Abstract Algebra II

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 342

Subsection 1

Definitions and Basic Theory

Dictionary of Terms (Modules versus Vector Spaces)

Terminology for R any Ring	**Terminology for R a Field**
M is an R-module	M is a vector space over R
m is an element of M	m is a vector in M
a is a ring element	a is a scalar
N is a submodule of M	N is a subspace of M
M/N is a quotient module	M/N is a quotient space
M is a free module of rank n	M is a vector space of dimension n
M is a finitely generated module	M is a finite dimensional vector space
M is a nonzero cyclic module	M is a 1-dimensional vector space
$\varphi : M \to N$ is an R-module homomorphism	$\varphi : M \to N$ is a linear transformation
M and N are isomorphic as R-modules	M and N are isomorphic vector spaces
the subset A of M generates M	the subset A of M spans M
$M = RA$	each element of M is a linear combination of elements of A, i.e., $M = \text{Span}(A)$

We assume F is a field and V a vector space over F.

Independence and Bases

Definition (Independent Vectors and Bases)

(1) A subset S of V is called a set of **linearly independent vectors** if an equation $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0$, with $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$ and $v_1, v_2, \ldots, v_n \in S$, implies $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$.

(2) A **basis** of a vector space V is an ordered set of linearly independent vectors which span V. In particular two bases will be considered different even if one is simply a rearrangement of the other. This is sometimes referred to as an **ordered basis**.

Example:

(1) The space $V = F[x]$ of polynomials in the variable x with coefficients from the field F is in particular a vector space over F.
The elements $1, x, x^2, \ldots$ are linearly independent by definition, i.e., a polynomial is 0 if and only if all its coefficients are 0.
Since these elements also span V by definition, they are a basis for V.

Additional Example

(2) The collection of solutions of a linear, homogeneous, constant coefficient differential equation (for example, $y'' - 3y' + 2y = 0$) over $\mathbb{C}$ form a vector space over $\mathbb{C}$ since differentiation is a linear operator.

Elements of this vector space are linearly independent if they are linearly independent as functions.

For example, e^t and e^{2t} are easily seen to be solutions of the equation $y'' - 3y' + 2y = 0$ (differentiation with respect to t).

They are linearly independent functions: Assume $ae^t + be^{2t} = 0$.

- Set $t = 0$. We get $a + b = 0$.
- Set $t = 1$. We get $ae + be^2 = 0$.

The only solution to these two equations is $a = b = 0$.

It is a theorem in differential equations that these elements span the set of solutions of this equation. Hence they are a basis for this space.

Minimal Spanning Sets form Bases

Proposition

Assume the set $\mathcal{A} = \{v_1, v_2, \ldots, v_n\}$ spans the vector space V but no proper subset of $\mathcal{A}$ spans V. Then $\mathcal{A}$ is a basis of V. In particular, any finitely generated (i.e., finitely spanned) vector space over F is a free F-module.

- It is only necessary to prove that $v_1, v_2, \ldots, v_n$ are linearly independent. Suppose

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0,$$

where not all of the α_i are 0. By reordering, we may assume that $a_1 \neq 0$ and then $v_1 = -\frac{1}{\alpha_1}(\alpha_2 v_2 + \cdots \alpha_n v_n)$. Using this equation, any linear combination of $v_1, v_2, \ldots, v_n$ can be written as a linear combination of only $v_2, v_3, \ldots, v_n$. It follows that $\{v_2, v_3, \ldots, v_n\}$ also spans V. This is a contradiction.

An Example

- Let F be a field and consider $F[x]/(f(x))$, where $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$.

  The ideal $(f(x))$ is a subspace of the vector space $F[x]$ and the quotient $F[x]/(f(x))$ is also a vector space over F.

  By the Euclidean Algorithm, every polynomial $a(x) \in F[x]$ can be written uniquely in the form $a(x) = q(x)f(x) + r(x)$, where $r(x) \in F[x]$ and $0 \leq \deg r(x) \leq n-1$. Since $q(x)f(x) \in (f(x))$, it follows that every element of the quotient is represented by a polynomial $r(x)$ of degree $\leq n-1$. Two distinct such polynomials cannot be the same in the quotient since this would say their difference (which is a nonzero polynomial of degree at most $n-1$) would be divisible by $f(x)$ (which is of degree n). It follows that:
  - The elements $\overline{1}, \overline{x}, \overline{x^2}, \ldots, \overline{x^{n-1}}$ (the bar denotes image in the quotient) span $F[x]/(f(x))$ as a vector space over F;
  - No proper subset of these elements also spans $F[x]/(f(x))$.

  Hence, these elements give a basis for $F[x]/(f(x))$.

Existence of Basic and Replacement

Corollary

Assume the finite set $\mathcal{A}$ spans the vector space V. Then $\mathcal{A}$ contains a basis of V.

- Any subset $\mathcal{B}$ of $\mathcal{A}$ spanning V such that no proper subset of $\mathcal{B}$ also spans V (there clearly exist such subsets) is a basis for V.

Theorem (A Replacement Theorem)

Assume $\mathcal{A} = \{a_1, a_2, \ldots, a_n\}$ is a basis for V containing n elements and $\{b_1, b_2, \ldots, b_m\}$ is a set of linearly independent vectors in V. Then there is an ordering $a_1, a_2, \ldots, a_n$, such that, for each $k \in \{1, 2, \ldots, m\}$, the set $\{b_1, b_2, \ldots, b_k, a_{k+1}, a_{k+2}, \ldots, a_n\}$ is a basis of V. In other words, the elements $b_1, b_2, \ldots, b_m$ can be used to successively replace the elements of the basis $\mathcal{A}$, still retaining a basis. In particular, $n \geq m$.

- Proceed by induction on k.
  If $k = 0$, there is nothing to prove, since $\mathcal{A}$ is given as a basis for V.

Proof of Replacement (New Spanning Set)

- Suppose now that $\{b_1, b_2, \ldots, b_k, a_{k+1}, a_{k+2}, \ldots, a_n\}$ is a basis for V. Then, in particular, this is a spanning set. So b_{k+1} is a linear combination: $b_{k+1} = \beta_1 b_1 + \cdots + \beta_k b_k + \alpha_{k+1} a_{k+1} + \cdots + \alpha_n a_n$. Not all of the α_i can be 0, since this would imply b_{k+1} is a linear combination of $b_1, b_2, \ldots, b_k$, contrary to the linear independence of these elements. By reordering if necessary, we may assume $\alpha_{k+1} \neq 0$. Solving this last equation for α_{k+1} as a linear combination of b_{k+1} and $b_1, b_2, \ldots, b_k, a_{k+2}, \ldots, a_n$ shows

$$\begin{aligned} \text{Span}\{b_1, b_2, \ldots, b_k, b_{k+1}, a_{k+2}, \ldots, a_n\} \\ &= \text{Span}\{b_1, b_2, \ldots, b_k, a_{k+1}, a_{k+2}, \ldots, a_n\} \\ &= V. \end{aligned}$$

Thus, $\{b_1, b_2, \ldots, b_k, b_{k+1}, a_{k+2}, \ldots, a_n\}$ is a spanning set for V.

Proof of Replacement (Independence of the New Set)

- It remains to show $b_1, \ldots, b_k, b_{k+1}, a_{k+2}, \ldots, a_n$ are linearly independent. Suppose

$$\beta'_1 b_1 + \cdots + \beta'_k b_k + \beta'_{k+1} b_{k+1} + \alpha'_{k+2} a_{k+2} + \cdots + \alpha'_n a_n = 0.$$

Substitute for b_{k+1} from the expression

$$b_{k+1} = \beta_1 b_1 + \cdots + \beta_k b_k + \alpha_{k+1} a_{k+1} + \cdots + \alpha_n a_n.$$

We obtain a linear combination of $\{b_1, b_2, \ldots, b_k, a_{k+1}, a_{k+2}, \ldots, a_n\}$ equal to 0, where the coefficient of a_{k+1} is $\beta'_{k+1}\alpha_{k+1}$. This set is a basis by induction. Hence, all the coefficients in the linear combination$= 0$. Thus, $\beta'_{k+1}\alpha_{k+1} = 0$. Since $\alpha_{k+1} \neq 0$, $\beta'_{k+1} = 0$. But then we get

$$\beta'_1 b_1 + \cdots + \beta'_k b_k + \alpha'_{k+2} a_{k+2} + \cdots + \alpha'_n a_n = 0.$$

Again by the induction hypothesis all the other coefficients must be 0 as well. Thus $\{b_1, b_2, \ldots, b_k, b_{k+1}, a_{k+2}, \ldots, a_n\}$ is a basis for V.

