Logic Symbols

F ⊨ F is Stmt

Stmt ⇒ Stmt

F → F is F

Proof Patterns

Direct Proof of an Implication

$S \Rightarrow T$ Assume S, prove T under this assumption

Indirect Proof of an Implication

$S \Rightarrow T$ Assume T is false, prove S is false under this assumption

Lemma 2.6: $\neg B \to \neg A \vDash A \to B$ ($\sqrt{x}$ is irrational, if x is)

Modus Ponens Prove statement S in 3 steps:

1. Find suitable statement R 2. Prove R 3. Prove $R \Rightarrow S$

Lemma 2.7 $A \wedge (A \to B) \vDash B$

Case Distinction Prove statement S in 3 steps:

1. Find finite list $R_1, \dots R_k$ of statements 2. Prove one R_i is true

3. Prove $R_i \Rightarrow S$ for $i = 1, \dots, k$

Lemma 2.8 $(A_1 \vee \dots \vee A_k) \wedge (A_1 \to B) \wedge (\dots) \wedge (A_k \to B) \vDash B$

Proof by Contradiction Prove statement S in 3 steps:

1. Find suitable statement T 2. Prove T is false

3. Assume S is false and prove (from assumption) that T is true (contradiction)

Lemma 2.9 $(\neg A \to B) \wedge \neg B \vDash A$

Existence Proof Consider set $\mathcal{X}$ of parameters where for each $x \in \mathcal{X}$ S_x is a statement. An existence proof is a proof of a statement, that S_x is true for at least one $x \in \mathcal{X}$. Constructive if there is a concrete example.

1: $\exists n(\text{prime}(n) \wedge \text{prime}(n+10) \wedge \text{prime}(n+10))$. Constructive proof: $P(13)$ true

Example 2: $\forall m \exists p(\text{prime}(p) \wedge p > m)$. Stmt S_p, parameterized by p

To prove we use fact, that every natural number $n \geq 2$ has at least one prime divisor. Consider $m!+1$. Observe that for k in range $2 \leq k \leq m$, $k \nmid m!+1$. Non constructively proof that there exists $p > m$ which divides $m!+1$.

Pigeonhole Principle (used for existence proofs)

If a set of n objects is partitioned into $k < n$ sets, then at least one of these sets contains at least $\lceil \frac{n}{k} \rceil$ objects. Proof by contradiction: Assume partition size max $\lceil \frac{n}{k} \rceil - 1$

$k(\lceil \frac{n}{k} \rceil - 1) < k((\frac{n}{k} - 1) + 1) = k(\frac{n}{k}) = n$

Example 1: In any subset A of $\{1, 2, \dots 2n\}$ of size $|A| = n+1$, there exist a, b such that $a | b$. Write $a_i = 2^{e_i} u_i$ with u_i odd. n possible values: $\{1, 3, 5, \dots 2n-1\}$. Thus there must exist two numbers a_i, a_j with same odd part. Therefore one of them has fewer factors 2 than the other.

Proof by Counterexample (used for existence proofs)

Proof of statement that S_x is not true for all $x \in \mathcal{X}$, by exhibiting an a such that S_a is false.

Proof by Induction 1. Basis step: Prove $P(0)$ 2. Induction step: $P(n) \Rightarrow P(n+1)$

Theorem 2.11: $U = \mathbb{N}$ and unary predicate P: $P(0) \wedge \forall n(P(n) \to P(n+1)) \Rightarrow \forall n\, P(n)$

Set Theory

Cardinality $|A|$ $A = \{n \in \mathbb{Z} \mid \exists k \in \mathbb{Z}\; n = 2k\}$

Def Set Equality

$A = B \overset{def}{\Longleftrightarrow} \forall x (x \in A \leftrightarrow x \in B)$

$A = B \Leftrightarrow (A \subseteq B) \wedge (B \subseteq A)$

Def of ordered pair

$(a,b) = (c,d) \overset{def}{\Longleftrightarrow} a = c \wedge b = d$

$(a,b) \overset{def}{=} \{a, \{a,b\}\}$

Def of subset

$A \subseteq B \overset{def}{\Longleftrightarrow} \forall x (x \in A \to x \in B)$

Def of $\emptyset$ $\forall x (x \notin \emptyset)$

Def of Power Set

$\mathcal{P}(A) \overset{def}{=} \{S \mid S \subseteq A\}$

$|\mathcal{P}(A)| = 2^{|A|}$

Def of Union

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

$\bigcup \mathcal{A} \overset{def}{=} \{x \mid x \in A \text{ for some } A \in \mathcal{A}\}$

Def of intersection

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

$\bigcap \mathcal{A} \overset{def}{=} \{x \mid x \in A \text{ for all } A \in \mathcal{A}\}$

Def of Complement

$\overline{A} \overset{def}{=} \{x \in U \mid x \notin A\} = \{x \mid x \notin A\}$

Def of Difference

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

Def of Cart. Product

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

$|A \times B| = |A| \cdot |B|$ for $1 \leq i \leq k$

$\times_{i=1}^{k} A_i = \{(a_1, \dots, a_k) \mid a_i \in A_i\}$

Lemma 3.1 $\{a\} = \{b\} \Rightarrow a = b$

Lemma 3.2 Only one empty set $\emptyset = \emptyset'$

Lemma 3.3 $\forall A (\emptyset \subseteq A)$ P.B.C

Natural numbers: $s(n) \overset{def}{=} n \cup \{n\}$

$0 \overset{def}{=} \emptyset$, $1 \overset{def}{=} \{\emptyset\} \Rightarrow 1 = s(0)$ $|s(n)| = n+1$

Def of +: $m + 0 \overset{def}{=} m$ and $m + s(n) \overset{def}{=} s(m+n)$

Theorem 3.4

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

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

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

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

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

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

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

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

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

Russell's Paradox

$R = \{A \mid A \notin A\}$ Either $R \in R$ or $R \notin R$

$\{x \mid P(x)\}$ is not well-defined but $\{x \in B \mid P(x)\}$ is.

Relations

$(a,b) \in \rho$ or $a \rho b$

Example Rel. For $\mathbb{Z}$: $=, \neq, \leq, \geq, <, >, |, \nmid$

Def of mod

$a \equiv_m b \overset{def}{\Longleftrightarrow} a - b = k \cdot m$ for some k

Def identity relation

$id_A = \{(a,a) \mid a \in A\}$

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

Def Composition of rel.

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

n-fold composition $\rho^n = \rho \circ \dots \circ \rho$

Def of transitive closure

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

Def of equivalence Relations $\equiv_m$ on $\mathbb{Z}$

reflexive, symmetric, transitive

Def of equivalence class $[x]$ $[y]$ are either equal or disjoint!!

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

Def of Partition A of mutually disjoint subsets of A, that cover A, i.e. a set $\{S_i \mid i \in I\}$

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

Def of Quotient set $A/\theta \overset{def}{=} \{[a]_\theta \mid a \in A\}$

Def of rat. Numbers $\mathbb{Q} \overset{def}{=} (\mathbb{Z} \times \mathbb{Z} \setminus \{0\})/\sim$

Def of partial order relation

reflexive, antisymmetric, transitive

Poset (Partially ordered set): $(A; \preceq)$

Def of comparable a and b are comparable if $a \preceq b$ or $b \preceq a$ for $(A; \preceq)$

Def of totally ordered If any two elements of poset are comparable

Lemma 3.5 comp. of rel. is associative $\rho \circ (\sigma \circ \phi) = (\rho \circ \sigma) \circ \phi$

Lemma 3.6 $\widehat{\rho\sigma} = \hat{\sigma}\hat{\rho}$

Def of reflexive $\geq, \leq, |$ on $\mathbb{Z} \setminus \{0\}$

$\forall a (a \rho a)$ i.e. $id \subseteq \rho$

Def of irreflexive

$\forall a (a \not\rho a)$ i.e. $\rho \cap id = \emptyset$

Def of symmetric $\equiv_m$ on $\mathbb{Z}$

$\forall a,b (a \rho b \Leftrightarrow b \rho a)$ i.e. $\rho = \hat{\rho}$

Def of antisymmetric $\leq, \geq, |$ on $\mathbb{N}$

$\forall a,b ((a \rho b \wedge b \rho a) \Rightarrow a = b)$ i.e. $\rho \cap \hat{\rho} \subseteq id$

