MATH 314 (Lecture 17)

Topics to be discussed today

Polynomial algebra

Let F be a field.

Define $F[x]$ = Set of polynomials with coefficients in F

$$f = a_0 + a_1 x + \cdots + a_n x^n$$

$$g = b_0 + b_1 x + \cdots + b_m x^m$$

$$f + g = (a_0 + b_0) + (a_1 + b_1) x + \cdots$$

For a scalar $c \in F$

$$cf = ca_0 + ca_1 x + \cdots + ca_n x^n$$

With addition & scalar multiplication defined as above $F[x]$ is a vector space over F.

Qn: What is the dimension of $F[x]$ over F?

We can also multiply two polynomials.

$$f = a_0 + a_1 x + \cdots + a_n x^n$$

$$g = b_0 + b_1 x + \cdots + b_m x^m$$

$$fg = a_0 (b_0 + b_1 x + \cdots + b_m x^m) +$$

$$a_1 x (b_0 + b_1 x + \cdots + b_m x^m) + \cdots$$

Some properties of this multiplication

1) Multiplication is associative

$$f(gh) = (fg)h$$

2) Distributive

$$f(g+h) = fg + fh$$

$$(f+g)h = fh + gh$$

3) If $c \in F$

$$c(fg) = (cf)g = f(cg)$$

$F[x]$ is an example of linear algebra over F.

Defn: Let F be a field. A linear algebra over the field F is a vector space V over F with an additional operation of multiplication of vectors such that

1) Multiplication is associative

2) Distributive property holds

3) For scalar $c \in F$

$$c(\alpha\beta) = (c\alpha)\beta = \alpha(c\beta)$$

Defn: Let V be a linear algebra over F. If there exists a multiplicative identity in V, i.e., there exists an element $1 \in V$ such that $(\alpha)(1) = (1)(\alpha) = \alpha \ \forall \alpha \in V$, we say that V is a linear algebra with identity. We say V is Commutative if $\alpha\beta = \beta\alpha \ \forall \alpha, \beta \in V$.

Example: 1) F over F

2) $F[x]$ over F

3) $M_{n\times n}(F)$ over F

4) $L(V, V)$ over F

Polynomial Algebra

Terminology

$$f(x) \neq 0$$

$$a_0 + a_1 x + \cdots + a_n x^n$$

If n is the largest power of x such that $a_n \neq 0$, then n is called degree of f.

$a_0, a_1, \ldots, a_n$ are called coefficients of f.

If $a_n = 1$ (n being degree of f) we say that $f(x)$ is monic.

Lemma: Let $f, g \in F[x]$ both non-zero. Then

i) fg is a non-zero polynomial.

