

## A primer of linear algebra

### Chapter one: Linear spaces and linear maps

Linear algebra is about linear spaces or vector spaces, and linear maps between them. The first topic is therefore linear spaces.

**Defn:** A (real) **vector space**  $V$  is a set of "vectors" closed under addition, and under "scalar" multiplication of vectors by real numbers, and which is an "abelian group" under addition (the usual properties hold, like associativity, commutativity and existence of a zero and negatives), and has the usual properties under scalar multiplication (multiplication by 1 acts as the identity, multiplication distributes over addition,  $a(bv) = (ab)v$  if  $a, b$ , are numbers and  $v$  is a vector).

**Eg:** The basic example is  $\mathbb{R}^n$ , ordered  $n$  - tuples of real numbers, with component - wise addition and multiplication, i.e.  $(v_1, \dots, v_n) + (w_1, \dots, w_n) = (v_1 + w_1, v_2 + w_2, \dots, v_n + w_n)$  and  $a(v_1, \dots, v_n) = (av_1, \dots, av_n)$ .

**Defn:** A "**subspace**" of  $V$  is a non empty subset  $W$  of  $V$ , closed under addition and scalar multiplication.

**Defn:** Given a subspace  $W$  of  $V$  we can define a new vector space  $V/W$ , the "quotient" of  $V$  by  $W$ , by identifying two vectors  $x, y$  in  $V$  provided  $x - y$  lies in  $W$ . Addition is defined by setting  $[v] + [w] = [v + w]$ , where  $[v]$  denotes the equivalence class of  $v$ , and also  $c[v] = [cv]$ .

**Defn:** For any two vector spaces  $V, W$  we can define a new space  $V \times W$ , the "direct product" of  $V$  and  $W$ , consisting of all ordered pairs  $(x, y)$  with  $x$  in  $V$  and  $y$  in  $W$ . Addition and multiplication are done on components as in  $\mathbb{R}^n =$  the product of  $n$  copies of the real numbers.

**Defn:** A map  $f: V \rightarrow W$  from  $V$  to  $W$  is **linear** if  $f(x + y) = f(x) + f(y)$  for all  $x, y$ , in  $V$ , and if also  $f(ax) = af(x)$  for all  $x$  in  $V$  and all real numbers  $a$ .

**Defn:** An **isomorphism** is a linear map with a linear inverse.

**Ex:** 1) A bijective linear map is an isomorphism.

2) Given a space  $V$  and subspace  $W$ , the map  $V \rightarrow V/W$  sending  $v$  to  $[v]$ , is a linear map sending precisely the vectors in  $W$  to zero.

3) The set  $\text{Hom}(V, W)$  of all linear maps  $V \rightarrow W$  is closed under addition and scalar multiplication, where  $(f + g)(v) = f(v) + g(v)$  and  $(cf)(v) = c(f(v))$ , hence  $\text{Hom}(V, W)$  also forms a vector space.

**Defn:** A "linear combination" of the vectors  $\{v_1, \dots, v_m, \dots\}$  is a vector  $w$  which is a finite sum of multiples of the given ones, i.e. a vector of form  $w = a_1 v_1 + \dots + a_m v_m$ . The term also denotes the summation on the right.

**Eg:** In  $\mathbb{R}^3$ ,  $(4, -5, 1)$  is a linear combination of  $(2, 2, 3)$  and  $(8, -1, 7)$ , since  $(4, -5, 1) = (8, -1, 7) - 2(2, 2, 3)$ .

**Defn:** A set  $S$  of vectors "spans" or "generates" a vector space  $V$  iff every non zero vector in  $V$  is a linear combination of vectors in  $S$ , or equivalently if the set  $S$  is not contained in any proper subspace of  $V$ . In particular, the empty set spans the space  $\{0\}$ .

**Eg:** The set  $\{(1, 0), (0, 1)\}$  generates  $\mathbb{R}^2$  since any vector  $(a, b)$  can be written as the linear combination  $a(1, 0) + b(0, 1) = (a, b)$ .

**Ex:** For any subset  $S = \{v_1, \dots, v_m, \dots\}$  of a vector space  $V$ , the set of all finite linear combinations of the vectors in  $S$ , plus  $0$  (in case  $S$  is empty), forms a subspace  $L(S)$  of  $V$  which is spanned by  $S$ .

**Defn:** A space  $V$  is **finite dimensional** if  $V$  has a finite spanning set.

**Defn:** An indexed set of vectors  $\{v_1, \dots, v_m, \dots\}$  is called **independent** if the only scalars  $a_1, \dots, a_m$  such that  $a_1 v_1 + \dots + a_m v_m = 0$  are  $a_1 = a_2 = \dots = a_m = 0$ , or equivalently if whenever any  $a_i$  is  $\neq 0$ , then  $a_1 v_1 + \dots + a_m v_m \neq 0$ .

**Eg.**  $\{(1, 0), (0, 1)\}$  is independent since the only way we can have  $a(1, 0) + b(0, 1) = (a, b) = (0, 0)$ , is to have  $a = b = 0$ . The empty set is independent.

**Ex:** In a dependent set some vector is in the space spanned by the others.

**Defn:** A subset  $S$  of  $V$  is a **basis**, if  $S$  is independent and  $L(S) = V$ .

**Eg:** The set of unit vectors  $e_1 = (1, 0, \dots, 0), \dots, e_n = (0, \dots, 0, 1)$ , is a basis of  $\mathbb{R}^n$  called the "standard basis".  $\{(3, 0), (2, 5)\}$  is another basis of  $\mathbb{R}^2$ .

**Ex: 1.** An isomorphism between two spaces takes a basis to a basis. In particular an isomorphism from  $\mathbb{R}^n$  to  $V$  takes the standard basis of  $\mathbb{R}^n$  to some basis of  $V$ , hence an isomorphism  $\mathbb{R}^n \rightarrow V$  defines a basis of  $V$ .

**2.** Conversely, a basis  $v_1, \dots, v_n$  of  $V$  determines a unique isomorphism from  $\mathbb{R}^n$  to  $V$  sending  $(a_1, \dots, a_n)$  to  $a_1 v_1 + \dots + a_n v_n$ .

**Defn:** An isomorphism  $V \rightarrow \mathbb{R}^n$  is called a **coordinate system** for  $V$ , and an isomorphism  $\mathbb{R}^n \rightarrow V$  is called a **parametrization** of  $V$ .

