Discrete Maths HS24 / cs.shivi.io

1 Propositional Logic

1.1 Basics

1.1.1 Basic Equivalences (Lemma 2.1)

1. **Idempotence:** $A \wedge A \equiv A$ and $A \vee A \equiv A$
2. **Commutativity:** $A \wedge B \equiv B \wedge A$ and $A \vee B \equiv B \vee A$
3. **Associativity:** $(A \wedge B) \wedge C \equiv A \wedge (B \wedge C)$ and $(A \vee B) \vee C \equiv A \vee (B \vee C)$
4. **Absorption:** $A \wedge (A \vee B) \equiv A$ and $A \vee (A \wedge B) \equiv A$
5. **1st Distr. Law:** $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$
6. **2nd Distr. Law:** $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$
7. **Double Neg.:** $\neg\neg A \equiv A$
8. **De Morgan:** $\neg(A \wedge B) \equiv \neg A \vee \neg B$ and $\neg(A \vee B) \equiv \neg A \wedge \neg B$

1.1.2 Logical Consequence

$F \vDash G$ is a **statement**. This statement is true if for all truth assignments $F \Rightarrow G$.

1.2 Tautologies and Satisfiability

Tautology: A formula F (denoted $\top$ or $\vDash F$) is a "tautology" (or valid) or valid if it's underlying formula resolves to true for any and all interpretations.

Satisfiable: A formula F is "satisfiable" if it's underlying formula can be made true for some arbitrary interpretation.

- **L2.2** F is tautology iff $\neg F$ is unsat.
- **L2.3** $F \to G$ is tautology iff $F \vDash G$.
  - $(\Rightarrow)$: Assume $F \to G \equiv \top$. Then when F is true G MUST be true, hence $F \vDash G$
  - $(\Leftarrow)$: Assume $F \vDash G$. Then F is true but G is false can't exist, hence $F \to G \equiv \top$.

2 Predicate Logic

Definition: A "k-ary" predicate P on a universe U is a function: $U^k \to \{0,1\}$.

2.1 Quantifiers

- $\forall P(x)$ means $P(x)$ is true for all $x \in U$.
- $\exists P(x)$ means $P(x)$ is true for at least one $x \in U$.

Example: $\forall x((P(x) \wedge Q(x) \to (P(x) \vee Q(x))) \equiv \top$

2.2 Useful Rules

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

3 Proof Patterns

3.1 Proof of Implications

3.1.1 Composition of Implications

L2.5: $(A \Rightarrow B) \wedge (B \Rightarrow C) \vDash A \Rightarrow C$

3.1.2 Direct Proof of an Implication

Assume S and show $S \Rightarrow T$.

3.1.3 Indirect Proof of an Implication

Show the contrapositive implication, i.e. $\neg B \Rightarrow \neg A \vDash A \Rightarrow B$. **(L2.6)**

3.2 Proof of Statements

3.2.1 Modus Ponens

Prove S by: 1. Find and prove R 2. Prove $R \Rightarrow S$

L2.7: $A \wedge (A \Rightarrow B) \vDash B$

3.2.2 Case Distinction

Prove S by: 1. Finding finite list of "cases" $A_1, A_2, \ldots, A_k$ 2. Showing at least one of the A_i is true: $A_1 \vee A_2 \vee \ldots \vee A_k$ and 3. Showing $A_i \Rightarrow S$ for $i = 1, \ldots, k$. Note that for $k = 1$ we are doing Modus Ponens...

L2.8: $(A_1 \vee \ldots \vee A_k) \wedge (A_1 \Rightarrow B) \wedge \ldots \wedge (A_k \Rightarrow B) \vDash B$

3.2.3 Proofs by Contradiction

Prove S by: 1. Find T and show $\neg T$ 2. Show that $\neg S \Rightarrow T$ (if S were false we get a wrong/contradictory result).

L2.9: $(\neg A \Rightarrow B) \wedge \neg B \vDash A$

3.3 Existence Proofs

Effectively show that there exists an assignment of parameters from a parameter space $x \in \mathcal{X}$ such that the statement with that assignment becomes true, i.e $\exists x \in \mathcal{X}(S_x)$.

Constructive proof provides a concrete example. **Non-Constructive** proof shows existence by proving otherwise.

3.3.1 Pigeonhole Principle

If a set of n objects is partitioned into $k < n$ sets, the at least one of those sets contains $\lceil \frac{n}{k} \rceil$ objects.

3.3.2 Proof by Conterexample

Obvious but... $\exists x \in \mathcal{X}(\neg S_x)$.

3.4 Proof by Induction

Meant to show $\forall n P(n)$. Proof by 1. Prove basis step $P(0)$ then 2. Show $P(n) \Rightarrow P(n+1)$.

Thm2.11: $P(0) \wedge \forall n(P(n) \to P(n+1)) \Rightarrow \forall n P(n)$.

4 Set Theory

A set is a new mathematical object which is defined by a single operation: the membership predicate ($x \in S$ or $x \notin S$).

Equality: $A = B \Leftrightarrow \forall x(x \in A \leftrightarrow x \in B)$.

4.1 Meta Operations

- $A \subseteq B \Leftrightarrow \forall x(x \in A \to x \in B)$
- $A = B \Leftrightarrow (A \subseteq B) \wedge (B \subseteq A)$
- $A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$ (transitivity)
- $A \cup B = \{x \mid x \in A \vee x \in B\}$
- $A \cap B = \{x \mid x \in A \wedge x \in B\}$
- $B \setminus A = \{x \in B \mid x \notin A\}$

4.2 Laws (Theorem 3.4)

- **Idempotence**, **Commutativity**, **Associativity**, **Absorption**, **Distribution**
- **Consistency:** $A \subseteq B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B$

4.3 Empty Set

$A = \emptyset \Leftrightarrow \forall x \neg(x \in A)$

- **L3.5: Uniqueness of emptyset**
  - Let $\emptyset$ and $\emptyset'$ be arbitrary emptysets. Now show using definition of equality that $\emptyset \subseteq \emptyset'$ and vice versa (both are vacuously true)...
- **L3.6: Emptyset is subset of all sets**, i.e $\forall A(\emptyset \subseteq A)$.
  - By contradiction: $\neg(\emptyset \subseteq A) \Leftrightarrow \neg\forall x(x \in \emptyset \to x \in A) \Leftrightarrow \exists x \neg(\neg(x \in \emptyset) \vee x \in A) \Leftrightarrow \exists x(x \in \emptyset) \wedge \exists x \neg(x \in A) \Rightarrow \exists x(x \in \emptyset)$

4.4 Meta Sets

- **Powerset:** $\mathcal{P}(A) = \{S \mid S \subseteq A\}$
  - $|\mathcal{P}(A)| = 2^{|A|}$
- **Cartesian product:** $A \times B = \{(a,b) \mid a \in A \wedge b \in B\}$
  - $|A \times B| = |A| \cdot |B|$

5 Relations

A (binary) relation is a subset of $A \times B$: $\rho \subseteq A \times B$. ρ is called a relation "on A" is $A = B$. We often write $a \rho b$ instead of $(a,b) \in \rho$.

