Assignment 1

Let R be a commutative ring.

Definition 1. A *matrix with coefficients in R* is a rectangular array where each entry is an element of R.

Matrix A as shown in Equation 1 is said to have m *rows*, n *columns* and is of size $m \times n$. The *transpose* of A, denoted $A^\top$, is the $n \times m$ matrix obtained by interchanging the rows and columns of A.

$$A = \begin{pmatrix} a_{00} & \cdots & a_{0(n-1)} \\ a_{10} & \cdots & a_{1(n-1)} \\ & \vdots & \\ a_{(m-1)0} & \cdots & a_{(m-1)(n-1)} \end{pmatrix}, \quad A^\top = \begin{pmatrix} a_{00} & \cdots & a_{(m-1)0} \\ a_{01} & \cdots & a_{(m-1)1} \\ & \vdots & \\ a_{0(n-1)} & \cdots & a_{(m-1)(n-1)} \end{pmatrix}. \tag{1}$$

The ith row of A is

$$\begin{pmatrix} a_{i0} & a_{i1} & \ldots & a_{i(n-1)} \end{pmatrix},$$

and the jth column of A is

$$\begin{pmatrix} a_{0j} \\ a_{1j} \\ \vdots \\ a_{(m-1)j} \end{pmatrix},$$

where a_{ij} denotes the entry of the ith row and jth column.

An $n \times n$ matrix is called a *square matrix* (i.e. a matrix with the same number of rows and columns). If A is a square matrix and $a_{ij} = 0$ for $i \neq j$, A is said to be a *diagonal matrix*. An $n \times n$ *identity matrix*, denoted I_n, is an $n \times n$ diagonal matrix whose diagonal entries are 1 and all the other entries are 0, i.e. $a_{ii} = 1$ for $i = 0, 1, \ldots, n-1$ and $a_{ij} = 0$ for $i \neq j$. A $1 \times n$ matrix is called a *row vector*. An $n \times 1$ matrix is called a *column vector*.

We define the *addition* of two $m \times n$ matrices component-wise:

$$\begin{aligned} &\begin{pmatrix} a_{00} & \cdots & a_{0(n-1)} \\ a_{10} & \cdots & a_{1(n-1)} \\ & \vdots & \\ a_{(m-1)0} & \cdots & a_{(m-1)(n-1)} \end{pmatrix} + \begin{pmatrix} b_{00} & \cdots & b_{0(n-1)} \\ b_{10} & \cdots & b_{1(n-1)} \\ & \vdots & \\ b_{(m-1)0} & \cdots & b_{(m-1)(n-1)} \end{pmatrix} \\ &= \begin{pmatrix} a_{00} + b_{00} & \cdots & a_{0(n-1)} + b_{0(n-1)} \\ a_{10} + b_{10} & \cdots & a_{1(n-1)} + b_{1(n-1)} \\ & \vdots & \\ a_{(m-1)0} + b_{(m-1)0} & \cdots & a_{(m-1)(n-1)} + b_{(m-1)(n-1)} \end{pmatrix}. \end{aligned} \tag{2}$$

Definition 2. The *scalar product* of a $1 \times n$ row vector $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ with an $n \times 1$ column vector $\mathbf{w} = (w_0, w_1, \ldots, w_{n-1})^\top$ is given by

$$\mathbf{v} \cdot \mathbf{w} = (v_0, v_1, \ldots, v_{n-1}) \begin{pmatrix} w_0 \\ w_1 \\ \vdots \\ w_{n-1} \end{pmatrix} = \sum_{i=0}^{n-1} v_i w_i$$

Question 1. (3 marks)

a) (0.5 mark) Let $R = \mathbb{Z}$. Matrix A defined below is a 2×2 matrix with coefficients in $\mathbb{Z}$. $a_{00} = 9$ and $a_{01} = 1$.

$$A = \begin{pmatrix} 9 & 1 \\ 0 & -2 \end{pmatrix}$$

What are a_{10} and a_{11}?

b) (0.5 mark) Let $R = \mathbb{Z}$. The identity matrices I_2 and I_3 are given by

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

What is I_4?

c) (0.5 mark) Let $R = \mathbb{Z}$. The matrix

$$\begin{pmatrix} 5 & 0 \\ 0 & -1 \end{pmatrix}$$

is a diagonal matrix. Provide another example of a diagonal matrix.

