Homework 3

1. Let V be a vector space over F and $U, W \subset V$ be subspaces. Explain why $U + W$ and $U \cap W$ are subspaces of V. Give an example of a vector space V, and two subspaces W_1, W_2 such that $W_1 \cup W_2$ is not a subspace. Next, give an example where it is a subspace. Can you figure out a general condition for when $W_1 \cup W_2$ is a subspace?

2. Show that the solution set to $A\overline{x} = \overline{b}$ is never a subspace when $\overline{b} \neq \overline{0}$.

3. In this problem we will go over an important construction of vector spaces. Let $W \subset V$ be a subspace. We say that vectors $\overline{x}, \overline{y} \in V$ are *congruent mod W* (and write $\overline{x} \cong \overline{y}(\text{mod W})$) if $\overline{x} - \overline{y} \in W$.

(a) Show that for every $\overline{x} \in V$, $\overline{x} \cong \overline{x}(\text{mod W})$.
(b) Show that for every $\overline{x}, \overline{y} \in V$, if $\overline{x} \cong \overline{y}(\text{mod W})$ then $\overline{y} \cong \overline{x}(\text{mod W})$.
(c) Show that if $\overline{x} \cong \overline{y}(\text{mod W})$ and $\overline{y} \cong \overline{z}(\text{mod W})$ then $\overline{x} \cong \overline{z}(\text{mod W})$.
(d) The previous three parts show that congruence mod W is an *equivalence relation*. Given $\overline{x} \in V$, denote its equivalence class by $[\overline{x}]$. Don't worry if you've never seen these terms before, they're covered in 321. Concretely, $[\overline{x}]$ is the set of all $\overline{y}$ such that $\overline{x} \cong \overline{y}(\text{mod W})$. Let V/W be the collection of all $[\overline{x}]$'s. The set V/W is called the *quotient space* of V by W, We can turn it into a vector space by defining $[\overline{x}] + [\overline{y}] = [\overline{x} + \overline{y}]$ and $c[\overline{x}] = [c\overline{x}]$. Take time to think about these definitions.
(e) Let $V = \mathbb{R}^2$, and W be the y-axis. What is the dimension of V/W?

4. Let $T : V \to W$ be a linear transformation.

(a) Let $U \subset V$ be a subspace of V. Show that $T(U)$ is a subspace of W.
(b) Let $U \subset W$ be a subspace of W. Show that $T^{-1}(U) = \{\overline{x} \in V \mid T(\overline{x}) \in U\}$ is a subspace of V.

5. Suppose we're trying to send a message composed of 1's and 0's. The line we're trying to send the message across has some noise in it which causes some of the bits we send to come out wrong on the other side. If we want to make sure that the person we are sending the message to gets the correct information, we can use something called an error correcting code. This is a method in which we can convert our original message to a longer one which is more resistant to noise - the recipient can recover the correct message, even if a certain percentage of the bits is wrong. In this problem, you will explore two simple error correcting codes. In each one of them, the original message is cut up into small chunks of a fixed size. Each chunk is considered as a vector over F_2. A linear transformation is then applied to this vector to produce a new vector which is the one that is actually sent down the line.

(a) Consider the map $T : F_2 \to F_2^5$ given by $T(x) = (x, x, x, x, x)$. Show that this is a linear transformation.

(b) We can create an error correcting code by taking our original message, cutting it into chunks of size 1, and sending T of each chunk down the line. If our original message was 1010, we would send 1111000011110000 down the line. What would we send down the line if our original message was 0010?

(c) The sender used the error correcting code outlined above. The recipient received the following message: 110111101000. What was the sender's original message?

(d) How much longer is the error correcting code version of a message than the original message? What percentage of the bits can be received incorrectly and still allow the receiver to decode the message?

(e) The following error correcting code is called the Hamming $(7, 4)$ code. It breaks up the original message into chunks of 4 bits, and replaces each 4 bit sequence with a 7 bit message using the linear transformation: $T(x, y, z, w) = (x, y, z, w, x+y+w, x+z+w, y+z+w)$. If we wanted to send the message 01001110, what would we send down the line?

(f) Is this linear transformation injective? Why is this question important in decoding?

(g) To decode a message, find the element of the image of T that has the most bits in common with the message you received. Decode 1101001.

(h) Verify that any two vectors in the image of T differ by at least 3 bits.

(i) If at most 1 out of every 7 bits in a line might be wrong, explain why the $(7, 4)$ Hamming code can always be used to decode messages. What can go wrong if more bits than that are incorrect?