Linear Algebra 4th Edition

2. Linear Transformations and Matrices

Linear Transformation

Definition

Let V and W be vector spaces (over F). We call a function $T:V\rightarrow W$ a linear transformation from V to W if for all $x, y\in V$ and $c\in F$, we have:
$$\begin{cases} 1.\, T(x+y)=T(x)+T(y)\\ 2.\,T(cx)=cT(x) \end{cases}$$

Notes

- If F is the field of rational numbers, then 1. implies 2.
- However, generally they are logically independent.

Properties

- $T(0) = 0$
- $T(cx+y)=cT(x)+T(y)$
- $T(x-y)=T(x)-T(y)$
- $T(\sum\limits_{i=1}^n a_ix_i)=\sum\limits_{i=1}^na_iT(x_i)$

Examples

- $T:R^2\rightarrow R^2 \text{ by } T(a_1,a_2)=(2a_1+a_2, a_1)$
- $T_\theta:R^2\rightarrow R^2 \text{ by } T_\theta(a_1,a_2)=(rcos(\alpha+\theta), rsin(\alpha+\theta))$ – Rotation
- $T:R^2\rightarrow R^2 \text{ by } T(a_1,a_2)=(a_1, -a_2)$ – Reflection
- $T:R^2\rightarrow R^2 \text{ by } T(a_1,a_2)=(a_1, 0)$ – Projection
- $T:M_{m\times n}(F)\rightarrow M_{n\times m}(F) \text{ by } T(A)=A^t$ – Transpose
- $T:P_n(R)\rightarrow P_{n-1}(R) \text{ by } T(f(x))=f^\prime(x)$ – Differentiation
- $T:C(R)\rightarrow R \text{ by }T(f)=\int_a^bf(t)dt$ – Integration
- $I:V\rightarrow V \text{ by }I(x)=x$ – Identity
- $T_0:V\rightarrow W \text{ by } T_0(x)=0$ – Zero

Nullspace (Kernel)

Definition

Let V and W be vector spaces. Let $T:V\rightarrow W$ be linear. We define the nullspace (or kernel) $N(T)$ of T to be the set of all vectors $x\in V$ such that $T(x)=0$; that is:
$$N(T)=\{x\in V:T(x)=0\}$$

Examples

- $N(I) = \{0\}$
- $N(T_0)=V$

Range (Image)

Definition

Define $R(T)$ of T to be the subset of W consisting of all images (under T) of vectors in V; that is:
$$R(T) ={T(x):x\in V}$$

Examples

- $R(I) = V$
- $R(T_0)=\{0\}$

Theorem 2.1

Let V and W be vector spaces and $T:V\rightarrow W$ be linear. Then N(T) and R(T) are subspaces of V and W, respectively.

Theorem 2.2

Let V and W be vector spaces, and let $T:V\rightarrow W$ be linear. If $\beta = \{v_1, v_2, \dots, v_n\}$ is a basis for V, then:
$$R(T)=span(T(\beta))=span(\{T(v_1),T(v_2),\dots,T(v_n)\})$$

Note

- True if β is infinite.

Important Concepts

Nullity

Definition: If $N(T)$ is finite-dimensional, then we define the nullity of T to be the dimension of $N(T)$.

Rank

Definition: If $R(T)$ is finite-dimensional, then we define the rank of T to be the dimension of $R(T)$.

Theorem 2.3 (Dimension Theorem)

If V is finite-dimensional, then:
$$nullity(T)+rank(T)=dim(V)$$

Theorem 2.4

T is one to one if and only if $N(T)=\{0\}$

Theorem 2.5

Let V and W be vector spaces of equal finite dimension, and let $T:V\rightarrow W$ be linear. Then the following are equivalent:

- (a) T is one-to-one
- (b) T is onto
- (c) $rank(T)=dim(V)$

Important Property

If T is linear and one-to-one, then a subset S is linearly independent if and only if T(S) is linearly independent.

Theorem 2.6

Suppose that $\{v_1,v_2,\dots,v_n\}$ is a basis for V. For $w_1,w_2, \dots, w_n$ in W, there exists exactly one linear transformation $T:V\rightarrow W$ such that $T(v_i)=w_i$ for $i=1,2,\dots,n$.

