MATH 2131

Honors in Linear and Abstract Algebra I

Prof. Meng

PUBLISHED BY PUBLISHER

BOOK-WEBSITE.COM

First printing, March 2013

Contents

Part One

1. Abstract Vector Spaces

1.1 Binary Operation

Definition 1.1.1 — Binary Operation. A *binary operation* on a set S is a mapping of the elements of the Cartesian product $S \times S$ to S.

$$\begin{aligned} f : S \times S &\to S \\ (x,y) &\mapsto f(x,y) \end{aligned}$$

■ **Example 1.1** A common example of a binary operation is addition on the set of natural numbers $\mathbb{N}$.

$$\begin{aligned} + : \mathbb{N} \times \mathbb{N} &\to \mathbb{N} \\ (x,y) &\mapsto x+y \end{aligned} \tag{1.1}$$

■

Definition 1.1.2 — Associative Operation. A binary operation $f : S \times S \to S$ is said to be *associative* if, for all $x,y,z \in S$,

$$f(x, f(y,z)) = f(f(x,y),z)$$

■ **Example 1.2** A common example of an associative (binary) operation is addition on the set of natural numbers $\mathbb{N}$. For all $x,y,z \in \mathbb{N}$, we have $x+(y+z) = (x+y)+z$. ■

Definition 1.1.3 — Identifiable Operation. A binary operation $f : S \times S \to S$ is said to be *identifiable*, or *unital*, if there exists an element $e \in S$, the *identity* or *unit element*, such that, for all $x \in S$

$$f(x,e) = x = f(e,x)$$

■ **Example 1.3** A common example of an identifiable (binary) operation is multiplication on the set of natural numbers $\mathbb{N}$. The identity element is 1, and for all $x \in \mathbb{N}$, we have $x \cdot 1 = x = 1 \cdot x$. ■

Proposition 1.1.1 The identity element of an identifiable operation is unique.

Proof. Let e_1 and e_2 be two identity elements for the operation f. Then, for any element $x \in S$, we have:

$$f(x,e_1) = x = f(e_1,x)$$
$$f(x,e_2) = x = f(e_2,x)$$

Now, consider the element e_1:

$$f(e_1,e_2) = e_1$$

But since e_2 is an identity element, we also have:

$$f(e_1,e_2) = e_2$$

Therefore, we conclude that $e_1 = e_2$, proving the uniqueness of the identity element. ■

R Two-sided identity must be unique, but one-sided identities need not be.

■ **Example 1.4** ■

Definition 1.1.4 — Inverse Operation. A binary operation $f : S \times S \to S$ is said to be *invertible* if, for every element $x \in S$, there exists an element $y \in S$, called the two-sided *inverse* of x, denoted as x^{-1}, such that

$$f(x,y) = e = f(y,x)$$

where e is the identity element of the operation.

R Invertible operation exists if inverse operation exists, i.e. there exists an identity element.

■ **Example 1.5** A common example of an invertible (binary) operation is addition on the set of integers $\mathbb{Z}$. For every integer $x \in \mathbb{Z}$, there exists an integer $y = -x$ such that:

$$x + (-x) = 0 = (-x) + x \tag{1.2}$$

where 0 is the identity element for addition. ■

Proposition 1.1.2 The inverse element of an invertible operation is unique.

Proof. Let y_1 and y_2 be two inverses of an element $x \in S$. Then, by definition of inverse, we have:

$$f(x,y_1) = e = f(y_1,x)$$
$$f(x,y_2) = e = f(y_2,x)$$

Now, consider the element y_1:

$$f(y_1,x) = e$$

But since y_2 is also an inverse of x, we can substitute e with $f(x,y_2)$:

$$f(y_1,x) = f(x,y_2) = e$$

By the associativity of the operation, we can rearrange this to:

$$y_1 = f(y_1,e) = f(y_1, f(x,y_2)) = f(f(y_1,x),y_2) = f(e,y_2) = y_2$$

Thus, the inverse element is unique. ■

Definition 1.1.5 — Commutative Operation. A binary operation $f : S \times S \to S$ is said to be *commutative* if, for all $x, y \in S$, the following holds:

