Chapter 6: Logic

alphabet: Σ strings: Σ^*

$S \subseteq \Sigma^*$: set of (syntactic) representations of statements

$P \subseteq \Sigma^*$: set of (syntactic representations) of proof strings

truth function: $J: S \to \{0,1\}$

verification function: $\phi: S \times P \to \{0,1\}$

(we can consider $S = P = \{0,1\}^*$)

D 6.1 A proof system is a quadruple $\Pi = (S, P, J, \phi)$.

D 6.2 A proof system Π is sound if no false statement has a proof, i.e. if for all $s \in S$ for which there exists $p \in P$ with $\phi(s,p) = 1$, we have $J(s) = 1$

D 6.3 A proof system Π is complete if every true statement has a proof, i.e. if for all $s \in S$ with $J(s) = 1$ there exists $p \in P$ with $\phi(s,p) = 1$

Goal: A goal of logic is to provide a specific proof system Π for which a very large class of mathematical statements can be expressed as an element of S.

D 6.4 The syntax of a logic defines an alphabet Λ (of allowed symbols) and specifies which strings in Λ^* are formulas (i.e. are syntactically correct)

D 6.5 The semantics of a logic defines (among other things) a function free, which assigns to each formula $F = (f_1, f_2, \cdots f_k) \in \Lambda^*$ a subset free$(F) \subseteq \{1, \dots, k\}$ of the indices. If $i \in$ free(F) then the symbol f_i is said to occur free in F.

D 6.6 An interpretation consists of a set $Z \subseteq \Lambda$ of symbols of Λ, a domain for each symbol in Z, and a function that assigns to each symbol in Z a value in its associated domain.

D 6.7 An interpretation is suitable for a formula F if it assigns a value to all symbols $\beta \in \Lambda$ occuring free in F.

D 6.8 The semantics of a logic also defines a function σ assigning to each formula F, and each interpretation $\mathcal{A}$ suitable for F, a truth value $\sigma(F, \mathcal{A})$ in $\{0,1\}$. One often writes $\mathcal{A}(F)$ instead of $\sigma(F, \mathcal{A})$ and calls $\mathcal{A}(F)$ the truth value of F under interpretation $\mathcal{A}$.

D 6.9 A suitable interpretation $\mathcal{A}$ for which a formula F is true is called a model for F and one also writes $\mathcal{A} \models F$.
For a set of formulas: $\mathcal{A} \models M$ if $\mathcal{A}(F) = 1$ for all $F \in M$.
$\mathcal{A}$ is not a model for M: $\mathcal{A} \not\models M$

D 6.10 A formula F (or a set M of formulas) is called satisfiable if there exists a model for F (or M) and unsatisfiable otherwise
$\bot$ stands for an arbitrary unsatisfiable formula, but is not a formula!

D 6.11 A formula F is called a tautology or valid if it is true for every suitable interpretation. $\top$ stands for a tautology.

D 6.12 A formula G is a logical consequence of a formula F (or a set M of formulas) den. $F \models G$ ($M \models G$) if every interpretation suitable for both F (or M) and G, which is a model for F (for M) is also a model for G.

D 6.13 Two formulas are equivalent, den. $F \equiv G$ if each one is a logical consequence of the other. $F \equiv G \overset{def}{\iff} F \models G$ and $G \models F$

D 6.14 If F is a tautology one also writes $\models F$.

D 6.15 If F and G are formulas, then also $\neg F$, $(F \wedge G)$, and $(F \vee G)$ are formulas.
$F \wedge G$ conjunction $F \vee G$ disjunction

D 6.16 $\mathcal{A}((F \wedge G)) = 1$ iff. $\mathcal{A}(F) = 1$ and $\mathcal{A}(F) = 0$
$\mathcal{A}((F \vee G)) = 1$ iff. $\mathcal{A}(F) = 1$ or $\mathcal{A}(G) = 1$
$\mathcal{A}(\neg F) = 1$ iff. $\mathcal{A}(F) = 0$

L 6.1
1) $F \wedge F \equiv F$ and $F \vee F \equiv F$ (idempotence)
2) $F \wedge G \equiv G \wedge F$ and $F \vee G \equiv G \vee F$ (commutativity)
3) $(F \wedge G) \wedge H \equiv F \wedge (G \wedge H)$ and $(F \vee G) \vee H \equiv F \vee (G \vee H)$ (associativity)
4) $F \wedge (F \vee G) \equiv F$ and $F \vee (F \wedge G) \equiv F$ (absorption)
5) $F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$ (distributive law)
6) $F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$ (distributive law)
7) $\neg\neg F \equiv F$ (double negation)
8) $\neg(F \wedge G) \equiv \neg F \vee \neg G$ and $\neg(F \vee G) \equiv \neg F \wedge \neg G$ (de Morgan's rules)
9) $F \vee \top \equiv \top$ and $F \wedge \top \equiv F$ (tautology rules)
10) $F \vee \bot \equiv F$ and $F \wedge \bot \equiv \bot$ (unsatisfiability rules)
11) $F \vee \neg F \equiv \top$ and $F \wedge \neg F \equiv \bot$

