E2 205: Error-Control Coding
Chapter 3: Mathematical Prelimaries

Navin Kashyap

Indian Institute of Science

Groups

A group $(G, \circ)$ is a non-empty set G equipped with a binary operation $\circ$ that satisfies the following properties (axioms):

- [Closure] $a \circ b \in G$ for all $a, b \in G$
- [Associativity] $a \circ (b \circ c) = (a \circ b) \circ c$ for all $a, b, c \in G$
- [Identity element] $\exists\, e \in G$ such that $a \circ e = e \circ a = a \;\; \forall\, a \in G$
- [Inverse] for each $a \in G$ there exists $a^{-1} \in G$ such that $a \circ a^{-1} = a^{-1} \circ a = e$

Groups

A group $(G, \circ)$ is a non-empty set G equipped with a binary operation $\circ$ that satisfies the following properties (axioms):

- [Closure] $a \circ b \in G$ for all $a, b \in G$
- [Associativity] $a \circ (b \circ c) = (a \circ b) \circ c$ for all $a, b, c \in G$
- [Identity element] $\exists\, e \in G$ such that $a \circ e = e \circ a = a \;\; \forall\, a \in G$
- [Inverse] for each $a \in G$ there exists $a^{-1} \in G$ such that $a \circ a^{-1} = a^{-1} \circ a = e$

If, furthermore, we have

- [Commutativity] $a \circ b = b \circ a$ for all $a, b \in G$

then $(G, \circ)$ is called a commutative or abelian group.

Groups

A group $(G, \circ)$ is a non-empty set G equipped with a binary operation $\circ$ that satisfies the following properties (axioms):

- [Closure] $a \circ b \in G$ for all $a, b \in G$
- [Associativity] $a \circ (b \circ c) = (a \circ b) \circ c$ for all $a, b, c \in G$
- [Identity element] $\exists\, e \in G$ such that $a \circ e = e \circ a = a \;\; \forall\, a \in G$
- [Inverse] for each $a \in G$ there exists $a^{-1} \in G$ such that $a \circ a^{-1} = a^{-1} \circ a = e$

If, furthermore, we have

- [Commutativity] $a \circ b = b \circ a$ for all $a, b \in G$

then $(G, \circ)$ is called a commutative or abelian group.

Examples of abelian groups:

- $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ etc.
- $(\mathbb{R} \setminus \{0\}, \times)$, $(\mathbb{C} \setminus \{0\}, \times)$
- $(\mathbb{Z}_n, +)$, i.e., the integers modulo-n under addition modulo-n

More Examples

- The set of non-singular $m \times m$ matrices $(m > 1)$ over $\mathbb{R}$ or $\mathbb{C}$, under matrix multiplication, is a non-abelian group.

- $(\mathbb{Z}, \times)$ is not a group, since 0 has no inverse.
- $(\mathbb{Z} \setminus \{0\}, \times)$ is also not a group (why?)

More Examples

- The set of non-singular $m \times m$ matrices $(m > 1)$ over $\mathbb{R}$ or $\mathbb{C}$, under matrix multiplication, is a non-abelian group.

- $(\mathbb{Z}, \times)$ is not a group, since 0 has no inverse.
- $(\mathbb{Z} \setminus \{0\}, \times)$ is also not a group (why?)

- $(\mathbb{Z}_n \setminus \{0\}, \times)$ is a group iff n is prime.

More Examples

- The set of non-singular $m \times m$ matrices $(m > 1)$ over $\mathbb{R}$ or $\mathbb{C}$, under matrix multiplication, is a non-abelian group.

- $(\mathbb{Z}, \times)$ is not a group, since 0 has no inverse.
- $(\mathbb{Z} \setminus \{0\}, \times)$ is also not a group (why?)

- $(\mathbb{Z}_n \setminus \{0\}, \times)$ is a group iff n is prime.

  (Only if) If $n = a \cdot b$ for $1 < a, b < n$, then $a, b \in Z_n \setminus \{0\}$ are such that $a \times b = 0 \pmod{n}$. This violates the closure property.

More Examples

- The set of non-singular $m \times m$ matrices $(m > 1)$ over $\mathbb{R}$ or $\mathbb{C}$, under matrix multiplication, is a non-abelian group.

- $(\mathbb{Z}, \times)$ is not a group, since 0 has no inverse.
- $(\mathbb{Z} \setminus \{0\}, \times)$ is also not a group (why?)

- $(\mathbb{Z}_n \setminus \{0\}, \times)$ is a group iff n is prime.

  (Only if) If $n = a \cdot b$ for $1 < a, b < n$, then $a, b \in Z_n \setminus \{0\}$ are such that $a \times b = 0 \pmod{n}$. This violates the closure property.

  (If) If n is prime, all the group properties are easy to check, except for the existence of inverses. The existence of inverses follows from the extended Euclidean division algorithm. [See Math module covering prime fields]

Derived Properties of Groups

Some properties of groups can be derived from the axioms.

If G is a group, then

- The identity element of G is unique.
- Each $a \in G$ has a unique inverse in G.

For proofs, see the Math module for groups.

Subgroups

If $(G, \circ)$ is a group, and for some $H \subseteq G$, $(H, \circ)$ constitutes a group by itself, then H is said to be a subgroup of G (with respect to the $\circ$ operation).

Examples:

- $H = G$ and $H = \{e\}$ are trivial subgroups of any group G, where e is the identity element of G.
- $\mathbb{Z}$ is a subgroup of $\mathbb{R}$ under addition.
- The set, $2\mathbb{Z}$, of even integers form a subgroup of $\mathbb{Z}$ under addition.

