HOW TO SHOW THAT A POLYNOMIAL IN $k[x,y]$ IS IRREDUCIBLE?

Recall the following definition:

Def: An irreducible algebraic set of $\mathbb{A}^n(k)$ is called an *affine variety*.

HOW TO SHOW THAT AN ALGEBRAIC SET IS A VARIETY?

k arbitrary field

If $V = V(I)$ where $I \subseteq k[x_1, \dots, x_n]$ then we proved that

$V(I)$ is irreducible (i.e. a variety) $\Leftrightarrow$ $I(V(I))$ is prime.

k algebraically closed

If k is algebraically closed, then, by the Hilbert's Nullstellensatz we have:

$V(I)$ is irreducible (i.e. a variety) $\Leftrightarrow$ $\mathrm{Rad}(I)$ is prime.

In particular, if V is an hypersurface of $\mathbb{A}^n(k)$, i.e. $V = V(F)$, $F \in k[x_1, \dots, x_n]$, then we have the following result.

Proposition: If k is algebraically closed then an hypersurface $V = V(F)$, $F \in k[x_1, \dots, x_n]$ is a variety if and only if F is irreducible in $k[x_1, \dots, x_n]$:

$V(F)$ is a variety $\Leftrightarrow$ F is irreducible

Proof

It is not difficult to show that $\mathrm{Rad}((F))$ is prime if and only if (F) is prime.

Moreover, $k[x_1, \dots, x_n]$ is an UFD. Therefore (F) is prime if and only if F is irreducible.

$\square$

Hence, the problem of showing that an hypersurface is irreducible, boils down to showing that a polynomial that describes it is irreducible.

We will consider this problem for hypersurfaces in $\mathbb{A}^2(x,y)$, i.e. curves in the plane.

HOW TO SHOW THAT A POLYNOMIAL IN TWO VARIABLES F(x,y) IS IRREDUCIBLE?

Basically there are two "methods":

① by using the definition of irreducible element

② by using some criterion of irreducibility ... EISENSTEIN!

We will apply both of these methods for proving that the circle $V(x^2+y^2-1) \subseteq \mathbb{A}^2(K)$ is a variety if K is algebraically closed and $\mathrm{char}(K) \neq 2$.

<u>Remark</u>: If $\mathrm{char}(K)=2 \Rightarrow x^2+y^2-1 = x^2+y^2+1 = (x+y+1)^2$
$\Rightarrow V(x^2+y^2-1)$ is <u>not</u> a variety.

① <u>Def</u>: Let R be an integral domain. A nonzero, nonunit element u is said to be IRREDUCIBLE if

$$u=ab,\ a,b \in R \Rightarrow \text{either } a \text{ or } b \text{ is a unit of } R.$$

Recall that, to any $F \in K[x_1,\dots,x_n]$ we can associate to F a nonnegative integer called the degree of F and denoted $\deg(F)$:

$$\deg(F) = \text{maximum of the degrees of all the terms in the polynomial}$$

<u>e.g.</u>: • The polynomial $2x^3y + xy + 3y^2 + 1 \in K[x,y]$ has degree 4.

• $\deg(F) = 0 \iff F \in K$ is a constant.

• $F \in K[x,y]$, $\deg(F)=1 \iff F(x,y) = ax+by+c$, $a,b,c \in K$, a and b non both zero.

<u>Remark</u>: $\deg(G \cdot H) = \deg(G) \cdot \deg(F)$.

So in $K[x,y]$ we have:

$$\{\text{units of } K[x,y]\} = K = \{F \in K[x,y] : \deg F = 0\}.$$

Remark: Sometimes it can be useful to consider an element of $K[x,y]$ as a polynomial of

$(K[y])[x]$: ring of polynomials with coefficients in $K[y]$

or

$(K[x])[y]$: ring of polynomials with coefficients in $K[x]$

In this way to each polynomial $F(x,y) \in K[x,y]$ we can also associate a degree in x and y:

$\deg_x(F(x,y))$ = degree of F as a polynomial in $(K[y])[x]$

$\deg_y(F(x,y))$ = degree of F as a polynomial in $(K[x])[y]$.

We have:

$$\max\{\deg_x(F(x,y)), \deg_y(F(x,y))\} \le \deg(F(x,y)).$$

e.g.: $F(x,y) = 2x^3y + xy + 3y^2 + 1$

$\rightarrow \underbrace{2y}_{\in K[y]} x^3 + \underbrace{y}_{\in K[y]} x + \underbrace{3y^2+1}_{\in K[y]} \in (K[y])[x] \Rightarrow \deg_x(F(x,y)) = 3$

$\rightarrow 3y^2 + (2x^3 + x)y + 1 \in (K[x])[y] \Rightarrow \deg_y(F(x,y)) = 2$

Remark: If $\deg(F) = 1 \Rightarrow F$ is irreducible.

