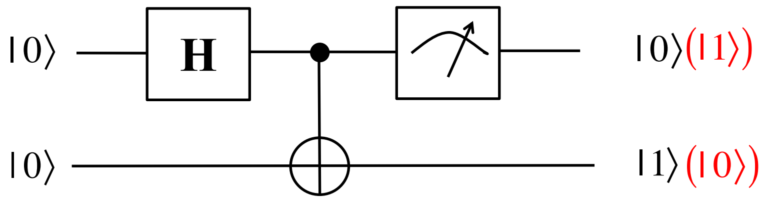
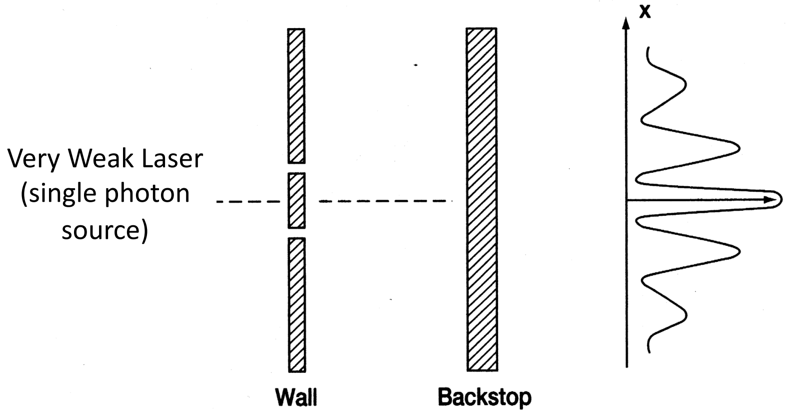
Big Picture Motivation



Representation, models, and the origin of Quantum Mechanics is essential to understand the Quantum Computing Program depicted above

1

Young's Double Slit Experiment as a Computation

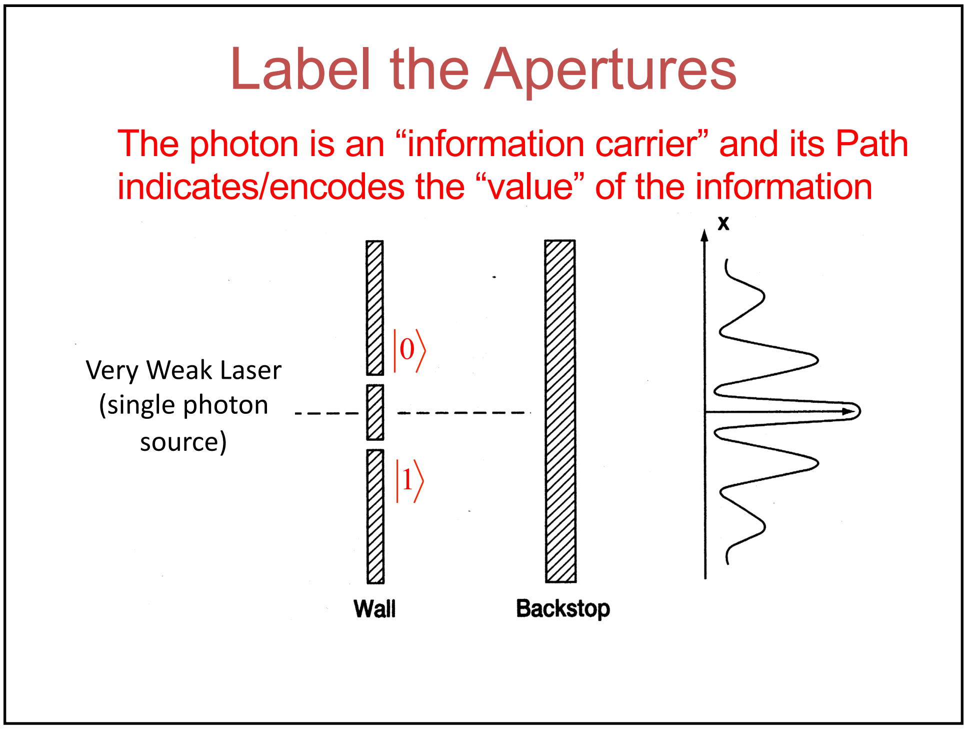

Very Weak Laser (single photon source)

Wall

Backstop

**A.D. Aczel, Entanglement, 2002, ISBN 1-55192-549-4*

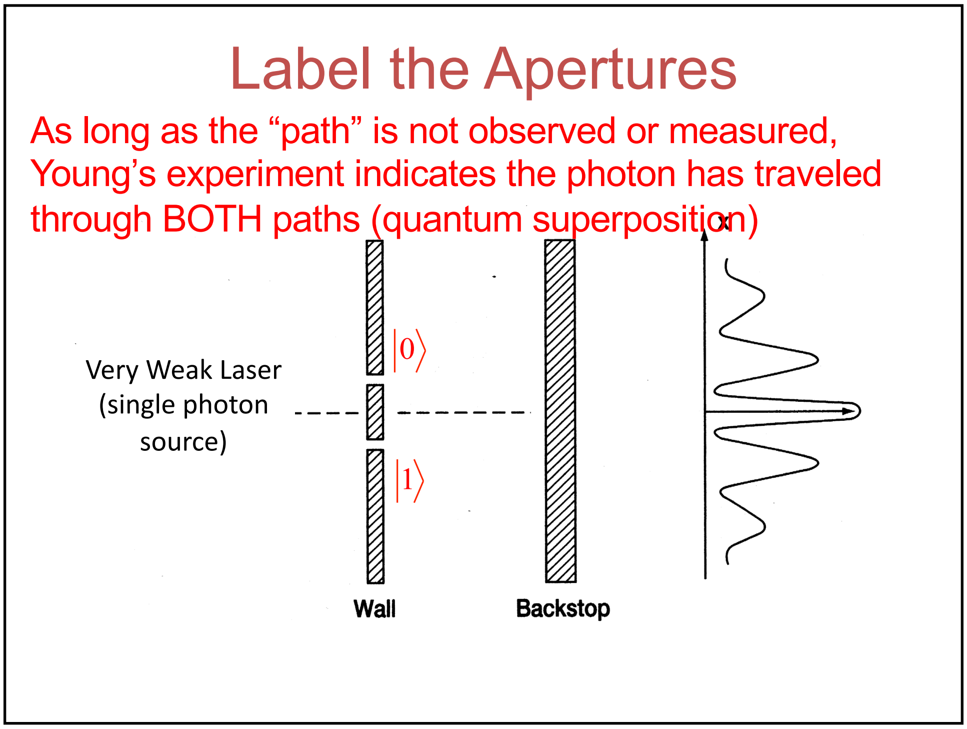
2



Label the Apertures

The photon is an “information carrier” and its Path indicates/encodes the “value” of the information

3



Label the Apertures

As long as the “path” is not observed or measured, Young’s experiment indicates the photon has traveled through BOTH paths (quantum superposition)

4

Thomas Young's Experiment

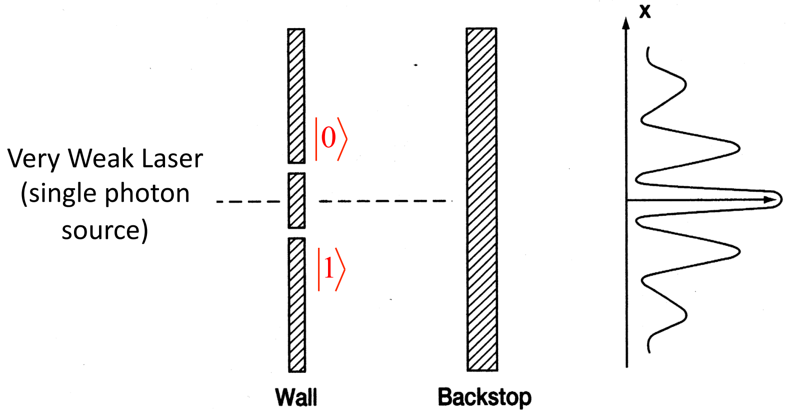
"We choose to examine a phenomenon (the double-slit experiment) that is impossible, *absolutely* impossible, to explain in any classical way, and which has in it the heart of quantum mechanics. In reality it contains the *only* mystery."

-Richard Feynman

5

Label the Apertures

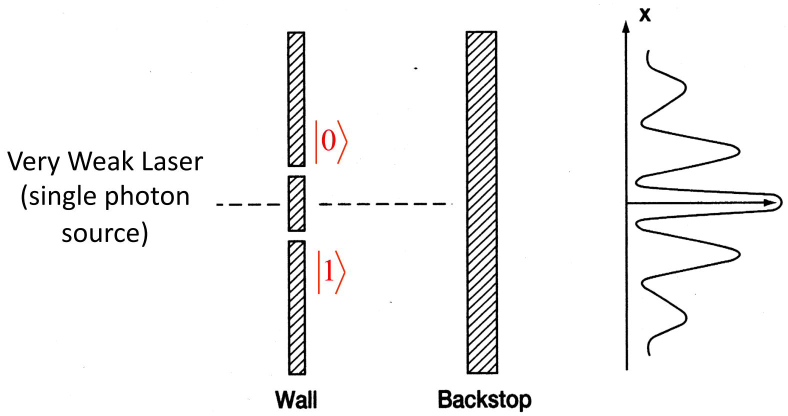
Thus, the photon is now carrying an information content of both "1" AND "0" !!!!! Referred to as $|0\rangle$ and $|1\rangle$.



6

Label the Apertures

Thus, the photon is now carrying an information content of both “1” AND “0” !!!!!



But, when we *measure* or *observe* the path, it will appear to only have traveled through either the top or the bottom path

7

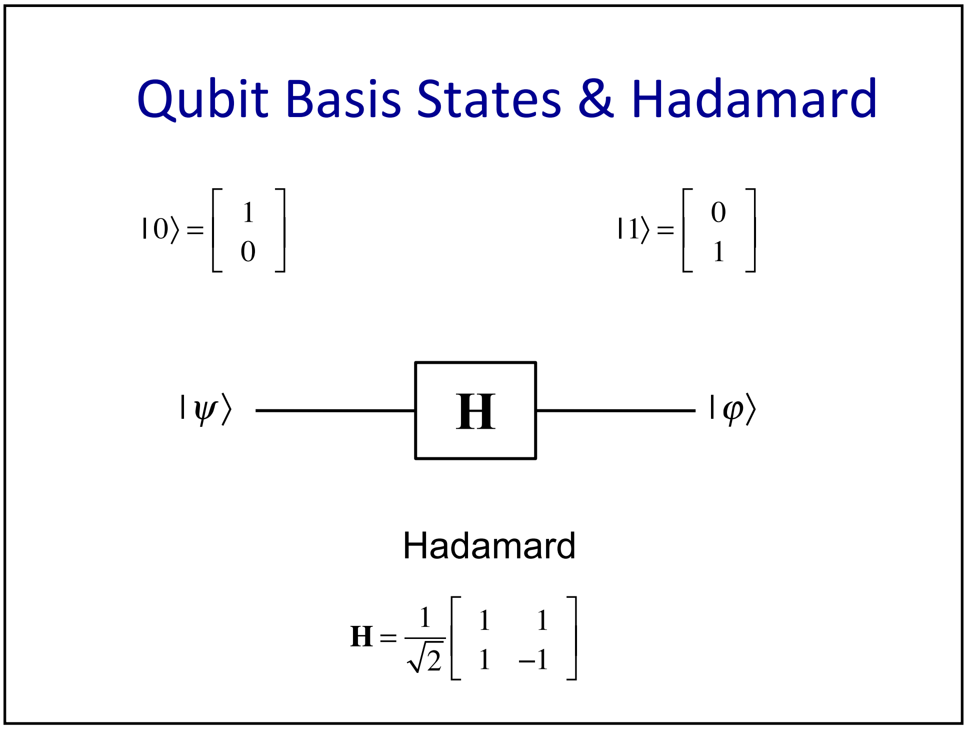
Double Slit Computation

- The CHARACTERISTIC/PROPERTY of the photon is serving as the Quantum Digit (or qubit)
  - in this case, the characteristic is its location (quantum observable)
- Causing the photon to have apparently traveled through BOTH paths is an example of “Quantum Superposition”
- Initializing qubits to be in a state of superposition is a common initial step in quantum informatics processing
- This is modeled mathematically as a “Hadamard” operation
- Denoted symbolically as:

