SANDIA REPORT

SAND2019-3361
Unlimited Release
Printed June 2018

Abstract Algebra Basics

Karthik V. Aadithya, Eric Keiter, and Ting Mei

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Approved for public release; further dissemination unlimited.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology and Engineering Solutions of Sandia, LLC.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online ordering: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2019-3361
Unlimited Release
Printed June 2018

Abstract Algebra Basics

Karthik V. Aadithya[‡], Eric Keiter, and Ting Mei
Sandia National Laboratories, Albuquerque, NM, USA
[‡]Corresponding author. Email: kvaadit@sandia.gov

Abstract

To understand the mathematics behind Uncertainty Quantification (UQ), one first needs to become familiar with orthogonal polynomials, which in turn requires a grasp of abstract algebra. This note covers some of the basics of abstract algebra.

Contents

1. Fields 9

2. Vector Spaces 13

3. Inner Products 17

4. Norms 22

List of Figures

1. Fields

Definition 1.0.1 (Field)**.** *A field $\mathbb{F}(F, +, *)$ is a set F, together with binary operations $+ : F \times F \to F$ (called "addition") and $* : F \times F \to F$ (called "multiplication") that satisfy the following properties (called "field axioms"):*

1. ***Closure of $+$ and $*$.***
   For all f_1 and f_2 in F, $f_1 + f_2$ and $f_1 * f_2$ also belong to F.

2. ***Commutativity of $+$ and $*$.***
   For all f_1 and f_2 in F, $f_1 + f_2 = f_2 + f_1$, and $f_1 * f_2 = f_2 * f_1$.

3. ***Associativity of $+$ and $*$.***
   For all f_1, f_2, and f_3 in F, $(f_1 + f_2) + f_3 = f_1 + (f_2 + f_3)$, and $(f_1 * f_2) * f_3 = f_1 * (f_2 * f_3)$.

4. ***Identities of $+$ and $*$.***
   There exist elements 0 (called "zero") and 1 (called "one") in F such that, for every f in F, $f + 0 = f$ and $f * 1 = f$. (And from the commutativity of $+$ and $*$, we have $0 + f = f$ and $1 * f = f$ as well.)

5. ***Inverses of $+$ and $*$.***

   (a) *For every f in F, there exists an element (called the field additive inverse of f, or the inverse of f with respect to $+$, and denoted f_-) in F such that $f + f_- = 0$, and*

   (b) *For every $f \neq 0$ in F, there exists an element (called the field multiplicative inverse of f, or the inverse of f with respect to $*$, and denoted f^{-1}) in F such that $f * f^{-1} = 1$.*

6. ***Distributivity of $*$ over $+$.***
   For all f_1, f_2, and f_3 in F, $f_1 * (f_2 + f_3) = (f_1 * f_2) + (f_1 * f_3)$.

Example 1.0.2. *The real numbers, together with "normal" addition and multiplication operations, form a field (denoted $\mathbb{R}$).*

Example 1.0.3. *The complex numbers, together with "normal" addition and multiplication operations, form a field (denoted $\mathbb{C}$).*

Lots of interesting lemmas and theorems can be deduced from the field axioms above. Some examples are given below.

Theorem 1.0.4 (Field Multiplication by Zero)**.** *Let $\mathbb{F}(F, +, *)$ be a field. Then, for every f in F, $f * 0 = 0$.*

Proof. This seems like a trivial result. After all, we all know that multiplying anything by zero results in zero. But, if you notice, the field axioms above say *nothing* about multiplying elements by zero. They only say that *adding* zero to elements leaves them unchanged. So we need to decude the "multiplication by zero" property from the field axioms. Here's how it's usually done:

Take any element f in F. Then, we have:

$$\begin{aligned}
f * 0 &= (f * 0) + 0 && \text{(by the identity of } +\text{)} \\
&= (f * 0) + ((f * f) + (f * f)_-) && \text{(by the inverse of } +\text{)} \\
&= ((f * 0) + (f * f)) + (f * f)_- && \text{(by the associativity of } +\text{)} \\
&= (f * (0 + f)) + (f * f)_- && \text{(by the distributivity of } * \text{ over } +\text{)} \\
&= (f * (f + 0)) + (f * f)_- && \text{(by the commutativity of } +\text{)} \\
&= (f * f) + (f * f)_- && \text{(by the identity of } +\text{)} \\
&= 0 && \text{(by the inverse of } +\text{).}
\end{aligned}$$

□

Theorem 1.0.5 (Unique Field Additive Inverse)**.** *Let $\mathbb{F}(F, +, *)$ be a field. Then, for every f in F, the field additive inverse f_- is unique.*

Proof. Suppose, for the sake of contradiction, that there is an f in F with two different field additive inverses $f_{-,1}$ and $f_{-,2}$. Then, we have:

$$\begin{aligned}
& f + f_{-,1} = 0 && \text{(by the inverse of } +\text{)} \\
\implies & f_{-,2} + (f + f_{-,1}) = f_{-,2} + 0 && \text{(adding } f_{-,2} \text{ to both sides)} \\
\implies & (f_{-,2} + f) + f_{-,1} = f_{-,2} + 0 && \text{(by the associativity of } +\text{)} \\
\implies & (f + f_{-,2}) + f_{-,1} = f_{-,2} + 0 && \text{(by the commutativity of } +\text{)} \\
\implies & 0 + f_{-,1} = f_{-,2} + 0 && \text{(by the inverse of } +\text{)} \\
\implies & f_{-,1} + 0 = f_{-,2} + 0 && \text{(by the commutativity of } +\text{)} \\
\implies & f_{-,1} = f_{-,2} && \text{(by the identity of } +\text{).}
\end{aligned}$$

Thus, the two field additive inverses $f_{-,1}$ and $f_{-,2}$ have to be identical. □

This means that, for every f in F, a corresponding f_- not only has to exist; it also has to be unique. Therefore, we don't have to be careful and say that f_- is *a* field additive inverse of f. We can go ahead and say that f_- is *the* field additive inverse of f.

Theorem 1.0.6 (Reciprocity of Field Additive Inverses)**.** *Let $\mathbb{F}(F, +, *)$ be a field. Then, for all f_1 and f_2 in F, $f_1 = (f_2)_- \iff f_2 = (f_1)_-$. That is, field additive inverses occur in "mutual pairs": if f_1 is the field additive inverse of f_2, then f_2 is also the field additive inverse of f_1, and vice versa.*

Proof.

$$\begin{aligned}
& f_1 \text{ is the field additive inverse of } f_2 \\
\iff\ & f_2 + f_1 = 0 && \text{(by the definition of field additive inverse)} \\
\iff\ & f_1 + f_2 = 0 && \text{(by the commutativity of} + \text{)} \\
\iff\ & f_2 \text{ is the field additive inverse of } f_1 && \text{(by the definition of field additive inverse).}
\end{aligned}$$

A succinct way of stating the above is: for every f in F, $(f_-)_- = f$. □

Theorem 1.0.7 (Unique Field Multiplicative Inverse)**.** *Let $\mathbb{F}(F, +, *)$ be a field. Then, for every $f \neq 0$ in F, the field multiplicative inverse f^{-1} is unique.*

