POLYNOMIAL

Polynomial Rings:

Let $\mathbb{F}$ be a field. Then a polynomial over $\mathbb{F}$ with the variable x is a polynomial of the form,

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

where $a_0, a_1, a_2, \ldots, a_n \in \mathbb{F}$ and $n \geq 0$

The polynomial ring over the field $\mathbb{F}$ is defined as:

$$\mathbb{F}[x] = \left\{ a_0 + a_1 x + \cdots + a_n x^n \;\middle|\; \forall a_i \in \mathbb{F},\ n \geq 0 \right\}.$$

with the 2 operations of the ring: $+$ and $\cdot$

$(\mathbb{F}[x], +, \cdot)$ is a commutative ring with identity.

(i) We have to define the operation $+_{\mathbb{F}[x]}$

$$f_1(x) := a_0 + a_1 x + \cdots + a_n x^n$$
$$f_2(x) := b_0 + b_1 x + \cdots + b_m x^m$$

Since $\forall a_i \in \mathbb{F}$ and $\forall b_i \in \mathbb{F}$ so in the polynomial expression the operation $+$ and $\cdot$ are as usual performed on the field $\mathbb{F}$. Naturally, $x \in \mathbb{F}$ for the operation to make sense.

$$f_1(x) +_{\mathbb{F}[x]} f_2(x) := (a_0 +_{\mathbb{F}} b_0) +_{\mathbb{F}} (a_1 +_{\mathbb{F}} b_1)x + \cdots + (a_K +_{\mathbb{F}} b_K)x^K$$

where $K = \max(m, n)$

When we use max then the other coefficients are padded with zeros.

(ii) Additive identity of $\mathbb{F}[x]$?

$$f(x) +_{\mathbb{F}[x]} 0_{\mathbb{F}[x]}(x) = f(x)$$

let, $0_{\mathbb{F}[x]}(x) := 0 + 0.x + 0.x^2 + \cdots \to 0.x^m$.

Then by the definition of $+_{\mathbb{F}[x]}$ note that,

$$f(x) +_{\mathbb{F}[x]} 0_{\mathbb{F}[x]}(x) = f(x).$$

Therefore the zero polynomial is the polynomial that has all the coefficients as $0_{\mathbb{F}}$.

(iii) Additive inverse of $\mathbb{F}[x]$?

$$f(x) +_{\mathbb{F}[x]} g(x) = 0_{\mathbb{F}[x]}(x)$$

let $f(x) := a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \quad \forall a_i \in \mathbb{F}$

$g(x) := -a_0 - a_1x - a_2x^2 - \cdots - a_nx^n \quad \forall -a_i \in \mathbb{F}$

Then we see that $g(x)$ is the additive inverse of $\mathbb{F}[x]$.

(iv) We have to define the multiplication operation $\cdot_{\mathbb{F}[x]}$.

$$f_1(x) := a_0 + a_1 x + \cdots + a_n x^n \qquad \forall a_i \in \mathbb{F}$$
$$f_2(x) := b_0 + b_1 x + \cdots + b_m x^m \qquad \forall b_i \in \mathbb{F}$$

$f_1(x) \cdot f_2(x)$: $\cdot_{\mathbb{F}[x]}$; $\cdot_{\mathbb{F}}$

$$:= (a_0 \cdot b_0) + (a_0 \cdot b_1)x^1 + (a_0 \cdot b_2)x^2 + \cdots + (a_0 b_m)x^m + (a_1 \cdot b_0)x + (a_1 \cdot b_1)x^2 + \cdots + (a_1 \cdot b_m)x^{m+1} + \cdots + (a_n b_0)x^n + (a_n \cdot b_1)x^{n+1} + \cdots + (a_n b_m)x^{n+m}.$$

$$= \sum_{k=0}^{m+n} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) x^k$$

(v) Multiplicative identity of $\mathbb{F}[x]$?

$$f(x) \cdot 1_{\mathbb{F}[x]}(x) = f(x)$$

let $f(x) := a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \qquad \forall a_i \in \mathbb{F}$

$$1_{\mathbb{F}[x]} := 1 + 0.x + 0.x^2 + \cdots + 0.x^n$$
$$= 1$$

$\mathbb{F}[x]$ is commutative ring with identity because it

satisfies all the axioms of commutative ring with identity but $\mathbb{F}[x]$ is not a field because the multiplication inverse doesn't exist.

So $\mathbb{F}[x]$ is the ring of polynomials over the field $\mathbb{F}$ where the ring is commutative with identity.

(vi) $\mathbb{F}[x]$ has no multiplicative inverse for some of the polynomials $f(x) \in \mathbb{F}[x]$. Hence it can't be a field.

