alex-levesque.com

MTHE 217 - Lecture Notes

Algebraic Structures with Applications

Prof. Felix Parraud • Fall 2025 • Queen's University

Contents

1 Algebraic Structures Overview **3**

2 Propositional Logic **4**
- 2.1 Connectives . . . 4

3 Valid Arguments **5**
- 3.1 Statement Definitions and Relationships . . . 5
- 3.2 Important Tricks and Definitions . . . 5

4 Proof Examples **7**
- 4.1 Proof with multiple premises . . . 7
- 4.2 Methods of proof . . . 8

5 Set Theory **9**
- 5.1 Quantifiers and definitions . . . 9
- 5.2 Sets . . . 9

6 Operations on Sets **10**
- 6.1 Definitions . . . 10
- 6.2 Proof: $A \subseteq B \Leftrightarrow A \cap B = A$ . . . 10
- 6.3 Finite and Disjoint Sets . . . 10
- 6.4 Inclusion-Exclusion Theorem . . . 11

7 Equivalence Relations **12**
- 7.1 Cartesian Product . . . 12
- 7.2 Binary Relation . . . 12
- 7.3 Equivalence Relations . . . 12

8 Equivalence Classes **14**
- 8.1 Congruence is an equivalence relation proof . . . 14
- 8.2 Equivalence class and congruence class . . . 14
- 8.3 Partition . . . 15

9 Functions and their properties **16**
- 9.1 Images . . . 16
- 9.2 Injective, Surjective, Bijective . . . 16

9.3 Composition, identity, and inverse . . . 16

10 Inverse of a Function **17**
10.1 Bijection-Invertibility Equivalence . . . 17
10.2 Cardinality . . . 18

11 Mathematical Induction **19**
11.1 Proof by Induction . . . 19

12 Factorization **20**
12.1 Strong Induction Example . . . 20

13 Division Algorithm **21**
13.1 Greatest Common Divisor and Bezout's Identity . . . 21
13.2 Bezout's identity and its proof . . . 21

14 The Euclidean Algorithm **22**

15 Modular Arithmetic **23**
15.1 Operations in $\mathbb{Z}_n$ . . . 23

16 Introduction to Groups, Rings and Fields **24**
16.1 Groups . . . 24
16.2 Rings . . . 24
16.3 Fields . . . 24
16.3.1 Units . . . 25

17 Fermat's little theorem and Euler's theorem **26**
17.0.1 Fermat's little theorem . . . 26
17.0.2 Euler's theorem . . . 26

18 Midterm 1 Whiteboard Proofs **27**

19 Cheat Sheet **31**
19.1 Propositional Logic . . . 31
19.2 Proof Techniques . . . 31
19.3 Set Theory . . . 32
19.4 Relations . . . 32
19.5 Equivalence Classes . . . 32
19.6 Functions . . . 33
19.7 Inverses & Cardinality . . . 33
19.8 Induction Principle . . . 33

#Math

1 Algebraic Structures Overview

[[09-03 Propositions and Statements]] [[09-05 Valid Arguments]] [[09-08 Proof Examples]] [[09-10 Set Theory]] [[09-12 Operations on Sets]] [[09-15 Equivalence Relations]] [[09-17 Equivalence Classes]] [[09-19 Functions and their properties]] [[09-22 Inverse of a Function]] [[09-24 Mathematical Induction]] [[MTHE 217 Cheat Sheet]] [[09-26 Factorization]] [[09-29 Division Algorithm]] [[10-01 The Euclidean Algorithm]] [[10-03 Modular Arithmetic]] [[10-21 Introduction to Groups, Rings and Fields]] [[10-23 Fermat's and Euler's theorem]] [Midterm 1 Whiteboard Proofs]

#Math

2 Propositional Logic

A proposition is a sentence or assertion that is true (T) or false (F), but not both A statement is a proposition, or two statements joined by a connective A conjunction $x_1 \wedge x_2 \wedge \ldots$ is true where all premises are true

[[09-10 Logic Circuits]]

2.1 Connectives

Connectives (or boolean operators) are functions that take one or more truth values and output a truth value

The negation of p, denoted by $\neg p$, is the denial of p. If p is T, then $\neg p$ is F

The conjunction of p and q is denoted by $p \wedge q$. It can also be calculated by pq AND is false if at least one of the statements is false

The disjunction of p and q is denoted by $p \vee q$. It can also be calculated by $p + q$ OR is true if at least one of the statements is true.

The conditional of p and q is denoted by $p \rightarrow q$. This is the same as $(\neg q \vee p)$, and as saying if p, then q

The biconditional of p and q is denoted by $p \leftrightarrow q$, and can also be written as $(p \rightarrow q) \wedge (q \rightarrow p)$

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

More Definitions

The **converse** of $p \rightarrow q$ is $q \rightarrow p$ The **inverse** of $p \rightarrow q$ is $\neg p \rightarrow \neg q$ The **contrapositive** of $p \rightarrow q$ is $\neg q \rightarrow \neg p$

#Math

3 Valid Arguments

A **premise** is a statement (a declarative sentence, either T or F) that is assumed to be true within an argument

When writing a final solution, we write the premises, then the conclusion:

$[\neg b \to (p \leftrightarrow r)] \wedge [\neg b \to r] \wedge [p \to \neg r]$

Conclusion: $\neg r$

3.1 Statement Definitions and Relationships

A statement is called a **tautology** if it is always true (e.g. $s = p \vee \neg p$)

A statement is called a **fallacy** if it is always false (e.g. $s = p \wedge \neg p$)

Let s and q be two statement forms involving the same set of propositions

We say that s **logically implies** q and write $s \Rightarrow q$ if whenever s is true, q is also true

We say that s **logically equivalent** q and write $s \Leftrightarrow q$ if both s and q have identical truth tables

3.2 Important Tricks and Definitions

a true statement cannot imply a false one

Contradiction (fallacy) $p \wedge \neg p \Leftrightarrow F$

Tautologies Law of excluded middle: $P \vee \neg P = T$ Law of non-contradiction: $\neg(P \wedge \neg P) = T$

$p \wedge F \Leftrightarrow F$ $p \wedge T \Leftrightarrow p$ $p \vee T \Leftrightarrow T$ $p \vee F \Leftrightarrow p$

if the engine fails, then part p or part q is failing $\neg(p \wedge q) \Leftrightarrow (\neg p) \vee (\neg q)$

Distributivity $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$ $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$

Contrapositive *if P implies Q, then not Q implies not P* $P \leftrightarrow Q \equiv (P \to Q) \wedge (Q \to P)$

[[DeMorgan]]'s laws: $\neg(P \wedge Q) \equiv (\neg P \vee \neg Q)$ $\neg(P \vee Q) \equiv (\neg P \wedge \neg Q)$

Double negation $\neg(\neg P) \equiv P$

Absorption *if it rains, it is wet,* but, *if it isn't wet, it didn't rain* $p \wedge (p \vee q) \Leftrightarrow p$ $p \vee (p \wedge q) \Leftrightarrow p$

Modus ponens: $(P \to Q), P \therefore Q$, means If P implies Q, and P is true, then Q must be true

Example: If it rains, then the ground is wet. So, when it rains, the ground is wet. However, if the ground is wet, it did not necessarily rain.

Modus tollens: $(P \to Q), \neg Q \therefore \neg P$, means if P implies Q, and Q is false, then P must also be false

Example: If it rains, then the ground is wet. If the ground is not wet, then it did not rain.