L 6.2 A formula F is a tautology if and only if $\neg F$ is unsatisfiable

L 6.3 equivalent statements
1) $\{F_1, \cdots, F_k\} \models G$
2) $F_1 \wedge \cdots \wedge F_k \to G$ is a tautology
3) $\{F_1, \dots, F_k, \neg G\}$ is unsatisfiable

Hilbert-style calculus: syntatic objects that are manipulated are formulas

D 6.17 A derivation rule or inference rule is a rule for deriving a formula from a set of formulas (precondition/premises). We write $\{F_1, \dots, F_k\} \vdash_R G$ if G can be derived from $\{F_1, \dots, F_k\}$ by rule R.

D 6.19 A logical calculus K is a finite set of derivation rules $K = \{R_1, \cdots, R_m\}$

D 6.20 A derivation of a formula G from a set M of formulas in a calculus K is a finite (length $= n$) of applications of rules in K, leading to G.
$M_0 := M$
$M_i := M_{i-1} \cup \{G_i\}$ $1 \leq i \leq n$ where $N \vdash_{R_j} G_i$ for some $N \subseteq M_{i-1}$ and for some $R_j \in K$
$G_n = G$
$M \vdash_K G \iff$ there is a derivation of G from M in the calculus K

D 6.21 A derivation rule is correct if $M \vdash_R F \Rightarrow M \models F$

D 6.22 A calculus K is sound if $M \vdash_K F \Rightarrow M \models F$ and complete if $M \models F \Rightarrow M \vdash_K F$

L 6.4 If $\{F_1 \cdots F_k\} \vdash_K G$ holds for a sound calculus K $\models F_1 \wedge \cdots \wedge F_k \to G$

Propositional Logic

D 6.23 (syntax) An atomic formula is a symbol of the form A_i with $i \in \mathbb{N}$. A formula is defined as follows
- An atomic formula is a formula
- If F and G are formulas then $\neg F$, $F \wedge G$ and $F \vee G$ are formulas

D 6.24 (semantics) For a set Z of atomic formulas, an interpretation $\mathcal{A}$, called truth assignment, is a function $\mathcal{A}: Z \to \{0,1\}$. $\mathcal{A}$ is suitable for F if it contains all atomic formulas in F. $\mathcal{A}(F) = \mathcal{A}(A_i)$ for an atomic formula A_i, for $\mathcal{A}(F)$ see D 6.16

D 6.25 A literal is an atomic formula or the negation of an atomic formula

D 6.26 A formula is in conjunctive normal form, if it is a conjunction of disjunctions of literals.

D 6.27 A formula is in disjunctive normal form, if it is a disjunction of conjunctions of literals

T 6.5 Every formula is equivalent to a formula in CNF and also to a formula in DNF.

D 6.28 A clause is a set of literals

D 6.29 The set of clauses associated to a formula in CNF is the set
$$K(F) = \{\{L_{11} \cdots L_{1m_1}\}, \dots, \{L_{n1} \cdots L_{nm_n}\}\}$$

D 6.30 A clause K is a resolvent of clauses K_1 and K_2 if there is a literal L such that $L \in K_1$, $\neg L \in K_2$ and $K = (K_1 \setminus \{L\}) \cup (K_2 \setminus \{\neg L\})$

L 6.6 The resolution calculus is sound

T 6.7 A set M of formulas is unsatisfiable if and only if $K(M) \vdash_{Res} \emptyset$.

L 6.8 For any formulas F and G, where x does not occur free in H, we have

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

Predicate Logic

D 6.31 (syntax)
- a variable symbol is of the form x_i with $i \in \mathbb{N}$
- a function symbol is of the form $f_i^{(k)}$ with $i, k \in \mathbb{N}$ where k denotes the number of arguments. Function symbols for $k=0$ are called constants.
- a predicate symbol is of the form $P_i^{(k)}$ with $i, k \in \mathbb{N}$ where k denotes the number of arguments
- a variable is a term and if $t_1 \cdots t_k$ are terms then $f^{(k)}(t_1 \cdots t_k)$ is a term. For $k=0$ no parentheses
- If $t_1 \cdots t_k$ are terms, then $P_i^{(k)}(t_1 \cdots t_k)$ is a formula, called an atomic formula, see D 6.15, if F is a formula then for any i $\forall x_i F$ and $\exists x_i F$ are formulas

D 6.32 Every occurence of a variable in a formula is either bound or free. If x occurs in a (sub-)formula of the form $\forall x G$ or $\exists x F$ then it is bound, otherwise it is free. A formula is closed if it contains no free variables.

