alex-levesque.com

MTHE 217 - Lecture Notes

Algebraic Structures with Applications

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

Contents

1 Propositional Logic **4**
1.1 Connectives . . . 4
1.2 Proof with multiple premises . . . 5
1.3 Methods of proof . . . 5
1.4 Important Tricks and Definitions . . . 5

2 Set Theory **7**
2.1 Quantifiers and definitions . . . 7
2.2 Sets . . . 7
2.3 Finite and Disjoint Sets . . . 7

3 Equivalence Relations **9**
3.1 Cartesian Product . . . 9
3.2 Binary Relation . . . 9
3.3 Equivalence Relations . . . 9

4 Equivalence Classes **11**
4.1 Congruence is an equivalence relation proof . . . 11
4.2 Equivalence class and congruence class . . . 11
4.3 Partition . . . 11

5 Functions and their properties **13**
5.1 Images . . . 13
5.2 Injective, Surjective, Bijective . . . 13
5.3 Composition, identity, and inverse . . . 13

6 Inverse of a Function **14**
6.1 Bijection-Invertibility Equivalence . . . 14
6.2 Cardinality . . . 15

7 Mathematical Induction **16**
7.1 Proof by Induction . . . 16

8 Factorization **17**
8.1 Primes and Composites . . . 17
8.2 Strong Induction and Prime Factorization . . . 17

8.2.1 Theorem (Existence): . . . 17
8.2.2 Theorem (Uniqueness): . . . 17

9 Division Algorithm **19**
9.1 Greatest Common Divisor . . . 19
9.2 Bezout's identity and proof . . . 19
9.3 Large power remainders . . . 19

10 The Euclidean Algorithm **21**

11 Modular Arithmetic **22**
11.1 Congruence Classes . . . 22
11.2 Operations in $\mathbb{Z}_n$ . . . 22

12 Rings and Fields **24**
12.1 Rings . . . 24
12.2 Fields . . . 24

13 Fermat's little theorem and Euler's theorem **25**
13.1 Units and Zero Divisors . . . 25
13.1.1 Cyclic property of units . . . 25
13.2 Fermat's little theorem . . . 26
13.3 Euler's theorem . . . 26

14 RSA Cryptography **27**
14.1 Math . . . 27
14.2 Implementation . . . 27
14.2.1 Encryption . . . 27
14.2.2 Decryption . . . 28

15 Group Theory **29**
15.1 Properties and attributes of groups . . . 29
15.2 Cayley Table . . . 29

16 Subgroups **30**
16.1 Subgroup conditions . . . 30
16.2 Subgroup types . . . 30
16.3 Center of a group . . . 31
16.4 Cyclic Groups . . . 31

17 Cosets and Lagrange's Theorem **33**
17.1 Right and Left Coset . . . 33
17.2 Lagrange's Theorem . . . 33
17.3 Proof of Euler's and Fermat's Theorems . . . 33

18 Group Quotients **35**
18.1 Normal Subgroups . . . 35
18.2 Quotient Group . . . 35

19 Group Homomorphisms and Isomorphisms **37**

20 Morphism Theorems and Lemmas **39**

21 Coding Theory **41**
21.1 Words And Their Measurements 41
21.2 Nearest Neighbour Decoding 42
21.3 Encoding and Decoding Group Codes 44
21.4 Matrix Method to En/Decode Group Codes 45
21.5 Syndrome Decoding 46

22 Midterm 1 Whiteboard Proofs **49**

23 Cheat Sheet **53**
23.1 Propositional Logic 53
23.2 Proof Techniques 53
23.3 Set Theory 54
23.4 Relations 54
23.5 Equivalence Classes 54
23.6 Functions 55
23.7 Inverses & Cardinality 55
23.8 Induction Principle 55
23.9 Factorization 56
23.10 Division Algorithm 56
23.11 Euclidean Algorithm 56
23.12 Modular Arithmetic 57
23.13 Operations in $\mathbb{Z}_n$ 57
23.14 Units and Zero Divisors 57
23.15 Groups, Rings, and Fields 57
23.16 Fermat's Little Theorem and Euler's Theorem 58
23.17 RSA Cryptography (Number-Theoretic Summary) 58
23.18 Cyclic Groups and Cayley Tables 59
23.19 Lagrange's Theorem and Subgroups 59

1 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

1.1 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

p	q	p→q
T	T	T
T	F	F
F	T	T
F	F	T

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 $\neg q \rightarrow \neg p$

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

1.2 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:

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

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

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

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

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

1.3 Methods of proof

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

1.4 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* $P \leftrightarrow Q \equiv (P \rightarrow Q) \wedge (Q \rightarrow P)$

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: $(P \rightarrow Q), P \therefore Q$, 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: $(P \rightarrow Q), \neg Q \therefore \neg P$, 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.

2 Set Theory

2.1 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: $P_A(x) =$

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

2.2 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

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

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

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

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

Theorem: If sets X, Y and Z are not disjoint, then: $|X \cup Y| = |X| + |Y| - |X \cap Y|$

3 Equivalence Relations

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

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

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

3.3 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

4 Equivalence Classes

4.1 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

4.2 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

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

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

5.1 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.

5.2 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

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

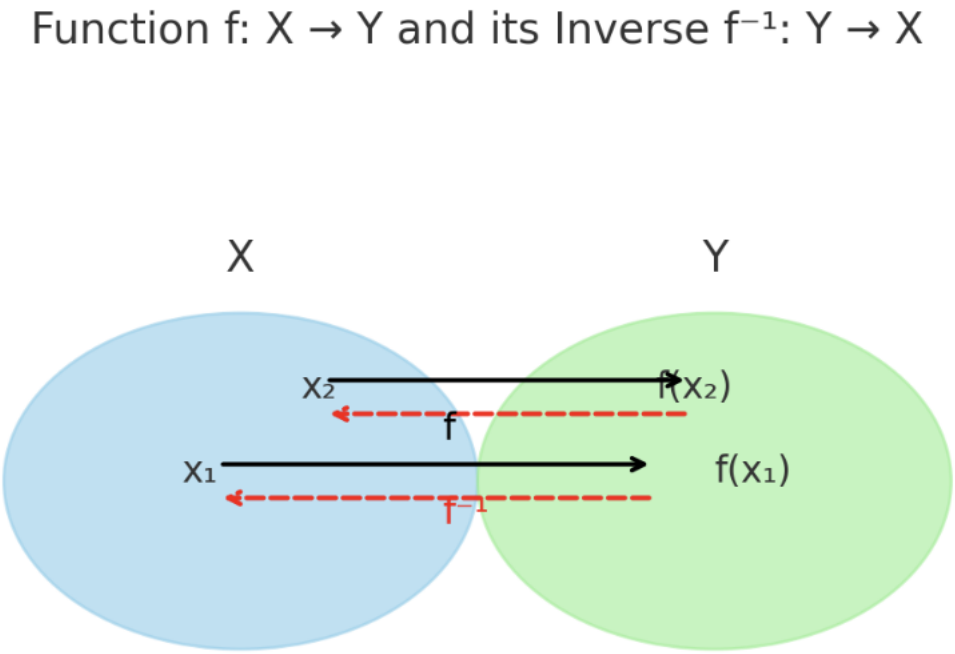
Definition: The identity function $id_X(x) = x$ acts like "do nothing", meaning if you compose it with any function, nothing changes

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

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.*

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

6.1 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.

6.2 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]

7 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

7.1 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 $n \geq n_0$

8 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 $a \mid (b + c)$.

8.1 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**.

8.2 Strong Induction and Prime Factorization

8.2.1 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.

8.2.2 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.

9 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 $q = q'$

9.1 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 $\gcd(p, m) = 1$

9.2 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 $d = \gcd(n, m)$

9.3 Large power remainders

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

Example: Compute $3^{100} \pmod{7}$. Note that $\gcd(7, 100) = 1$

Therefore, in $\mathbb{Z}_7$: $[3^{100}] = [3^{6\times 31}][3^4] = [3^4] = [81] = [4]$

10 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.

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

11 Modular Arithmetic

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

11.1 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, $7^{-1} \equiv 8 \pmod{11}$

11.2 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.

12 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.

12.1 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: $a \cdot b = b \cdot a \quad \forall a, b \in R$

12.2 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 $[a]^m = [1]$

13 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.

13.1 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

13.1.1 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".

