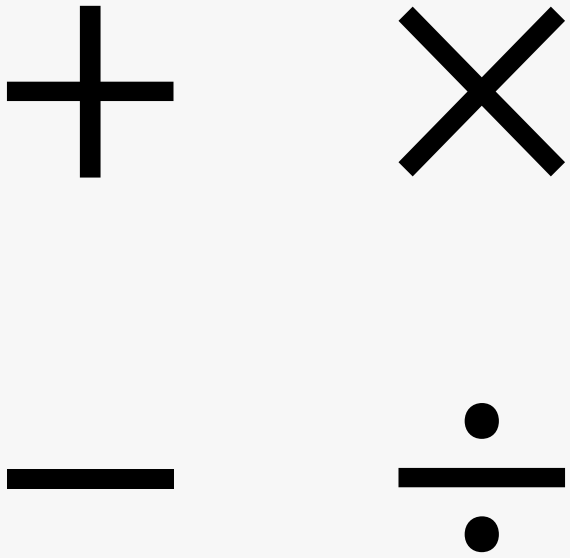


Discrete Maths

definition
theorem
lemma
corollary
example

Logic

D2.1 Mathematical statement (true or false): proposition

L 6.1

1) $F \wedge F \equiv F$, $F \vee F \equiv F$ — idempotence
2) $F \wedge G \equiv G \wedge F$, $F \vee G \equiv G \vee F$ — commutativity
3) $(F \wedge G) \wedge H \equiv F \wedge (G \wedge H)$, $(F \vee G) \vee H \equiv F \vee (G \vee H)$ — associativity
4) $F \wedge (F \vee G) \equiv F$, $F \vee (F \wedge G) \equiv F$ — absorption
5) $F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$ — distributive law 1
6) $F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$ — distributive law 2
7) $\neg\neg F \equiv F$ — double negation
8) $\neg(F \wedge G) \equiv \neg F \vee \neg G$, $\neg(F \vee G) \equiv \neg F \wedge \neg G$ — de Morgan's rules
9) $F \vee T \equiv T$, $F \wedge T \equiv F$
10) $F \vee \bot \equiv F$, $F \wedge \bot \equiv \bot$
11) $F \vee \neg F \equiv T$, $F \wedge \neg F \equiv \bot$ — tautology & unsatisfiability rules

General Concepts

D6.4 Syntax: Symbols (Λ) & constellation of them that are allowed
D6.32 Free/Bound variable: $\forall x \exists y (x \cdot y \cdot z = 1)$ x,y bound, z free
Formula is closed, if it contains no free variables.
D6.5 Semantics: defines function free(F) $\subseteq \Lambda^*$, D6.6, D6.8, ...
$i \in \text{free}(F) \Leftrightarrow i$ occurs free in F
D6.6 Interpretation $\mathcal{A}$: assigns each symbol $\lambda \in \Lambda^*$ a meaning
D6.7 Suitability of $\mathcal{A}$: $\mathcal{A}$ assigns meaning to all free var in F
D6.8 Truth function σ: $(F, \mathcal{A}) \mapsto \{0,1\}$, often $\mathcal{A}(F)$, truth value of F under $\mathcal{A}$ → is F correct with $\mathcal{A}$
D6.9 Model: If $\mathcal{A}(F)=1$, then $\mathcal{A}$ is a model for F or a set of formulas M. Notation: $\mathcal{A} \models F$, $\mathcal{A} \models M$; $\mathcal{A} \not\models F$

Satisfiability, Consequence, Equivalence

D6.10 Satisfiability: F satisfiable $\Leftrightarrow \exists \mathcal{A} \models$ | Unsatisfiable $\bot$ else.
D6.11 Tautology T: $F \equiv T \Leftrightarrow$ F is true $\forall \mathcal{A}$: $\mathcal{A}$ suitable, $\mathcal{A} \models F$
D6.12 Logical consequence: $F \models G$, if every suitable interp. of F, G that is a model for F is also a model for G (or H)
D6.13 Equivalence: $F \equiv G \overset{\text{def}}{\Leftrightarrow} F \models G$ and $G \models F$
L6.2 $F \equiv T \Leftrightarrow \neg F \equiv \bot$
L6.3 $\{F_1, \dots, F_k\} \models G \Leftrightarrow (F_1 \wedge \dots \wedge F_k) \to G$ is T
$\Leftrightarrow \{F_1, \dots, F_k, \neg G\}$ is $\bot$

Logical Operators

$\wedge$ conjunction, $\vee$ disjunction

D6.15 F, G formulas, then $\neg F$, $(F \wedge G)$ and $(F \vee G)$ formulas
D6.16 $\mathcal{A}((F \wedge G)) = 1 \Leftrightarrow \mathcal{A}(F)=1$ and $\mathcal{A}(G)=1$
$\mathcal{A}((F \vee G)) = 1 \Leftrightarrow \mathcal{A}(F)=1$ or $\mathcal{A}(G)=1$
$\mathcal{A}(\neg F) = 1 \Leftrightarrow \mathcal{A}(F)=0$

A	B	①	②
0	0	1	1
0	1	0	1
1	0	0	0
1	1	1	1

① $A \leftrightarrow B \equiv (A \to B) \wedge (B \to A)$
② $A \to B \equiv \neg A \vee B$

Logical Calculi (Hilbert-Style Calculi)

D6.17 Derivation rule: $\{F_1, \dots, F_k\} \vdash_R G$ OR $\frac{F_1\ F_2 \dots F_k}{G}$ (R) ($\{F_1, \dots, F_k\} = M$)
D6.18 Application of der. rule: - Select $N \subseteq M$ s.t. $N \vdash_R G$
- Add G to M (s.t. it can be reused)
D6.19 Calculus K: Finite set of derivation rules: $K = \{R_1, \dots, R_m\}$
D6.20 Derivation: From M in K, finite sequence of appl. of $R \in K$
D6.21 Correctness of R: $\forall F, M$ $M \vdash_R F \Rightarrow M \models F$ (logical consequence)
D6.22 Soundness: $M \vdash_K F \Rightarrow M \models F$ (F der. f. M $\Rightarrow$ F ✓ of M)
Completeness: $M \models F \Rightarrow M \vdash_K F$

Derivation rules: - All from L6.1, i.e. $\neg\neg F \vdash F, \dots$;
- Logical consequences: $F \wedge G \vdash F$; $F \wedge G \vdash G$; $\{F, G\} \vdash F \wedge G$;
$F \vdash F \vee G$; $F \vdash G \vee F$; $\{F, F \to G\} \vdash G$; $\{F \vee G, F \to H, G \to H\} \vdash H$;
- Derivation from empty set: Use tautology rules.