Let $f(x) = x$ where $x \neq 0_{\mathbb{F}}$.

Now $f(x) \cdot g(x) = 1_{\mathbb{F}[x]} = 1$

then $g(x)$ is called multiplicative inverse of $f(x)$.

For all x, the only way to get 1 is to select $g(x) = \frac{1}{x}$ which is definitely not a polynomial.

$g(x) = \frac{1}{x} = x^{-1}$ and in polynomial all the powers of x is ≥ 0.

polynomial must be in the form: $a_0 + a_1x + \dots + a_nx^n$ where $n \geq 0$. but we see that $n = -1$ in $g(x)$ so $g(x)$ is not polynomial hence mult. inverse doesn't exist.

Degree of a polynomial:

Let $\mathbb{F}$ be a field.
Let $\mathbb{F}[x]$ be a commutative ring with identity.

$f(x) = a_0 + a_1x + \cdots + a_nx^n$, $\forall a_i \in \mathbb{F}$ and $f(x) \in \mathbb{F}[x]$.

The degree of $f(x)$ is the largest $k \geq 0$ for which $a_k \neq 0$.
For this example, the $\deg(f) = n$.

The non-zero coefficient for largest k is called "leading coefficient".

By convention degree of $0_{\mathbb{F}[x]}(x)$ is assumed as $-\infty$.

① Let $f(x), g(x) \in \mathbb{F}[x]$.

$$\deg\left(f(x) \cdot g(x)\right) = \deg\left(f(x)\right) + \deg\left(g(x)\right)$$

$$f(x) \cdot g(x) = \sum_{i=1}^{m} \sum_{j=1}^{n} \left(a_i \cdot b_j\right) x^{i+j}$$

Note that the highest $k \geq 0$ for which $c_k \neq 0$ will be $k = m+n$. So $\deg\left(f(x) \cdot g(x)\right) = m+n$.

For any arbitrary ring S if $f(x), g(x) \in S[x]$ then $\deg(f \cdot g) \leq \deg(f) + \deg(g)$.

② let $f(x), g(x) \in \mathbb{F}[x]$

$$\deg\left(f(x)+g(x)\right) \leq \max\left(\deg(f(x)), \deg(g(x))\right)$$

$$f(x)+g(x) = \sum_{K=0}^{\max(m,n)} \left(a_K + b_K\right) x^K$$

Note that for $K = \max(m,n)$, the $a_K + b_K$ may vanish if we select $a_K = -b_K$ so the degree will always be less or equal to $\max(m,n)$.

Properties of polynomial rings:

① let $\mathbb{F}$ be a field.

let $f(x), g(x) \in \mathbb{F}[x]$ such that $f(x) \cdot g(x) = 0_{\mathbb{F}[x]}(x)$

Then either $f(x) = 0_{\mathbb{F}[x]}(x)$ or $g(x) = 0_{\mathbb{F}[x]}(x)$.

in other words $\mathbb{F}[x]$ is an integral domain.

⇒ If $f(x)$ is of deg at least 0 and $g(x)$ of deg at least 0 then,

$f(x) = a_0$; $a_0 \in \mathbb{F}$ and $a_0 \neq 0_{\mathbb{F}}$

$g(x) = b_0$; $b_0 \in \mathbb{F}$ and $b_0 \neq 0_{\mathbb{F}}$.

So $f(x) \cdot g(x) = a_0 \cdot b_0 \neq 0_{\mathbb{F}}$

Therefore, $f(x) \cdot g(x)$ can never be $0_{\mathbb{F}[x]}(x)$. That means no zero divisor will exist for polynomials of degree ≥ 0. Hence $\mathbb{F}[x]$ is integral domain.

If $f(x) \cdot g(x) = 0_{\mathbb{F}[x]}(x)$ then,

$$\deg\left(f(x) \cdot g(x)\right) = \deg\left(f(x)\right) + \deg\left(g(x)\right) = -\infty.$$

Now to satisfy the equation one of the deg must be $-\infty$.
hence either $f(x) = 0_{\mathbb{F}[x]}(x)$ or $g(x) = 0_{\mathbb{F}[x]}(x)$.

(2) A polynomial of the polynomial ring $\mathbb{F}[x]$ over a field $\mathbb{F}$ has a multiplicative inverse (unit element) if and only if it has degree 0.

$\Rightarrow$ Suppose, $f(x) = a_0$; $a_0 \in \mathbb{F}$ and $a_0 \neq 0_{\mathbb{F}}$.

$$f(x) \cdot g(x) = 1_{\mathbb{F}[x]} = 1 \quad \text{where } g(x) = f(x)^{-1}$$

$$\Rightarrow a_0 \cdot a_0^{-1} = 1$$

Hence if $g(x) = a_0^{-1}$ then the multiplicative inverse exists.

