MANCHESTER 1824
The University of Manchester

Combinatorial Mesh Calculus (CMC): Lecture 2

Lectured by: Dr. Kiprian Berbatov[1]

Lecture Notes Compiled by: Muhammad Azeem[1]

Under the supervision of: Prof. Andrey P. Jivkov[1]

[1] Department of Mechanical and Aerospace Engineering, The University of Manchester, Oxford Road, Manchester M13 9PL, UK

Definition of an n–ary Operation

Definition.

Let X be a nonempty set and $n \in \mathbb{N}$. An *n–ary operation* on X is a function

$$f : X^n \longrightarrow X.$$

Special cases:

- $n = 0$: a *nullary operation* (a constant $c \in X$).
- $n = 1$: a *unary operation* $f : X \to X$.
- $n = 2$: a *binary operation* $f : X \times X \to X$.

Notation: For a binary operation, we often write

$$f(x, y) = x * y.$$

Examples of n–ary Operations

Let $X = \mathbb{Z}$.

Nullary (0–ary):

$$c = 0 \in \mathbb{Z}.$$

Unary (1–ary):

$$f_1(x) = -x, \quad f_2(x) = x + 1, \quad f_3(x) = \frac{1}{x^2 + 1}.$$

Each maps $\mathbb{Z} \to \mathbb{Z}$ or $\mathbb{R} \to \mathbb{R}$.

Binary (2–ary):

$$f_1(x, y) = x + y, \quad f_2(x, y) = xy, \quad f_3(x, y) = x^y.$$

Check closure:

- $x + y \in \mathbb{Z}$: $\checkmark$ binary operation on $\mathbb{Z}$.
- $xy \in \mathbb{Z}$: $\checkmark$ binary operation.
- x^y may not be integer for all $x, y \in \mathbb{Z}$ (e.g. $x = -1, y = \frac{1}{2}$), so $\times$, not closed on $\mathbb{Z}$.

Associativity and Commutativity

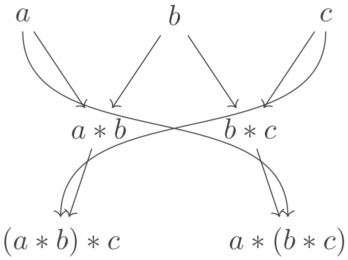
Let $* : X \times X \to X$ be a binary operation.

Definition (Associativity):

$$a * (b * c) = (a * b) * c, \quad \forall a, b, c \in X.$$

Definition (Commutativity):

$$a * b = b * a, \quad \forall a, b \in X.$$



Example

- On $(\mathbb{Z}, +)$: addition is both **associative** and **commutative**, since for all $a, b, c \in \mathbb{Z}$,

$$(a+b)+c = a+(b+c), \qquad a+b = b+a.$$

- On $(\mathbb{R}, -)$: subtraction is **neither associative nor commutative**, e.g.

$$(5-3)-2 = 0 \neq 5-(3-2) = 4, \quad 5-3 \neq 3-5.$$

- On $(\mathbb{R}, \times)$: multiplication is **associative and commutative**, since

$$(ab)c = a(bc), \qquad ab = ba.$$

The University of Manchester

Example

- On $(M_{2\times 2}(\mathbb{R}), \times)$: matrix multiplication is **associative** but **not commutative**; for example,

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \; B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \implies AB \neq BA.$$

- On $(\mathbb{R}, \div)$: division is **neither associative nor commutative**, e.g.

$$(8 \div 4) \div 2 = 1 \neq 8 \div (4 \div 2) = 4.$$

- On the set of functions $F(X)$ with pointwise addition $(f+g)(x) = f(x) + g(x)$: operation is both **associative** and **commutative**.

Identity (Neutral) Elements

Definition.

Let $(X, *)$ be a set with a binary operation. An element $e \in X$ is called a

- **left identity** if $e * x = x$ for all $x \in X$,
- **right identity** if $x * e = x$ for all $x \in X$,
- **two–sided identity (neutral element)** if both hold.

Remark

If both left and right identities exist, they are necessarily equal (proved later).

