Combinatorial Mesh Calculus (CMC): Lecture 3

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

MANCHESTER 1824
The University of Manchester

Definition: Monoid Homomorphism

Definition. Let $(M, *, e_M)$ and $(N, \circ, e_N)$ be monoids. A function $f : M \to N$ is called a **monoid homomorphism** if it satisfies:

1. **Compatibility with operation:**

$$f(a * b) = f(a) \circ f(b), \quad \forall a, b \in M.$$

2. **Preservation of identity:**

$$f(e_M) = e_N.$$

Diagrammatic Representation:

$$\begin{tikzcd} M \times M \arrow[r, "f \times f"] \arrow[d, "*"'] & N \times N \arrow[d, "\circ"] \\ M \arrow[r, "f"'] & N \end{tikzcd}$$

Commutativity of the diagram encodes: $f(a * b) = f(a) \circ f(b)$.

Examples of Monoid Homomorphisms

Example 1.

$(\mathbb{N}, +, 0)$ and $(\mathbb{N}, \times, 1)$ Define $f : \mathbb{N} \to \mathbb{N}$ by $f(n) = 2^n$.

$$f(a+b) = 2^{a+b} = 2^a \cdot 2^b = f(a)f(b).$$

Hence f is a monoid homomorphism.

Example 2.

$(\mathbb{R}, +, 0)$ and $(\mathbb{R}^+, \times, 1)$ Define $f(x) = e^x$.

$$f(x+y) = e^{x+y} = e^x e^y = f(x)f(y).$$

Thus f is a monoid (and in fact group) homomorphism.

Definition: Group Homomorphism

The University of Manchester

Definition.

Let $(G, *, e_G, i_G)$ and $(H, \circ, e_H, i_H)$ be groups. A map $f : G \to H$ is called a **group homomorphism** if it satisfies:

1. $f(a * b) = f(a) \circ f(b)$ (operation preservation)
2. $f(e_G) = e_H$ (identity preservation)
3. $f(i_G(a)) = i_H(f(a))$ (inverse preservation)

$$\begin{tikzcd}
G \times G \arrow[r, "f \times f"] \arrow[d, "*"'] & H \times H \arrow[d, "\circ"] \\
G \arrow[r, "f"'] & H
\end{tikzcd}$$

Diagrammatic form: The diagram commutes if $f(a * b) = f(a) \circ f(b)$.

Homomorphism Property Reduction

Proposition.

Let $f : G \to H$ be a function between groups. If f satisfies only

$$f(a * b) = f(a) \circ f(b),$$

then automatically:

$$f(e_G) = e_H, \quad f(a^{-1}) = f(a)^{-1}.$$

Proof. $f(e_G) = f(e_G * e_G) = f(e_G) \circ f(e_G) \Rightarrow f(e_G) = e_H.$
Next,

$$e_H = f(e_G) = f(a * a^{-1}) = f(a) \circ f(a^{-1}) \Rightarrow f(a^{-1}) = f(a)^{-1}. \quad \square$$

Hence: Only property (1) is needed to check; others follow automatically.

Isomorphism of Monoids or Groups

Definition.

Let $(X, *, e_X)$ and $(Y, \circ, e_Y)$ be monoids (or groups). A map $f : X \to Y$ is called an *isomorphism* if:

1. f is a homomorphism;
2. f is bijective;
3. f^{-1} is also a homomorphism.

Remark.

If f is bijective and satisfies $f(a * b) = f(a) \circ f(b)$, then its inverse f^{-1} automatically respects the operations. Hence, bijectivity is enough to guarantee isomorphism.

Notation:

$$(X, *, e_X) \cong (Y, \circ, e_Y).$$

Read as "X and Y are isomorphic as monoids (or groups)."

