Diskmath

you can do this !! :)

Logic

D2.1 A mathematical statement is a proposition

A	B	$A \vee B$	$A \wedge B$	$A \to B$	$A \leftrightarrow B$
0	0	0	0	1	1
0	1	1	0	1	0
1	0	1	0	0	0
1	1	1	1	1	1

(2^n)

$\wedge$ conjunction
$\vee$ disjunction

$A \leftrightarrow B \equiv (A \to B) \wedge (B \to A)$
$A \to B \equiv \neg A \vee B$

General Concepts

$\exists y \forall x\, P(x,y) \models \forall x \exists y\, P(x,y)$
$\forall x \exists y\, P(x,y) \not\models \exists y \forall x\, P(x,y)$

D 6.4 Syntax symbols that are allowed and which combinations
D 6.5 Semantics define a function free, which assigns each F a set of indexes that are free symbols
D.6.6 An interpretation A assigns each symbol a value
D.6.7 A is suitable if it assigns a value for all free symbols
D 6.8 Semantics also define a function $\sigma(F,A) = \{0,1\}$ or $A(F)$ giving truth value of F under A.
D 6.9 If $A(F)=1$, then A is a model for F or even a set for M. One writes $A \models F$

Satisfiability, Tautology, Consequence, Equivalence

D. 6.10 satisfiable model exists $\perp$ unsatisfiable otherwise
D 6.11 tautology $\top$ true: every suitable A
D. 6.12 logical consequence $F \models G$ suitable A for F
D 6.13 equivalent $F \models G$, $G \models F$ $\to F \equiv G$
L 6.2 tautology iff $\neg F$ unsatisfiable
L 6.3 statements, equivalent:
$\{F_1, \dots, F_k\} \models G$
$\{F_1 \wedge F_2 \dots \wedge F_k\} \to G$ is taut.
$\{F_1, \dots, F_k, \neg G\}$ unsatisfiable

Logical operators

D 6.15 F, G formulas, then $\neg F$, $F \vee G$ f.
D 6.16 • $A(F \wedge G) = 1 \iff A(F) = 1$ and $A(G) = 1$
• $A(F \vee G) = 1 \iff A(F) = 1$ or $A(G) = 1$
$A(\neg F) = 1 \iff A(F) = 0$

L6.1
1) $F \wedge F \equiv F$ and $F \vee F \equiv F$ idempotence
2) $F \wedge G \equiv G \wedge F$ and $F \vee G \equiv G \vee F$ commutivity
3) $(F \wedge G) \wedge H \equiv F \wedge (G \wedge H)$ and $(F \vee G) \vee H \equiv F \vee (G \vee H)$ asso.
4) $F \wedge (F \vee G) \equiv F$ and $F \vee (F \wedge G) \equiv F$ absorption
5) $F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$ distributive law
6) $F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$ distributive law
7) $\neg\neg F \equiv F$ double neg.
8) $\neg(F \wedge G) \equiv \neg F \vee \neg G$ and $\neg(F \vee G) \equiv \neg F \wedge \neg G$ Morgans.
9) $F \vee \top \equiv \top$ and $F \wedge \top \equiv F$ tautology rule
10) $F \vee \perp \equiv F$ and $F \wedge \perp \equiv \perp$ unsatisfiability
11) $F \vee \neg F \equiv \top$ and $F \wedge \neg F \equiv \perp$

Logical Calculi

$\frac{F_1 \dots F_k}{G}(R)$

D6.17 Derivation rule $\{F_1, \dots F_k\} \vdash_R G$
D6.18 Applying derivation rule
- Select $N \subseteq M$, Specify $N \vdash_R G$ - $M \cup \{G\}$

D6.19 A calculus K: finite set of derivation r.
D6.20 derivation of formula from M in K, finite sequence of applications of $R \in K$
D6.21 Derivation rule is correct $\forall M, F$ $M \vdash_R F \Rightarrow M \models F$
D6.22 Calculus sound $M \vdash_R F \Rightarrow M \models F$
Calculus complete $M \models F \Rightarrow M \vdash_K F$

Ex: complete, sound: $K = \{R\}$ where $\vdash_R F$
not complete, sound: $K = \{R\}$ where $\{F\} \vdash_R F$

D.6.25 Literal atomic formula, negation
D 6.26 Conjunctive Normal Form: $(L \vee L \vee L) \wedge \dots$
D6.27 Disjunctive Normal Form: $(L \wedge L \wedge L) \vee \dots$
DNF: (Row 1) $\vee$ (Row 2) ... only row which are t
$\hookrightarrow (A_1 \wedge A_2 \dots)$ A_i: A_i if 1 else $\neg A$
CNF (Row 1) $\wedge$ (Row 2) only row which a. f
$\hookrightarrow (A_1 \vee A_2 \dots)$ A_i: A_i if 0 else $\neg A$

Ex: Resolution calculus not complete:
Let $F = A$, $G = A \vee B$ we know $F \models G$ but cannot derive $K(A \vee B)$ from $K(A)$ using res.

Resolution Calculus

- prove unsatisfiability, logical consequence

$F \equiv \perp$	$F \equiv \top$	$F \models G$ $(M \models G)$
in CNF	$\neg F \equiv \perp$	$F \wedge \neg G \equiv$

!

D6.28 A clause $(L \wedge L \wedge \dots)$ set of literals
D6.29 set of clauses: $K(F)$
Empty clause: unsatisfiable
Empty clause set: tautology
D 6.30 clause K is resolvent if K_1, K_2 contain literal $L \in K_1$, $\neg L \in K_2$

$\{A\}$ $\{A, B\}$ $\{\neg B, A\}$
$\{A\}$
$\emptyset$

one step at the time
$\{K_1, K_2\} \vdash_{Res} K$
L 6.6. res. cal. sound:
$K \vdash_{Res} K \Rightarrow K \models K$

T 6.7 set M is unsatisfiable iff $K(M) \vdash_{Res} \emptyset$

Predicate Logic

D.6.31 Syntax: variable x_i $i \in \mathbb{N}$
function $f_i^{(k)}$ $i,k \in \mathbb{N}$, k #arg.
predicate $P_i^{(k)}$ "
term t_i, variables, functions
formulas atomic formula

D6.32 Variable bound or free, all bound: closed

D.6.33 For $F_iF_{[x/t]}$ formula by replacing every free x with term t
D.6.34 Semantics: interpretation $A = (U, \phi, \psi, \xi)$ tuple
- U - universe
- ϕ = function assigning function: f^A
- ψ - function assigning predicate p^A
- ξ = function assigning free variables

D.6.35 A is suitable all functions, predicates, free variables F defined
D.6.36 The value of a term is defined
- $A(t) = \xi(t)$ if variable
- $A(t) = \phi(t)(A(t_1), \dots A(t_n))$ if function

