Affine Varieties :-

we call $A^n : A^n_k = \{ (c_1, c_2, \ldots, c_n) : c_i \in k$ for $i = 1, \ldots n \}$

the affine n- space over K.

where K is a field.

A_k^n is K^n without an origin.

$A^2_{\mathbb{R}} = \mathbb{R}^2$

$A^n_K = \{(a_1, \ldots a_n) \mid a_i \in K\}$.

Zero locus / Vanishing locus :-

The set of points where a function vanishes, in other if that takes the value zero is called zero locus

For a subset $S \subset K[x_1, x_2, \ldots, x_n]$ of polynomial we call

$$V(S) = \{x \in A^n : f(x) = 0 \text{ for all } f \in S\} \subset A^n$$

Subsets of A^n of this form are called (affine) ~~Varieties~~ varieties.

If $S = \{f_1, \ldots, f_k\}$ is a finite set, we will write $V(S) = V(\{f_1, f_2, \ldots, f_k\})$ also as $V(f_1, f_2, \ldots, f_k)$

Affine Varieties :-

Let K be a field, and let $f_1, \ldots, f_s$ be polynomials in $K[x_1, \ldots, x_n]$.

$$V(f_1, f_2, \ldots, f_s) = \{(a_1, a_2, \ldots, a_n) \in K^n : f_i(a_1, a_2, \ldots, a_n) = 0 \text{ for all } 1 \le i \le s\}.$$

$V(f_1, f_2, \ldots, f_s)$ is called the affine variety defined by $f_1, f_2, \ldots, f_s$

$V(f_1, f_2, \ldots, f_s)$ is the set of solutions of the system of polynomial equations

$$f_1(x_1, x_2, \ldots, x_n) = 0$$

$$f_2(x_1, x_2, \ldots, x_n) = 0$$

$$\vdots$$

$$f_s(x_1, x_2, \ldots, x_n) = 0$$

$V(S) = V(f_1, f_2, \ldots, f_s) \subset K^n$ is the set of all solutions of the system of equations $f_1(x_1, x_2, \ldots, x_n) = \ldots = f_s(x_1, x_2, \ldots x_n) = 0$

where $S \subset k[x_1, x_2, \ldots, x_n]$ and $f_i \in S$

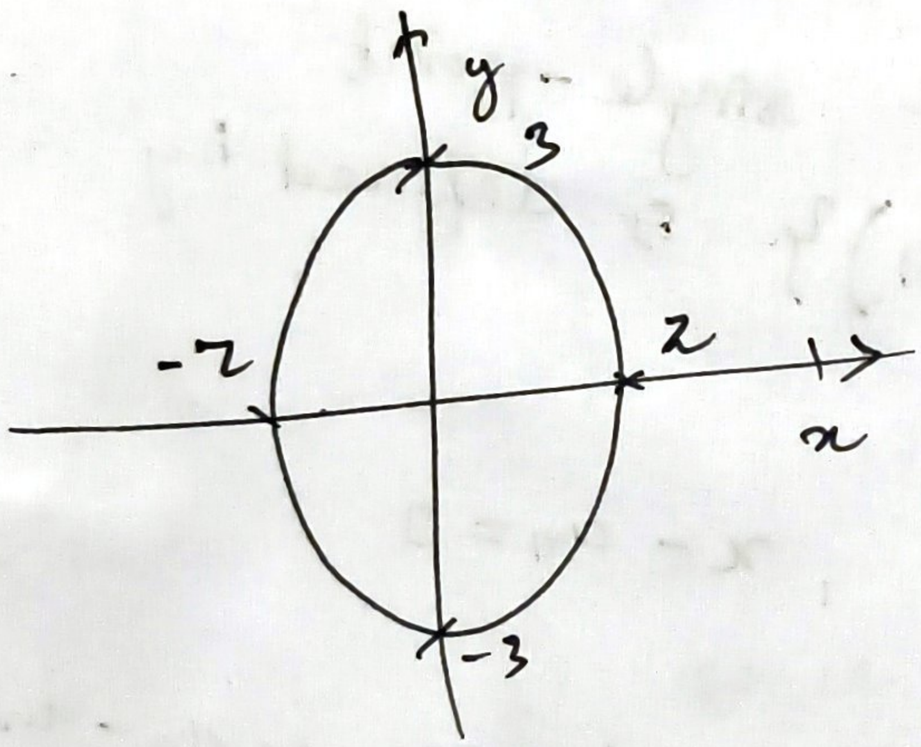
Examples :

Conic are affine varieties.

