Lecture Notes for MATH 3360: Applicable Algebra

Semester: Spring 2025

Taught by: Karola Mészáros

Notes taken by: Alex Kozik

Table of Contents

Lecture 1: Functions and Their Properties

Topics Covered: function, set, Identity function, inverse function, injectivity, surjectivity, bijectivity, cardinality, image, rationals, function composition

Summary:
This lecture introduces the fundamental concept of functions and their key properties. We explore three essential types of functions:

- Injective (one-to-one) functions, where each element in the codomain has at most one pre-image
- Surjective (onto) functions, where each element in the codomain has at least one pre-image
- Bijective functions, which are both injective and surjective

We also examine important properties of functions, including:

- Function composition and its properties
- The identity function and its role
- Inverse functions and their relationship to bijective functions
- The conditions under which a function has an inverse

These concepts form the foundation for understanding more complex mathematical structures and transformations that will be explored in later lectures.

Cardinality

- The cardinality of a (finite) set A, denoted $|A|$ or $\#A$ is the numbenr of elements in the set.

Note that

$$|A \times B| = |A| \cdot |B|$$

Functions

$$f : \mathbb{R} \to \mathbb{R}$$

$$f(x) = x^2$$

The graph of the function is

$$\{(x, y) \in \mathbb{R}^2 : \ y = f(x)\}$$

Cartesian product

$$A \times B = \{(a, b) : a \in A, b \in B\}$$

Note that

$$|A \times B| = |A| \cdot |B|$$

$|A|$ is the number of elements in a set

Definition - function: Let S and T be two sets. A function from S to T is a subset $F \subseteq S \times T$ such that $\forall x \in S.\ \exists y \in T.\ (x, y) \in F$.

S is called the domain of F

T is the codomain, or range of F

$$(x, y) \in F \iff f(x) = y$$

Example:

$$f : \mathbb{Q} \to \mathbb{Z}$$

$$f\left(\frac{m}{n}\right) = m$$

Note that this is not a function because a rational number can have multiple representations

$$f\left(\frac{1}{3}\right) = 1,\ f\left(\frac{2}{6}\right) = 2$$

And $\frac{1}{3} = \frac{2}{6}$, so, it is not the case that for any $r \in \mathbb{Q}.\ \exists! y \in \mathbb{Z}.\ f(r) = y$.

Definition: Let $A \subseteq S$. The **inclusion function** $\iota : A \to S$ is such that $\forall a \in A.\ \iota(a) = a$.

Definition: Let $f : S \to T$ and $g : T \to U$ be two functions. We define the composition

$$(g \circ f)(x) = g(f(x))$$

> Try writing the composition of functions in cartesian product language.

Proposition: Let $f : S \to T, g : T \to U, R : U \to V$. Then,

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

In other words, function composition is associative.

This is easy to prove using the definition of composition.

Definition: The function $f : S \to T$ is **onto** means $\text{im}(f) = T$. In other words, $\forall t \in T.\ \exists s \in S.\ f(s) = t$. This is also called a **surjection**.

Definition: The function $f : S \to T$ is **one-to-one** means $f(x_1) = f(x_2) \implies x_1 = x_2$. This is also called an injection.

Definition: The function $f : S \to T$ is a **one-to-one correspondence** means f is injective and surjective. This is also called a bijection.

Example:

$$f : \{1, 2\} \to \{3, 4, 5\}$$

Note that f cannot be a surjection.

f can be an injection, for example:

$$1 \to 3$$
$$3 \to 5$$

Consider the bijection

$$g : \{1, 2, 3\} \to \{3, 4, 5\}$$
$$1 \to 4$$
$$3 \to 3$$
$$2 \to 5$$

Note that on the left, each elements appears exactly once, and same on the right side.

Identity function:

$$1_S : S \to S$$
$$\forall x \in S.\ 1_S(x) = x$$

Note that for any function f, we have

$$1_S \circ f = f \circ 1_S = f$$

Inverse function:

Let $f : S \to T$ and let $g : T \to S$ be functions. The functions f and g are inverses of each other means

$$f \circ g = 1_T$$
$$g \circ f = 1_S$$

Proposition: If f has an inverse, then the inverse is unique.

Proof:

Suppose that $g, h : T \to S$ are inverses of f.

We want to show that $g = h$.

Note that

$$\underbrace{(h \circ f)}_{1_S} \circ g = h \circ \underbrace{(f \circ g)}_{1_T}$$
$$\implies 1_S \circ g = h \circ 1_T$$
$$\implies g = h$$
$$QED$$

Proposition: $f : S \to T, g : T \to U$. Then,

1. f and g are onto $\implies$ $g \circ f$ is onto
2. f and g are one-to-one $\implies$ $g \circ f$ one-to-one

Proof of 1:

$\forall z \in U.\ \exists t \in T.\ g(t) = u$, since g is onto.

$\forall t \in T.\ \exists s \in S.\ f(s) = t$, since f is onto

Therefore,

$$(g \circ f)s(s) = g(f(s)) = u \implies g \circ f \text{ is onto}$$
$$QED$$

Proof of 2:

$$g(f(x_1)) = g(f(x_2),\ x_1, x_2 \in S$$

Since g is one-to-one $\implies$ $f(x_1) = f(x_2)$

$$x_1 = x_2$$
$$QED$$

Corollary: If f, g are bijections $\implies$ $g \circ f$ is a bijection.

Proposition: Let $f : S \to T$ be a function.

f has an inverse $\iff$ f is bijective.

$\implies$ **proof:**

Suppose that f has an inverse $g : T \to S$ such that

$$g \circ f = 1_S,\ f \circ g = 1_T$$

Let $y \in T$. Note that

$$y = 1_T(y) = (f \circ g)(y) = f(g(y))$$
$$\forall y \in T.\ f : g(y) \to y$$

So, f is onto

Let $x_1, x_2 \in S$ and suppose

$$
\begin{aligned}
& f(x_1) = f(x_2) \\
\implies & g(f(x_1)) = g(f(x_2)) \\
\implies & (g \circ f)(x_1) = (g \circ f)(x_2) \\
\implies & x_1 = x_2
\end{aligned}
$$

Since $(g \circ f)$ is the identity function

$$QED$$

$\impliedby$ **proof:**

Suppose that f is a bijection. We want to show that g has an inverse.

Define $g : T \to S$ as follows

$$\forall y \in T.\ \exists x \in S.\ f(x) = y$$

Define $g(y) = x$.

We propose that g is the inverse of f.

We must check that

$$
\begin{aligned}
f \circ g &= 1_T \\
g \circ f &= 1_S
\end{aligned}
$$

Lecture 2: Functions and Permutations

Summary:
We explore functions and permutations, starting with a fundamental theorem connecting inverses and bijections. We prove that for finite sets of equal size, injectivity, surjectivity, and bijectivity are equivalent properties. We introduce permutations, cycle notation, and the symmetric group. We demonstrate how to represent permutations as products of disjoint cycles and prove that this representation is unique up to reordering.

Topics Covered: cycle, disjoint cycles, permutation, situational equivalence of injectivity and surjectivity, symmetric group

Theorem:

Let $f : S \to T$ be a function. Then, f has an inverse, $\iff$ f is a bijection

Proposition: Let $f : S \to T$ be a function and assume that S and T are finite sets with $|S| = |T|$. Then, TFAE:

1. f is bijection
2. f is surjective
3. f is injective

Note that in order for a bijection $f : S \to T$ to exist, it must be the case that $|S| = |T|$.

Proof of $2 \implies 1$:

Assume that f is surjective with $|S|, |T| < \infty$ and $|S| = |T|$. We want to show that f is injective.

Suppose, for contradiction, that f is not injective. This means there exist $s, s' \in S$ such that $s \neq s'$ and $f(s) = f(s')$.

Note that

$$|\text{im}(S - \{s, s'\})| \leq |S| - 2$$

This is because $|S - \{s, s'\}| = |S| - 2$, so at most $|S| - 2$ elements are mapped to in T.

Note that since $f(s) = f(s')$, we have that

$$\text{im}(S - \{s, s'\}) = \text{im}(S - \{s\})$$

So,

$$\begin{aligned} &|\text{im}(S - \{s, s'\})| = \text{im}(S - \{s\}) \leq |S| - 2 \\ \implies &|\text{im}(S)| \leq |S| - 2 + 1 = |S| - 1 = |T| - 1 < |T| \\ \implies &|\text{im}(S)| < |T| \\ \implies &\text{im}(S) \neq T \end{aligned}$$

Therefore, f is not surjective, which is a contradiction. So, we conclude that f must be injective.

$$QED$$

Proof of $3 \implies 1$:

Suppose that $f : S \to T$ is injective and $|S|, |T| < \infty$ and $|S| = |T|$. We want to show that f is surjective.

We know that

$$\text{im}(f) = \{f(s) : s \in S\}$$

Since f is injective, we know that $\forall s, s' \in S.\ s \neq s' \implies f(s) \neq f(s')$

$$\begin{aligned} &\implies |\text{im}(f)| = |\{f(s) : s \in S\}| = |S| = |T| \\ &\implies |\text{im}(f)| = |T| \end{aligned}$$

$$\implies \text{im}(f) = T$$

Therefore, f is surjective.

$$QED$$

We have shown that

- $1 \implies 2$
- $1 \implies 3$
- $2 \implies 1$
- $3 \implies 1$

Therefore, we have proven the equivalence.

$$QED$$

Definition:

Let S be a set. A function $\sigma : S \to S$ is called is called a permutation of S when σ is a bijection.

The set of all permutations of S is denoted $\text{Sym}(S)$.

Generally, we will take $S = \{1, 2, \dots, n\} = [n]$, in which we use the notation

$$S_n = \text{Sym}([n])$$

Recall that the composition of bijections is a bijection.

Therefore,

1. $\tau, \sigma \in S_n \implies \tau\sigma \in S_n$
2. $\iota_S \in S_n$
    - ι_S is the identity permutation for S
3. $\sigma \in S_n \implies \sigma^{-1} \in S_n$

Later, we will see that permutations of S with composition form a group.

Here is a 2 line notation we can use to describe a permutation

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots. & \sigma(n) \end{pmatrix}$$

Suppose that

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

Then, we have

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

Definition: The permutation σ is called a cycle of length k when there exist elements $a_1, \dots, a_k \in [n]$ such that

$$\sigma(a_1) = a_2, \sigma(a_2) = a_3, \dots, \sigma(a_{k-1}) = a_k, \sigma(a_k) = a_1$$

and

$$\forall x \in [n] - \{a_1, \dots, a_k\}.\ \sigma(x) = x$$

In this case, we use cycle notation as follows:

$$\sigma = (a_1, a_2, \dots, a_k)$$

Note that a permutation written in cycle notation can be written in several ways. For example:

$$(2,1,4) = (1,4,2) = (4,2,1)$$

Because it's a cycle so we can start at any element, as long as the order of the elements is the same.

The identity permutation is a cycle of length 0.

Definition: If $\sigma = (a_1, \ldots, a_k)$ and $\tau = (b_1, \ldots, b_m)$ are cycles in S_n, then σ and τ are said to be disjoint cycles when

$$\{a_1, \ldots, a_k\} \cap \{b_1, \ldots, b_m\} = \emptyset$$

Note that in general, for $\sigma, \tau \in S_n$, it is not the case that $\sigma\tau = \tau\sigma$ (the permutations commute).

For example:

$$(1,2)(3)\ (1,3)(2) = (1,3,2)$$
$$(1,3)(2)\ (1,2)(3) = (1,2,3)$$

Lemma:

If $\sigma, \tau \in S_n$ are disjoint cycles, then $\sigma\tau = \tau\sigma$ (σ and τ commute).

Proof:

Let $\sigma = (a_1, \ldots, a_k)$ let $\tau = (b_1, \ldots, b_m)$ with $\{a_1, \ldots\ldots, a_k\} \cap \{b_1, \ldots, b_m\} = \emptyset$.

Then, $\sigma\tau = \tau\sigma$ holds because the permutations are disjoint, so, they do not interfere with each other.

Definition:

We define the following exponent notation for the composition of permutations:

$$\sigma^i = \underbrace{\sigma \ldots \sigma}_{i}$$

$$\sigma^{m+n} = \sigma^m \sigma^n$$
$$(\sigma^m)^n = \sigma^{mn}$$
$$\sigma^1 \sigma^{-1} = \mathrm{id} = \sigma^0$$

Example:

Note that if

$$\sigma = (a_1, \ldots, a_n)$$

then

$$\sigma^{-1} = (a_n, \ldots, a_1)$$

To get the inverse of a cycle, just reverse the order of the cycle.

Theorem:

Every permutation $\sigma \in S_n$ can be written as a product of disjoint cycles. Moreover, up to the rearrangement of cycles, this representation is unique.

Example:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 11 & 7 & 6 & 5 & 4 & 8 & 9 & 1 & 10 & 2 & 3 \end{pmatrix}$$

$$\sigma = (1,11,3,6,8)(2,7,9,10)(4,5)$$

To do this, we start with an arbitrary element and just follow it until we get back to the start. We keep doing this, starting at new elements until we finish.

Proof: We will give an algorithm to write any σ as a product of disjoint cycles.

Successively apply powers of σ to 1

$$1, \sigma(1), \sigma^2(1), \sigma^3(1), \dots.$$

Eventually we will have $\sigma^k(1) = 1$ for some $k \in \mathbb{Z}^+$. Then, define the cycle

$$\sigma_1 = (1, \sigma(1), \dots, \sigma^k(1))$$

Then, pick another element $x \in [n] - \{1, \sigma(1), \dots, \sigma^k(1)\}$ and do the same thing

$$\sigma_2 = (x, \sigma(x), \dots, \sigma^l(x))$$

And keep going until all elements are in a cycle. If $\sigma_1, \dots, \sigma_m$ are the cycles that we've defined, then, we have

$$\sigma = \sigma_1 \dots \sigma_m$$

$$\text{QED}$$

Practice problem

Let $S = [n]$. Suppose that $\sigma \in S_n$ is n-cycle

$$\sigma = (a_1, \dots, a_n)$$

Show that σ^{n-1} is the inverse of σ.

It suffices to show that $\forall x \in [n].\ \sigma^n(x) = x$.

Note that x is guaranteed to be in the cycle, since it's an n-cycle and we are working with $S = [n]$.

Suppose that $x = a_1$.

Then,

$$\sigma(a_1) = a_2$$

$$\sigma^2(a_1) = a_3$$

$$\dots.$$

$$\sigma^n(a_k) = a_{k+1}$$

$$\implies \sigma^n(a_1) = a_1$$

$$QED$$

Another practice problem

Suppose that $\sigma \in S_n$ such that $\forall \tau \in S_n.\ \sigma\tau = \tau\sigma$. Show that $\sigma = \text{id}$.

Proof:

Suppose, for contradiction, that $\sigma \neq \text{id}$. Then, there exists $1 \in [n]$ such that

$$\sigma(1) = k \neq 1$$

Since σ is a bijection, there exists $m \neq 1$ such that $\sigma(m) = 1$.

Pick $t \neq 1, m$

$$\tau = (t, m)$$

$$\sigma\tau(m) = \sigma(t) \neq 1$$

$$\tau\sigma(m) = \tau(1) = 1$$

This is a contradiction because $\sigma\tau \neq \tau\sigma$.

We conclude that $\sigma = \text{id}$.

Lecture 3: More on Permutations, Division Algorithm

Summary:
We continue our exploration of permutations and introduce the division algorithm. We prove that every permutation can be written as a product of disjoint cycles, with a unique representation up to reordering. We define the order of a permutation and show that it equals the least common multiple of the lengths of its disjoint cycles. We present the division algorithm for integers and prove its existence and uniqueness. We use this algorithm to establish properties about the order of permutations and their powers. We prove that powers of a permutation are equal if and only if their exponents are congruent modulo the permutation's order.

Topics Covered: division algorithm for integers, identity permutation, order of a permutation, representation of a permutation as disjoint cycles

Theorem: Every permutation in S_n can be written as a product of disjoint cycles. Moreover, the presentation is unique up to reordering of cycles.