Rings

A ring $(R, +, \cdot)$ is a non-empty set R equipped with two binary operations $+$ and $\cdot$ that satisfy the following properties (axioms):

(R1) $(R, +)$ is an abelian group

(R2) [Closure under $\cdot$] $a \cdot b \in R$ for all $a, b \in R$.

(R3) [Associativity of $\cdot$] $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in R$

(R4) [Distributivity of $\cdot$ over $+$] For all $a, b, c \in R$,

- $a \cdot (b + c) = a \cdot b + a \cdot c$
- $(b + c) \cdot a = b \cdot a + c \cdot a$

Rings

A ring $(R, +, \cdot)$ is a non-empty set R equipped with two binary operations $+$ and $\cdot$ that satisfy the following properties (axioms):

(R1) $(R, +)$ is an abelian group

(R2) [Closure under $\cdot$] $a \cdot b \in R$ for all $a, b \in R$.

(R3) [Associativity of $\cdot$] $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in R$

(R4) [Distributivity of $\cdot$ over $+$] For all $a, b, c \in R$,

- $a \cdot (b + c) = a \cdot b + a \cdot c$
- $(b + c) \cdot a = b \cdot a + c \cdot a$

- The identity element w.r.t. $+$ is usually called the zero element, and is denoted by 0: $a + 0 = 0 + a = a$ for all $a \in R$.
- The inverse of $a \in R$ under $+$ is usually denoted by $-a$.

Rings

A ring $(R, +, \cdot)$ is a non-empty set R equipped with two binary operations $+$ and $\cdot$ that satisfy the following properties (axioms):

(R1) $(R, +)$ is an abelian group

(R2) [Closure under $\cdot$] $a \cdot b \in R$ for all $a, b \in R$.

(R3) [Associativity of $\cdot$] $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in R$

(R4) [Distributivity of $\cdot$ over $+$] For all $a, b, c \in R$,

- $a \cdot (b + c) = a \cdot b + a \cdot c$
- $(b + c) \cdot a = b \cdot a + c \cdot a$

- The identity element w.r.t. $+$ is usually called the zero element, and is denoted by 0: $a + 0 = 0 + a = a$ for all $a \in R$.
- The inverse of $a \in R$ under $+$ is usually denoted by $-a$.

Example: $(\mathbb{Z}_n, +, \cdot)$ the integers mod n under mod-n arithmetic.

More Definitions

- A ring $(R, +, \cdot)$ is commutative if $a \cdot b = b \cdot a$ for all $a, b \in R$.
- A ring with unity is a ring $(R, +, \cdot)$ in which $\cdot$ has an identity element.
- The identity element w.r.t. $\cdot$ (if it exists) is usually called the unity element, and is denoted by 1:

$$a \cdot 1 = 1 \cdot a = a \quad \text{for all } a \in R$$

Fields

A field is a commutative ring with unity, in which every non-zero element has an inverse w.r.t. $\cdot$.

Fields

A field is a commutative ring with unity, in which every non-zero element has an inverse w.r.t. $\cdot$.

Equivalently, a field $(\mathbb{F}, +, \cdot)$ is a non-empty set $\mathbb{F}$ equipped with two binary operations $+$ and $\cdot$ that satisfy the following properties (field axioms):

(F1) $(\mathbb{F}, +)$ is an abelian group (with identity element 0)

(F2) $(\mathbb{F} \setminus \{0\}, \cdot)$ is an abelian group (with identity element 1)

(F3) [Distributivity of $\cdot$ over $+$]

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{for all } a, b, c \in \mathbb{F}$$

Fields

A field is a commutative ring with unity, in which every non-zero element has an inverse w.r.t. $\cdot$.

Equivalently, a field $(\mathbb{F}, +, \cdot)$ is a non-empty set $\mathbb{F}$ equipped with two binary operations $+$ and $\cdot$ that satisfy the following properties (field axioms):

(F1) $(\mathbb{F}, +)$ is an abelian group (with identity element 0)

(F2) $(\mathbb{F} \setminus \{0\}, \cdot)$ is an abelian group (with identity element 1)

(F3) [Distributivity of $\cdot$ over $+$]

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{for all } a, b, c \in \mathbb{F}$$

Examples: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ equipped with the usual addition and multiplication operations.

Examples of Rings That Are Not Fields

- $(\mathbb{Z}, +, \cdot)$
- The set of $n \times n$ matrices over a field $\mathbb{F}$, equipped with the usual matrix addition and multiplication.
  (This is a non-commutative ring.)
- $(\mathbb{F}[x], +, \cdot)$, where
  - $\mathbb{F}[x]$ is the set of all polynomials in the indeterminate x, taking coefficients from a field $\mathbb{F}$, i.e.,
    $\mathbb{F}[x] = \{\sum_{j=0}^{d} a_j x^j : a_j \in \mathbb{F}$ and $d \geq 0$ an integer$\}$
  - $+$ and $\cdot$ are polynomial addition and multiplication, respectively
- $(\mathbb{Z}_n, +, \cdot)$ when n is *not* a prime.
  (We have seen that in this case $(\mathbb{Z}_n \setminus \{0\}, \cdot)$ is not a group.)

Prime Fields

An important example of a field is $\mathbb{Z}_2 = \{0, 1\}$ under mod-2 arithmetic. We denote this as $\mathbb{F}_2$.

More generally, the following is true.

Proposition:
When p is a prime, $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ under mod-p arithmetic is a field.

Prime Fields

An important example of a field is $\mathbb{Z}_2 = \{0, 1\}$ under mod-2 arithmetic. We denote this as $\mathbb{F}_2$.

More generally, the following is true.

Proposition:
When p is a prime, $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ under mod-p arithmetic is a field.

Proof:

- It is easy to verify that the field axioms
  (F1) $(\mathbb{Z}_p, +)$ is an abelian group
  and
  (F3) multiplication distributes over addition
  are true.