① $V(9x^2+4y^2-36) = \{(x,y) \in \mathbb{R}^2 \mid 9x^2+4y^2-36=0\}$

$= \{(x,y) \in \mathbb{R}^2 \mid 9x^2+4y^2=36\}$

$= \{(x,y) \in \mathbb{R}^2 \mid \frac{x^2}{4} + \frac{y^2}{9} = 1\}$



Here $\mathbb{C}^2 \neq \mathbb{R}^2 = \phi$

Affine Space $\mathbb{A}^n_k$

Entire space

No equation imposed

Dimension exactly n

Example : $\mathbb{A}^2$ plane

Affine Variety.

usually a subset

Defined by polynomial equations.

Dimension can be smaller

circle, parabola, line etc.

An affine variety is a subset of $\mathbb{A}^n_k$

$$X = V(f_1, \dots, f_r)$$

where $f_i \in k[x_1, \dots, x_n]$

That means

$$X = \{p \in \mathbb{A}^n_k : f_1(p) = \dots = f_r(p) = 0\}$$

~~#~~ $\mathbb{A}^2_k$ contains all points (a,b)

$V(y-x^2) \subset \mathbb{A}^2_k$.

$V(x^2+y^2-1) \subset \mathbb{A}^2_{\mathbb{R}}$.

$\mathbb{A}^n_k = V(0)$ (zero polynomial vanishes everywhere)

Affine variety is a set of common zeros of polynomials

$V(S) = \{p \in \mathbb{A}^n_k : f(p) = 0 \text{ for all } f \in S\}$

$$X = V(f_1, f_2, \cdots, f_n) = V(\{f_1, f_2, \cdots, f_n\})$$

Hypersurface !

An algebraic set (affine variety)

$X \subseteq \mathbb{A}^n_K$ is called a hypersurface

if $X = V(f)$ for some non-constant

polynomial $f \in K[x_1, x_2, \cdots, x_n]$

Example :- Consider subset of $\mathbb{A}^1$

The set $X_1 = \{5\}$ is a hypersurface

since. $X = V(x-5)$

for $f(x) = (x-5)$ is a non-constant

polynomial.

Theorem :- We consider subset in $\mathbb{A}^n$.

Let S_1 and S_2 be two sets of polynomial in $k[x_1, \dots, x_n]$: If $S_1 \supseteq S_2$, then

$$\boxed{V(S_1) \subseteq V(S_2)}$$

. In other words, the correspondence V is inclusion-reversing.

let R be a commutative ring with unity.

For any subset $S \subseteq R$, the ideal

$$I = \{ r_1 f_1 + \cdots + r_k f_k \mid k \in \mathbb{N},\ r_1, r_2, \dots, r_k \in R,\ f_1, \dots, f_k \in S \}$$

is called the ideal generated by S.

We say S is a set of generators of I.

An ideal I is said to be finitely generated if it is generated by a finite set

$S = \{ f_1, f_2, \dots, f_m \} \subseteq R$.

we write $\boxed{I = (f_1, \dots, f_m)}$

An ideal I is principal if it is generated by one-element $f \in R$.
we write $I = (f)$

~~Ex~~ Lemma:

(1) For any $S_1 \subset S_2 \subset K[x_1, \ldots, x_n]$ we have
$V(S_1) \supset V(S_2)$: Example?.

(2) For any $S_1, S_2 \subset K[x_1, \ldots, x_n]$ we have
$V(S_1) \cup V(S_2) = V(S_1 S_2)$ where
$S_1 S_2 = \{ fg : f \in S_1, g \in S_2 \}$

(3) If J is any index set and
$S_i \subset K[x_1, x_2, \ldots, x_n]$ for all $i \in J$
and then $\bigcap_{i \in J} V(S_i) = V\left(\bigcup_{i \in J} S_i\right)$

Ideals :

For $S \subset \mathbb{R}^n$, the ideal of S is

$$I(S) = \{ f \in \mathbb{R}[x_1, \ldots, x_n] \mid f(x) = 0 \text{ for all } x \in S \}$$

Ideal of $\{f_1, \ldots, f_m\}$ is the smallest ideal containing $f_1, \ldots f_m$. The polynomials $f_1, f_2, \ldots, f_m$ are called the generators of the ideal.

An ideal generated by one-polynomial is called a principal ideal.

Variety :

$$V(I) = \{ x \in K^n \mid f(x) = 0 \text{ for all } f \in I \}$$

Hilbert Nullstellensatz :

