Notes on linear algebra

Danny Nygård Hansen

6th March 2022

1 • Linear equations and matrices

1.1. *Linear equations*

Throughout we let F denote an arbitrary field and R a commutative ring. Let m and n be positive integers. A *linear equation in n unknowns* is an equation on the form

$$l\colon a_1x_1 + \cdots + a_nx_n = b,$$

where $a_1,\ldots,a_n,b \in F$. A *solution* to l is an element $v = (v_1,\ldots,v_n) \in F^n$ such that

$$a_1v_1 + \cdots + a_nv_n = b.$$

A *system of linear equations in n unknowns* is a tuple $L = (l_1,\ldots,l_m)$, where each l_i is a linear equation in n unknowns. An element $v \in F^n$ is a *solution* to L if it is a solution to each linear equation $l_1,\ldots,l_m$.

Let L and L' be systems of linear equations in n unknowns. We say that L and L' are *solution equivalent* if they have the same solutions. Furthermore, we say that they are *combination equivalent* if each equation in L' is a linear combination of the equations in L, and vice versa. Clearly, if L and L' are combination equivalent they are also solution equivalent, but the converse does not hold.

1.2. *Matrices*

It is well-known that a system of linear equations is equivalent to a matrix equation on the form $Ax = b$, where $A \in \mathcal{M}_{m,n}(F)$, $x \in F^n$ and $b \in F^m$. Recall the *elementary row operations* on A:

(1) multiplication of one row of A by a nonzero scalar,

(2) addition to one row of A a scalar multiple of another (different) row, and

(3) interchange of two rows of A.

If e is an elementary row operation, we write $e(A)$ for the matrix obtained when applying e to A. Clearly each elementary row operation e has an 'inverse', i.e. an elementary row operation e' such that $e'(e(A)) = e(e'(A)) = A$. Two matrices $A, B \in \mathcal{M}_{m,n}(F)$ are called *row-equivalent* if A is obtained by applying a finite sequence of elementary row operations to B (and vice versa, though this need not be assumed since each elementary row operation has an inverse).

Clearly, if $A, B \in \mathcal{M}_{m,n}(F)$ are row-equivalent, then the systems of equations $Ax = 0$ and $Bx = 0$ are combination equivalent, hence have the same solutions.

Definition 1.1

A matrix $H \in \mathcal{M}_{m,n}(F)$ is called *row-reduced* if

(i) the first nonzero entry of each nonzero row in H is 1, and

(ii) each column of H containing the leading nonzero entry of some row has all its other entries equal 0.

If H is row-reduced, it is called a *row-reduced echelon matrix* if it also has the following properties:

(iii) Every row of H only containing zeroes occur below every row which has a nonzero entry, and

(iv) if rows $1, \ldots, r$ are the nonzero rows of H, and if the leading nonzero entry of row i occurs in column k_i, then $k_1 < \cdots < k_r$.

An *elementary matrix* is a matrix obtained by applying a single elementary row operation to the identity matrix I. It is easy to show that if e is an elementary row operation and $E = e(I) \in \mathcal{M}_m(F)$, then $e(A) = EA$ for $A \in \mathcal{M}_{m,n}(F)$. If $B \in \mathcal{M}_{m,n}(F)$, then A and B are row-equivalent if and only if $A = PB$, where $P \in \mathcal{M}_m(F)$ is a product of elementary matrices.

Proposition 1.2

Every matrix in $\mathcal{M}_{m,n}(F)$ is row-equivalent to a unique row-reduced echelon matrix.

Proof. The usual Gauss–Jordan elimination algorithm proves existence. If $H, K \in \mathcal{M}_{m,n}(R)$ are row-equivalent row-reduced echelon matrices, we claim that $H = K$. We prove this by induction in n. If $n = 1$ then this is obvious, so assume that $n > 1$. Let H_1 and K_1 be the matrices obtained by deleting the nth column in H and K respectively. Then H_1 and K_1 are also row-equivalent[1] and row-reduced echelon matrices, so by induction $H_1 = K_1$. Thus if H and K differ, they must differ in the nth column.

Let H_2 be the matrix obtained by deleting columns in H, only keeping those columns containing pivots, as well as keeping the nth column. Define K_2 similarly. Thus we have deleted the same columns in H and K, so H_2 and K_2 are also row-equivalent. Say that the number of columns in H_2 and K_2 is $r+1$, and write the matrices on the form

$$H_2 = \begin{pmatrix} I_r & h \\ 0 & h' \end{pmatrix} \quad \text{and} \quad K_2 = \begin{pmatrix} I_r & k \\ 0 & k' \end{pmatrix},$$

where $h, k \in F^r$ and $h', k' \in F^{m-r}$ are column vectors. Since H_2 and K_2 are row-equivalent, the systems $H_2 x = 0$ and $K_2 x = 0$ are solution equivalent. If $h' = 0$, then $H_2 x = 0$ has the solution $(-h, 1)$. But this is also a solution to $K_2 x = 0$, so $h = k$ and $k' = 0$. If $h' \neq 0$, then $H_2 x = 0$ only has the trivial solution. But then $K_2 x = 0$ also only has the trivial solution, and hence $k' \neq 0$. But that must be because both H_2 and K_2 has a pivot in the rightmost column, so also in this case $H_2 = K_2$. □

1.3. Invertible matrices

Notice that elementary matrices are invertible, since elementary row operations are invertible.

Lemma 1.3

If $A \in \mathcal{M}_n(F)$, then the following are equivalent:

(i) *A is invertible,*

(ii) *A is row-equivalent to I_n,*

(iii) *A is a product of elementary matrices, and*

(iv) *the system $Ax = 0$ has only the trivial solution $x = 0$.*

Proof. *(i) ⇔ (ii):* Let $H \in \mathcal{M}_n(F)$ be a row-reduced echelon matrix that is row-equivalent to A. Then $R = PA$, where $P \in \mathcal{M}_n(F)$ is a product of elementary matrices. Then $A = P^{-1}H$, so A is invertible if and only if H is. But the only invertible row-reduced echelon matrix is the identity matrix, so (i) and (ii) are equivalent.