D 6.33 F formula, x variable, t term $F[x/t]$ denotes the formula obtained from F by substituting every free occurrence of x by t.

D 6.34 An interpretation or structure is a tuple $\mathcal{A} = (U, \phi, \psi, \xi)$ where U is a non-empty universe, ϕ is a function assigning to each function symbol a function $U^k \to U$, ψ is a function assigning to each predicate symbol a function $U^k \to \{0,1\}$ and ξ is a function assigning to each variable symbol a value in U.

D 6.35 A interpretation is suitable for F, if it defines all function symbols, predicate symbols and freely occuring variables of F.

D 6.36 (semantics) value of term t: if $t = x_i$ $\mathcal{A}(t) = \xi(x_i)$
if t is of the form $f^{(k)}(t_1 \cdots t_k)$ then $\mathcal{A}(t) = \phi(f)(\mathcal{A}(t_1) \cdots \mathcal{A}(t_k))$

truth value of F: see D 6.16, if F is of the form $F = P^{(k)}(t_1 \cdots t_k)$ then $\mathcal{A}(F) = \psi(P)(\mathcal{A}(t_1) \cdots \mathcal{A}(t_k))$, if F is of the form $\forall x G$ or $\exists x G$ then let $\mathcal{A}_{[x \to u]}$ $u \in U$ be the same structure as $\mathcal{A}$ except that $\xi(x)$ is overwritten by u (i.e. $\xi(x) = u$)

$$\mathcal{A}(\forall x G) = \begin{cases} 1 & \text{if } \mathcal{A}_{[x \to u]}(G) = 1 \text{ for all } u \in U \\ 0 & \text{else} \end{cases}$$

$$\mathcal{A}(\exists x G) = \begin{cases} 1 & \text{if } \mathcal{A}_{[x \to u]}(G) = 1 \text{ for some } u \in U \\ 0 & \text{else} \end{cases}$$

L 6.9 If one replaces a sub-formula G of a formula F by an equivalent (to G) formula H, then the resulting formula is equivalent to F.

L 6.10 For a formula G in which y does not occur we have (bound substitution)
- $\forall x G \equiv \forall y G[x/y]$
- $\exists x G \equiv \exists y G[x/y]$

D 6.37 A formula in which no variable occurs both as a bound and as a free variable and in which all variables appearing after the quantifiers are distinct is said to be in rectified form.

L 6.11 For any formula F and any term t we have $\forall x F \models F[x/t]$.

D 6.38 A formula of the form $Q_1 x_1 Q_2 x_2 \cdots Q_n x_n G$, where the Q_i are arbitrary quantifiers and G is a formula free of quantifiers, is said to be in prenex form.

T 6.12 For every formula there is an equivalent formula in prenex form.

T 6.13 $\neg \exists x \forall y (P(y,x) \Leftrightarrow \neg P(y,y))$

CNF: conjunction of the opposite of every interpretation making the formula false

A B	F
0 1	0

$(A \vee \neg B) \wedge (\cdots)$

DNF: disjunction of exactly every interpretation making the formula true

A B	F
0 1	1

$(\neg A \wedge B) \vee (\cdots)$

$x^2 + 2x + 1 : x + 1 = x + 1$
$\underline{x^2 + x}$
$\quad x + 1$
$\quad \underline{x + 1}$
$\quad\quad 0$

$x \equiv_{17} 5^{-1} \, 2 \Rightarrow x = 7$

$17 = 3 \cdot 5 + 2$
$5 = 2 \cdot 2 + 1$

backwards: $1 = 5 - 2 \cdot 2 = 5 - 2(17 - 3 \cdot 5)$
$= -2 \cdot 17 + 7 \cdot 5$

Chapter 3: Sets, Relations and Functions

D 3.2 $A = B \overset{def}{\iff} \forall x (x \in A \iff x \in B)$

L 3.1 a,b arb. $\{a\} = \{b\} \Rightarrow a = b$

D 3.3 $A \subseteq B \overset{def}{\iff} \forall x (x \in A \to x \in B)$ subset

L 3.2 $A = B \iff (A \subseteq B) \wedge (B \subseteq A)$

L 3.3 $A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$

D 3.4 $A \cup B \overset{def}{=} \{x \mid x \in A \vee x \in B\}$ union

$A \cap B \overset{def}{=} \{x \mid x \in A \wedge x \in B\}$ intersection

$\bigcup \mathcal{A}, \bigcap \mathcal{A}$ union and intersection of sets in $\mathcal{A}$

D 3.5 $B \setminus A \overset{def}{=} \{x \in B \mid x \notin A\}$ difference

T 3.4 Idempotence: $A \cap A = A$ $A \cup A = A$

Commutativity: $A \cap B = B \cap A$ $A \cup B = B \cup A$

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

Absorption: $A \cap (A \cup B) = A$ $A \cup (A \cap B) = A$

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

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

Consistency: $A \subseteq B \iff A \cap B = A \iff A \cup B = B$

D 3.6 A set is called empty if it contains no elements i.e. if $\forall x \neg (x \in A)$

L 3.5 There is only one empty set, $\{\}$ or $\emptyset$.