Let K be an algebraically closed field, and

$f_1, f_2, \ldots, f_r \in K[x_1, \ldots, x_n]$

$V(f_1, \ldots, f_r) = \phi$

$\Rightarrow$ ~~$1 \notin K$~~ $1 \in (f_1, \ldots, f_r)$

Ex.: Take $f(x) = 1$

$$V(1) = \{a \in K^n \mid 1 = 0\}$$

$$V(1) = \phi$$

$$(1) = K[x]$$

$1 \in (1)$

$1 \in (1) \Rightarrow 1 = g(x) \cdot 1.$

Eg 2 : $\mathbb{C}[x]$

$f_1 = x \quad , f_2 = x-1$

$V(x, x-1) = \{a \in \mathbb{C} \mid a=0 \text{ and } a=1\}$

$V(x, x-1) = \phi$

$1 = (x) - (x-1)$

$1 \in (x, x-1)$

Note : $I \subseteq \mathbb{C}$ $I = (x, x-1)$

$I = \{ f(x) \cdot x + g(x)(x-1) \mid$

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

$I \subset \mathbb{C}[x]$

with

$\mathbb{C}[x] = \{$ all polynomials in x complex coefficients $\}$

The Nullstellensatz :-

Suppose $f_1, \ldots, f_m \in \mathbb{C}[x_1, \ldots, x_n]$. Then

$1 \in$ ideal $\{f_1, \ldots, f_m\}$

$\iff V_{\mathbb{C}}\{f_1, \ldots, f_m\} = \phi$

i.e For Complex polynomial $f_1, \ldots, f_m \in \mathbb{C}[x_1, \ldots, x_n]$ we have

$1 \in$ ideal $\{f_1, \ldots, f_m\}$

$\iff V\{f_1, f_2, \ldots, f_m\} = \phi$

This doesn't hold for polynomial and varieties over the real number.

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

$V_R\{f\} = \{x \in R \mid f(x) = 0\}$

$= \phi$.

But $1 \notin$ ideal $\{f\}$ since any multiple of f will have degree ≥ 2.

$1 \in$ Ideal $\{f_1, \ldots, f_m\}$ means there are polynomial $h_1, h_2, \ldots, h_m \in \mathbb{C}[x_1, x_2, \ldots, x_n]$ such that

$$\boxed{1 = h_1 f_1 + \cdots + h_m f_m}$$

$\Rightarrow 1 = h f(x)$

$\Rightarrow 1 = h(x^2+1)$. Contradiction.

Theorem :-

For any subset $S \subseteq k[x_1, x_2, \ldots, x_n]$.

let $I \subseteq k[x_1, \ldots, x_n]$ be the ideal generated by S. Then $V(S) = V(I)$

Proof:- If $S \subseteq I$ then $V(S) \supseteq V(I)$

To show that $V(S) \subseteq V(I)$

For every point $P = (a_1, \ldots, a_n) \in V(S)$,

we need to show that $P \in V(I)$

Since I is generated by S, every element $g \in I$ can be written in the form

$$g = r_1 f_1 + r_2 f_2 + \cdots + r_k f_k$$

for some $k \in N$,

$r_1, r_2, \ldots, r_k \in k[x_1, x_2, \ldots, x_n]$

and $f_1, f_2, \ldots, f_k \in S$

Since $P \in V(S)$ ~~$\Rightarrow$~~ ~~$f_1 = f$~~ this implies

$$f_1(P) = f_2(P) = f_3(P) = \cdots = f_k(P) = 0$$

which implies $g(p) = r_1(p) f_1(p) + \cdots + r_k(p) f_k(p)$

$= 0$

Therefore $p \in V(I)$

It follows that $\boxed{V(S) \subseteq V(I)}$

Consider $X = \{0\} \subseteq A^1$. Consider two principal ideals $I_1 = (x)$ and $I_2 = (x^2)$ in $k[x]$. Then $X = V(I_1) = V(I_2)$

Note: If S is any set of polynomials in $k[x_1, \ldots, x_n]$ and let $V(S) = \{x \in A^n \mid f(x) = 0$ for all $x \in S\}$

Let $V(S) = \{ x \in A^n \mid f(x) = 0$ for all $f \in S \}$

$\Rightarrow \boxed{V(S) = \bigcap_{f \in S} V(f)}$

$f = (f_1, f_2, \ldots, f_m)$, $x = (x_1, x_2, \ldots, x_n)$

$V(f) = V(f_1, \ldots, f_m) = \{ x \in A^n \mid f(x) = 0 \}$

$= \{ x \in A^n \mid f_1(x) = \cdots = f_n(x) = 0 \}$

$$= \{x \in A^n \mid f_1(x) = 0\} \cap \dots \cap$$

$$\{x \in A^n \mid f_m(P) = 0\}$$

~~$= V(f_1) \cap V(f_2) \cap \dots \cap V(f_n)$~~

$$= V(f_1) \cap V(f_2) \cap \dots \cap V(f_m)$$

$$= \bigcap_{f \in S} V(f)$$

Theorem :-

Every affine algebraic subset of $A^1(K)$ is either finite or $A^1(K)$ itself.

proof :- let $X \subseteq A^1(K)$ be an affine algebraic set and $X \neq A^1(K)$. Then there is a proper ideal I of $K[x]$ so that $X = V(I)$ since every ideal in $K[x]$ is P.I.D so there exist some $f \in I$ such that $I = (f)$

we distinguish two cases

① If $f = 0$ then $I = 0$ and $X = V(0) = A^1(K)$

② If $f \neq 0$, then f has a finite number of zeros.

$$X = V(f) = \{ x \in A^1(K) \mid f(x) = 0 \}$$

$$= \{ \text{root of } f \}$$

$$= \bigcap_{f \in I} V(f)$$

$V(I)$ is the intersection of finite subsets of $A^1(K)$

Therefore $V(f)$ is a finite subset of $A^1(K)$ for all $f(x) \in K[x]$.

