CH3

Subset : $A \subseteq B \Leftrightarrow \forall x (x \in A \rightarrow x \in B)$
→ Trans. – Consistency : $A \subseteq B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B$

Empty set : $\forall x (x \notin \emptyset)$ L3.3

Power set : $\mathcal{P}(A) = \{S \mid S \subseteq A\}$

Equal sets : $A = B \Leftrightarrow (A \subseteq B) \wedge (B \subseteq A)$

Union : $A \cup B \Leftrightarrow \{x \mid x \in A \vee x \in B\}$
→ Idemp – Comm – Assoc – Absorb – Distrib.

Union for sets : $\bigcup \mathcal{A} = \{x \mid x \in A \text{ for some } A \in \mathcal{A}\}$

Intersection : $A \cap B \Leftrightarrow \{x \mid x \in A \wedge x \in B\}$
→ Idemp – Comm – Assoc – Absorb – Distrib.

Intersection for sets : $\bigcap \mathcal{A} = \{x \mid x \in A \text{ for all } A \in \mathcal{A}\}$

Complement : $\overline{A} = \{x \in U \mid x \notin A\} = \{x \mid x \notin A\}$

Difference : $B \setminus A = \{x \in B \mid x \notin A\}$

Cartesian product : $A \times B = \{(a,b) \mid a \in A \wedge b \in B\}$
→ NOT asso.

C.P. for sets : $\times_{i=1}^{k} A_i = \{(a_1, .., a_k) \mid a_i \in A_i\}$

Ordered pairs : $(a,b) = \{\{a\},\{a,b\}\}$

Cardinality of power set : $|A| \neq \infty \Rightarrow |\mathcal{P}(A)| = 2^{|A|}$

Cardinality of C.P. : $|A| \neq \infty \wedge |B| \neq \infty \Rightarrow |A \times B| = |A||B|$

L3.1 $\{a\} = \{b\} \Rightarrow a = b$

L3.3 $\forall A (\emptyset \subseteq A)$

T3.10 : For $(A; \preceq)$ & $(B; \sqsubseteq)$, $(A \times B; \leq)$ is a poset where,
$(a_1, b_1) \leq (a_2, b_2) \Leftrightarrow a_1 \preceq a_2 \wedge b_1 \sqsubseteq b_2$

T3.11 : For $(A; \preceq)$ & $(B; \sqsubseteq)$, $(A \times B; \leq_{lex})$ is a poset where,
$(a_1, b_1) \leq_{lex} (a_2, b_2) \Leftrightarrow a_1 \prec a_2 \vee (a_1 = a_2 \wedge b_1 \sqsubseteq b_2)$
→ $x \prec y \Leftrightarrow x \preceq y \wedge x \neq y$
→ if $\preceq$ & $\sqsubseteq$ are totally ordered, so is $\leq_{lex}$.

T3.14 : $A \preceq B \wedge B \preceq A \Rightarrow A \sim B$ (Bernstein – Schröder)

T3.15 : A is countable iff $|A| \neq \infty$ or $A \sim \mathbb{N}$

T3.16 : $\{0,1\}^*$ is countable

T3.17 : $\mathbb{N} \times \mathbb{N}$ is countable

C3.18 : The C.P of two countable sets is countable
→ $A \preceq \mathbb{N} \wedge B \preceq \mathbb{N} \Rightarrow A \times B \preceq \mathbb{N}$

C3.19 : $\mathbb{Q}$ is countable

T3.20 : For countable sets A & A_i, $i \in \mathbb{N}$
i) A^n, $n \in \mathbb{N}$ ii) $\bigcup_{i \in \mathbb{N}} A_i$ iii) A^* := finite sequences of elem. of A
↳ countable list of countable sets.
⇒ are countable

T3.21 : $\{0,1\}^\infty$ is uncountable : Cantor's diagonalization

C3.22 : $\exists$ uncomputable functions $\mathbb{N} \rightarrow \{0,1\}$

Relation ρ from A to B : subset of $A \times B$
→ $a \rho b = (a,b) \in \rho$

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

No. of rel. between two sets : $2^{|A||B|}$

Inverse rel. $\hat{\rho} = \rho^{-1} = \{(a,b) \mid (b,a) \in \rho\}$
→ $a \rho b \Leftrightarrow b \hat{\rho} a$

Composition of rel. $\rho \circ \sigma = \{(a,c) \mid \exists b \in B\ (a,b) \in \rho \wedge (b,c) \in \sigma\}$
→ asso.

