Math 20250
Abstract Linear Algebra

Cong Hung Le Tran

March 30, 2023

Course: MATH 20250: Abstract Linear Algebra
Section: 44
Professor: Zijian Yao
At: The University of Chicago
Quarter: Spring 2023
Course materials: Linear Algebra by Hoffman and Kunze (2nd Edition), Linear Algebra Done Wrong by Treil

Disclaimer: This document will inevitably contain some mistakes, both simple typos and serious logical and mathematical errors. Take what you read with a grain of salt as it is made by an undergraduate student going through the learning process himself. If you do find any error, I would really appreciate it if you can let me know by email at conghungletran@gmail.com.

Contents

21 Mar 2023

Lecture 1: Abelian Group, Field, Equivalence

Goal. Vector spaces and maps between vector spaces (linear transformations)

1.1 Abelian Group

Definition 1.1 (Abelian Group). A pair $(A, *)$ is an **Abelian group** if A is a set and $*$ is a map: $A \times A \mapsto A$ (closure is implied) with the following properties:

1. (Additive Associativity)
$$(x * y) * z = x * (y * z), \forall\, x, y, z \in A$$
2. (Additive Commutativity)
$$x * y = y * x, \forall\, x, y \in A$$
3. (Additive Identity)
$$\exists\, 0 \in A : 0 * x = x * 0 = x, \forall\, x \in A$$
4. (Additive Inverse)
$$\forall\, x \in A, \exists\, (-x) \in A : x * (-x) = (-x) * x = 0$$

Remark. ($*$ is just a symbol, soon to be $+$). Typically write as $(A, +)$ or simply A

Example.

1. $(\mathbb{Z}, +)$ is an Abelian group
2. $(\mathbb{Q}, +)$ is an Abelian group
3. $(\mathbb{Z}, \times)$ is **NOT** an Abelian group (because identity $= 1$, and 0 does not have a multiplicative inverse)
4. $(\mathbb{Q}, \times)$ is also not an Abelian group (0 does not have a multiplicative inverse)
5. $(\mathbb{Q}\backslash\{0\}, \times)$ is an Abelian group (identity is 1)
6. $(\mathbb{N}, \times)$ is NOT a group

Remark. A crucial difference between $\mathbb{Z}$ and $\mathbb{Q}\backslash\{0\}$ is that $\mathbb{Q}\backslash\{0\}$ has both $+$ and $\times$ while $\mathbb{Z}$ only has $+$. This gives us inspiration for the definition of a field!

Definition 1.2 (Field). A **field** is a triple $(F, +, \cdot)$ such that

1. $(F, +)$ is an Abelian group with identity 0
2. (Multiplicative Associativity)
$$(x \cdot y) \cdot z = x \cdot (y \cdot z), \forall\, x, y, z \in F$$
3. (Multiplicative Commutativity)
$$x \cdot y = y \cdot x, \forall\, x, y \in F$$

4. (Distributivity) ($+$ and $\cdot$ talking in the following way)
$$x \cdot (y + z) = (x \cdot y) + (x \cdot z), \forall\, x, y, z \in F$$
5. (Multiplicative Identity)
$$\exists\, 1 \in F : 1 \cdot x = x, \forall\, x \in F$$
6. (Multiplicative Inverse)
$$\forall\, x \in F \backslash \{0\}, \exists\, y \in F : x \cdot y = 1$$

Remark. In a field $(F, +, \cdot)$, assume that $1 \neq 0$

Example.

1. $(\mathbb{Z}, +, \cdot)$ is not a field (because property 6 failed)
2. $(\mathbb{Q}, +, \cdot)$ is a field
3. $(\mathbb{R}, +, \cdot)$ and $(\mathbb{C}, +, \cdot)$ are fields.

1.2 Finite Fields

Recall. $p \in \mathbb{Z}$ is a prime if $\forall\, m \in \mathbb{N} : m \mid p \Rightarrow m = 1$ or $m = p$

Definition 1.3 ($\mathbb{F}_p$ for p prime).
$$\mathbb{F}_p = \{[0], [1], \ldots, [p-1]\}$$
Then define the operations for $[a], [b] \in \mathbb{F}_p$
$$[a] + [b] = [a + b \mod p]; [a] \cdot [b] = [a \cdot b \mod p]$$
Then $\mathbb{F}_p$ is a field, but this is not trivial.

Lemma 1.1.

1. $(\mathbb{F}_p, +)$ is an Abelian group
2. $(\mathbb{F}_p, +, \cdot)$ is a field

Example. $\mathbb{F}_5 = \{[0], [1], [2], [3], [4]\}$
$$[1] + [2] = [3], [2] + [4] = [1], [4] + [4] = [3], [2] + [3] = [0]$$
Then it is trivial that $[0]$ is additive identity, and every element has additive inverse. $[1]$ is multiplicative identity, and every element except $[0]$ has multiplicative inverse. Therefore $\mathbb{F}_5$ is indeed a field.