L 3.6 The empty set is a subset of every set i.e. $\forall A (\emptyset \subseteq A)$

D 3.7 The power set of a set A, denoted $\mathcal{P}(A)$, is the of all subsets of A: $\mathcal{P}(A) \overset{def}{=} \{S \mid S \subseteq A\}$

D 3.8 The Cartesian Product $A \times B$ of two sets A, B

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

For finite sets: $|A \times B| = |A| \cdot |B|$

D 3.9 A (binary) relation ρ from a set A to a set B

anstellungen? 2 ((A,B)-relation) is a subset of $A \times B$. If $A = B$ 0 then ρ is called a relation on A.

$(a,b) \in \rho \overset{not.}{\iff} a \rho b$

D 3.10 For any set A, the identity relation on A denoted id_A, id is the relation $id_A = \{(a,a) \mid a \in A\}$

D 3.11 The inverse of a relation ρ from A to B is the relation $\hat{\rho}$ from B to A defined by

$\hat{\rho} \overset{def}{=} \{(b,a) \mid (a,b) \in \rho\}$

D 3.12 Composition of ρ and σ:

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

n-fold composition of ρ on a set A: ρ^n

L 3.7 The composition of relations is associative

L 3.8 ρ, σ relations $\widehat{\rho \sigma} = \hat{\sigma} \hat{\rho}$

D 3.13 A relation ρ on a set A is called reflexive if $a \rho a$ for all $a \in A$ i.e. $id_A \subseteq \rho$

D 3.14 A relation ρ on a set A is called irreflexive if $a \not\rho a$ for all $a \in A$, i.e. if $id_A \cap \rho = \emptyset$

D 3.15 A relation ρ on a set A is called symmetric if $a \rho b \iff b \rho a$ for all $a, b \in A$ i.e. if $\rho = \hat{\rho}$

D 3.16 A relation on a set A is called antisymmetric if $a \rho b \wedge b \rho a \Rightarrow a = b$ is true for all $a, b \in A$ i.e. if $\rho \cap \hat{\rho} \subseteq id$

D 3.17 A relation ρ on a set is called transitive if $a \rho b \wedge b \rho c \Rightarrow a \rho c$ is true for all $a, b, c \in A$

L 3.9 A relation ρ is transitive if and only if $\rho^2 \subseteq \rho$ ($\rho^n \subseteq \rho$ for $n > 1$)

D 3.18 The transitive closure of a relation ρ on a set A, denoted ρ^*, is $\rho^* = \bigcup_{n \in \mathbb{N} \setminus \{0\}} \rho^n$

D 3.19 An equivalence relation on a set is a relation on a set A that is reflexive, symmetric and transitive.

D 3.20 For an equivalence relation θ on a set A and for $a \in A$, the set of elements of A that are equivalent to a is called the equivalence class of a denoted $[a]_\theta$.

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

L 3.10 The intersection of two equivalence relations (on the same set) is an equivalence relation.

D 3.21 A partition of a set A is a set of mutually disjoint subsets of A that cover A.

D 3.22 The set of equivalence classes of an equivalence relation θ denoted by $A/\theta \overset{def}{=} \{[a]_\theta \mid a \in A\}$ is called the quotient set of A by θ, or A modulo θ or A mod θ

T 3.11 The set A/θ of equivalence classes of an equivalence relation θ on A is a partition of A.

D 3.23 A partial order (or order relation) on a set A is a relation that is reflexive, antisymmetric and transitive. A set A with a partial order $\preceq$ on A is called a partially ordered set (poset) and is denoted as $(A; \preceq)$.

D 3.24 For a poset $(A; \preceq)$ two elements a and b are called comparable if $a \preceq b$ or $b \preceq a$, otherwise they are called incomparable.

D 3.25 If any two elements of a poset $(A; \preceq)$ are comparable, then A is called totally ordered (or linearly ordered) by $\preceq$.

D 3.26 In a poset $(A; \preceq)$ an element b is said to cover an element a if $a \prec b$ and there exists no c with $a \prec c$ and $c \prec b$ (between).

D 3.27 The Hasse diagram of a (finite) poset $(A; \preceq)$ is the directed graph whose vertices are labeled with the elements of A and where there is an edge from a to b iff. b covers a.