13.2 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

13.3 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. $\phi(n) = |\{b \in \mathbb{Z} : 1 \leq b \leq n \text{ and } \gcd(b, n) = 1\}|$

The formula takes various forms:

1. $\phi(p^k) = p^k \left(1 - \frac{1}{p}\right)$. Ex: $\phi(100) = 100 \times \left(1 - \frac{1}{2}\right) \times (1 - \frac{1}{5}) = 40$
2. If m, n are coprime, $\phi(mn) = \phi(m)\phi(n)$. Recall that for prime p: $\phi(p) = p - 1$ Ex: $\phi(15) = \phi(3)\phi(5) = (3 - 1)(5 - 1) = 8$

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

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

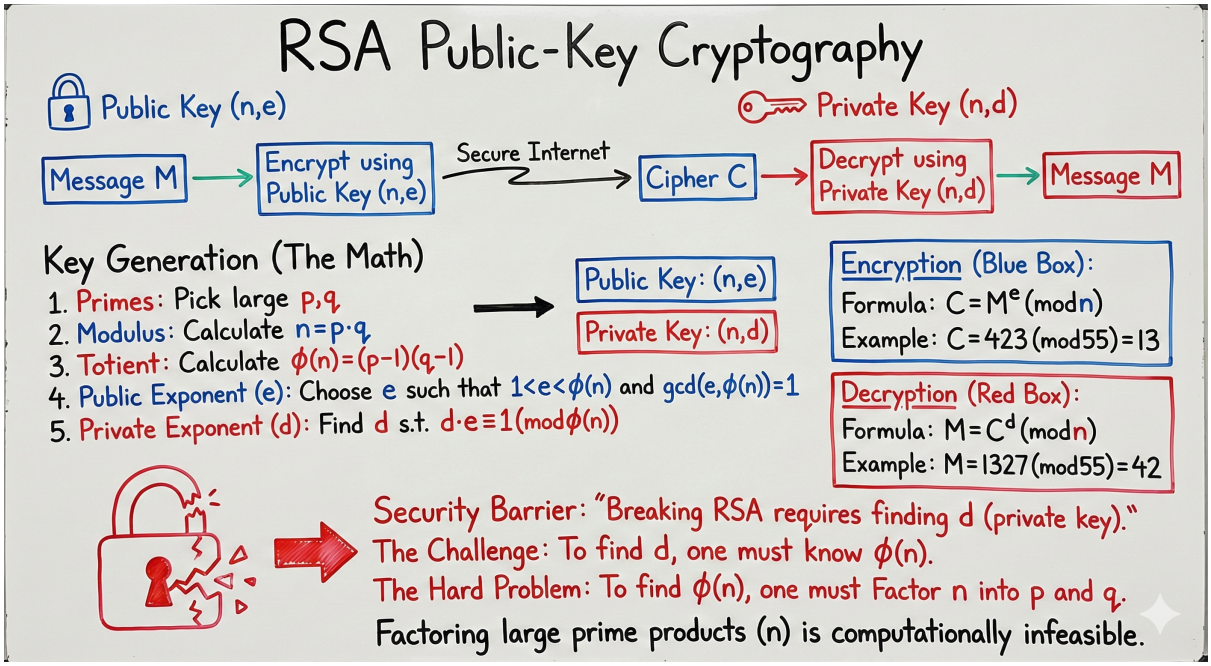
In words: if you have a positive integer n and any integer a that is relatively prime to n, then raising a to the power of $\phi(n)$ (the number of integers less than n that are relatively prime to n) will give a remainder of 1 when divided by n

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

Example: Compute the last two digits of 3^{2026}. When we find the last two digits, this is means $\pmod{100}$. Factor n into $2^2 \cdot 5^2$. Find that $\gcd(3, 100) = 1$ meaning we can use Euler's Theorem. $\phi(n) = \phi(2^2)\phi(5^2) = (4 - 2)(25 - 5) = 40 \Rightarrow 3^{40} \equiv 1 \pmod{100}$. $3^{2026} = 3^{26} \pmod{100} \Rightarrow 3^{16}3^8 3^2 = 21 \cdot 61 \cdot 9 \pmod{100} = 29$

Example: Compute the last digit of 7^{2025}, i.e. $7^{2025} \pmod{10}$. $\gcd(7, 10) = 1$, and $\phi(n) = 4$. Then, $7^{2025} = 7^{4 \cdot 506}7^1 = 7$

14 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)

14.1 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)

14.2 Implementation

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

14.2.2 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.

The mass $M_{k_i} \in \mathbb{R}$ of Voronoi region R_{k_i} is given by:

$$M_{k_i} = \int_{R_{k_i}} D(x, y)\, dA$$

$$C_{k_i} = \frac{1}{M_{k_i}} \left(\int_{R_{k_i}} x \cdot D(x, y)\, dA, \int_{R_{k_i}} y \cdot D(x, y)\, dA \right)$$

15 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:

15.1 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 $|G|$

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

Lemma: Let G be a group and a be an element in G such that $|a| = n$. For all integers k:

- $a^k = e$ if and only $n|k$
- $a^k = a^m$ if and only if $k \equiv m \pmod{n}$

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

15.2 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 $a +_3 b = (a + b) \pmod 3$

$$\left[\begin{array}{cccc} +_3 & 0 & 1 & 2 \\ -- & -- & -- & -- \\ 0 & 0 & 1 & 2 \\ 1 & 1 & 2 & 0 \\ 2 & 2 & 0 & 1 \end{array}\right]$$

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

16 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

16.1 Subgroup conditions

There are two main ways to prove that a subset H of a group G is a subgroup:

Proof by definition: 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 (i.e., H has the same identity as G)
2. for all $a, b \in H, a \cdot b \in H$
3. for all $a \in H, a^{-1} \in H$

Subgroup test:

- A nonempty subset $H \subseteq G$ is a subgroup if and only for all

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 $a, b \in H$

16.2 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 $n\mathbb{Z}$

16.3 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)

16.4 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 $(G, \times)$ such that every element of G can be written as a power of g:

$$\langle a \rangle = \{\dots, a^{-2}, a^{-1}, a^0, a^1, a^2, \dots\} = \{a^n | n \in \mathbb{Z}\}$$

If the operator was $+$, the cyclic group would be:

$$\langle a \rangle = \{n \cdot a | n \in \mathbb{Z}\}$$

Theorem: If G is a group and $a \in G$, then $\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$ is a subgroup of G.

The group $\langle a \rangle$ is called the **cyclic subgroup generated by** a. If the subgroup $\langle a \rangle$ is the entire group G, we say that G is a cyclic group.

Example: The multiplicative group of units in the ring $\mathbb{Z}_{15}$ is $U_{15} = \{1, 2, 4, 7, 8, 9, 11, 13, 14\}$. Determine the cyclic subgroup generated by 7:

$$7^1 = 7 \quad 7^2 = 4 \quad 7^3 = 13 \quad 7^4 = 1 = 7^0$$

Therefore, the element 7 has order 4 in U_{15}. Let 7^i be any element of $\langle 7 \rangle$, the integer i must be $\pmod 4$ to one of $0, 1, 2, 3$. Furthermore, note that $\langle 7 \rangle = \langle 13 \rangle$. Thus, *the same cyclic subgroup may be generated by different elements.*

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 $a^i \in C_n$

17 Cosets and Lagrange's Theorem

Definition: Let $H \leq G$ be a subgroup of G. We define a relation $\sim_H$ on G by: if $a, b \in G$ then $a \sim_H b$ if $ab^{-1} \in H$. Note that the relation $\sim_H$ is an equivalence relation.

17.1 Right and Left Coset

Definition: Let $H \leq G$ for a group G and let $\sim_H$ be the relation defined above. The equivalence class of $a \in G$ is called a **right coset** of H and is denoted Ha. The relation is $a \sim_R b \Leftrightarrow ab^{-1} \in H$

Definition: A **left coset** of H is a set $aH = \{ah : h \in H\} = \{b \in G : b^{-1}a \in H\}$

Example: $G = (Z, +), H = nZ$, i.e., $H = \{nk : k \in Z\}$

We know that $H \leq G$. Then for all $a \in G$:

$$\begin{aligned} Ha &= \{h * a : h \in H\} \\ &= \{h * a : h \in nZ\} \\ &= \{a + nk : k \in Z\} \\ &= [a]_n \end{aligned}$$

Example: Find all cosets of $H = \{0, 3\}$ in $\mathbb{Z}_6$ under addition. For all $h \in H$, compute cosets $g + H$. For example, Coset of 1 is $1 + H = \{1 + 0, 1 + 3\} = \{1, 4\}$. Also, the Coset of 3 is the same as the Coset of 0. The distinct cosets are $\{0, 3\}, \{1, 4\}, \{2, 5\}$

17.2 Lagrange's Theorem

Lagrange's Theorem: Let G be a finite group and let $H \leq G$. Note that $|aH| = |Ha| = |H|$. The theorem states that the order of H divides the order of G and there are $\frac{|G|}{|H|}$ left cosets of H and $\frac{|G|}{|H|}$ right cosets of H.