#Math

4 Proof Examples

A proof is an argument which shows that $S \Rightarrow Q$, where S and Q are statement forms

Proof 1

$S \Leftrightarrow Q$ if and only if $S \leftrightarrow Q$ is a tautology

$\Rightarrow$:

If $S \leftrightarrow Q$ is a tautology, then it cannot be false. So, while one statement is true, the other cannot be false. $\therefore$ if S and Q are T or F at the same time, then $S \Leftrightarrow Q$

$\Leftarrow$:

If S and Q are logically equivalent, $S = T$ and $Q = T$, or $S = F$ and $Q = F$, but no mixed case. $\therefore$ we are always in case of T if $S \leftrightarrow Q$. Hence, $S \leftrightarrow Q$ is a tautology

Proof 2

$S \Rightarrow Q$ iff $S \rightarrow Q$ is a tautology

$\Rightarrow$:

By definition, if $S \Rightarrow Q$, then whenever S is T, Q is also T

Consider the truth table of $S \rightarrow Q$, the only case where this is false is when S is T and Q is F. There is no interpretation of $S \Rightarrow Q$ where S is T and Q is F

Therefore, in every interpretation, $S \rightarrow Q$ is T, and is a tautology

$\Leftarrow$:

If $S \rightarrow Q$ is a tautology, then the interpretation where S is T and Q is false is excluded

Thus, whenever S is T, Q must also be T, and by definition, this means that $S \Rightarrow Q$

$\therefore S \Rightarrow Q \Leftrightarrow (S \rightarrow Q)$ is a tautology $\square$

4.1 Proof with multiple premises

Definition: An argument with premises $p_1, \ldots, p_n$ and conclusion q is valid (true) if $p_1 \wedge \cdots \wedge p_n \Rightarrow q$

We can prove $\neg b \rightarrow (p \leftrightarrow q) \wedge (r \rightarrow \neg b) \wedge (p \rightarrow \neg r) \Rightarrow \neg r$ by setting it equal to s and showing that it is a tautology

Instead of examining $2^3 = 8$ possible values for statements b, p, and r (brute force), we can prove that s is a tautology **by contradiction**

If s is not a tautology, there must be a truth-assignment making $\neg r = F$ and $q_1 = q_2 = q_3 = T$

Proof:

$$\neg r = F, r = T$$

$$q_3 = T, p \to \neg r = T, p \to F = T, p = F$$

$$q_2 = T, r \to \neg b = T, F \to \neg b = T, b = F$$

$$q_1 = \neg b \to (p \leftrightarrow r), T \to (F \leftrightarrow T), T \to F = F, \text{but } q_1 \text{ must be true}$$

So, this means that $s = F$ cannot happen $\therefore$ no truth assignment can make $s = F$, hence, s is a tautology $\square$

4.2 Methods of proof

1. Directly solve it, i.e. show that $P \to Q$ is a tautology
2. Proof by contraposition: show $\neg Q \Rightarrow \neg P$, i.e. show that $\neg Q \to \neg P$ is a tautology
3. Proof by contradiction: show that $\neg P \lor Q$is a tautology

#Math

5 Set Theory

5.1 Quantifiers and definitions

: stands for "such that" $\exists$ stands for "there exists" $\forall$ stands for "for all"

We can also apply **De Morgan's law** for quantifiers (we can distribute $\neg$):

$\neg(\exists x, P(x)) \Leftrightarrow \forall x, \neg P(x)$ $\neg(\forall x, P(x)) \Leftrightarrow \exists x, \neg P(x)$

The statement $P_A(x)$ is defined as: $P_A(x) =$

$$\begin{cases} T \text{ if } x \in A, \\ F \text{ if } x \notin A \end{cases}$$

5.2 Sets

A set S is a collection of objects Subset: $A \subseteq B$ if every element $\in A$ is $\in B$ Equal sets: $A = B \Leftrightarrow \forall x \in U, P_A(x) \Leftrightarrow P_B(x)$

The universal set U is the set that contains all the objects under consideration in a given context

$\mathbf{N} = \{0, 1, 2, \dots\}$ $\mathbf{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ $\mathbf{Q} = \left\{\frac{a}{b} : a, b \in \mathbf{Z}, b \neq 0\right\}$ $\mathbf{R}$, real numbers $\mathbf{C} = \{a + bi : a, b \in \mathbf{R}, i = \sqrt{-1}\}$

The following holds: $\mathbf{N} \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$

#Math

6 Operations on Sets

Sets are unordered.

6.1 Definitions

The union of sets, denoted by $X \cup Y$, $= \{x : x \in X \vee x \in Y\}$: **everything that's either in X or Y**

The intersection of sets, denoted by $X \cap Y$, $= \{x : x \in X \wedge x \in Y\} = \{x \in X : x \in Y\}$, **only the elements that X and Y have in common**

The set difference of sets, denoted by XY, $= \{x \in X : x \notin Y\}$ or $X \cap X^c$: **the elements that are in X but not in Y

The symmetric difference of sets, denoted by $X \Delta Y$, $= (X \cup Y)(X \cap Y)$ or $(XY) \cup (YX)$: **the elements that are in either X or Y, but not in both**

A **family** of elements of X is an indexed collection $(x_i)_{i \in A}$ where A is out index set and each $x_i \in X$

Further:

$A \cup \emptyset = A$ $A \cup U = U$ $A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap U = A$ If $Y \subseteq X$, then we sometimes write $Y^c = XY$ for the complement of Y in X

6.2 Proof: $A \subseteq B \Leftrightarrow A \cap B = A$

Forward: If $x \in A$, then $x \in A$ and $x \in B$, which means $x \in (A \cap B)$, hence $A \subseteq (A \cap B)$

Besides, if $x \in A \cap B$, then by definition $x \in A$, hence $A \cap B \subseteq A$

Since $A \subseteq (A \cap B)$ and $(A \cap B) \subseteq A$, we get $A \cap B = A$

Backward: Assume $A \cap B = A$

Take any $x \in A$. Then $x \in A \cap B$ since they are equal

By definition of intersection, $x \in B$ as well

Thus every element of A is also in B, i.e. $A \subseteq B$

Conclusion: $A \subseteq B$ if and only if $A \cap B = A$

6.3 Finite and Disjoint Sets

Finite sets: Sets X, Y and Z are finite sets if the number of distinct elements in these sets is given by a natural number (rather than some "infinite cardinal"). When a set is finite, we use $|X|$ to denote its size

Disjoint sets: Two sets A and B are disjoint if they have no elements in common. Essentially, they are non-overlapping

Pairwise disjoint sets: A collection of sets is pairwise disjoint if **every pair** of distinct sets in the collection is disjoint, i.e. $A_i \cap A_j = \emptyset$ for all $i \neq j$

If $X_1, \ldots, X_n$ are pairwise disjoint then $|X_1 \cup \cdots \cup X_n| = |X_1| + \cdots + |X_n|$

6.4 Inclusion-Exclusion Theorem

If sets X, Y and Z are not disjoint, then:

$|X \cup Y| = |X| + |Y| - |X \cap Y|$

The last term leaves if the sets are disjoint, because the intersection of disjoint sets is 0

Proof:

$|A \cup B| = |A| + |B| - |A \cap B|$

We can start by expression A and B as a union of disjoint sets. Here we are essentially saying that every set can be split into two disjoint parts using another set

$A = (A \cap B) \cup (A \cap B^c)$ and $B = (A \cap B) \cup (A^c \cap B)$

Now, we can express $A \cup B$ as a union of three disjoint pieces: $A \cup B = (A \cap B) \cup (A \cap B^c) \cup (A^c \cap B)$

These three sets are pairwise disjoint. So: $|A \cup B| = |A \cap B| + |A \cap B^c| + |A^c \cap B|$

From earlier, we can now rewrite: $|A| = |A \cap B| + |A \cap B^c|$ and $|B| = |A \cap B| + |A^c \cap B|$

$|A| + |B| = (|A \cap B| + |A \cap B^c|) + (|A \cap B| + |A^c \cap B|)$

$|A| + |B| = 2|A \cap B| + |A \cap B^c| + |A^c \cap B|$

We can now rearrange and see that the RHS is exactly $|A \cup B|$ from earlier: $|A| + |B| - |A \cap B| = |A \cap B| + |A \cap B^c| + |A^c \cap B|$

Therefore: $|A \cup B| = |A| + |B| - |A \cap B|$

#Math

7 Equivalence Relations

7.1 Cartesian Product

Definition: For two objects a, b, we write (a, b) for the ordered pair a and b

Definition: The Cartesian product of sets A, B is $A \times B = \{(a, b) | a \in A, b \in B\}$

Example: $A = \{a, b\}, B = \{1, 2, 3\}$

$A \times B = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$

7.2 Binary Relation

Definition: If X and Y are sets, then a **binary relation** from X to Y is a subset $R \subseteq X \times Y$. Whenever $(x, y) \in R$, we write xRy and say that "x is related to y under R"

The divisibility relation: Let $X = \{1, 2, 3, 4\}$, then D on X is the subset $D \subseteq X \times X$ given by $D = \{(2, 2), (2, 4), (2, 6), (3, 3) \dots\}$. We say $a|b$ if $b = Ra$ for some $R \in \mathbf{Z}$

The equality relation: Is the subset $E \subseteq X \times X$ given by $D = \{(1, 1), (2, 2), (3, 3), (4, 4)\}$

7.3 Equivalence Relations

Definition: A relation E on a set X is an equivalence relation if it is **reflexive, symmetric, and transitive**

Reflexive: xEx for all $x \in X$ Everyone is related to themselves

Symmetric: xEy implies yEx for all $x, y \in X$ If you're related to me, then I'm related to you. Both directions are always allowed.