Prime Fields

An important example of a field is $\mathbb{Z}_2 = \{0, 1\}$ under mod-2 arithmetic. We denote this as $\mathbb{F}_2$.

More generally, the following is true.

Proposition:
When p is a prime, $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ under mod-p arithmetic is a field.

Proof:

- It is easy to verify that the field axioms
  (F1) $(\mathbb{Z}_p, +)$ is an abelian group
  and
  (F3) multiplication distributes over addition
  are true.
- To check that the field axiom
  (F2) $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ is an abelian group
  also holds, the only non-trivial property to verify is the existence of (multiplicative) inverses.

Existence of Multiplicative Inverses in $\mathbb{Z}_p \setminus \{0\}$

In the following, all addition and multiplication operations are mod-p.

- Given $a \in \mathbb{Z}_p \setminus \{0\}$, consider $a,\ 2 \cdot a,\ 3 \cdot a,\ \ldots,\ (p-1) \cdot a$.
- Note that $b \cdot a \neq 0$ for any $b \in \{1, 2, \ldots, p-1\}$.
  ($b \cdot a = 0$ holds iff $p \mid ba$, which in turn holds iff either $p \mid a$ or $p \mid b$, both of which are impossible.)
- Also, note that $b \cdot a \neq c \cdot a$ for $b, c \in \{1, 2, \ldots, p-1\}$, $b \neq c$.
  (Otherwise, we would have $(b - c) \cdot a = 0$, which is not possible for the same reason as above.)
- Consequently, $a,\ 2 \cdot a,\ 3 \cdot a,\ \ldots,\ (p-1) \cdot a$ cover all the nonzero integers in $\mathbb{Z}_p$.
- In particular, we must have $b \cdot a = 1$ for some $b \in \{1, 2, \ldots, p-1\}$.
- This b is the multiplicative inverse of a in $\mathbb{Z}_p \setminus \{0\}$.

Some Remarks

- When p is a prime, we denote by $\mathbb{F}_p$ the field of integers modulo p.
- The multiplicative inverse of any nonzero $a \in \mathbb{F}_p$ can be computed using the extended Euclidean division algorithm — for details, refer to the Math module on prime fields.
- Fields with a finite number of elements (such as $\mathbb{F}_p$) are called finite fields. We will study them in more detail later.

Derived Properties of Fields

Some properties of fields can be derived from the axioms.

- $a \cdot 0 = 0$ for all $a \in \mathbb{F}$

  Proof:

  - $a \cdot (1 + 0)$ can be expressed in two different ways:

$$a \cdot (1 + 0) = a \cdot 1 = a$$
$$a \cdot (1 + 0) = a \cdot 1 + a \cdot 0 = a + a \cdot 0$$

  - Hence, $a = a + a \cdot 0$. Now, add $-a$ to both sides. $\square$

Derived Properties of Fields

Some properties of fields can be derived from the axioms.

- $a \cdot 0 = 0$ for all $a \in \mathbb{F}$

  Proof:

  - $a \cdot (1 + 0)$ can be expressed in two different ways:

$$a \cdot (1 + 0) = a \cdot 1 = a$$
$$a \cdot (1 + 0) = a \cdot 1 + a \cdot 0 = a + a \cdot 0$$

  - Hence, $a = a + a \cdot 0$. Now, add $-a$ to both sides. $\square$

- No zero divisors:

$$a \cdot b = 0 \implies a = 0 \text{ or } b = 0 \text{ (or both)}$$

  Proof:

  - Suppose $a \cdot b = 0$, but $a \neq 0$.
  - Then, multiply both sides of $a \cdot b = 0$ by a^{-1} to get $b = 0$. $\square$

Vector Spaces

A vector space $(V, +, \mathbb{F}, \cdot)$ consists of a non-empty set V of "vectors", a field $\mathbb{F}$ of "scalars", and two operations

- '$+$' representing vector addition, and
- '$\cdot$' representing scalar multiplication

that satisfy the following properties (vector space axioms):

(V1) $(V, +)$ is an abelian group (with identity element $\mathbf{0}$).

(V2) $\alpha \cdot \mathbf{v} \in V$ for all $\alpha \in \mathbb{F}$ and $\mathbf{v} \in V$.

(V3) $\alpha \cdot (\beta \cdot \mathbf{v}) = (\alpha\beta) \cdot \mathbf{v}$ for all $\alpha, \beta \in \mathbb{F}$ and $\mathbf{v} \in V$.

(V4) $(\alpha + \beta) \cdot \mathbf{v} = \alpha \cdot \mathbf{v} + \beta \cdot \mathbf{v}$ for all $\alpha, \beta \in \mathbb{F}$ and $\mathbf{v} \in V$,
$\alpha \cdot (\mathbf{v} + \mathbf{w}) = \alpha \cdot \mathbf{v} + \alpha \cdot \mathbf{w}$ for all $\alpha \in \mathbb{F}$ and $\mathbf{v}, \mathbf{w} \in V$.

(V5) $1 \cdot \mathbf{v} = \mathbf{v}$ for all $\mathbf{v} \in V$, where 1 is the multiplicative identity element of the field $\mathbb{F}$.

