Math 4310 Name: Rami Pellumbi (rp534)

Homework 1

Due 9/11/19 at 9:05AM

Please print out these pages. I encourage you to work with your classmates on this homework. Please list your collaborators on this cover sheet. (Your grade will not be affected.) Even if you work in a group, you should write up your solutions yourself! You should include all computational details, and proofs should be carefully written with full details. As always, please write neatly and legibly.

Please follow the instructions for the "extended glossary" on separate paper (LaTeX it if you can!) Hand in your final draft, including full explanations and write your glossary in complete, mathematically and grammatically correct sentences. Your answers will be assessed for style and accuracy.

Please **staple** *this cover sheet, your exercise solutions, and your glossary together, in that order, and hand in your homework in class.*

GRADES

Exercises _____ / 50

Extended Glossary

Component	Correct?	Well-written?
Definition	/6	/6
Example	/4	/4
Non-example	/4	/4
Theorem	/5	/5
Proof	/6	/6
Total	/25	/25

Exercises.

1. Let $\mathbb{F}$ be the field $\mathbb{F} = \mathbb{F}_5 = \mathbb{Z}_5$.

   (a) Find the multiplicative inverse of the elements $1, 2, 3, 4$ of $\mathbb{F}$.

   The multiplicative inverse of $x \in \mathbb{F} = \mathbb{F}_n = \mathbb{Z}_n$ (a finite field) is defined as the element of $x^{-1} \neq 0 \in \mathbb{F}_n$ such that

   $$x \cdot x^{-1} = 1 \tag{1}$$

   Thus for each element in $\mathbb{F}_n$ we multiply it with every other element in $\mathbb{F}_n$ and return the values for which (1) holds. This results in the following inverse pairs:

   (1,1), (2,3), (3,2), (4,4)

   (b) Compute the following in $\mathbb{F}^3$:

   To preface the following problems, it should be noted that the result of adding any combination of elements $a, b, c, ... \in \mathbb{F}_n$ is also in $\mathbb{F}_n$ Likewise, the result of multiplying any combination of elements $a, b, c, ... \in \mathbb{F}_n$ is also in $\mathbb{F}_n$

   (a) $\begin{pmatrix} 2 \\ 4 \\ 1 \end{pmatrix} + \begin{pmatrix} 3 \\ 1 \\ 4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$

   (b) $\begin{pmatrix} 1 \\ 3 \\ 4 \end{pmatrix} + \begin{pmatrix} 4 \\ 0 \\ 3 \end{pmatrix} = \begin{pmatrix} 0 \\ 3 \\ 2 \end{pmatrix}$

   (c) $4 \cdot \begin{pmatrix} 3 \\ 2 \\ 4 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \\ 1 \end{pmatrix}$

(d) $3 \cdot \begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix} = \begin{pmatrix} 1 \\ 4 \\ 2 \end{pmatrix}$

(c) Find a nonzero vector $\begin{pmatrix} a \\ b \\ c \end{pmatrix} \in \mathbb{F}^3$ such that

$$a \begin{pmatrix} 0 \\ 3 \\ 1 \end{pmatrix} + b \begin{pmatrix} 4 \\ 0 \\ 3 \end{pmatrix} + c \begin{pmatrix} 3 \\ 4 \\ 4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 4 & 3 \\ 3 & 0 & 4 \\ 1 & 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$R_2 = R_2 + 2R_3$

$$\begin{pmatrix} 0 & 4 & 3 \\ 0 & 0 & 4 \\ 1 & 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$b = 4$

$$4b + 3c = 0 \rightarrow c = 3$$

$$a + 3b + 4c = 0 \rightarrow a = 1$$

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 1 \\ 4 \\ 3 \end{pmatrix}$$

2. Let $\mathbb{R}^{n\times n}$ denote the $n \times n$ matrices with coefficients in $\mathbb{R}$, for $n \geq 1$. This set has two natural operations, matrix addition $+$ and matrix multiplication $\cdot$. For which n is $\mathbb{R}^{n\times n}$ with these operations a field? (Remember to justify your answers! If it is a field, prove it, if not, give a reason).

   A field is a set $\mathbb{F}$ equipped with the following:

   (a) Two special elements $0 \neq 1 \in \mathbb{F}$
   (b) Operation addition (+): $\mathbb{F} \times \mathbb{F} \to \mathbb{F}$
   (c) Operation multiplication $(\cdot)$: $\mathbb{F} \times \mathbb{F} \to \mathbb{F}$

   $(\mathbb{F}, 0, 1, +, \cdot)$ must satisfy the following axioms

   I. $\forall a, b \in \mathbb{F}$, $a + b = b + a$ and $a \cdot b = b \cdot a$
   II. $\forall a, b, c \in \mathbb{F}$, $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
   III. $\forall a \in \mathbb{F}$, $0 + a = a$ and $1 \cdot a = a$
   IV. $\forall a \in \mathbb{F}, \forall b \neq 0 \in \mathbb{F}, \exists c, d \in \mathbb{F}$ s.t $a + c = 0,$ and $b \cdot d = 1$
   V. $\forall a, b, c \in \mathbb{F}$, $a \cdot (b + c) = a \cdot b + a \cdot c$

   To show $\mathbb{R}^{n\times n}$ *is a field* for some n we need to show it satisfies all the field axioms.

