MATH 29 Bridging Course

Basic Concepts in Higher Mathematics

John Rick Dolor Manzanares

August 13, 2021

University of the Philippines Baguio

Table of Contents

Introduction

What is MATH 29?

MATH 29 course lays out the fundamental ideas of abstract mathematics and proof techniques that students will need to master for other higher math courses such as Analysis and Topology.

Thesis Preparation (Research Groups)

1. Applied Dynamical Systems
    - Delay Differential Equations
    - Mathematical Epidemiology
2. Algebra
    - Linear Algebra and Matrix Analysis
    - Algebraic Geometry
        - Motion Representations
        - Robot Kinematics
3. Mathematical Modeling and Simulation
4. Numerical Modeling
5. Number Theory
6. Statistics Research
7. Topological Data Analysis

Review of Previous Topics

Basic Methods of Proving

If **P** then **Q**.

1. Direct Proof (Assume P is true then show that Q holds.)
2. Indirect
   - Proof by Contraposition (Assume that the negation of Q is true then show that the negation of Q holds.)
   - Proof by Contradiction (Assume that P is true. Also, assume that the negation of Q is true. One must end up with a contradiction.)
3. Proof by Exhaustion (Assume P and consider every case possible. One must show that Q holds for every case.)
4. Mathematical Induction (Demonstrate the base case. Prove the inductive step.)
   - Weak Induction
   - Strong Induction

Warm-Up Exercises

Write down a concise and elegant proof of the following statements.

1. For any integer n, $n(n^2+2)$ is divisible by 3.
2. For integers $n \geq 5, 2^n > n^2$.
3. Let $f(x) = 3x + 1$ and $g(x) = 6x + 5$. Then there is a real number x such that $f(x) = g(x)$.
4. There are infinitely many prime numbers.
5. For any $x \in \mathbb{R}$, $\sqrt[3]{x}$ is irrational when x is irrational.

Basic Method of Proving: Set Theory Edition

Let A and B be two sets. Show that $A = B$.

1. Algebraic Proof
2. Pick-a-Point Method [for subset relations $A \subset B$] (Choose an arbitrary point x in A and show that x is also in B.)
   - Double Set Inclusion (Show that $A \subset B$ and $B \subset A$ to obtain $A = B$.)

Definition

The **Cartesian product** of the sets X and Y is defined by the set

$$X \times Y = \{(x, y) \mid x \in X, y \in Y\}.$$

In general, the Cartesian product of a finite collection $\{X_n\}_{n=1}^{k}$ of sets is

$$X_1 \times X_2 \cdots \times X_n = \{(x_1, x_2, \ldots, x_n) \mid x_i \in X_i \text{ for all } i = 1, 2, \ldots, k\}.$$

Warm-Up Exercises

1. Prove that $\{(x, 2x-2) \mid x \in \mathbb{R}\} = \{(t+1, 2t) \mid t \in \mathbb{R}\}$.
2. Let $A_n = \left[2, 5 + \frac{1}{n}\right)$. Show that
$$\bigcap_{n \in \mathbb{N}} A_n = [2, 5].$$
3. Let B be a set and A_α, for $\alpha \in \Delta$, an indexed family of sets. Prove that
$$B \cap \bigcup_{a \in \Delta} A_\alpha \subseteq \bigcup_{\alpha \in \Delta} (B \cap A_\alpha).$$

Let R be a relation on a set A.

- R is **reflexive** on A if xRx for every $x \in A$.
- R is **irreflexive** on A if $(x, x) \notin R$ for all $x \in A$.
- For each $x, y \in R$, R is **symmetric** if xRy implies yRx.
- For any $x, y \in R$, R is **antisymmetric** on A if $x = y$ whenever xRy and yRx.
- R is **transitive** if xRy and yRz implies xRz for every $x, y, z \in A$.
- R is **comparable** if either xRy or yRx for all $x, y \in A$.

An **equivalence relation** R on a set A is a relation on A that is reflexive, symmetric, and transitive.

Warm-Up Exercises

1. Suppose R and S are two equivalence relations on a set A. Prove that $R \cap S$ is also an equivalence relation.
2. Let R be a relation on $\mathbb{Z}$ such that xRy if and only if $x^2 + y^2$ is even. Prove that R is an equivalence relation. Describe its equivalence classes.
3. The relation $\sim$ defined on $R - \{0\}$ by $a \sim b$ if and only if $\frac{a}{b} \in \mathbb{Q}$ forms an equivalence relation. Prove that $[\sqrt{3}] = [\sqrt{12}]$.