Propositional Logic ⇒ PS for CNF/DNF

D6.23 Syntax: Atomic Formula of form A_i; D6.15 applies
D6.24 Semantics: See D6.16
D6.25 Literal L: Atomic Formula or negation thereof
D6.26 Conjunctive Normal Form (CNF): $(L \vee L \vee \dots) \wedge (L \vee \dots) \wedge \dots$
D6.27 Disjunctive Normal Form (DNF): $(L \wedge L \wedge \dots) \vee (L \wedge \dots) \vee \dots$
T6.4 Every formula is equivalent to a CNF & DNF formula

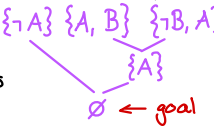
Ex. Given F calculate the truth table: (Row e.g. $(L \vee L \vee \dots)$)
CNF: Calculation can stop if found false row
DNF: Calculation can stop if found true row

Ex. Prove that the resolution calculus is not complete.
Let $F = A$ and $G = A \vee B$. We know $F \models G$. But we can't derive $\mathcal{K}(A \vee B))$ from $\mathcal{K}(A)$ using the resolution calculus

Resolution Calculus (sound, but incomplete)

Used to prove unsatisfiability & logical consequence (since $M \models F$ is true $\Leftrightarrow M \cup \{\neg F\}$ is unsatisfiable). Formulas in CNF
D6.28 Clause K: Set of literals, e.g. $\emptyset$, $\{A, B, \neg D\}$ or $(L \wedge L \wedge \dots)$
D6.29 Set of clauses: denoted $\mathcal{K}(F)$, $\mathcal{K}(M)$ union of all $\mathcal{K}(F)$
Empty clause is $\bot$, Empty set of clauses is T
D6.30 Resolvency: K resolvent of K_1 & K_2 if they contain literal $L \in K_1$, $\neg L \in K_2$ and $K = (K_1 \setminus \{L\}) \cup (K_2 \setminus \{\neg L\})$

Ex: Resolution steps have to be carried out one by one. For consistency, notation: $\{K_1, K_2\} \vdash_{res} K$; Resolution calculus notation: Res = {res}



L6.5 The resolution calculus is sound: $\mathcal{K} \vdash_{res} K \Rightarrow \mathcal{K} \models K$
T6.6 Set M unsatisfiable iff $\mathcal{K}(M) \vdash_{Res} \emptyset$
Tip: L6.3 can be very useful (last part $\bot$ → res. calc.)

Predicate Logic

D6.31 Syntax: variables $x_i : i \in \mathbb{N}$; functions $f_i^{(k)} : i, k \in \mathbb{N}$, k is # of arguments, if k=0 f constant; predicate $P_i^{(k)}$; term t_i (variables & functions); ← defined inductively
formulas: Predicates are atomic formulas, D6.15, if F is a formula, so is $\forall x F$ and $\exists x F$
D6.32 Closed formula: contains no free variables $\Leftrightarrow$ all var are bound, i.e. are in formulas of form $\forall x F$ or $\exists x F$
D6.33 Substitution: $F[x/t]$ after replacing all free x w/ term t in F
D6.34 Interpretation: aka. structure is a tuple $\mathcal{A} = (U, \phi, \psi, \xi)$.
$\mathcal{U}$ universe (non-empty); ϕ function assigning functions $f^{\mathcal{A}}$;
ψ assigns predicates $p^{\mathcal{A}}$; ξ assigns free variables
D6.35 Suitability of $\mathcal{A}$: all functions, predicates, free variables are defined ⇒ $\mathcal{A}$ is suitable
D6.36 Semantics: Value of a term is defined as $\mathcal{A}(t) = \xi(t)$ if variable, $\mathcal{A}(t) = \phi(f)(\mathcal{A}(t_1), \dots \mathcal{A}(t_k))$ if function
Truth value of a formula $\mathcal{A}(F) = \psi(p)(\mathcal{A}(t_1), \dots \mathcal{A}(t_k))$ if predicate, $\mathcal{A}(\forall x F) = \begin{cases} 1 \text{ if } \mathcal{A}_{[x \to u]}(F) = 1 \text{ for } \underline{\text{all}} \\ 0 \text{ else} \end{cases}$ ($\xi(x) = u$) $u \in \mathcal{U}$
$\mathcal{A}(\exists x F)$ some

L6.7 For any formulas F, G & H, x not 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 Replacing a subformula of F with equiv. one, F equiv. F'
L6.9 For form. G (w/o y), $\forall x \equiv \forall y\ G[x/y]$, $\exists x\ G \equiv \exists y\ G[x/y]$]
D6.37 Rectified form: Formula in which no variable is bound and free and all variables after Quantifiers are distinct
D6.38 Prenex form: All quantifiers are at the front
T6.10 There exists an equivalent formula in PF for every formula
L6.11 Any formula F, any term t, we have $\forall x F \models F[x/t]$
T6.12 $\neg\exists x \forall y (P(x,y) \leftrightarrow \neg P(x,y))$

Ex. Prove $\forall x (F \wedge G) \models (\forall x F) \wedge G$. Let F & G be any suitable formulas. Let $\mathcal{A}$ be any structure suitable for $\forall x (F \wedge G)$ and $(\forall x F) \wedge G$. Assume $\mathcal{A}(\forall x (F \wedge G)) = 1$
$\Leftrightarrow \mathcal{A}_{[x \to u]}(F \wedge G)) = 1$ for any $u \in \mathcal{U}^{\mathcal{A}}$ (sem. ∀)
$\Leftrightarrow (\mathcal{A}_{[x \to u]}(F)$ and $\mathcal{A}_{[x \to u]}(G))$ ② for any $u \in \mathcal{U}^{\mathcal{A}}$ (sem. ∧)
$\Leftrightarrow \mathcal{A}(\forall x F)$ and ① $\mathcal{A}_{[x \to u]}(G)$ for any $u \in \mathcal{U}^{\mathcal{A}}$ (sem. ∀)
split up here
Case 1: x not free in G, then we have $\mathcal{A}(G) = \mathcal{A}_{[x \to u]}(G) = 1$
Case 2: x free in G, then x free in $(\forall x F) \wedge G$. If $\mathcal{A}$ is suitable, it defines $x \in \mathcal{U}^{\mathcal{A}}$. Since ① = ②, in particular for $u = x^{\mathcal{A}}$, $\mathcal{A}_{[x \to x^{\mathcal{A}}]}(G) = 1$, so $\mathcal{A}(G) = \mathcal{A}_{[x \to x^{\mathcal{A}}]}(G) = 1$
Therefore, $\mathcal{A}(\forall x F) = 1$ and $\mathcal{A}(G) = 1 \overset{\text{sem.}\wedge}{\Leftrightarrow} \mathcal{A}((\forall x F) \wedge G) = 1$ □

Proof systems

D6.1 Proof system: a quadruple $\Pi = (S, P, \tau, \phi)$ (semantics assign, proof valid?)
- $s \in S$ statement — $\tau: S \to \{0,1\}$ truth function
- $p \in P$ proof — $\phi: S \times P \to \{0,1\}$ verification function

D6.2 Soundness: No false statement has a proof, i.e. if $\forall s \in S$ for which $\exists p \in P$ with $\phi(s,p)=1$, we have $\tau(s)=1$

D6.3 Completeness: Every true statement has a proof, i.e. if $\forall s \in S$ with $\tau(s)=1$, $\exists p \in P$ with $\phi(s,p)=1$

Proof Patterns:

D2.12 Composition of Implication: If $S \Rightarrow T$ and $T \Rightarrow U$ are both true, then $S \Rightarrow U$ is true. L2.5 $(A \to B) \wedge (B \to C) \vdash A \to C$

D2.13 Direct proof of Implication: Prove $S \Rightarrow T$ by assuming S and proving T under that assumption

D2.14 Indirect proof of $\Rightarrow$: Prove $S \Rightarrow T$ by assuming $\neg T$ and proving $\neg S$ under that assumption. L2.6 $\neg B \to \neg A \vdash A \to B$

D2.15 Modus ponens: Prove S by finding R, proving R and then proving $R \Rightarrow S$. L2.7 $A \wedge (A \to B) \vdash B$

D2.16 Case distinction: Prove S by finding a list $R_1, \dots, R_n$ (cases), proving one R_i, show $R_i \Rightarrow S$ for all R_i

D2.17 Proof by contradiction: Assume S is false, derive statements from S until we reach contradiction

D2.18 Existence proofs: Prove S is true for at least one $x \in \mathbb{N}$, if true constructive, otherwise non-constructive

D2.19 Pigeonhole principle: Set of n objects split into $k<n$ sets, at least one set contains $\lceil \frac{n}{k} \rceil$ objects.

