3 Sets, Relations, and Functions

3.2 Sets and Operations on Sets

Definition 3.1. *The cardinality, denoted $|A|$ of a set is the amount of elements it contains.*

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

Lemma 3.1. *For any (sets) a and b, $\{a\} = \{b\} \Rightarrow a = b$*

Definition 3.3. *The set A is a subset of the set B, denoted $A \subseteq B$, if every element of A is also an element of B, i.e.,*

$$A \subseteq B \overset{def}{\iff} \forall x(x \in A \rightarrow x \in B)$$

Lemma 3.2. $A = B \iff (A \subseteq B) \wedge (B \subseteq A)$.

Lemma 3.3. *For any sets A, B, and C,*

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

Definition 3.4. *The union of two sets A and B is defined as*

$$A \cup B \overset{def}{=} \{x | x \in A \vee x \in B\}$$

and their intersection is defined as

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

Definition 3.5. *The difference of sets B and A, denoted $B \backslash A$ is the set of elements of B without those that are elements of A:*

$$B \backslash A \overset{def}{=} \{x \in B | x \notin A\}$$

Theorem 3.4. *For any sets A, B, and C, the following laws hold:*

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:	$A \cap (A \cup B) = A$;
	$A \cup (A \cap B) = A$;
Dirstibutivity:	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;
	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;
Consistency:	$A \subseteq B \iff A \cap B = A \iff A \cup B = B$

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

Lemma 3.5. *There is onl one empty set (which is often denoted as $\emptyset$ or $\{\}$).*

Lemma 3.6. *The mepty set is a subset of every set, i.e., $\forall A(\emptyset \subseteq A)$.*

Definition 3.7. *The power set of a set A denoted $\mathcal{P}(A)$, is the set of all subsets of A:*

$$\mathcal{P}(A) \stackrel{def}{=} \{S | S \subseteq A\}$$

Remark 3.1. *For a finite set with cardinality k, the power set has cardinality 2^k (hence the name 'power-set' and the alternative notation 2^A)*

Definition 3.8. *The Cartesian product $A \times B$ of two sets A and B is the set of all ordered pairs with the first component form A and the second component from B:*

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

Remark 3.2. *For finite sets, the cardinality of the Cartesian producto of some sets is the product of their cardinalities: $|A \times B| = |A| \cdot |B|$*

3.3 Relations

Definition 3.9. *A (binary) relation ρ from a set A to a set B (also called an (A, B)-relation) is a subset of $A \times B$. If $A = B$, then ρ is called a relation on A.*

Definition 3.10. *The inverse of a relation ρ fro A to B is the relation $\widehat{\rho}$ from B to A defined by*

$$\widehat{\rho} \stackrel{def}{=} \{(b, a) | (a, b) \in \rho\}$$

Definition 3.11. *Let ρ be a relation from A to B and let σ be a relation from B to C. Then the composition of ρ and σ, denoted $\rho \circ \sigma$, is the relation from A to C defined by*

$$\rho \circ \sigma \stackrel{def}{=} \{(a, c) | \exists \left((a, b) \in \rho \wedge (b, c) \in \sigma\right)\}$$

The n-fold composition of a relation ρ on a set A with itself is denoted ρ^n.

Definition 3.12. *For any set A, the identity relation on A, denoted id_A (or simply id), is the relation $id_A = \{(a, a) | a \in A\}$.*

Lemma 3.7. *The composition of relations is associative i.e., we have $\rho \circ (\sigma \circ \phi) = (\rho \circ \sigma) \circ \phi$.*

Lemma 3.8. *Let ρ be a relation form A to B and let σ be a relation form B to C. Then the inverse $\widehat{\rho\sigma}$ of $\rho\sigma$ is the relation $\widehat{\sigma}\widehat{\rho}$.*

Definition 3.13. *A relation ρ on a set A is called reflexive if*

$$a\rho a$$

is true for all $a \in A$, i.e., if

$$id \subseteq \rho$$

Definition 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 $\rho \cap id = \emptyset$.*

Definition 3.15. *A relation ρ on a set A is called symmetrix if*

$$a\rho b \iff b\rho a$$

is true for all $a, b \in A$, i.e., if

$$\rho = \widehat{\rho}$$

Definition 3.16. *A relation ρ 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

$$\rho \cap \widehat{\rho} \subseteq id$$

Definition 3.17. *A relation ρ on a set A is called transitive if*

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

is true for all $a, b, c \in A$

Lemma 3.9. *A relation ρ is transitive $\iff \rho^2 = \rho$*

Definition 3.18. *The transitive closure of a relation ρ on a set A, denoted ρ^*, is*

$$\rho^* = \bigcup_{n \in \mathbb{N} \setminus \{0\}} \rho^n$$

3.4 Equivalence Relations

Definition 3.19. *An equivalence relation is a relation on a set A that is reflexive symmectric, and transitive.*

Definition 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 and is denoted as $[a]_\theta$:*

$$[a]_\theta \stackrel{def}{=} \{b \in A | b\theta a\}$$

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

Definition 3.21. *A partition of a set A is a set of mutually disjoint subsets of A that cover A, i.e., a set $\{S_i | i \in \mathcal{I}\}$ of sets S_i (for some index set $\mathcal{I}$) satisfyng*

$$S_i \cap S_j = \emptyset \quad \textit{for } i \neq j \quad \textit{and} \quad \bigcup_{i \in \mathcal{I}} S_i = A$$

Definition 3.22. *The set of equivalence classes of an equivalence relation θ, denoted by*

$$A/\theta \stackrel{def}{=} \{[a]_\theta | a \in A\}$$

is called the quotiont set of A by θ, or simply A modulo θ, or A mod θ.