Transitive: xEy and yEz implies xEz for all $x, y, z \in X$, If A is related to B, and B is related to C, then A is related to C

Equivalence Relation (and Classes) Example

Pg. 115, Problem 7

7. Let X be the set $\{1, 2, 3, 4\}$ and let

$$R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (3, 4), (4, 3), (4, 4)\}.$$

Show that R is an equivalence relation and write down its equivalence classes.

Reflexive: if $(x, x) \in R$ for all $x \in X$

$(1, 1), (2, 2), (3, 3), (4, 4)$ are all present, so R is reflexive

Symmetric: if whenever $(a, b) \in R$, then $(b, a) \in R$

$(1, 2)$ and $(2, 1)$ are both in R $(3, 4)$ and $(4, 3)$ are both in R, so R is symmetric

Transitive: if whenever $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$

From $(1, 2)$ and $(2, 1)$, we need $(1, 1)$, true From $(1, 2)$ and $(2, 2)$, we need $(1, 2)$, true From $(2, 1)$ and $(2, 2)$, we need $(2, 2)$, true etc., R is transitive

Equivalence classes: equivalence class of a is the set of all elements in X that are related to a under relation R

$a = 1$, all pairs starting with $1 : (1, 1), (1, 2) \therefore [1] = \{1, 2\}$ $a = 2$, all pairs starting with $2 : (2, 1), (2, 2) \therefore [2] = \{1, 2\} = [1]$, as expected in an equivalence relation $a = 3$, all pairs starting with $3 : (3, 3), (3, 4) \therefore [3] = \{3, 4\}$ $a = 4$, all pairs starting with $4 : (4, 3), (4, 4) \therefore [4] = \{3, 4\} = [3]$, as expected

The equivalence classes group the elements into disjoint sets: $\{1, 2\}, \{3, 4\}$, this is exactly the partition of$X$ induced by R

#Math

8 Equivalence Classes

8.1 Congruence is an equivalence relation proof

Definition: Two integers are congruent mod n, $n > 0$, if the integers leave the same remainder upon division by n

Congruence is an equivalence relation:

Reflexive:

$a \in \mathbf{Z}, a - a = 0 = 0n, \therefore a \equiv a \bmod n$

Symmetric:

$\forall a, b \in \mathbf{Z}$ with $a \equiv b \bmod n$, then $a - b = qn$ for some $q \in \mathbf{Z}$ Thus, $b - a = (-q)n$ and hence $b \equiv a \bmod n, \therefore$ symmetric

Transitive:

Take $a, b, c \in \mathbf{Z}$ with $a \equiv b \bmod n$ and $b \equiv c \bmod n$, we want to show that $a \equiv c \bmod n$ First, $a - b = qn$ and $b - c = rn$ for some $q, r \in \mathbf{Z}$. Adding these two expressions gives $a - c = qn + rn = (q + r)n, \therefore a \equiv c \bmod n$ and it is transitive

8.2 Equivalence class and congruence class

Given an equivalence relation $\sim$ on X, the equivalence class of $a \in X$ is the set $[a] = \{b \in X : b \sim a\}$. This is the group of all things in X that are related to a

If our equivalence relation is congruence modulo n on $\mathbf{Z}$, then equivalence classes of integers are called *congruence classes*.

Congruence classes example

Suppose we have integers $\ldots, -2, -1, 0, 1, 2, \ldots$

Pick a number n. Suppose $n = 4$ Now we build 4 buckets, labeled $0, 1, 2, 3$

Bucket 0: all integers that leave remainder 0 when divided by 4 $[0] = \{b \in \mathbf{Z} : b \equiv 0 (\bmod 4)\} = \ldots, -8, -4, 0, 4, 8, \ldots$

Bucket 1: all integers that leave remainder 1 when divided by 4 $[1] = \{b \in \mathbf{Z} : b \equiv 1 (\bmod 4)\} = \ldots, -7, -3, 1, 5, 9, \ldots$

Bucket 2: all integers that leave remainder 2 when divided by 4 $[2] = \{b \in \mathbf{Z} : b \equiv 2 (\bmod 4)\} = \ldots, -6, -2, 2, 6, 10, \ldots$

Bucket 3: all integers that leave remainder 3 when divided by 4 $[3] = \{b \in \mathbf{Z} : b \equiv 3 (\bmod 4)\} = \ldots, -5, -1, 3, 7, 11, \ldots$

These equivalence classes satisfy: $\mathbf{Z} = [0] \cup [1] \cup [2] \cup [3]$ This quotient set is exactly the integers modulo 4

8.3 Partition

Let X be a set, and $P(x)$ be the power set of X, meaning the set of all subsets of X

$Y \subseteq P(X)$ means that Y is some collection of subsets of X

A singular partition is the entire set of equivalence classes grouped together such that:

- every element of X is in exactly one class
- the classes don't overlap
- and together they cover all of X

Formal Definition: Y is a partition of X if:

- **Pairwise Disjoint:** No two different subsets in Y overlap. Formally, if $A, B \in Y$ and $A \neq B$, then $A \cap B = \emptyset$
- **Union equals** X: All the subsets in Y, taken together, cover X. That is, $\bigcup_{a \in Y} A = X$

#Math

9 Functions and their properties

Definition: A function $f : X \to Y$ is a relation $Gr(f) \subseteq X \times Y$ which satisfies the following condition: for all $x \in X$, there exists a unique $y \in Y$ with $(x, y) \in Gr(f)$

9.1 Images

Let $f : X \to Y$

The **image** of a set A under f is the set of all outputs of f when the input comes from A

The **pre-image** of a set B is the set of all inputs that map into B

Pre-image of an element: If we take a single element $a \in X$, then its image: $f(a) \in Y$. If we take a single element $b \in Y$, then its *pre-image* is: $f^{-1}(\{b\}) = \{x \in X | f(x) = b\}$

The image of an element is a single point, while the pre-image of an element can be empty, one element, or many elements.

9.2 Injective, Surjective, Bijective

[[Injective]]: A function is injective (one-to-one) if for every $a, b \in X$ with $a \neq b$ we have $f(a) \neq f(b)$. We can also say f is injective if $\forall a, b \in X, f(a) = f(b)$ implies $a = b$. This means that *no two different inputs collapse to the same output*

If α is injective, then every horizontal line intersects the graph of α *at exactly* one point

[[Surjective]]: A function is surjective (onto) if for every $c \in Y$ there exists some $a \in X$ with $f(a) = c$. We can also say that $\text{Im}(f) = Y$. This means that *a surjective function has every element of its codomain Y "hit" by at least one input*

If α is surjective, then every horizontal line intersects the graph of α at *at least* one point

Bijective: A function which is both injective and surjective is called bijective

9.3 Composition, identity, and inverse

Definition Given: $f : X \to Y$ and $g : Y \to Z$, then $(g \circ f)(x) = g(f(x))$ is $X \to Z$

Note: composition is not commutative: $g \circ f \neq f \circ g$, but it is associative: $h \circ (g \circ f) = (h \circ g) \circ f$

Definition: The identity function $id_X(x) = x$ acts like "do nothing", meaning if you compose it with any function, nothing changes