Let X and Y be two sets. Consider the function $f : X \to Y$ from X into Y.

1. f is **injective** (or **one-to-one**) if $x \neq y$ implies $f(x) \neq f(y)$ for all $x, y \in X$.
2. f is **surjective** (or **onto**) if for every $y \in Y$ there exists $x \in X$ such that $f(x) = y$.
3. f is **bijective** (or **one-to-one correspondence**) if f is both injective and surjective.

Warm-Up Exercises

1. Consider the function $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined by $f((a, b)) = a - b + 3$. Prove that f is onto.
2. Define $f : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ defined by $f(x) = (2x, x^2)$. Prove that f is injective.
3. Consider the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$. What is the preimage or inverse image of $[0, 4]$ under f?

Partially Ordered Sets

Poset

Definition

A (binary) relation R on a set A is called a **partial order relation** on A (or **partial ordering** on A) if it is reflexive, transitive and antisymmetric. The set A together with R, often written (A, R), is called a **partially ordered set** or **poset**.

Example

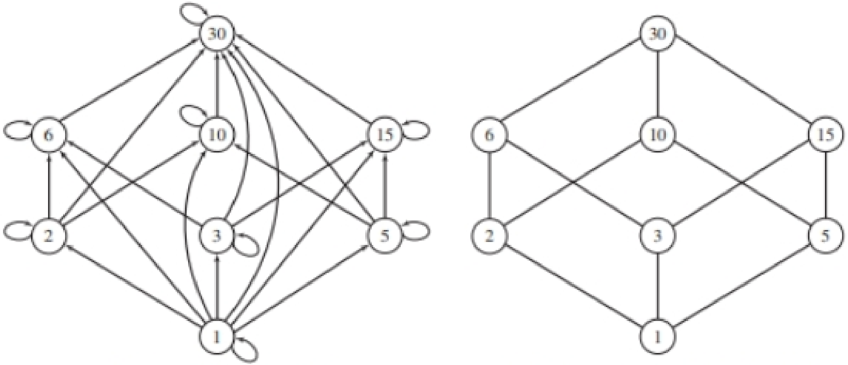
Let R be a relation on $\mathbb{R}$ given by xRy if $x \leq y$. Show that $(\mathbb{R}, R)$ is a poset.

Example

Let W be a relation on $\mathbb{N}$ defined by xRy if $x + y$ is even and $x \leq y$. Show that W is a partial ordering on $\mathbb{N}$.

Representation of a Poset

Let $M = \{1, 2, 3, 5, 6, 10, 15, 30\}$. The relation R defined by xRy if x divides y is a partial order for M. A digraph representing the relations is given below. The simplified digraph is called the **Hasse diagram** of the partial order R.



Upper and Lower Bound

Definition

Let R be a partial order for a set A. Also, suppose that B is any subset of A.

1. An element a of A is a **lower bound** for B if aRb for all $b \in B$.
2. An element a of A is a **upper bound** for B if bRa for all $b \in B$.

Definition

Let R be a partial order for a set A. Also, suppose that B is any subset of A.

- We say that $a \in A$ is a **least upper bound** for B (or **supremum** of B) if a is an upper bound for B and aRx for every upper bound x for B.
- Analogously, $a \in A$ is a **greatest lower bound** for B (or **infimum** of B) if a is a lower bound for B and xRa for every lower bound x for B.

We write $\sup(B)$ and $\inf(B)$ to denote the supremum and infimum of B respectively.

Example

1. For any set A, show that the power set $\mathcal{P}(A)$ of A with the relation $\subseteq$ is a poset.
2. Consider $A = \{1, 2, 3, 4, 5\}$ and $B = \{\{1, 2\}, \{1, 2, 3\}, \{1, 3\}\}$. Given the poset $(\mathcal{P}(A), \subseteq)$, find $\sup(B)$ and $\inf(B)$.

Property

Theorem

Let (R, A) *be a poset and* $B \subseteq A$. *If* $\sup(B)$ *exists then it must be unique. Similarly, if* $\inf(B)$ *exists then it must also be unique.*

Definition

Let R be a partial order on a set A. Assume $B \subseteq A$. If the greatest lower bound for B exists and is an element of B, it is called the **smallest** or **least element** of B. Moreover, if the least upper bound for B exists and is an element of B, it is called the **largest** or **greatest element** of B.