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

3.5 Partial Order Relations

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

Definition 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.*

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

Definition 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 $c \prec b$ (i.e., between a and b).*

Definition 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 if and only if b covers a.*

Definition 3.28. *The direct product of posets* $(A;\preceq)$ *and* $(B;\sqsubseteq)$*, denoted* $(A;\preceq)\times(B;\sqsubseteq)$*, is the set* $A\times B$ *with the relation* $\leq$ *(on* $A\times B$*) defined by*

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

Theorem 3.12. $(A;\preceq)\times(B;\sqsubseteq)$ *is a partial ordered set.*

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

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

Definition 3.29. *Let* $(A;\preceq)$ *be a poset, and let* $S\subseteq A$ *be some subset of* A*. Then*

1. $a\in A$ *is a minimal (maximal) element of* A *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* $a\preceq b$ $(a\succeq b)$ *for all* $b\in A$.
3. $a\in A$ *is a lower (upper) bound of* S *if* $a\preceq b$ $(a\succeq b)$ *for all* $b\in S$.
4. $a\in A$ *is the greatest lower (least upper) bound of* S *if* a *is the greatest (least) element of the set of all lower (upper) bounds of* S.

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

Definition 3.31. *Let* $(A;\preceq)$ *be a poset. If* a *and* b *(i.e., the set* $\{a,v\}\subseteq A$*) 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* $a\vee b$.

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

3.6 Functions

Definition 3.33. *A function* $f:A\to B$ *from a domain* A *to a codomain* B *is a relation from* A *to* B *with the special properties (using the relation notation* afb*):*

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

Definition 3.34. *The set of all functions $A \to B$ is denoted as B^A.*

Definition 3.35. *A partial function $A \to B$ is a relation from A to B such that ondition 2. above holds.*

Definition 3.36. *For a function $f : A \to B$ and a subset S of A, the image of S under f, denoted $f(S)$, is the set*

$$f(S) \stackrel{def}{=} \{f(a)|a \in S\}$$

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

Definition 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:*

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

Definition 3.39. *A function $f : A \to B$ is called*

1. *injective (or one-to-one or an injection) if for $a \neq a'$ we have $f(a) \neq f(a')$, i.e., no two distinct values are mapped to the same funciton value (there are no "collisions").*
2. *surjective (or onto) if $f(A) = B$, i.e., if for every $b \in B, b = f(a)$ for some $a \in A$ (every value in the codomain is taken on for some argument).*
3. *bijective (or bijection)if it is both injective and surjective.*

Definition 3.40. *For a bijective function f, the inverse (as a relation, see 3.9) is called the inverse function of f, usually denoted as f^{-1}.*

Definition 3.41. *The composition of a function $f : A \to B$ and a function $g : B \to C$, denoted by $g \circ f$ or simply gf, is defined by $(g \circ f)(a) = g(f(a))$.*

Lemma 3.14. *Function composition is associative, i.e., $(h \circ g) \circ f = h \circ (g \circ f)$.*

3.7 Countable and Uncountable Sets

Definition 3.42. .

(i) *Two sets* A *and* B *equinumerous, denoted* $A \sim B$*, if there exists a bijection* $A \to B$*.*

(ii) *The set* B *dominates the set* A*, denoted* $A \preceq B$*, if* $A \sim C$ *for some subset* $C \subseteq B$ *or, equivalently, if there exists an injective function* $A \to B$*.*

(iii) *A set* A *is called countable if* $A \preceq \mathbb{N}$*, and uncountable otherwise.*

Lemma 3.15. .

(i) *The relation* $\sim$ *is an equivalence relation.*

(ii) *The relation* $\preceq$ *is transitive:* $A \preceq B \wedge B \preceq C \Rightarrow A \preceq C$*.*

(iii) $A \subseteq B \Rightarrow A \preceq B$*.*

Theorem 3.16. $A \preceq B \wedge B \preceq A \Rightarrow A \sim B$

Theorem 3.17. *A set* A *is coutnable if and only if it is finite or if* $A \sim \mathbb{N}$*.*

Theorem 3.18. *The set* $\{0,1\}^* \stackrel{def}{=} \{\epsilon, 0, 1, 00, 01, 10, 11, 000, \dots\}$ *of finite binary sequences is countable.*

Theorem 3.19. *The set* $\mathbb{N} \times \mathbb{N}$ *(*$= \mathbb{N}^2$*) of ordered pairs of natual numbers is coutable.*

Corollary 3.20. *The Cartesial product* $A \times B$ *of two countable sets* A *and* B *is couable, i.e.,* $A \preceq \mathbb{N} \wedge B \preceq \mathbb{N} \Rightarrow (A \times B) \preceq \mathbb{N}$

Corollary 3.21. *The rational number* $\mathbb{Q}$ *are countable.*

Theorem 3.22. *Let* A *and* A_i*, for* $i \in \mathbb{N}$ *be countable sets.*

(i) *For any* $n \in \mathbb{N}$*, the set* A^n *of* n*-tuples over* A *is countable.*

(ii) *The union* $\bigcup_{i \in \mathbb{N} A_i}$ *of a countable list* $A_0, A_1, \dots$ *of countable sets is countable.*

(iii) *The set* A^* *of finite sequence of elements from* A *is countable.*

Definition 3.43. *Let* $\{0,1\}^\infty$ *denote the set of semi-infinite binary sequences or, equivalently, the set of functions* $\mathbb{N} \to 0, 1$*.*

Theorem 3.23. *The set* $\{0,1\}^\infty$ *is uncountable.*

Definition 3.44. *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 $f(n)$.*

Corollary 3.24. *There are uncomputable functions* $\mathbb{N} \to \{0, 1\}$

4 Number Theory

4.2 Divisors and Division

Definition 4.1. *For integers a and b we say that a devides b, denoted $a|b$, if there exists an integer c such that $b = ac$. In this case, a is called a divisor of b, and b is called a multiple of a. If $a \neq 0$ and a divisor c exists it is called the quotient when b is divided by a, and we write $c = \frac{b}{a}$ pr $c = b/a$. We write $a \not| b$ if a does not divide b.*

Theorem 4.1 (Euclid)**.** *For all integers a and $d \neq 0$ there exist unique integers q and r satisfying*

$$a = dq + r \quad \text{and} \quad 0 \leq r < |d|$$

Definition 4.2. *For integer a and b (not both 0), an integer d is called a greatest common divisor of a and b if d divides both a and b and if every common divisor of a and b divides d, i.e., if*

$$d|a \wedge d|b \wedge \forall c\,((c|a \wedge c|b) \leftarrow c|d)$$

Definition 4.3. *For $a, b \in \mathbb{Z}$ (not both 0) one denotes the unique positive greatest common divisor by $gcd(a, b)$ and usually calls it the greatest common divisor. If $gcd(a, b) = 1$, then a and b are called relatively prime.*