Proof. Suppose, for the sake of contradiction, that there is an $f \neq 0$ in F with two different field multiplicative inversess f_1^{-1} and f_2^{-1}. Then, we have:

$$\begin{aligned}
& f * f_1^{-1} = 1 && \text{(by the inverse of } *\text{)} \\
\implies & f_2^{-1} * (f * f_1^{-1}) = f_2^{-1} * 1 && \text{(pre-multiplying both sides by } f_2^{-1}\text{)} \\
\implies & (f_2^{-1} * f) * f_1^{-1} = f_2^{-1} * 1 && \text{(by the associativity of } *\text{)} \\
\implies & (f * f_2^{-1}) * f_1^{-1} = f_2^{-1} * 1 && \text{(by the commutativity of } *\text{)} \\
\implies & 1 * f_1^{-1} = f_2^{-1} * 1 && \text{(by the inverse of } *\text{)} \\
\implies & f_1^{-1} * 1 = f_2^{-1} * 1 && \text{(by the commutativity of } *\text{)} \\
\implies & f_1^{-1} = f_2^{-1} && \text{(by the identity of } *\text{).}
\end{aligned}$$

Thus, the two field multiplicative inverses f_1^{-1} and f_2^{-1} have to be identical. □

Again, this means that, for every $f \neq 0$ in F, a corresponding f^{-1} not only has to exist; it also has to be unique. Therefore, we don't have to be careful and say that f^{-1} is *a* field multiplicative inverse of f. We can go ahead and say that f^{-1} is *the* field multiplicative inverse of f.

Theorem 1.0.8 (Reciprocity of Field Multiplicative Inverses)**.** *Let $\mathbb{F}(F, +, *)$ be a field. Then, for all f_1 and f_2 in F, $f_1 = f_2^{-1} \iff f_2 = f_1^{-1}$. That is, field multiplicative inverses occur in "mutual pairs": if f_1 is the field multiplicative inverse of f_2, then f_2 is also the field multiplicative inverse of f_1, and vice versa.*

Proof.

$$\begin{aligned}
& f_1 \text{ is the field multiplicative inverse of } f_2 \\
\iff\ & f_2 * f_1 = 1 && \text{(by the definition of field multiplicative inverse)} \\
\iff\ & f_1 * f_2 = 1 && \text{(by the commutativity of} *\text{)} \\
\iff\ & f_2 \text{ is the field multiplicative inverse of } f_1 && \text{(by the definition of field multiplicative inverse).}
\end{aligned}$$

A succinct way of stating the above is: for every $f \neq 0$ in F, $(f^{-1})^{-1} = f$. □

Theorem 1.0.9 (Field Multiplication and Field Additive Inverses)**.** *Let $\mathbb{F}(F, +, *)$ be a field. Then, for all f in F, $f_- = f * 1_-$. In other words, the field additive inverse of any element can be obtained by multiplying the element with the field additive inverse of 1.*

Proof. Let f be any element of F. Then, we have:

$$\begin{aligned}
(f * 1_-) + f &= (f * 1_-) + (f * 1) && \text{(by the identity of } *\text{)} \\
&= f * (1_- + 1) && \text{(by the distributivity of } * \text{ over } +\text{)} \\
&= f * (1 + 1_-) && \text{(by the commutativity of } +\text{)} \\
&= f * 0 && \text{(by the inverse of } +\text{)} \\
&= 0 && \text{(by Theorem 1.0.4).}
\end{aligned}$$

Therefore, $f * 1_-$ and f are additive inverses of each other. So, $f_- = f * 1_-$. □

2. Vector Spaces

Definition 2.0.1 (Vector Space)**.** *A vector space* $\mathbb{V}(\mathbb{F}, V, \oplus, \bullet)$*, over a field* $\mathbb{F}(F, +, *)$*, is a set* V*, together with operations* $\oplus : V \times V \to V$ *(called "vector addition") and* $\bullet : F \times V \to V$ *(called "scalar multiplication") that satisfy the following properties (called "vector space axioms"):*

1. ***Closure of*** $\oplus$ ***and*** $\bullet$***.***
   For all $\vec{v}_1$ *and* $\vec{v}_2$ *in* V*,* $\vec{v}_1 \oplus \vec{v}_2$ *belongs to* V*, and*
   For every f *in* F *and* $\vec{v}$ *in* V*,* $f \bullet \vec{v}$ *belongs to* V*.*
2. ***Commutativity of*** $\oplus$***.***
   For all $\vec{v}_1$ *and* $\vec{v}_2$ *in* V*,* $\vec{v}_1 \oplus \vec{v}_2 = \vec{v}_2 \oplus \vec{v}_1$*.*
3. ***Associativity of*** $\oplus$***.***
   For all $\vec{v}_1$*,* $\vec{v}_2$*, and* $\vec{v}_3$ *in* V*,* $(\vec{v}_1 \oplus \vec{v}_2) \oplus \vec{v}_3 = \vec{v}_1 \oplus (\vec{v}_2 \oplus \vec{v}_3)$*.*
4. ***Identity of*** $\oplus$***.***
   There exists an element $\vec{0}$ *(called the "zero vector") in* V *such that, for every* $\vec{v}$ *in* V*,* $\vec{v} \oplus \vec{0} = \vec{v}$*.*
5. ***Inverse of*** $\oplus$***.***
   For every $\vec{v}$ *in* V*, there exists an element (called the vector space additive inverse of* $\vec{v}$*, or the inverse of* $\vec{v}$ *with respect to* $\oplus$*, and denoted* $\vec{v}_\ominus$*) in* V *such that* $\vec{v} \oplus \vec{v}_\ominus = \vec{0}$*.*
6. ***Scalar multiplication by 1.***
   For every $\vec{v}$ *in* V*,* $1 \bullet \vec{v} = \vec{v}$*.*
7. ***Compatibility of scalar multiplication.***
   For every $\vec{v}$ *in* V*, and for all* f_1 *and* f_2 *in* F*,* $f_1 \bullet (f_2 \bullet \vec{v}) = (f_1 * f_2) \bullet \vec{v}$*.*
8. ***Distributive properties.***
   For every $\vec{v}$ *in* V*, and for all* f_1 *and* f_2 *in* F*,* $(f_1 + f_2) \bullet \vec{v} = (f_1 \bullet \vec{v}) \oplus (f_2 \bullet \vec{v})$*, and*
   For every f *in* F*, and for all* $\vec{v}_1$ *and* $\vec{v}_2$ *in* V*,* $f \bullet (\vec{v}_1 \oplus \vec{v}_2) = (f \bullet \vec{v}_1) \oplus (f \bullet \vec{v}_2)$*.*

The elements of V above are usually called "vectors", while the elements of F are usually called "scalars".

Example 2.0.2. *The set of all* $m \times n$ *matrices, over the field of either real numbers or complex numbers, with* $\oplus$ *and* $\bullet$ *defined to be "normal" matrix addition and "normal" scalar matrix multiplication respectively, forms a vector space.*

Example 2.0.3. *The set of all polynomials (with complex coefficients) of degree* n*, over the field of complex numbers, with* $\oplus$ *and* $\bullet$ *defined to be "normal" polynomial addition and "normal" scalar polynomial multiplication respectively, forms a vector space.*

As with fields, several interesting lemmas and theorems can be deduced from the vector space axioms as well. Some important results are as follows.