Inverse of comp. : $\widehat{\rho\sigma} = \hat{\sigma}\hat{\rho}$

Reflexivity : $\forall a \in A$ $a \rho a$, ie. $id \subseteq \rho$

Symmetry : $\forall a \in A, \forall b \in B$: $a\rho b \Leftrightarrow b\rho a$, i.e. $\rho = \hat{\rho}$

Antisymm. : $\forall a \in A, \forall b \in B$: $(a\rho b \wedge b\rho a) \Rightarrow a = b$, ie. $\rho \cap \hat{\rho} \subseteq id$.

Transitiv. : $\forall a \in A, \forall b \in B, \forall c \in C$: $(a\rho b \wedge b\rho c) \Rightarrow a\rho c$
→ $\rho^2 \subseteq \rho$

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

Equivalence class : $[a]_\theta = \{b \in A \mid b \theta a\}$

Partition of a set : $S_i \cap S_j = \emptyset$ for $i \neq j$, $\bigcup_{i \in I} S_j = A$

Quotient set : $A/\theta = \{[a]_\theta \mid a \in A\}$ (A mod θ)

Poset : $(A; \preceq)$ T3.10, 11

Comparable : a and b, if $a \preceq b$ or $b \preceq a$ for $(A; \preceq)$

Totally ordered : $\forall a, b \in A$ are comparable, A is t.o. by $\preceq$

Cover : b covers a if, $a \preceq b \wedge b \neq a \wedge \neg \exists c (a \prec c \wedge c \prec b)$

Hasse diagram : edge from a to b iff b covers a.

Minimal ele. of A : $\neg \exists b \in A$ $b \prec a \rightarrow a$ is M.E

Max ele. : $\neg \exists b \in A$ $a \prec b$

Least ele. $\forall b \in A$ $a \preceq b \rightarrow a$ = L.E

Greatest ele. $\forall b \in A$ $b \preceq a$

Lower Bound of $S \subseteq A$: $\forall b \in S$ $a \preceq b \rightarrow a \in$ L.B.

Upper Bound : $\forall b \in S$ $b \preceq a$

Greatest L.B = G.E in L.B

Least U.B = L.E in U.B.

Well-ordered : $(A; \preceq)$ if totally ordered &
every non-empty subset of A has a L.E.
→ every totally ordered finite Poset is well ordered.

Meet of a & b : $(a \wedge b)$ = G.L.B. of $\{a,b\} \subseteq A$

Join $(a \vee b)$ = L.U.B of $\{a,b\} \subseteq A$

Lattice : a Poset where every pair of elem. has a meet & join.

Totally defined : $\forall a \in A\ \exists b \in B$ $a f b$, for $f : A \rightarrow B$

Well defined : $\forall a \in A\ \forall b, b' \in B$ $(a f b \wedge a f b' \rightarrow b = b')$

Set of all functions $A \rightarrow B$: B^A

Partial function : a func. that is only well-defined.

Image / Range : $f(A) = \{f(a) \mid a \in A\}$

Pre-image of $T \subseteq B$: $f^{-1}(T) = \{a \in A \mid f(a) \in T\}$

Injectiv. $a \neq b \Rightarrow f(a) \neq f(b)$ or $f(a) = f(b) \Rightarrow a = b$

Surjectiv. $f(A) = B$ or $\forall b \in B\ \exists a \in A$: $b = f(a)$

Composition of func. $(g \circ f)(a) = g(f(a))$
→ Assoc. $(h \circ g) \circ f = h \circ (g \circ f)$

Equinumerous : $A \sim B$ if $\exists$ bijection $A \rightarrow B$ T3.14

Domination : $A \preceq B$ if $A \sim C \wedge C \subseteq B$ i.e. $\exists$ injection $A \rightarrow B$

Countability : A is countable if $A \preceq \mathbb{N}$ T3.15

Computable : $f : \mathbb{N} \rightarrow \{0,1\}$, if $\exists$ program, $\forall n \in \mathbb{N}$, inputs n & outputs f(n) C3.22

CH4

Fermat's Last Theorem: $\neg\exists n,a,b,c \in \mathbb{Z}^+ \quad n \geq 3 \wedge a^n + b^n = c^n$

Catalan conjecture: $a^m - b^n = 1$ has no other int sol. than $3^2 - 2^3 = 1$ for $m,n \geq 2$

Divisor: $a|b \Leftrightarrow \exists c \in \mathbb{Z} \quad b = ac$

Euclead's T4.1: For all int a & $d \neq 0$, $\exists q,r \in \mathbb{Z} \quad a = dq + r \wedge 0 \leq r < |d|$.