The truthvalue of a formula:
- $A(F) = \psi(P)(A(t_1), \dots A(t_k))$ if predicate
- $A(\forall x F)$, $A(\exists x F)$ $= \begin{cases} 1 & \text{if } A_{[x \to u]}(F) = 1 \ \frac{\text{all}}{\text{some}}\ u \in U \\ 0 & \text{else} \end{cases}$

L.6.8 For all F, G, H, x 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) $(\forall x F) \land (\forall x G) \equiv \forall x (F \land G)$
4) $(\exists x F) \lor (\exists x G) \equiv \exists x (F \lor G)$
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) $(\forall x F) \land H \equiv \forall x (F \land H)$
8) $(\forall x F) \lor H \equiv \forall x (F \lor H)$
9) $(\exists x F) \land H \equiv \exists x (F \land H)$
10) $(\exists x F) \lor F \equiv \exists x (F \lor H)$

L.6.9 replace subformula F with equivalent formula, new f. $\equiv$ to F
L.6.10 For a formula G in which y does not occur:
$\forall x G \equiv \forall y G_{[x/y]}$ and $\exists x G \equiv \exists y G_{[x/y]}$
D.6.37 Formula in which no variable occurs both bound/free rectified
L.6.11 $\forall x F \models F_{[x/t]}$ for any t $\Rightarrow \forall x \models F$
D.6.38 $\forall x \exists y (P(x) \land Q(z) \to P(z))$ Prenexform

Prenex: 1) rename bound variables 2) remove all „$\to$" 3) apply morgan 4) shift $\exists, \forall$ to front

Ex: Prove $\forall x (F \land G) \models (\forall x F) \land G$
Let F, G be suitable formulas, Let A be any structure suitable for $\forall x (F \land G)$ and $(\forall x F) \land G$. Assume $A(\forall x (F \land G)) = 1$
sem $\forall$ $\Rightarrow A_{[x \to u]}(F \land G) = 1$ for any $u \in U^A$ n. at the end
sem $\land$ $\Rightarrow A_{[x \to u]}(F) = 1$ and $A_{[x \to u]}(G) = 1$ $\boxed{\text{for any } u \in U^A}$
$\Rightarrow A_{[x \to u]}(F) = 1$ for any $u \in U^A$ and
$A_{[x \to u]}(G) = 1$ for any $u \in U^A$
sem $\forall$ $\Rightarrow A(\forall x F) = 1$ and $A_{[x \to u]}(G) = 1$ for any $u \in U^A$
Case 1: x does not occur free in G. Then for any u we have $A_{[x \to u]}(G) = A(G)$ so $A(G) = A_{[x \to u]}(G) = 1$
Case 2: x does occur free in G. Then x occurs free in $(\forall x F) \land G$ so if A is suitable it defines $x \in U^A$. Since $A_{[x \to u]}(G) = 1$ for all $u \in U^A$, we have a particular for $u = x^A$, $A_{[x \to x^A]}(G) = 1$. So $A(G) = A_{[x \to x^A]}(G) = 1$
Therefore $A(\forall x F) = 1$ and $A(G) = 1 \overset{\text{sem} \land}{\Rightarrow} A((\forall x F) \land G) = 1$.

Proof system

D.6.2 proof system is sound if no false statement has proof
D.6.3 Proof system is complete every true statement has proof
Ex: $S = P = \{0,1\}^3$
complete: $J(S) = 1$ if s contains at most one 0
& not sound: $\phi(s,p) = 1$ if s contains at most two 0 and s = p
not complete: $\Upsilon(s) = 1$ if s contains at least one 1
& sound: $\phi(s,p) = 1$ if $d(s,p) = 3$ and p contains exactly one 0
d = Hamming distance

Proof Pattern

Composition of Implication: If S=>T and T=>U are both true then S=>U is true. $(A \to B) \land (B \to C) \models A \to C$
Direct Proof of an Impl. Proof S=>T by assuming S and proving T under the assumption
Indirect Proof of an Impl. Proof S=>T by assuming ¬T and proving ¬S under the assumption
Modus Ponens Prove S by finding R, proving R and then proving R=>S $(A \land (A \to B) \models B)$.
Case distinction Prove S by finding a list $R_1, \dots, R_k$ cases proving one R_i and prove for all $R_i \Rightarrow S$
Proof by Contradiction Prove S by finding T, proving T is false and then prove T is true under the assumption that S is false
Existence Proof Prove that S is true for at least one $x \in X$, if true constructive else non-constructive

Pigeonhole principle If a set of n objects is split into k<n sets, then at least one set contains $\lceil \frac{n}{k} \rceil$ objects
Proof by Counterexample Prove by counterexample that S not true
Proof by Induction: Prove P(0) Basis step, prove for any n $P(n) \Rightarrow P(n+1)$ Induction Step

Sets, Relations and Functions

Sets

D.3.1 $|A|$ cardinality = #elements in a finite set A
D.3.2 $A = B \iff \forall x (x \in A \land x \in B)$ $\Rightarrow A = B \iff A \subseteq B \land B \subseteq A$
D.3.3 $A \subseteq B \iff \forall x (x \in A \to x \in B)$
D.3.4 $\emptyset = \{\} \Rightarrow \forall A (\emptyset \subseteq A)$ $P(\emptyset) = \{\emptyset\}$
D.3.5 Powerset $P(A) = \{S \mid S \subseteq A\}$ $P(\emptyset \cup \{\emptyset\})$ $= \emptyset(\{\emptyset\} - \{\emptyset\}$ $P(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$
D.3.6 Union $A \cup B = \{x \mid x \in A \lor x \in B\}$ Let $x \in P(A)$ def Powerset: $x \subseteq A$
Intersection $A \cap B = \{x \mid x \in A \land x \in B\}$
D.3.7 Complement $\bar{A} = \{x \in U \mid x \notin A\}$ for some universe
D.3.8 Difference $B \setminus A = \{x \in B \land x \notin A\}$
T.3.4 Idempotence, Commutativity, Associativity -> logic
Consistency: $A \subseteq B \iff A \iff A \cup B = B$
D.3.9 Cartesian Product $A \times B = \{(a,b) \mid a \in A \land b \in B\}$ ordered pairs
$\emptyset \times A = \emptyset$ $(\{\{\emptyset\}\} \cup \{\emptyset\}) \times \{\emptyset, \emptyset\}$ $= \{\emptyset, \{\emptyset\}\} \times \{\emptyset\} = \{(\emptyset, \emptyset$

Relations

D.3.10 A relation ρ from set A to B is a subset of $A \times B$ if $B = A$, it's a relation on A
D.3.11 The identity relation on A is denoted id_A
D.3.13 The inverse of ρ is $\hat{\rho} = \{(b,a) \mid (a,b) \in \rho\}$
D.3.13 If ρ, σ are relations then
$\rho \circ \sigma = \{(a,c) \mid \exists b ((a,b) \in \rho \land (b,c) \in \sigma)\}$ is composition
L3.6 $\widehat{\rho \circ \sigma} = \hat{\sigma} \circ \hat{\rho}$ calculate ρ^2 etc. by matrix multiplication. for ρ^* add ρ, ρ^2, ρ^3