[1] It should be obvious that deleting columns preserves row-equivalence, but we give a more precise argument: If $P \in \mathcal{M}_m(F)$ is a product of elementary matrices and $a_1, \ldots, a_n \in F^m$ are the columns in A, then the columns in PA are $Pa_1, \ldots, Pa_m$. Thus elementary row operations are applied to each column independently of the other columns.

(i) ⇔ (iii): Clearly (iii) implies (i), and the above shows that (i) implies that $A = P^{-1}$.

(ii) ⇔ (iv): If A and I_n are row-equivalent, then the systems $Ax = 0$ and $I_n x = 0$ have the same solutions. Conversely, assume that $Ax = 0$ only has the trivial solution. If $H \in \mathcal{M}_{m,n}(F)$ is a row-reduced echelon matrix that is row-equivalent to A, then $Hx = 0$ has no nontrivial solution. Thus if r is the number of nonzero rows in H, then $r \geq n$. But then $r = n$, so H must be the identity matrix. □

Proposition 1.4

Let $A \in \mathcal{M}_n(F)$. Then the following are equivalent:

(i) *A is invertible,*

(ii) *A has a left inverse, and*

(iii) *A has a right inverse.*

Proof. If A has a left inverse, then $Ax = 0$ has no nontrivial solution, so A is invertible. If A has a right inverse $B \in \mathcal{M}_n(F)$, i.e. $AB = I$, then B has a left inverse and is thus invertible. But then A is the inverse of B and hence is itself invertible. □

2 • Determinants

2.1. Existence of determinants

If $M_1, \dots, M_n, N$ are modules over a commutative ring R, a map

$$\varphi \colon M_1 \times \cdots \times M_n \to N$$

is called *n-linear* if the maps $m_i \mapsto \varphi(m_1, \dots, m_n)$ are linear for all $m_i \in M_i$. Since $\mathcal{M}_{m,n}(R) \cong (R^m)^n$, a map $\varphi \colon \mathcal{M}_{m,n}(R) \to N$ that is linear in each row is also called n-linear.

In the case $M_1 = \cdots = M_n$, we call φ *alternating* if $\varphi(m_1, \dots, m_n) = 0$ whenever $m_i = m_j$ for some $i \neq j$. Furthermore, φ is called *skew-symmetric* if

$$\begin{aligned}\varphi(m_1, \dots, m_{i-1}, m_i, m_{i+1}, \dots, m_{j-1}, m_j, m_{j+1}, \dots, m_n) \\ = -\varphi(m_1, \dots, m_{i-1}, m_j, m_{i+1}, \dots, m_{j-1}, m_i, m_{j+1}, \dots, m_n)\end{aligned}$$

for all $i < j$.

LEMMA 2.1

Let M and N be R-modules, and let $\varphi\colon M^n \to N$ be an n-linear map.

(i) *If φ is alternating, then φ is skew-symmetric.*

(ii) *If $\varphi(m_1,\dots,m_n) = 0$ whenever $m_i = m_{i+1}$ for some $i = 1,\dots,n-1$, then φ is alternating.*

PROOF. *(i)*: Consider $m_1,\dots,m_n \in M$, and let $1 \leq i < j \leq n$. Define a map $\psi\colon M \times M \to N$ by

$$\psi(a,b) = \varphi(m_1,\dots,m_{i-1},a,m_{i+1},\dots,m_{j-1},b,m_{j+1},\dots,m_n),$$

and notice that it suffices to show that $\psi(m_i,m_j) = -\psi(m_j,m_i)$. But ψ is 2-linear and alternating, so for $a,b \in M$ we have

$$\psi(a+b,a+b) = \psi(a,a) + \psi(a,b) + \psi(b,a) + \psi(b,b) = \psi(a,b) + \psi(b,a).$$

Thus $\psi(m_i,m_j) = -\psi(m_j,m_i)$, so φ is skew-symmetric as claimed.

(ii): The argument above shows that, in particular, if $A,B \in M^n$, and B is obtained from A by interchanging two adjacent elements, then $\varphi(B) = -\varphi(A)$. Assuming now that B is obtained from A by interchanging the ith and jth elements in A, with $i < j$, we claim that we may obtain B by successively interchanging adjacent elements of A. Writing $A = (m_1,\dots,m_n)$, we first perform $j-i$ such interchanges and arrive that the tuple

$$(m_1,\dots,m_{i-1},m_{i+1},\dots,m_{j-1},m_j,m_i,m_{j+1},\dots,m_n),$$

moving m_i to the right $j-i$ places. Next we perform another $j-i-1$ interchanges, moving m_j to the left until we reach

$$B = (m_1,\dots,m_{i-1},m_j,m_{i+1},\dots,m_{j-1},m_i,m_{j+1},\dots,m_n).$$

Since each interchange results in a sign change, we have

$$\varphi(B) = (-1)^{2(j-i)-1}\varphi(A) = -\varphi(A).$$

If $m_i = m_j$ for $i < j$, then we claim that $\varphi(A) = 0$. For let B be obtained from A by interchanging m_{i+1} and m_j. Then $\varphi(B) = 0$, so $\varphi(A) = -\varphi(B) = 0$ by the above argument, and hence φ is alternating as claimed. □

DEFINITION 2.2

If n be a positive integer, a *determinant function* is a map $\varphi\colon \mathcal{M}_n(R) \to R$ that is n-linear, alternating, and which satisfies $\varphi(I_n) = 1$.

If $A \in \mathcal{M}_n(R)$ with $n > 1$ and $1 \le i, j \le n$, denote by $M(A)_{i,j}$ the matrix in $\mathcal{M}_{n-1}(R)$ obtained by removing the the ith row and the jth column of A. This is called the (i,j)-*th minor* of A. If $\varphi \colon \mathcal{M}_{n-1}(R) \to R$ is an $(n-1)$-linear function and $A \in \mathcal{M}_n(R)$, then we write $\varphi_{i,j}(A) = \varphi(M(A)_{i,j})$. Then $\varphi_{i,j} \colon \mathcal{M}_n(R) \to R$ is clearly linear in all rows except row i, and is independent of row i.