Examples

- $\mathbb{F}^n = \{(a_1, a_2, \ldots, a_n) : a_i \in \mathbb{F} \text{ for all } i\}$, where $\mathbb{F}$ is a field.
  - $(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$
  - $\alpha \cdot (a_1, \ldots, a_n) = (\alpha a_1, \ldots, \alpha a_n)$

- $\mathbb{F}_d[x] = \left\{\sum_{j=0}^{d} a_j x^j : a_j \in \mathbb{F} \text{ for all } j\right\}$, for a fixed $d \in \mathbb{Z}_+$
  (set of polynomials of a fixed degree d, taking coeffs from $\mathbb{F}$)

  This vector space is isomorphic to $\mathbb{F}^{d+1}$ via the bijection

$$\sum_{j=0}^{d} a_j x^j \longleftrightarrow (a_0, a_1, \ldots, a_d)$$

- $\mathbb{F}[x] = \left\{\sum_{j=0}^{d} a_j x^j : a_j \in \mathbb{F} \text{ for all } j,\ d \in \mathbb{Z}_+\right\}$
  (set of all polynomials taking coefficients from $\mathbb{F}$)

Derived Properties of Vector Spaces

Some properties of vector spaces can be derived from the axioms.

1). $0 \cdot \mathbf{v} = \mathbf{0}$ for all $\mathbf{v} \in V$

Proof:

- $(0+0) \cdot \mathbf{v}$ can be expressed in two different ways:

$$(0+0) \cdot \mathbf{v} = 0 \cdot \mathbf{v} \quad (\text{since } 0+0=0 \text{ in } \mathbb{F})$$
$$(0+0) \cdot \mathbf{v} = 0 \cdot \mathbf{v} + 0 \cdot \mathbf{v} \quad (\text{using axiom (V4)})$$

- Hence, $0 \cdot \mathbf{v} = 0 \cdot \mathbf{v} + 0 \cdot \mathbf{v}$. Now, add $-(0 \cdot \mathbf{v})$ to both sides. $\square$

Derived Properties of Vector Spaces

Some properties of vector spaces can be derived from the axioms.

1). $0 \cdot \mathbf{v} = \mathbf{0}$ for all $\mathbf{v} \in V$

Proof:

- $(0 + 0) \cdot \mathbf{v}$ can be expressed in two different ways:

$$(0 + 0) \cdot \mathbf{v} = 0 \cdot \mathbf{v} \quad (\text{since } 0 + 0 = 0 \text{ in } \mathbb{F})$$
$$(0 + 0) \cdot \mathbf{v} = 0 \cdot \mathbf{v} + 0 \cdot \mathbf{v} \quad (\text{using axiom (V4)})$$

- Hence, $0 \cdot \mathbf{v} = 0 \cdot \mathbf{v} + 0 \cdot \mathbf{v}$. Now, add $-(0 \cdot \mathbf{v})$ to both sides. $\square$

2). $\alpha \cdot \mathbf{0} = \mathbf{0}$ for all $\alpha \in \mathbb{F}$

Proof:

- $\alpha \cdot (\mathbf{0} + \mathbf{0})$ can be expressed in two different ways:

$$\alpha \cdot (\mathbf{0} + \mathbf{0}) = \alpha \cdot \mathbf{0} \quad (\text{since } \mathbf{0} + \mathbf{0} = \mathbf{0} \text{ in } V)$$
$$\alpha \cdot (\mathbf{0} + \mathbf{0}) = \alpha \cdot \mathbf{0} + \alpha \cdot \mathbf{0} \quad (\text{using axiom (V4)})$$

- Hence, $\alpha \cdot \mathbf{0} = \alpha \cdot \mathbf{0} + \alpha \cdot \mathbf{0}$. Add $-(\alpha \cdot \mathbf{0})$ to both sides. $\square$

Derived Properties of Vector Spaces

3). $\alpha \cdot \mathbf{v} = \mathbf{0} \iff$ either $\alpha = 0$ or $\mathbf{v} = \mathbf{0}$ (or both)

Proof:

($\Longleftarrow$) is proved in items 1) and 2).

($\Longrightarrow$) Suppose $\alpha \cdot \mathbf{v} = \mathbf{0}$, but $\alpha \neq 0$. Then,

$$\alpha^{-1} \cdot (\alpha \cdot \mathbf{v}) \; = \; \alpha^{-1} \cdot \mathbf{0} \; = \; \mathbf{0} \;\; \text{(as previously shown)}$$

$$\alpha^{-1} \cdot (\alpha \cdot \mathbf{v}) \; \overset{\text{(V3)}}{=} \; (\alpha^{-1}\alpha) \cdot \mathbf{v} \; = \; 1 \cdot \mathbf{v} \; \overset{\text{(V5)}}{=} \; \mathbf{v}$$

Thus, $\mathbf{v} = \mathbf{0}$. $\square$

Derived Properties of Vector Spaces

3). $\alpha \cdot \mathbf{v} = \mathbf{0} \iff$ either $\alpha = 0$ or $\mathbf{v} = \mathbf{0}$ (or both)

Proof:

($\Longleftarrow$) is proved in items 1) and 2).

($\Longrightarrow$) Suppose $\alpha \cdot \mathbf{v} = \mathbf{0}$, but $\alpha \neq 0$. Then,

$$\alpha^{-1} \cdot (\alpha \cdot \mathbf{v}) \;=\; \alpha^{-1} \cdot \mathbf{0} \;=\; \mathbf{0} \;\; \text{(as previously shown)}$$

$$\alpha^{-1} \cdot (\alpha \cdot \mathbf{v}) \;\overset{(V3)}{=}\; (\alpha^{-1}\alpha) \cdot \mathbf{v} \;=\; 1 \cdot \mathbf{v} \;\overset{(V5)}{=}\; \mathbf{v}$$

Thus, $\mathbf{v} = \mathbf{0}$. $\square$

4). $(-1) \cdot \mathbf{v} = -\mathbf{v}$ for all $\mathbf{v} \in V$.