Proof: since G is finite, there are a finite number of left costs in G, i.e., n left cosets. Therefore, $|G| = |a_1H| + \cdots + |a_nH| = |a_iN| = s|H| \Rightarrow \frac{|G|}{|H|} = s \in \mathbb{Z}$

Corollaries:

1. The order of a divides the order of G for $a \in G$
2. For any $a \in G$ and G is finite, with $|G| = m$, then $a^m = e$
3. A group G of prime order is cyclic

17.3 Proof of Euler's and Fermat's Theorems

Euler's Theorem: Recall that if a and n are coprime, then $a^{\phi(n)} \equiv 1 \pmod{n}$, where $\phi(n) = |\{b \in Z : 1 \leq b \leq n \text{ and } \gcd(b, n) = 1\}|$

Let $G_n = \{[a] \in \mathbb{Z}_n : [a] \text{ is a unit}\}$, then it is the same as stating $G_n = \{[a] \in \mathbb{Z}_n : \gcd(a, n) = 1\}$. Then, G_n is a group, thus $\forall [a] \in G_n, [a]^{|G_n|} = [1] \pmod{n}$, where G_n is the exact definition of Euler's totient function $\phi(n)$

Fermat's Little Theorem: If p is prime and $[a] \in \mathbb{Z}_p$ then $[a]^p = [a]$ and $[a]^{p-1} \equiv 1 \pmod{p}$

Since p is prime, $Z_p^* = Z_p \setminus \{[0]\} = \{[1], \ldots, [p-1]\}$ is a group under multiplication. By Corollary 2 above, $\forall a \in [p-1], [a]^{|Z_p^*|} = 1$. Since $|Z_p^*| = p - 1$, we have that $a^{p-1} \equiv 1 \pmod{p}$

18 Group Quotients

18.1 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: Let $H \leq G$ be a subgroup. Define a relation $\sim$ on G by $a \sim b \Leftrightarrow ab^{-1} \in H$. The equivalence class of an element a is the left coset $[a] = Ha = \{ha : h \in H\}$. We call H **normal** in G and write $H \trianglelefteq G$ if its left cosets equal its right cosets, equivalently any of the following equivalent conditions holds:

- $gHg^{-1} = H$ for all $g \in G$
- For every $g \in G$ and every $h \in H$ we have $ghg^{-1} \in H$
- $gH = Hg$ for all $g \in G$

18.2 Quotient Group

Definition: A **quotient group** is a group formed from the cosets of a normal subgroup of a larger group, denoted as G/N. It is constructed by "factoring out" the normal subgroup N, which means its elements are the distinct cosets of N within G.

Remarks:

1. Every subgroup of an abelian group is normal. Therefore, $\frac{G}{H}$ is a group for every subgroup H of an abelian group G
2. Another similar quotient group given by $\frac{G}{H} = \{Ha : a \in G\}$ can be formed under the binary operation $(Ha) \cdot (Hb) = H(ab)$

Example: Let $(G, +) = \mathbb{Z}$ and $H = n\mathbb{Z}$ (the set of all integer multiples of n) for some $n \geq 2$. The cosets of H are $\frac{G}{H} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$.

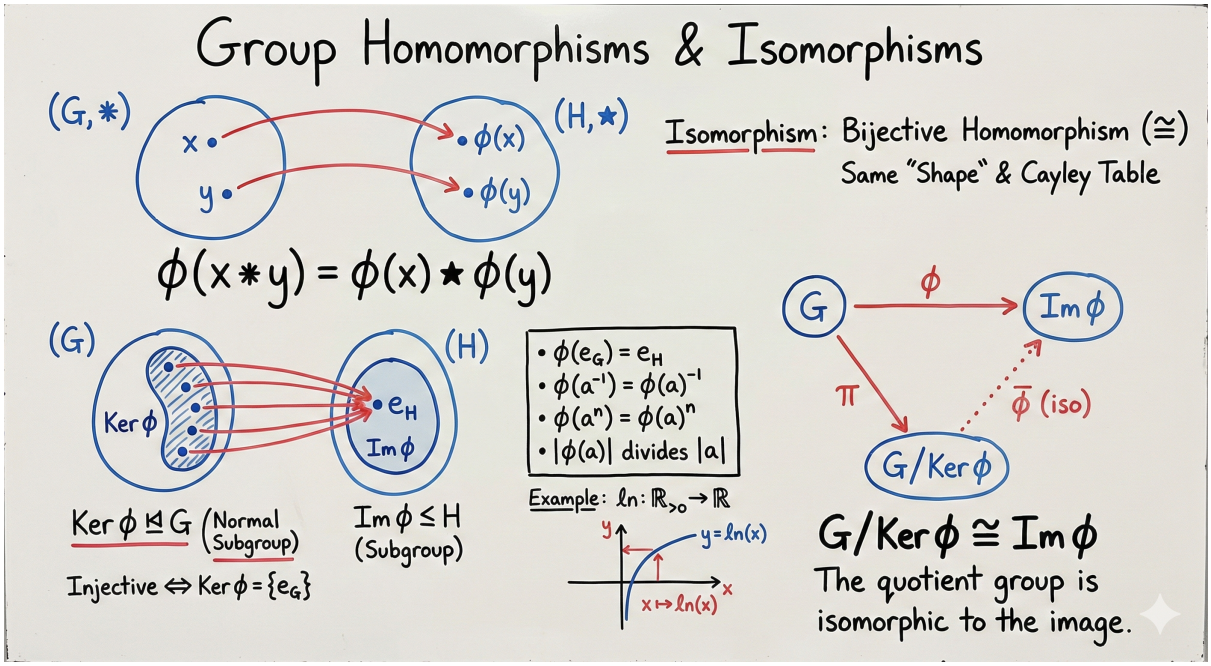
Example: Which coset does 7 belong to when $n = 4$? Recall that a coset is of the form $a + 4\mathbb{Z} = \{\ldots, a-4, a, a+4, a+8, \ldots\}$ where $a = 0, 1, 2,$ or 3. We write $7 = a + 4k$ and get solve: $7 = 1 \cdot 4 + 3$. The remainder, 3, is the representative a, so 7 falls into the coset $3 + 4\mathbb{Z} = \{\ldots, -5, -1, 3, 7, 11, \ldots\}$

Example: Let $a \in G$ and $|a| = 12$ (remember this means $a^{12} = e$). The set G generated by a (i.e., $G = \langle a \rangle$) is $G = \{e, \mathbf{a}.., a^{11}\}$ where 11 is $n - 1$. Let $k = \{e, a^4, a^8\}$. We know that $K \leq G$. Since G is cyclic, it is abelian, thus $K \trianglelefteq G$.

Cosets:

$$
\begin{aligned}
|\frac{G}{K}| = \frac{|G|}{|K|} = \frac{12}{3} = 4 \\
K = Ke = \{e, a^4, a^8\} \\
Ka = \{a, a^5, a^8\} \\
Ka^2 = \{a^2, a^6, a^{10}\} \\
Ka^3 = \{a^3, a^7, a^{11}\} \\
\therefore \frac{G}{K} = \{K, Ka, Ka^2, Ka^3\}
\end{aligned}
$$

19 Group Homomorphisms and Isomorphisms



This section discusses maps between groups, considering groups G and H, and note that, not necessarily, $H \not\trianglelefteq G$

Definition: a function $\phi : (G, *) \to (H, \star)$ is called a homomorphism if, for all $x, y \in G$, $\phi(x * y) = \phi(x) \star \phi(y)$

Examples:

1. Consider the groups $(\mathbb{R}, +)$ and $(\mathbb{R}_{>0}, \cdot)$. The function $\ln : \mathbb{R}_{>0} \to \mathbb{R}$ is a group homomorphism since $\ln(ab) = \ln(a) + \ln(b)$
2. Let H be a group, $a \in H$, $\langle a \rangle$ be the cyclic group generated by a. Set mapping $\alpha : Z \to \langle a \rangle$, $k \to a^k$. α is a homomorphism since: $\alpha(k + m) = a^{k+m} = a^k a^m = \alpha(k)\alpha(m)$
3. The map $\det : GL(n, \mathbb{R}) \to \mathbb{R}$ is a group homomorphism since $\alpha(NM) = \det(MN) = \det(M)\det(N) = \alpha(M)\alpha(N)$

Proposition: Suppose $\alpha : G \to H$ and $\beta : H \to K$. $\beta \circ \alpha : G \to K$ is also a group homomorphism

Definition: a **group isomorphism** is a group homomorphism ϕ that is also a bijection. If $\phi : G \to H$ is an isomorphism, we say that G and H are isomorphic and write $G \cong H$.