Special Properties

D.3.14 Reflexive: $a \rho a$ is true for all $a \in A$, $id \subseteq \rho$
Irreflexive $a \rho a$ is false for $\forall a$
D.1 Symmetric $a \rho b \iff b \rho a$ is true for all $a, b \in A$ 2

D3.17 Antisymmetric $(a\varrho b \wedge b\varrho a) \Rightarrow a=b$ is true for all $a,b \in A$

D3.18 Transitive: $(a\varrho b \wedge b\varrho c) \Rightarrow a\varrho c$ is true for all $a,b,c \in A$

L3.7 A relation is transitive iff $\varrho^2 \subseteq \varrho$. ϱ^* transitive closure

Equivalence Relations and Posets

D3.20 Equivalence Relation: reflexive, symmetric, transitive

D3.21 For θ on A, $[a]_\theta$ is an equivalence class $[a]_\theta = \{b \in A \mid b\theta a\}$

L3.8 Two intersections of equiv. relations form an equiv. relation

T3.9 The quotient set A/θ of equivalence classes of θ on A is partition on A

Ex: Let ϱ, σ be equivalence relation; prove $\varrho \circ \sigma$ is equiv. relation iff $\varrho\circ\sigma = \sigma\circ\varrho$

Reflexive: $\forall a \in A\ (a\varrho a \wedge a\sigma a) \overset{\varrho,\sigma \text{ reflexive}}{\Rightarrow} \overset{\text{def } \circ}{\forall a \in A}\ (a\ \varrho\circ\sigma\ a)$

Symmetric: For any $a,b \in A$ $(a,b) \in \widehat{\varrho\circ\sigma}$

$\Rightarrow (b,a) \in \widehat{\varrho\circ\sigma}$ | def inverse

$\Rightarrow (b,a) \in \widehat{\sigma\circ\varrho}$ | $\varrho\circ\sigma = \sigma\circ\varrho$

$\Rightarrow (b,a) \in \hat\varrho \circ \hat\sigma$ | L.3.6

$\Rightarrow (b,a) \in \varrho\circ\sigma$ | Symmetry of ϱ, σ

Transitive: For any $a,b,c \in A$ show $\varrho\circ\sigma = (\varrho\circ\sigma)^2$ which will prove T.L3.7

$(\varrho\circ\sigma)\circ(\varrho\circ\sigma) \overset{Ass}{=} \varrho\circ(\sigma\circ\varrho)\circ\sigma \overset{Assum}{=} \varrho\circ(\varrho\circ\sigma)\circ\sigma$

$\overset{Ass}{=} \varrho^2\circ\sigma^2 = \varrho\circ\sigma$ (since ϱ, σ are transitive

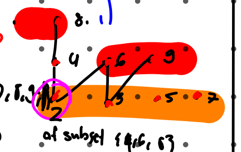
D3.24 A partial order on a set is reflexive, antisymmetric, transitive. A set with a partial order $\leq$ is called a poset

D.3.25 For a poset two elements are comparable if $a \leq b$ or $b \leq a$

D.3.26 If all elements are comparable, then A is totally-ordered

D.3.27 $a < b \Leftrightarrow a \leq b \wedge a \neq b$

D3.28 The Hasse diagram of a poset $v: A$, $e: a,b$ a covers b



T3.10 $(a_1,b_1) \leq (a_2,b_2) \Leftrightarrow a_1 \leq a_2 \wedge b_1 \sqsubseteq b_2$ is partial o. relation

T.3.11 $(a_1,b_1) \leq (a_2,b_2) \Leftrightarrow a_1 < a_2 \vee (a_1 = a_2 \wedge b_1 \leq b_2)$ lex.order, p.o. relation

D.3.29 Special Elements: let $(A;\leq)$ be a poset and $S \subseteq A$

1) $a \in A$ is a min/max element if $\nexists b$ with $b<a$ / $a<b$

2) $a \in A$ is the least/greatest element if for $\forall b$ $a \leq b$ / $b \leq a$

3) $a \in A$ is lower/upper bound of S if $\forall b \in S$ $a \leq b$ / $b \leq a$

4) $a \in A$ is greatest l.b. / least u.b. of S if a is greatest/least element of all lower/upper bounds of S.

D.3.30 A is well-ordered if it is totally ordered and every subset has least element

D.3.31 If $\{a,b\}$ have greatest lower bound $a \wedge b$ it is called meet; if they have a lowest upper bound $a \vee b$ it is called join

D.3.32 If all pairs of elements in a poset have meet/join → lattice

Functions

D.3.33 A function $f: A \to B$ from a domain to a codomain is a relation afb with special properties:

1) $\forall a \in A\ \exists b \in B\ afb$ — totally defined

2) $\forall a \in A\ \forall b,b' \in B\ (afb \wedge afb') \to b = b'$ — well defined

D.3.34 The set of all functions $f: A \to B$ is denoted B^A

D.3.35 A partial function is a relation s.t. 2) is true

D3.36 If $S \subseteq A$ then the image of S is $f(S) = \{f(a) \mid a \in S\}$

D3.37 The subset $f(A)$ of B is called the image of f $\mathrm{Im}(f)$

D3.38 for $T \subseteq B$, the preimage $f^{-1}(T) = \{a \in A \mid f(a) \in T\}$

D.3.39 Injective if $a \neq b$ then $f(a) \neq f(b)$

Surjective if $f(A) = B$ $\forall b \in B\ \exists a\ f(a) = b$

Bijective: injective, surjective → has inverse f^{-1}

For $f: A \to B$ and $g: B \to A$ f is injective iff g is surjective

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

D.3.41 The composition is defined $(g \circ f)(a) = g(f(a))$

L.3.12 Function composition is associative

Ex: Prove for $f: A \to A$ exists a g s.t. $g \circ f = id$ iff f is injective

⇒ consider $f(a) = f(b)$

$a = g\circ f(a)$
$= g(f(a))$
$= g(f(b))$
$= (g\circ f)(b)$
$= b$

⇐ we construct g as follows: any $b \in \mathrm{Im} f$ $g(b) = f(a)$ where $f(a) = b$. For $b \notin \mathrm{Im} f$, $g(b) = b$. We get $g \circ f = id$, because $\forall a \in A$, $f(a) \in \mathrm{Im} f$ so $g(f(a)) = a$ □

Countability

D.3.42 i) A and B are equinumerous if $A \sim B$ if there exists a bijection $A \to B$

ii) B dominates A, $A \preceq B$ if $A \sim C$ for $C \subseteq B$ or if there exists an injective function $A \to B$

iii) A is countable iff $A \preceq \mathbb{N}$ — $\mathbb{N}$ is countable

L3.13 i) $\preceq$ is transitive, ii) $A \subseteq B \Rightarrow A \preceq B$

T3.14 $A \preceq B \wedge B \preceq A \Rightarrow A \sim B$

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

Cantors diagonalization argument

We define α_{ij} as the jth digit of the ith sequence $f(i) = \alpha_{i0}\alpha_{i1}\alpha_{i2}\ldots$ we further define $\bar\alpha_{ij} = \alpha_{ij} + 1$

