30 November 2020 15:12

Polynomial Method in Combinatorics

Recalling definitions of some algebraic structures

Group

$(X, +)$, X is a set, $+$ is a binary op on X, is a group if:-

(i) closure $\forall a, b \in X$, $a+b \in X$

(ii) associativity $(a+b)+c = a+(b+c)$, $\forall a, b, c \in X$

(iii) Identity $\exists 0 \in X$ s.t. $a+0 = a$, $\forall a \in X$.

(iv) Inverse $\forall a \in X$, $\exists \bar{a}$ s.t.

$$a + \bar{a} = 0$$
$$\| $$
$$(-a).$$

In addition, if $+$ is a commutative op, ($a+b = b+a$)

then $(X, +)$ is an Abelian group.

Ring.

$R = (X, +, \cdot)$, where $+, \cdot$ are binary op on X, is a ring if

(i) $(X, +)$ is an Abelian group

(i) $(X, +)$ is an Abelian group

(ii)
(a) Closure under $\cdot$.
(b) Associativity under $\cdot$.

(iii) Distributive law:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

Let $R = (X, +, \cdot)$ be a Ring. If $i \in X$ such that $i \cdot a = a \cdot i = a$, $\forall a \in X$, then R is a ring with an identity. If R is a ring where $\cdot$ is a commutative op, then R is called a commutative ring.

A commutative ring with identity is called an integral domain if

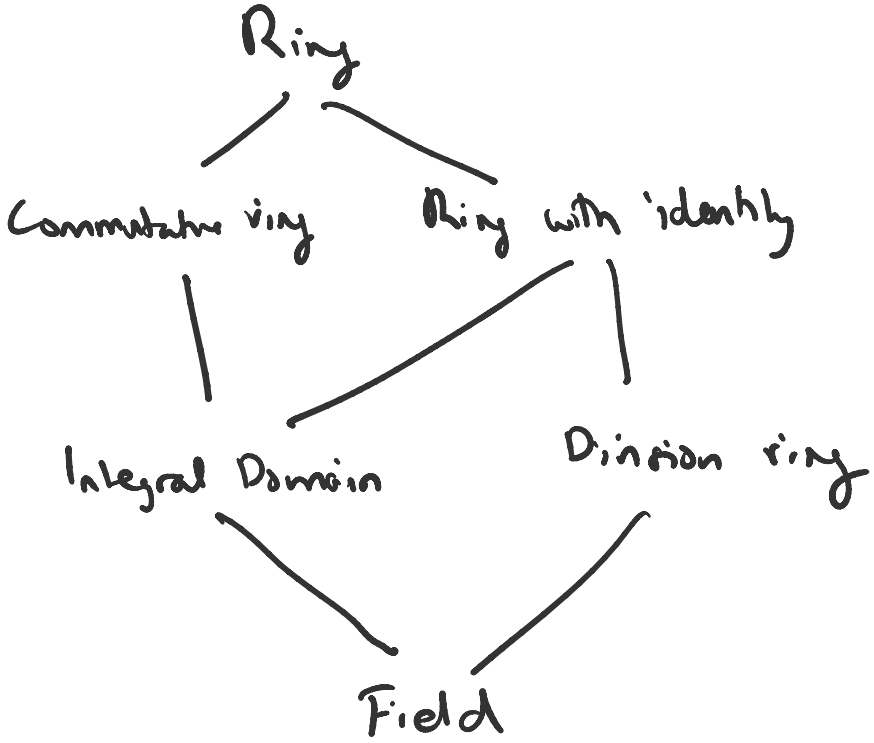
$$\forall a, b \in X, \quad (ab = 0) \Rightarrow (a = 0 \text{ or } b = 0).$$

Example of Integral Domain: Integers $(\mathbb{Z}, +, \cdot)$.

A ring with identity with every

A ring with identity with every $a \in X$, $a \neq 0$, having an inverse under $\circ$ op, is called a division ring.

A commutative division ring is called a Field.



Polynomial Ring

Let R be a Commutative ring with identity. An expression of the form:-

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

when every $a_i \in R$ and $a_n \neq 0$ is called a polynomial over R with

called a polynomial over R with indeterminate x.