D2.20 Proof by counterexample: Find an example where S is not true

D2.21 Proof by induction: Prove $P(0)$ (Base case), then prove for any n $P(n) \to P(n+1)$ (Induction step)
T2.11 $P(0) \wedge \forall n (P(n) \to P(n+1)) \Rightarrow \forall n\, P(n)$

To list all models of a set of formulas, all have to evaluate to true. Use truth table.

We can replace variables described with quantifiers when transforming e.g. into prenex form with any other name

---

F satisfiable, $\forall x F \equiv \bot$: $F = P(x) \wedge \neg P(y)$ Reason: x will at some point equal y, hence $P(y) \equiv \neg P(y)$ → contradiction

---

Function table approach for CNF/DNF: simply compute table, then find appropriate function

---

Complete, but not sound Calculus: $\{\} \vdash F$

Universal Instantiation: L6.11; $\forall x F \vdash F[x/t]$

$\mathcal{A}_{[x \to u]}$ is same structure as $\mathcal{A}$, but all $\xi(x)$ are replaced with u ($\xi(x)=u$). Useful to eliminate $\forall x$ and $\exists x$. See D6.36 for more details

---

Free symbols in part after $\wedge$ or $\vee$ in cases like: $\forall x (g(x)) \wedge f(x)$ — x in $f(x)$ is free

⇒ More on P.6!

Sets, relations and Functions

D3.1 Cardinality: number of elements in the set

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

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

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

L3.3 $A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$

D3.4 Union: $A \cup B \overset{\text{def}}{=} \{x \mid x \in A \vee x \in B\}$
Intersection: $A \cap B \overset{\text{def}}{=} \{x \mid x \in A \wedge x \in B\}$
(can be extended to a collection of sets)

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

T3.4 For any sets A, B, C we have

$A \cap A = A$;	$A \cup A = A$	(idempotence)
$A \cap B = B \cap A$;	$A \cup B = B \cup A$	(commutativity)
$A \cap (B \cap C) = (A \cap B) \cap C$;	$A \cup (B \cup C) = (A \cup B) \cup C$	(Associativity)
$A \cap (A \cup B) = A$;	$A \cap (A \cup B) = A$	(absorption)
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	(distributivity)
$A \subseteq B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B$		(Consistency)

D3.6 Empty set: $\emptyset$ or $\{\}$ unique; L3.6 $\forall A (A \subseteq A)$

D3.7 Power set: $\mathcal{P}(A) \overset{\text{def}}{=} \{S \mid S \subseteq A\}$, Set of all subsets of A

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

Relations: $a \rho b = (a,b) \in \rho$ $\quad |A \times B| = |A| \cdot |B|$ (fin. sets)

D3.9 Relation: ρ from A to B is a subset of $A \times B$. If $A = B$, then ρ is a relation on A

D3.10 Identity Relation: $id_A = \{(a,a), a \in A\}$
Relations can be represented by matrices.

	a	b	c
a	1	0	1
b	1	1	0
c	0	1	0

D3.11 Inverse: $\hat{\rho} \overset{\text{def}}{=} \{(b,a) \mid (a,b) \in \rho\}$ alt. $\hat{\rho} = \rho^{-1}$; $a \hat{\rho} b \Leftrightarrow b \rho a$

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

L3.7 $\rho \circ (\sigma \circ \phi) = (\rho \circ \sigma) \circ \phi$ L3.8 $\widehat{\rho \sigma} = \hat{\rho} \circ \hat{\sigma}$ (inverse)

D3.13 Reflexive: $a \rho a$ true for all $a \in A$, i.e. $id \subseteq \rho$

D3.14 Irreflexive: $a \not\rho a$ for all $a \in A$, i.e. $id \cap \rho = \emptyset$

D3.15 Symmetric: $a \rho b \Leftrightarrow b \rho a$ $\forall a,b \in A$, i.e. $\rho = \hat{\rho}$

D3.16 Antisymmetric: $a \rho b \wedge b \rho a \Rightarrow a = b$ $\forall a,b \in A$, i.e. $\rho \cap \hat{\rho} \subseteq id$

D3.17 Transitive: $a \rho b \wedge b \rho c \Rightarrow a \rho c$ $\forall a,b,c \in A$ ex: $\emptyset$

L3.9 Relation transitive $\Leftrightarrow \rho^2 \subseteq \rho$; D3.18 Trans. closure $\rho^* = \bigcup_{n \in \mathbb{N}} \rho^n$ $\rho^2 = \rho \circ \rho$

Equivalence Relations

D3.19 Equivalence relation: on set A; transitive, reflexive and symmetric

D3.20 Equivalence class: $[a]_\theta \overset{\text{def}}{=} \{b \in A \mid b \theta a\}$ for θ on A, $a \in A$

L3.10 Intersection of two equivalence relations is one

D3.21 Partition: $S_i \cap S_j = \emptyset$ for $i \neq j$ $\quad \bigcup_{i \in I} S_i = A$ for I index set

D3.22 Quotient set: Set of eq. classes, $A/\theta \overset{\text{def}}{=} \{[a]_\theta \mid a \in A\}$, A mod θ

T3.11 A/θ is a partition of A

ex: empty relation symmetric & antisymmetric

Partial order Relation

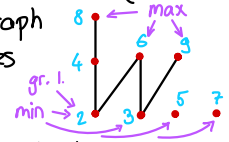
D3.23 Partial order relation: on set A, reflexive, transitive, antisymmetric. Partial order $\leq$: poset (partially ord. set)

D3.24 Comparability: If $a \leq b$ or $b \leq a$ for poset $(A; \leq)$

D3.25 Totally ordered: Any two elements of poset comparable

D3.26 Covering: b covers a if $a < b \wedge \neg \exists c (a < c \wedge c < b)$

D3.27 Hasse diagram: Directed graph of poset, vertices $v \in A$, edges (a,b) mean that a covers b
→ Lattice if single min & max



D3.28 Direct product: $(A; \leq) \times (B; \sqsubseteq) = (A \times B; \leq)$, where $\leq$ given by: $(a_1, b_1) \leq (a_2, b_2) \overset{\text{def}}{\Leftrightarrow} a_1 \leq a_2 \wedge b_1 \sqsubseteq b_2$

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

T3.13 Lexicographic order: $\leq_{lex}$ is poset, given by $(a_1, b_1) \leq_{lex} (a_2, b_2) \overset{\text{def}}{\Leftrightarrow} a_1 \leq a_2 \vee (a_1 = a_2 \wedge b_1 \sqsubseteq b_2)$

D3.29 Special elements: Let $(A; \leq)$ be poset, $S \subseteq A$

Notes p6!!

1. $a \in A$ min/max element, if $\nexists b \in A$ s.t. $b < a$ / $a < b$
2. $a \in A$ least/greatest el., if $a \leq b / b \leq a$ $\forall b \in A$ (or)
3. $a \in A$ lower/upper bound of S, if $a \leq b / b \leq a$ $\forall b \in S$
4. $a \in A$ greatest lower/least upper bound of S, if a is the greatest/least element of the set of l./u. bounds of S

D3.30 Well-ordered: Poset totally ordered & every non-empty subset of A has a least element.