Now we take $\beta = \bar\alpha_{00}\bar\alpha_{11}\bar\alpha_{22}$

s_0: 1 0 0 1 0, s_1: 0 0 0 1 0, s_2: 1 1 0 ... 1001 — β differs from all $f(i)$ at least one digit

Countable Sets

T.3.16 $\{0,1\}^*$

T3.18 $\mathbb{N} \times \mathbb{N} = \mathbb{N}^2$

C3.19 $\mathbb{Q}$

T3.20 i) set of n-tuples over A
ii) union of countable sets
iii) set A^* of finite sequences

T3.21 $\{0,1\}^\infty$ is uncountable ⇒ $\mathbb{R}$ uncountable

D3.44 A function $f: \mathbb{N} \to \{0,1\}$ is computable if there exists a program $p \in \{0,1\}^*$ that can compute $f(n)$ for all $n \in \mathbb{N}$

Number Theory

Division

D.4.1 If a divides b we write $a|b$, $ac = b$ c is unique quotient, b is a multiple and a is a divisor

T.4.1 For all integers a and $d \neq 0$, there exists unique q and r s.t. $a = dq + r$ and $0 \leq r < |d|$

D.4.2 For $a,b \in \mathbb{N}$ (not both 0), $d \in \mathbb{Z}$ is the greatest common divisor if $d|a \wedge d|b \wedge \forall c((c|a \wedge c|b) \to c|d)$

D4.3 If $\gcd(a,b) = 1$ then a,b are relatively prime

L4.2 $\gcd(m, n - qm) = \gcd(m,n)$
⇒ euclid alg. $\gcd(m,n) = \gcd(R_m(n), m) = \ldots$

D.4.4 The ideal of $a,b \in \mathbb{Z}$ is $(a,b) = \{ua + vb \mid u,v \in \mathbb{Z}\}$; $a \in \mathbb{Z}$ is $(a) = \{ua \mid u \in \mathbb{Z}\}$

L.4.3 For $a,b \in \mathbb{Z}$ there exists $d \in \mathbb{Z}$, $(a,b) = (d)$

L4.4 If $(a,b) = (d)$ then $d = \gcd(a,b)$ ⇒ $\gcd(a,b) = ua + vb$

D.4.5 The least common multiple l of $a,b \in \mathbb{Z}$ denoted $\mathrm{lcm}(a,b)$ is defined as $a|l \wedge b|l \wedge \forall c((a|c \wedge b|c) \to l|c)$

Primes

D.4.6 A positive integer $p > 1$ is a prime iff the only positive divisors of p are p and 1. Else a number is a composite

T.4.6 Every positive integer → uniquely written as product of prime

$a = \prod_i p_i^{e_i}$ and $b = \prod_i p_i^{f_i}$ $\gcd(a,b) = \prod_i p_i^{\min(e_i,f_i)}$ and $\mathrm{lcd} \prod_i p_i^{\max(e_i,f_i)}$. $\gcd(a,b) \cdot \mathrm{lcm}(a,b) = a \cdot b$ since $\min(e_i,f_i) + \max(e_i,f_i) = e_i + f_i$

Congruence and Modular Arithmetic

$R_9(a)$ = sum of decimal $R_9(\Sigma a)$

D.4.8 For $a, b, m \in \mathbb{Z}$, $m \geq 1$ we say a is congruent to b modulo m, if m divides $a-b$
$a \equiv_m b \iff m \mid a-b$

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

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

C4.15 $f(a_1, \dots, a_k) \equiv_m f(b_1, \dots, b_k)$ for $a_i \equiv_m b_i$

L.4.16 i) $a \equiv_m R_m(a)$
ii) $a \equiv_m b \iff R_m(a) = R_m(b)$

C.4.17 $R_m(f(a_1, \dots, a_k)) = R_m(f(R_m(a_1), \dots, R_m(a_k)))$
$\Rightarrow R_m(ab) = R_m(R_m(a) \cdot R_m(b))$
$R_m(a+b) = R_m(R_m(a) + R_m(b))$
$R_m(a^b) = R_m(R_m(a)^b)$

From Fermat's little theorem and Euler's theorem
if $\gcd(m, a) = 1$, then $R_m(a^b) = R_m(a^{R_{\varphi(m)}(b)})$

Multiplicative Inverse

$R_m(b^e) = 1$ then $R_m(a^n) = R_m(a^{R_e(n)})$

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

D4.9 This solution is called the multiplicative inverse $x \equiv_m a^{-1}$. Only exists if $\gcd(a, m) =$

Ex: $\gcd(3, 26) =$
$26 = 8 \cdot 3 + 2$
$3 = 1 \cdot 2 + 1$

Backwards
$\Rightarrow 2 = 26 - 8 \cdot 3$
$\Rightarrow 1 = 3 - 1 \cdot 2 = 3 - 1 \cdot (26 - 8 \cdot 3)$
$= 3 - 1 \cdot 26 + 8 \cdot 3$
$= 9 \cdot 3 - 1 \cdot 26$ $\quad 3 \cdot 9 \equiv_2$

CRT

T.4.19 Let m_1, m_2, m_r be pairwise relatively prime and let $M = \prod_{i=1}^r m_i$. For every list $a_1, \dots, a_r$ with $0 \leq a_i < m_i$ for $i = 1, \dots, r$ the system
$x \equiv_{m_1} a_1$
$\vdots$
$x \equiv_{m_r} a_r$
has a unique solution x with $0 \leq x < M$

Ex: $x \equiv_3 2$, $x \equiv_4 1$, $x \equiv_5 4$, $M = 60$
1) $M_i = \frac{M}{m_i}$: $M_1 = 20$, $M_2 = 15$, $M_3 = 12$
2) $N_i M_i \equiv_{m_i} 1$: $N_1 20 \equiv_3 1 \Rightarrow N_1 = 2$; $N_2 \cdot 15 \equiv_4 1 \Rightarrow N_2 = 3$; $N_3 \cdot 12 \equiv_5 1 \Rightarrow N_3 = 3$
3) $\sum_{i=1}^r a_i \cdot M_i \cdot N_i = 2 \cdot 20 \cdot 2 + 1 \cdot 15 \cdot 3 + 4 \cdot 12 \cdot 3 \equiv_{M} 29$

If we have something like $x \equiv_{12} 8$, $x \equiv_{15} 2$ we need to decompose since $\gcd(12, 15) \neq 1$. We get $x \equiv_3 2$, $x \equiv_3 2$, $x \equiv_4 0$, $x \equiv_5 2$ — need to be eq

Diffie-Hellman

Idea: Encryption using a one-way function (easy to calculate, hard to i.)