1.3 Vector Spaces in brief

Intuition. The motivation for vector spaces and maps between them (linear transformations) is essentially to solve linear equations. Let $(\mathbb{K}, +, \cdot)$ be a field. We are then interested in systems of linear equations / $\mathbb{K}$; if there are solutions, and if there are how many.

We then inspect a system of linear equations of n unknowns, m relations:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ \cdots &= \cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m \end{aligned}$$

where $a_{ij}, b_k \in \mathbb{K}$.

Example.

$$2x_1 - x_2 + x_3 = 0 \tag{1}$$
$$x_1 + 3x_2 + 4x_3 = 0 \tag{2}$$

over some field $\mathbb{K}$.

Explanation. Then, $3 \times (1) + (2)$ (carrying out the operations in $\mathbb{K}$) yields

$$\begin{aligned} 7x_1 + 7x_3 &= 0 \\ 7 \cdot (x_1 + x_3) &= 0 \end{aligned} \tag{3}$$

Then, we have 2 cases.
Case 1: $7 \neq 0$ in $\mathbb{K}$, then $\exists\, 7^{-1} \in \mathbb{K} : 7^{-1} \cdot 7 = 1$.
Then $(3) \Rightarrow 7^{-1} \cdot (7 \cdot (x_1 + x_3)) = 0$

$$\begin{aligned} ((7^{-1}) \cdot 7) \cdot (x_1 + x_3) &= 0 \\ 1 \cdot (x_1 + x_3) &= 0 \\ \Rightarrow x_1 + x_3 &= 0 \\ \Rightarrow x_1 &= -x_3 \end{aligned}$$

Let $x_3 = a \Rightarrow x_1 = -a \Rightarrow x_2 = 2x_1 + x_3 = -a$.
$\Rightarrow \{(-a, -a, a) \mid a \in \mathbb{K}\}$ are solutions.

Case 2: $7 = 0$ in $\mathbb{K}$ (e.g. in $\mathbb{F}_7$) then (3) is automatically true.
Let $x_1 = a, x_3 = b \Rightarrow x_2 = 2x_1 + x_3 = 2a + b$
$\Rightarrow \{(a, 2a + b, b) \mid a, b \in \mathbb{K}\}$ are solutions. □

Remark. When doing $3 \times (1) + (2)$, how do we know if we're gaining or losing information? e.g in $\mathbb{F}_7$ we can just multiply by 7 and get nothing new! Therefore some kind of "equivalence" concept must be introduced!

Definition 1.4 (Linear combination). Suppose $S = \{\sum a_{ij}x_j = b_i\}_{1 \leq i \leq m, 1 \leq j \leq n}$ is a system of linear equations over $\mathbb{K}$. $S' = \{\sum a'_{ij}x_j = b_i\}_{1 \leq i \leq m, 1 \leq j \leq n}$ is another system of linear equations (not too important how many equations there are in S'). Then, S' is a **linear combination** of S if every linear equations $\sum a'_{ij}x_j = b_i$ in S' can be obtained as linear combinations of equations in S, i.e. $\sum a'_{ij}x_j = b'_i$ is obtained through

$$\sum c_i \left(\sum a_{ij}x_j \right) = \sum c_i b_i, 1 \leq i \leq m, \text{ for some } c_i \in \mathbb{K}$$

Definition 1.5 (Equivalance). 2 systems S, S' are **equivalent** if S' is a linear combination of S and vice versa. Denote $\mathbf{S \sim S'}$

Example. In previous example, $S = \{(1), (2)\}, S' = \{(1), (3)\}, S'' = \{(2), (3)\}, S''' = \{(3)\}$.
Then, $S \not\sim S'', S \sim S'$ always , $S \sim S''$ only if 3 is invertible

Explanation.
From S', (1) = (1), (2) = (3) - 3 · (1). Therefore S is a linear combination of S'. $\Rightarrow S \sim S'$.
From S'', (2) = (2), 3 · (1) = (3) - (2). If $3^{-1} \in \mathbb{K}$(i.e. $3 \neq 0$) then (1) = 3^{-1}((3) - (2)) is thus recoverable from S'', then $S \sim S''$. Otherwise, no. □

28 Mar 2023

Lecture 2: Matrices

Proposition 2.1. If 2 systems of linear equations are equivalent, $S \sim S'$ then they have the same set of solutions

Remark. Why is this important? This becomes important if we have a complicated system and want to transform into a simpler system to solve.