Indeed, if F was reducible then

$$F = G \cdot H, \qquad \deg G, \deg H > 0.$$

$$\Rightarrow \underbrace{\deg(F)}_{= 1} = \underbrace{\deg(G) + \deg(H)}_{\geq 2} \Rightarrow 1 \geq 2. \ \lightning$$

Example

We will show now that x^2+y^2-1 is irreducible in $K[x,y]$ if $\mathrm{char}(K) \neq 2$.

Assume the x^2+y^2-1 is irreducible. Then there exist $G(x,y), H(x,y) \in K[x,y]$

$$x^2 + y^2 - 1 = G(x,y) \cdot H(x,y),$$

with $\deg(G), \deg(H) > 0$.

Then we get

$$2 = \deg(G) + \deg(H)$$
$$\Downarrow$$
$$\deg(G) = \deg(H) = 1$$

So $G(x,y) = a_1x + b_1y + c_1$ and $H(x,y) = a_2x + b_2y + c_2$.

We obtain:

$$x^2+y^2-1 = G(x,y)\cdot H(x,y) =$$
$$= (a_1x+b_1y+c_1)\cdot(a_2x+b_2y+c_2) =$$
$$= a_1a_2x^2 + (a_1b_2+a_2b_1)xy + b_1b_2y^2 + (a_1c_2+a_2c_1)x + (b_1c_2+b_2c_1)y + c_1c_2.$$

which implies that $(a_1, b_1, c_1, a_2, b_2, c_2)$ has to be a solution of the following system:

we can assume this

$$\begin{cases} c_1c_2 = -1 & \longrightarrow & c_1 = 1,\ c_2 = -1 \\ b_1c_2 + b_2c_1 = 0 & \longrightarrow & b_1 = b_2 \\ a_1c_2 + a_2c_2 = 0 & \longrightarrow & a_1 = a_2 \\ b_1b_2 = 1 & \longrightarrow & b_1^2 = 1 \Rightarrow b_1 \neq 0 \\ a_1b_2 + a_2b_1 = 0 & \longrightarrow & 2a_1b_1 = 0 \ \lightning \\ a_1a_2 = 1 & \longrightarrow & a_1^2 = 1 \Rightarrow a_1 \neq 0 \end{cases}$$

So x^2+y^2-1 is irreducible.

② **Recall**: EISENSTEIN'S CRITERION in $\mathbb{Z}[x]$

Let $f(x) = a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in \mathbb{Z}[x]$.

If there exists a prime number p such that:

- $p \mid a_i \ \forall\, i \neq n$.
- $p \nmid a_n$.
- $p^2 \nmid a_0$

then $f(x)$ is irreducible in $\mathbb{Z}[x]$ $\left(\overset{\text{Gauss's Lemma}}{\Longrightarrow} \text{ in } \mathbb{Q}[x]\right)$

e.g.: $f(x) = x^3+2x^2+2$ is irreducible in $\mathbb{Z}[x]$.
Eiseinstein's creterion applies with $p=2$.

There exists a genelized version of Eiseinstein's criterion which holds for every integral domain.

EISENSTEIN'S CRITERION (generalized version)

Let R be an integral domain and $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$.
If there exists a prime ideal $P \subseteq R$ such that:

- $a_i \in P \quad \forall\, i \neq n$.
- $a_n \notin P$
- $a_0 \notin P^2$

then $f(x)$ is irreducible in $R[x]$.

Remark: If R is an UFD, then for the irreducibility of $f(x)$ in $R[x]$ it is enough to show that there exists an irreducible element p such that $p \mid a_i \ \forall i \neq n$, $p \nmid a_n$, $p^2 \nmid a_0$.

We also have a generalized version of Gauss's lemma:

GAUSS'S LEMMA (generalized version).

Let R be a GCD domain and $F = \mathrm{Frac}(R)$ its field of fractions. Let $f(x)$ be a nonconstant polynomial in $R[x]$. Then:

f is irreducible in $R[x] \iff f$ is irreducible in $F[x]$ and f is primitive in $R[x]$

Remark

If f is not primitive the implication [f irreducible in $F[x]$ $\Rightarrow$ f irreducible in $R[x]$] is not true.

e.g. $R = \mathbb{Z}$, $F = \mathbb{Q}$.

$f(x) = 2x$ is irreducible in $\mathbb{Q}[x]$, but not in $\mathbb{Z}[x]$

(2 is irreducible in $\mathbb{Z}$, while it is a unit in $\mathbb{Q}$).

Example

Let us consider $x^2+y^2-1 \in K[x,y] = (K[y])[x]$.

We will apply the generalized version of Eiseinstein's criterion. In our case we can choose $R = K[y]$.

Now, $y-1$ is an irreducible element of $R=K[y]$ such that:

- $y-1 \mid y^2-1$;
- $y-1 \nmid 1$;
- $(y-1)^2 \nmid y^2-1$.

So x^2+y^2-1 is irreducible in $R[x] = K[y][x] = K[x,y]$.

We get, as a bonus, that x^2+y^2-1 is also irreducible in $K(y)[x]$!

<u>Remark</u>: The Eiseinstein's criterion is normally "faster" to apply, but it has the downside that it does not apply to any irreducible polynomial