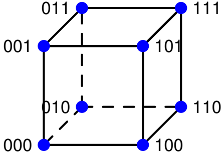
Week 11: Finite Fields and Vector Spaces (Textbook Chapter 12)

Prof. Michael Gastpar

Slides by Prof. M. Gastpar and Prof. em. B. Rimoldi

EPFL

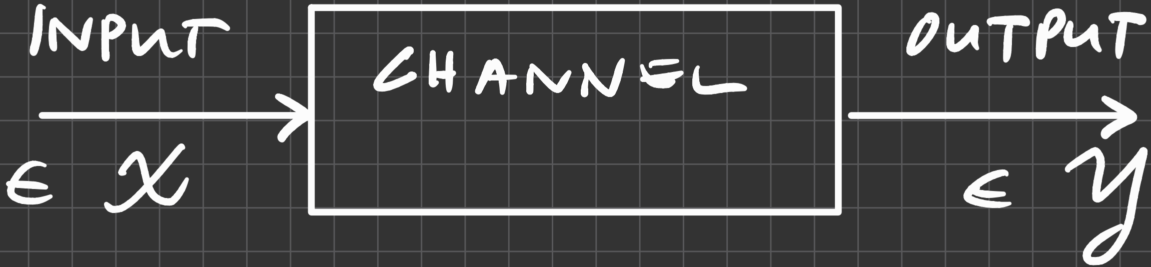
Spring Semester 2025



Outline

- Introduction and Organization
- Entropy and Data Compression
- Cryptography
- Channel Coding
    - Error Detection and Error Correction
    - Finite Fields and Vector Spaces
    - Linear Codes
    - Reed Solomon Codes
    - Summary of Chapter 3

LAST WEEK



INPUT

CHANNEL

OUTPUT

$\in \mathcal{X}$

$\in \mathcal{Y}$

STRATEGY: "CODE"

$$\mathcal{C} = \{ \underline{c}_1, \underline{c}_2, \dots, \underline{c}_M \}$$

SUBSET OF ALL POSSIBLE SEQUENCES.

$$\mathcal{C} \subseteq \mathcal{X}^n$$

$$|\mathcal{C}| = M \text{ codewords}$$

$$= |\mathcal{X}|^k \text{ codewords}$$

Ex: $\mathcal{C} = \{ (0\ 0\ 0\ 0 \cdots\ 0),$
$(1\ 1\ 1\ 1 \ldots\ 1) \}$

"REPETITION CODE"

$M = 2$

$k = 1$

$$\mathcal{C} \subseteq \mathcal{X}^n$$

$$|\mathcal{C}| = M \text{ codewords}$$

$$= |\mathcal{X}|^k \text{ codewords}$$

Rate : $0 \leq \dfrac{k}{n} \leq 1$

Minimum Distance:

$$d_{\min}(\mathcal{C}) := \min_{i \neq j} d(\underline{c}_i, \underline{c}_j)$$

$$\mathcal{C} \subseteq \mathcal{X}^n$$

$|\mathcal{C}| = |\mathcal{X}|^k$ codewords

Minimum Distance:

$$d_{min}(\mathcal{C}) := \min_{i \neq j} d(\underline{c}_i, \underline{c}_j)$$

Singleton's Bound:

$$d_{min} \leq n - k + 1$$

Ex: $\mathcal{C} = \{ (\overbrace{0\ 0\ 0\ 0 \cdots 0}^{n}), (1\ 1\ 1\ 1 \cdots 1) \}$

"REPETITION CODE"

$\mathcal{X} = \{0, 1\}$

$k = 1$

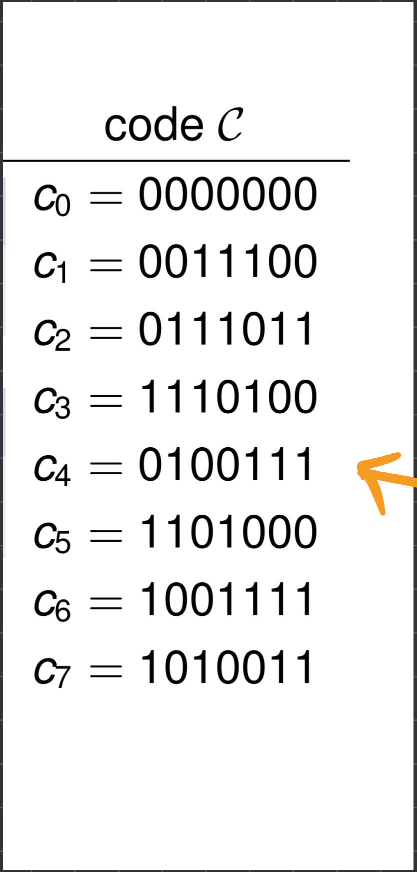
$d_{min} = n$

SINGLETON:

$n \leq n - 1 + 1$

$= n$

$\Rightarrow$ MDS code!



code $\mathcal{C}$
$c_0 = 0000000$
$c_1 = 0011100$
$c_2 = 0111011$
$c_3 = 1110100$
$c_4 = 0100111$
$c_5 = 1101000$
$c_6 = 1001111$
$c_7 = 1010011$

$$c_1 \oplus c_2$$

$$= (0,0,1,1,1,0,0)$$

$$\oplus (0,1,1,1,0,1,1)$$

$$\overline{}$$

$$(0,1,0,0,1,1,1)$$

$$= c_4$$

Finite Fields, Vector Spaces, and Linear Codes

- Our next goal is to bring **algebraic structure** into code design and decoding.

- Encoding, decoding, and computing d_{min} become easier if the code forms a vector space.

- Vector spaces are defined over fields.

- For coding, we care about **finite** fields.

Definition (Commutative group)

A **commutative group** (also called Abelian group) is a set G endowed with a binary operation $\star$ that combines any two elements a and b to form another element denoted $a \star b$. The group operation $\star$ must satisfy the following five axioms:

- (Closure:) For all $a, b \in G$, the result of the operation $a \star b$ is also in G.
- (Associativity:) For all $a, b \in G$, $a \star (b \star c) = (a \star b) \star c$.
- (Identity element:) There exists an element $e \in G$, such that for all $a \in G$, $a \star e = e \star a = a$.
- (Inverse element:) For all $a \in G$, there exists $b \in G$, such that $a \star b = b \star a = e$.
- (Commutativity:) For all $a, b \in G$, $a \star b = b \star a$.

FIELD

FRENCH: 'CORPS'

$(K, +, \times)$ SUCH THAT

(1) $(K, +)$: COMMUTATIVE GROUP

"ADDITIVE ORDER" IDENTITY ELEMENT: 0

(2) $(K \setminus \{0\}, \times)$: COMMUTATIVE GROUP

"MULTIPLICATIVE ORDER" IDENTITY ELEMENT: 1

(3) DISTRIBUTIVE LAW:

$$a \times (b + c) = a \times b + a \times c$$

DEFINITION OF A FIELD

A *field* is the triplet $(\mathcal{K}, +, \times)$ where $\mathcal{K}$ is a set, and $+$, $\times$ are two binary operators called addition and multiplication, such that the following axioms hold:

1. **Associativity**: $\forall a, b, c \in \mathcal{K}$,

$$a + (b + c) = (a + b) + c$$
$$a \times (b \times c) = (a \times b) \times c$$

2. **Commutativity**: $\forall a, b \in \mathcal{K}$,

$$a + b = b + a$$
$$a \times b = b \times a$$

3. **Identity under** $+$: $\mathcal{K}$ contains an element, typically denoted by 0, such that $\forall a \in \mathcal{K}$,

$$a + 0 = a$$

4. **Inverse under** $+$: $\forall a \in \mathcal{K}$, there exists a unique $b \in \mathcal{K}$ such that

$$a + b = 0$$

   b is the additive inverse of a, typically denoted by $-a$.