$$|\psi\rangle \;\text{———}\; \boxed{\mathbf{H}} \;\text{———}\; |\varphi\rangle$$

$$|\varphi\rangle = \mathbf{H}|\psi\rangle$$

8



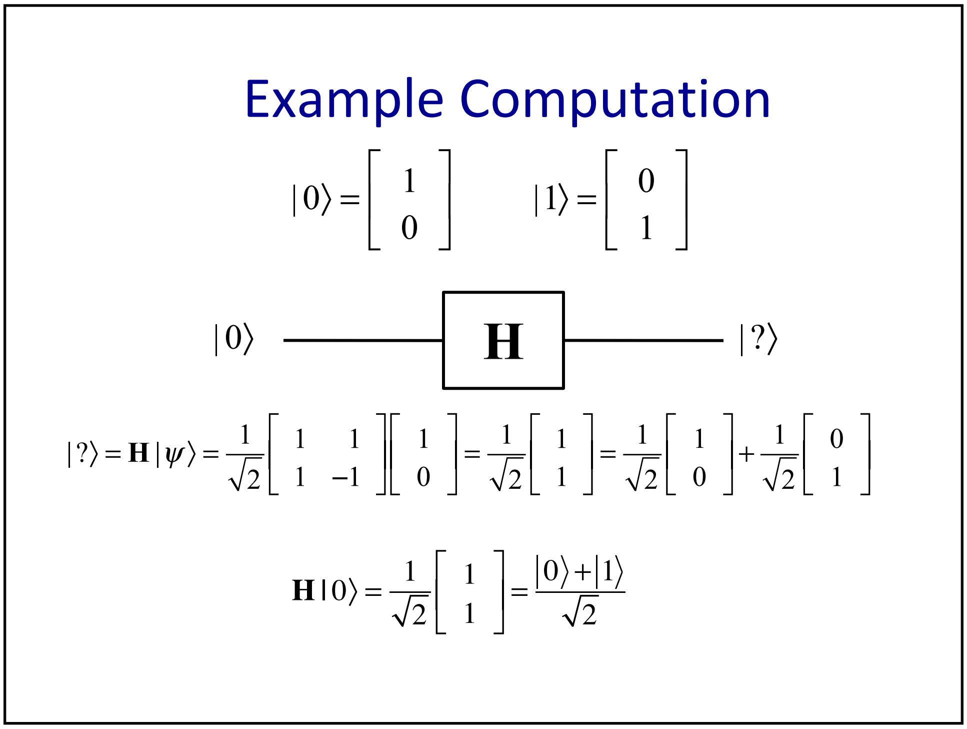
Qubit Basis States & Hadamard

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Hadamard

$$\mathbf{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

9



Example Computation

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

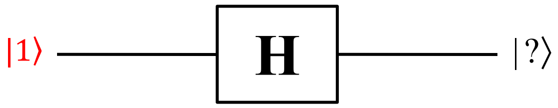
$$|?\rangle = \mathbf{H}\,|\psi\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$\mathbf{H}\,|0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

10

Example Computation (Init. to ket-1)

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$



$$|?\rangle = \mathbf{H}|1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 0 \end{bmatrix} + \frac{1}{\sqrt{2}}\begin{bmatrix} 0 \\ -1 \end{bmatrix}$$

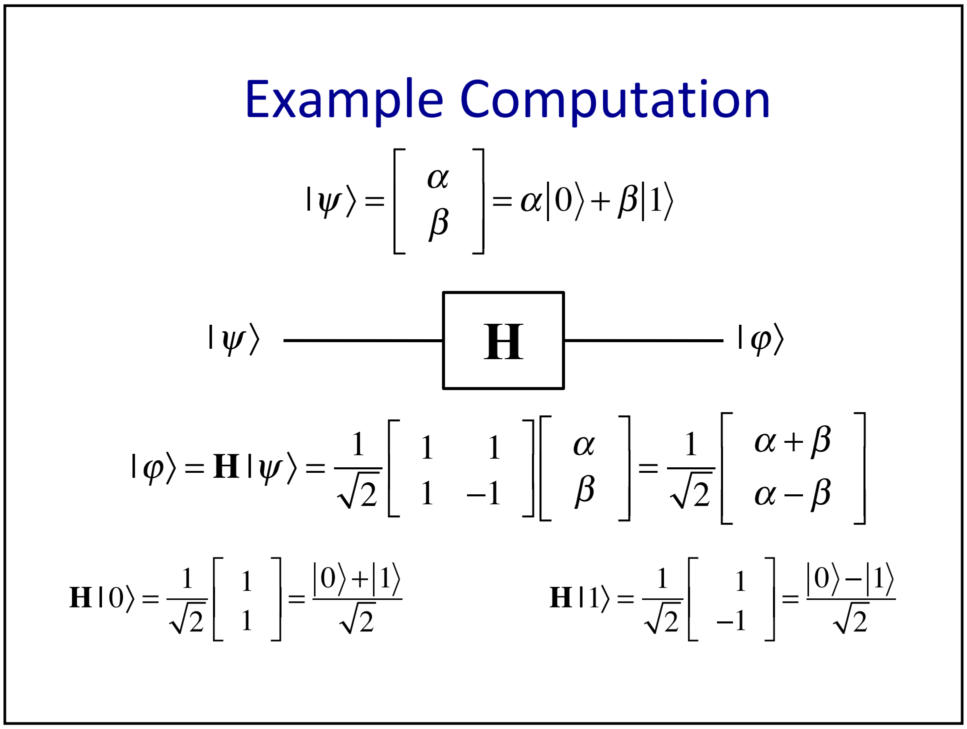
$$\mathbf{H}|1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Qubit Model

- Qubit exists in Linear Combination of Basis States
- “Ket" Notation Represents a Column Vector

$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \quad |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha\begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$



Example Computation

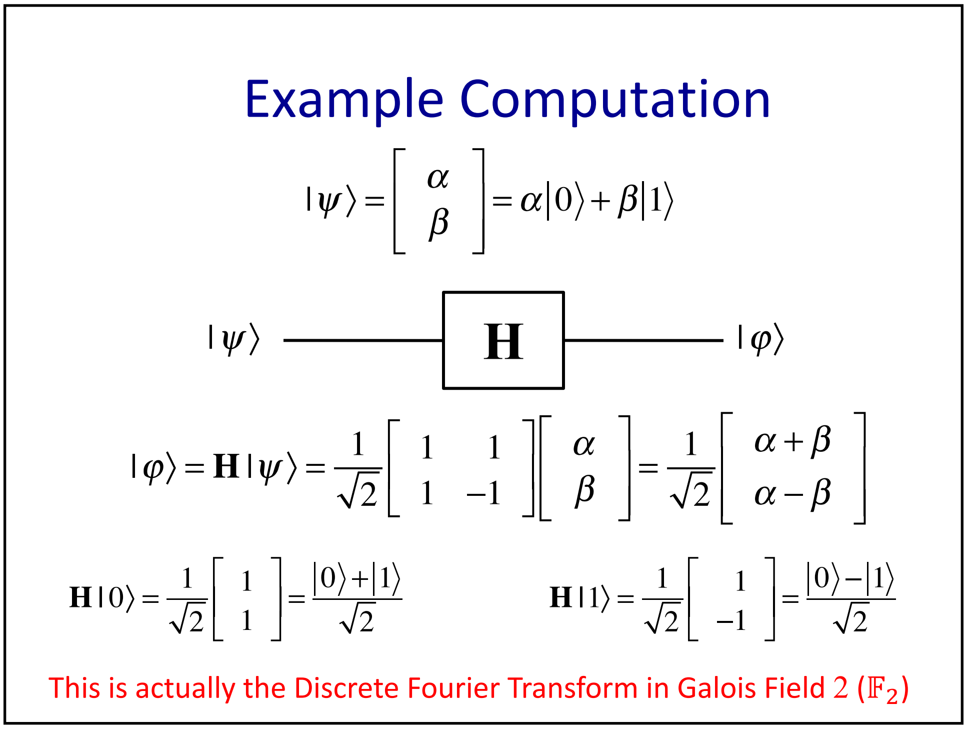
$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha|0\rangle + \beta|1\rangle$$

$$|\psi\rangle \;\text{———}\; \boxed{\mathbf{H}} \;\text{———}\; |\varphi\rangle$$

$$|\varphi\rangle = \mathbf{H}\,|\psi\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} \alpha+\beta \\ \alpha-\beta \end{bmatrix}$$

$$\mathbf{H}\,|0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \qquad \mathbf{H}\,|1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

13



Example Computation

$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha|0\rangle + \beta|1\rangle$$

$$|\psi\rangle \;\text{———}\; \boxed{\mathbf{H}} \;\text{———}\; |\varphi\rangle$$

$$|\varphi\rangle = \mathbf{H}\,|\psi\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} \alpha+\beta \\ \alpha-\beta \end{bmatrix}$$

$$\mathbf{H}\,|0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \qquad \mathbf{H}\,|1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

This is actually the Discrete Fourier Transform in Galois Field 2 ($\mathbb{F}_2$)

14

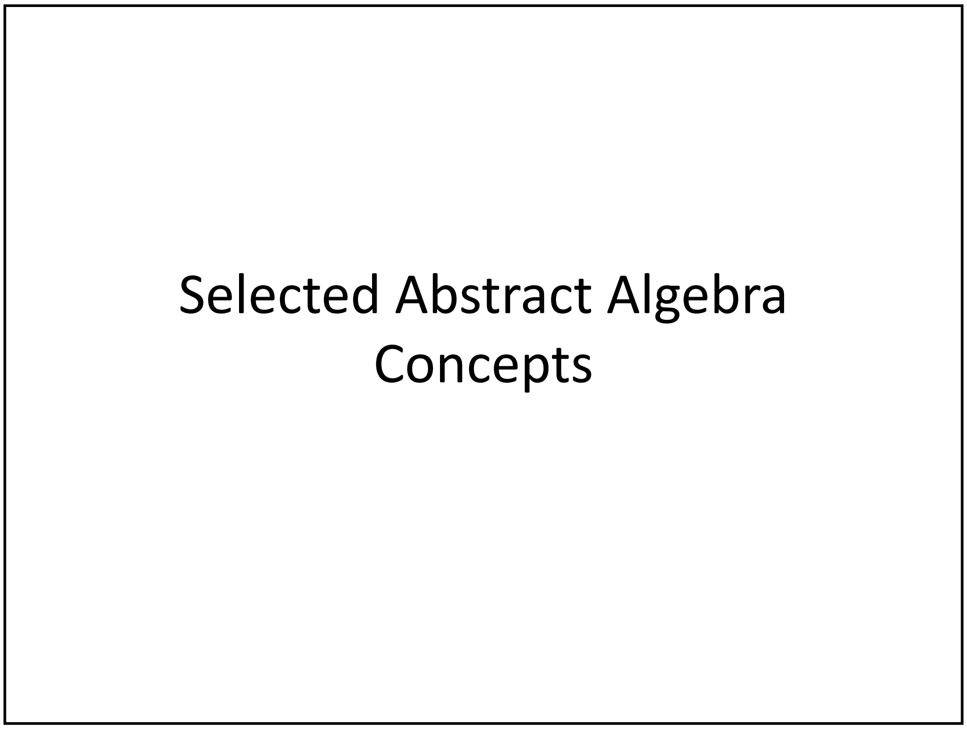
Physics/Math Class Content

- This is why we are reviewing classical and quantum behavior
- It is also why we are reviewing linear algebra
- QI is based on QM theory
- QI theory is described with linear algebra
- Please have patience, after one or two more classes, we will be prepared to focus solely on Quantum Informatics !!!!!