Proof:

$$\begin{aligned} \mathbf{v} + (-1) \cdot \mathbf{v} \;\overset{(V5)}{=}\; 1 \cdot \mathbf{v} + (-1) \cdot \mathbf{v} \;&\overset{(V4)}{=}\; (1 + (-1)) \cdot \mathbf{v} \\ &=\; 0 \cdot \mathbf{v} \;=\; \mathbf{0} \end{aligned}$$

Subspaces

A subspace of a vector space $(V, +, \mathbb{F}, \cdot)$ is a subset $W \subseteq V$ such that $(W, +, \mathbb{F}, \cdot)$ is itself a vector space.

Examples: The following are all the subspaces of $\mathbb{R}^3$ —

- $\mathbb{R}^3$ itself
- $\{\mathbf{0}\}$
- any line through the origin
- any plane through the origin

Testing if $W \subseteq V$ is a Subspace

Proposition:
Let $(V, +, \mathbb{F}, \cdot)$ be a vector space. A subset $W \subseteq V$ is a subspace of V if and only if

$$\alpha \cdot \mathbf{w} + \mathbf{w}' \in W \text{ for all } \mathbf{w}, \mathbf{w}' \in W \text{ and } \alpha \in \mathbb{F}. \tag{1}$$

Proof: "Only if" is obvious from the definition of a subspace.

For the "if" direction, assume that (1) holds. We need to show that the vector space axioms (V1)–(V5) hold for $(W, +, \mathbb{F}, \cdot)$.

- (V3)–(V5) directly follow from the fact that V is a vector space, and $W \subseteq V$.
- To verify (V1):
  - Set $\alpha = 1$ in (1) to get $\mathbf{w} + \mathbf{w}' \in W$ for all $\mathbf{w}, \mathbf{w}' \in W$.
  - Set $\alpha = -1$ and $\mathbf{w}' = \mathbf{w}$ in (1) to get $\mathbf{0} \in W$.
  - Set $\mathbf{w}' = \mathbf{0}$ and $\alpha = -1$ in (1) to get $-\mathbf{w} \in W$ for all $\mathbf{w} \in W$.
- To verify (V2):

  Set $\mathbf{w}' = \mathbf{0}$ in (1) to get $\alpha \cdot \mathbf{w} \in W$ for all $\mathbf{w} \in W$. $\square$

Special Case: $\mathbb{F} = \mathbb{F}_2$

If V is a vector space over the *binary* field $\mathbb{F}_2$, then the subspace test simplifies to:

$$W \subseteq V \text{ is a subspace} \iff \mathbf{w} + \mathbf{w}' \in W \text{ for all } \mathbf{w}, \mathbf{w}' \in W$$

An Application of the Subspace Test

Proposition:
Let H be an $m \times n$ matrix over a field $\mathbb{F}$. Then,

$$\mathcal{C} = \{\mathbf{x} \in \mathbb{F}^n : H\mathbf{x}^T = \mathbf{0}\}$$

is a subspace of $\mathbb{F}^n$. (This is called the nullspace of H.)

An Application of the Subspace Test

Proposition:

Let H be an $m \times n$ matrix over a field $\mathbb{F}$. Then,

$$\mathcal{C} = \{\mathbf{x} \in \mathbb{F}^n : H\mathbf{x}^T = \mathbf{0}\}$$

is a subspace of $\mathbb{F}^n$. (This is called the nullspace of H.)

Proof: Apply the subspace test to $\mathcal{C}$.

- Consider any $\mathbf{x}, \mathbf{x}' \in \mathcal{C}$ and $\alpha \in \mathbb{F}$. We must show that $\mathbf{y} = \mathbf{x}' + \alpha \cdot \mathbf{x}$ is in $\mathcal{C}$.
- To this end,

$$\begin{aligned} H\mathbf{y}^T &= H(\mathbf{x}' + \alpha \cdot \mathbf{x})^T \\ &= H\mathbf{x}'^T + \alpha \cdot H\mathbf{x}^T \quad \text{(by linearity of matrix multiplication)} \\ &= \mathbf{0} + \alpha \cdot \mathbf{0} \qquad\qquad \text{(since } \mathbf{x}, \mathbf{x}' \in \mathcal{C}\text{)} \\ &= \mathbf{0} + \mathbf{0} \;=\; \mathbf{0} \end{aligned}$$

- Hence, $\mathbf{y} = \mathbf{x}' + \alpha \cdot \mathbf{x}$ belongs to $\mathcal{C}$ $\square$

Linear Combinations and Span

Let V be a vector space over a field $\mathbb{F}$, and let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m$ be vectors in V.

- Any vector of the form

$$\mathbf{w} = \alpha_1 \cdot \mathbf{v}_1 + \alpha_2 \cdot \mathbf{v}_2 + \cdots + \alpha_m \cdot \mathbf{v}_m, \quad \text{with } \alpha_j \in \mathbb{F} \text{ for all } j$$

  is called a linear combination of $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m$.

Linear Combinations and Span

Let V be a vector space over a field $\mathbb{F}$, and let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m$ be vectors in V.

- Any vector of the form

$$\mathbf{w} = \alpha_1 \cdot \mathbf{v}_1 + \alpha_2 \cdot \mathbf{v}_2 + \cdots + \alpha_m \cdot \mathbf{v}_m, \quad \text{with } \alpha_j \in \mathbb{F} \text{ for all } j$$

  is called a linear combination of $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m$.

- It is easy to verify (using the subspace test) that the set

$$W = \left\{ \sum_{j=1}^{m} \alpha_j \cdot \mathbf{v}_j : \ \alpha_j \in \mathbb{F} \text{ for all } j \right\}$$

  consisting of all linear combinations of $\mathbf{v}_1, \ldots, \mathbf{v}_m$ is a subspace of V; denoted by $\text{span}(\mathbf{v}_1, \ldots, \mathbf{v}_m)$.

Linear Combinations and Span

Let V be a vector space over a field $\mathbb{F}$, and let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m$ be vectors in V.

