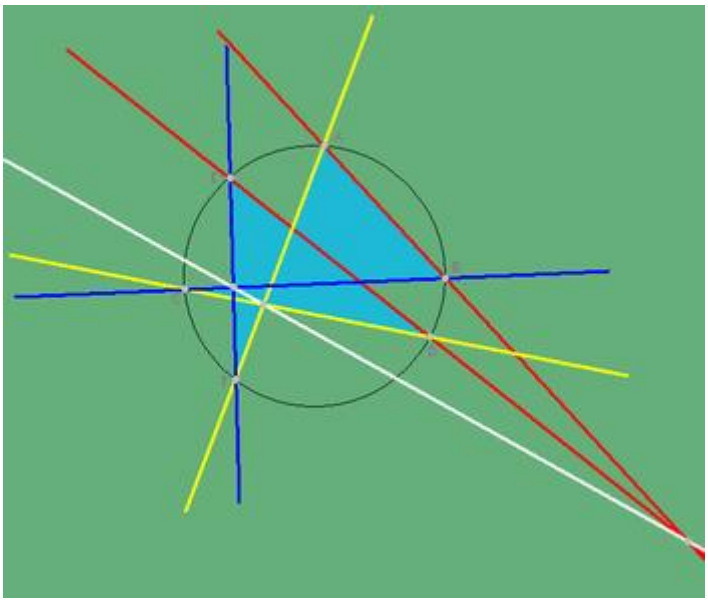
INTRODUCCIÓN AL ESTUDIO DE LAS CURVAS ALGEBRAICAS

Coordinadora: Concepción Romo Santos



INTRODUCCIÓN

A finales del siglo XIX los expertos en Álgebra Conmutativa estudiaban las curvas algebraicas en el plano proyectivo complejo, usando para ello métodos de geometría proyectiva, probablemente se había desarrollado con Abel, Jacobi, Weierstrass y Riemann la teoría de “funciones algebraicas” de una variable compleja. Es evidente la importancia de esta teoría en el desarrollo del estudio de curvas algebraicas planas, pero los métodos utilizados para el estudio de funciones algebraicas eran sobre todo de naturaleza trascendente incluso antes de Riemann. Con éste se acentúa más este carácter de trascendencia con la introducción de las superficies de Riemann y de funciones analíticas cualesquiera definidas sobre dichas superficies.

Después de la muerte de Riemann, Roch y Clebsch reconocieron que de los resultados obtenidos por los métodos trascendentes de Riemann se pueden obtener numerosas aplicaciones a la geometría proyectiva de curvas, lo cual incitó a los geómetras de aquella época a hacer demostraciones de aquellos resultados, puramente geométricas. En esta línea siguieron Gordan, Brill y M. Noëther. Pero estos razonamientos geométrico-analíticos no reposaban sobre fundamentos ciertos y es esencialmente para dar a la teoría de curvas algebraicas una base sólida, que Dedekind publica en 1.882 su gran memoria sobre este tema. La idea principal de su trabajo es la de abordar este tema desde el punto de vista afín, diferencia esencial con sus contemporáneos que consideraban invariablemente las curvas algebraicas sumergidas en el espacio proyectivo complejo.

En el mismo año 1.882 aparece también la memoria de Kronecker, mucho más ambiciosa que la de Dedekind pero también más vaga y más obscura. Su tema central es el estudio de los ideales de un álgebra finita íntegra sobre los anillos de polinomios C[ ] y Z[,…,].

Era natural asociar a cada ideal de estos anillos la variedad algebraica formada por los ceros comunes a todos los elementos del ideal. Los estudios realizados en el siglo XIX en las geometrías de dimensión 2 y de dimensión 3 conducen intuitivamente a la idea de que toda variedad es unión de un número finito de variedades irreducibles. La demostración de este hecho es el fin que se propone Kronecker aunque explícitamente en ninguna parte de su memoria se encuentra la definición de variedad irreducible y de dimensión. Tampoco se sabe si Kronecker tenía el concepto actual de ideal primo.

Es Lasker quien en su memoria define correctamente el concepto de variedad irreducible así como el concepto de dimensión. En las interesantes consideraciones históricas que inserta en su trabajo, Lasker indica que se basa no solamente en la tendencia puramente algebraica de Kronecker y Dedekind sino también en los métodos geométricos de la escuela de Clebsch y M. Noether y sobre todo en el famoso teorema demostrado por éste último en 1.873 publicado en Math. Ann. T. VI pág. 351-359, generalizado por Hilbert en 1.893, en su célebre “teorema de los ceros”. Sin duda, inspirado en este resultado, Lasker introduce en su memoria el concepto de ideal primario en los anillos C[,…,] y Z[ ] y demuestra la existencia de una descomposición primaria para todo ideal de estos anillos., aunque no se preocupa de la unicidad de esta descomposición. Es muy importante señalar que Lasker en esta memoria extiende los resultados anteriores al anillo de las series

enteras convergentes en el entorno de un punto, apoyándose para ello en el teorema preparatorio de Weirstrass.

Terminamos de mencionar a Hilbert, hablemos un poco de su obra. Hilbert escribió dos memorias, en 1.890 y 1.893. En la primera demuestra el teorema de la base de Hilbert que nos dice que todo ideal del anillo de polinomios está finitamente generado. La segunda memoria contiene el célebre Nullstellensatz, el cual establece una correspondencia biunívoca entre los ideales maximales del anillo K[,] siendo K un cuerpo algebraicamente cerrado y los puntos del espacio afín y también una correspondencia biunívoca entre los ideales primos del anillo K[,…,] y las variedades algebraicas irreducibles de .

De lo explicado anteriormente se deduce que gracias a Hilbert la teoría de curvas algebraicas experimentó un importante avance.

El objetivo de este libro es exponer algunos de los trabajos realizados en el curso de “Curvas Algebraicas” de la Facultad de Matemáticas de la Universidad Complutense de Madrid durante el curso académico 2.010-2.011.

Concepción Romo Santos

Catedrática de Álgebra

Facultad de Matemáticas

Universidad Complutense

ANILLOS DE VALORACIÓN. TEOREMA DE LOS CEROS DE HILBERT

DEFINICIONES PREVIAS:

1. ANILLO:

Un ANILLO A es un conjunto A con dos operaciones internas + y ., tal que:

-(A,+) grupo abeliano

-(A, .) semigrupo

-Distributivo

Si el producto de dos elementos es conmutativo entonces es A ANILLO CONMUTATIVO.

2. ANILLO LOCAL:

Es un anillo A que tiene exactamente un ideal maximal p.

3. SUBANILLO:

A anillo, un SUBANILLO DE A es B A tal que:

(B,+) < (A,+) y el producto es cerrado en B, $\Leftrightarrow$ B$\neq$ y para todo a, b$\in$B:

a-b$\in$ B y ab$\in$B

4. DOMINIO DE INTEGRIDAD:

A es DOMINIO DE INTEGRIDAD (D.I) Si A es anillo conmutativo con unidad y sin divisores de cero.

5. CUERPO DE FRACCIONES:

Si A es D.I, y S=A-{0} entonces el cuerpo S^1A se llama CUERPO DE FRACCIONES.

6. IDEAL MAXIMAL:

Sea A un anillo conmutativo con unidad, I ideal de A, diremos que I ES UN IDEAL MAXIMAL cuando verifique:

Si J es otro ideal de A tal que $I \subseteq J \subset A$ entonces necesariamente J=A ó J=I.

7. CUERPO ALGEBRAICAMENTE CERRADO:

Diremos que un cuerpo K es ALGEBRAICAMENTE CERRADO cuando todo polinomio no constante con coeficientes en K posee una raíz perteneciente al cuerpo K.

Por ejemplo: Q o R no son algebraicamente cerrado porque $x^2+1=0$ no tiene raíces en Q o R.

8. ELEMENTO MAXIMAL

Sea $(P, \leq)$ un conjunto parcialmente ordenado; $m \in P$ es un elemento maximal de P si el único $x \in P$ tal que $m \leq x$ es $x = m$.

9. EXTENSIÓN ALGEBRAICA FINITA

Una EXTENSION DE CUERPO L/K se dice ALGEBRAICA si cada elemento de L es algebraico sobre K, i.e. si cada elemento de L es una raíz de algún polinomio distinto de cero con coeficientes en K. Las extensiones de cuerpos que no son algebraicas, i.e. que contienen elementos trascendentes son llamadas transcendentes.

Por ejemplo, la extensión de cuerpos R/Q es trascendente, mientras que las extensiones de cuerpos C/R y Q(√2)/Q son algebraicas.

10. CLAUSURA ALGEBRAICA

La CLAUSURA ALGEBRAICA de un cuerpo *K* es una extensión algebraica de *K* que sea algebraicamente cerrada.

DEFINICIÓN:

Sea R un dominio de integridad, K su cuerpo de fracciones. R es UN ANILLO DE VALORACIÓN DE K si para cada $x \neq 0$ ó $x \notin R$ ó $x^{-1} \in R$ ambos.

PROPOSICIÓN 1:

(i)R es un anillo local

(ii)Si R' es un anillo tal que $R \subset R' \subseteq K$, entonces R es un anillo de valoración

(iii)R es íntegramente cerrado (en K)

DEMOSTRACIÓN:

(i)Sea p el conjunto de elementos que no son unidades de R, es decir:

$x \in p$ si y solo si $x = 0$ ó $x^{-1} \notin R$.

- Sea $a \in R$, $x \in p$ entonces $ax \in p$, ya que en caso contrario $(ax)^{-1} \in R$ y Por tanto $x^{-1} = a(ax)^{-1} \in R$.