D3.31 Meet: $(A; \leq)$ poset, $\{a,b\} \subseteq A$ have gr. l. bound
Join: Opposite of meet; $\{a,b\} \subseteq A$ have l.u. bound

D3.32 Lattice: Poset where every element has a meet and join — func. always have meet: $h(x) = gcd(f,g)$

Functions

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

1. $\forall a \in A \; \exists b \in B \; a f b$ — totally defined
2. $\forall a \in A \; \forall b, b' \in B \; (a f b \wedge a f b' \to b = b')$ — well-defined

D3.34 Set of functions: set of all $A \to B$ B^A

D3.35 Partial function: $A \to B$ such that 2 in D3.33 holds

D3.36 Image: $f(S) \overset{\text{def}}{=} \{f(a) \mid a \in S\}$, $S \subseteq A$, $A \to B$

D3.37 Image/range: $f(A) \subseteq B$, denoted $Im(f)$

D3.38 Preimage: $f^{-1}(T) \overset{\text{def}}{=} \{a \in A \mid f(a) \in T\}$, $T \subseteq B$

D3.39 Injective: if $a \neq b$, then $f(a) \neq f(b)$
Surjective: if $\forall b \in B \; \exists a \in A \; f(a) = b$
} both = bijective

D3.40 Inverse: f^{-1} for f bijective

For $f: A \to B$ and $g: B \to A$, f injective iff g surjective

D3.41 Composition: $(g \circ f)(a) = g(f(a))$

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

Countability

D3.42 (i) Two sets are equinumerous, $A \sim B$, if there exists a bijection $A \to B$
(ii) B dominates A, $A \preceq B$, if $A \sim C$ for $C \subseteq B$ or if there exists an injection $A \to B$
(iii) A is countable iff $A \preceq \mathbb{N}$ — $\mathbb{N}$ is countable

L3.15 (i) equiv. rel. (ii) $A \preceq B \wedge B \preceq C \Rightarrow A \preceq C$ (iii) $A \subseteq B \Rightarrow A \preceq B$
T3.16 $A \preceq B \wedge B \preceq A \Rightarrow A \sim B$
T3.17 A set is countable iff it is finite or if $A \sim \mathbb{N}$

Cantor's diagonalization argument

Define α_{ij} as the j-th digit in the i-th sequence $f(i) = \alpha_{i0}, \alpha_{i1}, \ldots$. We further define $\widehat{\alpha_{ij}} = \alpha_{ij} + 1$. Now, we take $\beta = \widehat{\alpha_{00}}\,\widehat{\alpha_{11}}\ldots$. From this definition, it is clear that β is different from all $f(i)$ by at least 1 digit.
$\Rightarrow$ proves uncountability

Countable sets

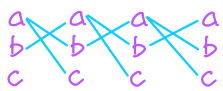
T3.17 $A \sim \mathbb{N}$ T3.18 $\{0,1\}^*$ T3.19 $\mathbb{N} \times \mathbb{N}$
C3.20 A, B countable, $A \times B$ countable C3.21 $\mathbb{Q}$
T3.22 (i) Set of n-tuples A^n countable
(ii) Union of countably many countable sets
(iii) Set A^* of finite sequences of elements of A
T3.23 $\{0,1\}^\infty$ is uncountable
D3.44 Function $f: \mathbb{N} \to \{0,1\}$ computable if exists program that outputs $f(n)$ for every $n \in \mathbb{N}$

$A = \{1,0,\{0\},1\}$ $B = \{\{0,1,0,\{0,0\}\},1,10,0\}$ ($\{0,0\} = \{0\}$)
$A \in B$, $A \notin B$, Set entries are unique (no duplicates)

Number of ... relations on set: $|A \times A \setminus \{\text{all pairs that don't satisfy ...}\}| = b$. Then 2^b $\to$ follows from remark in D3.8

Transitive closure: (D5.18) Draw graph or matrix. It essentially is a list of unique pairs, reachable. Form: (a,b)
Ex: $\rho = \{(a,b),(a,c),(b,a)\}$ on $\{a,b,c\}$
$(a,b),(a,c),(b,a),(a,a),(b,b),(b,c)$

	a	b	c
a	1	1	1
b	1	1	1
c	0	0	0



chained bc. rel. on set
(repeatable up to ∞ times technically)

Comparable only if poset operation applicable in any of the two directions

Paset: Set with partial order "attached" $\to$ to prove, prove that partial order is a such (by showing reflexivity, ..., see D3.23)

A s.t. $A \cap \mathcal{P}(A) \neq \emptyset$: $A = \{\emptyset\}$ or $A = \{13, \{13\}\}$

ρ^3: Compose $\rho \circ \rho$, then $\rho^2 \circ \rho$

More ex. on P5/6

Notation: $|\cup \equiv_2$ means check both $|$ and $\equiv_2$

Number of elements of $|\mathcal{P}(A)| = 2^{|A|}$ For $|$ join lcm, meet gcd

A/p disjoint equiv. classes: Not connected to other el.
Ex: $\{(1,2),(2,2),(2,1),(3,3)\}$ has $\{1,2\}, \{3\}$ as els of A/p

Number Theory

Division

D4.1 Divisibility: If $a|b$ (say a divides b), $a \cdot c = b$.
c quotient, a divisor, b multiple of a. $a \nmid b$ if not div.
T4.1 $\forall a, d \neq 0 \in \mathbb{Z}\ \exists a, r \in \mathbb{Z}\ (a = dq \wedge 0 \leq r < |d|)$; a, r unique
D4.2 GCD: $d = \gcd(a,b) \overset{\text{def}}{\Leftrightarrow} d|a \wedge d|b \wedge \forall c((c|a \wedge c|b) \to c|d)$
D4.3 Relatively prime: $\gcd(a,b) = 1$ ← $\gcd(m,n) = \gcd(m, R_m(n))$
L4.2 $\gcd(m, n - qm) = \gcd(m,n)$ for any $m, n, q \in \mathbb{Z}$
D4.4 Ideal: $(a,b) \overset{\text{def}}{=} \{ua + vb \mid u, v \in \mathbb{Z}\}$, $(a) \overset{\text{def}}{=} \{ua \mid u \in \mathbb{Z}\}$
L4.3 For $a, b \in \mathbb{Z}$ there exists d s.t. $(a,b) = (d)$
L4.4 If $(a,b) = (d)$ then d is a gcd of a and b
C4.5 For $a, b \neq 0 \in \mathbb{Z}\ \exists u, v \in \mathbb{Z}$ s.t. $\gcd(a,b) = ua + vb$
D4.5 LCM: $\ell = \operatorname{lcm}(a,b) \overset{\text{def}}{\Leftrightarrow} a|\ell \wedge b|\ell \wedge \forall m((a|m \wedge b|m) \to \ell|m)$

Primes

D4.6 Prime: $p \in \mathbb{N}$ if the only positive divisor of p is 1 or p
T4.6 Every positive integer can be written as product of primes
We can write $a = \prod_i p_i^{e_i}$ and $b = \prod_i p_i^{f_i}$. $\Rightarrow \gcd(a,b) = \prod_i p_i^{\min(e_i,f_i)}$ and $\operatorname{lcm}(a,b) = \prod_i p_i^{\max(e_i,f_i)}$. $\gcd(a,b) \cdot \operatorname{lcm}(a,b) = a \cdot b$
L4.12 Every composite (non-prime) int has a prime div. $\leq \sqrt{n}$

Congruences and modular arithmetic

D4.8 Congruence: a cong. to b mod m: $a \equiv_m b \overset{\text{def}}{\Leftrightarrow} m|(a-b)$
L4.13 $m \geq 1$, $\equiv_m$ is an equivalence relation on $\mathbb{Z}$
L4.14 If $a \equiv_m b$ and $c \equiv_m d$, $a + c \equiv_m b + d$, $ac \equiv_m bd$
C4.15 $f(a_1, \ldots, a_k) \equiv_m f(b_1, \ldots, b_k)$ for $a_i \equiv_m b_i$
L4.16 (i) $a \equiv_m R_m(a)$
(ii) $a \equiv_m b \Leftrightarrow R_m(a) = R_m(b)$
C4.17 $R_m(f(a_1,\ldots,a_k)) = R_m(f(R_m(a_1), \ldots, R_m(a_k)))$