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

GCD: for $a \neq 0, b \neq 0$, $\gcd(a,b) = d \Leftrightarrow d|a \wedge d|b \wedge \forall c((c|a \wedge c|b) \rightarrow c|d)$

LCM: for $a \neq 0, b \neq 0$, $\operatorname{lcm}(a,b) = l \Leftrightarrow a|l \wedge b|l \wedge \forall m((a|m \wedge b|m) \rightarrow l|m)$

Congruent: for $a,b,m \in \mathbb{Z}$ & $m \geq 1$ $\quad a \equiv_m b \Leftrightarrow m|(a-b)$

Equality: $a = b \Rightarrow a \equiv_m b$, $\quad a \not\equiv_m b \Rightarrow a \neq b$

Multiplicative Inverse: if $\gcd(a,m) = 1$, $ax \equiv_m 1$

$\rightarrow x \equiv_m a^{-1} \rightarrow$ if $\gcd(a,m) \neq 1$, a doesn't have M.I. mod m.

L4.2: $\gcd(m, n - qm) = \gcd(m,n)$, $\quad \gcd(m, R_m(n)) = \gcd(m,n)$

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

L4.4: For $a,b \in \mathbb{Z}$ (not both 0), $\exists d \in \mathbb{Z}$ $(a,b) = (d) \rightarrow d = \gcd(a,b)$

C4.5: For $a,b \in \mathbb{Z}$ (not both 0), $\exists u,v \in \mathbb{Z}$ $\gcd(a,b) = ua + vb$

Fund. Theo. of Arith.: every positive int. is uniquely written as a product of primes.

$\rightarrow$ for $a = \prod_i p_i^{e_i}$ & $b = \prod_i p_i^{f_i}$: $\begin{cases} \gcd(a,b) = \prod_i p_i^{\min(e_i, f_i)} \\ \operatorname{lcm}(a,b) = \prod_i p_i^{\max(e_i, f_i)} \end{cases}$

$\hookrightarrow \gcd(a,b) \cdot \operatorname{lcm}(a,b) = ab$

L4.12 every composite int. n has a prime divisor $\leq \sqrt{n}$

L4.13 for $m \geq 1$, $\equiv_m$ is equiv. relation on $\mathbb{Z}$

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

C4.15 if $a_i \equiv_m b_i$ for $1 \leq i \leq k$, then $f(a_1, \dots, a_k) \equiv_m f(b_1, \dots, b_k)$

L4.16 for $a,b,m \in \mathbb{Z}$ & $m \geq 1$,

i) $a \equiv_m R_m(a)$

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

C4.17 $R_m(f(a_1, \dots, a_k)) = R_m(f(R_m(a_1), \dots, R_m(a_k)))$

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

Chinese Remainder Theorem: for pairly relatively prime int $m_1, \dots, m_r$ and $M = \prod_{i=1}^r m_i$, every list of $a_1, \dots, a_r$ with $0 \leq a_i < m_i$ for $1 \leq i < r$ $x \equiv_{m_i} a_i$ for x has a solution in $0 \leq x < M$

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

Diffie-Hellman Key-Agreement uses the fact that $x \mapsto R_p(g^x)$ is one-way f

p, g: known

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

Alice $x_A \rightarrow R_p(g^{x_A}) =: y_A \rightarrow R_p(y_B^{x_A}) =: k_{AB}$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \|$

Bob $x_B \rightarrow R_p(g^{x_B}) =: y_B \rightarrow R_p(y_A^{x_B}) =: k_{BA}$

CH5

Operation: a func $S^n \rightarrow S$ (n = arity)

Algebra: $\langle S, \Omega \rangle$: S = carrier of algebra, Ω = list of operations on S

Neutral elem. of $\langle S, * \rangle$: $e \in S$ s.t. $\forall a \in S \quad a * e = e * a = a$

Associativity: $\forall a,b,c \in S \quad a * (b * c) = (a * b) * c$

Monoid: $\langle M; *, e \rangle$ i) $*$ is associative ii) e is the N.E.

Inverse elem. of $\langle S; *, e \rangle$: $b \in S$ s.t. $\forall a \in S \quad b * a = a * b = e$

Group: $\langle G; *, ^\wedge, e \rangle$ G1: $*$ is asso G2: $\forall a \in S \; a * e = e * a = a$ G3: $\forall a \in G \; \exists \hat{a} \in G$, i.e. $a * \hat{a} = \hat{a} * a = e$

Abelian: $a * b = b * a$, where $a,b \in G$

Direct Product of Groups: $\langle G_1; *_1 \rangle, \dots, \langle G_n; *_n \rangle \rightarrow \langle G_1 \times \dots \times G_n; \star \rangle$

where $(a_1, \dots, a_n) \star (b_1, \dots, b_n) = (a_1 *_1 b_1, \dots, a_n *_n b_n)$

Group Homomorphism: func ψ from $\langle G; *, ^\wedge, e \rangle$ to $\langle H; \star, ^\sim, e' \rangle$ s.t. $\forall a \forall b \; \psi(a * b) = \psi(a) \star \psi(b)$

