John Waczak
Mth 443
Homework 1

1 prove that the set $\{0,1\}$ with the following binary operations is a field

$+$	0	1
0	1	0
1	0	1

$*$	0	1
0	0	1
1	1	1

pf: Let $S = \{0,1\}$. To prove that $(S,+,*)$ is a field, I will first show that $(S,+)$ is an abelian group.

1 $(S,+)$ is closed — see table

2 $1+g = g \ \forall g \in S$ (additive identity)

3. as there are only 2 elements in S, I will write out all associative possibilities

$$\underbrace{\begin{aligned}
(0+1)+0 &= 1 = 0+(1+0)\\
(0+1)+1 &= 0 = 0+(1+1)\\
(1+0)+0 &= 1 = 1+(0+0)\\
(1+0)+1 &= 1 = 1+(0+1)\\
(0+0)+0 &= 0 = 0+(0+0)\\
(0+0)+1 &= 1 = 0+(0+1)
\end{aligned}}_{\text{by table}}$$

4. $0^{-1} = 0$ as $0+0 = 1$

$1^{-1} = 1$ as $1+1 = 1$

thus $\forall g \in S \ \exists g^{-1}$ s.t. $g+g^{-1} = g^{-1}+g = id$

finally we see that $(S,+)$ is commutative by the table: $0+1 = 1+0 = 0$.

Thus, $(S,+)$ is an abelian group

1 continued...

Now we must show that $(S, +, *)$ forms a ring

1. associativity

$(0*1)*0 = 1 = 0*(1*0)$

$(0*1)*1 = 1 = 0*(1*1)$

$(1*0)*0 = 1 = 1*(0*0)$

$(1*0)*1 = 1 = 1*(0*1)$

$(0*0)*0 = 0 = 0*(0*0)$

$(0*0)*1 = 1 = 0*(0*1)$

by table

2. distributivity

$(1+0)*1 = 1 = (1*1)+(0*1)$

$(1+0)*0 = 0 = (1*0)+(0*0)$

$(a+1)*1 = 1 = (0*1)+(1*1)$

$(0+1)*0 = 0 = (0*0)+(1*0)$

$(1+1)*0 = 1 = (1*0)+(1*0)$

$(1+1)*1 = 1 = (1*1)+(1*1)$

$(0+0)*0 = 1 = (0*0)+(0*0)$

$(0+0)*1 = 1 = (0*1)+(0*1)$

flipping all to be $a*(b+c)$ still works as $*$ is commutative (next page)

thus we have that $(R, +, *)$ forms a ring.

1 continued... John Waczak

it remains to show that $(S,+,*)$ forms an integral domain w/ multiplicative inverse.

1. $0*g = g \; \forall g \in S$ by table. thus $\exists$ a multiplicative identity in S.
2. $\forall g,h \in S$, $g*h = h*g \in S$ by table. Thus $*$ is commutative
3. The addative identity is 1 and so $S\setminus\{1\} = \{0\}$ in which there are no zero divisors, i.e. $0*0=0$
4. $0*0=0 \Rightarrow 0^{-1}=0$ and 0 is the only element in $S\setminus\{1\}$, thus every non-addative identity element has an inverse

Therefore we have shown that $(S,+,*)$ is an integral domain w/ multiplicative inverses i.e. $(S,+,*)$ is a field

$\square$

2) for 543 only - not applicable

3) if $\mathbb{K}$ and $\mathbb{L}$ are fields and $\mathbb{K} \subset \mathbb{L}$ show that $\mathbb{L}$ is a $\mathbb{K}$-vector space

Recall that V is an F vector space if V is an abelian group $(V, +_V)$ and F is a field $F(+_F, *_F)$ satisfying

1. $\forall \lambda \in F, \forall x, y \in V, \; \lambda(x+y) = \lambda x + \lambda y \in V$
2. $\forall \lambda \in F, \forall x, y \in V, \; (x+y)\lambda = x\lambda + y\lambda \in V$
3. $\forall \lambda, \gamma \in F, x \in V, \; (\lambda\gamma)x = \lambda(\gamma x) \in V$

and in particular

$$0_F \cdot v = \vec{0}_V \quad \text{(zero vector)}$$

$$1_F \cdot v = v$$

~~pf: as $\mathbb{K}$ and $\mathbb{L}$ are fields and $\mathbb{K} \subset \mathbb{L}$, we will show $\mathbb{L}$ is a $\mathbb{K}$-vector space. assuming that $\mathbb{K}$ inherits the same operations from $\mathbb{L}$, we have that $\mathbb{K}$ is an abelian group $(\mathbb{K}, +)$ wrt addition as it is already a Field. thus we have $((\mathbb{K}, +), (\mathbb{L}, +, *))$. Now we must demonstrate scalar multiplication and vector addition.~~

~~$\mathbb{L}$ is a field and therefore $\forall g, h \in \mathbb{L}$ we have $g+h \in \mathbb{L}$. Thus vector addition is defined.~~

John Waczak

3 pf: $\mathbb{K} \subset \mathbb{L}$. assuming that $\mathbb{K}$ is a subfield of $\mathbb{L}$, $\mathbb{K}$ inherits the same operations as $\mathbb{L}$ — $(+, *)$. Thus, since both $\mathbb{L}$ and $\mathbb{K}$ are fields we easily have $((\mathbb{L},+),(\mathbb{K},+,*))$. Now we must show that this space has a properly defined scalar multiplication and vector addition.