- Sean $x, y \in p$ elementos no nulos, entonces $xy^{-1} \in R$ o $x^{-1}y \in R$, por ser anillo de valoración y ser un elemento el inverso del otro.
  Si $xy^{-1} \in R$ $\quad x+y= (1 + xy^{-1}) y \in Rp \subset p$

Si $x^{-1}y \in R$ $\quad x+y= (1 + x^{-1}y)\, x \in Rp \subset p$

Por tanto p es un ideal con la propiedad de que si $x \in R - p$, $x^{-1} \in R$, x es una unidad en R, luego cualquier otro ideal propio de R estará contenido en p.
p es un ideal maximal y por consiguiente es un anillo local.

(ii) Es claro por definición.

(iii) Sea $x \in K$, entero sobre R, es decir:

$x^n + b_1 x^{n-1} + \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots + b_{n-1}x + b_n = 0$, $b_i \in R$

Si $x \in R$ ya estaría probado.

Si $x \notin R$, $x^{-1} \in R$, multiplicando por x^{-n+1}:

$x + b_1 + \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots + b_{n-1}x^{2-n} + b_n x^{1-n} = 0$

$x = -(b_1 + b_2 x^{-1} + \ldots\ldots\ldots\ldots\ldots\ldots + b_{n-1}x^{2-n} + b_n x^{1-n}) \in R$

Sea K un cuerpo, Ω un cuerpo algebraicamente cerrado.

Sea $\sum$ el conjunto de todos los pares (R, f) donde R es un subanillo de K

Y $f: R \to \Omega$ un homomorfismo.

Se puede ordenar parcialmente este conjunto:

$(R, f) \leq (R', f') \Leftrightarrow R \subset R'$ $\quad f'/ R \equiv f$

$\sum$ es no vacio y claramente satisface las condiciones del lema de Zorn, *(LEMA: Todo conjunto parcialmente ordenado no vacío en el que toda cadena tiene una cota superior, contiene al menos un elemento maximal)*

por tanto $\sum$ tiene un elemento maximal: (B,g).

Se quiere probar que B es un anillo de valoración de K. El primer paso de esta demostración:

LEMA 1:

B es un anillo local y p = ker (g) es su ideal maximal.

DEMOSTRACIÓN:

Como g(B) es un subanillo de un cuerpo y por tanto dominio de integridad el ideal p=ker(G) es primo. Se puede extender g a un homomorfismo.

$\overline{g}$: Bp $\rightarrow \Omega$ poniendo $\overline{g}$ (b/s)=g(b) /g(s) para todo b $\in$ B y todo s $\in$ B

g(s) $\neq$ 0

Puesto que el par (B, g) es maximal se deduce que B = Bp, por tanto B es un anillo local y p es su ideal maximal.

..Bp siempre es anillo local y p es su ideal maximal ..

LEMA 2:

Sea x un elemento no nulo de K. Sea B[x] el subanillo de K generado por x sobre B y sea p[x] la extensión de p en B[x]. Entonces o p[x] $\neq$ B[x] o

$P[x^{-1}] \neq B[x^{-1}]$.

DEMOSTRACIÓN:

Supongamos p[x]=B[x] ya $p[x^{-1}]=B[x^{-1}]$

Se tendría entonces las siguientes ecuaciones:

$U_0 + U_1 x + \ldots\ldots\ldots\ldots + U_m x^m = 1$ ($U_i \in$ p) (1)

$V_0 + V_1 x^{-1} + \ldots\ldots\ldots\ldots + V_n x^{-n} = 1$ ($V_i \in$ p) (2)

en las que se puede suponer que los grados m, n son los menores posibles.

Considerando $m \leq n$ se multiplica (2) por x^n :

$V_1 x^{n-1} + \ldots\ldots\ldots\ldots + V_n = (1- V_0) x^n$ (3)

Puesto que V_0 p se deduce del lema anterior que 1- V_0 es una unidad ya que 1- $V_0 \notin$ p y si un elemento no es una unidad debe estar contenido en un ideal maximal.

Luego (3) se puede escribir de la forma:

$x^n = W_1x^{n-1}+\ldots\ldots\ldots+W_n \quad (W_j \in p)$

Por tanto se puede sustituir x^m en (1) por:

$W_1x^{m-1}+\ldots\ldots\ldots\ldots\ldots w_nx^{m-n}$ contradiciendo la minimalidad del exponente m.

TEOREMA 1:

Sea (B, g) un elemento maximal de Σ . Entonces B es un anillo de valoración del cuerpo K.

DEMOSTRACIÓN:

Sea x un elemento de K, por el lema 2 podemos suponer que p[x] no es el ideal de un anillo:

B' =B[x] luego p[x] está contenido en un ideal maximal p' de B' de modo que $p' \cap B = p$ (puesto que $p' \cap B$ es un ideal propio de B y contiene a p).

Por tanto la inclusión de B en B' induce una inclusión del cuerpo C =B/p en el cuerpo C' =B'/p'=B[x]/p' entonces C' =C[$\bar{x}$] donde $\bar{x}$ es la imagen de x en C' luego $\bar{x}$ es algebraico sobre C y por tanto C' es una extensión algebraica finita de C.

El homomorfismo g induce ahora una inclusión $\bar{g}$ de $C \to \Omega$ puesto que en virtud del Lema 1 (p) es el núcleo de g.

Puesto que Ω es algebraicamente cerrado $\bar{g}$ se puede extender a una inclusión $\bar{g}'$ de C' en Ω.

Componiendo $\bar{g}'$ con el homomorfismo natural B' $\rightarrow$ C' se tiene g': B' $\rightarrow \Omega$ que extiende a g. Puesto que el par (B, g) es maximal se deduce que B' =B y por tanto x $\in$ B.

<u>COROLARIO 1:</u>

Sea R un subanillo de un cuerpo K. Entonces la clausura íntegra $\bar{R}$ de R

en K es la intersección de todos los anillos de valoración de K que contienen a R.

DEMOSTRACIÓN:

Sea B un anillo de valoración de K tal que R $\subseteq$ B. Entonces por la proposición 1 (iii) se tiene que B es íntegramente cerrado, y se deduce que $\bar{R} \subseteq$ B.

Recíprocamente, sea $x \notin \bar{R}$. Entonces x no pertenece al anillo

R' = R $[x^{-1}]$, ya que:

Si $x \in R'$, $x = a_0x^{-n} + a_1x^{-n+1} + \ldots + a_n$

$x^{n+1} = a_0 + a_1x + \ldots + a_nx^n \Rightarrow x \in \bar{R} \Rightarrow$ ¡contradicción!

Luego x^{-1} no es una unidad en R' y por tanto está contenido en un ideal maximal p' de R'.

Sea Ω una clausura algebraica del grupo K' = R'/p'.

Entonces la restricción de R al homomorfismo natural R' en K' define un homomorfismo de R en Ω.

$\pi \mid \quad : \quad R \longrightarrow R/p' \subset \Omega$

$\mid R \qquad\quad a \longrightarrow a + p'$

Por el teorema 1, $(R, \pi/R)$ se puede extender a algún anillo de valoración

$B \supseteq R$.

Puesto que x^{-1} se aplica en el cero ($x^{-1} \to x^{-1} + p' = p'$), se deduce que $x \notin B$.

PROPOSICIÓN 2:

Sean $R \subseteq R'$ dominios de integridad, R' de generación finita sobre R. Sea v un elemento no nulo de R'. Entonces existe $u \neq 0$ en R con la siguiente propiedad: cada homomorfismo f de R en un cuerpo algebraicamente cerrado Ω tal que

$f(u) \neq 0$ se puede extender a un homomorfismo g de R' en Ω tal que $g(v) \neq 0$.

DEMOSTRACIÓN:

Por inducción respecto al número de generadores de R' sobre R se reduce inmediatamente al caso en que R' es generado sobre R por un solo elemento x.

(i) Si se supone que x es trascendente sobre R, es decir que ningún polinomio no nulo con coeficientes en R tiene a x como raíz.
Sea $v = a_0x^n + a_1x^{n-1} + \ldots + a_n$, y tómese $u = a_0$.
Entonces si $f: R \longrightarrow \Omega$ es tal que $f(u) \neq 0$, existe entonces $\xi \in \Omega$ tal que $f(a_0)\xi^n + f(a_1)\xi^{n-1} + \ldots + f(a_n) \neq 0$, puesto que Ω es infinito.

Defínase entonces $g: R' \longrightarrow \Omega$ que extiende a f poniendo $g(x)=\xi$.
Entonces $g(v) \neq 0$ conforme al enunciado.

(ii) Supóngase ahora que x es algebraico sobre R (es decir sobre el cuerpo de fracciones de R). Entonces también lo es v^{-1}, puesto que v es un polinomio en x.

Por tanto, se tienen ecuaciones de la forma:

$a_0x^m + a_1x^{m-1} + \dots + a_m = 0 \quad (a_i \in R) \qquad (1)$

$a_0v^{-n} + a_1v^{1-n} + \dots + a_n = 0 \quad (a_j \in R) \qquad (2)$

Sea $u = a_0a_0'$ y sea $f: R \longrightarrow \Omega$ tal que $f(u) \neq 0$.

Entonces f se puede extender primero a un homomorfismo

$f_1: R[u^{-1}] \longrightarrow \Omega$

(con $f_1(u^{-1}) = f(u)^{-1}$), y después, por el teorema 1, a un homomorfismo

$h: B \longrightarrow \Omega$ donde B es un anillo de valoración que contiene a $R[u^{-1}]$.

Por (1), x es entero sobre $R[u^{-1}]$, y por el corolario 1 $x \in B$, de manera que B contiene a R', y en particular $v \in B$. Por otra parte, por (2), v^{-1} es entero sobre $R[u^{-1}]$ y por tanto por el corolario 1 también está en B.