Minimal and Maximal Element

Definition

Let R be a partial order on a set A. Assume $B \subseteq A$. The element $b \in B$ is called a **maximal element** for B. if there exists no $y \in B$ such that xRy. Similarly, x is a **minimal element** for B if there does not exist $y \in B$ such that yRx.

Example

Let $M = \{1, 2, 3, 5, 6, 10, 15\}$. The relation R defined by xRy if x divides y is a partial ordering for M. What are the maximal and minimal elements of M?

Linear Order

Definition

A partial ordering R on a set A is a **linear** or **total ordering** on A if it is comparable. We say that the set together with the relation (A, R) is a **linearly ordered set**.

Examples

1. The poset $(\mathbb{R}, \leq)$ is a linearly ordered set.
2. The partial ordering $\subseteq$ on $\mathcal{P}(A)$ is not a linear ordering.

Definition

Let L be a linear ordering on a set A. The linearly ordered set (A, L) is a **well ordering** on A if every nonempty subset B of A contains a least element.

Theorem (Well-Ordering Theorem)

Every linearly ordered set can be well ordered.

Exercises

1. Suppose that (A, R) is a partially ordered set. Show that $\left(A, R^{-1}\right)$ is also a partially ordered set.
2. Let $\sim$ be the relation on $\mathbb{N}$ given by $a \sim b$ if there exists an integer k such that $b = 2^k a$. Show that $\sim$ is a partial ordering on $\mathbb{N}$.
3. Let $(A, \preceq)$ be a poset. Define a function $f : A \to P(A)$ by $f(a) = \{x : x \in A \text{ and } x \preceq a\}$.
   3.1 Prove that f is injective.
   3.2 Prove that $a \preceq b$ if and only if $f(a) \subseteq f(b)$. (In this case, we say that f is an **order-preserving** function.)
4. Let R be a transitive and reflexive relation on the set A. Define a relation $\approx$ on A by $x \approx y$ if and only if xRy and yRx.
   4.1 Show that $\approx$ is an equivalence relation on A.
   4.2 Define a relation $\preceq$ on $A/\approx$ by $[x] \preceq [y]$ if and only if xRy. Show that $\preceq$ is well-defined.
   4.3 Show that $(A/\approx, \preceq)$ is a poset.

Might be Useful

Definition

Lei (A, R) be a partially ordered set. An element x of A is said to be an **immediate successor** of $y \in A$ if yRx and there does not exist an element $z \in A$ such that $y < z < x$. Likewise, $x \in A$ is said to be an **immediate predecessor** of $y \in A$ if yRx and there is no element $z \in A$ such that $x < z < y$.

Theorem

In a totally ordered set, immediate successors and immediate predecessors (when they exist) are unique.

Might be Useful (Continuation)

Definition

A partially ordered set in which every nonempty subset that is bounded above has a least upper bound is said to have the **least upper bound property**. Analogously, a partially ordered set in which every nonempty subset that is bounded below has a greatest lower bound is said to have the **greatest lower bound property**.

Theorem

Every partially ordered set with the least upper bound property also has the greatest lower bound property.

Cardinality

Definition

A set A is said to have the **same cardinality** as B if there exists a bijection $f : A \to B$ from A onto B. We also say that A is **equinumerous** to B. We write $A \approx B$ if A and B have the same cardinality.

Examples

1. The sets $\{1, 2, 3\}$ and $\{a, b, c\}$ are equinumerous.
2. The set $\mathbb{Z}$ of integers and the set E of even integers have the same cardinality.
3. The Cartesian product of the sets A and $\{b\}$ has the same cardinality as A.

Numerically Equivalent

Theorem

The relation $\approx$ *defined on any collection of sets is an equivalence relation.*

Some Theorems

Theorem

For any set A, $A \times \{b\} \approx A$.

Theorem

Let $A_1 \approx A_2$ *and* $B_1 \approx B_2$ *such that* $A_1 \cap B_1 = \emptyset$ *and* $A_2 \cap B_2 = \emptyset$. *Then* $A_1 \cup B_1 \approx A_2 \cup B_2$.

Definition

Let $S_n = \{j \in \mathbb{Z}^+ : 1 \leq j \leq n\} = \{1, 2, \ldots, n\}$. A set A is said to be **finite** if A is empty or has the same cardinality as S_n for some $n \in \mathbb{Z}^+$. The set A has **cardinality** n (or 0 for the empty set), written $|A| = n$. If A is not finite, then A is **infinite**.

Theorem

Any set B equinumerous to a finite set A is a finite set and $|B| = |A|$.

