alex-levesque.com

MTHE 217 - Lecture Notes

Algebraic Structures with Applications

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

Contents

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 Rings and Fields]] [[10-23 Fermat's and Euler's theorem]] [[10-27 RSA Cryptography]] [[10-29 Group Theory]] [[10-31 Subgroups]] [Midterm 1 Whiteboard Proofs]

2 Basis

Here is a basis to common mathematical notation that were not explicitly defined previously:

Definition: Introduces and precisely describes a new concept. They establish what something means, and do not require a proof.

Theorem: A major result that's proven from earlier results, axioms, or definitions. It states something important and is usually a main milestone of the theory.

Lemma: A smaller, supporting result used to prove a larger one. It is a technical stepping stone to help a bigger theorem.

Corollary: A result that follows easily or immediately from a theorem.

Proposition: A mathematical statement that is true, proved, but not as significant as a theorem.

Proof: A logical argument that demonstrates a statement is true.

Remark: A comment or observation related to a result, often giving intuition, warning, or connection.

Example: Illustrates a definition, theorem, or concept in action.

3 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]]

3.1 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 $\neg q \rightarrow \neg p$

4 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:

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

Conclusion: $\neg r$

4.1 Statement Definitions and Relationships

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

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

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

4.2 Important Tricks and Definitions

a true statement cannot imply a false one

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

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

$p \land F \Leftrightarrow F$ $p \land T \Leftrightarrow p$ $p \lor T \Leftrightarrow T$ $p \lor F \Leftrightarrow p$

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

Distributivity $p \land (q \lor r) \Leftrightarrow (p \land q) \lor (p \land r)$ $p \lor (q \land r) \Leftrightarrow (p \lor q) \land (p \lor r)$

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

[[DeMorgan]]'s laws: $\neg(P \land Q) \equiv (\neg P \lor \neg Q)$ $\neg(P \lor Q) \equiv (\neg P \land \neg Q)$

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

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

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.

5 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 $\square$

5.1 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 $\square$

5.2 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 $\neg P \vee Q$is a tautology

6 Set Theory

6.1 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: $P_A(x) =$

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

6.2 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: $\mathbf{N} \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$

7 Operations on Sets

Sets are unordered.

7.1 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

7.2 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 $A \cap B = A$

7.3 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 $|X_1 \cup \cdots \cup X_n| = |X_1| + \cdots + |X_n|$

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

8 Equivalence Relations

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

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

8.2 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 $D = \{(1, 1), (2, 2), (3, 3), (4, 4)\}$

8.3 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

9 Equivalence Classes

9.1 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

9.2 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 $[0] = \{b \in \mathbf{Z} : b \equiv 0 (\text{mod } 4)\} = \ldots, -8, -4, 0, 4, 8, \ldots$

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

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

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

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

9.3 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, $\bigcup_{a \in Y} A = X$

10 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 $(x, y) \in Gr(f)$

10.1 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.

10.2 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

10.3 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: $h \circ (g \circ f) = (h \circ g) \circ f$

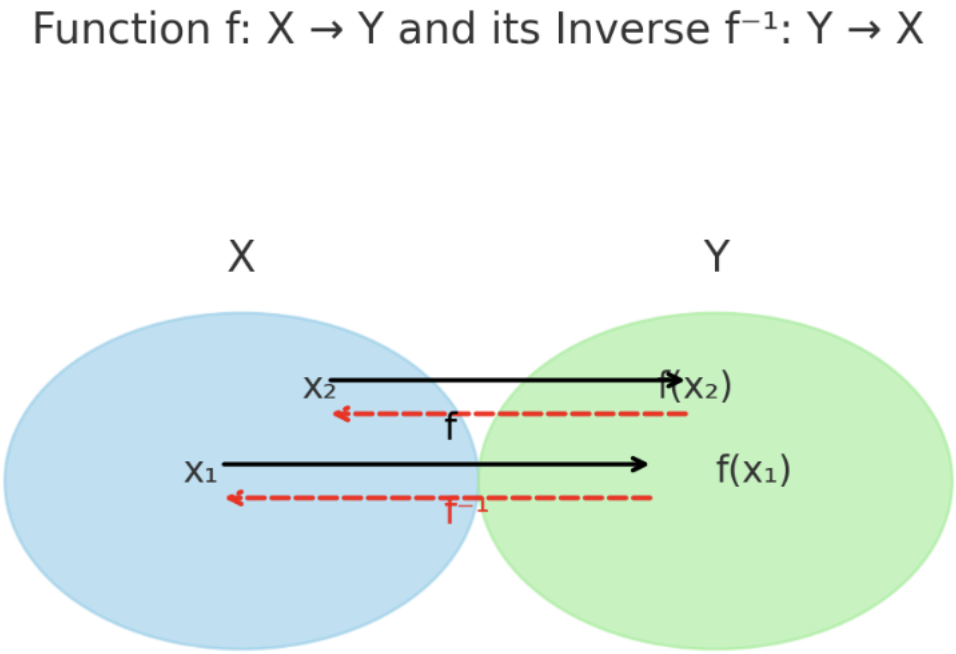
Definition: The identity function $id_X(x) = x$ acts like "do nothing", meaning if you compose it with any function, nothing changes

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

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.*

11 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 $f^{-1}(3) = 1$

11.1 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.

11.2 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]

12 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

12.1 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 $n \geq n_0$

13 Factorization

Definition: An integer a **divides** another integer b (denoted $a \mid b$) if there exists an integer q such that $b = qa$

In this case, a is called a **divisor** or **factor** of b.