Por consiguiente, v es una unidad en B, y por tanto $h(v) \neq 0$.

Basta tomar entonces g como la restricción de h en R'.

COROLARIO (**Teorema de los ceros de Hilbert**):

Sea K un cuerpo y B una K-álgebra con generación finita.

Si B es un cuerpo, entonces es una extensión algebraica finita de K.

DEMOSTRACIÓN:

Basta considerar R=K, v=1, y Ω = la clausura algebraica de K, $\overline{K}$, en la proposición anterior

Sea $g: B \rightarrow \overline{K}$, $g(1) \neq 0$. B es un cuerpo (y todo homomorfismo de cuerpo

distinto del cero es inyectivo), se tiene que $K \subseteq B \subseteq \overline{K}$ y necesariamente B es una extensión algebraica.

B es algebraico y de generación finita.

VARIEDAD DE UNIDEAL

Mª José Lara Puente

Rebeca José Calvo

Consideramos, a partir de ahora, un cuerpo C algebraicamente cerrado, y pasaremos a formalizar el concepto de Variedad Algebraica en el espacio afín C^n.

DEFINICIÓN 1:

Dado un número finito de polinomios, $f_1, f_2, ..., f_s$, del anillo $R_n = x_1, ..., x_n$, definiremos variedad algebraica en el espacio afín C^n, como el conjunto de puntos de C^n que satisfacen a las ecuaciones algebraicas:

$$f_1 = 0, f_2 = 0, ..., f_s = 0$$

Por tanto, toda variedad algebraica V, de C^n, puede expresarse como el conjunto

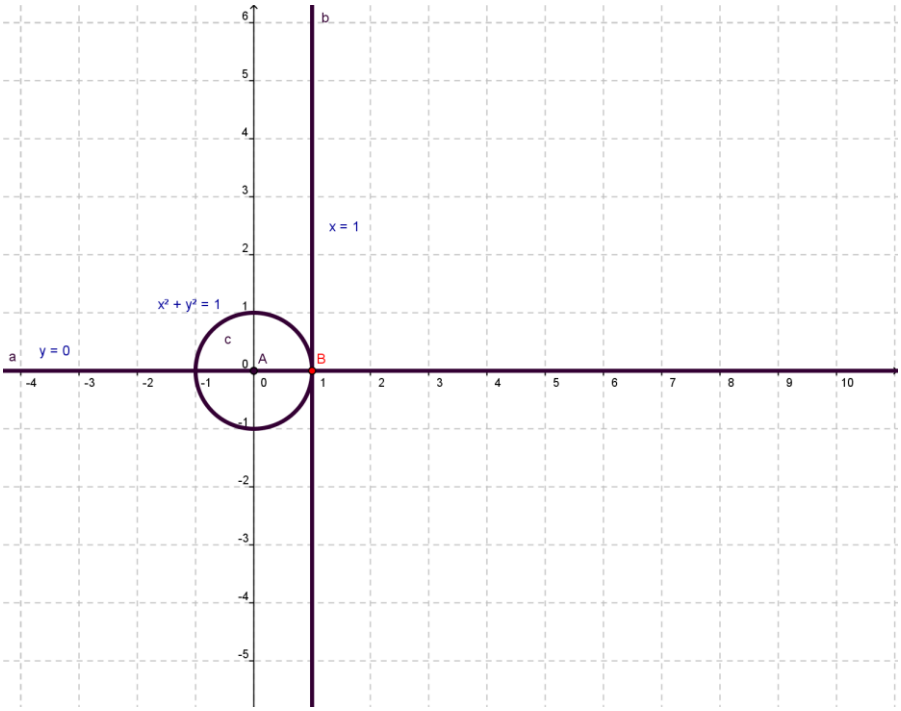
V={ $x \in C^n$ / $\exists S \subset R_n$: card(S) es finito y f(x)=0, $\forall f \in S$ }

*EJEMPLO 1: La variedad algebraica de C^2,constituida por el único punto (1,0), representa el conjuntos de puntos que satisfacen las ecuaciones algebraicas:

$$f_1 = x_2 = 0$$
$$f_2 = x_1^2 + x_2^2 - 1 = 0$$
$$f_3 = x_1 - 1 = 0$$

Con $f_1, f_2, f \in R_2$

Geométricamente, es la intersección de las rectas $x_2 = 0, x_1 = 1$, y la circunferencia de centro (0,0) y radio 1: $x_1^2 + x_2^2 = 1$



*EJEMPLO 2 : Una variedad algebraica del espacio afín C^3, sería por ejemplo, las dos circunferencias que surgen de la intersección de la esfera de radio 2 y centro (0,0,0) $x_1^2 + x_2^2 + x_3^2 = 4$ y $x_1^2 + x_2^2 = 1$. Pues es el conjunto de puntos que satisfacen las ecuaciones algebraicas:

$f_1 = 0$, $f_2 = 0$, siendo $f_1 = x_1^2 + x_2^2 + x_3^2 - 4$, $f_2 = x_1^2 + x_2^2 - 1$ elementos del anillo de polinomios R_3.

Tengamos en cuenta que no todos los subconjuntos de C^n son variedades algebraicas. Así, en C^2, el conjuntos de puntos de un segmento no es una variedad algebraica, pues no existe un conjunto finito de polinomios de $R_2 = C\ x_1, x_2$, que dé lugar a un conjunto de ecuaciones algebraicas, cuya solución sea el conjunto de puntos del segmento, y ningún otro punto. Los puntos, rectas, circunferencias, elipses y parábolas, sí son variedades algebraicas de C^2.

DEFINICIÓN 2:

Dado un ideal U del anillo de polinomios R_n, llamaremos Variedad del Ideal U, que representamos por V(U), al conjunto de puntos de C^n, en los que se anulan todos los polinomios de U, es decir:

$$V(U)=\{ x \in C^n \,/\, f(x)=0, \forall f \in U \}$$

Tal variedad coincide con la definida por los polinomios que constituyen una base cualquiera de U, en el sentido que dimos de variedad algebraica de la definición 1. Ya que si U es un ideal de R_n, sabemos que existe un número finito de polinomios de R_n, S={ $f_1, f_2, ..., f_s$ } tal que S es una base de U. Luego la Variedad del Ideal U, según la definición 2 sería el conjunto:

$$V(U)=\{ x \in C^n \,/\, f(x)=0, \forall f \in U = R_n(f_1, ..., f_s) \}$$

y la variedad algebraica definida por S, según la definición 1 sería:

$$\{ x \in C^n \,/\, f_i(x)=0, i=1,2,...,s \}$$

y evidentemente estos dos conjuntos son iguales.

Así si por ejemplo, V es la variedad definida en el ejemplo 2, entonces los polinomios : $f_1 = x_1^2 + x_2^2 + x_3^2 - 4$, $f_2 = x_1^2 + x_2^2 - 1$ se anulan en cualquier punto de V. Si consideramos el ideal U del anillo R_3, generado por f_1, f_2, entonces todos los polinomios de U se anulan en cualquier punto de V. Por lo tanto la variedad V coincide con el conjunto de puntos de C^3, que anulan a todos los polinomios del ideal $U = R_3(f_1, f_2)$.

Denotemos por $J(R_n)$ al conjunto de ideales del anillo R_n, y sea $P(C^n)$ el retículo de las partes del conjunto C^n. Definamos la aplicación V siguiente:

$V : J(R_n) \to P(C^n)$

que a cada ideal U de $J(R_n)$, le hace corresponder la variedad algebraica de C^n, V(U)=variedad del ideal U (de la definición 2).

PROPIEDADES:

Propiedad 1:

Dados U, U' elementos de $J(R_n)$, si U' contiene a U, entonces V(U) contiene a V(U').

En efecto si U es un ideal de R_n, entonces existen polinomios: $f_1, f_2, ..., f_s$ tales que $U = R_n(f_1, f_2, ..., f_s)$, y si U' contiene a U, los f_i son elementos de U', luego dado P de V(U'): $f_i(p) = 0$ para todo i=1,...,s, es decir, $P \in V(U)$

Propiedad 2:

La aplicación V definida anteriormente no es inyectiva, es decir, dos ideales distintos de R_n pueden definir la misma variedad en C^n.

Veamos un contraejemplo:

Los ideales $U = R_2(x_1^3, x_2)$, $U' = R_2(x_1, x_2^2)$ del anillo de polinomios R_2, son distintos, pues $x_1^3 \in U$ y $x_1^3 \notin U'$ y $x_2^2 \in U'$ y $x_2^2 \notin U$, sin embargo las variedades algebraicas de tales ideales consisten en el punto (0,0)

V(U)=V(U')={(0,0)}

Veamos a continuación algunos ejemplos relativos a estos dos resultados.

a) Los ideales de R_2 siguientes
$U = R_2(x_1^2 + x_2^2 - 4, x_1 - 1)$ y $U' = R_2(x_1^2 + x_2^2 - 4, x_1^2 + x_2^2 - 4x_1)$ definen la misma variedad de C^2.