Now consider $f(x) \cdot g(x) = 1_{\mathbb{F}[x]} = 1$.

$$\deg\left(f(x) \cdot g(x)\right) = \deg\left(f(x)\right) + \deg\left(g(x)\right) = \deg\left(1_{\mathbb{F}[x]}\right) = 0$$

Therefore unless $\deg(f(x)) = 0$ and $\deg(g(x)) = 0$ we can never satisfy the equation because deg is always positive except for $0_{\mathbb{F}[x]}$. So if $f(x)$ has deg ≥ 1 then multiplicative inverse can't exist.

(3) Cancellation of polynomials

$f(x) \in \mathbb{F}[x]$ and $\deg(f(x)) \geq 0$

$f(x) \cdot g(x) = f(x) \cdot h(x)$ for $g(x), h(x) \in \mathbb{F}[x]$

then $g(x) = h(x)$.

$\Rightarrow f(x) \cdot g(x) = f(x) \cdot h(x)$

$\Rightarrow f(x) \cdot g(x) - f(x) \cdot h(x) = f(x) \cdot h(x) - f(x) \cdot h(x)$

$\Rightarrow f(x) \cdot g(x) - f(x) \cdot h(x) = 0_{\mathbb{F}[x]}(x)$

$\Rightarrow f(x)\left(g(x) - h(x)\right) = 0_{\mathbb{F}[x]}(x)$ (mult. is distributive)

So either $f(x) = 0_{\mathbb{F}[x]}(x)$ (Not the case)

$g(x) - h(x) = 0_{\mathbb{F}[x]}$

$\Rightarrow g(x) = h(x)$.

④ Monic polynomial.

Let F be a field.

$f(x) \in F[x]$.

The polynomial $f(x)$ is monic if the leading coefficient is equal to 1.

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} + x^n$$

↳ Monic polynomial.

↳ leading coeff = 1.

Ideals of a ring:

Let R be a commutative ring with identity.
Let I be a subset of R Then I is called "ideal" of ring R if it satisfies the following –

(i) "I" must be subring of "R" that means the addition and multiplication operation on the ring $(R, +, \cdot)$ must be closed in "I". "I" must also be closed under additive inverse and "I" must contain the identity 1_R.

(ii) "I" must be closed under left multiplication by all the elements of R. (Left ideal)

(iii) "I" must be closed under right multiplication by all the elements of R. (right ideal)

Suppose $\mathbb{F}[x]$ is the commutative ring with identity. An ideal I of $\mathbb{F}[x]$ will be a subset $I \subseteq \mathbb{F}[x]$ such that the followings are true -

(i) $g(x), f(x) \in I \longrightarrow (g+f)(x) \in I$

(ii) $f(x) \in \mathbb{F}[x]$, $g(x) \in I \longrightarrow (f \cdot g)(x) \in I$

Note that the 2 definitions are equivalent. Ideals are more than subring. Ideals are that subrings that are not only closed under itself but also closed under the ring R for multiplication operation.

let R be a commutative ring with identity.
Define a subset I of R as:

$$I := \left\{ \sum_{i=1}^{n} a_i r_i \;\middle|\; r_i \in R, \text{ fixed } a_i \in I \right\}$$

Is I an ideal of R?

⇒ Take any 2 elements from I say f and g

$$f = \sum_{i=1}^{n} a_i r_i$$

$$g = \sum_{i=1}^{n} a_i s_i$$

$$f+g = \sum_{i=1}^{n} a_i \underbrace{(r_i + s_i)}_{r_i' \in R} \quad (r_i \in R,\ s_i \in R)$$

Hence $f+g \in I$

Take any 1 element from I say f.
Take any 1 element from R say g.

$$f = \sum_{i=1}^{n} a_i r_i$$

$$f \cdot g = \left(\sum_{i=1}^{n} a_i r_i \right) \cdot g = \sum_{i=1}^{n} a_i \underbrace{(r_i \cdot g)}_{r_i' \in R} \quad (r_i \in R,\ g \in R)$$

Hence $f \cdot g \in I$

We call I is an ideal generated by $a_1, a_2, \ldots, a_n \in R$ and the set of generators $\{a_1, a_2, \ldots, a_n\}$ is called a generating set of I.

$I = \langle \{a_1, a_2, \ldots, a_n\} \rangle$. Note generating set need not be unique. Two different set of generators may result same ideal.