This implies that $V(I)$ is either the empty set or a finite subset of $A^2(k)$

Q. Give an example of a countable collection of algebraic sets whose union is not algebraic.

Sol Let $k = \mathbb{R}$ $\Rightarrow A^2(k) = \mathbb{R}$

$$V(x-n) = \{x \in \mathbb{R} \mid x-n = 0\}$$

$$= \{n\}$$

Let $A_n = \{n\} = V(x-n)$

A_n is an algebraic set of $A^2(k)$

and $|A_n| < \infty$ for all n.

Thus $\{A_n\}_{n \in \mathbb{Z}}$ is a countable collection of algebraic sets, and $\cup A_n = \mathbb{Z}$

Also, $\mathbb{Z}$ is a countable union of single points and any single point is algebraic.

By using the theorem every affine algebraic subset of $A^2(K)$ is either finite or $A^2(K)$ itself.

$A^2(K) = \mathbb{R} \neq \mathbb{Z} = \bigcup A_n$.

and $|\bigcup A_n| = \infty$ (infinite)

Therefore $\bigcup A_n$ is not algebraic.

Q. Show that $\{(t, t^2, t^3) \in A^3(k) \mid t \in k\}$ is an algebraic set.

Sol. Let $X = \{(t, t^2, t^3) \in A^3(k) \mid t \in k\}$.

Let $k = \mathbb{R}$, $A^3(k) = \mathbb{R}^3$. Then

$X = \{(t, t^2, t^3) \in \mathbb{R}^3 \mid t \in \mathbb{R}\}$

Let $f = y - x^2$, $g = z - x^3$

$V(f) = \{(x, y, z) \in \mathbb{R}^3 \mid y - x^2 = 0\}$

$V(g) = \{(x, y, z) \in \mathbb{R}^3 \mid z - x^3 = 0\}$

Take $P = (t, t^2, t^3) \in X$

Then $f(P) = g(P) = 0$

$\Rightarrow P \in V(f)$ and $P \in V(g)$

$P \in V(f) \cap V(g)$

$X = V(f) \cap V(g)$

$$X = V(y-x^2, z-x^3) = V(y-x^2) \cap V(z-x^3)$$

The set of points (t, t^2, t^3) with in k

just the set of solutions to $y-x^2=0$,

$z-x^3=0$

Therefore X is an algebraic set

Q. Suppose C is an affine plane curve, and L is a line in $\mathbb{A}^2(k)$, $L \not\subset C$.

Suppose $C = V(F)$, $F \in k[x,y]$ a polynomial of degree n.

Show that $L \cap C$ is a finite set of no more than n points.

Soln:

let $L = V(y-(ax+b))$ where $a, b \in K$

$L \cap C = V(y-(ax+b)) \cap V(F)$

Take $P = (x, ax+b) \in L \cap C$, then

$F(P) = F(x, ax+b) \in K[x]$

is of degree no more than n.

By the fact that L is not contained in C, the number of roots of $F(P)$ is no more than n, i.e $L \cap C$ is finite of no more than n points.

$L \cap C = \{(x, ax+b) \in \mathbb{A}^2(k) \mid F(x, ax+b) = 0\}$

Q. Prove that $X = \{(x,y) \in \mathbb{A}^2(\mathbb{R}) \mid y = \sin x\}$ is not algebraic.

Sol. Suppose X is algebraic. Then there exist a non-zero polynomial $F(x,y)$ such that

$$X \subseteq V(F)$$

so $V(F)$ is a plane affine curve

Now consider the line

$$L = V(y) = \{(x,y) \in \mathbb{A}^2(\mathbb{R}) \mid y = 0\}$$

$$= V(y) = \{(x,y) \in \mathbb{A}^2(\mathbb{R}) \mid y = 0\}$$

L be a line in $\mathbb{A}^2(\mathbb{R})$

$$L \cap X = \{(k\pi, 0) \mid k \in \mathbb{Z}\}$$

because $\sin k\pi = 0$

L is not contained in X because the point $(\pi/2, 0)$ is in L but not in X.

Therefore $V(F)$ is an affine plane curve containing X and L is not contained in $V(F)$

$\Rightarrow$ so $L \cap X$ is an infinite set

since $X \subseteq V(F)$

$L \cap X \subseteq L \cap V(F)$

Hence ~~$L \cap f$~~ $L \cap V(F)$ is also infinite

Now using this theorem, If a line L is not contained in a plane affine curve $V(F)$, then $L \cap V(F)$ is finite.