An isomorphism is a structure-preserving bijection between G and H, meaning G and H have the same "shape", algebraic behaviour, but maybe different element names. Therefore, they are structurally identical with the same Cayley tables

Definition: a group isomorphism $\alpha : G \to G$ is called an **automorphism**

Examples:

1. The homomorphism $\alpha : \mathbb{R}^+ \setminus \{0\} \to \mathbb{R}$, $x \mapsto \log x$ is an isomorphism

Injectivity: $\log x_1 = \log x_2 \Rightarrow x_1 = x_2$

Surjectivity: Let $x = e^y$, then $\alpha(x) = \log e^y = y$

2. For $a \in G$, $\alpha : G \to G, g \mapsto a^{-1}ga$, then α is an automorphism

Homomorphism: $\alpha(xy) = a^{-1}xya = a^{-1}x(e)ya = (a^{-1}xa)(a^{-1}ya) = \alpha(x)\alpha(y)$

Injectivity : $\alpha(x) = \alpha(y) \Rightarrow a^{-1}xa = a^{-1}ya \Rightarrow x = y$

Surjectivity: Let $x = aya^{-1} \Rightarrow \alpha(x) = a^{-1}aya^{-1}a = y$

20 Morphism Theorems and Lemmas

Lemma: The following properties hold:

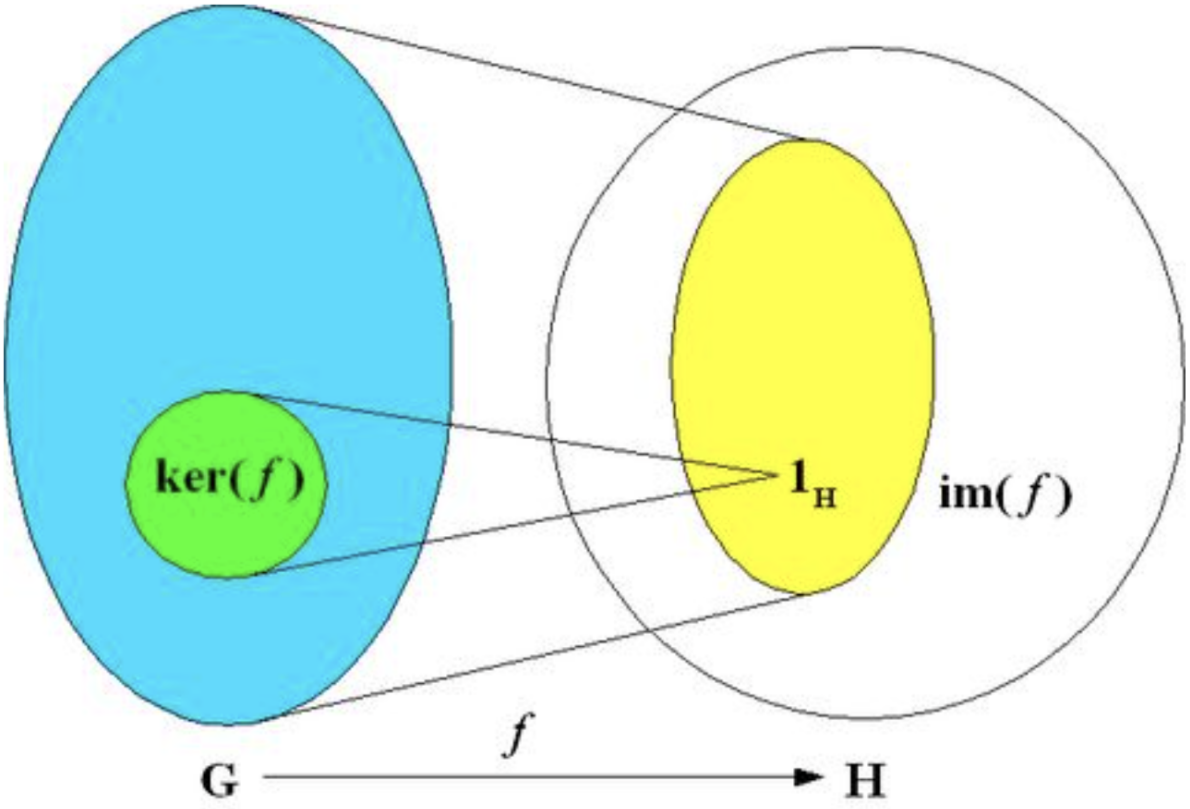
1. If e_G is the identity of G then $\phi(e_G) = e_H$ is the identity of H
2. For $a \in G, \phi(a^{-1}) = (\phi(a))^{-1}$
3. For $a \in G, \phi(a^n) = (\phi(a))^n$ for any integer n

Proposition: Suppose that $\phi : G \to H$ is a group homomorphism. If $a \in G$ has finite order, then $|\phi(a)|$ divides $|a|$

Example: For $\phi : (\mathbb{Z}_8, +_H) \to (\mathbb{Z}_4, +_4)$ defined by $\phi([x]_8) = [x]_4$, the element $[x]_8$ has order 4, but its image $[x]_4$ has order 2, which divides 4

Lemma: If $G \cong H$ and G is abelian, then so is H

Definition: Let $\alpha : G \to H$ be a group homomorphism. The **kernel** of α is $Ker\alpha = \{a \in G : \alpha(a) = e_H\}$. The **image** of α is $\text{Im}\alpha = \{b \in H : \exists a \in G, \alpha(a) = b\} = \{\alpha(a) : a \in G\}$



Lemma: Suppose that $\phi : G \to H$ is a group homomorphism. The image $\phi(K) = \{\phi(k) : k \in K\}$ of a subgroup $K \leq G$ is a subgroup of H. The pre-image $\phi^{-1}(L) = \{g \in G : \phi(g) \in L\}$ of a subgroup $L \leq H$ is a subgroup of G

Proof: $ker(\alpha) \leq G$**:** Nonempty: Since α is a homomorphism, $\alpha(e_G) = e_H$. For $x, y \in ker(\alpha)$, show that $xy^{-1} \in ker(\alpha)$, i.e. $\alpha(xy^{-1}) = e_H$. We know that $\alpha(xy^{-1}) = \alpha(x)\alpha(y^{-1}) = e_H e_H^{-1} = e_H$, therefore $ker(\alpha) \leq G$.

Example: Suppose $\phi : \mathbb{Z} \to \mathbb{Z}_3$ by $\phi(x) = x \pmod 3$. The Image $2\mathbb{Z}$ (even integers) is $\{0, 2\} \subset \mathbb{Z}_3$, which forms a subgroup. The pre-image of $\{0\} \subset \mathbb{Z}_3$ is $3\mathbb{Z}$, which is also a

subgroup of $\mathbb{Z}$

Proposition: The kernel of a group homomorphism $\alpha : G \to H$ is a normal subgroup of G. The image of α is a subgroup of H

Proposition: A group homomorphism $\phi : G \to H$ is injective if and only if $Ker(\phi) = \{e_G\}$

First Isomorphism Theorem: Let $\phi : G \to H$ be a group homomorphism and let $K = Ker\phi$. The function $\bar{\phi} : G/K \to \text{Im}(\phi)$ given by $\bar{\phi}(aK) = \phi(a)$ is a well-defined group isomorphism. In particular $G/Ker\phi \cong \text{Im}(\phi)$

In words: the quotient group (modulo the kernel) is isomorphic to the image of the homomorphism.

Theorem: (First isomorphism theorem) Suppose

- $\psi : G \to H$ is a group homomorphism
- K is the kernel of ψ
- $\phi : G \to G/K$ is the canonical homomorphism.

Then there exists a unique isomorphism $\eta : G/K \to \psi(G) \subset H$ such that $\psi = \eta\phi$.

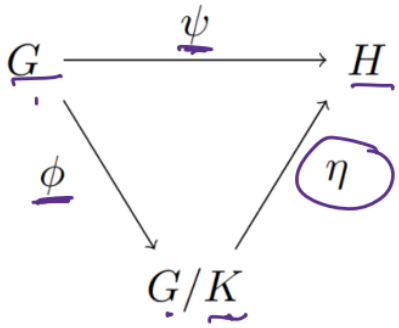
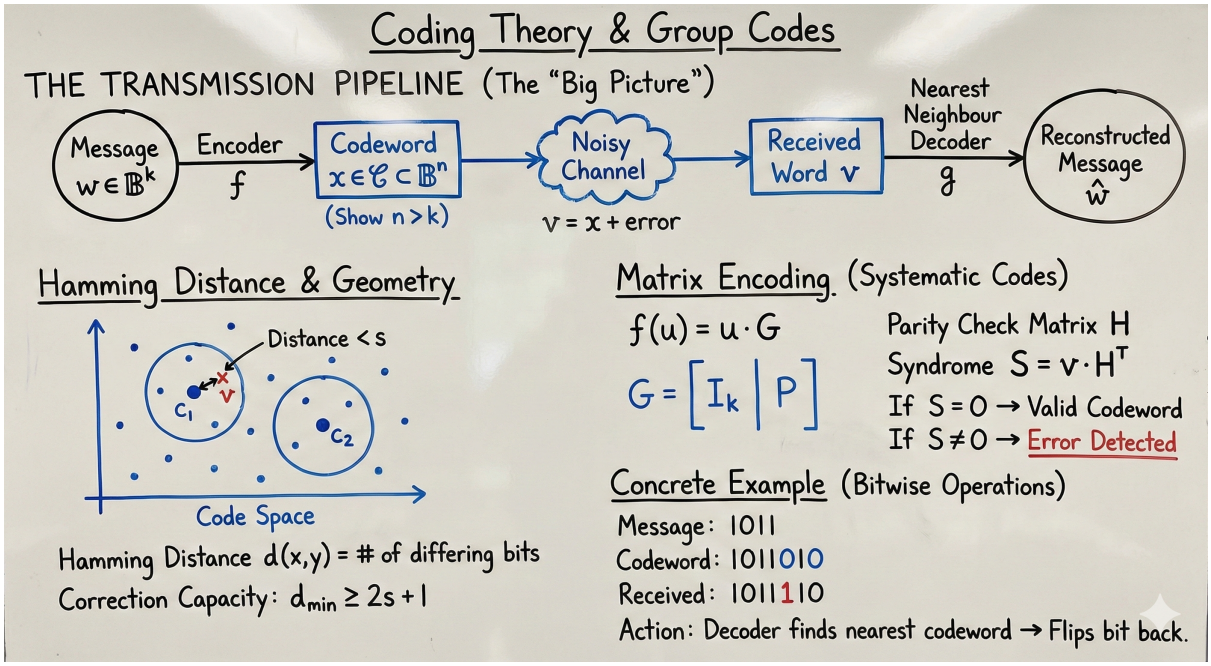