Theorem 2.3

Let $n > 1$, and let $\varphi \colon \mathcal{M}_{n-1}(R) \to R$ be alternating and $(n-1)$-linear. For $j = 1, \dots, n$ define a map $\psi_j \colon \mathcal{M}_n(R) \to R$ by

$$\psi_j(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \varphi_{i,j}(A),$$

for $A = (a_{ij}) \in \mathcal{M}_n(R)$. Then ψ_j is alternating and n-linear. If φ is a determinant function, then so is ψ_j.

Proof. Let $A = (a_{ij}) \in \mathcal{M}_n(R)$. Then $A \mapsto a_{ij}$ is independent of all rows except row i, and $\varphi_{i,j}$ is linear in all rows except row i. Thus $A \mapsto a_{ij}\varphi_{i,j}(A)$ is linear in all rows except row i. Conversely, $A \mapsto a_{ij}$ is linear in row i, and $\varphi_{i,j}$ is independent of row i, so $A \mapsto a_{ij}\varphi_{i,j}(A)$ is also linear in row i. Since ψ_j is a linear combination of n-linear maps, is it itself n-linear.

Now assume that A has two equal adjacent rows, say $a_k, a_{k+1} \in R^n$. If $i \neq k$ and $i \neq k+1$, then $M(A)_{i,j}$ has two equal rows, so $\varphi_{i,j}(A) = 0$. Thus

$$\psi_j(A) = (-1)^{k+j} a_{kj} \varphi_{k,j}(A) + (-1)^{k+1+j} a_{(k+1)j} \varphi_{k+1,j}(A).$$

Since $a_k = a_{k+1}$ we also have $a_{kj} = a_{(k+1)j}$ and $M(A)_{k,j} = M(A)_{k+1,j}$. Thus $\psi_j(A) = 0$, so Lemma 2.1(ii) implies that ψ_j is alternating.

Finally suppose that φ is a determinant function. Then $M(I_n)_{j,j} = I_{n-1}$ and we have

$$\psi_j(I_n) = (-1)^{j+j} \varphi_{j,j}(I_n) = \varphi(I_{n-1}) = 1,$$

so ψ_j is also a determinant function. □

Corollary 2.4

For every positive integer n, there exists a determinant function $\mathcal{M}_n(R) \to R$.

Proof. The identity map on $\mathcal{M}_1(R) \cong R$ is a determinant function for $n = 1$, and Theorem 2.3 allows us to recursively construct a determinant for each $n > 1$. □

2.2. Uniqueness of determinants

Theorem 2.5

Let n be a positive integer. There is precisely one determinant function on $\mathcal{M}_n(R)$, namely the function $\det\colon \mathcal{M}_n(R) \to R$ given by

$$\det A = \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}$$

for $A = (a_{ij}) \in \mathcal{M}_n(R)$. If $\varphi\colon \mathcal{M}_n(R) \to R$ is any alternating n-linear function, then

$$\varphi(A) = (\det A)\varphi(I_n).$$

We use the notation det for the unique determinant on $\mathcal{M}_n(R)$ for all n.

Proof. Let $e_1, \dots, e_n$ denote the rows of I_n, and denote the rows of a matrix $A = (a_{ij}) \in \mathcal{M}_n(R)$ by $a_1, \dots, a_n$. Then $a_i = \sum_{j=1}^n a_{ij} e_j$, so

$$\varphi(A) = \sum_{k_1,\dots,k_n} a_{1k_1} \cdots a_{nk_n} \varphi(e_{k_1}, \dots, e_{k_n}),$$

where the sum is taken over all $k_i = 1, \dots, n$. Since φ is alternating we have $\varphi(e_{k_1}, \dots, e_{k_n}) = 0$ if two of the indices $k_1, \dots, k_n$ are equal. Thus it suffices to sum over those sequences $(k_1, \dots, k_n)$ that are permutations of $(1, \dots, n)$, and so

$$\varphi(A) = \sum_{\sigma \in S_n} a_{1\sigma(1)} \cdots a_{n\sigma(n)} \varphi(e_{\sigma(1)}, \dots, e_{\sigma(n)}).$$

Next notice that, since φ is also skew-symmetric by Lemma 2.1(i), we have $\varphi(e_{\sigma(1)}, \dots, e_{\sigma(n)}) = (-1)^m \varphi(e_1, \dots, e_n)$, where m is the number of transpositions of $(1, \dots, n)$ it takes to obtain the permutation $(\sigma(1), \dots, \sigma(n))$. But then $(-1)^m$ is just the sign of σ, so

$$\varphi(A) = \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)} \varphi(I_n).$$

Finally, if φ is a determinant function, then $\varphi(I_n) = 1$, so we must have $\varphi = \det$. The rest of the theorem follows directly from this. ∎

2.3. Properties of determinants

Theorem 2.6

Let $A, B \in \mathcal{M}_n(R)$. Then

$$\det AB = (\det A)(\det B).$$

In particular, $\det\colon \mathrm{GL}_n(R) \to R^*$ *is a group homomorphism.*

PROOF. The map $\varphi\colon \mathcal{M}_n(R) \to R$ given by $\varphi(A) = \det AB$ is clearly n-linear and alternating. Hence $\varphi(A) = (\det A)\varphi(I)$, and $\varphi(I) = \det B$.

Furthermore, if A is invertible, then $1 = \det I = (\det A)(\det A^{-1})$. Thus $\det A \in R^*$, so det is a group homomorphism as claimed. □

PROPOSITION 2.7

Let $A_{11}, \dots, A_{nn}$ *be square matrices with entries in* R *and consider the block matrix*

$$M = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ 0 & A_{22} & \cdots & A_{2n} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & A_{nn} \end{pmatrix},$$

where the remaining A_{ij} *are matrices of appropriate dimensions. Then* $\det M = \prod_{i=1}^n \det A_{ii}$.