Corollary

Let V and W be vector spaces, and suppose that V has a finite basis $\{v_1,v_2,\dots,v_n\}$. If $U, T:V\rightarrow W$ are linear and $U(v_i)=T(v_i)$ for $i=1,2,\dots,n$, then $U=T$.

The Matrix Representation of a Linear Transformation

Ordered Basis

Definition

Let V be a finite-dimensional vector space. An ordered basis for V is a basis for V endowed with a specific order; that is, an ordered basis for V is a finite sequence of linearly independent vectors in V that generates V.

Example

- In F^n, the standard ordered basis is $\{e_1, e_2, \dots, e_n\}$

- In $P_n(F)$, the standard ordered basis is $\{1,x,\dots,x^n\}$

Coordinate Vectors

Definition

Let β be an unordered basis for a finite-dimensional vector space V. For $x\in V$, let $a_1,a_2,\dots, a_n$ be the unique scalars such that:

$$x=\sum\limits_{i=1}^na_iu_i$$

We define the coordinate vector of x relative to β, denoted by $[x]_\beta$, by:

$$[x]_\beta=\begin{pmatrix}a_1\\a_2\\\vdots\\a_n\end{pmatrix}$$

Using the notation above, we call the $m\times n$ matrix A defined by $A_{ij}=a_{ij}$ the matrix representation of T in the ordered bases β and γ and write $A=[T]_{\beta}^{\gamma}$

Important Note

Both sums and scalar multiples of linear transformation are also linear.

Theorem 2.7

Let V and W be vector spaces over a field F, and let $T, U:V\rightarrow W$ be linear.

- (a) For all $a\in F$, $aT+U$ is linear
- (b) Using operations of addition and scalar multiplication in the preceding definition, the collection of all linear transformations from V to W is a vector space over F

Definition

Let V and W be vector spaces over F. We denote the vector space of all linear transformations from V into W by $\mathcal{L}(V, W)$. In the case that V = W, we write $\mathcal{L}(V)$ instead of $\mathcal{L}(V,W)$.

Theorem 2.8

Let V and W be finite-dimensional vector spaces with ordered bases β and γ, respectively, and let $T, U:V\rightarrow W$ be linear transformations. Then it satisfies the properties of linear transformations.

Composition of Linear Transformations and Matrix Multiplication

Theorem 2.9

Let V, W, and Z be vector spaces over the same field F, and let $T:V\rightarrow W$ and $U:W\rightarrow Z$ be linear. Then $UT:V\rightarrow Z$ is linear.

Theorem 2.10

Let V be a vector space. Let T, U_1, $U_2 \in \mathcal{L}(V)$. Then:

- (a) $T(U_1+U_2)=TU_1+TU_2$ and $(U_1+U_2)T=U_1T+U_2T$
- (b) $TU_1U_2=(TU_1)U_2$
- (c) $TI=IT=T$
- (d) $a(U_1U_2)=(aU_1)U_2=U_1a(U_2)$ for all scalars a

Matrix Multiplication Definition

Let A be a $m\times n$ matrix and B be an $n\times p$ matrix. We define the product of A and B, denoted AB, to be the $m\times p$ matrix such that:
$$(AB)_{ij} = \sum\limits_{k=1}^nA_{ik}B_{kj} \text{ for } 1\leq k\leq m, 1\leq j\leq p$$

Theorem 2.11

Let V, W, and Z be finite-dimensional vector spaces with ordered bases α, β and γ, respectively. Let $T:V\rightarrow W$ and $U:W\rightarrow Z$ be linear transformations. Then:
$$[UT]_{\alpha}^{\gamma}=[U]_{\beta}^{\gamma}[T]_{\alpha}^{\beta}$$

Corollary 1

Let V be a finite-dimensional vector space with an ordered basis β. Let $T, U\in \mathcal{L}(V)$. Then:
$$[UT]_\beta=[U]_\beta[T]_\beta$$

Corollary 2

Let A be an $n\times n$ matrix. Then A is invertible iff L_A is invertible. Furthermore:
$$(L_A)^{-1}=L_{A^{-1}}$$

Kronecker Delta

Definition

We define the Kronecker delta $\delta_{ij} = 1$ if $i=j$ and $\delta_{ij} = 0$ if $i\neq j$. The $n\times n$ identity matrix I_n is defined by $(I_n)_{ij}=\delta_{ij}$.