Isomorphism: ψ is bijective $\rightarrow G \simeq H$

Subgroup: for $H \subseteq G$, $\langle H; *, ^\wedge, e \rangle$ is a S.G. of $\langle G; *, ^\wedge, e \rangle$ if 1 $\forall a,b \in H \; a * b \in H$ 2 $e \in H$ 3 $\forall a \in H \; \hat{a} \in H$

Order $\begin{cases} \text{elem: for } G \text{ and } a \in G, \operatorname{ord}(a) \text{ is the least } m \geq 1 \text{ s.t. } a^m = e \\ \text{group: } |G| \text{ for finite groups} \end{cases}$

$\hookrightarrow \operatorname{ord}(a) = \infty$ if $\neg\exists m$. $\rightarrow \operatorname{ord}(e) = 1 \rightarrow \operatorname{ord}(a) = 2 \Leftrightarrow a^{-1} = a$

Cyclic group: $G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\} = \{e, g, g^2, \dots, g^{\operatorname{ord}(g)-1}\}$

$\mathbb{Z}_m^* := \{a \in \mathbb{Z}_m \mid \gcd(a,m) = 1\}$

Euler Function: $\varphi: \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$: $\varphi(m) = |\mathbb{Z}_m^*|$

$\rightarrow$ for primes, $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ & $\varphi(p) = p - 1$

Ring: $\langle R; +, -, 0, \cdot, 1 \rangle$ where R1 - $\langle R; +, -, 0 \rangle$ is a comm. group. R2 - $\langle R, \cdot, 1 \rangle$ is a monoid R3 - $\forall a,b,c \in R \quad a(b+c) = ab + ac$ & $(b+c)a = ba + ca$

$\hookrightarrow$ comm. if $\cdot$ is comm. $(a \cdot b = b \cdot a)$

$\rightarrow \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ & $\langle \mathbb{Z}_m; +, -, 0, \cdot, 1 \rangle$ are comm. rings.

Characteristic of a ring $= \begin{cases} \text{the order of } 1 \text{ in additive Group} & \text{if finite} \\ 0 & \text{otherwise} \end{cases}$

Divisor of a comm ring: for a,b & $a \neq 0$, $a|b \Leftrightarrow \exists c \in R: b = ac$

$\rightarrow$ every non-zero element is a divisor of 0.

$\rightarrow$ 1 and -1 are divisors of every element.

Zerodivisor: a where $a \neq 0$ of comm. R & $ab = 0$ for some $b \neq 0 \in R$

Unit: u of comm. R if u is invertible, i.e. $uv = vu = 1$ for some $v \in R$

$\rightarrow R^*$ is the set of units of R.

Integral Domain: a non-trivial ($0 \neq 1$) comm. R without zerodivisors

$\rightarrow \forall a,b \; ab = 0 \rightarrow a = 0 \vee b = 0 \rightarrow \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are I.D.'s.

Degree of a polynomial: $\deg(a(x))$ is the greatest i for which $a_i \neq 0$.

$\rightarrow \deg(0) = -\infty$

Field: a non-trivial comm. R in which every non-zero elem. is a unit.

$\rightarrow F^* = F \setminus \{0\}$ $\quad \rightarrow \langle F \setminus \{0\}; \cdot, ^{-1}, 1 \rangle$ is a comm. G.

$\rightarrow \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ are fields ($\mathbb{Z}$ and $\mathbb{R}[x]$ are not fields)

GF(p) = field of p elements.

Monic: a polynomial $a(x) \in F[x]$ with leading coeff. = 1

Irreducible: a poly. $a(x) \in F[x]$ with $\deg \geq 1$, divisible only by constant poly.s & constant multiples of $a(x)$

$\gcd(a(x), b(x))$: monic poly $g(x)$ of largest degree, s.t. $\begin{matrix} g(x)|a(x) \\ g(x)|b(x) \end{matrix}$

Root: for $a(x) \in R[x]$, element $\alpha \in R$ for which $a(\alpha) = 0$

Multiplicity: for root α of $a(x)$, highest power of $(x - \alpha) | a(x)$

L5.1: there can be only 1 neutral element

L5.2: there can be only 1 inverse element.

