MATH 110: LINEAR ALGEBRA
HOMEWORK #1

CHU-WEE LIM

(1) Let us suppose $x, y, z \in F$, such that $x + z = y + z$. There exists an additive inverse of z, i.e. we can find $z' \in F$ such that $z + z' = z' + z = 0_F$. Then

$$x + z = y + z \Rightarrow (x + z) + z' = (y + z) + z' \Rightarrow x + (z + z') = y + (z + z')$$
$$\Rightarrow x + 0_F = y + 0_F \Rightarrow x = y.$$

(2) Since $\mathbb{Z}_2$ has only 2 elements, to verify the axioms, we can check all possible cases. E.g. to check distributivity:

$$0(0 + 0) = 0 \cdot 0 + 0 \cdot 0, \text{ since they are both } 0;$$
$$0(0 + 1) = 0 \cdot 0 + 0 \cdot 1, \text{ since they are both } 0;$$
$$0(1 + 0) = 0 \cdot 1 + 0 \cdot 0, \text{ since they are both } 0;$$
$$0(1 + 1) = 0 \cdot 1 + 0 \cdot 1, \text{ since they are both } 0;$$
$$1(0 + 0) = 1 \cdot 0 + 1 \cdot 0, \text{ since they are both } 0;$$
$$1(0 + 1) = 1 \cdot 0 + 1 \cdot 1, \text{ since they are both } 1;$$
$$1(1 + 0) = 1 \cdot 1 + 1 \cdot 0, \text{ since they are both } 1;$$
$$1(1 + 1) = 1 \cdot 1 + 1 \cdot 1, \text{ since they are both } 0;$$

(3) To prove that $\mathbb{Z}_p$ forms a field, we first have to make sense of what $\mathbb{Z}_p$ actually is, and what the addition/product operations are.

Consider the set of integers $\mathbb{Z}$. For $i = 0, 1, \ldots, p - 1$, let A_i be the subset of $\mathbb{Z}$ consisting of all j such that $j \equiv i \pmod{p}$ (i.e. $p|(j - i)$). For example, A_0 comprises of all multiples of p, while $A_1 = \{\ldots, 1, p + 1, 2p + 1, \ldots\}$. Then the disjoint union of $A_0, \ldots, A_{p-1}$ is $\mathbb{Z}$. In other words, if $i \neq j$, then $A_i \cap A_j = \emptyset$; while $A_0 \cup A_1 \cup \cdots \cup A_{p-1} = \mathbb{Z}$.

Now, $\mathbb{Z}_p$ is the set $\{A_0, A_1, \ldots, A_{p-1}\}$ (that's right, it's a set of sets). To add A_i and A_j, we pick any elements $a \in A_i$ and $b \in A_j$. *Now $A_i + A_j$ is simply the unique A_k which contains the integer $a + b$.* Likewise, $A_i \cdot A_j$ is the unique A_l which contains the integer $a \cdot b$. There is a slight caveat here: what if we pick a different $a' \in A_i$ and $b' \in A_j$? It turns out that since

$$a'b' - ab = a'(b' - b) + b(a' - a),$$

we still have $ab \equiv a'b' \pmod{p}$.

Date: September 8.

To make sense of the above abstract definition, let us take $p = 7$. Then we have $A_0, A_1, \ldots, A_6$:

$$A_0 = \{\ldots, 0, 7, 14, \ldots\}, \quad A_1 = \{\ldots, 1, 8, 15, \ldots\}, \quad \textit{etc.}$$

Suppose we want to compute $A_3 \cdot A_4$. Let us pick elements from A_3 and A_4, say $10 \in A_3$ and $18 \in A_4$. Then $18 \cdot 10 = 180 \in A_5$, so we have $A_3 \cdot A_4 = A_5$.

Now that we're done with the definition of $\mathbb{Z}_p$, associativity and commutativity becomes clear. These follow immediately from the fact that addition and multiplication on integers are associative and commutative. For example, to show that $A_i + A_j = A_j + A_i$, let us pick $a \in A_i$ and $b \in A_j$. Then $A_i + A_j$ (*resp.* $A_j + A_i$) is the unique A_k which contains $a + b$ (*resp.* $b + a$). Since a and b are integers, we have $a + b = b + a$.