La variedad V(U) está constituida por el conjunto de puntos de C^2 que son solución del sistema de ecuaciones algebraicas:

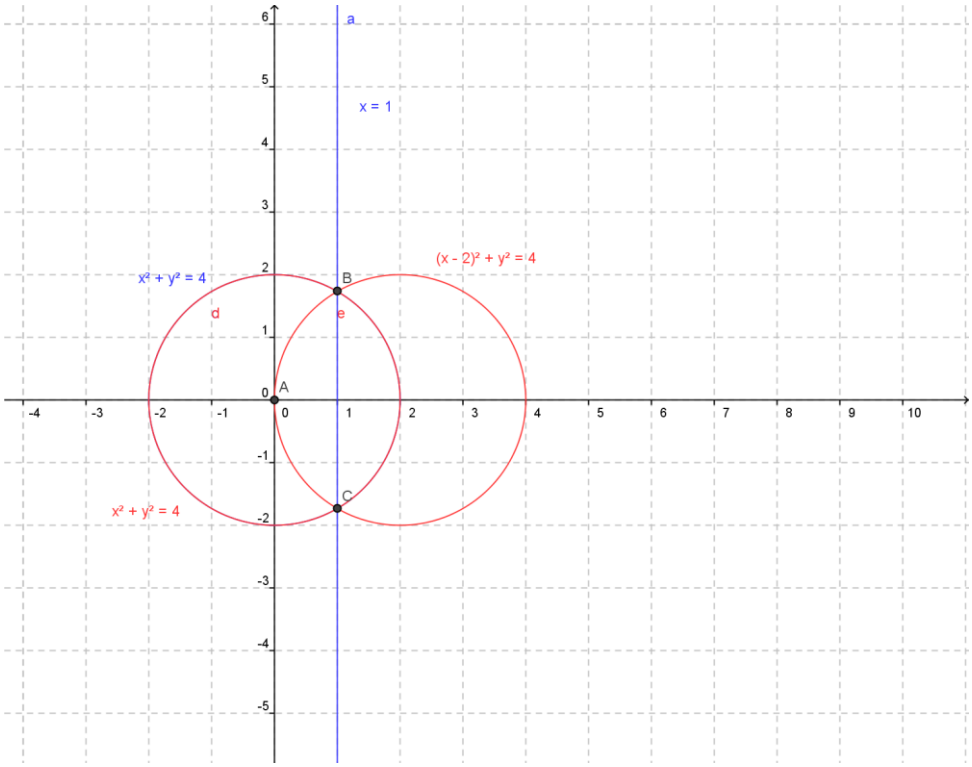
$$x_1^2 + x_2^2 - 4 = 0$$
$$x_1 - 1 = 0$$

ó intersección de la circunferencia de centro (0,0) y radio 2 y la recta $x_1 = 0$. Es decir:

$V(U) = (1, +\sqrt{3}), (1, -\sqrt{3})$ Por otra parte la variedad del ideal de U' serán los puntos de C^2 que son solución del sistema:

$$\left\{ \begin{array}{l} x_1^2 + x_2^2 - 4 = 0 \\ x_1^2 + x_2^2 - 4x_1 = 0 \end{array} \right\}$$

el cual representa la intersección de la circunferencia de centro (0,0) y radio 2 con la circunferencia de centro (2,0) y radio 2, resultando la solución del tal sistema los puntos $(1, +\sqrt{3})$ y $(1, -\sqrt{3})$. Luego, efectivamente V(U)=V(U').

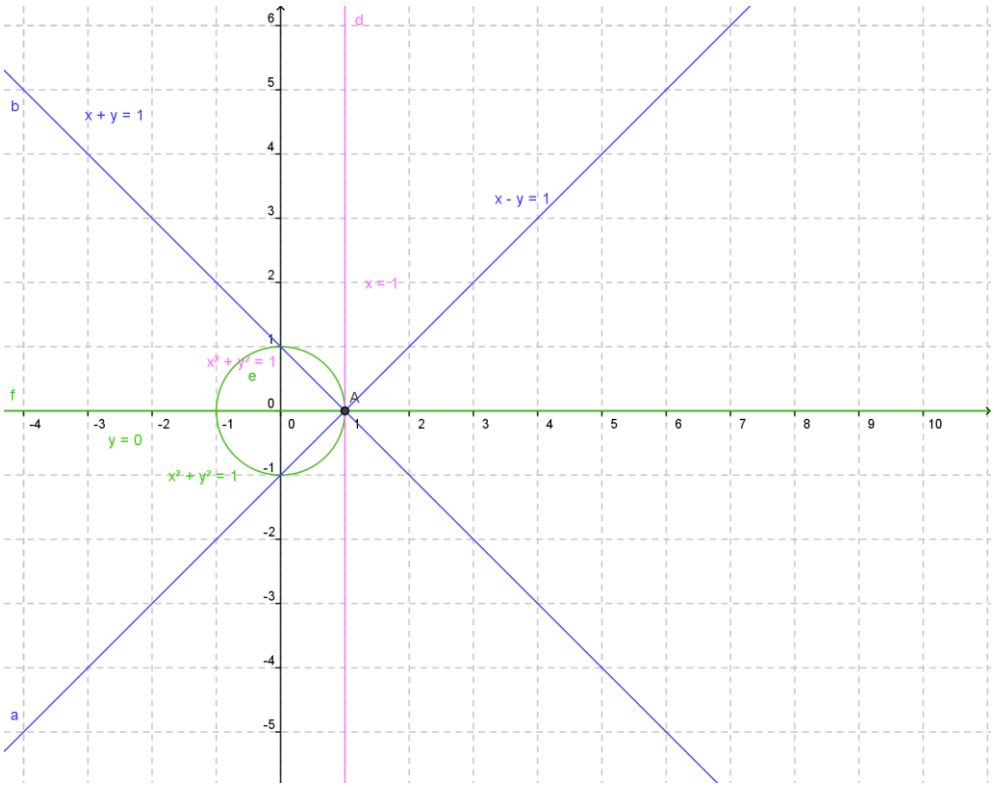


b) Sean $U = R_2(x_1 - x_2 - 1, x_1 + x_2 - 1)$; $U' = R_2(x_1^2 + x_2^2 - 1, x_1 - 1)$;
$U'' = R_2(x_1^2 + x_2^2 - 1, x_2)$, ideales del anillo R_2.

La variedad algebraica definida por V(U) está constituida por el único punto (1,0), intersección de las rectas: $x_2 = x_1 - 1$, $x_2 = 1 - x_1$, tal variedad coincide con V(U') pues es la intersección de la circunferencia de centro (0,0) y radio 1: $x_1^2 + x_2^2 = 1$, y la recta $x_1 = 1$. Por otra parte V(U'') está constituida por los puntos de C^2 solución del sistema:

$$\left\{\begin{matrix} x_1^2 + x_2^2 - 1 = 0 \\ x_2 = 0 \end{matrix}\right\}$$

Que son los puntos (1,0), (-1,0). Luego V(U'') contiene a V(U)=V(U'), y tenemos así un contraejemplo del recíproco de la propiedad 1, pues U'' no está contenido en U'($x_2 \in U''$ y $x_2 \notin U'$)



c) Los ideales U= $R_3(X_1)$, U'= $R_3(X_1, X_2)$, U''= $R_3(X_1, X_2, X_3)$ del anillo de polinomios R_3 verifican, de manera trivial: $U \supset U' \supset U''$, y también las variedades algebraicas del espacio afín C^3 verifican:. $V(U'') \supset V(U') \supset V(U)$.

La variedad V(U) está constituida por los puntos de C^3 que verifican X_1 =0, es decir, geométricamente es el plano determinado por los ejes X_2, X_3. Este plano contiene al eje X_3 representado por las ecuaciones X_1=0, X_2=0 que nos da la variedad V(U'), que a su vez contiene al origen de coordenadas (0,0,0), que es solución de X_1=0, X_2=0, X_3=0, ó variedad V(U'').

d) Los ideales: $U = R_2(X_1^2, X_2^2)$
$U' = R_2(X_1, X_2^2)$
$U'' = R_2(X_1, X_{2)}$
verifican: $U \subset U' \subset U''$, sin embargo las variedades algebraicas definidas por tales ideales coinciden: V(U)=V(U')=V(U'')=(0,0).

Propiedad 3:

La variedad definida por el ideal nulo (0)= $R_n(0)$ es el espacio afín C^n, es decir $V(R_n(0)) = C^n$.

Evidentemente todo punto de C^n se anula en el polinomio idénticamente cero.

Propiedad 4:

La variedad definida por el ideal impropio $R_{n'}$ del anillo R_n es el conjunto vacío, es decir: $V(R_n) = \varnothing$.

Efectivamente, no existe ningún elemento de C^n que anule a todos y cada uno de los polinomios de R_n

INTRODUCCIÓN A LA TEORÍA DE CUERPOS

-Dominios de factorización única y dominios euclídeos.

• **Notación**: A lo largo de esta exposición , ***A*** designará un dominio de integridad ó anillo.

• **Definición:** Sean a, b Є ***A;*** diremos que “a divide a b” (a|b) si y sólo si a≠0 y existe un c Є ***A*** tal que b=c.a .También podremos hablar de “a como divisor de b” ó” b múltiplo de a”.

Para esta relación de divisibilidad que se acaba de dar, se verifican propiedades análogas al caso de los enteros, como por ejemplo , sean a, b, c Є ***A*** se tiene:

- a|b y a|c => a| (b + c) y a|(b-c)
- a|b y b|c => a| c

Dos elementos a, b Є ***A*** son asociados si y sólo si a|b y b|a, es equivalente a que a=b.u donde u sería el elemento unidad del conjunto ***A***.

• **Definición:** Se dirá que un elemento a Є ***A***, a≠0 es irreducible si no es una unidad y si sus denominadores son, ó bien la unidad, ó un asociado suyo.

• **Definición:** Un dominio de factorización única (D.F.U) es un dominio de integridad que verifica las siguientes condiciones:

i) Toda no unidad distinta de cero es producto finito de factores irreducibles.

ii) La descomposición anterior es única salvo orden y producto por unidades.

Coloquialmente conocida como descomposición factorial del elemento. Un claro ejemplo sería el anillo de los números enteros cuyas únicas unidades son 1 y -1.