Dimension

Corollary

(1) Suppose V has a finite basis with n elements. Any set of linearly independent vectors has $\leq n$ elements. Any spanning set has $\geq n$ elements.

(2) If V has some finite basis, then any two bases of V have the same cardinality.

(1) This is a restatement of the last result of the theorem.

(2) A basis is both a spanning set and a linearly independent set.

Definition (Dimension)

If V is a finitely generated F-module (i.e., has a finite basis) the cardinality of any basis is called the **dimension** of V and is denoted by $\dim_F V$, or just $\dim V$ when F is clear from the context, and V is said to be **finite dimensional** over F. If V is not finitely generated, V is said to be **infinite dimensional** (written $\dim V = \infty$).

Examples

(1) The dimension of the space of solutions to the differential equation $y'' - 3y' + 2y = 0$ over $\mathbb{C}$ is 2 (with basis e^t, e^{2t}, for example).

In general, it is a theorem in differential equations that the space of solutions of an n-th order linear, homogeneous, constant coefficient differential equation of degree n over $\mathbb{C}$ form a vector space over $\mathbb{C}$ of dimension n.

(2) The dimension over F of the quotient $F[x]/(f(x))$ by the nonzero polynomial $f(x)$ considered above is $n = \deg f(x)$.

The space $F[x]$ and its subspace $(f(x))$ are infinite dimensional vector spaces over F.

Building Up Lemma and Isomorphism Theorem

Lemma (Building-Up Lemma)

If A is a set of linearly independent vectors in the finite dimensional space V, then there exists a basis of V containing A.

- This is also immediate from the theorem, since we can use the elements of A to successively replace the elements of any given basis for V (which exists by the assumption that V is finite dimensional).

Theorem

If V is an n dimensional vector space over F, then $V \cong F^n$. In particular, any two finite dimensional vector spaces over F of the same dimension are isomorphic.

- Let $v_1, v_2, \ldots, v_n$ be a basis for V. Define the map $\varphi : F^n \to V$ by $\varphi(\alpha_1, \alpha_2, \ldots, \alpha_n) = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$. The map φ is F-linear, surjective since the v_i span V, and is injective since the v_i are linearly independent. Hence φ is an isomorphism.

Example I

(1) Let $\mathbb{F}$ be a finite field with q elements and let W be a k-dimensional vector space over $\mathbb{F}$. The number of distinct bases of W is $(q^k-1)(q^k-q)(q^k-q^2)\cdots(q^k-q^{k-1})$.
Every basis of W can be built up as follows:

- Any nonzero vector w_1 can be the first element of a basis. Since W is isomorphic to $\mathbb{F}^k$, $|W|=q^k$, so there are q^k-1 choices for w_1.
- Any vector not in the 1-dimensional space spanned by w_1 is linearly independent from w_1 and so may be chosen for the second basis element, w_2. A 1-dimensional space is isomorphic to $\mathbb{F}$ and so has q elements. Thus, there are q^k-q choices for w_2.
- Proceeding in this way one sees that at the i-th stage, any vector not in the $(i-1)$-dimensional space spanned by $w_1,w_2,\ldots,w_{i-1}$ will be linearly independent from $w_1,w_2,\ldots,w_{i-1}$ and so may be chosen for the i-th basis vector w_i. An $(i-1)$-dimensional space is isomorphic to $\mathbb{F}^{i-1}$ and so has q^{i-1} elements. So, there are q^k-q^{i-1} choices for w_i.

The process terminates when w_k is chosen, for then we have k linear independent vectors in a k-dimensional space, hence a basis.

Example II

(2) Let $\mathbb{F}$ be a finite field with q elements and let V be an n-dimensional vector space over $\mathbb{F}$. For each $k \in \{1, 2, \ldots, n\}$, we show that the number of subspaces of V of dimension k is $\frac{(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})}$.

Any k-dimensional space is spanned by k independent vectors.

- By arguing as in the preceding example the numerator of the above expression is the number of ways of picking k independent vectors from an n-dimensional space.
- Two sets of k independent vectors span the same space W if and only if they are both bases of the k-dimensional space W.
  In order to obtain the formula for the number of distinct subspaces of dimension k we must divide by the number of repetitions, i.e., the number of bases of a fixed k-dimensional space. This factor which appears in the denominator is precisely this number.

The Dimensions of a Subspace and of its Quotient Space

- We prove a relation between the dimensions of a subspace, the associated quotient space and the whole space:

Theorem

Let V be a vector space over F and let W be a subspace of V. Then V/W is a vector space with $\dim V = \dim W + \dim V/W$, where, if one side is infinite, then both are.

- Suppose $\dim W = m$ and $\dim V = n$ and let $w_1, w_2, \ldots, w_m$ be a basis for W. These linearly independent elements of V can be extended to a basis $w_1, w_2, \ldots, w_m, v_{m+1}, \ldots, v_n$ of V. The natural surjective projection map of V into V/W maps each w_i to 0. No linear combination of the v_i is mapped to 0, since no linear combination is in W. Hence, the image V/W of this projection map is isomorphic to the subspace of V spanned by the v_i. Hence $\dim V/W = n - m$, the conclusion when the dimensions are finite.

  If either side is infinite the other side is also infinite.

Images and Kernels of Linear Transformations

Corollary

Let $\varphi : V \to U$ be a linear transformation of vector spaces over F. Then $\ker\varphi$ is a subspace of V, $\varphi(V)$ is a subspace of U and

$$\dim V = \dim\ker\varphi + \dim\varphi(V).$$

- We know that $\varphi(V) \cong V/\ker\varphi$.

  In particular, $\dim\varphi(V) = \dim V/\ker\varphi$.

  Now we get, using the theorem,

$$\begin{aligned} \dim V &= \dim\ker\varphi + \dim V/\ker\varphi \\ &= \dim\ker\varphi + \dim\varphi(V). \end{aligned}$$

Characteristic Properties of Isomorphisms

Corollary

Let $\varphi : V \to W$ be a linear transformation of vector spaces of the same finite dimension. Then the following are equivalent:

(1) φ is an isomorphism;
(2) φ is injective, i.e., $\ker\varphi = 0$;
(3) φ is surjective, i.e., $\varphi(V) = W$;
(4) φ sends a basis of V to a basis of W.

- The equivalence of these conditions follows from the corollary by counting dimensions.

Null Space and Nullity

Definition (Null Space and Nullity)

If $\varphi : V \to U$ is a linear transformation of vector spaces over F, $\ker\varphi$ is sometimes called the **null space** of φ and the dimension of $\ker\varphi$ is called the **nullity** of φ. The dimension of $\varphi(V)$ is called the **rank** of φ. If $\ker\varphi = 0$, the transformation is said to be **nonsingular**.

Example: Let F be a finite field with q elements, V an n-dimensional vector space over F. The general linear group $\mathrm{GL}(V)$ is the group of all nonsingular linear transformations from V to V under composition. The order is $|\mathrm{GL}(V)| = (q^n - 1)(q^n - q)(q^n - q^2)\cdots(q^n - q^{n-1})$. Fix a basis $v_1, \ldots, v_n$ of V. A linear transformation is nonsingular if and only if it sends this basis to another basis of V. Moreover, if $w_1, \ldots, w_n$ is any basis of V, by UMP, there is a unique linear transformation which sends v_i to w_i, $1 \leq i \leq n$. Thus, the number of nonsingular linear transformations from V to itself equals the number of distinct bases of V. This number is the order of $\mathrm{GL}(V)$.

Subsection 2

The Matrix of a Linear Transformation

Obtaining a Matrix of a Linear Transformation

- Let V, W be vector spaces over the same field F.
  - Let $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$ be an (ordered) basis of V;
  - Let $\mathcal{E} = \{w_1, w_2, \ldots, w_m\}$ be an (ordered) basis of W.

  Let $\varphi \in \mathrm{Hom}(V, W)$ be a linear transformation from V to W.
- For each $j \in \{1, 2, \ldots, n\}$, write the image of v_j under φ in terms of the basis $\mathcal{E}$:
$$\varphi(v_j) = \sum_{i=1}^{m} \alpha_{ij} w_i.$$
- Let $M_{\mathcal{B}}^{\mathcal{E}}(\varphi) = (a_{ij})$ be the $m \times n$ matrix whose i, j entry is α_{ij}.
- The matrix $M_{\mathcal{B}}^{\mathcal{E}}(\varphi)$ is called the **matrix of φ with respect to the bases $\mathcal{B}, \mathcal{E}$**.

  The domain basis is the lower and the codomain basis the upper letters appearing after the "M".

