Math 115A Homework 1

Mateo Umaguing

September 29, 2021

1. (a) Multiplication Tables

Table 2: Multiplication in $\mathbb{Z}/3\mathbb{Z}$

	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Table 3: Multiplication in $\mathbb{Z}/4\mathbb{Z}$

	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

(b) $\mathbb{Z}/p\mathbb{Z}$ is a field when p is prime.
Proof.
$\mathbb{Z}/p\mathbb{Z} \subset \mathbb{Z}/n\mathbb{Z}$
FS1: Commutative addition and multiplication

$$a, b \in \mathbb{Z}/n\mathbb{Z},\ \ a +_n b := a + b \pmod{n}$$
$$\forall a, b \in \mathbb{Z},\ \ a + b = b + a$$
$$a + b \pmod{n} = b + a \pmod{n}$$
$$b + a \pmod{n} = b +_n a$$
$$\therefore a +_n b = b +_n a\ \forall a, b \in \mathbb{Z}/n\mathbb{Z}.$$

$$a, b \in \mathbb{Z}/p\mathbb{Z},\ a \cdot_n b := a + b \pmod n$$
$$\forall a, b \in \mathbb{Z},\ a \cdot b = b \cdot a$$
$$a \cdot b \pmod n = b \cdot a \pmod n$$
$$b \cdot a \pmod n = b \cdot_n a$$
$$\therefore a \cdot_n b = b \cdot_n a\ \forall a, b \in \mathbb{Z}/n\mathbb{Z}.$$

FS2: Associative addition and multiplication

$$a, b, c \in \mathbb{Z}/n\mathbb{Z}, (a +_n b) +_n c = ((a + b \pmod n)) + c) \pmod n$$
$$= (a + (b + c) \pmod n)) \bmod n)$$
$$a +_n (b +_n c) = (a + (b + c)(\text{mod } n)) \pmod n$$
$$\therefore (a +_n b) +_n c = (a + (b + c) \pmod n)) \bmod n) = a +_n (b +_n c)$$
$$\therefore (a +_n b) +_n c = a +_n (b +_n c)$$

$$a, b, c \in \mathbb{Z}/n\mathbb{Z}, (a \cdot_n b) \cdot_n c = ((a \cdot b \pmod n)) \cdot c) \pmod n$$
$$= (a \cdot (b \cdot c) \pmod n)) \bmod n)$$
$$a \cdot_n (b \cdot_n c) = (a \cdot (b \cdot c)(\text{mod } n)) \pmod n$$
$$\therefore (a \cdot_n b) \cdot_n c = (a \cdot (b \cdot c) \pmod n)) \bmod n) = a \cdot_n (b \cdot_n c)$$
$$\therefore (a \cdot_n b) \cdot_n c = a \cdot_n (b \cdot_n c)$$

FS3: Existence of additive and multiplicative identities

$$0 \in \mathbb{Z}/p\mathbb{Z}$$
$$\forall a \in \mathbb{Z}/n\mathbb{Z},\ 0 +_n a := 0 + a \pmod n$$
$$0 + a = a,\ \therefore 0 + a \pmod n = a \pmod n$$
$$\forall a \in \mathbb{Z}/n\mathbb{Z},\ a \pmod n = a$$
$$(\text{Since } a < n\ \forall a \in \mathbb{Z}/n\mathbb{Z})$$
$$\therefore 0 +_n a = a\ \forall a \in \mathbb{Z}/n\mathbb{Z}.$$

$$1 \in \mathbb{Z}/n\mathbb{Z}$$
$$\forall a \in \mathbb{Z}/n\mathbb{Z},\ 1 \cdot_n a := 1 \cdot a \pmod n$$
$$1 \cdot a = a,\ \therefore 1 \cdot a \pmod n = a \pmod n$$
$$\forall a \in \mathbb{Z}/n\mathbb{Z},\ a \pmod n = a$$
$$(\text{Since } a < n\ \forall a \in \mathbb{Z}/n\mathbb{Z})$$
$$\therefore 1 \cdot_n a = a\ \forall a \in \mathbb{Z}/n\mathbb{Z}.$$

