Content:

Definition	Vector space over a field, F
Examples	$\mathbb{Q}[x]$ is a vs over $\mathbb{Q}$; $n\times n$ matrices over field, F, is a vs over F; For fields E and F such that $E \subseteq F$, F is a vs over E
Proposition	$0_F \bullet v = 0_V$; $-1_F \bullet v = -v$
Definition	subspace
Proposition	Let V be a vs over F. Let $U \subseteq V$. Then U is a subspace iff (1) $U \neq \emptyset$; (2) $u + v \in U\ \forall\ u, v \in U$; (3) $au \in U\ \forall\ a \in F, u \in U$.
Definitions	linear transformation; linearly dependent; span; basis
Example	$\{v_1, v_2, v_3\}$ is linearly independent $\Rightarrow a_1v_1 + a_2v_2 + a_3v_3 = 0$ only if $a_i = 0\ \forall\ i$.
Example	$\{1, x, x^2, \ldots\}$ is a basis for $\mathbb{Q}[x]$; $\{1, i\}$ is a basis for $\mathbb{Q}[i]$.
Theorem	If $\{v_1, v_2, v_3, \ldots\}$ is an infinite bases for a vector space V, then any basis for V will be infinite.
Theorem	If V is a vs, and $\{v_1, v_2, \ldots, v_n\}$ is a basis for V, then every basis for V has n vectors.
Definition	dimension
Theorem	If V is a vs over F and span $\{v_1, \ldots, v_n\} = V$, then there is a set $B \subseteq \{v_1, \ldots, v_n\}$ such that B is a basis for V.
Theorem	If V is a vs over F and $\{v_1, \ldots, v_n\}$ is a linearly independent set, then there is a set B such that $\{v_1, \ldots, v_n\} \subseteq B$ and B is a basis for V.

Announcements Hand in 6.2 #27 Monday. Hand in #7, 8, 13 from 3.7 handout on Wednesday.

Definition A set V is a *vector space* over a field F if V is an Abelian group and for each $a \in F$, $u \in V$, there is an element $au \in V$ such that
(1) $a(u + v) = au + av$; (2) $(a + b)v = av + bv$;
(3) $a(bv) = (ab)v$; (4) $1_F u = u$

Example $\mathbb{Q}[x]$ is a vector space over $\mathbb{Q}$.
$n\times n$ matrices over field, F, is a vector space over F
For fields E and F such that $E \subseteq F$, F is a vector space over E

Proposition (1) $0_F \bullet v = 0_V$; (2) $-1_F \bullet v = -v$

Proof: You do it.
Note that $0_F \bullet v \in V$, thus its inverse $-(0_F \bullet v)\ v \in V$, and by definition of additive inverses in an Abelian group, $0_F \bullet v + -(0_F \bullet v) = 0_V$.

(1) $0_F \bullet v = 0_F \bullet v + 0_V$
$= 0_F \bullet v + 0_F \bullet v + -(0_F \bullet v)$ (by comment noted above)
$= (0_F + 0_F)v + -0_F \bullet v$ (definition vector space)
$= 0_F \bullet v + -0_F \bullet v$
$= 0_V$

(2) $-1_F \bullet v = -1_F \bullet v + 0_V$
$= -1_F \bullet v + v + -v$
$= -1_F \bullet v + 1_F \bullet v + -v$ (definition vector space)
$= (-1_F + 1_F)v + -v$
$= 0_F v + -v$
$= 0_V + -v$ (by part (1))
$= -v$

Definition Let V be a vector space over a field F. Let $U \subseteq V$. We say U is a *subspace* of V if U is a vector space over F under the same operations as in V.

Proposition Let V be a vector space over F. Let $U \subseteq V$. Then U is a subspace iff
(1) $U \neq \emptyset$;
(2) $u + v \in U \; \forall \; u, v \in U$;
(3) $au \in U \; \forall \; a \in F, u \in U$.

Proof: HW
To prove the forward implication assume U is a subspace.
Then we have that U is an Abelian group, hence $0 \in U$, and so $U \neq \emptyset$.
If $u, v \in U$, then by additive closure of the Abelian group U, $u + v \in U$.
If $a \in F$ and $u \in U$, then as U is a vector space over F, we have $au \in U$.

To prove the converse, assume $U \subseteq V$ and the three properties hold.
Let $u \in U$. We know u exists by (1) $U \neq \emptyset$.
Since $0_F \in F$, then $0_F \bullet u \in U$ by (3). Since $u \in V$ and V is a vector space over F, then $0_F \bullet u = 0_V$. Thus $0_V \in U$.
Similarly $-1_F \bullet u \in -u \in U$.
So then if $u, v \in U$, we have $-v \in U$ and (2) gives us that $u - v \in U$.
Thus $U \leq V$. Since $U \subseteq V$, then U inherits its operations from V.
$\therefore$ U is a subspace of V.