PROOF. By induction it suffices to consider the case where M has the block form

$$M = \begin{pmatrix} A & C \\ 0 & B \end{pmatrix},$$

where $A \in \mathcal{M}_r(R)$, $B \in \mathcal{M}_s(R)$ and $C \in \mathcal{M}_{r,s}(R)$ for appropriate integers r, s. Notice that if we define the matrices

$$M_1 = \begin{pmatrix} I_r & 0 \\ 0 & B \end{pmatrix} \quad \text{and} \quad M_2 = \begin{pmatrix} A & C \\ 0 & I_s \end{pmatrix},$$

then $M = M_1 M_2$. But using Theorem 2.3 we easily see that $\det M_1 = \det B$ and $\det M_2 = \det A$, so it follows that

$$\det M = (\det M_1)(\det M_2) = (\det A)(\det B)$$

as desired. □

PROPOSITION 2.8

Let $A \in \mathcal{M}_n(R)$. *Then* $\det A = \det A^\top$.

PROOF. Writing $A = (a_{ij})$, first notice that

$$\det A^\top = \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma^{-1}) a_{\sigma(1)1} \cdots a_{\sigma(n)n},$$

since $\operatorname{sgn}\sigma = \operatorname{sgn}\sigma^{-1}$. Next notice that, if $j = \sigma(i)$, then $a_{\sigma(i)i} = a_{j\sigma^{-1}(j)}$. Since R is commutative, it follows that

$$\det A^\top = \sum_{\sigma\in S_n} (\operatorname{sgn}\sigma^{-1}) a_{1\sigma^{-1}(1)} \cdots a_{n\sigma^{-1}(n)},$$

and since $\sigma \mapsto \sigma^{-1}$ is a bijection on S_n, it follows that $\det A^\top = \det A$ as desired. ∎

Let $A \in \mathcal{M}_n(R)$. For $1 \leq i, j \leq n$, the (i,j)*-th cofactor* of A is the number $A_{i,j} = (-1)^{i+j} \det M(A)_{i,j}$, where we recall that $M(A)_{i,j}$ is the (i,j)-th minor of A. The *adjoint matrix* of A is the matrix $\operatorname{adj} A \in \mathcal{M}_n(R)$ whose (i,j)-th entry is the cofactor $A_{j,i}$. Note that

$$(A^\top)_{i,j} = (-1)^{i+j} \det M(A^\top)_{i,j} = (-1)^{j+i} \det M(A)_{j,i} = A_{j,i},$$

so $\operatorname{adj} A^\top = (\operatorname{adj} A)^\top$. We have the following:

Proposition 2.9

Let $A \in \mathcal{M}_n(R)$. Then

$$(\operatorname{adj} A)A = (\det A)I = A(\operatorname{adj} A).$$

Proof. Writing $A = (a_{ij})$ and fixing some $j \in \{1, \dots, n\}$, Theorem 2.3 implies that

$$\det A = \sum_{i=1}^n (-1)^{i+j} a_{ij} \det M(A)_{i,j} = \sum_{i=1}^n a_{ij} A_{i,j},$$

which is just the (j,j)-th entry in the product $(\operatorname{adj} A)A$.

Next we claim that if $k \neq j$, then $\sum_{i=1}^n a_{ik} A_{i,j} = 0$. Let $B = (b_{ij}) \in \mathcal{M}_n(R)$ be the matrix obtained from A by replacing the jth column of A by its kth column. Then B has two equal columns, so $\det B = 0$. Also, $b_{ij} = a_{ik}$ and $M(B)_{i,j} = M(A)_{i,j}$, so it follows that

$$\begin{aligned} 0 = \det B &= \sum_{i=1}^n (-1)^{i+j} b_{ij} \det M(B)_{i,j} \\ &= \sum_{i=1}^n (-1)^{i+j} a_{ik} \det M(A)_{i,j} = \sum_{i=1}^n a_{ik} A_{i,j}. \end{aligned}$$

That is, the (j,k)-th entry of the product $(\operatorname{adj} A)A$ is zero, so the off-diagonal entries of $(\operatorname{adj} A)A$ are zero. In total we thus have $(\operatorname{adj} A)A = (\det A)I$.

Finally we prove the equality $A(\operatorname{adj} A) = (\det A)I$, Applying the first equality to $A^\top$ yields

$$(\operatorname{adj} A^\top)A^\top = (\det A^\top)I = (\det A)I,$$

and transposing we get

$$A(\operatorname{adj} A) = A(\operatorname{adj} A^\top)^\top = (\det A)I$$

as desired. □

COROLLARY 2.10

Let $A \in \mathcal{M}_n(R)$. Then A is a unit in $\mathcal{M}_n(R)$ if and only if $\det A$ is a unit in R.

PROOF. This follows directly from Proposition 2.9. □

2.4. Determinants and eigenvalues

Let V be a vector space of dimension $n < \infty$. If $T \in \mathcal{L}(V)$, then recall that an *eigenvalue* of T is an element $\lambda \in F$ such that there is a nonzero vector $v \in V$ with $Tv = \lambda v$. The set of eigenvalues of T is called the *spectrum* of T and is denoted $\operatorname{Spec} T$. Clearly $\lambda \in \operatorname{Spec} T$ if and only if $\lambda I - T$ is not injective, i.e. if $\det(\lambda I - T) = 0$. This motivates the definition of the *characteristic polynomial* $p_T(t) \in F[t]$ of T, given by $p_T(t) = \det(tI - T)$. The eigenvalues of T are then precisely the roots of $p_T(t)$.

PROPOSITION 2.11

Let $T \in \mathcal{L}(V)$.

(i) *$p_T(t)$ is a monic polynomial of degree n.*

(ii) *The constant term of $p_T(t)$ equals $(-1)^n \det T$.*

(iii) *The coefficient of t^{n-1} in $p_T(t)$ equals $-\operatorname{tr} T$.*

Assume further that $p_T(t)$ splits over F. Then:

(iv) *T has an eigenvalue.*

(v) *$\det T$ is the product of the eigenvalues of T.*

(vi) *$\operatorname{tr} T$ is the sum of the eigenvalues of T.*

The condition that $p_T(t)$ splits over F means that $p_T(t)$ decomposes into a product of linear factors on the form $t - a \in F[t]$ (up to multiplication by a constant). This is in particular the case if F is algebraically closed.