15

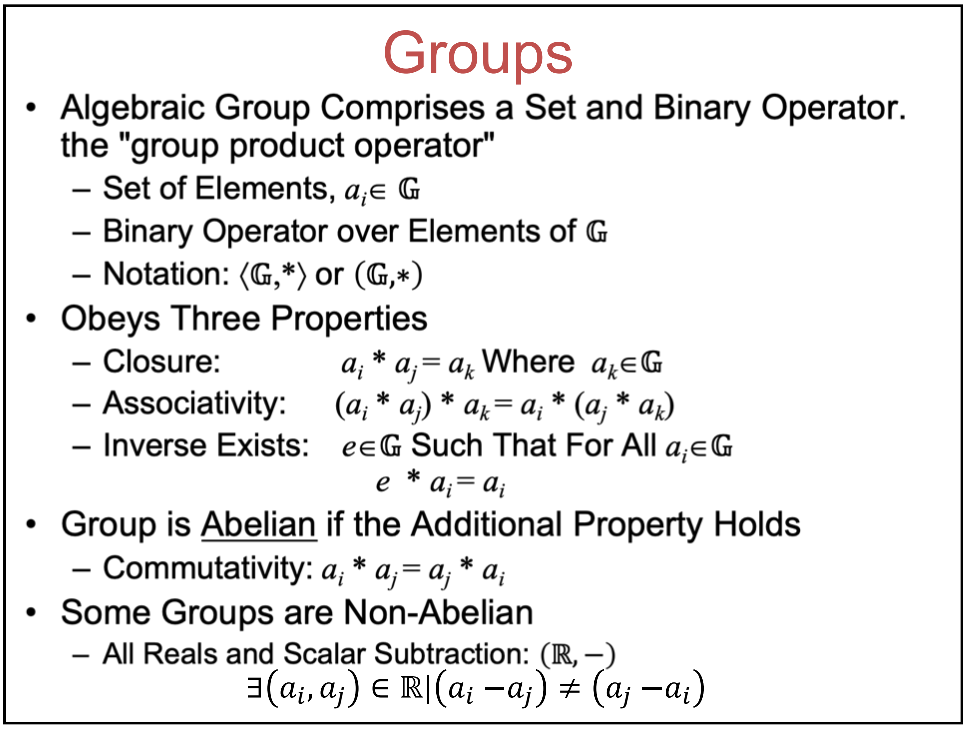
Anyone who is not shocked about quantum theory has not understood it
Niels Bohr

16



Selected Abstract Algebra Concepts

17



Groups

- Algebraic Group Comprises a Set and Binary Operator. the "group product operator"
  - Set of Elements, $a_i \in \mathbb{G}$
  - Binary Operator over Elements of $\mathbb{G}$
  - Notation: $\langle \mathbb{G}, * \rangle$ or $(\mathbb{G}, *)$
- Obeys Three Properties
  - Closure: $a_i * a_j = a_k$ Where $a_k \in \mathbb{G}$
  - Associativity: $(a_i * a_j) * a_k = a_i * (a_j * a_k)$
  - Inverse Exists: $e \in \mathbb{G}$ Such That For All $a_i \in \mathbb{G}$

    $e * a_i = a_i$
- Group is <u>Abelian</u> if the Additional Property Holds
  - Commutativity: $a_i * a_j = a_j * a_i$
- Some Groups are Non-Abelian
  - All Reals and Scalar Subtraction: $(\mathbb{R}, -)$

    $\exists (a_i, a_j) \in \mathbb{R} | (a_i - a_j) \neq (a_j - a_i)$

18

Group Axioms using Quantifiers

- A Group is an Algebraic Structure Composed of a Set of elements with an Associated Binary Operator usually called Multiplication or the Group Product Operator

group notation

$(\mathbb{G},*)$

binary product operator

$*: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}$

- A Group Must Satisfy the Three "Group Axioms" with closure:

G1: Associativity with respect to the group operator:

$$\forall (a, b, c) \in \mathbb{G}, a * (b * c) = (a * b) * c$$

G2: Identity Element Exists with respect to group operator:

$$\exists e_i \in \mathbb{G} \mid a_i * e_i = e_i * a_i = a_i, \forall a_i \in \mathbb{G}$$

G3: Inverse Elements Exist:

$$\forall a_i \in \mathbb{G},\ \exists a_i^{-1} \in \mathbb{G} \mid a_i * a_i^{-1} = a_i^{-1} * a_i = e_i$$

19

Abelian Group Axiom

- A Group that Also Obeys the Property of Commutativity is a Commutative or Abelian Group:

group notation

$(\mathbb{G},*)$

binary product operator

$*: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}$

G4: Commutativity (not required for group to exist):

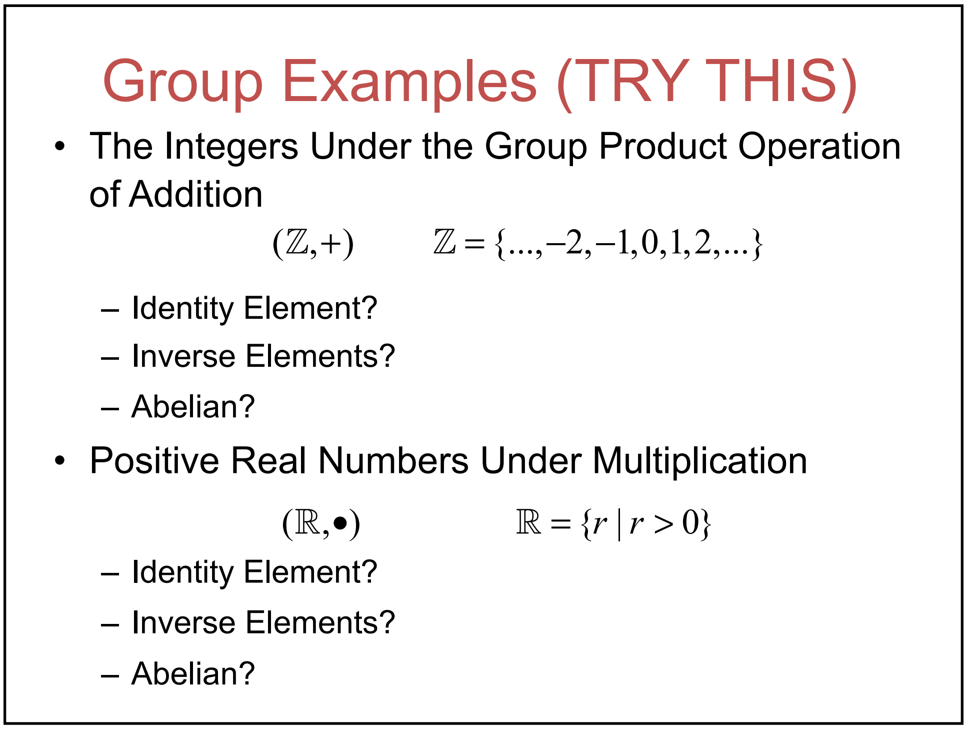
$$\forall (a_i, a_j) \in \mathbb{G}, a_i * a_j = a_j * a_i$$

- If Commutativity is not Obeyed, the Group is said to be non-Abelian or non-Commutative

Niels Henrik Abel

Proved that there is no general solution of a fifth-degree polynomial using radicals. Performed most of his research in poverty and died of tuberculosis at age 26.

20



Group Examples (TRY THIS)

- The Integers Under the Group Product Operation of Addition

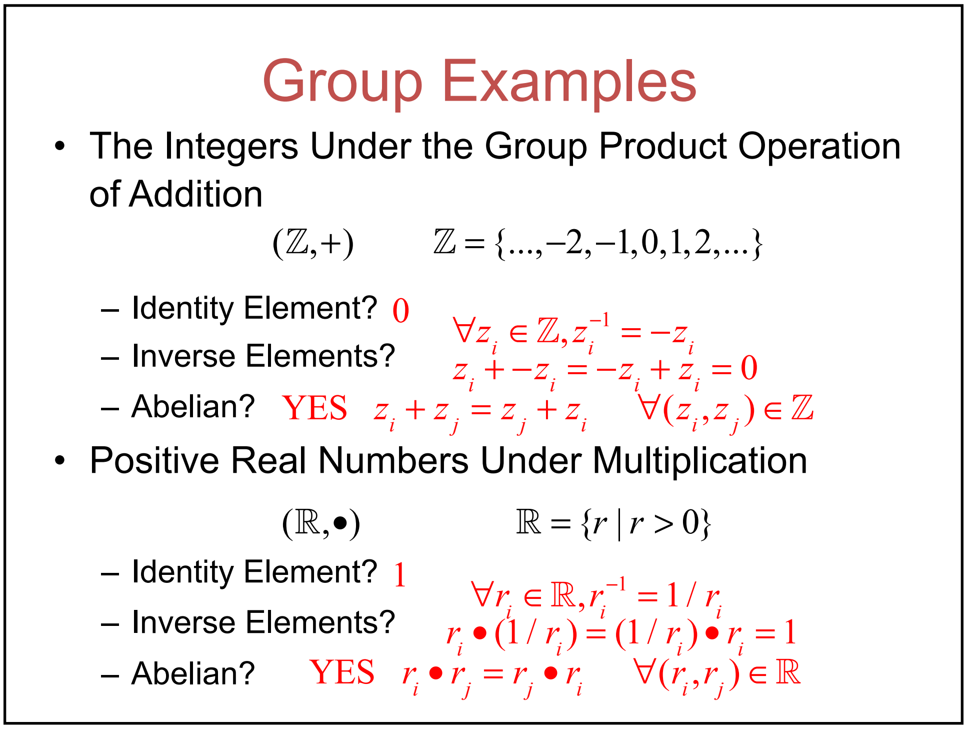
$$(\mathbb{Z},+) \qquad \mathbb{Z} = \{\ldots,-2,-1,0,1,2,\ldots\}$$

  - Identity Element?
  - Inverse Elements?
  - Abelian?
- Positive Real Numbers Under Multiplication

$$(\mathbb{R},\bullet) \qquad \mathbb{R} = \{r \mid r > 0\}$$

  - Identity Element?
  - Inverse Elements?
  - Abelian?

21



Group Examples

- The Integers Under the Group Product Operation of Addition

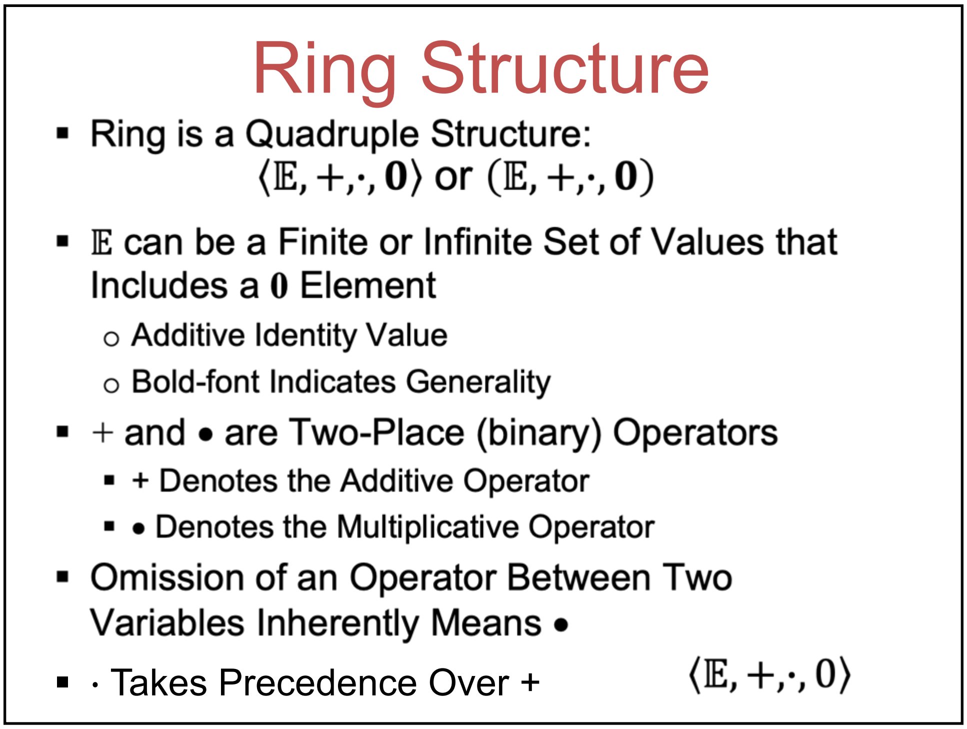
$$(\mathbb{Z},+) \qquad \mathbb{Z} = \{\ldots,-2,-1,0,1,2,\ldots\}$$