Corollary

The cardinality of a finite set is unique.

Theorem

If A is a finite set and $x \notin A$ then $A \cup \{x\}$ is also finite and $|A \cup \{x\}| = |A| + 1$.

Corollary

If B is finite and $x \in B$, then $B - \{x\}$ is finite and $|B - \{x\}| = |B| - 1$.

Additional Results

Lemma

For each natural number m, if $A \approx S_m$, then A is a finite set and $|A| \leq m$.

Theorem

Every subset A of a finite set B is finite and $|A| \leq |B|$.

Corollary

If B is a subset of a finite set A and $B \approx A$, then $B = A$.

Theorem (Pigeonhole Principle)

For finite sets A and B, no injective function $f : A \to B$ from A into B exists if $|B| < |A|$.

Example

I have 7 pairs of socks in my drawer, one of each color of the rainbow. How many socks do I have to draw out in order to guarantee that I have grabbed at least one pair?

Denumerable Sets

Definition

A set D is said to be **countably infinite** or **denumerable** if $D \approx \mathbb{Z}^+$. A **countable** set is a set that is either finite or denumerable. A set is **uncountable** if it is not countable.

Examples

1. The set $\mathbb{N}$ of natural numbers is infinite.
2. The set $\mathbb{N}$ of positive integers is denumerable.
3. The open interval $(0, 1)$ is uncountable.
4. The set $\mathbb{Q}$ of rational numbers is countably infinite.

Properties on Denumerable Sets

Theorem

A subset of a denumerable set is countable.

Corollary

A subset of a countable set is countable.

Corollary

If D is denumerable and $f : A \to D$ is injective, then A is countable. In addition, A is denumerable when A is infinite.

Corollary

The Cartesian product $A \times B$ of two denumerable sets A and B is denumerable.

Theorem

If A is countable and B is denumerable then $A \cup B$ is a denumerable.

Dedekind-Infinite

Definition

A set D is said to be **Dedekind-infinite** if there exists a proper subset of D equinumerous to D.

Theorem

A set is Dedekind-infinite if and only if it is infinite.

Might be Useful

Theorem

Let A and B be finite sets, $|A \times B| = |A| \cdot |B|$ and $|A \times B| = |B \times A|$. Moreover, if $\{A_k\}_{k=1}^{n}$ is a collection of finite sets then

$$|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdot \cdots \cdot |A_n|.$$

Theorem

Let A and B be disjoint finite sets. Then

$$|A \cup B| = |A| + |B|.$$

In general, if A and B are finite sets then

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

Might be Useful (Continuation)

Corollary

For finite sets A and B,

$$|A \cup B| \leq |A| + |B|.$$

Theorem

Let A, B, C, and D be sets such that $A \approx C$ and $B \approx D$, then $A \times B \approx C \times D$.

Theorem

If A, B, C, and D are sets such that $A \approx C$, $B \approx D$ and $A \cap B = \emptyset$ and $C \cap D = \emptyset$ then $A \cup B \approx C \cup D$.

Might be Useful (Continuation)

Theorem

If $A \subseteq B$ where B is a finite, then A is finite and $|A| \leq |B|$.

Theorem

If A is a set with cardinality n, then $|\mathcal{P}(A)| = 2^n$.

Might be Useful (Continuation)

Theorem

If A is denumerable, then $A \cup \{x\}$ is denumerable.

Corollary

If A is denumerable and B is finite, then $A \cup B$ is countably infinite.

Corollary

If $\mathcal{A}$ is a finite collection of countable sets, then $\bigcup_{A \in \mathcal{A}} A$ is countable.

Corollary

If $\mathcal{A}$ is a denumerable family of countable sets, then $\bigcup_{A \in \mathcal{A}} A$ is countable.

Groups

Definition

Let G be a set. A **binary operation** on G is a function that assigns each ordered pair of elements of G to an element of G.

The condition which maps an ordered pair from G to an element in G is called the **closure property**.

Examples

1. The usual addition, subtraction, and multiplication of integers are binary operations.
2. Division of integers is not a binary operation.
3. The operations addition modulo n and multiplication modulo n on

$$\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$$

   are binary operations.
4. We define an operation $*$ on $\mathbb{Z}^+$ by $a * b = \min\{a, b\}$. Also, let $*'$ be an operation on $\mathbb{Z}^+$ such that $a *' b = a$. The operations $*$ and $*'$ are binary operations on $\mathbb{Z}^+$.

