Vv214 Linear Algebra

First Midterm Exam - Review class

Li Yuzhou (Cr. Du Yang)

SJTU-UM Joint Institute
Shanghai Jiao-Tong University

June 15, 2019

Table of Contents

Table of Contents

Linear Equation

Definition

In mathematics, a **linear equation** is an equation that may be put in the form

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n + b = 0,$$

where $x_1, \cdots, x_n$ are the variables (or unknowns or indeterminates), and $b, a_1, \cdots, a_n$ are the coefficients, which are often real numbers.

System of linear equations

Definition

In mathematics, a **system of linear equations** has the form

$$\left| \begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1m}x_m &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2m}x_m &= b_2 \\ &\vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nm}x_m &= b_n \end{aligned} \right|$$

where here a_{ij} , b_i are coefficients and x_i are unknowns.

Matrix

We can write a system of linear equations in to a matrix form.

Coefficient Matrix

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{bmatrix} \in \mathbb{R}^{n \times m}$$

Augmented Matrix

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2m} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \ldots \\ a_{n1} & a_{n2} & \cdots & a_{nm} & b_n \end{bmatrix} \in \mathbb{R}^{n \times (m+1)}$$

Remark

1. For a specific system of linear equations, we use the augmented matrix.
2. Know how to judge the number of solutions to an augmented matrix.

Reduced Row-Echelon Form

A matrix is in **reduced row-echelon form(rref)** if it satisfies all of the following conditions:

- If a row has nonzero entries, then the first nonzero entry is a 1, called the **leading 1** (or **pivot**) in this row.
- If a column contains a leading 1, then all the other entries in that column are 0.
- If a row contains a leading 1, then each row above it contains a leading 1 further to the left.

Definition

The **rank** of a matrix A is the number of leading 1's in rref(A).

Elementary Row Operation

Types of elementary row operations

- Divide a row by a nonzero scalar.
- Subtract a multiple of a row from another row.
- Swap two rows.

Remarks

- The elementary row operations will NOT change the rank of a matrix, and will NOT change the solution of a system of linear equations.
- Rank(A)= Max number of independent row vectors of $A =$ Max number of independent column vectors of A.

Table of Contents

Problem

Let A be the following 3×3 matrix:

$$A = \begin{bmatrix} 1 & 0 & 3 \\ 3 & 0 & a \\ 0 & 3 & -a \end{bmatrix}.$$

(a) (6 points) Find all values of a such that the system $A\vec{x} = \vec{0}$ has a unique solution.

(b) (6 points) Find all pairs of values (a, k) such that the system

$$A\vec{x} = \begin{bmatrix} 3 \\ k \\ 9 \end{bmatrix}$$

has infinitely many solutions.

(c) (6 points) For the pairs (a, k) that you found in part (b), find all solutions to the equation

$$A\vec{x} = \begin{bmatrix} 3 \\ k \\ 9 \end{bmatrix}.$$

Express your answer in parametrized form, i.e., as $\{\vec{u} + t\vec{v} : t \in \mathbb{R}\}$.

Answer

(a) (6 points) Find all values of a such that the system $A\vec{x} = \vec{0}$ has a unique solution.

Solution: We row-reduce the augmented matrix:

$$\left[\begin{array}{ccc|c} 1 & 0 & 3 & 0 \\ 3 & 0 & a & 0 \\ 0 & 3 & -a & 0 \end{array}\right] \xrightarrow{\text{III}+\text{II},\text{II}-3\text{I}} \left[\begin{array}{ccc|c} 1 & 0 & 3 & 0 \\ 0 & 0 & a-9 & 0 \\ 3 & 3 & 0 & 0 \end{array}\right] \xrightarrow{\text{II}\leftrightarrow\text{III},\text{II}/3} \left[\begin{array}{ccc|c} 1 & 0 & 3 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & a-9 & 0 \end{array}\right].$$

$$\xrightarrow{\text{II}-\text{I}} \left[\begin{array}{ccc|c} 1 & 0 & 3 & 0 \\ 0 & 1 & -3 & 0 \\ 0 & 0 & a-9 & 0 \end{array}\right]$$

From this we see that the system has a unique solution if and only if $a \neq 9$.

