LA1 Fields and Vector Spaces

KYB

Thrn, it's a Fact

mathrnfact@gmail.com

February 8, 2021

Overview

Goal of LA

1. Objects in Linear Algebra
   - fields, vector spaces, linear operators (matrices)
2. Fundamental Theory of Linear Algebra
   - nullity + rank = dimension
3. Diagonalization
   - Eigenvalues, Eigenvectors, the Jordan Canonical Form

Definition (Fields)

A set F with $+, \times$ is called a field if F satisfies

0. $\alpha + \beta, \alpha \times \beta \in F$. (closed under $+$ and $\times$, simply write $\alpha \times \beta = \alpha\beta$)

1. $\alpha + \beta = \beta + \alpha$
2. $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$
3. $\exists 0$ such that $\alpha + 0 = \alpha$ for all α
4. $\exists - \alpha$ such that $\alpha + (-\alpha) = 0$ for all α

5. $\alpha\beta = \beta\alpha$
6. $(\alpha\beta)\gamma = \alpha(\beta\gamma)$
7. $\exists 1 \neq 0$ such that $\alpha \times 1 = \alpha$ for all α
8. $\exists \alpha^{-1}$ such that $\alpha \times \alpha^{-1} = 1$ for all $\alpha \neq 0$

9. $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$

Remark

- Every field has at least two elements, 0 and 1
- 0, 1, $-\alpha$, α^{-1} are unique
- (cancelation law for $+$) $\alpha + \gamma = \beta + \gamma \implies \alpha = \beta$
- (cancelation law for $\times$) $\alpha\gamma = \beta\gamma \implies \alpha = \beta$ if $\gamma \neq 0$
- $0 \cdot \alpha = 0$, $-1 \cdot \alpha = -\alpha$
- $\ldots$

Notation

- $\sum_{i=1}^{n} \alpha_i = \alpha_1 + \alpha_2 + \cdots + \alpha_n$
- $\sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} = \sum_{i=1}^{m} (a_{i1} + \cdots + a_{in})$
- $\beta \sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta \alpha_i$
- $\sum_{i=1}^{n} (\alpha_i + \beta_i) = \sum_{i=1}^{n} \alpha_i + \sum_{i=1}^{n} \beta_i$

Example

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ for prime number p

What is $\mathbb{Z}_p$? " a filed with exactly p elements" (if p is not a prime number $\mathbb{Z}_p$ is not a field)

$$\mathbb{Z}_2 = \{0, 1\}, \quad \mathbb{Z}_3 = \{0, 1, 1+1\}, \quad \mathbb{Z}_5 = \{0, 1, 1+1, 1+1+1, 1+1+1+1\}$$

Exercise

Prove $\mathbb{Z}_2$ is a field

Proof.

$$0+0=0, \quad 0+1=1, \quad 1+0=1, \quad 1+1=0$$

Check the tables of addition and multiplication

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

□

Example

$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$.
For $a, b \in \mathbb{Z}$,

$$\overline{a} = \overline{b} \iff a - b = nq \text{ for some } q \in \mathbb{Z}$$

(i.e., n divides $a - b$, or the remainder of a by $n =$ the remainder of b by n)
For instance, for $n = 6$, $\overline{1} = \overline{713} = \cdots$.
For any $a \in \mathbb{Z}$, there is $r \in \mathbb{Z}$ such that $0 \leq r \leq n - 1$ and $\overline{a} = \overline{r}$, or

$$a = nq + r$$

(using Euclidean Algorithm)

Example

We can define $+, \times$ on $\mathbb{Z}_n$ by

$$\overline{a} + \overline{b} := \overline{a+b}, \quad \overline{a} \times \overline{b} := \overline{ab}$$

Check : $+, \times$ well-defined

(1) $\overline{a} + \overline{b}, \overline{a} \times \overline{b} \in \mathbb{Z}_n$

(2) If $\overline{a}_1 = \overline{a}_2$ and $\overline{b}_1 = \overline{b}_2$, then

$$\begin{cases} \overline{a}_1 + \overline{b}_1 = \overline{a}_2 + \overline{b}_2 \\ \overline{a}_1 \times \overline{b}_1 = \overline{a}_2 \times \overline{b}_2 \end{cases}$$