Examples

- **Example:** $(\mathbb{N}, +): \; e = 0; \quad (\mathbb{R}, \times): \; e = 1.$
- **Counterexample:** Consider the operation $(-)$ on the real numbers $\mathbb{R}$, defined by $a * b = a - b$. We want to check whether there exists an element $e \in \mathbb{R}$ such that

$$a - e = a = e - a, \quad \forall a \in \mathbb{R}.$$

The first equation $a - e = a$ implies $e = 0$. Substituting $e = 0$ into the second equation gives $e - a = 0 - a = -a$. For this to equal a for all a, we would need $-a = a$, which is true only when $a = 0$.
Hence no single element e satisfies both conditions for all $a \in \mathbb{R}$. Therefore, subtraction has *no identity element* — it fails to form a monoid under subtraction.

MANCHESTER 1824
The University of Manchester

Inverse Elements

Definition.

Let $(X, *, e)$ have identity element e. An element $x' \in X$ is called

- a **left inverse** of x if $x' * x = e$,
- a **right inverse** of x if $x * x' = e$,
- an **inverse** if both hold.

Examples:

$$(\mathbb{Z}, +, 0): \text{ inverse of } x \text{ is } -x,$$

$$(\mathbb{R}^+, \times, 1): \text{ inverse of } x \text{ is } 1/x.$$

The University of Manchester

Example 1: $(\mathbb{N}, +)$

Let $X = \mathbb{N}$, define $\mu(x, y) = x + y$.

- **Associative?** $(x + y) + z = x + (y + z)$: $\checkmark$
- **Commutative?** $x + y = y + x$: $\checkmark$
- **Identity?** 0 satisfies $x + 0 = 0 + x = x$: $\checkmark$
- **Inverse?** No, since for $x > 0$, no $y \in \mathbb{N}$ s.t. $x + y = 0$: $\times$

Conclusion: $(\mathbb{N}, +)$ is a commutative monoid, not a group.

Example 2: $(\mathbb{Z}, \times)$

Let $X = \mathbb{Z}$, $\mu(x, y) = xy$.

- Associative: $x(yz) = (xy)z$: $\checkmark$
- Commutative: $xy = yx$: $\checkmark$
- Identity: 1: $\checkmark$
- Inverse: only for $x = \pm 1$: $\checkmark$ partial.

Conclusion: $(\mathbb{Z}, \times)$ is a commutative monoid, not a group.

The University of Manchester

Example 3: $(\mathbb{R}^+, \times)$

Let $X = \mathbb{R}^+$, $\mu(x, y) = xy$.

- Associative: $\checkmark$
- Commutative: $\checkmark$
- Identity: 1: $\checkmark$
- Inverse: $1/x \in \mathbb{R}^+$: $\checkmark$

Conclusion: $(\mathbb{R}^+, \times)$ is an abelian group.

The University of Manchester

Example 4: $(\mathbb{R}, \times)$

- Associative: $\checkmark$
- Commutative: $\checkmark$
- Identity: 1: $\checkmark$
- Inverse: fails for $x = 0$ (no $1/0$): $\times$

Hence $(\mathbb{R}, \times)$ is a commutative monoid, not a group.

The University of Manchester

Example 5: A Finite Operation Table

Let $X = \{a, b, c\}$ with operation $*$ defined as

$$\begin{array}{c|ccc} * & a & b & c \\ \hline a & c & a & c \\ b & a & b & c \\ c & c & c & a \end{array}$$

- Check for left/right identity: none satisfies $e * x = x * e = x$.
- Commutativity? Table not symmetric $\rightarrow \times$
- Associativity? test fails for example $a * (b * c) \neq (a * b) * c$: $\times$
- Invertibility? none globally.

Conclusion: Not a monoid, just a magma (set with binary operation).

Proposition: Uniqueness of the Unit

Proposition.

If a binary operation $*$ on X admits a left identity e_L and a right identity e_R, then they coincide: $e_L = e_R$.