$\Rightarrow$ $L \cap V(F)$ leads to contradiction.

Let I be an ideal in a ring R. The radical of I is

$$\sqrt{I} = \{ f \in R \mid f^n \in I \text{ for some } n \in \mathbb{N} \}$$

An ideal I is said to be a radical ideal if $I = \sqrt{I}$.

Every prime ideal of a ring is a radical ideal.

Sol: Let R be a Commutative ring and $P \subset R$ be a prime ideal

$$\text{rad}(P) = \sqrt{P} = \{ x \in R \mid x^n \in P \text{ for some } n \in \mathbb{Z}^+ \}$$

To show P is radical, we must prove that $x^n \in P \Rightarrow x \in P$.

To prove this, we first prove by induction over n that if $x \in R$ and $n \in \mathbb{N}$, $n > 0$ then $x^n \in P \Rightarrow x \in P$.

If $n = 1$, there is nothing to prove.

Now suppose $n \geq 1$ and $x^n \in P$

$\Rightarrow x \in P$ for every $x \in R$.

If we $x^{n+1} = x\,x^n \in P$ then either $x \in P$ or

$x^n \in P$. According to our assumption,

it still have $x^n \in P$ and $x \in P$

So, $\text{rad}(P) \subset P$

If $x \in \text{rad}(P)$ then $x^n \in P$ for some $n \in \mathbb{Z}^+$

by the definition of radical.

For every ideals of R the inclusion $P \subset \text{rad}(P)$

is obvious.

Hence $P = \text{rad}(P) = \sqrt{P}$

Q Show that $I = \langle x^2+1 \rangle \subset \mathbb{R}[x]$ is a radical (even a prime) ideal, but I is not the ideal of any set in $\mathbb{A}^1(\mathbb{R})$

Sol. x^2+1 is irreducible over $\mathbb{R}$

$$\frac{\mathbb{R}[x]}{\langle x^2+1 \rangle} \cong \mathbb{C} \quad \text{(An integral domain)}$$

$\Rightarrow x^2+1$ is a prime ideal

Let $X \subset \mathbb{A}^1(\mathbb{R})$ be any subset. Then ideal of X is given by

$$I(X) = \{ f \in \mathbb{R}[x] \mid f(x) = 0 \text{ for all } x \in X \}.$$

But for any $x \in \mathbb{A}^1(\mathbb{R})$, $(x^2+1) \neq 0$

$\Rightarrow \nexists$ set $X \subset \mathbb{A}^1(\mathbb{R})$ such that

$x^2+1 = 0 \ \forall \ x \in X$

Therefore I is not ideal of any set in $\mathbb{A}^1(\mathbb{R})$ except empty set

$I(\phi) = \mathbb{R}[x]$

An ideal I of a ring R is finitely generated if there is a finite subset A of R such that $I = \langle A \rangle$

Every principal ideal is finitely generated.

Noetherian :

A ring R is Noetherian if and if every non-empty set of ideals of R contains a maximal element and if every ideal in the ring is finitely generated.

Example :- ① Any field (as the only ideals are 0 and the whole ring)

② All rings with a finite number of ideals like $\frac{\mathbb{Z}}{n\mathbb{Z}}$ for $n \in \mathbb{Z}$

③ The ring $\mathbb{Z}$

④ Noetherian ring are principal ideal domains like $\mathbb{Z}$, and $K[x]$, or finite.

Reducible algebraic sets :-

An algebraic set $V \subseteq A^n$ is reducible if $V = V_1 \cup V_2$ for some non-trivial (i.e non-empty) algebraic sets $V_1, V_2 \in A^n$ with $V \neq V_1$ and $V \neq V_2$ otherwise V is irreducible.

Theorem :- An algebraic set V is irreducible if and only if $I(V)$ is prime.

proof :- Let X is irreducible and suppose $f, g \in k[x_1, x_2, \ldots, x_n]$ are such that $fg \in I(X)$. Then $\langle fg \rangle \subseteq I(X)$

so $X = V(I(X)) \subseteq V(fg)$

$V(fg) = V(f) \cup V(g)$

$\Rightarrow X \cap V(fg) = (X \cap V(f)) \cup (X \cap V(g))$

$\Rightarrow X = (X \cap V(f)) \cup (X \cap V(g))$

By the irreducibility of X, we have

$$X = X \cap V(f) \quad \text{or} \quad X = X \cap V(g)$$

$$X = X \cap V(f) \subseteq V(f) \ldots$$

$$\Rightarrow X = V(f)$$

Now by using Hilbert Nullstellensatz theorem, we have

$$I(X) = I(V(f)) = \sqrt{(f)}.$$

since $f \in \sqrt{(f)} \Rightarrow f \in I(X)$

Therefore $I(X)$ is prime.