Lemma 4.2. *For any integers m, n, and q, we have*

$$gcd(m, n - qm) = gcd(m, n)$$

Definition 4.4. *For $a, b \in \mathbb{Z}$, the ideal generated by a and b, denoted (a, b), is the set*

$$(a, b) \stackrel{def}{=} \{ua + vb | u, v \in \mathbb{Z}\}$$

Similarly, the ideal generated by a single integer a is

$$(a) \stackrel{def}{=} \{ua | u \in \mathbb{Z}\}$$

Lemma 4.3. *For $a, b \in \mathbb{Z}$ there exists $d \in \mathbb{Z}$ such that $(a, b) = (d)$.*

Lemma 4.4. *Let $a, b \in \mathbb{Z}$ (not both 0). If $(a, b) = (d)$, then d is a greatest common divisor of a and b.*

Corollary 4.5. *For $a, b \in \mathbb{Z}$ (not both 0), there exist $u, v \in \mathbb{Z}$*

$$gcd(a, b) = ua + vb$$

Definition 4.5. *The least common multiple l of two positive integers a and b, denoted $l = lcm(a, b)$, is the common multiple of a and b which divides every common multiple of a and b, i.e.,*

$$a|l \wedge b|l \wedge \forall m\,((a|m \wedge b|m) \rightarrow l|m)$$

4.3 Factorization into Primes

Definition 4.6. *A positive integer $p > 1$ is called prime if the only positive divisor of p are 1 and p. An integer greater than 1 that is not a prime is called composite.*

Theorem 4.6. *Every positive integer can be written uniquely (up to the order in which factors are listed) as the product of primes.*

Lemma 4.7. *If p is prime which divides the product $x_1x_2\cdots x_n$ of some integers $x_1,\ldots,x_n$, then p divides one of them, i.e., $p|x_i$ for some $i \in \{1,\ldots,n\}$.*

Remark 4.1. *Since we can write write any integers a and b as factors of primes*

$$a = \prod_i p_i^{e_i} \quad \text{and} \quad b = \prod_i p_i^{f_i}$$

we can write gcd like this

$$gcd(a,b) = \prod_i p_i^{\min(e_i,f_i)}$$

and lcm like this

$$lcm(a,b) = \prod_i p_i^{\max(e_i,f_i)}$$

It's easy to see that $gcd(a,b) \cdot lcm(a,b) = ab$ because for all i $\min(e_i,f_i) + \max(e_i,f_i) = e_i + f_i$

4.5 Congruence and Modular Arithmetic

Definition 4.8. *For $a,b,m \in \mathbb{Z}$ with $m \geq 1$, we say that a is congruent to b modulo m if m divides $a-b$. We write $a \equiv b(mod m)$ or simply $a \equiv_m b$, i.e.,*

$$a \equiv_m b \overset{def}{\Longleftrightarrow} m|(a-b)$$

Lemma 4.13. *For any $m \geq 1$, $\equiv_m$ is an equivalence relation on $\mathbb{Z}$.*

Lemma 4.14. *If $a \equiv_m b$ and $c \equiv_m d$, then*

$$a + c \equiv_m b + d \quad \text{and} \quad ac \equiv_m bd$$

Corollary 4.15. *Let $f(x_1,\ldots,x_k)$ be a multi-variable polynomial in k variables with integer coefficients, and let $m \geq 1$. If $a_i \equiv_m b_i$ for $1 \leq i \leq k$, then*

$$f(a_1,\ldots,a_k) \equiv_m f(b_1,\ldots,b_k)$$

Lemma 4.16. *For any $a,b,m \in \mathbb{Z}$ with $m \geq 1$,*

(i) $a \equiv_m R_m(a)$.

(ii) $a \equiv_m b \iff R_m(a) = R_m(b)$.

Corollary 4.17. *Let $f(x_1,\ldots,x_k)$ be a multi-variate polynomial in k variables with integer coefficients and let $m \geq 1$. Then*

$$R_m\left(f(a_1,\ldots,a_k)\right) = R_m\left(f(R_m(a_1),\ldots,R_m(a_k))\right).$$

Lemma 4.18. *The congruence equation*

$$ax \equiv_m 1$$

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

Definition 4.9. *If $gcd(a, m) = 1$, the unique solution $x \in \mathbb{Z}_m$ to the congruence equation $ax \equiv_m 1$ is called the multiplicative inverse of a modulo m. One also uses the notation $x \equiv_m a^{-1}$ or $x \equiv_m \frac{1}{a}$.*

Theorem 4.19. *Let $m_1, \ldots, m_r$ be pairwise relatively prime integers and let $M = \prod_{i=1}^{r} m_i$. For every list $a_1, \ldots, a_r$ with $0 \leq a_i < m_i$ for $1 \leq i \leq r$, the system of congruence equations*

$$\begin{aligned} x &\equiv_{m_1} a_1 x & \equiv_{m_2} a_2 \ldots \\ x &\equiv_{m_r} a_r \end{aligned}$$

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

5 Algebra

5.1 Introduction

Definition 5.1. *An operation on a set S is a function $S^n \to S$, where $n \geq 0$ is called the "arity" of the operation.*

Definition 5.2. *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 $\Omega = (\omega_1, \ldots, \omega_n)$) is a list of operations on S.*

5.2 Monoids and Groups

Definition 5.3. *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.*

Lemma 5.1. *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.*

Definition 5.4. *A binary operation $*$ on a set S is associative if $a * (b * c) = (a * b) * c$ for all $a, b, c \in S$.*

Definition 5.5. *A monoid is an algebra $\langle M; *, e \rangle$ where $*$ is associative and e is the neutral element.*

Definition 5.6. *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 $b * a = a * b = e$, hen b is simply called an inverse of a.*

Lemma 5.2. *In a monoid $\langle M; *, e \rangle$, if $a \in M$ has a left and right inverse, then they are equal. In particular, a has at most one inverse.*