Proof.

$$e_L = e_L * e_R \quad \text{(since } e_R \text{ is right identity)}$$

$$e_L * e_R = e_R \quad \text{(since } e_L \text{ is left identity)}$$

Hence $e_L = e_R$. $\square$

Corollary

A binary structure can have at most one identity element.

The University of Manchester

Definition of a Monoid

A *monoid* is a triple $(M, *, e)$ such that:

1. $* : M \times M \to M$ is a binary operation,
2. $*$ is associative: $(a * b) * c = a * (b * c)$,
3. $e \in M$ is an identity: $e * x = x * e = x$.

$$\begin{tikzcd}
 & M \times M \times M \arrow[dl, "* \times \mathrm{id}"'] \arrow[dr, "\mathrm{id} \times *"] & \\
M \times M \arrow[dr, "*"'] & & M \times M \arrow[dl, "*"] \\
 & M &
\end{tikzcd}$$

Remark on Commutative (Abelian) Monoids.

A monoid $(M, *, e)$ consists of a set M, a binary operation $* : M \times M \to M$, and an identity element e satisfying:

$$(a * b) * c = a * (b * c), \qquad e * a = a * e = a, \quad \forall a, b, c \in M.$$

If, in addition, the operation $*$ satisfies

$$a * b = b * a, \quad \forall a, b \in M,$$

then the monoid is called a **commutative monoid**, or equivalently, an **abelian monoid**.

Intuition: Commutativity means that the order in which elements are combined does not affect the result. In a commutative monoid, both the associative property and the commutative property coexist with an identity element.

Remark

Examples:

- $(\mathbb{N}, +, 0)$: addition of natural numbers — commutative and associative with identity 0.
- $(\mathbb{R}, \times, 1)$: multiplication of real numbers — commutative with identity 1.
- $(\mathbb{Z}, +, 0)$: addition of integers — commutative with identity 0.

Non-Example: $(M_{2\times 2}(\mathbb{R}), \times, I_2)$ is a monoid because matrix multiplication is associative and I_2 acts as the identity, but it is *not commutative* in general, since for many matrices A, B, $AB \neq BA$.

Historical Note: The term *abelian* originates from Niels Henrik Abel, a 19th-century mathematician who first studied commutative algebraic structures.

Examples of Monoids

- $(\mathbb{N}, +, 0)$ — additive monoid.
- $(\mathbb{N}, \times, 1)$ — multiplicative monoid.
- $(\mathbb{R}, \times, 1)$ — commutative monoid (but not group).
- $(M_{2\times 2}(\mathbb{Z}), +, O)$ where O is the zero matrix.
- $(M_{2\times 2}(\mathbb{Z}), \times, I_2)$ where I_2 is identity matrix.

Visualization

$$(\mathbb{N}, +) \longrightarrow (\mathbb{Z}, +) \longrightarrow (\mathbb{R}, +)$$

extension of inverses

Equality of Left and Right Inverses

Proposition. Let $(X, *, e)$ be a monoid, and let $a, b, c \in X$. If b is a left inverse of a and c is a right inverse of a, i.e.

$$b * a = e \quad \text{and} \quad a * c = e,$$

then $b = c$. Consequently, a is invertible and $b = c = a^{-1}$.

Proof.

$$b = b * e = b * (a * c) = (b * a) * c = e * c = c.$$

Hence $b = c$, and both satisfy $a * b = b * a = e$.

Conclusion

In a monoid, if both left and right inverses exist for an element, they coincide.

Product of Invertible Elements

The University of Manchester

Proposition. Let $(X, *, e)$ be a monoid. If $a, b \in X$ are invertible, then so is $a * b$.

Proof. Let a^{-1} and b^{-1} denote their inverses:

$$a * a^{-1} = e = a^{-1} * a, \quad b * b^{-1} = e = b^{-1} * b.$$

Consider $(a * b) * (b^{-1} * a^{-1})$:

$$(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = a * a^{-1} = e.$$

Similarly,

$$(b^{-1} * a^{-1}) * (a * b) = b^{-1} * (a^{-1} * a) * b = b^{-1} * e * b = e.$$

Thus $(b^{-1} * a^{-1})$ is the inverse of $(a * b)$.