If $a \mid (b + c)$, then $a \mid b$ and $a \mid c$ does not necessarily hold. However, the following is true: If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.

13.1 Primes and Composites

An integer $p > 1$ is **prime** if its only positive divisors are 1 and p itself. An integer greater than 1 that is not prime is called **composite**.

13.2 Strong Induction and Prime Factorization

13.2.1 Theorem (Existence):

Every integer $n > 1$ can be written as a product of one or more prime numbers.

Proof (by strong induction):

- **Base case:** $n = 2$. Since 2 is a prime, the statement holds.
- **Inductive hypothesis:** Assume for all integers m with $2 \leq m \leq k$, m can be written as a product of primes.
- **Inductive step:** Consider $n = k + 1$:
  - If $k + 1$ is prime, done.
  - If $k + 1$ is composite, then there exist integers a, b such that $k + 1 = ab$, with $1 < a \leq b < k + 1$.
  - By inductive hypothesis, both a and b have prime factorizations.
  - Multiplying these gives a prime factorization for $k + 1$.

Thus, by induction, every $n > 1$ has a prime factorization.

13.2.2 Theorem (Uniqueness):

The prime factorization of every positive integer greater than 1 is **unique up to ordering** of the factors.

Proof (outline by contradiction):

Suppose there exists a smallest integer $N > 1$ that has two distinct prime factorizations:

$$N = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

where p_i and q_j are primes and the two factorizations differ even after reordering.

- Since p_1 divides N, it must divide the product $q_1 q_2 \cdots q_s$.
- By primality, p_1 divides some q_j, implying $p_1 = q_j$.
- Cancel out the common prime $p_1 = q_j$:

$$\frac{N}{p_1} = p_2 \cdots p_r = q_1 \cdots q_{j-1} q_{j+1} \cdots q_s.$$

- But $\frac{N}{p_1} < N$, contradicting the minimality of N.
- Therefore, the prime factorization is unique up to order.

14 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 $0 \leq r < d$. This means that every integer division uniquely produces a quotient and a remainder.

Proof Highlights:

1. Existence:

- Consider $R = \{n - ad : a \in \mathbb{Z}, n - ad \geq 0\}$
- By the well-ordering principle, R has a smallest element r such that $r = n - qd$
- Show $r < d$:
  - If not, $r \geq d \Rightarrow r - d = n - (q + 1)d \geq 0$
  - But then $r - d < r$, contradicting minimality. So, $r < d$

2. Uniqueness

- If $n = qd + r = q'd + r'$ (with $0 \leq r, r' < d$)
- Subtract: $d(q - q') = r' - r$
- Since $-d < r' - r < d$ and $d|r' - r$, the only possibility is $r' - r = 0$, so $r = r'$ and $q = q'$

14.1 Greatest Common Divisor

Definition: For integers n, m, the $\gcd(n, m)$ is the largest positive integer dividing both.

Identities:

- $\gcd(am, bm) = m \gcd(a, b)$
- If $\gcd(a, c) = 1$ and $c|ab$, then $c|b$
- If p is prime and $p|ab$, then $p|a$ or $p|b$
- If p is prime and $p \nmid m$, then $\gcd(p, m) = 1$

14.2 Bezout's identity and proof

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

This identity shows that the greatest common divisor of two integers can be expressed as a linear combination of those integers.

Proof Sketch:

- 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. By the well ordering principle, W has a smallest element d
- $d|n$ and $d|m$, so d is a common divisor
- Any common divisor of n, m divides d, so $d = \gcd(n, m)$

14.3 Large power remainders

How to find the remainder of $a^{bcd} \pmod{x}$?

Example: Compute $3^{100} \pmod{7}$

Write in binary: $100_{10} = 1100100_2$, therefore $3^{100} = 3^{64} \cdot 3^{32} \cdot 3^4$

15 The Euclidean Algorithm

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

By the lemma: If $n = qm + r$ for any integers then $gcd(n, m) = gcd(m, r)$. Repeatedly, 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 $gcd(100, 28)$

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

The gcd is the last non-zero remainder, which is 4

Now, find a, b such that $an + bm = gcd(100, 28)$, i.e. express 4 as a linear combination of 100 and 28.

$$4 = 16 - 1 \cdot (28 - 1 \cdot 16) \Rightarrow 4 = 2 \cdot (100 - 3 \cdot 28) - 1 \cdot 28 = 2 \cdot 100 - 7 \cdot 28$$

16 Modular Arithmetic

Modular arithmetic deals with the integers under equivalence classes defined by division with remainder.

16.1 Congruence Classes

Two integers a and b are congruent modulo n if $n|(a-b)$, written as:

$$a \equiv b \pmod{n}$$

This relation is an equivalence relation on integers, partitioning $\mathbb{Z}$ into sets of integers called congruence classes.

The set of all such classes modulo n is denoted $\mathbb{Z}_n$:

$$\mathbb{Z}_n = \{[0], \cdots, [n-1]\}$$

Each congruence class $[a]$ is the set:

$$[a] = \{b \in \mathbb{Z} : b \equiv a \pmod{n}\} = \{a + qn : q \in \mathbb{Z}\}$$

Intuitively, two integers are in the same class if they leave the same remainder upon division 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 $[1] = \{4q + 1 : q \in \mathbb{Z}\}$

Definition: The inverse of $x \pmod{y}$ is denoted by:

$$x \cdot x^{-1} \equiv 1 \pmod{y}$$

Note that this inverse exists only if x and y are relatively prime (i.e., $\gcd(x, y) = 1$)

Example: Find the inverse of $7 \pmod{11}$

Firstly, find that $\gcd(7, 11) = 1$, and $1 = 2 \cdot 11 - 3 \cdot 7$

Taking $\pmod{11}$: $1 = 7 \cdot (-3) \equiv 7 \cdot 8 \equiv 1 \pmod{11}$

Therefore, $7^{-1} \equiv 8 \pmod{11}$

16.2 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.