Definition 5.7. *A group is an algebra $\langle G; *, \widehat{\ }, e \rangle$ 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 $\widehat{a}$, i.e., $a * \widehat{a} = \widehat{a} * a = e$.*

Definition 5.8. *A group $\langle G; * \rangle$ (or monoid) is called commutative or abelian if $a * b = b * a$ for all $a, b \in G$.*

Lemma 5.3. *For a group $\langle G; *, \widehat{\ }, e \rangle$, we have for all $a, b, c \in G$:*

(i) $\widehat{(\widehat{a})} = a$,

(ii) $\widehat{a * b} = \widehat{b} * \widehat{a}$,

(iii) *Left cancellation law:* $a * b = a * c \implies b = c$

(iv) *Right cancellation law:* $b * a = c * a \implies b = c$

(v) *The equation* $a * x = b$ *has a unique solution* x *for any* a *and* b*. So does the equation* $x * a = b$.

5.3 The Structure of Groups

Definition 5.9. *The direct product of* n *groups* $\langle G_1; *_1 \rangle, \ldots, \langle G_n; *_n \rangle$ *is the algebra.*

$$\langle G_1 \times \cdots \times G_n; \star \rangle$$

where the operation $\star$ *is component-wise:*

$$(a_1, \ldots, a_n) * (b_1, \ldots, b_2) = (a_1 *_1 b_1, \ldots, a_n *_n b_n)$$

Lemma 5.4. $\langle G_1 \times \cdots \times G_n; \star \rangle$ *is a group, where the neutral element and the inverstion operation are component-wise in the respective groups.*

Definition 5.10. *For two groups* $\langle G; *, \widehat{\ }, e \rangle$ *and* $\langle H; \star, \widetilde{\ }, e' \rangle$*, a function* $\psi : G \to H$ *is called a group homomorphism if, for all* a *and* b,

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

If ψ *is a bijection from* G *to* H*, then it is called an isomorphism, and we say that* G *and* H *are isomorphic and write* $G \simeq H$

Lemma 5.5. *A group homomorphism* ψ *from* $\langle G; *, \widehat{\ }, e \rangle$ *to* $\langle H; \star, \widetilde{\ }, e' \rangle$ *satisfies*

(i) $\psi(e) = e'$,

(ii) $\psi(\widehat{a}) = \widetilde{\psi(a)}$

Definition 5.11. *A subset* $H \subseteq G$ *if a group* $\langle G; *, \widehat{\ }, e \rangle$ *is called a subgroup of* G *if* $\langle H; *, \widehat{\ }, e \rangle$ *is a group, i.e., if* H *is closed with respect to all operations:*

(i) $a * b \in H$ *for all* $a, b \in H$,

(ii) $e \in H$*, and*

(iii) $\widehat{a} \in H$ *for all* $a \in H$.

Definition 5.12. *Let* G *be a group and let* a *be an element of* G*. The order of* a*, denoted* $\mathrm{ord}(a)$*, 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* $\mathrm{ord}(a) = \infty$.

Lemma 5.6. *In a finite grou* G*, every element has a finite order.*

Definition 5.13. *For a finite group G, $|G|$ is called the order of G.*

Definition 5.14. *For a group G and $a \in G$, the group generated by a, denoted $\langle a \rangle$, is defined as*

$$\langle a \rangle \stackrel{def}{=} \{a^n | n \in \mathbb{Z}\}$$

Remark 5.1. *The group generated by $\langle a \rangle$ is the smallest subgroup of G containing the element $a \in G$.*

Definition 5.15. *A group $G = \langle g \rangle$ generated by an element $g \in G$ is called cyclic, and g is called a generator of G.*

Theorem 5.7. *A cyclic group of order n is isomorphic to $\langle \mathbb{Z}_n; \oplus \rangle$ (and hence commutative/abelian)*

Theorem 5.8 (Lagrange)**.** *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 $|G|$.*

Corollary 5.9. *For a finite group G, the order of every element devides the group order, i.e.,* $\mathrm{ord}(a)$ *divides $|G|$ for every $a \in G$.*

Corollary 5.10. *Let G be a finite group. Then $a^|G| = e$ for every $a \in G$.*

Corollary 5.11. *Every group of prime order is cyclic, and in such a group every element except the natural element is a generator.*

Definition 5.16. $\mathbb{Z}_m^* \stackrel{def}{=} \{a \in \mathbb{Z}_m | \gcd(a, m) = 1\}$.

Definition 5.17. *The Euler function $\varphi(m) = |\mathbb{Z}_m^*|$*

Lemma 5.12. *If the prime factorization of m is $m = \prod_{i=1}^r p_i^{e_i}$, then*

$$\varphi(m) = \prod_{i=1}^{r} (p_i - 1) p_i^{e_i - 1}$$

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

Corollary 5.14 (Fermat,Euler)**.** *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,

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

Theorem 5.15. *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* $e \geq 1$.

5.4 Application: RSA Public-Key Encryption

Theorem 5.16. *Let* G *be some finte group (multiplicatively written), and let* $e \in \mathbb{Z}$ *be relatively prime to* $|G|$ *(i.e.* $\gcd(e, |G|) = 1$*). The function* $x \mapsto x^e$ *is a bijection and the (unique)* e*-th root of* $y \in G$*, namely* $x \in G$ *satisfying* $x^e = y$*, is*

$$x = y^d$$

where d *is the muliplicative inverse of* e *modulo* $|G|$*, i.e.,*

$$ed \equiv_{|G|} 1$$

5.5 Rings and Fields

Definition 5.18. *A ring* $\langle R; +, -, 0, \cdot, 1\rangle$ *is an algebra for which*

- ***R1*** $\langle R; +, -, 0\rangle$ *is a commutative group,*
- ***R2*** $\langle R; \cdot, 1\rangle$ *is a monoid, and*
- ***R3*** *left and right distributive law:* $a(a + b) = (ab) + (ac)$ *and* $(b + c)a = (ba) + (ca)$ *for all* $a, b, c \in R$.

A ring is called commutative if multiplication is commutative $(ab = ba)$

Lemma 5.17. *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. if it has more tha one element), then* $1 \neq 0$.