Def of transitive $\leq, \geq, <, >, |, \equiv_m$ on $\mathbb{Z}$

$\forall a,b,c (a \rho b \wedge b \rho c \Rightarrow a \rho c)$ i.e. $\rho^2 \subseteq \rho$

Theorem 3.9 The set A/θ of equivalent classes of an equivalence relation θ on A is a partition of A

Def of well-ordered

$(A; \preceq)$ is well ordered, if every subset of A has a least element

Def of cover b covers a if $\nexists c (a \prec c \wedge c \prec b)$

Def of Hasse Diagrams Directed graph

V = elements of $(A; \preceq)$ $E = (a,b)$ if b covers a

Def of poset combination $(A; \preceq) \times (B; \sqsubseteq)$

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

Def of lexicographic order

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

Def of Meet Poset $(A; \preceq)$, $\{a,b\} \subseteq A$

greatest lower bound is called meet of a, b: $a \wedge b$

Elements in Poset $(A; \preceq)$ poset $S \subseteq A$

min/max Element $\nexists b \in A (b \prec a) \| (b \succ a)$

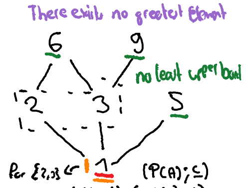
least/greatest Element $\forall b \in A (a \preceq b) \| (a \succeq b)$

lower (upper) bound $\forall b \in S (a \preceq b) \| (a \succeq b)$

greatest lower bound (least upper bound) of S if a is the greatest (least) element of set of all lower (upper) bounds of S

Def of join Poset $(A; \preceq)$, $\{a,b\} \subseteq A$

least upper bound is called join of a, b: $a \vee b$



$(\mathcal{P}(A); \subseteq)$

Ex: $(\mathbb{N}; \leq)$, $(\mathbb{N} \setminus \{0\}; |)$,

Def Lattice $(A; \preceq)$ in which every pair has a meet and join

Functions

Def Function $f: A \to B$ ($a f b$)

Relation from Domain A to Codomain B

1. $\forall a \in A\; \exists b \in B\; a f b$ (f is totally defined)

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

Def partial function ② holds

Def Composition of a function

$f: A \to B$, $g: B \to C$, $g \circ f = gf$: $(g \circ f)(a) = g(f(a))$

Def Image range

$f(A) = \text{Im}(f)$

Def of preimage

$f: A \to B$, $T \subseteq B$ $f^{-1}(T) \overset{def}{=} \{a \in A \mid f(a) \in T\}$

Def image of subset $S \subseteq A$

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

Lemma 3.12 Function composition is associative: $(h \circ g) \circ f = h \circ (g \circ f)$

Def of injective one-to-one injection

$a \neq b \Rightarrow f(a) \neq f(b)$

Def of surjective onto

$\text{Im}(f) = B$, $\forall b \in B\; \exists a \in A (b = f(a))$

Def of bijective bijection

injective and surjective

Countability

Equinumerous $A \sim B$, if there exists bijection $A \to B$

Dominates Set B dominates A ($A \preceq B$), if $A \sim C$, $C \subseteq B$

i.e. there exists an injective function $A \to B$

Countable if $A \preceq \mathbb{N}$ uncountable otherwise

Theorem 3.16 $\{0,1\}^* \overset{def}{=} \{\epsilon, 0, 1, 00, 01, 10, \dots\}$ of finite binary sequences is countable.

Proof: 1+ binary sequence to $\mathbb{N}$ (injection)

Theorem 3.20 Let A and A_i for $i \in \mathbb{N}$ be countable

(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 $A_0, A_1, A_2, \dots$ of countable sets is countable.

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

Lemma 3.13 (i) The relation $\preceq$ is transitive: $A \preceq B \wedge B \preceq C \Rightarrow A \preceq C$

(ii) $A \subseteq B \Rightarrow A \preceq B$ (Proof by Identity function on A)

Theorem 3.14 $A \preceq B \wedge B \preceq A \Rightarrow B \sim A$

Def of Countable A is countable if and only if it is finite or $A \sim \mathbb{N}$

Theorem 3.17 $\mathbb{N} \times \mathbb{N}$ ($= \mathbb{N}^2$) of ordered pairs is countable

Proof: $\mathbb{N} \sim \{0,1\}^*$ hence $\mathbb{N} \times \mathbb{N} \sim \{0,1\}^* \times \{0,1\}^*$ Show bijection

Corollary 3.18: $A \times B$ of two countable sets A and B is countable

Def semi infinite binary sequence $\{0,1\}^\infty$

Theorem 3.21 The set $\{0,1\}^\infty$ is uncountable

Proof by contradiction: Cantors Diagonalization argument.

Def computable Functions $f: \mathbb{N} \to \{0,1\}$ is called computable if there is a program that, for any $n \in \mathbb{N}$, when given Input n, outputs $f(n)$.

Corollary 3.22 There are uncomputable Functions $\mathbb{N} \to \{0,1\}$

Number Theory

Theorem 4.1 (Euclid) For all Integers a and $d \neq 0$ there exists unique Integers q and r satisfying:

$a = d \cdot q + r$ and $0 \leq r < |d|$

Def of Ideal

$(a,b) := \{ua + vb \mid u,v \in \mathbb{Z}\}$

$(a) := \{ua \mid u \in \mathbb{Z}\}$

Def of least common multiple

$a | l \wedge b | l \wedge \forall m((a | m \wedge b | m) \to l | m)$

Def of modular congruence

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

Lemma 4.13 For any $m \geq 1$, $\equiv_m$ is equivalence relation

Lemma 4.17

$R_m(f(a_1, \dots, a_k)) = R_m(f(R_m(a_1), \dots R_m(a_k)))$

Def greatest common divisor

$d | a \wedge d | b \wedge \forall c((c | a \wedge c | b) \to c | d)$

Def of relatively prime $\gcd(a,b) = 1 \Rightarrow a$ and b are relatively prime

Lemma 4.2 $\gcd(m, n - qm) = \gcd(m, n)$

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

Lemma 4.4 $a, b \in \mathbb{Z}$ (not both 0) If $(a,b) = (d)$, then d is $\gcd(a,b)$

Corollary 4.5 $\exists u,v (\gcd(a,b) = ua + vb)$

GCD & LCM $a = \prod_i p_i^{e_i}$ $b = \prod_i p_i^{f_i}$

$\gcd(a,b) = \prod_i p_i^{\min(e_i, f_i)}$ $\text{lcd}(a,b) = \prod_i p_i^{\max(e_i, f_i)}$ $\Rightarrow \gcd(a,b) \cdot \text{lcd}(a,b) = a \cdot b$

Lemma 4.14 If $a \equiv_m b$ and $c \equiv_m d$, then $a + c \equiv_m b + d$ and $ac \equiv_m bd$

Lemma 4.16 (i) $a \equiv_m R_m(a)$

(ii) $a \equiv_m b \Leftrightarrow R_m(a) = R_m(b)$

Lemma 4.18 $ax \equiv_m 1$ has solution if $\gcd(a,m) = 1$. It's unique

Def multiplicative inverse of a modulo m 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. $x \equiv_m a^{-1}$ or $x \equiv_m 1/a$

Chinese Remainder Theorem Let $m_1, \dots, m_r$ be pairwise relatively prime integers and let $M = \prod_{i=1}^{r} m_i$. For every list $a_1, \dots a_r$ with $0 \leq a_i \leq m_i$ for $1 \leq i \leq r$, the system of congruence equations $x \equiv_{m_1} a_1$, $x \equiv_{m_2} a_2$, … for x has a unique solution x satisfying $0 \leq x < M$

Algebra Groups

Def of neutral element
left (right) neutral element
$e * a = a \; [a * e = a]$ for all $a \in S$

Def of Associativity
$a * (b * c) = (a * b) * c$ for all $a, b, c \in S$

Def of monoid $\langle M; *, e \rangle$
$*$ is associative and e is the neutral element