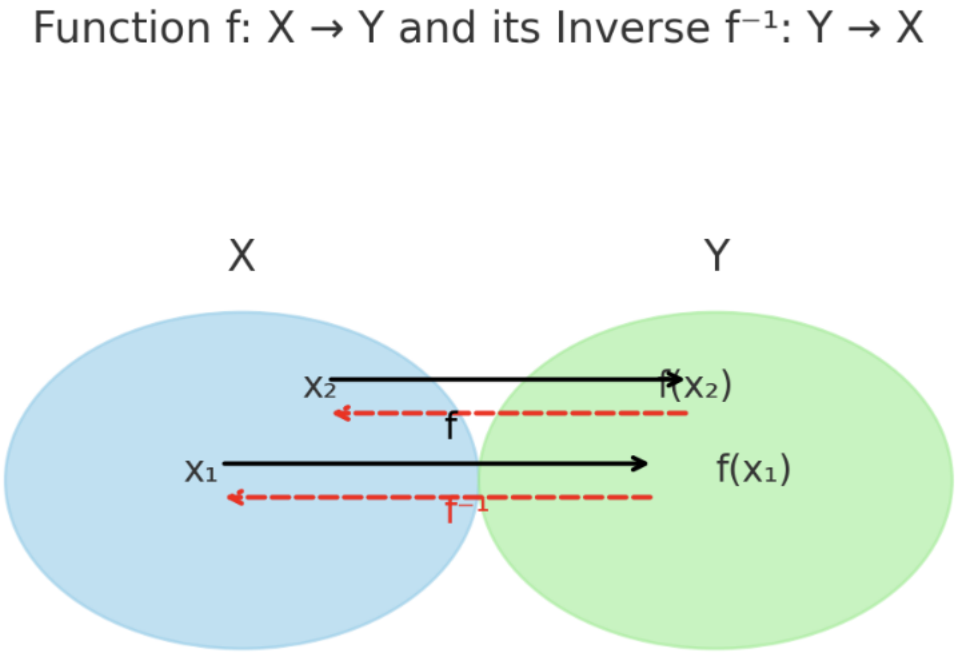
$f \circ id_X = f = id_Y \circ f$

Definition: The function $g : Y \to X$ is the inverse of $f : X \to Y$ if $f \circ g = id_Y$ and $g \circ f = id_X$. Thus, *only bijective functions have inverses.*

#Math

10 Inverse of a Function

Let $f : X \to Y$ and $g : Y \to X$ are functions. g is a compositional inverse of f if both $f \circ g = id_Y$ and $g \circ f = id_X$



If there is a composition inverse of f, then that compositional inverse is unique

Example: for the function $f : \{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4\}$, its compositional inverse is given below:

If $f(1) = 3$, then $f^{-1}(3) = 1$

10.1 Bijection-Invertibility Equivalence

Let $f : S \to T$ be a function between sets S and T. Then f is a bijection **if and only if** ff is invertible.

($\Rightarrow$) Suppose f is a bijection. Then:

- f is **injective**: each element of T has *at most one* pre-image in S.
- f is **surjective**: each element of T has *at least one* pre-image in S.

Together, this means **each** $y \in T$ **has exactly one pre-image** $x \in S$ such that $f(x) = y$.

Define $g : T \to S$ by setting $g(y) = x$, where x is the unique element in S such that $f(x) = y$. For any $y \in T$: $(f \circ g)(y) = f(g(y)) = f(x) = y$, so $f \circ g = id_T$. For any $x \in S$: $(g \circ f)(x) = g(f(x)) = g(y) = x$, so $g \circ f = id_S$.

Thus g is the inverse of f, so f is invertible.

($\Leftarrow$) Suppose f is invertible. Then there exists $g : T \to S$ such that:

$g \circ f = id_S$ and $f \circ g = id_T$.

Injectivity: If $f(x_1) = f(x_2)$, apply g: $g(f(x_1)) = g(f(x_2)) \Rightarrow x_1 = x_2$. Hence f is injective.

Surjectivity: For any $y \in T$, we have $y = (f \circ g)(y)$. Let $x = g(y)$. Then $f(x) = y$. Thus every $y \in T$ has a preimage in S.

Therefore f is bijective.

10.2 Cardinality

Two sets have the same cardinality (number of elements it contains) if there exists a bijection between the two sets. If two sets X and Y have the same cardinality, we write $|X| = |Y|$

Contrapositive:

Let $|A| = n, |B| = m, m \neq n$

If $m < n$, then at least one element $\in B$ has no preimage, so not surjective If $m > n$, then two elements $\in A$ maps to one $\in B$, so not injective

[Cardinality]

#Math

11 Mathematical Induction

Weak induction: A proof by *mathematical induction* is a proof that covers the *base case* $p(0)$ is true, and the *inductive case* $p(n) \Rightarrow p(n+1)$ for an arbitrary $n \in \mathbb{N}$

Or, we can introduce an *arbitrary base* N where $p(k) \Rightarrow p(k+1)$ for an arbitrary integer $k \geq N$

Strong induction: To prove a statement $P(n)$ with a base case $P(n_0)$ and assume *all previous cases* $P(n_0), P(n_0+1), \ldots, P(k)$ are all true to prove $P(k+1)$ is true

11.1 Proof by Induction

Define the base case $n = n_0$, where n_0 is the smallest value for which you claim the statement holds

Write an *Inductive Hypothesis*: Assume $P(k)$ is true for $k \geq n_0$, where k is typically $\in \mathbb{Z}$

Inductive Step: Using the assumption from above, prove $P(k+1)$ is true.

- Start with the LHS for $n = k+1$, plug in what you know from the hypothesis (e.g. substitution expressions, add the next term to a series)
- Simplify, show clearly how the assumption leads to the next case
- At the end, ensure the result matches the original claimed formula/form for $n = k+1$

End with a *summary line*: By induction, $P(n)$ is true for all $n \geq n_0$

#Math

12 Factorization

a divides b, and we write $a|b$, if there exists an integer q with $b = qa$, and a is a divisor/factor of b

Lemma: If $a|(b+c)$, then $a|b$ and $a|c$ because $b + c = qa \Rightarrow c = qa - b \Rightarrow c = qa - ra = (q - r)a$

An integer $p > 1$ is prime if its only positive divisors are 1 and p. Otherwise, p is called **composite**

12.1 Strong Induction Example

Theorem: every integer $n > 1$ can be written as a product of one or more primes

Induction base case: $n = 2$, since 2 is prime, the claim holds

Inductive hypothesis: Fix $k \geq 2$, and assume the claim holds for every integer m with $2 \leq m \leq k$

Inductive step: prove the claim for $n = k + 1$

If prime, we are done. If composite, then it can be written as a product of two integers a and b with $1 < a \leq b < k + 1$, in particular, $2 \leq a \leq k$ and $2 \leq b \leq k$

By the inductive hypothesis, a, b can be written as a product of primes. Multiplying those prime factorizations gives a prime factorization for $k + 1$

Theorem: Every positive integer can be expressed as a product of primes in a unique way, up to reordering the factors

Let $N = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$

p_1 divides N, so it must divide the right-hand product. If $p_1 = q_k$, then we can cancel that common prime and get $\frac{N}{p_1} = p_2 \dots p_r = q_1 \dots q_{k-1} q_{k+1} q_s$

But, $\frac{N}{p_1} < N$, so this smaller integer would have two distinct prime factorizations, contradicting the minimality of N, therefore $p_1 \neq$ any q_j

Thus, every integer > 1 has a prime factorization, and that factorization is unique up to ordering.