Alice	Eve	Bob
a = random number in $\{0, 1, \dots, p-2\}$	Eve only gets y_A, y_B	b = random number in $\{0, 1, \dots, p-2\}$
$y_A = g^a \bmod p$		$y_B = g^b \bmod p$
$k_{AB} = y_B^a = g^{ba}$		$k_{BA} = y_A^b = g^{ab}$

Algebra

D.5.1 An operation on a set S is a function: $S^n \to S$, where $n \geq 0$ is the arity

D.5.2. An algebra is a pair $\langle S; \Omega \rangle$, where S is a set and Ω a list of operations

Monoids and Groups

D.5.3 A left/right neutral element is an element $e \in S$ s.t. $\forall a \in S$ $e * a = a$ / $a * e = a$. If both are true it is simply a neutral element

L.5.1 $\langle S; \Omega \rangle$ can only have one NE.

D.5.4. A binary operation $*$ is associative if $a * (b * c) = (a * b) \dots$

D.5.5 A monoid is an algebra $\langle M; *, e \rangle$ where $*$ asso e N

D.5.6 A left/right inverse of an element $a \in S$ is a $b \in S$ s.t. $b * a = e$ / $a * b = e$. If both are true: inverse

D.5.7 A group is an algebra $\langle G; *, \hat{}, e \rangle$ satisfying the axioms
G1 $*$ is associative
G2 e is a NE $a * e = e * a = a$
G3 $\forall a \in G$ $\exists \hat{a}$ $a * \hat{a} = e = \hat{a} * a$

D.5.8. A group/monoid is commutative/abelian if $a * b = b * a$

L.5.3 For groups we have:
i) $\hat{\hat{a}} = a$
ii) $\widehat{a * b} = \hat{b} * \hat{a}$
iii) $a * b = a * c \Rightarrow b = c$
iv) $b * a = c * a \Rightarrow b = c$
v) $a * x = b$ has a unique solution

The Structure of Groups

D.5.9 The direct product of n groups is the algebra $\langle G_1 \times \dots \times G_n; \dots \rangle$ where $\bullet$ is a component wise operation

D.5.10 A function ψ from group G to group H is a group homomorphism if for all $\psi(a * b) = \psi(a) * \psi(b)$. If ψ is bijective it is an isomorphism, we write $G \cong H$

L.5.5 A group homomorphism ψ satisfies: $\psi(e) = e'$ $\psi(\hat{a}) = \widehat{\psi(a)}$

When proving that something is isomorphism:
- homomorphism
- ϕ bijective

There exists exactly 4 non-isom. subgroups of $\langle \mathbb{Z}_m; \oplus \rangle$ when m is product of two distinct primes

D.5.11 A subset $H \subseteq G$ is a subgroup if H is a group, meaning it's closed with respect to all operations: $a * b \in H$, $e \in H$, $\hat{a} \in H$

D.5.12 The order of $a \in G$, $\mathrm{ord}(a)$ is the least $m \geq 1$ s.t. $a^m = e$. If no such m exists, $\mathrm{ord}(a) = \infty$

L.5.6 In a finite group every element has a finite order

D.5.13 For a finite group G $|G|$ is called the order of G

D.5.14 For $a \in G$, the group generated by a $\langle a \rangle$ is defined as $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$

D.5.15 A group $G = \langle g \rangle$ is called cyclic and g is called a generator of G. g^{-1} is also a generator.

Finding generators

$\langle \mathbb{Z}_m; \oplus \rangle$ all elements a with $\gcd(a, m) = 1$

$\langle \mathbb{Z}_m^*; \odot \rangle$
- calculate order of group
- for all $d \mid$ order check each element a if $a^d = 1$
- if not a is a generator. (order $= 16$, $d = \{1, 2, 4, 8, 16\}$; we only need $a^8 = 1$ to check.

Same goes for generators of $F[x]_{m(x)}$ etc.

Reality check: #generators $= \varphi(\text{order})$

T.5.7 A cyclic group of order n is isomorphic to $\langle \mathbb{Z}_n; \oplus \rangle$ and therefore commutative. All groups of prime orders are commutative

T.5.8 Lagrange: If $H \subseteq G$, $|H|$ divides $|G|$

C.5.9 For a finite group G, the order of $a \in G$ divides $|G|$

C.5.10 For a finite group G, $a^{|G|} = e$

C.5.11 Every group of prime order is cyclic and every element except the NE is a generator

D.5.16 $\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m \mid \gcd(a, m) = 1\}$ Multiplicative group

D.17 Euler function $\varphi(m) = |\mathbb{Z}_m^*| = p - 1$ if p is prime

L.5.12 If $\prod_{i=1}^r p_i^{e_i}$ is prime factorization
$\varphi(m) = \prod_{i=1}^r (p_i - 1) p_i^{e_i - 1}$
$p_i^{e_i} - p_i^{e_i - 1}$

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

C.5.14 for all $m \geq 2$ and $\gcd(a, m) = 1$ $a^{\varphi(m)} \equiv_m 1$ and for all primes p with $p \nmid a$ $a^{p-1} \equiv_p 1$

T.5.15 $\mathbb{Z}_m^*$ is cyclic iff $m = 2$, $m = 4$, $m = p^e$ or $m = 2p^e$ where p is odd prime $e \geq$

Inverse of a: $a^{\varphi(m) - 1} = \hat{a}$
$a^{\varphi(m)} \equiv_m 1$ $\quad a^{p-1} \equiv_m 1$ p: prime!

RSA

T.5.16 Let G be a finite group and $e \in \mathbb{Z}$ with $\gcd(e, |G|) = 1$. Then is $x \to x^e$ a bijection & x is the e-th root of $g \in G$, $g = x^e$. $x = g^d$, where d is the multiplicative inverse of e mod $|G|$, $e \cdot d \equiv_{|G|} 1$. Without $|G|$ it's hard to calculate e-th root

Alice	insecure channel	Bob
p, q large primes		
$n = pq$		
$f = (p-1)(q-1) = \varphi(n)$		m = message
select $e \in \mathbb{Z}_n^*$	$\xrightarrow{n, e}$	
$d \equiv_f e^{-1}$		
$m = R_n(y^d)$	$\xleftarrow{y}$	$y = R_n(m^e)$

Rings

D.5.18. A ring is an algebra which:
i) $\langle R; +, -, 0\rangle$ commutative group
ii) $\langle R; \cdot, 1\rangle$ is a monoid
iii) left and right distributive law is true
Ring is commutative if multiplication is commutative

L.5.17 i) $0a = a0 = 0$ ii) $(-a)b = -(ab)$ iii) $(-a)(-b) = a$
iv) if R is non-trivial $\Rightarrow 1 \neq 0$

D.5.19 Characteristics of a ring: order of 1 in the additive group, 0 if it's not finite

Commutative rings:

D.5.20. $a, b \in R$ we say a divides b, $a | b$ if $\exists c \in R$ $a \cdot c = b$ (everything divides 0 (except 0))

L.5.18 i) if $a|b$ and $b|c$ then $a|c$
ii) if $a|b$ then $a|bc$ $\forall c \in R$
iii) if $a|b$ and $a|c$ then $a|(b+c)$

D.5.22 Zerodivisor $a, b \in R$, $a \neq 0$, $b \neq 0$, $ab = 0$ then are a, b zerodivisors. $\varphi(m)$ gives you the number of units (aka degree). The number of zerodivisors are the other ones! $\mathbb{Z}_{33}$ 3 in 21 zerodivisors (for example)

Finding Zerodivisors all elements $a \in \mathbb{Z}_m$ s.t. $\gcd(a, m) \neq 1$

$\langle \mathbb{Z}_n; +\rangle$ is isomorphic to $\langle \mathbb{Z}_p; +\rangle \times \langle \mathbb{Z}_q; +\rangle$ iff $n = pq$ and $\gcd(p, q) = 1$ (CRT) !

