6.2. Wednesday for MAT3040

Reviewing: Root Theorem: $p(\lambda) = 0$ iff $(x - \lambda)$ divdes $p(x)$.

Corollary 6.1 A polynomial with degree n has at most n roots counting multiplicity.

For example, the polynomial $(x-3)^2$ has one root $x = 3$ with multiplicity 2. When counting multiplicity, we say the polynomial $(x-3)^2$ has two roots.

Definition 6.2 [Algebraically Closed] A field $\mathbb{F}$ is called **algebraically closed** if every non-constant polynomial $p(x) \in \mathbb{F}[x]$ has a root $\lambda \in \mathbb{F}$.

Theorem 6.3 — Fundamental Theroem of Algebra. The set of complex numbers $\mathbb{C}$ is algebraically closed.

Proof. One way is by complex analysis; Another way is by the topology on $\mathbb{C} \setminus \{0\}$. ∎

(R) By induction, we can show that every polynomial with degree n on algebraically closed field $\mathbb{F}$ has **exactly** n roots, counting multiplicity. Therefore, for any $p(x)$ on algebraically closed field $\mathbb{F}$,

$$p(x) = c(x - \lambda_1) \cdots (x - \lambda_n) \tag{6.2}$$

for $c, \lambda_1, \ldots, \lambda_n \in \mathbb{F}$.

The polynomials on general field $\mathbb{F}$ may not necessarily be factorized as in (6.2) , but still admit unique factorization property:

Theorem 6.4 — Unique Factorization. Every $f(x) = a_n x^n + \cdots + a_0$ in $\mathbb{F}[x]$ can be factorized as

$$f(x) = a_n [p_1(x)]^{e_1} \cdots [p_k(x)]^{e_k}$$

where p_i's are **monic, irreducible,distinct**. Furthermore, this expression is unique up to the permutation of factors.

Definition 6.3 [Factor] If $p(x) = q(x)s(x)$ with $p, q, s \in \mathbb{F}[x]$, then we say

- $p(x)$ is **divisible** by $s(x)$;
- $s(x)$ is a **factor** of $p(x)$;
- $s(x) | p(x)$
- $s(x)$ **divides** $p(x)$
- $p(x)$ is **multiple** of $s(x)$

Definition 6.4 [Common Factor]

1. The polynomial $g(x)$ is said to be a **common factor** of $f_1, \dots, f_k \in \mathbb{F}[x]$ if

$$g | f_i, i = 1, \dots, k$$

2. The polynomial $g(x)$ is said to be a **greatest common divisor** of $f_1, \dots, f_k$ if
   - g is **monic**.
   - g is common factor of $f_1, \dots, f_k$
   - g is of largest possible (maximal) degree.

R

- $\gcd(f_1, \dots, f_k) = \gcd(\gcd(f_1, f_2), f_3, \dots, f_k) = \gcd(\gcd(f_1, f_2, f_3), \dots, f_k)$
- $\gcd(f_1, \dots, f_k)$ is unique.
- If $\gcd(f_1, \dots, f_k) = 1$, we say $f_1, \dots, f_k$ is **relatively prime**
- Polynomials $f_1, \dots, f_k$ are relatively prime does not necessarily mean $\gcd(f_i, f_j) = 1$ for any $i \neq j$.

Counter-example: Let $a_1, \ldots, a_n$ distinct irreducible polynomials, and

$$f_i(x) = a_1(x) \cdots \hat{a}_i(x) \cdots a_n(x) := a_1 \cdots a_{i-1} a_{i+1} \cdots a_n,$$

then $\gcd(f_1, \ldots, f_n) = 1$, but $\gcd(f_i, f_j) = a_1 \cdots \hat{a}_i \cdots \hat{a}_j \cdots a_n$, which does not necessarily equal to 1.

■ **Example 6.3** The $\gcd(f_1, f_2)$ is easy to compute for factorized polynomials. For example, let $f_1(x) = (x^2 + x + 1)^3 (x-3)^2 x^4$ and $f_2(x) = (x^2+1)(x-3)^4 x^2$ in $\mathbb{R}[x]$, then

$$\gcd(f_1, f_2) = (x-3)^2 x^2$$

■

The question is how to find $\gcd(f_1, f_2)$ for given un-factorized polynomials?