Example: Exponential Isomorphism

Example.

$$(\mathbb{R}, +, 0) \xrightarrow{f(x)=e^x} (\mathbb{R}^+, \times, 1).$$

Check:

$$f(x+y) = e^{x+y} = e^x e^y = f(x)f(y), \quad f(0) = 1.$$

Inverse map: $f^{-1}(y) = \ln(y)$. Then

$$\ln(xy) = \ln(x) + \ln(y).$$

Hence both f and f^{-1} are homomorphisms.

$$(\mathbb{R}, +) \cong (\mathbb{R}^+, \times).$$

The University of Manchester

Subgroup

Definition.

Let $(G, *, e, i)$ be a group. A subset $H \subseteq G$ is a *subgroup* of G, if it is a group with the same operations restricted to H. In other words, we need:

1. $e \in H$ (contains identity),
2. $\forall a, b \in H,\ a * b \in H$ (closed under operation),
3. $\forall a \in H,\ i(a) \in H$ (closed under inverses).

We denote it as $H \leq G$.

MANCHESTER 1824
The University of Manchester

Simplified Subgroup Test

Remark.

The above three properties can be reduced to a single condition:

$$\forall a, b \in H, \quad a * b^{-1} \in H.$$

Proof.

- Let $a = b = e$: gives $e \in H$.
- For $a, b \in H$, $b^{-1} \in H$ so $a * b^{-1} \in H \Rightarrow$ closure.
- Taking $a = e$, $e * b^{-1} = b^{-1} \in H$ gives closure under inverses.

Hence condition (4) implies all three original subgroup properties.
$\square$

MANCHESTER 1824
The University of Manchester

Example 1: $(\mathbb{Z}, +)$ and $n\mathbb{Z}$

Let $G = (\mathbb{Z}, +, 0)$ and $H = n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$.

Proof.

- $0 = n \cdot 0 \in n\mathbb{Z}$.
- For $a = nk_1, b = nk_2 \in n\mathbb{Z}$, $a - b = n(k_1 - k_2) \in n\mathbb{Z}$.

Hence H is a subgroup of G.

$$n\mathbb{Z} \leq \mathbb{Z}.$$

Diagram:

$$\mathbb{Z} \supset 2\mathbb{Z} \supset 4\mathbb{Z} \supset 8\mathbb{Z} \supset \cdots$$

Chain of nested subgroups under divisibility.

Example 2: $SL_n(\mathbb{R})$ in $GL_n(\mathbb{R})$

Let

$$G = GL_n(\mathbb{R}) = \{A \in M_{n\times n}(\mathbb{R}) \mid \det(A) \neq 0\},$$

$$H = SL_n(\mathbb{R}) = \{A \in G \mid \det(A) = 1\}.$$

Proof.

- $I_n \in H$ since $\det(I_n) = 1$.
- If $A, B \in H$, then $\det(AB) = \det(A)\det(B) = 1 \cdot 1 = 1 \Rightarrow AB \in H$.
- If $A \in H$, then $\det(A^{-1}) = 1/\det(A) = 1 \Rightarrow A^{-1} \in H$.

Hence $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$.

Two Views: $\mathbf{GL_n}(\mathbb{R})$, $\mathbf{SL_n}(\mathbb{R})$

Subgroup Hierarchy (Inclusion)

$$GL_n(\mathbb{R})$$

$$\uparrow \text{All det} \neq 0$$

$$SL_n(\mathbb{R})$$

$$\uparrow \text{Only det} = 1$$

$$\{I_n\}$$

Idea: $\mathbf{SL_n}(\mathbb{R})$ is a subgroup of $\mathbf{GL_n}(\mathbb{R})$.

Key Idea

The special linear group, $\mathbf{SL_n}(\mathbb{R})$, is the set of matrices where the determinant is exactly 1. This means it's the **kernel** (or null space) of the determinant function, and the whole relationship reveals that the quotient group $\mathbf{GL_n}(\mathbb{R})/\mathbf{SL_n}(\mathbb{R})$ is isomorphic to $\mathbb{R}^*$ (all non-zero real numbers).

