Linear Algebra - Key Theorems

Lectured by Dr Simon Wadsley

Michaelmas 2014

Theorem (Steinitz Exchange Lemma)**.** Let V be a vector space over $\mathbb{F}$. Suppose that $S = \{e_1, \ldots, e_n\}$ is a linearly independent subset of V and $T \subset V$ spans V. Then there is a subset T' of T of order n such that $(T \setminus T') \cup S$ spans V. In particular, $n \leqslant |T|$.

Corollary. If $\{e_1, \ldots, e_n\} \subset V$ is linearly independent and $\{f_1, \ldots, f_m\}$ spans V, then $n \leqslant m$ and, possibly after reordering the f_i, $\{e_1, \ldots, e_n, f_{n+1}, \ldots, f_m\}$ spans V.

Proof. By induction. Suppose that we have a subset T'_r of T of order $0 \leqslant r < n$ such that $T_r = (T \setminus T'_r) \cup \{e_1, \ldots, e_r\}$ spans V. Then we can write

$$e_{r+1} = \sum_{i=1}^{k} \lambda_i t_i$$

where $\lambda_i \in \mathbb{F}$ and $t_i \in T_r$. Since $\{e_1, \ldots, e_{r+1}\}$ is linearly independent, there must be some $1 \leqslant j \leqslant k$ such that $\lambda_j \neq 0$ and $t_j \notin \{e_1, \ldots, e_r\}$. Let $T'_{r+1} = T'_r \cup \{t_j\}$ and

$$T_{r+1} = (T \setminus T'_{r+1}) \cup \{e_1, \ldots, e_{r+1}\} = (T_r \setminus \{t_j\}) \cup \{e_{r+1}\}$$

Now

$$t_j = \frac{1}{\lambda_j} + \sum_{i \neq j} \frac{\lambda_i}{\lambda_j} t_i$$

so $t_j \in \langle T_{r+1} \rangle$ and so $\langle T_{r+1} \rangle = \langle T_{r+1} \cup \{t_j\} \rangle \supset \langle T_r \rangle = V$. □

Theorem (Rank-nullity Theorem)**.** If $\alpha : U \to V$ is a linear map between finite dimensional vector spaces over $\mathbb{F}$ then

$$r(\alpha) + n(\alpha) = \dim U \ .$$

Proof. Follows easily from the following proposition. □

Proposition. If $\alpha : U \to V$ is a linear map between finite dimensional vector spaces then there exists bases $\{e_1, \ldots, e_n\}$ for U and $\{f_1, \ldots f_m\}$ for V such that the matrix representing α is

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

where $r = r(\alpha)$.

Proof. Let $e_{k+1}, \dots, e_n$ be a basis for $\ker\alpha$ (so that $n(\alpha) = n - k$), and extend it to a basis $e_1, \dots, e_n$ for U. Let $f_i = \alpha(e_i)$ for $1 \leqslant i \leqslant k$. Claim that $\{f_1, \dots, f_k\}$ is a basis for $\operatorname{Im}\alpha$.

Independence. Suppose that $\sum_{i=1}^k \lambda_i f_i = 0$ for some $\lambda_i \in \mathbb{F}$. Then $\alpha\left(\sum_{i=1}^k \lambda_i e_i\right) = 0$, so $\sum_{i=1}^k \lambda_i e_i \in \ker\alpha$. But $\ker\alpha \cap \langle e_1, \dots, e_k\rangle = 0$ by construction, so $\sum_{i=1}^k \lambda_i e_i = 0$. Since $\{e_1, \dots, e_k\}$ are independent, each $\lambda_i = 0$.

Spanning. Suppose that $v \in \operatorname{Im}\alpha$, so $v = \alpha\left(\sum_{i=1}^k \mu_i e_i\right)$ for some $\mu_i \in \mathbb{F}$. But $\alpha(e_i) = 0$ for $i > k$ and $\alpha(e_i) = f_i$ for $i \leqslant k$, so $v = \sum_{i=1}^k \mu_i f_i \in \langle f_1, \dots, f_k\rangle$.