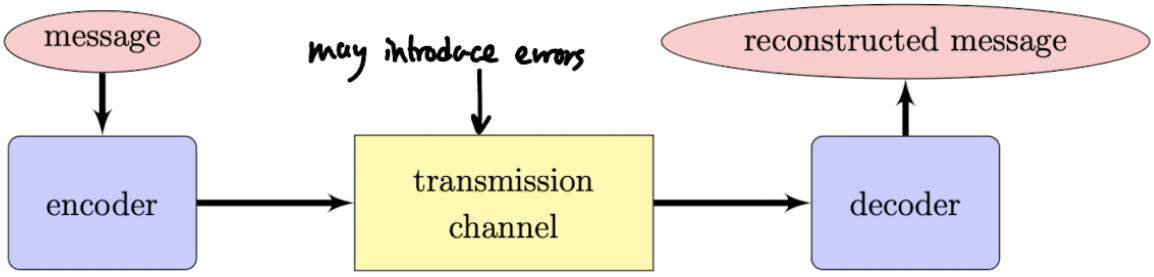
Figure 1: First isomorphism theorem diagram

21 Coding Theory



Digital data is subject to distortions like noise and fading. We establish error-correcting codes to reliably transmit information over noisy communication channels. These codes allow you to:

- detect whether an error has occurred during transmission, assuming that the number of errors is below a certain threshold
- correct and recover the original message if the number of errors in the transmitted message is below a tighter threshold



21.1 Words And Their Measurements

Binary data is simply binary digits, i.e., the group $\mathbb{Z}_2$. Note that we can add numbers under component-wise addition:

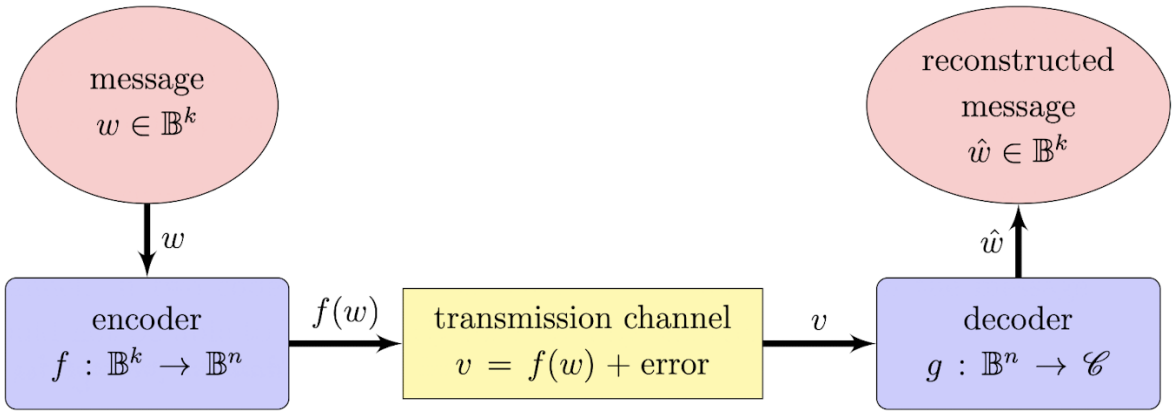
$$01101 + 01011 = (0, 1, 1, 0, 1) + (0, 1, 0, 1, 1) = 00110$$

Definition: An element $w \in \mathbb{B}^n$ (i.e. a string of n bits) is called a **binary word or a message** of length n. It is a binary vector of k-length bits and holds the original

information you want to send. However, this is *not* what you transmit directly because it has no redundancy to correct errors (it's the raw data).

Definition: A binary coding function is an injective function $F : \mathbb{B}^k \to \mathbb{B}^n$. Note that any binary word $c \in \mathbb{B}^n$ that is in the image of f is called a **codeword**. A codeword is what the encoder produces from the message using the encoding function. Codewords contain *extra structure or redundancy* to detect/correct errors during transmission.

Definition: The set $\mathscr{C} = \text{Im}f = f(\mathbb{B}^k)$ is called an (n, k)-binary code. This set is a specific subset of all possible binary words of length n. It is the collection of all valid codewords that the encoder can produce. A (n, k) binary code takes a $k-$bit message and turns it into an $n-$bit codeword



Definition: For an (n, k) binary code, the rate is $R = \frac{k}{n}$. Note that n = length of each codeword (total bits transmitted) and k = dimension of the code (number of information bits). *So the rate R measures how much of each codeword is actual information versus redundancy added for error correction.* Since encoding functions have to be injective, $n \leq k$, then $R \leq 1$. An encoding function must be injective, because if not, information may be lost.

Definition: The **Hamming weight** of a binary word $w \in \mathbb{B}^n$ is the number of 1's in its expression. We use $\bar{w}(w)$ to denote the weight. For example, $\bar{w}(10101) = 3$

Definition: The **Hamming distance** between two words $v, w \in \mathbb{B}^n$ is $d(v, w) = \bar{w}(v-w)$. Furthermore, note that $v = -v$ in $\mathbb{B}^n$. So, $\bar{w}(v - w) = \bar{w}(v + w)$. In words, the hamming distance is *the number of places where v and w disagree (i.e. $v_i \neq w_j$).*

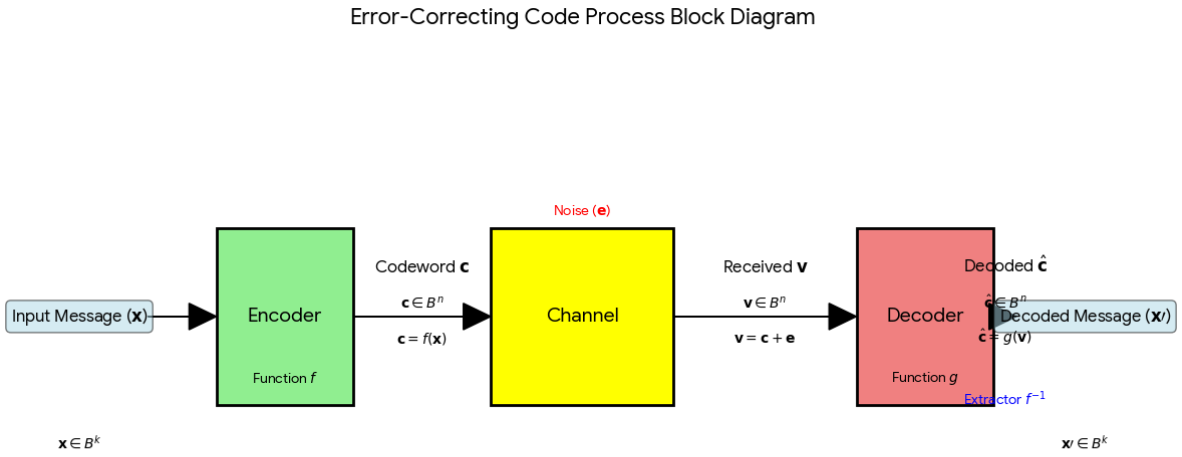
21.2 Nearest Neighbour Decoding

Given a (n, k)-code $\mathscr{C} \subseteq B^n$ with on injective function $f : B^k \to B^n$ so that $\mathscr{C} = f\left(B^k\right)$ (image). We have, by injectivity, $|\mathscr{C}| = \left|B^k\right| = 2^k$ Thus $\mathscr{C}$ contains 2^k codewords.