Multiplicative inverse

L4.18 $ax \equiv_m 1$ has a unique solution $x \in \mathbb{Z}$ iff $\gcd(a,m) = 1$
D4.9 Multiplicative inverse: $\hat{1}$ $x \equiv_m a^{-1}$. Exists if $\gcd(a,m) = 1$

Chinese Remainder Theorem (CRT)

T4.19 $m_1, \ldots, m_r$ pairwise relatively prime, $M = \prod_{i=1}^r m_i$. For every list $a_1, \ldots, a_r$ with $0 \leq a_i < m_i$ for $i = 1, \ldots, r$ the system $x \equiv_{m_1} a_1, \ldots, x \equiv_{m_r} a_r$ has a unique solution x with $0 \leq x < M$

Diffie-Hellman

Idea: Encryption w/ func (hard to invert, easy to calculate)

Alice	g: generator, p: large prime	Bob
a = random number in $\{0,\ldots,p-2\}$		b = random n. in $\{0,\ldots,p-2\}$
$y_A = g^a \bmod p$		$y_B = g^b \bmod p$
$k_{AB} = y_B^a = g^{b \cdot a}$		$k_{BA} = y_A^b = g^{a \cdot b}$

M.i.t. M only gets y_B and y_A

Strategies for calculating $R_m(x)$:

- Rewrite into computable terms
- Find ± 1 (i.e how terms have to be split to yield ± 1)
- Find multiples of m
- Rewrite as $x = mq + r$ (If necessary for individual terms)
- Euler's totient function. See below

$\Rightarrow$ last n-digits $R_{10^n}(x)$ ← by far quickest!
$\Rightarrow$ check if base is immediately -1 or 1

Multiplicative inverse

$\gcd(3,26)$ =
euclidean algorithm:
$26 = 8 \cdot 3 + 2$
$3 = 1 \cdot 2 + 1$
$2 = 2 \cdot 1 + 0$ once 0, done
gcd

backwards:
$2 = 26 - 8 \cdot 3$
$1 = 3 - 1 \cdot 2 = 3 - 1 \cdot (26 - 8 \cdot 3)$
$= 3 - 1 \cdot 26 + 8 \cdot 3$
$= \underline{9} \cdot 3 - 1 \cdot 26$

$9 \equiv_{26} 3^{-1}$
$3 \cdot 9 \equiv_{26} 1$

Raising an odd number to any power = odd number

For $f: \mathbb{Z}_m \to \mathbb{Z}_m$, (or any other case where cardinality is equal) f injective $\Rightarrow$ f surjective

$\gcd(a,b) \cdot \operatorname{lcm}(a,b) = ab$ because for all i we have $\min(e_i,f_i) + \max(e_i,f_i) = e_i + f_i$ in $a = \prod_i p_i^{e_i}$ and $b = \prod_i p_i^{f_i}$.
$\gcd(a,b) = \prod_i p_i^{\min(e_i,f_i)}$, $\operatorname{lcm}(a,b) = \prod_i p_i^{\max(e_i,f_i)}$

The last digit of a number: $R_{10}(x)$

Chinese remainder theorem all m_i rel. prime!
$\Rightarrow$ easy approach: split x up into n parts. ($y = 0$! ← when taking mod y, all parts w/)
ex. $x \equiv_3 2$, $x \equiv_4 2$, $x \equiv_5 1$.
$x = 4 \cdot 5 + 3 \cdot 5 + 3 \cdot 4$ then add multiplier to make parts correct
$20 \equiv_3 2$ ✓ $|\ 15 \equiv_4 3\ddot{=} \Rightarrow 15 \cdot z \equiv_4 2 \Leftrightarrow z = 2\ |\ 12 \equiv_5 2\ddot{=} \Rightarrow 12 \cdot a \equiv_5 1 \Leftrightarrow a = 3$
thus $x = 4 \cdot 5 + 3 \cdot 5 \cdot 2 + 3 \cdot 4 \cdot 3 = 86$

Congruence Systems $3x + y \equiv_6 3 \wedge 3x + 2y \equiv_6 4$
add the congruences: $(3x+y) + (3x+2y) \equiv_6 3 + 4$
apply mod to $6x + 3y \equiv_6 7 \Leftrightarrow 3y \equiv_6 1$
check $\gcd(3,6) = 1 \not\Leftrightarrow$ no solution, else solve like SLE

$R_{11}(2^{432})$ · $\varphi(11) = 10$ (C.5.14) thus $2^{10} \equiv_{11} 1$, so rewrite 2^{432} as $R_{11}(2^{430} \cdot 2^2) = 2^2 = 4$

$R_{100}(99^{99} + \ldots + 99^0) = 0$ because $99 \equiv_{100} 1$ and
$R_{100}\left(\sum_{i=0}^{99}(-1)^i\right) = R_{100}\left(\sum_{i=0}^{49}(-1)^{2i} + \sum_{i=0}^{49}(-1)^{2i+1}\right) = R_{100}(50 - 50) = 0$

To show unique solutions, consider ideal D4.4

For congruence systems with multiple vars, use add.-method to eliminate a var. Then, substitute back to solve normally.

Algebra

D5.1 Operation: on set S $f: S^n \to S$, $n \geq 0$ arity
D5.2 Algebra: pair $\langle S;\Omega\rangle$, S carrier (set), Ω list of operations
D5.3 Neutral element: el. e s.t. $e*a=a$ (left) / $a*e=a$ (right)
L5.1 $\langle S;*\rangle$ can only have one n.e. If both e_l and e_r, $e_l = e_r$
D5.4 Associativity: binary op. $*$ if $a*(b*c)=(a*b)*c$ $\forall a,b,c \in S$
D5.5 Monoid: $\langle M;*,e\rangle$, $*$ associative, e neutral element simply
D5.6 Inverse el: $b \in S$ s.t. $b*a=e$ (left) / $a*b=e$ (right). If both, inverse
L5.2 $\langle M;*,e\rangle$, $a \in M$, a has only one inverse ← group axioms
D5.7 Group: $\langle G;*,^{\wedge},e\rangle$ (i) $*$ ass. (ii) e n.e (iii) $\forall a \in G$, inv. el $\hat{a}$ exists
D5.8 Abelian / Commutative: $a*b=b*a$ $\forall a,b \in G$

L5.3
(i) $\hat{\hat{a}}=a$ (iii) $a*b=a*c \Rightarrow b=c$
(ii) $\widehat{a*b}=\hat{b}*\hat{a}$ (iv) $b*a=c*a \Rightarrow b=c$
(v) $a*x=b$ and $x*a=b$ have unique solution