Definition 5.19. *The characteristic of a ring is the order of* 1 *in the additive group if it is finitem and otherwise the characteristic is defined to be* 0 *(not infinite).*

Definition 5.20. *An element* u *of a ring* R *is claled a unit if* u *is invertible, i.e.,* $uv = vu = 1$ *for some* $v \in R$*. (We write* $v = u^{-1}$*.) The set of units of* R *is denoted by* R^*.

Lemma 5.18. *For a ring* R*,* R^* *is a multiplicative group (the group of units of* R*).*

Definition 5.21. *For* $a, b \in R$ *we say that* a *divides* b*, denoted* $a|b$*, 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.

Lemma 5.19. *In any commutative ring,*

(i) If $a|b$ and $b|c$, then $a|c$, i.e., the relation $|$ is transitive,

(ii) If $a|b$, then $a|bc$ for all c, and

(iii) If $a|b$ and $a|c$, then $a|(b+c)$.

Definition 5.22. *For ring elements a and b (not both 0), a ring element d is called a greatest common divisor of a and b if d divides both a and b and if every common divisor of a and b divides d, i.e., if*

$$d|a \wedge d|b \wedge \forall\,((c|a \wedge c|b) \rightarrow c|d)$$

Definition 5.23. *An element $a \neq 0$ of a commutative ring R is called a zerodivisor if $ab = 0$ for some $b \neq 0$ in R.*

Definition 5.24. *An integral domain is a (nontrivial) commutative ring without zerodivisors: $\forall a \forall b(ab = 0 \rightarrow a = 0 \vee b = 0)$.*

Lemma 5.20. *In an integral domain, if $a|b$, then c with $b = ac$ is unique (and is denoted by $c = \frac{b}{a}$ or $c = b/a$ and called quotient).*

Definition 5.25. *A polynomial $a(x)$ over a commutative ring R in the indeterminate x is a formal expression of the form*

$$a(x) = a_d x^d + \cdots + a_0 x^0 = \sum_{i=1}^{d} a_i x^i$$

for some non-negative integer d, with $a_i \in R$. The degree of $a(x)$, denoted $\deg(a(x))$, is the greatest i for which $a_i \neq 0$. The special polynomial 0 (i.e., all the a_i are 0) is defined to have degree "minus infinity". Let $R[x]$ denote the set of polynomials in x over R.

Theorem 5.21. *For any commutative ring R, $R[x]$ is a commutative ring.*

Lemma 5.22. *.*

(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: $D[x]^* = D^*$.

Definition 5.26. *A field is a nontrivial commutative ring F in which every nonzero element is a unit, i.e., $F^* = F \backslash \{0\}$.*

Theorem 5.23. *$\mathbb{Z}_p$ is a field if and only if p is prime.*

Theorem 5.24. *A field is an integral domain.*

5.6 Polynomials over a Field

Definition 5.27. *A polynomial $a(x) \in F[x]$ is called monic if the leading coefficient is 1.*

Definition 5.28. *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 $a(x)$.*

Definition 5.29. *The monic polynomial $g(x)$ of largest gegree such that $g(x)|a(x)$ and $g(x)|b(x)$ is called the greatest common divisor of $a(x)$ and $b(x)$, denoted $\gcd(a(x), b(x))$.*

Theorem 5.25. *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*

$$a(x) = b(x) \cdot q(x) + r(x) \quad \text{and} \quad \deg(r(x)) < \deg(b(x)).$$

Definition 5.30. *In an integral domain, a and b are called associates, denoted $a \sim b$, if $a = ub$ for some unit u.*

Definition 5.31. *In an integral domain, a non-unit $p \in D \backslash \{0\}$ is irreducible if, whenever $p = ab$, then either a or b is a unit.*

Lemma 5.26. $a \sim b \iff a|b \wedge b|a$

Definition 5.32. *A Euclidean domain is an integral domain D together with a so-called degree function $d : D \backslash \{0\} \to \mathbb{N}$ such that*

(i) For every a and $b \neq 0$ in D there exist q and r such that $a = bq + r$ and $d(r) < d(b)$ or $r = 0$.

(ii) For all nonzero a and b in D, $d(a) \leq d(ab)$

Theorem 5.27. *In a Euclidean domain every element can be factored uniquely (up to taking associates) into irreducible elements.*

5.7 Polynomials as Functions

Lemma 5.28. *Polynomials evaluation is compatible with the ring operations:*

- *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*.*

Definition 5.33. *Let* $a(x) \in R[x]$*. An element* $\alpha \in R$ *for whch* $a(\alpha) = 0$ *is called a root of* $a(x)$*.*

Lemma 5.29. *For a field* F*,* $\alpha \in F$ *is a root of* $a(x)$ *if and only if* $x - \alpha$ *divides* $a(x)$*.*

Corollary 5.30. *A polynomial* $a(x)$ *of degree* 2 *or* 3 *over a field* F *is irreducible if and only if it has no root.*

Theorem 5.31. *For a field* F*, a nonzero polynomial* $a(x) \in F[x]$ *of degree* d *has at most* d *roots.*

Lemma 5.32. *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* $a(\alpha_1), \ldots, a(\alpha_{d+1})$ *for any distinct* $\alpha_1, \ldots, \alpha_{d+1} \in F$*.*

Lemma 5.33. *Congruence modulo* $m(x)$ *is a equivalence relation on* $F[x]$*, and each equivalence class has a unique representation of degree less than* $\deg(m(x))$*.*

Definition 5.34. *Let* $m(x)$ *be a polynomial of degree* d *over* F*. Then*

$$F[x]_{m(x)} \stackrel{def}{=} \{a(x) \in F[x] | \deg(a(x)) < d\}$$

Lemma 5.34. *Let* F *e a finite field with* q *elements and let* $m(x)$ *be a polynomial of degree* d *over* F*. Then* $|F[x]_{m(x)}| = q^d$*.*

Lemma 5.35. $F[x]_{m(x)}$ *is a ring with respect to addition and multiplication modulo* $m(x)$*.*