The tricky part is to verify that $A_1, \ldots, A_{p-1}$ have inverses. Let $a \in A_i$, where $i \neq 0$. There are two ways we can proceed.

- We can use the fact that if p, q are coprime integers, then there exist integers c, d such that $pc + qd = 1$. Hence since a is not a multiple of p, and p is prime, a and p must be relatively prime. Thus, we can find $c, d \in \mathbb{Z}$, such that $ac + pd = 1$. This means $ac \equiv 1 \pmod{p}$ and so the unique A_k which contains c must be the multiplicative inverse of A_i.
- Or, if we're forced to use the hint provided in the problem, consider

  $$a, 2a, \ldots, (p-1)a.$$

  Since p is prime and a is not a multiple of p, none of the above numbers is a multiple of p. So each of them must belong to some A_k. Now, if none of them belongs to A_1, then we're left with $A_2, A_3, \ldots, A_{p-1}$ ($p - 2$ sets). By pigeonhole principle, two of the numbers (say ma and na) must belong to the same set; whence $ma - na = (m - n)a$ is a multiple of p which contradicts the fact that m, n are distinct elements of $\{1, 2, \ldots, p-1\}$. Hence, one of the na's must belong to A_1, which gives $na \equiv 1 \pmod{p}$.

§1.2: Vector Spaces

Problem 1.

(a) True. This is one of the axioms.
(b) False. Corollary 1 to Theorem 1.1.
(c) False. E.g. $a = b = 1$, and $x = 0_V$ is the zero vector.
(d) False. E.g. $a = 0$, and x, y can be any two distinct vectors.
(e) True. We may regard a vector as a column vector.
(f) False. It should have m rows and n columns.
(g) False. E.g. x^2 and $x + 3$ can be added to give $x^2 + x + 3$.
(h) False. E.g. $x^2 + x$ and $-x^2$ (of degree 2) can be added to give x (of degree 1).
(i) True. The leading coefficient (of x^n) is still nonzero, after mutiplying with a nonzero scalar.
(j) True, since $c \neq 0$ can be written as $c \cdot x^0$ and $x^0 = 1$.
(k) True. That's the definition of $\mathcal{F}(S, F)$ on page 9, example 3.

Problem 7. The function $f \in \mathcal{F}(S, \mathbb{R})$ takes $0 \mapsto 1$, $1 \mapsto 3$; while the function g takes $0 \mapsto 1$, $1 \mapsto 3$. Hence $f+g$ takes $0 \mapsto 1+1=2$ and $1 \mapsto 3+3=6$. Since h takes $0 \mapsto 2$ and $1 \mapsto 6$ as well, we see that $f+g=h$.

Problem 9. To prove corollary 1, let's suppose 0 and $0'$ are both additive identities of V, i.e. $0+x=0'+x=x$ for all $x \in V$. Now, if we let $x=0'$, we get $0+0'=0'$. And if we let $x=0$, we get $0=0'+0=0+0'$. Hence this shows that $0=0'$.

For corollary 2, suppose y and y' are both additive inverses of x, i.e. $x+y=x+y'=0$. Then by cancellation law, $y=y'$.

For theorem 1.2c, we have $a0+a0=a(0+0)=a0=a0+0$. By cancellation law, $a0=0$.

Problem 12. An easy shortcut is to "cheat" and apply the results in §1.3 here. The set W of odd functions is a subset of $V=\mathcal{F}(\mathbb{R},\mathbb{R})$. Let us prove that W is in fact a subspace of V. First, the 0 function is clearly odd since it takes $-t$ to $0=-0$. Now to show that W is closed under addition and scalar multiplication, let $f, g \in W$ and $c \in \mathbb{R}$ be a scalar.

$$(f+g)(-t) = f(-t)+g(-t) = (-f(t))+(-g(t)) = -(f(t)+g(t)) = -(f+g)(t),$$
$$(c \cdot f)(-t) = c \cdot (f(-t)) = c \cdot (-f(t)) = -c \cdot f(t) = -(c \cdot f)(t).$$

Hence, $f+g$ and $c \cdot f$ are odd and hence in W as well.