Structure of groups

D5.9 Direct product: $\langle G_1 \times \dots \times G_n; \circ\rangle$, $(a_1,..a_n)\circ(b_1,\dots,b_2) = (a_1 *_1 b_1, \dots, a_n *_n b_n)$ L5.10 D.P. n.e. & inv. comp.-wise
D5.10 Group homomorphism: $\varphi: G \to H$ if $\varphi(a*b)=\varphi(a)*\varphi(b)$
Isomorphism: $G \simeq H$ if φ bijection from G to H ← inv. in H
L5.5 Group homom. satisfies (i) $\varphi(e)=e$ (ii) $\varphi(\hat{a})=\hat{\varphi(a)}$ $\forall a$
D5.11 Subgroup: $H \subseteq G$, H closed under: (1) $a*b$ (2) e (3) $\hat{a}$ $\forall a$
D5.12 Order: $\text{ord}(a)$ is least $m \geq 1$ s.t. $a^m=e$. If no m, $\text{ord}(a)=\infty$
L5.6 In a finite group G, every element has a finite order
D5.13 For a finite group G, $|G|$ is the order of G
D5.14 Group generated by a: $\langle a\rangle \overset{\text{def}}{=} \{a^n \mid n \in \mathbb{Z}\}$; a generator
D5.15 Cyclic: group $G=\langle g\rangle$, $g \in G$, g generator
Finding generators: $\langle \mathbb{Z}_m;\oplus\rangle$: all elements with $\gcd(a,m)=1$
$\langle \mathbb{Z}^*_m;\odot\rangle$: - calculate order of group - $\forall d \mid \text{ord}(G)$ check if $a^d=1$
if a is not a generator, for e.g. $\text{ord}(G)=16$, $d \in \{1,2,4,8,16\}$, we only need to check up to $a^8=1$, where d set of divisors
T5.7 Cyclic group isomorphic to $\langle \mathbb{Z}_n;\oplus\rangle$, thus abelian, order = n
T5.8 Lagrange: If $H \subseteq G$, then $|H|$ divides $|G|$, G finite group
C5.9 G fin. gr. $\text{ord}(a) \mid |G|$ $\forall a \in G$ C5.10 $a^{|G|}=e$ $\forall a \in G$
C5.11 $\text{ord}(G)$ prime, G cyclic, all $a \neq e \in G$ generator
D5.16 Multiplicative group: $\mathbb{Z}^*_m \overset{\text{def}}{=} \{a \in \mathbb{Z}_m \mid \gcd(a,m)=1\}$
D5.17 Euler function: $\varphi(m)=|\mathbb{Z}^*_m|$ (if m is prime) $p_i^{e_i}-p_i^{e_i-1}$
L5.12 If $\prod_{i=1}^{r} p_i^{e_i}$ is prime fac. of, then $\varphi(m)=\prod_{i=1}^{r}(p_i-1)p_i^{e_i-1}$
T5.13 $\langle \mathbb{Z}^*_m;\odot,(\dots)^{-1},1\rangle$ is a group
C5.14 $\forall m \geq 2$ $\forall a$ with $\gcd(a,m)=1$, $a^{\varphi(m)} \equiv_m 1$. In particular $\forall p$ prime, $\forall a \not\equiv_p 0$: $a^{p-1} \equiv_p 1$
T5.15 $\mathbb{Z}^*_m$ is cyclic iff $m=2$, $m=4$, $m=p^e$ or $m=2p^e$ where p is an odd prime and $e \geq 1$

$\mathbb{Z}_m \times \mathbb{Z}_n$ cyclic $\Leftrightarrow \gcd(m,n)=1$; For any order, just 1 non-isomorphic, cyclic group bc. T5.7
Any subgroup of a cyclic subgroup is cyclic
$H \cap K$ subgroup of G, $H \cup K$ is not; for H,K subgroup of G
Order of $\mathbb{Z}^*_m = \varphi(m)$ by D5.17

RSA

T5.16 G fin. gr., $e \in \mathbb{Z}$ with $\gcd(e,|G|)=1$. Then $x \mapsto x^e$ is a bijection and the unique e-th root of $y \in G$, i.e. $x^e=y$, is $x=y^d$, d is the multiplicative inverse of e mod $|G|$, i.e. $ed \equiv_{|G|} 1$
⇒ without $|G|$ it's hard to calculate the e-th root

Alice	insecure channel	Bob
p, q large primes		
$n=p \cdot q$		
$f=(p-1)(q-1)=\varphi(n)$		
select $e \in \mathbb{Z}_n$	$n, e \rightarrow$	m = message
$d \equiv_f e^{-1}$		
$m=R_n(c^d)$	$\leftarrow y$	$c=R_n(m^e)$

Rings

D5.18 Ring: Algebra for which:
(i) $\langle R;+,-,1\rangle$ is a commutative group
(ii) $\langle R;\cdot,1\rangle$ is a monoid ← that too
(iii) $a(b+c)=(ab)+(ac)$ (left & right distributive laws apply)

L5.17
(i) $0a=a0=0$ (ii) $(-a)b=-(ab)$ (iii) $(-a)(-b)=ab$
(iv) If R is non-trivial, then $1 \neq 0$

D5.19 Characteristic: $\text{ord}(1)$ in additive gr. if finite, else 0
D5.20 Unit u: if $uv=vu=1$, i.e. $u=u^{-1}$. Set of u of R: R^*
L5.18 For a ring R, R^* is a multiplicative group
Finding units Find all elements a s.t. $\gcd(a,m)=1$
D5.21 Divides: $a \mid b$ if $\exists c \in R$ s.t. $b=ca$. a divisor of b (multiple)
L5.19 (i) if $a \mid b$ and $b \mid c$, then $a \mid c$
(ii) if $a \mid b$, then $a \mid b \cdot c$ $\forall c \in R$
(iii) if $a \mid b$ and $a \mid c$, then $a \mid (b+c)$
all non-zero el. divide 0
D5.22 GCD for rings as in D4.2
D5.23 Zerodivisor: $a \neq 0$ if $ab=0$ for some $b \neq 0$ ex. $\mathbb{Z}$ (no field)
Finding Z.D: all elements $a \in \mathbb{Z}_m$ s.t. $\gcd(a,m) \neq 0$
D5.24 Integral Domain: Commutative, non-trivial Ring, no Z.D
L5.20 If $a \mid b$, then c with $b=ac \Leftrightarrow c=\frac{b}{a}$ is unique. (c quotient)
D5.25 Polynomial $a(x)$ over R: $a(x)=\sum_{i=0}^{d} a_i x^i$. $\deg(a(x))$ largest $i \neq 0$. If all $i=0$, then $\deg(a(x))=-\infty$. $R_{[x]}$ set of p. over R.
T5.21 For any ring R, $R[x]$ is a ring
L5.22 (i) $D[x]$ integral Domain (ii) $\deg(p_1(x) \cdot p_2(x)) = \deg(p_1(x))+\deg(p_2(x))$
(iii) units of $D[x]$ constants pol. $D^*_{[x]}=D^*$ D integral Domain

Fields

D5.26 Field: non-trivial commutative ring, every non-0 el. unit
T5.23 $\mathbb{Z}_p$ field iff p prime T5.24 A field is an int. domain
D5.27 Monic: polynomial $a(x)$ if leading coefficient is 1
D5.28 Irreducible: $\deg(a(x)) \geq 1$; if $a(x) \in F_{[x]}$ divisible by a constant or constant multiple of $a(x)$ ← only
D5.29 GCD: monic pol. of largest deg s.t. $g(x) \mid a(x) \wedge g(x) \mid b(x)$
T5.25 For any $a(x)$ and $b(x) \neq 0$ in $F_{[x]}$, there exist unique $q(x), r(x)$ s.t. $a(x)=b(x) \cdot q(x) + r(x)$ and $\deg(r(x)) < \deg(b(x))$

D5.30 Associates: In Int. Domain, $a \sim b$ if $a=ub$ for some u
D5.31 Irreducibility in Int. Dom: non-unit $p \in D \setminus \{0\}$ if for $p=ab$, either a or b is a unit
L5.26 $a \sim b \Leftrightarrow a \mid b \wedge b \mid a$
D5.32 Euclidean Domain: Int. Dom w/ deg-fn $d: D \setminus \{0\} \to \mathbb{N}$ s.t.
(i) For every $a, b \neq 0 \in D$ $\exists q,r$ s.t. $a=bq+r$, $d(r)<d(b)$ or $r=0$
(ii) For all non-zero a and b in D, $d(a) \leq d(ab)$
T5.27 In a D5.32 every el. can be factored uniquely (up to taking associates) into irreducible elements