L5.3: For $\langle G; *, ^\wedge, e \rangle$ for all $a,b,c \in G$

L5.4: $\langle G_1 \times \dots \times G_n; \star \rangle$ is a group

L5.5: For group homomorphism ψ from $\langle G; *, ^\wedge, e \rangle$ to $\langle H; \star, ^\sim, e' \rangle$

i) $\psi(e) = e'$ ii) $\psi(\hat{a}) = \widetilde{\psi(a)}$ $\forall a$

$\begin{cases} \text{i) } \widehat{(\hat{a})} = a \\ \text{ii) } \widehat{a * b} = \hat{b} * \hat{a} \\ \text{iii) } a * b = a * c \Rightarrow b = c \\ \text{iv) } b * a = c * a \Rightarrow b = c \\ \text{v) } a * x = b \text{ has a unique sol.} \end{cases}$

L5.6: Finite group G, every elem. has finite order $\rightarrow$ hence, abelian

T5.7: A cyclic group with order n is isomorphic to $\langle \mathbb{Z}_n; + \rangle$

T5.8: (Lagrange) For a fin. G and a subgroup H, $|H| \mid |G|$

C5.9: For a fin. G, $\operatorname{ord}(a) \mid |G|$ for $\forall a \in G$

C5.10: For a fin. G, $a^{|G|} = e$ for $\forall a \in G$

C5.11: Every group of prime order is cyclic. $\rightarrow$ every non-neutral elem is a generator.

L5.12: For $m = \prod_{i=1}^r p_i^{e_i}$, $\varphi(m) = \prod_{i=1}^r (p_i - 1) p_i^{e_i - 1}$

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

C5.14: $\forall m \geq 2$, a $\gcd(a,m) = 1 \Rightarrow a^{\varphi(m)} \equiv_m 1$ $\quad (a^{p-1} \equiv_p 1)$

T5.15: $\mathbb{Z}_m^*$ is cyclic $\Leftrightarrow m = 2, 4, p^e, 2p^e$ where p = odd prime, $e \geq 1$

T5.16: For a fin. G and $e \in \mathbb{Z}$ s.t. $\gcd(e, |G|) = 1$,

i) $x \mapsto x^e$ is a bijection, $x^e = y \rightarrow x = y^d$ where $ed \equiv_{|G|} 1$

ii) $y \mapsto y^d$ is the inverse function

L5.17: For $\langle R; +, -, 0, \cdot, 1 \rangle$ and $\forall a,b \in R$ $\begin{cases} \text{i) } 0a = a0 = 0 \\ \text{ii) } (-a)b = -(ab) \\ \text{iii) } (-a)(-b) = ab \\ \text{iv) if R is nontrivial, } 1 \neq 0 \end{cases}$ $\hookrightarrow$ more than 1 elem.

L5.18: For a comm. R $\begin{cases} \text{i) } a|b \wedge b|c \Rightarrow a|c \\ \text{ii) } a|b \Rightarrow \forall c \; a|bc \\ \text{iii) } a|b \wedge a|c \Rightarrow a|(b+c) \end{cases}$

L5.19: For a R, R^* is a M.G.

L5.20: In an I.D., if $a|b$, then c s.t. $b = ac$ is unique

T5.21: For R, $R[x]$ is a ring

L5.22: i) D is a I.D $\Rightarrow$ D[x] is a I.D. $\quad \nearrow D[x]^* = D^*$

ii) units of D[x] are constant poly. that are units of D

T5.24 A field is an I.D.

T5.25: For any $a(x), b(x) \neq 0 \in F(x)$, $\exists$ unique $q(x), r(x)$ s.t. $a(x) = b(x) \cdot q(x) + r(x)$

L5.28: For a field F, $\alpha \in F$ is root of $a(x)$ if $x - \alpha | a(x)$

C5.29: a poly $a(x)$ of deg 2 or 3 over F is irr. if $\neg\exists$ root.

T5.30: For a field F, a non-zero poly $a(x) \in F[x]$ of deg d has at most d roots, counting multiplicities

L5.31: a poly $a(x) \in F[x]$ of deg d is uniquely defined by any d+1 values of $a(x)$

L5.32: Congr. mod. $m(x)$ is an equiv. rel. on $F[x]$

$\rightarrow$ Each E.C. has a unique representative w. $\deg < \deg(m(x))$

L5.33: for a fin. F with q elem., $|F[x]_{m(x)}| = q^d$ $(d = \deg(m(x)))$

L5.34: $F[x]_{m(x)}$ is a R with respect to + and × mod $m(x)$

L5.35: $a(x)b(x) \equiv_{m(x)} 1$ has a unique sol. iff $\gcd(a(x), m(x)) = 1$

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

T5.36: $F[x]_{m(x)}$ is a F iff $m(x)$ is irreducible

T5.37: $\forall p, d \geq 1$ $\exists$ irr. poly. of deg d in GF(p)[x]

$\rightarrow \exists$ finite F s.t. $|F| = p^d$

$\rightarrow GF(p^d) = GF(p)[x]_{m(x)}$ with $m(x)$ = irr & deg = d

T5.38: $\exists$ finite F with q elem. $\Leftrightarrow$ q is power of prime

Any two fields of same size are isomorphic

T5.39: for finite field GF(q), $GF(q)^*$ = cyclic

$\rightarrow |GF(q)^*| = q - 1$, $GF(q)^*$ has $\varphi(q-1)$ generators

Encoding func. (n,k)-encoding func E for alphabet $\mathcal{A}$: injective

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

Error-correcting code: (n,k)-e.c. code over $\mathcal{A}$ with $|\mathcal{A}| = q$

$\rightarrow$ subset of $\mathcal{A}^n$ of cardinality q^k

The Hamming distance: for two strings of equal lengths,

$\rightarrow$ number of positions at which they differ.