Example

(1) Since $a+b, ab \in \mathbb{Z}$, $\overline{a}+\overline{b}, \overline{a}\times\overline{b} \in \mathbb{Z}_n$

(2) Since $\overline{a}_1 = \overline{a}_2$ and $\overline{b}_1 = \overline{b}_2$, there exist $q_1, q_2 \in \mathbb{Z}$ such that

$$\begin{cases} a_1 - a_2 = nq_1 \\ b_1 = b_2 = nq_2 \end{cases}$$

- $$(a_1+b_1)-(a_2+b_2) = (a_1-a_2)+(b_1-b_2) = nq_1+nq_2 = n(q_1+q_2)$$
$$\implies \overline{a_1+b_1} = \overline{a_2+b_2} \implies \overline{a}_1+\overline{b}_1 = \overline{a_2}+\overline{b_2}$$

- $$(a_1b_1)-(a_2b_2) = a_1b_1 - a_1b_2 + a_1b_2 - a_2b_2 = a_1nq_2 + nq_1b_2 = n(a_1q_2+q_1b_2)$$
$$\implies \overline{a_1b_1} = \overline{a_2b_2} \implies \overline{a}_1\times\overline{b}_1 = \overline{a_2}\times\overline{b_2}$$

Example

Now we get some properties of $\mathbb{Z}_n$

1. $\overline{a}+\overline{b}=\overline{b}+\overline{a}$
2. $(\overline{a}+\overline{b})+\overline{c}=\overline{a}+(\overline{b}+\overline{c})$
3. $\overline{a}+\overline{0}=\overline{a}$
4. $-\overline{a}=\overline{-a}$
5. $\overline{a}\overline{b}=\overline{b}\overline{a}$
6. $(\overline{a}\overline{b})\overline{c}=\overline{a}(\overline{b}\overline{c})$
7. $\overline{a}\cdot\overline{1}=\overline{a}$
8. $\overline{a}(\overline{b}+\overline{c})=\overline{a}\overline{b}+\overline{ac}$

"Caution": in general, $\overline{a}^{-1}$ does not exists, for example, for $n=4$ $\overline{2}\cdot\overline{2}=\overline{4}=\overline{0}$. If $\overline{2}^{-1}$ exists, $\overline{2}=\overline{2}^{-1}\cdot\overline{2}\cdot\overline{2}=\overline{2}^{-1}\cdot\overline{0}=\overline{0}$, but $\overline{2}\neq\overline{0}$.
If every nonzero $a\in\mathbb{Z}_n$ has the inverse a^{-1}, then $\mathbb{Z}_n$ is a field.

Theorem

$\mathbb{Z}_n$ is a field if and only if n is a prime number.

Proof

($\Longrightarrow$) Since every field has at least two elements, $n \geq 2$. Suppose n is not a prime, say $n = ab$ where $a, b > 1$. Since $1 < a, b < n$, $a, b \in \mathbb{Z}_n$ (identify $\overline{a} = a$ and $\overline{b} = b$). So $ab = \in \mathbb{Z}_n$. Since $ab = n = n \cdot 1 + 0$, $ab = 0$ in $\mathbb{Z}_n$. Since $\mathbb{Z}_n$ is a field and $a \neq 0$, there is a^{-1}.

$$b = a^{-1}ab = a^{-1}\overline{n} = a^{-1}0 = \overline{0}$$

Since $0 < b < n$, $b = 0 \cdot n + b$ implies $b = 0$ (contradiction), hence n is prime.

Theorem

$\mathbb{Z}_n$ is a field if and only if n is a prime number.

Proof

($\Longleftarrow$) Suppose p is a prime. Let $\alpha \in \mathbb{Z}_n$ which is nonzero. Then $\{\alpha, \alpha^2, \alpha^3, \cdots\}$ is a subset of $\mathbb{Z}_n$ and $\alpha^k \neq 0$ for all k. Then there are $l, k \in \mathbb{N}$ such that $l \neq k$ and $\alpha^l = \alpha^k$ because $\mathbb{Z}_n$ is finite. Without loss of generality, assume $k > l$.

$$\alpha^k = \alpha^{k-l}\alpha^l = \alpha^l \implies \alpha^{k-l} = 1$$

(cancelation law still holds) Since $k - l - 1 \geq 0$, $1 = \alpha^{k-l} = \alpha^{k-l-1} \cdot \alpha$, or $\alpha^{-1} = \alpha^{k-l-1}$. So α^{-1} exists.