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

■ **Example 1.6** A common example of a commutative operation is addition on the set of integers $\mathbb{Z}$. For all $x, y \in \mathbb{Z}$, we have:

$$x + y = y + x$$

■

Definition 1.1.6 — Distributive Operation (Harmonic Property). A binary operation $g : S \times S \to S$ is said to be *distributive* with respect to another binary operation $f : S \times S \to S$ if, for all $x, y, z \in S$, the following holds:

$$g(x, f(y,z)) = f(g(x,y), g(x,z))$$
$$g(f(y,z), x) = f(g(y,x), g(z,x))$$

■ **Example 1.7** A common example of a distributive operation is multiplication over addition on the set of integers $\mathbb{Z}$. For all $x, y, z \in \mathbb{Z}$, we have:

$$x \cdot (y + z) = x \cdot y + x \cdot z$$
$$(y + z) \cdot x = y \cdot x + z \cdot x$$

■

1.2 Groups, Rings, Fields

Definition 1.2.1 — Monoid. A *monoid* is a set M equipped with a binary operation $f : M \times M \to M$ such that the following properties hold:

1. *Closure Property:* For all $x, y \in M$, $f(x,y) \in M$.
2. *Associative Property*
3. *Identifiable Property*

We say (M, f) is a monoid, and f is the *monoid operation* on the set M. A set M with a monoid operation f is the *monoid structure*.

Definition 1.2.2 — Group. A *group* is a set G equipped with a monoid operation $f : G \times G \to G$ with the additional property that every element has an inverse, *Invertible Property*.

■ **Example 1.8** $(\mathbb{R} \setminus \{0\}, \times)$ is a group, but $(\mathbb{R}, \times)$ is not a group since 0 does not have a multiplicative inverse. ■

Definition 1.2.3 — Abelian Monoid / Group. A monoid / group (G, f) is said to be an *abelian monoid / group* if the monoid / group operation f is commutative, *Commutative Property*.

Definition 1.2.4 — Unital Ring. A (unital) ring is a set R equipped with two binary operations $f : R \times R \to R$ (addition) and $g : R \times R \to R$ (multiplication) such that the following properties hold:

1. *Additive Group:* (R, f) is an abelian group.
2. *Multiplicative Monoid:* (R, g) is a monoid.
3. *Distributive Property:* g with respect to f.

Definition 1.2.5 — Commutative Ring. A *commutative ring* is a unital ring R such that the multiplication operation $g : R \times R \to R$ is commutative.

■ **Example 1.9** $(\mathbb{Z}, +, \times)$ is a unital commutative ring. ■

Definition 1.2.6 — Field. A *field* is a unital commutative ring F such that every non-zero element has a multiplicative inverse.

■ **Example 1.10** $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ and $(\mathbb{C}, +, \times)$ are fields. ■

■ **Example 1.11** $(\mathbb{Z}/2\mathbb{Z}, +, \times)$ is a field, where $\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$, $\bar{0}$ is the set of even integers and $\bar{1}$ is the set of odd integers. It follows the additions and multiplications below:

$$\begin{array}{c|cc} + & \bar{0} & \bar{1} \\ \hline \bar{0} & \bar{0} & \bar{1} \\ \bar{1} & \bar{1} & \bar{0} \end{array} \qquad \begin{array}{c|cc} \times & \bar{0} & \bar{1} \\ \hline \bar{0} & \bar{0} & \bar{0} \\ \bar{1} & \bar{0} & \bar{1} \end{array} \tag{1.3}$$

■

1.3 Morphisms

Definition 1.3.1 — Morphisms. A *morphism* is a structure-preserving map between two algebraic structures (e.g., groups, rings, fields). Formally, let $(A,\cdot_A)$ and $(B,\cdot_B)$ be two algebraic structures. A morphism $f : A \to B$ is a function such that:

$$f(x\cdot_A y) = f(x)\cdot_B f(y) \quad \forall x,y \in A$$

Definition 1.3.2 — Monoid Homomorphism. A *monoid homomorphism* is a morphism between two monoids that preserves the monoid structure. Formally, let $(M_1,\cdot_1)$ and $(M_2,\cdot_2)$ be two monoids with identity elements e_1 and e_2, respectively. A function $f : M_1 \to M_2$ is a monoid homomorphism if:

1. $f(x\cdot_1 y) = f(x)\cdot_2 f(y) \quad \forall x,y \in M_1$
2. $f(e_1) = e_2$

Definition 1.3.3 — Group Homomorphism. A *group homomorphism* is a morphism between two groups that preserves the group structure. Formally, let $(G_1,\cdot_1)$ and $(G_2,\cdot_2)$ be two groups with identity elements e_1 and e_2, respectively. A function $f : G_1 \to G_2$ is a group homomorphism if:

1. $f(x\cdot_1 y) = f(x)\cdot_2 f(y) \quad \forall x,y \in G_1$
2. $f(e_1) = e_2$
3. $f(x^{-1}) = (f(x))^{-1} \quad \forall x \in G_1$

Proposition 1.3.1 The second and third properties of a group homomorphism are consequences of the first property.