17 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.

17.1 Rings

Definition: A **ring** is a triple $(R, +, \cdot)$ of a set R which satisfy the following properties for all $a, b, c \in R$

1. $(a + b) + c = a + (b + c)$ (associativity of $+$)
2. $\exists 0 \in R$ with $0 + a = a$ (additive identity)
3. $a + b = b + a$ (commutativity of $+$)
4. for each $a \in R$, $\exists b \in R$ with $a + b = 0$ (additive inverse)
5. $a(bc) = (ab)c$ (associativity of $\cdot$)
6. $\exists 1 \in R$ with $1a = a = a1$ (multiplicative identity)
7. $a(b + c) = (ab + ac)$ and $(b + c)a = ba + ca$ (distributivity)

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

17.2 Fields

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

- F is a commutative ring under $+$ and $\cdot$
- 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.

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 $[a]^m = [1]$

18 Fermat's little theorem and Euler's theorem

These theorems describe important properties of powers of units (invertible elements) in modular arithmetic, showing that raising an element to a certain power brings you back to the identity element.

18.1 Units and Zero Divisors

Unit: An element $a \in R$ is called a unit if it has a multiplicative inverse, that is $\exists b \in R$ such that

$$a \cdot b = 1$$

In this case, we say a is invertible.

Zero Divisor: A zero divisor is a nonzero element $a \in R$ such that there exists a nonzero $b \in R$ such that

$$a \cdot b = 0$$

Zero divisors essentially "kill" other nonzero elements when multiplied, which is the *opposite behaviour of units.*

In a field, every nonzero element is a unit, and there are no zero divisors.

Example: in $\mathbb{Z}_6$, check if [3] is a unit, i.e. 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 $gcd(3, 6) = 3 \neq 1$.

So [3] is not a unit in $\mathbb{Z}_6$. Intuitively, if a and n share a common factor greater than 1, then a "collapses" some nonzero numbers to zero (making it a zero divisor), so it can't have an inverse

18.1.1 Cyclic property of units

If $[a]$ is a unit in $\mathbb{Z}_n$ (meaning $\gcd(a, n) = 1$ so it has a multiplicative inverse), then the sequence:

$$[a], [a]^2, [a]^3, \ldots$$

must eventually repeat because $\mathbb{Z}_n$ has a finite number of elements.

This says that powers of must "loop".

18.2 Fermat's little theorem

Statement: If p is prime and a is not divisible by p (i.e. $\gcd(a, p) = 1$), 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

18.3 Euler's theorem

Euler's totient function: $\phi(n)$ is the count of integers up to n that are relatively prime with n. Alternatively, $\phi(n)$ is the number of units in $\mathbb{Z}_n$, therefore $\phi(n) = |\mathbb{Z}_n^\times|$, i.e. $\phi(n) = |\{b \in \mathbb{Z} : 1 \leq b \leq n \text{ and } \gcd(b, n) = 1\}|$

Statement: Let n be a positive integer and $\phi(n)$ denote Euler's totient function, for any integer a with $\gcd(a, n) = 1$:

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

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 $\phi(p) = p - 1$)

19 RSA Cryptography

RSA is a type of public-key encryption used to securely send information over the internet

It uses two keys:

- public key (used by everyone to encrypt a message to you)
- private key (used only by you to decrypt the message)

19.1 Math

1. Pick two large prime numbers p and q
2. Multiply them: $n = p \times q$, where n is part of the public key
3. Calculate Euler's totient: $\phi(n) = (p-1) \times (q-1)$
4. Choose a public key exponent, pick integer e s.t. $1 < e < \phi(n)$ and e is relatively prime to $\phi(n)$
5. Find the private key exponent, find d s.t. $d \times e \equiv 1 \pmod{\phi(n)}$
6. Keys are:

- public key: (n, e)
- private key: (n, d)

19.2 Implementation

19.2.1 Encryption

Suppose someone wants to send you the number M (the message; must be less than n)

The encrypted message $C = M^e \pmod{n}$

For example: $C = 42^3 \pmod{55} = 13$

19.2.2 Decryption

You receive $C = 13$

$M = C^d \pmod{n}$, you'd get back the original 42 by $M = 13^{27} \pmod{55}$

To break RSA, you'd need to factor n into p and q, which is very hard and computationally heavy if the primes have hundreds of digits

Explanation:

n is known. We need d, which is the other part of the private key.

To find d, you need $\phi(n)$ by $d \equiv e^{-1} \pmod{\phi(n)}$

But $\phi(n) = (p-1)(q-1)$, so you need to find p and q with only n

So, if you can factor n into p and q, you eventually get d, which breaks RSA

However, breaking n into p and q is very challenging and factoring is hard for large primes.