5. **Identity under** $\times$: $\mathcal{K}$ contains an element, typically denoted by 1, such that $\forall a \in \mathcal{K}$,
$$a \times 1 = a$$

6. **Inverse under** $\times$: $\forall a \in \mathcal{K}$, $a \neq 0$, there exists a unique $b \in \mathcal{K}$, such that
$$a \times b = 1$$
b is the multiplicative inverse of a, typically denoted by a^{-1}.

7. **Distributivity**: $\forall a, b, c \in \mathcal{K}$,
$$a \times (b + c) = (a \times b) + (a \times c).$$

Some remarks:

- If $\mathcal{K}$ is finite, then $(\mathcal{K}, +, \times)$ is a *finite field*.
- Instead of $(+, \times)$ the binary operations of a field may be denoted by $(+, \cdot)$, $(\star, \circ)$, $(\oplus, \wedge)$, $\ldots$
- ab is a short hand for $a \times b$.
- $a - b$ is a short hand for $a + (-b)$.
- If n is a positive integer and $b \in \mathcal{K}$, nb means $\underbrace{b + b + \cdots + b}_{n \text{ times}}$.
- If k is a positive integer and $a \in \mathcal{K}$, a^k means $\underbrace{a \times a \times \cdots \times a}_{k \text{ times}}$.

Example

Well-known examples of fields:

- $(\mathbb{R}, +, \cdot)$, the (field of) real numbers
- $(\mathbb{C}, +, \cdot)$, the (field of) complex numbers
- $(\mathbb{Q}, +, \cdot)$, the (field of) rational numbers

Well-known examples that are *not* fields:

- $(\mathbb{N}, +, \cdot)$, the (set of) non-negative integers
- $(\mathbb{Z}, +, \cdot)$, the (set of) integers

EXERCISE

Are these finite fields?

- $(\mathbb{Z}/16\mathbb{Z}, +, \cdot)$, the integers modulo 16
- $(\mathbb{Z}/17\mathbb{Z}, +, \cdot)$, the integers modulo 17

SOLUTION

- $(\mathbb{Z}/16\mathbb{Z}, +, \cdot)$ is not a field because some non-zero elements do not have the multiplicative inverse.
- $(\mathbb{Z}/17\mathbb{Z}, +, \cdot)$ is a field because all its non-zero elements have an inverse.

USEFULNESS OF FINITE FIELDS

Any algebraic manipulation in a finite field behaves similarly to $\mathbb{R}$. For instance:

- we can solve equations
- we can do linear algebra (define vectors and matrices, compute determinants, etc.)

EXAMPLES OF CALCULATIONS OVER FINITE FIELDS

The following statements can be deduced from the field axioms:

- if $x \in \mathcal{K} \setminus 0$, then $x \cdot y = 0 \Rightarrow y = 0$
- $\forall x \in \mathcal{K}, 0 \cdot x = 0$
- $\forall x \in \mathcal{K}, k \in \mathbb{N}, x^k = 0 \Rightarrow x = 0$
- $(-1) \cdot x = -x$
- $(a+b)^2 = a^2 + 2ab + b^2$

$$= (a+b)\cdot(a+b) = a^2 + ab + ba + b^2$$

EXAMPLE CALCULATIONS (DETAILS)

1) We must have $0 \cdot x = 0, \ \forall x \in K.$

PROOF:

$$\underbrace{0 \cdot x}_{a} = (0+0) \cdot x$$

$$= \underbrace{0 \cdot x}_{a} + \underbrace{0 \cdot x}_{a}$$

$$a = a + a$$

$$\Rightarrow a = 0$$

EXAMPLE CALCULATIONS (DETAILS)

2) IF $x \cdot y = 0$

THEN $x=0$ OR $y=0$ OR $(x=0, y=0)$.

PROOF: INSTEAD PROVE:

IF $x \neq 0$ AND $y \neq 0$

THEN $x \cdot y \neq 0$.

Example

Find the solution of $3x + 6 = 4$ in $(\mathbb{Z}/7\mathbb{Z}, +, \cdot)$.

Solution

$$\begin{aligned} 3x + 6 = 4 &\Leftrightarrow 3x + 6 + (-6) = 4 + (-6) \\ &\Leftrightarrow 3x = 5 \\ &\Leftrightarrow 3^{-1} \cdot 3x = 3^{-1} \cdot 5 \\ &\Leftrightarrow x = 5 \cdot 5 = 25 = 4 \end{aligned}$$

Example

In $(\mathbb{Z}/7\mathbb{Z}, +, \cdot)$, we have

$$\underbrace{1 + 1 + \cdots + 1}_{\text{7 times}} = 0$$

Hence, the order of 1 with respect to $+$ is 7.

CHARACTERISTIC OF A FINITE FIELD

- Every field contains the special number 1.
- For a finite field, the order of 1 with respect to $+$ is a prime number *p* called the field characteristic.

EXAMPLE

Let *p* be prime, so that $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ is a finite field. Its characteristic is *p*.

EXERCISE

Can you prove that the characteristic of a finite field $(F, +, \cdot)$ is a prime number?

Hint: $(F, +)$ is a commutative group, hence there exists a smallest integer $m > 1$ such that

$$\underbrace{1 + 1 + \cdots + 1}_{m \text{ times}} = 0.$$

PROOF BY CONTRADICTION: $m = ab$

$$\underbrace{1 + \dots + 1}_{m \text{ times}} = \underbrace{(1 + 1 \cdot\cdot 1)}_{a \text{ times}} \cdot \underbrace{(1 + 1 \cdots 1)}_{b \text{ times}}$$

SOLUTION

- Let m be the smallest number such that $\underbrace{1+1+\cdots+1}_{m \text{ times}} = 0$
- Suppose that $m = ab$ with $a > 1$ and $b > 1$
- One of the field axioms (distributivity) implies

$$\underbrace{(1+1+\cdots+1)}_{a \text{ times}} \cdot \underbrace{(1+1+\cdots+1)}_{b \text{ times}} = 0$$

- Hence, either

$$\underbrace{1+1+\cdots+1}_{a \text{ times}} = 0 \quad \text{or} \quad \underbrace{1+1+\cdots+1}_{b \text{ times}} = 0$$

- Contradiction: Hence the smallest m is a prime number.

□

Definition

An **isomorphism** between two finite fields $\mathbb{F} = (\mathcal{F}, +, \times)$ and $\mathbb{K} = (\mathcal{K}, \oplus, \otimes)$ is a bijection

$$\phi : \mathcal{F} \to \mathcal{K}$$

such that, for all $a, b \in \mathcal{F}$,

$$\begin{aligned} \phi(a + b) &= \phi(a) \oplus \phi(b) \\ \phi(a \times b) &= \phi(a) \otimes \phi(b). \end{aligned}$$

We say $\mathbb{F}$ and $\mathbb{K}$ are **isomorphic** if there exists an isomorphism between them.

PROPERTIES OF FINITE FIELDS

THEOREM (TEXTBOOK THEOREM 12.1, WITHOUT PROOF)

1. The cardinality of a finite field is an integer power of its characteristic. (Hence all finite fields have cardinality p^m for some prime p and some positive integer m.)