Suppose $\mathbb{F}[x]$ is the commutative ring with identity. The ideal generated by $\{f_1, f_2, \dots, f_n\}$ where $\forall f_i \in \mathbb{F}[x]$ is given as:

$$I = \langle \{f_1, f_2, \dots, f_n\} \rangle \subseteq \mathbb{F}[x]$$

$$= \left\{ \sum_{i=1}^{n} g_i(x) \cdot f_i(x). \;\middle|\; \forall f_i \text{ are fixed}, \; \forall g_i \in \mathbb{F}[x] \right\}$$

$g_i(x)$ can be thought of polynomial coefficient from $\mathbb{F}[x]$

Suppose the ideal generated by $\{f\}$ where $f \in \mathbb{F}[x]$ is a fixed polynomial given as:

$$I = \langle \{f\} \rangle \subseteq \mathbb{F}[x]$$

$$= \left\{ g(x) \cdot f(x) \;\middle|\; \text{fixed } f(x) \text{ and } g(x) \in \mathbb{F}[x] \right\}$$

This set I is called "principal ideal" and the polynomial 'f' is called a principal generator of I. If an ideal is generated by single element of the ring then it is called "principal ideal."

A ring in which each ideal of it is a principal ideal is called principal ideal domain. Basically, the ring has to be an integral domain in order to be principal ideal domain. A PID is an integral domain in which every ideal is a principal ideal.

$\mathbb{F}[x]$ is an integral domain. Moreover $\mathbb{F}[x]$ is a principal ideal domain. And for any ideal of $\mathbb{F}[x]$, there is a unique monic polynomial which generates the ideal.

Annihilating Ideals:

Suppose T is a linear operator on V. over $\mathbb{F}$.
Suppose, $p(x) \in \mathbb{F}[x]$.

Then $p(T)$ is a linear operator on V.
We know that,

$$(p+q)(T) = p(T) + q(T)$$
$$(pq)(T) = p(T) \cdot q(T)$$

The collection of polynomials 'p' which annihilate T in the sense that $p(T) = 0$ (zero operator) is an ideal of $\mathbb{F}[x]$.

$$\operatorname{ann}(T) := \{ p(x) \in \mathbb{F}[x] \mid p(T) = 0 \} \subseteq \mathbb{F}[x]$$

↳ This is called annihilator ideal of $\mathbb{F}[x]$ by T.

proof: $\operatorname{ann}(T)$ is an ideal of $\mathbb{F}[x]$.

consider $p(x), q(x) \in \operatorname{ann}(T)$.

$$p(x) + q(x) = (p+q)(x) = (p+q)(T) = p(T) + q(T)$$
$$= 0 + 0 = 0 .$$

$$p(x) \cdot q(x) = (pq)(x) = (pq)(T) = p(T) \cdot q(T) = 0 \cdot 0 = 0$$

So $\operatorname{ann}(T)$ is an ideal of $\mathbb{F}[x]$.

Minimal Polynomial:

Let T be a linear operator on V over $\mathbb{F}$. The minimal polynomial for T is the unique monic generator polynomial of the annihilator ideal of $\mathbb{F}[x]$ by T.

The generator polynomial of the annihilator ideal is characterized by being the monic polynomial of min degree in the ideal. The minimal polynomial $p(x)$ for the operator T is characterized by 3 properties—

(i) $P(x)$ is monic polynomial

(ii) $P(T) = 0$

(iii) No polynomial $\in \mathbb{F}[x]$ which annihilates T has smaller degree than $P(x)$ has.

proof: Let $n = \dim(V)$.

consider the vector space $L(V,V)$ and it has dimension n^2. So any n^2+1 vectors in $L(V,V)$ can't be linearly independent.

consider: $\{ I, T, T^2, T^3, \cdots, T^{n^2} \}$

This set is not LI because it has n^2+1 vectors.

Suppose m be the smallest positive integer for which the set is linearly dependent.

$$\{ I, T, T^2, T^3, \cdots, T^m \} \quad (1 \leq m \leq n^2+1)$$

The moment, this set is LD, we will stop it. But unless the set is LD, we will keep on adding the elements.

Since the above set is LD that means one of the operator in the list can be written as Linear combination of other operators.

Since we have selected m in such a way that, the moment we get LD, we stop it so it must be the case that the last member T^m can be written as LC of others.

$$T^m = a_0' \cdot I + a_1' \cdot T + a_2' T^2 + \cdots + a_{m-1}' \cdot T^{m-1}$$

$$\Rightarrow a_0 I + a_1 T + a_2 T^2 + \cdots + a_{m-1} T^{m-1} + T_m = 0$$

(coeffecients can be reorganized)

Define a monic polynomial $P(x) \in \mathbb{F}[x]$.

$$P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{m-1} x^{m-1} + x^m$$

Evaluate $P(T)$.

$$P(T) = a_0 + a_1 T + a_2 T^2 + \cdots + a_{m-1} T^{m-1} + T^m = 0$$

Since we see that $P(T) = 0$ that means $P(x)$ is a generator for the ideal $\{ P(x) \in \mathbb{F}[x] \mid P(T) = 0 \}$ Cannihilating ideal of $\mathbb{F}[x]$ by T).