Proof. Let $f : G_1 \to G_2$ be a group homomorphism satisfying the first property. We will show that the second and third properties follow from it.

Second Property: To show that $f(e_1) = e_2$, we use the fact that e_1 is the identity element in G_1. For any element $x \in G_1$, we have:

$$f(x) = f(x\cdot_1 e_1) = f(x)\cdot_2 f(e_1)$$

Since $f(x)$ is an arbitrary element in G_2, this implies that $f(e_1)$ must be the identity element in G_2, i.e., $f(e_1) = e_2$.

Third Property: To show that $f(x^{-1}) = (f(x))^{-1}$ for all $x \in G_1$, we use the fact that x^{-1} is the inverse of x in G_1. We have:

$$e_2 = f(e_1) = f(x\cdot_1 x^{-1}) = f(x)\cdot_2 f(x^{-1})$$

This shows that $f(x^{-1})$ is the inverse of $f(x)$ in G_2, i.e., $f(x^{-1}) = (f(x))^{-1}$.

Therefore, both the second and third properties of a group homomorphism are indeed consequences of the first property. ■

R For monoid homomorphisms, the second property cannot be derived from the first property. Consider the identity element e_1 in M_1. If we apply the first property, we get $f(e_1\cdot_1 e_1) = f(e_1)\cdot_2 f(e_1)$. This simplifies to $f(e_1) = f(e_1)\cdot_2 f(e_1)$, which does not necessarily imply that $f(e_1)$ is the identity element in M_2, i.e., $f(e_1) \neq e_2$, but $f(e_1)$ is the idempotent element in M_2. Therefore, the second property must be explicitly stated for monoid homomorphisms.

However in the case of group homomorphisms, the existence of inverses ensures that there is only one element that can be idempotent under the group operation, which is the identity element. Thus, for group homomorphisms, the second property can be derived from the first property.

Definition 1.3.4 — Ring Homomorphism. A *ring homomorphism* is a morphism between two rings that preserves both the additive and multiplicative structures. Formally, let $(R_1, +_1, \cdot_1)$ and $(R_2, +_2, \cdot_2)$ be two rings with identity elements 0_1, 1_1 and 0_2, 1_2, respectively. A function $f : R_1 \to R_2$ is a ring homomorphism if:
1. $f(x +_1 y) = f(x) +_2 f(y) \quad \forall x, y \in R_1$
2. $f(x \cdot_1 y) = f(x) \cdot_2 f(y) \quad \forall x, y \in R_1$
3. $f(1_1) = 1_2$

Definition 1.3.5 — Endomorphism. An *endomorphism* is a morphism from an algebraic structure to itself. Formally, let $(A, \cdot)$ be an algebraic structure. An endomorphism $f : A \to A$ is a function such that:

$$f(x \cdot y) = f(x) \cdot f(y) \quad \forall x, y \in A$$

Definition 1.3.6 — Endomorphism Ring. The set of all endomorphisms of an abelian group $(A, +)$, denoted by $\mathrm{End}(A)$, forms a (non-commutative) ring under pointwise addition and composition of functions. The addition and multiplication operations are defined as follows:

$$\begin{aligned} + : \mathrm{End}(A) \times \mathrm{End}(A) &\to \mathrm{End}(A) \\ (f, g) &\mapsto (f + g : x \mapsto f(x) + g(x)) \qquad f + g : A \to A \end{aligned}$$

$$\begin{aligned} \circ : \mathrm{End}(A) \times \mathrm{End}(A) &\to \mathrm{End}(A) \\ (f, g) &\mapsto (f \circ g : x \mapsto f(g(x))) \qquad f \circ g : A \to A \end{aligned}$$

The identity element for addition is the zero endomorphism, which maps every element to the identity element of the group.

$$\begin{aligned} 0 : A &\to A \\ x &\mapsto 0 \end{aligned}$$

The identity element for multiplication is the identity endomorphism, which maps every element to itself.

$$\begin{aligned} 1 : A &\to A \\ x &\mapsto x \end{aligned}$$

1.4 Vector Spaces

Definition 1.4.1 — Linear Structure. A *linear structure* over a field F on a set V is a pair $(+,\cdot)$ where $(V,+)$ is an abelian group with a ring homomorphism $F \to \mathrm{End}(V)$, where $\mathrm{End}(V)$ is the endomorphism ring of the abelian group $(V,+)$.