- Any vector of the form

  $$\mathbf{w} = \alpha_1 \cdot \mathbf{v}_1 + \alpha_2 \cdot \mathbf{v}_2 + \cdots + \alpha_m \cdot \mathbf{v}_m, \quad \text{with } \alpha_j \in \mathbb{F} \text{ for all } j$$

  is called a linear combination of $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m$.

- It is easy to verify (using the subspace test) that the set

  $$W = \left\{ \sum_{j=1}^{m} \alpha_j \cdot \mathbf{v}_j : \ \alpha_j \in \mathbb{F} \text{ for all } j \right\}$$

  consisting of all linear combinations of $\mathbf{v}_1, \ldots, \mathbf{v}_m$ is a subspace of V; denoted by $\text{span}(\mathbf{v}_1, \ldots, \mathbf{v}_m)$.

  Example: For a $k \times n$ matrix G over $\mathbb{F}$, with rows $\mathbf{g}_1, \ldots, \mathbf{g}_k$, $\text{span}(\mathbf{g}_1, \ldots, \mathbf{g}_k)$ is called the rowspace of G.

Linear Independence

Definition:

Vectors $\mathbf{v}_1, \ldots, \mathbf{v}_m$ are linearly independent over a field $\mathbb{F}$ if, for $\alpha_1, \ldots, \alpha_m \in \mathbb{F}$, we have

$$\sum_{j=1}^{m} \alpha_j \cdot \mathbf{v}_j \; = \; \mathbf{0} \quad \Longrightarrow \quad \alpha_1 = \cdots = \alpha_m = 0.$$

Example: $\mathbf{v}_1 = [1\ 1\ 0]$, $\mathbf{v}_2 = [1\ 0\ 1]$, $\mathbf{v}_3 = [0\ 1\ 1]$

- It is easy to check that these vectors are linearly independent over $\mathbb{R}$.

Linear Independence

Definition:

Vectors $\mathbf{v}_1, \ldots, \mathbf{v}_m$ are linearly independent over a field $\mathbb{F}$ if, for $\alpha_1, \ldots, \alpha_m \in \mathbb{F}$, we have

$$\sum_{j=1}^{m} \alpha_j \cdot \mathbf{v}_j \;=\; \mathbf{0} \quad\Longrightarrow\quad \alpha_1 = \cdots = \alpha_m = 0.$$

Example: $\mathbf{v}_1 = [1\ 1\ 0]$, $\mathbf{v}_2 = [1\ 0\ 1]$, $\mathbf{v}_3 = [0\ 1\ 1]$

- It is easy to check that these vectors are linearly independent over $\mathbb{R}$.
- However, they are linearly dependent over $\mathbb{F}_2$, since $\mathbf{v}_1 + \mathbf{v}_2 + \mathbf{v}_3 = \mathbf{0}$ when vector addition is done modulo 2.

RREF and Rank

Let $\mathbb{F}$ be a given field.

To determine if a collection of vectors $\mathbf{v}_1, \ldots, \mathbf{v}_m$ from $\mathbb{F}^n$ is linearly independent over $\mathbb{F}$, we can do the following:

- Put the vectors into the rows of a matrix

$$A = \begin{bmatrix} \text{------} & \mathbf{v}_1 & \text{------} \\ & \vdots & \\ \text{------} & \mathbf{v}_m & \text{------} \end{bmatrix}$$

- Using elementary row operations over $\mathbb{F}$, bring A into reduced row-echelon form (RREF)
- The number of non-zero rows in the RREF gives the maximum number of linearly independent vectors among $\mathbf{v}_1, \ldots, \mathbf{v}_m$.

RREF and Rank

Let $\mathbb{F}$ be a given field.

To determine if a collection of vectors $\mathbf{v}_1, \ldots, \mathbf{v}_m$ from $\mathbb{F}^n$ is linearly independent over $\mathbb{F}$, we can do the following:

- Put the vectors into the rows of a matrix

$$A = \begin{bmatrix} \rule{2cm}{0.5pt} & \mathbf{v}_1 & \rule{2cm}{0.5pt} \\ & \vdots & \\ \rule{2cm}{0.5pt} & \mathbf{v}_m & \rule{2cm}{0.5pt} \end{bmatrix}$$

- Using elementary row operations over $\mathbb{F}$, bring A into reduced row-echelon form (RREF)
- The number of non-zero rows in the RREF gives the maximum number of linearly independent vectors among $\mathbf{v}_1, \ldots, \mathbf{v}_m$.

Recall from linear algebra that

$$\begin{aligned} \mathrm{rank}_{\mathbb{F}}(A) &\triangleq \text{max. no. of lin. indep. rows of } A \\ &= \text{max. no. of lin. indep. columns of } A \;=\; \mathrm{rank}_{\mathbb{F}}(A^T) \end{aligned}$$

Example

$$\mathbf{v}_1 = [1\ 1\ 0], \quad \mathbf{v}_2 = [1\ 0\ 1], \quad \mathbf{v}_3 = [0\ 1\ 1]$$

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \xrightarrow{\text{RREF over } \mathbb{R}} \begin{bmatrix} 1 & 1 & 0 \\ 0 & -1 & 2 \\ 0 & 0 & 2 \end{bmatrix} \implies \begin{array}{l} \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3 \\ \text{lin. indep.} \\ \text{over } \mathbb{R} \end{array}$$

Example

$$\mathbf{v}_1 = [1\ 1\ 0], \quad \mathbf{v}_2 = [1\ 0\ 1], \quad \mathbf{v}_3 = [0\ 1\ 1]$$

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \xrightarrow{\text{RREF over } \mathbb{R}} \begin{bmatrix} 1 & 1 & 0 \\ 0 & -1 & 2 \\ 0 & 0 & 2 \end{bmatrix} \implies \begin{array}{l} \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3 \\ \text{lin. indep.} \\ \text{over } \mathbb{R} \end{array}$$