  - Identity Element? 0
  - Inverse Elements? $\forall z_i \in \mathbb{Z}, z_i^{-1} = -z_i$ $\quad z_i + -z_i = -z_i + z_i = 0$
  - Abelian? YES $z_i + z_j = z_j + z_i \quad \forall (z_i, z_j) \in \mathbb{Z}$
- Positive Real Numbers Under Multiplication

$$(\mathbb{R},\bullet) \qquad \mathbb{R} = \{r \mid r > 0\}$$

  - Identity Element? 1
  - Inverse Elements? $\forall r_i \in \mathbb{R}, r_i^{-1} = 1/r_i$ $\quad r_i \bullet (1/r_i) = (1/r_i) \bullet r_i = 1$
  - Abelian? YES $r_i \bullet r_j = r_j \bullet r_i \quad \forall (r_i, r_j) \in \mathbb{R}$

22

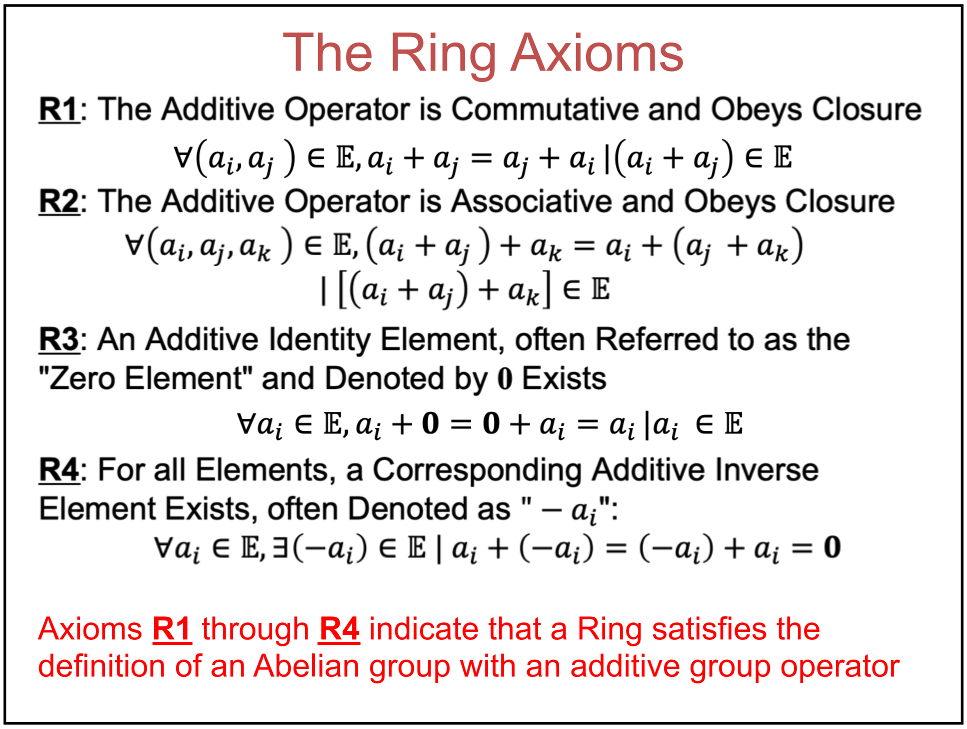


Ring Structure

- Ring is a Quadruple Structure:
  $\langle \mathbb{E}, +, \cdot, \mathbf{0} \rangle$ or $(\mathbb{E}, +, \cdot, \mathbf{0})$
- $\mathbb{E}$ can be a Finite or Infinite Set of Values that Includes a $\mathbf{0}$ Element
  - o Additive Identity Value
  - o Bold-font Indicates Generality
- $+$ and • are Two-Place (binary) Operators
  - + Denotes the Additive Operator
  - • Denotes the Multiplicative Operator
- Omission of an Operator Between Two Variables Inherently Means •
- · Takes Precedence Over +

$\langle \mathbb{E}, +, \cdot, 0 \rangle$

23



The Ring Axioms

R1: The Additive Operator is Commutative and Obeys Closure

$$\forall(a_i, a_j) \in \mathbb{E}, a_i + a_j = a_j + a_i \,|\, (a_i + a_j) \in \mathbb{E}$$

R2: The Additive Operator is Associative and Obeys Closure

$$\forall(a_i, a_j, a_k) \in \mathbb{E}, (a_i + a_j) + a_k = a_i + (a_j + a_k)$$
$$|\, \left[(a_i + a_j) + a_k\right] \in \mathbb{E}$$

R3: An Additive Identity Element, often Referred to as the "Zero Element" and Denoted by $\mathbf{0}$ Exists

$$\forall a_i \in \mathbb{E}, a_i + \mathbf{0} = \mathbf{0} + a_i = a_i \,|\, a_i \in \mathbb{E}$$

R4: For all Elements, a Corresponding Additive Inverse Element Exists, often Denoted as "$-a_i$":

$$\forall a_i \in \mathbb{E}, \exists(-a_i) \in \mathbb{E} \,|\, a_i + (-a_i) = (-a_i) + a_i = \mathbf{0}$$

Axioms **R1** through **R4** indicate that a Ring satisfies the definition of an Abelian group with an additive group operator

24

The Ring Axioms (cont.)

R5: The Multiplicative Operator is Associative and Obeys Closure

$$\forall(a_i, a_j, a_k) \in \mathbb{E}, (a_i \cdot a_j) \cdot a_k = a_i \cdot (a_j \cdot a_k) \mid [(a_i \cdot a_j) \cdot a_k] \in \mathbb{E}$$

R6: Distributivity over the Additive Operator with Closure

$$\forall(a_i, a_j, a_k) \in \mathbb{E}, a_i + (a_j \cdot a_k) = (a_i + a_j) \cdot (a_i + a_k) \mid [a_i + (a_j \cdot a_k)] \in \mathbb{E}$$

R7: Distributivity over the Multiplicative Operator with Closure

$$\forall(a_i, a_j, a_k) \in \mathbb{E}, a_i \cdot (a_j + a_k) = (a_i \cdot a_j) + (a_i \cdot a_k) \mid [a_i \cdot (a_j + a_k)] \in \mathbb{E}$$

A Ring is further referred to as a **Commutative Ring** when:

$$\forall(a_i, a_j) \in \mathbb{E}, a_i \cdot a_j = a_j \cdot a_i \mid (a_i \cdot a_j) \in \mathbb{E}$$

A Ring is further referred to as **Unital** or a **Ring with Identity** when it comprises a Multiplicative Identity Element, $\mathbf{1}$:

$$\forall a_i \in \mathbb{E}, a_i \cdot \mathbf{1} = \mathbf{1} \cdot a_i = a_i \mid a_i \in \mathbb{E}$$

25

Field Structure

- A Field $\mathbb{F}$ is an algebraic structure with two associated binary operators usually referred to as addition and multiplication
- A Field also Obeys the following Three Axioms:
  1. Under Addition, $\mathbb{F}$ is an **Abelian Group** with Multiplicative Identity Element $\mathbf{0}$ Such That:

     $$\mathbf{0} + a_i = a_i \forall a_i \in \mathbb{F}$$

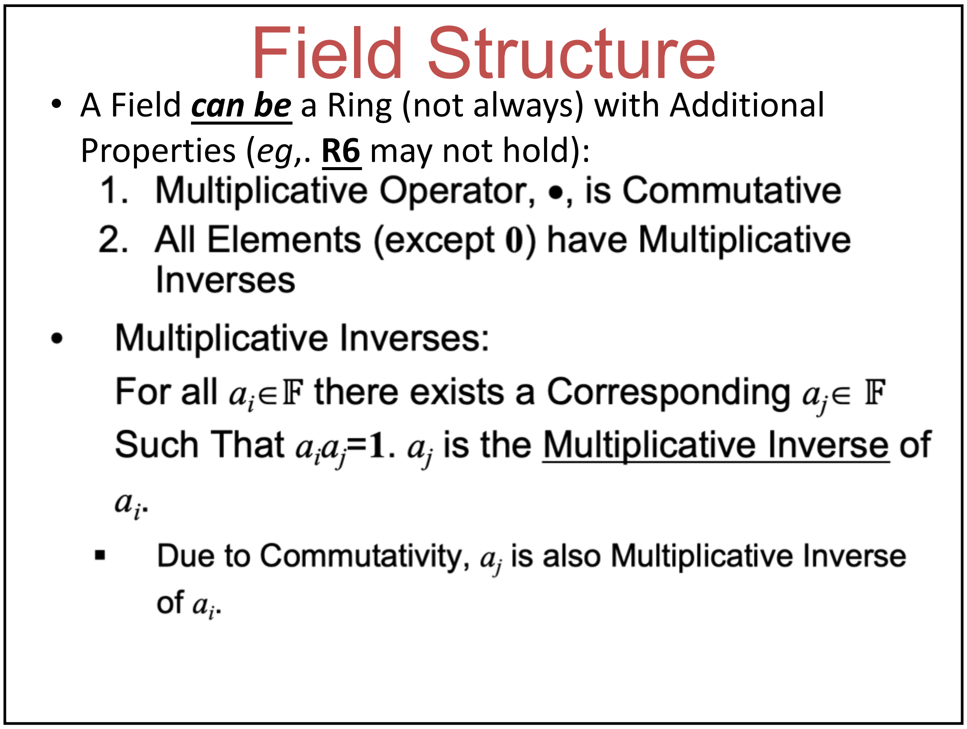
  2. Under Multiplication, the non-zero elements of $\mathbb{F}$ form an Abelian Group with Identity Element 1 Such That:

     $$\forall a_i \in \mathbb{F}, \mathbf{1} \cdot a_i = a_i \qquad \forall a_i \in \mathbb{F}, \mathbf{0} \cdot a_i = \mathbf{0}$$

  3. Distributivity Over the Multiplicative Operator Holds:

     $$\forall(a_i, a_j, a_k) \in \mathbb{F}, a_i \cdot (a_j + a_k) = (a_i \cdot a_j) + (a_i \cdot a_k)$$

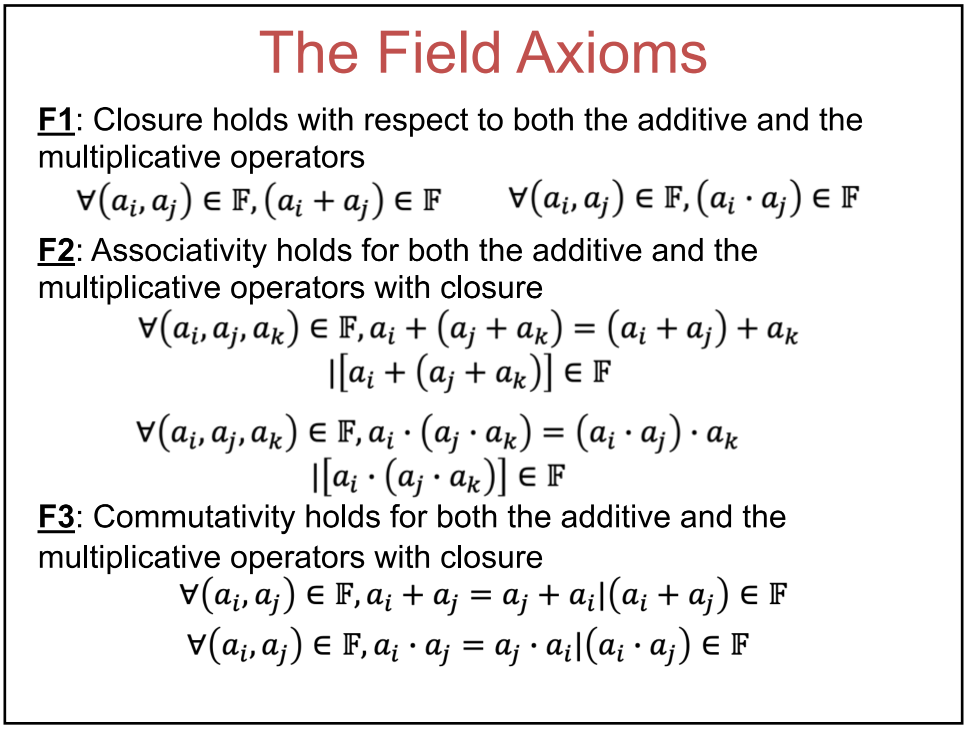
26



Field Structure

- A Field ***can be*** a Ring (not always) with Additional Properties (*eg*,. **R6** may not hold):
  1. Multiplicative Operator, •, is Commutative
  2. All Elements (except $\mathbf{0}$) have Multiplicative Inverses
- Multiplicative Inverses:
  For all $a_i \in \mathbb{F}$ there exists a Corresponding $a_j \in \mathbb{F}$ Such That $a_i a_j = \mathbf{1}$. a_j is the Multiplicative Inverse of a_i.
  - Due to Commutativity, a_j is also Multiplicative Inverse of a_i.