Example:

Consider the following permutation:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 3 & 4 & 6 & 7 & 5 \end{pmatrix}$$

We can write it as a product of disjoint cycles as follows:

$$\sigma = (1,2)(3)(4)(5,6,7)$$

Proof:

Consider

$$1, \sigma(1), \sigma^2(1), \sigma^3(1), \dots.$$

Assume that j is the smallest positive number such that

$$\sigma^j(1) \in \{1, \sigma(1), \dots., \sigma^{j-1}(1)\}$$

We want to understand which $i < j$ is such that

$$\sigma^j(1) = \sigma^i(1)$$

We want to show that $i = 0$.

Suppose, for contradiction that $i > 0$, but, j is still the smallest positive number such that

$$\sigma^j(1) = \in \{1, \sigma(1), \dots., \sigma^{j-1}\}$$

So, we have that

$$\sigma^i(1) = \sigma^j(1)$$

Apply σ^{-1} to each side, which exists since σ is a bijection.

$$\implies \sigma^{i-1}(1) = \sigma^{j-1}(1)$$

Which contradicts the minimality of j.

So, we now know that $i = 0$.

$$\implies$$

If

$$\{1, \sigma(1), \dots., \sigma^{j-1}(1)\} = [n]$$

then

$$\sigma = (1, \sigma(1), \ldots, \sigma^{j-1}(1)\}$$

Otherwise, pick the smallest element

$$a \in [n] - [\{1, \sigma(1), \ldots, \sigma^{j-1}(1)\}$$

and consider the sequence

$$a, \sigma(a), \sigma^2(a), \ldots.$$

Getting your next cycle $(a, \sigma(a), \ldots, \sigma^{k-1}(a))$ and continue this fashion until your cycles contain all elements in $[n]$.

We can represent the permutation as a graph of disjoint cycles.

> Exercise: show that the product of disjoint cycles is unique up to reordering of the cycles

Consider the following cycle

$$\sigma = (1, 2)(3, 4, 5)$$

Note that

$$\sigma^2(1) = 1$$
$$\sigma^2(2) = 2$$
$$\sigma^3(3) = 3$$
$$\sigma^3(4) = 4$$
$$\sigma^3(5) = 5$$

Therefore,

$$\sigma^3 = (1, 2)(3)(4)(5)$$

Definition: The smallest positive integer m such that $\sigma^m = \mathrm{id}$ is called the **order** of σ.

Question: What is the order of $\sigma = (a_1, \ldots, a_k)$?

It's k, because $\sigma^k = \mathrm{id}$ and for any $i \in \{1, \ldots k-1\}$, $\sigma^i(a_j) \neq a_j$

$$\sigma^k = \mathrm{id}$$
$$\sigma^{k+1} = \sigma$$

Consider

$$\pi = (1, 2)(3, 4, 5, 6)$$

The order of π is 4.

Proposition: The order of σ is the least common multiple of the lengths of the disjoint cycles in the cycle representation of σ.

Proof:

If we have one cycle longer than 1, then we know the proposition.

If we have 2 cycles longer than 1

$$(a_1, \ldots a_k)(b_1, \ldots, b_m), \;\; (a_1, \ldots, a_k) \cap (b_1, \ldots, b_m) \neq \emptyset$$
$$(a_1, \ldots, a_k)^k = \mathrm{id} \;\; \text{on} \;\; a_1, \ldots, a_k$$
$$(b_1, \ldots, b_m)^m = \mathrm{id} \;\; \text{on} \;\; b_1, \ldots, b_m$$
$$\sigma^j = (a_1, \ldots, a_k)^j \, (b_1, \ldots, b_m)^j$$

Note that the LCM of m, k satisfies

$$\sigma^{\text{LCM}(m,k)} = \text{id}$$

Proposition: Let $\sigma \in S_n$ have order m. Then, $\forall i, j \in \mathbb{Z}$, we have

$$\sigma^i = \sigma^j \iff m \mid i - j$$

We can also write the right side as

$$i \equiv j \ (\bmod m)$$

To prove this theorem, we will need the division algorithm

Theorem: (Existence of quotient and remainder):

Let $a, b \in \mathbb{Z}$ and $a \geq 0$ and $b > 0$. Here, a is the number we are dividing, and b is the divisor.

Then, $\exists q, r \in \mathbb{Z}$ such that

$$a = qr + r$$

and

$$0 \leq r < b$$

q is the quotient and r is the remainder.

Proof:

$0 \cdot b = 0, 1 \cdot b, 2 \cdot b, 3 \cdot b, ...$

$\exists q \in \mathbb{Z}$ such that

$$q \cdot b \leq a < (q+1)b$$
$$r = a - qb$$

Theorem: uniqueness of quotient and remainder:

Let $a, b \in \mathbb{Z}$ with $a \geq 0$ and $b > 0$ and let $q, r, q', r' \in \mathbb{Z}$ such that

$$a = qb + r$$
$$0 \leq r < b$$
$$a = q'b + r'$$
$$0 \leq r' < b$$

Then, it holds that $q = q', r = r'$.

Proof:

We know that $a = qb + r$ and $a = q'b + r'$, Subtract them to get

$$(q - q')b = r' - r$$

Since $0 \leq r, r' < b$, we know that $-b < r' - r < b$

$$\implies -b < (q - q')b < b$$
$$-1 < q - q' < 1 \implies q - q' = 0 \implies q = q', r = r'$$
$$QED$$

Going back to the other theorem

$$i - j = (qm + r) - (q'm + r') = m(q - q') + (r - r')$$

Note that $i \equiv j \ (\bmod m)$ means the remainders of i and j upon division by m are equal.

Proof: The smallest positive integer for which $\sigma^j = \mathrm{id}$ is $m : \sigma^m = \mathrm{id}$

Assuming $\sigma^i = \sigma^j, i, j \in \mathbb{Z}$

Multiply by σ^{-i}, we get

$$\sigma^{i-i} = \sigma^0 = \mathrm{id} = \sigma^{j-i}$$

So,

$$\mathrm{id} = \sigma^{j-i} = \sigma^{qm+r} = \sigma^{qm}\sigma^r = (\sigma^m)^q\sigma^r = (\mathrm{id})^q\sigma^r = \sigma^r$$
$$0 \leq r < m$$
$$\implies r = 0$$
$$\implies m | j - i$$

Which means $i \equiv j \pmod m$

$$QED$$

The proof in the other direction is not difficult.

Lecture 4: transpositions, more properties of cycles

Summary:
We explore transpositions and their importance in permutation theory. We prove that the order of a permutation is the least common multiple of its disjoint cycle lengths. We show that every permutation can be written as a product of transpositions. We prove that the number of transpositions needed to write a permutation is either always even or always odd, establishing the concept of parity. We define even and odd permutations and provide examples of writing permutations as products of transpositions.

Topics Covered: even permutation, odd permutation, order of a permutation, parity of a permutation, transposition

Proposition: If $\sigma \in S_n$ is a product of disjoint cycles of lengths $l_1, \dots, l_z$, then the order of σ is the least common multiple of $l_1, \dots, l_z$.

This is the smallest positive integer k such that $l_i \mid k$ for all $i \in [z]$.

Consider these permutations

$$\sigma = (1,2)(3,4,5)$$
$$\pi = (1,2)(3,4,5,6)$$

Note that

$$(1,2)(1,2) = (1)(2)$$

Definition: A cycle of the form (a_1, a_2) is called a transposition.

Proposition: Every $\sigma \in S_n$ can be written as a product of transposition.

Proof: Since $\sigma \in S_n$ is a product of disjoint cycles, it suffices to prove the above claim for a cycle $(a_1, \dots, a_k)$.

Note that

$$(a_1, \dots, a_k) = (a_{k-1}, a_k) \dots (a_3, a_k)(a_2, a_k)(a_1, a_k)$$

We can also write it as

$$(a_1, \dots, a_k) = (a_1, a_2)(a_2, a_3) \dots (a_{k-1}, a_k)$$

Both ways show that the cycle $(a_1, \dots, a_k)$ can be written as a product of transpositions.

> The goal is to show that all of these complex permutations can be constructed using tiny building blocks.

Example: Try writing $(1,2,3,4)$ as a product of three transpositions.

$$(1,2,3,4) = (1,2)(2,3)(3,4)$$

Theorem: If $\sigma \in S_n$ is written as a product of transpositions in two ways, then the number of transpositions in both cases is either both even or both odd. That is to say that the parity of the number of transpositions remains the same.

Proof: Assume to the contrary that for some $\sigma \in S_n$ and transpositions $\tau_1, \dots, \tau_{2m}$, $\delta_1, \dots, \delta_{2n+1}$ we have

$$\sigma = \tau_1 \dots \tau_{2m} = \delta_1 \dots \delta_{2n+1}$$

We can write σ^{-1} as follows:

$$\sigma^{-1} = \tau_{2m}^{-1} \dots \tau_1^{-1}$$

But, note that each $\tau_i^{-1} = \tau_i$, since τ_i is a transposition, and a transposition is its own inverse.

$$\implies \sigma^{-1} = \tau_{2m} \dots \tau_1$$

Similarly, we have

$$\sigma^{-1} = \delta_{2n+1} \dots \delta_1$$

So, we have that

$$\mathrm{id} = \sigma\sigma^{-1} = \underbrace{\tau_1 \dots \tau_{2m} \delta_{2n+1} \dots \delta_1}_{\text{odd number of transpositions}}$$

Thus, we have a way of writing the identity on an odd number of transpositions. Suppose k is the smallest positive odd number for which the product of k transpositions is the id. We see that $k \geq 3$.

$$\sigma = \rho_1 \dots \rho_k$$

We let $\rho_1 = (a, b)$.

Note that a must appear in some ρ_i for $i > 1$, because otherwise a would get stuck and wouldn't map to a in id.

Among the products $\rho_1 \dots \rho_k = \mathrm{id}$, let this expression have the fewest $\rho_1(a, \star)$ of a's in transposition (at least two a's we know from above!)

Let ρ_i with $i > 1$ be the leftmost such that $\rho = (a, c)$.

a, u, v, v distinct

$$(u, v)(a, r) = (a, r)(u, v)$$

$$(u, v)(a, u) = (a, u)(u, v)$$

$$\underbrace{(a, b)}_{\rho_1} \dots \underbrace{(a, c)}_{\rho_i}$$

Using relation $\star$, we have

$$\mathrm{id} = (a, c)(a, c')\rho_3' \dots \rho_k'$$

In the case that $b = c' \implies \mathrm{id} = \rho_3' \dots \rho_k'$, so we can write id as a product of $k - 2$ transpositions, which is a contradiction to the minimality of k.

In the case that $b \neq c' \implies$

$$\mathrm{id} = (a, c')(b, c')\rho_3 \dots \rho_k'$$

Which contradicts that we picked transpositions with the least number of a's.

So, in either case, we've reached a contradiction. So, we conclude that the lengths of the products of transpositions must have the same length.

$$QED$$

Definition: A permutation $\sigma \in S_n$ is called even when it can be written as a product of an even number of transpositions. A permutation $\sigma \in S_n$ is called odd when it can be written as a product of an odd number of transpositions. This notion is well-defined, as proven above.

Examples:

id is even. You can write it as $(1, 2)(1, 2)$. You can also write it as the empty composition!

(a_1, a_2, a_3) is even, you can write it as $(a_1, a_2)(a_2, a_3)$.

Lecture 5: Monoids, Groups, and Their Properties

Summary:
We explore the fundamental structures of monoids and groups. We begin with the multiplication table for the symmetric group S_3. We define binary operations and their properties: identity, associativity, commutativity, and inverses. We define monoids as sets with an associative binary operation and an identity element, with examples from matrices and integers. We investigate invertibility in monoids and define groups as monoids where every element is invertible. We prove the uniqueness of inverses and the cancellation lemma. We show that the symmetric group is a group under composition and provide guidelines for checking if a structure is a group.

Topics Covered: closure of operations, group, monoid, symmetric group

Multiplication table for S_3:

	$(1)(2)(3)$	$(1,2,3)$	$(1,3,2)$	$(1,2)(3)$	$(1,3)(2)$	$(2,3)(1)$
$(1)(2)(3)$	$(1)(2)(3)$	$(1,2,3)$	$(1,3,2)$	$(1,2)(3)$	$(1,3)(2)$	$(2,3)(1)$
$(1,2,3)$	$(1,2,3)$	$(1,3,2)$	$(1)(2)(3)$	$(2,3)(1)$	$(1,2)(3)$	$(1,3)(2)$
$(1,3,2)$	$(1,3,2)$	$(1)(2)(3)$	$(1,2,3)$	$(1,3)(2)$	$(2,3)(1)$	$(1,2)(3)$
$(1,2)(3)$	$(1,2)(3)$	$(1,3)(2)$	$(2,3)(1)$	$(1)(2)(3)$	$(1,2,3)$	$(1,3,2)$
$(1,3)(2)$	$(1,3)(2)$	$(2,3)(1)$	$(1,2)(3)$	$(1,3,2)$	$(1)(2)(3)$	$(1,2,3)$
$(2,3)(1)$	$(2,3)(1)$	$(1,2)(3)$	$(1,3)(2)$	$(1,2,3)$	$(1,3,2)$	$(1)(2)(3)$

Groups

Definition: A binary operation $(\cdot)$ on a set A is a function $A \times A \to A$.

Operations may satisfy

1. $\exists e \in A. \forall a \in A.\ \ a \cdot e = e \cdot a = a$
   - Identity
2. $\forall a, b, c \in A.\ a \cdot (b \cdot c) = (a \cdot b) \cdot c$
   - Associative
3. $\forall a, b \in A.\ a \cdot b = b \cdot a$
   - Commutative
4. If identity e exists, then we may have $\forall a \in A.\ \exists a^{-1} \in A.\ a \cdot a^{-1} = a^{-1} = e$
   - Inverse

Suppose that $(\cdot)$ is a binary operation on A and has identities $e, e' \in A$.

Note that we have

$$\begin{aligned} e' = e' \cdot e = e \\ \implies e = e' \end{aligned}$$

Therefore, identity is unique.

Definition: A monoid is a set M together with binary operation on M such that

1. $\exists e \in A. \forall a \in A.\ \ a \cdot e = e \cdot a = a$
   - Identity
2. $\forall a, b, c \in A.\ a \cdot (b \cdot c) = (a \cdot b) \cdot c$
   - Associative

- Examples of monoid

- 2×2 real-valued matrices with $+$
  - Matrices with $\det M = 0$ do not have an inverse
- $(\mathbb{Z}, +)$
- $(\mathbb{Z}, \cdot)$
  - 0 does not have an inverse

Invertibility in a monoid: Let $(M, \cdot)$ be a monoid. We say that element $a \in M$ is **invertible** means $\exists b \in M$ such that $a \cdot b = b \cdot a = e$ where $e \in M$ is the identity element of M.

Examples of monoids:

- In $(\mathbb{Z}, \cdot)$ the set of invertible elements is $\{1, -1\}$
- $(\mathcal{M}_2(\mathbb{R}), \cdot)$
  - The set of 2×2 real-valued matrices
  - The set of invertible elements is 2×2 matrices with nonzero determinant

Note that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{R})$$

is invertible $\iff ad - bc \neq 0$.

Proposition (uniqueness of inverses):

Let $(M, \cdot)$ be a monoid. If $b, b' \in M$ are both inverses of $a \in M$, then $b = b'$.

Proof:

We know that

$$\begin{gathered} b' \cdot \underbrace{(a \cdot b)}_{e} = \underbrace{(b' \cdot a)}_{e} \cdot b \\ \implies b' \cdot e = e \cdot b \\ \implies b' = b \\ QED \end{gathered}$$

Let's denote the unique inverse of a as a^{-1} or $(-a)$.

Lemma (a monoid always has at least one invertible element):

Let $(M, \cdot)$ be a monoid.

Then, we know that e is invertible. Moreover, $e^{-1} = e$, since $e \cdot e = e$.

Cancellation lemma:

Let $a \in M$ be an invertible element of the monoid $(M, \cdot)$. Let $x, x' \in M$. Then,

$$a \cdot x = a \cdot x' \implies x = x'$$

Proof:

Multiply on the left by a^{-1}

$$\begin{gathered} a^{-1} \cdot a \cdot x = a^{-1} \cdot a \cdot x' \\ \implies e \cdot x = e \cdot x' \\ \implies x = x' \end{gathered}$$

QED

Example:

Let $a \in M$ be invertible. Let $c \in M$. Consider the equation

$$a \cdot x = c$$

$$a \cdot x = c = a \cdot (a^{-1} \cdot c)$$

Therefore, this equation does have a solution. It is $a^{-1} \cdot c$.