Example

Q. Let F be finite field. If $|F|$ ($\#$ of elements of F) a prime number? No!
Let $F = \{0, 1, \omega, \omega + 1\}$ with operations followed by

$+$	0	1	ω	$\omega+1$
0	0	1	ω	$\omega+1$
1	1	0	$\omega+1$	ω
ω	ω	$\omega+1$	0	1
$\omega+1$	$\omega+1$	ω	1	0

$\times$	0	1	ω	$\omega+1$
0	0	0	0	0
1	0	1	ω	$\omega+1$
ω	0	ω	$\omega+1$	1
$\omega+1$	0	$\omega+1$	1	ω

Then F is a field and there are exactly 4 elements.

Ex 2.1.19

Suppose F is a finite field.

(a) There is $n = \text{char } F$ (n is the smallest k such that $\underbrace{1+1+\cdots+1}_{k \text{ times}} = 0$)

Proof.

Consider $\{1, 1+1, \cdots\} \subset F$. Let $|F| = p$ (may not prime) Since $\{1, 1+1, \cdots\}$ has at most p many elements, there are $a, b \in \mathbb{N}$ with $a < b$ such that

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

Then

$$\begin{aligned} 0 &= \underbrace{1+1\cdots+1}_{a \text{ times}} - 1\underbrace{1+1\cdots+1}_{a \text{ times}} = \underbrace{1+1\cdots+1}_{b \text{ times}} - 1\underbrace{1+1\cdots+1}_{a \text{ times}} \\ &= \underbrace{1+1\cdots+1}_{b-a \text{ times}} \end{aligned}$$

Using the fact that every nonempty subset of $\mathbb{N}$ has the smallest n, we can find char $F = n$. $\square$

Ex 2.1.19

Suppose F is a finite field.

(b) Let $n = \text{char}\, F$. Then $\underbrace{\alpha + \cdots + \alpha}_{n \text{ times}} = 0$ for any $\alpha \in F$.

Proof.

$$\alpha + \cdots + \alpha = (1 + \cdots = 1) \cdot \alpha$$

$\square$

(c) char F is a prime number.

Proof.

Suppose $n = l \cdot k$. Then

$$(\underbrace{1 + 1 \cdots + 1}_{l \text{ times}})(\underbrace{1 + 1 \cdots + 1}_{k \text{ times}}) = 0(\text{contradiction})$$

$\square$

(d)

Example (Quaterian H)

Let H be the set of all element of the form

$$a + bi + cj + dk \quad a, b, c, d \in \mathbb{R}$$

where

$$i^2 = j^2 = k^2 = -1, \quad ij = k, ji = -k, jk = i, kj = -i, ki = j, ik = -j$$

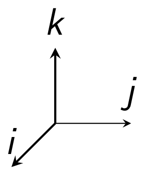
Then

(1) $\alpha\beta \neq \beta\alpha$

(2) there are 0 and 1

(3) there is α^{-1} if $\alpha \neq 0$.

We call such set a "division ring" or "skew field"



Remark

$-1 \neq 0$ because $1 \neq 0$. Suppose not. $0 = 1 + (-1) = 1 + 0 = 1$.

Remark

$\alpha x + \beta = 0$ has a unique solution if $\alpha \neq 0$.

Proof.

(1) (Existence) Let $x = \alpha^{-1}(-\beta)$. Then
$\alpha(\alpha^{-1} \cdot (-\beta)) = \beta = (\alpha \cdot \alpha^{-1})(-\beta) + \beta) = 1 \cdot (-\beta) + \beta = -\beta + \beta = 0.$

(2) (Uniqueness) Suppose x' is another solution. Then
$\alpha x' + \beta = 0 \implies \alpha x' = -\beta \implies x' = \alpha^{-1}(-\beta).$

$\square$

Ex 2.1.9

$\alpha/\beta = \alpha\beta^{-1}$

Ex 2.1.13

Let $F = \{(\alpha, \beta) : \alpha, \beta \in F\} = \mathbb{R} \times \mathbb{R}$. Define addition and multiplication on F as follows:

$$(\alpha, \beta) + (\gamma, \delta) = (\alpha + \gamma, \beta + \delta),$$
$$(\alpha, \beta) \cdot (\gamma, \delta) = (\alpha\gamma, \beta\delta).$$

Then F is not a field because $(1, 0) \cdot (0, 1) = (0, 0) = 0$.