FS4: Existence of additive and multiplicative inverses

$$\text{Since } \mathbb{Z}/n\mathbb{Z} := \{0, 1, ..., n-1\},\ a < n\ \forall a \in \mathbb{Z}/n\mathbb{Z}.$$
$$\therefore \exists b \in \mathbb{Z}/n\mathbb{Z} : a + b = n.$$
$$\text{Since } n \pmod n = 0 \text{ and } \exists b \in \mathbb{Z}/n\mathbb{Z}\ \forall a \in \mathbb{Z}/n\mathbb{Z} : a + b = n,$$
$$\forall a \in \mathbb{Z}/n\mathbb{Z}\ \exists b \in \mathbb{Z}/n\mathbb{Z} : a +_n b = 0.$$

For every value in $\mathbb{Z}/p\mathbb{Z}$ in which p is a prime number, the greatest common denominator of any number $a \in \mathbb{Z}/p\mathbb{Z}$ and p is 1.

$$\therefore \exists x, y \in \mathbb{Z} : ax + py = 1$$
$$x = kp + c \text{ for some value } k \in \mathbb{Z}, c \in \mathbb{Z}/p\mathbb{Z}$$
$$\therefore a(kp + c) + py = 1$$
$$akp + ac + py = 1,\ ac + p(ak + y) = 1,\ ac = p(-ak - y) + 1$$
$$\therefore \exists a, c \in \mathbb{Z}/p\mathbb{Z} : a \cdot_n \mathrm{c} = 1$$

FS5: Distributive multiplication

$$\begin{gathered}
a \cdot_n (b +_n c) \\
= (a \cdot (b+c) \pmod n) \pmod n \\
= (a \cdot ((b \pmod n) + (c \pmod n)) \pmod n) \pmod n \\
= ((a \cdot b) \pmod n + (a \cdot c) \pmod n) \pmod n \\
a \cdot_n b +_n a \cdot_n c = ((a \cdot b) \pmod n + (a \cdot c) \pmod n) \pmod n \\
\text{Since both } a \cdot_n (b +_n c) \text{ and } a \cdot_n b +_n a \cdot_n c = ((a \cdot b) \pmod n + (a \cdot c) \pmod n) \pmod n, \\
a \cdot_n (b +_n c) = a \cdot_n b +_n a \cdot_n c \quad \square
\end{gathered}$$

(c) $\mathbb{Z}/n\mathbb{Z}$ is not a field when n is composite.

There does not always exist a multiplicative inverse $b \in \mathbb{Z}/n\mathbb{Z}$ in which $a \cdot_n b = 1 \; \forall a \in \mathbb{Z}/n\mathbb{Z}$.
If n is divisible by some value $a \in \mathbb{Z}/n\mathbb{Z},$ no value of b can by multiplied in $\mathbb{Z}/n\mathbb{Z} : a \cdot_n b = 1$.

For example, 2 multiplied by every number in $\mathbb{Z}/4\mathbb{Z}$ will yield either a 0 or 2 shown above.
None of these values are 1, thus 2 does not have a multiplicative inverse.

(d) Vector spaces over $\mathbb{Z}/2\mathbb{Z}$

$$(\mathbb{Z}/n\mathbb{Z})^2, \; (\mathbb{Z}/n\mathbb{Z})^3, \; (\mathbb{Z}/n\mathbb{Z})^4$$

2. Is $\mathbb{R}$ a vector space over $\mathbb{Q}$?
Yes.

$\mathbb{Q} \subset \mathbb{R},$ and all of $\mathbb{R}$ satisfies all of the axioms for a vector space.
Therefore, $\mathbb{R}$ can be a vector space over $\mathbb{Q}$.

Is $\mathbb{Q}$ a vector subspace of R over $\mathbb{Q}$?
Yes.