Def of inverse
left [right] inverse element
$b * a = e \; [a * b] = e$

Lemma 5.3 $\langle G; *, \hat{}, e \rangle$
(i) $\hat{\hat{a}} = a$ P: $\hat{\hat{a}} = \hat{\hat{a}} * e = \hat{\hat{a}} * (\hat{a} * a) = (\hat{\hat{a}} * \hat{a}) * a = e * a = a$
(ii) $\widehat{a * b} = \hat{b} * \hat{a}$ P: $\widehat{a * b} = (\widehat{a * b}) * (a * (b * \hat{b}) * \hat{a}) = (\widehat{a * b}) * (a * b) * \hat{b} * \hat{a}$
$= e * (\hat{b} * \hat{a}) = \hat{b} * \hat{a}$
(iii) left cancellation law $a * b = a * c \Rightarrow b = c$
(iv) right cancellation law $b * a = c * a \Rightarrow b = c$
(v) $a * x = b$ has unique solution for any a, b

Def direct product of groups
Product of $\langle G_1; *_1 \rangle \dots \langle G_n; *_n \rangle$ is $\langle G_1 \times \dots \times G_n; * \rangle$
where $(a_1, \dots, a_n) * (b_1, \dots, b_n) = (a_1 *_1 b_1, \dots, a_n *_n b_n)$

Def of group Homomorphism
$\langle G; *, \hat{}, e \rangle$ and $\langle H; \star, \tilde{}, e' \rangle$ $\psi: G \to H$
$\psi(a * b) = \psi(a) \star \psi(b)$. If ψ bijection it's an isomorphism. $G \simeq H$ "isomorphic"

Def of subgroup $H \leq G$
Subset H is called subgroup if $\langle H; *, e, \hat{} \rangle$ is a group. (1) $a * b \in H$ for all $a, b \in H$
(2) $e \in H$ (3) $\hat{a} \in H$ for all $a \in H$

Def of order
$\mathrm{ord}(a)$, is the least $m \geq 1$ such that $a^m = e$ if m exists. else $\mathrm{ord}(a) = \infty$
$\mathrm{ord}(e) = 1$. $\mathrm{ord}(a) = 2 \Rightarrow a$ is self-inverse
$|G|$ is the order of G.

Def of cyclic groups
$\langle a \rangle \overset{def}{=} \{a^n \mid n \in \mathbb{Z}\}$ for a group G
for finite groups: $\langle a \rangle = \{e, a, a^2, \dots, a^{\mathrm{ord}(a)-1}\}$
A group $G = \langle g \rangle$ generated by generator g is called cyclic.

Def of $\mathbb{Z}_m^*$
$\mathbb{Z}_m^* \overset{def}{=} \{a \in \mathbb{Z}_m \mid \gcd(a, m) = 1\}$

Def of euler function
$\varphi: \mathbb{Z}^+ \to \mathbb{Z}^+$ $\varphi(m) = |\mathbb{Z}_m^*|$
if n is prime $\varphi(m) = m - 1$
$\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$

Corollary 5.14 (Fermat, Euler)
For all $m \geq 2$ and all a with $\gcd(a, m) = 1$
$a^{\varphi(m)} \equiv_m 1$ | For every prime p and a not divisible by p: $a^{p-1} \equiv_p 1$

Lemma 5.1 P: $e = e * e' = e'$
If $\langle S; * \rangle$ has right and left neutral element then they are equal. $\langle S; * \rangle$ has at most 1.

Lemma 5.2 In a monoid, if a has left and right inverse, they are equal
P: $\hat{a} = \hat{a} * e = \hat{a} * (a * \hat{a}') = (\hat{a} * a) * \hat{a}' \dots$

Def of abelian (comm.)
$\langle G; * \rangle$ if $a * b = b * a$ for all $a, b \in G$

Def of group $\langle G; *, \hat{}, e \rangle$
G1 $*$ is associative
G2 e is the neutral element
G3 Every $a \in G$ has inverse $\hat{a}$

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

Lemma 5.5 if ψ: Homomorphism
(i) $\psi(e) = e'$ P: $\psi(a) = \psi(a) \star \psi(e)$
(ii) $\psi(\hat{a}) = \widetilde{\psi(a)}$
P: $\psi(\hat{a}) = \psi(\hat{a}) \star (\psi(a) \star \widetilde{\psi(a)})$

Lemma 5.6 In a finite group G every element has a finite order.
P: $a^r = a^s = b \Rightarrow a^{s-r} = a^s \cdot a^{-r} = b \cdot b^{-1} = e$

Theorem 5.7 A cyclic group of order n is isomorphic to $\langle \mathbb{Z}_n; \oplus \rangle$

Theorem 5.8 (Lagrange) $H \leq G$
H subgroup of G. $|H|$ divides $|G|$

Corollary 5.9 $\mathrm{ord}(a)$ divides $|G|$ for every $a \in G$

Corollary 5.10 G is a finite group. $a^{|G|} = e$ for every $a \in G$
P: $|G| = k \cdot \mathrm{ord}(a)$
$a^{|G|} = a^{k \cdot \mathrm{ord}(a)} = (a^{\mathrm{ord}(a)})^k = e^k = e$

Corollary 5.11 Every group of prime order is cyclic and every element except the neutral element is a generator

Lemma 5.12 if the prime factorization of $m = \prod_{i=1}^{r} p_i^{e_i}$ 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.

Theorem 5.15
The group $\mathbb{Z}_m^*$ is cyclic if $m = 2$, $m = 4$, $m = p^e$ or $m = 2p^e$ p odd prime

Def e-th roots in a group
G: finite group and $e \in \mathbb{Z}$ be relatively prime to $|G|$. 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 multiplicative inverse of e modulo $|G|$
$ed \equiv_{|G|} 1$
P: $(x^e)^d = x^{ed} = x^{k \cdot |G| + 1} = (x^{|G|})^k \cdot x = x$

Rings & Fields

Def of Ring $\langle R; +, -, 0, \cdot, 1 \rangle$
(i) $\langle R; +, -, 0 \rangle$ is a commutative group
(ii) $\langle R; \cdot, 1 \rangle$ is monoid
(iii) $a(b + c) = (ab) + (ac)$ and $(b + c)a = (ba) + (ca)$ for all $a, b, c \in R$ (left and right distribution laws)
A ring is called commutative, if $ab = ba$

Def of characteristics
is the order of 1 in the additive Group if it is finite and otherwise the characteristic is defined to be 0.
Ex: $\langle \mathbb{Z}_m; \oplus, \ominus, 0, \odot, 1 \rangle$ has characteristic m.

Def of integral domain a nontrivial $(1 \neq 0)$ commutative ring without zero-divisors $\forall a, b \, (ab = 0 \to a = 0 \lor b = 0)$

Def polynomial ring
$a(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_1 x + a_0 = \sum_{i=1}^{d} a_i x^i$
for some non-negative integer, with $a_i \in R$. $R[x]$ is the set of polynomials (in x) over R.

Def of Field a nontrivial commutative ring F in which every nonzero element is a unit
$F^* = F \setminus \{0\}$

Def of monic $a(x) \in F[x]$ is monic if leading coefficient is 1

Def of irreducible
$a(x) \in F[x]$ with $\deg(a(x)) \geq 1$ is irreducible if it is divisible only by constant polynomials and by constant multiple of $a(x)$

Def of greatest common divisor
$g(x)$ of largest degree $\gcd(a(x), b(x))$

Def of root $a(x) \in R[x]$.
$\alpha \in R$ for which $a(\alpha) = 0$ is called root of $a(x)$

Def of multiplicity
If α is root of $a(x)$ then multiplicity is the highest power of $x - \alpha$ dividing $a(x)$.

Theorem 5.30 For a field F, a nonzero polynomial $a(x) \in F[x]$ of degree d has at most d roots, counting multiplicities.