27



The Field Axioms

F1: Closure holds with respect to both the additive and the multiplicative operators

$$\forall(a_i, a_j) \in \mathbb{F}, (a_i + a_j) \in \mathbb{F} \qquad \forall(a_i, a_j) \in \mathbb{F}, (a_i \cdot a_j) \in \mathbb{F}$$

F2: Associativity holds for both the additive and the multiplicative operators with closure

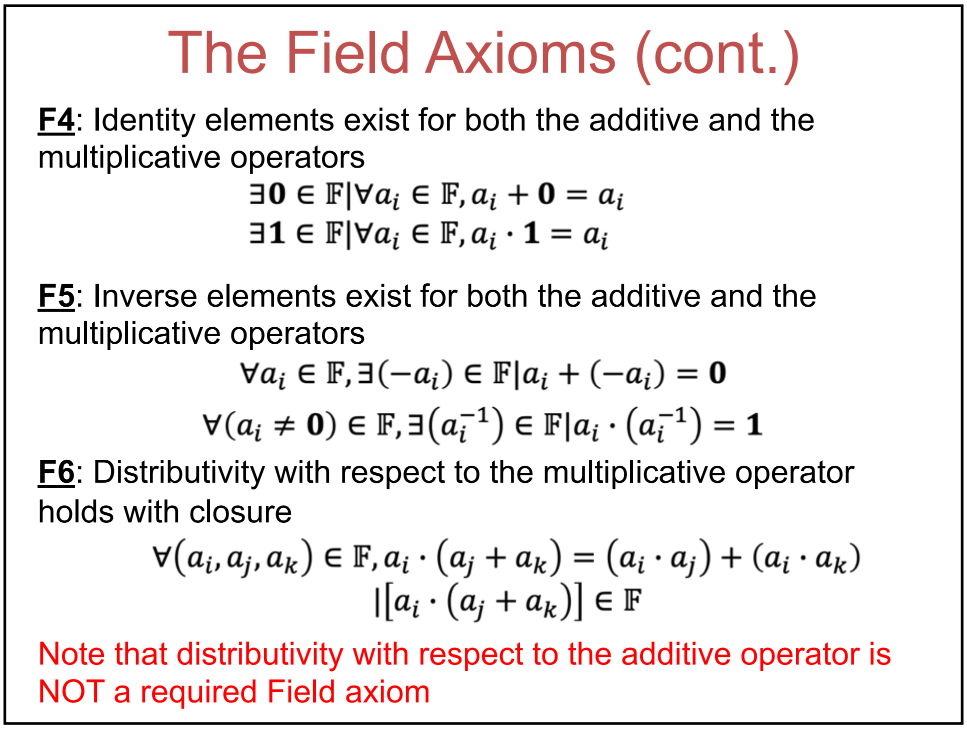
$$\forall(a_i, a_j, a_k) \in \mathbb{F}, a_i + (a_j + a_k) = (a_i + a_j) + a_k$$
$$|[a_i + (a_j + a_k)] \in \mathbb{F}$$

$$\forall(a_i, a_j, a_k) \in \mathbb{F}, a_i \cdot (a_j \cdot a_k) = (a_i \cdot a_j) \cdot a_k$$
$$|[a_i \cdot (a_j \cdot a_k)] \in \mathbb{F}$$

F3: Commutativity holds for both the additive and the multiplicative operators with closure

$$\forall(a_i, a_j) \in \mathbb{F}, a_i + a_j = a_j + a_i | (a_i + a_j) \in \mathbb{F}$$
$$\forall(a_i, a_j) \in \mathbb{F}, a_i \cdot a_j = a_j \cdot a_i | (a_i \cdot a_j) \in \mathbb{F}$$

28



The Field Axioms (cont.)

F4: Identity elements exist for both the additive and the multiplicative operators

$$\exists \mathbf{0} \in \mathbb{F} | \forall a_i \in \mathbb{F}, a_i + \mathbf{0} = a_i$$
$$\exists \mathbf{1} \in \mathbb{F} | \forall a_i \in \mathbb{F}, a_i \cdot \mathbf{1} = a_i$$

F5: Inverse elements exist for both the additive and the multiplicative operators

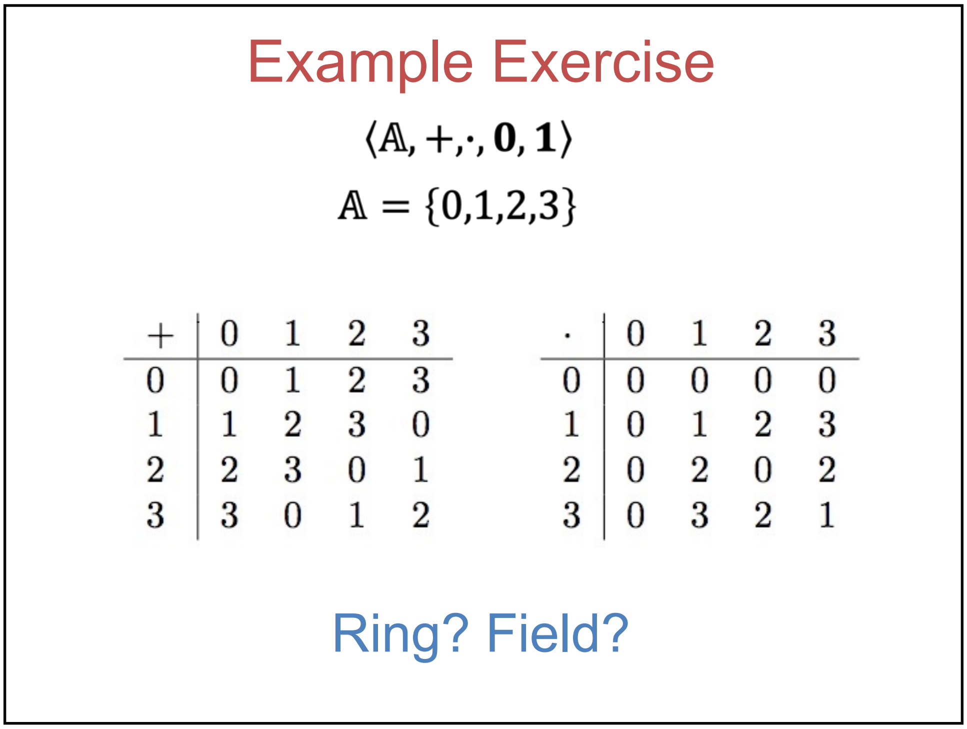
$$\forall a_i \in \mathbb{F}, \exists(-a_i) \in \mathbb{F} | a_i + (-a_i) = \mathbf{0}$$
$$\forall(a_i \neq \mathbf{0}) \in \mathbb{F}, \exists\left(a_i^{-1}\right) \in \mathbb{F} | a_i \cdot \left(a_i^{-1}\right) = \mathbf{1}$$

F6: Distributivity with respect to the multiplicative operator holds with closure

$$\forall\left(a_i, a_j, a_k\right) \in \mathbb{F}, a_i \cdot \left(a_j + a_k\right) = \left(a_i \cdot a_j\right) + \left(a_i \cdot a_k\right)$$
$$|\left[a_i \cdot \left(a_j + a_k\right)\right] \in \mathbb{F}$$

Note that distributivity with respect to the additive operator is NOT a required Field axiom

29



Example Exercise

$$\langle \mathbb{A}, +, \cdot, \mathbf{0}, \mathbf{1} \rangle$$

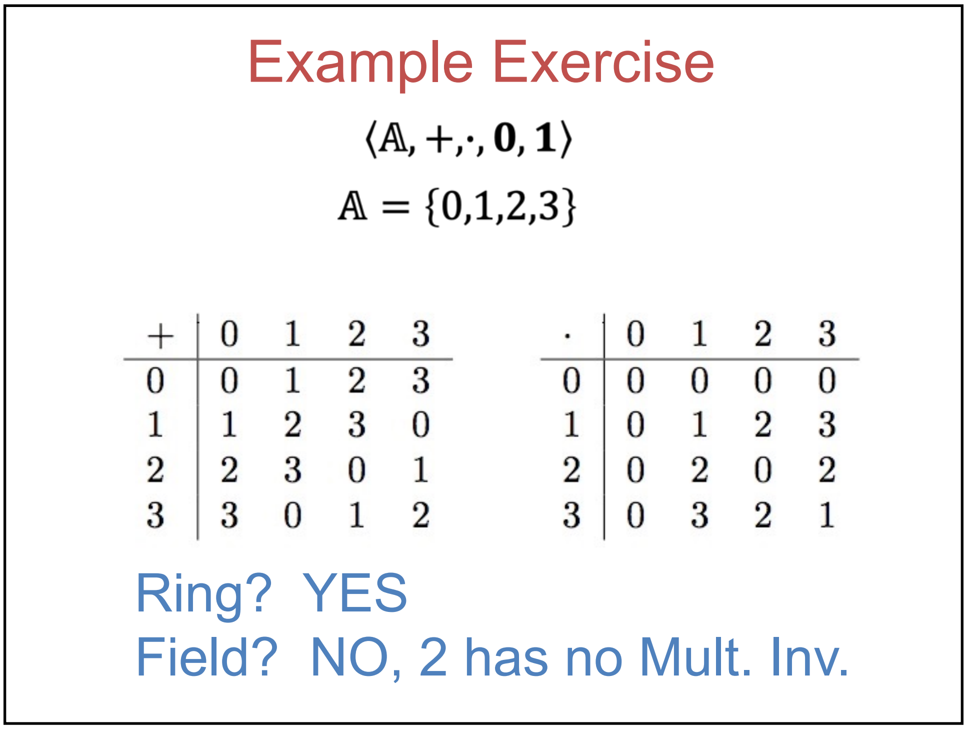
$$\mathbb{A} = \{0,1,2,3\}$$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Ring? Field?

30



Example Exercise

$\langle \mathbb{A}, +, \cdot, \mathbf{0}, \mathbf{1} \rangle$

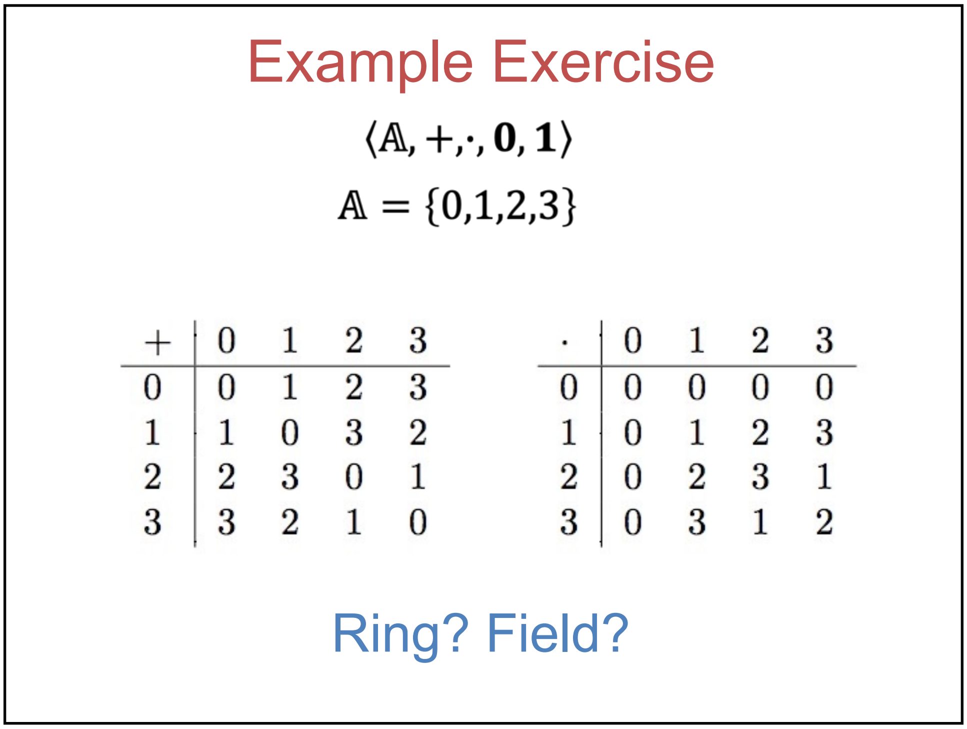
$\mathbb{A} = \{0,1,2,3\}$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Ring? YES

Field? NO, 2 has no Mult. Inv.