PROOF. *(i):* Let $A = (a_{ij}) \in \mathcal{M}_n(F)$ be a matrix representation of T. The (i, j)-th entry of $tI - A$ is then $t\delta_{ij} - a_{ij}$, so

$$\det(tI - T) = \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma)(t\delta_{1\sigma(1)} - a_{1\sigma(1)}) \cdots (t\delta_{n\sigma(n)} - a_{n\sigma(n)}) \tag{2.1}$$

by Theorem 2.5. Thus $p_T(t)$ is a polynomial in t. Furthermore, the only entries in $tI - A$ containing t are the diagonal entries, and the largest number of such entries occurring in a single term of (2.1) is n, so $\deg p_T(t) \leq n$. But notice that there is only one term in which t appears n times, namely the term corresponding to the identity permutation in S_n, giving the product of the diagonal entries in $tI - A$. This term equals

$$(t - a_{11})(t - a_{22}) \cdots (t - a_{nn}), \tag{2.2}$$

and multiplying out we see that the only resulting term containing t^n is t^n itself. Hence $p_T(t)$ is monic and of degree n. Thus we may write $p_T(t) = \sum_{i=0}^{n} c_i t^i$ for appropriate $c_0, \ldots, c_n \in F$.

(ii): Simply notice that

$$(-1)^n \det T = \det(-T) = p_T(0) = c_0$$

by n-linearity of det and the definition of $p_T(t)$.

(iii): The only way for one of the terms in (2.1) to contain the factor t^{n-1} is for at least $n-1$ of the b_{ij} to be a diagonal element. But in choosing $n-1$ elements along the diagonal we are forced to also choose the final diagonal element, since otherwise σ would not be a permutation. Hence the factor t^n can only appear in the product (2.2). It is then clear that

$$c_{n-1} = -(a_{11} + \cdots + a_{nn}) = -\operatorname{tr} T$$

as claimed.

(iv): Now assume that $p_T(t)$ splits over F. Then some linear factor $t - \lambda \in F[t]$ divides $p_T(t)$, which implies that $\lambda \in F$ is an eigenvalue of T.

(v): Since $p_T(t)$ is monic we have

$$p_T(t) = (t - \lambda_1)(t - \lambda_2) \cdots (t - \lambda_n)$$

for appropriate $\lambda_1, \ldots, \lambda_n \in F$. These are then the (not necessarily distinct) eigenvalues of T. Thus $p_T(0) = (-1)^n \lambda_1 \cdots \lambda_n$, and the claim follows from (ii).

(vi): We similarly find that $c_{n-1} = -(\lambda_1 + \cdots + \lambda_n)$, so the final claim follows from (iii). □

2.5. *Proofs without determinants*

Existence of eigenvalues

Assume that F is algebraically closed, and consider $T \in \mathcal{L}(V)$. For $d \in \mathbb{N}$, let $F[t]_d$ denote the vector space of polynomials in $F[t]$ with degree strictly less than d, such that $\dim F[t]_d = d$. Consider the map $\mathrm{ev}_T \colon F[t]_{n^2+1} \to \mathcal{L}(V)$ given by $\mathrm{ev}_T(p) = p(T)$. This cannot be injective, so there is some nonzero $p(t) \in F[t]_{n^2+1}$ such that $p(T) = 0$. Note that $p(t)$ cannot be constant.

Since F is algebraically closed, there exist $c, \lambda_1, \dots, \lambda_m \in F$ such that $p(t) = c\prod_{i=1}^m (t - \lambda_i)$. But then

$$0 = p(T) = c\prod_{i=1}^{m} (T - \lambda_i I),$$

so at least one $T - \lambda_i I$ is not injective. Hence λ_i is an eigenvalue of T.

Trace is sum of eigenvalues

Corollary 2.12

Let F be algebraically closed, and let $T \in \mathcal{L}(V)$. Then the sum of the eigenvalues of T is $\operatorname{tr} T$.

Proof. Let $A \in \mathcal{M}_n(F)$ be an upper triangular matrix for T. The diagonal elements of A are the eigenvalues, and the trace of T is just the sum of these elements. □

3 • Triangularisation and diagonalisation

3.1. *Triangularisation*

Proposition 3.1

Let V be an F-vector space with $n = \dim V < \infty$, and let $\mathcal{V} = (v_1, \dots, v_n)$ be an ordered basis for V. The matrix of an operator $T \in \mathcal{L}(V)$ is upper triangular with respect to $\mathcal{V}$ if and only if $\operatorname{span}(v_1, \dots, v_i)$ is invariant under T for all $i \in \{1, \dots, n\}$.

Proof. This is obvious. □

Lemma 3.2

Let V be an F-vector space, and let $T \in \mathcal{L}(V)$ be an isomorphism. If U is a finite-dimensional subspace of V that is invariant under T, then U is also invariant under T^{-1}.

Proof. Since U is finite-dimensional and $T|_U \colon U \to U$ is injective, applying the rank–nullity theorem implies that $T|_U$ is also surjective. Hence if $u \in U$, then there exists a $v \in U$ such that $Tv = u$. It follows that

$$T^{-1}u = T^{-1}Tv = v \in U,$$

so U is invariant under T^{-1}. □

PROPOSITION 3.3

Let V be a finite-dimensional F-vector space, and let $\mathcal{V}$ be an ordered basis for V. If $T \in \mathcal{L}(V)$ is an isomorphism that is upper triangular with respect to $\mathcal{V}$, then T^{-1} is also upper triangular with respect to $\mathcal{V}$.

In particular, the subset of $\mathrm{GL}_n(F)$ consisting of upper triangular matrices is a subgroup.