Lemma 5.31 A polynomial $a(x) \in F[x]$ of degree d is uniquely determined by any $d+1$ values of $a(x)$. i.e by any $a(\alpha_1), \dots, a(\alpha_{d+1})$ for any distinct $\alpha_1, \dots, \alpha_{d+1} \in F$

Lemma 5.17 $\langle R; +, -, 0, \cdot, 1 \rangle$
(i) $0a = a0 = 0$
(ii) $(-a)b = -(ab)$ more than
(iii) $(-a)(-b) = ab$ 1 element
(iv) If R is non-trivial, then $1 \neq 0$

Lemma 5.18
(i) If $a \mid b$ and $b \mid c$, then $a \mid c$
(ii) If $a \mid b$, then $a \mid bc$ for all c
(iii) If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$

Def of greatest common divisor
$d \mid a \land d \mid b \land \forall c ((c \mid a \land c \mid b) \to c \mid d)$

Def of unit In commutative ring
$u \in R$ is unit if u is invertible, i.e
$uv = vu = 1$ for some $v \in R$ $(v = u^{-1})$
The set of units is denoted by R^*

Lemma 5.19 For a ring R, R^* is a multiplicative Group

Def of zerodivisor $a \neq 0$ is zerodivisor if $ab = 0$ for some $b \neq 0$

Def of degree $\deg(a(x))$ is the greatest i for which $a_i \neq 0$.
$\deg(0) = -\infty$

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

Lemma 5.22
(i) If D is integral domain, so is $D[x]$
(ii) The units of $D[x]$ are the constant polynomials that are units of D:
$D[x]^* = D^*$

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

Theorem 5.25 Let F be a field
For any $a(x)$ and $b(x) \neq 0$ in $F[x]$ there exist a unique $q(x)$ and $r(x)$
$a(x) = b(x) q(x) + r(x)$ $\deg(r(x)) < \deg(q(x))$

Lemma 5.28
For a field F, $\alpha \in F$ is a root of $a(x)$ if and only if $x - \alpha$ divides $a(x)$

Corollary 5.29 A polynomial $a(x)$ of degree 2 or 3 over a field F is irreducible if and only if it has no root.

Lagrange interpolation formula
$a(x) = \sum_{i=1}^{d+1} \beta_i u_i(x)$ where
$\beta_i = a(\alpha_i)$ and $(x - \alpha_i)$ is not there
$u_i(x) = \frac{(x - \alpha_1) \dots (x - \alpha_{i-1})(x - \alpha_{i+1}) \dots}{(\alpha_i - \alpha_1) \dots (\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1}) \dots}$
same

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

Def of (n-k)-error-correcting-code
An (n,k)-error-correcting-code over the alphabet A with $|A| = q$ is a subset of A^n of cardinality q^k

Def of hamming Distance The Hamming distance between two strings of equal length over a finite alphabet A is the number of positions at which the two strings differ.

Def of minimum distance The minimum distance of an error-correcting-code C is the minimum of the hamming distances between any two codewords.

Def of decoding-function $D: A^n \to A^k$

Def of t-error correcting A decoding function D is t-error-correcting for encoding function E if for any $(a_0, \dots, a_{k-1})$
$D((r_0, \dots, r_{n-1})) = (a_0, \dots, a_{k-1})$ for any $(r_0, \dots, r_{n-1})$ with hamming distance at most t from $E((a_0, \dots, a_{k-1}))$. A code is t-error correcting if there exists E and D with $C = \mathrm{Im}(E)$ where D is t-error correcting

Theorem 5.40 A code C with minimum distance d is t-error correcting if and only if $d \geq 2t + 1$

Theorem 5.41 Let $A = GF(q)$ and let $\alpha_0, \dots, \alpha_{n-1}$ be arbitrary distinct elements of $GF(q)$. Consider the encoding function
$E((a_0, \dots, a_{k-1})) = (a(\alpha_0), \dots, a(\alpha_{n-1}))$ where $a(x)$ is the polynomial
$a(x) = a_{k-1} x^{k-1} + \dots + a_1 x + a_0$. This code has minimum distance of $n - k + 1$

Proof Systems

Def of Proof-System $\Pi = (S, P, \tau, \phi)$

Def of sound Π is sound, if no false statement has a proof.
i.e. if for all $s \in S$ for which there exists $p \in P$ with $\phi(s, p) = 1$, $\tau(s) = 1$

Def of complete Π is complete if every true statement has a proof. i.e. for all $s \in S$ with $\tau(s) = 1$, there exists $p \in P$ with $\phi(s, p) = 1$

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

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

Def of interpretation Consists of a set $Z \subseteq \Lambda$ of symbols of Λ, a domain (a set of possible values) for each symbol in Z, and a function that assigns to each symbol in Z a value in its associated domain.

Def of suitable An interpretation is suitable for a formula F if it assigns a value to all symbols $\beta \in \Lambda$ occurring free in F

Def of truth values 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 $\mathcal{A}$.

Def of model A suitable interpretation $\mathcal{A}$ with $\mathcal{A}(F)$ is a model for F. $\mathcal{A} \models F$. 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
$\mathcal{A} \models M$. If $\mathcal{A}$ is not a model $\mathcal{A} \not\models M$

Def of satisfiable F or M is satisfiable if there exists a model for F (or M), and unsatisfiable otherwise. $\perp$ is used for unsatisfiable formula

Def of tautology A formula F is called tautology or valid if it is true for every suitable interpretation. $\top$ for tautology

Def of logical consequence $F \models G$ (or $M \models G$) if every interpretation suitable both for F (or M) and G, which is a model for F is also a model for G

Def of equivalent $F \equiv G \overset{def}{\iff} F \models G$ and $G \models F$

Def of F is tautology $\models F$

Def of recursive formulas If F and G are formulas, so is $\neg F$, $(F \land G)$, $(F \lor G)$

Def of semantics $\land \lor \neg$
$\mathcal{A}((F \land G)) = 1$ if and only if $\mathcal{A}(F) = 1$ and $\mathcal{A}(G) = 1$
$\mathcal{A}((F \lor G)) = 1$ if and only if $\mathcal{A}(F) = 1$ or $\mathcal{A}(G) = 1$
$\mathcal{A}(\neg F) = 1$ if and only if $\mathcal{A}(F) = 0$

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

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:
1. $\{F_1, F_2, \dots, F_k\} \models G$
2. $(F_1 \land F_2 \dots \land F_k) \to G$ is a tautology
3. $\{F_1, F_2, \dots, F_k, \neg G\}$ is unsatisfiable

Def of derivation rule $\{F_1, \dots F_k\} \vdash_R G$ if G can be derived from $\{F_1, \dots, F_k\}$ by rule R

Def application of rule 1. select $N \subseteq M$ 2. $N \vdash_R G$ 3. add G to M

Def of calculus A calculus K is a finite set of derivation rules $K := \{R_1, \dots\}$

Def of derivation $M \vdash_K G$ if G can be derivated with calculus K

Def of correct rule $M \vdash_R F \Rightarrow M \models F$

Def of correct calculus correct or sound: $M \vdash_K F \Rightarrow M \models F$

Def of complete calculus $M \models F \Rightarrow M \vdash_K F$

Lemma 6.4 If $\{F_1, \dots, F_k\} \vdash_K F$ holds for a sound calculus, then
$\models ((F_1 \land \dots \land F_k) \to G)$

Propositional Logic

Def of atomic Formula A_i with $i \in \mathbb{N}$. ← Syntax

Def of truth assignment $\mathcal{A}(F) = \mathcal{A}(A_i)$ $\mathcal{A}: Z \to \{0, 1\}$

Def of a literal Atomic formula or its negation.

Def CNF Conjunctive normal form

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

Def DNF Disjunctive normal form

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

Theorem 6.5 Every formula is equivalent to a formula in CNF and DNF

Def of clause Set of literals

Def set of clauses $F = (L_{11} \vee \dots \vee L_{1m_1}) \wedge \dots$

$\mathcal{K}(F) = \{\{L_{11}, \dots, L_{1m_1}\}, \dots\}$ $M = \{F_1, \dots, F_k\}$

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

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

Lemma 6.6 The resolution calculus is sound, i.e. if $\mathcal{K} \vdash_{Res} K$ then $\mathcal{K} \models K$

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

Predicate Logic (First order logic)

Def Syntax of predicate logic

- Variable symbol: x_i with $i \in \mathbb{N}$
- function symbol: $f_i^{(k)}$ with $i,k \in \mathbb{N}$
  - $\rightarrow$ if $k=0 \Rightarrow f_i$ is a constant
- predicate symbol: $P_i^{(k)}$ with $i,k \in \mathbb{N}$
- term: inductively. $t_1, \dots, t_k$ then $f_i^{(k)}(t_i)$ is term
- Formula: - for any i and k $P_i^{(k)}(t_1, \dots, t_k)$ is an atomic formula $(F \vee G)$, $\neg F$
  - If F and G are formulas, so is $(F \wedge G)$
  - If F formula then $\forall x_i F$, $\exists x_i F$ as well

Def of bound and free If variable occurs in a (sub)formula of the form $\forall x G$ or $\exists x G$, then it's bound. otherwise it's free. If no free variable, G is closed

Def of substitution $F[x/t]$ denotes the formula obtained from F by substituting every x by t.