Theorem 6.5 — **Rezout.** Let $g = \gcd(f_1, f_2)$, then there exists $r_1, r_2 \in \mathbb{F}[x]$ such that

$$g(x) = r_1(x) f_1(x) + r_2(x) f_2(x)$$

More generally, $g = \gcd(f_1, \ldots, f_k)$ implies there exists $r_1, \ldots, r_k$ such that

$$g = r_1 f_1 + \cdots + r_k f_k$$

The derivation of r_i's is by applying **Euclidean algorithm**. For example, given $x^3 + 6x + 7$ and $x^2 + 3x + 2$, we imply

$$x^3 + 6x + 7 - (x-3)(x^2 + 3x + 2) = 13x + 13$$

and

$$x^2 + 3x + 2 - \frac{x+2}{13}(13x + 13) = 0$$

Therefore, $\gcd(x^3 + 6x + 7, x^2 + 3x + 2) = \gcd(x^2 + 3x + 2, 13x + 13) = x + 2.$

6.2.1. Eigenvalues & Eigenvectors

Definition 6.5 [Eigenvalues] Let $T: V \to V$ be a linear operator.

1. We say $\boldsymbol{v} \in V \setminus \{\mathbf{0}\}$ is an eigenvector of T with eigenvalue λ if $T(\boldsymbol{v}) = \lambda \boldsymbol{v}$;
2. Or equivalently, $\boldsymbol{v} \in \ker(T - \lambda I)$, the λ-eigenspace of T. Here the mapping $I: V \to V$ denotes identity map, i.e., $I(\boldsymbol{v}) = \boldsymbol{v}, \forall \boldsymbol{v} \in V$.

Definition 6.6 A vector $\boldsymbol{v} \in V \setminus \{\mathbf{0}\}$ is a **generalized eigenvector** of T with **generalized eigenvalue** λ if $\boldsymbol{v} \in \ker((T - \lambda I)^k)$ for some $k \in \mathbb{N}^+$.

Note that an eigenvector is a generalized eigenvector of T; while the converse does not necessarily hold.

Example 6.4 Consider the linear transformation $A: \mathbb{R}^2 \to \mathbb{R}^2$ with

$$\begin{aligned} A: \quad & \mathbb{R}^2 \to \mathbb{R}^2 \\ \text{with} \quad & \boldsymbol{x} \to \boldsymbol{A}\boldsymbol{x} \\ \text{where} \quad & \boldsymbol{A} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

1. Note that $[1,0]^{\mathrm{T}}$ is an eigenvector with eigenvalue 1, since

$$A \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

2. However, $[0,1]^{\mathrm{T}}$ is not an eigenvector, since

$$A \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Note that

$$(A-I)^2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad (A-I)^3 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

and therefore

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} \in \ker(A-I)^2,$$

i.e., a generalized eigenvector with generalized eigenvalue 1.

■

■ **Example 6.5** Consider $V = \mathcal{C}^\infty(\mathbb{R})$, which is a set of all infinitely differentiable functions.

Define the linear operator $T : V \to V$ as $T(f) = f''$. Then the (-1)-eigenspace of T has $f \in V$ satisfying

$$f'' = -f$$

From ODE course, we imply $\{\sin x, \cos x\}$ forms a basis of (-1)-eigenspace. ■

Assumption. From now on, we assume V has finite dimension by default.

Definition 6.7 [Determinant] Let $T : V \to V$ be a linear operator. The **determinant** of T is given by

$$\det(T) = \det((T)_{\mathcal{A},\mathcal{A}})$$

where $\mathcal{A}$ is some basis of V. ■

R Assume we have complete knowledge about $\det(M)$ for matrices for now. The determinant is well-defined, i.e., independent of the choice of basis $\mathcal{A}$. For another basis $\mathcal{B}$, we imply

$$\det(T_{\mathcal{B},\mathcal{B}}) = \det(C_{\mathcal{B},\mathcal{A}} T_{\mathcal{A},\mathcal{A}} C_{\mathcal{A},\mathcal{B}}) = \det(C_{\mathcal{B},\mathcal{A}}) \det(T_{\mathcal{A},\mathcal{A}}) \det(C_{\mathcal{A},\mathcal{B}}) = \det(T_{\mathcal{A},\mathcal{A}})$$

Definition 6.8 [characteristic polynomial] The **characteristic polynomial** $\mathcal{X}_T(x)$ of $T: V \to V$ is defined as

$$\mathcal{X}_T(x) = \det((T)_{\mathcal{A},\mathcal{A}} - xI)$$

for any basis $\mathcal{A}$

In the next few lectures, we will study

- Cayley-Hamilton Theorem
- Jordan Canonical Form

These theorems can be stated using matrices, and they both hold up to change of basis. We have a unified statement of these theorem using vecotor space rather than $\mathbb{R}^n$.