Definitely, such a $P(x)$ will exist in the annihilating ideal of $\mathbb{F}[x]$. Denote $P(x) = \mu_T(x)$

Degree of $P(x) = m$ (smallest positive integer)

The choice of m implies, no other monic polynomial $q \in \mathbb{F}[x]$ with degree smaller than m can satisfy $q(T) = 0$. So in that sense $p(x)$ is minimal polynomial.

But now we will prove that $p(x)$ is unique.

Suppose $q(x)$ is a monic polynomial of deg m. such that $q(T) = 0$

$$\Rightarrow \quad p(T) = 0$$
$$q(T) = 0$$
$$\overline{(p-q)(T) = 0}$$
$$\Rightarrow (p-q)(x) = 0$$

So $(p-q)$ must have deg m and it must be monic.

$$p(x) = a_0 + a_1 x + \cdots + a_m x^m$$
$$q(x) = b_0 + b_1 x + \cdots + b_m x^m$$

$$(p-q)(x) = (a_0 - b_0) + (a_1 - b_1)x + \cdots + (a_m - b_m)x^m = 0_{\mathbb{F}[x]}$$

$$\Rightarrow \begin{aligned} a_0 &= b_0 \\ a_1 &= b_1 \\ &\vdots \\ a_m &= b_m \end{aligned}$$

Hence the minimal polynomial is unique monic polynomial.

The way minimal polynomial was introduced, it may seem that the degree of minimal polynomial can be at most n^2. But it can be shown later that the degree of minimal polynomial is at most n when $N = \mathbb{F}^n$.

Suppose $T \in L(V,V)$. and $q(x) \in \mathbb{F}[x]$.
$q(T) = 0$ if and only if $q(x) = p(x) \cdot s(x)$ where $p(x)$ is minimal polynomial and $s(x) \in \mathbb{F}[x]$.

proof: Suppose, $q(x) = p(x) \cdot s(x)$

We have, $q(T) = p(T) \cdot s(T) = 0 \cdot s(T) = 0$

Suppose $q(T) = 0$
We have Eucledian division algorithm for polynomials,

$$\underbrace{q(x)}_{\text{dividend}} = \underbrace{p(x)}_{\text{divisor}} \cdot \underbrace{s(x)}_{\text{quotient}} + \underbrace{r(x)}_{\text{remainder}} \quad \text{where } \deg(r) < \deg(p)$$

$$q(T) = p(T) \cdot s(T) + r(T) = 0$$

$$\Rightarrow r(T) = -p(T) \cdot s(T)$$

Since $p(x)$ is minimal polynomial so $p(T) = 0$

So $r(T) = 0$

$\Rightarrow$ $r(x)$ is a member of annihilating ideal.

If $\deg(r(x)) \geq 0$ then it is contradiction because $p(x)$ is minimal polynomial & $\deg(r) < \deg(p)$ so now $r(x)$ is minimal now but minimal polynomial is unique with smallest degree.

So $\deg(r(x)) < 0$ means $r(x) = 0_{\mathbb{F}[x]}(x)$ or zero polynomial.

So, $q(x) = p(x) \cdot b(x)$.

Algorithm to find minimal polynomial:

The annihilator ideal of $\mathbb{F}[x]$ w.r.t T is given as-

$$\text{ann}(T) = \{ p(x) \in \mathbb{F}[x] \mid p(T) = 0_{L(V,V)} \}$$

The annihilator ideal of $\mathbb{F}[x]$ w.r.t. T acting on v is -

$$\text{ann}_v(T) = \{ p(x) \in \mathbb{F}[x] \mid p(T)v = 0_V \}$$

We can prove that $\text{ann}_v(T)$ is an ideal of $\mathbb{F}[x]$.

Consider the vector space V with dimension n.

Look at the set $\{ Iv, Tv, T^2v, \cdots, T^nv \}$

Definitely, this set is not linearly independent.

Consider the least positive integer m for which the set becomes linearly dependent.

$\{ Iv, Tv, T^2v, \cdots, T^mv \}$. is Linearly dependent.

$$T^mv = a_0' Iv + a_1' Tv + a_2' T^2v + \cdots + a_{m-1}' T^{m-1}v$$

$$\Rightarrow a_0 Iv + a_1 Tv + a_2 T^2v + \cdots + T^mv = 0_V.$$

$$\Rightarrow \left(a_0 I + a_1 T + a_2 T^2 + \cdots + T^m \right) v = 0_V.$$

Define a monic polynomial $q(x) \in F[x]$ s.t.

$$q(x) = a_0 + a_1 x + a_2 x^2 + \cdots + x^m$$

Evaluate $q(T)$.

$$q(T) = a_0 I + a_1 T + a_2 T^2 + \cdots + T^m$$

So, $q(T)v = \left(a_0 I + \cdots + T^m \right) v = 0_V$.