2. All finite fields of the same cardinality are isomorphic.

3. For every prime number p and positive integer m, there is a finite field of cardinality p^m.

EVARISTE
GALOIS

(1811 —

EVARISTE GALOIS

(1811 — 1832)

USEFUL FOR US TO KNOW

- $(\mathbb{Z}/k\mathbb{Z}, +, \cdot)$ is a finite field iff $k = p$ for some prime p.
- A field that has p elements is isomorphic to $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$.
- In $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$, we know how to add and multiply without tables.
- A field with p^m elements is denoted by $\mathbb{F}_{p^m}$.
- Rather than developing the theory that allows us to add and multiply in $\mathbb{F}_{p^m}$, in most of our examples we stick to $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$, keeping in mind that all we do generalizes to arbitrary finite fields.

EXAMPLE ($\mathbb{F}_2$)

The smallest finite field is $(\mathbb{Z}/2\mathbb{Z}, +, \cdot)$, denoted by $\mathbb{F}_2$. Its elements are 0 and 1 and the operations are

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

$$\boxed{\mathbb{F}_3} \quad \rightsquigarrow \quad (\mathbb{Z}/3\mathbb{Z}, +, \cdot)$$

$$\mathbb{F}_3 = \{ 0, \ 1, \ 2 \}$$

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

EXERCISE ($\mathbb{F}_3$)

Define the finite field of cardinality 3.

SOLUTION ($\mathbb{F}_3$)

$\mathbb{F}_3$ is isomorphic to $(\mathbb{Z}/3\mathbb{Z}, +, \cdot)$, with addition and multiplication defined as follows:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$$\boxed{\mathbb{F}_4} = \{0, 1, a, b\}$$

$$= \mathbb{F}_{2^2} \Rightarrow \text{CHARACTERISTIC } 2$$

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

x	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Example ($\mathbb{F}_4$)

Because 4 is of the form p^m, there exists a finite field with 4 elements.

Let us denote the elements $0, 1, a, b$.

The axioms associated to 0 and 1 imply

$+$	0	1	a	b
0	0	1	a	b
1	1			
a	a			
b	b			

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a		
b	0	b		

Example (cont.)

The field characteristic is $p = 2$, therefore $1 + 1 = 0$.
Similarly, $x + x = x \cdot (1 + 1) = x \cdot 0 = 0$ for all x, so we can complete the diagonal of the $+$ table:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

Finally, we can complete the remaining blanks knowing that each element has to show up exactly once in each row and each column.

Example (cont.)

Similarly, the $\cdot$ table is completed using the fact that $\mathbb{F}_4^* = (\{1, a, b\}, \cdot)$ is a group.

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Exercise

Is $\mathbb{F}_4$ isomorphic to $(\mathbb{Z}/4\mathbb{Z}, +, \cdot)$?

Solution

It cannot be, because $(\mathbb{Z}/4\mathbb{Z}, +, \cdot)$ is not a field.

Other reason: in $\mathbb{F}_4$, the characteristic is $p = 2$. Hence $a + a = 0$ for all $a \in \mathbb{F}_4$. Not the case for $(\mathbb{Z}/4\mathbb{Z}, +, \cdot)$.

Example (group isomorphism?)

Let $(\mathbb{F}_4, +)$ be $\mathbb{F}_4$ without multiplication. Is $(\mathbb{F}_4, +)$ isomorphic to $((\mathbb{Z}/2\mathbb{Z})^2, +)$?

Recall: $(\mathbb{Z}/2\mathbb{Z})^2 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ with addition component-wise over $(\mathbb{Z}/2\mathbb{Z}, +)$.

Solution

The answer is YES: both are finite commutative groups. In both cases, all nonzero elements have order 2. Since they have the same set of orders, they are isomorphic.

The isomorphism is: $0 \Rightarrow 00$, $1 \Rightarrow 11$, $a \Rightarrow 01$, $b \Rightarrow 10$
or $0 \Rightarrow 00$, $1 \Rightarrow 11$, $a \Rightarrow 10$, $b \Rightarrow 01$.

Example (field isomorphism?)

Is $\mathbb{F}_4$ isomorphic to $((\mathbb{Z}/2\mathbb{Z})^2, +, \cdot)$?

Solution

The answer is NO, because $((\mathbb{Z}/2\mathbb{Z})^2, +, \cdot)$ is not a field: $(0, 1)$ is a non-zero element that has no multiplicative inverse.

However, since they have the same number of elements, we can redefine the multiplication of $((\mathbb{Z}/2\mathbb{Z})^2, +, \cdot)$ so that the result is a field. It suffices to use the multiplication table from $\mathbb{F}_4$ and substitute $0 \Rightarrow 00$, $1 \Rightarrow 11$, $a \Rightarrow 01$, $b \Rightarrow 10$. (We are just re-labeling the elements of a previously established field.)

Solution (cont.)

$\mathbb{F}_4$

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

$((\mathbb{Z}/2\mathbb{Z})^2, +, \otimes)$

$+$	00	11	01	10
00	00	11	01	10
11	11	00	10	01
01	01	10	00	11
10	10	01	11	00

$\otimes$	00	11	01	10
00	00	00	00	00
11	00	11	01	10
01	00	01	10	11
10	00	10	11	01

$$\boxed{\mathbb{F}_5} = (\mathbb{Z}/5\mathbb{Z}, +, \cdot)$$ ✓

$\boxed{\mathbb{F}_6}$ = DOES NOT EXIST.

FINITE-DIMENSIONAL VECTOR SPACES

This is a review, since you *should* know everything that we need from linear algebra. (MATH-111e.)

We review only what we need for the chapter on linear block codes (next week).

For missing proofs, see e.g.

- Sheldon Axler, “Linear Algebra Done Right”, Springer
- Tom M. Apostol, “Linear Algebra: A First Course with Applications to Differential Equations”, Wiley.
- David C. Lay, “ Linear Algebra and Its Applications”, Addison-Wesley.

DEFINITION (VECTOR SPACE)

A nonempty set V is said to be a *vector space* over a finite field $\mathbb{F}$ if:

I. there exists an operation called addition that associates to each pair $\vec{u}, \vec{v} \in V$ a vector $\vec{u} + \vec{v} \in V$ called the sum of $\vec{u}$ and $\vec{v}$;

II. there exists an operation called scalar multiplication that associates to each $\alpha \in \mathbb{F}$ and $\vec{v} \in V$ a new vector $\alpha\vec{v} \in V$ called the product of α and $\vec{v}$;

and these operations satisfy the following axioms:

Definition (cont.)

- $\vec{u} + \vec{v} = \vec{v} + \vec{u}$ for all $\vec{u}, \vec{v} \in V$;
- $(\vec{u} + \vec{v}) + \vec{w} = \vec{u} + (\vec{v} + \vec{w})$ for all $\vec{u}, \vec{v}, \vec{w} \in V$;
- There exists an element $\vec{0} \in V$ such that $\vec{0} + \vec{v} = \vec{v}$ for all $\vec{v} \in V$;
- For all $\vec{v} \in V$, there exists an element $-\vec{v} \in V$ such that $\vec{v} + (-\vec{v}) = \vec{0}$;
- $\alpha(\vec{u} + \vec{v}) = \alpha\vec{u} + \alpha\vec{v}$ for all $\alpha \in \mathbb{F}$ and all $\vec{u}, \vec{v} \in V$;
- $(\alpha + \beta)\vec{v} = \alpha\vec{v} + \beta\vec{v}$ for all $\alpha, \beta \in \mathbb{F}$ and all $\vec{v} \in V$;
- $\alpha(\beta\vec{v}) = (\alpha\beta)\vec{v}$ for all $\alpha, \beta \in \mathbb{F}$ and all $\vec{v} \in V$;
- $1\vec{v} = \vec{v}$ for all $\vec{v} \in V$, where 1 is the (multiplicative) identity in $\mathbb{F}$.