Theorem 2.12

Let A be an $m\times n$ matrix, B and C be $n\times p$ matrices, and D and E be $q\times m$ matrices. Then:

- (a) $A(B+C)=AB+AC$ and $(D+E)A=DA+EA$
- (b) $a(AB)=(aA)B=A(aB)$ for any scalar A

- (c) $I_mA=A=AI_n$
- (d) If V is an n-dimensional vector space with an ordered basis β, then $[I_v]_\beta=I_n$

Corollary

Let A be an $m\times n$ matrix, $B_1, B_2, \dots, B_k$ be $n\times p$ matrices, $C_1, C_2, \dots, C_k$ be $q\times m$ matrices, and $a_1, a_2, \dots, a_k$ be scalars. Then:
$$A(\sum\limits_{i=1}^k a_iB_i)=\sum\limits_{i=1}^ka_iAB_i$$
and
$$(\sum\limits_{i=1}^ka_iC_i)A=\sum\limits_{i=1}^ka_iC_iA$$

Theorem 2.13

Let A be an $m\times n$ matrix and B be an $n\times p$ matrix. For each j ($1\leq j\leq p$) let u_j and v_j denote the jth columns of AB and B, respectively. Then:

- (a) $u_j=Av_j$
- (b) $v_j=Be_j$, where e_j is the jth standard vector of F^p

Theorem 2.14

Let V and W be finite-dimensional vector spaces having ordered bases β and γ, respectively, and let $T:V\rightarrow W$ be linear. Then, for each $u\in V$, we have:
$$[T(u)]_\gamma=[T]_\beta^\gamma[u]_\beta$$

Theorem 2.15

Let A be an $m\times n$ matrix with entries from F. Then the multiplication transformation $L_A:F^n\rightarrow F^m$ is linear. Furthermore, if B is any other $m\times n$ matrix (with entries from F) and β and γ are the standard ordered bases for F^n and F^m, respectively, then we have the following properties:

- (a) $[L_A]_\beta^\gamma = A$
- (b) $L_A=L_B$ iff $A=B$
- (c) $L_{A+B}=L_A+L_B$ and $L_{aA}=aL_A \,\,\forall a\in F$
- (d) If $T:F^n\rightarrow F^m$ is linear, then there exists a unique matrix $m\times n$ matrix C such that $T=L_C$. In fact, $C=[T]_\beta^\gamma$
- (e) If E is an $n\times p$ matrix, then $L_{AE}=L_AL_E$
- (f) If $m=n$, then $L_{I_n}=I_{F^n}$

Theorem 2.16

Let A, B, and C be matrices such that A(BC) is defined. Then (AB)C is also defined and A(BC)=(AB)C; that is, matrix multiplication is associative.

Invertibility and Isomorphisms

Definition

Let V and W be vector spaces, and let $T:V\rightarrow W$ is said to be an inverse of T if $TU=I_W$ and $UT=I_V$. If T has an inverse, then T is said to be invertible. As noted in Appendix B, if T is invertible, then the inverse of T is unique and is denoted by T^{-1}.

Theorem 2.17

Let V and W be vector spaces, and let $T:V\rightarrow W$ be linear and invertible. Then $T^{-1}:W\rightarrow V$ is also linear.

Definition

Let A be an $n\times n$ matrix. Then A is invertible if there exists an $n\times n$ matrix B such that $AB=BA=I$.

Lemma

Let T be an invertible linear transformation from V to W. Then V is finite-dimensional iff W is finite-dimensional. In this case, $dim(V)=dim(W)$.

Theorem 2.18

Let V and W be finite-dimensional vector spaces with ordered bases β and γ, respectively. Let $T:V\rightarrow W$ be linear. Then T is invertible iff $[T]_\beta^\gamma$ is invertible. Furthermore, $[T^{-1}]_\gamma^\beta=([T]_\beta^\gamma)^{-1}$

Corollary 1

Let V be a finite-dimensional vector space with an ordered basis β, and let $T:V\rightarrow V$ be linear. Then T is invertible iff $[T]_\beta$ is invertible. Furthermore, $[T^{-1}]_\beta=([T]_\beta)^{-1}$

Corollary 2

Let A be an $n\times n$ matrix. Then A is invertible iff L_A is invertible. Furthermore, $(L_A)^{-1}=L_{A^{-1}}$

Definition

Let V and W be vector spaces. We say that V is isomorphic to W if there exists a linear transformation $T:V\rightarrow W$ that is invertible. Such a linear transformation is called the isomorphism from V onto W.