Theorem 2.0.4 (Multiplication by the Zero Vector)**.** *Let* $\mathbb{V}(\mathbb{F}, V, \oplus, \bullet)$ *be a vector space. Then, for every* f *in* F*,* $f \bullet \vec{0} = \vec{0}$*.*

Proof. Take any element f in F. Then, we have:

$$\begin{aligned}
f \bullet \vec{0} &= (f \bullet \vec{0}) \oplus \vec{0} && \text{(by the identity of } \oplus\text{)} \\
&= (f \bullet \vec{0}) \oplus \Big((f \bullet \vec{0}) \oplus (f \bullet \vec{0})_{\ominus}\Big) && \text{(by the inverse of } \oplus\text{)} \\
&= \Big((f \bullet \vec{0}) \oplus (f \bullet \vec{0})\Big) \oplus (f \bullet \vec{0})_{\ominus} && \text{(by the associativity of } \oplus\text{)} \\
&= \Big(f \bullet (\vec{0} \oplus \vec{0})\Big) \oplus (f \bullet \vec{0})_{\ominus} && \text{(by the second distributive property)} \\
&= (f \bullet \vec{0}) \oplus (f \bullet \vec{0})_{\ominus} && \text{(by the identity of } \oplus\text{)} \\
&= \vec{0} && \text{(by the inverse of } \oplus\text{).}
\end{aligned}$$

□

Theorem 2.0.5 (Multiplication by Scalar Zero)**.** *Let* $\mathbb{V}(\mathbb{F}, V, \oplus, \bullet)$ *be a vector space. Then, for every* $\vec{v}$ *in* V*,* $0 \bullet \vec{v} = \vec{0}$*.*

Proof. Take any element $\vec{v}$ in V. Then, we have:

$$\begin{aligned}
0 \bullet \vec{v} &= (0 \bullet \vec{v}) \oplus \vec{0} && \text{(by the identity of } \oplus\text{)} \\
&= (0 \bullet \vec{v}) \oplus ((0 \bullet \vec{v}) \oplus (0 \bullet \vec{v})_{\ominus}) && \text{(by the inverse of } \oplus\text{)} \\
&= ((0 \bullet \vec{v}) \oplus (0 \bullet \vec{v})) \oplus (0 \bullet \vec{v})_{\ominus} && \text{(by the associativity of } \oplus\text{)} \\
&= ((0 + 0) \bullet \vec{v}) \oplus (0 \bullet \vec{v})_{\ominus} && \text{(by the first distributive property)} \\
&= (0 \bullet \vec{v}) \oplus (0 \bullet \vec{v})_{\ominus} && \text{(by the identity of } +\text{)} \\
&= \vec{0} && \text{(by the inverse of } \oplus\text{).}
\end{aligned}$$

□

Theorem 2.0.6 (Unique Vector Space Additive Inverse)**.** *Let* $\mathbb{V}(\mathbb{F}, V, \oplus, \bullet)$ *be a vector space. Then, for every* $\vec{v}$ *in* V*, the vector space additive inverse* $\vec{v}_{\ominus}$ *is unique.*

Proof. Suppose, for the sake of contradiction, that there is a $\vec{v}$ in V with two different vector space additive inverses $\vec{v}_{\ominus,1}$ and $\vec{v}_{\ominus,2}$. Then, we have:

$$\begin{aligned}
&\vec{v} \oplus \vec{v}_{\ominus,1} = \vec{0} && \text{(by the inverse of } \oplus\text{)} \\
\implies &\vec{v}_{\ominus,2} \oplus (\vec{v} \oplus \vec{v}_{\ominus,1}) = \vec{v}_{\ominus,2} \oplus \vec{0} && \text{(vector adding } \vec{v}_{\ominus,2} \text{ to both sides)}
\end{aligned}$$

$$
\begin{aligned}
&\implies (\vec{v}_{\ominus,\,2} \oplus \vec{v}) \oplus \vec{v}_{\ominus,\,1} = \vec{v}_{\ominus,\,2} \oplus \vec{0} && \text{(by the associativity of } \oplus\text{)}\\
&\implies (\vec{v} \oplus \vec{v}_{\ominus,\,2}) \oplus \vec{v}_{\ominus,\,1} = \vec{v}_{\ominus,\,2} \oplus \vec{0} && \text{(by the commutativity of } \oplus\text{)}\\
&\implies \vec{0} \oplus \vec{v}_{\ominus,\,1} = \vec{v}_{\ominus,\,2} \oplus \vec{0} && \text{(by the inverse of } \oplus\text{)}\\
&\implies \vec{v}_{\ominus,\,1} \oplus \vec{0} = \vec{v}_{\ominus,\,2} \oplus \vec{0} && \text{(by the commutativity of } \oplus\text{)}\\
&\implies \vec{v}_{\ominus,\,1} = \vec{v}_{\ominus,\,2} && \text{(by the identity of } \oplus\text{)}
\end{aligned}
$$

Thus, the two vector space additive inverses $\vec{v}_{\ominus,\,1}$ and $\vec{v}_{\ominus,\,2}$ have to be identical. □

Again, this means that, for every $\vec{v}$ in V, a corresponding $\vec{v}_{\ominus}$ not only has to exist; it also has to be unique. Therefore, we don't have to be careful and say that $\vec{v}_{\ominus}$ is *a* vector space additive inverse of $\vec{v}$. We can go ahead and say that $\vec{v}_{\ominus}$ is *the* vector space additive inverse of $\vec{v}$.

Theorem 2.0.7 (Reciprocity of Vector Space Additive Inverses)**.** *Let $\mathbb{V}(\mathbb{F},\, V,\, \oplus,\, \bullet)$ be a vector space. Then, for all $\vec{v}_1$ and $\vec{v}_2$ in V, $\vec{v}_1 = (\vec{v}_2)_{\ominus} \iff \vec{v}_2 = (\vec{v}_1)_{\ominus}$. That is, vector space additive inverses occur in "mutual pairs": if $\vec{v}_1$ is the vector space additive inverse of $\vec{v}_2$, then $\vec{v}_2$ is also the vector space additive inverse of $\vec{v}_1$, and vice versa.*

Proof.

$$
\begin{aligned}
&\vec{v}_1 \text{ is the vector space additive inverse of } \vec{v}_2\\
\iff\ &\vec{v}_2 \oplus \vec{v}_1 = \vec{0} && \text{(by the definition of vector space additive inverse)}\\
\iff\ &\vec{v}_1 \oplus \vec{v}_2 = \vec{0} && \text{(by the commutativity of } \oplus\text{)}\\
\iff\ &\vec{v}_2 \text{ is the vector space additive inverse of } \vec{v}_1 && \text{(by the definition of vector space additive inverse).}
\end{aligned}
$$

A succinct way of stating the above is: for every $\vec{v}$ in V, $(\vec{v}_{\ominus})_{\ominus} = \vec{v}$. □

Definition 2.0.8 (Linear Independence)**.** *Let $\mathbb{V}(\mathbb{F},\, V,\, \oplus,\, \bullet)$ be a vector space over the field $\mathbb{F}(F,\, +,\, *)$. Then, a set of n vectors $\{\vec{v}_1,\, \vec{v}_2,\, \ldots,\, \vec{v}_n\}$ (where each $\vec{v}_i$ ($1 \leq i \leq n$) belongs to V) is said to be linearly independent if:*

$$
\begin{aligned}
&\left(\sum_{i=1}^{n} (c_i \bullet \vec{v}_i)\right) = (c_1 \bullet \vec{v}_1) \oplus (c_2 \bullet \vec{v}_2) \oplus \ldots \oplus (c_n \bullet \vec{v}_n) = \vec{0}\\
\iff\ &c_1 = c_2 = \ldots = c_n = 0,
\end{aligned}
$$

where each c_i ($1 \leq i \leq n$) belongs to F. That is, if any of the scalars c_i is not 0, then the sum $\sum_{i=1}^{n} (c_i \bullet v_i)$ will not be $\vec{0}$.