Under Theorem 1.3, W is a subspace of a vector space $V \iff$
$\vec{0} \in W, \; \forall x, y \in W, \; x + y \in W, \; \forall \lambda \in F, \; \forall w \in W, \lambda w \in W$
a) $\vec{0} \in \mathbb{Q}$ (0 is a rational number)
b) $x, y \in \mathbb{Q}$. $x + y \in \mathbb{Q}$ since $\mathbb{Q}$ is a field.
c) $\lambda \in \mathbb{Q}, x \in \mathbb{Q}$. $\lambda \cdot x \in \mathbb{Q}$ since both $\lambda, x \in \mathbb{Q}$.

3. **General field-valued functions as vector spaces.**

(a) Addition on elements of $\mathrm{Fun}(S, F)$

$$f, g \in \mathrm{Fun}(S, F)$$
$$(f + g)(x) := f(x) + g(x), x \in S$$

(b) Scalar multiplication of elements of $\mathrm{Fun}(S, F)$ by elements of F

$$f \in \mathrm{Fun}(S, F)$$
$$(\lambda f)(x) := \lambda \cdot f(x), \lambda \in \mathbb{R}, x \in S$$

(c) $\mathrm{Fun}(S, F)$ is a vector space.
Proof.

$\forall f \in \mathrm{Fun}(S, f), f$ abides by the axioms of a field since $\mathrm{Fun}(S, F)$ is over a field F.

VS1 Commutative addition

$$f, g \in \text{Fun}(S, F), x \in S$$
$$(f+g)(x) = f(x) + g(x), x \in S \text{ as defined above}$$
$$(g+f)(x) = g(x) + f(x), x \in S$$
$$g(x) + f(x) = f(x) + g(x), \ \therefore (f+g)(x) = (g+f)(x)$$

VS2 Associative addition

$$f, g, h \in \text{Fun}(S, F), x \in S$$
$$(f+g)(x) + h(x) = f(x) + g(x) + h(x) \text{ by def. of addition}$$
$$f(x) + (g+h)(x) = f(x) + g(x) + h(x) \text{ by def. of addition}$$
$$\therefore (f+g)(x) + h(x) = f(x) + (g+h)(x)$$

VS3 Existence of additive identity

$$0, f \in \text{Fun}(S, F), x \in S$$
$$(f+0)(x) = f(x) + 0$$
$$f(x) + 0 = f(x), \ \therefore \exists 0 \in \text{Fun}(S, F) : (f+0)(x) = f(x)$$
$$0 \text{ is an infinitely differentiable continuous function } \in C^{\infty}(\mathbb{R})$$

VS4 Existence of additive inverse

$$f \in \text{Fun}(S, F), x \in S, \ \exists g \in \text{Fun}(S, F) : (f+g)(x) = 0 \text{ (Since } f \text{ and } g \text{ are field elements)}$$
$$(f+g)(x) = f(x) + g(x) = 0$$
$$\therefore \exists g \in \text{Fun}(S, F) : \forall f, \ (f+g)(x) \ (f+g)(x) = 0$$
$$(g \text{ equals } -f)$$

VS5 Existence of multiplicative identity

$$1, f \in \text{Fun}(S, F), x \in S$$
$$(1 \cdot f)(x) = 1 \cdot f(x) \text{ by def. of multiplication}$$
$$1 \cdot f(x) = f(x), \ \therefore \forall f \in \text{Fun}(S, F), \ (1 \cdot f)(x) = f(x)$$

VS6 Associative multiplication

$$a, b \in \mathbb{R}, f \in \text{Fun}(S, F), x \in S$$
$$a(bf)(x) = a \cdot b \cdot f(x)$$
$$b(af)(x) = b \cdot a \cdot f(x)$$
$$a \cdot b = b \cdot a \text{ by commutative mult. in } \mathbb{R}$$
$$\therefore a(bf)(x) = b(af)(x)$$