Def of interpretation $\mathcal{A} = (U, \phi, \psi, \xi)$

- U: non-empty set, the universe
- ϕ: assigns function to function symbols $\phi(f): U^k \rightarrow U$
- ψ: assigns function to predicate symbols $\psi(P): U^k \rightarrow \{0,1\}$
- ξ: assigns value in U to a free variable

Def of semantics

- $\mathcal{A}(t)$ is defined recursively
  - if t is a variable, i.e. $t = x_i$, then $\mathcal{A}(t) = \xi(x_i)$
  - if t is of form $f(t_1, \dots, t_k)$, then $\mathcal{A}(t) = \phi(f)(\mathcal{A}(t_1) \dots)$
- Truth value of F
  - if $F = P(t_1, \dots, t_k)$, then $\mathcal{A}(F) = \psi(P)(\mathcal{A}(t_1) \dots \mathcal{A}(t_k))$
  - if F is $\forall x G$ or $\exists x G$

    $\mathcal{A}(\forall x G) = 1$ if $\mathcal{A}_{[x \rightarrow u]}(G) = 1$ for all $u \in U$

    $\mathcal{A}(\exists x G) = 1$ if $\mathcal{A}_{[x \rightarrow u]}(G) = 1$ for some $u \in U$

Lemma 6.8

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

Lemma 6.9 If one replaces sub-formula G of F by an equivalent formula H, the the formula is equivalent to F

Lemma 6.10 $\forall x G \equiv \forall y G[x/y]$, $\exists x G \equiv \exists y G[x/y]$

Def of rectified No variable occurs free and bound in F

Lemma 6.11 $\forall x F \models F[x/t]$

Def of prenex form $Q_1 x_1 Q_2 x_2 \dots Q_n x_n G$

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

Diffie-Hellman protocol

Public: p/g

1. A selects $x_A \in \{0, \dots, p-2\}$ (secret key)
2. A calculates $y_A = R_p(g^{x_A})$ (public)
3. B selects $x_B \in \{0, \dots, p-2\}$ (secret key)
4. B calculates $y_B = R_p(g^{x_B})$ (public)
5. A & B exchange y_A and y_B
6. A calculates $k_{AB} = R_p(y_B^{x_A})$
7. B calculates $k_{BA} = R_p(y_A^{x_B})$

$k_{AB} = k_{BA}$

RSA

1. Generate primes p and q
   $n = p \cdot q \Rightarrow |\mathbb{Z}_n^*| = \varphi(n) = (p-1)(q-1)$
   $f = (p-1)(q-1)$
2. Select e (e relatively prime to f)
   $d \equiv_f e^{-1}$
   } Alice
3. send n, e to Bob } insecure
4. plaintext $m \in \{1, \dots, n-1\}$
5. Ciphertext $y = R_n(m^e)$
   } Bob
6. send y to Alice } insecure
7. $m = R_n(y^d)$ } Alice

Galois Fields

$GF(p)$ exist if p^n where p is prime.

$GF(16) = GF(2^4) \Rightarrow |GF(2^4)^*| = 15$

$\quad \nwarrow GF(16) \setminus \{0\}$

Example for GF(16): $GF(2)[x]_{x^4+x+1}$

GF(81): $GF(3)[x]_{x^4+x+1}$

Generator of $GF(16)^*$

Lagrange: possible $|H| = 1, 3, 5, 15$

Take arbitrary $x \in GF(16)^*$

Check: x^1, x^3, x^5, x^{15}. If only $x^{15} = e$ then x is generator of $GF(16)^*$

Nice to know: irreducible polynomials

GF(2)[x]

- x ; $x+1$
- x^2+x+1
- x^3+x+1 ; x^3+x^2+1
- x^4+x+1 ; $x^4+x^3+x^2+x+1$; x^4+x^3+1
- x^5+x^2+1 ; x^5+x^3+1 ; $x^5+x^3+x^2+x+1$

GF(3)[x]

- x ; $x+1$; $2x$; $2x+1$; $x+2$; $2x+2$
- x^2+x+2 ; x^2+2x+2
- x^3+2x+1 ; x^3+2x^2+1
- x^4+x+2 ; x^4+2x^3+2
- x^5+2x+1 ; x^5+x^4+2x+1

Test irreducibility

- Deg 1 always irreducible by definition.
- Deg 2/3 irreducible $\Leftrightarrow$ no roots (5.29)
- Deg 4: No root and no irreducible factor of Deg 2
- Deg >4: No roots and no irreducible factor of deg d/2

Nice to know: Zerodivisors

\# of Zerodivisors: $|m| - \varphi(m) - 1$

Since $\varphi(m)$ is the number of units and 1 is the element 0.

Find zerodivisors $\mathbb{Z}_m$: $\{a \mid \gcd(a,m) \neq 1\} \setminus \{0\}$

since for all units $\gcd(u,m) = 1$

How to calculate gcd easily

1. prime factorization of both numbers
2. Product of common prime factors is gcd

$\gcd(234, 345)$

$234 = 2 \cdot 117 = 2 \cdot 3 \cdot 39 = 2 \cdot \underline{3} \cdot 3 \cdot 13$

$345 = 5 \cdot 69 = 5 \cdot \underline{3} \cdot 23 \Rightarrow \gcd = 3$

CRT application

1) x is unique
2) $x = R_M\left(\sum_{i=1}^{r} a_i M_i N_i\right)$

$M = \prod_{i=1}^{r} m_i \quad M_i = \frac{M}{m_i}$

$M_i N_i \equiv_{m_i} 1 \Rightarrow N_i \equiv_{m_i} M_i^{-1}$

$x \equiv_4 2$

$x \equiv_3 1$

$M = 4 \cdot 3 = 12$

$M_1 = \frac{M}{4} = 3$

$M_2 = \frac{M}{3} = 4$

$3 N_1 \equiv_4 1 \Rightarrow N_1 = 3$

$4 N_2 \equiv_3 1 \Rightarrow N_2 = 1$

$x = R_{12}(2 \cdot 3 \cdot 3 + 1 \cdot 4 \cdot 1) = R_{12}(10) = \underline{\underline{10}}$

CRT if non-coprime m_i

$a \equiv_{m \cdot n \cdot q} b \Rightarrow a \equiv_m b \quad a \equiv_n b \quad a \equiv_q b$

$x \equiv_{10} 6 \qquad 10 = 2 \cdot 5$

$x \equiv_{15} 11 \qquad 15 = 3 \cdot 5$

$x \equiv_{10} 6 \Rightarrow x \equiv_2 6 \equiv_2 0$

$\qquad x \equiv_5 6 \equiv_5 1$

$x \equiv_{15} 11 \Rightarrow x \equiv_3 11 \equiv_3 2$

$\qquad x \equiv_5 11 \equiv_5 1$

CRT mit $m_1 = 2$, $m_2 = 5$, $m_3 = 3$

Example proofs with sets

$x \simeq y \overset{def}{\Leftrightarrow} x \cdot y^{-1} \in H \qquad H \leq G$

To prove: $[x] = \{h \cdot x \mid h \in H\}$

($\subseteq$) Let $z \in [x]$ be arbitrary. Let $x \in G$

$\Rightarrow z \simeq x$ (def equiv. class)

$\Rightarrow z \cdot x^{-1} \in H$ (def $\simeq$)

$\Rightarrow (z \cdot x^{-1}) \cdot x \in \{h \cdot x \mid h \in H\}$

$\Rightarrow z \cdot (x^{-1} \cdot x) \in \{h \cdot x \mid h \in H\}$ (Ass. $\cdot$)

$\Rightarrow z \cdot e \in \{h \cdot x \mid h \in H\}$ (Def inv.)

$\Rightarrow z \in \{h \cdot x \mid h \in H\}$ (Def of neutr.)

($\supseteq$) let $z \in \{h \cdot x \mid h \in H\}$ be arbitrary

$\Rightarrow \exists h (z = h \cdot x)$ (Def of set)

$\Rightarrow \exists h (z \cdot x^{-1} = (h \cdot x) \cdot x^{-1})$ (Right mult.)