• **Proposición:** Sea una ***A*** un dominio de integridad que satisface la condición i) de la definición anterior, entonces la condición ii) es equivalente a:

> Sean a, b Є ***A*** tales que a es irreducible y a|b.c; entonces es necesariamente a|b ó a|c.

Vamos a estudiar ahora cómo en un D.F.U se puede definir la noción de máximo común divisor y mínimo común múltiplo, al modo de los números enteros.

• **Proposición:** a es divisor propio de b si a no es unidad y ∀ c tal que a.c = b, c no es unidad.

Otra forma de ver que a es irreducible es, si a no es unidad y a no posee divisores propios.

• **Proposición:** Sean a, b Є ***A*** , a|b <=> existe c Є ***A*** *tal que b=a.c*

Consecuencias:

1) ∀ a Є ***A,*** a | a, a = a.1

2) ε es una unidad entonces ∀ a Є ***A,*** ε|a , a= ε(ε^{-1} .a) a tiene divisores triviales son él mismo y sus unidades .Los llamaremos divisores impropios.

• **Proposición:** Sea ***A*** un dominio de integridad a, b asociados <=> a|b y b|a.

Demostracion /

(=>) Sean a, b Є ***A***, son asociados, existe ε unidad a=b. ε => b|a ε^{-1} .a=b => a|b

(<=) a,b Є ***A*** son asociados a|b y b|a. A dominio de integridad

=> existe c b=a.c

=> existe c' a=b.c'

donde deducimos a=a.c.c' => a.(1-c.c')=0 => 1- c.c'=0 => c.c'=1 => c es unidad => a, b son asociados.

• **Definición:** Sea ***A*** un dominio de integridad y sean a,b Є ***A*** elementos distintos de cero. Se llamará máximo común divisor de a y b [mcd(a,b)] a un elemento c Є ***A*** que verifique

- c| a y c | b
- Si d Є ***A,*** d| a y d | b => d | c

Si existe mcd(a,b) será único salvo productos por unidades.

• **Definición:** Sea ***A*** un dominio de integridad y sean a, b Є ***A*** elementos distintos de cero. Se llamará mínimo común múltiplo de a y b [mcm(a,b)] a un elemento c Є ***A*** que verifique:

- a| c y b | c
- Si d Є ***A,*** a| d y b | d => c | d

Si existe mcm(a,b) será único salvo productos por unidades.

• **Observación:** En todo D.F.U A $\exists$ el mcd y mcm de dos elementos no nulos a, b Є A. En efecto, el mcd(a,b) no es otra cosa que el producto de los factores irreducibles comunes a las descomposiciones de a y b en producto de factores irreducibles y

$$\text{mcm}(a, b) = \frac{a.b}{mcd(a,b)}$$

DOMINIOS EUCLÍDEOS

• **Definición:** Un dominio euclídeo es un par (A, g) donde A es un dominio de integridad y g: $A \rightarrow Z$ es una aplicación, llamada función de grado, que verifica:

i) Si a, b $\in A$ son dos elementos distintos de ceros tales que a | b, entonces g(a)≤ g(b)

ii) $\forall$ a, b $\in A$ con b ≠0, $\exists$ c, r $\in A$ tales que a= b·c + r y g(r)≤g(b)

Ejemplos

- $\mathbb{Z}$, con g: $\mathbb{Z} \rightarrow \mathbb{Z}$ dada por g(a)= |a|
- El anillo K[x] de los polinomios en una indeterminada x con coeficientes en un cuerpo k, con g:K[x]→Z definida por g(f(x))= gr (f(x)) si f(x)≠0 y g(0)=-1.

NOTA. Sea a $\in A$, a≠ 0, $\exists$ c, r A tales que 0= a·c+r, y se tiene que r=0. Pues que en caso contrario a/r y por definición (i), g(a)≤g(r), lo que contradice (ii) que dice que g(r)<g(a). Así que r=0, g(r)<g(a), g(0)<g(a) ($\forall$a $\in A$). Si ponemos g_1(a)= g(a) -g(0) , tenemos que es función de grado y que g_1(0)=0.

- *a, b $\in A$ son asociados (a/b y b/a) $\leftrightarrow$ a/b y ga)=g(b)*

  $\rightarrow$ Si son asociados, tenemos que a/b y b/a luego g(a)$\leq$ g(b), g(b) $\leq$g(a). Es decir g(a)=g(b).

  $\leftarrow$ Si a/b y g(a)=g(b), entonces si b $\neq$0, $\exists$ c, r $\in A$ tales que a= b·c + r y g(r)$\leq$g(b)=g(a), pero como a/b esto implica a/r luego g(a)$\leq$g(r) ¡! r=0. b/a.

• **Proposición:** Si (A,g) es un dominio euclídeo, a, b$\neq$ 0 con a, b $\in A$, $\exists$ d $\in A$ tal que d=mcd(a,b) y d = α·a+β·b, α, β$\in A$.

Demostración /

Se define B= { α'·a+β'·b / α', β'$\in A$, α'·a+β'·b$\neq$ 0}.

Elegimos d $\in$ B / d = α·a+β·b con g(d) mínimo. Ahora se quiere comprobar que d=mcd(a,b).

Puesto que d $\neq$ 0, $\exists$ c, r $\in A$ tales que a= d·c + r y g(r)<g(d). Así se tiene a=c·(α·a+β·b)+r, lo que implica que r=a·(1-c·α)-c· β·b. Si r$\neq$ 0, r $\in$ B, g(r)<g(d) ¡!.

Así se tiene r=0, y por tanto d/ a. Análogamente se prueba que d/b y puesto que d= α·a+β·b, todo divisor común divide a d.

• **Proposición:** SI (A, g) es un dominio euclídeo, entonces A es D.F.U (Dominio de factorización única).

Demostración /

Sea a $\in \boldsymbol{A}$ no nulo, se quiere ver que a se puede descomponer en producto de un número finito de factores irreducibles.

Esto es trivial, si g(a)=g(1) (ya que entonces 1 y a serían asociados). Supongamos pues que g(a)<g(1), y que esto está probado $\forall$ a' $\in \boldsymbol{A}$ tales que g(a')<g(a). Si a es irreducible ya está.

Si a es reducible se puede escribir a=b·c, por hipótesis de recurrencia esto prueba la existencia de factorización.

Para probar la unicidad (de la anterior descomposición). Sean a, b, c $\in \boldsymbol{A}$ donde a es irreducible y a/ b·c. Supongamos que a no divide a b, entonces mcd(a,b)=1, 1= $\alpha \cdot a+\beta \cdot b$ → c= $\alpha \cdot a \cdot c+\beta \cdot b \cdot c$, y como a/ b·c , se tiene que a/c. Esto por la proposición que se ha visto anteriormente equivale a que la descomposición es única.

Cálculo del MCD en un Dominio Euclídeo

Sea a, b $\in \boldsymbol{A}$. Calculamos el mcd por el algoritmo de Euclides. Sea g(a)>g(b),

a =b·c_1+r_1, g($r_{1)<g(b),}$ r_1=a-b·c_1. Se verifica que los divisores comunes (a,b) también lo son de (b,r_1), b=$r_1 \cdot c_2$ + r_2 , g(r_2)<g(r_1), aquí pasa lo mismo. Al no poder decrecer g indefinidamente, llega a la división exacta. $r_n = r_{n-1} \cdot c_n$

→ divisores (a,b)= divisores (r_{n-1} , r_n) → mcd(a,b)=$r_{n-1.}$

- **Ejemplo:**

Dominio Euclídeo de los enteros mcd (296, 104).

296=104·2+88

104=88·1+16

88=16·5+8

16=8·2 Por tanto el mcd(296, 104)= 8.

8=88-16·5=88-5·(104-88)=6·88-5·104= 6·(296-104·2)-5·104=**6**·296-**17**·104.

Un Dominio Euclídeo es dominio de ideales principales

Si (E,φ) es D.E, todo ideal es principal. Sea ***A*** ideal, ∃ d tal que φ(d) es mínimo.

∀ a ∈***A***, φ(a)≥ φ(d). Entonces d/a pues si a=d·q+r siendo φ(r)< φ(d) ¡! Ya que φ(d) era el mínimo y r ∈***A***, pues a∈***A***, d ∈***A*** , q ∈ E → q·d ∈***A***, r=a-d·q ∈***A*** .

Es decir tenemos, que d/a, y ***A*** =(d).

DOMINIO EUCLÍDEO. LOS ENTEROS DE GAUSS.

Sea ¢ el cuerpo de los complejos. Sea ***G*** el subanillo de ¢

G = { a + bi | a,bєZ }

G recibe el nombre de anillo de los enteros de Gauss.

Se verifica que ***G*** es un dominio euclídeo, ya que ***G*** es dominio de integridad al ser un subconjunto de un cuerpo (un cuerpo no tiene divisores de cero).

Definimos la aplicación

φ : **G** –>Z

$\alpha = a + bi \rightarrow \varphi(a + bi) = a + b = N(\alpha)$

que la llamaremos norma y que verifica las siguientes propiedades:

i) Si $\alpha, \beta \epsilon G$, entonces $N(\alpha\beta) = N(\alpha)N(\beta)$.

Dem.

Sea $\alpha = a + bi$, $\beta = c + di$. Si realizamos el producto de ambos, tenemos que

$\alpha\beta = (ac - db) + i(ad + bc)$, si hacemos su norma obtenemos

$N(\alpha\beta) = (ac - db)^2 + (ad + bc)^2 = a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2$

$N(\alpha)N(\beta) = (a^2 + b^2)(c^2 + d^2) = a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2$

ii) Si $\alpha, \beta \epsilon G$ y α/β entonces $\beta = \alpha\sigma$ luego por i) $N(\beta) = N(\alpha)N(\sigma)$ con los que $N(\sigma) < N(\beta)$.