Obtaining a Linear Transformation from a Matrix

- Given $M_{\mathcal{B}}^{\mathcal{E}}(\varphi)$, we can recover the linear transformation φ as follows: To compute $\varphi(v)$ for $v \in V$, write v in terms of the basis $\mathcal{B}$

$$v = \sum_{i=1}^{n} \alpha_i v_i, \quad \alpha_i \in F;$$

Then calculate the product of the $m \times n$ and $n \times 1$ matrices

$$M_{\mathcal{B}}^{\mathcal{E}}(\varphi) \times \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_m \end{pmatrix}.$$

The image of v under φ is $\varphi(v) = \sum_{i=1}^{m} \beta_i w_i$, i.e., the column vector of coordinates of $\varphi(v)$ with respect to the basis $\mathcal{E}$ are obtained by multiplying the matrix $M_{\mathcal{B}}^{\mathcal{E}}(\varphi)$ by the column vector of coordinates of v with respect to the basis $\mathcal{B}$: $[\varphi(v)]_{\mathcal{E}} = M_{\mathcal{B}}^{\mathcal{E}}(\varphi)[v]_{\mathcal{B}}$.

Representation

Definition

The $m \times n$ matrix $A = (a_{ij})$ associated to the linear transformation φ above is said to **represent** the linear transformation φ **with respect to the bases** $\mathcal{B}, \mathcal{E}$. Similarly, φ is the linear transformation **represented by** A **with respect to the bases** $\mathcal{B}$, $\mathcal{E}$.

Example: Let $V = \mathbb{R}^3$ with the standard basis $\mathcal{B} = \{(1,0,0), (0,1,0), (0,0,1)\}$. Let $W = \mathbb{R}^2$ with the standard basis $\mathcal{E} = \{(1,0), (0,1)\}$. Let φ be the linear transformation

$$\varphi(x,y,z) = (x + 2y, x + y + z).$$

Since $\varphi(1,0,0) = (1,1)$, $\varphi(0,1,0) = (2,1)$, $\varphi(0,0,1) = (0,1)$, the matrix $A = M_{\mathcal{B}}^{\mathcal{E}}(\varphi)$ is the matrix $\left(\begin{array}{ccc} 1 & 2 & 0 \\ 1 & 1 & 1 \end{array}\right)$.

Another Example

- Let $V = W$ be the 2-dimensional space of solutions of the differential equation $y'' - 3y' + 2y = 0$ over $\mathbb{C}$ and let $\mathcal{B} = \mathcal{E}$ be the basis $v_1 = e^t$, $v_2 = e^{2t}$.

  Since the coefficients of this equation are constants, it is easy to check that, if y is a solution then its derivative y' is also a solution.

  It follows that the map

$$\varphi = \frac{d}{dt} = \text{differentiation (with respect to } t\text{)}$$

  is a linear transformation from V to itself.

  Note that $\varphi(v_1) = \frac{d(e^t)}{dt} = e^t = v_1$ and $\varphi(v_2) = \frac{d(e^{2t})}{dt} = 2e^{2t} = 2v_2$. Thus, the corresponding matrix with respect to these bases is the diagonal matrix $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$.

A Third Example

- Let $V = W = \mathbb{Q}^3 = \{(x, y, z) : x, y, z \in \mathbb{Q}\}$ be the 3-dimensional vector space of ordered 3-tuples with entries from the field $F = \mathbb{Q}$ of rational numbers.

  Let $\varphi : V \to V$ be the linear transformation

  $$\varphi(x, y, z) = (9x + 4y + 5z, -4x - 3z, -6x - 4y - 2z), \; x, y, z \in \mathbb{Q}.$$

  Take the standard basis $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$, $e_3 = (0, 0, 1)$ for V and for $W = V$.

  We have $\varphi(1, 0, 0) = (9, -4, -6)$, $\varphi(0, 1, 0) = (4, 0, -4)$, $\varphi(0, 0, 1) = (5, -3, -2)$.

  Hence, the matrix A representing this linear transformation with respect to these bases is $A = \begin{pmatrix} 9 & 4 & 5 \\ -4 & 0 & -3 \\ -6 & -4 & -2 \end{pmatrix}$.

Isomorphism Between $\mathrm{Hom}_F(V, W)$ and $M_{m\times n}(F)$

Theorem

Let V be a vector space over F of dimension n and let W be a vector space over F of dimension m, with bases $\mathcal{B}, \mathcal{E}$, respectively. Then the map $\mathrm{Hom}_F(V, W) \to M_{m\times n}(F)$ from the space of linear transformations from V to W to the space of $m \times n$ matrices with coefficients in F defined by $\varphi \mapsto M_{\mathcal{B}}^{\mathcal{E}}(\varphi)$ is a vector space isomorphism. In particular, there is a bijective correspondence between linear transformations and their associated matrices with respect to a fixed choice of bases.

- The columns of the matrix $M_{\mathcal{B}}^{\mathcal{E}}(\varphi)$ are determined by the action of φ on $\mathcal{B}$. Thus, the map $\varphi \mapsto M_{\mathcal{B}}^{\mathcal{E}}(\varphi)$ is F-linear, since φ is F-linear.
  - This map is surjective: Let $M \in M_{m\times n}(F)$. Define $\varphi : V \to W$ by $\varphi(v_j) = \sum_{i=1}^{m} \alpha_{ij} w_i$ and extend it by linearity. Then φ is a linear transformation and $M_{\mathcal{B}}^{\mathcal{E}}(\varphi) = M$.
  - The map is injective: Two linear transformations agreeing on a basis are the same.

Nonsingularity

Corollary

The dimension of $\mathrm{Hom}_F(V, W)$ is $(\dim V)(\dim W)$.

- The dimension of $M_{m\times n}(F)$ is mn.

Definition

An $m \times n$ matrix A is called **nonsingular** if $Ax = 0$, with $x \in F^n$, implies $x = 0$.

- The connection of the term nonsingular applied to matrices and to linear transformations is the following:

  Let $A = M_{\mathcal{B}}^{\mathcal{E}}(\varphi)$ be the matrix associated to the linear transformation φ (with some choice of bases $\mathcal{B}, \mathcal{E}$).

  Then independently of the choice of bases, the $m \times n$ matrix A is nonsingular if and only if the linear transformation φ is a nonsingular linear transformation from the n-dimensional space V to the m-dimensional space W.

Linear Transformations and Matrices

Theorem

$M_{\mathcal{D}}^{\mathcal{E}}(\varphi \circ \psi) = M_{\mathcal{B}}^{\mathcal{E}}(\varphi) M_{\mathcal{D}}^{\mathcal{B}}(\psi)$, i.e., with respect to a compatible choice of bases, the product of the matrices representing the linear transformations φ and ψ is the matrix representing the composite linear transformation $\varphi \circ \psi$.

- Assume that U, V and W are all finite dimensional vector spaces over F with ordered bases $\mathcal{D}, \mathcal{B}$ and $\mathcal{E}$, respectively, where $\mathcal{B}$ and $\mathcal{E}$ are as before and suppose $\mathcal{D} = \{u_1, u_2, \ldots, u_k\}$. Assume $\psi : U \to V$ and $\varphi : V \to W$ are linear transformations. Their composite, $\varphi \circ \psi$, is a linear transformation from U to W. So we can compute its matrix with respect to the appropriate bases. $M_{\mathcal{D}}^{\mathcal{E}}(\varphi \circ \psi)$ is found by computing $\varphi \circ \psi(u_j) = \sum_{i=1}^{m} \gamma_{ij} w_i$ and putting the coefficients γ_{ij} down the j-th column of $M_{\mathcal{D}}^{\mathcal{E}}(\varphi \circ \psi)$. Next, compose the matrices of ψ and φ separately: $\psi(u_j) = \sum_{p=1}^{n} \alpha_{pj} v_p$ and $\varphi(v_p) = \sum_{i=1}^{m} \beta_{ip} w_i$, so that $M_{\mathcal{D}}^{\mathcal{B}}(\psi) = (\alpha_{pj})$ and $M_{\mathcal{B}}^{\mathcal{E}}(\varphi) = (\beta_{ip})$.