D.5.23 Unit: $u \in R$ is a unit if it is invertible, $uv = vu = 1$, $v = u^{-1}$. The set of units of R is denoted R^*

$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$ $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$

L.5.19 For a ring R, R^* is a multiplicati

Finding units all elements s.t. $\gcd(a, m) = 1$

Order of $F[x]^*_{m(x)}$: L.5.33 $|F[x]_{m(x)}| = |F|^{\deg(m(x))}$
D.5.26 $|F[x]^*_{m(x)}| = |F[x]_{m(x)}| - 1$ ↳ if $F[x]_{m(x)}$ is a field

D.5.24 An integral domain is a commutative, non-trivial ring without zerodivisors.

L.5.20 In an integral domain with $a|b$, $b = ac$, c is unique and can be denoted $c = b/a$.

$\mathbb{Z}_m$ can only be an integral domain if m is prime

D.5.25 A polynomial $a(x)$ over R is $a(x) = \sum_{i=0}^{d} a_i x^i$ for some $d \geq 0$ and $a_i \in R$. $\deg(a(x))$ is equal to the largest $i \neq 0$. If all $a_i = 0$ it has degree $-\infty$. $R[x]$ denotes the set of polynomials over R

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

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

Calculate mod: in $\mathbb{Z}_5[x]_{x^2+1}$: simply substitute x^2 with 4 step
$x^2 + 1 \equiv_{x^2+1} 0$, $x^2 \equiv_{x^2+1} -1$ $x^2 \equiv_{x+1} 4$

Ex: List all elements $R \setminus R^*$ ($R = \mathbb{Z}_7[x]_{x^2+x+1}$). We have to remove all units. $x^2 + x + 1 = (x+3)(x+5)$ all elements that are not a linear combination of these factors are units. Therefore $R \setminus R^*$ = all multiples of $x+3$ and $x+5$

Fields

D.5.26 A field F is a non-trivial commutative ring in which every element $\neq 0$ is a unit: $F^* = F \setminus \{0\}$.

T.5.23 $\mathbb{Z}_p$ is a field iff p is prime $\mathbb{Z}_p = GF(p)$

T.5.24 Every field is an integral domain
unit → not zerodivisor

$\boxed{\mathbb{Z} \text{ integral domain, not a field}}$

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

D.5.28 A polynomial $a(x) \in F[x]$ with degree ≥ 1 is called irreducible if it's divisible only by a constant polynomial or a constant multiple of $a(x)$.

D.5.29 The monic polynomial of largest degree s.t. $g(x) | a(x)$ and $g(x) | b(x)$ is the gcd of $a(x)$ and $b(x)$.

T.5.25 For any $a(x)$ and $b(x) \neq 0$ in $F[x]$, there exists a unique monic $q(x)$ and a unique $r(x)$ s.t. $a(x) = q(x)b(x) + r(x)$ and $\deg(b(x)) > \deg(r(x))$

$\boxed{\text{If } F \text{ field, } F[x] \text{ cannot be field}}$

Polynomials as Functions

D.5.33 Let $a(x) \in R[x]$, $\alpha \in R$ for which $a(\alpha) = 0$ is called a root of $a(x)$

L.5.28 For a field F, $\alpha \in F$ is a root if $x - \alpha$ divides $a(x)$.

C.5.29 A polynomial of deg 2/3 is irreducible, if it has no roots

D.5.39 If α is a root of $a(x)$, then its multiplicity is the highest power of $(x-\alpha)$ dividing $a(x)$

T.5.30 For a field F, a nonzero polynomial of degree d has at most d roots, counting multiplicities

L.5.31 A polynomial $a(x) \in F[x]$ of degree d can be uniquely determined by $d+1$ values:
$a(x) = \sum_{i=1}^{d+1} \beta_i u_i(x)$ where $u_i(x) = \frac{(x-\alpha_1)\cdots(x-\alpha_{i+1})\cdots(x-\alpha_n)}{(\alpha_i - \alpha_1)\cdots(\alpha_i - \alpha_n)}$

gcd of two polynomials: apply euclid algorithm
Ex: $\gcd(x^3 + x + 2, x^2 + x + 1) = \gcd(x^2 + x + 1, x + 3) = \gcd(x+3, 0)$ $= x + 3$
always divide by smaller polynomial and keep the remain

Ex $2x + 1 \in \mathbb{Z}_7[x]_{x^2+x+1}$ find multiplicative inverse.
Divide $x^2 + x + 1$ $+1$ by $2x + 1$ to get the result

Irreducibility of Polynomials:
- deg 1: always irreducible
- deg 2/3: irreducible if they have no root
- deg 4: irreducible if they have no root / no factor deg 2
- deg 5: irreducible if they have no root / no factor of 2/

GF(2)	GF(3)		GF(5)		
10	10	1112	10	123	1021
11	11	1121	11	124	1024
111	12	1201	12	133	1032
1011	101	1211	14	134	1033
1101	112	1222	102	141	1042
10011	122	10012	103	142	1043
11001	1021	10022	111	1011	1101
11111	1102	10102	112	1014	1102
100101	10111	10121			1113

GF(7)								
10	15	113	125	145	163	1004	1026	1052
11	16	114	131	146	164	1005	1032	1055
12	101	116	135	152	166	1011	1035	1062
13	102	122	136	153	1002	1016	1041	1065
14	104	123	141	155	1003	1021	1046	[illegible]

Finite Fields

D.5.35 Let $m(x)$ be a polynomial of deg. d over F. Then $F[x]_{m(x)} = \{a(x) \in F[x] \mid \deg(a(x)) < d\}$

L.5.35 Let F be a finite field with q elements and let $m(x)$ be of degree d over F. Then $|F[x]_{m(x)}| = q^d$

L.5.34 $F[x]_{m(x)}$ is a ring with respect to addition and multiplication modulo $m(x)$