(b) (6 points) Find all pairs of values (a, k) such that the system

$$A\vec{x} = \begin{bmatrix} 3 \\ k \\ 9 \end{bmatrix}$$

has infinitely many solutions.

Solution: For this system to have infinitely many solutions, first of all, we must have $\operatorname{rank}(A) < 3$. From the computation in the previous subpart, this can only happen when $a = 9$. So we may simply consider the case $a = 9$. We row-reduce the augmented matrix:

$$\left[\begin{array}{ccc|c} 1 & 0 & 3 & 3 \\ 3 & 0 & 9 & k \\ 0 & 3 & -9 & 9 \end{array}\right] \xrightarrow{\text{II}-3\text{I},\text{III}/3} \left[\begin{array}{ccc|c} 1 & 0 & 3 & 3 \\ 0 & 0 & 0 & k-9 \\ 0 & 1 & -3 & 3 \end{array}\right] \xrightarrow{\text{II}\leftrightarrow\text{III}} \left[\begin{array}{ccc|c} 1 & 0 & 3 & 3 \\ 0 & 1 & -3 & 3 \\ 0 & 0 & 0 & k-9 \end{array}\right].$$

From this we see that to have infinitely many solutions, we must have $k = 9$ as well. Thus the only pair (a, k) for which we get infinitely many solutions is $(a, k) = (9, 9)$.

Answer

(c) (6 points) For the pairs (a, k) that you found in part (b), find all solutions to the equation

$$A\vec{x} = \begin{bmatrix} 3 \\ k \\ 9 \end{bmatrix}.$$

Express your answer in parametrized form, i.e., as $\{\vec{u} + t\vec{v} : t \in \mathbb{R}\}$.

Solution: From the previous subpart we may assume that $(a, k) = (9, 9)$. The augmented matrix in this case is:

$$\left[\begin{array}{ccc|c} 1 & 0 & 3 & 3 \\ 0 & 1 & -3 & 3 \\ 0 & 0 & 0 & 0 \end{array}\right].$$

There is one "independent" variable, namely x_3 and two "dependent" variables x_1, x_2. The general solution is:

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 3 - 3t \\ 3 + 3t \\ t \end{bmatrix} = \begin{bmatrix} 3 \\ 3 \\ 0 \end{bmatrix} + t \begin{bmatrix} -3 \\ 3 \\ 1 \end{bmatrix}.$$

Table of Contents

Span

Definition

Consider the vectors $v_1, \cdots, v_m$ in $\mathbb{R}^n$. The set of all linear combinations of the vectors $v_1, \cdots, v_m$ is called their **span**:

$$span(v_1, \cdots, v_m) = \{c_1 v_1 + \cdots + c_m v_m : c_1, \cdots, c_m \in \mathbb{R}\}.$$

Linear Independence

Definition

Consider vectors $v_1, \cdots, v_m$ in $\mathbb{R}^n$.

- We say that a vector v_i in the list $v_1, \cdots, v_m$ is **redundant** if v_i is a linear combination of the preceding vectors $v_1, \cdots, v_{i-1}$.
- The vectors $v_1, \cdots, v_m$ are called **linearly independent** if none of them is redundant. Otherwise, the vectors are called **linearly dependent** (meaning that at least one of them is redundant).

Remark

The vectors $v_1, \cdots, v_m$ are linearly independent if and only if

$$c_1 v_1 + \cdots + c_m v_m = 0 \quad \Rightarrow \quad c_1 = \cdots = c_m = 0.$$

Subspace of $\mathbb{R}^n$

Definition

A subset W of the vector space $\mathbb{R}^n$ is called a **(linear) subspace** of $\mathbb{R}^n$ if it has the following three properties:

1. W contains the zero vector in $\mathbb{R}^n$.
2. W is closed under addition: If w_1 and w_2 are both in W, then so is $w_1 + w_2$.
3. W is closed under scalar multiplication: If w is in W and k is an arbitrary scalar, then kw is in W.