20 Group Theory

Definition: A non-empty set G along with a binary operation is called a **group** $(G, \cdot)$ if it satisfies the following properties:

20.1 Properties and attributes of groups

- Associativity: $a \cdot (b \cdot c) = (a \cdot b) \cdot c, \quad \forall a, b, c \in G$
- Identity: $\exists e \in G$ such that $a \cdot e = a = e \cdot a$ 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 $g \cdot g^{-1} = g^{-1} \cdot g = e$

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

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

Definition: A group G is **abelian** (or **commutative**) if $a \cdot b = b \cdot a$ 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 $|G|$

20.2 Cayley Table

The multiplication table of a group is called its **Cayley table**, where every row (and every column) in the Cayley table for a group G contains every element of G

Example: Consider the group of integers $\pmod 3$ addition modulo 3: $\mathbb{Z}_3 = \{0, 1, 2\}$, and the operation is $a +_3 b = (a + b) \pmod 3$

$$\begin{bmatrix} +_3 & 0 & 1 & 2 \\ -- & -- & -- & -- \\ 0 & 0 & 1 & 2 \\ 1 & 1 & 2 & 0 \\ 2 & 2 & 0 & 1 \end{bmatrix}$$

Notice how every row and column includes $0, 1$, and 2, because $2 +_3 1 = (2+1) \pmod 3 = 3 \pmod 3 \equiv 0$ $2 +_3 2 = (2 + 2) \pmod 3 = 4 \pmod 3 \equiv 1$

20.3 Cyclic Groups

A **cyclic group** is a group that can be generated by a single element, meaning there exists an element g in the group G such that every element of G can be written as a power of g:

$G = \langle g \rangle = \{g^n : n \in \mathbb{Z}\}$

Definition: Let $a \in G$. The **order** of a is the least positive integer n with $a^n = e$, and write $|a| = n$. If, $\forall n \geq 1$, $a^n \neq e$, then a has **infinite order**

Further: $ord(a) = \frac{n}{\gcd(a,n)}$

Contrarily, every element in a finite group has a finite order if $a^n = e, n \geq 1$

Definition: Let $C_n = \{e = a^0, a, a^2, \ldots, a^{n-1}\}$ be an n-element set and define $a^i \cdot a^j = a^k$ where $0 \leq k \leq n$ is the remainder of $i + j$ after division by n. The set C_n along with this operation is called a **cyclic group** of order n. The element a is called the **generator** of C_n and has order n

Note that C_n is nothing more than $\mathbb{Z}_n$ written multiplicatively. Each $[i] \in \mathbb{Z}_n$ with $0 \leq i < n$ corresponds to $a^i \in C_n$

20.4 Subgroups

21 Subgroups

Definition: A **subgroup** generated by an element a is: $\langle a \rangle = \{ka \pmod{12} | k \in \mathbb{Z}\}$

Example: In $\mathbb{Z}_{12}$, 5 generates what subgroup?

In the additive group $\mathbb{Z}_{12}$, the elements are: $\{0, 1, 2, \ldots, 11\}$. Computing $5k \pmod{12}$ for $k = 0, 1, 2, \ldots$ until it repeats 0:

We find that the subgroup $\langle 5 \rangle = \{0, 5, 12, 3, 8, 1, 6, 11, 4, 9, 2, 7\}$ Since $\langle 5 \rangle$ contains every element, it means 5 is a generator of the entire group

$\therefore \langle 5 \rangle = \mathbb{Z}_{12}$, and the order of 5 (the number of distinct elements it generates) is 12

21.1 Subgroup conditions

A non-empty subset $H \subseteq G$ is a subgroup of G if and only if:

1. the identity $e \in G$ is also in H
2. for all $a, b \in H, a \cdot b \in H$
3. for all $a \in H, a^{-1} \in H$

By these conditions, a non-empty subset $H \subseteq G$ is a subgroup of G if and only if $ab^{-1} \in H$ for all $a, b \in H$

21.2 Subgroup types

If G is a group with identity e then both $\{e\}$ and G are sub-groups of G

We call $\{e\}$ the **trivial subgroup** of G

A **proper subgroup** of G is any subgroup $H \leq G$ with $H \neq G$. When H is a proper subgroup of G, we write $H < G$

Example: By the Cayley table of $\mathbb{Z}_{10}^* = \{[1], [3], [7], [9]\}$, we can find that the set $H = \{[1], [9]\}$ is a subgroup of $\mathbb{Z}_{10}^*$

·	[1]	[3]	[7]	[9]
[1]	[1]	[3]	[7]	[9]
[3]	[3]	[9]	[1]	[7]
[7]	[7]	[1]	[9]	[3]
[9]	[9]	[7]	[3]	[1]

·	[1]	[9]
[1]	[1]	[9]
[9]	[9]	[1]

Example: Let $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$. The set $n\mathbb{Z}$ is an **additive subgroup** of $\mathbb{Z}$ (i.e. a subgroup of $(\mathbb{Z}, +)$)

Proof: Check all conditions of a subgroup, i.e. that $n\mathbb{Z}$ contains the identity of $\mathbb{Z}$, is closed under addition, and taking inverses

$0 \in n\mathbb{Z}$ is the identity

If $m \in n\mathbb{Z}$ and $l \in n\mathbb{Z}$, then $m = na$ and $l = nb$ for some $a, b \in \mathbb{Z}$, therefore $m + n = na + nb = n(a + b) \in n\mathbb{Z}, \therefore n\mathbb{Z}$ is closed under addition

Finally, if $m \in n\mathbb{Z}$, then $m = nk$ for some $k \in \mathbb{Z}$, therefore $-m = n(-k)$ and hence $-m \in n\mathbb{Z}$. Thus, the inverse of an element in $n\mathbb{Z}$ is also in $n\mathbb{Z}$

21.3 Normal Subgroups

Definition: Let G be a group and let $H \leq G$ and $g \in G$, the **conjugation** of H by g is the set:

$$gHg^{-1} = \{ghg^{-1} : h \in H\}$$

Conjugation means "viewing an element through the lens of another element's symmetry". When you conjugate H by g, we ask "what does H look like if I move the system by g, apply H, then move back by g^{-1}"?