**Ex:** i) If  $S = \{v_1, \dots, v_n\}$  is a finite sequence in  $V$ , there is a unique linear map  $f: \mathbb{R}^n \rightarrow V$  sending  $(a_1, \dots, a_n)$  to  $a_1 v_1 + \dots + a_n v_n$ .  
ii) The map  $f$  is injective if and only if  $S = \{v_1, \dots, v_n\}$  is independent, and  
iii)  $f$  is surjective if and only if  $S = \{v_1, \dots, v_n\}$  generates  $V$ , and  
iv)  $f$  is an isomorphism if and only if  $S = \{v_1, \dots, v_n\}$  is a basis for  $V$ .

**Cor:** There is a one to one correspondence between linear maps  $f: \mathbb{R}^n \rightarrow V$  and ordered subsets  $\{v_1, \dots, v_n\}$  of  $n$  vectors in  $V$ .

**Rmk:** An (ordered) basis for  $V$  gives a way to introduce linear coordinates into  $V$ , since via the associated isomorphism with  $\mathbb{R}^n$  each vector in  $V$  gets represented by a sequence of numbers, i.e. by a coordinate vector in  $\mathbb{R}^n$ .

**Eg:** The set of polynomials of degree  $\leq d$ , has as basis the set of  $d+1$  monomials  $\{1, X, \dots, X^d\}$ . In this basis the coordinates of the polynomial  $a_0 + a_1 X + \dots + a_n X^n$ , are its coefficients  $(a_0, a_1, \dots, a_d)$ . Another basis is the set of  $d+1$  polynomials  $\{1, (1+X), (1+X+X^2), \dots, (1+X+\dots+X^d)\}$ . Then the coordinate vector of  $1$  is  $(1, 0, \dots, 0)$ , the coordinate vector of  $(1+X)$  is  $(0, 1, 0, \dots, 0)$ , ..., and the coordinate vector of  $(1+X+\dots+X^d)$  is  $(0, \dots, 0, 1)$ .

**Ex:** If  $\{v_1, \dots, v_n\}$  is a basis of  $V$ , and  $\{w_1, \dots, w_m\}$  is a basis of  $W$ , then  $\{(v_1, 0), \dots, (v_n, 0), (0, w_1), \dots, (0, w_m)\}$  is a basis of  $V \times W$ .

**Thm:** Every finite dimensional space  $V$  has a basis, i.e.  $V$  admits an isomorphism with some  $\mathbb{R}^n$ .

**Pf:** Choose a finite spanning set  $S = \{v_1, \dots, v_n\}$  of  $V$ . Throw out all zero vectors. If  $v_2$  is a multiple of  $v_1$ , throw out  $v_2$ , if not keep it. If  $v_3$  is a linear combination of  $\{v_1, v_2\}$ , throw out  $v_3$ , if not keep it. Continue throwing out vectors which are linear combinations of previous ones. Then the ones left are a basis. (exercise.) **QED**.

**Rmk:** The fact that in a dependent set, some vector is a linear combination of the others, uses only that we can divide by any  $\neq 0$  scalar, hence is true for scalars in any field  $k$ , eg.  $k = \mathbb{R}[X]/(f)$ ,  $f$  irreducible.

**Cor:** A basis  $S$  of  $V$  defines a one - one correspondence between linear maps from  $V$  to  $W$  and set functions from  $S$  to  $W$ , i.e. every function  $S \rightarrow W$

extends uniquely to a linear map  $V \rightarrow W$ .

**Pf :** This is true of  $\mathbb{R}^n$ , hence of all finite dimensional spaces  $V$ . QED.

**Cor:** A linear surjection  $f: \mathbb{R}^n \rightarrow V$  which is not injective, restricts to an isomorphism from some linear subspace  $\mathbb{R}^m$  of  $\mathbb{R}^n$  to  $V$  (where  $m < n$ ).

**Pf:**  $f$  takes the standard basis of  $\mathbb{R}^n$  to a generating set  $S$  for  $V$ . Reduce  $S$  to a basis  $B$ , and choose a subset  $T$  of standard basis vectors of  $\mathbb{R}^n$  mapping bijectively to  $B$ , hence an isomorphism from the subspace  $L(T)$  of  $\mathbb{R}^n$ , to  $V$ .  $L(T)$  is easily identified with  $\mathbb{R}^m$  where  $m$  is the number of vectors in the subset  $T$ . QED.

**Ex:** If  $V = \mathbb{R}^n$  and  $W$  is the subspace spanned by  $e_n$ , then  $V/W$  is isomorphic to  $\mathbb{R}^{n-1}$ .

**Defn:** If  $f: V \rightarrow W$  is a linear map, then  $\ker(f) = \{v \in V: f(v) = 0\}$ , and  $\text{Im}(f) = \{w \in W: w = f(v) \text{ for some } v \in V\}$ .

**Ex:** If  $f: V \rightarrow W$  is a linear map then

i)  $\ker(f)$  is a subspace of  $V$ , and  $\text{Im}(f)$  is a subspace of  $W$ .

ii)  $f$  is constant on equivalence classes in  $V/\ker(f)$ .

iii)  $f$  defines a linear map  $[f]: V/\ker(f) \rightarrow W$  sending  $[v]$  to  $[f(v)]$ .

iv)  $[f]$  in iii) is injective, and  $[f]$  is surjective if and only if  $f$  was, hence  $[f]$  is an isomorphism if and only if  $f$  was surjective.

v) A linear map  $[f]$  can be defined the same way on  $V/U$ , for any subspace  $U$  contained in  $\ker(f)$ , but  $[f]$  will not be injective unless  $U = \ker(f)$ .

**Defn:** A space  $V$  has **dimension**  $= n$ , iff  $V$  is isomorphic to  $\mathbb{R}^n$ , iff  $V$  has a basis consisting of  $n$  vectors.