Definition

A (nonempty) set G together with a binary operation $*$ is a group, denoted by $(G, *)$, under $*$ if the following properties are satisfied:

1. (Associativity) For all a, b, and c in G, we have $(a * b) * c = a * (b * c)$.
2. (Existence of Identity) There exists e in G such that $a * e = e * a = a$ for all a in G.
3. (Existence of Inverse) For each element a in G, there exists an element b in G such that $a * b = b * a = e$.

The element e is called an **identity** of the group. The **inverse** b of a satisfies $a * b = b * a = e$, and we write $b = a^{-1}$. A group with only one element (or consisting only of the identity element) is called a **trivial group**.

1. The set of integers $\mathbb{Z}$, the set of rational numbers $\mathbb{Q}$, and the set of real numbers $\mathbb{R}$ are groups under the usual addition.
2. The set of integers $\mathbb{Z}$ under ordinary multiplication and under ordinary subtraction are not groups. However, the set of positive rational numbers $\mathbb{Q}_{>0}$ and the set of nonzero real numbers R^* are groups under the usual multiplication.
3. The set S of positive irrational numbers together with the rational number 1 under ordinary multiplication is not a group.
4. The set of 2×2 matrices with real entries is a group under matrix addition. Moreover, the set

$$GL(2, \mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R}, ad - bc \neq 0 \right\}$$

consisting of 2×2 matrices with real entries and nonzero determinants is a group under matrix multiplication. This group is called the **general linear group** of degree 2 over $\mathbb{R}$.

More Examples

1. Let G be a set consisting all real-valued functions on $\mathbb{R}$, with the binary operation given by pointwise addition of functions, that is, $(f+g)(x) = f(x) + g(x)$ for all $x \in \mathbb{R}$.
2. Given a positive integer n, the set $\mathbb{Z}_n = \{1, \dots, n-1\}$ is a group under addition $+_n$ modulo n.
3. The following table defines a binary operation $*$ on the set $S = \{a, b, c\}$.

*	a	b	c
a	a	b	c
b	b	a	c
c	c	b	a

4. Let $\mathbb{Z}_n^* = \{x : \gcd(x, n) = 1\}$ where $n \in \mathbb{Z}^+$. The set $\mathbb{Z}_n^*$ under multiplication $\cdot_n$ modulo n is a group.

1. There are only two groups (up to an isomorphism) with exactly four elements. The first group is $(\mathbb{Z}_4, +_4)$ and the second group is known as the **Klein 4-group** denoted as V under the operation defined by the table

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Abelian Group

Definition

An **Abelian** or commutative group is a group G that has a commutative binary operation, that is, $a * b = b * a$ for every pair of elements a and b in G. Otherwise, we say that G is **non-Abelian**.

Definition

Given a group $(G, *)$, we say that $(G, *)$ is a **finite group** if G is a finite set. Otherwise, $(G, *)$ is an **infinite group**. The number of elements in a group $(G, *)$ is called the **order** of G denoted by $|G|$. By assumption, the order of an infinite group is equal to ∞.

1. Let $\star$ be an operation on $\mathbb{Z} \times \mathbb{Z}$ defined by

$$(a, b) \star (c, d) = (ad + bc, bd).$$

   Determine if the set $\mathbb{Z} \times \mathbb{Z}$ under $\star$ is a group.

2. Let $G = \{a + b\sqrt{2} \in \mathbb{R} : a, b \in \mathbb{Q}\}$. Prove that G is a group under ordinary addition.
3. Let G be the set of all non-constant linear functions, that is, functions $f : \mathbb{R} \to \mathbb{R}$ of the form $f(x) = ax + b$ with $a, b, \in \mathbb{R}$ and $a \neq 0$. Show that G is a group under the operation

$$x * y = \frac{x + y}{1 + xy}.$$

4. A group $(G, *)$ is Abelian when $x^2 = e$ for every x in G.

Properties of a Group

Theorem

Let $(G, *)$ be a group. Suppose a and b are any elements of G. The linear equations $a * x = b$ and $y * a = b$ have unique solutions x and y in G. In particular, the identity of a group and the inverse of every element in a group are unique.

Theorem

For a group G, the right and left cancellation laws hold, that is, $ba = ca$ implies $b = c$ and $ca = cb$ implies $a = b$ for all a, b, and c in G.

Theorem

For each element a in a group G, the inverse $\left(a^{-1}\right)^{-1}$ of a^{-1} is a.