Proof Sketch: Let $H \leq G$ and fix $g \in G$. Consider $gHg^{-1} = \{ghg^{-1} : h \in H\}$. Prove its a subgroup of G

1. Nonempty: $e \in H$ so $geg^{-1} = e \in gHg^{-1}$
2. Closure under inverses: If $x = ghg^{-1} \in gHg^{-1}$, then $x^{-1} = gh^{-1}g^{-1}$

Definition: A subgroup $H \leq G$ is **normal** if $gHg^{-1} = H \forall g \in G$. We write $H \trianglelefteq G$ when H is a normal subgroup of G.

21.4 Center of a group

The center of a group G, denoted $Z(G)$, is the set of all elements in G that commute to every element of G, denoted by:

$$Z(G) = \{a \in G : ag = ga \text{ for all } g \in G\}$$

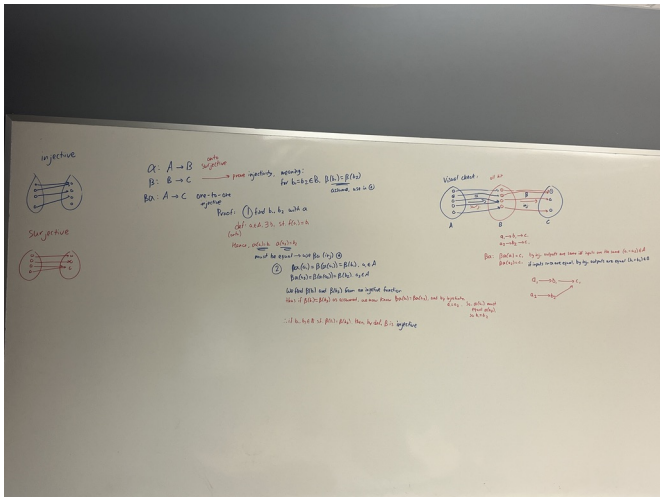
Intuitively, the center consists of elements that are "invisible" under multiplication, they don't change the order of multiplication with any other element.

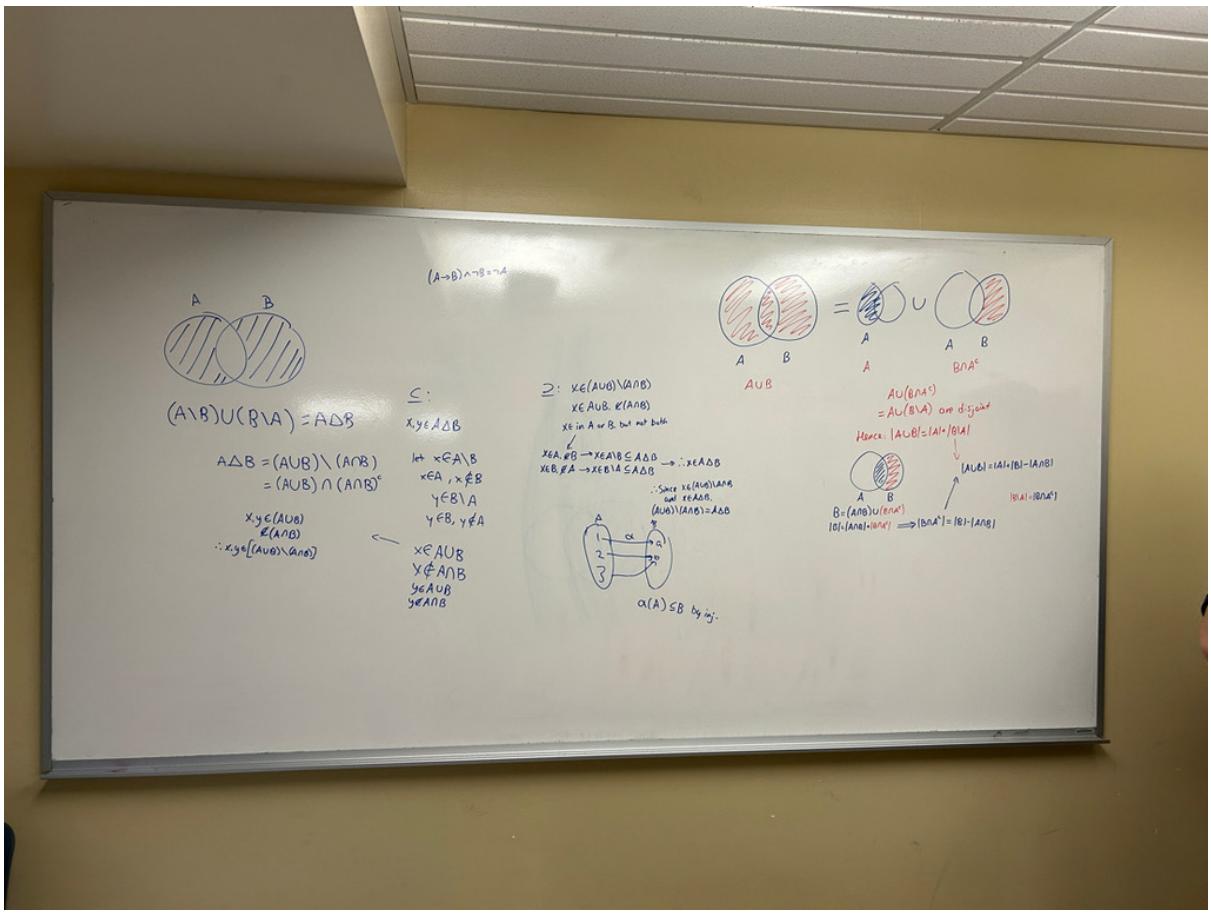
Example: the identity element $e \in G$ satisfies this automatically, by:

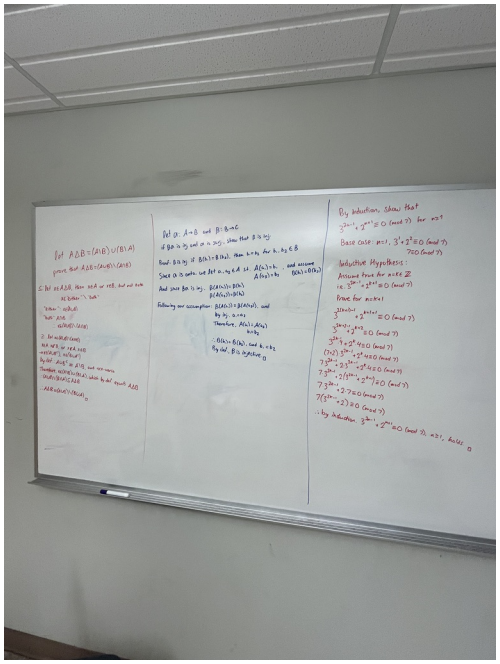
$$eg = ge = g, \quad \therefore e \in Z(G)$$

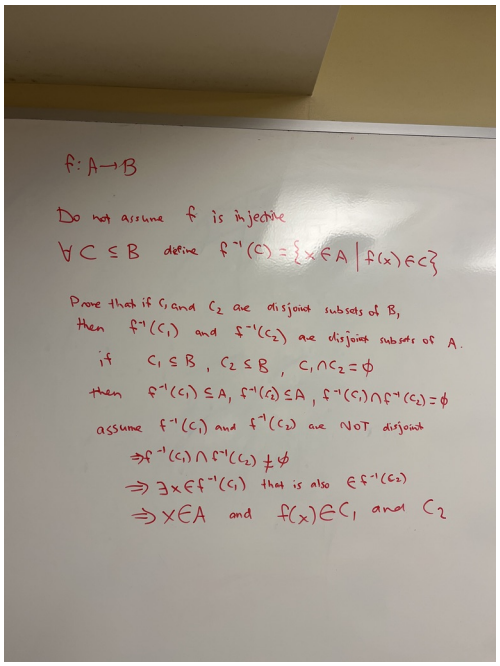
Remark: If G is abelian, then $Z(G) = G$ (every element commutes with every other)