The Minimum distance of e.c. code: min(H.D) of two codewords

Decoding func: for (n,k)-encoding func $\rightarrow$ $D: A^n \rightarrow A^k$

t-error correcting: if $\forall$ string x, $D(x') = x$ where $HD(x', E(x)) \leq t$

$\rightarrow$ code C is t-error correcting if $\exists E, D$ $C = \operatorname{Im}(E) \wedge D = t$-e.c.

T5.40: C with M.D. d is t-e.c $\Leftrightarrow d \geq 2t + 1$

T5.41: For $\mathcal{A} = GF(q)$ (of GF(q)) and $\alpha_0, \dots, \alpha_{n-1}$ arbitrary distinct elem. and the E. function $E((a_0, \dots, a_{k-1})) = (a(\alpha_0), \dots, a(\alpha_{n-1}))$ where $a(x) = a_{k-1}x^{k-1} + \dots + a_1 x + a_0$

$\rightarrow$ The M.D. is $n - k + 1$

Remarks

- $\langle \mathbb{Z}_n; + \rangle$ is cyclic for every n
  - $\rightarrow$ generators: $\forall g \in \mathbb{Z}_n$ $\gcd(g,n) = 1$
- $\exists$ infinite cyclic groups, e.g. $\langle \mathbb{Z}; +, -, 0 \rangle = \langle +1 \rangle = \langle -1 \rangle$
- $\mathbb{R}[x]_{x^2+1}$ is isomorphic to $\mathbb{C}$

RSA

$|\mathbb{Z}_{pq}^*| = \varphi(pq) = (p-1)(q-1)$ $\quad e \cdot d \equiv_{(p-1)(q-1)} 1$

pq, e = known

$m \mapsto y = R_{pq}(m^e)$: encryption

$y \mapsto m = R_{pq}(y^d)$: decryption

CH6

Set of mathematical statements: $\mathcal{S} \subseteq \Sigma^*$

Set of proofs: $\mathcal{P} \subseteq \Sigma^*$

Truth function: $\tau : \mathcal{S} \to \{0,1\}$ assigns each $s \in \mathcal{S}$ to each truth value and defines the semantics of objects of $\mathcal{S}$.

Verification function: $\Phi : \mathcal{S} \times \mathcal{P} \to \{0,1\}$ checks if s is a valid proof to p.
→ has to be efficiently computable.

Proof System: $\Pi = (\mathcal{S}, \mathcal{P}, \tau, \Phi)$

Soundness of P.S.: $\forall s \in \mathcal{S}\ \exists p \in \mathcal{P}\ \Phi(s,p) = 1 \Rightarrow \tau(s) = 1$

Completeness of P.S.: $\forall s \in \mathcal{S}\ \tau(s) = 1 \Rightarrow \exists p \in \mathcal{P}\ \Phi(s,p) = 1$

Syntax: defines alphabet Λ and specifies which strings Λ^* are formulas

Semantics: defines 1) a function FREE that assigns to each formula $F = (f_1, \dots, f_k) \in \Lambda^*$ a subset $FREE(F) \subset \{1, \dots, k\}$ of the indices.
→ if $i \in FREE(F)$, f_i is occuring free in F
2) a function σ that assigns to each formula F and intepret. $\mathcal{A}$ suitable for F, a truth value $\sigma(F, \mathcal{A})$ in $\{0,1\}$
→ $\sigma(F, \mathcal{A}) = \mathcal{A}(F)$

Intepretation: a set $\mathcal{X} \subseteq \Lambda$ of symbols, a domain for each symbol & function to assign values.

Suitable: if an intepretation assigns a value for all symbols occuring free.

Model: a suitable intep. $\mathcal{A}$ for which F is true, i.e. $\mathcal{A}(F) = 1$ or $\mathcal{A} \models F$
→ also works for set of formulas $\mathcal{A} \models M$

Satisfiable: $\exists$ model for F

Unsatisfiable: $\neg\exists$ model for F, $\bot$

Tautology / Valid: the formula is true for all intepretation, $\top$
→ if F is a tautology, $\models F$.