Linear Transformations and Matrices (Cont'd)

- Using $M_{\mathcal{D}}^{\mathcal{B}}(\psi) = (\alpha_{pj})$ and $M_{\mathcal{B}}^{\mathcal{E}}(\varphi) = (\beta_{ip})$ we can find an expression for the γ's in terms of the α's and β's as follows:

$$\begin{aligned} \varphi \circ \psi(u_j) &= \varphi(\textstyle\sum_{p=1}^n \alpha_{pj} v_p) = \sum_{p=1}^n \alpha_{pj} \varphi(v_p) \\ &= \textstyle\sum_{p=1}^n \alpha_{pj} \sum_{i=1}^m \beta_{ip} w_i \\ &= \textstyle\sum_{p=1}^n \sum_{i=1}^m \alpha_{pj} \beta_{ip} w_i \\ &= \textstyle\sum_{i=1}^m (\sum_{p=1}^n \alpha_{pj} \beta_{ip}) w_i. \end{aligned}$$

  - Thus, γ_{ij}, which is the coefficient of w_i in the above expression, is $\gamma_{ij} = \sum_{p=1}^n \alpha_{pj} \beta_{ip}$;
  - Computing the product of the matrices for φ and ψ (in that order) we obtain $(\beta_{ij})(\alpha_{ij}) = (\delta_{ij})$, where $\delta_{ij} = \sum_{p=1}^m \beta_{ip} \alpha_{pj}$.

By comparing the two sums above and using the commutativity of field multiplication, we see that for all i and j, $\gamma_{ij} = \delta_{ij}$.

Associativity and Distributivity of Matrix Multiplication

Corollary

Matrix multiplication is associative and distributive (whenever the dimensions are such as to make products defined).
An $n \times n$ matrix A is nonsingular if and only if it is invertible.

- Let A, B and C be matrices such that the products $(AB)C$ and $A(BC)$ are defined. Let S, T and R denote the associated linear transformations. By the theorem, the linear transformation corresponding to AB is the composite $S \circ T$. So the linear transformation corresponding to $(AB)C$ is the composite $(S \circ T) \circ R$. Similarly, the linear transformation corresponding to $A(BC)$ is the composite $S \circ (T \circ R)$. Since function composition is associative, these linear transformations are the same. Hence, $(AB)C = A(BC)$.

  The distributivity is proved similarly.

Nonsingularity and Invertibility

- Suppose A is invertible and $Ax = 0$. Then

$$x = A^{-1}Ax = A^{-1}0 = 0.$$

So A is nonsingular.

Conversely, suppose A is nonsingular. Fix bases $\mathcal{B}, \mathcal{E}$ for V. Let φ be the linear transformation of V to itself represented by A with respect to these bases. By the corollary, φ is an isomorphism of V to itself. Hence, it has an inverse, φ^{-1}. Let B be the matrix representing φ^{-1} with respect to the bases $\mathcal{E}, \mathcal{B}$. Then

$$AB = M_{\mathcal{B}}^{\mathcal{E}}(\varphi) M_{\mathcal{E}}^{\mathcal{B}}(\varphi^{-1}) = M_{\mathcal{E}}^{\mathcal{E}}(\varphi \circ \varphi^{-1}) = M_{\mathcal{E}}^{\mathcal{E}}(1) = I.$$

Similarly, $BA = I$. So B is the inverse of A.

Group of Linear Transformations

Corollary

(1) If $\mathcal{B}$ is a basis of the n-dimensional space V, the map $\varphi \mapsto M_{\mathcal{B}}^{\mathcal{B}}(\varphi)$ is a ring and a vector space isomorphism of $\mathrm{Hom}_F(V, V)$ onto the space $M_n(F)$ of $n \times n$ matrices with coefficients in F.

(2) $\mathrm{GL}(V) \cong \mathrm{GL}_n(F)$, where $\dim V = n$. In particular, if F is a finite field, the order of the finite group $\mathrm{GL}_n(F)$ (which equals $|\mathrm{GL}(V)|$) is given by the formula developed previously.

(1) We have already seen that this map is an isomorphism of vector spaces over F. The corollary shows that $M_n(F)$ is a ring under matrix multiplication. The theorem shows that multiplication is preserved under this map. Hence, it is also a ring isomorphism.

(2) This is immediate from Part (1) since a ring isomorphism sends units to units.

Row and Column Rank

Definition (Row Rank and Column Rank)

If A is any $m \times n$ matrix with entries from F, the **row rank** (respectively, **column rank**) of A is the maximal number of linearly independent rows (respectively, columns) of A (where the rows or columns of A are considered as vectors in affine n-space, m-space, respectively).

- The rank of φ as a linear transformation equals the column rank of the matrix $M_{\mathcal{B}}^{\mathcal{E}}(\varphi)$.
- We will see that the row rank and the column rank of any matrix are the same.

Similarity

Definition (Similarity)

Two $n \times n$ matrices A and B are said to be **similar** if there is an invertible (i.e., nonsingular) $n \times n$ matrix P, such that

$$P^{-1}AP = B.$$

Two linear transformations φ and ψ from a vector space V to itself are said to be **similar** if there is a nonsingular linear transformation ξ from V to V, such that

$$\xi^{-1}\varphi\xi = \psi.$$

Transition or Change of Basis Matrix

- Suppose $\mathcal{B}$ and $\mathcal{E}$ are two bases of the same vector space V and let $\varphi \in \mathrm{Hom}_F(V, V)$.

  Let I be the identity map from V to V and let $P = M_{\mathcal{E}}^{\mathcal{B}}(I)$ be its associated matrix:
  - Write the elements of the basis $\mathcal{E}$ in terms of the basis $\mathcal{B}$;
  - Use the resulting coordinates for the columns of the matrix P.

  Note that if $\mathcal{B} \neq \mathcal{E}$ then P is not the identity matrix.

  Then $P^{-1} M_{\mathcal{B}}^{\mathcal{B}}(\varphi) P = M_{\mathcal{E}}^{\mathcal{E}}(\varphi)$.

  If $[v]_{\mathcal{B}}$ is the $n \times 1$ matrix of coordinates for $v \in V$ with respect to the basis $\mathcal{B}$, and similarly $[v]_{\mathcal{E}}$ is the $n \times 1$ matrix of coordinates for $v \in V$ with respect to the basis $\mathcal{E}$, then $[v]_{\mathcal{B}} = P[v]_{\mathcal{E}}$.
- The matrix P is called the **transition** or **change of basis matrix** from $\mathcal{B}$ to $\mathcal{E}$. This similarity action on $M_{\mathcal{B}}^{\mathcal{B}}(\varphi)$ is called a **change of basis**.
- Thus, the matrices associated to the same linear transformation with respect to two different bases are similar.

Transition or Change of Basis Matrix (Cont'd)

- Conversely, suppose A and B are $n \times n$ matrices similar by a nonsingular matrix P.

  Let $\mathcal{B}$ be a basis for the n-dimensional vector space V.

  Define the linear transformation φ of V (with basis $\mathcal{B}$) to V (again with basis $\mathcal{B}$) using the given matrix A, i.e., $\varphi(v_j) = \sum_{i=1}^{n} \alpha_{ij} v_i$.

  Then $A = M_{\mathcal{B}}^{\mathcal{B}}(\varphi)$ by definition of φ.

  Define a new basis $\mathcal{E}$ of V by using the i-th column of P for the coordinates of w_i in terms of the basis $\mathcal{B}$ ($P = M_{\mathcal{E}}^{\mathcal{B}}(I)$ by definition).

  Then $B = P^{-1}AP = P^{-1}M_{\mathcal{B}}^{\mathcal{B}}(\varphi)P = M_{\mathcal{B}}^{\mathcal{E}}(I)M_{\mathcal{B}}^{\mathcal{B}}(\varphi)M_{\mathcal{E}}^{\mathcal{B}}(I) = M_{\mathcal{E}}^{\mathcal{E}}(\varphi)$ is the matrix associated to φ with respect to the basis $\mathcal{E}$.

- This shows that any two similar $n \times n$ matrices arise in this fashion as the matrices representing the same linear transformation with respect to two different choices of bases.

Similarity Classes or Conjugacy Classes

- Change of basis for a linear transformation from V to itself is the same as conjugation by some element of the group $\mathrm{GL}(V)$ of nonsingular linear transformations of V to V.
- In particular, the relation "similarity" is an equivalence relation whose equivalence classes are the orbits of $\mathrm{GL}(V)$ acting by conjugation on $\mathrm{Hom}_F(V, V)$.
- If $\varphi \in \mathrm{GL}(V)$ (i.e., φ is an invertible linear transformation), then the similarity class of φ is none other than the conjugacy class of φ in the group $\mathrm{GL}(V)$.

Example

- Let $V = \mathbb{Q}^3$ and let φ be the linear transformation

  $$\varphi(x, y, z) = (9x + 4y + 5z, -4x - 3z, -6x - 4y - 2z),\ x, y, z \in \mathbb{Q},$$

  from V to itself.