D 3.28 For given posets $(A; \preceq)$ and $(B; \sqsubseteq)$, their direct product, denoted $(A; \preceq) \times (B; \sqsubseteq)$, is the set $A \times B$ with the relation $\leq$ on $A \times B$ defined by

$(a_1, b_1) \leq (a_2, b_2) \overset{def}{\iff} a_1 \preceq a_2 \wedge b_1 \sqsubseteq b_2$

T 3.12 $(A; \preceq) \times (B; \sqsubseteq)$ is a poset.

T 3.13 For given posets $(A; \preceq)$ and $(B, \sqsubseteq)$, the relation $\leq_{lex}$ defined on $A \times B$ by

$(a_1, b_1) \leq_{lex} (a_2, b_2) \overset{def}{\iff} a_1 \prec a_2 \vee (a_1 = a_2 \wedge b_1 \sqsubseteq b_2)$

is a partial order relation.

D 3.29 Let $(A; \preceq)$ be a poset and let $S \subseteq A$. Then:

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

D 3.30 A poset $(A; \preceq)$ is well-ordered if it is totally ordered and if every non-empty subset of A has a least element.

D 3.31 Let $(A; \preceq)$ be a poset. If a and b have a greatest lower bound, then it is called the meet of a and b, often denoted $a \wedge b$. If a and b have a least upper bound then it is called the join of a and b, often denoted $a \vee b$.

D 3.32 A poset $(A; \preceq)$ in which every pair of elements has a meet and a join is called a lattice.

D 3.33 A function $f: A \to B$ from a domain A to a codomain B is a relation from A to B:

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

D 3.34 Set of all functions $A \to B$: B^A

D 3.35 A partial function is a relation with 2.

D 3.36 $f: A \to B, S \subseteq A$ image of S under f $f(S)$:

$f(S) \overset{def}{=} \{f(a) \mid a \in S\}$

D 3.37 The subset $f(A)$ of B is called the image (or range) of f and is also denoted $Im(f)$.

D 3.38 For a subset T of b the preimage of T denoted $f^{-1}(T)$ is the set of values in A that map into T:

$f^{-1}(T) \overset{def}{=} \{a \in A \mid f(a) \in T\}$

D 3.39 A function $f: A \to B$ is called
1. injective if for $a \neq b$ we have $f(a) \neq f(b)$
2. surjective if $f(A) = B$
3. bijective if both

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

D3.41 The composition of a function $f: A \to B$ and a function $g: B \to C$ den. by $g \circ f$ or gf, is defined by $(g\circ f)(a) = g(f(a))$!

L3.14 Function composition is associative.

D3.42 A and B equinumerous $A \sim B$ if there exists a bijection $A \to B$
B dominates A $A \preceq B$ if $A \sim C$ for $C \subseteq B$ or if there exists an injective function $A \to B$
A is countable if $A \preceq \mathbb{N}$ and uncountable otherwise

L3.15 $A \preceq B \wedge B \preceq C \Rightarrow A \preceq C$
$A \subseteq B \Rightarrow A \preceq B$

T3.16 $A \preceq B \wedge B \preceq A \Rightarrow A \sim B$

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

T3.18 The set $\{0,1\}^*$ of finite binary sequences is countable.

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

T3.22 Let A and A_i for $i \in \mathbb{N}$ be countable sets.
i) For any $n \in \mathbb{N}$ A^n (n-tuples over A) is countable
ii) The union $\bigcup_{i \in \mathbb{N}} A_i$ of a countable list of countable sets is countable
iii) The set A^* is countable

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

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

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

Cor 3.24 There are uncomputable functions $\mathbb{N} \to \{0,1\}$

Number of subgroups of $\mathbb{Z}_n$: $J(n)$, $n = p_1^{e_1} \cdot p_2^{e_2} \cdot (\dots)$
$J(n) = (e_1+1)(e_2+1) \cdot (\dots)$

Find zerodivisors of $F[x]_{m(x)}$ / $\langle \mathbb{Z}_n, \oplus, \odot \rangle$
1. factor $m(x)$/n 2. all multiples of the factors (not 0)

Find generators of $\mathbb{Z}_n / \mathbb{Z}_n^*$:
1. find $|\mathbb{Z}_n/\mathbb{Z}_n^*| = n/\varphi(n)$ 2. factor n and brute force elements (no efficient way except order is prime)

Find units: 1. find zerodivisors 2. strike 0 3. list remaining elements 4. check with $\varphi(n)$

Chapter 4 Number Theory

D 4.1 For $a,b \in \mathbb{Z}$ we say that a divides b den. $a|b$ if $\exists c \in \mathbb{Z}$ $b = ac$. a is called a divisor of b, b is a multiple of a. If $a \neq 0$ it is called the quotient when b is divided by a and we write $c = \frac{b}{a}$ or $c = b/a$.