$\Rightarrow \exists h (z \cdot x^{-1} = h \cdot (x \cdot x^{-1}))$ (Ass. of $\cdot$)

$\Rightarrow \exists h (z \cdot x^{-1} = h \cdot e)$ (Def of inv)

$\Rightarrow \exists h (z \cdot x^{-1} = h)$ (Def of neutr.)

$\Rightarrow z \simeq x$ (Def of $\simeq$)

$\Rightarrow z \in [x]$

Some missed lemmas for finite fields

Lemma 5.32 Congruence modulo $m(x)$ is an equivalence relation on $F[x]$ and each equivalence class has a representative with degree less than $\deg(m(x))$

Lemma 5.33 Let F be a finite field with q elements and let $m(x)$ be a polynomial of degree d over F. Then $|F[x]_{m(x)}| = q^d$

Lemma 5.34 $F[x]_{m(x)}$ is a ring in respect to addition/mult. modulo $m(x)$

Lemma 5.35 The congruence equation $a(x) \cdot b(x) \equiv_{m(x)} 1$ (for given $a(x)$) has a unique solution $b(x) \in F[x]_{m(x)}$ if and only if $\gcd(a(x), b(x)) = 1$.

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

Theorem 5.36 The ring $F[x]_{m(x)}$ is a field if and only if $m(x)$ is irreducible

Theorem 5.37 For every prime p and every $d \geq 1$ there exists an irreducible polynomial of degree d in $GF(p)[x]$. In particular, there exists a finite field with p^d elements.

Theorem 5.38 There exist finite field with q element if q is power of prime and two fields with same size q are isomorphic.

Theorem 5.39 Multiplicative group of every finite field $GF(q)$ is cyclic. Order is $q-1$ and $q-1$ generators.

CNF & DNF

A	B	$B \wedge (\neg B \rightarrow A)$
0	0	0
0	1	1
1	0	0
1	1	1

CNF: $(\neg A \wedge B) \vee (A \wedge B)$

"or" all rows with 1.

DNF: $(A \vee B) \wedge (\neg A \vee B)$

"and" all rows with 0. Negate Literals!

Algebra Examples

Monoid: $\langle \mathbb{Z}; +, 0 \rangle$, $\langle \mathbb{Z}; \cdot, 1 \rangle$, $\langle \mathbb{Q}; +, 0 \rangle$, $\langle \mathbb{R}; +, 0 \rangle$, $\langle R[x]; \cdot \rangle$, $\langle \mathbb{R}; \cdot, 1 \rangle$, $\langle \mathbb{Z}_m; \oplus, 0 \rangle$, $\langle \mathbb{Z}_m; \odot, 1 \rangle$, $\langle \Sigma^*; \|, \varepsilon \rangle$, $\langle A^A; \circ, id \rangle$

Group $\langle \mathbb{Z}; +, -, 0 \rangle$, $\langle \mathbb{Q}; +, -, 0 \rangle$, $\langle \mathbb{Q} \setminus \{0\}, \cdot, ^{-1}, 1 \rangle$, $\langle \mathbb{R}; +, -, 0 \rangle$, $\langle \mathbb{R} \setminus \{0\}; \cdot, ^{-1}, 1 \rangle$, $\langle \mathbb{Z}_n; \oplus, \ominus, 0 \rangle$

Ring $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, $\langle \mathbb{Z}_m; \oplus, \ominus, 0, \odot, 1 \rangle$, $\mathbb{Z}_3 \times \mathbb{Z}_3$

Integral Domain $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}[x]$

Field $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, $\mathbb{Z}_p[x]_{irreducible}$, $GF(p^q)$

Number of Isomorphisms

\# Isomorphisms = \# generators, since each generator can be mapped to another generator.

Set Proofs

Infinite amount of sets A with $A \subseteq P(A)$ Induction

Base Case: $\{\emptyset\} \subseteq P(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$. Now we show that $A \subseteq P(A)$
$\Rightarrow P(A) \subseteq P(P(A))$: Let $S \in P(A)$ be arbitrary.
$S \in P(A) \Rightarrow S \subseteq A \Rightarrow S \subseteq P(A) \Rightarrow S \in P(P(A)) \Rightarrow P(A) \subseteq P(P(A))$

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

Let $b \in B$ be arbitrary. Case distinction:
1.) $b \in A$: $b \in A \Rightarrow b \in (A \cup B) \wedge b \in (A \cap B) \Rightarrow b \notin (A \cup B)\setminus(A \cap B) \Rightarrow b \notin (A \cup C)\setminus(A \setminus C)$
$\Rightarrow b \in (A \cap C) \Rightarrow b \in C$
2.) $b \notin A$: $b \in (A \cup B) \wedge b \notin (A \cap B) \Rightarrow b \in (A \cup B)\setminus(A \cap B) \Rightarrow b \in (A \cup C)\setminus(A \cap C)$
$\Rightarrow b \in (A \cup C) \Rightarrow b \in C \Rightarrow B \subseteq C$ (same for $C \subseteq B$)

$A \subseteq B \iff P(A) \subseteq P(B)$ ($\Rightarrow$) Let B be any set and $A \subseteq B$. Let $S \in P(A)$ arbitrary then by def of P $S \subseteq A$. By assumption that $A \subseteq B$ and by transitivity of $\subseteq$ it follows that $S \subseteq B \Rightarrow S \in P(B)$ ($\Leftarrow$) Let A, B be any sets and assume $P(A) \subseteq P(B)$ since $A \in P(A)$ and by assumption $P(A) \subseteq P(B)$ we have $A \in P(B)$. By def. of $P \Rightarrow A \subseteq B$

Relation Proofs

Lemma 3.6 $\widehat{\rho\sigma} = \hat{\sigma}\hat{\rho}$ $\widehat{\rho\sigma} = \{(c,a) \mid a \rho\sigma c\}$
$= \{(c,a) \mid \exists b: a \rho b \wedge b \sigma c\} = \{(c,a) \mid \exists b: b \sigma c \wedge a \rho b\} = \{(c,a) \mid \exists b: c \hat{\sigma} b \wedge b \hat{\rho} a\}$

$(A; \preceq)$ is poset, then $(A; \hat{\preceq})$ is also poset

We show $\hat{\preceq}$ is partial order relation on A. Reflexivity: For any $a \in A$ $a \preceq a \Rightarrow a \hat{\preceq} a$
Antisymmetry: Let $a, b \in A$ such that $a \hat{\preceq} b$ and $b \hat{\preceq} a$ This means $b \preceq a$ and $a \preceq b$ by antisymmetry of $\preceq \Rightarrow a = b$. Transitivity: Let $a, b, c \in A$ be such that $a \hat{\preceq} b$ and $b \hat{\preceq} c$ This means $b \preceq a$ and $c \preceq b$. By transitivity of $\preceq$ it follows $c \preceq a$. Hence $a \hat{\preceq} c$

$f(A \cap B) = f(A) \cap f(B) \iff f$ is injective

($\Rightarrow$) Let $a, b \in Y$ such that $a \neq b$ (if not possible f is trivially injective)
Let $A = \{a\}$ and $B = \{b\}$. $A \cap B = \emptyset \Rightarrow f(A) \cap f(B) = \emptyset$ (Assumption) $\Rightarrow f(a) \neq f(b) \Rightarrow f$ inj.
($\Leftarrow$) ① $f(A \cap B) \subseteq f(A) \cap f(B)$: Let $A \cap B \neq \emptyset$ (otherwise it's trivially true). Let $z \in f(A \cap B)$ arbr. with $a \in (A \cap B)$, $f(a) = z$. $a \in A \wedge a \in B \Rightarrow f(a) \in f(A) \wedge f(a) \in f(B) \Rightarrow z \in f(A) \wedge z \in f(B)$
$\Rightarrow f(A \cap B) \subseteq f(A) \cap f(B)$ ② $f(A) \cap f(B) \subseteq f(A \cap B)$: Let $z \in f(A) \cap f(B)$ be arbitrary
$\Rightarrow z \in f(A) \wedge z \in f(B) \Rightarrow \exists a \in A\, \exists b \in B: z = f(a) \wedge z = f(b) \overset{\text{inj}}{\Rightarrow} a = b \Rightarrow \exists a \in A \cap B: f(a) = z$

No surjective mapping $f: A \to P(A)$ exists We define $S = \{a \in A \mid a \notin f(a)\}$
$S \subseteq A \Rightarrow S \in P(A)$. We assume f is surjective $\Rightarrow$ There exists $a \in A$ for which $f(a) = S$
1.) $a \in S$: $a \in S \Rightarrow a \notin f(a)$ (Def of S) $\Rightarrow a \notin S$ ($S = f(a)$) | $\Rightarrow$ such a does not exist
2.) $a \notin S$: $a \notin S \Rightarrow a \in f(a)$ (Def of S) $\Rightarrow a \in S$ ($S = f(a)$) | $\Rightarrow f$ is not surjective

Proofs in Number Theory

$\log_5(7)$ is irrational

Assume it is rational: $\log_5(7) = \frac{a}{b}$. Leads to a contradiction.
$\log_5(7) = \frac{a}{b} \Rightarrow 5^{\frac{a}{b}} = 7 \Rightarrow 7^b = 5^a$ (contradicts unique prime factorization)

Is the set of bij. $f: \mathbb{N} \to \mathbb{N}$ countable?