   Whereas to show $\mathbb{R}^{n\times n}$ *is NOT a field* for some n we only need to show ONE axiom does not hold. Lets begin.

   Claim: For n = 1, $\mathbb{R}^{1\times 1}$ is a field.

   Proof: An element of the field $\mathbb{R}^{1\times 1}$ is thus a one element matrix whose coefficient can take on any value in the reals. We define the 0 element to be [0] and the 1 element to be [1].

   We define operation addition between element $A = [a] \in \mathbb{F}$ and $B = [b] \in \mathbb{R}^{1\times 1}$ $(a, b \in \mathbb{R})$ to be [a+b].

   We define operation multiplication between element $A = [a] \in \mathbb{R}^{1\times 1}$ and $B = [b] \in \mathbb{F}$ $(a, b \in \mathbb{R})$ to be $[a \cdot b]$.

   Letting a capital letter denote an element of the field and the corresponding lowercase letter denote the coefficient in that element we show this satisfies the field axioms below.

   I. $\forall A, B \in \mathbb{R}^{1\times 1}$ (as above) we have

   $$A + B = [a] + [b] = [a + b] = [b + a] = [b] + [a] = B + A$$

   and

   $$A \cdot B = [a] \cdot [b] = [a \cdot b] = [b \cdot a] = [b] \cdot [a] = B \cdot A$$

   II. $\forall A, B, C \in \mathbb{R}^{1\times 1}$

   $$A + (B + C) = [a] + ([b] + [c]) = [a] + [b + c] = [a + b + c] = [a + b] + [c] = (A + B) + C$$

   and

   $$A \cdot (B \cdot C) = [a] \cdot [b \cdot c] = [a \cdot b \cdot c] = [a \cdot b] \cdot [c] = (A \cdot B) \cdot C$$

III. $\forall A \in \mathbb{R}^{1\times 1}$

$$0 + A = [0] + [a] = [0 + a] = [a] = A$$

and

$$1 \cdot A = 1 \cdot [a] = [1 \cdot a] = [a] = A$$

IV. $\forall A \in \mathbb{R}^{1\times 1}, \forall B \neq 0 \in \mathbb{R}^{1\times 1}, \exists C, D \in \mathbb{R}^{1\times 1}$ s.t $A + C = 0$, and $B \cdot D = 1$
Since every coefficient of $A, B, C, D \in \mathbb{R}$ this must hold
with multiplication and addition defined as above.

V. $\forall A, B, C \in \mathbb{R}^{1\times 1}$

$$A\cdot(B+C) = [a]\cdot([b]+[c]) = [a]\cdot[b+c] = [a\cdot(b+c)] = [a\cdot b+a\cdot c] = [a\cdot b]+[a\cdot c] = A\cdot B+A\cdot C$$

Claim: For $n \geq 2$, $\mathbb{R}^{n\times n}$ is a **NOT** a field.

Proof: Since the question specifies matrix multiplication as an operation on the field instead of scalar multiplication we will only take a look at the second part of axiom (I) listed above.

$$A \cdot B = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \dots & b_{nn} \end{pmatrix}$$

$$A \cdot B = \begin{pmatrix} (a_{11}\cdot b_{11} + \dots + a_{1n}\cdot b_{n1}) & \dots & (a_{11}\cdot b_{1n} + \dots + a_{1n}\cdot b_{nn}) \\ \vdots & \ddots & \vdots \\ (a_{n1}\cdot b_{11} + \dots + a_{nn}\cdot b_{n1}) & \dots & (a_{n1}\cdot b_{1n} + \dots + a_{nn}\cdot b_{nn}) \end{pmatrix}$$

$$B \cdot A = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \dots & b_{nn} \end{pmatrix} \cdot \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

$$B \cdot A = \begin{pmatrix} (b_{11}\cdot a_{11} + \dots + b_{1n}\cdot a_{n1}) & \dots & (b_{11}\cdot a_{1n} + \dots + b_{1n}\cdot a_{nn}) \\ \vdots & \ddots & \vdots \\ (b_{n1}\cdot a_{11} + \dots + b_{nn}\cdot a_{n1}) & \dots & (b_{n1}\cdot a_{1n} + \dots + b_{nn}\cdot a_{nn}) \end{pmatrix}$$

In general we cannot guarantee equality holds.

$$A \cdot B \neq B \cdot A \textit{ all the time}$$

Thus $\mathbb{R}^{n\times n}$ is only a field for n = 1

3. Let $\mathbb{F}$ be a field. The **characteristic** of $\mathbb{F}$ is defined to be the smallest positive integer p such that $1+1+\cdots+1=0$, where there are p 1's in this formula. If no such sum is 0, then we say the characteristic of $\mathbb{F}$ is 0.