ii) $\deg(fg) = \deg f + \deg g$

iii) Assume $f+g \neq 0$, then

$$\deg(f+g) \leq \max(\deg f, \deg g)$$

Pf: $f = a_0 + a_1 x + \cdots + a_n x^n$ $\deg f = n$, $a_n \neq 0$

$g = b_0 + b_1 x + \cdots + b_m x^m$ $b_m \neq 0$, $\deg g = m$

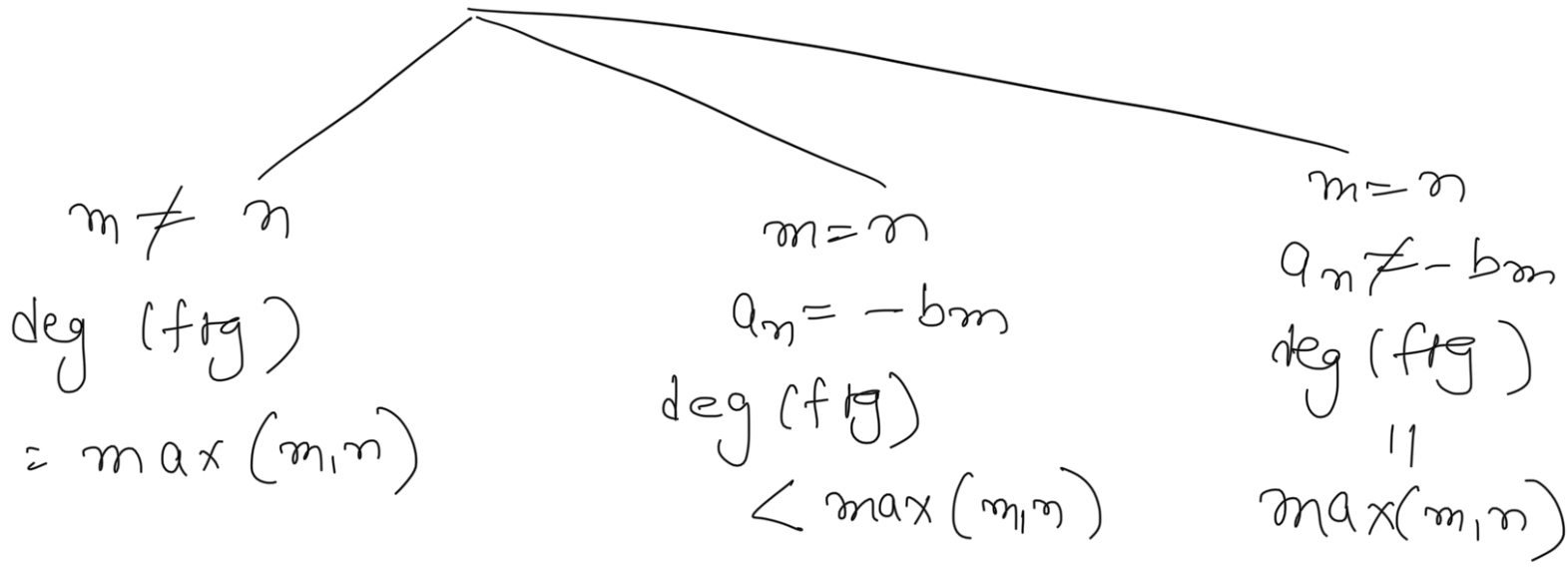
$$fg = a_0 b_0 + (a_0 b_1 + a_1 b_0) x + \cdots + a_n b_m x^{n+m}$$

$a_n b_m \neq 0$ because $a_n \neq 0$ & $b_m \neq 0$

$\deg(fg) = n+m = \deg f + \deg g$

So, (i) & (ii) are proved.

iii) $f+g$



So, $\deg(f+g) \leq \max(m,n)$

—

Evaluating polynomials

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

X can take values in any linear algebra over F, not just F.

Example: Consider $X^2+1 \in \mathbb{R}[X]$

We can plug in X for any element of linear algebra over $\mathbb{R}$.

$$A = \begin{pmatrix} \sqrt{2} & 0 \\ 0 & -1 \end{pmatrix}$$

$$f(A) = A^2 + I$$

$$A^2 = \begin{pmatrix} \sqrt{2} & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \sqrt{2} & 0 \\ 0 & -1 \end{pmatrix}$$

$$= \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$$

$$A^2 + I = \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix} \in M_{2\times 2}(\mathbb{R})$$

We will revisit this idea when we discuss characteristic polynomials.

Revisiting integers $\mathbb{Z}$

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

We have division algorithm in $\mathbb{Z}$.

Division algorithm: For $a, b \in \mathbb{Z}$, $b \neq 0$

there exists a quotient q and a remainder r such that

$$a = bq + r$$

where $r = 0$ or $0 < r < |a|$

This division algorithm allows us to compute GCD of two integers.

↓

Greatest Common Divisor

Example: Let us compute GCD(36, 20).

$$36 = 20(1) + 16$$

$$20 = 16(1) + 4 \leftarrow 4 \text{ is the GCD}$$

$$16 = 4(4) + 0$$

In general

$$a = bq + r \qquad r < b$$

$$b = rq_1 + r_1 \qquad r_1 < r < b$$

$$r = r_1 q_1 + r_2$$

$$\vdots$$

$$r_i = r_{i+1} q_{i+1} + 0 \longrightarrow \text{GCD}$$

Division algorithm allows us to define prime numbers.

Defn: An integer p is called prime if its only divisors are $\pm p$ and ± 1.