Definition:

A group is a monoid $(M, \cdot)$ such that every element $a \in M$ is invertible.

Proposition:
$(S_n, \cdot)$ is a group, where $\cdot$ is composition.

Proof:

1. $S_n \times S_n \to S_n$ (closed) since composition of bijections is a bijection
2. $\mathrm{id} = (1)(2)\ldots(n)$
3. Associativity of composition
4. Existence of inverses
    - Follows from the theorem that a function has an inverse $\iff$ it's a bijection

$(S_n, \cdot)$ is called the **symmetric group**.

Note that each row and each column of the multiplication table of $(S_n, \cdot)$ have unique elements because of the cancellation property, since each $\sigma \in S_n$ is invertible.

Checking if something is a group:

1. Closure
    - $(\cdot)$ is a binary operation
2. Identity element
3. Associative
4. Existence of inverses

Examples of groups:

- $(\{(1)(2)(3)\}, \circ)$
- $(\{(1)(2)(3), (1,2)(3)\}, \circ)$

Lecture 6: More on Monoids and Groups, Lagrange's Theorem, Cyclic Groups

Summary:
We explore further properties of monoids and groups. We examine examples of monoids that are not groups, such as integers under multiplication and matrices under multiplication. We prove that the set of invertible elements in a monoid forms a group. We introduce subgroups and Lagrange's theorem, which states that the order of a subgroup divides the order of the group, when the group is finite. We define cyclic groups and prove that they are the smallest subgroups containing a given element.

Topics Covered: cyclic group, group, Lagrange's theorem, monoid

Recall that a group is a monoid where every element is invertible.

Examples of monoids (but not groups, since not every element is invertible):

- $(\mathbb{Z}, \cdot)$
- $(\mathcal{M}_n(\mathbb{R}), \cdot)$

Examples of groups:

- $(\{-1, 1\}, \cdot)$
- $(\{M \in \mathcal{M}_n(\mathbb{R}) : \det M \neq 0\}, \cdot)$
  - Note that this follows because $\det AB = \det A \cdot \det B$
  - This group is called $\mathrm{GL}_n(\mathbb{R})$
- Given a monoid $(M, \cdot)$, we denote M^x the set of invertible elements of M.

Proposition: Given a monoid $(M, \cdot)$, then $(M^\times, \cdot)$ is a group

Proof: We need to show the following things

1. Closure
   - $\forall a, b \in M^\times.\ a \cdot b \in M^\times$
2. $e \in M$ is invertible $\implies e \in M^\times$
3. Associativity
4. Every element is invertible in $M^\times$

Lemma:

$a, b \in M^\times$ where $(M, \cdot)$ is a monoid.

Then, $a \cdot b \in M^x$ and

$$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$$

Proof:

The inverse, if it exists, is unique.

$$(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = e$$
$$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = e$$

Definition:

Let $(G, \cdot)$ be a group. Let $H \subseteq G$. If $(H, \cdot)$ is a group, then we say it is a subgroup of G under the operation induced by G.

Lagrange's theorem:

If G is a finite group and H is a subgroup of G, then the cardinality of H divides the cardinality of G.

Proposition:

Let G be a group with identity element e, and $H \subseteq G$.

H is a subgroup of $G \iff G$ satisfies

1. $a, b \in H \implies ab \in H$
2. $e \in H$.
3. $a \in H \implies a^{-1} \in H$

$\implies$ **proof:**

Let G be a group and let $H \subseteq G$ be a subgroup of G.

Since H is a group, closure holds, which means the first condition has to hold.

Since H is a group, we know that H has an identity element $e' \in H \in G$.

Since e' is an identity element of H, we know that

$$e'e' = e' = e'e$$

We have that, in G

$$e'e' = e'e$$

So, by the cancellation property,

$$e' = e$$

Therefore, $e \in H$, so the second condition holds.

Since $a \in H$ and H is a subgroup, meaning it is a group, $\exists b \in H$ such that $ab = e = ba$. This is in H, therefore, this also holds in G.

Therefore, in G, we also have

$$aa^{-1} = a^{-1}a = e$$

Therefore, the third condition holds.

$$QED$$

$\impliedby$ **proof:**

Let G be a group with $H \subseteq G$ and H satisfies 1, 2, and 3.

We want to show that H is a subgroup of G.

For H to be a group we need closure by 1.

Need identity $\implies$ e is an identity in H

Associativity

Need inverses, a^{-1} is an inverse, so third holds.

$$QED$$

Note that for a group G, G itself is always a subgroup of G, and $(\{e\}, \cdot)$ is called the trivial subgroup.

Corollary: Let G be a group and $H \subseteq G$. Note that H is a subgroup of $G \iff H \neq \emptyset$ and $\forall a, b \in H.\ ab^{-1} \in H$.

$\implies$ **proof:**

Let H be a subgroup of G. Using proposition ii, we know that $e \in H \implies H \neq \emptyset$.

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

QED

$\impliedby$ **proof:**

$H \neq \emptyset$ and $\forall a, b \in H \implies ab^{-1} \in H$.

Since $H \neq \emptyset$, $\exists a \in G$ such that $a \in H \implies a, a^{-1} \in H \implies aa^{-1} \in H, \implies e \in H$.

$e, a \in H$

$e, a \in H \implies a^{-1} = ea^{-1} \in H$.

Corollary:

Let G be a group, let H be a finite nonempty subset of G.

Then, H is a subgroup of $G \iff \forall a, b \in H. ab \in H$.

$\implies$ proof is trivial

$\impliedby$ **proof:**

We know that

$$\forall a, b \in H \implies ab \in H$$

We also know that $H \neq \emptyset$ and $|H| < \infty$.

Let $b \in H$ be finite.

Then, we know that $b, b^2, b^3, \ldots$.

$$\implies m > n \in \mathbb{Z}_{\geq 0}.\ b^n = b^m$$
$$\implies e = b^{m-n}$$
$$\implies b^{-1} = b^{m-n-1}$$
$$\implies b^{-1} \in H$$

Definition:

Let G be a group with $a \in G$.

Define

$$\langle a \rangle = \{a^n \in G \mid n \in \mathbb{Z}\}$$

This is called the cyclic subgroup generated by a.

Moreover, a group H is called cyclic when $\exists a \in H$ such that $H = \langle a \rangle$.

Note that S_3 is not cyclic.

Proposition:
Let G be a group with $a \in G$.

1. $\langle a \rangle$ is a subgroup of G
2. if K is a subgroup of G and $a \in K$, then $\langle a \rangle \subseteq K$.

Proof:

1. Closure
   - $a^m \cdot a^n = a^{m+n}$

$$(a^n)^{-1} = (a^{-1})^n = a^{-n}$$

2. By closure

Lecture 7: Groups, Order, Equivalence Relations

Summary:
We begin by studying the order of elements in groups, defining both finite and infinite order and establishing properties about powers of elements. We prove that the order of an element equals the size of its cyclic subgroup. Building on this foundation, we introduce equivalence relations and their fundamental properties. We show that equivalence relations naturally partition sets into equivalence classes.

Topics Covered: equivalence relation, group, order

Proposition (last time):

Let G be a group and let $a \in G$. Then,

1. $\langle a \rangle$ is a group
2. If K is a subgroup of G and $a \in K$, then $\langle a \rangle \subseteq K$

Definition:

Let G be a group and let $a \in G$. If there exists a positive integer $n \in \mathbb{Z}^+$ such that $a^n = e$, then a has **finite order** and the smallest positive integer n such that $a^n = e$ is called the order of a. If there does not exist a positive integer $n \in \mathbb{Z}^+$ such that $a^n = e$, then a is said to have **infinite order**.

Example:

Consider the group $(\mathbb{Z}, +)$. In this group, the identity element is 0. In this group, any element other than 0 has infinite order.

Proposition:

Let G be a group and let $a \in G$. If a has infinite order, then

1. $k \neq m \implies a^k \neq a^m$
   - Suppose not. Then, we have that $a^{k-m} = e$, which contradicts that a has infinite order. Therefore, it must hold that $a^k \neq a^m$.
2. If a has finite order and $k \in \mathbb{Z}$, then $a^k = e \iff \sigma(a) \mid k$
   - This means $\sigma(a)$ divides k
3. If a has finite order $\sigma(a) = n$, then $\forall k, m \in \mathbb{Z}\ a^m = a^k \iff k \equiv m \pmod{n}$
   - Furthermore, $|\langle a \rangle| = \sigma(a)$

Lagrange's Theorem:

If H is a subgroup of a finite group G, then $|H| \mid |G|$.

In other words, if H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

Definition:

Let S be a set. A collection $\mathcal{P}$ of nonempty subsets of S is called a partition of S when each element of S belongs to exactly one set in $\mathcal{P}$.

For example

$$S = \{1, 2, \star, \circ, ?, !\}$$
$$= \{1\} \sqcup \{2, \circ\} \sqcup \{\star\} \sqcup \{?, !\}$$

Definition: Let S be a set. A subset $R \subseteq S \times S$ is an equivalence relation on S means

1. $\forall a \in S.\ (a, a) \in R$
   - Reflective

2. $\forall a, b \in S.\ (a, b) \in S \implies (b, a) \in S$
   - Symmetric
3. $\forall a, b, c \in S.\ (a, b), (b, c) \in S \implies (a, c) \in S$
   - Transitive

Equivalence class of $a \in S$: $[a] = \{x \in S \mid x \sim a\}$

Theorem: Let $\sim$ be an equivalence relation on S, Then, the distinct equivalence classes partition S into nonempty sets. Moreover, given any partition of S, there is an equivalence relation on S whose equivalence classes are the parts of the partition.

Example:

Let $f : S \to T$ be a function. Define $x_1, x_2 \in S$.

$$x_1 \sim_f x_2 \iff f(x_1) = f(x_2)$$

Claim: $\sim_f$ is an equivalence relation on S.

Example 2:

$\mathbb{Z}$, fix $n \in \mathbb{Z}_{\geq 0}$. $a \sim b \iff n \mid a - b$ is an equivalence relation.

Proof of theorem 1:

Note that $a \in [a]$, so none of the equivalence classes are empty. Moreover, $\forall a \in S$ appears in an equivalence class.

Suppose $a, b \in S$ and $[a] \cap [b] \neq \emptyset$. $c \in [a] \cap [b] \implies c \sin a$ and $c \sim b \implies a \sim b$.

$$x \in [a] \iff x \sim a$$

and we have $a \sim b \implies x \sim b \implies x[b].\ a \sim c$.

$$\implies [a] \subseteq [b]$$

Doing the same we get $[b] \subseteq [a]$.

$$\implies [a] = [b]$$

$$QED$$

Example:

$$H = \langle (1, 2) \rangle = \{\mathrm{id}, (1, 2)\} = H\ \mathrm{id}$$

Let $a \in G$

$$H\ a = \{h\ a \mid h \in H\}$$

$$H\ (1, 2) = H$$

$$H\ (1, 3) = \{(1, 3), (1, 3, 2)\}$$

$$H\ (1, 3, 2) = \{(1, 3, 2), (1, 3)\}$$

$$H\ (2, 3) = \{(2, 3), (1, 2, 3)\} = H\ (1, 2, 3)$$

Lemma:

Let H be a subgroup of G. For $a, b \in G$, define $a \sim b \iff ab^{-1} \in H$. Then, $\sim$ is an equivalence relation.

Proof:

1. Reflexive
   - $a \sim a \implies a^{-1} = e \in H$
2. Symmetric
   - $a \sim b \iff b \sim a$
3. Transitivity

- $a \sim b, b \sim c \implies a \sim c$

Lecture 8: Equivalence Relations, Lagrange's Theorem, Groups, Isomorphisms, Homomorphisms

Summary:
We continue our study of equivalence relations and groups. We prove Lagrange's theorem using cosets and equivalence relations. We use Lagrange's theorem to show that any group of prime order is cyclic. We introduce group isomorphisms and homomorphisms, proving that they preserve important group properties. We demonstrate that isomorphic groups have the same structure and prove that the order of elements is preserved under isomorphisms. We show that isomorphisms map identity elements to identity elements and that the inverse of an isomorphism is also an isomorphism.

Topics Covered: equivalence relation, group, homomorphism, isomorphism, Lagrange's theorem

Lemma: Let H be a subgroup of G. For any $a, b \in G$, define the relation $a \sim b \iff ab^{-1} \in H$. Then, $\sim$ is an equivalence relation.

Lagrange's theorem: Given a finite group G and subgroup H, the cardinality of H divides G.

Proof:

Recall that, given any element $a \in G$, we can define $H\ a \subseteq G$

$$Ha = \{ha \mid h \in H\}$$

Note that for $h, a \in G$, ha is the product $h \cdot a$ in H.

For example

$$S_3 = G$$
$$H = \langle (1,2) \rangle = \{e, (1,2)\} = He = H(1,2)$$
$$a = (1,2,3)$$
$$Ha = \{e(1,2,3), (1,2)(1,2,3)\}$$
$$= \{(1,2,3), (1)(2,3)\}$$

To prove claim 1, we will show that

1. $[a] \subseteq Ha$
2. $[a] \supseteq Ha$

We have

1. $x \in [a] : x \sim a \iff xa^{-1} \in H \iff ax^{-1}$
2. $x \in Ha \implies x = ha$ for some $h \in H : xa^{-1} = haa^{-1} = h \in H$

We need to prove that $x \sim a \iff xa^{-1} \in H$.

Claim 1: $[a] = Ha$

Claim 2: $|Ha| = |H|$, because of the cancellation property - $\forall a \in G.\ (\forall b, c \in G.\ ab = ac) \implies \forall b, c \in G.\ b = c$

Corollary:

Let G be a finite group of order n (this means $|G| = n$). Then,

1. $\forall a \in G.\ \sigma(a) \mid n$
2. $\forall a \in G.\ a^n = e$

Proof:

Let $a \in G$ and let $H = \langle a \rangle$ be the cyclic group generated by a. We showed last time that $|\langle a \rangle| = \sigma(a)$.

Thus, since $\langle a \rangle$ is a subgroup of $G \implies \sigma(a) \mid |G| = n$

1. $\forall k \in \mathbb{Z}.\ \left(a^{\sigma(a)}\right)^k = e$

Corollary:

Any group of prime order is cyclic.

Proof:

Let G be a group with prime order $|G| = p$. This means

$$\forall a \in G.\ \sigma(a) \mid p \implies \sigma(a) = 1 \text{ or } \sigma(a) = p$$

Only e is of order 1 means

$$\exists a \in G.\ \sigma(a) = p \implies |\langle a \rangle| = p, \langle a \rangle \subseteq G \implies G = \langle a \rangle$$

$$QED$$

$$G = \{e, a, a^2, a^3, a^4, a^5, a^6\}$$

$$a^7 = e$$

- $\sigma(a \cdot 2) = 7$
- $\sigma(a^3) = 7$
- $\sigma(a^4) = 7$
- $\sigma(a^5) = 7$
- $\sigma(a^6) = 7$

This is because 7 is prime. Therefore, every element in G except for e is a generator of G.

Definition:

Let G_1 and G_2 be groups and let $\phi : G_1 \to G_2$ be a function. ϕ is a group isomorphism means

1. ϕ is a bijection
2. $\phi(ab) = \phi(a)\phi(b)$
   - On the left, multiplication is in G_1
   - On the right, multiplication is in G_2

When such a ϕ exists, we say that G_1 is isomorphic to G_2 and we write $G_1 \cong G_2$. This essentially means the groups G_1 and G_2 are the same group with the same structure, but with differently-named elements.

Example:

$$G = \langle a \rangle,\ \ \sigma(a) = 7$$

$$\phi : G \to \langle (1, 2, 3, 4, 5, 6, 7) \rangle$$

$$\phi(a) = (1, 2, 3, 4, 5, 6, 7)$$

$$\phi(a)^2 = (\phi(a))^2$$

Here, ϕ is a group isomorphism.

Definition:

Let G_1, G_2 be groups. A homomorphism is a function $\phi : G_1 \to G_2$ such that $\forall a, b \in G_1.\ \phi(ab) = \phi(a)\phi(b)$.