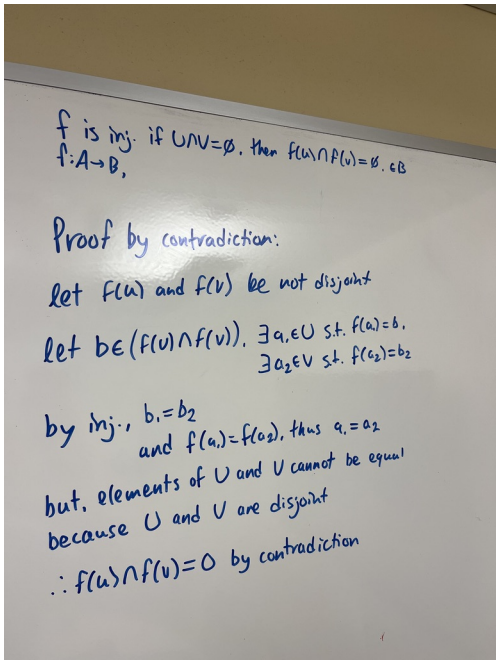
22 Midterm 1 Whiteboard Proofs

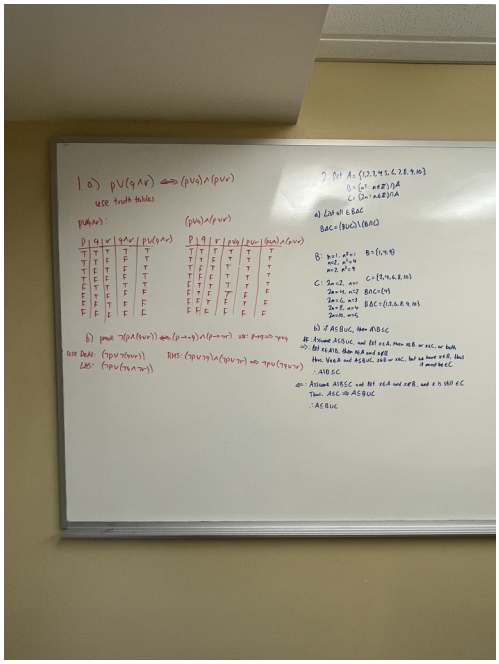


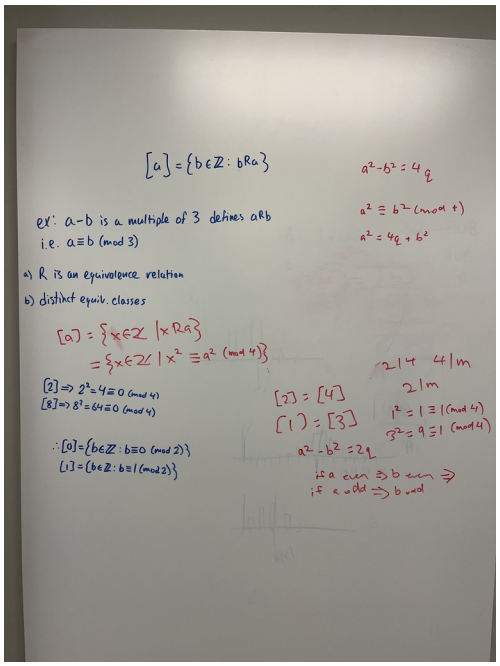


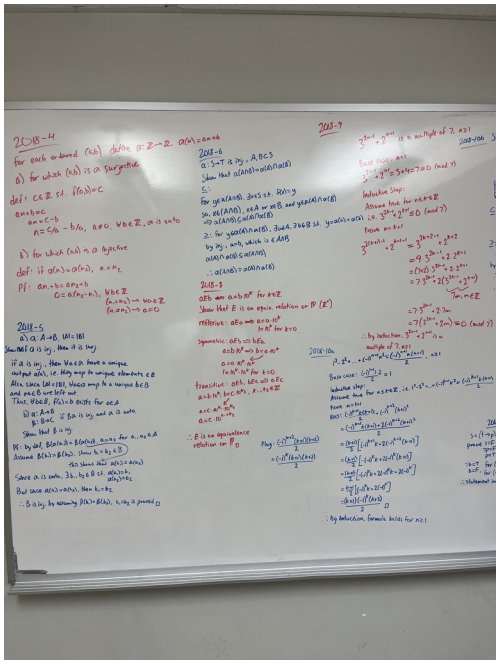


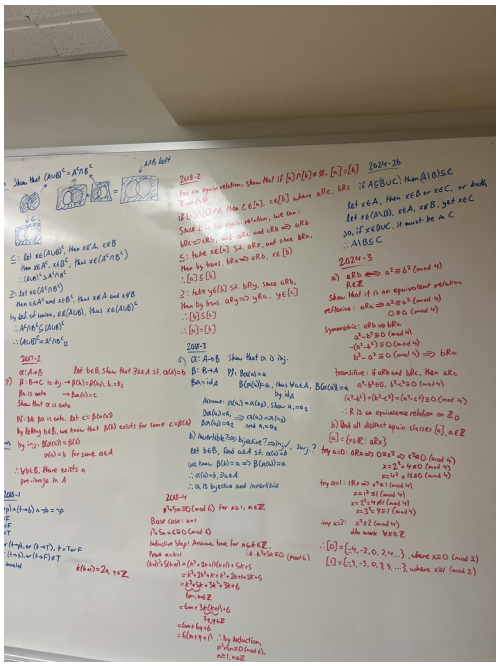

f: A → B
Do not assume f is injective
∀ C ⊆ B define f⁻¹(C) = {x ∈ A | f(x) ∈ C}
Prove that if C1 and C2 are disjoint subsets of B,
then f⁻¹(C1) and f⁻¹(C2) are disjoint subsets of A.
if C1 ⊆ B, C2 ⊆ B, C1 ∩ C2 = ∅
then f⁻¹(C1) ⊆ A, f⁻¹(C2) ⊆ A, f⁻¹(C1) ∩ f⁻¹(C2) = ∅
assume f⁻¹(C1) and f⁻¹(C2) are NOT disjoint
⇒ f⁻¹(C1) ∩ f⁻¹(C2) ≠ ∅
⇒ ∃x ∈ f⁻¹(C1) that is also ∈ f⁻¹(C2)
⇒ x ∈ A and f(x) ∈ C1 and C2


f is inj. if U∩V=∅, then f(U)∩f(V)=∅. 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)=b,
∃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)=∅ by contradiction




[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]
[1]=[3]
a²-b²=2q
if a even ⇒ b even ⇒
if a odd ⇒ b odd
2|4 4|m
2|m
1²=1≡1 (mod 4)
3²=9≡1 (mod 4)





23 Cheat Sheet

23.1 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: $\neg(p \wedge q) \equiv (\neg p \vee \neg q)$, $\neg(p \vee q) \equiv (\neg p \wedge \neg q)$
  - Law of Excluded Middle: $p \vee \neg p = T$

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 $\neg Q \to \neg P$

23.2 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 $\Leftrightarrow$:$\Rightarrow \wedge \Leftarrow$ and =: $\subset \wedge \supset$
- 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.

23.3 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:**
  $|A \cup B| = |A| + |B| - |A \cap B|$
- $|B \setminus A| = |B \cap A^C|$

23.4 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 ($\forall x, y : x \leq y \vee y \leq x$).

23.5 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 $a \equiv b \pmod 2$

23.6 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 $(BA)(a) = a$

23.7 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 $f : X \to Y$

23.8 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

23.9 Factorization

- **Definition:** Express an integer $n > 1$ as a product of primes: $n = p_1 p_2 \cdots p_k$. The factorization is unique up to ordering.
- **Trial Division:** Test divisibility by primes $2, 3, 5, \ldots$ up to $\sqrt{n}$.
- **Fermat's Method:** Write odd n as $a^2 - b^2 = (a-b)(a+b)$. Try $a = \lceil \sqrt{n} \rceil$ upwards, check if $a^2 - n$ is a perfect square.

23.10 Division Algorithm

- For integers n, d with $d > 0$, there exist unique q, r such that:

$$n = qd + r, \quad 0 \leq r < d$$

- q is the quotient, r the remainder when dividing n by d.