Lagrange Interpolation Formula

- $P(x)=\sum\limits_{i=0}^ny_i\cdot L_i(x)$
- $L_i(x)=\prod\limits_{\substack{j=0\\j\neq i}}^n\frac{x-x_j}{x_i-x_j}$

Theorem 2.19

Let V and W be finite-dimensional vector spaces (over the same field). Then V is isomorphic to W iff $dim(V)=dim(W)$.

Corollary

Let V be a vector space over F. Then V is isomorphic to F^n iff $dim(V)=n$.

Theorem 2.20

Let V and W be finite-dimensional vector spaces over F of dimensions n and m, respectively, and let β and γ be ordered bases for V and W, respectively. Then the function $\Phi : \mathcal{L}(V,W)\rightarrow M_{m\times n}(F)$, defined by $\Phi(T)=[T]_\beta^\gamma$ for $T\in \mathcal{L}(V,W)$, is isomorphism.

Corollary

Let V and W be finite-dimensional vector spaces of dimensions n and m, respectively. Then $\mathcal{L}(V,W)$ is finite-dimensional of dimension mn.

Definition

Let β be an ordered basis for an n-dimensional vector space V over the field F. The standard representation of V with respect to β is the function $\phi_B:V\rightarrow F^n$ defined by $\phi_B(x)=[x]_\beta$ for each $x\in V$.

Theorem 2.21

For any finite-dimensional vector space V with ordered basis β, ϕ_β is an isomorphism.

The Change of Coordinate Matrix

Theorem 2.22

Let β and $\beta^\prime$ be two ordered bases for a finite-dimensional vector space V, and let $Q=[I_v]^\beta_{\beta^\prime}$. Then:

- (a) Q is invertible
- (b) For any $v\in V$, $[v]_\beta=[I_V(v)]_\beta=[I_V]_{\beta^\prime}^\beta[v]_{\beta^\prime}=Q[v]_{\beta^\prime}$

Theorem 2.23

Let T be a linear operator on a finite-dimensional vector space V, and let β and $\beta^\prime$ be ordered bases for V. Suppose that Q is the change of coordinate matrix that changes $\beta^\prime\text{-coordinates}$ into $\beta\text{-cooridnate}$. Then:

$$[T]_{\beta^\prime}=Q^{-1}[T]_\beta Q$$

Corollary

Let $A\in M_{n\times n}(F),$ and let γ be an ordered basis for F^n. Then $[L_A]_\gamma=Q^{-1}AQ$, where Q is the $n\times n$ matrix whose jth column is the jth vector of γ.

Definition

Let A and B be matrices in $M_{n\times n}(F)$. We say that B is similar to A if there exists an invertible matrix Q such that $B=Q^{-1}AQ$.

Dual Spaces

Definition

For a vector space V over F, we define the dual space of V to be the vector space $\mathcal{L}(V, F)$, denoted by $V^\star$.

Theorem 2.24

Suppose that V is a finite-dimensional vector space with the ordered basis $\beta=\{x_1, x_2, \dots, x_n\}$. Let $f_i(1\leq i\leq n)$ be the ith coordinate function with respect to β as just defined, and let $\beta^\star=\{f_1, f_2,\dots,f_n\}$. Then $\beta^\star$ is an ordered basis for $V^\star$, and, for any $f\in V^\star$, we have:

$$f=\sum\limits_{i=1}^nf(x_i)f_i$$

Definition

We call the ordered basis $\beta^\star=\{f_1,f_2,\dots,f_n\}$ of $V^\star$ that satisfies $f_i(x_j)=\delta_{ij}(1\leq i, j\leq n)$ the dual basis of β.

Theorem 2.25

Let V and W be finite-dimensional vector spaces over F with ordered bases β and γ, respectively. For any linear transformation $T:V\rightarrow W$, the mapping $T^t:W^\star\rightarrow V^\star$ defined by $T^t(g)=gT$ for all $g\in W^\star$ is a linear transformation with the property that $[T^t]_{\gamma^\star}^{\beta^\star}=([T]_\beta^\gamma)^t$

Lemma

Let V be a finite-dimensional vector space, and let $x\in V$. If $\hat{x}(f)=0$ for all $f\in V^\star$, then $x=0$.