To show a space cannot have two different dimensions, we prove:

**Thm:** If  $\mathbb{R}^n$  and  $\mathbb{R}^m$  are isomorphic, then  $n = m$ .

**Pf:** (induction on  $n$ ) There is no linear surjection  $f: \mathbb{R}^1 \rightarrow \mathbb{R}^m$  if  $m > 1$ , since the image vectors of  $f$  all have proportional entries. If  $2 \leq n < m$  assume  $f$  is a linear surjection  $f: \mathbb{R}^n \rightarrow \mathbb{R}^m$ , and  $\{e_1, \dots, e_n\}$ , and  $\{u_1, \dots, u_m\}$  are the standard bases of  $\mathbb{R}^n$  and  $\mathbb{R}^m$ . Then the composition  $\mathbb{R}^n \rightarrow \mathbb{R}^m / \text{span}(u_m)$  is surjective but not injective, since if  $v \neq 0$  and  $f(v) = u_m$ , then  $v$  maps to  $[0]$  in  $\mathbb{R}^m / \text{span}(u_m)$ . Hence by previous Cor,  $\mathbb{R}^n \rightarrow \mathbb{R}^m / \text{span}(u_m)$  restricts to a surjection from some subspace  $\mathbb{R}^k$  of  $\mathbb{R}^n$ , with  $k < n$ , to  $\mathbb{R}^m / \text{span}(u_m) = \mathbb{R}^{m-1}$ . Since  $k < m-1$ , this contradicts the inductive hypothesis. QED.

**Cor:** Two spaces are isomorphic iff they have the same dimension.

**Cor:** All bases of a finite dimensional space have the same cardinality.

**Convention:** The space  $\{0\}$  has dimension zero; the empty set is a basis.

**Thm:** If  $W$  is a subspace of  $V$ , then  $\dim W + \dim(V/W) = \dim V$ .

**Pf/Ex:** Choose a basis  $w_1, \dots, w_s$  for  $W$ , and extend it to a basis  $\{w_1, \dots, w_s, v_1, \dots, v_t\}$  of  $V$ . Then  $\{[v_1], \dots, [v_t]\}$  is a basis for  $(V/W)$ . **QED.**

**Thm:** If  $f: V \rightarrow W$  is a linear surjection,  $\dim(\ker(f)) + \dim W = \dim V$ .

**Pf:**  $f$  induces an isomorphism from  $V/\ker(f)$  to  $W$ . **QED.**

**Cor:**  $\dim(V \times W) = \dim V + \dim W$

**Pf:** The projection taking  $(x, y)$  to  $y$  is a linear surjection from  $V \times W$  to  $W$  with kernel  $V$ . **QED.**

**Lemma:** If  $\dim(V) < \infty$ , every independent set in  $V$  is contained in a basis.

**Pf:** If  $\{v_1, \dots, v_n\}$  is independent, and  $\{w_1, \dots, w_m\}$  is a basis, reducing the generating set  $\{v_1, \dots, v_n, w_1, \dots, w_m\}$  to a basis, as above, does it. **QED.**

**Ex: 1)** If  $\dim(V) = n$ , an independent set of vectors in  $V$  has  $\leq n$  vectors.

**2)** If  $\dim V > \dim W$ , no linear map  $V \rightarrow W$  is injective, and no linear map  $W \rightarrow V$  is surjective.

**3)** If  $S = \{x_1, \dots, x_k\}$  are vectors in  $V$ , and  $\dim(V) = n$ , then any two of the following implies the third. **a)**  $S$  is independent, **b)**  $S$  spans  $V$ , **c)**  $k = n$ .

## **Chapter Two: dot products, matrices, eigenvectors, and diagonalizable linear maps.**

**Definition:** The “dot product” of two vectors  $(a_1, \dots, a_n)$  and  $(b_1, \dots, b_n)$  in  $\mathbb{R}^n$  is defined as:  $(a_1, \dots, a_n) \cdot (b_1, \dots, b_n) = a_1 b_1 + \dots + a_n b_n$ . It is a number.

### **The matrix of a linear map $\mathbb{R}^n \rightarrow \mathbb{R}^m$**

Given a linear map  $f: \mathbb{R}^n \rightarrow \mathbb{R}^m$ , arrange the image vectors  $f(e_1), \dots, f(e_n)$  as columns in a rectangular “matrix”  $A$ . Then there are  $m$  rows and  $n$  columns; we call  $A$  an “ $m$  by  $n$ ” matrix. If  $v = (a_1, \dots, a_n)$  is any vector in  $\mathbb{R}^n$ ,  $f(v) = a_1 f(e_1) + \dots + a_n f(e_n)$ , is the linear combination of the columns of  $A$  having the coordinates of  $v$  as coefficients. Thus the  $i$ th entry of  $f(v)$  is obtained by dotting  $v$  with the  $i$ th row of  $A$ .

Thus  $f(v)$  can be computed by multiplying  $A$  by  $v$  as follows: write  $v$  as a length  $n$  column vector to the right of  $A$ . The product  $Av$  is a length

$m$  column vector, where the  $i^{\text{th}}$  entry of  $Av$  is the dot product of the  $i^{\text{th}}$  row of  $A$  with  $v$ . Thus each linear map from  $\mathbb{R}^n$  to  $\mathbb{R}^m$  is represented by multiplying by a (unique)  $m$  by  $n$  matrix.

**Eg:** The matrix of the map  $\mathbb{R}^2 \rightarrow \mathbb{R}^2$  defined by  $f(v) = 6v$ , has rows (and columns):  $(6,0)$  and  $(0,6)$ . The matrix of the rotation map of  $\mathbb{R}^2$  counter clockwise through  $\pi/2$  radians has columns  $(0,1)$  and  $(-1,0)$ .

**Ex:** Find the matrix of the reflection map of  $\mathbb{R}^2$  in the line spanned by  $(1,0)$ , and the matrix for c.c. rotation about  $(0,0)$  through  $t$  radians.

**Ex: i)** The space of all  $m$  by  $n$  matrices forms a vector space  $\text{Mat}(m,n)$  where  $A+B$  is the matrix whose  $(i,j)$  entry, i.e. the entry in the  $i^{\text{th}}$  row and  $j^{\text{th}}$  column, is the sum of the  $(i,j)$  entries of  $A$  and  $B$ , and where  $cA$  is the matrix whose  $(i,j)$  entry is  $c$  times the  $(i,j)$  entry of  $A$ .

**ii)** The space  $\text{Hom}(\mathbb{R}^n, \mathbb{R}^m)$  is isomorphic to the space  $\text{Mat}(m,n)$ , (note the indices  $n,m$  occur correctly in the reverse order here).