Lemma 5.36. *The congruence equation*

$$a(x)b(x) \equiv_{m(x)} 1$$

(for a given $a(x)$*) has a solution* $b(x) \in F[x]_{m(x)}$ *if and only if* $\gcd(a(x), m(x)) = 1$*. The solution is unique. In other words,*

$$F[x]^*_{m(x)} = \{a(x) \in F[x]_{m(x)} | \gcd(a(x), m(x)) = 1\}$$

Theorem 5.37. *The ring* $F[x]_{m(x)}$ *is a field if and only if* $m(x)$ *is irreducible.*

Theorem 5.38. *For every prime* p *and every* $d \geq 1$ *there exists an irreducible polynomial of degree* d *in* $GF(p)[x]_{m(x)}$*. In particular, there exists a finite field with* p^d *elements.*

Theorem 5.39. *There exists a finite field with q elements if and only if q is a power of a prime. Moreover, any two finite fields of the same size q are isomorphic.*

Theorem 5.40. *The muliplicative group of every finite field $GF(q)$ is cyclic.*

5.8 Application: Error-Correcting Codes

Definition 5.35. *A $(n-k)$-encoding function E for some alphabet $\mathcal{A}$ is an injecive function that mpas a list $(a_0, \ldots, a_{k-1}) \in \mathcal{A}^k$ of K (information) symbols to a list $(c_0, \ldots, c_{n-1}) \in \mathcal{A}^n$ of $n > k$ (encoded) symbols in $\mathcal{A}$, called codeword:*

$$E : \mathcal{A}^k \to \mathcal{A}^n : (a_0, \ldots, a_{k-1}) \mapsto E((a_0, \ldots, a_{k-1})) = (c_0, \ldots, c_{n-1})$$

Definition 5.36. *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.*

Definition 5.37. *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.*

Definition 5.38. *The minimum distance of an error-correcring code $\mathcal{C}$, denoted $d_{min}(\mathcal{C})$, is the minimum of the Hamming distance between any two codewords.*

Definition 5.39. *A decoding function D for an (n, k)-encoding function is a function $D : \mathcal{A}^n \to \mathcal{A}^k$.*

Definition 5.40. *A decoding function D is t-error correcting for encoding function E if for any $(a_0, \ldots, a_{k-1})$*

$$D((r_0, \ldots, r_{n-1})) = (a_0, \ldots, a_{k-1})$$

for any $(r_0, \ldots, r_{n-1})$ with Hamming distance at most t from $E((a_0, \ldots, a_{k-1}))$. A code $\mathcal{C}$ is t-error correcting if there eists E and D with $\mathcal{C} = Im(E)$ where D is t-error correcting.

Theorem 5.41. *A code $\mathcal{C}$ with minimum distance d is t correcting if and only if $d \geq 2t+1$.*

Theorem 5.42. *Let $\mathcal{A} = GF(q)$ and let $\alpha_0, \ldots, \alpha_{n-1}$ be arbitrary distinct elements of $GF(q)$. Consider the encoding function*

$$E((a_0, \ldots, a_{k-1})) = (a(\alpha_0), \ldots, a(\alpha_{n-1}))$$

where $a(x)$ is the polynomial

$$a(x) = a_{k-1}x^{k-1} + \cdots + a_0x^0$$

This code has minimum distance $n-k+1$.

6 Logic

6.2 Proof Systems

Definition 6.1. *A proof system is a quadruple $\Pi = (\mathcal{S}, \mathcal{P}, \tau, \phi)$, where $\mathcal{S}$ is the set of all possible statements, $\mathcal{P}$ is the set of all possible proofs, $\tau : \mathcal{S} \to \{0,1\}$, and $\phi : \mathcal{S} \times \mathcal{P} \to \{0,1\}$*

Definition 6.2. *A proof system $\Pi = (\mathcal{S}, \mathcal{P}, \tau, \phi)$ is sound if no false statement has a proof, i.e., if for all $s \in \mathcal{S}$ for which there exists $p \in \mathcal{P}$ with $\phi(s,p) = 1$, we have $\tau(s) = 1$.*

Definition 6.3. *A proof system $\Pi = (\mathcal{S}, \mathcal{P}, \tau, \phi)$ is complete if every true statement has a proof, i.e., if for all $s \in \mathcal{S}$ whit $\tau(s) = 1$, there exists $p \in \mathcal{P}$ with $\phi(s,p) = 1$.*

6.3 Elementary General Concepts in Logic

Definition 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).*

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

Definition 6.6. *An interpretation consists of a set $\mathcal{Z} \subseteq \Lambda$ of symbols of Λ, a domain (a set of possible values) for each symbol in $\mathcal{Z}$, and a function that assigns to each symbol in $\mathcal{Z}$ a value in its associated domain.*

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

Definition 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 $\{0,1\}$. In treatments of logic one often writes $\mathcal{A}(F)$ instead of $\sigma(F, \mathcal{A})$ and calls $\mathcal{A}(F)$ the truth value of F under interpretation $\mathcal{A}$.*

Definition 6.9. *A (suitable) interpretation $\mathcal{A}$ for which a formula F is true, (i.e., $\mathcal{A}(F) = 1$) is called a model for F, and one also writes*

$$\mathcal{A} \models F$$

More generally, for a set M of formulas, a (suitable) interpretation for which all formulas *in M are true is called a model for M, denoted as*

$$\mathcal{A} \models M$$

If $\mathcal{A}$ is not a model for M one write $\mathcal{A} \not\models M$.

Definition 6.10. *A formula F (or set M of formulas) is called satisfiable if there exists a model for F (or M), and unsatifiable otherwise. The symbol $\perp$ is used for an unsatisfiable formula.*

Definition 6.11. *A formula F is called a tautology or valid if it is true for every suitabke interpretation. The symbol $\top$ is used for a tautology.*

Definition 6.12. *A formula G is a logical consequence of a formula F (or a set M of formulas), denoted*

$$F \models G \quad (or \quad M \models G)$$

if very interpretation suitable for both F (or M) and G, which is a model for F (for M), is also a model for G.