Note: $I(X) = \{ f \in k[x_1, \ldots, x_n] : f(p) = 0 \text{ for every } p \in X \}$

$X \subseteq V(g) \Rightarrow f$ vanishes on $X \Rightarrow f \in I(X)$

Q Show that $A^n(k)$ is irreducible if k is infinite.

Sol Let $V = A^n(k)$ be an algebraic

Let

If $I(V) = I(A^n(k)) = 0$

then $I(V)$ is zero ideal

in $k[x_1, x_2, \ldots, x_n] = A$

since $k[x_1, x_2, \ldots x_n]$ is an integral

domain.

$\Rightarrow \{0\}$ is prime if and only if the quotient

ring $A/\langle 0 \rangle$ is an integral domain.

Therefore $I(V)$ is prime ideal

$\Rightarrow A^n(k)$ is irreducible.

Q let $k = \mathbb{R}$. Show that $I(V(x^2+y^2+1)) = (1)$.

Sol. Since $x^2+y^2+1 = 0$ has no solution in

$$\mathbb{A}^2(\mathbb{R}) \Rightarrow V(x^2+y+1) = \phi$$

$$\text{so } I(V(x^2+y^2+1)) = I(\phi) = (1)$$
$$= \mathbb{R}[x,y]$$

Q. find the irreducible components of $V(y^2-xy-x^2y+x^3)$ in $\mathbb{A}^2(\mathbb{R})$ and also in $\mathbb{A}^2(\mathbb{C})$.

Sol. $V(y^2-xy-x^2y+x^3) = V((y-x)(y-x^2))$

$$= V(y-x) \cup V(y-x^2)$$

Since $V(y-x) = \{(t,t) \in \mathbb{A}^2(\mathbb{R}) \mid t \in \mathbb{R}\}$

$\Rightarrow I(V(y-x)) = (y-x)$ is prime.

similarly $V(y-x^2) = \{(t,t^2) \in \mathbb{A}^2(\mathbb{C}) \mid t \in \mathbb{C}\}$

$I(V(y-x^2)) = (y-x^2)$ is prime

Hence, the irreducible components of
$V(y^2 - xy - x^2y + x^3)$ in $\mathbb{A}^2(\mathbb{R})$ or in $\mathbb{A}^2(\mathbb{C})$
are the same i.e. $V(y-x)$ and $V(y-x^2)$

Square free polynomial :-

Let F be a field or an integral domain $\mathbb{Z}$.

A polynomial f in $F[x]$ is a square free polynomial if there is no polynomial g in $F[x]$ with $\deg(g(x)) > 0$, such that

$$g^2 \mid f$$

$\Rightarrow$ the polynomial doesn't have a factor of the form g^n with $n \geq 2$.

Example :- ① $f(x) = x^2 + 3x + 2$

$= (x+1)(x+2)$ is a Square free.

② $f(x) = x^4 + 7x^3 + 18x^2 + 20x + 8$

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

$f(x) = (x+1)\, g(x)^2$ where $g(x) = (x+2)$

$\Rightarrow g^2 \mid f$

$\Rightarrow f(x)$ is not square free.

Also, we can say that a square-free polynomial is a univariate polynomial over a field or an integral domain that has no multiple root in an algebraically closed field containing its coefficients.

Square-free integer :-

Square free integer is an integer which is divisible by no square number other than 1.

That is, its prime factorization has exactly one factor for each prime that appears in it.

Example :- ① $10 = 2 \cdot 5$ is square free

but $18 = 2 \cdot 3 \cdot 3$ is not square free

because 18 is divisible by $3^2 = 9$

$\Rightarrow$ 18 is divisible by square number

$\Rightarrow$ 18 is not square free.

② The smallest positive square free numbers are

1, 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19, 21

Theorem :-

Let k be a field and consider the polynomial ring

$R = k[x_1, \ldots, x_n]$.

Let $f \in R \setminus \{0\}$ then (f) is radical if and only if f factors into a product of irreducible polynomial of multiplicity 1.

proof :- We know that R is a UFD.

So let $f = f_1 \cdots f_m$ be a product of f into irreducible factors such that for all $i \neq j$, $(f_i) \neq (f_j)$. Then

$$(f) = (f_1 \cdots f_m)$$

$$= (f_1) \cap \cdots \cap (f_m)$$

(f) is an intersection of prime ideals of R and hence radical.

Also, f is a square free.

⇒ If K is a field, then $K[x]$ is a UFD and so (f) is radical ideal if and only if f is a square free.

Let $(P_1), \ldots, (P_n)$ be distinct prime ideals of a unique factorization domain, and let $k_1, k_2, \ldots, k_n$ be positive integer. Then the radical of $(P_1^{k_1} \ldots P_n^{k_n})$ is clearly $(P_1 \ldots P_2)$

Let $f(x)$ be a non-zero polynomial in $\mathbb{C}[x]$ then $(f) \subseteq \mathbb{C}[x]$ is a radical ideal iff $f(x)$ has no repeated roots.