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

Possible relations: There are 2^{n^2} relations on a set, since $n^2 = |A^2|$ and each of these pairs can be in/excluded.

Inverse Relation: $\hat{\rho} = \{(b,a) \mid (a,b) \in \rho\}$. Alternatively: $b \hat{\rho} a \Leftrightarrow a \rho b$

Composition of relations: $\rho \circ \sigma = \{(a,c) \mid \exists b(a \rho b \wedge b \sigma c)\}$

5.1 Types of Relations

- **Reflexive (D3.13):** $\forall a \in A(a \rho a)$, i.e. $\mathrm{id} \subseteq \rho$. *Examples:* $\leq, \geq, (\mid$ on $\mathbb{Z} \setminus \{0\})$, *Non Examples:* $<, >$
  - In a graph, we have self loops for all nodes.
  - **Irreflxive (D3.14):** $\rho \cap \mathrm{id} = \emptyset$
- **Symmetric (D3.15):** $a \rho b \Leftrightarrow b \rho a$ or $\rho = \hat{\rho}$
  - **Antisymmetric (D3.16):** $a \rho b \wedge b \rho a \Rightarrow a = b$ or $\rho \cap \hat{\rho} \subseteq \mathrm{id}$. *Examples:* $\leq, \geq, (\mid$ on $\mathbb{N}$ but not on $\mathbb{Z})$
    - In a graph: no cycle of length 2.
  - **L3.9:** ρ is transitive iff $\rho^2 \subseteq \rho$.
    - *"if $(\Leftarrow)$:"* Assume $\rho^2 \subseteq \rho$ i.e $a \rho^2 b \Rightarrow a \rho b$. If $a \rho b \wedge b \rho c \Rightarrow a \rho^2 c$ but by assumption $\Rightarrow a \rho c$ which exactly is transitivity.
    - *"only if $(\Rightarrow)$:"* Assume ρ is transitive. Then $a \rho^2 b \Rightarrow \exists c(a \rho c \wedge c \rho b)$. By transitivity: $a \rho b$. Hence $\rho^2 \subseteq \rho$.
  - **Transitive Closure (D3.18):** $\rho^* = \bigcup_{n \in \mathbb{N} \setminus \{0\}} \rho^n$. i.e reachability with arbitrary finite steps.
    - $p^n \subseteq p$. Proof by induction:
      - Base Case: $p^1 \subseteq p$
      - Induction Step: $(a \rho^{k+1} c \Rightarrow a \rho^k b \wedge b \rho c \Rightarrow a \rho b \wedge b \rho c$ (By I.H) $\Rightarrow a \rho c) \Rightarrow \rho^{k+1} \subseteq \rho$

5.1.1 Equivalence Relation

- **Equivalence Relationship (D3.19):** Relation that's 1) reflexive 2) symmetric and 3) transitive.
- **Equivalence Class (D3.20):** Let θ be an equivalence relation on A. The equivalence class of a is defined as: $[a]_\theta = \{b \in A \mid a \theta b\}$. *Trivial Examples:* $[a]_\theta = A$ if $\theta = A \times A$, $[a]_\theta = \{a\}$ if $\theta = \mathrm{id}$.
- **L3.10:** $\theta = \theta_1 \cap \theta_2$ and θ is an equivalence relation. Trivial, since each pair in theta inherits reflexivity, symmetry and transitivity from $\theta_{1 \vee 2}$.
- **Partition (D3.21):** Partition on a set A: $\{S_i \mid i \in \mathcal{I}\}\left((S_i \cap S_j = \emptyset \text{ for } i \neq j) \wedge \bigcup_{i \in \mathcal{I}} S_i = A\right)$
- **Quotient Set (D3.22):** Set of equivalence classes denoted by: $A/\theta = \{[a]_\theta \mid a \in A\}$. Also called $A \bmod \theta$.
  - **Thm3.11:** A/θ is a partition of A.

5.1.2 Posets

- **Partial Order Relation (D3.23):** Relation that's 1) reflexive 2) antisymmetric and 3) transitive. Denoted by $\preceq$ i.e $(A, \preceq)$ *Examples:* $\leq, \geq$. *Non Examples:* $<, >$ (since not reflexive)
  - $a \prec b \Leftrightarrow a \preceq b \wedge a \neq b$
  - **D3.24:** a, b are "comparable" if $a \preceq b \vee b \preceq a$, else "incomparable".
  - **Totally ordered (D3.25):** If any two elements are comparable then A is totally ordered.

5.1.2.1 Hasse Diagrams

- **Cover (D3.26):** a covers b if $a \prec b$ and $\neg(\exists c(a \prec c \wedge c \prec b))$.
- **Hasse Diagram (D3.27):** A digraph of a finite poset where $a \to b$ iff b covers a

5.1.2.2 Lexicographic Order

Let $(A; \preceq), (B; \sqsubseteq)$. Now we define $(a_1, b_1) \leq (a_2, b_2) \Leftrightarrow a_1 \preceq a_2 \wedge b_1 \sqsubseteq b_2$.

- **Thm3.12:** $(A; \preceq) \times (B; \sqsubseteq)$ is a poset.
- **Lexicographic Order (Thm 3.13):** $(a_1, b_1) \underset{\text{lex}}{\leq} (a_2, b_2) \Leftrightarrow a_1 \prec a_2 \vee (a_1 = a_2 \wedge b_1 \sqsubseteq b_2)$ is also a poset.

5.1.2.3 Special Elements

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

1. a is minimal[maximal] of A if $\neg(\exists b \in A(b \prec a[b \succ a]))$ *tldr: no element of A is strictly smaller/larger than a. Comparability with all elements is not required. There can be many minimal/maximal elements.*
2. a is least [greatest] element of A if $\forall b \in A(a \preceq b[a \succeq b])$ *tldr: comparable to all elements of A and smallest/largest. The element is unique if it exists.*
3. a is lower [upper] element of S if $\forall b \in S(a \preceq b[a \succeq b])$ *tldr: comparable to all elements of S and below/above them. There can be many or no lower/upper elements.*
4. a is 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. *tldr: the largest/smallest element that bounds S from below/above.*

Well Ordered (D3.30): A poset is well-ordered if it is totally ordered and every non-empty subset of A has a least element.

5.1.2.4 Meet, Join, Lattices

- **Meet:** If the set $\{a,b\}$ has a glb, it's called the meet. Denoted by $a \wedge b$.
- **Join:** If the set $\{a,b\}$ has lub, it's called the join. Denoted by $a \vee b$.
- **Lattice:** A poset where each pair of elements has a meet and lattice is called lattice.

6 Functions

A function $f : A \to B$ from domain to codomain is a relation with properties:

1. Totally defined: $\forall a \in A \exists b \in B(b = f(a))$, i.e each element maps to atleast one element.
2. Well defined: $\forall a \in A \forall b, b' \in B(b = f(a) \wedge b' = f(a) \Rightarrow b = b')$, i.e each element maps to maximally one element.