VS7 Distributive addition

$$a \in \mathbb{R}, f, g \in \text{Fun}(S, F), x \in S$$
$$a(f+g)(x) = a \cdot (f(x) + g(x)) \text{ by def. of addition}$$
$$a \cdot (f(x) + g(x)) = af(x) + ag(x) \text{ by axiom F5 for fields}$$
$$\therefore a(f+g)(x) = af(x) + ag(x)$$

VS8 Distributive multiplication

$$a, b \in \mathbb{R}, f \in \text{Fun}(S, F), x \in S$$
$$((a+b)f)(x) = (a+b)(f(x))$$
$$a \cdot f(x) + b \cdot f(x) \text{ by distributivity}$$
$$= (af)(x) + (bf)(x) \text{ by def. of addition}$$
$$= (af + bf)(x) = ((a+b)f)(x) \text{ by distributivity} \quad \square$$

(d) The set $\text{Fun}(\mathbb{R},\mathbb{R})$ forms a vector space over $\mathbb{R}$.
Since $\text{Fun}(S,F)$ is a vector space and $\mathbb{R}$ is a set and a field, $\text{Fun}(\mathbb{R},\mathbb{R})$ is a vector space over $\mathbb{R}$.

(e) $C^\infty(\mathbb{R})$ is a vector subspace of $\text{Fun}(\mathbb{R},\mathbb{R})$ over $\mathbb{R}$.
Proof.

$$\text{Under Theorem 1.3, } W \text{ is a subspace of a vector space } V \iff$$
$$\vec{0} \in W,\ \forall x, y \in W,\ x+y \in W,\ \forall \lambda \in F,\ \forall w \in W, \lambda w \in W$$

a) $\vec{0} \in C^\infty(\mathbb{R})$ since 0 is an infinitely differentiable function

b) The sum of two infinitely differentiable continuous function is an infinitely differentiable continuous function.

c) The product of a scalar and an infinitely differentiable continuous function is an infinitely differentiable continuous function.

Since all conditions of being a subspace are met, $C^\infty(\mathbb{R})$ is a subspace of $\text{Fun}(\mathbb{R},\mathbb{R})$ over $\mathbb{R}$. □

4. **Uniqueness of inverses.**
Additive inverses are unique.
Proof.

$$\text{Let } x, y, z \in \text{ vector space } V : x+y=0,\ x+z=0.$$
$$\text{By the definition of the additive inverse, } y \text{ and } z \text{ are additive inverses of } x.$$
$$\text{Since both } x+y \text{ and } x+z=0, x+y=x+z.$$
$$\text{By Theorem 1.1, for some values } x,y,z \in V, \text{ if } x+z=x+y, z=y.$$
$$\therefore \text{ there is a single value in which } y \text{ and } z \text{ are equal to } : x+ \text{ this value } = 0. \quad \square$$

5. **Linear combinations.**

$$\lambda_1 a(x) + \lambda_2 b(x) + \lambda_3 c(x) + \lambda_4 d(x) + \lambda_5 e(x)$$
$$= \lambda_1(x^4 - x) + \lambda_2(x^3 + x^2) + \lambda_3(\sqrt{2}x^2) + \lambda_4(x-1) + \lambda_5(1)$$
$$\text{Let } \lambda_1 = 1, \lambda_2 = 0, \lambda_3 = 2\sqrt{2}, \lambda_4 = 1, \lambda_5 = (1-\sqrt{2})$$
$$\text{(All of these numbers} \in \mathbb{R})$$
$$\lambda_1 a(x) + \lambda_2 b(x) + \lambda_3 c(x) + \lambda_4 d(x) + \lambda_5 e(x)$$
$$= 1 \cdot (x^4 - x) + 2\sqrt{2} \cdot (\sqrt{2}x^2) + 0 \cdot (x^3 + x^2) + 1 \cdot (x-1) + (1-\sqrt{2}) \cdot (1)$$
$$= x^4 - x + 4x^2 + x - 1 + 1 - \sqrt{2}$$
$$= x^4 + 4x^2 - \sqrt{2}$$

$$\lambda_1 = 1, \lambda_2 = 0, \lambda_3 = 2\sqrt{2}, \lambda_4 = 1, \lambda_5 = (1-\sqrt{2})$$

6. 1.2 # 2, 3
2. Zero vector of $M_{3\times 4}(F)$

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

3. M_{13}, M_{21}, and M_{22}

$$M = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$$
$$M_{13} = 3, M_{21} = 4, M_{22} = 5$$

7. 1.2 # 13

Is V a vector space over $\mathbb{R}$ with these operations?