- Property: if d divides m, n, then d divides $xm + yn$

23.11 Euclidean Algorithm

- Efficient method for computing $\gcd(a, b)$.
- Recursive step:

$$\gcd(a, b) = \gcd(b, a \bmod b)$$

- Terminates when remainder becomes 0; last nonzero remainder is gcd. - Can be extended to find integers x, y such that

$$ax + by = \gcd(a, b)$$

(known as Bézout's identity).

Properties:

- m and n are relatively prime iff $\exists x, y \in \mathbb{Z}$ such that $xm + yn = 1$

23.12 Modular Arithmetic

- Two integers a, b are congruent modulo n if $n \mid (a - b)$:

$$a \equiv b \pmod{n}$$

- Basic operations respect modular equivalence:

$$(a + b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$$

$$(a \times b) \bmod n = ((a \bmod n) \times (b \bmod n)) \bmod n$$

- Modular inverses exist for a with $\gcd(a, n) = 1$, i.e., there is a^{-1} such that:

$$aa^{-1} \equiv 1 \pmod{n}$$

23.13 Operations in $\mathbb{Z}_n$

- Addition: $[a] + [b] = [a + b]$
- Multiplication: $[a] \cdot [b] = [a \cdot b]$
- Subtraction: $[a] - [b] = [a - b]$

Properties: For all $[a], [b], [c] \in \mathbb{Z}_n$

- Commutativity: $[a] + [b] = [b] + [a]$ and $[a][b] = [b][a]$
- Associativity: $([a] + [b]) + [c] = [a] + ([b] + [c])$
- Identity: $[a] + [0] = [a]$ and $[a] \cdot [1] = [a]$
- Additive inverse: $[a] + [-a] = [0]$
- Distributivity: $[a]([b] + [c]) = [a][b] + [a][c]$

23.14 Units and Zero Divisors

Multiplicative Inverse (Unit): $[b]$ is the multiplicative inverse of $[a]$ iff $[a][b] = [1]$

Zero Divisor: $[a] \neq [0]$ is a zero divisor if $\exists [b] \neq [0]$ s.t. $[a][b] = [0]$

Invertibility Theorem: $[a]$ is a unit in $\mathbb{Z}_n$ iff $\gcd(a, n) = 1$

23.15 Groups, Rings, and Fields

- **Group:** Set G with a binary operation such that:
  - *Closure*: $a, b \in G \Rightarrow a * b \in G$
  - *Associativity*: $(a * b) * c = a * (b * c)$
  - *Identity*: $\exists e \in G, a * e = e * a = a$
  - *Inverse*: $\forall a, \exists a^{-1} : a * a^{-1} = a^{-1} * a = e$
  - *Abelian (commutative)*: $a * b = b * a \; \forall a, b$
  - *Order*: Number of elements
  - *Finite Group:* If $(G, *)$ is finite and $a \in G$, then $\exists n \geq 1$ s.t. $a^n = e$
- **Ring:** Set R with two operations $(+, *)$ such that:
  - $(R, +)$ is an abelian group
  - $(R, *)$ is associative; distributive over $(+)$
  - *Commutative*: $a * b = b * a$
  - *Multiplicative identity*: Sometimes required $(1 \in R : a * 1 = a)$

- **Field:** Commutative ring F with multiplicative inverses for all nonzero elements:
  - *No zero divisors*
  - $\forall f \neq 0, \exists f^{-1} : f * f^{-1} = 1$
- **Units and Zero Divisors:**
  - Unit: element with inverse
  - Zero-divisor: nonzero element $a : \exists b \neq 0, ab = 0$, never in a field

Properties:

- $(ab)^{-1} = b^{-1}a^{-1}$
- Identity is unique
- Every element has a unique inverse
- $a \cdot b = a \cdot c \Rightarrow b = c$
- $b \cdot a = c \cdot a \Rightarrow b = c$

23.16 Fermat's Little Theorem and Euler's Theorem

- **Fermat's Little Theorem:** If p is prime and $a \not\equiv 0 \pmod{p}$, then $a^{p-1} \equiv 1 \pmod{p}$
  - Fast test for modulo powers, can simplify large exponent calculations
- **Euler's Theorem:** If $\gcd(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$ where $\varphi(n)$ is Euler's totient.
  - Fermat is a special case where $n = p$ prime, so $\varphi(p) = p - 1$

23.17 RSA Cryptography (Number-Theoretic Summary)

- **Setup:**
  - Choose primes p, q; set $n = p \times q$
  - Find $\varphi(n) = (p - 1)(q - 1)$
  - Pick public exponent e coprime to $\varphi(n)$
  - Compute d such that $de \equiv 1 \pmod{\varphi(n)}$
- **Encryption:** $C = M^e \bmod n$
- **Decryption:** $M = C^d \bmod n$
  - Security relies on hardness of factoring n

23.18 Cyclic Groups and Cayley Tables

- **Cyclic Group:** Generated by a single element g: every element is g^k for some integer k
  - "Order" of the group is number of elements, order of element is the smallest $n : g^n = e$
  - In $\mathbb{Z}_n$ (integers mod n), every element may not be a generator unless n is prime
- **Cayley Table:** Group multiplication/addition table: each row and column contains every group element exactly once

23.19 Lagrange's Theorem and Subgroups

- **Lagrange's Theorem:** In finite group G, the order of any subgroup H divides the order of G

- **Subgroup conditions:**
  - Identity is in H
  - Closed under operation and inverses
  - H nonempty, and for all $a, b \in H$, $ab^{-1} \in H$