Dem.

Sean $\alpha, \beta \epsilon G$; β distinto de cero. Consideramos $\theta' = \alpha/\beta$ siendo α/β la división de complejos, θ' es de la forma $\theta' = a' + b'i$ donde a', b' son racionales. Sea $\theta = a + bi$, con " a " el número entero más próximo a " a' " y " b " el número entero más próximo a " b' ". Sea $\sigma = \alpha - \beta\theta$, $\alpha = \beta\theta + \sigma$.

Por otro lado, calculamos $\theta' - \theta = (a' - a) + (b' - b)i$ y sabemos que la diferencia entre $(a' - a)$ y $(b' - b)$ es como máximo de 1/2. De todo lo anterior, tenemos que $\sigma = \alpha - \beta\theta = \beta\theta' - \beta\theta = \beta(\theta' - \theta)$ si aplicamos la norma, obtenemos que $N(\sigma) = N(\beta(\theta' - \theta)) = N(\beta)N(\theta' - \theta) \leq N(\beta)N((1/2)^2 + (1/2)^2) = N(\beta)(1/2)$ luego la $N(\sigma) < N(\beta)$.

•Ejemplo:

Sea por ejemplo $3+2i$, $1+i$

$(3+2i)/(1+i) = (3+2i)(1-i)/2 = (5/4) - (1/2)\cdot i$, se aproxima por $2-i$.

$(3+2i) = (1+i)(2-i) + \sigma$,

$(3+2i) = (3+i) + \sigma$, $\sigma = i$

$(3+2i) = (3+i) + i$.

UNIDADES

$(a + bi)$ es una unidad si y solo si $1/(a+bi)$ es un entero de Gauss.

Dem.

Veamos la implicación hacia la izquierda:

Suponemos que 1/(a+bi) es un entero de Gauss por tanto

$1/(a+bi)=(a-bi)/(a^2+b^2)$ aplicando la hipótesis tenemos que $(a^2+b^2)/a$ y $(a^2+b^2)/b$,

entonces a=0 ó b=0 ya que si a y b son distintos de cero, entonces $(a^2+b^2)>a$,

$(a^2+b^2)>b$ y no puede ser.

Si a=0 tenemos que b^2/b eso implica que b=±1.

Si b=0 tenemos que $a^2/1$ eso implica que a=±1.

Entonces las unidades son 1,(-1),i,(-i), y cada elemento tiene asociadas a,(-a),

ai,(-ai)

Los enteros de Gauss son un D.F.U pues todo D.E. es un D.F.U (como hemos visto anteriormente).

DESCOMPOSICIÓN EN FACTORES PRIMOS DE LOS ENTEROS DE GAUS.

Si el entero de Gauss (a+bi) no es primo, entonces se puede descompones como

(a+bi)=(c+di)(e+fi), luego por la propiedad i) de la aplicación norma

N(a+bi)=N(c+di)N(e+fi) {observación: ||=N}

|a +bi|=|c+di||e+fi|.

Luego si |a+bi| es primo implica que (a+bi) es primo.

- **Ejemplo:**

(2+i) es primo ya que |2+i|=5 que es un número primo.

$|a+bi|=|c+di||e+fi|=(a^2+b^2)(c^2+d^2)(e^2+f^2)$.

Entonces si (a^2+b^2) no se puede descomponer como productos de dos número que son suma de cuadrados enteros, (a+bi) es primo.

Debemos observar que:

$(a^2+b^2)=(c^2+d^2)(e^2+f^2)$ NO IMPLICA que (a+bi)=(c+di)(e+fi)

- **Ejemplo:**

Tenemos 3+i, aplicamos la norma y obtenemos $|3+i|=(3^2+1^2)=10$

Pero 10 lo podemos expresar como 10=5*2= y tenemos que $5=(2^2+1^2)$ y $2=(1^2+1^2)$ si sustituimos $10=5*2=(2^2+1^2)(1^2+1^2)$. Pero eso NO implica que (3+i)=(2+i)(1+i), para ello calculamos ambos por separado.

(3+i)=(3+i)

(2+i)(1+i)=1 +3i

Y como podemos ver son distintos.

Sin embargo si se cumple que :

(a+bi)=(c+di)(e+fi) IMPLICA QUE $(a^2+b^2)=(c^2+d^2)(e^2+f^2)$.

Luego para averiguar si un entero de Gauss es primo, en primer lugar hallamos la norma, si la norma no es un número primo vemos si se puede descomponer en forma de cuadrados y finalmente ver si es posible ponerlo de la forma (a+bi)(e+fi).

Es aconsejable formar la siguiente tabla, donde aparecen los resultados de ir calculando (a^2+b^2):

	0	1	2	3
0	0	1	4	9
1	1	2	5	10
2	4	5	8	13

- **Ejemplo:**

Si consideramos el entero de Gauss (2 +3i), calculamos su norma |2+3i|=13,

Como el número 13 es primo entonces tenemos que (2+3i) es primo.

- **Ejemplo:**

Si consideramos el entero de Gauss (3+4i), calculamos su norma |3+4i|=25,

25 lo podemos expresar como $25=5*5=(2^2+1^2)(2^2+1^2)$ y tenemos que

(3+4i)=(2+i)(2+i), (2+i) es primo pues su norma, |2+i|=5

- **Ejercicios:**

Descomponer los enteros de Gauss 2 y 3 en productos de factores primos.

- descomponer el número 2:

N(2)=4, 4 no es primo

$4=4*1=2^2*1=2*2$

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

$4=(2^2+0^2)(1^2+0^2)$

Puesto que las unidades 1,(-1),i,(-i) tienen norma 1, si consideramos la descomposición $4=(2^2+0^2)(1^2+0^2)$ la descomposición va ser la trivial, el mismo número por una unidad. Consideramos entonces $4=(1^2+1^2)(1^2+1^2)$.

Como $\sqrt{1^2}=\pm 1$ entonces tenemos que 2=(1+i)(1-¡) queda descompuesto ya que si consideramos la norma N(1+i)=2 y 2 es un número primo.

- descomponer el número 3:

N(3)=9

9=9*1 pero esta descomposición no sirve, puesto que como en el caso anterior es la trivial.

9=3*3, 3 no es suma de cuadrados, luego tampoco podemos, luego el entero de Gauss 3 es primo.

POLINOMIOS CON COEFICIENTES EN UN CUERPO

Sea **K** un cuerpo, **X** una variable indeterminada y **K[X]** el anillo de polinomios en la variable **X** con coeficientes en **K**.Ya se ha visto que el dominio **(K[x],g)**, con **g** la función de grado ordinaria, es euclídeo.

PROPOSICION 1:

Sea (A,g) un dominio euclideo.Entonces se verifica:

a)Todo ideal de A es principal (A es D.I.P).

b)Sea $a \in A$, $a \neq 0$; A/<a> es un cuerpo si y solo si a es irreducible

* NOTACION: **<a>** es el ideal generado por a **(<a>={ax tal que $x \in A$})**

A/<a> es el anillo cociente **(A/<a> ={x+<a> tal que $x \in A$})**

[b] es la clase de **b** en **A/<a>** **([b]=b+<a>)**

Demostración:

a) Sea **J** un ideal arbitrario de **A**. Si **J=<0>, J** es principal, pues solo necesita un generador. Si **$J \neq <0>$,**sea **$a \in J$** con **$a \neq 0$**, un elemento de grado minimo.Entonces,como **A** es euclideo, para todo **$x \in J$**, existen **c,r $\in$ A** tales que **x=ac+r** con **g(r)<g(a)**.Si **r** fuese distinto de 0,como **r=x-ac** , **$r \in J$** y tiene grado menor que el de **a**, lo que contradice la minimalidad del grado de **a**.Asi que **r=0** y por tanto **$x \in$ <a>**, asi que **J** es principal.
b) Supongamos primero que **A/<a>** es un cuerpo y que **a** es reducible.Entonces se puede escribir **a=bc** donde ni **b** ni **c** estan asociados con **a**. Ademas **[b],[c] ≠ [0],** porque no son multiplos de **a**, pero **[b][c]=[0],** asi que **[b]** y **[c]** son divisores de cero no nulos dentro del cuerpo **A/<a>**.Esto es una contradicción, ya que en el los cuerpos no hay divisores de cero, salvo el **0**. Asi que **a** es irreducible.

   Supongamos ahora que **a** es irreducible y sea **$b \in A$**, tal que **$[b] \neq [0]$**,que es equivalente a que **b** no es multiplo de **a**. Hay que demostrar que existe un inverso para **[b]** dentro de **A/<a>** .Al ser **a** un irreducible y **b** no ser multiplo suyo, entonces **mcd(a,b)=1**, con lo que existen **u, v $\in$ A** determinados

unívocamente por **a y b** tales que **1=au+bv**. Tomando clases modulo **<a>** y usando que **[au]=[a][u]=[0]** se tiene que **[1]=[v][b]** con lo que **[b]** tiene un inverso en el cociente, asi que **A/<a>** es un cuerpo puesto que b era arbitrario tal que **[b]≠[0].**

Se estudiaran a continuación el concepto de la raíz de un polinomio de **K[x]**

DEFINICION 2: **Sea f(x) $\in$ K[x] y a $\in$ K. a es una raiz de f(x) si f(a)=0.**

LEMA 3: **Sea f(x) $\in$ K[x] y a $\in$ K, entonces se verifica que a es raiz de f(x) si y solo si el polinomio x-a divide a f(x) en K[x].**

Demostracion:

Supongamos que **a** es raiz de **f(x)**, si se divide **f(x)** entre **x-a**, $\exists$ **q(x)** y **r(x)** tales que f**(x)=(x-a)q(x)+r(x)** con **gr(r(x))<gr(x-a)=1**, luego **r(x)** es una constante y evaluando en **a** en ambos lados de la igualdad **f(x)=(x-a)q(x)+r(x)** se tiene que **0=r(a)**, y como **r** es constante, **r** $\equiv$ **0**.