PROOF. This is an obvious consequence of the above two results. □

LEMMA 3.4

Let $A \in \mathcal{M}_n(F)$ be upper triangular. Then A is invertible if and only if all its diagonal elements are nonzero.

PROOF. Denote the diagonal elements of A by $\lambda_1, \dots, \lambda_n$, and let $e_1, \dots, e_n$ denote the standard basis of F^n. First assume that the diagonal elements are nonzero. Then notice that $e_1 \in R(A)$, and that

$$Ae_i = a_1 e_1 + \cdots + a_{i-1} e_{i-1} + \lambda_i e_i$$

for appropriate $a_1, \dots, a_{i-1} \in F$. By induction we then have $e_i \in R(A)$. Since $(e_1, \dots, e_n)$ is a basis, this implies that $R(A) = F^n$.

Conversely, assume that some diagonal element λ_i is zero. If $i = 1$, then $Ae_1 = 0$ so A is singular. If $i > 0$, then

$$A \operatorname{span}(e_1, \dots, e_i) \subseteq \operatorname{span}(e_1, \dots, e_{i-1}),$$

so again A is singular. □

LEMMA 3.5

Let $A \in \mathcal{M}_n(F)$ be upper triangular. Then the eigenvalues of A are its diagonal elements.

PROOF. Let $\lambda \in F$, and denote the diagonal elements of A by $\lambda_1, \dots, \lambda_n$. By [lemma], the matrix $\lambda I - A$ is singular if and only if $\lambda - \lambda_i = 0$ for some i, and hence $\lambda_1, \dots, \lambda_n$ are the eigenvalues of A. □

PROPOSITION 3.6

Let F be algebraically closed, and let V be a finite-dimensional F-vector space. If $T \in \mathcal{L}(V)$, then V has an ordered basis with respect to which the matrix of T is *upper triangular.*

PROOF. This is obvious if $\dim V = 1$, so assume that $n = \dim V > 1$, and assume that the claim is true for F-vector spaces of dimension $n-1$. Let $v_1 \in V$ be an eigenvector for T, and let $U = \operatorname{span}(v_1)$. Since U is invariant under T, we may define a linear operator[2] $\tilde{T} \in \mathcal{L}(V/U)$ by $\tilde{T}(v+U) = Tv + U$. Since $\dim V/U = n-1$, by induction there is a basis $v_2 + U, \dots, v_n + U$ of V/U with respect to which the matrix of $\tilde{T}$ is upper triangular. It is easy to show that the collection $v_1, \dots, v_n$ is linearly independent, hence a basis for V.

Now notice that

$$Tv_i + U = \tilde{T}(v_i + U) \in \operatorname{span}(v_2 + U, \dots, v_i + U)$$

for $i \in \{2, \dots, n\}$. That is, there exist $a_2, \dots, a_i \in F$ such that

$$Tv_i + U = (a_2 v_2 + \cdots + a_i v_i) + U.$$

But then $Tv_i \in \operatorname{span}(v_1, \dots, v_i)$ for all $i \in \{2, \dots, n\}$, and since U is invariant under T this also holds for $i = 1$. Hence T is upper triangular with respect to the basis $v_1, \dots, v_n$ of V. □

THEOREM 3.7: *Schur's Theorem*

Let F be algebraically closed, and let V be a finite-dimensional inner product space over F. If $T \in \mathcal{L}(V)$, then V has an ordered orthonormal basis with respect to which the matrix of T is upper triangular.

PROOF. By [proposition] V has an ordered basis $\mathcal{V} = (v_1, \dots, v_n)$ with respect to which the matrix of T is upper triangular. Now apply the Gram–Schmidt procedure to $\mathcal{V}$ and obtain an orthonormal basis $\mathcal{E} = (e_1, \dots, e_n)$ for V such that

$$\operatorname{span}(e_1, \dots, e_i) = \operatorname{span}(v_1, \dots, v_i)$$

for all $i \in \{1, \dots, n\}$. Then [proposition with invariant subspaces] shows that the matrix of T with respect to $\mathcal{E}$ is also upper triangular, proving the claim. □

3.2. Orthonormal diagonalisation

Let $T: V \to V$ is an operator on an F-vector space V, and let U be a subspace of V that is invariant under T. Say that W is a complement of V, i.e. that $V = U \oplus W$, then W is not necessarily invariant under T. However, we have the following:

[2] The operator $\tilde{T}$ may arise as follows: Let $\pi: V \to V/U$ be the quotient map. Then $U \subseteq \ker(\pi \circ T)$ since U is invariant under T, so $\pi \circ T$ descends to a linear map $\tilde{T}: V/U \to V/U$.

Lemma 3.8

Let $T \in \mathcal{L}(V)$ be an operator on a finite-dimensional inner product space V. If a subspace U of V is invariant under T, then $U^\perp$ is invariant under T^*.

Proof. Let $v \in U^\perp$. For $u \in U$ we have $Tu \in U$, so

$$\langle T^* v, u \rangle. = \langle v, Tu \rangle = 0.$$

Since this holds for all $u \in U$, it follows that $T^* v \in U^\perp$ as desired. □

Theorem 3.9: *The spectral theorem*

Let F be either the real or the complex numbers, let V be a finite-dimensional inner product space over F, and consider $T \in \mathcal{L}(V)$. Then T is orthogonally diagonalisable if and only if

(i) *$F = \mathbb{R}$ and T is self-adjoint, or*

(ii) *$F = \mathbb{C}$ and T is normal.*

Proof. Assume that either $F = \mathbb{R}$ and T is self-adjoint, or that $F = \mathbb{C}$ and T is normal. We prove by induction in $n = \dim V$ that T is orthogonally diagonalisable. If $n = 1$ then this follows since T has an eigenvalue, so assume that the claim is proved for operators on spaces of dimension strictly less than n.

Let $\lambda \in \operatorname{Spec} T$, and consider the corresponding eigenspace $E_T(\lambda)$. If $d = \dim E_T(\lambda) = n$, then any orthonormal basis of $E_T(\lambda)$ will suffice. Assume therefore that $0 < d < n$.