Definition 2.0.9 (Linear Dependence)**.** *Let $\mathbb{V}(\mathbb{F},\, V,\, \oplus,\, \bullet)$ be a vector space over the field $\mathbb{F}(F,\, +,\, *)$. Then, a set of n vectors $\{\vec{v}_1,\, \vec{v}_2,\, \ldots,\, \vec{v}_n\}$ (where each $\vec{v}_i$ ($1 \leq i \leq n$) belongs to V) is said to be linearly dependent if it is not linearly independent. That is, there exist scalars c_i ($1 \leq i \leq n$) belonging to F, not all of which are 0, such that:*

$$
\sum_{i=1}^{n} (c_i \bullet v_i) = (c_1 \bullet \vec{v}_1) \oplus (c_2 \bullet \vec{v}_2) \oplus \ldots \oplus (c_n \bullet \vec{v}_n) = \vec{0}.
$$

Definition 2.0.10 (Span)**.** *Let $\mathbb{V}(\mathbb{F},\, V,\, \oplus,\, \bullet)$ be a vector space over the field $\mathbb{F}(F,\, +,\, *)$. Then, the span of a set of n vectors $\{\vec{v}_1,\, \vec{v}_2,\, \ldots,\, \vec{v}_n\}$ (where each $\vec{v}_i$ ($1 \leq i \leq n$) belongs to V) is the set of all vectors $\vec{v}$ in V that can be written as a linear combination of the vectors $\vec{v}_i$ ($1 \leq i \leq n$). That is:*

$$\text{span}\left(\{v_i\}_{1 \leq i \leq n}\right) = \left\{ \sum_{i=1}^{n} (c_i \bullet v_i),\ \text{where } c_i \in F \text{ for each } 1 \leq i \leq n \right\}.$$

Note: the concepts of linear independence and dependence, as well as span, have only been defined for *finite* subsets of V above. When you deal with *infinite* subsets of V, you have to grapple with notions of convergence and so on. This becomes hairy very quickly, so I'm not getting into it.

Definition 2.0.11 (Basis)**.** *Let $\mathbb{V}(\mathbb{F},\, V,\, \oplus,\, \bullet)$ be a vector space. Then, a linearly independent set of n vectors $B = \{\vec{v}_1,\, \vec{v}_2,\, \ldots,\, \vec{v}_n\}$ (where each $\vec{v}_i$ ($1 \leq i \leq n$) belongs to V) is said to form a basis (or be a basis set) of $\mathbb{V}$ if* span $\left(\{v_i\}_{1 \leq i \leq n}\right) = V$*. That is, any vector $\vec{v}$ in the vector space can be expressed as a linear combination of the basis vectors $\vec{v}_i$ ($1 \leq i \leq n$). The number n, which is the size of the basis set B, is called the dimension of B.*

Note: the notion of basis above assumes that n is finite. As such, the definition above applies only to the so called *finite dimensional vector spaces* (those that have a finite basis). Infinite dimensional vector spaces are far more complicated, and we're not going to concern ourselves with those here.

Theorem 2.0.12 (Dimension Theorem for Vector Spaces)**.** *Let $\mathbb{V}(\mathbb{F},\, V,\, \oplus,\, \bullet)$ be a vector space, and let B_1 and B_2 be two (finite) basis sets of $\mathbb{V}$. Then, B_1 and B_2 have the same dimension.*

Proof. See the Wikipedia article on the dimension theorem for vector spaces [1]. □

3. Inner Products

In this section, we'll consider vector spaces whose underlying field is either the real numbers or the complex numbers (with $+$ and $*$ defined to be the "normal" addition and multiplication of such numbers respectively). We'll also assume that the reader is familiar with the basics of complex arithmetic, including addition and multiplication of complex numbers, properties of the complex conjugate, absolute values of complex numbers *etc*. We won't cover these basics here; a good place to look them up would be the Wikipedia article on complex numbers [2].

Below, we'll use $\overline{z}$ to denote the complex conjugate of the real/complex number z; of course, if z is real, $\overline{z}$ and z are the same thing. Also, we'll use $|z|$ to denote the absolute value of the real/complex number z.

Definition 3.0.1 (Inner Product)**.** *Suppose you have a vector space $\mathbb{V}(\mathbb{F},\, V,\, \oplus,\, \bullet)$ over the field $\mathbb{F}(F,\, +,\, *)$. Suppose the field $\mathbb{F}$ is either $\mathbb{R}$ (the real numbers) or $\mathbb{C}$ (the complex numbers), where the field operations $+$ and $*$ correspond to "normally" adding and multiplying real/complex numbers respectively. Then, an "inner product" is a function $\langle .,\, . \rangle : V \times V \to F$, that assigns to every pair of vectors $(\vec{v}_1, \vec{v}_2)$ from V a number in F (denoted $\langle \vec{v}_1,\, \vec{v}_2 \rangle$), and that satisfies the following properties (called the "inner product axioms"):*

1. ***Closure.***
   For all $\vec{v}_1$ and $\vec{v}_2$ in V, $\langle \vec{v}_1,\, \vec{v}_2 \rangle$ belongs to F (and as we said above, F is either the set of real numbers or the set of complex numbers).

2. ***Conjugate symmetry.***
   For all $\vec{v}_1$ and $\vec{v}_2$ in V, $\langle \vec{v}_2,\, \vec{v}_1 \rangle = \overline{\langle \vec{v}_1,\, \vec{v}_2 \rangle}$.

3. ***Linearity in the first argument.***
   For all $\vec{v}_1$, $\vec{v}_2$, and $\vec{v}_3$ in V, and for all f in F, we have:

   Additivity: $\langle\, (\vec{v}_1 \oplus \vec{v}_2),\, \vec{v}_3\, \rangle = \langle \vec{v}_1,\, \vec{v}_3 \rangle + \langle \vec{v}_2,\, \vec{v}_3 \rangle$, and
   Homogeneity: $\langle\, (f \bullet \vec{v}_1),\, \vec{v}_2)\, \rangle = f * \langle \vec{v}_1,\, \vec{v}_2 \rangle$.

4. ***Realness and non-negativity on the diagonal.***
   For every $\vec{v}$ in V, $\langle\, \vec{v},\, \vec{v}\, \rangle \geq 0$. That is, the inner product of every vector with itself is real and non-negative.

5. ***Definiteness.***
   For every $\vec{v}$ in V, $\langle\, \vec{v},\, \vec{v}\, \rangle = 0 \iff \vec{v} = \vec{0}$.

If an inner product function $\langle ., . \rangle$ satisfying the properties above is defined for a vector space $\mathbb{V}$, then $\mathbb{V}$ is called an "inner product space" associated with the inner product $\langle ., . \rangle$.