Polynomials as Functions

L5.28 Polynomial evaluation is compatible with the ring ops:
- If $c(x)=a(x)+b(x)$, then $c(\alpha)=a(\alpha)+b(\alpha)$ for any α
- If $c(x)=a(x) \cdot b(x)$, then $c(\alpha)=a(\alpha) \cdot b(\alpha)$ for any α
D5.33 Root: Element $\alpha \in R$ for which $a(\alpha)=0$
L5.29 Field F, $\alpha \in F$ is a root of $a(x) \Leftrightarrow x-\alpha$ divides $a(x)$
C5.30 $a(x)$ of deg 2 or 3 over field F irreducible iff it has no root
T5.31 $a(x) \in F[x]$, $d=\deg(a(x))$ has at most d roots
L5.32 $a(x)$ uniquely determined by $d+1$ values, i.e $a(\alpha_1),\dots,a(\alpha_{d+1})$ for any distinct $\alpha_1,\dots,\alpha_{d+1} \in F$

Finite fields

L5.33 Congruence mod $m(x)$ equiv. rel on $F[x]$, each equiv. class has a unique representative of $\deg < \deg(m(x))$
D5.34 $\deg(m(x))=d$, $F[x]_{m(x)} \overset{\text{def}}{=} \{a(x) \in F[x] \mid \deg(a(x)) < d\}$
L5.34 F fin. field w/ q el., $\deg(m(x))=d$, then $|F[x]_{m(x)}|=q^d$
L5.35 $F[x]_{m(x)}$ ring for addition, multiplication mod $m(x)$
L5.36 $F[x]^*_{m(x)} = \{a(x) \in F[x]_{m(x)} \mid \gcd(a(x),m(x))=1\}$
T5.37 $F[x]_{m(x)}$ is a field iff $m(x)$ is irreducible If F is field $F[x]$ is not
T5.38 $|GF(q)|=q-1$ for $q=p^e$, p = prim, $e \geq 1$
← Galois field with q elements, = finite fields

ECC

D5.35 Encoding function $E(n,k)$: maps $\mathcal{A}^k$ to $\mathcal{A}^n$ where $n>k$
Codeword: Result of E
D5.36 ECC(n,k): $|\mathcal{A}|=q$ is a subset of $\mathcal{A}^n$ of cardinality q^k
D5.37 Hamming distance: number of positions in which two strings over $\mathcal{A}$ differ
D5.38 Minimum distance: minimal Hamming distance of two codewords of an ECC.
D5.39 Decoding function D: for (n,k) encoding fn, $D: \mathcal{A}^n \to \mathcal{A}^k$
D5.40 t-error correcting: $D((r_0,\dots,r_{n-1}))=(a_0,\dots,a_{k-1})$ for any $(r_0,\dots,r_{n-1})$ w/ Hamming distance at most t from $E((a_0,\dots,a_{k-1}))$
A code C is t-error correcting if $\exists E,D$ with $C=\text{Im}(E)$, where D is t-error correcting
T5.41 C w/ min. dist. d is t-ec iff $d \geq 2t+1$
T5.42 Let $A=GF(q)$ and let $\alpha_0,\dots,\alpha_{n-1} \in \mathcal{A}$. The enc. fn. $E((a_0,\dots,a_{k-1}))=(a(\alpha_0),\dots,a(\alpha_{n-1}))$ where $a(x)=a_{k-1}x^{k-1}+\dots+a_0$
This ECC has minimum distance $n-k+1$

For minimum distance, can't be between itself, only between itself and another element

Multiplicative inverse of x^2+1 **in** $GF(3)[x]_{x^3+2x+1}$

$x^3+2x+1 = x \cdot (x^2+1) + (x+1)$ | $(x^3+2x+1) : (x^2+1) = x$, $-(x^3+x)$, $x+1$

$x^2+1 = (x+2)(x+1) + (2)$

$x+1 = (2x)(2)+1$

Proceed as with numbers:

$1 = (x+1) - 2x2$ then substitute the 2 for the transformed second equation. Repeat, simplify.

$= (2x^2+x+1)(x^3+2x+1) + (x^3+2x^2)(x^2+1)$

(x^3+2x^2) = 0 in $GF(3)[x]_{x^3+2x+1}$

$\Rightarrow x^3+2x^2 \equiv_{x^3+2x+1} x^3+2x^2-(x^3+2x+1) \equiv_{x^3+2x+1} 2x^2+x+2$

Euler's totient function $\varphi(n)$ for $1 \le n \le 100$ (see D5.17)

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

← $\varphi(50)$ ← $\varphi(100)$

L5.12 states that we can compute $\varphi(n)$ using the prod. of all prime factors, each (p_i-1)

$\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$

Finding generators: Evaluate the sets generated by the set's elements. When the set is equal, then generator

Example: Find generators of $\mathbb{Z}_{14}^*$. $\mathbb{Z}_{14}^* = \{1,3,5,9,11,13\}$

$\langle 1 \rangle = \{1\}$, $\langle 3 \rangle = \{1,3,5,9,11,13\}$, $\langle 5 \rangle = \{1,3,5,9,11,13\}$

$\langle 9 \rangle = \{1,9,11\}$, $\langle 11 \rangle = \{1,9,11\}$, $\langle 13 \rangle = \{1,13\}$

Factoring into irreducible polynomials = write as product of irreducible elements: $x^2+x+1 = (x-2) \cdot (x-4) \equiv_7 (x+5) \cdot (x+3)$

Number of Subgroups: For cyclic groups, we know $|H| \,|\, |G|$ (Lagrange theorem). E.g. $\langle \mathbb{Z}_{60}; \oplus \rangle$. From T5.7 follows that every subgroup of $\mathbb{Z}_n$ of n elements is unique.

Decompose 60: $2^2 \cdot 3^1 \cdot 5^1$. How many exponent combinations are there? $\{0,1,2\}$ for 2, $\{0,1\}$ for 3, $\{0,1\}$ for 5.

Thus: $3 \cdot 2 \cdot 2 = 12$. → right!

Better/Easier: τ-function: number of divisors of number. Each divisor generates a subgroup (except number itself).

→ 11 subgroups, 12th is $\{0\}$

For a **cyclic group**, e.g. $\mathbb{Z}_{14}$, the **subgroups** are def by divisors of 14: $\{0\}$, $\{0,7\}$, $\{0,2,4,6,8,10,12\}$, $\{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14\}$. Length of s.g. is a divisor.

RSA Example: Encrypted pw of ronalddump@potus.com is 2. Public key: $(N,e) = (299, 151)$

- Do prime factorization (low number), i.e. $n = p \cdot q : 299 = 13 \cdot 23$
- Compute group order: $|\mathbb{Z}_n^*| = \varphi(n) = (p-1) \cdot (q-1) = 12 \cdot 22 = 264$
- According to T5.16, we can decrypt the password $y=2$, by finding the private key d, which is the multiplicative inverse of $e = 151 \bmod |\mathbb{Z}_n^*|$ i.e. $151 \bmod 264$.
- This task already provided the multiplicative inverse in the hint: $1 = 151 \cdot 7 - 4 \cdot 264$, i.e. $151 \cdot d \equiv_{264} 1$

$1 = 151 \cdot 7 - 4 \cdot 264 \Rightarrow 151 \cdot 7 \equiv_{264} 1 \Rightarrow 7$

- Decrypt with d:

$x \equiv_n y^d \iff x \equiv_{299} 2^7 \iff x \equiv_{299} 128 \iff x = 128$

The **generators** of a group $\langle \mathbb{Z}_n; \oplus_n \rangle$ are all elements of $\mathbb{Z}_n$ that are coprime to n, i.e. $\gcd(a,n) = 1$

$\Rightarrow a$ is a generator — alternatively: (also see D5.15) According to T5.8, the subgroup's order must divide the group's order. To find generator, simply check the order of the group generated by e.g. x and if $\neg(\text{ord}(\langle x \rangle) \,|\, \text{ord}(G))$, or $\text{ord}(\langle x \rangle) = \text{ord}(G) \Rightarrow x$ generator

# of gen of cyclic grp: $n-1$ for n prime

# of zero div of $\mathbb{Z}_n$: number of multiples of all divisors in group. Otherwise: $n - \varphi(n) - 1$ (−1 bc. no 0)

 # units of $\mathbb{Z}_n$: $\varphi(n)$ | Find grp. w/ n el: L5.34

ECC **Minimum Distance:** Write as matrix, noting the hamming distance (number of elements differing). Minimum distance is the lowest number > 0.