**iii)** The dimension of  $\text{Mat}(m,n)$ , hence that of  $\text{Hom}(\mathbb{R}^n, \mathbb{R}^m)$ , is  $mn$ .

**The matrix associated to a linear map  $f:V \rightarrow W$  by bases of  $V,W$ .**

If  $f$  is any linear map from any vector space  $V$  to another  $W$ , then by choosing bases for  $V$  and  $W$  we obtain isomorphisms between these abstract spaces and some coordinate spaces  $\mathbb{R}^n$  and  $\mathbb{R}^m$ . Hence we obtain a resulting linear map from  $\mathbb{R}^n$  to  $\mathbb{R}^m$  which has a matrix  $A$ . This  $A$  is called the matrix of  $f$  associated to the given bases for  $V$  and  $W$ . A map from  $V$  to itself has a matrix associated to any given basis of  $V$ .

If  $f$  is a linear map  $f:V \rightarrow W$  and  $v_1, \dots, v_n$ , and  $w_1, \dots, w_m$  are bases of  $V, W$ , the  $j^{\text{th}}$  column of the associated matrix for  $f$ , is composed of the coefficients  $c_1, \dots, c_m$  where  $f(v_j) = c_1 w_1 + \dots + c_m w_m$ , is the unique basis expansion in  $W$ , for the image under  $f$  of the  $j^{\text{th}}$  basis vector of  $V$ .

**Eg:** If  $D:V \rightarrow V$  takes a polynomial of degree  $\leq 2$  to its derivative, the matrix in the basis  $\{1, X, X^2\}$  has columns  $(0,0,0)$ ,  $(1,0,0)$ ,  $(0,2,0)$ , since  $D(1) = 0 = 0(1,0,0) + 0(0,1,0) + 0(0,0,1)$ , and  $D(X) = 1 = 1(1,0,0) + 0(0,1,0) + 0(0,0,1)$ , and  $D(X^2) = 2X = 0(1,0,0) + 2(0,1,0) + 0(0,0,1)$ .

**Matrix multiplication corresponds to map composition.**

**Ex:** If  $f:V \rightarrow W$  and  $g:W \rightarrow U$  are linear maps, and we choose bases for all three spaces, the matrix of the composition  $g \circ f$  has as entry in its  $i^{\text{th}}$  row and  $j^{\text{th}}$  column, the dot product of the  $i^{\text{th}}$  row of the matrix for  $g$  with the  $j^{\text{th}}$  column of  $f$ . If  $A$  is the matrix of  $f$ , and  $B$  is the matrix for  $g$ , we write

this matrix product as  $BA =$  the matrix for  $g \circ f$ , (in the same bases).

**Defn:** An **eigenvector** of a linear map  $f$ , is a non zero vector  $v$  such that  $f(v)$  is a scalar multiple of  $v$ , i.e. such that  $f(v) = cv$  for some scalar  $c$ . The scalar  $c$  is the **eigenvalue** associated to  $v$ .

**Geometry of eigenvectors:** Recall that a vector  $v$  has both a length and (if  $v \neq 0$ ) a direction. An eigenvector is a non zero vector  $v$  such that either  $f(v) = 0$ , or  $v$  and  $f(v)$  have the same direction. Hence  $v$  spans a line that is mapped by  $f$  into itself.

**Eigenvectors and diagonal matrices:** If  $V$  has a basis consisting of eigenvectors for the map  $f: V \rightarrow V$ , i.e. an "eigenbasis", then the matrix  $A$  for  $f$  in this basis is "diagonal", i.e.  $A$  has the eigenvalues of this basis on its main diagonal (upper left to lower right) and zeroes elsewhere.

**Eg:** The map  $c: V \rightarrow V$  multiplication by the scalar  $c$ , has diagonal matrix  $c.I$  in any basis. Viz., every basis is an eigenbasis for the identity map.

**Eg.** The map  $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$  sending  $(1,0)$  to  $(1,0)$  and  $(0,1)$  to  $(0,2)$  has diagonal matrix with columns  $(1,0)$  and  $(0,2)$  in the standard basis, i.e. the standard basis is an eigenbasis. But  $(1,1)$  is not an eigenvector, so in the basis  $\{(1,0), (1,1)\}$ , the matrix of  $f$  has columns  $(1,0), (-1,2)$ .

**Ex:** The derivative map  $D$  on polynomials above, has no eigenbasis.

**The transpose of a matrix, symmetric matrices.**

**Defn:** An  $n$  by  $n$  matrix  $A$  is **symmetric** if the entry in the  $i^{\text{th}}$  column and  $j^{\text{th}}$  row equals the entry in the  $j^{\text{th}}$  column and  $i^{\text{th}}$  row, for every  $i$  and  $j$ . The matrix  $A^*$  obtained from  $A$  by interchanging its rows and columns is called the **transpose of  $A$** . Thus  $A$  is symmetric if and only if  $A = A^*$ .

**Ex: i)** If the operations are defined,  $(A+B)^* = A^* + B^*$ , and  $(AB)^* = B^*A^*$ .

**ii)** If  $A$  is any  $m$  by  $n$  matrix, and  $v, w$  are any vectors in  $\mathbb{R}^n, \mathbb{R}^m$  respectively, then  $v \cdot (A^*w) = (Av) \cdot w$ .

**iii)** If  $A = A^*$ , then  $Av \cdot w = v \cdot Aw$ , for all  $v, w$ .

**The "spectral theorem" (symmetric matrices are diagonalizable)**

**Thm:** If  $A$  is symmetric, then  $\mathbb{R}^n$  has a basis of eigenvectors for  $A$ .

**Pf:** The real valued function  $f(x) = Ax \cdot x$  has a maximum on the unit sphere in  $\mathbb{R}^n$ , at some point  $y$  where the gradient  $df$  of  $f$  is "zero", i.e.  $df(y)$  is perpendicular to the tangent space of the sphere at  $y$ . The tangent space

at  $y$  is the subspace of vectors in  $\mathbb{R}^n$  perpendicular to  $y$ , and  $df(y) = 2Ay$ . Hence  $Ay$  is perpendicular to the tangent space at  $y$ , i.e.  $Ay = 0$  or  $Ay$  is parallel to  $y$ , so  $Ay = cy$  for some  $c$ , and  $y$  is an eigenvector for  $A$ .