Two Views: $\mathbf{GL_n}(\mathbb{R})$, $\mathbf{SL_n}(\mathbb{R})$

The University of Manchester

Short Exact Sequence (Quotient)

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

The Sequence: $1 \to SL_n(\mathbb{R}) \to GL_n(\mathbb{R}) \xrightarrow{\text{det}} \mathbb{R}^* \to 1$

Distributivity

The University of Manchester

Definition.

Let $(R, +, .)$ be a set with two binary operations: addition $(+)$ and multiplication $(.)$. We say multiplication is *distributive over addition* if for all $a, b, c \in R$:

$$a.(b+c) = a.b + a.c \quad \text{and} \quad (a+b).c = a.c + b.c.$$

Remark:

This property ensures addition and multiplication interact consistently-fundamental to defining rings.

Ring

Definition

A *ring* is a set R together with two binary operations $+$ (addition) and $.$ (multiplication) such that the following properties hold for all $a, b, c \in R$:

1. $a + (b + c) = (a + b) + c$ (Associativity of addition)
2. $a + b = b + a$ (Commutativity of addition)
3. There exists $0 \in R$ such that $a + 0 = a = 0 + a$ (Additive identity)
4. For every $a \in R$, there exists $(-a) \in R$ such that $a + (-a) = 0$ (Additive inverse)
5. $a.(b.c) = (a.b).c$ (Associativity of multiplication)
6. $a.(b + c) = a.b + a.c$ and $(a + b).c = a.c + b.c$ (Distributivity)

Then $(R, +)$ is an abelian group and $(R, .)$ is a semigroup.

Refinements of Rings

Definition (Commutative Ring).

A ring $(R, +, .)$ is called *commutative* if $a.b = b.a$ for all $a, b \in R$.

Definition (Ring with Unity).

A ring having an element 1 such that $1.a = a.1 = a$ for all $a \in R$ is called a *ring with unity.*

Definition (Division Ring).

A ring with unity where every nonzero element has a multiplicative inverse, but multiplication need not be commutative.

Definition (Field).

A *field* is a commutative division ring:

$$\forall a \neq 0,\ \exists a^{-1} \in R :\ a.a^{-1} = a^{-1}.a = 1.$$

From Ring to Field: Structural Properties

A structure $(R, +, ., 0, 1, -)$ satisfies the following ten axioms:

Additive properties:

1. $a + (b + c) = (a + b) + c$
2. $a + b = b + a$
3. $\exists 0 \in R$ s.t. $a + 0 = a$
4. $\forall a \in R, \exists(-a)$ s.t. $a + (-a) = 0$

Multiplicative and mixed properties:

5. $a.(b.c) = (a.b).c$
6. $a.(b + c) = a.b + a.c$
7. $(a + b).c = a.c + b.c$
8. $\exists 1 \in R$ s.t. $a.1 = 1.a = a$
9. $\forall a \neq 0, \exists a^{-1}$ s.t. $a.a^{-1} = 1$
10. $a.b = b.a$

Observation:

- 1–7 $\rightarrow$ Ring
- 1–8 $\rightarrow$ Ring with Unity
- 1–9 $\rightarrow$ Division Ring
- 1–10 $\rightarrow$ Field

Examples

Ring-like Structures

1. $(\mathbb{Z}, +, .)$ — commutative ring with unity 1.
2. $(2\mathbb{Z}, +, .)$ — commutative ring without unity.
3. $(\mathbb{N}, +, .)$ — semiring (no additive inverses).
4. $(\mathbb{Q}, +, .)$ — field.
5. $(\mathbb{R}, +, .)$ — field.
6. $(\mathbb{C}, +, .)$ — field.

MANCHESTER 1824
The University of Manchester

Examples

Non-Commutative Rings and Division Rings

7 $(M_{n\times n}(\mathbb{R}), +, .)$ — ring with unity, not commutative for $n > 1$.