Definition: If an encoder is the map $f : \mathbb{B}^k \to \mathbb{B}^n$, then a simple decoder is the function $g : \mathbb{B}^n \to \mathbb{B}^k$. However, this is not optimal because this outputs an error if the codeword $v \not\in \mathscr{C}$. We propose a **nearest neighbour decoder**, a function $g : \mathbb{B}^n \to \mathscr{C}$ where:

$$\text{For any word } v \in \mathbb{B}^n, d(g(v), v) \leq d(c, v) \text{ for all } c \in \mathscr{C}$$

Essentially, a NND is simply a function which takes a word to the nearest codeword. Since the encoder function is a bijection, we can decode $v \in \mathbb{B}^n$ as $f^{-1}(g(v))$, i.e., the reconstructed message, since $f^{-1} : \mathscr{C} \to \mathbb{B}^k$



Definition: The **minimum distance** of a binary code $\mathscr{C} \subseteq \mathbb{B}^n$ is

$$d_{min} = min\{d(c, c') : c, c' \in \mathscr{C}, c \neq c'\}$$

Definition: If $\mathscr{C}$ is a binary code with d_{min}, then:

1. $\mathscr{C}$ is guaranteed to detect up to $(d_{min} - 1)$ errors
2. $\mathscr{C}$ is guaranteed to correct up to $\left(\left[\frac{d_{min}-1}{2}\right]\right)$

Example: $n = 4$, $k = 3$. This tells us there are $2^3 = 8$ codewords. A simple example of a $(4, 3)$ binary code is the single-party-check $(4, 3)$ code, where the last digit of the codewords is the sum of the first three bits (i.e. hamming weight):

Message $m = (x_1x_2x_3)$	**Codeword** $c = (x_1, x_2, x_3, x_1 + x_2 + x_3)$
000	0000
001	0011
010	0101
011	0110
100	1001
101	1010
110	1100
111	1111

We find that $d_{min} = 2$, therefore 1 error detected and 0 errors corrected.

21.3 Encoding and Decoding Group Codes

Definition: A **group code** $\mathscr{C} \subseteq \mathbb{B}^n$ is a binary code which is a subgroup of $\mathbb{B}^n$. Since a subgroup must have the identity, 0^n is the identity and we can shortcut our way to d_{min} by simply finding the minimum hamming weight of a codeword in $\mathscr{C}$

Definition: Let $\mathscr{C} \leq \mathbb{B}^n$ be a group code (n, k) with $f(\mathbb{B}^k)$ be the encoding function. Recall that $B^n/E = \{\mathscr{C} + r : r \in \mathbb{B}^n\}$ is the set of cosets of $\mathscr{C}$ in $\mathbb{B}^n$ since $|\mathscr{C}| = \underbrace{|f(\mathbb{B}^k)| = |\mathbb{B}^k|}_{\text{by injectivity}} = 2^k$

Thus, $|\mathbb{B}^n/\mathscr{C}| = |\mathbb{B}^n|/|\mathbb{B}^k|$ by Lagrange's Theorem, and finally $= 2^{n-k}$. Therefore, there are 2^{n-k} cosets.

Definition: If $C \leq \mathbb{B}^n$ is a group code, and $\mathscr{C} + r$ is a coset ($r \in \mathbb{B}^n$), the coset leader is the element(s) in $\mathscr{C} + r$ with minimum $\bar{w}$

Definition: A coset decoding table (CDT) for (n, k) group code is a table with 2^k columns $\left(|\mathscr{C}| = 2^k\right)$ and 2^{n-k} rows $\left(|B^n|/|\mathscr{C}| = 2^{n-k}\right)$ 1) first row starts with 0^n then list all elements of $\mathscr{C}$ 2) each remaining $2^{n-k} - 1$ rows contains a distinct coset of $\mathscr{C}$

The first entry of each row is the coset leader and the rest of the row is obtained by adding the coset leader to the respective element of $\mathscr{C}$ the first row

CDT Construction Algorithm:

(i) Write $\mathscr{C}$ as a row starting with 0^n.

(ii) Pick a word $w \in \mathbb{B}^n$ which is not in any of the previous rows, and which has smallest Hamming weight. Write this word in a new row below 0^n.

(iii) Multiply w by every element in $\mathscr{C}$, coming from the first column, and write the result in that column in the new row. This new row will contain $w + \mathscr{C}$ and w will be of smallest weight; w is our coset leader for $w + \mathscr{C}$.

(iv) Repeat steps 2 and 3, until you have used up all elements in $\mathbb{B}^n$. There will be 2^{n-k} rows and 2^k columns in the table.

Example Consider the $(4, 2)$ group code $\mathscr{C} = \{0000, 1011, 0110, 1101\}$. The first row of our coset table is

$$\mathscr{C} : 0000, 1011, 0110, 1101.$$

The word 1000 has the least weight of all words in $\mathbb{B}^4 \backslash \mathscr{C}$. There are other words of weight 1 , but we pick 1000 arbitrarily. Adding 1000 to our first row gives

$$1000 + \mathscr{C} : 1000, 0011, 1110, 1101.$$

Notice that 0100 has not appeared in either of the first two rows and it has weight one - that is, lowest weight out of the remaining words. We now construct the third row:

$$0100 + \mathscr{C} : 0100, 1111, 0010, 1001.$$

The smallest weight word remaining is 0001 , which gives the row,

$$0001 + \mathscr{C} : 0001, 1010, 0111, 1100.$$

Our entire table is now:

$$\begin{aligned} \mathscr{C} &: 0000, 1011, 0110, 1101 \\ 1000 + \mathscr{C} &: 1000, 0011, 1110, 1101 \\ 0100 + \mathscr{C} &: 0100, 1111, 0010, 1001 \\ 0001 + \mathscr{C} &: 0001, 1010, 0111, 1100 \end{aligned}$$

Here is how we use this table: If we receive message 1111, we look up which column it appears in our decoding table. In this case, 1111 appears in column 1011, so 1011 is the decoded message. The row of 1111 is labeled by the coset leader 0100, which is the error that was (mostly likely) applied to the original coded message 1011 to obtain 1111; $1111 = w = c + r = 1011 + 0100$.

21.4 Matrix Method to En/Decode Group Codes

Recall: $I_k \in M_k$ is $I_k = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ (for $k = 2$)

Definition: Given $n, k > 0, n, k \in \mathbb{Z}, n > k$. The systematic generator matrix G is $k \times n$ matrix with binary entries ($\in \mathbb{B}^n$) such that the first k columns form I_k :

$$G = \left[\underbrace{I_k}_{k} \middle| \underbrace{A}_{n-k} \right]$$

Example: $n = 3, k = 2$ $G = \left[\begin{array}{cc|c} 1 & 0 & 1 \\ 0 & 1 & 1 \end{array}\right]$

Example: $n = 5, k = 3$, $G = \left[\begin{array}{ccc|cc} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{array}\right]$

Encoding: $f_G : \mathbb{B}^k \to \mathbb{B}^n$ defined by $f_G(x) = xG$ where $x \in \mathbb{B}^k$ is viewed as a $1 \times k$ matrix $x = [x_1, x_2, \ldots, x_k]$ and addition and multiplication are $\pmod 2$

Example: $n = 3, k = 2$, $G = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$ and take $x = [01]$

Since $f_G(x) = xG$, then $[01]G = \begin{bmatrix} 011 \end{bmatrix}$

Definition: an (n, k) group code $\mathscr{C} \leq \mathbb{B}^n$ with encoding function $f : \mathbb{B}^k \to \mathbb{B}^n$ is called a systematic code it $\forall x \in \mathbb{B}^k$. the first k bits of f are equal to x

Theorem: If G is a $k \times n$ systematic generator matrix, then the encoding function $f_G(x)$ yields a systematic group code denoted by

$$\mathscr{C} = \text{Im}(f_G) = f_G(\mathbb{B}^k) = \{f_G(x) \mid x \in \mathbb{B}^k\} = \{xG \mid x \in \mathbb{B}^k\}$$

Proof Sketch: we can say $\underbrace{(x-y)}_{\mathscr{C}} G = xG - yG \Rightarrow a \neq b^{-1} \in C, \therefore e \leq \mathbb{B}^k$

Then, $xG = x\,[I_k \mid A] = [xI_k \mid xA] \Rightarrow xI_k = x \therefore \mathscr{C}$ is systematic

Example: $G = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}$ matrix

Take words $x \in \mathbb{B}^n : \{00, 01, 10, 00\}$. Then, codewords are $f_c(x) = xG = [x_1, x_2, x_3, x_4]\, G = \{00000, 01011, 10110, 11101\}$

Now we can compute $d_{min} = 3$. Therefore, we can detect up to 2 errors and correct up to 1 error.