$\cdot$	e	a	a^2	b	ab	a^2b
e	$(1)(2)(3)$	$(1, 2, 3)$	$(1, 3, 2)$	$(1, 2)$	$(1, 3)$	$(2, 3)$
a						

$\cdot$	e	a	a^2	b	ab	a^2b
a^2						
b						
ab						
a^2b						

This creates an isomorphism.

Proposition:

Let $\phi : G_1 \to G_2$ be a group isomorphism. Then,

1. $\forall a \in G.\ \sigma_{G_1}(a) = \sigma_{G_2}(\phi(a))$
2. If G_1 is abelian (commutative), so is G_2
3. If G_1 is cyclic, then G_2 is cyclic

Note that for an isomorphism $\phi : G_1 \to G_2$ with $e_1 \in G_1$ and $e_2 \in G_2$ identity elements, we have $\phi(e_1) = e_2$. This is shown by verifying that $\phi(e_1) \in G_2$ is an identity element of G_2. Then, by the uniqueness of identity elements, we know that $e_2 = \phi(e_1)$, so they are indeed the same element.

Since ϕ is an isomorphism, there exists an inverse isomorphism that maps $\phi(a) \mapsto a$.

Therefore,

$$\sigma(\phi(a)) \mid \sigma(a)$$

and

$$\sigma(a) \mid \sigma(\phi(a))$$

Therefore,

$$\sigma(a) = \sigma(\phi(a))$$

Lecture 9: Cayley's Theorem, Group Action, Orbit, Stabilizer

Summary:
We prove Cayley's theorem, which states that every group is isomorphic to a permutation group. We introduce group actions and show how they provide a way for groups to act on sets. We define orbits and stabilizers, proving that orbits partition the set and that stabilizers are subgroups. We demonstrate how group actions can be used to study symmetries, using the example of a necklace with beads. We prove that the size of an orbit times the size of its stabilizer equals the order of the group, when the group is finite.

Topics Covered: Cayley's theorem, group action, orbit, stabilizer

Definition:

A subgroup of the symmetric group $\mathrm{Sym}(S)$ on a set S is called a permutation group.

Example:

$$S_3 \supseteq \langle (1,2,3) \rangle$$

Theorem (Cayley):

Every group is isomorphic to a permutation group.

Proof:

Let G be an arbitrary group. We want an isomorphism from G to some permutation group.

$$\phi : G \to \mathrm{Sym}(G)$$
$$a \mapsto \lambda_a \in \mathrm{Sym}(G)$$

Note that $\lambda_a : G \to G$ is a bijection, due to the invertibility of $a \in G$.

Given any $x \in G$, we need to define $\lambda_a(x)$.

Define $\lambda_a : G \to G$ as

$$\lambda_a(x) = a \cdot x$$

Note that λ_a is a bijection

- λ_a is an injection because
  - $ax_1 = ax_2 \implies x_1 = x_2$ (cancellation lemma)
- λ_a is a surjection because
  - $\forall b \in G.\ ax = b \iff x = a^{-1}b$

Let

$$G_\lambda = \phi(G) \subseteq \mathrm{Sym}(G)$$

We want to verify that

1. G_λ is a subgroup of G
2. $\phi : G \to G_\lambda$ as defined above is a group isomorphism

Want G_λ to be a subgroup of $\mathrm{Sym}(G)$

$$e \in G$$
$$\lambda_e : G \to G$$
$$g \mapsto g$$

Therefore, $\lambda_e \in G_\lambda$ is the identity

- We also need $\lambda_a \lambda_b = \lambda_{ab}$
  - $a(bx) = (ab)x \implies \forall \lambda_a, \lambda_b \implies \lambda_a \lambda_b \in G_\lambda$

$$(\lambda_a)^{-1} = \lambda_{a^{-1}}$$

Group actions

Suppose we have a necklace with 9 beads. We want to describe the permutations of the necklace as a group.

We can generate the group as follows:

$$\left\langle \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 1 \end{pmatrix} \right\rangle$$

Definition:

Let G be a group with identity e, and let X be a set. We say that G acts on X if $\forall g \in G$ there exists a map $g : X \to X$ such that $\forall x \in X$

1. $\forall h, g \in G.\ h(g(x)) = (hg)(x)$
2. $e(x) = x$

Lemma: In the above setup, $\forall g \in G$ the map $g : X \to X$ is a bijection.

Proof:

To prove that g is a bijection, it suffices to show that it has an inverse.

Example:

$$(1,2,3,4) \in S_4$$

$$G = \langle (1,2,3,4) \rangle = \{e, (1,2,3,4), (1,3)(2,4), (1,4,3,2)\}$$

G acts on $[4]$.

$$X = \{\{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}$$

We claim that $g^{-1} : X \to X$

$$g^{-1}(g(x)) = (g^{-1}g)(x) = e(x) = x$$

and

$$g(g^{-1}(x)) = g^{-1}(g(x))$$

Definition:

If G acts on X, then the orbit of $x \in X$ is

$$\mathcal{O}_x = \{g(x) \ : \ g \in G\} \subseteq X$$

$$\mathcal{O}_{\{1,2\}} = \{e\ \{1,2\}, (1,2,3,4)\ \{1,2\}, (1,3)(24)\ \{1,2\}, (1,4,3,2)\ \{1,2\}\}$$

Note that

$$X = \mathcal{O}_{\{1,2\}} \sqcup \mathcal{O}_{\{1,3\}}$$

Definition:

If G acts on X, then the stabilizer of $x \in X$ is

$$G_x = \{g \in G \ : \ gx = x\} \subseteq G$$

Note that the stabilizer G_x is a subgroup of G.

Lecture 10: Group Action, Burnside's Lemma

Summary:
We continue our study of group actions and apply them to counting problems. We prove that orbits partition the set and that stabilizers are subgroups. We introduce fixed points and prove Burnside's lemma, which provides a formula for counting the number of distinct orbits in a group action. We demonstrate how to use Burnside's lemma to solve counting problems involving symmetries, such as counting distinct colorings of objects under rotational symmetry.

Topics Covered: Burnside's lemma, coset, fixed point set, group action, group action orbit, group action stabilizer

Group action:

Let G be a group with $e \in G$ identity. Let X be a set. We say that group G acts on X when $\forall g \in G$ we have a map $g : X \to X$ such that $\forall x \in X$

1. $h(g(x)) = (hg)(x)$
2. $e(x) = x$

Note that we use g to denote both the group element $g \in G$ and the corresponding function $g : X \to X$.

Permutation groups (subgroups of S_n) naturally act on the numbers $[n] = \{1, 2, \ldots, n\}$ in the obvious way; by mapping each number to its image under the permutation. For example,

$$G = \langle (1,4,3,2) \rangle = \langle (1,2,3,4) \rangle \leq S_4$$

For example

$$\langle (1,4,3,2) \rangle = \langle (1,2,3,4) \rangle \subseteq S_4$$
$$X = \{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}\}$$

We define

$$g\{a,b\} = \{ga, gb\}$$

Orbit:

Let $x \in X$. Then, we have

$$\mathcal{O}_x = \{g(x) \in X \ : \ g \in G\}$$

Stabilizer:

$$G_x = \{g \in G \ : \ g(x) = x\}$$
$$\mathcal{O}_{\{1,2\}} = \{e\{1,2\}, (1,2,3,4)\{1,2\}, (1,3)\{1,2\}, (1,4,3,2)\{1,2\}\}$$
$$= \{\{1,2\},\{2,3\},\{3,4\},\{4,1\}\}$$

We notice that

$$|\mathcal{O}_{\{1,2\}}| \cdot |G_{\{1,2\}}| = |\mathcal{O}_{\{1,3\}}| \cdot |G_{\{1,3\}}| = |G|$$

Lemma 1:

Let G act on X

1. The distinct orbits partition X
2. Let $x \in X$. Then, G_x is a subgroup of G
3. If G and X are finite, then for $x \in X$, we have $|\mathcal{O}_x| \cdot |G_x| = |G|$

Proof of 1:

Let $\mathcal{O}^{(1)}, \ldots . \mathcal{O}^{(k)}$ be all the distinct orbits.

Note that by definition,

$$\mathcal{O}^{(i)} \subseteq X \implies \bigcup_{i=1}^{k} \mathcal{O}^{(i)} \subseteq X$$

Moreover, $\forall x \in X$,

$$x \in \mathcal{O}_x \implies X \subseteq \bigcup_{i=1}^{k} \mathcal{O}^{(i)}$$

$$\implies X = \bigcup_{i=1}^{k} \mathcal{O}^{(i)}$$

To show that the orbits partition, we must show that $\mathcal{O}^{(1)}, \ldots, \mathcal{O}^{(k)}$ are disjoint. Equivalently, we will show that

$$\mathcal{O}_x \cap \mathcal{O}_y \neq \emptyset \implies \mathcal{O}_x = \mathcal{O}_y$$

We'll show that $\mathcal{O}_x \subseteq \mathcal{O}_y$, and the containment $\mathcal{O}_y \subseteq \mathcal{O}_x$ is similar.

$$z \in \mathcal{O}_x \implies \exists g \in G.\ g(x) = z$$

$$u \in \mathcal{O}_x \cap \mathcal{O}_y \implies \exists h, k \in G.\ u = hx \text{ and } u = ky$$

Claim:

$$u = hx \iff x = h^{-1}u$$

$$x = ex = (h^{-1}h)(x) = h^{-1}(h(x)) = h^{-1}(u)$$

$$z = gx = g(h^{-1}u) = g(h^{1}ky) = (gh^{-1}k)y \in \mathcal{O}_y$$

Proof of 2:

We want to show that $\forall x \in X.\ \ G_x$ is a subgroup of G.

Note that $e \in G_x$ because $e(x) = e$. So, e is in the stabilizer of x.

We know that

$$g \in G_x \iff gx = x$$

Note that

$$gx = x \iff g^{-1}x = x$$

Therefore, G_x is closed under inverses.

Now, we want to show that

$$\forall g, h \in G_x.\ gh \in G_x$$

Let $g, h \in G_x$. Then,

$$(gh)(x) = g(h(x)) = g(x) = x$$

$$\implies (gh) = x$$

$$\implies gh \in G_x$$

Therefore, G_x is closed under multiplication [composition].

Therefore, G_x is a subgroup of G.

$$QED$$

Theorem (Lagrange):

Let G be a finite group and H be a subgroup of G. Then, we have that $|H|$ divides $|G|$.

Idea: For each $a \in G$, we have

$$Ha = \{ha \ : \ h \in H\}$$
$$|Ha| = |H|$$

The Has partition H

Equivalently, we have

$$aH = \{ah \ : \ h \in H\}$$
$$|aH| = |H|$$

The aHs also partition H.

This is the start to the proof of Lagrange's theorem.

G: the left cosets of G_x partition G (as we've written the proof of Lagrange's theorem)

3 claims that the number of distinct left cosets is $\mathcal{O}_x$

$$\mathcal{O}_{\{1,3\}} = \{\{1,3\},\{2,4\}\}$$
$$G_{\{1,3\}} = \{e,(1,3),(2,4)\} = eG_{\{1,3\}}$$
$$G = \langle (1,2,3,4) \rangle$$
$$(1,2,3,4)G_{\{1,3\}} = \{(1,2,3,4),(1,4,3,2)\}$$

We will find a bijection

$$f : \{aG_x \ : \ a \in G\} \to \mathcal{O}_x$$

The left side of the function is the set of left cosets of $\mathcal{O}_x$

$$f\left(gG_x\right) = gx \in \mathcal{O}_x$$

We want to show that this function is well-defined, which means

$$gG_x = hG_x \implies gx = hx$$

> Fill this in later

We will show that f is a bijection by showing that it is invertible.

$$f^{-1} : \mathcal{O}_x \to \{aG_x \ : \ a \in G\}$$
$$gx \mapsto gG_x$$

We need to show that f^{-1} is well-defined, which we show by verifying

$$gx = hx \implies gG_x = hG_x$$

Suppose that $gx = hx$. Then,

$$\implies x = \left(g^{-1}h\right)x$$
$$\implies g^{-1}h \in G_x$$
$$\iff gG_x = hG_x$$
$$QED$$

Definition:

If G acts on X, then the fixed point set of $g \in G$ is

$$X^g = \{x \in X \ : \ gx = x\} \subseteq X$$

Example:

$$X^{(1,3)} = X^{(2,4)} = \{\{1,3\},\{2,4\}\}$$

Burnside's lemma:

Let G act on X with G, X finite.

Then,

$$\text{number of orbits of a group action} = \frac{1}{|G|}\sum_{g \in G} |X^g|$$

Lecture 10.5: Counting

Summary:
We study fundamental counting principles, permutations, and subsets. We establish that n elements have n! permutations and 2^n subsets, and introduce binomial coefficients and the binomial theorem.

Topics Covered: addition principle, binomial coefficient, binomial theorem, counting subset, multiplication principle, permutation

Two basic counting principles

- Multiplication principle
  - If there are a ways of performing task A and b ways of performing task B, then, there are ab ways of performing A then B.
- Addition principle
  - If there are a ways of performing task A and b ways of performing task B, then, there are $a+b$ ways of performing A or B

Permutations

$$S_n = \{\text{permutations of } [n]\}$$

$$|S_n| = n!$$

Subsets

$$2^S = \{\text{Subsets of } S\}$$

Note that

$$|2^S| = 2^{|S|}$$

Note that there is a bijection

$$2^S \to \{0,1\}^{|S|}$$

Binomial coefficient

$$\binom{n}{k} := \frac{n!}{k!(n-k)!}$$

$\binom{n}{k}$ is the number of ways we can pick a k-subset from a set of size n.

Generating functions

The multivariate generating function for subsets of $[n]$ is

$$\sum_{A \subseteq [n]} \prod_{i \in A} x_i = (1+x_1)(1+x_2)\dots(1+x_n)$$

Plug in $x_1 = x_2 = \dots = x_n = x$ to get

$$\sum_{A \subseteq [n]} x^{|A|} = (1+x)^n$$

Binomial theorem:

$$\sum_{i=0}^{n} \binom{n}{k} x^k = (1+x)^n$$

Lecture 11: Burnside's Lemma, Fixed Point Set, Number Theory

Summary:
We examine fixed point sets and prove Burnside's lemma, applying it to count distinct colorings of objects under symmetries. We then introduce fundamental concepts of divisibility, including greatest common divisors and least common multiples, establishing the linear combination lemma for integers.

Topics Covered: Burnside's lemma, common divisor, common multiple, fixed point lemma for permutation action, fixed point set, greatest common divisor, least common multiple, linear combination lemma for integers

Fixed point set:

Let G be a group action on X and $g \in G$. Then, we have

$$X^g = \{x \in X.\ g(x) = x\}$$

X^g is just the set of all fixed points of g.

Burnside's Lemma:

Let G act on X with G and X finite. Then, we have

$$\text{number of orbits} = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

Consider the collection of functions $f : X \to Y$ from X to some set of colors Y. We have a group action of G on this collection by

$$(gf)(x) = (f \circ g^{-1})(x)$$

Lemma:

Let G act on X, and Y is any other set with G, X, Y finite. Let $g \in G$. Let $c(g)$ be the number of cycles of G. Then, we have

$$|(Y^X)^g| = |Y|^{c(g)}$$

- Y^X is the set of functions $X \to Y$
- $(Y^X)^g$ is the set of functions fixed by g
- $c(g)$ is the number of disjoint cycles required to represent g as a product of disjoint cycles. Note that $g : X \to X$ is a bijective, so it is a permutation. $g \in \text{Sym}(X)$.

> The key insights here is that g can be expressed as a product of disjoint cycles. So,

G acts on Y^X naturally. We have

$$(gf)(x) = f(g^{-1}(x))$$

Above, we have

- $g : X \to X$
- $f : X \to Y$

We define it in the above way because, otherwise, the composition wouldn't work as desired in a group action.

Example:

Suppose we are interested in counting the number of necklaces with four beads up to rotation, where each bead is black or white. Number the beads 1, 2, 3, 4. We can think of ordered colorings of the beads as functions

$$f : [4] \to \{B, W\}^4$$

The group $G = \langle (1, 2, 3, 4) \rangle$ acts in the obvious way on $X = [4]$, so it also acts on the set of functions $f : [4] \to \{B, W\}^4$

Distinct colorings (up to rotation) correspond precisely to orbits of $\{B, W\}^4$ under this group action.