If only the 2nd condition holds, we call the function a partial function.

There are $|B|^{|A|}$ possible functions $A \to B$.

6.1 Image/Preimage

- **Image/Range:** Let $f : A \to B, S \subseteq A$ then $f(S) = \{f(a) \mid a \in S\}$. $Y = f(A), Y \subseteq B, Y = \mathrm{Im}(f)$.
- **Preimage:** $T \subseteq T, f^{-1}(T) = \{a \in A \mid f(a) \in T\}$

6.2 Function Types

- **Injective (1to1):** $a \neq b \Rightarrow f(a) \neq f(b)$, i.e unique mapping.
- **Surjective (onto):** $\mathrm{Im}(f) = B$, i.e. each element in B can be reached.
- **Bijective:** If both injective and surjective, i.e an invertible function defined for all elements of B.

7 Un/Countability

1. $A \sim B$ if there exists a bijection $A \to B$
2. $A \preceq B$ if 1) $A \sim C \wedge C \subseteq B$ or 2) there exists an injection $A \to B$
3. If $A \preceq \mathbb{N}$ then A is countable. Otherwise uncountable.

L3.15:

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

Thm 3.17: A is countable iff A is finite or $A \sim \mathbb{N}$.

7.1 Countable Sets

- **Finite bit sequences:** $\{0,1\}^* \mapsto \text{decimal}('1' + \text{seq})$
- **Pairs of $\mathbb{N}$:** 1) $f : \mathbb{N} \to \mathbb{N}^2, f(n) = (k,m), k + m = t - 1 \wedge m = n - \binom{t}{2}$ or 2) $(a,b) \mapsto 0^{|a|} \| 1 \| a \| b$
- **Rational numbers:** $\mathbb{Q} \preceq \mathbb{Z} \times \mathbb{N} \wedge \mathbb{Z} \sim \mathbb{N} \Rightarrow \mathbb{Q} \sim \mathbb{N}$.

Thm 3.22:

1. A countable $\Rightarrow A^n$ countable.
2. $\bigcup_{i \in \mathbb{N}} A_i$ is countable if A_i is countable.

3. A^* is countable if A is countable.

7.2 Uncountable Sets

- **Infinite bit sequences or set of functions $\mathbb{N} \to \{0,1\}$:** By cantor's diagonalization...

7.3 How to Approach

Intuition: Understand what the set represents. Determine wether it's countable/uncountable. Let A be the set which is uncountable.

Proof (Uncountable):

1. Find an injection: $f : \{0,1\}^\infty \to A$ (we'll prove injectivity later)
2. Show f is a function, i.e 1) each elements gets mapped to at least one element 2) each element gets mapped to maximally one element. 3) Do you actually map to A and not somewhere else?
3. Proving injectivity: 1) $a, b \in \{0,1\}^\infty, a \neq b \Rightarrow \ldots \Rightarrow f(a) \neq f(b)$ or 2) $f(a) = f(b) \Rightarrow \ldots \Rightarrow a = b$
4. We have $\{0,1\}^\infty \preceq A$ but we need to add "for formality" that $A \not\preceq \mathbb{N}$. We can argue this via transitivity since $\{0,1\}^\infty \not\preceq \mathbb{N}$.

Tricks:

- **Complement Trick:** To show A is uncountable find B also uncountable such that $A \subseteq B$. Now show that $B \setminus A$ is countable. Sound since by contradiction if A were countable, $A \cup (B \setminus A) = B$ LHS would be countable but RHS isn't.
- **Prime Factorization:** e.g. $f : \mathbb{N}^2 \to N, f : (a,b) \mapsto 2^a 3^b$. f is injective since each number can be uniquely factored into primes by the FTA...

8 Number Theory

- $a \mid b$ if $\exists c(ac = b)$. Every non-zero int divides 0. $1, -1$ divide all integers.
- **Thm 4.1 (Euclid):** $\forall a \in \mathbb{Z} \wedge d \neq 0 \exists q \exists r (a = dq + r \wedge 0 \leq r < |d|)$

8.1 GCD, LCM

GCD (D4.2): $\gcd(a,b) = d$ if d divides both $a \wedge b$ and is the greatest in terms of the divisibility relation.

Relative Prime (D4.3): Two numbers are rel. prime if $\gcd(a,b) = 1$.

- **L4.2:** $\gcd(a, b - xa) = \gcd(a,b)$. Proof by expanding into definition of $\mid$ and showing $d_{\text{LHS}} = d_{\text{RHS}}$.
- $\gcd(a,b) = \gcd(m, R_m(n))$

Ideal (D4.4): $(a,b) = \{ua + vb \mid u, a \in \mathbb{Z}\}$

- **L4.3:** $\exists d : (a,b) = (d)$.
  - *Show* $(d) \subseteq (a,b)$: Trivially holds since d is smallest in (a,b) then $(d) \subseteq (a,b)$
  - *Show* $(a,b) \subseteq (d)$: Let $c \in (a,b) \Rightarrow c = qd + r \Rightarrow r = c - qd$ but $0 \leq r < d$ and d is smallest in $(a,b) \Rightarrow r = 0 \Rightarrow c = qd \Rightarrow c \in (d)$.
- **L4.4:** $(a,b) = (d) \Rightarrow d = \gcd(a,b)$
  - $d \in (a,b) \Leftrightarrow d = ua + vb$. Any common divisor c of a and b must $\mid d$. Since $a, b \in (d)$ and transitivity of $\mid \Rightarrow c \mid d$, d is the gcd.

LCM (D4.5): $\text{lcm}(a,b) = l$ if both $a \wedge b$ divide l and it is the least in terms of the divisibility relation.

8.2 Fundamental Theorem of Arithmetic (FTA)

Prime (D4.6): A positive integer $p > 1$ is prime if it's only positive divisors are $1 \wedge p$. $\neg$ prime = composite.

FTA (Thm 4.6): TLDR: Every number can be uniquely factored intro a product of primes.

Alternate GCD and LCM definition:

- Let $a = \prod_i p_i^{e^i}$ and $b = \prod_i p_i^{f^i}$
- $\gcd(a,b) = \prod_i p_i^{\min(e^i, f_i)}$ and $\text{lcm}(a,b) = \prod_i p_i^{\max(e^i, f_i)}$
- $\Rightarrow \gcd(a,b) \cdot \text{lcm}(a,b) = ab$

8.3 Modular Arithmetic

$a \equiv_m b \Leftrightarrow m \mid (a - b)$

L4.14: Compatibility with Arithmetic Operations

If $a \equiv_m b \wedge c \equiv_m d$, then:

1. $a + c \equiv_m b + d$
   - $m \mid (a - b) \wedge m \mid (c - d) \Rightarrow m \mid ((a - b) + (c - d)) \Rightarrow m \mid ((a + c) - (b + d)) \Rightarrow a + c \equiv_m b + d$
2. $ac \equiv_m bd$
   - $ac = (b + km)(d + lm) = bd + b(lm) + k(dm) + klm^2 = bd + m(bl + kd + klm) \Rightarrow m \mid (ac - bd) \Rightarrow ac \equiv_m bd$

- **C4.15:** $a_i \equiv_m b_i \Rightarrow f(a_1, \ldots, a_k) \equiv_m f(b_1, \ldots, b_k)$ if f is a multivariate polynomial with integer coeffcients.