Definition 6.13. *Two formulas F and G are equivalent, denoted $F \equiv G$, if every interpretation suitable for both F and G yields the same truth value for F and G, i.e., if each one is a logical consequence of the other:*

$$F \equiv G \overset{def}{\iff} F \models G \text{ and } G \models F$$

Definition 6.14. *If F is a tautology, one also write $\models F$.*

Definition 6.15. *If F and G are formulas, then also $\neg F$, $(F \wedge G)$, and $(F \vee G)$ are formulas.*

Remark 6.1.

$$(F \rightarrow G) \overset{def}{\iff} (\neg F \vee G)$$
$$(F \leftrightarrow G) \overset{def}{\iff} ((F \wedge G) \vee (\neg F \wedge \neg G))$$

Definition 6.16.

$$\mathcal{A}((F \wedge G)) = 1 \overset{def}{\iff} \mathcal{A}(F) = 1 \text{ and } \mathcal{A}(G) = 1$$
$$\mathcal{A}((F \vee G)) = 1 \overset{def}{\iff} \mathcal{A}(F) = 1 \text{ or } \mathcal{A}(G) = 1$$
$$\mathcal{A}(\neg F) = 1 \overset{def}{\iff} \mathcal{A}(F) = 0$$

Lemma 6.1. *For any formulas F,G, and H we have*

(i) $F \wedge F \equiv F$ *and* $F \vee F \equiv F$ *(idempotence);*

(ii) $F \wedge G \equiv G \wedge F$ *and* $F \vee G \equiv G \vee F$ *(commutativity);*

(iii) $(F \wedge G) \wedge H \equiv F \wedge (G \wedge H)$ *and* $(F \vee G) \vee H \equiv F \vee (G \vee H)$ *(associativity);*

(iv) $F \wedge (F \vee G) \equiv F$ *and* $F \vee (F \wedge G)$ *(absorption);*

(v) $F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$ *(distributive law);*

(vi) $F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$ *(distributive law);*

(vii) $\neg\neg F \equiv F$ *(double negation);*

(viii) $\neg(F \wedge G) \equiv \neg F \vee \neg G$ *and* $\neg(F \vee G) \equiv \neg F \wedge \neg G$ *(de Morgan's law);*

(ix) $F \vee \top \equiv \top$ *and* $F \wedge \top \equiv F$ *(tautology rules);*

(x) $F \vee \bot \equiv F$ *and* $F \wedge \bot \equiv \bot$ *(unsatisfiability rules);*

(xi) $F \vee \neg F \equiv \top$ *and* $F \wedge \neg F \equiv \bot$*;*

Lemma 6.2. *A formula F is a tautology if and only if $\neg F$ is unsatisfiable.*

Lemma 6.3. *The following three statements are equivalent:*

(i) $\{F_1, \ldots, F_k\} \models G$

(ii) $(F_1, \ldots, F_k) \to G$ *is a tautology*

(iii) $\{F_1, \ldots, F_k, \neg G\}$ *is unsatisfiable.*

6.4 Logical Calculi

Definition 6.17. *A dervation rule or inference rule is a rule for deriving a formula from a set of formulas (called the precondition or premises). We write*

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

if G can be derived from the set $\{F_1, \ldots, F_k\}$ by rule R.

Definition 6.18. *The application of a derivation rule R to a set M of forumulas means. Assigning a formula $F \in M$ to any placeholder in R and adding the resulting formula G to the set M.*

Definition 6.19. *A (logical) calculus K is a finite set of derivation rules $K = \{R_1, \ldots, R_m\}$.*

Definition 6.20. *A derivation of a formula G from a set M of formulas in a calculus K is a finite sequence (of some length n) of applications of rules in$K$, leading to G. More precisely, we have*

- $M_0 := M$,

- $M_i := M_{i-1} \cup \{G_i\}$ *for* $1 \le i \le n$, *where* $N \vdash_{R_i} G_i$ *for some* $N \subseteq M_{i-1}$ *and for some* $R_j \in K$, *and where*
- $G_n = G$.

We write

$$M \vdash_K G$$

if three is a derivation of G *from* M *in the calculus* K.

Definition 6.21. *A derivation rule* R *is correct if for every set* M *of formulas and every formula* F, $M \vdash_R F$ *implies* $M \models F$.

Definition 6.22. *A calculus* K *is sound or correct if for every set* M *of formulas and every formula* F, *if* F *can be derived from* M *then* F *is also a logical consequence of* M:

$$M \vdash_K F \implies M \models F$$

and K *is complete if for every* M *and* F, *if* F *is a logical consequence of* M *then* F *can also be derived from* M:

$$M \models F \implies M \vdash_K F$$

6.5 Propositional Logic

Definition 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 also* $\neg F$, $(F \wedge G)$, *and* $(F \vee G)$ *are formulas.*

Definition 6.24 (Semantics)**.** *For a set* Z *of atomic formulas, an interpretation* $\mathcal{A}$, *called truth assignment, is a function* $\mathcal{A} : Z \to \{0,1\}$. *A truth assignment* $\mathcal{A}$ *is suitable for a formula* F *if* Z *contains all atomic formulas appearing in* F. *The semantics (i.e., the truth value of* $\mathcal{A}(F)$ *of a formula* F *under interpretation* $\mathcal{A}$*) is defined by* $\mathcal{A}(F) = \mathcal{A}(A_i)$ *for any atomic formula* $F = A_i$, *and by Definition 6.16*

$$\begin{aligned} \mathcal{A}((F \wedge G)) = 1 &\overset{def}{\iff} \mathcal{A}(F) = 1 \text{ and } \mathcal{A}(G) = 1 \\ \mathcal{A}((F \vee G)) = 1 &\overset{def}{\iff} \mathcal{A}(F) = 1 \text{ or } \mathcal{A}(G) = 1 \\ \mathcal{A}(\neg F) = 1 &\overset{def}{\iff} \mathcal{A}(F) = 0 \end{aligned}$$

Definition 6.25. *A literal is an atomic formula or the negation of an atomic formula.*

Definition 6.26. *A formula F is in conjunctive normal form (CNF) if it is a conjunction of disjunctions of literals, i.e., if it is of the form*

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

for some literals L_{ij}.