Thus, the number of distinct necklaces (up to rotation) is computed by Burnside's lemma:

$$\text{number of orbits} = \frac{1}{|G|} \sum_{g \in G} |(Y^X)^g|$$

$$\langle (1,2,3,4) \rangle = \{(1)(2)(3)(4), (1,2,3,4), (1,3)(2,4), (1,4,3,2)\}$$

Compute the following quantities

g	$c(g)$	$\|(Y^X)^g\| = \|Y\|^{c(g)}$
$(1)(2)(3)(4)$	4	2^4
$(1,2,3,4)$	1	2^1
$(1,3)(2,4)$	2	2^2
$(1,4,3,2)$	1	2^1

For a permutation g with $c(g)$ cycles, there are $2^{c(g)}$ fixed points. This is because $|Y| = 2$.

Therefore, the number of orbits is

$$\text{number of orbits} = \frac{1}{4}(2^4 + 2^1 + 2^2 + 2^1) = 6$$

The orbits are

- `BBBB`
- `BBBW`
- `BBWW`
- `BWBW`
- `BWWW`
- `WWWW`

and their rotations.

Example:

Suppose we want to color the faces of a cube from a set of r colors. It has ^ faces, label them

- 1 - top
- 2 - front
- 3 - right
- 4 - back
- 5 - left
- 6 - bottom

Let us say colors of the faces are equivalent if they can be achieved by rotation. There are three types of rotations:

- About an axis perpendicular to opposite faces, with an angle of rotation in $\{0, 90, 180, 270\}$
- About an axis perpendicular to opposite edges, with angle of rotation in $\{0, 180\}$
- About an axis passing through opposite vertices, with an angle of rotation in $\{0, 120, 240\}$

Now, we want to know how many cycles are in each of these rotations. They are as follows:

Type of rotation	# of such elements in G	Example $g \in G$	$c(g)$	$\|(Y^X)^g\|$
Identity	1	$(1)(2)(3)(4)(5)(6)$	6	r^6

Type of rotation	# of such elements in G	Example $g \in G$	$c(g)$	$\|(Y^X)^g\|$
Face rotation $\pm$ 90	$3 \cdot 2$	$(1)(6)(2,3,4,5)$	3	r^3
Face rotation $\pm$ 180	$3 \cdot 1$	$(1)(6)(2,4)(3,5)$	4	r^4
Edge rotation $\pm$ 180	$6 \cdot 1$	$(1,4)(2,6)(3,5)$	3	r^3
Vertex rotation $\pm$ 120	$4 \cdot 2$	$(1,2,5)(3,6,4)$	2	r^2

By Burnside's lemma, we have
{

$$\text{number of distinct colorings} = \frac{1}{4}(r^6 + 6r^3 + 3r^4 + 6r^3 + 8r^2) = \frac{r^6 + 3r^4 + 12r^3 + 8r^2}{24}$$

Cryptography and number theory

Definition 5:

Let $a, b \in \mathbb{Z}$. Then, we have

1. If $c \mid a$ and $c \mid b$, then we say that c is a common divisor of a and b. Among all the common divisors of a, b, there is a largest one. We call this the greatest common divisor, and denote it $\gcd(a, b)$.
2. If $a \mid c$ and $b \mid c$, then we say that c is a common multiple of a and b. Among all the common multiples of a and b, there is a smallest one. We call this the least common multiple and denote it $\operatorname{lcm}(a, b)$.

Lemma:

Suppose that $a, b, c \in \mathbb{Z}$. If $c \mid a$ and $c \mid b$, then

$$c \mid xa + yb$$

for any $x, y \in \mathbb{Z}$.

In particular,

$$\forall x, y \in \mathbb{Z}.\ \ \gcd(a, b) \mid xa + yb$$

Proof:

We have

$$c \mid a \implies a = qc, q \in \mathbb{Z}$$
$$c \mid b \implies b = q', c, q' \in \mathbb{Z}$$

Thus,

$$xa + yb = xqc + yq'c = c(xq + yq')$$

So, $c \mid xa + yb$ as claimed. Take $c = \gcd(a, b)$ to get the final claim.

$$\text{QED}$$

Lecture 12: Euclid's Lemma, Euclidean Algorithm, Be'zout's Theorem

Summary:
We introduce the Euclidean algorithm for finding greatest common divisors and prove Be'zout's theorem, which establishes that the gcd of two integers can be expressed as a linear combination of those integers. We examine Euclid's lemma and its applications to prime numbers, proving that there are infinitely many primes.

Topics Covered: Be'zout's theorem, composite number, Euclidean algorithm, Euclid's lemma, greatest common divisor, prime number

Lemma:

Let $a, b, c \in \mathbb{Z}$. Note that

$$c \mid a \wedge c \mid b \implies c \mid xa + yb$$

In particular,

$$\gcd(a, b) \mid xa + yb$$

Lemma:

Let $a, b \in \mathbb{Z}$. Let $d = \gcd(a, b)$

$$\implies a' = \frac{a}{d},\ b' = \frac{b}{d}$$
$$\implies \gcd(a', b') = 1$$

Euclidean Algorithm:

The Euclidian algorithm is used for finding the gcd of integers $a, b \in \mathbb{Z}$.

1. Replace the largest of the two numbers by their difference, keep the smaller
2. Repeat until we get a 0 in one of the entires
3. The last nonzero integer is the gcd

Example:

- $(56, 20)$
- $(36, 20)$
- $(16, 20)$
- $(16, 4)$
- $(12, 4)$
- $(8, 4)$
- $(4, 4)$
- $(4, 0)$

Therefore,

$$\gcd(56, 20) = 4$$

Lemma:

Let $a, b \in \mathbb{Z}$. We have

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

Proof:

We will show that the common divisors of a, b are the same as the common divisors $a - b, b$.

If we have a common divisor c of a and b, we know that

1. $c \mid a$
2. $c \mid b$

By lemma 1, we know that

$$c \mid a - b$$

This is because $a - b$ is an integer linear combination of a and b.

In particular, c is a common divisor of $a - b$ and b.

$$d \mid a - b \ \wedge \ d \mid b \implies 1 \cdot (a - b) + 1 \cdot b = a, d \mid . b$$

$$\text{QED}$$

Theorem:

The Euclidean algorithm terminates and yields the gcd of the two integers we started with.

Proof:

Looking at the long form of the algorithm, in each step, we preserve the gcd of the numbers, so, as long as we terminate, we get the gcd.

It terminates because in short form the smaller number between the two is strictly decreasing at each step, so we must reach 0.

Theorem - Be'zout's Theorem:

Let $a, b \in \mathbb{Z}$ and let $d = \gcd(a, b)$ such that $\exists \alpha, \beta \in \mathbb{Z}$ such that $d = \alpha a + \beta b$.

There are infinitely many possible $\alpha, \beta \in \mathbb{Z}$ satisfying the above property.

Proof:

For $a \geq b$, we have

$$\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a - b \\ b \end{pmatrix}$$

For $a \leq b$, we have

$$\begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ b - a \end{pmatrix}$$

Thus, there exists a matrix

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

such that

$$\begin{pmatrix} \gcd(a, b) \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$\text{QED}$$

Corollary:

Let $a, b \in \mathbb{Z}$ with $c \mid a$ and $c \, b$. Then, we have

$$c \mid \gcd(a, b)$$

Corollary - Euclid's Lemma:

Let $a, b, c \in \mathbb{Z}$ with $\gcd(b, c) = 1$ and $c \mid ab \implies abc \mid a$

Proof:

By Be'zout's theorem, we know that

$$1 = \beta b + \gamma c, \beta, \gamma \in \mathbb{Z}$$

Hence, we have that

$$a = \beta ab + \gamma ac$$

- $c \mid ab$ (hypothesis)
- $c \mid ac \implies$ c divides any integer linear combination of ab and ac

$\implies$ by $a = \beta ab + \gamma ac$, we have that $c \mid a$.

$$\text{QED}$$

Our goal is to simultaneously with converging of the Euclidean Algorithm, also calculate (α, β).

Definition:

Let p be a positive integer. p is prime means:

1. $p \neq 1$
2. The only positive divisors of p are 1 and p

A positive integer n is composite if

1. $n \neq 1$
2. n has at least one divisor other than 1 and n

All positives (besides 1) are partitioned into primes and composites.

Lemma:

Let $n \in \mathbb{Z}^+$. Then, $\exists p$ prime such that $p \mid n$.

Proof:

We prove the lemma by induction on n.

Base case: $n = 2$. The statement holds with $p = 2$, since 2 is prime.

Inductive step: Consider $n \in \mathbb{Z}^+$.

- In the case that n is prime, it divides itself
- In the case that n is composite, $\exists k,\ 1 < k < n, k \mid n$. By the inductive hypothesis, we have $\exists p$ prime such that $p \mid k \implies p \mid n$.

Theorem (Euclid):

There exist infinitely many primes.

Proof:

Suppose otherwise. Let $p_1, \ldots, p_k$ be all of the primes.

$$n = \prod_{i=1}^{k} p_i \ + 1 > 1 \implies \exists p \text{ prime }.\ p \mid \prod_{i=1}^{k} p_i + 1 = n$$

Also, $p \mid \prod_{i=1}^{k} p_i + 1$, since all of them are primes.

Therefore,

$$p \mid 1 \cdot \left(\prod_{i=1}^{k} p_i + 1 \right) + (-1) \cdot \left(\prod_{i=1}^{k} p_i \right) \implies p = 1 \text{ (contradiction)}$$

Therefore, there are infinitely many primes.

QED

Lecture 13: Linear Diophantine Equations

Summary:
We study linear Diophantine equations and their solutions. We examine Euclid's lemma and its role in understanding divisibility properties.

Topics Covered: fundamental theorem of arithmetic, greatest common divisor, linear diophantine equation

Lemma:

Let p be prime and let $b, c \in \mathbb{Z}$. If $p \mid bc$ then $p \mid b$ or $p \mid c$.

> Is a prime number necessarily positive?

Example:

$$5 \mid 100 = 4 \cdot 25$$
$$\implies 5 \mid 4 \ \vee \ 5 \mid 25$$

Euclid's lemma:

Let $a, b, c \in \mathbb{Z}$ with $\gcd(b, c) = 1$. Then

$$c \mid ab \implies c \mid a$$

Example:

Proof:

$$d = \gcd(p, b) \implies d \mid p \ \wedge \ d \mid b$$

Case 1:

$$d = p \implies p \mid b$$

Case 2:

$$d = 1$$

Apply Euclid's lemma to $b, c, p \implies p \mid c$

Theorem - Fundamental theorem of arithmetic:

Let $n \in \mathbb{Z}$ with $n > 1$.

1. There exists primes $p_1, \ldots, p_r$ such that $n = p_1 \cdot \ldots \cdot p_r$.
2. If $q_1, \ldots, q_s$ are primes such that $n = q_1 \cdot \ldots \cdot q_s$, then $p_1, \ldots, p_r$ is a rearrangement of $q_1, \ldots, q_s$.

Proof:

By strong induction on n.

Base case:

$n = 2, r = 1, p_1 = 2$.

Inductive hypothesis:

$\forall k \in \mathbb{Z}$, k has a prime factorization.

Inductive step: We have to prove that n has a prime factorization.

Case 1: If n is prime, $r = 1$ and $p_1 = n$.

Case 2: If n is composite, then $\exists$ prime p such that

$$n = pq$$

$$1 < pq < n$$

By the inductive hypothesis, we know that both p and q have prime factorizations.

Proof that prime factorizations are unique:

Suppose that

$$n = p_1 \cdot \ldots \cdot p_r . = q_1 \cdot \ldots \cdot q_s$$

Take arbitrary prime p. If $p \notin \{p_1, \ldots, p_r, q_1, \ldots, q_s\}$, do nothing, If $p \in \{p_1, \ldots, p_r, q_1, \ldots, q_s\}$, then assume WLOG that $p = p_i$ with $i \in [r]$.

$$p \mid n = q_1 \cdot \ldots \cdot q_s$$

$$p \mid q_1 \cdot \ldots \cdot q_s = q \cdot (q_2 \cdot \ldots \cdot q_s)$$

$$\implies p \mid q_1 \ \vee \ p \mid q_2 \cdot \ldots \cdot q_s$$

$$\implies \ldots \implies p \mid q_j$$

for some $j \in [s] \implies q_j = p$.

Now, cross out on both sides

$$p_1 p_2 \ldots p_{i-1} p_{i+1} \ldots p_r = q_1 \ldots q_{j-1} q_{j+1} q_s$$

and repeat.

$$\text{QED}$$

Proposition:

Let $a, b \in \mathbb{Z} > 0$. By the fundamental theorem of arithmetic, we have

$$a = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$$

$$b = p_1^{\beta_1} \ldots p_r^{\beta_r}$$

1. $a = b \iff \alpha_i = \beta_i \ \forall i \in [r]$
2. $a \mid b \iff \alpha_I \leq \beta_i \ \forall i \in [r]$
3. $\gcd(a, b) = \prod_{i=1}^{r} p_i^{\min(\alpha_i, \beta_i)}$

Lemma:

$\sqrt{2}$ is irrational.

Proof:

Suppose otherwise. Suppose that $\exists a, b \in \mathbb{Z}$ such that

$$\sqrt{2} = \frac{a}{b}$$

$$\implies 2b^2 = a^2$$

$$a = 2^{\alpha_1} 3^{\alpha_2} \ldots .$$

$$b = 2^{\beta_1} 3^{\beta_2} \ldots .$$

$$\implies 2^{\beta_1 + 1} = 2^{\alpha_1}$$

This is a contradiction.

$$\text{QED}$$

Linear equations:

$$ax + by = e$$

$$a, b, c \in \mathbb{Z}$$

We start with $e = 0$.

$$(a, b) \cdot (x, y) = 0$$

Proposition

The integer solutions of $ax + by = 0$ for $a, b \in \mathbb{Z}$ are

$$x = b'k$$

$$y = a'k$$

where $k \in \mathbb{Z}$ is arbitrary,

$$a' = \frac{a}{\gcd(a, b)}$$

$$b' = \frac{b}{\gcd(a, b)}$$

We must show that this is a solution for all $k \in \mathbb{Z}$, and, conversely, all solutions are of this form. Denote

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

To see that this is a solution, note that

$$a\frac{b}{d}k + b\left(-\frac{a}{d}\right)k = \frac{abk}{d} - \frac{abk}{d} = 0$$

Now, we prove that all integer solutions of $ax + by = 0$ are of the form above.

$$ax + by = 0$$

Divide LHS and RHS by d.

$$a'x + b'y = 0$$

$$a'x = b'(-y)$$

$$b' \mid a'x$$

Recall that $\gcd(a', b') = 1$. Therefore,

$$b' \mid x \implies x = b'k$$

for some $k \in \mathbb{Z}$.

$$\implies ab'k + b'y = 0$$

$$\implies y = -a'k$$

$$\text{QED}$$

Example:

Using this method, we want to find all integer solutions of

$$56x + 20y = 0$$

First, we compute $\gcd(56, 20)$. In this case, we have

$$\gcd(56, 20) = 4$$

$$a' = \frac{56}{4} = 14$$

$$a' = \frac{56}{4} = 14$$

$$b' = \frac{20}{4} = 5$$

$$x = 5k,\ y = -14k\ \ \forall k \in \mathbb{Z}$$

Lecture 14: Solutions to Linear Diophantine Equations, Modular Congruence

Summary:
We examine solutions to linear Diophantine equations, establishing conditions for their existence and methods for finding them. We introduce modular congruence and prove that the integers modulo m form a group under addition and a monoid under multiplication.

Topics Covered: Be'zout's theorem, Euclidean algorithm, greatest common divisor, group, integers modulo m, linear equation, linear equation solution lemma, modular congruence, monoid

Let

$$ax + by = e$$

with $a, b, e \in \mathbb{Z}$ be a linear equation.

We are looking for integral solutions $x, y \in \mathbb{Z}$.

Example:

$$2x + 4y = 3$$

Note that this doesn't have any integral solutions because the LHS is always even and the RHS is always odd.