$a_0, a_1, \ldots, a_n$ are coefficients

a_n ↳ leading coefficient

If n is the largest non-negative number for which $a_n \neq 0$, we say

$$\deg(f(x)) = n.$$

Polynomial Method

Some facts we know of single variable polynomials:-

(i) Every non-zero polynomial of degree d has at most d roots.

(ii) For every set S of points from R, $\exists$ a non-zero polynomial $f(x)$ of degree at most $|S|$ such that

$$f(x) = 0, \quad \forall x \in S.$$

$S = \{d_1, d_2, d_3\}$

$$f(x) = (x - d_1)(x - d_2)(x - d_3)$$

We try to extend these facts to multivariate polynomials.

Definition: Let $x_1, x_2, \ldots, x_n$ be variables/indeterminates. A monomial of degree t is $x_1^{t_1} x_2^{t_2} \cdots x_n^{t_n}$, where $t_i \geq 0$, $\forall i \in [n]$, and $t_1 + t_2 + \cdots + t_n = t$. The only monomial of degree 0 is 1.

For a given field $\mathbb{F}$, let $\mathbb{F}(x_1, x_2, \ldots, x_n)$ denote the ring of all multivariate polynomials over $\mathbb{F}$, where $x_1, x_2, \ldots, x_n$ are indeterminates. Each such polynomial is a linear combination of monomials with coefficients

of monomials with coefficients taken from $\mathbb{F}$.

$5(x_1 x_2) + 3(x_1 x_3^2) + \dots$

The degree of f, denoted by $\deg(f)$, is the maximum degree among monomials with a non-zero coefficient.

"Root": $x \in \mathbb{F}^n$ is a root of f if $f(x) = 0$.

"Vanishes": Let $S \subseteq \mathbb{F}^n$. If $f(x) = 0$ $\forall x \in S$, then we say that f vanishes on S.

"Zero polynomial": A polynomial is called a zero polynomial if all its coefficients (when expressed in canonical form) are zeroes.

Lemma: Given a set $E \subseteq \mathbb{F}^n$ of size $|E| < \binom{n+d}{d}$, there exists

a polynomial $f \in \mathbb{F}(x_1, x_2, \ldots, x_n)$ of degree at most d that vanishes on E.

$n = 1$
$|E| < \binom{1+d}{d} = d+1$
$\deg(f) \le d$.

Proof:

Let V_d be the vector space of all polynomials f, where $f \in \mathbb{F}(x_1, x_2, \ldots, x_n)$ of degree at most d.

What is $\dim(V_d)$?

Ans: $\dim(V_d) = \binom{n+d}{d}$ — (1)

Basis

$\{ 1 \;\; x_1, x_2, \ldots, x_n \;\; x_i x_j \; (i \le j) \;\; \ldots \;\; (x_1 x_2 \ldots x_d) \;\; \ldots (x_{n-d+1} \ldots x_n) \}$