  With respect to the standard basis, $\mathcal{B}$, $b_1 = (1, 0, 0)$, $b_2 = (0, 1, 0)$, $b_3 = (0, 0, 1)$, we saw that the matrix A representing this linear transformation is

  $$A = M_{\mathcal{B}}^{\mathcal{B}}(\varphi) = \begin{pmatrix} 9 & 4 & 5 \\ -4 & 0 & -3 \\ -6 & -4 & -2 \end{pmatrix}.$$

Example (Cont'd)

$$\varphi(x,y,z) = (9x+4y+5z, -4x-3z, -6x-4y-2z),\ x,y,z \in \mathbb{Q}.$$

- Take now the basis, $\mathcal{E}$, $e_1 = (2,-1,-2)$, $e_2 = (1,0,-1)$, $e_3 = (3,-2,-2)$ for V.
  We have
  $$\begin{aligned} \varphi(e_1) &= \varphi(2,-1,-2) = (4,-2,-4) = 2e_1 + 0e_2 + 0e_3; \\ \varphi(e_2) &= \varphi(1,0,-1) = (4,-1,-4) = 1e_1 + 2e_2 + 0e_3; \\ \varphi(e_3) &= \varphi(3,-2,-2) = (9,-6,-6) = 0e_1 + 0e_2 + 3e_3. \end{aligned}$$
  Hence, the matrix representing φ with respect to this basis is the matrix
  $$B = M_{\mathcal{E}}^{\mathcal{E}}(\varphi) = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

Example (Cont'd)

- We have
  - $\mathcal{B} = \{b_1, b_2, b_3\} = \{(1,0,0),(0,1,0),(0,0,1)\}$;
  - $\mathcal{E} = \{e_1, e_2, e_3\} = \{(2,-1,-2),(1,0,-1),(3,-2,-2)\}$.
- Writing the elements of the basis $\mathcal{E}$ in terms of the basis $\mathcal{B}$, we have

$$\begin{array}{lcl} e_1 & = & 2b_1 - b_2 - 2b_3; \\ e_2 & = & b_1 - b_3; \\ e_3 & = & 3b_1 - 2b_2 - 2b_3. \end{array}$$

So the matrix $P = M_{\mathcal{E}}^{\mathcal{B}}(I) = \begin{pmatrix} 2 & 1 & 3 \\ -1 & 0 & -2 \\ -2 & -1 & -2 \end{pmatrix}$ with inverse

$$P^{-1} = \begin{pmatrix} -2 & -1 & -2 \\ 2 & 2 & 1 \\ 1 & 0 & 1 \end{pmatrix}.$$

This P conjugates A into B, i.e., $P^{-1}AP = B$.

Subsection 3

Dual Vector Spaces

Dual Space and Linear Functionals

Definition (Dual Space, Linear Functional)

(1) For V any vector space over F, let $V^* = \text{Hom}_F(V, F)$ be the space of linear transformations from V to F, called the **dual space** of V. Elements of V^* are called **linear functionals**.

(2) If $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$ is a basis of the finite dimensional space V, define $v_i^* \in V^*$, for each $i \in \{1, 2, \ldots, n\}$ by its action on the basis $\mathcal{B}$:

$$v_i^*(v_j) = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases}, \quad 1 \leq j \leq n.$$

Proposition

With notations as above, $\{v_1^*, v_2^*, \ldots, v_n^*\}$ is a basis of V^*. In particular, if V is finite dimensional, then V^* has the same dimension as V.

Dual Basis

- Observe that since V is finite dimensional,

$$\dim V^* = \dim \mathrm{Hom}_F(V, F) = \dim V = n.$$

So, since there are n of the v_i^*'s, it suffices to prove that they are linearly independent. Suppose

$$\alpha_1 v_1^* + \alpha_2 v_2^* + \cdots + \alpha_n v_n^* = 0$$

in $\mathrm{Hom}_F(V, F)$. Applying this element to v_i, we obtain $\alpha_i = 0$. Since i is arbitrary these elements are linearly independent.

Definition (Dual Basis)

The basis $\{v_1^*, v_2^*, \ldots, v_n^*\}$ of V^* is called the **dual basis** to $\{v_1, v_2, \ldots, v_n\}$.

Remarks on Linear Functionals

- If V is infinite dimensional it is always true that $\dim V < \dim V^*$.
- For spaces of arbitrary dimension, the space V^* is the "algebraic" dual space to V.
- If V has some additional structure, for example a continuous structure (i.e., a topology), then one may define other types of dual spaces (e.g., the continuous dual of V, defined by requiring the linear functionals to be continuous maps).
- One has to be careful when reading other works (particularly analysis books) to ascertain what qualifiers are implicit in the use of the terms "dual space" and "linear functional."

  Example: Let $[a, b]$ be a closed interval in $\mathbb{R}$. Let V be the real vector space of all continuous functions $f : [a, b] \to \mathbb{R}$. If $a < b$, V is infinite dimensional. For each $g \in V$, the function $\varphi : V \to \mathbb{R}$ defined by $\varphi_g(f) = \int_a^b f(t)g(t)dt$ is a linear functional on V.

The Double Dual

Definition (The Double Dual)

The dual of V^*, namely V^{**}, is called the **double dual** or **second dual** of V.

- Note that for a finite dimensional space V,

$$\dim V^{**} = \dim V^* = \dim V.$$

  Hence, V and V^{**} are isomorphic vector spaces.
- For infinite dimensional spaces $\dim V < \dim V^{**}$.

  So V and V^{**} cannot be isomorphic.

Evaluation at x

- Let X is any set.
- Let S be any set of functions of X into the field F.
- Fix a point x in X.
- Compute $f(x)$ as f ranges over all of S.
- This process, called **evaluation at** x, shows that for each $x \in X$, there is a function $E_x : S \to F$ defined by

$$E_x(f) = f(x).$$

- This gives a map $x \to E_x$ of X into the set of F-valued functions on S.
- If S "separates points", i.e., for distinct points x and y of X, there is some $f \in S$, such that $f(x) \neq f(y)$, then the map $x \mapsto E_x$ is injective.

A Vector Space and its Double Dual

Theorem

There is a natural injective linear transformation from V to V^{**}. If V is finite dimensional then this linear transformation is an isomorphism.

- Let $v \in V$. Define the map (evaluation at v) $E_v : V^* \to F$ by $E_v(f) = f(v)$. Then

$$E_v(f + \alpha g) = (f + \alpha g)(v) = f(v) + \alpha g(v) = E_v(f) + \alpha E_v(g).$$

So E_v is a linear transformation from V^* to F. Hence E_v is an element of $\mathrm{Hom}_F(V^*, F) = V^{**}$. This defines a natural map $\varphi : V \to V^{**}$ by

$$\varphi(v) = E_v.$$

φ is a linear map: For $v, w \in V$, $\alpha \in F$, we get, for all $f \in V^*$,

$$E_{v+\alpha w}(f) = f(v + \alpha w) = f(v) + \alpha f(w) = E_v(f) + \alpha E_w(f).$$

So $\varphi(v + \alpha w) = E_{v+\alpha w} = E_v + \alpha E_w = \varphi(v) + \alpha\varphi(w)$.

A Vector Space and its Double Dual (Cont'd)

- We set $\varphi : V \to V^{**}$, $\varphi(v) = E_v$ and showed φ is linear.

  To see that φ is injective let v be any nonzero vector in V. By the Building Up Lemma there is a basis $\mathcal{B}$ containing v. Let f be the linear transformation from V to F defined by sending v to 1 and every element of $\mathcal{B} - \{v\}$ to zero. Then $f \in V^*$ and

  $$E_v(f) = f(v) = 1.$$

  Thus $\varphi(v) = E_v$ is not zero in V^{**}. This proves $\ker\varphi = 0$, i.e., φ is injective.

  If V has finite dimension n, then, by the proposition, V^* and hence also V^{**} has dimension n. In this case φ is an injective linear transformation from V to a finite dimensional vector space of the same dimension. Hence, it is an isomorphism.

Relating Dual Spaces

- Let V, W be finite dimensional vector spaces over F with bases $\mathcal{B}, \mathcal{E}$, respectively, and let $\mathcal{B}^*, \mathcal{E}^*$ be the dual bases.
  Fix some $\varphi \in \mathrm{Hom}_F(V, W)$. Then, for each $f \in W^*$, the composite $f \circ \varphi$ is a linear transformation from V to F, that is $f \circ \varphi \in V^*$.
  Thus, the map $f \mapsto f \circ \varphi$ defines a function from W^* to V^*. We denote this induced function on dual spaces by φ^*.

Theorem

With notations as above, φ^* is a linear transformation from W^* to V^* and $M_{\mathcal{E}^*}^{\mathcal{B}^*}(\varphi^*)$ is the transpose of the matrix $M_{\mathcal{B}}^{\mathcal{E}}(\varphi)$ (recall that the transpose of the matrix (a_{ij}) is the matrix (a_{ji})).