Lemma:

Let $ax + by = e$ be a linear equation with $a, b, e \in \mathbb{Z}$, and $x, y \in \mathbb{Z}$ are variables.

Let $d = \gcd(a, b)$.

1. If $d \not| e$ then $ax + by = e$ has no integer solutions
2. If $d \mid e$ then $ax + by = e$ has infinitely many solutions

Proof of 1:

Suppose that $d \not| e$. We want to show that $ax + by = e$ has no integer solutions.

Suppose, for contradiction, that $ax + by = e$ has an integer solution (x, y).

We proved that any common divisor of a and b [in particular, $d = \gcd(a, b)$] divides any integral linear combination of a and b. In particular, $ax + by$ is a linear combination of a and b.

Therefore, we have that

$$d \mid ax + by$$

Recall that $ax + by = e$, so, we have that

$$d \mid e$$

which contradicts our initial assumption that $d \not| e$.

Therefore, we conclude that $ax + by = e$ has no integer solutions.

$$\text{QED}$$

Proof of 2:

Suppose that $d \mid e$. Then, Be'zout's theorem tells us that

$$d = \alpha a + \beta b$$

for some $\alpha, \beta \in \mathbb{Z}$.

Since $d \mid e$, we know that $e = qd$ for some $q \in \mathbb{Z}$.

Multiply by q. Then, we have

$$e = qd = (q\alpha)a + (q\beta)b$$
$$\implies x_0 = q\alpha, \;\; y_0 = q\beta$$

are integral solutions of $ax + by = e$

Recall that the associated homogeneous linear equation $ax + by = 0$ has infinitely many solutions

$$S_{\text{homogenous}} = \{(x', y') \in \mathbb{Z}^2 \;:\; ax' + by' = 0\}$$
$$|S_{\text{homogenous}}| = \infty$$

Then, we have infinitely many solutions to the non-homogeneous equation

$$S_{\text{non-homogenous}} = \{(x_0 + x', y_0 + y') \;:\; (x', y') \in S_{\text{homogenous}}\}$$
$$|S_{\text{non-homogenous}}| = \infty$$
$$\text{QED}$$

Summary of results:

- If $d \not\mid e$ then there are no integral solutions
- If $d \mid e$, then there are infinitely many integral solutions. We find **all of them** as follows:
  - Find all solutions (x', y') to the homogeneous equation $ax + by = 0$
  - Find one solution (x_0, y_0) to the non-homogeneous equation $ax + by = e$
  - Then, the solutions are parameterized by $x = x' + x_0, \;\; y = y' + y_0$

We also proved that there are no solutions other than the ones described above.

Example:

Find all integer solutions of

$$56x + 20y = 8$$

Note that $\gcd(56, 20) = 4$ which divides 8. So, by the lemma we proved above, we know that this equation has infinitely many solutions.

First, we find a particular solution

$$-2 \cdot 56 + 6 \cdot 20 = 8$$
$$(x_0, y_0) = (-2, 6)$$

Then, we find all solutions to the homogeneous equation as follows:

$$56x + 20y = 0$$
$$a' = \frac{56}{\gcd(56, 20)} = 14$$
$$b' = \frac{20}{\gcd(56, 20)} = 5$$

Then, the solutions to the homogeneous equation are.

$$x' = 5k, \;\; y' = -14k, \;\; k \in \mathbb{Z}$$

Translating the solutions to the homogeneous equation by the particular solution, we get

$$(5k + 2, -14k + 6) \;\; \forall k \in \mathbb{Z}$$

which is all solutions to $ax + by = e$.

$$\text{QED}$$

Definition - modulus:

$$a \equiv b \pmod{m} \iff m \mid a - b \iff \exists q \in \mathbb{Z}.\ a - b = qm$$
$$\iff \text{residue of a - b upon division by m is } 0$$
$$\iff \text{the residues of a and b upon fivision by m are equal}$$

Recall:

$\equiv$ is an equivalence relation on $\mathbb{Z}$, which means it is

1. Reflexive
2. Symmetric
3. Transitive

Proposition:

Let $a, b \in \mathbb{Z}$ and suppose that

$$a \equiv b \pmod{m}$$
$$a' \equiv b' \pmod{m}$$

Then, it follows that

1. $a + a' \equiv b + b' \pmod{m}$
2. $aa' \equiv bb' \pmod{m}$

Proof of 1:

We know that

$$m \mid (a - b)$$
$$m \mid (a' - b')$$

Therefore, there exist $k, k' \in \mathbb{Z}$ such that

$$a - b = km$$
$$a' - b' = k'm$$

This implies that

$$(a - b) + (a' - b') = m(k + k')$$
$$\implies (a + a') - (b + b') = m(k + k')$$
$$\implies a + a' \equiv b + b' \pmod{m}$$
$$\text{QED}$$

Proof of 2:

We know that

$$m \mid (a - b)$$
$$m \mid (a' - b')$$

So, there exist $k, k' \in \mathbb{Z}$ such that

$$a = b + km$$
$$a' = b' + k'm$$

Now, consider the product aa':

$$aa' = (b + km)(b' + k'm)$$

Expanding this expression, we get

$$aa' = bb' + b(k'm) + b'(km) + (km)(k'm)$$

$$aa' = bb' + m(k'b) + m(kb') + m^2(kk')$$

Factor out m:

$$aa' = bb' + m\left(k'b + kb' + mkk'\right)$$

This shows that

$$aa' - bb' = m\left(k'b + kb' + mkk'\right)$$

which means

$$m \mid (aa' - bb')$$

Thus,

$$aa' \equiv bb' \pmod{m}$$

$$\text{QED}$$

Congruence classes in $\mathbb{Z}$:

Define the congruence class notation:

$$[a]_m = \{b \in \mathbb{Z} \ : \ a \equiv b \pmod{m}\}$$

This is the set of integers that yield the remainder a when divided by m.

Then, define the $+$ and $\cdot$ operations on congruence classes:

$$[a]_m + [b]_m = [a + b]_m$$

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

Note that $+$ and $\cdot$ are well-defined operations.

Proof that $+$ is well-defined:

Assume that

$$[a]_m = [a']_m$$

$$[b]_m = [b']_m$$

This means

$$a \equiv a' \pmod{m}$$

$$b \equiv b' \pmod{m}$$

This implies that

$$m \mid (a - a')$$

$$m \mid (b - b')$$

Consider

$$(a + b) - (a' - b') = (a - a') + (b - b')$$

Since m divides both $(a - a')$ and $(b - b')$, m divides their sum too. We write:

$$m \mid (a + b - a' - b')$$

Therefore,

$$a + b \equiv a' + b' \pmod{m}$$

$$\implies [a+b]_m = [a'+b']_m$$

Therefore, $+$ is well-defined.

$$\text{QED}$$

Proof that $\cdot$ is well-defined:

$$\text{Proof omitted}$$

Congruence classes:

Denote $\mathbb{Z}_m$ to be the set of congruence classes modulo m

$$\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$$

Then, we have the following structures:

- $(\mathbb{Z}_m, +)$ is a group
- $(\mathbb{Z}, \cdot)$ is a monoid
    - It isn't necessarily a group because elements won't always be invertible!

Proof that $(\mathbb{Z}_m, +)$ is a group:

Note that $\mathbb{Z}_m$ is closed under $+$, by definition of $+$.

The associativity of $+$, as defined above, follows from the associativity of addition on integers.

Note that $[0]_m \in \mathbb{Z}_m$ is the identity element in $\mathbb{Z}_m$ with respect to $+$.

Finally, we have that for any $[a]_m \in \mathbb{Z}_m$, it holds that

$$[a]_m + [-a]_m = [a-a]_m = [0]_m = e_{\mathbb{Z}_m}$$
$$[-a]_m + [a]_m = [-a+a]_m = [0]_m = e_{\mathbb{Z}_m}$$

Therefore, every element in $\mathbb{Z}_m$ is invertible under $+$.

So, $(\mathbb{Z}_m, +)$ is a group.

$$\text{QED}$$

**Proof that $(\mathbb{Z}_m, \cdot)$ is a monoid:

By definition, $\mathbb{Z}_m$ is closed under $\cdot$. Note that $\mathbb{Z}_m$ has an identity element $[1]_m \in \mathbb{Z}_m$. Since multiplication of integers is associative, it follows that $\cdot$ is associative. So, $(\mathbb{Z}_m, \cdot)$ is a monoid.

$$\text{QED}$$

Lecture 15: Modular Congruence

Summary:
We continue our study of modular arithmetic, examining the structure of integers modulo m. We prove that the invertible group of integers modulo m consists of integers coprime to m, and establish conditions for the existence of multiplicative inverses.

Topics Covered: modular congruence relation, modular congruence ring

For a positive integer m, we define

$$\mathbb{Z}_m = \{[a]_m \ : \ a \in \mathbb{Z}\} = \{[0]_m, [1]_m, \ \ldots \ , [m-1]_m\}$$

to be the set of equivalence classes of $\mathbb{Z}$ under the equivalence relation

$$a \sim b \iff m \mid a - b$$

We checked last class that addition and multiplication defined on $\mathbb{Z}$ in the obvious way

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

is well-defined.

Lemma:

$(\mathbb{Z}_m, +)$ is a group

Example:

The addition table for $(\mathbb{Z}_3, +)$ is

$+$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[1]_3$	$[1]_3$	$[2]_3$	$[0]_3$
$[2]_3$	$[2]_3$	$[0]_3$	$[1]_3$

Example:

The addition table for $(\mathbb{Z}_4, +)$ is

$+$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

Lemma:

The cyclic group $(\mathbb{Z}_m, +)$ is generated by $[a]_m \iff \gcd(a, m) = 1$.

Proof:

If $\gcd(a, m) = 1$, then we can use Bezout's theorem to write 1 as a linear combination of a and m. This shows that $[1]_m \in \langle [a]_m \rangle$, so $[a]_m$ generates all of $\mathbb{Z}_m$.

Conversely, if $\gcd(a, b) = d > 1$, then everything generated by $[a]_m$ is a multiple of d. In particular, you cannot reach $[1]_m$.

$$\text{QED}$$

Lemma:

$$(\mathbb{Z}_m, \cdot)$$

is a monoid.

Note that $[0]_m$ is never invertible in $(\mathbb{Z}_m, \cdot)$.

Recall that the grou pof units in a monoid $(M, \cdot)$ is the set

$$M^\times = \{x \in M \ : \ x \text{ is invertible}\}$$

We saw many lectrues ago that $(M^\times, \cdot)$ is always a group, What does that group look like for $\mathbb{Z}_m$?

Lemma:

$$\mathbb{Z}_m^\times = \{[a]_m \ : \ \gcd(a, b) = 1\}$$

Here, we are looking for elements $[a]_m$ which are invertible. In particular, these are the elements such that there exists $x \in \mathbb{Z}$ with $[a]_m[x]_m = [1]_m$.

This is the same as requiring $[ax]_m = [1]_m$, which in trun is the same as

$$ax \equiv 1 \pmod m$$

Proposition:

Let $a \in \mathbb{Z}$. Then,

1. $\exists x \in \mathbb{Z}$ such that $ax \equiv 1 \pmod m \iff \gcd(a, b) = 1$ and
2. Such an x is unique modulo m

Lecture 16: Properties of Modular Congruence, Euler's Totient Function, RSA

Summary:
We explore properties of modular arithmetic and their applications to cryptography. We prove Fermat's little theorem and examine Euler's totient function, establishing its properties for semiprime numbers. We conclude with an introduction to RSA encryption, demonstrating how these concepts enable secure communication.

Topics Covered: Euler totient function, Euler totient theorem, Fermat's little theorem, modular congruence, semiprime, RSA

Proposition 1:

Let $a \in \mathbb{Z}$ and let p be prime. Then,

1. $a^p \equiv a \pmod{p}$
2. $a^{k(p-1)+1} \equiv a \pmod{p},\ k \in \mathbb{Z}_{\geq 0}$

Example:

Let

$$p(x) = 2x^7 + x^5 + 3x^3 + 4x + 10$$

Prove that $p(n) \equiv 0 \pmod{5}$

Proof:

We know that for any prime p, in particular, for $p = 5$, that

$$\forall a \in \mathbb{Z},\ a^p = a \pmod{p}$$

$$\implies \forall a \in \mathbb{Z}.\ a^5 = a \pmod{5}$$

$$(2x^7 + x^5 + 3x^3 + 4x + 10) \equiv 2x^3 + x + 3x^3 + 4x + 10$$

$$\equiv 5x^3 + 5x + 10 = 5(x^3 + x + 2) \equiv 0 \bmod 5$$

$$\text{QED}$$

Definition:

A positive integer n is semiprime if $n = pq$ for distinct primes p, q.

For example,

$$\phi(n) = (p-1)(q-1) = pq - p - q + 1$$

There are a total of q multiples of $p \leq n$

There are a total of p multiples of $q \leq n$

Then, we have to add back 1, we overcounted one of the primes

For example, in the case of $n = 5 \cdot 3$, we overcounted 15.

The total number of numbers $\leq n$ that are not relatively prime ot n is $p + 1 -$ however many are divisible

Proposition 2:

Let $a \in \mathbb{Z}$ and let $n = pq$ be semiprime,. Then,

$$a^{k\phi(n)+1} \equiv a \pmod{n},\ \forall k \in \mathbb{Z}_{\geq 0}$$

Proof:

Proposition 1 part 2 says that for primes p and q, we have

$$a^{r(p-1)+1} \equiv a \pmod{p},\ r \in \mathbb{Z}_{\geq 0}$$

$$a^{s(q-1)+1} \equiv a \pmod{q},\ \forall s \in \mathbb{Z}_{\geq 0}$$

Set $r = k(q-1),\ k \in \mathbb{Z}_{\geq 0}$, $s = k(p-1),\ k \in \mathbb{Z}_{\geq 0}$

The lemma implies that

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

Lemma:

Let $a, b, r, s \in \mathbb{Z}$. Then,

- $a \equiv b \pmod{r}$
- $a \equiv b \pmod{s}$

  $\iff$

  $$a \equiv b(\bmod(\operatorname{lcm}(r,s)))$$

  $\impliedby$ **proof:**

  $$a \equiv b \pmod{\operatorname{lcm}(r,s)} \implies \text{lemma} \implies a \equiv b \pmod{r} \implies a \equiv b \pmod{s}$$

RSA encryption:

Let Alice pick a semiprime $n = pq$ where p and q are distinct primes.

Alice also picks an integer e such that $\gcd(e, \phi(n)) = 1$.

Alice finds d, the multiplicative inverse of $e \pmod{\phi(n)} = 1$

$$de \equiv 1 \pmod{\phi(n)}$$

$$de + k\phi(n) = 1$$

Alice makes n, e public, and she keeps p, q, d private

Alice picks

- $p = 47$
- $q = 59$
- $n = pq = 2773$

$$\phi(n) = (p-1)(q-1) = 2668$$

$e = 17$ such that $\gcd(e, \phi(n)) = 1$

Then, we use the extended Euclidean algorithm

$$157 \cdot 17 = (-1)(2668) = 1$$

$$d = 157$$

Message: THIS IS ALL GREEK TO ME

We encode the message as follows

- blank space = 00
- $A = 01$
- $B = 02$
- ....
- $Z = 26$

Bob writes a message and turns it into an integer (or a sequence of integers) $0 \leq x \leq n$

Bob sends the residue $x^e \pmod n$ through the chanel

Alice gets $x^e \pmod n$ and computes

$$(x^e)^d \equiv x^{de} \equiv x^{-k\phi(n)+1} \equiv x \pmod n$$

Where the last equivalence follows from proposition 2.

Thus, Alice can recover x.

Proposition:

Let n be semiprime with $n = pq$ and p, q prime.

Then, p and q are uniquely determined by n and $\phi(n)$.

Proof:

Consider the equation

$$x^2 + (\phi(n) - n - 1)x + n = 0$$

$$x^2 + bx + c = 0$$

$$\implies (x - \alpha)(x - \beta)$$

Then, we have that

$$b = -(\alpha + \beta),\ c = \alpha\beta$$

$$\phi(b) = (p-1)(q-1) = pq - (p+1) + 1 \implies \phi(n) - n - 1 = -(p+q)$$

The solutions to this equation are exactly p and q

$$\text{QED}$$

Lecture 17: Rings, Error Correcting Codes

Summary:
We introduce rings and their properties and provide some examples. We prove the absorption property and establish that rings are commutative under addition. We then explore error correcting codes, focusing on the k-fold repetition code and its applications in reliable data transmission.