Therefore, $q(x) \in \text{ann}_v(T)$. and it is having the least degree and it is unique. Denote $\mu_v(x) = q(x)$.

Consider the vector space $\mathbb{V}$ and look at the basis $\{v_1, v_2, \ldots, v_n\}$.

Construct $\text{ann}_{v_1}(T) := \{ P(x) \in \mathbb{F}[x] \mid P(T)v_1 = 0_{\mathbb{V}} \}$

construct $\text{ann}_{v_2}(T) := \{ P(x) \in \mathbb{F}[x] \mid P(T)v_2 = 0_{\mathbb{V}} \}$

$\vdots$

construct $\text{ann}_{v_n}(T) := \{ P(x) \in \mathbb{F}[x] \mid P(T)v_n = 0_{\mathbb{V}} \}$.

For each of the above ideal, find the unique monic generator of least degree polynomial.

$\text{ann}_{v_1}(T) \longrightarrow \mu_{Tv_1}(x)$ of deg m_1

$\text{ann}_{v_2}(T) \longrightarrow \mu_{Tv_2}(x)$ of deg m_2

$\vdots$ $\qquad\qquad$ $\vdots$

$\text{ann}_{v_n}(T) \longrightarrow \mu_{Tv_n}(x)$ of deg m_n

The minimal polynomial of deg m is given as -

$$\mu_T(x) = \text{LCM}\left(\mu_{Tv_1}(x), \mu_{Tv_2}(x), \ldots, \mu_{Tv_n}(x) \right).$$

[Check if $\mathbb{V} = \mathbb{F}^n$ then deg of $\mu_T(x)$ can't be more than n].

Division Algorithm for polynomials:

Let $\mathbb{F}$ be a field. Suppose, $f(x), g(x) \in \mathbb{F}[x]$ with $g(x) \neq 0_{\mathbb{F}[x]}(x)$.

Then there exists an unique polynomial $q(x)$ & $r(x)$ $\in \mathbb{F}[x]$ such that,

$$f(x) = q(x) \cdot g(x) + r(x)$$

and $\deg(r(x)) < \deg(q(x))$

$q(x)$: Quotient

$r(x)$: Remainder

Ex: $f(x) = x^4 + x^2 + x - 2$

$g(x) = x^2 - 1$

Find $q(x)$ and $r(x)$ s.t. $f(x) = q(x) \cdot g(x) + r(x)$.

$x^2-1 \;\big|\; x^4 + x^2 + x - 2 \;\big|\; x^2$

$(-) \; x^4 \; (+) \; -x^2$

$x^2-1 \;\big|\; 2x^2 + x - 2 \;\big|\; 2$

$(-) \; 2x^2 \; (+) \; -2$

$x^2-1 \;\big|\; x$

x^2-1 ← deg = 2

x ← deg = 1

So we stop.

$q(x) = x^2 + 2$

$r(x) = x$.

Factors of a polynomial:

Let $\mathbb{F}$ be a field and $f(x), g(x) \in \mathbb{F}[x]$. We say that g divides f or (g is a factor of f) if there is some polynomial $h(x) \in \mathbb{F}[x]$ such that,

$$f(x) = h(x) \cdot g(x).$$

① If $h(x) \mid g(x)$ and $g(x) \mid f(x)$ then $h(x) \mid f(x)$.

② If $h(x) \mid f(x)$ and $h(x) \mid g(x)$ then
$h(x) \mid a(x) \cdot f(x) + b(x) \cdot g(x)$ for any $a(x), b(x) \in \mathbb{F}[x]$

③ If $g(x) \mid f(x)$ then $g(x) \mid f(x) + g(x) \cdot h(x)$. for any $h(x) \in \mathbb{F}[x]$.

GCD / HCF of 2 polynomials:

Let $\mathbb{F}$ be a field and $f(x), g(x) \in \mathbb{F}[x]$. where not both equal to $0_{\mathbb{F}[x]}(x)$. Then $\gcd(f(x), g(x))$ is a monic polynomial of largest degree satisfying —

(i) $\gcd(f(x), g(x)) \mid f(x)$ and $\gcd(f(x), g(x)) \mid g(x)$.

(ii) if $d(x) \mid f(x)$ and $d(x) \mid g(x)$ then
$d(x) \mid \gcd(f(x), g(x))$.