Denote set of bD as S. We give injection from $\{0,1\}^\infty \to S$.
Let $s \in S$ be arbitrary and denote s_i as the i-th bit of s.
$g(s) = f(i) \iff \begin{cases} f(2i) = \begin{cases} 2i & \text{if } s_i = 1 \\ 2i+1 & \text{if } s_i = 0 \end{cases} \\ f(2i+1) = \begin{cases} 2i+1 & \text{if } s_i = 1 \\ 2i & \text{if } s_i = 0 \end{cases} \end{cases}$ It is bijective, since it is linear with adjacent values shuffled.
Now assume $s, t \in \{0,1\}^\infty$ with $s \neq t$. Let $i \in \mathbb{N}$ be the smallest integer such that $s_i \neq t_i$. We have $g(s) \neq g(t)$ since $g(s)(2i) \neq g(t)(2i)$ as well as $g(s)(2i+1) \neq g(t)(2i+1)$. Hence g is injective. S dominates $\{0,1\}^\infty$.

For all $m, n \in \mathbb{N}$ if $m \equiv_4 n$, then $123^m \equiv_{10} 33^n$

Let $m, n \in \mathbb{N}$ be arbitrary and w.l.o.g. assume $m \leq n$. If $m \equiv_4 n$
$\Rightarrow n - m = 4k$ for some $k \in \mathbb{N}$. $123^m \equiv_{10} 33^n \Rightarrow$
$3^m - 3^n \equiv_{10} 3^m(1 - 3^{n-m}) \equiv_{10} 3^m(1 - 3^{4k}) \equiv_{10} 3^m(1 - 9^{2k})$
$\equiv_{10} 3^m(1 - (-1)^{2k}) \equiv_{10} 3^m(1 - 1) \equiv_{10} 0$

Lemma 4.14 $a \equiv_m b$ and $c \equiv_m d \Rightarrow a + c \equiv_m b + d$

We have $m \mid a - b$ and $m \mid c - d \Rightarrow m \mid (a-b) + (c-d)$
$\Rightarrow m \mid (a+c) - (b+d) \Rightarrow a + c \equiv_m b + d$

Lemma 4.18 $ax \equiv_m 1$ has solution $\iff \gcd(a,m) = 1$

($\Rightarrow$) If x solution $ax \equiv_m 1$, then $ax = km + 1$ for some $k \in \mathbb{N}$. Note that $\gcd(a,m)$ divides both a and m, hence also $ax - km$, which is 1.
Thus $\gcd(a,m) = 1$. Therefore if $\gcd(a,m) > 1$, no solution x exists.
($\Leftarrow$) Assume $\gcd(a,m) = 1$. According to Lemma 4.4 there exist integers u and v such that $ua + vm = \gcd(a,m) = 1$. Since $vm \equiv_m 0$ we have $ua \equiv_m 1$. Hence $x = u$ is a solution in $\mathbb{Z}$ and thus $x = R_m(u)$ is a solution in $\mathbb{Z}_m$. To prove uniqueness suppose there is another solution x'. $ax - ax' \equiv_m 0$, thus $a(x - x') \equiv_m 0$ and hence $m \mid a(x - x')$. Since $\gcd(a,m) = 1$, $m \mid x - x' \Rightarrow R_m(x) = R_m(x')$

Theorem 5.36 For an irreducible polynomial $m(x)$ we have $\gcd(a(x), m(x)) = 1$ for all $a(x) \neq 0$ with $\deg(a(x)) < \deg(m(x))$ and therefore according to Lemma 5.35, $a(x)$ is invertible in $F[x]_{m(x)}$. In other words $F[x]^*_{m(x)} = F[x]_{m(x)} \setminus \{0\}$. If $m(x)$ is reducible, then $F[x]_{m(x)}$ is not a field because nontrivial factors of $m(x)$ have no multiplicative inverse.

Linear equations over $\mathbb{Z}_{11}$ $5x \oplus 2y = 4$, $2x \oplus 7y = 9$
Eliminate x by adding 2 times the first $\ominus 5 = 6$ times the second one
$(2 \odot 5 \oplus 6 \odot 2)x + (2 \odot 2 + 6 \odot 7)y = 2 \odot 4 \oplus 6 \odot 9$
$\Rightarrow 2y = 7 \Rightarrow y = 9 \Rightarrow x = 6$

Algebra Proofs

Minimality of the group axioms

1.) $a * e = a \Rightarrow e * a = a$: $e * a = (a * \hat{a}) * a = a * (\hat{a} * a) = a * e$
2.) $a * \hat{a} = e = \hat{a} * a$: $\hat{a} * a = (\hat{a} * a) * e = (\hat{a} * a) * (\hat{a} * \hat{\hat{a}}) = \hat{a} * (a * \hat{a}) * \hat{\hat{a}} = \hat{a} * (e * \hat{\hat{a}}) = e$

Give isomorphism from $\langle \mathbb{Z}^*_{15}; \odot \rangle$ to $\langle \mathbb{Z}^*_{20}; \odot \rangle$

$\varphi: \mathbb{Z}^*_{15} \to \mathbb{Z}^*_{20}$. We construct 3 isomorphisms. $\alpha: \mathbb{Z}^*_{15} \to \mathbb{Z}^*_3 \times \mathbb{Z}^*_5$, $\beta: \mathbb{Z}^*_3 \times \mathbb{Z}^*_5 \to \mathbb{Z}^*_4 \times \mathbb{Z}^*_5$ and $\gamma: \mathbb{Z}^*_4 \times \mathbb{Z}^*_5 \to \mathbb{Z}^*_{20}$
φ is the composition of these isomorphism: $\gamma \circ \beta \circ \alpha$. $\alpha: a \mapsto (R_3(a), R_5(a))$. Let f be the isomorphism $f: \mathbb{Z}^*_{20} \to \mathbb{Z}^*_4 \times \mathbb{Z}_5$ defined by $f: a \mapsto (R_4(a), R_5(a))$. $\gamma = f^{-1}$ (can be computed efficiently using CRT). Note that the function $g: \mathbb{Z}^*_3 \to \mathbb{Z}^*_4$ defined by $g(1) = 1$, $g(2) = 3$ is an isomorphism. It's trivially bijective. We also have $g(1 \odot 1) = 1 = g(1) \odot g(1)$, $g(2 \odot 1) = 3 = g(2) \odot g(1)$ and $g(2 \odot 2) = 1 = g(2) \odot g(2)$. Therefore g is also a homomorphism. Therefore β defined by $\beta((a,b)) = (g(a), b)$ is an isomorphism.

Theorem 5.7 Let $G = \langle g \rangle$ be a cyclic group of order n. The bijection $\mathbb{Z}_n \to G: i \mapsto g^i$ is a group isomorphism since $i \oplus j \mapsto g^{i+j} = g^i * g^j$

Theorem 5.13 (Theorem 5.2)) is similar) $\mathbb{Z}^*_m$ is closed under $\odot$ since $\gcd(a,m) = 1$ and $\gcd(b,m) = 1$, then $\gcd(ab, m) = 1$
This is true since if ab and m have a common divisor > 1, then they also have a prime divisor > 1, which would be a divisor of a and m or b and m, contradicting that $\gcd(a,m) = 1$ and $\gcd(b,m) = 1$. The associativity is inherited from the associativity of multiplication in $\mathbb{Z}$. 1 is a neutral element and inverse exists (Lemma 4.18).