#Math

13 Division Algorithm

For any two integers n, d with $d \geq 1$, there exist unique integers q and r such that $n = qd + r$, with $0 \leq r < d$

Where: n is the dividend, d is the divisor, q is the quotient, r is the remainder

[[Division Algorithm Proof]] main idea: It formalizes every ordinary integer division: q is the quotient and r is the remainder If there were tow different pairs of (q, r), then subtracting gives $b(q_1 - q_2) = r_2 - r_1$, which is impossible unless they're equal because the remainder range is too small

13.1 Greatest Common Divisor and Bezout's Identity

The greatest common divisor $n, m \in \mathbb{Z}$ is the unique integer $gcd(n, m) \in \mathbb{N}$ The gcd of two integers is unique

Identities:

For $a, b, m \in \mathbb{Z}$, $gcd(am, bm) = mgcd(a, b)$ If $a, b, c \in \mathbb{Z}$ have $gcd(a, c) = 1$ and $c|ab$ then $c|b$ If $a, b \in \mathbb{Z}$ and p is prime then if $p|ab$ then $p|a$ or $p|b$

13.2 Bezout's identity and its proof

Bezout's Identity: For $n, m \in \mathbb{N}$, there exists $a, b \in \mathbb{Z}$ with $gcd(n, m) = an + bm$

Let $W = \{an + bm : a, b \in \mathbb{Z} \text{ for } an + bm > 0\}$ be the set of all integer combinations of n and m that are positive

If we choose $a = n$ and $b = m$, then $n^2 + m^2 > 0$, $\therefore W \neq \emptyset$

We know there exists a smallest element $d \in W$ such that $d = sn + tm$ for some $s, t \in \mathbb{Z}$

Show that $d = \gcd(n, m)$ by verifying the properties of gcd

1. Show that d divides n

$n = qd + r$ for some $0 \leq r < d$. $r = n - qd = n - q(sn + tm) = (1 - qs)n + qtm$. Thus r is a linear combination of n and m and is smaller than d. Since d is the smallest positive linear combination, r must be zero. Thus, $n = qd + 0 = qd$ and hence $d|n$. Vice-versa shows that $d|m$

2. Show that k divides d

Take an integer k with $k|n$ and $k|m$. Since $n = qd$ and $m = q'k$, we have $d = sn + tm = sqk + tq'k = (sq + tq')k$ and hence k divides d. Therefore, $d = \gcd(n, m)$

#Math

14 The Euclidean Algorithm

The Euclidean algorithm is an efficient algorithm for computing greatest common divisors.

By the [[Lemma 5.8]]: If $n = qm + r$ for any integers then $gcd(n, m) = gcd(m, r)$, we have $gcd(n, m) = gcd(m, r_1) = gcd(r_1, r_2) = \cdots = gcd(r_{k-1}, r_k)$

The algorithm must terminate in at most $m + 1$ steps, as the last step $gcd(r_{k-1}, r_k)$ is where the gcd can be computed explicitly as r_k with remainder 0

Example: compute $gcd(100, 28)$

$$\begin{aligned} 100 &= 3(28) + 16 \\ 28 &= 1(16) + 12 \\ 16 &= 1(12) + 4 \\ 12 &= 3(4) + 0 \end{aligned}$$

Now, find a, b such that $an + bm = gcd(100, 28)$

We can reverse the algorithm, for example take $16 = 1(12) + 4 \Rightarrow 4 = 16 - 1(12)$

$$\begin{aligned} 16 = 1(12) + 4 &\Rightarrow 4 = 16 - 1(12) \\ 28 = 1(16) + 12 &\Rightarrow= 16 - 1(28 - 1(16)) \\ 100 = 3(28) + 16 &\Rightarrow= 2(100 - 3(28)) - 1(28) \Rightarrow= 2(100) - 7(28) \end{aligned}$$

[[Lemma 5.9]]

#Math

15 Modular Arithmetic

Recall congruent modulo n: $n|(a-b) \Leftrightarrow a \equiv b \pmod{n}$

Congruence is an equivalence relation on the integers. The set of *all congruence classes modulo n* (quotient set of all equivalence classes) is denoted $\mathbb{Z}_n$

A general equivalence class $[a] \in \mathbb{Z}_n$ takes the form $[a] = \{b \in \mathbb{Z} : b \equiv a \text{ mod n}\}$ $[a] = \{a + qn : q \in \mathbb{Z}\}$

Essentially, if two numbers give the same remainder when divided by n, they're in the same congruence class or "bin"

Also $[a]$ means the equivalence class of all integers that have remainder a when divided by n

Example: As integers -3, 1, 5, and 9 all differ by multiples of 4, we know that every pair of these are congruent modulo 4

The congruence class $[1] \in \mathbb{Z}_4$ is $[1] = \{4q + 1 : q \in \mathbb{Z}\}$

[[Proposition 6.2]]

15.1 Operations in $\mathbb{Z}_n$

$[a] + [b] = [a + b]$ $[a] \cdot [b] = [ab]$

For example, take $[3], [5] \in \mathbb{Z}_6$

We get different representatives of each class, $[3] = [9]$ and $[5] = [11]$

We show that $[3] + [5] = [3 + 5]$ because 8 divided by 6 also gives remainder 2 Also, $[9] + [11] = [20]$ where 20 divided by 6 is also 2

Furthermore, $[3] \cdot [5] = [15] = [3]$ and $[9] \cdot [11] = [99] = [3]$

Thus, *addition and multiplication do not depend* on the choice of representative.

#Math

16 Introduction to Groups, Rings and Fields

An algebraic structure is a collection of objections, and one or more operations that can be performed on those objects. We categorize algebraic structures based on the properties of the operations.

We do this to draw generalizations among number systems, discover new systems with similar properties, and prove theorems about all systems with the same basic properties.

16.1 Groups

A **group** is a collection of objects G, together with one operation $\oplus$, which has the following properties

- Associativity: $a \oplus (b \oplus c) = (a \oplus b) \oplus c, \quad \forall a, b, c \in G$
- Identity: $\exists e \in G$ such that $a \oplus e = a = e \oplus a$ for all $a \in G$. The element e is called the *identity* of G
- Inverse: For every $g \in G$, there exists $g^{-1} \in G$ such that $g \oplus g^{-1} = g^{-1} \oplus g = e$

Common examples are $\mathbb{Z}$ with $+$, $\mathbb{Z}_n$ with $+$, $\mathbb{R}^*$ with $\times$, etc.

In saying that $\oplus$ is a binary operator $G \times G \to G$ is that given any $a, b \in G$, $a \oplus b$ must also be in G. We refer to this property by saying that G is closed under $\oplus$

Definition: A group G is **abelian** (or **commutative**) if $a \oplus b = b \oplus a$ for all $a, b \in G$

Definition: If G is a group with a finite number of elements, then the number of elements in G is called the *order* of G and is denoted by $|G|$

16.2 Rings

A **ring** is a set R, together with two operations $\oplus$ and $*$, which has the following properties:

- Under addition, the set $(R, +)$ must form a commutative group
- R is associative under $*$
- Multiplicative identity: There is an element 1 such that $r * 1 = 1 * r = r$ for all $r \in R$
- The operation $*$ distributes over $\oplus$: $a*(b \oplus c) = (a*b) \oplus (a*c)$ $(a \oplus b)*c = (a*c) \oplus (b*c)$

A ring is **commutative** if multiplication is commutative: $a \cdot b = b \cdot a \quad \forall a, b \in R$

Common examples include $\mathbb{Z}_n$ with addition and multiplication, etc.

16.3 Fields

A **field** is a set F, together with two operations $\oplus$ and $*$, which has the following properties:

- F is a commutative ring under $\oplus$ and $*$
- Every nonzero $f \in F$ has a multiplicative inverse, that is, some element $g \in F$ for which $f * g = g * f = 1$

Common examples include $\mathbb{Z}p$ where p is prime, $\mathbb{R}, \mathbb{C}$, etc.

16.3.1 Units

- If $a \in R$ has a multiplicative inverse, its called a **unit** (or said to be invertible)
- A **zero-divisor** is a nonzero element $a \in R$ such that there exists $b \neq 0$ with $a \cdot b = 0$, essentially the opposite of a multiplicative inverse
- In a field, there are no zero-divisors, every nonzero element is invertible

Example: in $\mathbb{Z}_6, [3]$ has no multiplicative inverse

Find some $b \in \{0, 1, 2, 3, 4, 5\}$ such that $3b \equiv 1 \mod 6$

By checking all possible b, we never get a remainder of 1. This happens because $gcd(3, 6) = 3 \neq 1$.