Topics Covered: division ring, field, group, k-fold repetition code, monoid, ring

Definition:

A ring is a set R with operations $+$ and $\cdot$ such that

1. $(R, +)$ is a group with identity $0 \in R$
2. $(R, \cdot)$ is a monoid with identity $1 \in R$
3. Distributivity
   - $\forall a, b, c \in R.\ a \cdot (b + c) = a \cdot b + a \cdot c$
   - $\forall a, b, c \in R.\ (a + b) \cdot c = a \cdot c + b \cdot c$

Examples and non-examples:

- $(\mathbb{Z}, +, \cdot)$
  - Is a ring
- $(\mathbb{Z}_{\geq 0}, +, \cdot)$
  - Is not a ring because $(\mathbb{Z}_{\geq 0}, +)$ is not a group
- $(\mathbb{Z}_m, +, \cdot)$
  - This is a ring

Recall that in the third example, we defined $+$ and $\cdot$ as

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

Absorption property:

Let $(R, +, \cdot)$ be a ring. Let $a \in R$. Then,

$$0 \cdot a = a \cdot 0 = 0$$

Proof:

Since 0 is the identity for $+$, then, we have

$$0 + 0 = 0$$

Therefore,

$$\begin{aligned} 0 \cdot a = (0 + 0) \cdot a &= 0 \cdot a + 0 \cdot a \\ \implies 0 \cdot a &= 0 \cdot a + 0 \cdot a \\ \implies 0a + (-(0a)) &= 0a + 0a + (-(0a)) \\ \implies 0 &= 0a \end{aligned}$$

The other statement is very similar.

$$\text{QED}$$

Proposition:

Let $(R, +, \cdot)$ be a ring. Then, $\forall a, b \in R.\ a + b = b + a$.

Proof:

Let $a, b \in R$. We first show that

$$a + a + b + b = a + b + a + b$$

$$\begin{aligned} a + a + b + b &= 1 \cdot a + 1 \cdot a + 1 \cdot b + 1 \cdot b \\ &= (1 + 1) \cdot a + (1 + 1) \cdot b \\ &= (1 + 1)(a + b) \\ &= 1 \cdot (a + b) + 1 \cdot (a + b) = a + b + a + b \end{aligned}$$

Which is what we wanted to show.

Finally, we cancel the a on the left and the b on the right to get

$$a + b = b + a$$

$$\text{QED}$$

Example:

Note that for a ring $(R, +, \cdot)$, $(R, \cdot)$ is not necessarily commutative.

Here's an example:

$$(\mathcal{M}_n(\mathbb{R}), +, \cdot)$$

for $n \geq 2$.

Where $+$ is element-wise addition and $\cdot$ is matrix multiplication.

We know that $\cdot$ is not commutative on $\mathcal{M}_n(\mathbb{R})$ when $n \geq 2$.

Exercise:

Let $(R, +, \cdot)$ with $0 \in R$ additive identity and $1 \in R$ multiplicative identity and $0 = 1$. Then, $|R| = 1$ and $R = \{0\}$.

Recall: In a ring, $+$ is always commutative.

Definition:

1. Let $(R, +. \cdot)$ with $a \in R$ and $R \neq \{0\}$. We say that a is invertible in R when a is invertible in the monoid $(R, \cdot)$.
   - Note that we define this notion specifically for $(R, \cdot)$ because $(R, +)$ is a group, Thus, a is always invertible in $(R, +)$.
2. a is a zero-divisor in R when $\exists b \in R, b \neq 0,\ a \cdot b = 0 \text{ or } b \cdot a = 0$

Example:

Consider the ring $(\mathbb{Z}_6, +, \cdot)$. Here, the invertible elements are $[a]$ such that $\gcd(a, 6) = 1$ (relatively prime).

Proposition:

An element a of a ring R cannot be both a zero divisor and invertible.

Proof:

Assume, for contradiction, that $a \in R$ is both a zero divisor and and invertible.

This means

$$a \cdot b = 0$$

for some $b \in R,\ b \neq 0$

Since a is invertible, we know that we can multiply by a^{-1} on both sides. Then, we get

$$b = 1 \cdot b = a^{-1} \cdot a \cdot b = a^{-1} \cdot 0 = 0$$

$$\implies b = 0$$

which contradicts the assumption that $b \neq 0$.

$$\text{QED}$$

Therefore, every $a \in R$ is exactly one of the following:

1. A zero-divisor
2. Invertible
3. Neither

Definition:

A division ring is a ring in which every nonzero element is invertible.

Definition:

A field is a division ring where, in addition to $+$, $\cdot$ is also commutative.

Theorem:

A finite field must have cardinality $q = p^{\alpha}$, where p is a prime number.

Error correcting codes

We will be working with the field $\mathbb{F}_2 = \{0, 1\}$.

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Bob encodes his message as a string of 0's and 1's.

$$x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$$

We add an extra dimension to x as follows

$$x_{n+1} = \begin{cases} 0 \ ; \ \text{there is an even number of 1s among the } x_1, \ldots, x_n \\ 1 \ ; \ \text{otherwise} \end{cases}$$

Consider the message

$$0110111$$

Here, something went wrong because this encoding doesn't follow the definition for x_{n+1}.

Note that, since we are in $\mathbb{F}_2$, we can define x_{n+1} as

$$x_{n+1} = x_1 + \ldots . + x_n$$

Note that

$$x_1 + \ldots . + x_n + x_{n+1} = 0$$

because of the definition of x_{n+1}.

$$z = (z_1, \ldots, z_n, z_{n+1})$$

If $z_1 + \ldots + z_n + z_{n+1} \neq 0$, there is an odd number of errors.

If $z - 1 + \ldots + z_n + z_{n+1} = 0$, there are no errors or there is an even number of errors.

K-fold repetition code:

Suppose Bob's message is

$$x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$$

Then, we build

$$y = (\underbrace{x, \ldots, x}_{k}) \in \mathbb{F}_2^{kn}$$

Alice gets

$$z \in \mathbb{F}_2^{kn}$$

And Alice decodes to message to be the z_i that appears the most number of times.

Lets assume that $k = 2m + 1$, $m \in \mathbb{Z}_{\geq 0}$, in our k-fold repetition code.

If $z \in \mathbb{F}_2^{kn}$, the word that Alice receives at most m errors. Then, Alice decodes correctly.

Alice can detect up to $k - 1$ errors.

Lecture 18: K-fold Repetition Code

Summary:
We examine the k-fold repetition code in detail, introducing fundamental concepts of coding theory including code size, length, and rate. We define Hamming distance and weight, proving that Hamming distance forms a metric. We establish conditions for error detection and correction, demonstrating how the minimum distance of a code determines its error-correcting capabilities.

Topics Covered: code, Hamming distance, Hamming distance and error correction theorem, Hamming weight, k-fold repetition code

K-fold repetition code:

We have a message $n \in \mathbb{F}_2^n$

The code word is

$$y = (\underbrace{x, x, \ldots, x}) \in \mathbb{F}_2^{kn}$$

For example, if $x = 01$ and $k = 3$, then, we have

$$y = 010101$$

Codes:

$\mathbb{F}_q$ is a finite field with q elements. $q = p^\alpha$ for prime p and $\alpha \in \mathbb{Z}_{>0}$

Messages are all possible words of length n (vectors in $\mathbb{F}_2^n$)

A code is

$$C \subseteq \mathbb{F}_q^m$$

for some $m \geq n$

We want an injective function

$$\mathbb{F}_q^n \to C$$

- $y \in C$ is the encoded word
- $z \in \mathbb{F}^m$ is the word after transmission

When $z \notin C$, an error has been detected.

If $y' = y$, we decoded correctly.

Definition:

The size of the code is the number of code words in it.

Definition:

The length of a code is the number of bits in a code word. In the case of $C \subseteq \mathbb{F}_q^m$, it is m.

Definition:

The rate of a code is defined as

$$\text{ratio} = \frac{\text{number of bits in message}}{\text{number of bits in codeword}}$$

Definition:

Let $y = (y_1, \ldots, y_m) \in \mathbb{F}_q^m$. We define the hamming weight

$$w(y) = |\{i \in [k] \ ; \ y_i \neq 0\}|$$

Definition:

Let $y, z \in \mathbb{F}_q^m$. We define the hamming distance

$$d(y, z) = w(y - z) = w(z - y)$$

The hamming distance counts the number of bits in which y and z differ.

Definition:

Let $C \subseteq \mathbb{F}_q^m$. We define the hamming distance of the code to be

$$d(C) = \min\{d(x, y) \ : \ x, y \in C. \ x \neq y\}$$

Definition:

Let $y \in C$ (the codeword sent) and $z \in \mathbb{F}_q^m$ (word received).

1. $z \notin C$ we say that an error has been detected
2. If there is a unique $y' \in C$ such that $d(y', z) < d(y'', z), \ \forall y'' \in C, y'' \neq y'$, then we say that y' is the decoding of z
    - y' is the unique code word with the closest hamming distance to z

Exercise:

Show that the Hamming distance is a metric, meaning it satisfies the following axioms:

1. $\forall x. \ d(x, x) = 0$
2. $\forall x, y. \ d(x, y) = d(y, x)$
3. $\forall x, y, z. \ d(x, y) \leq d(x, z) + d(z, y)$

Theorem:

Let C be a code with the Hamming distance $d(C)$.

1. C detects up to s errors $\iff d(C) \geq s + 1$.
2. C corrects up to t errors $\iff d(C) \geq 2t + 1$

$(1) \impliedby$ **proof:**

Assume that $d(C) \geq s + 1$. Suppose we send $y \in C$ and we receive $z \in \mathbb{F}_q^n$ and i errors occurred. This means

$$d(y, z) = i$$

We need to show that if $i \leq s$ then the error was detected.

We know that $d(y, z) = i \leq s < s + 1 \leq d(C)$

$$\implies d(y, z) < d(C)$$

Suppose, for contradiction, that z was a code word. Then, we also have

$$d(y, z) \geq d(C)$$

Which is a contradiction. Therefore, we conclude that z is not a code word. So, we have detected the error.

$$\text{QED}$$

$(1) \implies$ **proof:**

C detects $1, 2, \ldots, s$ errors

Let $d(C) = i \implies \exists y_1 \neq y_2$ with $y_1, y_2 \in C, d(y_1, y_2) = i$. Note that if we send y, make i errors and receive y_2, we won't know that errors occurred!

$$d(C) = i \geq s + 1$$

$$\text{QED}$$

$(2) \impliedby$ **proof:**

Assume that $d(C) \geq 2t + 1$. We want to prove that one can correct up to t errors.

We send $y \in C$ and receive $z \in \mathbb{F}_q^m$ with i errors, $i \leq t$, i.e. $d(y, z) = i$. To correct the error means that y is the unique closest codeword to z. Suppose that to the contrary, $x \in C$ is such that $d(x, z) < i$.

$$d(x, y) \leq d(x, z) + d(z, y) \leq i + i = 2i < 2t + 1 \leq d(C)$$

$$\implies d(x, y) < d(C)$$

This implies that x and y are not code words. Therefore, $x \notin C$.

$$\text{QED}$$

$(2) \implies$ **proof:**

Assuming our code can correct $1, 2, 3, \ldots, t$ errors. Want to conclude that $d(C) \geq 2t + 1$.

Let $d(C) = i$. This means $\exists y_1 \neq y - 2, y_1, y_2 \in C$ such that $d(y_1, y_2) = i$.

$$f = \left\lfloor \frac{i}{2} \right\rfloor$$

$$c = \left\lceil \frac{i}{2} \right\rceil$$

$$i = f + c$$

Build a new word z be replacing f of the i bits in y, in which y_1 and y_2 differed

$$d(y_1, z) = f$$

$$d(y_2, z) = c$$

$$d(y_1, z) \leq d(y_2, z)$$

Send y_2 as our message, receive z. We don't know how to correct $\implies i \geq t + 1$.

$$d(C) = i = f + c \geq c - 1 + c = 2c - 1 \geq 2(t + 1) = 2t + 1$$

$$\text{QED}$$

Lecture 19: Hamming Sphere and Ball, Vector Space

Summary:
We explore Hamming spheres and balls, establishing formulas for their sizes and examining their role in error correction. We prove bounds on code size based on error-correcting capabilities and introduce vector spaces, defining their fundamental properties and operations. We demonstrate how these concepts provide a framework for understanding linear codes.

Topics Covered: Hamming ball, Hamming sphere, vector space

Proposition:

C is a code with Hamming distance $d(C)$

1. C detects up to s errors $\iff d(C) \geq s+1$
2. C corrects up to t errors $\iff d(C) \geq 2t+1$

Hamming sphere:

$$x \in \mathbb{F}_q^m, r \in \mathbb{N}$$

The Hamming sphere with center x and radius r is denoted

$$S(x,r) = \{y \in \mathbb{F}_q^m \ : \ d(x,y) = r\}$$

Hamming ball:

$$B(x,r) = \{y \in \mathbb{F}_q^m \ : \ d(x,y) \leq r\}$$

Note that

$$|\mathbb{F}_q^m| = q^m$$

Example 1:

$$x = (1,1) \in \mathbb{F}_2^2, \ r = 1$$
$$S(x,r) = \{(0,1),(1,0)\}$$
$$B(x,r) = \{(1,1),(0,1),(1,0)\}$$

Suppose we have $r = 2$. Then, we get

$$S(x,r) = \{(0,0)\}$$
$$B(x,r) = \mathbb{F}_2^2$$

Example 2:

$$x = (a,b,c,d) \in \mathbb{F}_q^4, \ r = 2$$

Lemma:

$$|S(x,r)| = \binom{m}{r}(q-1)^r$$

$$|B(x,r)| = \sum_{i=0}^{r} \binom{m}{r}(q-1)^i$$

Note that

$$B(x,r) = \bigsqcup_{i=0}^{r} S(x,i)$$

Binomial theorem:

> binomial theorem

- tags
  - math
  - CS
- related
  - binomial coefficients

Theorem 23.1 — Binomial Theorem.

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k \, y^{n-k}.$$

$$(x+y)^n = \underbrace{(x+y)\,(x+y)\,\dots\,(x+y)}_{n \text{ times}}.$$

Fact D.2. (Binomial theorem) Let n be a positive integer. Then for any x, y,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}. \tag{D.10}$$

Theorem:

Let $C \subseteq \mathbb{F}_q^m$ be a code of size $M = |C|$.

Suppose that C corrects up to t errors.

Then,

$$M \sum_{i=0}^{t} \binom{m}{i} (q-1)^i \leq q^m$$

$$M \leq \frac{q^m}{\sum_{i=0}^{t} \binom{m}{i} (q-1)^i}$$

Proof:

Since C corrects up to t errors, we know that $d(C) \geq 2t+1$.

$$\implies y_1, y_2 \in C,\ y_1 \neq y_2,\ d(y_1, y_2) \geq 2t+1 \implies$$

$$B(y,t) \cap B(y_2,t) = \emptyset$$

$$a \in B(y_1,t) \cap B(y_2,t)$$

$$d(y_1,y_2) \subseteq d(y-1,a) + d(a,y_2) \leq 2t$$

Note that

$$|\mathbb{F}_q^m| = q^m$$

points

For each of the M elements of C, we have a ball of radius t around it with

$$\sum_{i=1}^{t} \binom{m}{i} (q-1)^i \leq q^m$$

Example:

$C \subseteq \mathbb{F}_2^{10}$ code that corrects up to 2 errors. Show that $|C| \leq 18$.