T 4.1 $a,d \in \mathbb{Z}, d \neq 0$ there exist unique integers q and r satisfying $a = dq + r$ and $0 \le r < |d|$

D 4.2 $a,b \in \mathbb{Z}$ (not both 0) $d \in \mathbb{Z}$ is called a greatest common divisor of a and b if d divides both a and b and if every common divisor a and b divides d
i.e. if $d|a \wedge d|b \wedge (\forall d' \ d'|a \wedge d'|b \to d'|d)$

D 4.3 The greatest common divisor of a and b is the unique positive greatest common divisor den. $\gcd(a,b)$.
If $\gcd(a,b) = 1$ a and b are called relatively prime.

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

D4.4 $a,b \in \mathbb{Z}$ the ideal generated by a and b denoted (a,b) is the set $(a,b) := \{ua + vb \mid u,v \in \mathbb{Z}\}$. The ideal generated by a single integer is analogous.

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

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

C4.5 $a,b \in \mathbb{Z}$ (not both 0), there exist $u,v \in \mathbb{Z}$ such that $\gcd(a,b) = ua + vb$

D4.5 The least common multiple l of two positive integers a and b denoted $\mathrm{lcm}(a,m)$ is the common multiple of a and b which divides every common multiple of a and b i.e.
$a|l \wedge b|l \wedge (a|c \wedge b|c \to l|c)$

D4.6 A positive integer is called prime if the only positive divisors of p are 1 and n. An integer greater than 1 that is not a prime is called composite.

T4.6 Every positive integer can be written uniquely (up to the order) as a product of primes.

D4.8 For $a,b,m \in \mathbb{Z}$ with $m \ge 1$, we say that a is congruent to b modulo m if m divides $a-b$ den. $a \equiv b \pmod m$ or $a \equiv_m b$ i.e.
$a \equiv_m b \overset{def}{\iff} m \mid (a-b)$.

L4.13 For any $m \ge 1$ $\equiv_m$ is an equivalence relation on $\mathbb{Z}$

L4.14 $a \equiv_m b$, $c \equiv_m d \Rightarrow a+c \equiv_m b+d$ and $ac \equiv_m bd$

C4.15 $f(x_1,\dots,x_k)$ multi-variate polynomial in k variables with integer coefficients and $m \ge 1$. If $a_i \equiv_m b_i$ for $1 \le i \le k$ then $f(a_1,\dots,a_k) \equiv_m f(b_1,\dots,b_k)$

L4.16 $a,b,m \in \mathbb{Z}, m \ge 1$
i) $a \equiv_m R_m(a)$ ii) $a \equiv_m b \iff R_m(a) = R_m(b)$

C4.17 Same requirements as in C4.15. Then $R_m(f(a_1,\dots,a_k)) = R_m(f(R_m(a_1),\dots,R_m(a_k)))$.

L4.18 $ax \equiv_m 1$ has a solution $x \in \mathbb{Z}_m$ if and only if $\gcd(a,m) = 1$. The solution is unique.

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

T4.19 Let $m_1, m_2, \dots, m_r$ be pairwise relatively prime integers and let $M = \prod_{i=1}^r m_i$. For every list $a_1,\dots,a_r$ with $0 \le a_i < m_i$ for $1 \le i \le r$ the system of congruence equations

$$x \equiv_{m_1} a_1$$
$$(\dots)$$
$$x \equiv_{m_r} a_r$$

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

Solution $x = R_M\left(\sum_{i=1}^r a_i M_i N_i\right)$ where $M_i N_i \equiv_{m_i} 1$.

Diffie-Hellman Key-Agreement

public parameters: prime p, basis g

Alice		Bob
select x_A at random from $\{0,\dots,p-2\}$		select x_B at random from $\{0,\dots,p-2\}$
$y_A := R_p(g^{x_A})$	$\xrightarrow{y_A}$ $\xleftarrow{y_B}$	$y_B := R_p(g^{x_B})$
$k_{AB} := R_p(y_B^{x_A})$		$k_{BA} := R_p(y_A^{x_B})$

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

A code C is t-error correcting if there exists E and D with $C = \mathrm{Im}(E)$ where D is t-error correcting.

T 5.41 A code C with minimum distance d is t-error correcting iff. $d \ge 2t+1$.

T 5.42 $\mathcal{A} = GF(q)$, $\alpha_0 \cdots \alpha_{n-1}$ arbitrary & distinct $\in \mathcal{A}$
$E((a_0 \cdots a_{k-1})) = (a(\alpha_0) \cdots a(\alpha_{n-1}))$ where $a(x)$ is the polynomial
$a(x) = a_{k-1}x^{k-1} + (\dots) + a_1 x + a_0$.
This code has minimum distance $n-k+1$.

Chapter 5: Algebra

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

D5.2 An algebra (or algebraic structure or Ω-algebra) is a pair $\langle S; \Omega \rangle$ where S is a set (the carrier of the algebra) and $\Omega = (\omega_1, \dots, \omega_n)$ is a list of operations on S.