If $f(x), g(x) \in \mathbb{F}[x]$ then

$\gcd(f(x), g(x)) = a(x) \cdot f(x) + b(x) \cdot g(x)$ for some $a(x), b(x) \in \mathbb{F}[x]$.

If $\gcd(f(x), g(x)) = 1_{\mathbb{F}[x]}(x)$ then there exists polynomials $a(x), b(x) \in \mathbb{F}[x]$ such that,

$$a(x) \cdot f(x) + b(x) \cdot g(x) = 1_{\mathbb{F}[x]}(x).$$

These $f(x)$ & $g(x)$ are called "coprime" polynomials.

Eucledian Algorithm to find $\gcd(f(x), g(x))$:

$f(x), g(x) \in \mathbb{F}[x]$

① Apply division algorithm to find $q(x), r(x)$ s.t.

$$f(x) = q(x) \cdot g(x) + r(x).$$

Here consider choosing $f(x)$ which has larger degree than $g(x)$.

② If $r(x) = 0_{\mathbb{F}[x]}(x)$ then $\gcd(f(x), g(x)) = g^*(x)$ where $g^*(x) = \frac{g(x)}{a}$ where a is the coeff. of high. power of $g(x)$ to make it monic polynomial.

③ If $r(x) \neq 0_{\mathbb{F}[x]}(x)$ then replace $f(x)$ by $g(x)$ and replace $g(x)$ by $r(x)$ and repeat the process.

Example: $f(x) = 3x^4 + 2x^3 + x^2 - 4x + 1$

$g(x) = x^2 + x + 1$

$$f(x) = \underbrace{(3x^2 - x - 1)}_{q(x)} \cdot g(x) + \underbrace{(-2x+2)}_{r(x)}.$$

Since $r(x) \neq 0_{\mathbb{F}[x]}(x)$ therefore,

$f(x) = x^2 + x + 1$

$g(x) = -2x + 2$

$$f(x) = \left(-\frac{1}{2}x - 1\right) g(x) + \underbrace{3}_{r(x)}$$

Since $r(x) \neq 0_{\mathbb{F}[x]}(x)$ therefore,

$f(x) = -2x + 2$

$g(x) = 3$

$$f(x) = \left(-\frac{2}{3}x + \frac{2}{3}\right) g(x) + \underbrace{0}_{0_{\mathbb{F}[x]}(x)}.$$

Hence we stop the algorithm, $\gcd = \frac{g(x)}{3} = 1_{\mathbb{F}[x]}(x)$.

In the reverse way, we can find the polynomials $a(x), b(x)$ such that, $1 = a(x) f(x) + b(x) \cdot g(x)$.

In the backward algorithm,

$$3 = \left(\frac{1}{2}x+1\right)(-2x+2) + g(x)$$

$$= \left(\frac{1}{2}x+1\right)\left(f(x) - (3x^2-x-1)\cdot g(x)\right) + g(x)$$

$$= f(x)\cdot\left(-\frac{1}{2}x+1\right) + g(x)\cdot\left(\frac{3}{2}x^3+\frac{5}{2}x^2-\frac{3}{2}x-2\right).$$

$$\Rightarrow 1 = f(x)\cdot \underbrace{\frac{1}{3}\left(-\frac{1}{2}x+1\right)}_{a(x)} + g(x)\cdot \underbrace{\frac{1}{3}\left(\cdots\right)}_{b(x)}.$$

Least common multiples of 2 polynomials:

Let $\mathbb{F}$ be a field. $f(x), g(x) \in \mathbb{F}[x]$. $\operatorname{lcm}(f,g)$ is the monic polynomial satisfying –

(i) $f(x) \mid \operatorname{lcm}(f,g)$ and $g(x) \mid \operatorname{lcm}(f,g)$

(ii) if $f(x) \mid m(x)$ and $g(x) \mid m(x)$ then

$$\operatorname{lcm}(f,g) \mid m(x)$$

We have, $\operatorname{lcm}(f,g)\cdot \gcd(f,g) = f(x)\cdot g(x)$.

Characteristic Polynomial:

Suppose V is a complex vector space & $T \in L(V, V)$. Let $\lambda_1, \lambda_2, \ldots, \lambda_m$ be the distinct eigenvalues of T with multiplicities $d_1, d_2, \ldots, d_m$.

$$\chi_T(x) = (z-\lambda_1)^{d_1} \cdot (z-\lambda_2)^{d_2} \cdots (z-\lambda_m)^{d_m}$$

is called characteristic polynomial of T.
The ch. polynomial has degree of n (dim of V).

Suppose, $T \in L(V, V)$. let $q(x)$ be the characteristic polynomial of T. Then $q(T) = 0$ is called "Caley Hamilton theorem".

proof: $G(\lambda_i, T) = \ker\left((T - \lambda_i I)^n\right)$.

