Exercise 1

Let $F$ be a field, $m \geq 0$ a fixed nonnegative integer, and let

$$V = \{a_0 + a_1 x + \cdots + a_m x^m : a_0, \ldots, a_m \in F\}$$

be the vector space consisting of all polynomials over $F$ of degree at most $m$. Suppose that $p_1, p_2, \ldots, p_{m+1} \in V$ are polynomials such that $p_j(1) = 0$ for all $j$. Prove that the vectors $p_1, \ldots, p_{m+1}$ are linearly dependent.

We define $W$ to be the subspace

$$W = \{a_0 + a_1 x + \cdots + a_m x^m : a_0 + a_1 x + \cdots + a_m x^m : a_0, \ldots, a_m \in F, \sum_{i=0}^{m} a_i = 0 \} \subseteq V.$$ 

To see that $W$ is in fact a subspace, we note that for a polynomial $a(x) = a_0 + a_1 x + \cdots + a_m x^m$, the condition $\sum_{i=0}^{m} a_i = 0$ is true if and only if $a(1) = 0$. It is then clear that $0 \in W$, and if $\lambda \in F, a, a' \in W$, we see that $\lambda a(1) = \lambda \cdot 0 = 0$ and $(a + a')(1) = a(1) + a'(1) = 0$; therefore $W$ is closed under scalar multiplication and addition.

Note further that $W \neq V$, because the polynomial $f(x) = x$ is in $V$ but not in $W$.

Now choose a basis $w_1, \ldots, w_r$ of $W$, for $r = \dim W$. By the Basis Theorem (Simon Chapter 1 Section 5 Theorem 5.3), we know that since $w_1, \ldots, w_r \in W$ are linearly independent, there is a basis $v_1, \ldots, v_q$ for $V$ with $q \geq r$ and $v_j = w_j$ for each $j = 1, \ldots, k$.

In fact we must have $q > r$; if $q = r$, then we would be claiming that $w_1, \ldots, w_r$ span $V$, which is impossible since $w_1, \ldots, w_r \in W \neq V$. This means that $\dim W < \dim V$.

Since $\{1, x, \ldots, x^m\}$ span $V$, $\dim V \leq m + 1$. This means that $\dim W \leq m$.

Note that our polynomials $p_1, \ldots, p_{m+1}$ are in $W$ since $p_j(1) = 0$ for all $j$. Therefore the $p_j$ are $m+1$ vectors in $W$, which has dimension $\leq m$. Hence by the linear dependence lemma, the $p_j$ are linearly dependent.
Exercise 2

Let $V$ be a finite dimensional vector space over a field $F$ and suppose that $U_1, \ldots, U_m$ are subspaces of $V$. Define

$$U_1 + \cdots + U_m = \{u_1 + \cdots + u_m : u_j \in U_j \forall 1 \leq j \leq m\}.$$ 

Prove that $\dim(U_1 + \cdots + U_m) \leq \dim U_1 + \cdots + \dim U_m$.

We proceed by induction; we will consider two separate base cases, $m = 1$ and $m = 2$.

The base case $m = 1$ is trivial since $\dim U_1 \leq \dim U_1$.

Now consider $m = 2$. Let $d = \dim U_1, n = \dim U_2$. Then we can choose bases $\{v_1, \ldots, v_d\}$ of $U_1$ and $\{w_1, \ldots, w_n\}$ of $U_2$.

Given any $u_1 + u_2 \in U_1 + U_2$, we see that there exist $c_j \in F, 1 \leq j \leq d, b_i \in F, 1 \leq i \leq n$ so that $u_1 = \sum_{j=1}^{d} c_j v_j$ and $u_2 = \sum_{i=1}^{n} b_i w_i$, because $u_1 \in U_1 = \text{span}(v_j)$ and $u_2 \in U_2 = \text{span}(w_i)$.

Therefore $u_1 + u_2 \in \text{span}(v_1, \ldots, v_d, w_1, \ldots, w_n)$. This implies that $U_1 + U_2 \subseteq \text{span}(v_1, \ldots, v_d, w_1, \ldots, w_n)$; hence $\dim(U_1 + U_2) \leq n + d = \dim U_1 + \dim U_2$. This completes the second base case.

Now we consider the case of general $m \geq 3$. For our inductive hypothesis, we assume that for any $m$ subspaces $V_1, \ldots, V_m$ that $\dim(V_1 + \cdots + V_m) \leq \dim V_1 + \cdots + \dim V_m$. Now we wish to show the same is true for $m + 1$.