Supongamos ahora que **x-a** divide a **f(x)**, entonces existe un polinomio **q(x)** $\in$ **K[x]** que verifica que **f(x)=(x-a)q(x)** y por tanto **f(a)=0**,luego **a** es raiz de **f(x).**

NOTA 4: **Sean $a_1,\ldots,a_n \in K$, f(x) $\in$ K[x]; se dice que $\{a_1,\ldots,a_n\}$ son las raices de f(x) si verifican:**

1)a_i es una raiz de f(x) , i $\in$ {1,…,n}

2)si i $\in$ {2,…,n} entonces,a_i es una raiz del polinomio

$$\frac{f(x)}{(x-a_1)...(x-a_{i-1})}$$

3) No existe ningún a $\in$ K, tal que x-a divide a

$$\frac{f(x)}{x-a_1 \ \ldots \ x-a_n}$$

LEMA 5: **Sea f(x) $\in$ K[x] un polinomio no nulo de grado m y sean $\{a_1,\ldots,a_n\}$ las raices de f(x) en K.Entonces n $\leq$ m.**

Demostracion:

Como $(x-a_1)\ldots(x-a_n)$ divide a $f(x)$, $n=gr((x-a_1)\ldots(x-a_n))\leq$

$gr(f(x))=m$

De aquí se deduce que un polinomio tiene a lo sumo **m** raíces en **K**, donde **m** es el grado del polinomio.Se dice que **f(x)** tiene todas las raíces en **K** cuando existan $a_1,\ldots,a_n \in K$, raíces de **f(x)** tal que n coincide con el grado de **f(x).**

LEMA 6: PRINCIPIO DE IDENTIDAD DE POLINOMIOS EN UNA VARIABLE

Si K es un cuerpo con infinitos elementos y si $f(x)\in K[x]$ es un polinomio tal que $f(a)=0 \ \forall \ a\in K$, entonces $f(x)=0$.

Demostracion: si **f** no fuera nulo, por el lema anterior se tendría que **gr(f)=m** es infinito, lo que es absurdo puesto que **f** es un polinomio y se expresa mediante una base finita de **K**.

LEMA 7: Sea K un cuerpo infinito, $X_1,\ldots,X_n$ unas variables indeterminadas sobre K y $f(X_1,\ldots,X_n) \in K[X_1,\ldots,X_n]$ un polinomio no nulo, entonces existen unos elementos $a_1,\ldots,a_n$ de K tales que $f(a_1,\ldots,a_n)\neq 0$.

Demostración:

Por inducción sobre **n**.Para **n=1** se prueba usando el contrareciproco del **lema 6**.Supongamos cierto para **n-**1 indeterminadas. Supongamos que X_n aparece en **f(** $X_1,\ldots,X_n$ **),** pues de lo contrario se le aplicaría la hipótesis de inducción y el resultado seria cierto.Asi pues**,** $f(X_1,\ldots,X_n)=\sum_{i=0}^{m} f_i(X_1,\ldots,X_{n-1})X_n^i$ donde $f_i(X_1,\ldots,X_{n-1})\in K[X_1,\ldots,X_{n-1}]$ $m>0$ y $f_m(X_1,\ldots,X_{n-1})$ 0 Por hipótesis de inducción existen unos elementos $a_1,\ldots a_{n-1}$ en **K** tales que $f_m(a_1,\ldots a_{n-1})$ 0. Entonces

$f(a_1,\ldots a_{n-}1,Xn)=\sum_{i=0}^{m} f_i\ a_1,\ldots a_{n-1}\ X_n^{\,i}$ es un polinomio no nulo en $K[X_n]$,

y por el caso **n=1** existe un a_n en **K** tal que $\sum_{i=0}^{m} f_i\ a_1,\ldots,a_n\ a_n^{\,i} \neq 0$, de donde se deduce que $f(a_1,\ldots,a_n) \neq 0$ y entonces esta probado para todo **n** natural.

LEMA 8: PRINCIPIO DE IDENTIDAD DE POLINOMIOS EN VARIAS VARIABLES

Si K es un cuerpo infinito y $f(X_1,\ldots,X_n) \in K[X_1,\ldots,X_n]$ un polinomio tal que $f(a_1,\ldots,a_n)$ para todo $(a_1,\ldots,a_n) \in K^n$, entonces $f(X_1,\ldots,X_n)=0$

Es el contrarecíproco del **lema 7**.

OBSERVACION 9: Es importante señalar que no es lo mismo que dos polinomios sean iguales como funciones que como polinomios.

Ejemplos:

a)En el anillo de polinomios $\mathbf{Z_2[x]}$, los polinomios $\mathbf{f(x)= x^2}$ **y g(x)**= **-x** son iguales como funciones pues **f([0])=g([0])=[0] y f([1])=g([1])=[1]** pero como polinomios obviamente no son iguales.

b)En el anillo de polinomios **R[x]** todo polinomio $\mathbf{f(x)=f(a)+f^{1)}(a)(x-a)+\ldots+\frac{1}{n!}f^{n)}(a)}$ $(x-a)^n$ desarrollando por Taylor alrededor de a. Esta igualdad es como funciones y como polinomios, pero si desarrollo hasta solo orden 2 por ejemplo:

$\mathbf{f(x)=f(a)+f^{1)}(a)(x-a)+\frac{1}{2!}f^{2)}(t)}\,(x-a)^2$ **con** $\mathbf{t\in(a,x)\cup(x,a)}$, estas funciones son iguales, pero como polinomios son distintos, uno tiene grado n y otro grado 2.

Veamos ahora el concepto de orden de una raíz, volvemos al anillo de polinomios en una variable **X** con coeficientes en **K, K[X].**

DEFINICION 10: Sea $\mathbf{f(x)\in K[X]}$**, un polinomio de grado mayor que 0 y sea a** $\in$ **K una raíz de f(x),sea** $\mathbf{s>=1}$ **el máximo entero tal que** $(x-a)^s$ **divide a f(x). A este máximo, que existe porque está entre 1 y el grado de f, se le llama orden de a en f(x).Cuando s=1, se dice que a es una raíz simple de f(x) y cuando s>1 se dice que a es una raíz múltiple de f(x).**

NOTA 11: Se puede definir la derivada $\mathbf{g'(x)=}\frac{d}{dx}$ **g(x)** de cualquiera polinomio **g(x).**

Si $\mathbf{g(x)=a_0+a_1x+\ldots+a_nx^n}$, entonces $\mathbf{g'(x)=a_1+2a_2x+\ldots+na_nx^{n-1}}$. Para esta forma de calcular derivadas, se verifican las reglas conocidas.

PROPOSICION 12: Sea $\mathbf{f(x)\in K[X]}$**, un polinomio de grado mayor que 0 y sea a** $\in$ **K una raíz de f(x). Entonces a es raíz simple (resp. múltiple) de f(x) si y solo si** $\mathbf{f'(a)\neq 0}$ **(resp.** $\mathbf{f'(a)=0}$**).**

Demostracion: Sea **s** el orden de **a** en **f(x)**, entonces **f(x)=** $(x-a)^s$ **g(x)**, de esta forma **x-a** no divide a **g(x),** luego **g(a)** $\neq$ **0 (lema 3).** Si derivamos usando la regla de Leibniz se tiene que:

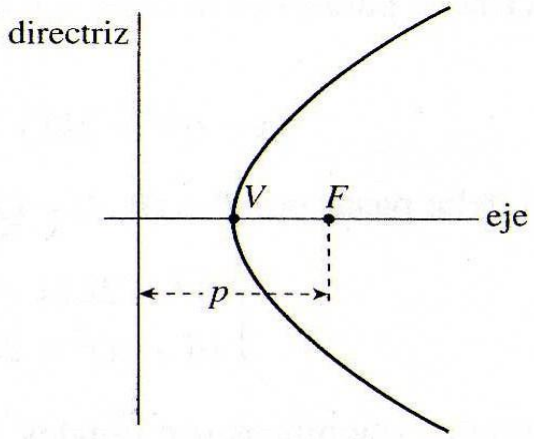
f'(x)=s $(x-a)^{s-1}$ **g(x)+** $(x-a)^s$ **g'(x)** de donde se deduce que **s=1(resp. s>1)** si y solo si **f** $'$ **(a)** $\neq$ **0 (resp. (a) =0).**

.

LA PARÁBOLA

LA PARÁBOLA:

La parábola es el lugar geométrico de los puntos P que equidistan de un punto F y una recta r dados:



Invariantes de la parábola:

El punto F es el llamado **foco** de la parábola y la recta r es la **directriz**. Llamaremos **eje** de la parábola a la recta perpendicular a la directriz que pasa por el foco. El punto de intersección entre el eje y la parábola será el **vértice** de la parábola. Además Se considera la distancia del foco a la directriz, que notaremos p.

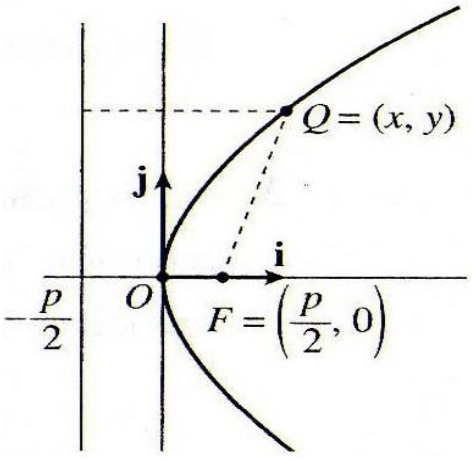
Ecuación implícita de la parábola:

Elegimos un sistema de referencia {0;i,j} con origen en el vértice de la parábola, con i paralelo al eje y j paralelo a la directriz de la parábola. Es decir:

$$i = \frac{\overrightarrow{VF}}{\left|\overrightarrow{VF}\right|}$$

En este sistema de referencia:

$$\begin{cases} F = (\frac{p}{2}, 0) \\ V = (0,0) \\ r: \quad x = -\frac{p}{2} \end{cases}$$, puesto que V equidista del foco F y de la directriz r.