Definition (equivalent, compact definition)

$(V, +, \times)$ is a vector space over a field $\mathbb{F}$ if:

- $(V, +)$ is a commutative (abelian) group;
- The binary operator $\times$ is between an element of V and one of $\mathbb{F}$, with the following properties:
  - (associativity) $\forall \vec{v} \in V$ and $\alpha, \beta \in \mathbb{F}$, $\alpha(\beta\vec{v}) = (\alpha\beta)\vec{v}$;
  - (identity) $1\vec{v} = \vec{v}$;
  - (distributivity) $\alpha(\vec{u} + \vec{v}) = \alpha\vec{u} + \alpha\vec{v}$ and $(\alpha + \beta)\vec{v} = \alpha\vec{v} + \beta\vec{v}$.

THE MOST IMPORTANT SPECIAL CASE

- $V = \mathbb{F}^n$

$$= \{ (v_1, v_2, .., v_n) : v_i \in \mathbb{F} \}$$

- VECTOR ADDITION IS DEFINED AS

$$(v_1, .., v_n) + (u_1, .., u_n)$$
$$= (v_1 + u_1, .., v_n + u_n)$$

- SCALAR MULTIPLY:

$$\alpha(v_1, .. v_n) = (\alpha v_1, .., \alpha v_n)$$

Example (vector space)

For every field $\mathbb{F}$ and every positive integer n, $V = \mathbb{F}^n$ is the vector space of n-tuples.

Vector-addition is done component-wise according to the addition rule of $\mathbb{F}$:

$$(u_1, \ldots, u_n) + (v_1, \ldots, v_n) = (u_1 + v_1, \ldots, u_n + v_n)$$

Multiplication of a vector by a scalar is also done component-wise according to the multiplication rule of $\mathbb{F}$:

$$\alpha(v_1, \ldots, v_n) = (\alpha v_1, \ldots, \alpha v_n)$$

Example (vector space)

For every field $\mathbb{F}$ and positive integer n, the set of polynomials of the form $p(x) = a_0 + a_1 x + \cdots + a_n x^n$ with coefficients $a_0, \ldots, a_n \in \mathbb{F}$ is a vector space, where the addition of polynomials and the multiplication of a polynomial by a scalar are done according to the "usual rules".

$$p_1(x) = a_0 + a_1 x + \ldots + a_n x^n$$

$$p_2(x) = b_0 + b_1 x + \ldots + b_n x^n$$

$$p_1(x) + p_2(x) = a_0 + b_0 + (a_1 + b_1)x + \ldots + (a_n + b_n)x^n$$

$$= c_0 + c_1 x + \ldots + c_n x^n$$

Example (vector space)

Let p be a prime number and consider the field $\mathbb{F} = (\mathbb{Z}/p\mathbb{Z}, +, \cdot)$.

Let n be a positive integer and consider the vector space $V = \mathbb{F}^n$. This is a vector space over (the finite field) $\mathbb{F}$.

It turns out that for all vector spaces of the form $V = \mathbb{F}^n$, $\mathbb{F}$ finite field, we can define a multiplication among vectors that fulfills all the axioms of a field.

Hence $\mathbb{F}^n$, where $\mathbb{F} = (\mathbb{Z}/p\mathbb{Z}, +, \cdot)$, is a vector space that can be made into the finite field $\mathbb{F}_{p^n}$.

In fact it has p^n elements, and its characteristic is p, and there is only one such field (up to isomorphism).

All finite fields can be put in this form. We have already seen $((\mathbb{Z}/2\mathbb{Z})^2, +, \cdot)$.

We are not proving the above result, because we will not make use of it in this course.

SUBSPACES

V : vector space over $\mathbb{F}$

$S \subseteq V$ IS CALLED A **SUBSPACE** IF

(1) $\vec{s}_1, \vec{s}_2 \in S$

$\Rightarrow \quad \vec{s}_1 + \vec{s}_2 \in S$

(2) $\vec{s} \in S \Rightarrow \alpha \vec{s} \in S, \quad \forall \alpha \in \mathbb{F}.$

$\Rightarrow \quad \vec{0} \in S$

OBSERVATION:

A SUBSPACE IS ITSELF A VECTOR SPACE.

$$\boxed{\text{YESTERDAY}}$$

VECTOR SPACE $\mathbb{F}_p^n$

$$\vec{v} = (v_1, v_2, \dots, v_n)$$

$$v_i \in \mathbb{F}_p$$

↖ FINITE FIELD.

SUBSPACE OF A VECTOR SPACE

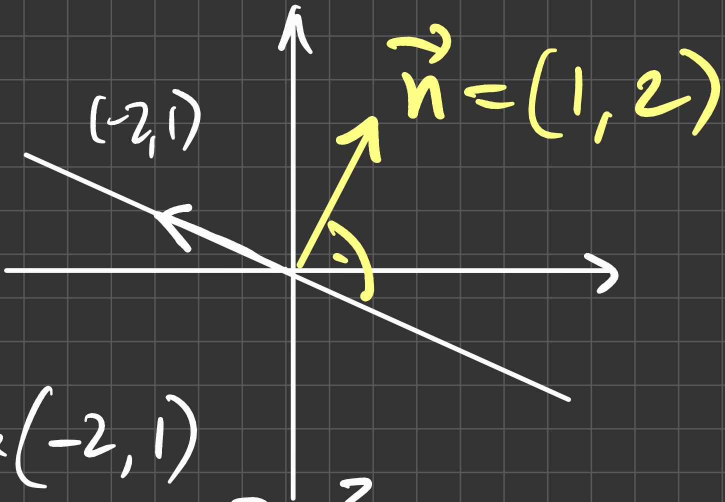
If V is a vector space and $S \subseteq V$ with the property that S is closed under vector addition and multiplication by a scalar, then S is itself a vector space.

(Closure of S with respect to vector addition and multiplication of a vector by a scalar are required by two axioms. Verify for yourself that the other axioms that S has to fulfill to be a vector space are automatically inherited from V.)

We call such an S a **subspace** of V.

__Ex:__ $V = \mathbb{R}^2$

Fix $\vec{v} = (-2, 1)$



$$S := \{ \vec{s} \in V : \vec{s} = a(-2,1) \text{ for all } a \in \mathbb{R} \}$$

$$= \{ \vec{s} \in V : \vec{s} \cdot \vec{n} = 0 \}$$

$$= \{ \vec{s} \in V : s_1 + 2s_2 = 0 \}$$

TO CHECK: ANY $\vec{s} \in S$ CAN BE WRITTEN AS

$$\vec{s} = \Big(\underbrace{-2\alpha}_{\substack{\downarrow \\ s_1}}, \underbrace{\alpha}_{\substack{\downarrow \\ s_2}}\Big)$$

EVERY $\vec{s}$ IN S satisfies

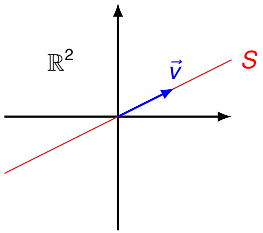
$$0 = s_2 + 2s_2 = -2\alpha + 2\alpha = 0 \checkmark$$

Example

Let $V = \mathbb{R}^2$, $\vec{v} \in V$, and define $S = \{\vec{s} \in V : \vec{s} = a\vec{v}, a \in \mathbb{R}\}$.