Proof. If $(x_1 = \alpha_1, x_2 = \alpha_2, \ldots, x_n = \alpha_n)$ is a solution ot S then we claim that it's also a solution of S' and vice versa. This is trivial because $S \sim S'$. □

Definition 2.6 (Matrix). Let $\mathbb{K}$ be a field. Then an $\mathbf{m \times n}$ **matrix** with coefficients in $\mathbb{K}$, is an ordered tuple of elements in $\mathbb{K}$, typically written as

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \in \mathbb{M}_{m\times n}(\mathbb{K})$$

Definition 2.7 (Matrix Multiplication). If $T_1 \in \mathbb{M}_{m\times n}(\mathbb{K}), T_2 \in \mathbb{M}_{n\times l}(\mathbb{K})$ then $T_1 \cdot T_2 \in \mathbb{M}_{m\times l}(\mathbb{K})$ (where $m, n, l \in \mathbb{N}$). Specifically,

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \cdots & \vdots \\ a_{m1} & a_{m2} & \cdots & \cdots & a_{mn} \end{bmatrix} \cdot \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1l} \\ b_{21} & b_{22} & \cdots & b_{2l} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nl} \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} & \cdots & \cdots & c_{1l} \\ c_{21} & c_{22} & \cdots & \cdots & c_{2l} \\ \vdots & \vdots & \ddots & \cdots & \vdots \\ c_{m1} & c_{m2} & \cdots & \cdots & c_{ml} \end{bmatrix}$$

where

$$\begin{aligned} c_{ij} &= \text{ the "inner product" of i-th row of } T_1 \text{ and j-th row of } T_2 \\ &= \sum_{t=1}^{n} a_{it} b_{tj} \\ &\forall\, (i, j), 1 \leq i \leq m, 1 \leq j \leq l \end{aligned}$$

In particular, if $T_1, T_2 \in \mathbb{M}_n := \mathbb{M}_{n\times n}(\mathbb{K})$ then $T_1 \cdot T_2$ and $T_2 \cdot T_1$ are both valid. In general, they're often not equal.

Observe. We can write system of linear equations as

$$T \cdot \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}$$

where

$$T \in \mathbb{M}_{m\times n}(\mathbb{K}), \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \in \mathbb{M}_{n\times 1}(\text{indeterminants}), \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix} \in \mathbb{M}_{m\times 1}(\mathbb{K})$$

Then, finding solutions to S is equivalent to finding $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{K}$ such that

$$T \cdot \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}$$

Exercise 2.1. If $T_1, T_2, T_3 \in \mathbb{M}_n(\mathbb{K})$ then $(T_1 \cdot T_2) \cdot T_3 = T_1 \cdot (T_2 \cdot T_3)$. This is by no means obvious.

Definition 2.8 (Identity Matrix)**.**

$$I_n = id_n = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \ddots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \vdots & 0 & \ddots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix} \in \mathbb{M}_n(\mathbb{K})$$

Observe.

$$I_n \cdot T = T \cdot I_n, \forall\, T \in \mathbb{M}_n(\mathbb{K})$$

Thus, $(\mathbb{M}_n(\mathbb{K}), \cdot)$ is "trying" to be a group, but it's not.

Definition 2.9 (Invertible Matrix)**.** A matrix $T\mathbb{M}_n(\mathbb{K})$ is **invertible** if $\exists\, T' \in \mathbb{M}_n(\mathbb{K})$ such that $T \cdot T' = I_n$

Exercise 2.2. If $T \cdot T' = I_n \Rightarrow T' \cdot T = I_n$

Definition 2.10 (General Linear Group $GL_n(\mathbb{K})$)**.**

$$GL_n(\mathbb{K}) = \{T \in \mathbb{M}_n(\mathbb{K}) \mid T \text{ is invertible}\}$$

Remark. Then $GL_n(\mathbb{K})$ is a group.

Definition 2.11 (Elementary Row operations). Let S be the system of equations:

$$\sum a_{1j}x_j = b_1 \quad (1)$$
$$\sum a_{2j}x_j = b_2 \quad (2)$$
$$\vdots = \vdots$$
$$\sum a_{mj}x_j = b_m \quad (m)$$

then there are 3 **elementary row operations**:

1. Switching 2 of the equations
2. Replace (i) with $c \cdot$ (i) where $c \neq 0$
3. Replace (i) by (i) + d(j) where $i \neq j$

Proposition 2.2. If S' can be obtained from S via a finite sequence of elementary row operations then $S \sim S'$.

Corollary 2.1. S can also be obtained from S' via a finite sequence of elementary row operations.

Corollary 2.2. If S' can be obtained from S via a finite sequence of elementary row operations then they have the same solutions.