Example: $(7, 4)$ Hamming code

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$$f_G : \mathbb{B}^4 \to \mathbb{B}^7 \text{ and } d_{min} = 3$$

Detect ≤ 2 errors, correct ≤ 1 error

Also, rate $= 4/7$, and a $(6, 2)$ repetition code's rate $= 1/3$ with $d_{min} = 3$

Therefore, the Hamming code is more efficient than $(6, 2)$ with the same $d_{min} = 3$

Remark: If you are given a systematic group code $\mathscr{C}$, then keep in mind that $xG = [x \mid xA]$. Thus if $v \in \mathscr{C}$ and $v = [x \mid \omega] \in C$, then by injectivity of f_G, necessarily $w = xA$ and we can compute A with this

21.5 Syndrome Decoding

Definition: Given a (n, k) systematic generator matrix $G = [I_0|A]$. H is the parity check matrix corresponding to G is the $n \times (n - k)$

$$H = \begin{bmatrix} A \\ I_0 \end{bmatrix}_{n-k}^{k} \quad G = \underbrace{[\, I_k \; A \,]}_{n-k}$$

For any $v \in \mathbb{B}^n$, the syndrome of v is the word $s = vH = (1 \times n)(n \times (n - k)) \in \mathbb{B}^{n-k}$

Example: for the $(2, 4)$ Hamming code:

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$$H = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Compute the syndrome vH of v: 0000011 in $\mathbb{B}^7$

Orthogonality Theorem: For any (n, k) systematic group code with parity check matrix H, we have $v \in C \Leftrightarrow vH = 0^{n-k} = \underbrace{0 \ldots 0}_{n-k}$

Remark: The theorem can be stated with the following formula:

$$\mathscr{C} = \left\{ v \in \mathbb{B}^n \mid vH = 0^{n-k} \right\}$$

Note that if we define $g_n : \mathbb{B}^n \to \mathbb{B}^k$ by $g_n(v) = H$, then you can check that g_H is a group homomorphism and thus $\mathscr{C} = ker\,(g_H)$

Corollary: Two words $u, v \in \mathbb{B}^n$ are in the same row of the CDT, (i.e. are the same coset) for $\mathscr{C} \Leftrightarrow$ they have the same syndrome

Proof: $vH = uH \Leftrightarrow (v - u)H = 0^{n-k}$

$$\Leftrightarrow (v - u) \in \mathscr{C}$$

$\Leftrightarrow v, u$ are in the same coset for $\mathscr{C}$

Conclusion: cosets of $C \in \mathbb{B}^n$ are uniquely determined by syndromes. Thus there is no need to write out the entire CDT. We only need the coset leaders and their syndromes

Example: $G = \begin{bmatrix} 10110 \\ 01011 \end{bmatrix}$, $n = 5, k = 2$, then G is 2×5

Compute H with I and A :

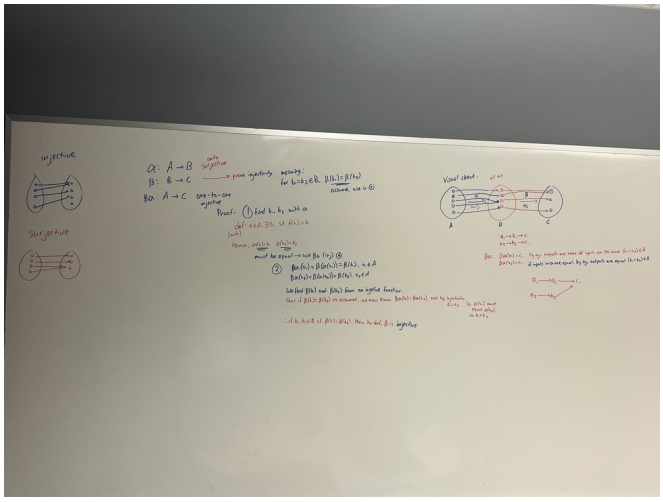
$$H = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \begin{array}{l} k = 2 \\ n - k = 3 \end{array}$$

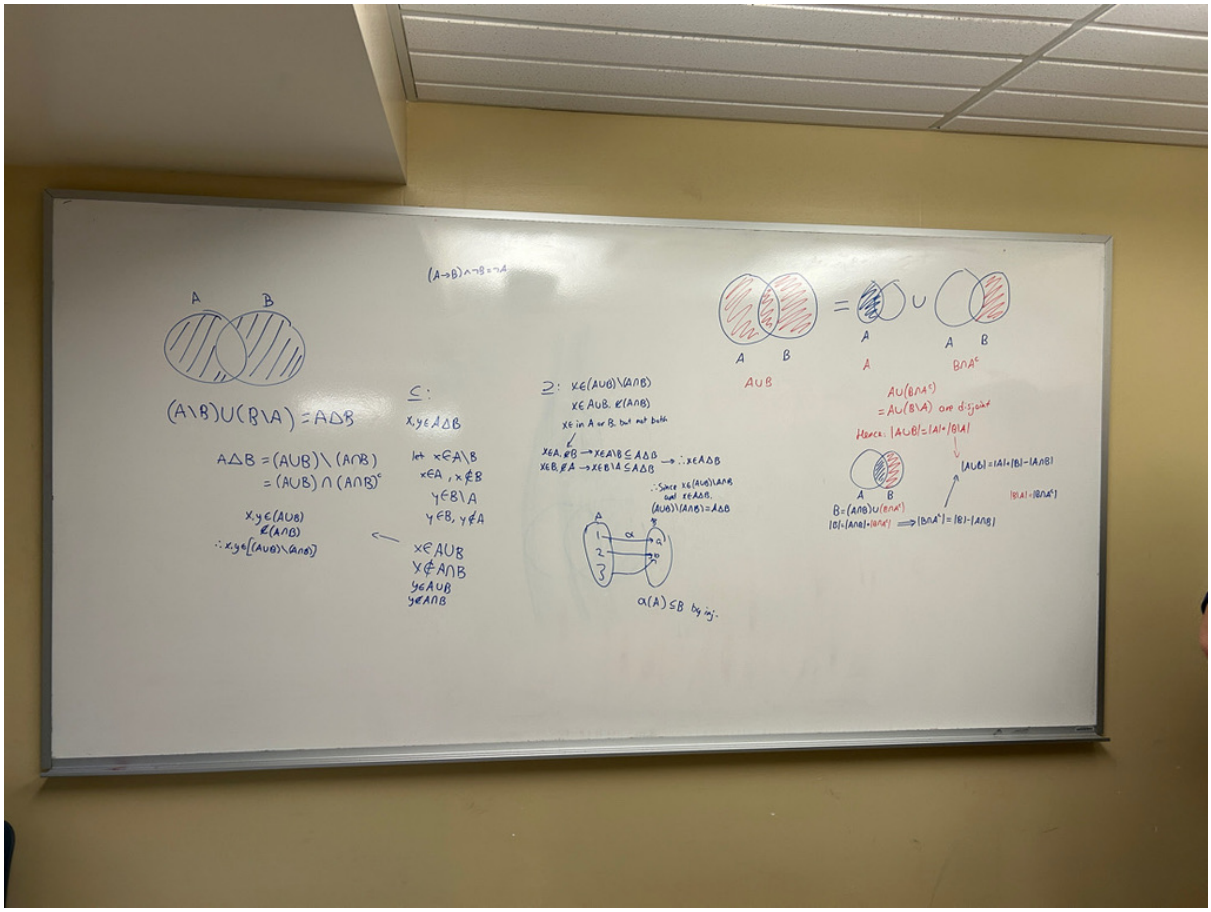
Compute syndromes, enumerate all words in $\mathbb{B}^5$ in increasing Hamming weight order and generate syndromes in $\mathbb{B}^{n-k} = \mathbb{B}^3$

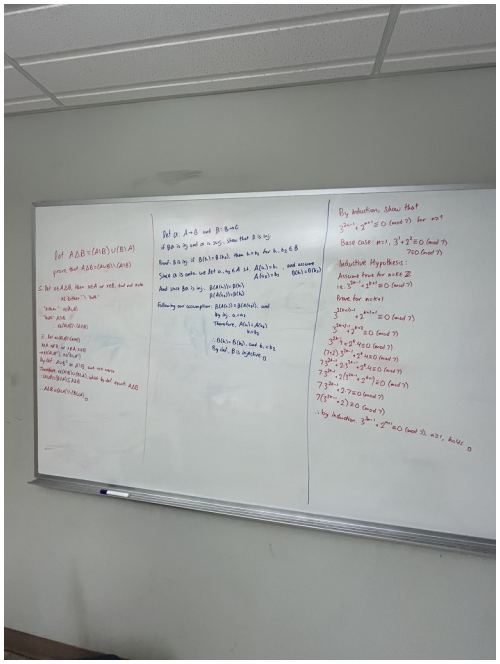
$$
\begin{aligned}
00000 &: zH = 000 \\
00001 &: zH = 001 \\
00010 &: zH = 010 \\
00100 &: zH = 100 \\
01000 &: zH = 011 \\
10000 &: zH = 110 \\
00011 &: zH = \cancel{011} \\
00101 &: zH = 101 \\
10001 &: zH = 111
\end{aligned}
$$