Logical Consequence: $F \models G$ if for $\forall \mathcal{A}$ suitable for F, G, $\mathcal{A}(F) = 1 \Rightarrow \mathcal{A}(G) = 1$

Equivalent: $F \equiv G \Leftrightarrow F \models G \wedge G \models F$

Logical Operators: if F, G are formulas, $\neg F, (F \wedge G), (F \vee G)$ are formulas.
→ $\mathcal{A}(F \vee G) = 1 \Leftrightarrow \mathcal{A}(F) = 1 \vee \mathcal{A}(G) = 1$
→ $\mathcal{A}(F \wedge G) = 1 \Leftrightarrow \mathcal{A}(F) = 1 \wedge \mathcal{A}(G) = 1$
→ $\mathcal{A}(\neg F) = 1 \Leftrightarrow \mathcal{A}(F) = 0$

Logical Calculi

Derivation rule: $\{F_1, \dots, F_k\} \vdash_R G$ Application
1) Select a $N \subseteq M$
2) $N \vdash_R G$
3) $M \leftarrow M \cup \{G\}$

Calculus: a set of derivation rules $K = \{R_1, \dots, R_n\}$

Derivation of G from M in calc K: finite sequence of applications.
→ $M_0 = M$, $M_i = M_{i-1} \cup \{G_i\}$ where $N \vdash_{R_j} G_i$ for $N \subseteq M_{i-1}$
→ $M \vdash_K G$

Correct derivation rule: $M \vdash_R F \Rightarrow M \models F \quad \forall M, F$

Correct / sound calculus: $M \vdash_K F \Rightarrow M \models F$ "

Complete calculus: $M \models F \Rightarrow M \vdash_K F$ "

Propositional Logic:

Syntax: an atomic formula is A_i, $i \in \mathbb{N}$
a formula is 1) atomic formula 2) $\neg F, F \vee G, F \wedge G$

Semantics: for a set Z of A.F., an intep. is a function $\mathcal{A} : Z \to \{0,1\}$
→ suitable for F if Z contains all A.F. in F

Literal: an A.F or its negation

CNF: $F = (L_1 \vee L_2) \wedge \dots \wedge (L_3 \vee L_4)$
→ write down 0s with 1s as negation

DNF: $F = (L_1 \wedge L_2) \vee \dots \vee (L_3 \wedge L_4)$
→ write down 1s with 0s as negation

Resolution Calculus

Clause: set of literals ($\emptyset$ is also a clause)

Set of clauses in CNF: $F = (L_1 \vee L_2) \wedge \dots \wedge (L_3 \wedge L_4)$
$\to \mathcal{K}(F) = \{\{L_1, L_2\}, \dots, \{L_3, L_4\}\}$

For $M = \{F_1, \dots, F_k\} \to \mathcal{K}(M) = \bigcup_{i=1}^{k} \mathcal{K}(F_i)$

Resolvant: $L \in K_1, \neg L \in K_2 \to K = (K_1 \setminus \{L\}) \cup (K_2 \setminus \{\neg L\})$
→ $\{K_1, K_2\} \vdash_{res} K$ → Res. calc. only has 1 rule: $\{res\}$
→ Sound but not complete

Application:

Unsatisfiable: M is unsatis. $\Leftrightarrow \mathcal{K}(M) \vdash_{res} \emptyset$

Tautology: M is $\top \Leftrightarrow \mathcal{K}(\neg M) \vdash_{res} \emptyset$

Logical Consequence: $M \models F \Leftrightarrow \mathcal{K}(M \cup \{\neg F\}) \vdash_{res} \emptyset$

Predicate Logic:

Syntax: 1) variable symbol x_i, $i \in \mathbb{N}$
2) function symbol f_i^k, $i, k \in \mathbb{N}$ (called constants when $k = 0$)
3) Predicate symbol P_i^k, $i, k \in \mathbb{N}$
4) term: I) variable II) $f_i^k(t_1, \dots, t_k)$
5) formula I) $P_i^k(t_1, \dots, t_k) \to$ A.F. II) $\neg F, F \wedge G, F \vee G$, III) $\forall x F, \exists x F$

Bound: if variable occurs in $\forall x G$ or $\exists x G$, **free** otherwise.

Closed: no free variables

$F[x/t]$: substitute every free occurrences of x in F with t.

Semantics I: an intep. $\mathcal{A} = (U^{\mathcal{A}}, \phi, \psi, \xi)$
→ U is a non-empty set → ϕ assigns a func. to each func. $\phi(f) : U^k \to U$
→ ψ assigns a func. to each P. $\psi(P) : U^k \to \{0,1\}$ → ξ each var. a value in $U^{\mathcal{A}}$

Suitable: $\mathcal{A}$ is suitable if all function, predicate symbols and free variables.