- The map φ^* is linear because $(f + \alpha g) \circ \varphi = (f \circ \varphi) + \alpha(g \circ \varphi)$. The equations which define φ are (from its matrix)

$$\varphi(v_j) = \sum_{i=1}^{m} \alpha_{ij} w_i, \quad 1 \leq j \leq n.$$

Relating Dual Spaces (Cont'd)

- To compute the matrix for φ^*, observe that by the definitions of φ^* and w_k^*,

$$\varphi^*(w_k^*)(v_j) = (w_k^* \circ \varphi)(v_j) = w_k^*(\sum_{i=1}^{m} \alpha_{ij} w_i) = \alpha_{kj}.$$

Also, for all j,

$$(\sum_{i=1}^{n} \alpha_{ki} v_i^*)(v_j) = \alpha_{kj}.$$

This shows that the two linear functionals below agree on a basis of V, hence they are the same element of V^*: $\varphi^*(w_k^*) = \sum_{i=1}^{n} \alpha_{ki} v_i^*$. This determines the matrix for φ^* with respect to the bases $\mathcal{E}^*$ and $\mathcal{B}^*$ as the transpose of the matrix for φ.

Row Rank and Column Rank of a Matrix

Corollary

For any matrix A, the row rank of A equals the column rank of A.

- Let $\varphi : V \to W$ be a linear transformation whose matrix with respect to some fixed bases of V and W is A. By the theorem, the matrix of $\varphi^* : W^* \to V^*$ with respect to the dual bases is the transpose of A. The column rank of A is the rank of φ and the row rank of A ($=$ the column rank of the transpose of A) is the rank of φ^*. It therefore suffices to show that φ and φ^* have the same rank.

  Now $f \in \ker\varphi^*$ iff $\varphi^*(f) = 0$ iff $f \circ \varphi(v) = 0$, for all $v \in V$, iff $\varphi(V) \subseteq \ker f$ iff $f \in \text{Ann}(\varphi(V))$, where $\text{Ann}(S)$ is the annihilator of S.

  Thus $\text{Ann}(\varphi(V)) = \ker\varphi^*$. But $\dim\ker\varphi^* = \dim W^* - \dim\varphi^*(W^*)$. We can also show $\dim\text{Ann}(\varphi(V)) = \dim W - \dim\varphi(V)$. But W and W^* have the same dimension. So $\dim\varphi(V) = \dim\varphi^*(W^*)$.

Subsection 4

Determinants

Multilinear Functions

- Let R be any commutative ring with 1.
  Let $V_1, V_2, \ldots, V_n, V$ and W be R-modules.

Definition (Multilinear Functions)

(1) A map $\varphi : V_1 \times V_2 \times \cdots \times V_n \to W$ is called **multilinear** if, for each fixed i and fixed elements $v_j \in V_j$, $j \neq i$, the map $V_i \to W$,

$$x \mapsto \varphi(v_1, \ldots, v_{i-1}, x, v_{i+1}, \ldots, v_n)$$

is an R-module homomorphism.

If $V_i = V$, $i = 1, 2, \ldots, n$, then φ is called an ***n*-multilinear function on V**.

If, in addition, $W = \mathbb{R}$, φ is called an ***n*-multilinear form on V**.

(2) An n-multilinear function φ on V is called **alternating** if $\varphi(v_1, v_2, \ldots, v_n) = 0$, whenever $v_i = v_{i+1}$, for some $i \in \{1, 2, \ldots, n-1\}$ (i.e., φ is zero whenever two consecutive arguments are equal).

The function φ is called **symmetric** if interchanging v_i and v_j, for any i and j in $(v_1, v_2, \ldots, v_n)$ does not alter the value of φ on this n-tuple.

Remarks on Multilinear Functions

- When $n = 2$ (respectively, 3) one says φ is **bilinear** (respectively, **trilinear**).
- Also, when n is clear from the context we shall simply say φ is multilinear.

  Example: For any fixed $m \geq 0$ the usual dot product on $V = \mathbb{R}^m$ is a bilinear form.

Properties of Alternating Multilinear Functions

Proposition

Let φ be an n-multilinear alternating function on V. Then:

(1) $\varphi(v_1, \ldots, v_{i-1}, v_{i+1}, v_i, v_{i+2}, \ldots, v_n) = -\varphi(v_1, v_2, \ldots, v_n)$, for any $i \in \{1, 2, \ldots, n-1\}$, i.e., the value of φ on an n-tuple is negated if two adjacent components are interchanged.

(2) For each $\sigma \in S_n$,

$$\varphi(v_{\sigma(1)}, v_{\sigma(2)}, \ldots, v_{\sigma(n)}) = \epsilon(\sigma)\varphi(v_1, v_2, \ldots, v_n),$$

where $\epsilon(\sigma)$ is the sign of the permutation σ.

(3) If $v_i = v_j$, for any pair of distinct $i, j \in \{1, 2, \ldots, n\}$, then $\varphi(v_1, v_2, \ldots, v_n) = 0$.

(4) If v_i is replaced by $v_i + \alpha v_j$ in $(v_1, \ldots, v_n)$, for any $j \neq i$ and any $\alpha \in R$, the value of φ on this n-tuple is not changed.

Properties of Alternating Multilinear Functions (Cont'd)

(1) Let $\psi(x, y)$ be the function φ with variable entries x and y in positions i and $i+1$, respectively, and fixed entries v_j in position j, for all other j. Thus, (1) is the same as showing $\psi(y, x) = -\psi(x, y)$. Since φ is alternating $\psi(x+y, x+y) = 0$. Expanding $x+y$ gives $\psi(x+y, x+y) = \psi(x, x) + \psi(x, y) + \psi(y, x) + \psi(y, y)$. Again, by the alternating property of φ, the first and last terms on the right hand side of the latter equation are zero. Thus $0 = \psi(x, y) + \psi(y, x)$.

(2) Every permutation can be written as a product of transpositions. Furthermore, every transposition may be written as a product of transpositions which interchange two successive integers. Thus, every permutation σ can be written as $\tau_1 \cdots \tau_m$, where τ_k is a transposition interchanging two successive integers, for all k. Apply (1) m times:

$$\varphi(v_{\sigma(1)}, v_{\sigma(2)}, \ldots, v_{\sigma(n)}) = \epsilon(\tau_m) \cdots \epsilon(\tau_1)\varphi(v_1, v_2, \ldots, v_n).$$

But ϵ is a homomorphism into the abelian group ± 1. Hence, we get $\epsilon(\tau_1) \cdots \epsilon(\tau_m) = \epsilon(\tau_1 \cdots \tau_m) = \epsilon(\sigma)$.

Properties of Alternating Multilinear Functions (Cont'd)

(3) Choose σ fixing i and moving j to $i+1$.

Then, $(v_{\sigma(1)}, v_{\sigma(2)}, \ldots, v_{\sigma(n)})$ has two equal adjacent components.

So φ is zero on this n-tuple.

By (2), we get

$$\varphi(v_1, v_2, \ldots, v_n) = \pm \varphi(v_{\sigma(1)}, v_{\sigma(2)}, \ldots, v_{\sigma(n)}) = 0.$$

(4) On expanding by linearity in the i-th position and, then, applying (3), we get

$$\begin{aligned} &\varphi(v_1, \ldots, v_i + \alpha v_j, \ldots, v_j, \ldots, v_n) \\ &\quad = \varphi(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_n) \\ &\qquad + \alpha \varphi(v_1, \ldots, v_j, \ldots, v_j, \ldots, v_n) \\ &\quad = \varphi(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_n). \end{aligned}$$

Alternating Multilinear Function in Determinant Form

Proposition

Assume φ is an n-multilinear alternating function on V and that for some $v_1, v_2, \ldots, v_n$ and $w_1, w_2, \ldots, w_n \in V$ and some $\alpha_{ij} \in R$, we have

$$\begin{array}{rcl} w_1 & = & \alpha_{11} v_1 + \alpha_{21} v_2 + \cdots + \alpha_{n1} v_n \\ w_2 & = & \alpha_{12} v_1 + \alpha_{22} v_2 + \cdots + \alpha_{n2} v_n \\ & \vdots & \\ w_n & = & \alpha_{1n} v_1 + \alpha_{2n} v_2 + \cdots + \alpha_{nn} v_n \end{array}$$

Then

$$\varphi(w_1, w_2, \ldots, w_n) = \sum_{\sigma \in S_n} \epsilon(\sigma) \alpha_{\sigma(1)1} \alpha_{\sigma(2)2} \cdots \alpha_{\sigma(n)n} \varphi(v_1, v_2, \ldots, v_n).$$

Proof of the Determinant Form

- If we expand $\varphi(w_1, w_2, \ldots, w_n)$ by multilinearity, we obtain a sum of n^n terms of the form $\alpha_{i_1,1}\alpha_{i_2,2}\cdots\alpha_{i_n,n}\varphi(v_{i_1}, v_{i_2}, \ldots, v_{i_n})$, where the indices $i_1, i_2, \ldots, i_n$ each run over $1, 2, \ldots, n$. By the proposition, φ is zero on the terms where two or more of the i_j's are equal. Thus, in this expansion we need only consider the terms where $i_1, \ldots, i_n$ are distinct. Such sequences are in bijective correspondence with permutations in S_n. So each nonzero term may be written as

$$\alpha_{\sigma(1)1}\alpha_{\sigma(2)2}\cdots\alpha_{\sigma(n)n}\varphi(v_{\sigma(1)}, v_{\sigma(2)}, \ldots, v_{\sigma(n)}),$$

for some $\sigma \in S_n$. Applying (2) of the proposition to each of these terms in the expansion of $\varphi(w_1, w_2, \ldots, w_n)$ gives the expression in the proposition.