Example Exercise

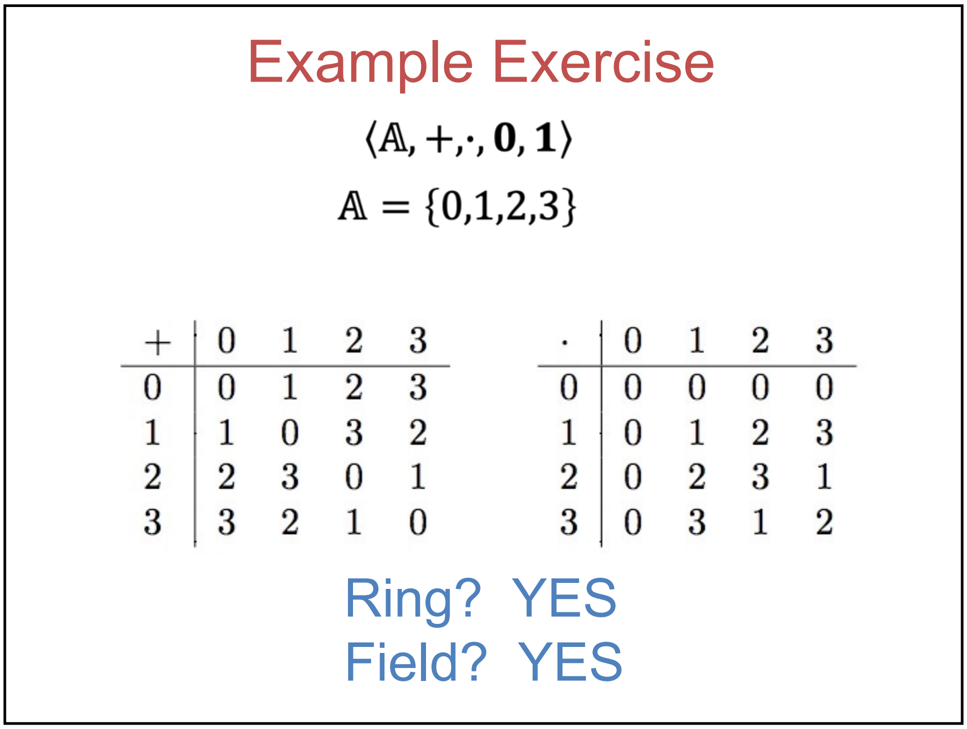
$\langle \mathbb{A}, +, \cdot, \mathbf{0}, \mathbf{1} \rangle$

$\mathbb{A} = \{0,1,2,3\}$

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Ring? Field?



Example Exercise

$$\langle \mathbb{A}, +, \cdot, \mathbf{0}, \mathbf{1} \rangle$$

$$\mathbb{A} = \{0,1,2,3\}$$

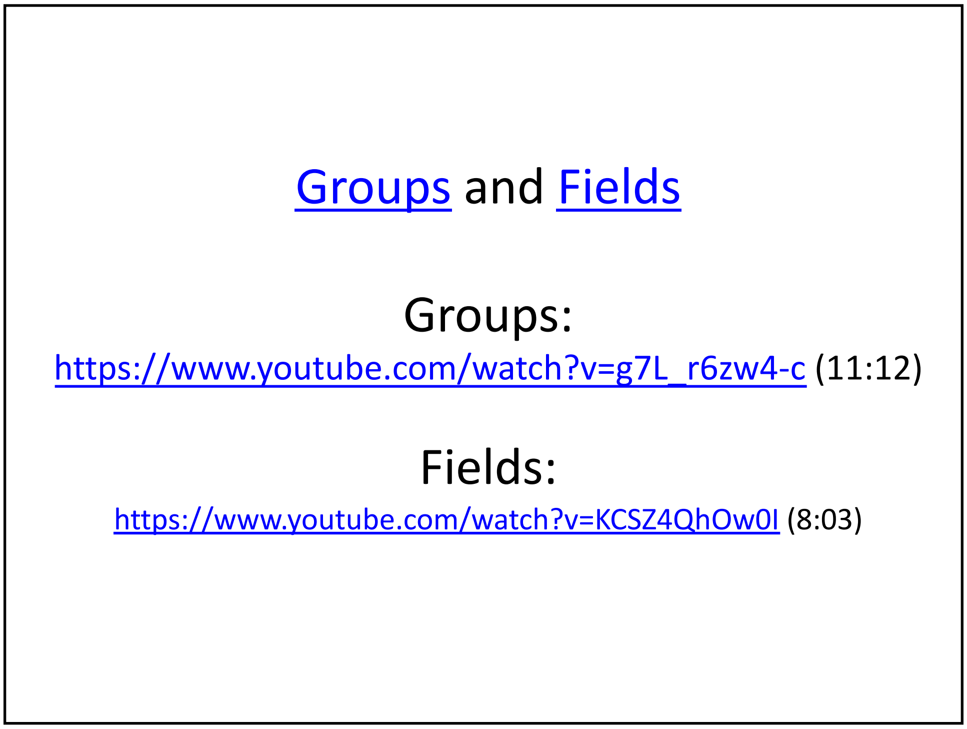
+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Ring? YES

Field? YES

33



Groups and Fields

Groups:

https://www.youtube.com/watch?v=g7L_r6zw4-c (11:12)

Fields:

https://www.youtube.com/watch?v=KCSZ4QhOw0I (8:03)

34

Algebra

- Not as Strictly Defined as Groups, Rings, Fields
- General Definition is a Structure Comprised of:
  - At least one set of Elements, $\mathbb{A}$, (can be more than one)
  - One or Axioms over the one or more sets of elements
- Another definition is a field of study of "algebraic structures"
- EXAMPLES
  - The Field of Reals
  - The Set $\mathbb{B}$ with the Huntington Postulates (Switching Algebra)
  - The Set $\{0,1,2\}$ with $min\{x,y\}$, $max\{x,y\}$, $J_0(x)$,$J_1(x)$,$J_2(x)$(3-valued Post Algebra) where

$$J_0(x) = \begin{cases} 2, x = 0 \\ 0, \text{otherwise} \end{cases} \quad J_1(x) = \begin{cases} 2, x = 1 \\ 0, \text{otherwise} \end{cases} \quad J_2(x) = \begin{cases} 2, x = 2 \\ 0, \text{otherwise} \end{cases}$$

Lattice Algebra

Lattice Algebra – defined by the tuple:

$$\langle A, \vee, \wedge \rangle$$

Where:

A is a non-empty set

$\vee, \wedge$ are binary operations disjunction and conjunction

And, the Following Axioms Hold:

$$\begin{array}{lll} a \vee a = a & a \wedge a = a & \text{(Idempotence)} \\ a \vee b = b \vee a & a \wedge b = b \wedge a & \text{(Commutativity)} \\ a \vee (b \vee c) = (a \vee b) \vee c & a \wedge (b \wedge c) = (a \wedge b) \wedge c & \text{(Associativity)} \\ a \vee (a \wedge b) = a & a \wedge (a \vee b) = a & \text{(Absorption)} \\ & a,b,c \in A & \end{array}$$

Distributive Lattice Algebra

Distributive Lattice Algebra

And, the Following Distributive Laws Hold:

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$
$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

Complemented Distributive Lattice Algebra

1) maximal element = 1
2) minimal element = 0
3) For any $a \in A$ if $\exists\, x_a \in A$ such that $a \wedge x_a = 0$
4) For any $a \in A$ if $\exists\, x_a \in A$ such that $a \vee x_a = 1$

A Complemented Distributive Algebra is a Boolean Algebra

37

Lattice Algebra

Lattice Algebra – defined by the tuple:

$\langle A, \vee, \bullet \rangle$

Where:

A is a non-empty set
$\vee, \bullet$ are binary operations

And, the Following Axioms Hold:

$a \vee a = a$	$a \bullet a = a$	(Idempotence)
$a \vee b = b \vee a$	$a \bullet b = b \bullet a$	(Commutativity)
$a \vee (b \vee c) = (a \vee b) \vee c$	$a \bullet (b \bullet c) = (a \bullet b) \bullet c$	(Associativity)
$a \vee (a \bullet b) = a$	$a \bullet (a \vee b) = a$	(Absorption)

$a,b,c \in A$

38

Distributive Lattice Algebra

Distributive Lattice Algebra

And, the Following Distributive Laws Hold:

$$a \vee (b \bullet c) = (a \vee b) \bullet (a \vee c)$$
$$a \bullet (b \vee c) = (a \bullet b) \vee (a \bullet c)$$

Complemented Distributive Lattice Algebra

1) maximal element = 1
2) minimal element = 0
3) For any $a \in A$ if $\exists\ x_a \in A$ such that $a \bullet x_a = 0$
4) For any $a \in A$ if $\exists\ x_a \in A$ such that $a \vee x_a = 1$

A Complemented Distributive Algebra is a Boolean Algebra

39

Boolean Algebra

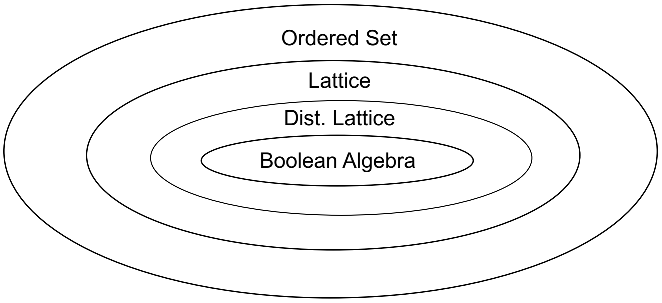
$$\langle B, \vee, \bullet, {}^{-}, 0, 1\rangle$$

$$0, 1 \in B$$

is $^{-}$ a unary operation over B

$\vee$, $\bullet$ are binary operations over B

0 is the “identity element” wrt $\vee$
1 is the “identity element” wrt $\bullet$



40

Selected Linear Algebra Concepts

41

Vector Space

- Consists of
  1) An Abelian (commutative) group $(\mathbb{V}, +)$ whose elements are called vectors and whose product operator is vector addition, characterized by a "dimension," n
  2) A field $\mathbb{F}$ (usually the real field $\mathbb{R}$ or the complex field $\mathbb{C}$) whose elements are called "scalars"
  3) An multiplicative operation called "scaling" denoted by an absence of an operation symbol between a scalar and a vector that associates a scalar $\alpha \in \mathbb{F}$ and vector $\mathbf{x} \in \mathbb{V}$ and results in another vector $\alpha\mathbf{x} \in \mathbb{V}$ or $\alpha\mathbf{x} \in \mathbb{V}$, $\{\alpha, \mathbf{x}\} \rightarrow \alpha\mathbf{x}$

$$\alpha(\mathbf{x}+\mathbf{y}) = \alpha\mathbf{x} + \alpha\mathbf{y}$$

$$(\alpha+\beta)\mathbf{x} = \alpha\mathbf{x} + \beta\mathbf{x}$$

$$(\alpha\beta)\mathbf{x} = \alpha(\beta\mathbf{x})$$

$$(1)\mathbf{x} = \mathbf{x}$$

42

Complex/Hilbert Vector Spaces

- Hilbert Space is generally an infinite-dimensional vector space
  - with an inner product
  - and with associated norm
- Quantum Computing Literature Traditionally Refers to Finite n-dimensional Complex Euclidean Vector Space as a Hilbert Space (technically correct)
- FOR OUR PURPOSES: Hilbert Space:
  n-dimensional vector space over the field of complex numbers with an inner product and associated norm