Solution:

$$|C| \left(\sum_{i=0}^{2} \binom{10}{i} \right) \leq 2^{10}$$

$$\binom{10}{0} + \binom{10}{1} + \binom{10}{2}$$

$$|C| \leq \frac{1024}{56} = 18.3$$

Definition:

A vector space is a set $\mathcal{V}$ over a field $\mathbb{F}$ with a binary operation $+$ on $\mathcal{V}$ and a scalar multiplication operation $\cdot : \mathbb{F} \times \mathcal{V} \to \mathcal{V}$ such that

1. $\forall u, v \in \mathcal{V}.\ u + v \in \mathcal{V}$
2. $\forall u, v, w \in \mathcal{V}.\ (u + v) + w = u + (v + w)$
3. $\exists \vec{0} \in \mathcal{V}.\ \forall v \in \mathcal{V}.\ \vec{0} + v = v$
4. $\forall v \in \mathcal{V}.\ \exists (-v) \in \mathcal{V}.\ v + (-v) = \vec{0}$
5. $\forall u, v \in \mathcal{V}.\ . u + v = v + u$
6. $\forall a \in \mathbb{F}. \forall v \in \mathcal{V}.\ \ av \in \mathcal{V}$
7. $\forall a, b \in \mathbb{F}.\ \forall v \in \mathcal{V}.\ a(bv) = (ab)v$
8. $\forall a, b \in \mathbb{F}.\ \forall v \in \mathcal{V}.\ (a + b) \cdot v = av + bv$
9. $\forall a \in \mathbb{F}.\ \forall u, v \in \mathcal{V}.\ a(u + v) = au + av$
10. $\forall v \in \mathcal{V}.\ 1 \cdot v = v$

Lecture 20: Review of Linear Algebra

Summary:
We review essential concepts in linear algebra, focusing on vector spaces, subspaces, and linear transformations. We examine the fundamental subspaces of a matrix and prove the rank-nullity theorem. We explore orthogonality and its applications to coding theory, establishing connections between vector spaces and linear codes.

Topics Covered: basis, dimension, image, kernel, linear code, linear transformation, orthogonality, subspace, vector space

Review of linear algebra

Let $\mathcal{V}$ be a vector space over a field $\mathbb{F}$.

In $\mathcal{V}$, we have linear combinations of the form

$$av + bw$$

where $a, b \in \mathbb{F}$ and $v, w \in \mathcal{V}$.

$\mathcal{W} \subseteq \mathcal{V}$ is a subspace of $\mathcal{V}$ means it is closed under linear combinations

If we have two vector spaces $\mathcal{V}, \mathcal{V}'$ over $\mathbb{F}$, a function $T : \mathcal{V} \to \mathcal{V}'$ is called a linear transformation when it preserves linear combinations

A linear transformation has two fundamental subspaces

$$\ker(T) = \{v \in \mathcal{V} \ : \ T(v) = \vec{0}\} \subseteq \mathcal{V}$$
$$\operatorname{im}(T) = \{v' \in \mathcal{V}' \ : \ \exists v \in \mathcal{V}.\ T(v) = v'\} \subseteq \mathcal{V}'$$

Note that $\ker(T)$ and $\operatorname{im}(T)$ are subspaces, meaning they are closed under linear combinations.

A basis of a vector space is a set of vectors that are linearly independent and span the space.

Every basis has the same cardinality, and we call that $\dim \mathcal{V}$.

Rank nullity theorem:

$$\dim \mathcal{V} = \dim \ker(T) + \dim \operatorname{im}(T)$$

Exercise:

Let $\mathbb{F} = \mathbb{F}_q$ be a field with q elements.

1. Let $\mathcal{V} = \mathbb{F}_q^n$. What is $\dim \mathcal{V}$ and $|V|$?
2. Let $\mathcal{W} \subseteq \mathcal{V}$ be a subspace with $\dim \mathcal{W} = k$. What does Lagrange's theorem tell us?

Part 1:

$$|\mathcal{V}| = q^n$$
$$\dim V = n$$

Part 2:

Note that $(\mathcal{W}, +)$ is a subgroup of $(\mathcal{V}, +)$. Both groups are finite. By Lagrange's theorem, we know that $|\mathcal{W}|$ divides $|\mathcal{V}|$.

Suppose that $\mathcal{V} = \mathbb{F}^n$.

$v, w \in \mathcal{V}$ are orthogonal means $v \cdot w = \sum_{i=1}^n v_i \cdot w_i = v^T w = 0$, where

$$v = (v_1, \ldots, v_n) \in \mathbb{F}^n$$
$$w = (w_1, \ldots, w_n) \in \mathbb{F}^n$$

Let $\mathcal{W} \subseteq \mathcal{V}$ be a subspace. We denote the orthogonal subspace

$$\mathcal{W}^\perp = \{v \in \mathcal{V} \ : \ \forall w \in \mathcal{W}.\ v \cdot w = 0\}$$

Note that

$$\mathcal{V} = \mathcal{W} \oplus \mathcal{W}^\perp$$

Which means

1. $\mathcal{V} = \mathcal{W} + \mathcal{W}^\perp$
2. $\mathcal{W} \cap \mathcal{W}^\perp = \{0\}$

Therefore, when $\dim \mathcal{W}, \dim \mathcal{W}^\perp < \infty$, we have that

$$\dim \mathcal{V} = \dim \mathcal{W} + \dim \mathcal{W}^\perp$$

Views of linear combinations:

Row vector multiplication on the left

$$\begin{bmatrix} x_1 & x_2 \end{bmatrix} \begin{bmatrix} \alpha & \alpha' & \alpha'' \\ \beta & \beta' & \beta'' \end{bmatrix} = x_1[\alpha\ \alpha'\ \alpha''] + x_2[\beta\ \beta'\ \beta'']$$

Column vector multiplication on the right

$$\begin{bmatrix} \alpha & \alpha' & \alpha'' \\ \beta & \beta' & \beta'' \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = y_1 \begin{bmatrix} \alpha \\ \beta \end{bmatrix} + y_2 \begin{bmatrix} \alpha' \\ \beta' \end{bmatrix} + y_3 \begin{bmatrix} \alpha'' \\ \beta'' \end{bmatrix}$$

4 subspaces of a matrix A:

$$A \in \mathbb{F}^{m \times n}$$
$$T : \mathbb{F}^m \to \mathbb{F}^n$$
$$T(y) = Ay$$

- $\ker T = \{y \in \mathbb{F}^m \ : \ Ay = 0\}$ is called the **kernel** or **right nullspace** of A
- $\operatorname{im} T$ is called the **image** or **column space** of A

$$\tilde{T} : \mathbb{F}^n \to \mathbb{F}^m$$
$$\tilde{T}(x) = xA$$

- $\ker \tilde{T}$ is called the **left nullspace** of A
- $\operatorname{im} \tilde{T}$ is called the **row space** of A

Theorem:

Fix $A \in \mathbb{F}^{n \times m}$. Then, we have

$$\text{nullspace}(A) = \text{rowspace}(A)^\perp$$

Note that

$$y \in \text{null}(A) \iff Ay = 0 \iff \text{dot productof every row of A with y is 0}$$
$$\iff \text{y is orthogonal to every row of A}$$
$$y \in \text{row}(A)^\perp$$

Reminder:

$$\dim \text{row}\ A = \dim \text{col}\ A = \text{rank}\ A$$

Graphs:

Each vertex represents a vector and each edge represents the difference of two vectors $e_i - e_j$.

$$S_G = \{e_i - e_j \ : \ (i,j) \in G, \ i < j\}$$

$$\mathcal{V} = \text{span}_{\mathbb{R}} S_G$$

Bases for a graph-based vector space:

A basis corresponds to an MST of the graph.

An MST is a minimal subset of edges that spans the graph.

Definition:

A linear code C is a vector subspace of $\mathbb{F}_q^m$. Furthermore, if $\dim C = n$, then call it an $[m, n]$ code.

Let C be a 3-fold repitition code over $\mathbb{F}_2$ with message length 2.

$$C = \{00000, 101010, 010101, 111111\} \subseteq \mathbb{F}_2^6$$

Note that C is a subspace of $\mathbb{F}_q^m$.

$$= \text{span}\{y_2, y_3\}$$

Then, we have $y_2 + y_3 = y_4$.

The Hamming distance of C is

$$d(C) = 3$$

Lemma 1:

Let C be a linear code. Then,

$$d(C) = \min\{w(y) \ : \ y \in C\}$$

- $w(y)$ denotes the weight of y

Proof:

By definition, we have

$$d(C) = \min\{d(x,y) \ : \ x, y \in C, x \neq y\}$$

Note that $d(x,y) = w(x-y)$.

Let $x, y \in C$. Then, we have

$$d(x,y) = w(x-y)$$

And, since C is a subspace, we have

$$x - y \in C$$

Lecture 21: Linear Codes

Summary:
We examine linear codes and their representation through generator and parity-check matrices. We prove that the minimum distance of a linear code equals its minimum weight, and establish the Singleton bound. We demonstrate how to construct parity-check matrices from generator matrices and explore their role in error detection and correction.

Topics Covered: generator matrix, linear code, parity-check matrix, singleton bound, subspace

Proposition:

For a linear code C, we have

$$d(C) = \min\{w(y) \ : \ y \in C, \ y \neq 0\}$$

Today:

- Linear codes
- Generator matrix
- Parity-check matrix $\rightarrow$ decoding
    - This has nothing to do with parity-check code

$n \leq m$, n lengths of the messages, $\dim C = n$, m is the length of code words.

Definition:

Let C be an $[m, n)$ code and let G be an $n \times m$ matrix.

G is a generator matrix for C is $C = \text{rowspace}(G)$.

Since $\dim C = n$, $\text{rank}(G) = n \implies G$ is a full rank matrix, meaning the rows are linearly independent.

$$\tilde{T} : \mathbb{F}_q^n \to \mathbb{F}_q^m$$

$$x \mapsto xG$$

$$\text{im}(\tilde{T}) = C, \quad \text{by definition}$$

Example:

$$C = \{0000, 1101, 1010, 0111\} \subseteq \mathbb{F}_2^4$$

Note that this is a linear code, meaning it is a vector subspace.

Here, $m = 4$ and $n = 2$. n is the length of messages and m is the lengths of codewords.

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

The rows form a basis for C.

Definition:

Let C be an $[m, n]$ code and let H be an $(m - n) \times m$ matrix. We say that H is a **parity check matrix** for C when $C = \text{null}(H)$.

H will be our way of decoding.

$$\text{row}(G) = C = \text{null}(H)$$

$$C = \text{null}(H) = \{y \in \mathbb{F}_q^m \ : \ Hy = 0\} \subseteq \mathbb{F}_q^m$$

$$\dim C = n, \ \ \dim(\text{null}(H)) = n$$

A $n \times m$ matrix with $n \leq m$ and $\text{rank}(A) = n$. Rows are a basis of $\text{row}(A)$.

$$\tilde{\text{null}} = 0$$

is the kernel of $\tilde{T} : \mathbb{F}^n \to \mathbb{F}^m$. $\tilde{T}$ is injective.

Problem:

Given a full rank $n \times m$ matrix A, find a matrix B such that

$$\text{row}(A) = \text{null}(B)$$

We will use row operations to get from A to A', where

$$A = \{\underbrace{I_n}_{n} \ : \ \underbrace{M}_{m-n}\}$$

$$B = \left[\underbrace{-M^t}_{n} \mid \underbrace{I_{m-n}}_{m-n}\right]$$

Claim:

$$\text{null}(B) = \text{row}(A') = \text{row}(A)$$

For example, we have the following generator:

$$H = [-M^t \ : \ I_{m-n}] = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

Theorem:

Let H be a parity check matrix for a linear code C.

Then,

$$d(C) = \text{the smallest size of a linearly dependent set of columns of H}$$

Proof:

We proved that for a linear code C, $d(C) = \min\{w(y) \ : \ y \in C, y \neq 0\}$. By assumption $y \in C \iff Hy = 0$.

Corollary - Singleton bound:

Let C be an $[m, n]$ code. Then,

$$d(C) \leq m - n + 1$$

Proof:

$$\text{rank}(H) = m - n$$

$$\implies \text{any m - n + 1 columns are linearly dependent}$$

$$\text{QED}$$

Lemma:

Let C be a linear code and H be a parity check matrix for it. When receiving the word z, we detect an error exactly when $Hz \neq 0$.

Proof:

$$C = \text{null}(H), \ z \in C \iff Hz \neq 0$$

$$\text{QED}$$

How do we decode: we pick the closest codeword to z!

Recall that given a finite group G and finite subgroup H, we have

$$x \sim_H y \iff xy^{-1} \in H$$

is an equivalence relation on G. Thus, it partitions G, and we proved while proving Lagrange's theorem, that we get classes of the form Hx.

We will apply the previous to $(C, +)$ viewed as a finite subgroup of a finite group $(\mathbb{F}_q^m, +)$.

$$C = \{0000, 1101, 1010, 0111\}$$

$$1000 + C = \{1000, 0101, 0010, 1111\}$$

$$0100 + C = \{0100, 1001, 1110, 0011\}$$

$$0001 + C = \{0001, 1100, 1011, 0110\}$$

Lecture 22: Syndrome Decoding, Single Errors

Summary:
We explore syndrome decoding for linear codes, establishing a systematic method for error correction. We prove that syndrome decoding identifies the closest codeword to a received word and examine conditions for detecting and correcting single errors. We demonstrate how the columns of a parity-check matrix determine the error-correcting capabilities of a code.

Topics Covered: coset decoding, generator matrix, parity-check matrix, single bit error in a linear code, syndrome decoding

Proposition:

Given word $z \in \mathbb{F}_q^m$, we do the following:

1. Locate the coset $c + C$ of C, such that $c + C \ni z$
2. Among the elements of $v + C$, find an element e of lowest weight
3. Decode $y' = z - e$

Then, $y' \in C$, and no other codeword is closer to z than y'

$$C = \{0000, 1101, 1010, 0111\} \subseteq \mathbb{F}_2^4$$

- y is what we send
- z is what receive
- y' is what we decode into

Proof:

$z, e \in v + C$, $z = x + y_1$, $e = x + y_2$, $x_1, y_2 \in C$.

$$y' = z - e = y_1 - y_2 \in C$$

Since $z \in v + C$ and $y'' \in C$, we know that

$$z - y'' \in v + C$$
$$d(z, y'') = w(z - y'')$$

Note that $z - y'' \in v + C$ and $e \in v + C$ is the lowest weight element. Therefore, we have

$$d(z, y'') = w(z - y'') \geq w(e) = d(z, y')$$
$$\text{QED}$$

Proposition (Syndrome decoding):

C is a linear code and H is a parity check matrix for C.

Let z, e as in previous proposition. Then,

$$Hz = He$$

and none of the lowest weight vectors e' coming from the cosets other than $v + C \in z$ satisfy $Hz = He'$.

Example:

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

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

$$Hz = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = He$$

$$He_1 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$He_2 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

$$He_3 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Proof:

$$z - e \in C = \text{null}(H) \implies H(z-e) = 0 \implies Hz = He$$

Let e' be the lowest weight vector in the coset that doesn't contain z

$$\implies z - e' \notin C$$

$$H(z-e') \neq 0$$

$$\implies Hz \neq He'$$

$$\text{QED}$$

Proof:

Given a linear code C, we calculate the cosets and choose a lowest weight vector in each coset (those will do the decoding). For each lowest weight vector e (of which there are $\frac{q^m}{|C|}$ many), we calculate and store He. These are called the syndromes of the code.

When we receive a word $z \in \mathbb{F}_q^m$, we do the following to decode:

1. Compute Hz
2. Search through the syndromes to find e for which $Hz = He$
3. Decode to $y' = z - e$

> The rest of the lecture is over $\mathbb{F}_2$.

Denote the standard basis as:

$e_1 = (1, 0, \dots, 0, e_2 = (0, 1, 0, \dots, 0)$, ..., $e_m = (0, \dots, 0, m)$.

This is a basis of $\mathbb{F}_2^m$.

Proposition:

Let C be a linear code with parity check matrix H. C detects a single error in bit $i \iff He \neq 0$.

He_i is the i^{th} column on H.

Proof:

$y \in C$. Suppose that, during transmission, exactly one error occurred and it is in bit i.

This implies that

$$z = y + e_i$$

We know that an error is detected $\iff Hz \neq 0$. This is because $C = \text{null}(H)$.

$$y \in C \implies Hy = 0$$

$$z \notin C = \text{null}(H)$$

$$Hz = H(y + e_i) = Hy + He_i \neq 0$$

Proposition:

Let C be a linear code with parity-check matrix H. Then, C can correct all single errors $\iff$ the columns of H are nonzero and distinct.

A single error means one bit is modified.

Proof:

We know that C corrects all single errors $\iff d(C) \geq 3$.