$\text{ord}((\pi, \sigma)) = \text{lcm}(\text{ord}(\pi), \text{ord}(\sigma))$. Order of permutation / transformation is number of times it has to be applied to reach the start again.

Number of Isomorphisms between two cyclic groups of order 14: $\varphi(14) = 6$

Group **isomorphic** to $\langle \mathbb{Z}_{12}; + \rangle : \langle \mathbb{Z}_3; + \rangle \times \langle \mathbb{Z}_4; + \rangle$

List of subgroups: All possible subsets of group. e.g. $\langle \mathbb{Z}_2; + \rangle \times \langle \mathbb{Z}_2; + \rangle : \{(0,0),(0,1),(1,0),(1,1)\}$ (this & all subs.)

Every **group of prime order** is cyclic (see C.5.11)

GCD of polynomial: Find roots of one poly. Check if other poly shares same roots. GCD = the root they don't share. Respect the mod!

Homomorphism: If we need to separate terms, e.g. $\phi(a \circ \hat{a})$, then we can: $\phi(a) * \phi(\hat{a})$ (by switching op to second group's op ($\phi: G \to H$) $\langle G; \circ, \hat{}, e_\circ \rangle$, $\langle H; *, ^{-1}, e_* \rangle$

Proof for valid formula using resolution calculus: Show that ¬F is invalid / unsatisfiable

Order of element in group: $\text{ord}(x^n)$ in $\mathbb{R}_m = \frac{\text{lcm}(m,n)}{n}$

Order of two elements in direct product: $\text{ord}((x^n, x^t))$ in $\mathbb{R}^m = \text{lcm}(\text{ord}(x^n), \text{ord}(x^t))$

List of **elements not a gen.** usually includes 0

To rewrite **polynomial** as **irreducible** ones, find roots

To find **m(x)** s.t. **field has n el:** L5.34 & 5.37

Cyclic groups of same order are isomorphic

Number of subgrp/set of **direct prod:** $\mathbb{Z}_m \times \mathbb{Z}_n$

$\sum_{a|m \wedge b|n} \gcd(a,b)$ where $a|m$ is the set of all divisors of m. Sum of all combin.

Ex: $m=2, n=6$. $a|m = \{1,2\}$, $b|n = \{1,2,3\}$ then sum is:

$\sum_{b|6} \gcd(1,b) + \sum_{b|6} \gcd(2,b) = 4+6 = 10$

For any kind of fundamental proof of **group properties**, D5.3 & L5.3 are very handy.

Isomorph groups share same order

G cyclic ⇒ G abelian; only single-sided impl.

gcd of polynomials: apply euclidean algorithm

Irreducibility of Polynomials:

- deg 1 always irreducible
- deg 2&3 if no root, see C5.30
- deg 4 if no root or factor deg 2
- deg 5 if no root or factor deg 2/3

Set theory

Transitive closure ρ^*: relation $\rho \cup$ (union) with all transitive elements. If not present, add them. (1 2 3 4 ← alias)
Example: Set $A = \{\emptyset, \{\emptyset\}\}$, thus $P(A) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, A\}$
$\rho = \{(\emptyset, \{\emptyset\}), (\{\emptyset\}, A), (A, \{\{\emptyset\}\})\}$. Matrix repr. of ρ^*

$\rho = \{(1,2), (2,4), (4,3)\}$. Additional elements through transitivity:
(1,2) & (2,4) → (1,4)
(1,4) & (4,3) → (1,3)
(2,4) & (4,3) → (2,3)

$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

See also 4 down note

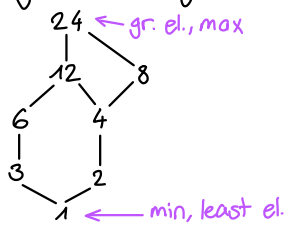
Equivalence Relation & partial order rel. on non-empty set
$S = \{\emptyset\}$, $\rho = \{(\emptyset, \emptyset)\}$ or $S = \{1,2\}$, $\rho = \{(1,1), (2,2)\} = id$

To **prove transitivity** under assumption, consider L3.9, then associativity and the assumption

We can **transform set expressions** into logic ones using predicates: $A = x \in A$. Then translate
$A \cup B \iff A \vee B$; $A \cap B \iff A \wedge B$; $A \setminus B \iff A \wedge \neg B$

Transitive sets (commonly) include (a,a)-style els

Bounds Can determine using Hasse diagram
$(\{1,2,3,4,6,8,12,24\}, |)$
any subset here has lub and glb.
Example: {8,12} has lower bounds 1, 2 & 4, where 4 glb. lub is 24 in this case
This poset is a lattice



Countability proofs: Look at Theorems/Lemmas on P3. For example, ρ^* is a union. Use T3.22 and w/ induction to prove ρ^n is countable

To compute explicit ρ^3, consider drawing graph and find all paths of length exactly 3

Logic

CNF & DNF: Not mutually exclusive. None if de Morgan. Both if only $\vee$ or $\wedge$ because could be a single con-/disjunction, A, B, ... could be literals. Example: $A \wedge B \wedge \neg C$ is in CNF & DNF (as oppased to just CNF). Read carefully!

A **derivation rule is not sound** if there exists an interpretation for which L.H.S. false & R.H.S. true. We can check with table

When **deriving formula in calculus**, can pick symbols arbitrarily from input. Example:

$$\{F, G\} \vdash_{R_1} F \to G$$
$$\{(F \to G) \to H, (G \to H) \to (F \to G)\} \vdash_{R_2} F \to H$$

Derive $C \to A$ from $\{A, B \to A, C \to B\}$ in the calculus.

$\{(C \to B), A\} \vdash_{R_1} (C \to B) \to A$ $(F = C \to B, G = A)$
$\{(B \to A), (C \to B)\} \vdash_{R_1} (B \to A) \to (C \to B)$ $(F = B \to A, G = C \to B)$
$\{(C \to B) \to A, (B \to A) \to (C \to B)\} \vdash_{R_2} C \to A$ $(F = C, G = B, H = A)$

Further trick: start at last step to find steps!

Number Theory

For **primality proofs** use the fact that any prime $p > 3$ can't fulfill $R_3(p) = 0$. Then show that $R_3(f(p)) \neq 0$ because that implies divisible by 3. Apply C4.17 to f! So if $R_3(p) = 1$ and $f = p^2$, $f = 1^2$

For any True / False Questions, think of short (potentially informal) proof

Justify each step!

Showing **equiv. statement** ① & ②: actually ① ⟺ ②

I just wanted to add a remark as to how massive of a waste of time having to write a cheat-sheet by hand is. It took me in excess of 50h to write this one. I write terribly slowly by hand and I also hate it tremendously. We are CS-students and LaTeX is the best typesetting tool (or Tex in general). Why not allow that?!