Course Name : Advanced Cryptography
Course Code : ICT-6115
Presentation Topic : Matrix Groups

Submitted By,
Dr. Ziaur Rahman
Assistant Professor,
Dept of ICT, MBSTU

Submitted to,
Urmi Bose
IT23620
Dept of ICT, MBSTU

Content

Definition of a Matrix

Matrices are the rectangular arrangement of numbers, expressions, symbols which are arranged in columns and rows.

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ . & . & & . \\ . & . & & . \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

An $m \times n$ matrix with entries in R represents a linear transformation from R_n to R_m. If we write vectors $x=(x_1,\ldots,x_n)t$ and $y=(y_1,\ldots,y_n)t$ in R_n as column matrices, then an $m \times n$ matrix,

$$A= \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ . & . & & . \\ . & . & & . \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}$$

Some Facts from Linear Algebra

Before we study matrix groups, we must recall some basic facts from linear algebra. One of the most fundamental ideas of linear algebra is that of a linear transformation. A linear transformation or linear map **$T:R^n \to R^m$** is a map that preserves vector addition and scalar multiplication; that is, for vectors x and y in R^n and a scalar $\alpha \in R$,

$$T(x+y)=T(x)T(y)$$

$$T(\alpha y)=\alpha T(y)$$

Now, maps the vectors to R_m
linearly by matrix multiplication. Observe that if α is a real number,

$$A(x+y) = Ax + Ay \quad \text{and} \quad \alpha Ax = A(\alpha x),$$

Where,

$$x = \begin{pmatrix} x_1 \\ x_2 \\ \cdots \\ \cdots \\ x_n \end{pmatrix}$$

We will often abbreviate the matrix A by writing (aij)

Example

Question: If we let $T:R_2 \to R_2$
be the map given by

$T(x_1,x_2)=(2x_1+5x_2,-4x_1+3x_2)$,

the axioms that T
must satisfy to be a linear transformation are easily verified.

Solution:

The column vectors $Te_1=(2,-4)^t$
and $Te_2=(5,3)^t$
tell us that T
is given by the matrix

$$A=\begin{pmatrix} 2 & -4 \\ 5 & 3 \end{pmatrix}$$

The General and Special Linear Groups

The set of all $n \times n$ invertible matrices forms a group called the general linear group. We will denote this group by $GL_n(\mathbb{R})$.

The general linear group has several important subgroups. The multiplicative properties of the determinant imply that the set of matrices with determinant one is a subgroup of the general linear group. Stated another way,

suppose that, **$\det(A) = 1$**

and **$\det(B) = 1$.**

Then **$\det(AB) = \det(A)\det(B) = 1$**

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

This subgroup is called the special linear group and is denoted by **$SL_n(\mathbb{R})$.**

The Orthogonal Group O(n)

I. Another subgroup of $GL_n(\mathbb{R})$ is the orthogonal group. A matrix A is orthogonal if $A^{-1}=A^t$.
II. The orthogonal group consists of the set of all orthogonal matrices. We write $O(n)$ for the $n\times n$ orthogonal group.
III. We leave as an exercise the proof that $O(n)$ is a subgroup of $GL_n(\mathbb{R})$.

Symmetry

In Mathematics, symmetry means that one shape is identical to the other shape when it is moved, rotated, or flipped. If an object does not have symmetry, we say that the object is asymmetrical. The concept of symmetry is commonly found in geometry.

Types of Symmetry

Symmetry can be viewed when you flip, turn or slide an object. There are four types of symmetry that can be observed in various cases.

- Translational symmetry
- Rotational symmetry
- Reflexive symmetry
- Glide symmetry

References

1. https://www.cuemath.com/geometry/symmetry/
2. https://www.britannica.com/science/matrix-mathematics
3. https://math.libretexts.org/Bookshelves/Abstract_and_Geometric_Algebra/Abstract_Algebra%3A_Theory_and_Applications_(Judson)/12%3A_Matrix_Groups_and_Symmetry/12.01%3A_Matrix_Groups

Thank You