Basis

Definition

We say that the vectors $v_1, \cdots, v_m$ form a **basis** of a subspace V of $\mathbb{R}^n$ if they span V **and** are linearly independent. (Also, it is required that vectors $v_1, \cdots, v_m$ be in V.)

Unique representation

Every vector v in V can be expressed **uniquely** as a linear combination of basis,

$$v = c_1 v_1 + \cdots + c_m v_m.$$

Dimension

Consider a subspace V of $\mathbb{R}^n$. The number of vectors in a basis of V is called the **dimension** of V, denoted by $\dim(V)$,

Table of Contents

Kernel and Image

Image

The **image** of a function (not necessarily linear) consists of all the values the function takes in its target space. If f is a function from X to Y ,then

$$image(f) = \{f(x) : x \in X\}.$$

Kernel

The **kernel** of a linear transformation (matrix) A from $\mathbb{R}^m$ to $\mathbb{R}^n$ consists of all zeros of the transformation, that is, the solutions of the equation $Ax = 0$.

Kernel and Image

Remarks

- The image of a linear transformation A is the span of the column vectors of A.
- If A is a linear transformation from $\mathbb{R}^m$ to $\mathbb{R}^n$, then $ker(A)$ is a subspace of $\mathbb{R}^m$ and $image(A)$ is a subspace of $\mathbb{R}^n$.

Dimension Formula

Remarks

- $dim(image(A)) = rank(A)$.

Rank-Nullity Theorem

For any $n \times m$ matrix A, or equivalently a linear transform A from $\mathbb{R}^m$ to $\mathbb{R}^n$, we always have

$$dim(ker(A)) + dim(image(A)) = m.$$

Problem

We give the matrix M and its row reduction. For each question, make clear how you have computed the answer.

$$M = \begin{bmatrix} 1 & 3 & 1 & 2 & 10 & 4 & 4 \\ 5 & 15 & 5 & 2 & 26 & 4 & 4 \\ 4 & 12 & 4 & 1 & 19 & 3 & 3 \\ 5 & 15 & 5 & 3 & 29 & 1 & 1 \end{bmatrix} \qquad \mathrm{rref}(M) = \begin{bmatrix} 1 & 3 & 1 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 1 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

(a) (3 points) What is the rank of M? Why?

(b) (4 points) Give a basis for the image of M and make it clear how you have computed the answer.

(c) (6 points) Give a basis for the kernel of M and make it clear how you have computed the answer.

(d) (5 points) For which value(s) of x and y will the vector $\begin{bmatrix} 1 \\ 2 \\ 1 \\ x \\ y \\ 0 \\ 0 \end{bmatrix}$ be in the kernel of M?

(e) (2 points) Give any basis for the image of M **other than** the one you gave in part (b). This is meant to be easy, if you understand what a basis is.

Answer

(a) (3 points) What is the rank of M?

Solution: The rank of M is the number of pivot columns in rref(M), i.e. the number of columns with leading ones in rref(M). In our case the rank of M is 3.

(b) (4 points) Give a basis for the image of M.

Solution: A basis for the image of M is given by the column vectors in M that become pivot columns in rref(M). So in our case, a basis for the image of M is given by

$$\begin{bmatrix}1\\5\\4\\5\end{bmatrix}, \begin{bmatrix}2\\2\\1\\3\end{bmatrix}, \begin{bmatrix}4\\4\\3\\1\end{bmatrix}.$$

Answer

(c) (6 points) Give a basis for the kernel of M.

Solution: Solving the system of linear equations $Mx = 0$, we obtain

$$\begin{aligned} x_1 + 3x_2 + x_3 + 4x_5 &= 0 \\ x_4 + 3x_5 &= 0 \\ x_6 + x_7 &= 0 \end{aligned}$$

So the general solution is

$$x_2 \begin{bmatrix} -3 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + x_3 \begin{bmatrix} -1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + x_5 \begin{bmatrix} -4 \\ 0 \\ 0 \\ -3 \\ 1 \\ 0 \\ 0 \end{bmatrix} + x_7 \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ -1 \\ 1 \end{bmatrix}$$

where x_2, x_3, x_5, x_7 are arbitrary real numbers. A basis of the kernel of M is given by the list of vectors

$$\begin{bmatrix} -3 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} -1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} -4 \\ 0 \\ 0 \\ -3 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ -1 \\ 1 \end{bmatrix}.$$

Answer

(d) (5 points) For which value(s) of x and y will the vector $\begin{bmatrix} 1 \\ 2 \\ 1 \\ x \\ y \\ 0 \\ 0 \end{bmatrix}$ be in the kernel of M?