Theorem 2.26

Let V be a finite-dimensional space, and define $\psi:V\rightarrow V^{\star\star}$ by $\psi(x)=\hat{x}$. Then ψ is an isomorphism.

Corollary

Let V be an finite-dimensional vector space with dual space $V^{\star}$. Then every ordered basis for $V^\star$ is the dual basis for some basis for V.

Homogeneous Linear Differential Equations with Constant Coefficients

Definition

Given a function $x\in \mathcal{F}(\mathcal{R}, \mathcal{C})$ with real part x_1 and imaginary part x_2, we say that x is differentiable if x_1 and x_2 are differentiable. If x is differentiable, we define the derivative of x by $x^\prime = x_1^\prime + ix_2^\prime$.

Theorem 2.27

Any solution to a homogeneous linear differential equation with constant coefficients has derivatives of all orders; that is, if x is a solution to such an equation, then $x^{(k)}$ exists for every positive integer k.

Important Notes

- We use C^{∞} to denote the set of all functions in $\mathcal{F}(\mathcal{R}, \mathcal{C})$ that has derivatives of all orders.
- For any polynomial $p(t)$ over C of positive degree, p(D) is called a differential operator. The order of the differential operator p(D) is the degree of the polynomial p(t).
- Given the differential equations above, the complex polynomial $p(t)=t^n+a_{n-1}t^{n-1}+\dots+a_1t+a_0$ is called the auxiliary polynomial associated with equation.

Corollary

The set of all solutions to a homogeneous linear differential equation with constant coefficients is a subspace of C^{∞}.

Important Definitions

1. Let $c=a+ib$ be a complex number with real part a and imaginary part b. Define:
   $$e^c=e^a(cosb+isinb)$$
   The special case:
   $$e^{ib}=cosb+isinb$$
   is called Euler's formula.

2. A function $f:R\rightarrow C$ defined by $f(t)=e^{ct}$ for a fixed complex number c is called an exponential function.

Theorem 2.29

For any exponential function $f(t)=e^{ct}$, $f^\prime(t)=ce^{ct}$.

Theorem 2.30

The solution space for $y^\prime+y_0y=0$ is of dimension 1 and has $\{e^{-a_0t}\}$ as a basis.

Corollary

For any complex number c, the null space of the differential operator $D-cI$ has $\{e^{ct}\}$ as a basis.

Theorem 2.31

Let p(t) be the auxiliary polynomial for a homogeneous linear differential equation with constant coefficients. For any complex number c, if c is a zero of p(t), then e^{ct} is a solution to the differential equation.

Theorem 2.32

For any differential operator p(D) of order n, the null space of p(D) is an n-dimensional subspace of C^∞.

Lemma 1

The differential operator $D-cI:C^\infty\rightarrow C^\infty$ is onto for any complex number c.

Lemma 2

Let V be a vector space, and suppose T and U are linear operators on V such that U is onto and the null spaces of T and U are finite-dimensional. Then the null space of TU is finite-dimensional, and:
$$dim(N(TU))=dim(N(T))+dim(N(U))$$

Corollary

The solution space of any nth-order homogeneous linear differential equation with constant coefficients is an n-dimensional subspace of C^∞

Theorem 2.33

Given n distinct complex numbers $c_1, c_2, \dots, c_n$, the set of exponential functions $\{e^{c_1t}, e^{c_2t},\dots,e^{c_nt}\}$ is linearly independent.

Corollary

For any nth-order homogeneous linear differential equation with constant coefficients, if the auxiliary polynomial has n distinct zeros $c_1, c_2,\dots, c_n,$ then ${e^{c_1t}, e^{c_2t}, \dots, e^{c_nt}}$ is a basis for the solution space of the differential equation.

Lemma

For a given complex number c and positive integer n, suppose that $(t-c)^n$ is the auxiliary polynomial of a homogeneous linear differential equation with constant coefficients. Then the set:
$$\beta = \{e^{ct}, te^{ct}, \dots, t^{n-1}e^{ct}\}$$
is a basis for the solution space of the equation.