D5.3 A left/right neutral element (or identity element) of an algebra $\langle S; * \rangle$ is an element $e \in S$ such that $e * a = a$ / $a * e = a$ for all $a \in S$. If $e * a = a * e = a$ for all $a \in S$ then e is simply called neutral element.

L5.1 If $\langle S; * \rangle$ has both a left and a right neutral element, then they are equal. In particular $\langle S; * \rangle$ can have at most one neutral element.

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

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

D5.6 A left/right inverse element of an element a in an algebra $\langle S; *, e \rangle$ with neutral element e is an element $b \in S$ such that $b * a = e$ / $a * b = e$. If $b * a = a * b = e$ then b is simply called an inverse of a.

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

D5.7 A group is an algebra $\langle G; *, \hat{\ }, e \rangle$ satisfying the following axioms:
- G1: $*$ is associative
- G2: e is a neutral element: $a * e = e * a = a$ for all $a \in G$
- G3: Every $a \in G$ has an inverse element $\hat{a}$, i.e., $a * \hat{a} = \hat{a} * a = e$.

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

L5.3 For a group we have for all $a, b, c \in G$:
i) $\hat{(\hat{a})} = a$ ii) $\widehat{a*b} = \hat{b} * \hat{a}$
iii) $a * b = a * c \Rightarrow b = c$
iv) $b * a = c * a \Rightarrow b = c$
v) The equation $a * x = b$ has a unique solution x for any a and b. So does the equation $x * a = b$.

D5.9 The direct product of n groups $\langle G_1; *_1 \rangle, (\dots), \langle G_n; *_n \rangle$ is the algebra
$\langle G_1 \times (\dots) \times G_n; * \rangle$ where the $*$ operation is component-wise.

L5.4 $\langle G_1 \times (\dots) \times G_n; * \rangle$ is a group, where the neutral element and the inversion operation are component-wise in the respective groups.

D5.10 For two groups G and H, a function $\psi: G \to H$ is called a group homomorphism, if for all a and b, $\psi(a * b) = \psi(a) * \psi(b)$. If ψ is bijective, then it is called an isomorphism, and we say that G and H are isomorphic and write $G \simeq H$.

L5.5 A group homomorphism ψ satisfies:
(i) $\psi(e) = e'$
(ii) $\psi(\hat{a}) = \widehat{\psi(a)}$

D5.11 A subset $H \subseteq G$ of a group $\langle G; *, \hat{\ }, e \rangle$ is called a subgroup of G if $\langle H; *, \hat{\ }, e \rangle$ is a group, i.e. if H is closed with respect to all operations:
(1) $a * b \in H$ for all $a, b \in H$
(2) $e \in H$
(3) $\hat{a} \in H$ for all $a \in H$

D5.12 Let G be a group and let a be an element of G. The order of a, den. $\mathrm{ord}(a)$, is the least $m \geq 1$ such that $a^m = e$, if such an m exists, and $\mathrm{ord}(a)$ is said to be infinite otherwise, written $\mathrm{ord}(a) = \infty$
self-inverse: $\hat{a} = a$

L5.6 In a finite group G, every element has a finite order.

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

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

D5.15 A group generated by an element $g \in G$ is called cyclic, and g is called a generator of G.

T5.7 A cyclic group of order n is isomorphic to $\langle \mathbb{Z}_n; \oplus \rangle$ (and hence abelian).

T5.8 Let G be a finite group and let H be a subgroup of G. Then the order of H divides the order of G, i.e. $|H|$ divides $|G|$.

C5.9 For a finite group G, the order of every elements divides the group order, i.e. $\mathrm{ord}(a)$ divides $|G|$ for every $a \in G$.

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

C5.11 A group of prime order is cyclic and in such a group every element except the neutral element is a generator.

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

D5.17 The Euler function $\varphi: \mathbb{Z}^+ \to \mathbb{Z}^+$ is defined as the cardinality of $\mathbb{Z}_m^*$:
$$\varphi(m) = |\mathbb{Z}_m^*|$$

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

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

C5.14 For all $m \geq 2$ and all a with $\gcd(a, m) = 1$
$$a^{\varphi(m)} \equiv_m 1$$
In particular, for every prime p and every a not divisible by p,
$$a^{p-1} \equiv_p 1$$

T5.15 The group $\mathbb{Z}_m^*$ is cyclic if and only if $m = 2, m = 4, m = p^e$, or $m = 2p^e$ where p is an odd prime and $e \geq 1$.