Important theorems and lemmas: $\mathbb{Z}_n$ is a commutative ring. The congruence class $[a] \in \mathbb{Z}_n$ has a multiplicative inverse $\Leftrightarrow \gcd(a, n) = 1$ Fix $n \geq 2$: Every non-zero element $[a] \in \mathbb{Z}_n$ has an inverse, $\mathbb{Z}n$ contains no zero-divisors, and n is prime Given a unit $[a] \in \mathbb{Z}_n$, there is some $m \in \mathbb{Z}$ with $[a]^m = [1]$

#Math

17 Fermat's little theorem and Euler's theorem

Given a unit $[a] \in \mathbb{Z}_n$, there is some $m \in \mathbb{Z}$ with $[a]^m = [1]$

Proof. Consider the sequence $[a], [a]^2, [a]^3, \ldots$ Since there are a finite number of elements in $\mathbb{Z}_n$, at some point an element must repeat itself. That is, there are some distinct integers $1 \leq k < l$ with $[a]^k = [a]^l$. Since $[a]$ is invertible we can multiply both sides by $[a]^-k$ to obtain $[1] = [a]^0 = [a]^{l-k}$. Therefore, $[a]^m = [1]$ where $m = l - k$. **Fermat's little theorem and Euler's theorem** gives us a choice of m which works for all units in $\mathbb{Z}_n$ simultaneously.

17.0.1 Fermat's little theorem

If p is prime and $[a] \in \mathbb{Z}_p$ is non-zero (i.e. $\gcd(a, p) = 1$) , then $[a]^p = [a]$, or phrased using modular arithmetic: if p is prime and $a \neq 0$ then $a^{p-1} \equiv 1 \pmod p$

In words: For any integer a that is not a multiple of a prime p, a^{p-1} is congruent to 1 modulo p

Example: compute the remainder of 9^{1234} upon division by 11

By Fermat's little theorem, since $\gcd(9, 11) = 1$, we get $9^{10} \equiv 1 \pmod{11}$

Working modulo 11,

$$\begin{aligned} 9^{1234} &\equiv (9^{1230})(9^4) \equiv (9^{10})^{123}(9^4) \\ &\equiv (1)^{123}(9^4) \equiv 9^4 \equiv 81^2 \\ &\equiv 4^2 \equiv 16 \equiv 5 \end{aligned}$$

Thus, the remainder of 9^{1234} after division by 11 is 5

17.0.2 Euler's theorem

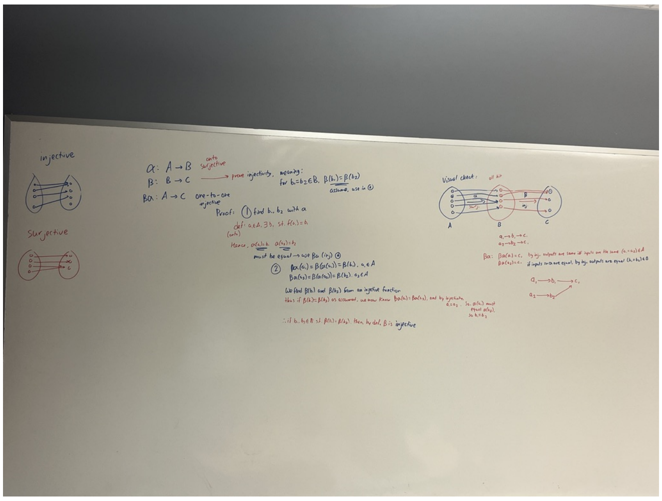
If $[a]$ is a unit in $\mathbb{Z}_n$, then $[a]^{\phi(n)} = [1]$, where $\phi(n)$ is the number of units in $\mathbb{Z}_n$.

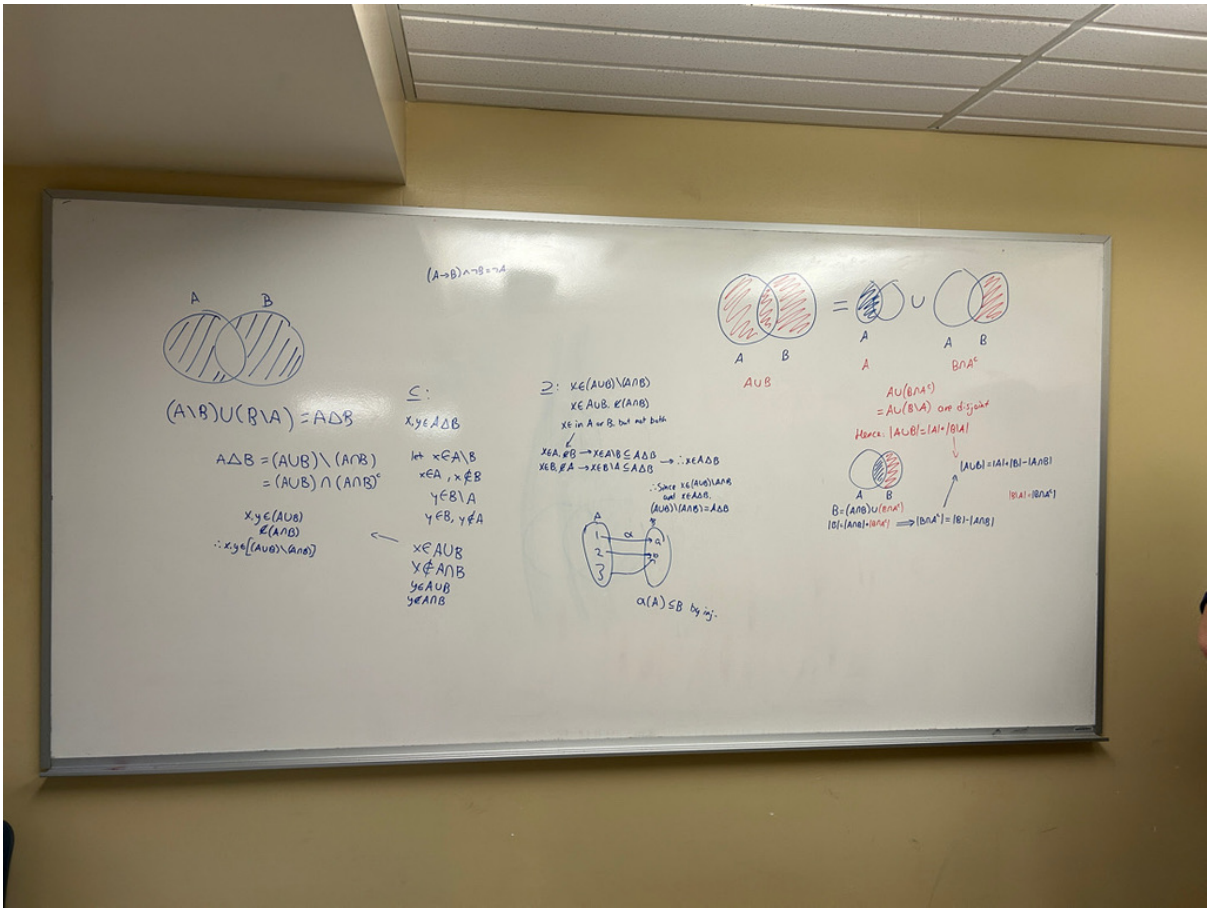
In terms of modular arithmetic: If $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod n$, where $\phi(n) = |\{b \in \mathbb{Z} : 1 \leq b \leq n \text{ and } \gcd(b, n) = 1\}|$.