Problem 15. No, it is not a vector space over $\mathbb{R}$. For instance, if $(0,1) \in V$ and $i=\sqrt{-1} \in \mathbb{C}$, then $i(0,1)=(0,i) \notin V$.

Problem 16. Yes, it is a vector space over $\mathbb{Q}$, because multiplying a real number by a rational number gives us a real number. Hence, multiplying an element of V by a rational number gives us an element of V. The rest of the axioms are easy to verify.

Problem 19. No, distributivity fails. E.g. we have $1(1,1)=(1,1)$ but $2(1,1)=(2,\frac{1}{2})$. Hence, this gives $1(1,1)+1(1,1) \neq (1+1)(1,1)$.

§1.3: Subspaces

Problem 1.

(a) False. This is rather pedantic though. What happens if W is a subset of V that is a vector space, *under some other operations*?
(b) False. That's why we need the axiom $0 \in W$.
(c) True. We can always take the zero subspace $\{0\} \subsetneq V$.
(d) False. It would be true for any two *subspaces* though.
(e) True, since there are only n diagonal entries and all other entries are 0.
(f) False. It's the *sum*.
(g) False. It's not *equal* to $\mathbb{R}^2$ per se, although it certainly is isomorphic (as you'll learn in a few weeks' time).

Problem 2d. The transpose is $\begin{pmatrix} 10 & 2 & -5 \\ 0 & -4 & 7 \\ -8 & 3 & 6 \end{pmatrix}$ while the trace is $10+(-4)+6=12$.

Problem 5. The ij-th entry of the matrix A^t is a_{ji}. Hence, the ij-th entry of $A+A^t$ is $a_{ij}+a_{ji}$. This shows that the ij-th entry and the ji-th entry of $A+A^t$ are the same. Thus $A+A^t$ is symmetric.

Problem 8.

(a) Yes, it contains $(0,0,0)$ since $0 = 3(0)$ and $0 = -0$. Also, suppose (a_1, a_2, a_3) and (b_1, b_2, b_3) are in W_1, and $c \in \mathbb{R}$ is a scalar. Then $a_1 = 3a_2$, $a_3 = -a_2$ and $b_1 = 3b_2$, $b_3 = -b_2$. So this gives: $a_1 + b_1 = 3(a_2 + b_2)$ and $a_3 + b_3 = -(a_2 + b_2)$ which shows that $(a_1 + b_1, a_2 + b_2, a_3 + b_3) \in W_1$ as well.

Finally, $ca_1 = c(3a_2)$ and $ca_3 = -(ca_2)$, so $(ca_1, ca_2, ca_3) = c(a_1, a_2, a_3)$ is in W_1. This shows that W_1 is closed under addition and scalar multiplication.

(b) No, it does not contain 0.

(c) Yes, it contains $(0,0,0)$ since $2(0) - 7(0) + 0 = 0$. Next, if (a_1, a_2, a_3) and (b_1, b_2, b_3) are in W_1, $c \in \mathbb{R}$, then $2a_1 - 7a_2 + a_3 = 2b_1 - 7b_2 + b_3 = 0$. Adding these two equations give $2(a_1 + b_1) - 7(a_2 + b_2) + (a_3 + b_3) = 0$, which shows W_3 is closed under addition. Also, $0 = c(2a_1 - 7a_2 + a_3) = 2(ca_1) - 7(ca_2) + (ca_3)$, which shows that W_3 is closed under scalar multiplication.

(d) Yes, and the proof is identical to (c).

(e) No, it does not contain the zero vector $(0,0,0)$.