Clearly $E_T(\lambda)$ is invariant under T, and we claim that it is also invariant under T^*. If T is self-adjoint this is obvious, and if T is normal then for all $w \in E_T(\lambda)$,

$$TT^* w = T^* T w = T^*(\lambda w) = \lambda T^* w,$$

so we also have $T^*(w) \in E_T(\lambda)$. It follows from Lemma 3.8 that $E_T(\lambda)^\perp$ is also invariant under both T and T^*. We furthermore have $\dim E_T(\lambda)^\perp = n - d$ and $0 < n - d < n$. Let $T_\parallel \in \mathcal{L}(E_T(\lambda))$ and $T_\perp \in \mathcal{L}(E_T(\lambda)^\perp)$ denote the restrictions of T to $E_T(\lambda)$ and $E_T(\lambda)^\perp$ respectively. Both these operators are also self-adjoint or normal, depending on the hypothesis, so the induction hypothesis furnishes orthonormal bases $\mathcal{U}$ and $\mathcal{W}$ for $E_T(\lambda)$ and $E_T(\lambda)^\perp$ consisting of eigenvectors of T. But then $\mathcal{V} = \mathcal{U} \cup \mathcal{W}$ is an orthonormal basis for V as desired.

Conversely, assume that $\mathcal{V}$ is an orthonormal basis of V consisting of eigenvectors for T, and let $A \in \mathcal{M}_n(F)$ be the matrix of T with respect to $\mathcal{V}$. Then A is diagonal with the eigenvalues of T on its diagonal. If $F = \mathbb{R}$ then the eigenvalues of T are real, so A is a real symmetric matrix, and hence T

is self-adjoint. If instead $F = \mathbb{C}$, then since A is diagonal we have $A^*A = AA^*$, which implies that T is normal. □

4 • Complex numbers

It is well-known that a complex number $z = a + \mathrm{i}\,b$ has a representation as a matrix

$$A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix},$$

and that the subring of $\mathcal{M}_2(\mathbb{R})$ consisting of such matrices is isomorphic to $\mathbb{C}$. Letting $r = |z| = \sqrt{\det A}$ we obtain a matrix $Q = A/r \in \mathrm{SO}(2)$. Let us call the pair (r, Q) the *geometric representation* of z.

Let $\mathbb{C}^*$ denote the group of nonzero complex numbers under multiplication. We define an action of $\mathbb{C}^*$ on $\mathbb{R}^2$ as follows: If $v \in \mathbb{R}^2$ then, in the notation above, we let $zv = rQv$; that is, z acts on v by applying the rotation matrix Q and scaling by r.

Alternatively, given $v = (x, y) \in \mathbb{R}^2$ form the complex number $w = x + \mathrm{i}\,y$ with corresponding matrix

$$B = \begin{pmatrix} x & -y \\ y & x \end{pmatrix}.$$

Then zw has the corresponding matrix rQB, the first column of which is $zv = rQv$. Thus the action of $\mathbb{C}^*$ on $\mathbb{R}^2$ is also obtained by considering a vector in $\mathbb{R}^2$ as a complex number and performing complex multiplication.

LEMMA 4.1

The action of $\mathbb{C}^*$ on $\mathbb{R}^2$ preserves angles.

PROOF. Let $z \in \mathbb{C}^*$ have have the geometric representation (r, Q), and let $v, u \in \mathbb{R}^2$. Then notice that

$$\langle zv, zu \rangle = r^2 \langle Qv, Qu \rangle = r^2 \langle v, u \rangle,$$

since Q is orthogonal. In particular we have $\|zv\| = r\|v\|$. If $\theta \in [0, \pi]$ is the angle between zv and zu, then the Cauchy–Schwarz inequality implies that

$$\cos\theta = \frac{\langle zv, zu \rangle}{\|zv\|\,\|zu\|} = \frac{r^2 \langle v, u \rangle}{r^2 \|v\|\,\|u\|} = \frac{\langle v, u \rangle}{\|v\|\,\|u\|},$$

which is just the cosine of the angle between v and u. This proves the lemma. □

Now let $U \subseteq \mathbb{C}$ be a nonempty open set, and let $f\colon U \to \mathbb{C}$ be a holomorphic function that does not attain the value zero.[3] Considering U and $\mathbb{C}$ as real two-dimensional manifolds, let $T_pf\colon T_pU \to T_{f(p)}\mathbb{C}$ be the tangent map of f at $p \in U$. The Jacobian matrix of f at p is then simply the matrix corresponding to the complex number $f'(p)$, so if $v \in T_pU$, then the vector $T_pf(v) \in T_{f(p)}\mathbb{C} \cong \mathbb{R}^2$ is just the action of $f'(p)$ on v. The lemma then implies that, for $v, u \in T_pU$,

$$\langle T_pf(v), T_pf(u)\rangle = \langle f'(p)v, f'(p)u\rangle = |f'(p)|^2\langle v, u\rangle.$$

Since f is holomorphic it is smooth as a function on $\mathbb{R}^2$, the map $p \mapsto |f'(p)|^2$ is also smooth and nonzero everywhere, and so f is conformal.

5 • Gray codes

[This doesn't belong here, I just needed a LaTeX editor to write the proof.]

If a and b are binary strings of the same length, we denote the bitwise exclusive disjunction of a and b by $a \oplus b$. We denote the concatenation of a with b either by $a \circ b$ or ab. Also, if b is a binary string, denote by $b^{\gg}$ the right logical shift of b, i.e. the string obtained by removing the rightmost bit of b and appending a 0 on the left of the result.