Vector Space Inner Products

- Consider an n-dimensional Vector Space:
- If, for all pairs of vectors $\mathbf{x}$ and $\mathbf{y}$, an associated real number exists, an inner product $(\mathbf{x},\ \mathbf{y})$, such that the following conditions are satisfied:

$$(\mathbf{x},\mathbf{y}) = (\mathbf{y},\mathbf{x})$$

$$(c\mathbf{x},\mathbf{y}) = c(\mathbf{x},\mathbf{y}) \text{ if } c \in \mathbb{R} \text{ (or } \mathbb{C}\text{)}$$

$$(\mathbf{x}+\mathbf{z},\mathbf{y}) = (\mathbf{x},\mathbf{y}) + (\mathbf{z},\mathbf{y}) \quad \forall \mathbf{z} \in \mathbb{R}^n \text{ (or } \mathbb{C}^n\text{)}$$

$$(\mathbf{x},\mathbf{x}) \geq 0 \text{ such that } \quad (\mathbf{x},\mathbf{x}) = 0 \text{ if and only if } \mathbf{x} = \mathbf{0}$$

- Then, we have an n-dimensional ***Euclidean*** Vector Space
- $(\mathbf{x},\ \mathbf{y})$ is the ***Inner Product*** of Vectors $\mathbf{x}$ and $\mathbf{y}$
  - "dot" product, $(\mathbf{x},\ \mathbf{y})=\mathbf{x}\bullet\mathbf{y}$, is one form of an inner product that yields a scalar product value
  - most common is the "Euclidean" inner product

Euclidean Vector Spaces

- Euclidean Spaces use “dot product” & “L_2 norm”
- “Length” of a Euclidean Vector & inner/dot product:

$$\|\mathbf{x}\| = \sqrt{(\mathbf{x},\mathbf{x})} \qquad (\mathbf{x},\mathbf{y}) = \mathbf{x}\bullet\mathbf{y}$$

- Euclidean Angle between the two vectors α and β:

$$\boldsymbol{\theta} = \cos^{-1}\frac{(\mathbf{x},\mathbf{y})}{\|\mathbf{x}\|\ \|\mathbf{y}\|} \qquad \cos(\boldsymbol{\theta}) = \frac{(\mathbf{x},\mathbf{y})}{\|\mathbf{x}\|\ \|\mathbf{y}\|}$$

- If $(\mathbf{x}, \mathbf{y})=0$, then $\mathbf{x}$ and $\mathbf{y}$ are *orthogonal*
  - Orthogonality occurs when the inner product is zero
- From a Euclidean viewpoint, 90 degrees apart

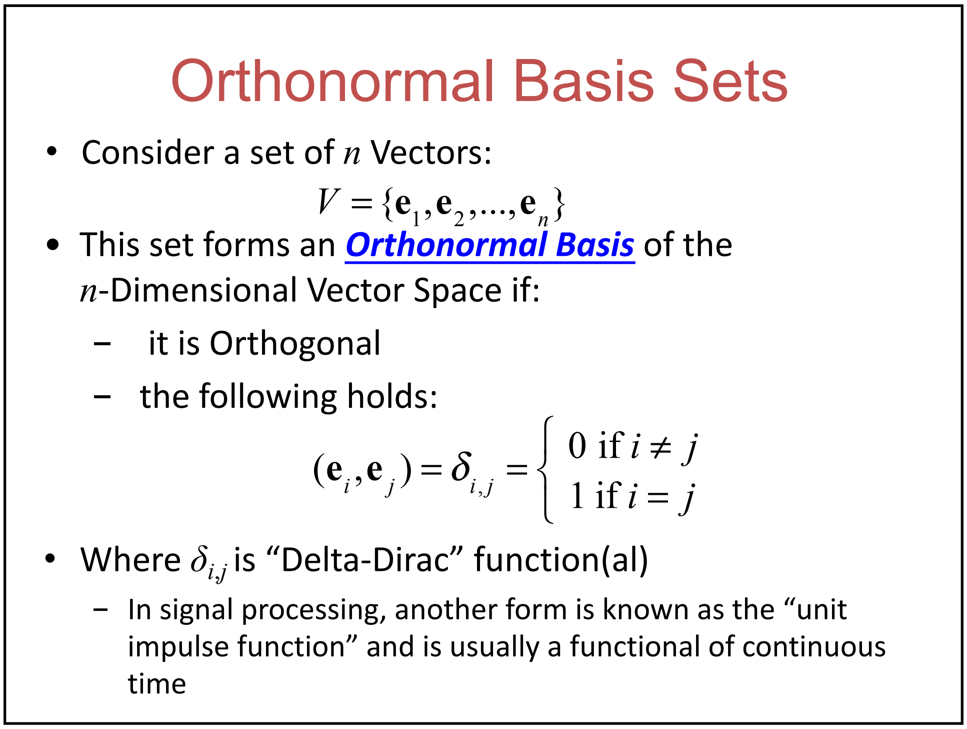
$$\theta = \pi / 2 = 90^\circ$$

45

Orthogonal Basis Sets

- Consider a set of *n* Vectors: $V = \{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n\}$
- This set forms an ***Orthogonal Basis*** of the n-Dimensional Vector Space if: $(\mathbf{e}_i, \mathbf{e}_j) = 0, \forall i \neq j$
- Vector space elements (all vectors in the space) can ALWAYS be represented as a linear combination of scaled basis vectors, the ***Basis Set*** or Basis of the Space
  - Different/Alternative Basis sets (Bases) may be used to represent the SAME Vector Space
- Finding an alternative Basis Set is known as a ***Change of Basis*** and can be accomplished via a ***Basis Transform***
  - very important in QM, provides a different “point of view” of the Vector Space

46



Orthonormal Basis Sets

- Consider a set of n Vectors:

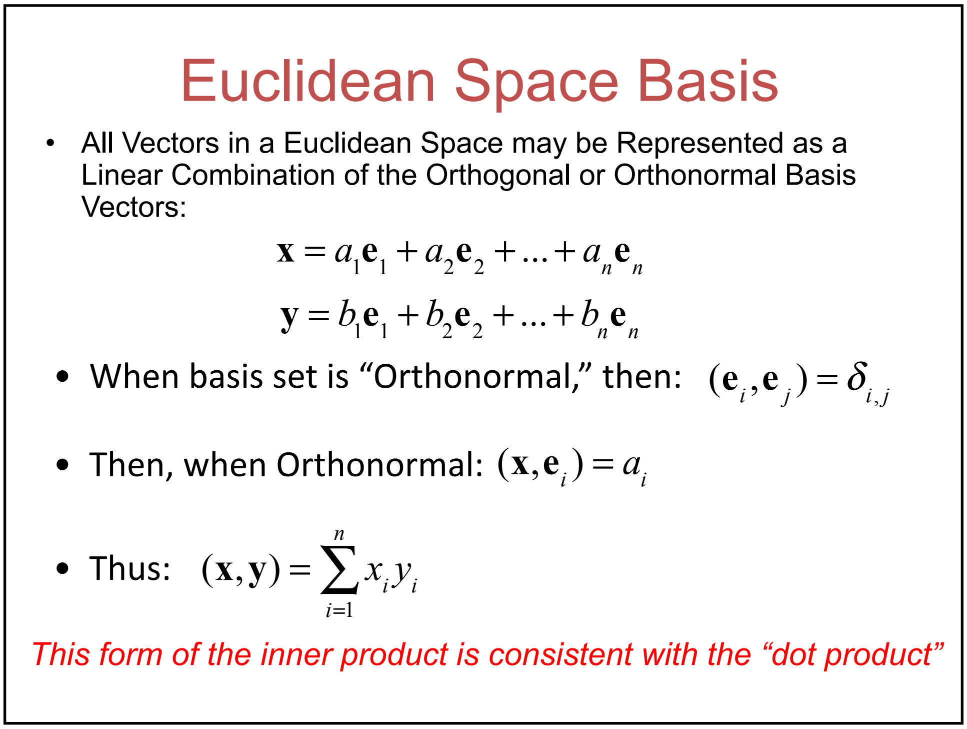
$$V = \{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n\}$$

- This set forms an ***Orthonormal Basis*** of the n-Dimensional Vector Space if:
  - it is Orthogonal
  - the following holds:

$$(\mathbf{e}_i, \mathbf{e}_j) = \delta_{i,j} = \begin{cases} 0 \text{ if } i \neq j \\ 1 \text{ if } i = j \end{cases}$$

- Where $\delta_{i,j}$ is "Delta-Dirac" function(al)
  - In signal processing, another form is known as the "unit impulse function" and is usually a functional of continuous time

47



Euclidean Space Basis

- All Vectors in a Euclidean Space may be Represented as a Linear Combination of the Orthogonal or Orthonormal Basis Vectors:

$$\mathbf{x} = a_1\mathbf{e}_1 + a_2\mathbf{e}_2 + \ldots + a_n\mathbf{e}_n$$

$$\mathbf{y} = b_1\mathbf{e}_1 + b_2\mathbf{e}_2 + \ldots + b_n\mathbf{e}_n$$

- When basis set is "Orthonormal," then: $(\mathbf{e}_i, \mathbf{e}_j) = \delta_{i,j}$
- Then, when Orthonormal: $(\mathbf{x}, \mathbf{e}_i) = a_i$
- Thus: $(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{n} x_i y_i$

This form of the inner product is consistent with the "dot product"

48

Vector Spaces

https://www.youtube.com/watch?v=ozwodzD5bJM (6:57)

49

Matrices

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix} \qquad \mathbf{A} = \left[a_{ij} \right]_{n \times m}$$

- $\mathbf{A}$ maps/transforms/operates on Vectors from a Vector Space of Dimension n to Vector Space of Dimension m: $\mathbf{A} : \mathbb{V}^n \to \mathbb{V}^m$
- When $\mathbf{A}$ is a Square Matrix, n=m, it Represents a Linear Mapping to od vector to another within the same space: $\mathbf{A} : \mathbb{V}^n \to \mathbb{V}^n$
- Each Row of $\mathbf{A}$ is a Row Vector and Each Column is a Column Vector
- Row/Column Vectors Span the Domain/Range of the Vector Spaces, $\mathbb{V}^n$ and $\mathbb{V}^m$

50

Elementary Row Operations

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$$

1. Any row may be interchanged with any other
2. Any row may be replaced by itself multiplied by a constant
3. Any row may be replaced by the column-wise sum of itself and a multiple of another row

Two Matrices are Row-Equivalent if one is Obtained from the Other by a Finite Sequence of Row Operations

51

Identity Matrix

$$\mathbf{I} = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

- Identity Matrix is $n \times n$ Square Matrix whose Row-Vectors and Column Vectors Form an Orthonormal Basis for the n-dimensional Euclidean Vector Space
- Sometimes denoted as $\mathbf{I}_n$ to emphasize its dimension is $n \times n$
- A Permutation Matrix is an Identity Matrix that has Undergone an Arbitrary Series of Row or Column Interchanges

52

Trace of a Matrix

- Trace of a Matrix $\mathbf{A}$ is:

$$\mathrm{Tr}(\mathbf{A}) = \mathrm{tr}(\mathbf{A}) = \sum_{i=1}^{n} a_{ii}$$

- Given two matrices $\mathbf{A}$ and $\mathbf{B}$:

$$\mathrm{Tr}(\mathbf{AB}) = \mathrm{Tr}(\mathbf{BA})$$

$$\mathrm{Tr}(\mathbf{A}+\mathbf{B}) = \mathrm{Tr}(\mathbf{A}) + \mathrm{Tr}(\mathbf{B})$$

$$\mathrm{Tr}(c\mathbf{A}) = c\,\mathrm{Tr}(\mathbf{A})$$

$$\mathrm{Tr}(\mathbf{SAS}^\dagger) = \mathrm{Tr}(\mathbf{S}^\dagger\mathbf{SA}) = \mathrm{Tr}(\mathbf{A})$$
$$\mathrm{Tr}(\mathbf{SBS}^\dagger) = \mathrm{Tr}(\mathbf{S}^\dagger\mathbf{SB}) = \mathrm{Tr}(\mathbf{B})$$