- **L4.16**
  - $a \equiv_m R_m(a)$
  - $a \equiv_m b \Leftrightarrow R_m(a) = R_m(b)$
  - C4.17: $R_m(f(a_1, \ldots, a_k)) = R_m(f(R_m(f_1), \ldots, R_m(f_k)))$

L4.18: Multiplicative Inverse

- $ax \equiv_m 1$ has a solution iff $\gcd(a, m) = 1$. The solution is unique.
- **Calculating Inverse using Extended GCD:**
  - Find x, y such that $ax + my = \gcd(a,m)$. If $\gcd(a,m) = 1$, then $ax \equiv_m 1$, so x is the inverse.
  - Example: Inverse of 5 modulo 11:
    1. $5x + 11y = 1 \Leftrightarrow R_{11}(5x + 11y) = R_{11}(1) \Leftrightarrow R_{11}(5x) = 1$
    2. Using Extended GCD: $x = -2 \equiv_{11} 9$, $y = 1$.
    3. $-2 + 11 = 9$. Therefore, $5^{-1} \equiv_{11} 9$.

Fermats little theorem and Eulers Theorem:

$\gcd(m,a) = 1 \Rightarrow R_m(a^b) = R_m\left(a^{R_{\varphi(m)}(b)}\right)$

Thm 4.19: CRT

- Given: $x \equiv_{m1} a_1, \ldots, x \equiv_{mr} a_r$.
- For relatively prime $m_1, \ldots, m_r$, let $M = m_1 \cdot \ldots \cdot m_r$.
- Let $M_i = \frac{M}{m_i} \Rightarrow M_i N_i \equiv_{mi} 1$. Find N_i, the multiplicative inverse using extended Euclidian algorithm.
- Solution: $x = R_M\left(\sum_{i=1}^r a_i M_i N_i\right)$

8.4 Diffie Hellman

DH is a key-exchange protocol leveraging the discrete logarithm problem for constructing one-way functions.

Alice	**insecure channel**	**Bob**
select x_A at random from $\{0, \ldots, p-2\}$		select x_B at random from $\{0, \ldots, p-2\}$
$y_A := R_p(g^{x_A})$		$y_B := R_p(g^{x_B})$
	y_A $\longrightarrow$	
	$\longleftarrow$ y_B	
$k_{AB} := R_p(y_B^{x_A})$		$k_{BA} := R_p(y_A^{x_B})$

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

Note that this protocol requires the group $\mathbb{Z}_p^*$.

9 Algebra

- **Operation** on set S is a function $S^n \to S$
- An **algebra** is a pair $\langle S; \Omega \rangle$ where S is the set and Ω is the list of operations of S.

9.1 Overview of Algebraic Structures

9.1.1 Properties

- **Addition:** A1: Closure, A2: Associative, A3: Identity, A4: Inverse, A5: Commutative
- **Multiplication:** M1: Closure, M2: Associative, M3: Distributive, M4: Commutative, M5: Identity, M6: No Zero Divisors, M7: Inverse

9.1.2 Structures

- **Monoid**: A: 1, 2, 3
- **Group**: A: 1, 2, 3, 4
- **Abelian Group (Commutative Group)**: A: 1, 2, 3, 4, 5
- **Ring**: A: 1, 2, 3, 4, 5, M: 1, 2, 3
- **Commutative Ring**: A: 1, 2, 3, 4, 5, M: 1, 2, 3, 4
- **Integral Domain**: A: 1, 2, 3, 4, 5, M: 1, 2, 3, 4, 5, 6
- **Field**: A: 1, 2, 3, 4, 5, M: 1, 2, 3, 4, 5, 6, 7

9.2 Monoids and Groups

- A **monoid** has 1) closure 2) associativity and 3) an identity.
- A **group** is a monoid with an 4) inverse.

9.2.1 Neutral Elements

D5.3: A left [right] neutral/identity element ($e \in S$): $e * a = a[a * e = a]$. If $e * a = a * e = a$ then e is the neutral element.

- **L5.1:** If LN and RN then LN = RN. Since $e * e' = e' \wedge e * e' = e \Rightarrow e = e'$

9.2.2 Associativity

D5.4: Associative means $a * (b * c) = (a * b) * c$.

9.2.3 Inverse Elements

D5.6: A left [right] inverse of a called b is such that $b * a = e[a * e = e]$. If $a * b = b * a = e$ we simply call it inverse.

- **L5.2:** If LI and RI then LI = RI. Proof: Let b be LI and c be RI. Then $b = b * e = b * (a * c) = (b * a) * c = e * c = c$.

- **Uniqueness of Inverse:** $a * b = a * b' = e \Rightarrow b * a * b = b * a * b' = b * e \Rightarrow b = b' = b$

9.2.4 Group Axioms

Group: $\langle G; *, \widehat{\ }, e \rangle$.

- **L5.3:** For any group we have:
  1. $\widehat{(\hat{a})} = a$
  2. $\widehat{a * b} = \hat{b} * \hat{a}$
  3. Left cancellation: $a * b = a * c \Rightarrow b = c$, Right cancellation: $b * a = c * a \Rightarrow b = c$
  4. $a * x = b \wedge x * a = b$ have both a unique solution for any x, a, b.

Minimal axioms:

- **G1:** associative, **G2′:** RN, **G3′:** RI
- First prove **G3** before proving **G2**!!!
- **G3:** $\hat{a} * a = (\hat{a} * a) * e = (\hat{a} * a) * \left(\hat{a} * \hat{\hat{a}}\right) = \hat{a} * \left(a * \left(\hat{a} * \hat{\hat{a}}\right)\right) = \hat{a} * \left((a * \hat{a}) * \hat{\hat{a}}\right) = \hat{a} * \left(e * \hat{\hat{a}}\right) = (\hat{a} * e) * \hat{\hat{a}})\hat{a} * \hat{\hat{a}} = e$
- **G2:** $a * e = a * (\hat{a} * a) = (a * \hat{a}) * a = e * a$

9.2.5 Group Structures

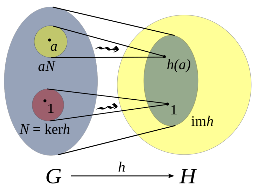
- **Direct Product (D5.9):** $\langle G_1 \times \ldots \times G_n; * \rangle$. $*$ is component wise.

9.2.6 Homomorphisms

D5.10: Let G, H be two groups. Let $\varphi : G \to H$. If we can have $\varphi(a *_G b) = \varphi(a) *_H \varphi(b)$ we have a group homomorphism. If φ is a bijection then we have a isomorphism.