- If $\vec{u} \in S$, then $b\vec{u} = b(a\vec{v}) = (ba)\vec{v} \in S$ for all $b \in \mathbb{R}$
- If $\vec{u}, \vec{w} \in S$, then $\vec{u} + \vec{w} = a_1\vec{v} + a_2\vec{v} = (a_1 + a_2)\vec{v} \in S$

Hence S is a subspace of V.



EXAMPLE

Let $V = \mathbb{F}_7^3$ and define $S = \{(x_1, x_2, x_3) : x_i \in \mathbb{F}_7$ and $x_1 + 2x_2 + 3x_3 = 0\}$.

S is a subspace of V. (Be sure that you see why.)

NB: there are four kinds of operations in a vector space:

1. scalar addition,
2. scalar multiplication,
3. vector addition,
4. multiplication of a vector with a scalar.

The one used is always clear from the context.

For instance, it is clear that the above equation $x_1 + 2x_2 + 3x_3 = 0$ involves additions and multiplications in $\mathbb{F}_7$.

LET US VERIFY THIS

LET $\vec{x}, \vec{y} \in S$.

(1) IS $a\vec{x} \in S$?

(2) IS $\vec{x} + \vec{y} \in S$?

(1) $$ax_1 + 2ax_2 + 3ax_3$$
$$= a\underbrace{(x_1 + 2x_2 + 2x_3)}_{> 0} = 0$$

(2) $$(x_1 + y_1) + 2(x_2 + y_2) + 3(x_3 + y_3)$$

$$= \underbrace{x_1 + 2x_2 + 3x_3}_{=0} + \underbrace{y_1 + 2y_2 + 3y_3}_{=0}$$

$$= 0.$$

✓

WE WILL USE YELLOW WHENEVER WE SPECIFY A SUBSPACE IN THIS FASHION, VIA HOMOGENEOUS EQUATIONS.

↓

A linear combination of a **list** $(\vec{v}_1, \ldots, \vec{v}_n)$ of vectors in V is a vector of the form $\sum_{i=1}^{n} \lambda_i \vec{v}_i$, where $\lambda_1, \ldots, \lambda_n \in \mathbb{F}$.

The set of all linear combinations of $(\vec{v}_1, \ldots, \vec{v}_n)$ is called the **span** of $(\vec{v}_1, \ldots, \vec{v}_n)$, denoted $\mathsf{span}(\vec{v}_1, \ldots, \vec{v}_n)$.

If $\mathsf{span}(\vec{v}_1, \ldots, \vec{v}_n) = V$, we say that $(\vec{v}_1, \ldots, \vec{v}_n)$ **spans** V.

A vector space is called **finite-dimensional** if some list of vectors in it spans the whole space. (A list has finite length by definition.)

The vectors $\vec{v}_i$, $i = 1, \ldots, n$ are said to be **linearly independent** iff $\sum_{i=1}^{n} \lambda_i \vec{v}_i = 0$ implies $\lambda_1 = \cdots = \lambda_n = 0$.

A **basis** of V is a list of vectors in V that is linearly independent and spans V.

Theorem

A list $(\vec{v}_1, \ldots, \vec{v}_n)$ of vectors in V is a basis of V iff every $\vec{v} \in V$ can be written uniquely in the form

$$\vec{v} = \sum_{i=1}^{n} \lambda_i \vec{v}_i$$

Exercise (Proof of $\Rightarrow$)

Prove that if $(\vec{v}_1, \ldots, \vec{v}_n)$ is a basis of V, then for every vector $\vec{v} \in V$, there is a unique set of coefficients $\lambda_1, \ldots, \lambda_n$, such that

$$\vec{v} = \sum_{i=1}^{n} \lambda_i \vec{v}_i.$$

THM

$\{\vec{v}_1, \dots, \vec{v}_n\}$ BASIS $\Rightarrow$ UNIQUE REPRESENTATION $\vec{v} = \lambda_1 \vec{v}_1 + \dots + \lambda_n \vec{v}_n$

PROOF: SUPPOSE (BY CONTRADICTION)

$$\underbrace{\left(\vec{v} =\right) \sum_{i=1}^{n} \lambda_i \vec{v}_i - \sum_{i=1}^{n} \beta_i \vec{v}_i}_{} = \vec{0}$$

$$= \sum_{i=1}^{n} \underbrace{(\lambda_i - \mu_i)}_{=0} \vec{v}_i = \vec{0}$$

$$\Rightarrow \lambda_i = \beta_i$$

$\square$

SOLUTION

$(\vec{v}_1, \ldots, \vec{v}_n)$ is a basis of V, hence it spans V (by definition), which means that every $\vec{v} \in V$ can be written as

$$\vec{v} = \sum_{i=1}^{n} \lambda_i \vec{v}_i.$$

We need to prove uniqueness. Suppose that $\sum_{i=1}^{n} \lambda_i \vec{v}_i = \sum_{i=1}^{n} \beta_i \vec{v}_i$.

Then $\sum_{i=1}^{n} \lambda_i \vec{v}_i - \sum_{i=1}^{n} \beta_i \vec{v}_i = 0$.

Using the axioms, we rewrite as $\sum_{i=1}^{n}(\lambda_i - \beta_i)\vec{v}_i = 0$.

The linear independence of the basis vectors implies $\lambda_i - \beta_i = 0$, i.e., $\lambda_i = \beta_i$ for all i. □

Exercise (Proof of $\Leftarrow$)

Prove that if every vector $\vec{v} \in V$ has a unique set of coefficients $\lambda_1, \ldots, \lambda_n$, such that

$$\vec{v} = \sum_{i=1}^{n} \lambda_i \vec{v}_i,$$

then $(\vec{v}_1, \ldots, \vec{v}_n)$ is a basis of V.

Solution

By assumption, $(\vec{v}_1, \dots, \vec{v}_n)$ spans V. It remains to be shown that the list $(\vec{v}_1, \dots, \vec{v}_n)$ is of linearly independent vectors.

Write the zero vector as $0 = \sum_{i=1}^{n} \lambda_i \vec{v}_i$. The uniqueness of the coefficients implies that $\lambda_i = 0$ for all i.

Hence the vectors $\vec{v}_1, \dots, \vec{v}_n$ are linearly independent. □

Theorem

Every spanning list in a vector space can be reduced to a basis of the vector space.

Proof (outline)

Remove all the zero-elements of the list.

Of the new list, remove the second element if it is in the linear span of the first. Repeat the same until we have a list in which the second element is not in the linear span of the first.

Of the new list, remove the third element if it is in the linear span of the first two.

Continue similarly.

The result is a list of vectors that span the vector space and are linearly independent (or else one vector can be written as the linear combination of vectors with smaller index). □

The above theorem implies that every finite-dimensional vector space has a basis.

THEOREM (WITHOUT PROOF)

Any two bases of a finite-dimensional vector space have the same length.

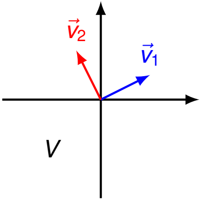
The **dimension** of a finite-dimensional vector space V, denoted by $\mathrm{dim}(V)$, is defined to be the length of any basis of V.

A FEW PROPERTIES OF THE DIMENSION OF A VECTOR SPACE

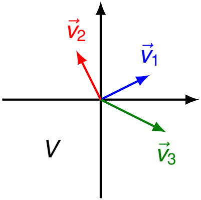
Let V be a vector space and suppose that $\dim(V) = n$.