The Determinant Function

Definition (The Determinant Function)

An $n \times n$ **determinant function** on R is any function $\det : M_{n \times n}(R) \to R$ that satisfies the following two axioms:

(1) det is an n-multilinear alternating form on R^n $(= V)$, where the n-tuples are the n columns of the matrices in $M_{n \times n}(R)$;

(2) $\det(I) = 1$, where I is the $n \times n$ identity matrix.

- On occasion we shall write $\det(A_1, A_2, \ldots, A_n)$ for $\det A$, where $A_1, A_2, \ldots, A_n$ are the columns of A.

Existence of a Determinant Function

Theorem

There is a unique $n \times n$ determinant function on R and it can be computed for any $n \times n$ matrix (α_{ij}) by the formula:

$$\det(\alpha_{ij}) = \sum_{\sigma \in S_n} \epsilon(\sigma)\alpha_{\sigma(1)1}\alpha_{\sigma(2)2}\cdots\alpha_{\sigma(n)n}.$$

- Let $A_1, A_2, \ldots, A_n$ be the column vectors in a general $n \times n$ matrix (α_{ij}). We check that the formula given in the statement of the theorem satisfies the axioms of a determinant:

$$\begin{aligned}
&\det(A_1 \cdots A_i + \gamma B_i \cdots A_n) \\
&= \textstyle\sum_{\sigma \in S_n} \epsilon(\sigma)\alpha_{\sigma(1)1} \cdots (\alpha_{\sigma(i)i} + \gamma\beta_{\sigma(i)i}) \cdots \alpha_{\sigma(n)n} \\
&= \textstyle\sum_{\sigma \in S_n} \epsilon(\sigma)\alpha_{\sigma(1)1} \cdots \alpha_{\sigma(i)i} \cdots \alpha_{\sigma(n)n} \\
&\quad + \gamma \textstyle\sum_{\sigma \in S_n} \epsilon(\sigma)\alpha_{\sigma(1)1} \cdots \beta_{\sigma(i)i} \cdots \alpha_{\sigma(n)n} \\
&= \det(A_1 \cdots A_i \cdots A_n) + \gamma\det(A_1 \cdots B_i \cdots A_n);
\end{aligned}$$

Existence of a Determinant Function (Cont'd)

- Suppose that the kth and $(k+1)$-st columns of A are equal. Note that for $\tau = (k\ \ k+1)\sigma$,

$$\begin{aligned} &\epsilon(\tau)\alpha_{\tau(1)1}\cdots\alpha_{\tau(k)k}\alpha_{\tau(k+1)k+1}\cdots\alpha_{\tau(n)n} \\ &= -\epsilon(\sigma)\alpha_{\sigma(1)1}\cdots\alpha_{\sigma(k+1)k}\alpha_{\sigma(k)k+1}\cdots\alpha_{\sigma(n)n} \\ &= -\epsilon(\sigma)\alpha_{\sigma(1)1}\cdots\alpha_{\sigma(k)k}\alpha_{\sigma(k+1)k+1}\cdots\alpha_{\sigma(n)n}. \end{aligned}$$

As σ runs over S_n, $(k\ \ k+1)\sigma$ also runs over S_n. So, we get that

$$\begin{aligned} &2\textstyle\sum_{\sigma\in S_n}\epsilon(\sigma)\alpha_{\sigma(1)1}\cdots\alpha_{\sigma(n)n} \\ &= \displaystyle\sum_{\sigma\in S_n}\epsilon(\sigma)\alpha_{\sigma(1)1}\cdots\alpha_{\sigma(n)n} + \sum_{\substack{\sigma\in S_n \\ \tau:=(k\ \ k+1)\sigma}}\epsilon(\tau)\alpha_{\tau(1)1}\cdots\alpha_{\tau(n)n} \\ &= 0. \end{aligned}$$

Hence $\det(A) = 0$.

$\det(I) = \sum_{\sigma\in S_n}\epsilon(\sigma)i_{\sigma(1)1}\cdots i_{\sigma(n)n} = +1\cdot 1\cdots 1 + \sum_{\substack{\sigma\in S_n \\ \sigma\neq id}} 0 = 1.$

Hence a determinant function exists.

Uniqueness of the Determinant Function

- To prove uniqueness let e_i be the column n-tuple with 1 in position i and zeros in all other positions. Then

$$\begin{array}{rcl} A_1 & = & \alpha_{11}e_1+\alpha_{21}e_2+\cdots+\alpha_{n1}e_n \\ A_2 & = & \alpha_{12}e_1+\alpha_{22}e_2+\cdots+\alpha_{n2}e_n \\ & \vdots & \\ A_n & = & \alpha_{1n}e_1+\alpha_{2n}e_2+\cdots+\alpha_{nn}e_n \end{array}$$

By the proposition,

$$\det A=\sum_{\sigma\in S_n}\epsilon(\sigma)\alpha_{\sigma(1)1}\alpha_{\sigma(2)2}\cdots\alpha_{\sigma(n)n}\det(e_1,\ldots,e_n).$$

By axiom (2) of a determinant function $\det(e_1,e_2,\ldots,e_n)=1$. Hence, the value of $\det A$ is as claimed.

Determinant of the Transpose Matrix

Corollary

The determinant is an n-multilinear function of the rows of $M_{n\times n}(R)$ and for any $n\times n$ matrix A, $\det A = \det(A^t)$, where A^t is the transpose of A.

- The first statement is an immediate consequence of the second. So we show that a matrix and its transpose have the same determinant.
  For $A = (\alpha_{ij})$ we have $\det A^t = \sum_{\sigma\in S_n}\epsilon(\sigma)\alpha_{1\sigma(1)}\alpha_{2\sigma(2)}\cdots\alpha_{n\sigma(n)}$. Each number from 1 to n appears exactly once among $\sigma(1),\ldots,\sigma(n)$. So we may rearrange the product $\alpha_{1\sigma(1)}\alpha_{2\sigma(2)}\cdots\alpha_{n\sigma(n)}$ as $\alpha_{\sigma^{-1}(1)1}\alpha_{\sigma^{-1}(2)2}\cdots\alpha_{\sigma^{-1}(n)n}$. Also, the homomorphism ϵ takes values in $\{\pm 1\}$. So $\epsilon(\sigma)=\epsilon(\sigma^{-1})$. Thus, the sum for $\det A^t$ may be rewritten as $\sum_{\sigma\in S_n}\epsilon(\sigma^{-1})\alpha_{\sigma^{-1}(1)1}\alpha_{\sigma^{-1}(2)2}\cdots\alpha_{\sigma^{-1}(n)n}$. The latter sum is over all permutations. So the index σ may be replaced by σ^{-1}. The resulting expression is the sum for $\det A$.

Cramer's Rule

Theorem (Cramer's Rule)

If $A_1, A_2, \ldots, A_n$ are the columns of an $n \times n$ matrix A and $B = \beta_1 A_1 + \beta_2 A_2 + \cdots + \beta_n A_n$, for some $\beta_1, \ldots, \beta_n \in R$, then

$$\beta_i \mathrm{det} A = \mathrm{det}(A_1, \ldots, A_{i-1}, B, A_{i+1}, \ldots, A_n).$$

- Start from the right side.

  Replace B by $\beta_1 A_1 + \beta_2 A_2 + \cdots + \beta_n A_n$.

  Expand using multilinearity.

  Use the fact that a determinant of a matrix with two identical columns is zero.

Determinant and Linear Independence

Corollary

If R is an integral domain, then $\det A = 0$, for $A \in M_n(R)$ if and only if the columns of A are R-linearly dependent as elements of the free R-module of rank n.
Also, $\det A = 0$ if and only if the rows of A are R-linearly dependent.