Hence: The set of invertible elements in a monoid is closed under the binary operation.

MANCHESTER 1824
The University of Manchester

Definition of a Group

Definition. A *group* is a quadruple $(G, *, e, i)$ where

1. $(G, *, e)$ is a monoid,
2. For every $x \in G$, there exists an inverse $i(x) \in G$ such that

$$x * i(x) = i(x) * x = e.$$

Remarks:

- The map $i : G \to G$ sending $x \mapsto i(x)$ is called the *inverse map*.
- The group is called *commutative* or *abelian* if

$$x * y = y * x, \quad \forall x, y \in G.$$

Examples of Groups

Examples:

1. $(\mathbb{Z}, +, 0, -)$ Abelian group under addition.
   $\forall x \in \mathbb{Z},\ x + (-x) = 0.$
2. $(M_{n\times n}(\mathbb{Z}), +, O_n, -)$ Additive abelian group of integer matrices.
3. $(M_{n\times n}(\mathbb{R}), +, O_n, -)$ and $(M_{n\times n}(\mathbb{Q}), +, O_n, -)$ Additive abelian groups of real or rational matrices.

$$(\mathbb{Z}, +) \longrightarrow (\mathbb{Q}, +) \longrightarrow (\mathbb{R}, +)$$

extensions by density

All are *abelian* since addition is commutative.

Definition: Group of Units

MANCHESTER 1824
The University of Manchester

Definition.

Let $(X, *, e)$ be a monoid. The set of all invertible elements of X is denoted by

$$X^* = \{ x \in X \mid \exists x^{-1} \in X,\ x * x^{-1} = x^{-1} * x = e \}.$$

This set forms a group under $*$, called the **group of units** of X.

Proof (Sketch).

- Closure: proved earlier (product of invertibles is invertible).
- Associativity: inherited from the monoid.
- Identity: $e \in X^*$, $e^{-1} = e$.
- Inverse: each $x \in X^*$ has inverse $x^{-1} \in X^*$.

Examples of Groups of Units

Multiplicative Groups:

$(X, *, e)$	X^*	Reason
$(\mathbb{Z}, \times, 1)$	$\{-1, 1\}$	only ± 1 have multiplicative inverses in $\mathbb{Z}$
$(\mathbb{Q}, \times, 1)$	$\mathbb{Q} \setminus \{0\}$	nonzero invertible
$(\mathbb{R}, \times, 1)$	$\mathbb{R} \setminus \{0\}$	nonzero invertible

Additive/Other Groups:

$(\mathbb{N}, +, 0)$	$\{0\}$	identity only
$(\mathbb{N}, \times, 1)$	$\{1\}$	1 only

Remark: Restriction of a Function

Let X, Y are two sets and $f : X \to Y$ and $U \subseteq X$.

Definition. The *restriction* of f to U is the function

$$f|_U : U \to Y, \quad f|_U(x) = f(x) \text{ for } x \in U.$$

Remark. If $U \subseteq V \subseteq X$, then

$$(f|_V)|_U = f|_U.$$

$$\begin{tikzcd}
U \arrow[r, "f|_U"] \arrow[d, hook] & Y \\
X \arrow[ur, "f"'] &
\end{tikzcd}$$

Remark: Shrink of a Function

Remark (Shrink). Sometimes one considers a *shrinking* of a function's domain to a subset where a certain property holds (e.g., continuity, invertibility).
Formally, if $P(x)$ is a property on X, define

$$\text{Shrink}_P(f) = f|_{\{x\in X \mid P(x) \text{ holds}\}}.$$

Thus, a *shrink* is a restricted version of f preserving only the portion of its domain where it satisfies a given property.

General and Special Linear Groups

Definition (General Linear Group).

For a field F and integer $n \geq 1$,

$$GL_n(F) = \{A \in M_{n\times n}(F) \mid \det(A) \neq 0\}.$$

Under matrix multiplication, $GL_n(F)$ forms a group.
Identity: I_n.
Inverse: $A^{-1} = \frac{1}{\det(A)} \operatorname{adj}(A)$.