d) (0.5 mark) Below is an example of addition between two 2×2 matrices with coefficients in $\mathbb{Z}$:

$$\begin{pmatrix} 2 & 3 \\ 1 & 1 \end{pmatrix} + \begin{pmatrix} 4 & 2 \\ 0 & 5 \end{pmatrix} = \begin{pmatrix} 6 & 5 \\ 1 & 6 \end{pmatrix}.$$

Now, let $R = \mathbb{Z}_6$. Compute the addition between the following two matrices:

$$\begin{pmatrix} 2 & 3 \\ 1 & 1 \end{pmatrix} + \begin{pmatrix} 4 & 2 \\ 0 & 5 \end{pmatrix} \mod 6 = ?$$

e) (1 mark) Let $R = \mathbb{Z}$. The scalar product of $\begin{pmatrix} 2 & 3 \end{pmatrix}$ and $\begin{pmatrix} 4 & 0 \end{pmatrix}^\top$ is

$$\begin{pmatrix} 2 & 3 \end{pmatrix} \begin{pmatrix} 4 \\ 0 \end{pmatrix} = 2 \times 4 + 3 \times 0 = 8 + 0 = 8.$$

In case $R = \mathbb{Z}_5$, what is the scalar product of $\begin{pmatrix} 2 & 3 \end{pmatrix}$ and $\begin{pmatrix} 4 & 0 \end{pmatrix}^\top$?

Question 2. (5 marks) Recall that a group $(G, \cdot)$ is a non-empty set G with a binary operation $\cdot$ satisfying the following conditions:

1. G is closed under $\cdot$, $\forall g_1, g_2 \in G$, $g_1 \cdot g_2 \in G$ (closure)
2. $\cdot$ is associative, $\forall g_1, g_2, g_3 \in G$, $g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3$
3. $\exists e \in G$, an identity element, s.t. $\forall g \in G$, $e \cdot g = g \cdot e = g$
4. Every $g \in G$ has an inverse $g^{-1} \in G$ s.t. $g \cdot g^{-1} = g^{-1} \cdot g = e$

During the lecture, we have seen proof that $(\mathbb{R}_{>0}, \times)$ is a group. Let n be a positive integer. We define $\mathcal{M}_{n \times n}(R)$ to be the set of $n \times n$ square matrices with coefficients in R. Prove that $\mathcal{M}_{n \times n}(R)$ together with addition defined in Equation 2 is an abelian group.

Question 3. (2 marks) During the lecture, we discussed that a byte can be considered as an element in $\mathbb{F}_2/(f(x))$, where $f(x) = x^8 + x^4 + x^3 + x + 1$. Consequently, we can define the addition and multiplication between bytes using the addition and multiplication in $\mathbb{F}_2/(f(x))$.

We have also seen that $\mathbb{F}_2/(f(x)) \cong \mathbb{F}_{2^8}$. In particular, $\mathbb{F}_2/(f(x))$ is a commutative ring. Compute the scalar product of the following two vectors with coefficients in $\mathbb{F}_2/(f(x))$.

$$\begin{pmatrix} \texttt{02} & \texttt{03} & \texttt{01} & \texttt{01} \end{pmatrix} \begin{pmatrix} \texttt{D4} \\ \texttt{BF} \\ \texttt{5D} \\ \texttt{30} \end{pmatrix} = ?$$

What is the result of multiplying the following matrix with the column vector? Provide the details of your computations.

$$\begin{pmatrix} \texttt{02} & \texttt{03} & \texttt{01} & \texttt{01} \\ \texttt{01} & \texttt{02} & \texttt{03} & \texttt{01} \\ \texttt{01} & \texttt{01} & \texttt{02} & \texttt{03} \\ \texttt{03} & \texttt{01} & \texttt{01} & \texttt{02} \end{pmatrix} \begin{pmatrix} \texttt{D4} \\ \texttt{BF} \\ \texttt{5D} \\ \texttt{30} \end{pmatrix} = ?$$

What to submit.

- The submission should include detailed solution written in latex
- PDF to be submitted in AIS
- Add full name in both the file name and inside the file

When to submit: by Week 2 Thursday 8 am