Theorem 3.0.2 (Inner Product with the Zero Vector)**.** *Let $\mathbb{V}(\mathbb{F}, V, \oplus, \bullet)$ be an inner product space, associated with the inner product $\langle ., . \rangle$, over the field $\mathbb{F}(F, +, *)$. Then, for any vector $\vec{v}$ in V, $\left\langle \vec{v}, \vec{0} \right\rangle = 0$.*

Proof. Let $\vec{v}$ be any vector in V. Then, we have:

$$\begin{aligned}
\left\langle \vec{v}, \vec{0} \right\rangle &= \langle \vec{v}, (0 \bullet \vec{v}) \rangle && \text{(by Theorem 2.0.5)} \\
&= \overline{\langle (0 \bullet \vec{v}), \vec{v} \rangle} && \text{(by the conjugate symmetry of } \langle ., . \rangle \text{)} \\
&= \overline{0 * \langle \vec{v}, \vec{v} \rangle} && \text{(by the homogeneity of } \langle ., . \rangle \text{ in the first argument)} \\
&= \overline{\langle \vec{v}, \vec{v} \rangle * 0} && \text{(by the commutativity of } * \text{)} \\
&= \overline{0} && \text{(by Theorem 1.0.4)} \\
&= 0 && \text{(from the definition of complex conjugate).}
\end{aligned}$$

□

Theorem 3.0.3 (Inner Products and Additive Inverses)**.** *Let $\mathbb{V}(\mathbb{F}, V, \oplus, \bullet)$ be an inner product space, associated with the inner product $\langle ., . \rangle$, over the field $\mathbb{F}(F, +, *)$. Then, for all $\vec{v}_1$ and $\vec{v}_2$ in V, $\langle \vec{v}_1, (\vec{v}_2)_\ominus \rangle = \langle (\vec{v}_1)_\ominus, \vec{v}_2 \rangle = \langle \vec{v}_1, \vec{v}_2 \rangle_- = \langle \vec{v}_1, \vec{v}_2 \rangle * 1_-$*

Proof. Let $\vec{v}_1$ and $\vec{v}_2$ be any two vectors in V. Then, we have:

$$\begin{aligned}
\langle \vec{v}_1, (\vec{v}_2)_\ominus \rangle + \langle \vec{v}_1, \vec{v}_2 \rangle &= \overline{\langle (\vec{v}_2)_\ominus, \vec{v}_1 \rangle} + \overline{\langle \vec{v}_2, \vec{v}_1 \rangle} && \text{(by the conjugate symmetry of } \langle ., . \rangle \text{)} \\
&= \overline{\langle (\vec{v}_2)_\ominus, \vec{v}_1 \rangle + \langle \vec{v}_2, \vec{v}_1 \rangle} && \text{(because } \overline{z_1 + z_2} = \overline{z_1} + \overline{z_2} \text{ for all real/complex } z_1, z_2\text{)} \\
&= \overline{\langle ((\vec{v}_2)_\ominus \oplus \vec{v}_2), \vec{v}_1 \rangle} && \text{(by the additivity of } \langle ., . \rangle \text{ in the first argument)} \\
&= \overline{\langle (\vec{v}_2 \oplus (\vec{v}_2)_\ominus), \vec{v}_1 \rangle} && \text{(by the commutativity of } \oplus \text{)} \\
&= \overline{\left\langle \vec{0}, \vec{v}_1 \right\rangle} && \text{(by the inverse of } \oplus \text{)} \\
&= \left\langle \vec{v}_1, \vec{0} \right\rangle && \text{(by the conjugate symmetry of } \langle ., . \rangle \text{)} \\
&= 0 && \text{(by Theorem 3.0.2).}
\end{aligned}$$

Therefore, $\langle \vec{v}_1, (\vec{v}_2)_\ominus \rangle$ and $\langle \vec{v}_1, \vec{v}_2 \rangle$ are field additive inverses of each other. Therefore, we have:

$$\begin{aligned}
\langle \vec{v}_1, (\vec{v}_2)_\ominus \rangle &= \langle \vec{v}_1, \vec{v}_2 \rangle_- \\
&= \langle \vec{v}_1, \vec{v}_2 \rangle * 1_- && \text{(by Theorem 1.0.9).} \qquad (3.1)
\end{aligned}$$

Furthermore, we have:

$$\begin{aligned}
\langle (\vec{v}_1)_\ominus, \vec{v}_2 \rangle + \langle \vec{v}_1, \vec{v}_2 \rangle &= \langle (\vec{v}_1)_\ominus \oplus \vec{v}_1, \vec{v}_2 \rangle && \text{(by the additivity of } \langle ., . \rangle \text{ in the first argument)} \\
&= \langle \vec{v}_1 \oplus (\vec{v}_1)_\ominus, \vec{v}_2 \rangle && \text{(by the commutativity of } \oplus \text{)} \\
&= \left\langle \vec{0}, \vec{v}_2 \right\rangle && \text{(by the inverse of } \oplus \text{)}
\end{aligned}$$

$$
\begin{aligned}
&= \overline{\left\langle \vec{v}_2,\, \vec{0} \right\rangle} && \text{(by the conjugate symmetry of } \langle .,\, . \rangle\text{)} \\
&= \overline{0} && \text{(by Theorem 3.0.2)} \\
&= 0 && \text{(because the complex conjugate of 0 is 0).}
\end{aligned}
$$

Therefore, $\langle (\vec{v}_1)_\ominus,\, \vec{v}_2 \rangle$ and $\langle \vec{v}_1,\, \vec{v}_2 \rangle$ are field additive inverses of each other. Therefore, we have:

$$
\begin{aligned}
\langle (\vec{v}_1)_\ominus,\, \vec{v}_2 \rangle &= \langle \vec{v}_1,\, \vec{v}_2 \rangle_- \\
&= \langle \vec{v}_1,\, \vec{v}_2 \rangle * 1_- && \text{(by Theorem 1.0.9).}
\end{aligned} \tag{3.2}
$$

From Eq. (3.1) and Eq. (3.2), it follows that $\langle \vec{v}_1,\, (\vec{v}_2)_\ominus \rangle = \langle (\vec{v}_1)_\ominus,\, \vec{v}_2 \rangle = \langle \vec{v}_1,\, \vec{v}_2 \rangle_- = \langle \vec{v}_1,\, \vec{v}_2 \rangle * 1_-$. □

Lemma 3.0.4. *Let $\mathbb{V}(\mathbb{F},\, V,\, \oplus,\, \bullet)$ be an inner product space, associated with the inner product $\langle .,\, . \rangle$, over the field $\mathbb{F}(F,\, +,\, *)$. Then, for all $\vec{v}_1$ and $\vec{v}_2$ in V, $\langle (\vec{v}_1)_\ominus,\, (\vec{v}_2)_\ominus \rangle = \langle \vec{v}_1,\, \vec{v}_2 \rangle$.*

Proof. Let $\vec{v}_1$ and $\vec{v}_2$ be any two vectors in V. Then, we have:

$$
\begin{aligned}
\langle (\vec{v}_1)_\ominus,\, (\vec{v}_2)_\ominus \rangle &= \langle (\vec{v}_1)_\ominus,\, \vec{v}_2 \rangle_- && \text{(by Theorem 3.0.3)} \\
&= (\langle \vec{v}_1,\, \vec{v}_2 \rangle_-)_- && \text{(by Theorem 3.0.3)} \\
&= \langle \vec{v}_1,\, \vec{v}_2 \rangle && \text{(by Theorem 1.0.6).}
\end{aligned}
$$

□

Theorem 3.0.5 (Cauchy-Schwarz Inequality)**.** *Let $\mathbb{V}(\mathbb{F},\, V,\, \oplus,\, \bullet)$ be an inner product space, associated with the inner product $\langle .,\, . \rangle$, over the field $\mathbb{F}(F,\, +,\, *)$. Then, for any two vectors $\vec{v}_1$ and $\vec{v}_2$ in V, we have:*

$$
|\langle \vec{v}_1,\, \vec{v}_2 \rangle|^2 \leq \langle \vec{v}_1,\, \vec{v}_1 \rangle * \langle \vec{v}_2,\, \vec{v}_2 \rangle\,. \tag{3.3}
$$