8 $(M_{n\times n}(\mathbb{Z}), +, .)$ — commutative in addition only.

9 $(\mathbb{H}, +, .)$ — quaternions: division ring, not commutative.

$$\mathbb{H} = \{a+bi+cj+dk \mid a, b, c, d \in \mathbb{R}\}, \quad i^2 = j^2 = k^2 = ijk = -1.$$

10 $(\mathbb{Z}_n, +, \cdot)$ — commutative ring with unity; field iff n prime.

11 Polynomial rings $(\mathbb{R}[x], +, .)$ — commutative ring with unity.

12 Continuous functions $(C([0, 1]), +, .)$ — commutative ring with unity.

Function Ring R^X

Definition

Let R be a commutative ring with unity and X a nonempty set. Define

$$R^X = \{f : X \to R\}.$$

Define operations:

$$(f \tilde{+} g)(x) = f(x) + g(x), \qquad (f \tilde{\cdot} g)(x) = f(x) \cdot g(x).$$

Define $\tilde{0}(x) = 0$ and $\tilde{1}(x) = 1$ for all $x \in X$.
Claim: $(R^X, \tilde{+}, \tilde{\cdot}, \tilde{0}, \tilde{1})$ is a commutative ring with unity.

$(R^X, \tilde{+}, \tilde{\cdot})$ - Commutative Ring with Unity

Proof (Sketch):
Addition: For all $f, g, h \in R^X$,

$$(f\tilde{+}(g\tilde{+}h))x = fx + (gx + hx) = (fx + gx) + hx = ((f\tilde{+}g)\tilde{+}h)x.$$

Hence associative. Commutativity and additive inverse follow pointwise.
Multiplication:

$$(f\tilde{\cdot}(g\tilde{\cdot}h))x = fx(gxhx) = (fxgx)hx = ((f\tilde{\cdot}g)\tilde{\cdot}h)x.$$

Distributivity:

$$(f\tilde{\cdot}(g\tilde{+}h))x = fx(gx + hx) = fxgx + fxhx = (f\tilde{\cdot}g\tilde{+}f\tilde{\cdot}h)x.$$

Unity: $\tilde{1}x = 1$ satisfies $f\tilde{\cdot}\tilde{1} = f$.
Hence, all ring axioms hold pointwise. □

(1): Proof that R^X is a Commutative Ring

Solution.

The verification above confirms:

$$(R^X, \tilde{+}, \tilde{\cdot}, \tilde{0}, \tilde{1})$$

inherits all ring properties from R under pointwise operations.
Hence, R^X is a *commutative ring with unity.*

(2): Ring Structure on $\mathbb{Q}$ via $a * b = a + b + ab$

Define: $a * b = a + b + ab$ for $a, b \in \mathbb{Q}$.
Check Associativity:

$$a*(b*c) = a+(b+c+bc)+a(b+c+bc) = a+b+c+ab+ac+bc+abc.$$

$$(a*b)*c = (a+b+ab)+c+(a+b+ab)c = a+b+c+ab+ac+bc+abc.$$

Hence associative. ✓
Unity: find e s.t. $a * e = a$.

$$a + e + ae = a \Rightarrow e(1 + a) = 0 \Rightarrow e = 0.$$

So 0 is unity. ✓
Group of units: $a * b = 0 \Rightarrow a + b + ab = 0 \Rightarrow (1 + a)(1 + b) = 1$.
Hence unit a exists iff $1 + a \neq 0$, and inverse is $b = -a/(1 + a)$.
Thus units: $\mathbb{Q} \setminus \{-1\}$.