L.S.35 $F[x]^*_{m(x)} = \{a(x) \in F[x]_{m(x)} \mid \gcd(a(x), m(x)) = 1\}$

T.5.36 The ring $F[x]_{m(x)}$ is a field iff $m(x)$ is irreducible

T.5.35 $|GF(q)| = q-1$ for $q = p^e$, p = prime $e \geq 1$

If F is a field $F[x]$ can't be a field

.	assoc	e	$^{-1}$	comm.
monoid	✓	✓	X	X
Group	✓	✓	✓	X
Abelian Group	✓	✓	✓	✓

monoid: $\langle \mathbb{Z}; +, 0 \rangle$

group: $\langle \mathbb{Z}; +, -, 0 \rangle$, $\langle \mathbb{Z}[x]; +, -, 0 \rangle$

ring: $\langle \mathbb{R}; +, -, 0, \cdot, 1 \rangle$, $\mathbb{Z} \times \mathbb{Z}$

finite ring: $\langle \mathbb{Z}_m; +, -, 0; \cdot, 1 \rangle$ } $\langle G; +, -, 0, \cdot, 1 \rangle$ left away for simplicity

field: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, GF$

finite field: $\mathbb{Z}_{prime}$

$E((0,1,1)) = (0,1,1,0,1,1)$
$(6,3)$ encoding function
cardinality $q^k = 2^3$
where $q = |\{0,1\}|$

Application: ECC

D.5.36 $A(n,k)$-encoding function maps A^k to A^n, where $n > k$, the result is called a codeword

D.5.37. An (n,k)-ECC over A with $|A| = q$ is a subset of A^n with cardinality q^k

D5.38 Hamming Distance: number of positions in which two strings over A differ

D.5.39 Minimum Distance: minimal Hamming distance between any two codewords of an ECC

D5.40 A decoding function D for an (n,k)-encoding function is a function $D: A^n \to A^k$

T.5.40 An ECC with minimum distance d is t-error correcting iff $d \geq 2t+1$

T.5.41 Let $A = GF(a)$ and let $\alpha_0, \dots, \alpha_{n-1} \in A$
The encoding function $E((a_0, \dots, a_{k-1})) =$
$(a(\alpha_0), \dots, a(\alpha_{n-1}))$, where $a(x) = a_{k-1}x^{k-1} + \dots + a_0$
This ECC has minimum distance $n-k+1$

$t+1$ errors: correct encoding? $hw(c_{min}) = 2t+1$.
$c + c_{min} \in C$: $d(c, c + c_{min}) = hw(c_{min}) = 2t+1$. c and c_{min} differ on exactly $2t+1 = (t+1) + t$ pos.

GCD fast

a	b	q	u1	u2	v1	v2
553	26	21	1	0	0	1
26	7	3	0	1	1	-21
7	5	1	1	-3	-21	64
5	2	2	-3	4	64	-85
2	1	0	4	-11	-85	234
1	0	2	-11	4	234	-85

$a, b, q = \lfloor \frac{a}{b} \rfloor, 1\,0\,0\,1$

$a_i = b_{i-1}$ $b_i = a_{i-1} \bmod b_{i-1}$
$q_i = \lfloor \frac{a_i}{b_i} \rfloor$ $(u_1)_i = (u_2)_{i-1}$ $(v_1)_i = (v_2)_{i-1}$
$(u_2)_i = (u_1)_{i-1} - (q_{i-1} \cdot (u_2)_{i-1})$
$(v_2)_i = (v_1)_{i-1} - (q_{i-1} \cdot (v_2)_{i-1})$

a contains gcd, u_1, v_1 factors

Logarithm:

$\log_5 7 = \frac{a}{b} \Rightarrow 7 = 5^{\frac{a}{b}} \Rightarrow 7^b = 5^a$ Proof that $\log_5 7$ irrational

relatively prime

$|\mathbb{Z}_{14}| = 14$ $|\mathbb{Z}_2 \times \mathbb{Z}_4| = 4$ $|\mathbb{Z}^*_{42}| = 12$ $|GF(4)^*| = 3$

$|GF(4)| = 4$

Subgroups $\langle \mathbb{Z}_9; + \rangle = \{0\}; \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ $\{0, 3, 6\}$ generators 3, 6: $0, 0+3, 0+3+3$; $0, 0+6, 0+6+6$

Proving Injective:

$\forall x, u \in A$, $F(x) = F(u) \Rightarrow x = u$ To prove that a function $G: A \to B$ is injective we start by „fix any $x, u \in B$ with $(G(x) = G(u))$" then (using algebraic manipulation) we show that $x = u$.

Proving Surjective:

$\forall y \in B, \exists x \in A (y = F(x))$
- Fix any $y \in B$
- Scrap work: look at the equation $G(x) = y$ (Try to express x in terms of y)
- Write something like: „consider $x = \dots$" this being the expression in terms of y (scrap work). Show that $x \in A$. Then show $f(x) = y$

Ex: $ax \equiv_m b$ for some $x \in \mathbb{Z}$
$\Leftrightarrow ax - b = km$ for some $x, k \in \mathbb{Z}$
$\Leftrightarrow ax + (-k)m = b$ for some $x, k \in \mathbb{Z}$
$\Leftrightarrow b \in (a, m)$
$\Leftrightarrow b \in (d)$, where $d = \gcd(a, m)$
$\Leftrightarrow b = u \cdot \gcd(a, m)$ for some $u \in \mathbb{Z}$
$\Leftrightarrow \gcd(a, m) \mid b$

Ideals Example

f is θ consistent iff $(b_1 \theta b_1'$ and $b_2 \theta b_2') \Rightarrow f(b_1, b_2) \theta f(b_1', b_2')$

$P(A \cap B) \Leftrightarrow P(A) \cap P(B)$
$P(A \cup B) \cancel{\Leftrightarrow} P(A) \cup P(B)$
$A \subseteq B \Leftrightarrow P(A) \subseteq P(B)$

$(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$
$\Leftrightarrow ab' = ba'$ and $cd' = dc'$
$\Rightarrow ab' \cdot dd' + cd' \cdot bb' = ba' \cdot dd' + dc' \cdot bb'$
$\Rightarrow ad \cdot b'd' + bc \cdot b'd' = bd \cdot a'd' + bd \cdot b'c'$
$\Rightarrow (ad + bc) \cdot b'd' = bd \cdot (a'd' + b'c')$
$\Rightarrow (ad + bc, bd) \sim (a'd' + b'c', b'd')$
$\Rightarrow$ sum $((a,b),(c,d)) \sim$ sum $((a',b'),(c',d'))$

A is sufficient for B if $A \Rightarrow B$ holds
A is necessary for B if $\neg A \Rightarrow \neg B$ holds

Sufficient Necessary

$\{\forall y\, G_y\ \exists x\, \forall z\, F\} \vDash (\exists y\, G) \wedge (\forall z\, \exists x\, F)$ true!