Now restrict  $A$  to the subspace  $V$  of vectors orthogonal to  $y$ . If  $v \cdot y = 0$ , then  $Av \cdot y = v \cdot Ay = v \cdot cy = c(v \cdot y) = 0$ . Hence  $A$  preserves  $V$ .  $A$  still has the property  $Av \cdot x = v \cdot Ax$  on  $V$ , so the restriction of  $A$  to  $V$  has an eigenvector in  $V$ . (Although  $V$  has no natural representation as  $\mathbb{R}^{n-1}$ , the argument for producing an eigenvector depended only the symmetry property  $Av \cdot x = v \cdot Ax$ .) Repeating,  $A$  has an eigenbasis. **QED.**

**Alternate proof:** Choose  $y$  in the unit sphere where  $f(x) = Ax \cdot x$  has minimum value  $c$ , and set  $B = A - cI$ . Then for all  $x, t$ ,  $0 \leq B(y+tx) \cdot (y+tx) = 2t Bx \cdot y + t^2 Bx \cdot x$ . Hence  $Bx \cdot y = 0$  for every  $x$  in  $V$ , i.e.  $Bx = 0$ , so  $Ay = cy$ .

**Cor:** If  $A = A^*$ ,  $A$  has a basis of **mutually perpendicular** eigenvectors.

### Minimal polynomials of linear maps (in finite dimensions)

Given a vector space  $V$  and a linear map  $f: V \rightarrow V$ , define a multiplication of the polynomial ring  $R[X]$  on  $V$  by saying that  $X$  times a vector  $v$  is  $f(v)$ . similarly,  $X^2$  times  $v$  is  $f(f(v))$ , and so on. Sending a polynomial  $P$  to multiplication by  $P$ , i.e. sending  $P$  to  $P(f)$ , defines a linear map from  $R[X]$  to  $\text{Hom}(V, V)$ . If  $\dim(V) = n$ , then  $\dim(\text{Hom}(V, V)) = n^2$ , but  $R[X]$  is infinite dimensional, with basis all monomials  $\{1, X, X^2, X^3, \dots\}$ . Thus the map  $R[X] \rightarrow \text{Hom}(V, V)$  has a non zero kernel, i.e. for some  $P \neq 0$ ,  $P(f) = 0$ .

**Defn:** If  $f: V \rightarrow V$  is a linear map, the monic polynomial  $P$  of least degree such that  $(P(f))v = 0$  for all  $v$  in  $V$ , is the **minimal polynomial** of  $f$ .

**Rmk:** By the division algorithm, every polynomial in the kernel of the map  $R[X] \rightarrow \text{Hom}(V, V)$ , is a multiple of the minimal polynomial of  $f$ .

### Characterizing diagonalizability by the minimal polynomial.

**Prop:** If the minimal polynomial of a map  $V \rightarrow V$  has form  $P(X) = (X - c_1)(X - c_2) \dots (X - c_t)$  where  $t \leq n$  and all  $c_i$  are distinct, and if for each root  $c_i$  of the polynomial  $P$ ,  $V_i = \ker(f - c_i \text{Id})$ , then  $V$  is isomorphic to the product of the subspaces  $V_i$ .

**Pf:** There is a map from that product to  $V$ , taking  $(v_1, \dots, v_t)$  to  $v_1 + \dots + v_t$ , which we claim is injective and surjective. If not injective, some sum  $v_1 + \dots + v_t = 0$ . Then  $v_t$  is in the span of the vectors  $v_1, \dots, v_{t-1}$ , which are all sent to zero by  $(X - c_1)(X - c_2) \dots (X - c_{t-1})$ . Then  $v_t$  must also be sent to zero by this polynomial, but this is false. I.e.  $X - c_1$  sends  $v_t$  to  $f(v_t) - c_1 v_t = (c_t -$



$c_1)v_t \neq 0$ . Then  $X - c_2$  sends  $(c_t - c_1)v_t$  to  $(c_t - c_1)(c_t - c_2)v_t \neq 0, \dots$  etc.

For surjectivity, let  $v$  be any vector in  $V$ , and define the polynomials  $P_1, \dots, P_t$ , where  $P_1 = (X - c_2)(X - c_3) \dots (X - c_t)$ ,  $P_2 = (X - c_1)(X - c_3) \dots (X - c_t)$ ,  $P_3 = (X - c_1)(X - c_2)(X - c_4) \dots (X - c_t)$ , ...,  $P_t = (X - c_1)(X - c_2) \dots (X - c_{t-1})$ . These  $P_i$  are relatively prime, so the Euclidean algorithm gives  $Q_1, \dots, Q_t$  such that  $P_1 Q_1 + \dots + P_t Q_t = 1$ . Applying this equation to  $v$  gives  $v = 1v = P_1(Q_1(v)) + \dots + P_t(Q_t(v))$ , which is in the sum of the images of the  $P_i$ . Since the image of each  $P_i$  is in  $V_i$ , we have proved surjectivity. **QED.**

**Thm:** A linear map  $f: V \rightarrow V$  is diagonalizable iff its minimal polynomial is  $(X - c_1)(X - c_2) \dots (X - c_t)$  where  $t \leq \dim V$  and all  $c_i$  are distinct.

**Pf:** If  $f$  has a diagonal matrix with entries  $c_1, \dots, c_n$  on the diagonal, note that the polynomial  $(X - c_1)(X - c_2) \dots (X - c_n)$  does give zero when  $f$  is substituted for  $X$ . This is still true when we omit repeated occurrences among the scalars  $c_i$ . On the other hand no proper factor of this reduced polynomial can annihilate all vectors in  $V$  as we saw in the last proof. Thus  $(X - c_1)(X - c_2) \dots (X - c_t)$ ,  $t \leq n$ , is the minimal polynomial.

Conversely if the map  $f$  has such a minimal polynomial, then  $V$  is isomorphic as above to the product of its subspaces  $\ker(f - c_i I)$ . Choosing bases of each of these subspaces, and taking their union then gives a basis for  $V$  consisting of eigenvectors for  $f$ . **QED.**

**Eg:** Since the map  $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$  with  $f(1,0) = (0,1)$ , and  $f(0,1) = (0,0)$ , satisfies  $X^2 = 0$ , i.e.  $f(f(v)) = 0$  for all  $v$ , but  $f$  is not itself zero,  $f$  has minimal polynomial  $X^2$ . Hence by the theorem,  $f$  is not diagonalizable.

**Ex:** Prove directly that in the example  $f$  just above the only eigenvectors are  $(0,a)$ . (Show  $f(v) = cv$  implies  $v = 0$  or  $c = 0$ ).