- If $(\vec{v}_1, \ldots, \vec{v}_n)$ is a list of linearly independent vectors in V, then it is a basis of V.
- If $(\vec{v}_1, \ldots, \vec{v}_n)$ spans V, then it is a basis of V.
- A list of $m > n$ vectors in V cannot be linearly independent.
- A list of $m < n$ vectors cannot span V.

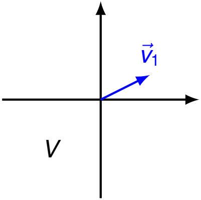
$m = n$



$m > n$



$m < n$



Example

Let $\mathbb{F}$ be a finite field. A basis of $\mathbb{F}^n$ is

$$\big((1,0,\ldots,0),(0,1,0,\ldots,0),\ldots,(0,\ldots,0,1)\big).$$

It is called **canonical** basis.

$\dim(\mathbb{F}^n) = n$.

A KEY EXAMPLE

$V = \mathbb{F}_5^3$

LET $S = \{ \vec{v} : \vec{v} = \alpha(1, 2, 3), \alpha \in \mathbb{F}_5 \}$

$= \text{span}\big((1, 2, 3) \big).$

GOAL: DESCRIBE THE SUBSPACE AS:

$S = \{ \vec{v} : \vec{v}$ SATISFIES SOME EQUATIONS $\}$

$$\vec{v} = \begin{pmatrix} \alpha \\ 2\alpha \\ 3\alpha \end{pmatrix} = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix}$$

$$\Rightarrow \begin{cases} 2v_1 = v_2 \\ 3v_1 = v_3 \end{cases} \Leftrightarrow \begin{cases} 2v_1 - v_2 = 0 \\ 3v_1 - v_3 = 0 \end{cases}$$

$$\Updownarrow$$

$$\begin{aligned} 2v_1 + 4v_2 &= 0 \\ 3v_1 + 4v_3 &= 0 \end{aligned}$$

$$\boxed{S = \left\{ \vec{v} : \begin{array}{l} 2v_1 + 4v_2 = 0 \\ \underline{\text{and}} \\ 3v_1 + 4v_3 = 0 \end{array} \right\}}$$

$$\vec{v} = \begin{pmatrix} \alpha \\ 2\alpha \\ 3\alpha \end{pmatrix}$$

$$\left.\begin{aligned} v_1 &= \alpha \\ v_2 &= 2\alpha \\ v_3 &= 3\alpha \end{aligned}\right\} \Rightarrow \begin{aligned} v_2 &= 2v_1 \\ v_3 &= 3v_1 \end{aligned} \Leftarrow \begin{aligned} 2v_1 - v_2 &= 0 \\ 3v_1 - v_3 &= 0 \end{aligned}$$

$$\Updownarrow$$

$$\boxed{\vec{0} = (v_1, v_2, v_3)\begin{pmatrix} 2 & 4 & 0 \\ 3 & 0 & 4 \end{pmatrix}^T} \quad \begin{cases} 2v_1 + 4v_2 = 0 \\ 3v_1 + 4v_3 = 0 \end{cases}$$

SECOND KEY EXAMPLE

$V = \mathbb{F}_5^3$

$$S = \left\{ \vec{v} : \overbrace{2v_1 + 3v_2 + v_3 = 0}^{(v_2, v_2, v_3)\begin{pmatrix}2 & 3 & 1\end{pmatrix}^T = 0} \right\}$$

GOAL: DESCRIBE S BY A BASIS.

SECOND KEY EXAMPLE

$$V = \mathbb{F}_5^3$$

$$S = \left\{ \vec{v} : \overbrace{2v_1 + 3v_2 + v_3 = 0}^{(v_1, v_2, v_3)\begin{pmatrix} 2 & 3 & 1 \end{pmatrix}^T = 0} \right\}$$

GOAL: DESCRIBE S BY A <u>BASIS</u>.

LET $v_1 = \alpha$ AND $v_2 = \beta$.

$$\alpha, \beta \in \mathbb{F}_5.$$

$$\Rightarrow \quad v_3 = -2\alpha - 3\beta = 3\alpha + 2\beta$$

$$\vec{v} = (\alpha, \beta, 3\alpha + 2\beta)$$

$$= \alpha(1, 0, 3) + \beta(0, 1, 2)$$

$$\Rightarrow \quad S = \text{Span}\{(1,0,3), (0,1,2)\}$$

$$\vec{v} = \alpha \begin{pmatrix} 1 & 0 & 3 \end{pmatrix} + \beta \begin{pmatrix} 0 & 1 & 2 \end{pmatrix}$$

$$S = \left\{ \vec{v} : \vec{v} = \begin{pmatrix} \alpha & \beta \end{pmatrix} \begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 2 \end{pmatrix} \text{ for some } \alpha, \beta \in \mathbb{F} \right\}$$

$$= \operatorname{span}\{ (1, 0, 3), (0, 1, 2) \}$$

Example

Let S be the subspace of $\mathbb{F}_7^3$ spanned by $\vec{v} = (4, 3, 1)$.

Define S by means of equations.

Solution

$(x, y, z) \in S$ implies $(x, y, z) = \alpha\vec{v}$ for some $\alpha \in \mathbb{F}_7$. Equivalently, $(x, y, z) = (4\alpha, 3\alpha, \alpha)$ or

$$\begin{cases} x = 4\alpha \\ y = 3\alpha \\ z = \alpha \end{cases}$$

After eliminating α,

$$\begin{cases} x = 4z \\ y = 3z \end{cases}$$

or, using the fact that $-4 = 3$,

$$\begin{cases} x + 3z = 0 \\ y + 4z = 0 \end{cases} \tag{1}$$

Solution (cont.)

Conversely, suppose that $(x, y, z) \in \mathbb{F}_7^3$ satisfies (1). Let α be the value of z. Then

$$\begin{cases} x = -3\alpha \\ y = -4\alpha \\ z = \alpha \end{cases}$$

or, equivalently

$$\begin{cases} x = 4\alpha \\ y = 3\alpha \\ z = \alpha, \end{cases}$$

which can be written as $(x, y, z) = \alpha\vec{v}$ for some $\alpha \in \mathbb{F}_7$.

We have proved that a vector $(x, y, z) \in \mathbb{F}_7^3$ is in S iff it satisfies the system of equations (1).

Example (Finding a basis)

Let $V \subseteq \mathbb{F}_7^3$ such that

$$V = \{(x_1, x_2, x_3) \in \mathbb{F}_7^3 : \; 3x_1 + 2x_2 + x_3 = 0\}$$

Find $\dim(V)$.

The above equation can be described by the **vector of coefficients** $(3, 2, 1) \in \mathbb{F}_7^3$.

Specifically, the equation is satisfied for (x_1, x_2, x_3) iff $(3, 2, 1)(x_1, x_2, x_3)^T = 0$.

Solution

We must obtain a basis of V. The equation $3x_1 + 2x_2 + x_3 = 0$ has two free variables, say x_1 and x_2.

Choose $x_1 = \alpha$ and $x_2 = \beta$.

$$\begin{aligned}(x_1, x_2, x_3) &= (\alpha, \beta, -3\alpha - 2\beta) = (\alpha, \beta, 4\alpha + 5\beta)\\ &= (1, 0, 4)\alpha + (0, 1, 5)\beta\end{aligned}$$

Clearly $\vec{v}_1 = (1, 0, 4)$ and $\vec{v}_2 = (0, 1, 5)$ are linearly independent and are in V.