$$\begin{aligned} \cdot : F &\to \mathrm{End}(V) \\ \alpha &\mapsto (\alpha\cdot : \vec{x} \mapsto \alpha\vec{x}) \qquad \alpha\cdot : V \to V \end{aligned}$$

The ring homomorphism is a (ring) action of the field F on the abelian group $(V,+)$, called *scalar multiplication*. The ring action can be written as a binary operation:

$$\begin{aligned} \cdot : F \times V &\to V \\ (\alpha, \vec{x}) &\mapsto \alpha\vec{x} \end{aligned}$$

Definition 1.4.2 — Linear Spaces / Vector Spaces. A linear space / vector space is a set with a linear structure over a field on the set.

Corollary 1.4.1 — Vector Spaces. A vector space over a field F is a set V equipped with two operations: vector addition $+ : V \times V \to V$ and scalar multiplication $\cdot : F \times V \to V$, satisfying the following axioms for all $\vec{u}, \vec{v}, \vec{w} \in V$ and $\alpha, \beta \in F$:

Axiom	Statement
1. Associativity of addition	$(\vec{u}+\vec{v})+\vec{w} = \vec{u}+(\vec{v}+\vec{w})$
2. Existence of additive identity	$\exists\vec{0} \in V$ such that $\forall\vec{u} \in V$, $\vec{u}+\vec{0} = \vec{u}$
3. Existence of additive inverses	$\forall\vec{u} \in V$, $\exists -\vec{u} \in V$ such that $\vec{u}+(-\vec{u}) = \vec{0}$
4. Commutativity of addition	$\vec{u}+\vec{v} = \vec{v}+\vec{u}$
5. Distributivity of scalar multiplication with respect to vector addition	$\alpha(\vec{u}+\vec{v}) = \alpha\vec{u}+\alpha\vec{v}$
6. Distributivity of scalar multiplication with respect to field addition	$(\alpha+\beta)\cdot = \alpha\cdot+\beta\cdot$
7. Compatibility of scalar multiplication with field multiplication	$(\alpha\beta)\cdot = (\alpha\cdot)\circ(\beta\cdot)$
8. Identity element of scalar multiplication	$F \ni 1 = (1\cdot : x \mapsto x) \in \mathrm{End}(V)$

Note that the first four axioms ensure that $(V,+)$ is an abelian group, while the fifth axiom describes the endomorphism structure and the last three axioms describe the ring homomorphism.

■ **Example 1.12** F is a linear space over itself with the usual addition and multiplication operations.

$$\begin{aligned} \cdot : F \times F &\to F \\ (\alpha, \beta) &\mapsto \alpha\beta \end{aligned}$$

The first F is the field acting on the second F, which is the abelian group. ■

■ **Example 1.13** Let X be a set and F be a field.

$$\begin{aligned} F[[X]] = \mathrm{Map}(X,F) &\overset{\text{def}}{=\!=} \text{the set of all } F\text{-valued functions on } X \\ &=\!= \{f : X \to F \mid f \text{ is a set map}\} \end{aligned}$$

$F[[X]]$ is a vector space over F with the following operations defined pointwisely:

$$\begin{aligned} + : F[[X]] \times F[[X]] &\to F[[X]] \\ (f,g) &\mapsto (f+g : x \mapsto f(x)+g(x)) \qquad f+g : X \to F \end{aligned}$$

$$\begin{aligned} \cdot : F \times F[[X]] &\to F[[X]] \\ (\alpha,f) &\mapsto (\alpha f : x \mapsto \alpha f(x)) \qquad \alpha f : X \to F \end{aligned}$$

■

■ **Example 1.14** Let X be a set and F be a field.

$$\begin{aligned} F[X] = \mathrm{Map}_{\mathrm{fin}}(X,F) &\overset{\text{def}}{=\!=} \text{the set of all finitely supported } F\text{-valued functions on } X \\ &=\!= \{f : X \to F \mid f \text{ is a set map and } f(x) \neq 0 \text{ for only finitely many } x \in X\} \end{aligned}$$

$F[X]$ is a vector space over F as $F[X] \subseteq F[[X]]$ and the operations are defined pointwisely as in the previous example.