Hence $\{f_1, \dots, f_k\}$ is a basis for $\operatorname{Im}\alpha$ and in particular $k = r$. Extend this to a basis $\{f_1, \dots, f_m\}$ for V, then

$$\alpha(e_i) = \begin{cases} f_i & 1 \leqslant i \leqslant r \\ 0 & r+1 \leqslant i \leqslant m \end{cases}$$

so the matrix representing α is as given. □

Theorem (Change of basis)**.** Suppose that $\alpha : U \to V$ is a linear map. Let A be the matrix representing α with respect to bases $\langle e_1, \dots, e_m\rangle$ for U and $\langle f_1, \dots, f_n\rangle$ for V, and B the matrix representing α with respect to bases $\langle u_1, \dots, u_m\rangle$ for U and $\langle v_1, \dots, v_n\rangle$ for V. Then $B = Q^{-1}AP$ where $u_i = \sum P_{ki}e_k$ for $i = 1, \dots, m$ and $v_j = \sum Q_{lj} f_l$ for $j = 1, \dots, n$.

(Note that P represents the identity map from U with basis $\langle u_1, \dots, u_m\rangle$ to U with basis $\langle e_1, \dots, e_m\rangle$. Similarly, Q represents the identity map from V with basis $\langle v_1, \dots, v_n\rangle$ to V with basis $\langle f_1, \dots, f_n\rangle$.)

Theorem. If $A \in \operatorname{Mat}_n(\mathbb{F})$ then $(\operatorname{adj} A)A = A(\operatorname{adj} A) = (\det A)I_n$.

Lemma. Let $\alpha \in \operatorname{End}(V)$ and $\lambda_1, \dots, \lambda_k$ be the distinct eigenvalues of α. Then $E(\lambda_1) + \dots + E(\lambda_k)$ is direct.

Proof. Suppose $\sum_{i=1}^k x_i = \sum_{i=1}^k$ with $x_i, y_i \in E(\lambda_i)$. Consider $\beta_j = \prod_{i \neq j}(\alpha - \lambda_i \iota)$. Then

$$\begin{aligned} \beta_j\left(\sum_{i=1}^k x_i\right) &= \sum_{i=1}^k \beta_j(x_i) \\ &= \sum_{i=1}^k \left(\prod_{r \neq j}(\alpha - \lambda_r \iota)(x_i)\right) \\ &= \sum_{i=1}^k \left(\prod_{r \neq j}(\lambda_i - \lambda_r) x_i\right) \\ &= \prod_{r \neq j}(\lambda_j - \lambda_r) x_j \end{aligned}$$

and similarly $\beta_j\left(\sum_{i=1}^k y_i\right) = \prod_{r \neq j}(\lambda_j - \lambda_r) y_j$. Then since $\prod_{r \neq j}(\lambda_j - \lambda_r) \neq 0$, have $x_j = y_j$ for each j. □

Theorem. Let $\alpha \in \operatorname{End}(V)$ and let $\lambda_1, \dots, \lambda_k$ be the distinct eigenvalues of α. Write $E_i = E(\lambda_i)$. The following are equivalent

(i) α is diagonalisable

(ii) V has a basis consisting of eigenvectors of α

(iii) $V = \oplus_{i=1}^{k} E_i$

(iv) $\sum \dim E_i = \dim V$

Proof. **(i) $\iff$ (ii).** Suppose A represents α with respect to the basis $\langle e_1, \dots, e_n \rangle$.
A is diagonal $\iff$ $\alpha(e_i) = A_{ii} e_i$ $\iff$ $\langle e_1, \dots, e_n \rangle$ is a basis of eigenvectors.

(ii) $\iff$ (iii). (ii) is equivalent to $V = \sum E_i$, but the sum of eigenspaces is direct, so this is equivalent to (iii).

(iii) $\iff$ (iv). This is a basic property of direct sums. □

Theorem (Diagonalisability Theorem)**.** The linear map $\alpha \in \mathrm{End}(V)$ is diagonalisable if and only if $m_\alpha(t)$ has distinct linear factors.

Theorem (Cayley-Hamilton Theorem)**.** Suppose that V is a finite dimensional vector space over $\mathbb{F}$ and $\alpha \in \mathrm{End}(V)$. Then $\chi_\alpha(\alpha) = 0$. In particular, m_α divides χ_α.

Theorem (Jordan Normal Form)**.** Every matrix $A \in \mathrm{Mat}_n(\mathbb{C})$ is similar to a matrix in Jordan Normal Form, which is unique up to reordering of the Jordan blocks.

Theorem (Generalised eigenspace decomposition)**.** Let V be a finite dimensional $\mathbb{C}$-vector space and $\alpha \in \mathrm{End}(V)$. Suppose that $m_\alpha(t) = (t - \lambda_1)^{c_1} \dots (t - \lambda_k)^{c_k}$ with $\lambda_1, \dots, \lambda_k$ distinct. Then $V = V_1 \oplus V_2 \oplus \dots \oplus V_k$ where $V_j = \ker((\alpha - \lambda_j \iota)^{c_k})$.