L5.5: 1) $\varphi(e_G) = e_H$ and 2) $\varphi(\hat{a}) = \widehat{\varphi(a)}$

Note that φ need not be an injection, if the kernel of φ (= $\{a \in G \mid \varphi(a) = 1\}$) is non-zero, since then φ can't be injective.



9.2.6.1 How to prove isomorphism

1. Define mapping function which you suspect is an isomorphism φ.
2. Check if map is well defined. i.e maps to max one element
3. Check if map is totally defined. i.e maps to at least one element
4. Verify $\varphi(g) \in H \forall g \in G$. i.e image of φ is $\subseteq H$.
5. Check homomorphism: $\varphi(g_1 *_G g_2) = \varphi(g_1) *_H \varphi(g_2)$
6. Check injectivity: $\varphi(g_1) = \varphi(g_2) \Rightarrow g_1 = g_2$ or it's contrapositive.
7. Check surjectivity: Show that $\forall h \in H \exists g \in G(\varphi(g) = h)$
8. Conclude isomorphism

9.2.7 Subgroups

If $H \subseteq G$ and H itself satisfies all group properties then H is a subgroup of G. For any group $\{e\}$ and G are trivial subgroups.

9.2.7.1 Order

The order of a **group** is the number of elements. The order of an **element** $\text{ord}(a) = m \wedge m \geq 1 \Leftrightarrow a^m = e$. If $\neg(\exists \text{ ord}(a)) \Rightarrow \text{ord}(a) = \infty$. Naturally $\text{ord}(e) = 1$, $\text{ord}(a) = 2 \Rightarrow a^2 = e \Rightarrow a = a^{-1}$

L5.6: Each element of a finite group must have finite order.

- Since G is finite we must at some point have $a^r = a^s = b \wedge r < s$ by pigeon hole $\Rightarrow a^{s-r} = a^s * a^{-r} = b * b^{-1} = e \Rightarrow \exists x(x = s - r \wedge a^x = e)$.

It follows that $a^m = a^{R_{\text{ord}(a)}(m)}$

9.2.8 Cyclic Groups

D5.14: $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$. $\langle a \rangle$ is the smallest subgroup of G which contains a. Notice how $\langle a \rangle = \left\{e, a, a^2, \ldots, a^{\text{ord}(a)-1}\right\}$.

D5.15: If a group can be generated by an element, it's called cyclic. If g is a generator, so is g^{-1}.

- $\langle \mathbb{Z}_n; + \rangle$ is cycle for every n where 1 is a generator. The generators of the group are all $g \in \mathbb{Z}_n$ where $\gcd(g, n) = 1$.

Thm 5.7: A cyclic group of order n is alway isomorphic to $\langle \mathbb{Z}_n; + \rangle$ and hence commutative too.

9.2.9 Order of Subgroups

Thm 5.8, Lagrange Thm (!!!): $H \subseteq G \Rightarrow |H|$ divides $|G|$.

- **C5.9:** For every finite group, the order of its element divides the group order. i.e $\text{ord}(a)$ divides $|G|$ $\forall a \in G$.
- **C5.10:** $a^{|G|} = e \forall a \in G$ (for finite groups). Proof: $a^{|G|} = a^{k \cdot \text{ord}(a)} = (a^{\text{ord}(a)})^k = e^k = e$.
- **C5.11:** Every group of prime order is cycle and every element except e is a generator. Proof: Every subgroup divides $p \Rightarrow \text{ord}(g) = 1 \vee p$. $\text{ord}(g) = 1 \Rightarrow g = e$ otherwise any other element works.

9.2.10 Euler's Function and $\mathbb{Z}_m^*$

D5.16: $\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m \mid \gcd(a, m) = 1\}$, i.e a set of all coprime to m numbers in $\mathbb{Z}_m$.

D5.17: The Euler function is defined as $\varphi(m) = |\mathbb{Z}_m^*|$. Can be calculated by: $m = p_1^{e_1} \cdot \ldots \cdot p_k^{e_k} \Rightarrow \varphi(m) = (p_1^{e_1} - p_1(e_1 - 1)) \ldots \left(p_k^{e_k} - p_k^{e_k - 1}\right)$. E.g. $\varphi(60) = (2^2 - 2^1)(3 - 1)(5 - 1) = 16$.

Thm 5.13: $\langle \mathbb{Z}_m^*; \odot, ^{-1}, 1\rangle$ is a group.

C5.14 (Fermat, Euler): 1) $\forall m \geq 2 \wedge \gcd(a,m) = 1$ we have $a^{\varphi(m)} \equiv_m 1$. 2) For every prime p we have $a^{p-1} \equiv_p 1 \Leftrightarrow a^p \equiv_p a$.

Thm 5.15: The group $\mathbb{Z}_m^*$ is cyclic iff $m = 2, m = 4, m = p^e, m = 2p^e$, where $p \neq 2$ and is prime $\wedge\, e \geq 1$.

9.3 RSA

For RSA we need to know the following theorem following from Lagrange's theorem:

Thm 5.16:
- Let G be a finite group.
- Let $e \in \mathbb{Z}$ be relatively prime to $|G|$.
- The function $x \mapsto x^e$ is a bijection.
- The unique e-th root of y such that $x^e = y \Leftrightarrow x = y^d$ where d is the multiplicative inverse of e modulo $|G|$, i.e $ed \equiv_{|G|} 1$.
- Proof: 1) $ed = k \cdot |G| + 1$ 2) $(x^e)^d = x^{ed} = x^{k \cdot |G| + 1} = \left(x^{(|G|)^k}\right) \cdot x = x$.
- This means that $y \mapsto y^d$ is the inverse function of $x \mapsto x^e$.

Protocol:

Alice	**insecure channel**	**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 $m \in \{1, \dots, n-1\}$
$m = R_n(c^d)$	$\xleftarrow{c}$	ciphertext $c = R_n(m^e)$

The idea is as follows:
1. Let $n = p \cdot q$.
2. Let $f = |\mathbb{Z}_n^*| = (p-1)(q-1)$
3. Choose some e and calculate $d \equiv_f e^{-1}$ using Ext. Eucl. algorithm.
4. Make n, e public.
5. The message m can be encrypted by $m \mapsto c = R_n(m^e)$.
6. The decryption can be done by $c \mapsto m = R_n(c^d)$.

9.4 Rings and Fields

- A **ring** is an additive abelian group with 1) multiplicative closure 2) multiplicative associativity 3) distributivity
- A **commutative ring** is a ring with 4) commutativity
- An **integral domain** is a commutative ring with 5) a multiplicative identity and 6) no zero divisors
- A **field** is an integral domain with 7) multiplicative inverses

L5.17: For any ring $\langle R; +, -, 0, \cdot, 1\rangle$
1. $0a = a0 = 0$. Proof: $0 = -(a0) + a0 = -(a0) + a(0 + 0) = (-(a0) + a0) + a0 = 0 + a0 = a0$. $0a$ gets proven in a similar manner.
2. $(-a)b = -(ab)$. Proof: $(-a)b + ab = (-a + a)b = 0b = 0 \Rightarrow (-a)b = -(ab)$
3. $(-a)(-b) = ab$. Proof: $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$
4. If $|R| > 1 \Rightarrow 1 \neq 0$. Proof by contradiction: Let a, b be distinct elements. Then $a = a * 1 = a * 0 = 0 \wedge b = \ldots = 0 \Rightarrow a = b$ which contradicts our precondition.