$f : X \to F$ is finitely supported if the set $\{x \in X \mid f(x) \neq 0\}$ is finite. ■

■ **Example 1.15** Let t be a formal variable and F be a field.

$$X = \{1, t, t^2, \cdots\}$$

Then $F[t] = F[X_t]$ is the set of all polynomials in the variable t with coefficients in F and $F[[t]] = F[[X_t]]$ is the set of all formal power series in the variable t with coefficients in F. Both of them are vector spaces over F. ■

1.5 Citation

This statement requires citation [1]; this one is more specific [2, page 122].

1.6 Lists

Lists are useful to present information in a concise and/or ordered way[1].

1.6.1 Numbered List

1. The first item
2. The second item
3. The third item

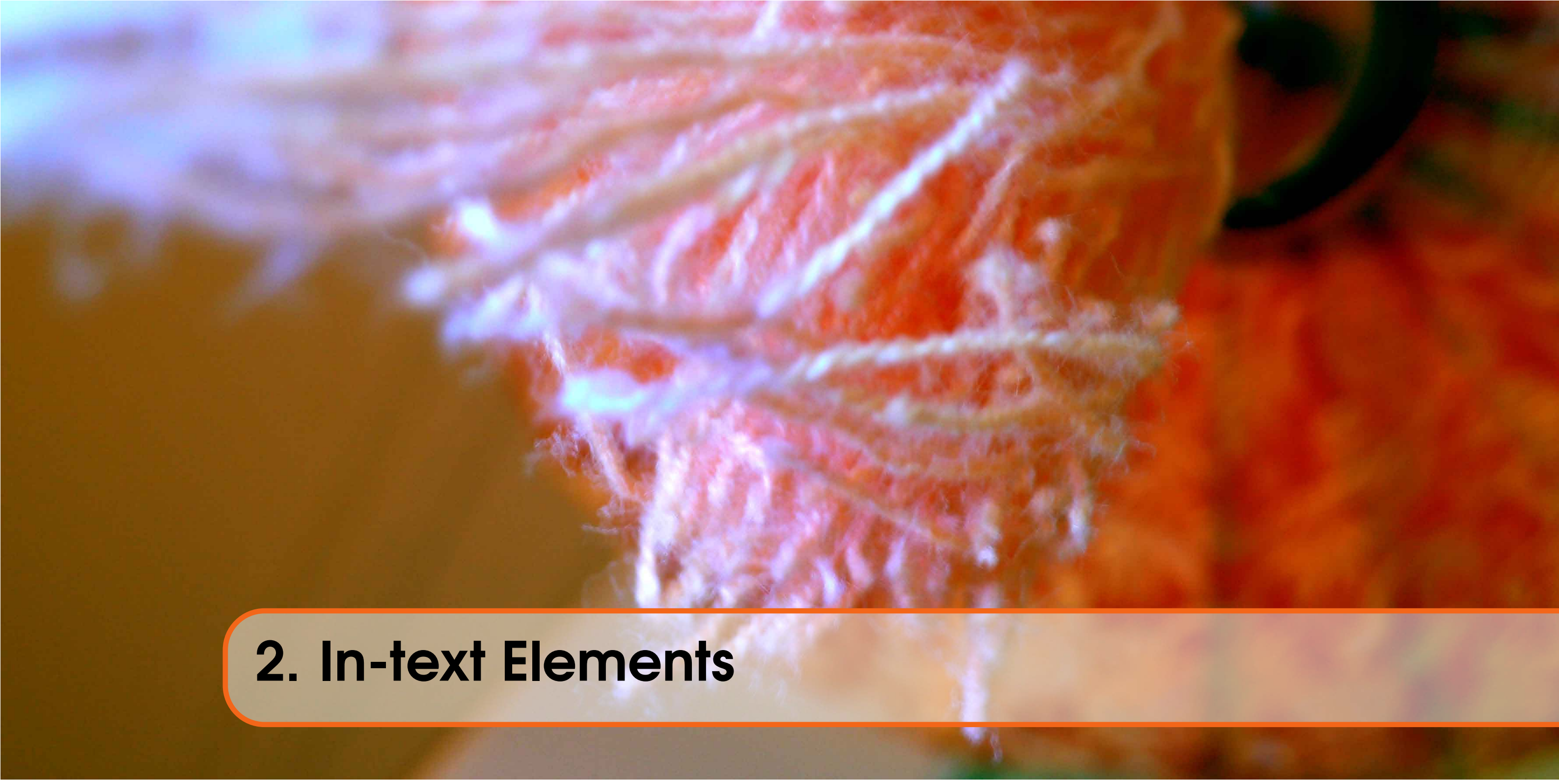
1.6.2 Bullet Points

- The first item
- The second item
- The third item

1.6.3 Descriptions and Definitions

Name Description
Word Definition
Comment Elaboration

[1] Footnote example...