(f) No, it is not closed under addition. E.g. it contains $(0, \sqrt{2}, 1)$ and $(0, \sqrt{2}, -1)$ but not $(0, \sqrt{2}, 1) + (0, \sqrt{2}, -1) = (0, 2\sqrt{2}, 0)$.

Problem 9. The vector (a_1, a_2, a_3) is in $W_1 \cap W_3$ iff it lies in both W_1 and W_3. Hence it must satisfy $a_1 = 3a_2$ and $a_3 = -a_2$; as well as $2a_1 - 7a_2 + a_3 = 0$. Solving them, we get $a_2 = 0$ and hence $a_1 = a_3 = 0$. This shows that $W_1 \cap W_3 = \{0\}$.

Using similar techniques, we find that $W_1 \cap W_4 = W_1$ and $W_3 \cap W_4$ consists of all multiples of $(11, 3, -1)$.

Problem 11. No, because W contains $x^n + 1$ and $-x^n + 1$ but not their sum 1.

However, in the alternate problem where W has all $f(x)$ of degree $\leq n$, W is a subspace. Note that W is precisely the set of polynomials of the form $a_0 + a_1 x + \cdots + a_n x^n$, where the a_i's are scalars (possibly zero). Hence if $f(x), g(x) \in W$, then we may write:

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n, \quad g(x) = b_0 + b_1 x + \cdots + b_n x^n,$$

for some scalars a_i's and b_i's. This gives:

$$(f + g)(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n$$

which has degree at most n. Hence $f + g \in W$. Similarly, any constant scalar multiple of f lies in W as well.

Problem 12. Let A and B be upper-triangular matrices. Hence the entries A_{ij} and B_{ij} are 0 whenever $i > j$. This means the entry $(A + B)_{ij} = A_{ij} + B_{ij}$ would also be 0 when $i > j$. Hence, $A + B$ is upper-triangular.

Likewise, if c is a constant scalar, then the entry $(cA)_{ij} = c \cdot A_{ij}$ would also be 0 when $i > j$. Hence cA is upper-triangular. Finally, the zero matrix is clearly upper-triangular. Thus, the upper-triangular matrices form a subspace of $M_{m \times n}(F)$.

Problem 15. Yes. Again, suppose $f, g \in C(\mathbb{R})$ are differentiable functions $\mathbb{R} \to \mathbb{R}$. By elementary calculus, we know that $f + g$ is also differentiable and in fact, $(f + g)'(t) = f'(t) + g'(t)$ for any $t \in \mathbb{R}$. Also, if c is a scalar (i.e. constant function), then $(c \cdot f)'(t) = c \cdot f'(t)$. Finally, the zero function $f(t) = 0$ is clearly differentiable. This shows that the set of differentiable real-valued functions on $\mathbb{R}$ is a subspace of $C(\mathbb{R})$.

Problem 23. (a) To show that $W_1 \subseteq W_1 + W_2$, let $w_1 \in W_1$. Then since $0 \in W_2$, we have $w_1 = w_1 + 0 \in W_1 + W_2$. Hence, this proves our inclusion. The proof for $W_2 \subseteq W_1 + W_2$ is similar.

Next, we have to show $W_1 + W_2$ is a subspace of V:

- Since $0 \in W_1$ and $0 \in W_2$, $0 = 0 + 0 \in W_1 + W_2$.
- Suppose $x \in W_1 + W_2$ and $x' \in W_1 + W_2$. We have to show $x + x' \in W_1 + W_2$. By definition, x is of the form $w_1 + w_2$ for some $w_1 \in W_1, w_2 \in W_2$. Likewise, $x' = w_1' + w_2'$, for some $w_1' \in W_1, w_2' \in W_2$. Hence,
$$x + x' = (w_1 + w_2) + (w_1' + w_2') = (w_1 + w_1') + (w_2 + w_2') \in W_1 + W_2,$$
since $w_1 + w_1' \in W_1$ and $w_2 + w_2' \in W_2$.
- Suppose $x \in W_1 + W_2$ and c is a scalar. Then we can write $x = w_1 + w_2$, where $w_1 \in W_1$ and $w_2 \in W_2$; whence $cx = (cw_1) + (cw_2)$. Since $cw_1 \in W_1$ and $cw_2 \in W_2$, we have $cx \in W_1 + W_2$.