Theorem 2.34

Given a homogeneous linear differential equation with constant coefficients and auxiliary polynomial:
$$(t-c_1)^{n_1}(t-c_2)^{n_2}\cdots(t-c_k)^{n_k}$$
where $n_1, n_2, \dots, n_k$ are positive integers, and $c_1, c_2\dots, c_k$ are distinct complex numbers, the following set is a basis for the solution space of the equation:
$$\{e^{c_1t}, te^{c_1t},\dots, t^{n_1-1}e^{c_1t}, \dots, e^{c_kt},\dots,t^{n_k-1}e^{c_kt}\}$$

Appendix A: Sets

Key Concepts

- The elements of a set are listed is immaterial
- If $B\subseteq A$, and $B\neq A$, then B is called a proper subset of A
- $A=B$ iff $A\subseteq B$ and $B\subseteq A$

- A technique for proving $A=B$
- $\emptyset$ is a subset of every set
- A index set's elements have their own indices respectively
- A relation on A is a set of ordered pairs of elements of A such that $(x,y)\in S$ iff x stands in the given relationship to y

Equivalence Relation S on A

- For each $x\in A$, $x\sim x$ (reflexivity)
- If $x\sim y$, then $y\sim x$ (symmetry)
- If $x\sim y$ and $y\sim z$, then $x\sim z$ (transitivity)

Appendix B: Functions

Basic Concepts

- f(x) is called the image of x under f
  - If $S\subseteq A,$ we denote by $f(S)$ that $\{f(x):x\in S\}$ of all images of elements of S
- x is called a preimage of f(x) under f
  - If $T\subseteq B,$ we denote by $f^{-1}(T)$ that $\{x\in A:f(x)\in T\}$ of all preimages of elements in T
- If $f:A\rightarrow B$, then A is called the domain of f, and B is called the codomain of f
  - The set $\{f(x):x\in A\}$ is called the range of f
  - Range is a subset of codomain

Important Properties

- Each element of the range has a unique preimage are called one-to-one
- If codomain equals to the range, then the function is called onto
- Let $f:A\rightarrow B$ be a function and $S\subseteq A$. Then a function $f_S:S\rightarrow B$, called the restriction of f to S, can be defined by $f_S(x)=f(x)$ for each $x\in S$
- Functional composite is associative
- A function is invertible iff it's one-to-one and onto
  - $(f\circ g)(y)=y\,\forall y\in B, (g\circ f)(x)=x\,\forall x\in A$
  - If f is invertible, f^{-1} is invertible, and $(f^{-1})^{-1} = f$
  - If $f:A\rightarrow B$ and $g:B\rightarrow C$ are invertible, then $g\circ f$ is invertible and $(g\circ f)^{-1}=f^{-1}\circ g^{-1}$

Appendix C: Fields

Definition

A field F is a set on which two operations $+$ and $\cdot$(called addition and multiplication, respectively) are defined so that, for each pair of elements $x,y\in F$, there are unique elements $x+y$ and $x\cdot y$ in F for which the following conditions hold for all elements a, b, c in F:

- Commutativity of Addition and Multiplication
- Associativity of Addition and Multiplication
- Existence of Identity Elements
- Existence of Inverses
- Distributivity of multiplication over addition

Important Notes

- The set of integers is not a field
- The elements 0 and 1, and the inverses are unique
- The additive identity of a field has no multiplicative inverse
- The smallest positve integer p for which a sum of p 1's equals 0 is called the characteristic of F. If no such positive integer exists, then F is said to have characteristic zero

Appendix D: Complex Numbers

Definition

A complex number is an expression of the form $z=a+bi$, where a and b are numbers called the real part and the imaginary part of z, respectively.

Theorem D.1

The set of complex numbers with the operations of addition and multiplication previously defined is a field.

Important Definitions

- The complex conjugate of a complex number a+bi is the complex number a-bi. We denote the conjugate of the complex number by $\bar{z}$
- The absolute value(or modulus) of z is the real number $\sqrt{a^2+b^2}$. We denote the absolute value of z by $|z|$

Theorem D.3 (Part)

- $|z+w|\leq |z|+|w|$

- $|z|-|w|\leq |z+w|$

Corollary

- If $p(z)=a_nz^n+a_{n-1}z^{n-1}+\cdots+a_1z+a_0$ is a polynomial of degree $n\geq 1$ with complex coefficients, then there exist complex numbers $c_1, c_2,\cdots,c_n$(not necessarily distinct) such that:
  $$p(z)=a_n(z-c_1)(z-c_2)\cdots (z-c_n)$$
- $\mathbb{C}$ is Algebraically Closed