Solution: The kernel of the row reduced matrix is the same as the kernel of the original matrix, and this computation is much easier with the row reduced matrix. We have

$$\begin{bmatrix} 1 & 3 & 1 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 1 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 1 \\ x \\ y \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 8+4y \\ x+3y \\ 0 \\ 0 \end{bmatrix}.$$

So this is 0 when $8 + 4y = x + 3y = 0$. In other words, $y = -2$ and $x = 6$.

(e) (2 points) Give any basis for the image of M **other than** the one you gave in part (b). This is meant to be easy, if you understand what a basis is.

Solution: There are many solutions. Perhaps the easiest is to multiply one of the vectors by a scalar, such as 2:

$$\begin{bmatrix} 2 \\ 10 \\ 8 \\ 10 \end{bmatrix}, \begin{bmatrix} 2 \\ 2 \\ 1 \\ 3 \end{bmatrix}, \begin{bmatrix} 4 \\ 4 \\ 3 \\ 1 \end{bmatrix}.$$

Table of Contents

Linear Operation

Definition

A function T from $\mathbb{R}^m$ to $\mathbb{R}^n$ is called a **linear transformation** if there exists an $n \times m$ matrix A such that

$$T(x) = Ax$$

for all x in the vector space $\mathbb{R}^m$.

Properties

If A is an $n \times m$ matrix; x and y are vectors in $\mathbb{R}^m$ and k is a scalar, then

1. $A(x + y) = Ax + Ay$, and
2. $A(kx) = k(Ax)$.

Column Vectors of a Matrix

Remarks

- The i^{th} column vector of the **identical matrix** in $\mathbb{R}^n$ is called **the i^{th} vector of the elementary basis**, denoted by e_i.
- For example, e_2 in $\mathbb{R}^4$ is $\begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$.
- A matrix is a linear transformation which maps e_i to the i^{th} column vector of the matrix.

Inverse of Matrices

Definition

A $n \times n$ matrix A is **invertible** if and only if

- $rref(A) = I_n$ or
- $rank(A) = n$ or
- $det(A) \neq 0$.

Inverse

A matrix A^{-1} is the **inverse** of A if $AA^{-1} = A^{-1}A = I$.

Theorem

$(AB)^{-1} = B^{-1}A^{-1}$.

Find the Inverse

Gauss-Jordan method

$$\begin{bmatrix} A & I \end{bmatrix} \xrightarrow{\text{row elimination}} \begin{bmatrix} I & A^{-1} \end{bmatrix}$$

Adjugate matrix method

$A^* := (cof\ A)^T$, the transpose of the cofactor matrix of A is called an **adjugate matrix** of A. Then

$$A^{-1} = \frac{1}{det(A)} A^*.$$

See the slide of RC3.

Geometric Meaning

Orthogonal Projection Matrix

- $A^2 = A$.
- Column vectors are on a line.

Reflection Matrix

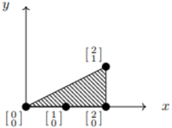
- $A^2 = I$, where I is the identity.
- $A = A^{-1}$.
- The eigenvalues of A equal ± 1.

Rotation, Scaling, Shear

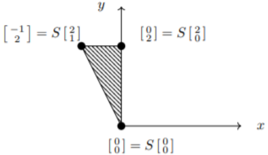
- Recall the general form of the Rotation matrix, Scaling Matrix, Shear and their combination. Refer to the slide in RC3.

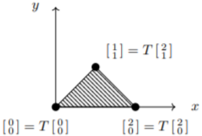
Problem

Consider the triangle Δ with vertices $(0,0)$, $(2,0)$, and $(2,1)$. We have drawn this triangle below.