- Since $\det A = \det A^t$, the first sentence implies the second.

  Assume, first, that the columns of A are linearly dependent and $0 = \beta_1 A_1 + \beta_2 A_2 + \cdots + \beta_n A_n$ is a dependence relation on the columns of A with, say, $\beta_i \neq 0$. By Cramer's Rule,

$$\begin{aligned} \beta_i \det A &= \det(A_1, \ldots, A_{i-1}, B, A_{i+1}, \ldots, A_n) \\ &= \det(A_1, \ldots, A_{i-1}, 0, A_{i+1}, \ldots, A_n) \\ &= 0. \end{aligned}$$

But R is an integral domain and $\beta_i \neq 0$. Hence, $\det A = 0$.

Determinant and Linear Independence (Converse)

- Conversely, assume the columns of A are independent. Consider the integral domain R as embedded in its quotient field F. Then $M_{n\times n}(R)$ may be considered as a subring of $M_{n\times n}(F)$. Note that the determinant function on the subring is the restriction of the determinant function from $M_{n\times n}(F)$. The columns of A in this way become elements of F^n. Any nonzero F-linear combination of the columns of A which is zero in F^n gives, by multiplying the coefficients by a common denominator, a nonzero R-linear dependence relation. The columns of A must therefore be independent vectors in F^n. Since A has n columns, these form a basis of F^n. Thus, there are elements β_{ij} of F, such that for each i, the i-th basis vector e_i in F^n may be expressed as $e_i = \beta_{1i}A_1 + \beta_{2i}A_2 + \cdots + \beta_{ni}A_n$. The $n \times n$ identity matrix is the one whose columns are $e_1, e_2, \ldots, e_n$. The determinant of the identity matrix is some F-multiple of $\det A$. But the determinant of the identity matrix is 1. Hence, $\det A \neq 0$.

Multiplicativity of the Determinant

Theorem

For matrices $A, B \in M_{n\times n}(R)$, $\det AB = (\det A)(\det B)$.

- Let $B = (\beta_{ij})$ and let $A_1, A_2, \ldots, A_n$ be the columns of A.
  $C = AB$ is the $n \times n$ matrix whose j-th column is
  $$C_j = \beta_{1j}A_1 + \beta_{2j}A_2 + \cdots + \beta_{nj}A_n.$$
  By the determinant formula, we obtain
  $$\begin{aligned}\det C &= \det(C_1, \ldots, C_n)\\ &= [\textstyle\sum_{\sigma \in S_n} \epsilon(\sigma)\beta_{\sigma(1)1}\beta_{\sigma(2)2}\cdots\beta_{\sigma(n)n}]\det(A_1, \ldots, A_n).\end{aligned}$$
  The sum inside the brackets is the formula for $\det B$.
  Hence, $\det C = (\det B)(\det A)$.

Cofactors and Cofactor Expansion Formula

Definition (Cofactor)

Let $A = (\alpha_{ij})$ be an $n \times n$ matrix. For each i, j, let A_{ij} be the $(n-1) \times (n-1)$ matrix obtained from A by deleting its i-th row and j-th column (an $(n-1) \times (n-1)$ **minor** of A). Then $(-1)^{i+j}\text{det}(A_{ij})$ is the ij **cofactor of** A.

Theorem (The Cofactor Expansion Formula Along the i-th Row)

If $A = (\alpha_{ij})$ is an $n \times n$ matrix, then for each fixed $i \in \{1, 2, \ldots, n\}$, the determinant of A can be computed from the formula

$$\text{det}A = (-1)^{i+1}\alpha_{i1}\text{det}A_{i1} + (-1)^{i+2}\alpha_{i2}\text{det}A_{i2} + \cdots + (-1)^{i+n}\alpha_{in}\text{det}A_{in}.$$

- For each A let $D(A)$ be the element of R obtained from the cofactor expansion formula. We prove that D satisfies the axioms of a determinant function. Hence it must be the determinant function. Proceed by induction on n.

The Cofactor Expansion Formula (Multilinearity)

- For $n = 1$, let (α) be a 1×1 matrix.

  Then $D((\alpha)) = \alpha$ and the result holds.
- Assume now that $n \geq 2$. We want to show that D is an alternating multilinear function of the columns. Fix an index k and consider the k-th column as varying and all other columns as fixed.
  - If $j \neq k$, α_{ij} does not depend on k. So $D(A_{ij})$ is linear in the k-th column by induction.
  - As the k-th column varies linearly, so does α_{ik}, whereas $D(A_{ik})$ remains unchanged (the k-th column has been deleted from A_{ik}).

  Thus, each term in the formula for D varies linearly in the k-th column. This proves D is multilinear in the columns.

The Cofactor Expansion Formula (Alternation)

- To prove D is alternating, assume columns k and $k+1$ of A are equal. If $j \neq k$ or $k+1$, the two equal columns of A become two equal columns in the matrix A_{ij}. By induction $D(A_{ij}) = 0$. The formula for D, therefore, has at most two nonzero terms: When $j = k$ and when $j = k+1$.
  - The minor matrices A_{ik} and A_{ik+1} are identical and $\alpha_{ik} = \alpha_{ik+1}$;
  - Thus, the two remaining terms in the expansion for D,

$$(-1)^{i+k}\alpha_{ik}D(A_{ik}) \quad \text{and} \quad (-1)^{i+k+1}\alpha_{ik+1}D(A_{ik+1}),$$

    are equal and appear with opposite signs;
  - Hence they cancel.

Thus, $D(A) = 0$ if A has two adjacent columns which are equal, i.e., D is alternating.

Finally, it follows easily from the formula and induction that $D(I) = 1$, where I is the identity matrix.

This completes the induction.

Cofactor Formula for the Inverse of a Matrix

Theorem (Cofactor Formula for the Inverse of a Matrix)

Let $A = (\alpha_{ij})$ be an $n \times n$ matrix and let B be the transpose of its matrix of cofactors, i.e., $B = (\beta_{ij})$, where $\beta_{ij} = (-1)^{i+i}\text{det}A_{ji}$, $1 \le i, j \le n$. Then $AB = BA = (\text{det}A)I$. Moreover, $\text{det}A$ is a unit in R if and only if A is a unit in $M_{n\times n}(R)$. In this case the matrix $\frac{1}{\text{det}A}B$ is the inverse of A.

- The i, j entry of AB is $\alpha_{i1}\beta_{1j} + \alpha_{i2}\beta_{2j} + \cdots + \alpha_{in}\beta_{nj}$. This equals $\alpha_{i1}(-1)^{j+1}D(A_{j1}) + \alpha_{i2}(-1)^{j+2}D(A_{j2}) + \cdots + \alpha_{in}(-1)^{j+n}D(A_{jn})$.
  - If $i = j$, this is the cofactor expansion for $\text{det}A$ along the i-th row. The diagonal entries of AB are thus all equal to $\text{det}A$.
  - If $i \neq j$, let $\overline{A}$ be the matrix A with the j-th row replaced by the i-th row, so $\text{det}A = 0$. By inspection $\overline{A}_{jk} = A_{jk}$ and $\alpha_{ik} = \overline{\alpha}_{jk}$, for every $k \in \{1, 2, \ldots, n\}$. By making these substitutions in the equation above, for each $k = 1, 2, \ldots, n$, one sees that the i, j entry in AB equals $\overline{\alpha}_{j1}(-1)^{1+j}D(\overline{A}_{j1}) + \cdots + \overline{\alpha}_{jn}(-1)^{n+j}D(\overline{A}_{jn})$. This expression is the cofactor expansion for $\text{det}\overline{A}$ along the j-th row. But $\text{det}\overline{A} = 0$. Hence, all off diagonal terms of AB are zero. So $AB = (\text{det}A)I$.

Cofactor Formula for the Inverse of a Matrix (Cont'd)

- It follows directly from the definition of B that the pair (A^t, B^t) satisfies the same hypotheses as the pair (A, B). By what has already been shown it follows that $(BA)^t = A^t B^t = (\det A^t)I$. Since $\det A^t = \det A$ and the transpose of a diagonal matrix is itself, we obtain $BA = (\det A)I$ as well.
- If $d = \det A$ is a unit in R, then $d^{-1}B$ is a matrix with entries in R whose product with A (on either side) is the identity, i.e., A is a unit in $M_{n\times n}(R)$.

  Conversely, assume that A is a unit in R, with (2-sided) inverse matrix C. But $\det C \in R$ and, moreover,

  $$1 = \det I = \det AC = (\det A)(\det C) = (\det C)(\det A).$$

  It follows that $\det A$ has a 2-sided inverse in R.