We know that, $(T-\lambda_i I)\Big|_{G(\lambda_i, T)}$ is a nilpotent operator.

Since $(T-\lambda_i I)\Big|_{G(\lambda_i, T)} \in L\left(G(\lambda_i, T), G(\lambda_i, T)\right)$

$\dim\left(G(\lambda_i, T)\right) = d_i$

Hence, $(T-\lambda_i I)^{d_i}\Big|_{G(\lambda_i, T)} = 0_{L(G(\lambda_i, T), G(\lambda_i, T))}$

$$V = G(\lambda_1, T) \oplus G(\lambda_2, T) \oplus \cdots \oplus G(\lambda_m, T)$$

$$v = v_1 + v_2 + \cdots + v_m \quad \text{where } v_i \in G(\lambda_i, T)$$

$$q(x) = (x-\lambda_1)^{d_1} \cdot (x-\lambda_2)^{d_2} \cdots (x-\lambda_m)^{d_m}$$

$$q(T) = (T-\lambda_1 I)^{d_1} \cdot (T-\lambda_2 I)^{d_2} \cdots (T-\lambda_m I)^{d_m}$$

$$q(T)\Big|_{G(\lambda_1, T)} = (T-\lambda_2 I)^{d_2} \cdots (T-\lambda_m I)^{d_m} \cdot (T-\lambda_1 I)^{d_1}\Big|_{G(\lambda_1, T)}$$

$$= 0$$

We have to show that

$$q(T)v = \underbrace{q(T)v_1}_{\text{must be } 0} + \underbrace{q(T)v_2}_{\text{must be } 0} + \cdots + \underbrace{q(T)v_m}_{\text{must be } 0} = 0_V.$$

if $q(T)$ were to be 0 for all v. then

Since $v_i \in G(\lambda_i, T)$ therefore $q(T) \cdot v_i = 0$ means,

$$q(T)\Big|_{G(\lambda_i, T)} \cdot v_i = 0.$$ which was already proved.

$\Rightarrow q(T) = 0$. (Caley Hamilton theorem).

Characteristic polynomial $\chi_T(x)$ is the multiple of minimal polynomial $\mu_T(x)$.

proof: From Caley hamilton theorem, $\chi_T(T) = 0$

Annihilating ideal of $\mathbb{F}[x]$ under T is

$$\text{ann}(T) := \{ p(x) \in \mathbb{F}[x] \mid p(T) = 0 \}.$$

$$= \langle \{ \mu_T(x) \} \rangle$$

$$= \{ \mu_T(x) \cdot g(x) \mid g(x) \in \mathbb{F}[x] \}$$

$\chi_T(T) = 0$ means $\chi_T(x) \in \text{ann}(T)$.

and $\mu_T(x) \in \text{ann}(T)$.

So we have, $\chi_T(x) = \mu_T(x) \cdot g(x)$.

and $\mu_T(x) \mid \chi_T(x)$.

Eigenvalues are the roots of minimal polynomial but the multiplicity may differ.

proof: $\mu_T(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{m-1} x^{m-1} + x^m$

(say $\mu_T(x)$ is of degree m).

Suppose λ is a root of $\mu_T(x)$. then we can write,

$$\mu_T(x) = (x-\lambda)\cdot q(x) \qquad \exists\, q(x) \in \mathbb{F}[x].$$

$q(x)$ is the monic polynomial.

We know that $\mu_T(T) = 0$ (By definition)

$$\Rightarrow (T-\lambda I)\, q(T) = 0$$

$$\Rightarrow (T-\lambda I)\, q(T)(v) = 0_V \quad \forall v \in V.$$

Because the deg of $q(x)$ is less than the deg of $\mu_T(x)$ so $q(T)v \neq 0$ otherwise $\mu_T(x)$ can't be minimal polynomial.

$$\Rightarrow (T-\lambda I)\, w = 0_V \quad \text{where } w \text{ is an eigenvector}$$

$\Rightarrow \lambda$ is an eigenvalue of T.

Suppose λ is an eigenvalue of T.

$$\Rightarrow Tv = \lambda v.$$

$$\Rightarrow T^j v = \lambda^j v$$

$$\mu_T(T)v = (a_0 I + a_1 T + a_2 T^2 + \cdots + T^m)v = 0$$

$$= (a_0 + a_1\lambda + a_2\lambda^2 + \cdots + \lambda^m)v = 0$$

$\Rightarrow \mu_T(\lambda).v = 0$

Since $v \neq 0$ so $\mu_T(\lambda) = 0$ therefore λ is an root of $\mu_T(x)$.

Hence λ is a root of $\mu_T(x) \iff \lambda$ is an eigenvalue of T.