Convention

We sometimes omit the operation $*$ and write ab to denote $a * b$. Moreover, the expression a^n for a positive integer n denotes the product

$$aa \cdots a \quad (n \text{ factors})$$

and $a^n = e$ for $n = 0$.When n is negative,

$$a^n = \left(a^{-1}\right)^{|n|}.$$

Theorem (Socks-Shoes Property)

For any elements a and b of a group, $(ab)^{-1} = b^{-1}a^{-1}$.

Theorem

For any element a of a group and every integer m and n, we have

1. $a^{m+n} = a^m a^n$,
2. $(a^m)^n = a^{mn}$.

Group Table and Properties

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

1. Every element of the gropu must appear once and only once in each row and column of the table.
2. The group is Abelian if the matrix is symmetric along the diagonal.

Definition

Let $(G, *)$ and $(H, \star)$ be groups, and $f : G \to H$. We say that f is a **group isomorphism** if f is a bijective homomorphism, that is,

1. The function f is one-to-one and maps onto H.
2. For all $a, b \in G$, $f(a * b) = f(a) \star f(b)$.

We say that $(G, *)$ is **isomorphic** to $(H, \star)$ if there exists an isomorphism between $(G, *)$ and $(H, \star)$.

Properties of an Isomorphism

Theorem

Let $f : G \to H$ *be a group isomorphism between* $(G, *)$ *and* $(H, \star)$*. Then* $f^{-1} : H \to G$ *is also a group isomorphism.*

Examples

1. The groups $(\mathbb{Z}, +)$ and $(2\mathbb{Z}, +)$ are isomorphic.
2. The groups $(\mathbb{Z}_n, +_n)$ and $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, \oplus\right)$ are isomorphic.

Definition

A **permutation** of a set A is a function $\phi : A \to A$ from a set into itself that is both one-to-one and onto.

Theorem

The collection of all permutations of a set A into itself is a group under function composition.

The group of all permutations on a set A forms a group called the **symmetric group** on A. By considering A as the set $S_n := \{1, \dots, n\}$, we call the group as the **symmetric group on n letters**.

Two-Line Notation

A permutation σ on S_n can be expressed in the two-line notation shown below

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

With this notation, the inverse of a permutation is given by

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

Examples

1. What are the elements of S_2 and S_3?
2. Consider the permutations on S_6 given by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 6 & 1 & 4 & 3 \end{pmatrix} \text{ and } \delta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 6 & 5 & 3 \end{pmatrix}.$$

   What are $\sigma \circ \delta$ and $\delta \circ \sigma$?

Given a permutation on S_6,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{pmatrix},$$

it can be expressed in cycle notation as

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

A cycle of the form $(a_1\ a_2\ \ldots\ a_m)$ is called a **cycle of length** m or an m**-cycle**. Cycles that have no entries in common are said to be **disjoint**.

1. What is the cycle notation for

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{pmatrix}?$$

2. Consider the permutations in S_7 given by $\sigma = (1\,5\,7\,3)$ and $\delta = (2\,4)$, compute for $\sigma\delta$ and $\delta\sigma$.

Properties

Theorem

Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.

Theorem

Given any pair of disjoint cycles σ and δ, we must have $\sigma\delta = \delta\sigma$.

Theorem

Every permutation is a product of 2-cycles.

MATH 120 (Algebraic Structures I) Topics

1. Binary Operation and Groups
2. Subgroups
3. Cyclic Groups
4. Permutation and Dihedral Groups
5. Factor or Quotient Groups
6. Cosets and Normal Groups
7. Lagrange's Theorem
8. Group Homomorphisms and Isomorphisms
9. External Direct Product and Fundamental Theorem of Abelian Groups

Questions?

References i

C. M. Campbell.
***Introduction to Advanced Mathematics: A Guide to Understanding Proofs*.**
Brooks/Cole, 2012.

R. Hammack.
***Book of Proof*.**
Richard Hammack, 3.2 edition, 2018.

M. W. Liebeck.
***A Concise Introduction to Pure Mathematics*.**
Chapman & Hall/CRC, 2017.

N. R. Nicholson.
***A Transition to Proof: An Introduction to Advanced Mathematics*.**
CRC Press, 2019.

References ii

C. E. Roberts.
***Introduction to Mathematical Proofs: A Transition to Advanced Mathematics*.**
CRC Press, Taylor & Francis Group, 2015.

D. Smith, M. Eggen, and S. R. Andre.
***A Transition to Advanced Mathematics*.**
Cengage Learning, 2015.