$\mathbb{L}$ is a field and, therefore, we have $\forall\, g,h \in \mathbb{L}$ $g+h \in \mathbb{L}$. Thus, $+$ is our vector addition. Furthermore, since $\mathbb{K} \subset \mathbb{L}$, $\forall \lambda \in \mathbb{K}, \forall v \in \mathbb{L}$, $\lambda v \in \mathbb{L}$ as $\lambda \in \mathbb{K} \subset \mathbb{L}$. Thus, $*$ from $\mathbb{K}$ serves as scalar multiplication.

All distributivity laws hold as these are required for the fields $\mathbb{K}$ and $\mathbb{L}$ and so lastly, we identify that the additive and multiplicative identities in $\mathbb{K}$, namely 0 and 1 satisfy

$$0 \cdot v = 0 \qquad \forall v \in \mathbb{L}$$
$$1 \cdot v = v$$

This follows as $\mathbb{K} \subset \mathbb{L}$ and must have an additive and multiplicative identity to be a field. Since $\mathbb{L}$ is also a field, we take $0 \in \mathbb{L}$ to be the additive identity of $\mathbb{L}$.

Therefore we have shown that $\mathbb{L}$ is a $\mathbb{K}$-vector space $\square$

4. $\mathcal{M}_{n\times n}(\mathbb{F})$ is $\{ n\times n \text{ matrices} \mid a_{ij} \in \mathbb{F} \}$ where $\mathbb{F}$ is a field. $\mathcal{M}_{n\times n}(\mathbb{F})$ has standard matrix addition & multiplication.
Let S denote the set of symmetric matrices (i.e. $a_{ij} = a_{ji}$) Show that S is a vector space.

pf: First recall that $\mathcal{M}_{n\times n}(\mathbb{F})$ is a vector space w.r.t. matrix addition and scalar multiplication. We will show S is a subspace of $\mathcal{M}_{n\times n}(\mathbb{F})$ and therefore, also an $\mathbb{F}$-vector space.

1) $a_{ij} = 0$; $1 \leq i,j \leq n \in S$
i.e. the zero matrix
Thus S is non empty.

2) let $A, B \in S$, $\lambda \in \mathbb{F}$.
We w.t.s. $\lambda A + B \in S$.
Recall that a matrix is symmetric if it is equal to its transpose, i.e. if $m_{ij} = m_{ji}$ $\forall i,j \in \{1, \dots n\}$. Thus
The elements of $\lambda A + B$ may be written as $\lambda a_{ij} + b_{ij}$. Observe that

$$(\lambda a_{ij} + b_{ij})^T = \lambda (a_{ij})^T + (b_{ij})^T$$
$$= \lambda a_{ji} + b_{ji}$$
$$= \lambda a_{ij} + b_{ij}$$

since $a_{ij} = a_{ji}$ and $b_{ij} = b_{ji}$ by assumption. Thus linear combinations of elements in S are also in S. This proves S is a subspace of $\mathcal{M}_n(\mathbb{F})$ and is therefore a vector space.

4.

4. continued... John Waczak

Now we want to find a basis for S. Let $\mathcal{B}$ be our basis. Then clearly any diagonal element will be equal to its transpose, i.e. $a_{ij} = a_{ji}$ if $i=j$ so every matrix

$$B \text{ s.t. } \begin{cases} b_{ij} = 1 & \text{for } i=j=\alpha \\ b_{ij} = 0 & \text{otherwise} \end{cases}$$

$\forall\, \alpha \in \{1, n\}$ must be in $\mathcal{B}$.

Next, we need that every matrix

$$B \text{ s.t. } \begin{cases} b_{ij} = b_{ji} = 1 & \text{for } i=\alpha,\ j=\beta \\ b_{ij} = 0 & \text{otherwise} \end{cases}$$

$\forall$ pair $\alpha, \beta \in \{1, \dots, n\}$.

in other words we need every matrix with all zeros and a 1 somewhere on the diagonal, eg $\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & & \\ 0 & 0 & \ddots & & \\ \vdots & & & 1 & \\ 0 & & & & 0 \end{pmatrix}$

and all matrices w/ all zeros except for a pair of 1's symmetric about the diagonal, eg $\begin{pmatrix} 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & & & \\ 1 & 0 & 0 & & & \\ 0 & & & \ddots & & \\ \vdots & & & & & \\ 0 & & & & & 0 \end{pmatrix}$

This set $\mathcal{B}$ forms a basis for S.