Proof. Let $\vec{v}_1$ and $\vec{v}_2$ be any two vectors in V. Then, we have:

$$
\begin{aligned}
0 &\leq \langle (\langle \vec{v}_2,\, \vec{v}_2 \rangle \bullet \vec{v}_1) \oplus (\langle \vec{v}_1,\, \vec{v}_2 \rangle \bullet (\vec{v}_2)_\ominus)\,,\, (\langle \vec{v}_2,\, \vec{v}_2 \rangle \bullet \vec{v}_1) \oplus (\langle \vec{v}_1,\, \vec{v}_2 \rangle \bullet (\vec{v}_2)_\ominus) \rangle \\
&\quad \text{(apply } \langle\, \vec{v},\, \vec{v}\, \rangle \geq 0\text{, with } \vec{v} = (\langle \vec{v}_2,\, \vec{v}_2 \rangle \bullet \vec{v}_1) \oplus (\langle \vec{v}_1,\, \vec{v}_2 \rangle \bullet (\vec{v}_2)_\ominus)\text{)} \\
&= \langle \vec{v}_2,\, \vec{v}_2 \rangle * \langle \vec{v}_1,\, (\langle \vec{v}_2,\, \vec{v}_2 \rangle \bullet \vec{v}_1) \oplus (\langle \vec{v}_1,\, \vec{v}_2 \rangle \bullet (\vec{v}_2)_\ominus) \rangle \\
&\qquad + \langle \vec{v}_1,\, \vec{v}_2 \rangle * \langle (\vec{v}_2)_\ominus,\, (\langle \vec{v}_2,\, \vec{v}_2 \rangle \bullet \vec{v}_1) \oplus (\langle \vec{v}_1,\, \vec{v}_2 \rangle \bullet (\vec{v}_2)_\ominus) \rangle \\
&\quad \text{(by the linearity of } \langle .,\, . \rangle \text{ in the first argument)} \\
&= \langle \vec{v}_2,\, \vec{v}_2 \rangle * \overline{\langle (\langle \vec{v}_2,\, \vec{v}_2 \rangle \bullet \vec{v}_1) \oplus (\langle \vec{v}_1,\, \vec{v}_2 \rangle \bullet (\vec{v}_2)_\ominus)\,,\, \vec{v}_1 \rangle} \\
&\qquad + \langle \vec{v}_1,\, \vec{v}_2 \rangle * \overline{\langle (\langle \vec{v}_2,\, \vec{v}_2 \rangle \bullet \vec{v}_1) \oplus (\langle \vec{v}_1,\, \vec{v}_2 \rangle \bullet (\vec{v}_2)_\ominus)\,,\, (\vec{v}_2)_\ominus \rangle} \\
&\quad \text{(by the conjugate symmetry of } \langle .,\, . \rangle\text{)} \\
&= \langle \vec{v}_2,\, \vec{v}_2 \rangle * \overline{(\langle \vec{v}_2,\, \vec{v}_2 \rangle * \langle \vec{v}_1,\, \vec{v}_1 \rangle) + (\langle \vec{v}_1,\, \vec{v}_2 \rangle * \langle (\vec{v}_2)_\ominus,\, \vec{v}_1 \rangle)} \\
&\qquad + \langle \vec{v}_1,\, \vec{v}_2 \rangle * \overline{(\langle \vec{v}_2,\, \vec{v}_2 \rangle * \langle \vec{v}_1,\, (\vec{v}_2)_\ominus \rangle) + (\langle \vec{v}_1,\, \vec{v}_2 \rangle * \langle (\vec{v}_2)_\ominus,\, (\vec{v}_2)_\ominus \rangle)} \\
&\quad \text{(by the linearity of } \langle .,\, . \rangle \text{ in the first argument)} \\
&= \langle \vec{v}_2,\, \vec{v}_2 \rangle * \left(\overline{\langle \vec{v}_2,\, \vec{v}_2 \rangle} * \overline{\langle \vec{v}_1,\, \vec{v}_1 \rangle} + \overline{\langle \vec{v}_1,\, \vec{v}_2 \rangle} * \overline{\langle (\vec{v}_2)_\ominus,\, \vec{v}_1 \rangle} \right)
\end{aligned}
$$

$$+ \langle \vec{v}_1,\, \vec{v}_2 \rangle * \left(\overline{\langle \vec{v}_2,\, \vec{v}_2 \rangle} * \overline{\langle \vec{v}_1,\, (\vec{v}_2)_\ominus \rangle} + \overline{\langle \vec{v}_1,\, \vec{v}_2 \rangle} * \overline{\langle (\vec{v}_2)_\ominus,\, (\vec{v}_2)_\ominus \rangle} \right)$$

(using basic properties of complex conjugates)

$$= \langle \vec{v}_2,\, \vec{v}_2 \rangle * (\langle \vec{v}_2,\, \vec{v}_2 \rangle * \langle \vec{v}_1,\, \vec{v}_1 \rangle + \langle \vec{v}_2,\, \vec{v}_1 \rangle * \langle \vec{v}_1,\, (\vec{v}_2)_\ominus \rangle)$$
$$+ \langle \vec{v}_1,\, \vec{v}_2 \rangle * (\langle \vec{v}_2,\, \vec{v}_2 \rangle * \langle (\vec{v}_2)_\ominus,\, \vec{v}_1 \rangle + \langle \vec{v}_2,\, \vec{v}_1 \rangle * \langle (\vec{v}_2)_\ominus,\, (\vec{v}_2)_\ominus \rangle)$$

(by the conjugate symmetry of $\langle .,\, . \rangle$)

$$= \langle \vec{v}_2,\, \vec{v}_2 \rangle * (\langle \vec{v}_2,\, \vec{v}_2 \rangle * \langle \vec{v}_1,\, \vec{v}_1 \rangle + \langle \vec{v}_2,\, \vec{v}_1 \rangle * \langle \vec{v}_1,\, (\vec{v}_2)_\ominus \rangle)$$
$$+ \langle \vec{v}_1,\, \vec{v}_2 \rangle * \left(\langle \vec{v}_2,\, \vec{v}_2 \rangle * \langle \vec{v}_2,\, \vec{v}_1 \rangle_- + \langle \vec{v}_2,\, \vec{v}_1 \rangle * \langle \vec{v}_2,\, \vec{v}_2 \rangle \right)$$

(by Theorem 3.0.3 and Lemma 3.0.4)

$$= \langle \vec{v}_2,\, \vec{v}_2 \rangle * (\langle \vec{v}_2,\, \vec{v}_2 \rangle * \langle \vec{v}_1,\, \vec{v}_1 \rangle + \langle \vec{v}_2,\, \vec{v}_1 \rangle * \langle \vec{v}_1,\, (\vec{v}_2)_\ominus \rangle)$$
$$+ (\langle \vec{v}_1,\, \vec{v}_2 \rangle * \langle \vec{v}_2,\, \vec{v}_2 \rangle) * \left(\langle \vec{v}_2,\, \vec{v}_1 \rangle + \langle \vec{v}_2,\, \vec{v}_1 \rangle_- \right)$$

(using basic properties of addition and multiplication of real/complex numbers)

$$= \langle \vec{v}_2,\, \vec{v}_2 \rangle * (\langle \vec{v}_2,\, \vec{v}_2 \rangle * \langle \vec{v}_1,\, \vec{v}_1 \rangle + \langle \vec{v}_2,\, \vec{v}_1 \rangle * \langle \vec{v}_1,\, (\vec{v}_2)_\ominus \rangle) + (\langle \vec{v}_1,\, \vec{v}_2 \rangle * \langle \vec{v}_2,\, \vec{v}_2 \rangle) * 0$$

(by the inverse of $+$)

$$= \langle \vec{v}_2,\, \vec{v}_2 \rangle * (\langle \vec{v}_2,\, \vec{v}_2 \rangle * \langle \vec{v}_1,\, \vec{v}_1 \rangle + \langle \vec{v}_2,\, \vec{v}_1 \rangle * \langle \vec{v}_1,\, (\vec{v}_2)_\ominus \rangle) + 0$$

(by Theorem 1.0.4)

$$= \langle \vec{v}_2,\, \vec{v}_2 \rangle * (\langle \vec{v}_2,\, \vec{v}_2 \rangle * \langle \vec{v}_1,\, \vec{v}_1 \rangle + \langle \vec{v}_2,\, \vec{v}_1 \rangle * \langle \vec{v}_1,\, (\vec{v}_2)_\ominus \rangle)$$

(by the identity of $+$).