No. VS8 fails.

VS8. Distributive multiplication

$$\text{Let } x \in V : x = (x_1, x_2), a, b \in \mathbb{R}.$$
$$\text{Let } c = a + b, \therefore\ cx = (a + b)x$$
$$\forall a \in V,\ c(a_1, a_2) = (ca_1, a_2). \therefore c(x_1, x_2) = (cx_1, x_2)$$
$$(cx_1, x_2) = ((a + b)x_1, x_2) = (ax_1 + bx_1, x_2) \text{ by distributivity in } \mathbb{R}$$
$$ax + bx = a(x_1, x_2) + b(x_1, x_2) = (ax_1, x_2) + (bx_1, x_2) \text{ by def. of scalar mult. in } V$$
$$(ax_1, x_2) + (bx_1, x_2) = (ax_1 + bx_1, x_2^2) \text{ by def. of addition in } v$$
$$(ax_1 + bx_1, x_2^2) \neq (ax_1 + bx_1, x_2), \therefore \text{ since } (ax_1 + bx_1, x_2^2) = ax + bx \text{ and } (ax_1 + bx_1, x_2) = (a + b)x,$$
$$(a + b)x \neq ax + bx.$$

Since VS8 fails, V is not a vector space.

8. 1.3 #5

Proof.

$$\text{For any } n \times n \text{ matrix, } A,\ A^t_{ij} = A_{ji}, \forall i, j \in n.$$
$$\text{The addition of two } n \times n \text{ matrices } A \text{ and } B \text{ is } A + B = C.\ C_{ij} = A_{ij} + B_{ij}\ \forall i, j \in n.$$
$$\text{Let } A + A^t = C \text{ in which } C_{ij} = A_{ij} + A^t_{ij}. \text{ Since } A^t_{ij} = A_{ji},$$
$$C_{ij} = A_{ij} + A_{ji}\ \forall i, j \in n.$$
$$C_{ji} = A_{ji} + A^t_{ji}, \text{ and } A^t ji = A_{ij}.$$
$$\therefore C_{ji} = A_{ji} + A_{ij}.$$
$$A_{ij} + A_{ji} = A_{ji} + Aij \text{ by the commutative property of addition, } \therefore C_{ij} = C_{ji}\ \forall i, j \in n.$$
$$\text{Since } C_{ij} = C_{ji},\ C = A + A^t \text{ is symmetric for all } n \times n \text{ matrices.} \quad \square$$

9. 1.3 # 27

V is a direct sum of W_1 and W_2.

Proof.

$$W_1 \text{ consists of all diagonal matrices. Thus, } W_1 = \{A \in V : A_{ij} = 0 \text{ whenever } i \neq j\}$$
$$W_2 = \{A \in V : A_{ij} = 0 \text{ whenever } i \geq j\}$$
$$W_2 \text{ consists of all upper triangular matrices but with the elements along the diagonal equal to 0.}$$
$$W_1 \cap W_2 = \{A \in V : A_{ij} = 0\}$$

The only matrix that is both a diagonal matrix and an upper triangular matrix with diagonal elements equal to 0 is the zero vector,

$$\begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & \vdots \\ \vdots & \dots & \ddots & \vdots \\ 0 & \dots & \dots & 0 \end{pmatrix}$$
$$\therefore W_1 \cap W_2 = \vec{0}$$
$$\text{Since } W_1 \cap W_2 = \vec{0} \text{ and } W_1 \text{ and } W_2 \text{ are subspaces of } V,\ W_1 \oplus W_2 = V \quad \square$$