(b) Suppose W is a subspace of V that contains W_1 and W_2. We wish to prove that it contains $W_1 + W_2$. But every element of $W_1 + W_2$ is of the form $w_1 + w_2$ (for some $w_1 \in W_1$ and $w_2 \in W_2$); and $w_1 \in W_1 \subseteq W$ and $w_2 \in W_2 \subseteq W$. Since W is a subspace of V, it is closed under addition and so $w_1 + w_2 \in W$. This shows that W contains $W_1 + W_2$.

Problem 28. To summarize, a square matrix M is symmetric if $M = M^t$ and skew-symmetric if $M^t = -M$. First, we want to show $W_1 \subseteq M_{n\times n}(F)$ is a subspace.

- $0^t = 0 = -0$, so $0 \in W_1$.
- If $A, B \in W_1$, then $A^t = -A$ and $B^t = -B$. Hence, $(A + B)^t = A^t + B^t = (-A) + (-B) = -(A + B)$, so $A + B$ is also in W_1.
- If $A \in W_1$ and c is a scalar, then $(cA)^t = c \cdot A^t = c(-A) = -(cA)$, so cA is also in W_1.

This shows that W_1 is a subspace of $M_{n\times n}(F)$. Our next task is to show that $M_{n\times n}(F)$ is the direct sum of W_1 and W_2. Thus, we have two statements to prove.

- *To show* $W_1 \cap W_2 = \{0\}$: suppose $A \in W_1 \cap W_2$. Hence A is both symmetric and skew-symmetric, i.e. $A^t = A$ and $A^t = -A$. This gives $A + A = 0$, or $2A = 0$. Since the characteristic is not 2, we can divide by 2 to get $A = 0$.
- *To show* $M_{n\times n}(F) = W_1 + W_2$: let $A \in M_{n\times n}(F)$ be any $n \times n$ matrix. Write A as the sum:
$$A = \frac{A + A^t}{2} + \frac{A - A^t}{2}.$$
Note that we have no qualms dividing by 2 since the characteristic of F is not 2. Now:
$$\left(\frac{A + A^t}{2}\right)^t = \frac{A^t + A^{tt}}{2} = \frac{A^t + A}{2}, \quad \left(\frac{A - A^t}{2}\right)^t = \frac{A^t - A^{tt}}{2} = \frac{A^t - A}{2} = -\frac{A - A^t}{2}.$$
Since we can write A as a sum of a symmetric matrix and a skew-symmetric matrix, we see that $A \in W_1 + W_2$.

§1.4: Linear Combinations and Systems of Linear Equations

Problem 1.

(a) True. We can take all coefficients to be 0 in the linear combination, which will give us the zero vector.
(b) False. The span of $\emptyset$ is the zero vector space $\{0\}$.
(c) True. That is simply restating theorem 1.5 (page 30).
(d) False, we can multiply by any constant except 0.
(e) True. See step 3 on page 27.
(f) False. For example, $x + y = 1$ and $x + y = 2$ have no simulateneous solutions.

Problem 13. Let w be any element of the span of S_1. This means we can write

$$w = c_1 s_1 + c_2 s_2 + \ldots c_n s_n,$$

for some elements $s_1, \ldots, s_n \in S_1$ and scalars $c_1, \ldots, c_n$. Since S_1 is a subset of S_2, we see that the s_i's are also elements of S_2. Hence, w is a finite linear combination of elements of S_2. This proves that w lies in the span of S_2, and so $span(S_1) \subseteq span(S_2)$.

For the second statement, if $span(S_1) = V$ then $V = span(S_1) \subseteq span(S_2)$ by the above paragraph. On the other hand, since $S_2 \subseteq V$, the span of S_2 must be a subspace of V. Hence $span(S_2) \subseteq V$. By these two inclusions, $span(S_2) = V$.