We have drawn the image of Δ, and each of its vertices, under two linear transformations, S and T



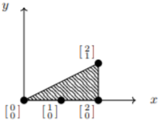


(a) (4 points) Give the matrix of S.

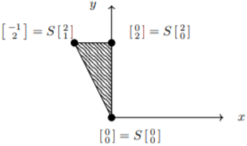
(b) (4 points) Give the matrix of T.

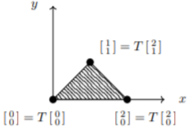
Answer

Consider the triangle Δ with vertices $(0,0)$, $(2,0)$, and $(2,1)$. We have drawn this triangle below.



We have drawn the image of Δ, and each of its vertices, under two linear transformations, S and T





(a) (4 points) Give the matrix of S.

Solution: We have

$$S\begin{bmatrix}1\\0\end{bmatrix} = \frac{1}{2}\cdot S\begin{bmatrix}2\\0\end{bmatrix} = \frac{1}{2}\begin{bmatrix}0\\2\end{bmatrix} = \begin{bmatrix}0\\1\end{bmatrix}$$

$$S\begin{bmatrix}0\\1\end{bmatrix} = S\left(\begin{bmatrix}2\\1\end{bmatrix} - \begin{bmatrix}2\\0\end{bmatrix}\right) = S\begin{bmatrix}2\\1\end{bmatrix} - S\begin{bmatrix}2\\0\end{bmatrix} = \begin{bmatrix}-1\\2\end{bmatrix} - \begin{bmatrix}0\\2\end{bmatrix} = \begin{bmatrix}-1\\0\end{bmatrix}.$$

Therefore, S is represented by

$$\begin{bmatrix}0 & -1\\1 & 0\end{bmatrix}.$$

Alternatively, S is rotation by $\pi/2$, therefore S is represented by

$$\begin{bmatrix}\cos(\pi/2) & -\sin(\pi/2)\\ \sin(\pi/2) & \cos(\pi/2)\end{bmatrix} = \begin{bmatrix}0 & -1\\1 & 0\end{bmatrix}.$$

Answer

(b) (4 points) Give the matrix of T.

Solution: We have

$$T\begin{bmatrix}1\\0\end{bmatrix} = \frac{1}{2}\cdot T\begin{bmatrix}2\\0\end{bmatrix} = \frac{1}{2}\begin{bmatrix}2\\0\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix}$$

$$T\begin{bmatrix}0\\1\end{bmatrix} = T\left(\begin{bmatrix}2\\1\end{bmatrix} - \begin{bmatrix}2\\0\end{bmatrix}\right) = \begin{bmatrix}1\\1\end{bmatrix} - \begin{bmatrix}2\\0\end{bmatrix} = \begin{bmatrix}-1\\1\end{bmatrix}.$$

Therefore, T is represented by $\begin{bmatrix}1 & -1\\0 & 1\end{bmatrix}$.

Remark

Definition 2.2.1 Orthogonal Projections

Consider a line L in the coordinate plane, running through the origin. Any vector $\vec{x}$ in $\mathbb{R}^2$ can be written uniquely as

$$\vec{x} = \vec{x}^{\parallel} + \vec{x}^{\perp},$$

where $\vec{x}^{\parallel}$ is parallel to line L, and $\vec{x}^{\perp}$ is perpendicular to L.

The transformation $T(\vec{x}) = \vec{x}^{\parallel}$ from $\mathbb{R}^2$ to $\mathbb{R}^2$ is called the *orthogonal projection of $\vec{x}$ onto L*, often denoted by $\mathrm{proj}_L(\vec{x})$. If $\vec{w}$ is a nonzero vector parallel to L, then

$$\mathrm{proj}_L(\vec{x}) = \left(\frac{\vec{x} \cdot \vec{w}}{\vec{w} \cdot \vec{w}}\right) \vec{w}.$$