$GF(16) = GF(2^4) \to$ irreducible polynomial of degree 4 over $GF(2)$

$GF(p^x)$ (p is prime, x is degree)

Cyclic groups
- All cyclic groups are commutative, cyclic of same order are isomorphic
- For $\langle \mathbb{Z}_n; \oplus, \ominus, 0 \rangle$ any element g with $\gcd(g, n) = 1$ is generator
- $\operatorname{ord}(a + b) = \operatorname{ord}(b + a) \Rightarrow \operatorname{ord}(a+b) = n \Rightarrow \operatorname{ord}(b + a) \leq n$: $(a+b)^n = e$; $(b+a)^n = e$

Show that $f_a: G \to G$ with $a \in G$ arbitrary is bijective
$x \mapsto a * x$

Injective, surjective,

Injective: $f(x) = f(x') \Leftrightarrow a * x = a * x' \Rightarrow$
$x = 1x = (\hat{a} * a) * x = \hat{a} * (a * x) = \hat{a} * (a * x') = (\hat{a} * a) * x' = 1 * x' = x'$

Surjective: $f(c) = b$. We can define b as $c = \hat{a} + b$, $c \in G$
$f(c) = a + (\hat{a} + b) = (a + \hat{a}) + b = e + b = b$

$f: A \to B$ inj. $\Leftrightarrow g: B \to A$ surj.
$\Rightarrow$ we give surje. $B \to A \overset{def}{\Leftrightarrow} g(b) = \begin{cases} \text{some } x \in f^{-1}(\{b\}), \text{if } b \in f(A) \\ \text{an arbitrary } a \in A, \text{ if } b \notin f(A) \end{cases}$

Injective surjective

$\Leftarrow$ we give inj. $A \to B \overset{def}{\Leftrightarrow} f(a) = b$, where b denotes an arbitrary element $b \in g^{-1}(\{a\})$
can't write $f^{-1}(x) \to$ not bijective $\to$ why $f^{-1}(\{x\})$

Countability:
$A = \bigcup_{i \in \mathbb{N}} A_i$: countable $F: \bigcup_{i=1}^{\infty} A_i \to \mathbb{N} \times \mathbb{N}$
$F(a_i) = (i, f_i(a_i)) \to$ surjective, countable

$S = \{g \in \{0,1\}^{\mathbb{N}} \mid \forall x \exists y (x < y \wedge g(x) = g(y))\}$ is uncountable

x	0	1	2	3		
g(x)	0	1	0	0	0	1
$g_b(x)$	b_0	0	1	b_1	0	1	b_2	...

$g_b(3i) = b_i$
$g_b(3i+1) = 0$
$g_b(3i+2) = 1$

$\{0,1\}^{\infty} \leq S$

$10 \equiv_8 2$
$2 \equiv_8 2$

$6 \cdot 11 \equiv_{13} 1$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
mod 1																			
mod 2	1																		
mod 3	1	2																	
mod 4	1	X	3																
mod 5	1	3	2	4															
mod 6	1	X	X	X	5														
mod 7	1	4	5	2	3	6													
mod 8	1	X	3	X	5	X	7												
mod 9	1	5	X	7	2	X	4	8											
mod 10	1	X	7	X	X	X	3	X	9										
mod 11	1	6	4	3	9	2	8	7	5	10									
mod 12	1	X	X	X	5	X	7	X	X	X	11								
mod 13	1	7	9	10	8	11	2	5	3	4	6	12							
mod 14	1	X	5	X	3	X	X	X	11	X	9	X	13						
mod 15	1	8	X	4	X	X	13	2	X	X	11	X	7	14					
mod 16	1	X	11	X	13	X	7	X	9	X	3	X	5	X	15				
mod 17	1	9	6	13	7	3	5	15	2	12	14	10	4	11	8	16			
mod 18	1	X	X	X	11	X	13	X	X	X	5	X	7	X	X	X	17		
mod 19	1	10	13	5	4	16	11	12	17	2	7	8	3	15	14	6	9	18	
mod 20	1	X	7	X	X	X	3	X	9	X	11	X	17	X	X	X	13	X	19

Function between two finite sets of equal cardinality is injective iff it is surjective

$(-a)b = a(-b)$: $(-a)b = 0 + (-a)b = a0 + (-a)b = a(-b+b) + (-a)b =$
$a(-b) + ab + (-a)b = a(-b) + (a-a)b = a(-b) + 0b =$
$a(-b) + 0 = a(-b)$

Isomorphism between $\mathbb{Z}_3 \times \mathbb{Z}_{35}$ and $\mathbb{Z}_{21} \times \mathbb{Z}_5$
As $\gcd(3, 35) = 1$ $f: \langle \mathbb{Z}_{105} \rangle \to \mathbb{Z}_3 \times \mathbb{Z}_{35}$ $x \mapsto \mathbb{Z}_3(x), \mathbb{Z}_{35}(x)$ is isom.
As $\gcd(21, 5) = 1$ $g: \mathbb{Z}_{105} \to \mathbb{Z}_{21} \times \mathbb{Z}_5$ $x \mapsto \mathbb{Z}_{21}(x), \mathbb{Z}_5$ is isom.
Therefore $g \circ f^{-1}$ is isomorphism

Let $f: P(\mathbb{N}) \to P(\mathbb{N})$ be any function. Prove that either image of f $\operatorname{im}(f)$ is unc. or there exists an $A \in P(\mathbb{N})$ s.t. $f^{-1}(\{A\})$ is uncountable or both
Assume $\operatorname{Im}(f)$ is countable, we show that there exists $A \in P(\mathbb{N})$ s.t. $f^{-1}(A)$ is uncountable. We assume towards a contradiction that $\forall A \in P(\mathbb{N})$ the set $f^{-1}(A)$ is countable. As $P(\mathbb{N})$ is uncountable and $P(\mathbb{N}) = \bigcup_{A \in \operatorname{Im}(f)} f^{-1}(A)$, since the countable union of countable sets is countable we have reached a contradiction. Therefore there must exist $A \in \operatorname{Im}(f)$ s.t. $f^{-1}(A)$ is uncountable

Let $C \subseteq GF(q)^n$ be a code that forms a group with elementwise addition. Let $d(c_1, c_2)$ denote the Hamming distance between two codewords $c_1, c_2 \in C$. Moreover, let $hw(c)$ denote the Hamming weight of a codeword $c \in C$
Assume that there exists $t \in \mathbb{N}$ s.t. $\min_{c \in C \setminus \{c^n\}} hw(c) = 2t+1$
Prove that C is t-error correcting.
Let $c_1, c_2 \in C$ with $c_1 \neq c_2$ be arbitrary. Since C forms a group we know that $c = c_1 + (-c_2) \in C$. We have $d(c_1, c_2) = hw(c_1 + (-c_2)) = hw(c) \geq 2t+1$. • two codewords differ at a position iff difference of their value is non-zero. last step, assumption from above, together with $c_1 \neq c_2$ implies $c \neq c^n$. $d_{min}(C) \geq 2t+1$