Lemma 5.17

(i) $0a = a0 = 0$: $a0 = a(0+0) \Rightarrow a0 = a0 + a0 \Rightarrow a0 + (-a0) = a0 + a0 + (-a0) \Rightarrow 0 = a0$
(ii) $(-a)b = a(-b)$: $(-a)b = 0 + (-a)b = a0 + (-a)b = a(-b+b) + (-a)b = a(-b) + ab + (-a)b = a(-b) + (a-a)b = a(-b) + 0b$
(iii) $(-a)(-b) = ab$: $0 = (a + (-a))b = ab + (-a)b = 0 \Rightarrow (-a)b = -(ab)$
$0 = (-a)(b + (-b)) = (-a)b + (-a)(-b) = -(ab) + (-a)(-b) \Rightarrow ab = (-a)(-b)$
(iv) $1 = 0 \Rightarrow a = a \cdot 1 = a \cdot 0 = 0$

Lemma 5.19 For any Ring R, R^* is a multiplicative group ① closed under multiplication $u, v \in R^*$ $\Rightarrow uv \in R^*$ (uv has inverse) $(uv) \cdot (v^{-1}u^{-1}) = \ldots = 1$ ② R^* contains neutral element, since 1 has inverse. ③ Ass is inherited

ψ: isomorphism from $\langle G; *, \hat{\ }, e \rangle$ to $\langle H; \star, \tilde{\ }, e' \rangle$ Claim: ψ^{-1} is an isomorphism
ψ^{-1} is surjective. For any $g \in G$, there exists an $h \in H$, namely $h = \psi(g)$, such that $\psi^{-1}(h) = \psi^{-1}(\psi(g)) = g$
ψ^{-1} is injective. Assume there exists $h_1, h_2 \in H$ such that (1) $\psi^{-1}(h_1) = \psi^{-1}(h_2)$ and (2) $h_1 \neq h_2$. Let $g_1 = \psi^{-1}(h_1)$ and $g_2 = \psi^{-1}(h_2)$. From (1) we get $g_1 = g_2$ and from (2) we get $\psi^{-1}(g_1) = h_1 \neq h_2 = \psi^{-1}(g_2)$. That contradicts that ψ is well defined. ψ^{-1} is a homomorphism. For any $h_1, h_2 \in H$ let $g_1 = \psi^{-1}(h_1)$ and $g_2 = \psi^{-1}(h_2)$
$\psi^{-1}(h_1 \star h_2) = \psi^{-1}(\psi(g_1) \star \psi(g_2)) = \psi^{-1}(\psi(g_1 * g_2)) = g_1 * g_2$ (def inverse) $= \psi^{-1}(h_1) * \psi^{-1}(h_2)$

Theorem 5.24 A field is an integral domain Contradiction: Assume $uv = 0$ for some v. $v = 1 \cdot v = u^{-1}u \cdot v = u^{-1} \cdot 0 = 0$
$\Rightarrow u$ is not zero divisor $\quad$ ↳ u arbitrary

Lemma 5.28 $\alpha \in F$ is a root of $a(x) \iff x - \alpha$ divides $a(x)$

($\Rightarrow$) Assume α is root. According to Theorem 5.25, we can write $a(x)$ as $a(x) = (x - \alpha) \cdot q(x) + r(x)$ where $\deg(r(x)) < \deg(x - \alpha) = 1$, i.e. $r(x)$ is constant r, where $r = a(x) - (x - \alpha) \cdot q(x)$. Setting $x = \alpha$ gives:
$r = a(\alpha) - (\alpha - \alpha) \cdot q(\alpha) = 0$. Hence $x - \alpha$ divides $a(x)$.
($\Leftarrow$) Assume $x - \alpha$ divides $a(x)$, i.e. $a(x) = (x - \alpha)q(x)$ for some $q(x)$. Then $a(\alpha) = (\alpha - \alpha) \cdot q(\alpha) = 0$, i.e. α is a root of $a(x)$

Lemma 5.34 $F[x]_{m(x)}$ is a group with respect to pol. addition. The neutral element is 0 and the negative of $a(x) \in F[x]_{m(x)}$ is $-a(x)$. Associativity is inherited from $F[x]$. $F[x]_{m(x)}$ is a monoid with respect to pol. multiplication The neutral element is 1. Associativity of multiplication is inherited from $F[x]$, as is the distributive law

Popular Proofs

n^2 is odd $\Rightarrow$ n is odd (indirect proof)

n is even $\Rightarrow n \cdot n$ is even $\Rightarrow n^2$ is even

$42^n - 1$ is a prime $\Rightarrow$ n is odd (indirect proof)

n is even $\Rightarrow$ There exists a natural number k such that $k > 0$ and $n = 2k$
$\Rightarrow$ We have $42^n - 1 = 42^{2k} - 1 = (42^k - 1)(42^k + 1)$ for $k > 0$ $\Rightarrow$
there exists two non-trivial divisors of $42^n - 1$, namely $(42^k - 1), (42^k + 1)$
$\Rightarrow 42^n - 1$ is not a prime.

$n^3 + 2n + 6$ is divisible by 3 for all $n \geq 0$

Let n be any natural number ≥ 0. Let $n = 3k + c$, where $0 \leq c \leq 2$ and $k \in \mathbb{N}$.
We have $n^3 + 2n + 6 = (3k+c)^3 + 2(3k+c) + 6 = c^3 + 9c^2k + 27ck^2 + 2c + 27k^3 + 6k + 6$
Each summand is divisible by 3 except the term $c^3 + 2c$. Hence we only need to show that $c^3 + 2c$ is divisible by 3 for $0 \leq c \leq 2$. Case $c = 0$: $c^3 + 2c = 0$ which is divisible by 3. Case $c = 1$: $c^3 + 2c = 3$, which is divisible by 3. Case $c = 2$: $c^3 + 2c = 12$, which is divisible by 3. Since the cases cover all possibilities for c, we can conclude the proof.

If p and $p^2 + 2$ are primes, then $p^3 + 2$ is also prime

For any prime number p, we can distinguish the following cases:
$p = 2$: If $p = 2$, then $p^2 + 2 = 6$ is not prime, thus the claim holds for $p = 2$.
$p = 3$: If $p = 3$, then $p^2 + 2 = 11$ is prime. $p^3 + 2 = 29$ is prime. Thus the claim holds.
$p > 3$: If $p > 3$ is prime, then 3 cannot divide p. Therefore we have $R_3(p) \in \{1, 2\}$.
Thus it holds that $R_3(p^2) = R_3(R_3(p) \cdot R_3(p)) = 1$. It follows that $R_3(p^2 + 2) = R_3(R_3(p^2) + R_3(2)) = R_3(1 + 2) = 0$. Therefore $p^2 + 2$ must not be divisible by 3 and so is not a prime. Thus the claim holds for $p > 3$.

$\forall x (F \wedge G) \models (\forall x F) \wedge G$ is true

Let $\mathcal{A}$ be an interpretation suitable for $\forall x (F \wedge G)$ and $(\forall x F) \wedge G$, such that $\mathcal{A}(\forall x (F \wedge G)) = 1$. According to the semantics of $\forall$, we have $\mathcal{A}_{[x \mapsto u]}(F \wedge G) = 1$ for all $u \in U^{\mathcal{A}}$. According to semantics of $\wedge$, we further have $\mathcal{A}_{[x \mapsto u]}(F) = 1$ for all $u \in U^{\mathcal{A}}$ (1) or $\mathcal{A}_{[x \mapsto u]}(G) = 1$ for all $u \in U$ (2). The fact (1) implies (3) $\mathcal{A}(\forall x F) = 1$, according to the semantics of $\forall$. Furthermore note that if x occurs free in G, then it also occurs free in $(\forall x F) \wedge G$. and since $\mathcal{A}$ is suitable for $(\forall x F) \wedge G$, it must assign a value to x. We now define u^* as follows: if x occurs free in G, then u^* is the value assigned to x by $\mathcal{A}$, else u^* is arbitrary. By definition of u^*, we have $\mathcal{A}_{[x \mapsto u^*]}(G) = \mathcal{A}_u(G)$, so by (2) we have (4) $\mathcal{A}(G) = 1$. The facts (3) and (4) imply that $\mathcal{A}((\forall x F \wedge G) = 1$.