Take some $m + 1$ subspaces $U_1, \ldots, U_{m+1}$. We note that the subspace $U_1 + \cdots + U_{m+1}$ is the same as the subspace $(U_1 + \cdots + U_m) + U_{m+1}$. Therefore, applying the second base case, we see that

$$\dim(U_1 + \cdots + U_{m+1}) \leq \dim(U_1 + \cdots + U_m) + \dim U_{m+1}.$$ 

Now we may apply the inductive hypothesis to $U_1 + \cdots + U_m$, so we see that

$$\dim(U_1 + \cdots + U_{m+1}) \leq \dim(U_1 + \cdots + U_m) + \dim U_{m+1} \leq \dim U_1 + \cdots + \dim U_m + \dim U_{m+1}.$$ 

This completes the inductive step and hence completes the proof.

Exercise 3
Determine all values of $\lambda \in \mathbb{R}$ such that the collection of vectors

$$(\lambda, 1, 1), (1, \lambda, 1), (1, 1, \lambda)$$

is linearly dependent.

These three vectors are linearly dependent if and only if there exist $a_1, a_2, a_3 \in \mathbb{R}$, not all 0, so that

$$a_1(\lambda, 1, 1) + a_2(1, \lambda, 1) + a_3(1, 1, \lambda) = (0, 0, 0).$$

Hence these three vectors are linearly dependent if and only if there exist $a_1, a_2, a_3 \in \mathbb{R}$, not all 0, so that

$$\lambda a_1 + a_2 + a_3 = 0$$
$$a_1 + \lambda a_2 + a_3 = 0$$
$$a_1 + a_2 + \lambda a_3 = 0.$$

Subtracting pairs of equations from one another, we find that $(\lambda - 1)a_1 = (\lambda - 1)a_2 = (\lambda - 1)a_3$; hence $a_1 = a_2 = a_3$ unless $\lambda = 1$.

First, we note that if $\lambda = 1$, then all three vectors are the same, so they must be linearly dependent. We therefore assume in what follows that $\lambda \neq 1$ since that case has been covered.

Now we assume $a_1 = a_2 = a_3$. Then, using substitution, we see that $(\lambda + 2)a_1 = 0$. Hence either $\lambda = -2$ or $a_1 = a_2 = a_3 = 0$. Since we are looking for solutions with not all $a_i = 0$, we must have $\lambda = -1$.

Therefore the only $\lambda$ for which these three vectors are linearly dependent are $\lambda = 1$ and $\lambda = -2$.

**Exercise 4**

Suppose that $V$ is a vector space over $F$, that $v_1, \ldots, v_k$ are linearly independent, and that $u \in V$ is any other vector. Show that

$$\dim \text{span}(v_1 + u, \ldots, v_k + u) \geq k - 1.$$

Can equality be achieved?
First we show that equality can be achieved: consider $F = \mathbb{R}, V = \mathbb{R}^3, v_1 = (1, 2, 0), v_2 = (1, 1, 0)$. Then letting $u = (-1, 0, 0)$, we see that
\[ \dim \text{span}((1, 2, 0) + (1, 1, 0) + (-1, 0, 0)) = \dim \text{span}((0, 2, 0), (0, 1, 0)) = 1 = 2 - 1. \]

Let $W = \text{span}(v_1 + u, \ldots, v_k + u)$.

Now we consider the general case. For each $i$ with $1 \leq i \leq k - 1$, note that $v_i - v_k \in \text{span}(v_1 + u, \ldots, v_k + u)$; this is because $v_i - v_k = v_i + u - (v_k + u) \in W$. We will show that \{v_1 - v_k, \ldots, v_{k-1} - v_k\} are linearly independent.

Take $a_1, \ldots, a_{k-1} \in F$ such that $\sum_{i=1}^{k-1} a_i(v_i - v_k) = 0$. Then
\[
- \left( \sum_{j=1}^{k-1} a_j \right) v_k + \left( \sum_{i=1}^{k-1} a_i v_i \right) = 0.
\]

Because \{v_1, \ldots, v_k\} are linearly independent, this means that $a_1, \ldots, a_{k-1}, -\sum_{j=1}^{k-1} a_i$ are all equal to 0. Therefore \{v_1 - v_k, \ldots, v_{k-1} - v_k\} are linearly independent.