2. In-text Elements

2.1 Theorems

This is an example of theorems.

2.1.1 Several equations

This is a theorem consisting of several equations.

Theorem 2.1.1 — Name of the theorem. In $E = \mathbb{R}^n$ all norms are equivalent. It has the properties:

$$\big| ||\mathbf{x}|| - ||\mathbf{y}|| \big| \leq ||\mathbf{x} - \mathbf{y}|| \tag{2.1}$$

$$||\sum_{i=1}^{n} \mathbf{x}_i|| \leq \sum_{i=1}^{n} ||\mathbf{x}_i|| \quad \text{where } n \text{ is a finite integer} \tag{2.2}$$

2.1.2 Single Line

This is a theorem consisting of just one line.

Theorem 2.1.2 A set $\mathscr{D}(G)$ in dense in $L^2(G)$, $|\cdot|_0$.

2.2 Definitions

This is an example of a definition. A definition could be mathematical or it could define a concept.

Definition 2.2.1 — Definition name. Given a vector space E, a norm on E is an application, denoted $||\cdot||$, E in $\mathbb{R}^+ = [0, +\infty[$ such that:

$$||\mathbf{x}|| = 0 \;\Rightarrow\; \mathbf{x} = \mathbf{0} \tag{2.3}$$

$$||\lambda \mathbf{x}|| = |\lambda| \cdot ||\mathbf{x}|| \tag{2.4}$$

$$||\mathbf{x} + \mathbf{y}|| \leq ||\mathbf{x}|| + ||\mathbf{y}|| \tag{2.5}$$

2.3 Notations

Notation 2.1. *Given an open subset G of $\mathbb{R}^n$, the set of functions φ are:*
1. *Bounded support G;*
2. *Infinitely differentiable;*

a vector space is denoted by $\mathscr{D}(G)$.

2.4 Remarks

This is an example of a remark.

R The concepts presented here are now in conventional employment in mathematics. Vector spaces are taken over the field $\mathbb{K} = \mathbb{R}$, however, established properties are easily extended to $\mathbb{K} = \mathbb{C}$.

2.5 Corollaries

This is an example of a corollary.

Corollary 2.5.1 — Corollary name. The concepts presented here are now in conventional employment in mathematics. Vector spaces are taken over the field $\mathbb{K} = \mathbb{R}$, however, established properties are easily extended to $\mathbb{K} = \mathbb{C}$.

2.6 Propositions

This is an example of propositions.

2.6.1 Several equations

Proposition 2.6.1 — Proposition name. It has the properties:

$$\left| ||\mathbf{x}|| - ||\mathbf{y}|| \right| \leq ||\mathbf{x} - \mathbf{y}|| \tag{2.6}$$

$$||\sum_{i=1}^{n} \mathbf{x}_i|| \leq \sum_{i=1}^{n} ||\mathbf{x}_i|| \quad \text{where } n \text{ is a finite integer} \tag{2.7}$$

2.6.2 Single Line

Proposition 2.6.2 Let $f, g \in L^2(G)$; if $\forall \varphi \in \mathscr{D}(G)$, $(f, \varphi)_0 = (g, \varphi)_0$ then $f = g$.

2.7 Examples

This is an example of examples.

2.7.1 Equation and Text

■ **Example 2.1** Let $G = \{x \in \mathbb{R}^2 : |x| < 3\}$ and denoted by: $x^0 = (1, 1)$; consider the function:

$$f(x) = \begin{cases} e^{|x|} & \text{si } |x - x^0| \leq 1/2 \\ 0 & \text{si } |x - x^0| > 1/2 \end{cases} \tag{2.8}$$

The function f has bounded support, we can take $A = \{x \in \mathbb{R}^2 : |x - x^0| \leq 1/2 + \varepsilon\}$ for all $\varepsilon \in]0; 5/2 - \sqrt{2}[$. ■

2.7.2 Paragraph of Text

■ **Example 2.2 — Example name.** Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris. ■

2.8 Exercises

This is an example of an exercise.