Example: $2, 3, 5, 7, 11, 13, - - - -$

FUNDAMENTAL THEOREM OF ARITHMETIC

Let $N \in \mathbb{Z}$, $N \neq 0, \pm 1$. Then, there exists unique (upto permutations of primes & signs) factorization of N as a product of primes.

Proof: Let's see an example.

$$36 = 4 \cdot 9 = 2^2 \cdot 3^2 = 3^2 \cdot 2^2 = (-3)^2 \cdot 2^2$$

It is sufficient to prove this result for positive integers.

We will prove this via induction on N.

If $N = 2$, then N is already a prime.

Suppose the theorem holds for

$$N \in \{2, 3, \ldots k-1\}.$$

Consider $N = k$. If N is already a prime, we are done. Otherwise N is composite and hence

$$N = N_1 N_2$$

$$2 \leq N_i \leq k-1$$

Apply induction on N_1 & N_2 to get their prime factorizations.

So, $N = p_1^{q_1} p_2^{q_2} \cdots p_r^{q_r}$.

Analogous to $\mathbb{Z}$, we have division algorithm in $F[x]$. (F field).

Example: Let us divide $x^4+x^3+x^2+x+1$ by $x+1$.

$$x+1 \;\overline{)\; x^4+x^3+x^2+x+1}$$

Multiply: x^3+x

$$x^4+x^3+x^2+x+1$$
$$-\,x^4+x^3$$
$$0+0+x^2+x+1$$

(Multiply x with $x+1$): x^2+x

$$0+0+x+1$$

1 ← remainder

$$(x^4+x^3+x^2+x+1) = (x+1)(x^3+x)+1$$

x^3+x ← quotient; 1 ← remainder

Thm: Let $f, g \in F[x]$, $g \neq 0$. Then there exists $q(x)$ (quotient) and $r(x)$ (remainder) such that

$$f = gq + r \quad \text{where} \quad r = 0 \text{ or } \deg r < \deg g.$$

Proof: If $\deg f < \deg g$, then $q = 0$ & $r = f$.

Otherwise say

$$f = a_0 + a_1 x + \cdots + a_n x^n \qquad n \geq m$$

$$g = b_0 + b_1 x + \cdots + b_m x^m$$

$$f - \left(\frac{a_n}{b_m}\right) x^{n-m} g = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$$

If $n-1 < m$ or RHS $= 0$ then stop

Otherwise, repeat.

$$\left(c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}\right) - \left(\frac{c_{n-1}}{b_m}\right) x^{n-1-m} g$$

$$= \cdots$$

$$f - \left(\frac{a_n}{b_m} x^{n-m} + \frac{c_{n-1}}{b_m} x^{n-1-m}\right) g$$

$$= h(x)$$

:

Repeat this till RHS $= 0$ or deg (RHS) $<$ deg g.

$$f - q(x) g = r(x)$$

$q(x)$: quotient

$r(x)$: remainder

Irreducible Polynomials

(Analogs of prime numbers)

Defn: We say a non-constant polynomial $f(x)$ is irreducible in $F[x]$ if whenever $f = gh$, $\deg g = 0$ or $\deg h = 0$.

Example: 1) All degree 1 polynomials are irreducibles.

2) x^2+1 is irreducible in $\mathbb{R}[x]$.

3) x^2-2 is irreducible in $\mathbb{Q}[x]$.

but reducible in $\mathbb{R}[x]$.

$$x^2-2 = (x-\sqrt{2})(x+\sqrt{2})$$

Thm: A non-constant monic (top degree coefficient is 1) polynomial in $F[x]$ can be factored as a product of monic irreducibles in $F[x]$ uniquely (upto ordering).

Pf: Same as $\mathbb{Z}$. Use induction on degree.

So, if $f \in F[x]$, monic non-constant then

$$f = f_1^{q_1} f_2^{q_2} \cdots f_n^{q_n}$$

irreducibles

This decomposition is called primary decomposition.

$\mathbb{Z}$	$F[x]$
Absolute value	Degree
Division algorithm	Division algorithm
primes	irreducibles
Unique factorization into primes	Unique factorization into irreducibles.