Proposition. If V is a finite dimensional vector space over $\mathbb{F}$ and P is the change of basis matrix from $\langle e_n, \dots, e_n \rangle$ to $\langle f_1, \dots, f_n \rangle$, then the change of basis matrix between the corresponding dual bases $\langle \epsilon_1, \dots, \epsilon_n \rangle$ and $\langle \eta_1, \dots, \eta_n \rangle$ is $(P^{-1})^T$.

Proposition. Suppose that V is finite dimensional over $\mathbb{F}$ and $U \subset V$ is a subspace. Then $\dim U + \dim V^\circ = \dim V$.

Proposition. Suppose V and W are finite dimensional vector spaces over $\mathbb{F}$. If $\alpha : V \to W$ is represented by A with respect to the bases $\langle e_n, \dots, e_n \rangle$ and $\langle f_1, \dots, f_n \rangle$, then the dual map α^* is represented by A^T with respect to the corresponding dual bases $\langle \epsilon_1, \dots, \epsilon_n \rangle$ and $\langle \eta_1, \dots, \eta_n \rangle$.

Proposition (Polarisation Identity)**.** If $q : V \to \mathbb{F}$ is a quadratic form then there exists a unique symmetric bilinear form $\phi : V \times V \to \mathbb{F}$ such that $q(v) = \phi(v, v)$ for all $v \in V$.

Theorem (Canonical form for symmetric bilinear forms)**.** If $\phi : V \times V \to \mathbb{F}$ is a symmetric bilinear form on a finite dimensional vector space V over $\mathbb{F}$ then there is a basis $\langle e_1, \dots, e_n \rangle$ for V such that ϕ is represented by a diagonal matrix.

Corollary. If ϕ is a symmetric bilinear form on a finite dimensional $\mathbb{C}$-vector space V then there is a basis $\langle v_1, \dots, v_n \rangle$ for V such that ϕ is represented by a matrix of the form

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

where $r = r(\phi)$.

Corollary. Every symmetric matrix is $\mathrm{Mat}_n(\mathbb{C})$ is congruent to a matrix of the form

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

Corollary. If ϕ is a symmetric bilinear form a a finite dimensional $\mathbb{R}$-vector space V then there is a basis $\langle v_1, \ldots, v_n \rangle$ for V such that ϕ is represented by a matrix of the form

$$\begin{pmatrix} I_s & 0 & 0 \\ 0 & I_{r-s} & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

where $r = r(\phi)$ and $0 \leqslant s \leqslant r$.

Corollary. Every real symmetric matrix is congruent to a matrix of the form

$$\begin{pmatrix} I_s & 0 & 0 \\ 0 & I_{r-s} & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Theorem (Sylvester's Law of Inertia)**.** Let V be an n-dimensional real vector space and ϕ a symmetric bilinear form on V. Then there exist unique integers s, r such that V has a basis $Span v_1, \ldots, v_n$ with respect to which ϕ is represented by the matrix

$$\begin{pmatrix} I_s & 0 & 0 \\ 0 & I_{r-s} & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

The *signature* of the symmetric bilinear form is defined to be $s - (r - s) = 2s - r$.

Lemma (Cauchy-Schwarz)**.** Let V be an inner product space and $v, w \in V$. Then $|(v, w)| \leqslant \|v\|\|w\|$.

Corollary (Minkowski's inequality)**.** Let V be an inner product space and $v, w \in V$. Then $\|v + w\| \leqslant \|v\| + \|w\|$.

Lemma (Parseval's identity)**.** Suppose hat V is a finite dimensional inner product space with orthonormal basis $\langle v_1, \ldots, v_n \rangle$. Then $(v, w) = \sum_{i=1}^{n} \overline{(v_i, v)}(v_i, w)$. In particular,

$$\|v\|^2 = \sum_{i=1}^{n} |(v_i, v)|^2$$

Theorem (Gram-Schmidt process)**.** Let V be an inner product space and $e_1, e_2, \ldots$ linearly independent vectors. Then there is a sequence $v_1, v_2, \ldots$ of orthonormal vectors such that the $\langle e_1, \ldots, e_k \rangle = \langle v_1, \ldots, v_k \rangle$ for each k.

Lemma. Suppose that V is an inner product space and $\alpha \in \mathrm{End}(V)$ is self-adjoint. Then

(i) α has a real eigenvalue

(ii) all eigenvalues of α are real

(iii) eigenvectors with distinct eigenvalues are orthogonal