Semantics II: $\mathcal{A}(t) = \xi(t)$ if t is var, $\mathcal{A}(t) = \phi(f)(\mathcal{A}(t_1), \dots, \mathcal{A}(t_k))$ for $f(t_1, \dots, t_k)$
$\mathcal{A}(F) = \psi(P)(\mathcal{A}(t_1), \dots, \mathcal{A}(t_k))$ for $F = P(t_1, \dots, t_k)$

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

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

Universal Instantiation: $\forall x F \models F[x/t]$

Prenex Form: 1) Free var identify 2) Rectify bound var 3) Apply equiv rules

L6.1
1) $F \wedge F \equiv F$, $F \vee F \equiv F$ (idempotence)
2) $F \wedge G \equiv G \wedge F$, $F \vee G \equiv G \vee F$ (commutativ)
3) $(F \wedge G) \wedge H \equiv F \wedge (G \wedge H)$, $(F \vee G) \vee H \equiv F \vee (G \vee H)$ (associativ)
4) $F \wedge (F \vee G) \equiv F$, $F \vee (F \wedge G)$ (absorption)
5) $F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$, $F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$ (distributiv)
6) $\neg\neg F \equiv F$ (double negation)
7) $\neg(F \wedge G) \equiv \neg F \vee \neg G$, $\neg(F \vee G) \equiv \neg F \wedge \neg G$ (De Morgan's rules)
8) $F \vee \top \equiv \top$, $F \wedge \top \equiv F$ (tautology rules)
9) $F \vee \bot \equiv F$, $F \wedge \bot \equiv \bot$ (unsatisfiability rules)
10) $F \vee \neg F \equiv \top$, $F \wedge \neg F \equiv \bot$

L6.2: $F \equiv \top \Leftrightarrow \neg F \equiv \bot$

L6.3: the following are equivalent.
1) $\{F_1, F_2, \dots, F_k\} \models G$
2) $\{F_1 \wedge F_2 \wedge \dots \wedge F_k\} \to G$ is $\top$
3) $\{F_1, F_2, \dots, F_k, \neg G\}$ is $\bot$

L6.4: for a sound calculus, $\{F_1, \dots, F_k\} \vdash_K G \Rightarrow \models ((F_1 \wedge \dots \wedge F_k) \to G)$

T6.5: every formula is equiv to a formula in CNF & DNF

L6.6: the res. calc is sound: $\mathcal{K} \vdash_{res} K \Rightarrow \mathcal{K} \models K$

L6.8 for F, G, H where x does not occur free in H,
1) $\neg(\forall x F) \equiv \exists x \neg F$
2) $\neg(\exists x F) \equiv \forall x \neg F$
3) $(\forall x F) \wedge (\forall x G) \equiv \forall x (F \wedge G)$
4) $(\exists x F) \vee (\exists x G) \equiv \exists x (F \vee G)$
5) $\forall x \forall y F \equiv \forall y \forall x F$
6) $\exists x \exists y F \equiv \exists y \exists x F$
7) $(\forall x F) \wedge H \equiv \forall x (F \wedge H)$
8) $(\forall x F) \vee H \equiv \forall x (F \vee H)$
9) $(\exists x F) \wedge H \equiv \exists x (F \wedge H)$
10) $(\exists x F) \vee H \equiv \exists x (F \vee H)$

L6.9: changing subformula with an equivalent subformula remains equiv.

L6.10: For form. G where y does not occur,
→ $\forall x G \equiv \forall y G[x/y]$
→ $\exists x G \equiv \exists y G[x/y]$

T6.13: $\neg\exists x \forall y\ (P(y,x) \leftrightarrow \neg P(y,y))$

C6.14: $\neg\exists$ set that contains all sets S that do not contain themselves
→ $\neg\exists R \forall S\ (S \in R \leftrightarrow S \notin S)$

C6.15: $\{0,1\}^\infty$ is uncountable

C6.16: $\exists$ uncomputable functions $\mathbb{N} \to \{0,1\}$

C6.17: the func. $\mathbb{N} \to \{0,1\}$ assigning to each $y \in \mathbb{N}$ the complement of what prog. y outputs on input y is uncomputable

Correct deviation Rules: 1) $F \wedge G \vdash F$ 2) $F \wedge G \vdash G$ 3) $\{F, G\} \vdash F \wedge G$ 4) $F \vdash F \vee G$ 5) $F \vdash G \vee F$
6) $\{F, F \to G\} \vdash G$ 7) $\{F \vee G, F \to H, G \to H\} \vdash H$ 8) $\vdash F \vee \neg F$ (TND) 9) $\vdash \neg(F \leftrightarrow \neg F)$