Moreover, since (x_1, x_2, x_3) is an arbitrary vector in V, the equation above clearly shows that $V = \operatorname{span}(\vec{v}_1, \vec{v}_2)$.

$(\vec{v}_1, \vec{v}_2)$ is both linearly independent and spans V, so it is a basis of V.

Therefore $\dim(V) = 2$. □

Theorem (without proof)

The set of solutions in $V = \mathbb{F}^n$ of m linear homogeneous equations in n variables is a subspace S of V.

Let r be the dimensionality of the vector space spanned by the coefficient vectors. Then $\mathrm{dim}(S) = n - r$.

In particular, if the m vectors of coefficients are linearly independent, then $\mathrm{dim}(S) = n - m$.

Conversely, if S is a subspace of $V = \mathbb{F}^n$ with $\mathrm{dim}(S) = k$, there exists a set of $n - k$ linear equations with coefficients that form linearly independent vectors in V, the solution of which are the vectors in S.

THE THEOREM SAYS:

ANY SUBSPACE $S \subseteq \mathbb{F}_p^n$ OF DIMENSION k CAN BE DEFINED:

(1) BY SPECIFYING A BASIS WITH k ELEMENTS:

$$(\alpha_1, \alpha_2 \dots \alpha_k) \begin{pmatrix} — & \vec{g}_1 & — \\ — & \vec{g}_2 & — \\ & \vdots & \\ — & \vec{g}_k & — \end{pmatrix}$$

THE THEOREM SAYS:

ANY SUBSPACE $S \subseteq \mathbb{F}_p^n$ OF DIMENSION k CAN BE DEFINED:

(1) BY SPECIFYING A BASIS WITH k ELEMENTS:

$$S = \left\{ \vec{v} \; ; \; \vec{v} = (\alpha_1, \alpha_2 \dots \alpha_k)\, G \text{ for some } \alpha_i \in \mathbb{F}_p \right\}$$

THE THEOREM SAYS:

ANY SUBSPACE $S \subseteq \mathbb{F}_p^n$

OF DIMENSION k CAN BE DEFINED:

(2) BY GIVING $n-k$ LINEARLY INDEPENDENT LINEAR EQUATIONS:

$$\vec{v} \begin{pmatrix} \longleftarrow \vec{h}_1 \longrightarrow \\ \longleftarrow \vec{h}_2 \longrightarrow \\ \vdots \\ \longleftarrow \vec{h}_{n-k} \longrightarrow \end{pmatrix}^T = \underset{\uparrow \atop \text{vector of length } n-k}{\vec{0}}$$

THE THEOREM SAYS:

ANY SUBSPACE $S \subseteq \mathbb{F}_p^n$ OF DIMENSION k CAN BE DEFINED:

(2) BY GIVING $n-k$ LINEARLY INDEPENDENT LINEAR EQUATIONS:

$$S = \left\{ \vec{v} : \quad \vec{v} H^T = \underset{\substack{\uparrow \\ \text{vector} \\ \text{of length} \\ n-k}}{\vec{0}} \right\}$$

$\boxed{\text{EXAMPLE}}$ $\quad S \subseteq \mathbb{F}_2^3 \quad \boxed{k = \dim(S) = 2}$

$$S = \left\{ \vec{v} : \vec{v} = (\alpha_1 \;\; \alpha_2) \underbrace{\begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}}_{G} \right\}$$

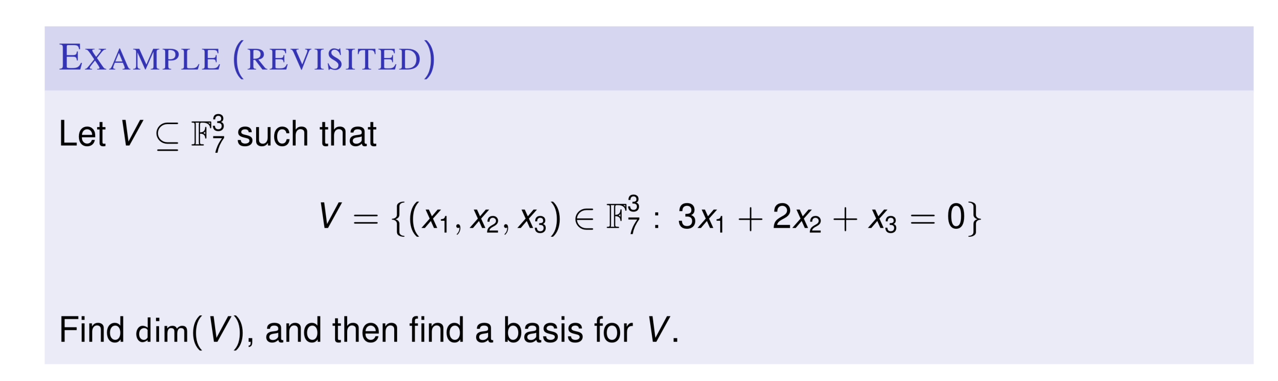
$$= \{ 000, \; 001, \; 110, \; 111 \}$$

$$S = \{ \vec{v} : \; v_1 = v_2 \}$$

$$= \{ \vec{v} : \; v_1 - v_2 = 0 \}$$

$$= \{ \vec{v} : \; v_1 + v_2 = 0 \}$$

$$= \{ \vec{v} : \; \vec{v} \, \overbrace{(1 \;\; 1 \;\; 0)}^{H}{}^{T} = 0 \}$$



Example (revisited)

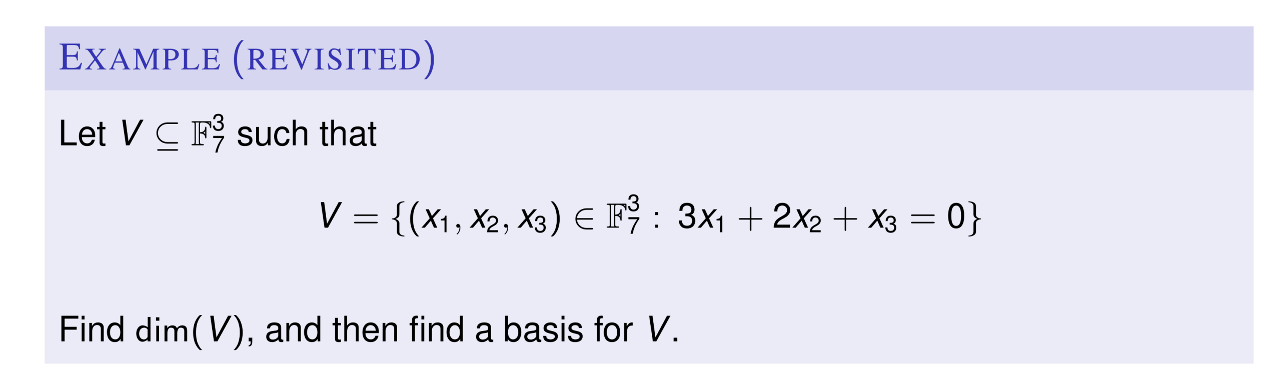
Let $V \subseteq \mathbb{F}_7^3$ such that

$$V = \{(x_1, x_2, x_3) \in \mathbb{F}_7^3 : \; 3x_1 + 2x_2 + x_3 = 0\}$$

Find $\dim(V)$, and then find a basis for V.

$m = 1$ Equations.