Characteristic of a Ring (D5.19): Order of 1 in the additive group if finite, 0 otherwise. Hence the characteristic in the ring $\mathbb{Z}_m$ is 1 and in $\mathbb{Z}$ 0.

9.4.1 Units and Multiplicative Group

D5.20: An element of a ring $u \in R$ is called **unit if it's invertible**, i.e $\exists v \in R(uv = vu = 1)$, $v = u^{-1}$. The set of units is R^*.
- Examples: $\mathbb{Z}^* = \{1, -1\}, \mathbb{R}^* = \mathbb{R} \setminus \{0\}$, Gaussian Integers$^* = \{1, -1, i, -i\}$

L5.18: For a ring R, R^* is a multiplicative group.
- Proof: We need to show that $\forall u, v \exists y (y = (uv)^{-1}) \Rightarrow y = v^{-1}u^{-1}$. $1 \in R^*$ since $1 = 1^{-1}$. Associativity is inherited from R.

9.4.2 Divisors

D5.21: $\exists c \in R(b = ac) \Rightarrow a \mid b$. Where R is a commutative ring.

L5.19: 1) $\mid$ is transitive. 2) $a \mid b \Rightarrow a \mid (bc)$ 3) $a \mid b \wedge a \mid c \Rightarrow a \mid (b + c)$

D5.22: The GCD definition is identical as in number theory, just using the divides definition from above (L5.19).

9.4.3 Zero Divisors and Integral Domains

Zero Divisor (D5.23): $a \neq 0 \wedge \exists b (b \neq 0 \wedge ab = 0) \Rightarrow a \mid 0$. a is called a zerodivisor of that commutative ring.

Integral Domain (D5.24): An integral domain D is a non-trivial ($|D| > 1$) commutative ring without zerodivisors. *Examples:* $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, *Non Examples:* $\mathbb{Z}_m$ if m isn't prime, any element not relatively prime to m is a zerodivisor.

L5.20: In an ID $a \mid b \Rightarrow \exists c (b = ac)$ then that $c = \frac{b}{a}$ is unique. Proof: $0 = ac - ac' = a(c + -c') \Rightarrow c + -c' = 0 \Rightarrow c = c'$.

9.4.4 Polynomial Rings

Thm 5.21: For any commutative ring R, $R[x]$ is a commutative ring too.

L5.22: Let D be an ID, then:
1. $D[x]$ is an ID. Proof: If there were zerodivisors then for $p(x)q(x) = 0$ the polynomial coefficients would need to be zerodivisors, cause otherwise we'd never get $= 0$.
2. $\deg(ab) = \deg(a) + \deg(b)$. Proof: Similar to (1), since we don't have zerodivisors the highest degree can't simply disappear and hence must be present.
3. Units of $D[x]$ are constants that are units of D. i.e $D[x]^* = D^*$. Proof: We need to get a polynomial where only the constant coefficient is $= 1$, the others must $= 0$. Now since we don't have zerodivisors we can only have units by inheriting them from D.

9.4.5 Fields

D5.26: A **field** is a non-trivial commutative ring F where every non-zero element is a unit, i.e is invertible. *Examples:* $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. *Non Examples:* $\mathbb{Z}$, $R[x]$(for any arbitrary rings).

Thm 5.23: $\mathbb{Z}_p$ is a field iff p is prime.

Thm 5.24: A field is an integral domain. Proof: It suffices to show that a unit is not a zerodivisor. Assume $uv = 0 \Rightarrow v = 0$ since $v = 1v = u^{-1}uv = u^{-1}0 = 0$. Hence u is not a zerodivisor.

9.4.6 Polynomials over a Field

D5.27: A polynomial is called a **monic** if the leading coefficient is 1.

D5.28: A polynomial with degree ≥ 1 is **irreducible** if it is only divisible by constants or constant multiples of itself. Similar to primality.

D5.29: The monic polynomial of largest degree such that $g(x) \mid a(x) \wedge g(x) \mid b(x) \Rightarrow g(x) = \gcd(a(x), b(x))$.

9.4.7 Division in Fields

Thm 5.25: $a(x) = b(x) \cdot q(x) + r(x)$.

9.4.8 Roots

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

L5.29: For $\alpha \in F(a(\alpha) = 0 \Leftrightarrow (x - \alpha) \mid a(x))$
- $\Rightarrow$: Assume $a(\alpha) = 0$. Then $a(x) = (x - \alpha)q(x) + r(x)$ where $\deg(r(x)) < \deg(x - \alpha) = 1 \Rightarrow r(x)$ is a constant $\Rightarrow r = a(x) - (x - \alpha)q(x)$. Now if $x = \alpha \Rightarrow r = 0 - 0 \cdot q(\alpha) = 0$. Since $r = 0$ we know that $a(x) = (x - \alpha)q(x) \Rightarrow (x - \alpha) \mid a(x)$
- $\Leftarrow$: Assume $(x - \alpha) \mid a(x) \Rightarrow a(\alpha) = (\alpha - \alpha)q(\alpha) = 0 \Rightarrow \alpha$ is a root
- Note that this implies that an irreducible polynomial of degree ≥ 2 has no roots.

C5.30: A polynomial of degree 2 or 3 over a field is irreducible iff it has no root. Proof: A reducible polynomial has a factor of degree 1 and hence a root.

Thm 5.31: A non-zero polynomial $a(x) \in F[x]$ of degree d has atmost d roots.
- Proof: To show contradiction assume $a(x)$ has degree d but $e > d$ roots, then $\prod_{i=1}^{e} \mid a(x)$ by Lemma 5.29, but then becomes a polynomial of degree e instead.

9.4.9 Polynomial Interpolation

L5.32: A polynomial $a(x) \in F[x]$ of degree d can be uniquely determined by any $d + 1$ values (!!!) of $a(x_i)$ s.t. x_i are distinct.
- Proof by construction: Assume $\beta_i = a(\alpha_i)$ for $i \in [1, d+1]$
- $a(x) = \sum_{i=1}^{d+1} \beta_i u_i(x)$ where $u_i(x) = \frac{x - \alpha_1}{\alpha_i - \alpha_1} \cdot \ldots \cdot \frac{x - \alpha_{i-1}}{\alpha_i - \alpha_{i-1}} \frac{x - \alpha_{i+1}}{\alpha_i - \alpha_{i+1}} \cdot \ldots \cdot \frac{x - \alpha_{d+1}}{\alpha_i - \alpha_{d+1}}$
- $u_i(x)$ is well defined since $a_i - a_j \neq 0$ iff $i \neq j$ and hence is invertible. We also naturally agree with the given values. $a(x)$ has degree of at most d.
- Uniqueness: Assume $a \neq a' \wedge \in O(x^n)$ are interpolated by the same $d + 1$ points. To show contradiction let $b = a' - a \neq 0$. b must be $\in O(x^n)$ by Thm 5.31, however all $d + 1$ points are valid roots of b (contradiction), hence $b = 0 \Rightarrow a = a'$.