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \xrightarrow{\text{RREF over } \mathbb{F}_2} \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix} \implies \begin{array}{l} \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3 \\ \text{lin. dep.} \\ \text{over } \mathbb{F}_2 \end{array}$$

Example

$$\mathbf{v}_1 = [1\ 1\ 0], \quad \mathbf{v}_2 = [1\ 0\ 1], \quad \mathbf{v}_3 = [0\ 1\ 1]$$

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \xrightarrow{\text{RREF over } \mathbb{R}} \begin{bmatrix} 1 & 1 & 0 \\ 0 & -1 & 2 \\ 0 & 0 & 2 \end{bmatrix} \Longrightarrow \begin{array}{l} \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3 \\ \text{lin. indep.} \\ \text{over } \mathbb{R} \end{array}$$

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \xrightarrow{\text{RREF over } \mathbb{F}_2} \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix} \Longrightarrow \begin{array}{l} \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3 \\ \text{lin. dep.} \\ \text{over } \mathbb{F}_2 \end{array}$$

- $\text{rank}_{\mathbb{R}}(A) = 3$, while $\text{rank}_{\mathbb{F}_2}(A) = 2$

Finite-Dimensional Vector Spaces

A vector space V over $\mathbb{F}$ is finite-dimensional if there is a *finite* set, S, of vectors in V such that $V = \text{span}(S)$.

- In this course, we deal with finite-dimensional vector spaces only.

Finite-Dimensional Vector Spaces

A vector space V over $\mathbb{F}$ is finite-dimensional if there is a *finite* set, S, of vectors in V such that $V = \text{span}(S)$.

- In this course, we deal with finite-dimensional vector spaces only.

Example: The vector space $\mathbb{F}[x]$, consisting of all polynomials in x taking coefficients from $\mathbb{F}$, is not finite-dimensional!

Basis

Let V be a (finite-dimensional) vector space over a field $\mathbb{F}$.

A set of vectors that is linearly independent over $\mathbb{F}$ and that also spans V is called a basis of V.

Examples:

- $V = \mathbb{F}^n$ always has the standard basis

  $$\mathbf{e}_1 = [1\,0\,0\,\cdots\,0],\; \mathbf{e}_2 = [0\,1\,0\,\cdots\,0],\; \ldots,\; \mathbf{e}_n = [0\,0\,\cdots\,0\,1].$$

  Of course, other bases also exist: e.g.,
  $\mathbf{e}_1,\;\; \mathbf{e}_1 + \mathbf{e}_2,\;\; \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3,\; \ldots,\;\; \mathbf{e}_1 + \mathbf{e}_2 + \cdots + \mathbf{e}_n$

Basis

Let V be a (finite-dimensional) vector space over a field $\mathbb{F}$.

A set of vectors that is linearly independent over $\mathbb{F}$ and that also spans V is called a basis of V.

Examples:

- $V = \mathbb{F}^n$ always has the standard basis

  $$\mathbf{e}_1 = [1\ 0\ 0\ \cdots\ 0],\ \ \mathbf{e}_2 = [0\ 1\ 0\ \cdots\ 0],\ \ \ldots,\ \ \mathbf{e}_n = [0\ 0\ \cdots\ 0\ 1].$$

  Of course, other bases also exist: e.g.,
  $\mathbf{e}_1,\ \ \mathbf{e}_1 + \mathbf{e}_2,\ \ \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3,\ \ldots,\ \ \mathbf{e}_1 + \mathbf{e}_2 + \cdots + \mathbf{e}_n$

- $\mathbb{F}_d[x]$: the vector space of polynomials over $\mathbb{F}$, in the indeterminate x, with degree $\leq d$

  Standard basis: $1,\ x,\ x^2,\ \ldots,\ x^d$

Basis Properties

Proposition B1:

Let $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ be a basis of a vector space V. Then, any $\mathbf{v} \in V$ can be uniquely expressed as a linear combination of $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$.

Basis Properties

Proposition B1:

Let $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ be a basis of a vector space V. Then, any $\mathbf{v} \in V$ can be uniquely expressed as a linear combination of $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$.

Proof:

- Since $\mathbf{b}_1, \ldots, \mathbf{b}_n$ spans V, any $\mathbf{v} \in V$ can be expressed as a linear combination of $\mathbf{b}_1, \ldots, \mathbf{b}_n$.
- Suppose that

$$\mathbf{v} = \alpha_1 \cdot \mathbf{b}_1 + \alpha_2 \cdot \mathbf{b}_2 + \cdots + \alpha_n \cdot \mathbf{b}_n \tag{2}$$

$$\text{and} \quad \mathbf{v} = \alpha_1' \cdot \mathbf{b}_1 + \alpha_2' \cdot \mathbf{b}_2 + \cdots + \alpha_n' \cdot \mathbf{b}_n \tag{3}$$

  Then, subtracting (3) from (2), we obtain

$$\mathbf{0} = (\alpha_1 - \alpha_1') \cdot \mathbf{b}_1 + (\alpha_2 - \alpha_2') \cdot \mathbf{b}_2 + \cdots + (\alpha_n - \alpha_n') \cdot \mathbf{b}_n.$$

- But $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ are linearly independent; so we must have $\alpha_j - \alpha_j' = 0$ for all j, i.e., $\boxed{\alpha_j = \alpha_j' \text{ for all } j}$.

Dimension

Proposition B2:

Let S be a set of vectors that spans a vector space V, and let T be a linearly independent set of vectors from V. Then, $|S| \geq |T|$.

Dimension

Proposition B2:

Let S be a set of vectors that spans a vector space V, and let T be a linearly independent set of vectors from V. Then, $|S| \geq |T|$.