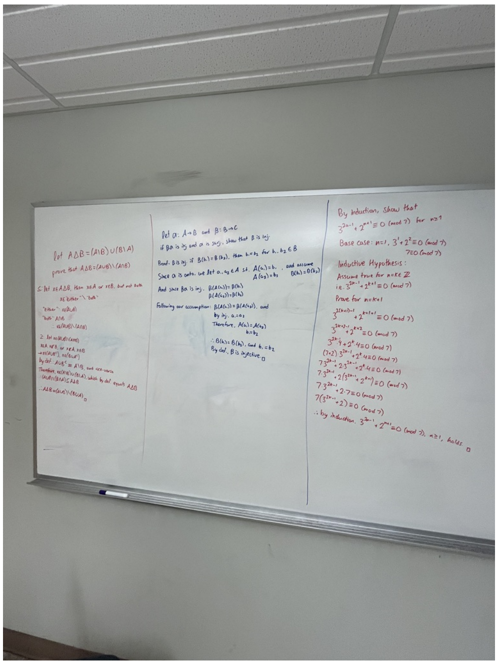
In words: if you have a positive integer n and any integer a that is relatively prime to n, then raising a to the power of $\phi(n)$ (the number of integers less than n that are relatively prime to n) will give a remainder of 1 when divided by n

Fermat's little theorem is just a special case of Euler's theorem where n is a prime number (since $\phi(p) = p - 1$)

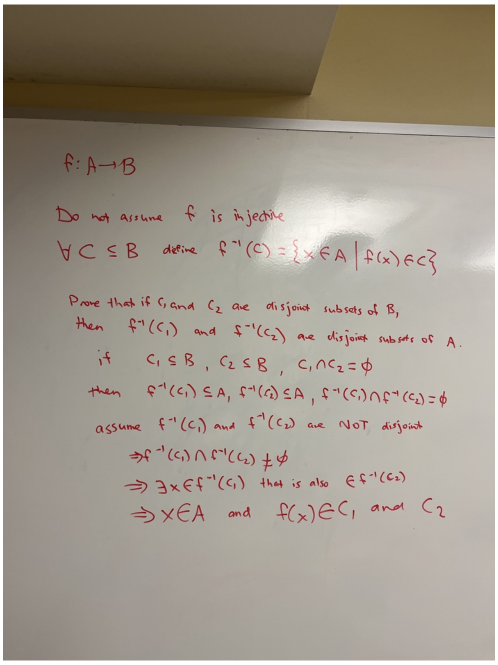
18 Midterm 1 Whiteboard Proofs



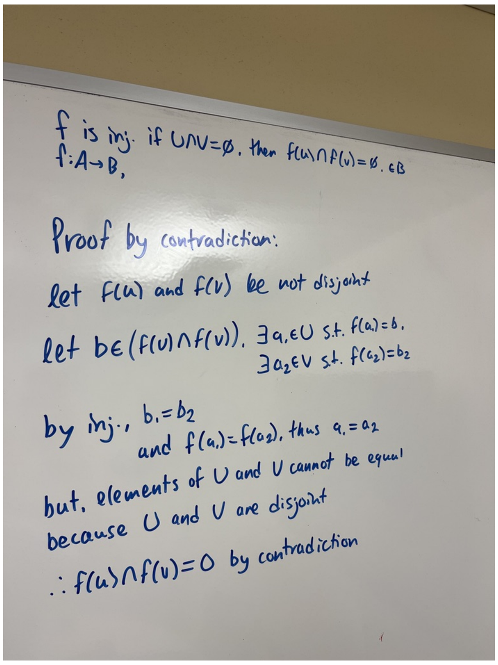


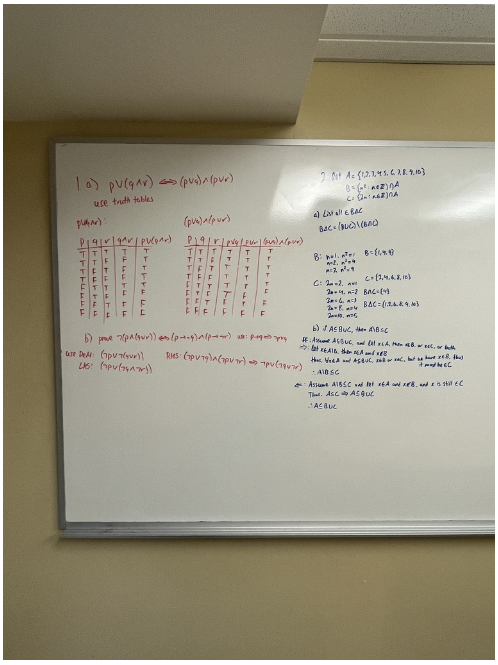


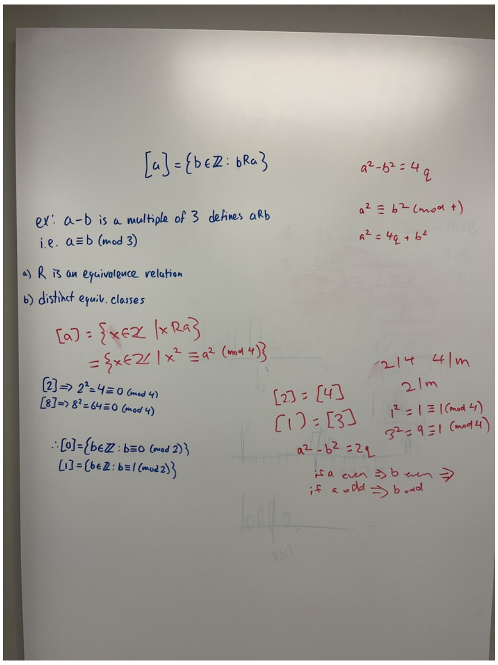
Let $A \Delta B = (A \setminus B) \cup (B \setminus A)$
prove that $A \Delta B = (A \cup B) \setminus (A \cap B)$
Let $\alpha: A \to B$ and $\beta: B \to C$
if $\beta\alpha$ is inj. and α is surj., show that β is inj.
By def., β is injective.
By induction, show that
$3^{2n-1} + 2^{n+1} \equiv 0 \pmod 7$ for $n \geq 1$
Base case: $n=1$, $3^1 + 2^2 \equiv 0 \pmod 7$
$7 \equiv 0 \pmod 7$
Inductive Hypothesis:
Assume true for $n = k \in \mathbb{Z}$
i.e. $3^{2k-1} + 2^{k+1} \equiv 0 \pmod 7$
Prove for $n = k+1$
$3^{2(k+1)-1} + 2^{k+1+1} \equiv 0 \pmod 7$
$3^{2k+2-1} + 2^{k+2} \equiv 0 \pmod 7$
$3^{2k-1} \cdot 9 + 2^k \cdot 4 \equiv 0 \pmod 7$
$(7+2) \cdot 3^{2k-1} + 2^k \cdot 4 \equiv 0 \pmod 7$
$7 \cdot 3^{2k-1} + 2 \cdot 3^{2k-1} + 2^k \cdot 4 \equiv 0 \pmod 7$
$7 \cdot 3^{2k-1} + 2(3^{2k-1} + 2^{k+1}) \equiv 0 \pmod 7$
$7 \cdot 3^{2k-1} + 2 \cdot 7 \equiv 0 \pmod 7$
$7(3^{2k-1} + 2) \equiv 0 \pmod 7$
$\therefore$ by induction, $3^{2n-1} + 2^{n+1} \equiv 0 \pmod 7$, $n \geq 1$, holds.