Remark

$\mathbb{R} \times \mathbb{R}$ can not be field for all $+, \times$?

$$(\alpha, \beta) + (\gamma, \delta) = (\alpha + \gamma, \beta + \delta),$$
$$(\alpha, \beta) \cdot (\gamma, \delta) = (\alpha\gamma - \beta\delta, \alpha\delta + \beta\delta).$$

In these $+, \cdot$, $\mathbb{R} \times \mathbb{R}$ is a field. In fact, $\mathbb{C} \cong \mathbb{R} \times \mathbb{R}$.

Definition (Vector Spaces)

A set V with $+, \times$ is called a vector space over a field F if V satisfies

0. For all $u, v \in V$, $u + v \in V$, and for all $\alpha \in F$ and $v \in V$, $\alpha \cdot v \in V$.

1. $u + v = v + u$
2. $(u + v) + w = u + (v + w)$
3. $\exists 0 \in V$ such that $u + 0 = u$ for all u
4. $\exists -u$ such that $u + (-u) = 0$ for all u

5. $\alpha(\beta u) = (\alpha\beta)u$
6. $\alpha(u + v) = \alpha u + \alpha v$
7. $(\alpha + \beta)u = \alpha u + \beta u$
8. $1 \cdot u = u$

Remark

$$V = \{\text{vectors}\}, F = \{\text{scalars}\}$$

- $0, -u$ are unique
- $-(u+v) = (-u) + (-v)$
- $u + v = u + w$ implies $v = w$
- For $0 \in V$, $\alpha \cdot 0 = 0$
- $\alpha \cdot u = 0$ implies $\alpha = 0$ or $u = 0$.
- $0 \cdot u = 0$, $(-1) \cdot u = -u$.
- $\cdots$

Example

- Consider

$$\mathbb{R}^n = \{(x_1, \cdots, x_n) : x_1, \cdots, x_n \in \mathbb{R}\} = \left\{ \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} : x_1, \cdots, x_n \in \mathbb{R} \right\}$$

  - Scalar multiplication $\alpha x = (\alpha x_1, \cdots, \alpha x_n)$
  - Addition $x + y = (x_1 + y_1, \cdots, x_n + y_n)$
- In general, if F is a field, then F^n is a vector space.
- $\mathbb{C}$ is a vector space over $\mathbb{R}$.

Example

- Let $F[a, b] = \{f : [a, b] \to \mathbb{R}\}$. For $r \in \mathbb{R}$ and $f, g \in F[0, 1]$, define
  - $(rf)(x) = rf(x)$
  - $(f + g)(x) = f(x) + g(x)$

  Then $F[a, b]$ is a vector space over $\mathbb{R}$.
- $C[a, b] = \{f : [a, b] \to \mathbb{R} | f \text{ is continuous}\}$
- $C^1[a, b] = \{f : [a, b] \to \mathbb{R} | f \text{ is differentible on } [a, b] \text{ and } f' \text{ is continuous on } [a, b]\ \}$

Example

- $\mathcal{P}_n = \{a_n x^n + \cdots + a_0 | a_0, \cdots, a_n \in \mathbb{R}\}$ the set of polynomials of degree $\leq n$
- $\{ax^n : a \in \mathbb{R}\}$ the set of all monomials of degree n and 0
- If P is the set of all polynomial of degree exactly n together with 0 is not a vector space. Consider $(x^n + 1) - x^n = 1$.

Ex 2.1.1

$\{0\}$ is a vector space, say trivial vector space.

Ex 2.1.2

If F is an infinite field and V is a nontrivial vector space over F. Then F is infinite.

Proof.