Definition (Special Linear Group).

$$SL_n(F) = \{A \in GL_n(F) \mid \det(A) = 1\}.$$

It is a normal subgroup of $GL_n(F)$.

Relation Between $\mathbf{GL_n}$ and $\mathbf{SL_n}$

$$\mathbf{1} \longrightarrow \mathbf{SL_n}(\mathbf{F}) \longrightarrow \mathbf{GL_n}(\mathbf{F}) \xrightarrow{\text{det}} \mathbf{F}^* \longrightarrow \mathbf{1}$$

Short Exact Sequence

$$1 \to SL_n(F) \to GL_n(F) \xrightarrow{\text{det}} F^* \to 1$$

Interpretation: $\mathbf{SL_n}(\mathbf{F})$ (matrices with determinant 1) is the **kernel** of the determinant map, making it a normal subgroup of $\mathbf{GL_n}(\mathbf{F})$. The quotient group $\mathbf{GL_n}(\mathbf{F})/\mathbf{SL_n}(\mathbf{F})$ is isomorphic to $\mathbf{F}^*$, the multiplicative group of the field F.

The University of Manchester

Proposition on Composition of Functions

Let A, B, C, D be sets and let $f : A \to B,\ g : B \to C,\ h : C \to D.$

Proposition.

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

That is, function composition is associative.

Proof. For all $x \in A$,

$$[h \circ (g \circ f)](x) = h(g(f(x))) = [(h \circ g) \circ f](x).$$

Therefore both sides define the same function.

Consequences

Function composition forms a monoid operation on the set of all maps from a set to itself.

The University of Manchester

Corollary: The Function Monoid

Corollary.

Let A be a set. Then $(\mathrm{End}(A), \circ, \mathrm{id}_A)$ is a monoid, where $\mathrm{End}(A) = \{f : A \to A\}$.

Proof.

- Composition is associative (previous proposition).
- Identity function acts as neutral element: $f \circ \mathrm{id}_A = \mathrm{id}_A \circ f = f$.

Hence it satisfies monoid axioms. $\square$

Definition: Group of Bijections

Automorphisms

The set of all bijections $f : A \to A$ under composition forms a group, denoted by $\mathrm{Aut}(A)$ or S_A, called the *group of automorphisms (permutations)* of A.

Properties:

- Closure: composition of bijections is bijection.
- Associativity: inherited from function composition.
- Identity: id_A.
- Inverse: each bijection has inverse function.

The University of Manchester

Permutation Group S_n

Definition.

For a finite set $A = \{1, 2, \ldots, n\}$,

$$S_n = \{\text{all bijections } A \to A\}$$

is called the *symmetric group on* n *letters*. $|S_n| = n!$.

Notation:

permutations often written in two-line form:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \text{means } \sigma(1) = 2,\ \sigma(2) = 3,\ \sigma(3) = 1.$$

Example: The Group S_3

Elements of S_3:

identity:	$e = (1)(2)(3)$,
transpositions:	$(12), (13), (23)$,
3-cycles:	$(123), (132)$.

Non-commutativity Example:

$$(12) \circ (23) = (123), \qquad (23) \circ (12) = (132),$$

and $(123) \neq (132)$. Hence S_3 is **not commutative** (non-abelian).

$$\begin{tikzcd}
& (132) & \\
(12) \arrow[rr] \arrow[dr] & & (23) \arrow[ul] \\
& (123) &
\end{tikzcd}$$

Summary

- Proved equality of left and right inverses and closure of invertibles.
- Defined groups, abelian groups, and examples.
- Introduced the group of units X^*.
- Defined $GL_n(F)$, $SL_n(F)$ with exact-sequence relation.
- Proved associativity of composition, showed $(\mathrm{End}(A), \circ)$ monoid.
- Defined groups of bijections and permutation groups S_n, with S_3 as first non-abelian example.
- Clarified restriction and shrink remarks for functions.

MANCHESTER 1824
The University of Manchester

Thanks