Dividing both sides above by the non-negative quantity $\langle \vec{v}_2,\, \vec{v}_2 \rangle$, we obtain:

$$0 \leq \langle \vec{v}_2,\, \vec{v}_2 \rangle * \langle \vec{v}_1,\, \vec{v}_1 \rangle + \langle \vec{v}_2,\, \vec{v}_1 \rangle * \langle \vec{v}_1,\, (\vec{v}_2)_\ominus \rangle$$
$$= \langle \vec{v}_2,\, \vec{v}_2 \rangle * \langle \vec{v}_1,\, \vec{v}_1 \rangle + \langle \vec{v}_2,\, \vec{v}_1 \rangle * (\langle \vec{v}_1,\, \vec{v}_2 \rangle * 1_-) \qquad \text{(by Theorem 3.0.3)}$$
$$= \langle \vec{v}_2,\, \vec{v}_2 \rangle * \langle \vec{v}_1,\, \vec{v}_1 \rangle + (\langle \vec{v}_2,\, \vec{v}_1 \rangle * \langle \vec{v}_1,\, \vec{v}_2 \rangle) * 1_- \qquad \text{(by the commutativity of } *\text{)}$$
$$= \langle \vec{v}_2,\, \vec{v}_2 \rangle * \langle \vec{v}_1,\, \vec{v}_1 \rangle + (\langle \vec{v}_2,\, \vec{v}_1 \rangle * \langle \vec{v}_1,\, \vec{v}_2 \rangle)_- \qquad \text{(by Theorem 1.0.9)}$$
$$= \langle \vec{v}_2,\, \vec{v}_2 \rangle * \langle \vec{v}_1,\, \vec{v}_1 \rangle + (\overline{\langle \vec{v}_1,\, \vec{v}_2 \rangle} * \langle \vec{v}_1,\, \vec{v}_2 \rangle)_- \qquad \text{(by the conjugate symmetry of } \langle .,\, . \rangle\text{)}$$
$$= \langle \vec{v}_2,\, \vec{v}_2 \rangle * \langle \vec{v}_1,\, \vec{v}_1 \rangle + (|\langle \vec{v}_1,\, \vec{v}_2 \rangle|^2)_- \qquad \text{(because } \overline{z}z = |z|^2 \text{ for all real/complex } z\text{).}$$

Adding $|\langle \vec{v}_1,\, \vec{v}_2 \rangle|^2$ to both sides, we obtain:

$$|\langle \vec{v}_1,\, \vec{v}_2 \rangle|^2 \leq \left(\langle \vec{v}_2,\, \vec{v}_2 \rangle * \langle \vec{v}_1,\, \vec{v}_1 \rangle + \left(|\langle \vec{v}_1,\, \vec{v}_2 \rangle|^2 \right)_- \right) + |\langle \vec{v}_1,\, \vec{v}_2 \rangle|^2$$
$$= \langle \vec{v}_2,\, \vec{v}_2 \rangle * \langle \vec{v}_1,\, \vec{v}_1 \rangle + \left(\left(|\langle \vec{v}_1,\, \vec{v}_2 \rangle|^2 \right)_- + |\langle \vec{v}_1,\, \vec{v}_2 \rangle|^2 \right)$$

(by the associativity of $+$)

$$= \langle \vec{v}_2,\, \vec{v}_2 \rangle * \langle \vec{v}_1,\, \vec{v}_1 \rangle + \left(|\langle \vec{v}_1,\, \vec{v}_2 \rangle|^2 + \left(|\langle \vec{v}_1,\, \vec{v}_2 \rangle|^2 \right)_- \right)$$

(by the commutativity of $+$)

$$= \langle \vec{v}_2,\, \vec{v}_2 \rangle * \langle \vec{v}_1,\, \vec{v}_1 \rangle + 0$$

(by the inverse of $+$)

$$= \langle \vec{v}_2,\, \vec{v}_2 \rangle * \langle \vec{v}_1,\, \vec{v}_1 \rangle$$

(by the identity of $+$)

$$= \langle \vec{v}_1,\, \vec{v}_1 \rangle * \langle \vec{v}_2,\, \vec{v}_2 \rangle$$

(by the commutativity of $*$).

Therefore, we have:

$$|\langle \vec{v}_1,\, \vec{v}_2 \rangle|^2 \leq \langle \vec{v}_1,\, \vec{v}_1 \rangle * \langle \vec{v}_2,\, \vec{v}_2 \rangle\,,$$

which is the required result. $\square$

4. Norms

Below, we use R_+ to denote the set of non-negative real numbers.

Definition 4.0.1 (Norm)**.** *Suppose you have a vector space $\mathbb{V}(\mathbb{F},\, V,\, \oplus,\, \bullet)$ over the field $\mathbb{F}(F,\, +,\, *)$. Suppose the field $\mathbb{F}$ is either $\mathbb{R}$ (the real numbers) or $\mathbb{C}$ (the complex numbers), where the field operations $+$ and $*$ correspond to "normally" adding and multiplying real/complex numbers respectively. Then, a "norm" is a function $\|.\| : V \to R_+$, that assigns to every vector $\vec{v}$ in V a non-negative real number (denoted $\|\vec{v}\|$), and that satisfies the following properties (called the "norm axioms"):*

1. ***Realness and non-negativity.***
   For every $\vec{v}$ in V, $\|\,\vec{v}\,\|$ is real and non-negative, i.e., $\|\,\vec{v}\,\| \geq 0$.

2. ***Definiteness.***
   $\|\,\vec{v}\,\| = 0 \iff \vec{v} = \vec{0}$.

3. ***Absolute homogeneity.***
   For every f in F and $\vec{v}$ in V, $\|\,f \bullet \vec{v}\,\| = |f| * \|\,\vec{v}\,\|$.

4. ***The triangle inequality.***
   For all $\vec{v}_1$ and $\vec{v}_2$ in V, $\|\vec{v}_1 \oplus \vec{v}_2\| \leq \|\vec{v}_1\| + \|\vec{v}_2\|$.

Theorem 4.0.2 (Norm Induced by an Inner Product)**.** *Let $\mathbb{V}(\mathbb{F},\, V,\, \oplus,\, \bullet)$ be an inner product space, associated with the inner product $\langle .,\, . \rangle$, over the field $\mathbb{F}(F,\, +,\, *)$. Define a function $g : V \to R_+$, where $g(\vec{v}) = \sqrt{\langle\, \vec{v},\, \vec{v}\,\rangle}$ for every vector $\vec{v}$ in V. Then, g is a norm. That is, g satisfies all the norm axioms of Definition 4.0.1.*

Proof. Let's take the norm axioms one at a time and prove that g satisfies all of them.