   Know that every field contains the element 1. Since a field is closed under addition we know that the sum of 1 with itself is also in the field. There are thus two outcomes. We either have an infinite number of elements and the sum never equals zero, OR we cycle through the values after reaching the last element in the field implying we have a finite amount of values. If we have a field with a finite number of values we expect the characteristic to be the amount of values in the finite field.

   (a) Find the characteristics of the fields $\mathbb{R}, \mathbb{C}, \mathbb{Z}_p$.

   For $\mathbb{R}$ and $\mathbb{C}$ we have the first case described above (both contain an infinite number of elements) and the characteristic p is zero for both.

   The characteristic p of $\mathbb{Z}_p$ however is not zero. Since we are given that $\mathbb{Z}_p$ is a field we just observe that for an integer finite field with p elements ($p \geq 2$) we must add the element 1 to itself p times in order for

$$(1 + ... + 1) = 0$$

   Thus the characteristic p of $\mathbb{Z}_p$ is p

   (b) If $\mathbb{F}$ is a finite field, show that the characteristic p of $\mathbb{F}$ is not zero.

   A finite field with p elements ($p \geq 2$) must be closed under addition. Thus for some finite number k

$$\underbrace{1 + ... + 1}_{\text{k times}} = 0$$

   by properties of the field.

   (c) If $\mathbb{F}$ is a finite field, show that the characteristic p of $\mathbb{F}$ is a prime number.

   As analysis taught me, let us assume that p is the characteristic of $\mathbb{F}$ and that p is **NOT** a prime number. Let $p = m \cdot n$ for some integer m,n.

   What does this mean? This means that

$$\underbrace{1 + ...1}_{\text{p times}} = (\underbrace{1 + ...1}_{\text{m times}}) \cdot (\underbrace{1 + ...1}_{\text{n times}}) = 0$$

   But we said that p was the characteristic of $\mathbb{F}_n$ and this would mean that m OR n (both smaller than p) would be the characteristic of $\mathbb{F}_n$.

   Contradiction.

   Thus p must be prime.

4. In this problem we will investigate fields with 4 elements.

   (a) If $\mathbb{F}_4$ is a field with exactly 4 elements, what must the characteristic be? (justify your answer, of course! But you may use without proof statements from the previous problem).

   For a field with 4 elements the characteristic must be 2. To see this observe the field $\mathbb{F}_4 = \{0, 1, a, b\}$. A property we want to hold is that every element must have an additive inverse. Thus $a + a = 0$ and $b + b = 0$ must hold. It follows that 1 must be its own additive inverse so that $1 + 1 = 0$

   Thus the characteristic of $\mathbb{F}_4$ is 2

   (b) Find a field $\mathbb{F}_4$ that has 4 elements. Write down the addition and multiplication tables of this field. Remember that two of your elements are 0 and 1!

   Consider the same field as in part (a), $\mathbb{F}_4 = \{0, 1, a, a + 1\}$

   The addition and multiplication tables are:

+	0	1	a	a+1
0	0	1	a	a+1
1	1	0	a+1	a
a	a	a+1	0	1
a+1	a+1	a	1	0

$(\cdot)$	0	1	a	a+1
0	0	0	0	0
1	0	1	a	a+1
a	0	a	a+1	1
a+1	0	a+1	1	a

   (c) Find all fields with 4 elements (i.e. write down all possible addition and multiplication tables. Your first two elements should be 0 and 1).

   See part (b) but a+1 could be any element b so long as the field axioms are satisfied.

5. Show that $\mathbb{C}$ is a vector space over the field $\mathbb{R}$. More generally, if $\mathbb{F} \subset \mathbb{K}$ are both fields (with addition, multiplication, 0, 1, in $\mathbb{F}$. induced from the same operations/elements on $\mathbb{K}$), is $\mathbb{K}$ a vector space over $\mathbb{F}$? (for this one case, you should either provide a counter-example or a one or two line reason, no proof is required this time).

   We know that $\mathbb{R} \subset \mathbb{C}$ since elements of $\mathbb{C}$ can be written as the tuple (a, b) where $a, b \in \mathbb{R}$.

   Thus we must show

   1. $\forall x, y \in \mathbb{C}, x + y \in \mathbb{C}$
   2. $\forall a \in \mathbb{R}, x \in \mathbb{C}, a \cdot x \in \mathbb{C}$

   This is simple since we know that $\mathbb{C}$ is closed under addition and multiplication. Thus $\mathbb{C}$ is a vector space over $\mathbb{R}$.