Theorem:

All bases of a vector space have the same cardinality (i.e., size).

Dimension

Proposition B2:

Let S be a set of vectors that spans a vector space V, and let T be a linearly independent set of vectors from V. Then, $|S| \geq |T|$.

Theorem:

All bases of a vector space have the same cardinality (i.e., size).

Proof: Let B_1 and B_2 be two bases for V.

- As B_1 spans V and B_2 is a lin. indep. set, we have $|B_1| \geq |B_2|$.
- As B_2 spans V and B_1 is a lin. indep. set, we have $|B_2| \geq |B_1|$.

Hence, $|B_1| = |B_2|$. $\square$

Dimension

Proposition B2:

Let S be a set of vectors that spans a vector space V, and let T be a linearly independent set of vectors from V. Then, $|S| \geq |T|$.

Theorem:

All bases of a vector space have the same cardinality (i.e., size).

Proof: Let B_1 and B_2 be two bases for V.

- As B_1 spans V and B_2 is a lin. indep. set, we have $|B_1| \geq |B_2|$.
- As B_2 spans V and B_1 is a lin. indep. set, we have $|B_2| \geq |B_1|$.

Hence, $|B_1| = |B_2|$. $\square$

The no. of elements in any basis of a vector space V over a field $\mathbb{F}$ is called the dimension of V; denoted by $\dim_{\mathbb{F}}(V)$ or $\dim(V)$.

Basis Properties

Proposition B3:

Let V be a n-dimensional vector space, i.e., $\dim(V) = n$.

(i). If $\mathbf{v}_1, \ldots, \mathbf{v}_m$ is lin. indep., then $m \leq n$.

(ii). If $\mathbf{v}_1, \ldots, \mathbf{v}_m$ spans V, then $m \geq n$.

Proof: Take any basis B of V, so that $|B| = n$, and apply Proposition B2. $\square$

Basis Properties

Proposition B3:

Let V be a n-dimensional vector space, i.e., $\dim(V) = n$.

(i). If $\mathbf{v}_1, \ldots, \mathbf{v}_m$ is lin. indep., then $m \leq n$.

(ii). If $\mathbf{v}_1, \ldots, \mathbf{v}_m$ spans V, then $m \geq n$.

Proof: Take any basis B of V, so that $|B| = n$, and apply Proposition B2. $\square$

Thus,

- a basis is a maximal linearly independent set;
- a basis is a minimal spanning set.

Basis Properties

Proposition B4:

Any linearly independent set of vectors from V can be extended (by adding more vectors if necessary) to a basis of V.

Basis Properties

Proposition B4:

Any linearly independent set of vectors from V can be extended (by adding more vectors if necessary) to a basis of V.

Proof: Let $\mathbf{v}_1, \ldots, \mathbf{v}_m$ be a lin. indep. set, and let $n = \dim(V)$.

- If $m = n$, then we already have a maximal lin. indep. set, i.e., a basis.
- So assume $m < n$. In this case, for $j = m, m+1, \ldots, n-1$, do the following:
  - Since $\mathbf{v}_1, \ldots, \mathbf{v}_j$ is not a spanning set, find a $\mathbf{u} \in V$ such that $\mathbf{u} \notin \operatorname{span}(\mathbf{v}_1, \ldots, \mathbf{v}_j)$.
  - Set $\mathbf{v}_{j+1} := \mathbf{u}$.

Then, $\mathbf{v}_1, \ldots, \mathbf{v}_n$ is a maximal lin. indep. set, i.e., a basis. $\square$

The Rank-Nullity Theorem

Recall that, for a matrix A over $\mathbb{F}$,

- $\text{rank}_{\mathbb{F}}(A) \triangleq$ max. no. of lin. indep. row vectors of A
- $\text{rowspace}(A) \triangleq \text{span}_{\mathbb{F}}(\text{row vectors of } A)$

Hence, $\boxed{\text{rank}_{\mathbb{F}}(A) = \dim_{\mathbb{F}}(\text{rowspace}(A))}$

The Rank-Nullity Theorem

Recall that, for a matrix A over $\mathbb{F}$,

- $\text{rank}_{\mathbb{F}}(A) \triangleq$ max. no. of lin. indep. row vectors of A
- $\text{rowspace}(A) \triangleq \text{span}_{\mathbb{F}}(\text{row vectors of } A)$

Hence, $\boxed{\text{rank}_{\mathbb{F}}(A) = \dim_{\mathbb{F}}(\text{rowspace}(A))}$

Definition: $\text{nullity}_{\mathbb{F}}(A) \triangleq \dim_{\mathbb{F}}(\text{nullspace}(A))$

The Rank-Nullity Theorem

Recall that, for a matrix A over $\mathbb{F}$,

- $\text{rank}_{\mathbb{F}}(A) \triangleq$ max. no. of lin. indep. row vectors of A
- $\text{rowspace}(A) \triangleq \text{span}_{\mathbb{F}}(\text{row vectors of } A)$

Hence, $\boxed{\text{rank}_{\mathbb{F}}(A) = \dim_{\mathbb{F}}(\text{rowspace}(A))}$

Definition: $\text{nullity}_{\mathbb{F}}(A) \triangleq \dim_{\mathbb{F}}(\text{nullspace}(A))$

Theorem (The Rank-Nullity Theorem):
Let A be an $m \times n$ matrix over a field $\mathbb{F}$. Then,

$$\text{rank}_{\mathbb{F}}(A) + \text{nullity}_{\mathbb{F}}(A) = n.$$

Equivalently,

$$\dim_{\mathbb{F}}(\text{rowspace}(A)) + \dim_{\mathbb{F}}(\text{nullspace}(A)) = n.$$