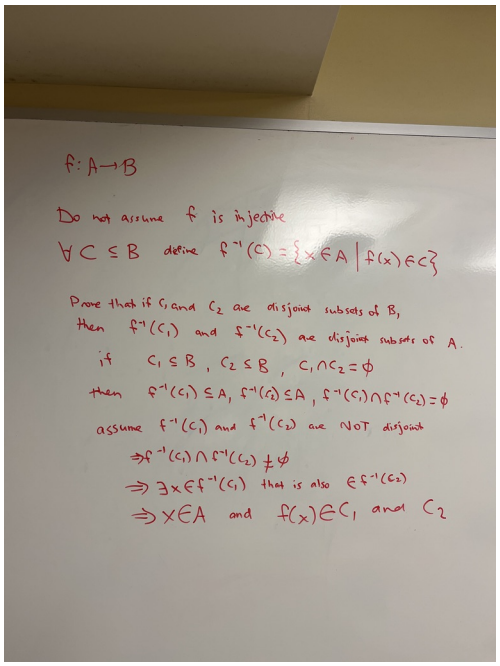
Decoding: Suppose you receive $v = 10101$. We compute the syndrome $vH = 011$. Then, from the table, we know the coset leader is 01000. The "corrected" codeword is the message received $-$ coset leader $= v - z = 10101 - 01000 = 11101$. The message is the decoded codeword ($k = 2$): $x = 11$

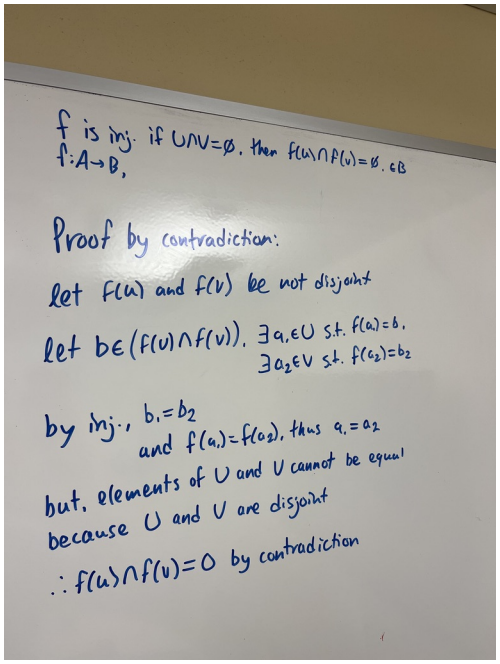
22 Midterm 1 Whiteboard Proofs

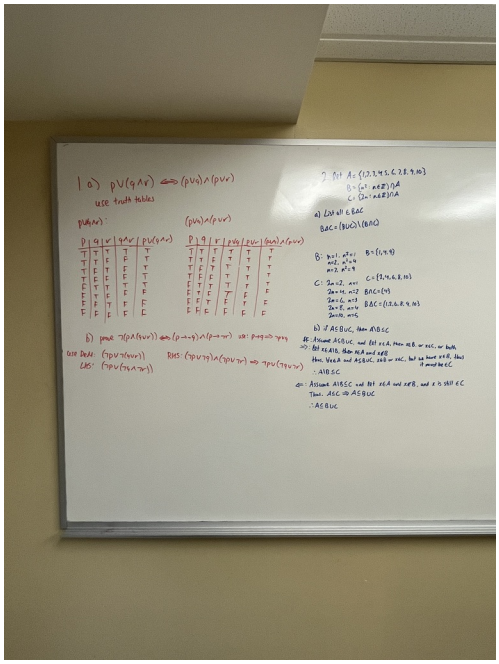


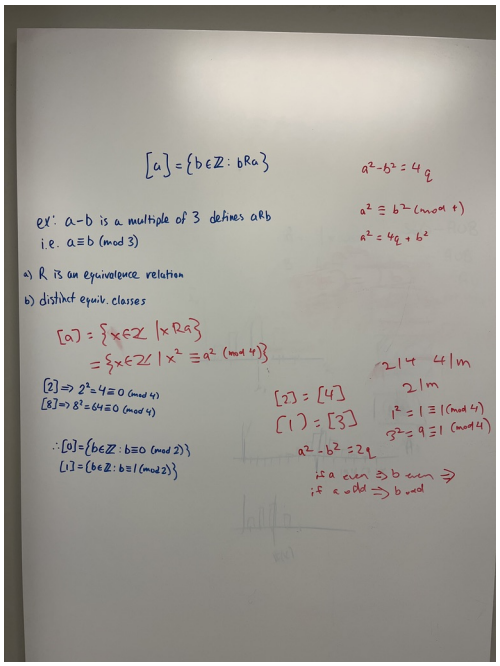


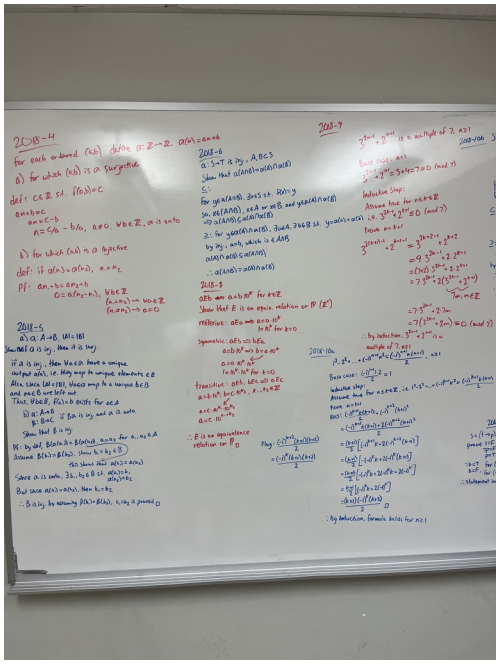


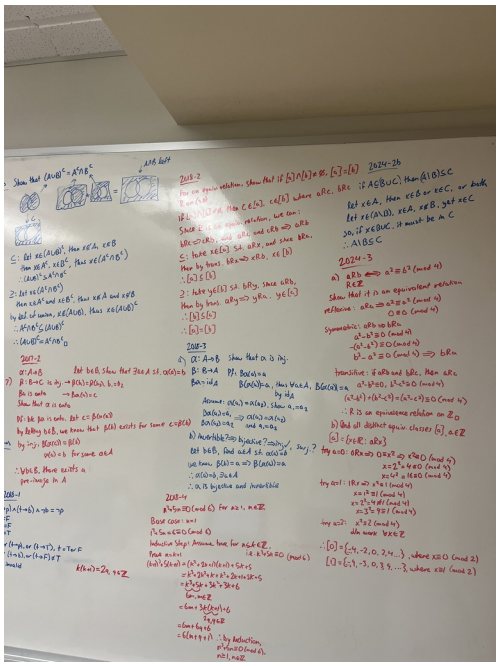

f: A → B
Do not assume f is injective
∀ C ⊆ B define f⁻¹(C) = {x ∈ A | f(x) ∈ C}
Prove that if C1 and C2 are disjoint subsets of B,
then f⁻¹(C1) and f⁻¹(C2) are disjoint subsets of A.
if C1 ⊆ B, C2 ⊆ B, C1 ∩ C2 = ∅
then f⁻¹(C1) ⊆ A, f⁻¹(C2) ⊆ A, f⁻¹(C1) ∩ f⁻¹(C2) = ∅
assume f⁻¹(C1) and f⁻¹(C2) are NOT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

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.

Properties:

- if d divides m, n, then d divides $xm + yn$
- For any a, b, k, we have: $\gcd(a, b) = \gcd(a, b - ka)$
- For coprime n, m and $k \in \mathbb{Z}$, $lcm(m, n) = mn$, and if $m|k$ and $n|k$, then k must be divisible by $lcm(m, n) = mn$

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:

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

Properties:

- If $a \equiv r_1 \pmod{n}$ and $b = r_2 \pmod{n}$, then $ab \equiv r_1 r_2 \pmod{n}$

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 $[a][b] = [1]$. This happens iff $\gcd(a, n) = 1$

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
- $a \cdot b = a \cdot c \Rightarrow b = c$
- $b \cdot a = c \cdot a \Rightarrow b = c$
- Let $(G, *)$ and $(H, \star)$, define $\oplus$ on $G \times H$ by $(g, h) \oplus (g', h') = (g * g', h \star h')$
  - Then $G \times H$ is a group, if G, H are abelian, so is $G \times H$
  - $|G \times H| = |G||H|$

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 $a, b \in H$, $ab^{-1} \in H$