Let $n \in \mathbb{N}$. For a number $k \in \mathbb{N}$ with $k < 2^n$ we denote the n-bit binary representation of k by $\mathrm{bin}_n(k)$. Furthermore, we denote the n-bit Gray code for k by $\mathrm{gr}_n(k)$. By definition, $\mathrm{gr}_0(0) = \lambda$ and

$$\mathrm{gr}_{n+1}(k) = \begin{cases} 0 \circ \mathrm{gr}_n(k), & k < 2^n, \\ 1 \circ \mathrm{gr}_n(2^{n+1} - 1 - k), & k \geq 2^n. \end{cases}$$

for all $n \in \mathbb{N}$ and $(n+1)$-bit numbers k. We claim the following:

Proposition 5.1

Let $n \in \mathbb{N}$, and let $k \in \mathbb{N}$ be an n-bit number. Writing $\mathrm{bin}_n(k) = b_{n-1} \cdots b_0$ we have $\mathrm{gr}_n(k) = a_{n-1} \cdots a_0$, where $a_{n-1} = b_{n-1}$ and

$$a_i = b_{i+1} \oplus b_i \tag{5.1}$$

for $i \in \{0, \dots, n-2\}$. That is,

$$\mathrm{gr}_n(k) = b_{n-1}(b_{n-1} \oplus b_{n-2}) \cdots (b_1 \oplus b_0).$$

[3] If f is not identically zero, then $f^{-1}(\mathbb{C}^*)$ is a nonempty open subset of $\mathbb{C}$, so this is a very natural assumption.

Conversely we have
$$b_i = a_i \oplus \cdots \oplus a_{n-1}.$$

The formula (5.1) also holds in the case $i = n-1$ if we let $b_n = 0$, i.e. we prepend zeros if necessary.

PROOF. If $n = 0$, then the claim is obvious since there are no 0-bit numbers. Now let k be an $(n+1)$-bit number, so that $k < 2^{n+1}$, and write $\mathrm{bin}_{n+1}(k) = b_n \cdots b_0$. If $k < 2^n$, then $b_n = 0$ and $\mathrm{gr}_{n+1}(k) = 0 \circ \mathrm{gr}_n(k)$. By induction we have

$$\begin{aligned} \mathrm{gr}_n(k) &= b_{n-1}(b_{n-1} \oplus b_{n-2}) \cdots (b_1 \oplus b_0) \\ &= (b_n \oplus b_{n-1})(b_{n-1} \oplus b_{n-2}) \cdots (b_1 \oplus b_0), \end{aligned}$$

so it follows that

$$\mathrm{gr}_{n+1}(k) = b_n \circ \mathrm{gr}_n(k) = b_n(b_n \oplus b_{n-1})(b_{n-1} \oplus b_{n-2}) \cdots (b_1 \oplus b_0)$$

as claimed. If instead $k \geq 2^n$, then $b_n = 1$. Writing $k = 2^n + r$ with $0 \leq r < 2^n$ we have $\mathrm{bin}_n(r) = b_{n-1} \cdots b_0$. Now notice that $\mathrm{bin}_n(2^n - 1 - r) = \bar{b}_{n-1} \cdots \bar{b}_0$ since

$$(\bar{b}_{n-1} \cdots \bar{b}_0)_2 + r + 1 = (\bar{b}_{n-1} \cdots \bar{b}_0)_2 + (b_{n-1} \cdots b_0)_2 + 1 = 2^n.$$

By induction we have

$$\begin{aligned} \mathrm{gr}_n(2^n - 1 - r) &= \bar{b}_{n-1}(\bar{b}_{n-1} \oplus \bar{b}_{n-2}) \cdots (\bar{b}_1 \oplus \bar{b}_0) \\ &= (b_n \oplus b_{n-1})(b_{n-1} \oplus b_{n-2}) \cdots (b_1 \oplus b_0) \end{aligned}$$

since $b_n = 1$, so it follows that

$$\begin{aligned} \mathrm{gr}_{n+1}(k) &= b_n \circ \mathrm{gr}_n(2^n - 1 - r) \\ &= b_n(b_n \oplus b_{n-1})(b_{n-1} \oplus b_{n-2}) \cdots (b_1 \oplus b_0) \end{aligned}$$

as desired.

For the final claim, simply notice that

$$\begin{aligned} a_i \oplus \cdots \oplus a_{n-1} &= (b_i \oplus b_{i+1}) \oplus (b_{i+1} \oplus b_{i+2}) \oplus \cdots \oplus (b_{n-2} \oplus b_{n-1}) \oplus b_{n-1} \\ &= b_i \oplus (b_{i+1} \oplus b_{i+1}) \oplus (b_{i+2} \oplus \cdots \oplus b_{n-2}) \oplus (b_{n-1} \oplus b_{n-1}) \\ &= b_i. \end{aligned}$$

Alternatively we may notice that (5.1) defines a linear system of equations with coefficients in $\mathbb{Z}/2\mathbb{Z}$ and invert this. $\square$

Corollary 5.2

For $n \in \mathbb{N}$ and any n-bit number k, we have

$$\mathrm{gr}_n(k) = \mathrm{bin}_n(k) \oplus \mathrm{bin}_n(k)^{\gg}.$$

Proof. Writing $\mathrm{bin}_n(k) = b_{n-1} \cdots b_0$, the proposition implies that

$$\begin{aligned}\mathrm{gr}_n(k) &= b_{n-1}(b_{n-1} \oplus b_{n-2}) \cdots (b_1 \oplus b_0) \\ &= (0 \oplus b_{n-1})(b_{n-1} \oplus b_{n-2}) \cdots (b_1 \oplus b_0).\end{aligned}$$

But $\mathrm{bin}_n(k)^{\gg} = 0b_{n-1} \cdots b_1$, so the claim follows. □

References

Axler, Sheldon (2015). *Linear Algebra Done Right*. 3rd ed. Springer. 340 pp. ISBN: 978-3-319-11079-0. DOI: 10.1007/978-3-319-11080-6.

Hoffman, Kenneth and Ray Kunze (1971). *Linear Algebra*. 2nd ed. Prentice-Hall. 407 pp.

Knuth, Donald E. (2011). *The Art of Programming, Volume 4A: Combinatorial Algorithms, Part 1*. 1st ed. Addison-Wesley. 883 pp. ISBN: 978-0-201-03804-0.

Roman, Steven (2008). *Advanced Linear Algebra*. 3rd ed. Springer. 522 pp. ISBN: 978-0-387-72828-5.