Similarity Transform when A and B are "similar" Matrices

Matrix Determinant

- Determinant of a Matrix is Denoted as:

$$|\mathbf{A}| \qquad\qquad \det(\mathbf{A})$$

- Examples of Determinant Computation:

scalar case

$$\mathbf{A}_1 = \begin{bmatrix} a_{11} \end{bmatrix} \quad \mathbf{A}_2 = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \mathbf{A}_3 = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

scalar case is absolute value

$$|\mathbf{A}_1| = a_{11} \qquad |\mathbf{A}_2| = a_{11}a_{22} - a_{12}a_{21}$$

$$|\mathbf{A}_3| = a_{11}\begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{12}\begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{13}\begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix}$$

Matrix Operations

- Transpose of a matrix, reflection about the diagonal:

$$\mathbf{A} = \left[a_{ij} \right] \qquad \mathbf{A}^{\mathrm{T}} = \left[a_{ji} \right]$$

- Determinant of $\mathbf{A}$ is Equal to Determinant of $\mathbf{A}^{\mathrm{T}}$
- If Two or More Rows (or columns) of $\mathbf{A}$ are Equivalent then $|\mathbf{A}|=0$
- A Square $n \times n$ Matrix is Triangular When:

$$\forall i > j, a_{ij} = 0 \text{ (upper triangular)}$$
$$\forall i < j, a_{ij} = 0 \text{ (lower triangular)}$$

- Determinant of Triangular Matrix $\mathbf{A}_{\mathrm{tri}}$

$$\det(\mathbf{A}_{\mathrm{tri}}) = |\mathbf{A}_{\mathrm{tri}}| = a_{11} \bullet a_{22} \bullet \ldots \bullet a_{nn}$$

55

Rank of a Matrix

- Rank of a Square Matrix, r, is an Integer that is Equal to Number of Linearly Independent Row (Column) Vectors of a Square Matrix
- A Matrix must be Full Rank for a Distinct inverse to Exist
- All Full Rank Matrices may be Converted into Triangular Matrices through Elementary Row Operations
  - allows iterative solution to $\mathbf{Ax}=\mathbf{b}$ through back substitution
- A Full Rank Matrix Must have a non-zero Determinant
- A non-Square Matrix Cannot Have a Rank Larger than $\min(m,n)$

56

Linear Independence

- Given:

$$\{c_1, c_2, \cdots, c_m\} \in \mathbb{C} \qquad \{\mathbf{a}_1, \mathbf{a}_2, \cdots, \mathbf{a}_m\} \in \mathbb{R}^n$$

- The set of m Vectors are ***Linearly Independent*** if:

$$c_1\mathbf{a}_1 + c_2\mathbf{a}_2 + \cdots + c_i\mathbf{a}_i + \cdots + c_m\mathbf{a}_m = \mathbf{0} \Rightarrow c_i = 0 \forall i$$

No Solution for c_i Other Than all Equal 0

- Otherwise, the set of Vectors are Said to be ***Linearly Dependent***
- Linear Independence is a Property of a Specific Subset of Vectors all of dimension n

57

Linear Independence Example (TRY THIS)

$$\alpha_1 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \quad \alpha_2 = \begin{bmatrix} 0 \\ 2 \\ -2 \end{bmatrix} \quad \alpha_3 = \begin{bmatrix} 1 \\ -2 \\ 1 \end{bmatrix} \quad \alpha_4 = \begin{bmatrix} 4 \\ 2 \\ 3 \end{bmatrix}$$

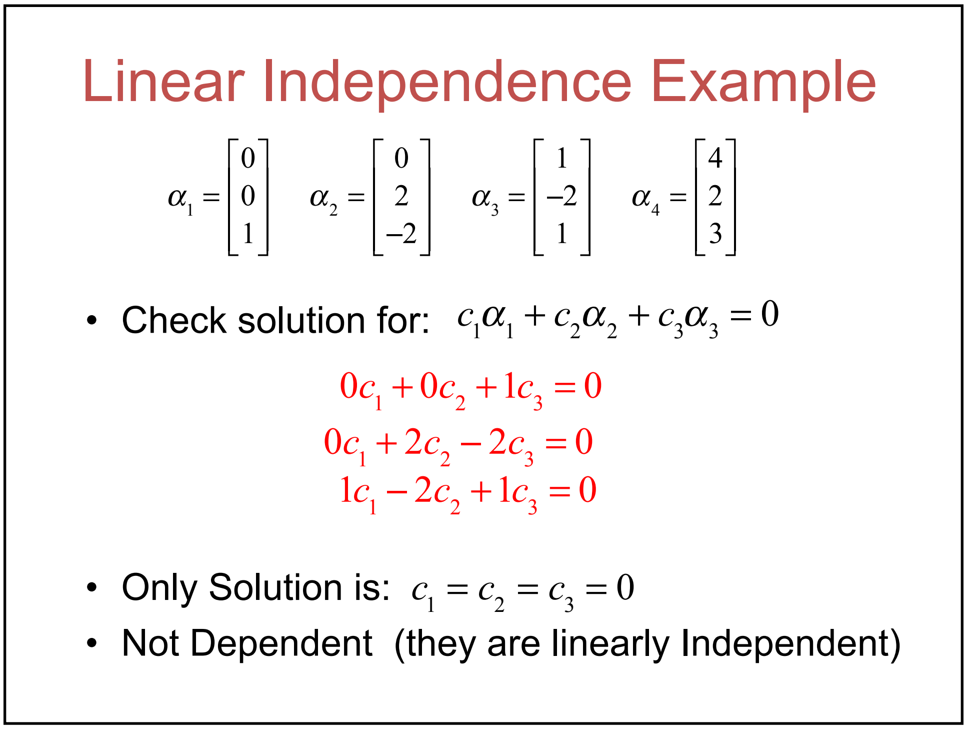
- Is the Following set of Vectors Linearly Dependent?:

$$\{\alpha_1, \alpha_2, \alpha_3\}$$

- Check solution for: $c_1\alpha_1 + c_2\alpha_2 + c_3\alpha_3 = 0$

Compute This on Paper

58



Linear Independence Example

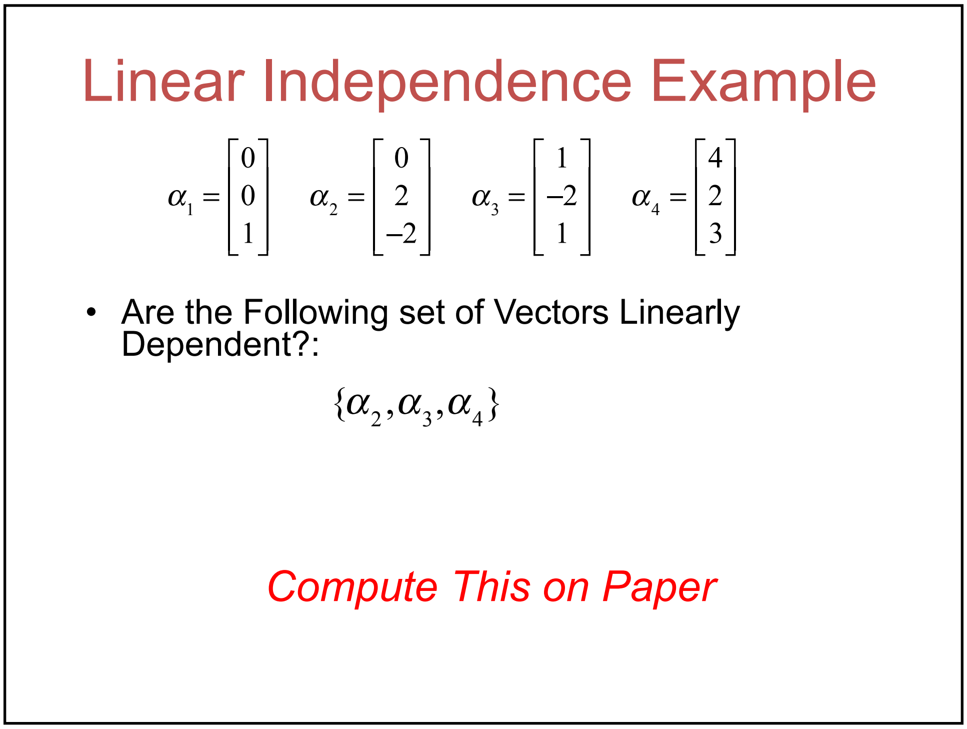
$$\alpha_1 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \quad \alpha_2 = \begin{bmatrix} 0 \\ 2 \\ -2 \end{bmatrix} \quad \alpha_3 = \begin{bmatrix} 1 \\ -2 \\ 1 \end{bmatrix} \quad \alpha_4 = \begin{bmatrix} 4 \\ 2 \\ 3 \end{bmatrix}$$

- Check solution for: $c_1\alpha_1 + c_2\alpha_2 + c_3\alpha_3 = 0$

$$0c_1 + 0c_2 + 1c_3 = 0$$
$$0c_1 + 2c_2 - 2c_3 = 0$$
$$1c_1 - 2c_2 + 1c_3 = 0$$

- Only Solution is: $c_1 = c_2 = c_3 = 0$
- Not Dependent (they are linearly Independent)

59



Linear Independence Example

$$\alpha_1 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \quad \alpha_2 = \begin{bmatrix} 0 \\ 2 \\ -2 \end{bmatrix} \quad \alpha_3 = \begin{bmatrix} 1 \\ -2 \\ 1 \end{bmatrix} \quad \alpha_4 = \begin{bmatrix} 4 \\ 2 \\ 3 \end{bmatrix}$$

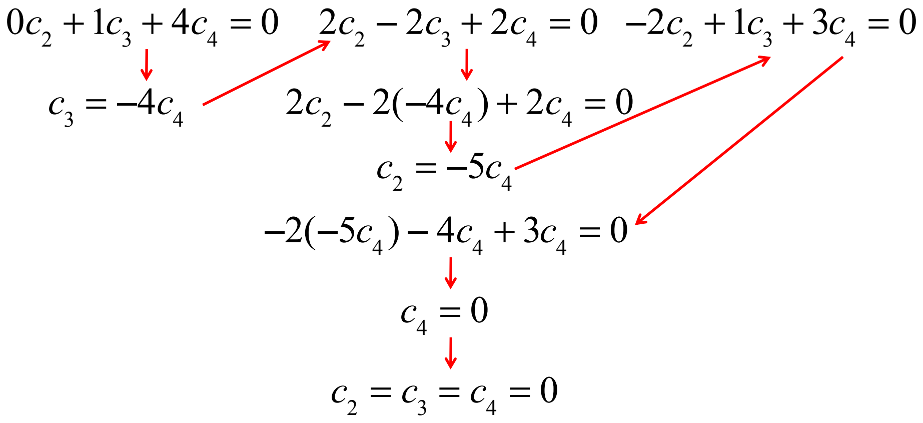
- Are the Following set of Vectors Linearly Dependent?:

$$\{\alpha_2, \alpha_3, \alpha_4\}$$

Compute This on Paper

60

Linear Independence Example



$$0c_2 + 1c_3 + 4c_4 = 0 \qquad 2c_2 - 2c_3 + 2c_4 = 0 \qquad -2c_2 + 1c_3 + 3c_4 = 0$$

$$c_3 = -4c_4$$

$$2c_2 - 2(-4c_4) + 2c_4 = 0$$

$$c_2 = -5c_4$$

$$-2(-5c_4) - 4c_4 + 3c_4 = 0$$

$$c_4 = 0$$

$$c_2 = c_3 = c_4 = 0$$

- Not Dependent (they are linearly Independent)

Linear Independence Example

$$\alpha_1 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \quad \alpha_2 = \begin{bmatrix} 0 \\ 2 \\ -2 \end{bmatrix} \quad \alpha_3 = \begin{bmatrix} 1 \\ -2 \\ 1 \end{bmatrix} \quad \alpha_4 = \begin{bmatrix} 4 \\ 2 \\ 3 \end{bmatrix}$$

- The following sets are Linearly Independent:

$$\{\alpha_1, \alpha_2, \alpha_3\} \qquad \alpha_4 = 9\alpha_1 + 5\alpha_2 + 4\alpha_3$$

$$\{\alpha_2, \alpha_3, \alpha_4\} \quad \alpha_1 = \left(-\frac{5}{9}\right)\alpha_2 + \left(-\frac{4}{9}\right)\alpha_3 + \left(\frac{1}{9}\right)\alpha_4$$

- The following set is Linearly Dependent:

$$\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$$