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

RSA:

Alice		Bob
Generate primes p and q		
$n = p \cdot q$		
$f = (p-1)(q-1)$		
select e		
$d \equiv_f e^{-1}$	$\xrightarrow{n, e}$	plaintext $m \in \{1, \dots, n-1\}$
		ciphertext
$m = R_n(y^d)$	$\xleftarrow{y}$	$y = R_n(m^e)$

DS.18 A **ring** $\langle R;+,-,0,\cdot,1\rangle$ is an algebra for which
(i) $\langle R;+,-,0\rangle$ is a commutative group
(ii) $\langle R;\cdot,1\rangle$ is a monoid
(iii) $a(b+c)=(ab)+(ac)$ and $(b+c)a=(ba)+(ca)$ for all $a,b,c\in R$
A ring is called **commutative** if multiplication is commutative ($ab=ba$).

LS.17 For any ring $\langle R;+,-,0,\cdot,1\rangle$ and for all $a,b\in R$,
(i) $0a=a0=0$
(ii) $(-a)b=-(ab)$
(iii) $(-a)(-b)=ab$
(iv) if R is non trivial (i.e has more than one element), then $1\neq 0$.

DS.19 The **characteristic** of a ring is the order of 1 in the additive group if it is finite, and otherwise the characteristic is defined to be 0 (not ∞).

DS.20 An element of a ring R is called a **unit** if u is invertible, i.e. $uv=vu=1$ for some $v\in R$. The inverse is unique. The set of units of R is denoted R^*.

LS.18 For a ring R R^* is a multiplicative group (the group of units of R).

In the following: R commutative ring

DS.21 For $a,b\in R$ with $a\neq 0$ we say that **a divides b**, den. $a\mid b$, if there exists $c\in R$ such that $b=ac$. In this case, a is called a **divisor** of b and b is called a **multiple** of a.

LS.19 In any commutative ring,
(i) $a\mid b \wedge b\mid c \Longrightarrow a\mid c$
(ii) $a\mid b \Longrightarrow a\mid bc$ for all c
(iii) $a\mid b \wedge a\mid c$ then $a\mid(b+c)$

DS.22 $a,b\in R$ (not both 0) **greatest common divisor** (see D 4.3)

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

DS.24 An **integral domain** is a (nontrivial) commutative ring without zerodivisors: $\forall a\forall b\,(ab=0\rightarrow a=0 \vee b=0)$.

LS.20 In an integral domain, if $a\mid b$ then c with $b=ac$ is unique den. by $c=\frac{b}{a}$ or $c=b/a$ and called **quotient**.

DS.25 A **polynomial** $a(x)$ over a commutative ring R in the indeterminate x is a formal expression of the form $a(x)=a_dx^d+(\dots)+a_1x+a_0$ for some $d\in\mathbb{Z}$, $d\geq 0$ with $a_i\in R$. The **degree** of $a(x)$, den. $\deg(a(x))$, is the greatest i for which $a_i\neq 0$. 0 has degree **minus infinity**. $R[x]$ den. the set of polynomials (in x) over R.

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

LS.22 (i) If D is an integral domain, then so is $D[x]$
(ii) The units of $D[x]$ are the constant polynomials that are units of D: $D[x]^*=D^*$

DS.6 A **field** is a nontrivial commutative ring F in which every nonzero element is a unit, i.e., $F^*=F\setminus\{0\}$

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

TS.24 A field is an integral domain.

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

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

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

TS.25 Let F be a field. For any $a(x)$ and $b(x)\neq 0$ in $F[x]$ there exist a unique $q(x)$ (the **quotient**) and a unique $r(x)$ (the **remainder**) such that
$$a(x)=b(x)\cdot q(x)+r(x) \text{ and } \deg(r(x))<\deg(b(x))$$

LS.28 Polynomial evaluation is compatible with the ring operations:
- $c(x)=a(x)+b(x)\Longrightarrow c(\alpha)=a(\alpha)+b(\alpha)$
- $c(x)=a(x)\cdot b(x)\Longrightarrow c(\alpha)=a(\alpha)b(\alpha)$

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

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

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

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

LS.32 A polynomial $a(x)\in F[x]$ of degree at most d is uniquely determined by any $d+1$ values of $a(x)$, i.e. by $a(\alpha_1),\dots,a(\alpha_{d+1})$ for distinct $\alpha_1,\dots,\alpha_{d+1}\in F$.

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

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

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

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

LS.36 Multiplicative inverses for polynomials over fields modulo a polynomial.

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

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

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

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

DS.38 The **minimum distance** of an error correcting code C, den. $d_{min}(C)$, is the minimum of the Hamming distance between any two codewords.

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

DS.40 A decoding function D is t-error-correcting for encoding function E if for any $(a_0\cdots a_{k-1})$
$D((r_0\cdots r_{n-1}))=(a_0\cdots a_{k-1})$ for any $(r_0\cdots r_{n-1})$ with H. distance at most t from $E((a_0\cdots a_{k-1}))$.