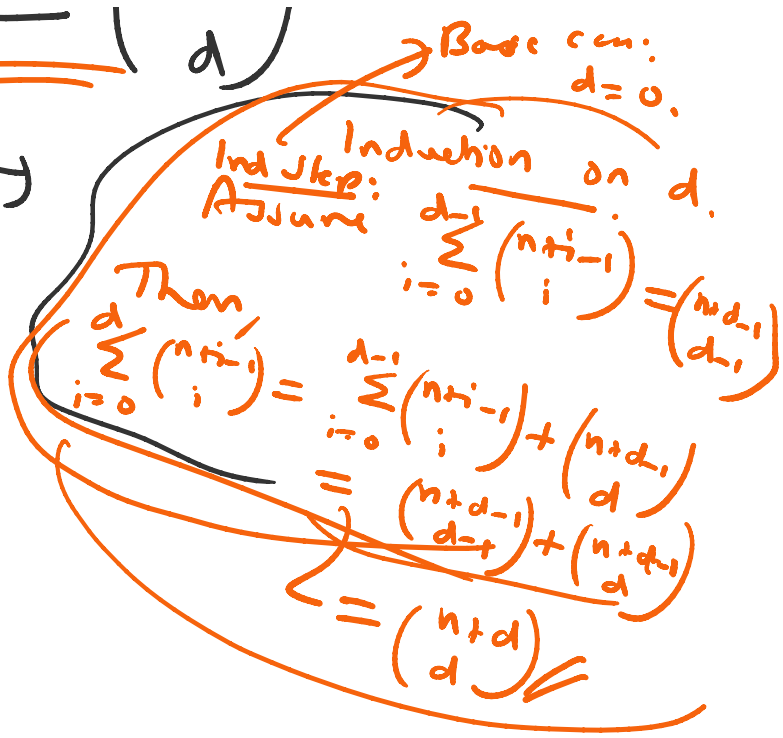
$1 \;\; n \;\; \binom{n}{2} + n$

no. of ways of choosing i elements from n elements with repetition (choosing 2 elements from n elements with repetition)

$$\sum_{i=0}^{d} \binom{n+i-1}{i} = \binom{n+d}{d}$$

Base case: $d = 0$

$i=0$ ( ) — ( ) d



Consider the vector space of all the functions from E to $\mathbb{F}$, i.e. Consider the V.S. $\mathbb{F}^E$ over $\mathbb{F}$.

We can see that,

Recall, $|E| < \binom{n+d}{d}$

$$\dim(\mathbb{F}^E) < \binom{n+d}{d} \quad \text{— (2)}$$

[Reason: let $E = \{a_1, a_2, \ldots, a_m\}$, where each $a_i \in \mathbb{F}^n$ and $m < \binom{n+d}{d}$.

Then the following functions span $\mathbb{F}^E$. For $1 \le i \le m$,

$f_i : E \to \mathbb{F}$ is defined as

$\forall a \in \mathbb{F}^n$, $f_i(a) = \begin{cases} 1 & \text{, if } a = a_i \\ \end{cases}$

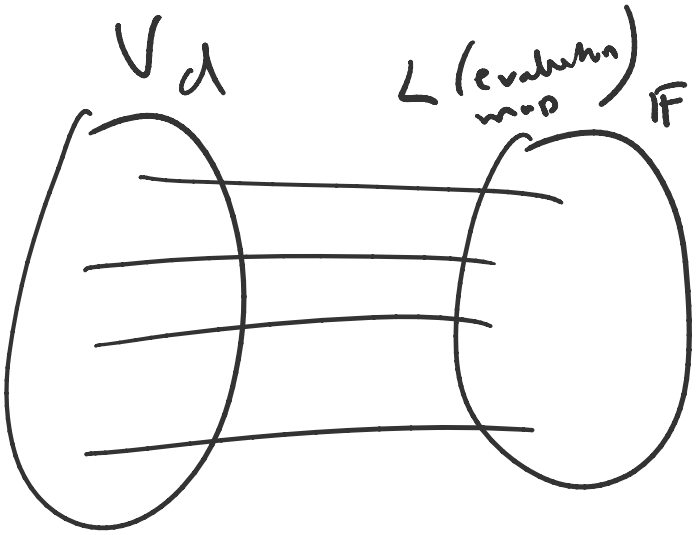
$\forall a \in E$, $t_i(a) = \begin{cases} 1, & a = a_i \\ 0, & \text{otherwise} \end{cases}$

Define a linear map

$$L: V_d \to \mathbb{F}^E \quad \text{where}$$

L: evaluation map

$$L(f) = (f(a))_{a \in E}$$



From Rank Nullity Theorem, we know that

$$\dim(V_d) = \dim(\ker(L)) + \dim(\text{Im}(L))$$

From (1) and (2), we know that

$$\dim(V_d) = \binom{n+d}{d} \quad \text{and}$$

$$\dim(\text{Im}(L)) \leq \dim(\mathbb{F}^E) < \binom{n+d}{d}$$

(a)

So this implies that,

$$\dim(\ker(L)) > 0.$$

Hence, L is not injective.

That is, $\exists f_1, f_2 \in V_d$, $f_1 \neq f_2$, such that

$$L(f_1) = L(f_2)$$

This means, $\rightarrow L(f_1 - f_2) = L(f_1) - L(f_2) = 0_{FG}$

$f_1 - f_2$ is a non-zero polynomial in V_d that vanishes on all points in E.

□