Definition 6.27. *A formula F is in disjunctive normal form (DNF) if it is a disjunction of conjunctions of literals, i.e., if it is of the form*

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

for some literals L_{ij}.

Theorem 6.4. *Every formula is equivalent to a formula in CNF and also to a formula in DNF.*

Definition 6.28. *A clause is a set of literals.*

Definition 6.29. *The set of clauses associated to a formula*

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

in CNF, denoted as $\mathcal{K}(F)$, is the set

$$\mathcal{F} \stackrel{def}{=} \{\{L_{11}, \ldots, L_{1m_1}\}, \ldots, \{L_{n1}, \ldots, L_{nm_n}\}\}$$

The set of clauses associated with a set $M = \{F_1, \ldots, F_k\}$ of formulas is the union of their clause sets:

$$\mathcal{K}(M) \stackrel{def}{=} \bigcup_{i=1}^{k} \mathcal{K}(F_i)$$

Definition 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*

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

Lemma 6.5. *The resolution calculus is sound, i.e., if $\mathcal{K} \vdash_{Res} K$ then $\mathcal{K} \models K$.*

Theorem 6.6. *A set M of formulas is unsatisfiable if and only if $\mathcal{K}(M) \vdash_{Res} \emptyset$.*

6.6 Predicate Logic (First-order Logic)

Definition 6.31 (Syntax of predicate logic).

- *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 of the function. Funcion 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 f arguments of the predicate.*
- *A term is defined inductively: A variable is a term and if* $t_1, \ldots, t_k$ *are terms, then* $f_i^{(k)}(t_1, \ldots, t_k)$ *are terms, then* $f_i^{(k)}(t_1, \ldots, t_k)$ *is a term. For* $k = 0$ *one writes no parentheses.*
- *A formula is defined inductively:*
  - *For any* i *and* k*, if* $t_1, \ldots, t_k$ *are terms, then* $P_i^{(k)}(t_1, \ldots, t_k)$ *is a formula, called an atomic formula.*
  - *If* F *and* G *are formulas, then* $\neg F$*,* $(F \wedge G)$*, and* $(F \vee G)$ *are formulas.*
  - *If* F *is a formula, then, for any* i*,* $\forall x_i F$ *and* $\exists x_i F$ *are formulas.*

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

Definition 6.33. *For a formula* F*, a variable* x *and a term* t*,* $F[x/t]$ *denotes the formula obtained from* F *by subtituting every free occurence of* x *by* t*.*

Definition 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 (in a certain subset of all function symbols) a function, where for a* k*-ary function symbol* f*,* $\phi(f)$ *is a function* $U^k \to U$*,*
- ψ *is a function assigning to each predigcate symbol (in a certain subset of all predicate symbols) a function, where for a* k*-ary predicate symbol* P*,* $\psi(P)$ *is a function* $U^k \to \{0, 1\}$*, and where*
- ξ *is a function assigning to each variable symbol (in a certain subset of all variable symbols) a value in* U*.*

Definition 6.35. *A interpretation (structure)* $\mathcal{A}$ *is suitable for a formula* F *if it defines all functions symbols, predicate symbols, and freely occuring variables of* F*.*

Definition 6.36 (Semantics)**.** *For aninterpretation (structure) $\mathcal{A} = (U, \phi, \psi, \xi)$, we define the value (in U) of the terms and the truth value of formulas under that structure.*

- *The value $\mathcal{A}$ of a ter t is defined recursively as follows:*
  - *If t is a veriable, i.e. $t = x_i$, then $\mathcal{A}(t) = \xi(x_i)$.*
  - *If t is of the form $f(t_1, \ldots, t_k)$ for terms $t_1, \ldots, t_k$ and a k-ary predicate symbol P, then $\mathcal{A}(t) = \phi(f)(\mathcal{A}(t_1), \ldots, \mathcal{A}(t_k))$.*
- *The truth value of a formula F is defined recursively by Definition 6.16 and*
  - *If F is of the form $F = P(t_1, \ldots, t_k)$ for term $t_1, \ldots, t_k$ and a k-ary predicate symbol P, then $\mathcal{A}(F) = \psi(P)(\mathcal{A}(t_1), \ldots, \mathcal{A}(t_k))$.*
  - *If F is of the form $\forall xG$ or $\exists xG$, then let $\mathcal{A}_{[x\to u]}$ for $u \in U$ be the same structure as $\mathcal{A}$ except that $\xi(x)$ is overwritten by u (i.e.,$\xi(x) = u$):*

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

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

Definition 6.37. *For any formulas F, G, and H, where x does not occur free in H, we have*

(i) $\neg(\forall xF) \equiv \exists x\neg F$;

(ii) $\neg(\exists xF) \equiv \forall x\neg F$;

(iii) $(\forall xF) \wedge (\forall xG) \equiv \forall x(F \wedge G)$;

(iv) $(\exists xF) \vee (\exists xG) \equiv \exists(F \vee G)$;

(v) $\forall x\forall yF \equiv \forall x\forall yF$;

(vi) $\exists x\exists yF \equiv \exists x\exists yF$;

(vii) $(\forall xF) \wedge H \equiv \forall(F \wedge H)$;

(viii) $(\forall xF) \vee H \equiv \forall(F \vee H)$;

(ix) $(\exists xF) \wedge H \equiv \exists(F \wedge H)$;

(x) $(\exists xF) \vee H \equiv \exists(F \vee H)$;

Lemma 6.7. *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.*

Lemma 6.8. *For a formula G in which y does not occure we have*

- $\forall xG \equiv \forall yG[x/y]$,
- $\exists xG \equiv \exists yG[x/y]$,

Definition 6.38. *A formula in which no variable occurs both as a bound and as a free variable and in which all variables appreaing after the quantifiers are distinct is said to be rectified form.*

Definition 6.39. *A formula of the form*

$$Q_1x_1 \cdots Q_nx_nG$$

where the Q_i are arbitrary quantifiers ($\forall$ or $\exists$) and G is a formula free of quantifiers, is said to be in prenex form.

Theorem 6.9. *For every formula there is an equivalent formula in prenex form.*

Lemma 6.10. *For any formula F and any term t we have*

$$\forall xF \models F[x/t]$$