### Jordan canonical form

As suggested by the previous example, transformations  $T$  whose minimal polynomials have repeated linear factors  $(X - c)^r$ , lead to a decomposition of the space into a product of subspaces on which the map  $T - c$  is not identically zero but is nilpotent, i.e. on which  $(T - c)^r$  is identically zero.

**Lemma:** If  $f: V \rightarrow V$  has minimal polynomial  $(X - c_1)^{r_1}(X - c_2)^{r_2} \dots (X - c_t)^{r_t}$  with all  $c_i$  distinct,  $V$  is isomorphic to the product of  $V_i = \ker(T - c_i)^{r_i}$ .

**Pf:** Again consider the map from the product of the  $V_i$  to  $V$ , taking  $(v_1, \dots, v_t)$  to  $v_1 + \dots + v_t$ , which we must show is injective and surjective.

Define polynomials  $P_1, \dots, P_t$ , where  $P_1 = (X - c_2)^{r_2}(X - c_3)^{r_3} \dots (X - c_t)^{r_t}$ ,  $P_2 =$

$(X-c_1)^{r_1}(X-c_3)^{r_3}\dots(X-c_t)^{r_t}, \dots, P_t = (X-c_1)^{r_1}(X-c_2)^{r_2}\dots(X-c_{t-1})^{r_{t-1}}$ . The Euclidean algorithm gives  $Q_1, \dots, Q_t$  such that  $P_1Q_1 + \dots + P_tQ_t = 1$ . Hence for any vector  $v$  in  $V$ ,  $v = P_1(Q_1(v)) + \dots + P_t(Q_t(v))$  is in the sum of the images of the polynomials  $P_i$ . Since  $\text{Im}(P_i)$  is in  $V_i$ , we have proved surjectivity.

For injectivity, assume  $v_1 + \dots + v_t = 0$ . Then each  $v_i$  is a sum of the other  $v_j$  hence  $v_i$  lies in the kernel of  $P_i$ . But each  $v_i$  also lies in the kernel of every  $P_j$  with  $j \neq i$ , hence each  $v_i$  is in the kernel of  $Q_1P_1 + \dots + Q_tP_t = 1$ , i.e. every  $v_i = 0$ . This proves injectivity. **QED.**

**Thm:** With the same hypotheses as above, in some basis  $f$  has a matrix which is almost diagonal: each scalar  $c_i$  occurs  $\dim V_i$  times on the diagonal, but there may also be 1's in some places just below the diagonal. [This is called a "Jordan" matrix for  $f$ .]

**Pf:** Since  $f$  commutes with any polynomial in  $f$ , each subspace  $V_i$  is left invariant by  $f$ , i.e.  $f(V_i)$  is contained in  $V_i$ , so it suffices to show each  $V_i$  has such a basis. Assume  $V$  is a space on which  $(f-c)^r = 0$ , but  $(f-c)^{r-1} \neq 0$ , i.e.  $g = (f-c)$  is nilpotent on  $V$  of order  $r$ . Consider the quotient space  $V/\ker(g^{r-1})$ , and choose a basis  $[x_1], \dots, [x_n]$  for it. Note that  $g$  induces an injection of  $V/\ker(g^{r-1})$  to the quotient  $\ker(g^{r-1})/\ker(g^{r-2})$ , hence we may extend the independent set  $\{[g(x_1)], \dots, [g(x_n)]\}$  to a basis  $\{[y_1], \dots, [y_{n+m}]\}$  for  $\ker(g^{r-1})/\ker(g^{r-2})$ . Continuing, we obtain a basis  $\{[z_1], \dots, [z_{n+m+\dots+q}]\}$  for  $\ker(g)$ , and then the set  $\{x_1, \dots, x_n, y_1, \dots, y_{n+m}, \dots, z_1, \dots, z_{n+m+\dots+q}\}$  is a basis for  $V$ .

(For independence, note any relation among these, and involving  $x$ 's, would yield a relation among the  $[x_i]$ , a contradiction. Similarly if no  $x$ 's occur, but some  $y$ 's occur, we get a relation among the  $[y_j]$ , also a contradiction, ... For spanning, count dimensions, using that  $\dim V =$  the sum of the dimensions of the  $V_i$ .) Then this is the desired basis:

$\{x_1, y_1, \dots, z_1; x_2, y_2, \dots, z_2; \dots; x_n, y_n, \dots, z_n; y_{n+1}, \dots, z_{n+1}; y_{n+2}, \dots, z_{n+2}; y_{n+m}, \dots, z_{n+m}; \dots; z_{n+m+\dots+1}, \dots, z_{n+m+\dots+q}\}$ .

Note each  $x_i$  is annihilated by  $g^r$ , each  $y_i$  is annihilated by  $g^{r-1}$ , ..., and each  $z_i$  is annihilated by  $g$ . Thus the  $z_i$  are the eigenvectors for  $f$ . Moreover  $g$  acts cyclically on these vectors in each block. I.e.  $g(x_i) = y_i$ ,  $g(y_i) = \dots$  (we did not assign a letter to this one), ..., and so on down to  $g(\dots) = z_i$ . All the  $z_i$  belong to  $\ker(g)$ . Thus the  $r$  by  $r$  matrix for  $g$  acting on the block of basis vectors  $\{x_i, y_i, \dots, z_i\}$  has first column  $(0, 1, 0, \dots, 0)$ , second column  $(0, 0, 1, 0, \dots, 0)$ , 3rd column  $(0, 0, 0, 1, 0, \dots, 0)$ , and  $r^{\text{th}}$  column all zeroes  $(0, \dots, 0)$ .

There are  $n$  blocks like this, then  $m$  blocks of size  $(r-1)$  by  $(r-1)$  corresponding to the blocks of basis vectors  $\{y_{n+j}, \dots, z_{n+j}\}$ , and finally

there are  $q$  blocks of size 1 by 1, i.e. one  $q$  by  $q$  block of all zeroes, corresponding to the remaining eigenvectors  $\{z_{n+m+\dots+1}, \dots, z_{n+m+\dots+q}\}$ . Hence the matrix for  $f = g + cI$ , in this basis, is the same as just described, except also with  $c$ 's everywhere on the diagonal. **QED.**

**Eg:** A linear map  $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$  with minimal polynomial  $(X-c)^2$  has Jordan matrix with columns  $(c, 1)$ ,  $(0, c)$ . The derivative  $D: V \rightarrow V$  acting on polynomials of degree at most 2, has minimal polynomial  $X^3$ , Jordan basis  $\{X^2, 2X, 2\}$  and Jordan matrix with columns  $(0, 1, 0)$ ,  $(0, 0, 1)$ ,  $(0, 0, 0)$ .