1. *Realness and non-negativity.*
   For every $\vec{v}$ in V, we have:

$$
\begin{aligned}
g(\vec{v}) &= \sqrt{\langle\, \vec{v},\, \vec{v}\,\rangle} \\
&= \sqrt{\text{a real non-negative number}} \\
&\quad \text{(from the "realness and non-negativity on the diagonal" of } \langle .,\, .\rangle\text{)} \\
&= \text{a real non-negative number} \\
&\quad \text{(using basic properties of the square root).}
\end{aligned}
$$

2. *Definiteness.*
   We have:

$$
\begin{aligned}
& g(\vec{v}) = \sqrt{\langle\, \vec{v},\, \vec{v}\,\rangle} = 0 \\
\iff & \langle\, \vec{v},\, \vec{v}\,\rangle = 0 && \text{(using basic properties of the square root)} \\
\iff & \vec{v} = \vec{0} && \text{(from the “definiteness” of } \langle .,\, .\rangle\text{).}
\end{aligned}
$$

3. *Absolute homogeneity.*
   For every $\vec{v}$ in V and f in F, we have:

$$
\begin{aligned}
g(f \bullet \vec{v}) &= \sqrt{\langle\, f \bullet \vec{v},\, f \bullet \vec{v}\,\rangle} && \text{(from the definition of } g\text{)} \\
&= \sqrt{f * \langle\, \vec{v},\, f \bullet \vec{v}\,\rangle} && \text{(from the homogeneity of } \langle .,\, .\rangle \text{ in the first argument)} \\
&= \sqrt{f * \overline{\langle\, f \bullet \vec{v},\, \vec{v}\,\rangle}} && \text{(from the conjugate symmetry of } \langle .,\, .\rangle\text{)} \\
&= \sqrt{f * \overline{f * \langle\, \vec{v},\, \vec{v}\,\rangle}} && \text{(from the homogeneity of } \langle .,\, .\rangle \text{ in the first argument)} \\
&= \sqrt{f * \overline{f} * \overline{\langle\, \vec{v},\, \vec{v}\,\rangle}} && \text{(using basic properties of the complex conjugate)} \\
&= \sqrt{|f|^2 * \overline{\langle\, \vec{v},\, \vec{v}\,\rangle}} && \text{(using basic properties of the complex conjugate)} \\
&= \sqrt{|f|^2 * \langle\, \vec{v},\, \vec{v}\,\rangle} && \text{(from the conjugate symmetry of } \langle .,\, .\rangle\text{)} \\
&= |f| * \sqrt{\langle\, \vec{v},\, \vec{v}\,\rangle} && \text{(using basic properties of the square root)} \\
&= |f| * g(\vec{v}) && \text{(from the definition of } g\text{).}
\end{aligned}
$$

4. *The triangle inequality.*
   Let $\vec{v}_1$ and $\vec{v}_2$ be any two vectors in V. Then, we have:

$$
\begin{aligned}
g(\vec{v}_1 \oplus \vec{v}_2) &= \sqrt{\langle\, \vec{v}_1 \oplus \vec{v}_2,\, \vec{v}_1 \oplus \vec{v}_2\,\rangle} \\
&\quad \text{(from the definition of } g\text{)} \\
&= \sqrt{\langle\, \vec{v}_1,\, \vec{v}_1 \oplus \vec{v}_2\,\rangle + \langle\, \vec{v}_2,\, \vec{v}_1 \oplus \vec{v}_2\,\rangle} \\
&\quad \text{(from the additivity of } \langle .,\, .\rangle \text{ in the first argument)} \\
&= \sqrt{\overline{\langle\, \vec{v}_1 \oplus \vec{v}_2,\, \vec{v}_1\,\rangle} + \overline{\langle\, \vec{v}_1 \oplus \vec{v}_2,\, \vec{v}_2\,\rangle}} \\
&\quad \text{(from the conjugate symmetry of } \langle .,\, .\rangle\text{)} \\
&= \sqrt{\overline{\langle\, \vec{v}_1,\, \vec{v}_1\,\rangle + \langle\, \vec{v}_2,\, \vec{v}_1\,\rangle} + \overline{\langle\, \vec{v}_1,\, \vec{v}_2\,\rangle + \langle\, \vec{v}_2,\, \vec{v}_2\,\rangle}} \\
&\quad \text{(from the additivity of } \langle .,\, .\rangle \text{ in the first argument)} \\
&= \sqrt{\overline{\langle\, \vec{v}_1,\, \vec{v}_1\,\rangle} + \overline{\langle\, \vec{v}_2,\, \vec{v}_1\,\rangle} + \overline{\langle\, \vec{v}_1,\, \vec{v}_2\,\rangle} + \overline{\langle\, \vec{v}_2,\, \vec{v}_2\,\rangle}} \\
&\quad \text{(using basic properties of the complex conjugate)} \\
&= \sqrt{\langle\, \vec{v}_1,\, \vec{v}_1\,\rangle + \langle\, \vec{v}_1,\, \vec{v}_2\,\rangle + \overline{\langle\, \vec{v}_1,\, \vec{v}_2\,\rangle} + \langle\, \vec{v}_2,\, \vec{v}_2\,\rangle} \\
&\quad \text{(from the conjugate symmetry of } \langle .,\, .\rangle\text{)} \\
&= \sqrt{\langle\, \vec{v}_1,\, \vec{v}_1\,\rangle + 2 * \mathrm{Re}\,(\langle\, \vec{v}_1,\, \vec{v}_2\,\rangle) + \langle\, \vec{v}_2,\, \vec{v}_2\,\rangle} \\
&\quad \text{(using basic complex arithmetic)} \\
&\leq \sqrt{\langle\, \vec{v}_1,\, \vec{v}_1\,\rangle + 2 * |\langle\, \vec{v}_1,\, \vec{v}_2\,\rangle| + \langle\, \vec{v}_2,\, \vec{v}_2\,\rangle}
\end{aligned}
$$

(because Re$(z) \leq |z|$ for all real/complex z)

$$\leq \sqrt{\langle \vec{v}_1, \vec{v}_1 \rangle + 2 * \sqrt{\langle \vec{v}_1, \vec{v}_1 \rangle \langle \vec{v}_2, \vec{v}_2 \rangle} + \langle \vec{v}_2, \vec{v}_2 \rangle}$$

(by the Cauchy-Schwarz inequality (Theorem 3.0.5))

$$= \sqrt{(g(\vec{v}_1))^2 + 2 * \sqrt{(g(\vec{v}_1))^2 (g(\vec{v}_2))^2} + (g(\vec{v}_2))^2}$$

(from the definition of g)

$$= \sqrt{(g(\vec{v}_1))^2 + 2 * g(\vec{v}_1) * g(\vec{v}_2) + (g(\vec{v}_2))^2}$$

(using basic properties of the square root)

$$= \sqrt{(g(\vec{v}_1) + g(\vec{v}_2))^2}$$

(using basic real arithmetic)

$$= g(\vec{v}_1) + g(\vec{v}_2)$$

(using basic properties of the square root).

□

Thus, whenever $\langle ., . \rangle$ is a valid inner product, the function defined by $\| \vec{v} \| \triangleq \sqrt{\langle \vec{v}, \vec{v} \rangle}$ is a valid norm, called the "norm induced by the inner product" $\langle ., . \rangle$.

References

[1] https://en.wikipedia.org/wiki/Dimension_theorem_for_vector_spaces.

[2] https://en.wikipedia.org/wiki/Complex_Number.

DISTRIBUTION:

1 MS 0899 Technical Library, 9536 (electronic copy)

Sandia National Laboratories