9.5 Finite Fields

$\mathrm{GF}(p) \equiv \mathbb{Z}_p$ is a basic finite field. Recall $F[x]$ (coefficients are field elements) is analogous to $\mathbb{Z}$. Now we can define $F[x]_{m(x)}$.

D5.34: $F[x]_{m(x)} = \{a(x) \in F[x] \mid \deg(a(x)) < d\}$

- **L5.33:** Congruence mod $m(x)$ is an equivalence relation on $F[x]$ where each equivalence class has a unique rep of deg $< \deg(m(x))$.
- **L5.34:** $|F[x]_{m(x)}| = |F|^{\deg(m)}$
- **L5.35:** $F[x]_{m(x)}$ is a ring with respect to addition and multiplication mod $m(x)$.
- **L3.36:** $a(x)b(x) \underset{m(x)}{\equiv} 1$ iff $\gcd(a, b) = 1$
- **Thm 5.37:** A ring $F[x]_{m(x)}$ is a field iff $m(x)$ is irreducible.

9.6 Error Correcting Codes

Idea:
- Let $\mathcal{A}$ represent our alphabet. A msg of length k is $M \in \mathcal{A}^k, (a_0, \ldots, a_{k-1}) = M$.
- Now we create a polynomial $a(x)$ with coefficients parameterized using these values. We now evaluate $n > k$ points in $a(x)$.
- Now to reconstruct $a(x)$ we can only need $k + 1$ points, which means $n - k + 1$ can be "lost" and we should still know how to recover the msg.

Definitions:
- **D5.35:** Let's define encoding function $E : \mathcal{A}^k \to \mathcal{A}^n : (a_0, \ldots, a_{k-1}) \mapsto E((a_0, \ldots, a_{k-1})) = (c_0, \ldots, c_{n-1})$. E is an injection because $n > k$ and the output is called "codeword".
- **D5.36:** $C = \mathrm{Im}(E)$ since we have an injection think of C as the reachable space $\in \mathcal{A}^n$. This is called the set of codewords aka an error correcting code. $|C| = |\mathcal{A}|^k$
- **Hamming Distance (D5.37):** Basically char diff between two equal length strings.
- **D5.38:** The minimum distance of an error-correcting code C denoted $d_{\min}(C)$ is the minimum Hamming distance between any two codewords.

Now suppose Alice sends Bob the codeword C. The error correcting capability can be characterized by the number of errors t which can be corrected.
- **D5.40:** A decoding function D is t-error correcting for E for ANY $M \in \mathcal{A}^k$. $D((r_0, \ldots, r_{n-1})) = (a_0, \ldots, a_{k-1})$ for any input with at most t Hamming distance from E. A code C is t-error correcting if there $\exists E, D : C = \mathrm{Im}(E) \wedge D$ is t-error correcting
- **Thm 5.41:** A code C with $d_{\min}(C) = d$ is t-error correcting iff $d \geq 2t + 1$.
  - $\Leftarrow$: Take any two codewords with Hamming dist of $2t + 1$. Now corrupt both words t times each. Now you still have a distance of 1 with which you can identify the nearest source and hence reconstruct the information completely.
  - $\Rightarrow$: If two codewords differ in $\leq 2t$ positions then there exists a word in the middle, i.e. with equal distance to both codewords, hence it's possible that t errors cannot be uniquely corrected. Hence they need to differ by $2t + 1$

We call these: (n, k)-error-correcting code.

10 Proof Systems

- **Syntactic objects** are finite strings over some alphabet: Σ^*. Objects such as statements and proofs can be syntactically represented using such a string.
- **Statement:** $S \subseteq \Sigma^*$, **Proof:** $P \subseteq \Sigma^*$.
- We define a truth function $\tau : S \to \{0, 1\}$ which gives us the (god given) truth of a statement. For a $s \in S, \tau(s)$ defines the meaning, called **semantics** of the object in S.
- An element $p \in P$ either is a valid proof for a statement $s \in S$ or not. This can be defined by the **verification function** $\varphi : S \times P \to \{0, 1\}$ where $\varphi(s, p) = 1$ means p is a valid proof for s. φ needs to be efficiently computable.
- **Proof System:** A proof system is a quadruple $\Pi = (S, P, \tau, \varphi)$
- **Soundness:** $\forall s \in S \exists p \in P(\varphi(s, p) = 1 \Rightarrow \tau(s) = 1)$. Meaning if we say a statement is true using a provided proof, it actually is true.
- **Completeness:** $\forall s \in S(\tau(s) = 1 \Rightarrow \exists p \in P(\varphi(s, p) = 1))$. Meaning for all true statements, we can provide a proof showing such.

11 Logic

The goal of logic is to provide a specific proof system $\Pi = (S, P, \tau, \varphi)$ for which a very large class of mathematical statements can be expressed as an element of S.

Such a proof system can *never* capture all possible statements, in particular about the proof system itself (paradoxical).

In logic $s \in S$ consists of a formula and/or a set of formulas. A proof consists of **syntactic derivation** steps. Such steps consist of applying syntactic rules. The set of allowed rules is called **calculus**.

- The **syntax** of logic defines an alphabet Λ and specifies which strings in Λ^* are formulas (syntactically correct).
- The **semantics** of logic defines:
  - A function **free** which takes a formula and returns a set of indices of free symbols (variables).
  - An **interpretation** consists of $Z \subseteq \Lambda$, a set of possible values (domain) for each symbol in Z, and a function assigning each symbol in Z a value in its associated domain. Often (not in propositional logic) the domain is defined by a universe U.
  - An **interpretation is suitable** for a formula F if each free variable is assigned a value.
  - A function σ assigning each formula F and each interpretation A suitable for F a truth value $\sigma(F, A) \in \{0, 1\}$. We often write $A(F)$ instead and call this the truth value of F under interpretation A.
- A suitable interpretatin A for which $\sigma(F, A) = 1$ or $A(F) = 1$ is called a model for F, one writes $A \vDash F$. The same can be done for a set of formulas.

11.1 Satisfiability, Tautology, Consequence, Equivalence

- A formula F or a set of formulas M is **satisfiable** if there exists a model for F(or M). Unsatisfiable otherwise (denoted $\bot$).
- A formula F is a **tautology** or **valid** if it is true for every suitable interpretation (denoted $\top$).
- A formula G is a **logical consequence** of F if every interpretation suitable for both F, G which model F also model G, denoted $F \vDash G$.
- F, G are **equivalent** ($F \equiv G$) if for every interpretation suitable for both F, G they yield the same truth value for F, G. $F \equiv G \Leftrightarrow F \vDash G$ and $G \vDash F$.
- A set M of formulas can be interpreted as the conjunction (AND) of all formulas.