**Cor:** If the field of scalars is algebraically closed, e.g. the complex numbers, the minimal polynomial always has the form in the theorem, so every linear map has a Jordan matrix, (but not always a diagonal matrix).

**An infinite dimensional example:**  $V$  = continuously differentiable functions on the real line,  $W$  = continuous functions. The derivative map  $D: V \rightarrow W$ , is linear and surjective by the fundamental theorem of calculus. The kernel of  $D$  is all constant functions by the mean value theorem. For any scalar  $c$ ,  $f(x) = e^{cx}$  is an eigenvector for  $D$  with eigenvalue  $c$ .

**Ex:** If  $Lf = f^{(n)} + a_{n-1}f^{(n-1)} + \dots + a_1f' + a_0f = 0$  is a linear d.e. with constant coefficients  $a_i$ , and if the polynomial  $X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0$  factors into a product of distinct linear factors  $(X - c_i)$ , then the eigenfunctions  $f(x) = e^{c_i x}$ , for  $i = 1, \dots, n$ , are a basis of eigenvectors of the solution space  $V = \{f: Lf = 0\}$ . [For  $n = 1$ , and any solution  $f$ ,  $(f/e^{cX})' = 0$ , so  $\dim \ker(D - c) = 1$ . So  $\ker((D - c_1)(D - c_2)\dots(D - c_n)) = (D - c_1)^{-1}(\ker(D - c_2)\dots(D - c_n))$  has dimension  $\leq n$ . Then prove  $\{e^{c_i x}: i = 1, \dots, n\}$ , is independent.]

If the associated polynomial factors as a product of powers  $(X - c_i)^{r_i}$ , with some  $r_i > 1$ , there is no eigenbasis of  $N(L) = \{f: Lf = 0\}$ , but there is a Jordan basis  $\{\dots; e^{c_i x}, x e^{c_i x}, (1/2)x^2 e^{c_i x}, \dots, (1/(r_i - 1)!)x^{r_i - 1} e^{c_i x}; \dots\}$ . In particular,  $N(L)$  still has dimension  $n = \text{degree of the polynomial}$ .

### **Rational Canonical form, Cayley - Hamilton theorem.**

We can push the same ideas further when the minimal polynomial of a linear map  $f: V \rightarrow V$  factors as a product of (not necessarily linear) irreducible factors, say as  $P_1^{r_1} \dots P_n^{r_n}$ , where each  $P_i$  is irreducible in  $k[X]$ , and  $k$  is the field of scalars. The same arguments show  $V$  is isomorphic to the product of the subspaces  $V_i = \ker(P_i^{r_i})$ , and these are invariant under the action of  $f$ . If the power  $r_i = 1$ , we can view  $V_i$  as a vector space over

the field  $k[X]/(P)$ , since the Euclidean algorithm for polynomials shows that one can divide in this quotient ring. I.e.  $k[X]$  is a  $k$  vector space, and the multiples of  $P$  are a subspace, so the set of equivalence classes of polynomials  $k[X]/(P)$ , (where two polynomials  $R, S$  are equivalent if  $P$  divides  $R-S$ ), is a  $k$  vector space of dimension  $d = \deg(P)$ , with basis  $[1], [X], [X^2], \dots, [X^{d-1}]$ . It is also a ring containing  $k$  as a subring, and since  $P$  is irreducible, for any polynomial  $R$  not divisible by  $P$ , we have  $RS + PQ = 1$ , for some polynomials  $S, Q$ . Hence in  $k[X]/(P)$  division by  $R$  is equivalent to multiplication by  $S$ , so  $k[X]/(P)$  is a field.

Recall dividing by  $\neq 0$  scalars was the key to producing vector bases, so  $V$  is also a vector space over the field  $k[X]/(P)$  if the minimal polynomial  $P$  of  $f$  is irreducible [Rmk. p. 3]. A basis for  $V$  over this field, consisting of  $s$  vectors, decomposes  $V$  into a product of  $s$  subspaces, each  $d$  - dimensional over  $k$  and invariant under  $f$ , i.e. under multiplication by  $X$ . If  $v \neq 0$  in  $V$ , the  $k[X]/(P)$  - subspace spanned by  $v$ , has  $k$  - basis  $\{v, f(v), f(f(v)), \dots, f^{d-1}(v)\}$ , corresponding to  $\{1, X, X^2, \dots, X^{d-1}\}$ . Since  $P(v) = 0$ , if  $P(X) = a_0 + a_1X + a_2X^2 + \dots + a_{d-1}X^{d-1} + X^d$ , then  $f^d(v) = -a_0v - a_1f(v) - a_2f^2(v) - \dots - a_{d-1}f^{d-1}(v)$ , so the matrix of  $f$  in this  $k$  - basis has columns of form  $(0, 1, 0, \dots, 0), (0, 0, 1, 0, \dots, 0), \dots, (-a_0, -a_1, -a_2, \dots, -a_{d-1})$ . Thus the matrix of  $f$  acting on a subspace with irreducible minimal polynomial  $P$ , and having dimension  $s$  over  $k[X]/(P)$ , consists of  $s$   $d$ -by- $d$  blocks of that same form. Thus, if the minimal polynomial of  $f$  is a product of distinct irreducible factors  $P_i$ , the  $k$  - matrix of  $f$  in a suitable basis consists of a finite number  $s_i$  of such  $d_i$ -by- $d_i$  blocks for each factor  $P_i$ .

**Eg:** If  $f: V \rightarrow V$  is a linear map on a real vector space, with minimal polynomial  $X^2+1$ ,  $V$  decomposes as a sum of subspaces isomorphic to  $R[X]/(X^2+1)$ , i.e. of 2 dimensional real subspaces, each of them one - dimensional over the field  $R[X]/(X^2+1)$ . This quotient field is isomorphic to the complex numbers  $C$ , where  $X$  corresponds to  $i = \sqrt{-1}$ , so the operator  $f$  on this space corresponds to multiplication by  $i$ . If  $V$  has dimension  $s$  over  $C$ , the real rational canonical matrix of  $f$  on  $V$ , consists of exactly  $s$  blocks, and each block is 2 by 2, with columns  $(0, 1), (-1, 0)$ .