Exercise 2.1 This is a good place to ask a question to test learning progress or further cement ideas into students' minds. ■

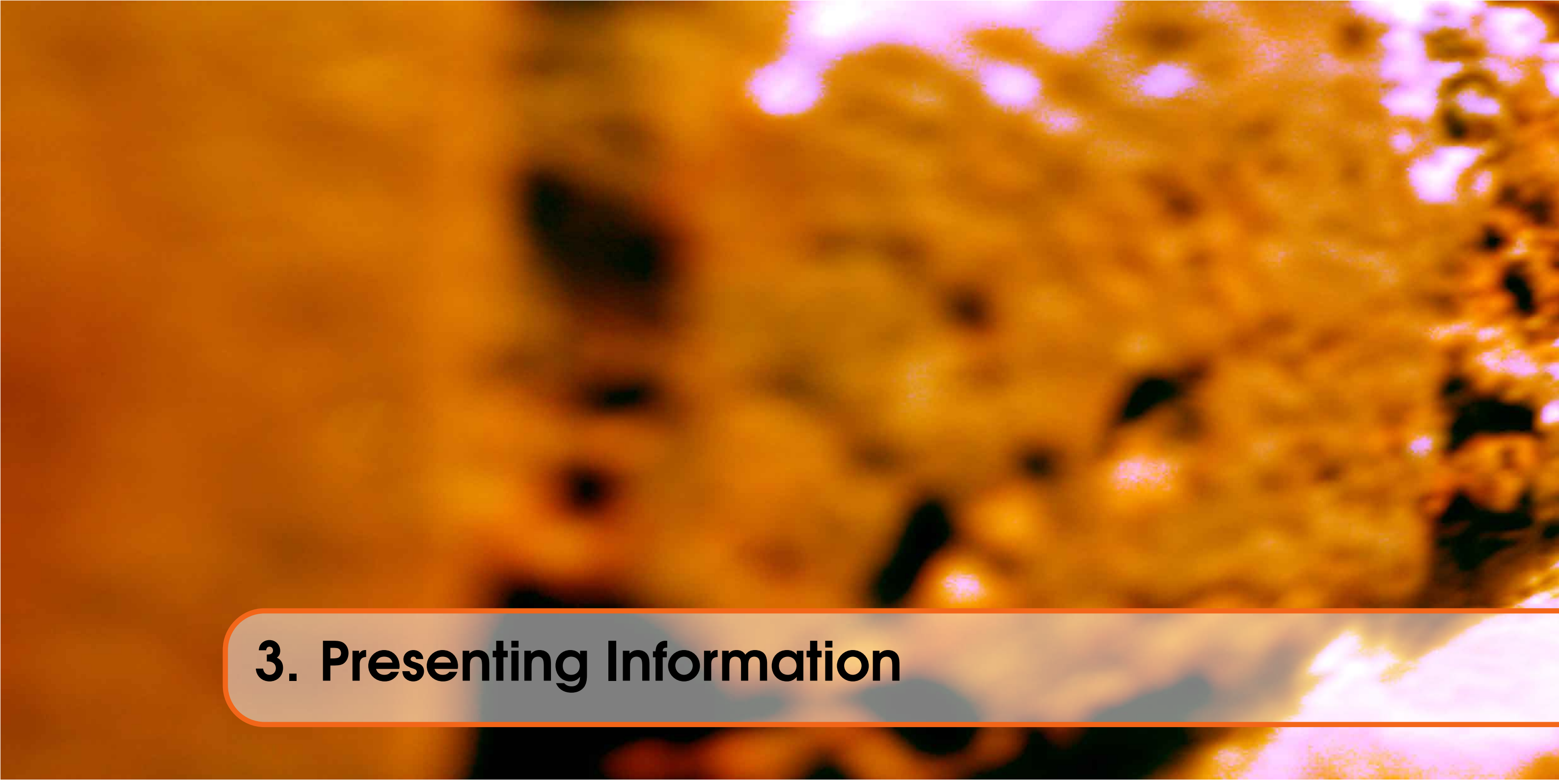
2.9 Problems

Problem 2.1 What is the average airspeed velocity of an unladen swallow?

2.10 Vocabulary

Define a word to improve a students' vocabulary.
Vocabulary 2.1 — Word. Definition of word.