11.1.1 Logical Consequence vs Unsatisfiability

- **L6.2:** F is tautology iff $\neg F$ is unsat.
- **L6.3:** The following are equivalent:
  1. $\{F_1, ..., F_k\} \vDash G$
  2. $(F_1 \wedge ... \wedge F_k) \to G$ is a tautology
  3. $\{F_1, ..., F_k, \neg G\}$ is unsat.

11.2 Logical Operators

- **D6.16:**
  - $A((F \wedge G)) = 1$ iff $A(F) = 1$ and $A(G) = 1$
  - $A((F \vee G)) = 1$ iff $A(F) = 1$ or $A(G) = 1$
  - $A(\neg F) = 1$ iff $A(F) = 0$

11.3 Hilbert-Style Calculi

- **D6.17:** A **derivation rule** or **inference rule** $\{F_1, ..., F_k\} \underset{R}{\vdash} G$ is a syntactic step.
- **D6.19:** A **logical calculus** K is a finite set of dervation rules $K = \{R_1, ..., R_m\}$.
- **6.20:** A **derivation** of a formula G from a set M in calculus K is finite sequence of derivation rules applied on M leading to G. We write $M \underset{K}{\vdash} G$ if there is such a derivation.

11.4 Soundness and Completeness of a Calculus

- **D6.22:** A calculus K is **sound** if for every set M and every F: $M \underset{K}{\vdash} F \Rightarrow M \vDash F$. Meaning if F is derived from M then F is a logical consequence of M. Similarly K is **complete** if $M \vDash F \Rightarrow M \underset{K}{\vdash} F$.

11.5 Normal Forms

11.5.1 Prenex Normal Form

All quantifiers are at the beginning. Every formula in predicate logic can be converted into PNF form. Build a tree and let the quantifiers "bubble up".

11.5.2 Skolem Normal Form

The SNF **doesn't** preserve logical equivalence but preservers satisfiability. We want to eliminate existance quantifiers.
Process:
1. First convert to PNF.
2. Eliminate existance quantifiers. If we have $\forall a, b, c \exists y$ then we replace y by $f(a, b, c)$.

11.5.3 Conjunctive Normal Form

The CNF of a formula is the conjunction (AND) of disjunctions (OR) of literals ($= x$ or $\neg x$). $F = (a \vee b \vee c) \wedge (a \vee \neg b \vee \neg c) \wedge ....$ Construct by making truth table. For each row evaluating to 0, take the disjunct **negation** of that row ($A = 0, B = 1 \equiv 0 \Rightarrow (\neg A \vee B)$).

11.5.4 Disjunctive Normal Form

The DNF of a formula is the disjunction (OR) of conjunctions (AND) of literals. Construct by looking at rows evaluating to 1 and take those ($A = 0, B = 1 \equiv 1 \Rightarrow (\neg A \wedge B)$).

11.6 Resolution Calculus

- **D6.28:** A **clause** is a set of literals.
- **D6.29:** The set of clauses for a formula in CNF $F = ((a \vee ... \vee f) \wedge ... \wedge (x \vee ...z))$ is $K(F) = \{\{a, ...f\}, ..., \{x, ..., z\}\}$. For sets M we unionize the clauses of the individual formulas.
- A clause K is **resolvent** of K_1, K_2 if there is a literal L s.t. $L \in K_1 \wedge \neg L \in K_2 \Rightarrow K = (K_1 \setminus \{L\}) \cup (K_2 \setminus \{\neg L\})$
- **Unsat:** If we can derive the empty clause denoted $\{\}$ from a clause set using the resolution rule, then the original clause set is unsatisfiable.
- **Empty clause set:** An empty set of clauses is always satisfiable and hence a tautology and also always false and unsatisfiable (both vacuously)

11.7 Predicate Logic (First-order Logic)

11.7.1 Syntax

- Variable symbol x_i
- Function symbol $f_i^{(k)}$
- Predicate symbols $P_i^{(k)}$
- Term, defined recursively: 1) Variable is a term 2) If $t_1, ..., t_k$ are terms then $f(t_1, ..., t_k)$ is a term.
- Formula, defined recursively: 1) $P(t_1, ..., t_k)$ is a formula. 2) F and G are formulas then $\neg F$, $(F \wedge G)$, $(F \vee G)$ are each formulas. 3) If F is a formula, then $\forall x_i F$, $\exists x_i F$ are formulas.

11.7.2 Semantics

The interpretation is a tuple $A = (U, \varphi, \psi, \xi)$.
- U is a universe. φ assigns each function symbol a semantic function. ψ assigns each predicate symbol a predicate function. ξ assigns each variable symbol a value.
- We write U^A or f^A or P^A or x^A instead.
- **D6.36:**
  - The value $A(t)$ of term t is defined as follows:
    - If t is a variable $= x_i$, then $A(t) = x_i^A$ - If t is of the form $f(t_1, ...t_k)$, then $A(t) = f^A(A(t_1), ..., A(t_k))$.
  - The truth value of a formula F is defined recursively by D6.16 and:
    - If F is of the form $P(t_1, ..., t_k)$ then $A(f) = P^A(A(t_1), ..., A(t_k))$
    - 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 structure as A except x^A is overwritten by u:
      - $A(\forall x G) = \begin{cases} 1 \text{ if } A_{[x \to u]}(G)=1 \text{ for all } u \in U \\ 0 \text{ else} \end{cases}$
      - $A(\exists x G) = \begin{cases} 1 \text{ if } A_{[x \to u]}(G)=1 \text{ for some } u \in U \\ 0 \text{ else} \end{cases}$

L6.7: For any formuas F, G and H where x doesn't occur free in H we have:
1. $\neg(\forall x F) \equiv \exists x \neg F$
2. $\neg(\exists x F) \equiv \forall x \neg F$
3. $(\forall x F) \wedge (\forall x G) \equiv \forall x (F \wedge G)$
4. $(\exists x F) \vee (\exists x G) \equiv \exists x (F \vee G)$
5. $\forall x \forall y F \equiv \forall y \forall x F$
6. $\exists x \exists y F \equiv \exists y \exists x F$
7. $(\forall x F) \wedge H \equiv \forall x (F \wedge H)$
8. $(\forall x F) \vee H \equiv \forall x (F \vee H)$
9. $(\exists x F) \wedge H \equiv \exists x (F \wedge H)$
10. $(\exists x F) \vee H \equiv \exists x (F \vee H)$

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

11.7.2.1 Substitution of Bound Variables

L6.9: For a formula G in which y doesn't occur:
- $\forall x G \equiv \forall y G[x/y]$
- $\exists x G \equiv \exists y G[x/y]$

12 Helpful Stuff

$\varphi(n)$ for $1 \leq n \leq 100$

+	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

For $\mathbb{Z}_a \times \mathbb{Z}_b$ is cyclic iff $\gcd(a, b) = 1$.