MANCHESTER 1824
The University of Manchester

(3): Real Interval Group with Parameter $k > 0$

Define for $a, b \in (-k, k)$:

$$a * b = \frac{a+b}{1+kb}.$$

Closure: If $a, b \in (-k, k)$, then $|a * b| < k$ (exercise: verify using $|a+b| < 2k$ and $1 + kb > 1 - k^2 > 0$).
Associativity: Compute:

$$a * (b * c) = \frac{a + \frac{b+c}{1+kc}}{1 + k\frac{b+c}{1+kc}} = \frac{a(1+kc) + b + c}{1 + k(a+b+c) + k^2(bc + ac + ab)}.$$

A tedious but direct algebra shows symmetry, hence associative. ✓

Identity: 0, since $a * 0 = \frac{a+0}{1+0} = a$. ✓ **Inverse:** $a^{-1} = -\frac{a}{1+ka}$. ✓
Hence $((-k, k), *, 0)$ is a group (nonlinear addition law, used in hyperbolic geometry).

MANCHESTER 1824
The University of Manchester

(4): Constructing a Ring on $\mathbb{R}^2$

Define operations for $(a,b),(c,d) \in \mathbb{R}^2$:

$$(a,b)\tilde{+}(c,d) = (a+c, b+d), \quad (a,b)\tilde{\cdot}(c,d) = (ac,\ bc+ad).$$

Check Ring Properties:

- Addition is componentwise abelian group: ✓
- Multiplication associative:
  $(a,b)\tilde{\cdot}((c,d)\tilde{\cdot}(e,f)) = (a(b+c)+\dots)$ (verify explicitly). ✓
- Distributivity holds componentwise: ✓
- Unity element: $(1,0)$ since

$$(a,b)\tilde{\cdot}(1,0) = (a,b).$$

- Commutativity: $(a,b)\tilde{\cdot}(c,d) = (ac, bc+ad) = (c,a)\tilde{\cdot}(a,b)$. ✓

Hence $(\mathbb{R}^2, \tilde{+}, \tilde{\cdot})$ is a commutative ring with unity $(1,0)$.

Algebraic Structure of $\mathbb{R}^2$ with Custom Multiplication

Custom Multiplication Diagram

$$
\begin{tikzcd}
(a,b) \arrow[dr] & \times & (c,d) \arrow[dl] \\
& (\mathbf{ac}, \mathbf{bc} + \mathbf{ad}) &
\end{tikzcd}
$$

Interpretation and Clarification

This diagram illustrates the algebraic structure of $\mathbb{R}^2$ under the explicit multiplication rule:

$$(a, b) * (c, d) = (ac, bc + ad)$$

Algebraic Structure of $\mathbb{R}^2$

Interpretation and Clarification

This diagram illustrates the algebraic structure of $\mathbb{R}^2$ under the explicit multiplication rule: $(a, b) * (c, d) = (ac, bc + ad)$

- With standard vector addition, this operation defines a **Ring** structure on $\mathbb{R}^2$.
- **Note on Affine Transformations:** While the multiplication is commutative in the second component ($bc + ad$), the standard way to model affine transformations $f(x) = ax + b$ is through composition, which results in the pair:

$$(a, b) \circ (c, d) = (\mathbf{ac}, \mathbf{ad} + \mathbf{b})$$

- Your rule and the affine group rule are related, but they define different algebraic structures!

Summary

- Introduced distributivity linking addition and multiplication, then defined ring, commutative ring, ring with unity, division ring, and field.
- Outlined 10 structural axioms progressing from semiring to field.
- Provided 12 diverse examples, including quaternions.
- Proved $(R^X, \tilde{+}, \tilde{\cdot})$ is a commutative ring with unity.
- Solved four constructive problems demonstrating new ring-like and group structures.
- Defined monoid and group homomorphisms with formal diagrams; proved that for group homomorphisms, one property implies the rest.
- Defined and illustrated isomorphisms with exponential–log example.
- Defined subgroup and proved simplified test using $a * b^{-1}$; worked examples: $(\mathbb{Z}, +)$ and $(GL_n(\mathbb{R}), \times)$.

MANCHESTER
1824
The University of Manchester

Thanks