Appendix E: Polynomials

Definition

A polynomial of f(x) divides a polynomial g(x) if there exists a polynomial q(x) such that $g(x)=f(x)q(x)$

Theorem E.1 (The Division Algorithm for Polynomials)

- $f(x)=g(x)q(x)+r(x)$ is unique.
  - $deg(r(x)) < deg(g(x))$

Corollary 1

- Factor Theorem

Corollary 2

- Any polynomial of degree $n\geq 1$ has at most n distinct zeros.

Definition

Two nonzero polynomials are called relatively prime if no polynomial of positive degree divides each of them.

Theorem E.2

If $f_1(x)$ and $f_2(x)$ are relatively prime polynomials, there exist polynomials $q_1(x)$ and $q_2(x)$ such that:
$$q_1(x)f_1(x)+q_2(x)f_2(x)=1$$

Definitions

Let $f(x)=a_0+a_1(x)+\cdots+a_nx^n$ be a polynomial with coefficients from a field F. If T is a linear operator on a vector space V over F, we define:

- $f(T)=a_0I+a_1T+\cdots+a_nT^n$

- Similarly, if A is a n x n matrix with entries from F, we define $f(A)=a_0I+a_1A+\cdots+a_nA^n$

Theorem E.3

Let f(x) be a polynomial with coefficients from a field F, and let T be a linear operator on a vector space V over F. Then the following statements are true:

- f(T) is a linear operation on V
- If β is a finite ordered basis for V and $A=[T]_\beta$, then $[f(T)]_\beta=f(A)$.

Theorem E.4

Let T be a linear operator on a vector space V over a field F, and let A be a square matrix with entries from F. Then, for any polynomials $f_1(x)$ and $f_2(x)$ with coefficients from F:

- $f_1(T)f_2(T)=f_2(T)f_1(T)$
- $f_1(A)f_2(A)=f_2(A)f_1(A)$

Theorem E.5

Let T be a linear operator on a vector space V over a field F, and let A be a n x n matrix with entries from F. If $f_1(x)$ and $f_2(x)$ are relatively prime polynomials with entries from F, then there exist polynomials $q_1(x)$ and $q_2(x)$ with entries from F such that:

- $q_1(T)f_1(T)+q_2(T)f_2(T)=I$
- $q_1(A)f_1(A)+q_2(A)f_2(A)=I$

Definition

A polynomial f(x) with coefficients from a field F is called monic if its leading coefficient is 1. If f(x) has positive degree and cannot be expressed as a product of polynomials with coefficients from F each having positive degree, then f(x) is called irreducible.

Theorem E.6

Let $\phi(x)$ and f(x) be polynomials. If $\phi(x)$ is irreducible and $\phi(x)$ does not divide f(x), then $\phi(x)$ and f(x) are relatively prime.

Theorem E.7

Any two distinct irreducible monic polynomials are relatively prime.

Theorem E.8

Let f(x), g(x), and $\phi(x)$ be polynomials. If $\phi(x)$ is irreducible and divides the product $f(x)g(x)$, then $\phi(x)$ divides f(x) or $\phi(x)$ divides g(x).

Corollary

Let $\phi(x), \phi_1(x), \phi_2(x),\dots,\phi_n(x)$ be irreducible monic polynomials. If $\phi(x)$ divides the product $\phi_1(x)\phi_2(x)\cdots\phi_n(x)$, then $\phi(x)=\phi_i(x)$ for some i($i = 1,2,\cdots, n$).

Theorem E.9 (Unique Factorization Theorem for Polynomials)

For any polynomial $f(x)$ of positive degree, there exist a unique constant c; unique distinct irreducible monic polynomials $\phi_1(x), \phi_2(x), \dots,\phi_k(x)$; and unique positive integers $n_1, n_2,\dots, n_k$ such that:

$$f(x)=c[\phi_1(x)]^{n_1}[\phi_2(x)]^{n_2}\cdots [\phi_k(x)]^{n_k}$$

Theorem E.10

Let f(x) and g(x) be polynomials with coefficients from an infinite field F. If f(a)=g(a) for all $a\in F$, then $f(x)$ and g(x) are equal.