Proof:- $g^m \in (f) = \{ h(x) f(x) : h(x) \in \mathbb{C}[x] \}$

$\Rightarrow g^m = h(x) f(x)$

$g^m = hf$ for some polynomial h,

Then each α_i must be a root of g^m.

where $f(x) = (x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)$.

Since ϕ is a field, that means that the α_i are root of g as well.

Therefore f must divide g.

$\Rightarrow g \in (f)$.

Therefore (f) is radical.

Q. $\langle x^2+y^2-1 \rangle$ is prime in $\mathbb{C}[x,y]$. True/False.

Sol True ; because $\mathbb{C}[x,y]$ is a U.F.D. In a UFD, a non-zero element is a prime if and only if it is irreducible.

x^2+y^2-1 is irreducible because there is no polynomial $f(y) \in \mathbb{C}[y]$ such that

$$f(y)^2 + y^2 - 1 = 0$$

Also, we can show that

$\frac{\mathbb{C}[x,y]}{\langle x^2+y^2-1 \rangle}$ is an integral domain.

let $u = x+iy$, $v = x-iy$

$\mathbb{C}[x,y]$ $\mathbb{C}[x+iy, x-iy]$

$\frac{\mathbb{C}[x,y]}{\langle x^2+y^2-1 \rangle}$

$$\frac{\mathbb{C}[x,y]}{\langle x^2+y^2-1 \rangle} \cong \frac{\mathbb{C}[u,v]}{\langle uv-1 \rangle}$$

$$uv = (x+iy)(x-iy) = x^2+y^2$$

$$\Rightarrow \quad \frac{\phi[u,v]}{\langle uv-1\rangle} \cong \phi\left[t, \frac{1}{t}\right]$$

$$\Phi : \phi[u,v] \longrightarrow \phi\left[t, \frac{1}{t}\right] \quad \phi\left[t, \frac{1}{t}\right]$$

$$\phi(u) = t, \quad \phi(v) = \frac{1}{t}$$

This homomorphism is surjective.

$$\text{Ker}\,\phi = \langle uv-1\rangle$$

$\langle x, y \rangle$ is a prime ideal of $k[x,y]$

Proof:- $\dfrac{k[x,y]}{\langle x,y \rangle} \cong \dfrac{\frac{k[x,y]}{\langle x \rangle}}{\frac{\langle x,y \rangle}{\langle x \rangle}}$

$$= \frac{k[y]}{\langle y \rangle} \cong k$$

k is an integral domain

$\Rightarrow \langle x,y \rangle$ is a prime ideal.

Q. x^2+y^2-1 is irreducible in $\mathbb{Q}[x,y]$

Sol: Let $\mathbb{Q}[x,y] = \mathbb{Q}[x].[y] = R[y]$ where $R = \mathbb{Q}[x]$

In $R = \mathbb{Q}[x]$, $x-1$ is irreducible.

Since $\mathbb{Q}[x]$ is U.F.D $\Rightarrow x-1$ is prime

We can see $x^2+y^2-1 = y^2 + (x+1)(x-1)$

prime $x-1 \in \mathbb{Q}[x]$ divide the constant term (x^2-1)

But Note that $y^2 + (x^2-1) \in \mathbb{Q}[x][y]$

but $(x-1)^2$ doesn't divides (x^2-1) constant term.

So by Eisenstein's Criterion with the prime $p = (x-1)$,

x^2+y^2-1 is Irreducible in ~~$R[xy]$~~ $R[y]$ where $R = \mathbb{Q}[x]$

Similarly we can show that x^2+y^2-1 is Irreducible in $\mathbb{C}[x,y]$.

$p \nmid a_n$.

$p^2 \nmid a_0$

① Decompose $V(x^2+y^2-1, x^2-z^2-1) \subset \mathbb{A}^3(\mathbb{C})$ into irreducible components.

Sol^n We know that a point $(x,y,z) \in \mathbb{C}^3$ is in the intersection iff $x^2+y^2-1=0$ and

$$x^2-z^2-1=0$$

In particular, we must have

$$\therefore x^2+y^2-1 = x^2-z^2-1=0$$

$$\Rightarrow y^2+z^2=0 \quad \Rightarrow y^2 = -z^2$$

$$z = \pm iy \quad \text{or} \quad y = \pm iz$$

Thus the point must lie on one of the two hyperplanes $V(z \pm iy)$.

