\ F \models \forall y\ \exists x\ F$
  - assume $\exists x$, call it x', s.t. F is true for all y
    $\Rightarrow$ For all y $\exists y$, namely x', s.t. F is true.

- $F \to G \wedge G \to H$ is satis $\Rightarrow F \to H$ satis
  - false: • $F = A \vee \neg A$ $(\top)$
    • $H = A \wedge \neg A$ $(\bot)$
    $\Rightarrow F \to H$ unsatisfiable
  - Choose G s.t. $F \to G$ or $G \to H$ is satisfied: $G = A$
    • $\mathcal{A}(A) = 1$ (first)
    • $\mathcal{A}(A) = 0$ (second)

- $\forall A, B, C : (A \setminus B) \setminus C = A \setminus (B \cup C)$
  - $\subseteq$: $a \in (A \setminus B) \setminus C$
    • By def of $\setminus$: $a \in A,\ a \notin B, C$
    • $a \notin B \cup C$
  - $\supseteq$: $a \in (A \setminus B) \setminus C$
    • $a \in A,\ a \notin B \cup C$
    • $a \in A \setminus B,\ a \in (A \setminus B) \setminus C$

- ρ an δ are poset $\Rightarrow \rho \cup \delta$ poset is wrong

- ρ, δ are equiv. rel, if $\rho\delta = \delta\rho \Rightarrow \rho\delta$ is equiv rel.
  - ref. $\forall a\ (a \rho a \wedge a \delta a)$
    $\Rightarrow a \rho\delta a$
  - Sym. $(a, b) \in \rho\delta$
    $\Rightarrow (b, a) \in \widehat{\rho\delta}$
    $\Rightarrow (b, a) \in \widehat{\delta}\,\widehat{\rho}$
    $\Rightarrow (b, a) \in \hat{\rho}\,\hat{\delta}$
    $\Rightarrow (b, a) \in \rho\delta$
  - trans: Show: $\rho\delta = (\rho\delta)^2$
    $\Rightarrow (\rho\delta)^2 = (\rho\delta)(\rho\delta)$
    $\Rightarrow \rho(\rho\delta)\delta$
    $\Rightarrow \rho^2\delta^2$
    $\Rightarrow \rho\delta$

- Show $10 \mid (43^{43} - 17^{17})$
  - $43^{43} \equiv_{10} 7$
  - $17^{17} \equiv_{10} 7$
    $\Rightarrow 43^{43} - 17^{17} \equiv_{10} 7 - 7 \equiv_{10} 0$

- Find group isomorphic to $\mathbb{Z}_{18}$
  - $\langle \mathbb{Z}_2; + \rangle \times \langle \mathbb{Z}_9; + \rangle$

- Find all units of ring $\mathbb{Z}[x]$
  - $\{1, -1\}$

- Find all zero-divides of ring $\mathbb{Z}_{12}$
  - $\gcd(a, 12) \neq 1 : \{2, 3, 4, 6, 8, 9, 10\}$

- $\langle G; * \rangle$ group, $H := \{a \in G \mid \forall b \in G\ a * b = b * a\}$ is subgroup. prove
  - closed under $*$: $a, a' \in H,\ b \in G$
    $(a * a') * b = a * (b * a') = b * (a * a')$
  - closed under e: $b \in G$
    $e * b = b * e = e$
  - closed under $^{-1}$: $b \in G$
    $\hat{a} * b = (\hat{a} * b) * e = \hat{a} * (b * (a * \hat{a})) =$
    $\hat{a} * ((a * b) * \hat{a}) = ((\hat{a} * a) * b) * \hat{a} = b * a$

- Find mult. inv. of $2x + 1 \in R^*$ of
  $R := \mathbb{Z}_7[x]_{x^2+x+1}$
  $(2x + 1)p(x) \equiv_{x^2+x+1} 1$
  $\Rightarrow x^2 + x + 1 \mid (2x+1)p(x) - 1$
  $x^2 + x + 2 \mid (2x+1)p(x)$
  $x^2 + x + 2 \mid 2x + 1 = \underline{\underline{4x + 2}}$
  $-(2x^2 + 4x$
  $-3x + 2$
  $4x + 2$
  $-(4x + 2$
  0