$\Rightarrow \dim(V) = n - m = 3 - 1 = 2$



Example (revisited)

Let $V \subseteq \mathbb{F}_7^3$ such that

$$V = \{(x_1, x_2, x_3) \in \mathbb{F}_7^3 : 3x_1 + 2x_2 + x_3 = 0\}$$

Find $\dim(V)$, and then find a basis for V.

$n - k = m = 1$, $n = 3$

$\Rightarrow k = 2 = \dim(V)$

$g_1 = (1 \quad 0 \quad \beta) \rightarrow \beta = 4$

$g_2 = (0 \quad 1 \quad \gamma) \rightarrow \gamma = 5$

Example (revisited)

Let $V \subseteq \mathbb{F}_7^3$ such that

$$V = \{(x_1, x_2, x_3) \in \mathbb{F}_7^3 : \; 3x_1 + 2x_2 + x_3 = 0\}$$

Find $\dim(V)$, and then find a basis for V.

Solution

There is only one vector $\vec{v} = (3, 2, 1)$ of coefficients. It spans a vector space of dimension $r = 1$. Hence $\dim(V) = 3 - 1 = 2$.

If we choose $\vec{v}_1 = (1, 0, v_{11})$ and $\vec{v}_2 = (0, 1, v_{21})$, then we are guaranteed that they are linearly independent. We choose v_{11} so as to satisfy the above equation, i.e., $v_{11} = -3 = 4$. Hence $\vec{v}_1 = (1, 0, 4)$

Similarly we obtain $\vec{v}_2 = (0, 1, 5)$.

Example (revisited)

Let S be the subspace of $\mathbb{F}_7^3$ spanned by $\vec{v} = (4, 3, 1)$.

Define S by means of equations.

$$\dim(S) = k = 1$$

$$\Rightarrow \# \text{Equations} = m = n - k = 2$$

SOLUTION

S is a one-dimensional subspace of $V = \mathbb{F}_7^3$, hence it can be described by $3 - 1 = 2$ equations.

Let us find two linearly independent vectors $\vec{c}_1, \vec{c}_2 \in V$ such that $\sum_{j=1}^{3} c_{ij} v_j = 0$, $i = 1, 2$. (The above theorem implies that they exist.)

We can choose $\vec{c}_1 = (1, 0, c_{13})$ and $\vec{c}_2 = (0, 1, c_{23})$ and complete to fulfill the above equation.

Hence, $\vec{c}_1 = (1, 0, -4) = (1, 0, 3)$ and $\vec{c}_2 = (0, 1, -3) = (0, 1, 4)$.

Therefore S is the set of vectors (x_1, x_2, x_3) that satisfy

$$\begin{cases} x_1 + 3x_3 = 0 \\ x_2 + 4x_3 = 0 \end{cases} .$$

□

ORTHOGONALITY ?

CANNOT BE DEFINED IN A USEFUL WAY HERE!

↳ SO, <u>DON'T USE IT</u>.

(INSTEAD: USE LINEAR INDEPENDENCE)

$\mathbb{F}_2^9$

$$\vec{v} = (1, 1, 1, 0, 0, 0, 0, 1, 0)$$

$$\vec{v} \cdot \vec{u} = \sum_{i=1}^{n} v_i u_i \pmod 2$$

HENCE

$\vec{v} \cdot \vec{v} = 0$ (!) $\vec{v}$ IS ORTHOGONAL TO ITSELF.

$\Rightarrow$ NOT A GOOD DEFINITION OF ORTHOGONALITY!

Rank of a matrix

For any matrix with entries in a field $\mathbb{F}$:

- the dimension of the vector space spanned by its rows ...
- equals the dimension of the vector space spanned by its columns.

It is called the *rank* of the matrix.

$$A = \begin{pmatrix} \text{---} & \vec{a}_1 & \text{---} \\ \text{---} & \vec{a}_2 & \text{---} \\ & \vdots & \\ \text{---} & \vec{a}_m & \text{---} \end{pmatrix} = \begin{pmatrix} | & | & & | \\ \vec{\alpha}_1 & \vec{\alpha}_2 & \cdots & \vec{\alpha}_n \\ | & | & & | \end{pmatrix}$$

$r =$ column rank (A) :

$\Rightarrow \{ \underline{v}_1, \underline{v}_{22} \dots \underline{v}_r \}$ spans all coluns

$$\Rightarrow \alpha_i = \sum_{j=1}^{r} \gamma_{ij} v_j$$

$$\Rightarrow A = \begin{pmatrix} | & & | \\ \alpha_1 & \cdots & \alpha_n \\ | & & | \end{pmatrix} = n \updownarrow \overset{\leftarrow r \rightarrow}{\begin{pmatrix} | & & | \\ v_1 & \cdots & v_r \\ | & & | \end{pmatrix}} \underset{\leftarrow n \rightarrow}{\begin{pmatrix} \gamma_{11} & \cdots & \gamma \\ & \ddots & \\ \gamma & & \gamma_{mn} \end{pmatrix}} \updownarrow r$$

$\Rightarrow$ row rank $(A) \leq r$

Example

Let S be the subspace of $V = \mathbb{F}_7^3$ whose elements (x_1, x_2, x_3) verify

$$\begin{cases} 4x_1 + x_2 = 0 \\ x_1 + x_3 = 0 \end{cases}$$

- The coefficient matrix is $A = \begin{bmatrix} 4 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$.
- Its rank is $r = 2$.
- $\dim(S) = \dim(V) - r = 3 - 2 = 1$.

EXAMPLE:

Consider $\mathbb{F}_3^2$.

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$

$\operatorname{rank}(A) = 1$.

THE THEOREM SAYS:

ANY SUBSPACE $S \subseteq \mathbb{F}_p^n$ OF DIMENSION k CAN BE DEFINED:

(1) BY SPECIFYING A MATRIX G OF RANK k:

$$S = \{ \vec{v} : \vec{v} = \vec{\alpha}\, G \quad \text{for } \vec{\alpha} \in \mathbb{F}_p^k \}$$

THE THEOREM SAYS:

ANY SUBSPACE $S \subseteq \mathbb{F}_p^n$ OF DIMENSION k CAN BE DEFINED:

(2) BY GIVING A MATRIX H OF RANK $n-k$:

$$S = \{ \vec{v} : \vec{v} H^T = \vec{0} \}$$

Cardinality and Dimension

Theorem (12.2 of textbook)

An n-dimensional vector space V over a finite field $\mathbb{F}$:

- is finite,
- has cardinality
$$\mathrm{card}(V) = [\mathrm{card}(\mathbb{F})]^n.$$

Proof:

Let $(\vec{v}_1, \ldots, \vec{v}_n)$ be a basis of V. For every $\vec{v} \in V$, there is a unique n-tuple $(\lambda_1, \ldots, \lambda_n) \in \mathbb{F}^n$ such that $\vec{v} = \sum_i \lambda_i \vec{v}_i$.

Hence the mapping

$$\begin{aligned} \mathbb{F}^n &\to V \\ (\lambda_1, \ldots, \lambda_n) &\mapsto \vec{v} = \sum_i \lambda_i \vec{v}_i \end{aligned}$$

is a bijection.

By the pigeonhole principle,

$$\mathrm{card}(V) = \mathrm{card}(\mathbb{F}^n) = [\mathrm{card}(\mathbb{F})]^n.$$

□

COROLLARY

A k- DIMENSIONAL SUBSPACE

$$S \subseteq V$$

OVER A FINITE FIELD $\mathbb{F}$:

(1) IS FINITE

(2) HAS CARDINALITY

$$[\mathrm{card}(\mathbb{F})]^{k}$$