On the other hand, suppose that (x,y,z) satisfies $x^2-z^2-1=0$

and $z = \pm iy$

$$\Rightarrow x^2 - (\pm iy)^2 - 1 = 0$$

$$\Rightarrow x^2+y^2-1=0$$

Thus, we see that we can describe the intersection as

$$V(x^2+y^2-1, z-iy) \cup V(x^2+y^2-1, z+iy)$$

Therefore,

$$V(x^2+y^2-1, x^2-z^2-1) = V(x^2+y^2-1, y^2+z^2)$$

$$= V(x^2+y^2-1, z-iy) \cup V(x^2+y^2-1, z+iy)$$

$$\boxed{V = V_1 \cup V_2}$$

By Hilbert Nullstellensatz, we have

$$I(V_1(I)) = I$$

$$I(V_1) = (x^2+y^2-1, z-iy)$$

$$\frac{\phi[x,y,z]}{I(V_1)} = \frac{\phi[x,y,z]}{\langle x^2+y^2-1, z-iy \rangle}$$

$$\frac{\phi[x,y,z]}{\langle z-r^2y\rangle} \cong \phi[x,y]$$

Since x^2+y^2-1 is irreducible polynomial

$$= \frac{\phi[x,y]}{\langle x^2+y^2-1\rangle}$$

$$\cong I(V_L) \text{ is prime}$$

$$\cong V_L \text{ is irreducible}$$

$$\frac{\phi[x,y]}{\langle x^2+y^2-1\rangle}$$

is integral domain

since $\frac{\phi[x,y,z]}{\langle h_i - z\rangle} \cong \phi[x,y]$

$$\frac{\langle h_i - z\rangle}{\langle h_i - z,\ 1-z^2+z^2\rangle}$$

$$\frac{\langle h_i - z\rangle}{[z,h,\kappa]\phi} =$$

Therefore, all irreducible components of

$V(x^2+y^2-1,\ x^2-z^2-1)$ are

$V(x^2+y^2-1,\ z+iy)$ and $V(x^2+y^2-1,\ z-iy)$

Note:

Every prime ideal of a ring is a radical ideal.

But converse is not true.

Def. Radical of a positive integer n is defined as product of the distinct prime numbers dividing n.

Each prime factor of n occurs exactly once as a factor of this product

$$\text{rad}(n) = \prod_{p \mid n} p$$

p prime

Take $R = \mathbb{Z}$, $n = 6$

Then $\text{rad}(n\mathbb{Z}) = \text{rad}(6\mathbb{Z})$

$= \sqrt{6\mathbb{Z}}$

$= r\mathbb{Z}$

$\text{rad}(n\mathbb{Z}) = \sqrt{n\mathbb{Z}} = r\mathbb{Z}$

where $r = \prod_{p \mid n} p$ and p is a prime number

$$\sqrt{6\mathbb{Z}} = (2.3)\mathbb{Z}$$
$$= 6\mathbb{Z}$$

But $6\mathbb{Z}$ is not a prime ideal

neither $2 \notin 6\mathbb{Z}$ nor $3 \notin 6\mathbb{Z}$

Q. Let $V = \{(t, t^2, t^3) \in \mathbb{A}^3(\mathbb{C}) \mid t \in \mathbb{C}\}$

find $I(V)$, and show that V is irreducible.

Sol^n

$$V = \{(t, t^2, t^3) \in \mathbb{A}^3\mathbb{C} \mid t \in \mathbb{C}\}$$

$$= V(x^2 - y, x^3 - z)$$

or

$$V = V(y - x^2, z - x^3)$$

V is an algebraic ~~set~~.

Take $I = \langle y - x^2, z - x^3 \rangle$

I is a prime ideal in $\mathbb{C}[x, y, z]$ if and only if the set

$$V = \{(x, y, z) \mid \in A^3(\mathbb{C}) \mid y = x^2, z = x^3\}$$

is an irreducible set in $A^3(\mathbb{C})$.

V can be parameterizes as:

$$V = \{(t, t^2, t^3) : ~~t \in \mathbb{C}~~ \; t \in \mathbb{C}\}$$

Therefore, it is possible to find a bijection

$f : \mathbb{A}^1(\mathbb{C}) \longrightarrow V$ by

$f(t) = (t, t^2, t^3)$

$t \longmapsto (t, t^2, t^3)$

$\Rightarrow$ f is an isomorphism

$V \cong \mathbb{A}^1(\mathbb{C})$

since $\mathbb{A}^1(\mathbb{C})$ is irreducible, V must be irreducible.

$\Rightarrow$ $I(V)$ is prime

$$\frac{k[x,y,z]}{\langle y-x^2, z-x^3\rangle} \cong \frac{k[x,y]}{\langle y-x^2\rangle} \cong k[x]$$

$\Rightarrow$ $\langle y-x^2, z-x^3\rangle$ is prime ideal since $k[x]$ is integral domain.

$\Rightarrow$ $I(V) = V$ by Hilbert Nullstellensatz since (x^2-y, x^3-z) is radical