Definition Let V, W be vector spaces over F. A mapping $T: V \to W$ is said to be a *linear transformation* if
(1) $T(u + v) = T(u) + T(v) \; \forall \; u, v \in V$.
(2) $T(au) = aT(u) \; \forall \; a \in F, u \in V$.

Example $\mathbb{Q}[x]$ is a vector space over $\mathbb{Q}$.

Definition A set S of vectors is said to be *linearly dependent* over F if there are vectors $v_1, \ldots, v_n \in S$ such that $a_1v_1 + a_2v_2 + \cdots + a_nv_n = 0$ where $a_i \in F$ and not all the a_i are 0.

Example $\{1 + i, i, 2 + 3i\}$ is linearly dependent over $\mathbb{R}$ as $-2(1 + i) + -1 \bullet i + 2 + 3i = 0$.

Definition A set S *spans* the vector space V if for every element $v \in V$ there are vectors $v_1, \ldots, v_n \in S$ such that $v = a_1v_1 + a_2v_2 + \cdots + a_nv_n$ for some $a_1, a_2, \ldots, a_n \in F$.

Example $\{1 + i, i, 2 + 3i\}$ spans the vector space $\mathbb{C}$ as we can write $a + bi = 3a(1 + i) + bi + -a(2 + 3i) \; \forall \; a, b \in \mathbb{R}$.

Definition A set S is a *basis* for V if S is a linearly independent set and span(S) = V where span(S) = $\{ a_1v_1 + a_2v_2 + \cdots + a_nv_n \mid a_i \in F, v_i \in S, n \in \mathbb{N}\}$.

Example $\{1, i\}$ is a basis for $\mathbb{C}$ over $\mathbb{R}$.
$\{1 + i, 2i\}$ is also a basis for $\mathbb{C}$ over $\mathbb{R}$, as we can write
$a + bi = a(1 + i) + ½\,(b - a)2i$ for any $a, b \in \mathbb{R}$.

Example $\{v_1, v_2, v_3\}$ is linearly independent $\Rightarrow$
$a_1v_1 + a_2v_2 + a_3v_3 = 0$ only if $a_i = 0\ \forall\ i$.

Examples $\{1, x, x^2, \ldots\}$ is a basis for $\mathbb{Q}[x]$
$\{1, i\}$ is a basis for $\mathbb{Q}[i]$.

Theorem Let $\{v_1, v_2, v_3, \ldots\}$ be an infinite basis for a vector space V. Then any basis for V will be infinite.

Proof:
Suppose $\{w_1, \ldots, w_n\}$ is a basis for V.
Then $w_1 = a_{1_1} v_1 + a_{2_1} v_2 + \cdots + a_{m_1} v_{m_1}$
where m_1 is the largest index of the a_{i_1}'s such that $a_{i_1} \neq 0$.
And $w_2 = a_{1_2} v_1 + a_{2_2} v_2 + \cdots + a_{m_2} v_{m_2}$ where
where m_2 is the largest index of the a_{i_2}'s such that $a_{i_2} \neq 0$.
Let m_r be the largest index of the a_{i_r}'s such that $a_{i_r} \neq 0$ for at least one of the linear combinations for $w_1, \ldots, w_n$.
Let $t > m_r$. Then since $\{w_1, \ldots, w_n\}$ is a basis for V,
v_t is a linear combination of $w_1, \ldots, w_n$, hence is a linear combination of $v_1, v_2, v_3, \ldots v_{m_r}$. Thus $v_t = a_1v_1 + \cdots + a_{m_r} v_{m_r}$.
But then $0 = -1_F v_t + a_1v_1 + \cdots + a_{m_r} v_{m_r}$ not all a_i's are 0, namely -1_F, a contradiction to linear independence of $\{v_1, v_2, v_3, \ldots\}$.
Thus any basis for V must be infinite.

Theorem If V is a vector space over F, and $X = \{v_1, v_2, \ldots, v_n\}$ is a basis for V, then every basis for V has n vectors.