Main idea)

$$\begin{cases} \underbrace{1+\cdots+1}_{n} \neq 0 & n > 0 \\ \alpha u \neq u & \text{if } \alpha \neq 0, u \neq 0 \end{cases}$$

$\square$

Ex 2.2.6

(a) $\left|\mathbb{Z}_p^n\right| = p^n$

(b) $\mathbb{Z}_2^2 = \{(0,0),(0,1),(1,0),(1,1)\}$

Ex 2.2.7

(a) $\mathcal{P}_1(\mathbb{Z}_2) = \{0, 1, x, 1+x\}$

Ex 2.2.8

Let $V = (0, \infty)$ and define addition $\oplus$ and scalar multiplication $\odot$ by

$$u \oplus v = uv\alpha \odot u = u^{\alpha}$$

Is V a vector space over $\mathbb{R}$?

Proof.

1. $u \oplus v = v \oplus u$
2. $(u \oplus v) \oplus w = u \oplus (v \oplus w)$
3. $\overline{0} = 1$
4. $\ominus u = u^{-1}$
5. $(\alpha\beta) \odot u = \alpha \odot (\beta \odot u)$
6. $\alpha \odot (u \oplus v) = (\alpha \odot u) \oplus (\alpha \odot v)$
7. $\alpha + \beta) \odot u = (\alpha \odot u) \oplus (\beta \odot u)$
8. $1 \odot u = u^1 = u.$

$\square$

Ex 2.2.10

Let $V = \mathbb{R}^2$. Fix $\alpha_1, \beta_1, \alpha_2, \beta_2 \in \mathbb{R}$. Define vector addition on V by

$$u \oplus v = (\alpha_1 u_1 + \beta_1 v_1, \alpha_2 u_u + \beta_2 v_2)$$

and assume scalar multiplication on V is defined by the usual componentwise formula. What values of $\alpha_1, \beta_1, \alpha_2 \beta_2$ will make V a vector space over $\mathbb{R}$ under these operations?

Proof

- $(1,1) \oplus (0,0) = (\alpha_1, \alpha_2)$, $(0,0) \oplus (1,1) = (\beta_1, \beta_2)$ and $u \oplus v = v \oplus u$ implies $\alpha_1 = \beta_1$ and $\alpha_2 = \beta_2$.
- $u \oplus 0 = u$ where $0 = (e_1, e_2)$ implies

$$\begin{cases} \alpha_1 u_1 + \alpha_1 e_1 = u_1 \\ \alpha_2 u_2 + \alpha_2 e_2 = u_2 \end{cases}$$

  for all $u = (u_1, u_2)$.
  Put $u = (0,0)$, then $\alpha_1 e_1 = \alpha_2 e_2 = 0$.

(continued)

Ex 2.2.10

Proof.

- $u \oplus 0 = u$ where $0 = (e_1, e_2)$ implies

$$\begin{cases} \alpha_1 u_1 + \alpha_1 e_1 = u_1 \\ \alpha_2 u_2 + \alpha_2 e_2 = u_2 \end{cases}$$

for all $u = (u_1, u_2)$.
Put $u = (0, 0)$, then $\alpha_1 e_1 = \alpha_2 e_2 = 0$. Then there are four cases

$$(1)\ \alpha_1 = \alpha_2 = 0, \quad (2)\ \alpha_1 = e_2 = 0, \quad (3)\ e_1 = \alpha_2 = 0, \quad (4)\ e_1 = e_2 = 0.$$

(1) $u \oplus 0 = u$ implies $u_1 = u_2 = 0$ for all u_1, u_2 (contradiction)
(2) $\alpha_1 e_2 = u_1$ for all u_1 (contradiction), (3) is similar to (2)
(4) 0=(0,0). Then $(1, 1) = (1, 1) \oplus (0, 0) = (\alpha_1, \alpha_2)$. Hence $\alpha_1 = \beta_1 = \alpha_2 = \beta_2 = 1$.

$\square$

Ex 2.2.15

If X and Y are any two sets, then the Cartesian product of X and Y is the set

$$X \times Y = \{(x, y) : x \in X, y \in Y\}.$$

If U and V are two vector spaces over a field F, then we define operations on $U \times V$ by

$$(u, v) + (w, z) = (u + w, v + z),$$
$$\alpha(u, v) = (\alpha u, \alpha v).$$

Prove that $U \times V$ is a vector space over F.

The End