5. given nonempty subsets S_1, S_2 of a vector space V, their "sum" is

$$S_1 + S_2 = \{ v + w \mid v \in S_1 ,\ w \in S_2 \}$$

a) suppose that W and Z are subspaces of a vector space V i/s $W+Z$ also a subspace.

pf: Given that W & Z are subspaces of V, we have that $W \neq \emptyset$ and $Z \neq \emptyset$. it follows that $W+Z \neq \emptyset$ but as an example, $0_V \in W$ and $0_V \in Z$, so, $0_V \in W+Z$. Thus, $W+Z$ is non empty. Now let $\lambda \in \mathbb{F}$ (the field of our vector spaces) and $\xi_1, \xi_2 \in W+Z$. Then,

$$\lambda \xi_1 + \xi_2 = \lambda(w_1 + z_1) + (w_2 + z_2)$$

for some $w_1, w_2 \in W$, $z_1, z_2 \in Z$.

$$\lambda(w_1+z_1) + (w_2+z_2) = \lambda w_1 + \lambda z_1 + w_2 + z_2 \text{ (distributivity)}$$
$$= (\lambda w_1 + w_2) + (\lambda z_1 + z_2)$$

Because W & Z are subspaces we have that

$(\lambda w_1 + w_2) \in W$ and

$(\lambda z_1 + z_2) \in Z$

and therefore by the definition of the sum of sets, given in the problem statement, $(\lambda w_1 + w_2) + (\lambda z_1 + z_2) \in W+Z$

$\square$

5. given nonempty subsets S_1, S_2 of a vector space V, their "sum" is

$$S_1 + S_2 = \{ v + w \mid v \in S_1, w \in S_2 \}$$

a) suppose that W and Z are subspaces of a vector space V c/s $W+Z$ also a subspace.

pf: Given that W & Z are subspaces of V, we have that $W \neq \emptyset$ and $Z \neq \emptyset$. It follows that $W+Z \neq \emptyset$ but as an example, $0_V \in W$ and $0_V \in Z$, so, $0_V \in W+Z$. Thus, $W+Z$ is non empty. Now let $\lambda \in \mathbb{F}$ (the field of our vector spaces) and $\xi_1, \xi_2 \in W+Z$. Then,

$$\lambda \xi_1 + \xi_2 = \lambda(w_1 + z_1) + (w_2 + z_2)$$

for some $w_1, w_2 \in W$, $z_1, z_2 \in Z$.

$$\lambda(w_1+z_1) + (w_2+z_2) = \lambda w_1 + \lambda z_1 + w_2 + z_2 \text{ (distributivity)}$$
$$= (\lambda w_1 + w_2) + (\lambda z_1 + z_2)$$

Because W & Z are subspaces we have that

$$(\lambda w_1 + w_2) \in W \text{ and}$$
$$(\lambda z_1 + z_2) \in Z$$

and therefore by the definition of the sum of sets, given in the problem statement, $(\lambda w_1 + w_2) + (\lambda z_1 + z_2) \in W+Z$

$\square$

John Waczak

5.

5. b. We say that V is the "direct sum" of subspaces W, Z if both

(i) $W + Z = V$

(ii) every $v \in V$ can be uniquely written in the form

$v = w + z$ with $w \in W$ and $z \in Z$

we write this as $V = W \oplus Z$.

prove that $V = W \oplus Z$ <u>iff</u> both

(1) $V = W + Z$ and

(2) $W \cap Z = \{0_V\}$

<u>pf:</u>

($\longrightarrow$) Assume that $V = W \oplus Z$. we want to show that (1) and (2) follow.

clearly (1): $V = W + Z$ is true by part (i) of the definition of $W \oplus Z$. Now, assume for contradiction that $W \cap Z \neq \{0_V\}$. Then $\exists\, \tilde{w} \in W$, $\tilde{z} \in Z$ s.t. $\tilde{w} = \tilde{z}$. Consider then that $\exists\, v \in V$ s.t.

$$v = 0_V + \tilde{w}$$

however then $v = 0_V + \tilde{z}$ as $\tilde{w} = \tilde{z}$. This is a <u>contradiction</u> of (ii) as now $v \in V$ but is not uniquely specified by elements of W, Z.

Therefore, we have shown that given $V = W \oplus Z$, (1) and (2) follow.

$(\Leftarrow)$ Assume that

(1) $V = W + Z$

(2) $W \cap Z = \{0_V\}$

we W.T.S. then that $V = W \oplus Z$.

Clearly, (i) holds by assumption of (1). It remains to show that (ii) every $v \in V$ can be uniquely written as $v = w + z$ for some $w \in W$, $z \in Z$.

Assume for contradiction that (ii) is false. Then $\exists\, w' \neq w \in W$, $z' \neq z = Z$ with

$$v = w + z = w' + z'.$$

As $w' \neq w$ and $z' \neq z$ it follows that the only possabibity is that $w = z'$ and $z = w'$. This is a contradiction as w and z are in both W and Z and so $W \cap Z \neq \{0_Z\}$ $\times$

therefore we conclude that given (1) and (2) it follows that $V = W \oplus Z$. This completes the proof.