Proof:
Let $Y = \{w_1, \ldots, w_m\}$ be another basis.
Without loss of generality, we can assume $n \le m$.
$w_1 \in \text{span}(X)$, so $w_1 = a_1v_1 + a_2v_2 + \cdots + a_nv_n$ for some $a_1, a_2, \ldots, a_n \in F$.
Since w_1 is an element in a basis, $w_1 \ne 0$, and $\exists\, a_i$ such that $a_i \ne 0$.
Without loss of generality, assume $a_1 \ne 0$. Then
$v_1 = a_1^{-1}(w_1 - a_2v_2 - \cdots - a_nv_n)$.
Then span (X) = span $\{w_1, v_2, \ldots, v_n\}$. **Go through this.
Let $u \in V$. Then, since $\{v_1, v_2, \ldots, v_n\}$ is a basis for V, we have
$u = b_1v_1 + b_2v_2 + \cdots + b_nv_n$ for some $b_i \in F$.
So $u = b_1(a_1^{-1}(w_1 - a_2v_2 - \cdots - a_nv_n) + b_2v_2 + \cdots + b_nv_n$
$= d_1w_1 + d_2v_2 + \cdots + d_nv_n$ where $d_1 = b_1a_1^{-1}$ and $d_i = b_1a_i$ for $i \ge 2$.
Thus $u \in$ span $\{w_1, v_2, \ldots, v_n\}$. So $\{w_1, v_2, \ldots, v_n\}$ spans V.
Now $w_2 \in V$, hence $w_2 \in$ span $\{w_1, v_2, \ldots, v_n\}$, so
$w_2 = k_1w_1 + k_2v_2 + \cdots + k_nv_n$ for some $k_1, k_2, \ldots, k_n \in F$.
We claim $k_i \ne 0$ for some $i = 2, \ldots, n$ (otherwise $w_2 = k_1w_1$, which contradicts linear independence of the w_i's).
Without loss of generality, assume $k_2 \ne 0$. Then
$v_2 = k_2^{-1}(k_1w_1 - k_3v_3 - \cdots - k_nv_n)$.
We now have span$\{w_1, v_2, \ldots, v_n\}$ = span $(w_1, w_2, v_3, \ldots, v_n\}$.
Continuing, we get span $\{w_1, w_2, \ldots, w_n\} = V$.
If $n < m$, then $w_{n+1} \in$ span $\{w_1, w_2, \ldots, w_n\}$, hence is a linear combination of $w_1, w_2, \ldots, w_n$. This contradicts the linear independence of the w's. $\therefore\ n = m$.

Definition Let V be a vector space over F. The *dimension* of V is the size of the basis.

Theorem If V is a vector space over F and span $\{v_1, \ldots, v_n\} = V$, then there is a set $B \subseteq \{v_1, \ldots, v_n\}$ such that B is a basis for V.

Proof:
If $v_1, \ldots, v_n$ are linearly independent, then $B = \{v_1, \ldots, v_n\}$ and we're done.
If not, then $\exists\, a_i \in F$, not all 0, such that $a_1v_1 + a_2v_2 + \cdots + a_nv_n = 0$.
Without loss of generality assume $a_1 \ne 0$. Then
$v_1 = a_1^{-1}(- a_2v_2 - \cdots - a_nv_n)$. Thus, span$\{v_1, \ldots, v_n\}$ = span$\{v_2, \ldots, v_n\}$.
We can continue in this manner deleting v_i's until the remaining elements are linearly independent.

Theorem If V is a vector space over F and $\{v_1, \ldots, v_n\}$ is a linearly independent set, then there is a set B such that $\{v_1, \ldots, v_n\} \subseteq B$ and B is a basis for V.

Proof:
If span $\{v_1, \ldots, v_n\} = V$, then $B = \{v_1, \ldots, v_n\}$ and we're done.
If not, $\exists\, v_{n+1} \in V$ such that $v_{n+1} \notin$ span $\{v_1, \ldots, v_n\}$.
Claim: $\{v_1, \ldots, v_n, v_{n+1}\}$ is a linearly independent set.
Suppose $a_1v_1 + a_2v_2 + \cdots + a_nv_n + a_{n+1}v_{n+1} = 0$.
If $a_{n+1} \neq 0$, then $v_{n+1} = a_{n+1}^{-1}(-a_1v_1 - a_2v_2 - \cdots - a_nv_n)$.
But this contradicts that $v_{n+1} \notin$ span $\{v_1, \ldots, v_n\}$ by assumption.
So $a_{n+1} = 0$. And by linear independence of $v_1, \ldots, v_n$, all $a_i = 0$, hence $\{v_1, \ldots, v_n, v_{n+1}\}$ is a linearly independent set.
If span $\{v_1, \ldots, v_n, v_{n+1}\} = V$, then $B = \{v_1, \ldots, v_n, v_{n+1}\}$ are we're done.
If not, repeat the procedure until $\{v_1, \ldots, v_t\} = V$ for some t.