Part Two



3. Presenting Information

3.1 Table

Treatments	Response 1	Response 2
Treatment 1	0.0003262	0.562
Treatment 2	0.0015681	0.910
Treatment 3	0.0009271	0.296

Table 3.1: Table caption

3.2 Figure

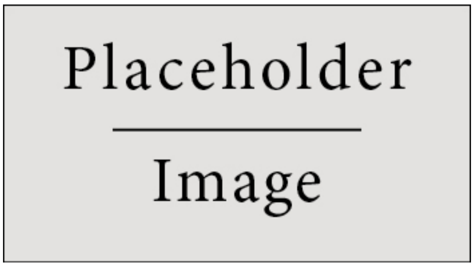
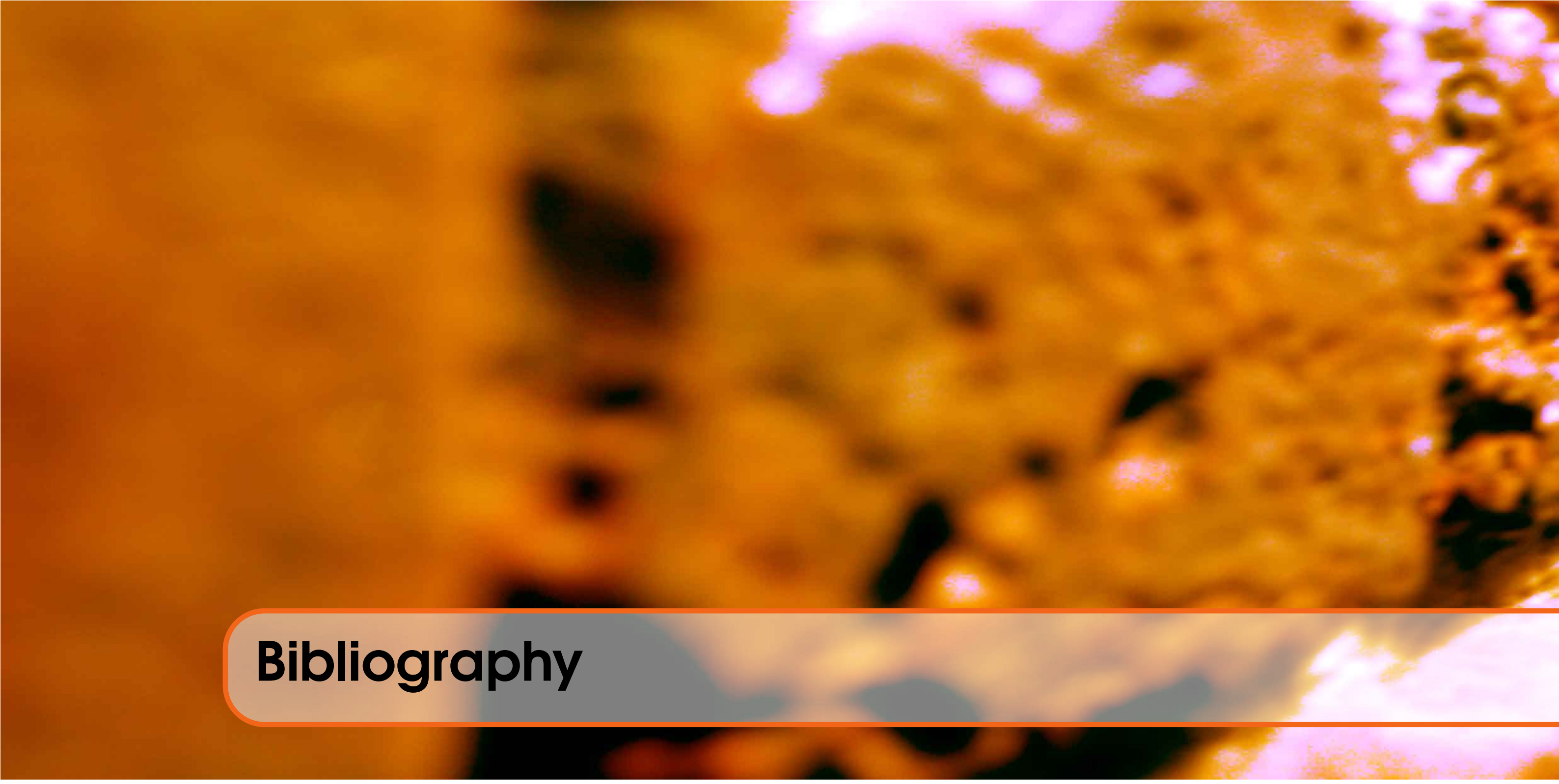


Figure 3.1: Figure caption



Bibliography

Books

[Smi12] John Smith. *Book title*. 1st edition. Volume 3. 2. City: Publisher, Jan. 2012, pages 123–200 (cited on page 15).

Articles

[Smi13] James Smith. “Article title”. In: 14.6 (Mar. 2013), pages 1–8 (cited on page 15).

Index