Hence $W$ contains $k - 1$ linearly independent vectors, so $\dim W \geq k - 1$.

**Exercise 5**

Let $p$ be a prime and $\mathbb{F}_p$ the finite field with $p$ elements. Prove that every subspace of $\mathbb{F}_p^n$ of dimension $d$ has exactly $p^d$ elements.

Let $W \subset \mathbb{F}_p^n$ be a subspace of dimension $d$; choose a basis \{w_1, \ldots, w_d\} of $W$.

Since the basis must span $W$, we see that any element in $W$ may be written as $a_1w_1 + \cdots + a_dw_d$ for $a_1, \ldots, a_d \in \mathbb{F}_p$.

Therefore, since there are $p$ choices for each $a_i$, there are at most $p^d$ elements in $W$; it remains to show that each choice of $a_i$ gives a unique element of $W$.

Assume we have some $w \in W$ such that $w = a_1w_1 + \cdots + a_dw_d = b_1w_1 + \cdots + b_dw_d$. Then
\[
(a_1w_1 + \cdots + a_dw_d) - (b_1w_1 + \cdots + b_dw_d) = (a_1 - b_1)w_1 + \cdots + (a_d - b_d)w_d = 0.
\]

Then since the $w_i$ are linearly independent, $a_i - b_i = 0$ for all $i$, so $a_i = b_i$ for all $i$. Hence the expression for $w$ is unique.

Therefore $W$ contains exactly $p^d$ elements.
Exercise 6

Let $p$ be a prime. Suppose a town has $n$ residents who form $m$ clubs with the following rules:

(i) The number of members of each club is not a multiple of $p$.

(ii) The number of common members in each pair of distinct clubs is a multiple of $p$.

Prove that $m \leq n$.

Let $L_1, \ldots, L_m$ be the $m$ clubs, and number the residents from 1 to $n$.

We define an $m$ by $n$ matrix $A$ with entries $a_{ij}$ in the field $\mathbb{F}_p$ as follows: $a_{ij}$ is 1 if resident $j$ is in club $L_i$, and 0 otherwise.

Now consider the $m$ by $m$ matrix $AA^T$, with entries $b_{ij}$; then $b_{ij} = \sum_{k=1}^{n} a_{ik}a_{jk}$. Since $a_{ik}a_{jk} = 1$ if and only if resident $k$ is in $L_i \cap L_j$, we see that $b_{ij} = |L_i \cap L_j| \mod p$.

Therefore, by the given rules, $b_{ij} = 0 \in \mathbb{F}_p$ for $i \neq j$, and $b_{ii} \neq 0$ for all $i$.

Hence if some linear combination of the columns of $AA^T$ was 0, we would need $c_1, \ldots, c_m \in \mathbb{F}_p$ such that $c_ib_{ii} = 0$ for all $i$; this would mean $c_1 = \cdots = c_m = 0$. Hence $AA^T$ has full rank, which is $m$.

Necessarily we must have rank($A$) $\geq$ rank($AA^T$); therefore, rank($A$) $\geq m$. Since $A$ is an $m$ by $n$ matrix, rank($A$) $\leq n$; hence $m \leq n$ as we desired to show.

Exercise 7

Suppose a town has $n$ residents who form $m$ clubs with the following rules:

(i) The number of members of each club is not a multiple of 15.

(ii) The number of common members in each pair of distinct clubs is a multiple of 15.

Prove that $m \leq 2n$.

Let $L_1, \ldots, L_m$ be the $m$ clubs, and number the residents from 1 to $n$. 
Note that for every $i$, 15 does not divide $|L_i|$; therefore for each $i$, either $|L_i|$ is not a multiple of 3 or $|L_i|$ is not a multiple of 5. (If both were true, then $|L_i|$ would be divisible by 15.)

Let $S = \{i \in \{1, \ldots, m\} : 3 \nmid |L_i|\}$. Similarly let $T = \{i \in \{1, \ldots, m\} : 5 \nmid |L_i|\}$. The observation above shows that $\{1, \ldots, m\} = S \cup T$.

First consider $S$. Note that for any $i \in S$, $|L_i|$ is not a multiple of 3, and for any distinct $i, j \in S$ we have $3 \mid 15 \mid |L_i \cap L_j|$. Applying the previous problem with $p = 3$, $|S| \leq n$.