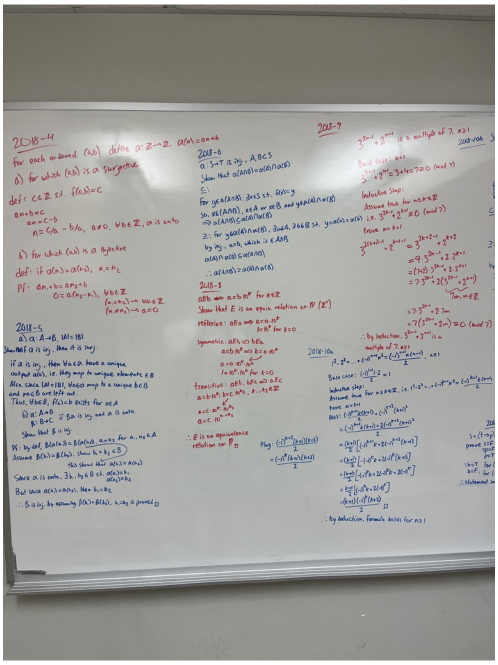


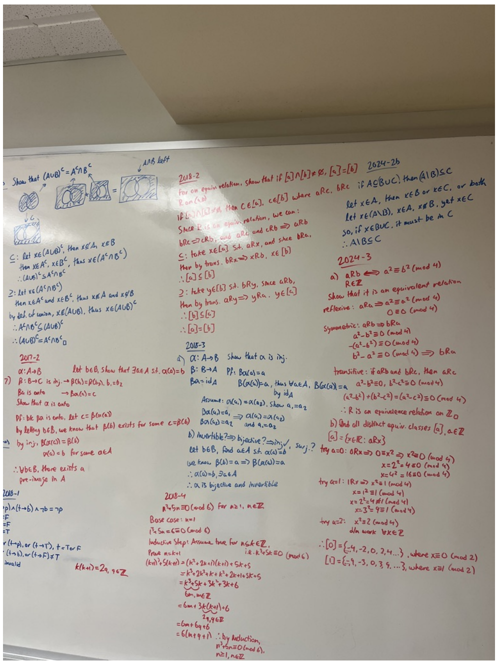
$f: A \to B$
Do not assume f is injective
$\forall C \subseteq B$ define $f^{-1}(C) = \{x \in A \mid f(x) \in C\}$
Prove that if C_1 and C_2 are disjoint subsets of B,
then $f^{-1}(C_1)$ and $f^{-1}(C_2)$ are disjoint subsets of A.
if $C_1 \subseteq B$, $C_2 \subseteq B$, $C_1 \cap C_2 = \phi$
then $f^{-1}(C_1) \subseteq A$, $f^{-1}(C_2) \subseteq A$, $f^{-1}(C_1) \cap f^{-1}(C_2) = \phi$
assume $f^{-1}(C_1)$ and $f^{-1}(C_2)$ are NOT disjoint
$\Rightarrow f^{-1}(C_1) \cap f^{-1}(C_2) \neq \phi$
$\Rightarrow \exists x \in f^{-1}(C_1)$ that is also $\in f^{-1}(C_2)$
$\Rightarrow x \in A$ and $f(x) \in C_1$ and C_2


f is inj. if U∩V=∅, then f(U)∩f(V)=∅. ∈B
f:A→B,
Proof by contradiction:
let f(U) and f(V) be not disjoint
let b∈(f(U)∩f(V)). ∃a₁∈U s.t. f(a₁)=b₁
∃a₂∈V s.t. f(a₂)=b₂
by inj., b₁=b₂
and f(a₁)=f(a₂), thus a₁=a₂
but, elements of U and V cannot be equal
because U and V are disjoint
∴ f(U)∩f(V)=0 by contradiction


1 a) p∨(q∧r) ⟺ (p∨q)∧(p∨r)
use truth tables


[a]={b∈ℤ: bRa}
ex: a−b is a multiple of 3 defines aRb
i.e. a≡b (mod 3)
a) R is an equivalence relation
b) distinct equiv. classes
[a] = {x∈ℤ | xRa}
= {x∈ℤ | x² ≡ a² (mod 4)}
[2] ⟹ 2²=4≡0 (mod 4)
[8] ⟹ 8²=64≡0 (mod 4)
∴ [0]={b∈ℤ: b≡0 (mod 2)}
[1]={b∈ℤ: b≡1 (mod 2)}
a²−b² = 4q
a² ≡ b² (mod 4)
a² = 4q + b²
2|4 4|m
2|m
[2] = [4]
[1] = [3]
1² = 1 ≡ 1 (mod 4)
3² = 9 ≡ 1 (mod 4)
a² − b² = 2q
if a even ⟹ b even ⟹
if a odd ⟹ b odd





19 Cheat Sheet

19.1 Propositional Logic

- Conditional: $p \to q$ (false only if $p = T$, $q = F$)

- Biconditional: $p \leftrightarrow q$ (iff)
- **Equivalences:**
  - Contrapositive: $(p \to q) \equiv (\neg q \to \neg p)$

  - De Morgan: $\neg(p \land q) \equiv (\neg p \lor \neg q)$,
    $\neg(p \lor q) \equiv (\neg p \land \neg q)$

  - Law of Excluded Middle: $p \lor \neg p = T$

Inference rules:

- Modus Ponens: $(p \to q),\ p \ \Rightarrow \ q$

- Modus Tollens: $(p \to q),\ \neg q \ \Rightarrow \ \neg p$

Converse vs Contrapositive Statements

- Converse of $P \to Q$ is $Q \to P$. Simply switch the hypothesis and the conclusion of the original statement. This may change whether the statement is T/F
- Contrapositive to $P \to Q$ is $\neg Q \to \neg P$

19.2 Proof Techniques

General Strategy:

- restate in your own words
- list known facts
- clarity the goal
- look for patterns/theorems
- try examples, use concrete numbers or finite sets to test ideas
- break into sub-parts
- don't forget both sides of $\Leftrightarrow$:$\Rightarrow \land \Leftarrow$ and $=$:$\subset \land \supset$
- try to visualize (e.g. sets)

- **Direct Proof:** Show $P \to Q$.

- **Contrapositive:** Show $\neg Q \to \neg P$.

- **Contradiction:** Assume $\neg Q$ and derive a falsehood.

19.3 Set Theory

- **Common Sets:**
  $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

Operations on Sets

- Union: $A \cup B = \{x : x \in A \vee x \in B\}$

- Intersection: $A \cap B = \{x : x \in A \wedge x \in B\}$

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

- Symmetric Difference: $A \Delta B = (A \setminus B) \cup (B \setminus A)$

- **Inclusion-Exclusion:**
  $|A \cup B| = |A| + |B| - |A \cap B|$
- $|B \setminus A| = |B \cap A^C|$

19.4 Relations

- **Cartesian Product:** $A \times B = \{(a, b) : a \in A, b \in B\}$

- **Relation:** $R \subseteq A \times B$

- **Equivalence Relation:** Reflexive, Symmetric, Transitive.

- **Partial Order:** Reflexive, Antisymmetric, Transitive.

- **Total Order:** Partial order + comparability ($\forall x, y : x \leq y \vee y \leq x$).

19.5 Equivalence Classes

- Equivalence class of a: $[a] = \{x \in X : x \sim a\}$

- **Partition:** Disjoint classes covering X.

- **Congruence mod n:**
  $a \equiv b \pmod{n} \Leftrightarrow n \mid (a - b)$

Example: $10 \equiv 2 \pmod{4}$

- Equivalence classes either are completely separate or exactly the same
- If two equivalence classes share even one element, they must be identical
- Parity is the property of an integer of whether it is even or odd

- Ex: On $\mathbb{Z}$, define aRb if $\frac{a+b}{2} \in \mathbb{Z}$, meaning a and b have the same parity, or $a \equiv b \pmod 2$

19.6 Functions

- Function $f : X \to Y$: $\forall x \in X, \exists! y \in Y$ with $f(x) = y$

- **Image:** $f(A) = \{f(x) : x \in A\}$

- **Preimage:** $f^{-1}(B) = \{x \in X : f(x) \in B\}$
- **Injective (1–1):** $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$ no two inputs map to the same output
- **Surjective (onto):** $\forall y \in Y, \exists x \in X : f(x) = y$ every output is hit by some input $\Leftrightarrow \text{Im}(f) = Y$

- **Bijective:** Both injective & surjective.

- **Identity:** $\text{id}_X(x) = x$

- **Inverse:** f^{-1} exists $\Leftrightarrow f$ is bijective.

- f is invertible if $\exists g$ s.t. $g \circ f = id_A$ and $f \circ g = id_B$

Let $\alpha : A \to B$ is injective, then: - $\alpha(A) \subseteq B$ - $|A| \leq |B|$

For the identify function id_A, if $BA = id_A$, then A is injective because $(BA)(a) = a$

19.7 Inverses & Cardinality

- **Bijection $\Leftrightarrow$ Invertible.**

- If $|A| = n, |B| = m$:
  - If $m < n$: not surjective

  - If $m > n$: not injective

- **Equal cardinality:** $|X| = |Y| \Leftrightarrow \exists$ bijection $f : X \to Y$

19.8 Induction Principle

- **Well-Ordering Principle:** Every non-empty $X \subseteq \mathbb{N}$ has a least element.

- **Weak Induction:**
  1. Base Case: prove $P(0)$.

2. Inductive Step: $P(n) \Rightarrow P(n+1)$.

- **Strong Induction:** Assume $P(k)$ true for all $k \leq n$, then prove $P(n+1)$.

Tricks during inductive step: - General: find a way to relate this step to the base case - Don't simplify (k+1) multiplications until necessary - Break down constant multiples (e.g. $9 = 8 + 1$) - Change inductive step: $3^n - 1 = 8m \Rightarrow 3^n = 8m + 1$ - Use parity properties: $k(k+1) = even, k + (k+1) = odd$ - For series, add the next step to RHS and simplify, then sub k+1 for n and solve for LHS, equate both sides