**Rmk:** A rational canonical matrix always exists, composed of blocks like those above, but we must give a different proof for decomposability of the space when the minimal polynomial of  $f$  has repeated irreducible factors. We have already split our space as a product of subspaces  $\ker(P_i^{r_i})$ , but now the ring  $k[X]/(P^r)$  operating on each of these subspaces, is no longer a field, so we have to prove we can decompose each  $\ker(P^r)$  into  $f$  - invariant subspaces. Then if  $V = \ker(P^r)$  where  $P$  is irreducible,  $f$

will have a matrix of blocks of the form above, but the coefficients in the last column of each block are those of some power  $P^s$  of  $P$ , with  $s \leq r$ .

In the simplest possible case,  $\dim(\ker(P^r)) = rd$ , where  $d = \deg(P)$ , there is a  $v \neq 0$  with  $P^{r-1}(v) \neq 0$ . Then a basis for  $V$  is given by  $\{v, f(v), \dots, f^{dr-1}(v)\}$ , and the  $k$ -matrix for  $f$  is the one block associated to the coefficients of  $P^r$ . Thus there is no problem when  $\dim_k(\ker(P_i^{r_i})) = r_i \cdot \deg(P_i)$  for all  $i$ , since no decomposition is necessary. In the general case, the spaces  $\ker(P_i^{r_i})$  may be bigger. There is always a vector  $v$  in  $\ker(P^r)$  with  $P^{r-1}(v) \neq 0$ , but then we must prove  $\ker(P^r)$  splits as a product of the  $rd$  dimensional subspace spanned by  $\{v, f(v), \dots, f^{dr-1}(v)\}$ , and another  $f$ -invariant subspace. Then we can finish by induction on dimension. To get this splitting we can adapt the following result.

**Splitting Lemma:** If  $G$  is a finite (additive) abelian group of order  $p^r$  where  $p$  is prime,  $w$  an element generating a subgroup  $(w)$  of maximal order, and  $G/(w) = (z)$  is cyclic, then  $G$  is isomorphic to  $(w) \times (z)$ .

**Pf:** Assume  $f: G \rightarrow (z)$  sends  $y$  to  $z$ , and has kernel  $(w)$ . If  $\text{ord}(z) = p^a$ ,  $[p^a z = 0, \text{ but no smaller multiple} = 0]$  then  $\text{ord}(y) = p^{a+b}$ , and  $\text{ord}(w) = p^{a+b+c}$ , where  $a, b, c, \geq 0$ . We seek  $u = y + tw$  with  $p^a u = 0$ . Then  $f(u) = z$ , so  $p^a \geq \text{ord}(u) \geq \text{ord}(z) = p^a$ , so mapping  $z$  to  $u$  splits  $G$  as  $(w) \times (u)$ , isom. to  $(w) \times (z)$ . But  $f(p^a y) = p^a z = 0$  so  $p^a y$  is in  $(w)$ , and no smaller multiple is, so  $(y) \cap (w) = (p^a y)$  has order  $p^b$ , so  $(p^a y) = (p^{a+c} w)$ . So for some  $s$ ,  $p^a y = sp^{a+c} w = p^a (sp^c w)$ , and  $p^a (y - sp^c w) = 0$ . So let  $u = (y - sp^c w)$ . **QED.**

**Cor:** If  $G$  is a finite abelian  $p$  group,  $w$  an element with  $\text{ord}(w)$  maximal,  $G/(w)$  splits as product of cyclic groups  $(z_i)$  by induction. If  $f: G \rightarrow G/(w) = \prod (z_i)$  sends  $y_i$  to  $z_i$ , apply lemma to the map  $f: (w, y_i) \rightarrow (z_i)$ , with kernel  $(w)$ . Mapping each  $z_i$  to the corresponding  $u_i$  in  $G$  splits  $G$  as  $(w) \times \prod (u_i)$ .

**Ex:** Prove the splitting lemma needed for the general rational canonical form, with an irred. poly  $P$  replacing the prime integer  $p$ .

**Eg:** If  $f$  has minimal polynomial  $X^r$ , then  $f$  has a matrix of blocks of size  $\leq r$ , with columns  $(0, 1, 0, \dots, 0)$ ,  $(0, 0, 1, 0, \dots, 0)$ , ...,  $(0, 0, \dots, 0, 1)$ ,  $(0, 0, \dots, 0)$ . This is both the Jordan and rational canonical form of  $f$ .

**Computations (for those who know about determinants):**

Recall all matrices for a linear map  $f: V \rightarrow V$  have the same determinant, so we define the "characteristic polynomial" of  $f$  as  $\det(f - X.I)$ . It follows from expanding about the last column that a rational canonical block

matrix satisfies its own characteristic polynomial. In fact the map acts cyclically on all but the last vector, so no power of  $f$  smaller than the size of the block is a linear combination of smaller powers, so the polynomial associated to the last column of a rational canonical block equals both the minimal and characteristic polynomial. Since every linear map  $f:V \rightarrow V$  has a rational canonical form, we obtain:

**Thm(Cayley Hamilton):** Every linear map  $f:V \rightarrow V$  on a finite dimensional space  $V$ , satisfies its characteristic polynomial.

Examining the decomposition, the characteristic polynomial of  $f$  equals the product of the associated polynomials of every block in its rational canonical matrix, and the minimal polynomial equals only the product of the polynomials associated to the largest block for each irreducible factor. In particular the minimal and the characteristic polynomial have the same irreducible factors. By computing a determinant and then factoring the characteristic polynomial into irreducible factors  $P_i$ , one can explicitly compute canonical forms of a matrix, by finding bases for the kernels of the powers  $P_i^s(f)$ ,  $s \leq r_i$ .

**Ex:** A scalar  $c$  is an eigenvalue of  $f$  if and only if  $\det(f-c.I) = 0$ , iff  $c$  is a root of the characteristic polynomial of  $f$ , if and only if  $c$  is a root of the minimal polynomial of  $f$ .

**Ex:** Find all Jordan and rational canonical forms of linear maps of  $\mathbb{R}^3$  with minimal polynomials  $(X-2)^3$ ,  $(X-2)^2$ , and  $(X-2)$ .

Roy Smith