Similarly, for any $i \in T$, $|L_i|$ is not a multiple of 5, and for any distinct $i, j \in T$ we have $5 \mid 15 \mid |L_i \cap L_j|$. Applying the previous problem with $p = 5$, $|T| \leq n$.

Since $|S \cup T| = |S| + |T| - |S \cap T|$, we have $|\{1, \ldots, m\}| \leq |S| + |T| \leq 2n$. Therefore $m \leq 2n$ as desired.

**Exercise 8**

Show that for each positive integer $n$:

\[
\frac{n}{n+1} = \sum_{r=1}^{n} \frac{(-1)^{r+1}}{r+1} \binom{n}{r}.
\]

We will count the number of permutations $\pi$ of $\{1, 2, \ldots, n+1\}$ for which $\pi(n+1) \neq n+1$. Recall that a permutation is a bijective function from a set to itself.

Let the set of such permutations be $P$. Then for each $\pi \in P$, we may determine $\pi$ by first deciding $\pi(n+1)$, then $\pi(n)$, and so on. There are $n$ choices for $\pi(n+1)$, since $\pi(n+1) \neq n+1$. There are then $n$ choices for $\pi(n)$, since $\pi(n) \neq \pi(n+1)$; there are $n-1$ choices for $\pi(n-1)$, since it must be distinct from $\pi(n), \pi(n+1)$, and so forth. Therefore $|S| = n(n!)$.

Now for $1 \leq k \leq n$, let $A_k$ be the set of permutations $\pi$ of $1, \ldots, n+1$ which satisfy $\pi(n+1) < \pi(k)$. We note that if $\pi(n+1) < \pi(k)$, then necessarily $\pi(n+1) \neq n+1$; this is because $n+1$ is the greatest element in $\{1, \ldots, n+1\}$. Therefore for all $k$, $A_k \subset S$; therefore $\bigcup_{k=1}^{n} A_k \subset S$.

Similarly for any $\pi \in S$, if $\pi(n+1) \neq n+1$, then there is some $k < n+1$ for which $\pi(k) = n+1$ (since $\pi$ is bijective). Therefore $\pi(n+1) < n+1 = \pi(k)$, meaning $\pi \in A_k$. Therefore $S \subset \bigcup_{k=1}^{n} A_k$.

Hence $S = \bigcup_{k=1}^{n} A_k$.  

6
By the principle of inclusion-exclusion, we see that

\[ |S| = \left| \bigcup_{k=1}^{n} A_k \right| = \sum_{J \subseteq \{1, \ldots, n\}, J \neq \emptyset} (-1)^{|J|+1} \left| \bigcap_{i \in J} A_i \right|. \]

We now calculate \( \left| \bigcap_{i \in J} A_i \right| \) for each \( J \). Let \( |J| = r \). By definition, \( \bigcap_{i \in J} A_i \) is the set of permutations \( \pi \) such that for all \( i \in J \) we have \( \pi(n+1) < \pi(i) \).

Given \( \pi \in \bigcap_{i \in J} A_i \), we may determine \( \pi \) as follows. First we choose the \( r + 1 \) elements of \( \{1, \ldots, n+1\} \) which will be \( \pi(i) \) for \( i \in J \) and \( \pi(n+1) \). After assigning \( \pi(n+1) \) to the least of these \( r + 1 \) elements, there remain \( r! \) ways to assign the other elements for \( \pi(i), i \in J \). To assign the remaining \( \pi(j) \), we have \( (n-r)! \) choices, since we have \( n-r \) remaining elements in \( \{1, \ldots, n+1\} \).

Therefore the number of such \( \pi \) is \( \binom{n+1}{r+1} \cdot r! \cdot (n-r)! = \frac{(n+1)!}{r+1} \).

Then by our previous equation,

\[ |S| = \sum_{J \subseteq \{1, \ldots, n\}, J \neq \emptyset} (-1)^{|J|+1} \frac{(n+1)!}{|J| + 1}. \]

There are \( \binom{n}{r} \) subsets of \( \{1, \ldots, n\} \) of size \( r \); therefore

\[ |S| = \sum_{r=1}^{n} (-1)^{r+1} \frac{(n+1)!}{r+1} \binom{n}{r}. \]

Recalling that \( |S| = n(n!) \), we note that

\[ \frac{|S|}{(n+1)!} = \frac{n}{n+1} = \sum_{r=1}^{n} \frac{(-1)^{r+1}}{r+1} \binom{n}{r}, \]

which is what we desired to show.