In particular, if $\vec{u} = \begin{bmatrix} u_1 \\ u_2 \end{bmatrix}$ is a *unit* vector parallel to L, then

$$\mathrm{proj}_L(\vec{x}) = (\vec{x} \cdot \vec{u})\vec{u}.$$

The transformation $T(\vec{x}) = \mathrm{proj}_L(\vec{x})$ is linear, with matrix

$$\frac{1}{w_1^2 + w_2^2} \begin{bmatrix} w_1^2 & w_1 w_2 \\ w_1 w_2 & w_2^2 \end{bmatrix} = \begin{bmatrix} u_1^2 & u_1 u_2 \\ u_1 u_2 & u_2^2 \end{bmatrix}.$$

In a similar way, we can derive the formula for orthogonal projection and reflection in R^3.

Table of Contents

Concept

Abelian Groups

Definition: A set A with a binary operation $+ : A \times A \to A$, i.e. $x, y \to x + y$, is called an Abelian group provided

1. $x + y = y + x \quad \forall x, y \in A$ (commutativity)
2. $x + (y + z) = (x + y) + z \quad \forall x, y, z \in A$ (associativity)
3. $\exists 0$ s.t. $x + 0 = 0 + x = x \quad \forall x \in A$ (identity)
4. $\forall x \in A \, \exists (-x)$ s.t. $x + (-x) = 0$ (inverse)

Examples:

- $(\mathbb{N}, +)$ no additive inverses
- $(\mathbb{Z}, +)$ Yes $\quad (\mathbb{Q}, +)$ Yes $\quad (\mathbb{R}, +)$ Yes.
- $(\mathbb{Z}, \cdot)$, $(\mathbb{R}, \cdot)$ no multiplicative inverses
- $(\mathbb{Q} \setminus \{0\}, \cdot)$ Yes $\quad (\mathbb{R} \setminus \{0\}, \cdot)$ Yes

Concept

Cyclic Groups

Definition: We say that $a, b \in \mathbb{Z}$ are congruent modulo m, $m \in \mathbb{Z}$ and write $a \equiv b \mod m$ if

$$m | a - b \Rightarrow a - b = k \cdot m$$

Example: $7 + 3 \mod 6 = 4$, $12 \mod 7 = 5$
Definition: We denote $\mathbb{Z}_n$ all integers modulo n ($n > 0$).
Example: $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$
Definition: An Abelian group is cyclic if A is generated by an element: $\exists a \in A \colon A = \langle a \rangle, \quad \langle a \rangle = \{na, n \in \mathbb{Z}\}$

Example: $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\} \Rightarrow \langle 0 \rangle = \{0\}, \langle 1 \rangle = \mathbb{Z}_7,$

$$\langle 2 \rangle = \{0, 2, 4, 6, 1, 3, 5\}, \langle 3 \rangle = \{0, 3, 6, 2, 5, 1, 4, \} = \mathbb{Z}_7$$

1, 2, 3 are the generators of $\mathbb{Z}_7$. Other generators of $\mathbb{Z}_7$?

Concept

Is $\mathbb{Z}_n$ a linear space?

- Well, scalar multiplication in $\mathbb{Z}_n$ over number fields is not defined. We define a general field:
- **Definition:** A set $\mathbb{F}$ is called a field provided it is an additive Abelian group with the additive inverse 0 and nonzero elements of $\mathbb{F}$ form a multiplicative Abelian group with the multiplicative inverse 1. AND Multiplication distributes addition

  Is $\mathbb{Z}_n$ a field?
- Consider $\mathbb{Z}_4 = \{0, 1, 2, 3\}$.

  In $\mathbb{Z}_4$, $2 \cdot 2 = 4 = 0 \mod 4 \Rightarrow 2$ does not have a multiplicative inverse.

  $\mathbb{Z}_n$ is a field if $n = p$ is a prime number.

  $\mathbb{F}_2 = \mathbb{Z}_2 = \{0, 1\}$ is an important example of a finite field.

Table of Contents

Summary

Go over

- The textbook,
- Homework 1-3,
- Slides and exercises on recitation classes.

For exam

- No calculator.
- Good handwriting and clear steps shown contribute to partial credits.
- Make sure your answer is in clear position.