Por tanto:

$$dist(Q,F)=\sqrt{(x-\frac{p}{2})^2+y^2}$$

$$dist(Q,R)=\left|x+\frac{p}{2}\right|$$

De forma que Q estará en la parábola si y sólo si

$$\sqrt{(x-\frac{p}{2})^2+y^2}=\left|x+\frac{p}{2}\right| \quad \Leftrightarrow \quad (x-\frac{p}{2})^2+y^2=(x+\frac{p}{2})^2 \quad \Leftrightarrow \quad y^2=2px$$

Observaciones:

1. En el razonamiento anterior vemos que el eje de la parábola de ecuación $y^2=2px$ es la recta $y=0$. Si cambiamos el orden de las coordenadas, la ecuación que obtenemos para la parábola es $x^2=2py$ y entonces el eje de la parábola será $x=0$. Por lo tanto:

$$ecuación\ de\ la\ parábola:\ y^2=2px \ \Rightarrow\ eje\ de\ la\ parábola:\ y=0$$

$$ecuación\ de\ la\ parábola:\ x^2=2py \ \Rightarrow\ eje\ de\ la\ parábola:\ x=0$$

2. La parábola de ecuación $y^2=2px$ esta contenida en el semiplano $x\geq 0$. Si tomáramos $i=-\frac{\overrightarrow{VF}}{\left|\overrightarrow{VF}\right|}$ obtendríamos la ecuación $y^2=-2px$ y la parábola estaría contenida entonces en el semiplano $x\leq 0$.

En resumen:

Una ecuación del tipo $y^2 = 2kx, con\ k \neq 0, es\ la\ ecuación\ de\ una\ parábola\ con\ eje\ y = 0$

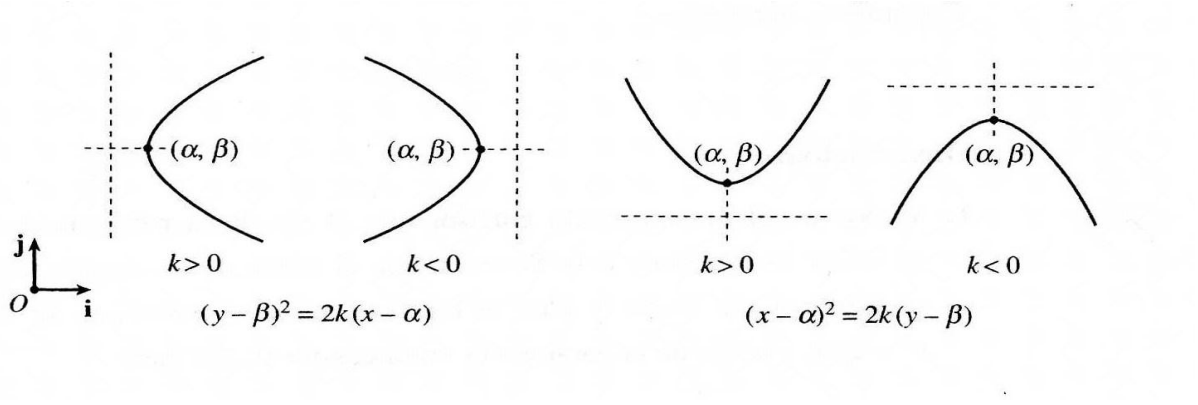
▷ *contenida en* $x \geq 0$ *si* $k > 0, con\ k\ dist\ del\ foco\ a\ la\ directriz$

▷ *contenida en* $x \leq 0$ *si* $k < 0, con\ k\ opuesto\ de\ la\ dist\ del\ primer\ caso$

3. Supongamos ahora que tomamos el sistema de referencia {0;i,j} como habíamos hecho pero ahora el origen no es el vértice de la parábola, sino un punto $C = (\alpha, \beta)$. Entonces la ecuación resultante de nuestra parábola será:

$$(y - \beta)^2 = 2k(x - \alpha)$$

Las cuatro posibilidades que hemos descrito se resumen en:



Ejemplo: Determinar una parábola cuyo foco es el punto F=(2, 5/2) y que pasa por los puntos P=(0,4) y Q=(4,4). ¿Cuántas soluciones hay?

Denotemos la directriz por r. Entonces:

$$dist(P,r) = dist(P,F) = \sqrt{(2-0)^2 + (\frac{5}{2} - 4)^2} = \frac{5}{2}$$
$$dist(Q,r) = dist(Q,F) = \sqrt{(2-4)^2 + (\frac{5}{2} - 4)^2} = \frac{5}{2}$$

Esto significa que la directriz es paralela a la recta que une los puntos P y Q. Por tanto la directriz es paralela a la recta $y = 4$, y la ecuación de la parábola será del tipo:

$$(x-\alpha)^2 = 2k(y-\beta), \quad k \neq 0$$

Esta parábola debe pasar por P=(0,4) y Q=(4,4), luego debe cumplirse

$$\begin{cases} \alpha^2 = 2k(4-\beta), & k \neq 0 \\ (4-\alpha)^2 = 2k(4-\beta), & k \neq 0 \end{cases}$$

Como los segundos miembros son iguales, igualamos también los primeros:

$$\alpha^2 = (4-\alpha)^2 \quad \Rightarrow \quad \alpha = 2$$

Por otra parte, la distancia de la directriz a P es $\frac{5}{2}$, luego la directriz (paralela a y=4) es una de las dos rectas siguientes:

$$\begin{cases} (i) \;\; y = 4 - \frac{5}{2} = \frac{3}{2} \\ (ii) \; y = 4 + \frac{5}{2} = \frac{13}{2} \end{cases}$$

Por lo que tenemos dos posibles valores de k:

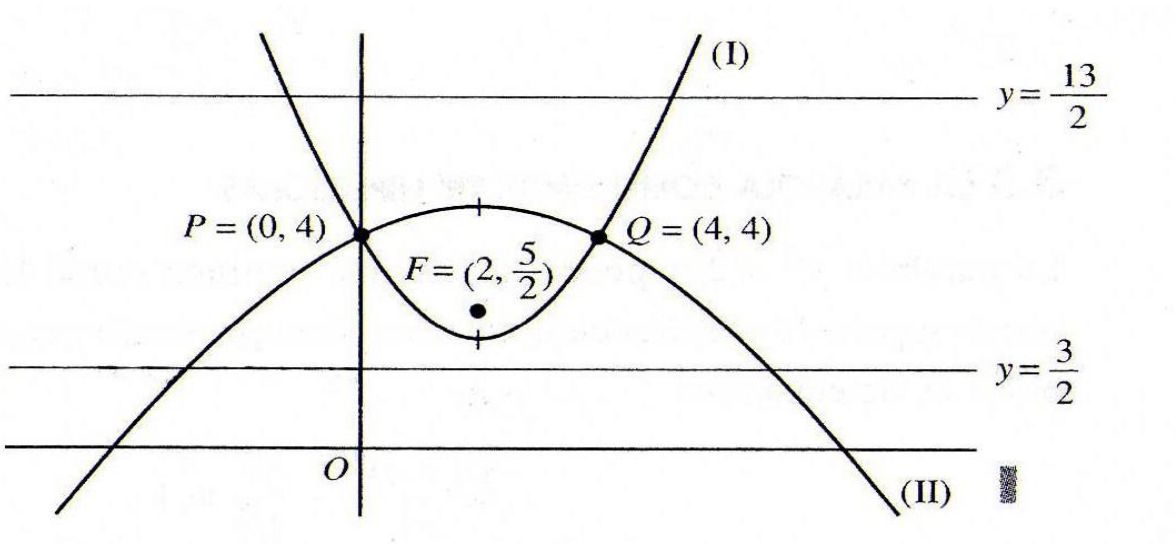
$$\begin{cases} (i)\ \ k = dist(F,r) = \dfrac{5}{2} - \dfrac{3}{2} = 1 \\ (ii)\ k = -dist(F,r) = \dfrac{5}{2} - \dfrac{13}{2} = -4 \end{cases}$$

Sustituyendo los valores de k y α en la ecuación que teníamos $\alpha^2 = 2k(4-\beta)$ obtenemos:

$$\begin{cases} (i)\ \ 4 = 2(4-\beta) \Rightarrow \beta = 2 \\ (ii)\ 4 = -8(4-\beta) \Rightarrow \beta = \dfrac{9}{2} \end{cases}$$

Obtenemos así dos parábolas que cumples las condiciones requeridas, de ecuaciones:

$$\begin{cases} (i)\ \ (x-2)^2 = 2(y-2) \\ (ii)\ \ (x-2)^2 = -8(y-\dfrac{9}{2}) \end{cases}$$



Ecuaciones paramétricas:

Si tenemos por ejemplo la parábola de ecuación implícita $y^2 = 2kx$, basta escribir

$$\begin{cases} x = \dfrac{1}{2k}t^2 \\ y = t \end{cases}$$

Las ecuaciones paramétricas tiene poco interés práctico pero tienen el interés teórico de distinguir a la parábola de circunferencia, elipses e hipérbolas en cuanto a que éstas no pueden parametrizarse mediante polinomios, mientras que la parábola sí.

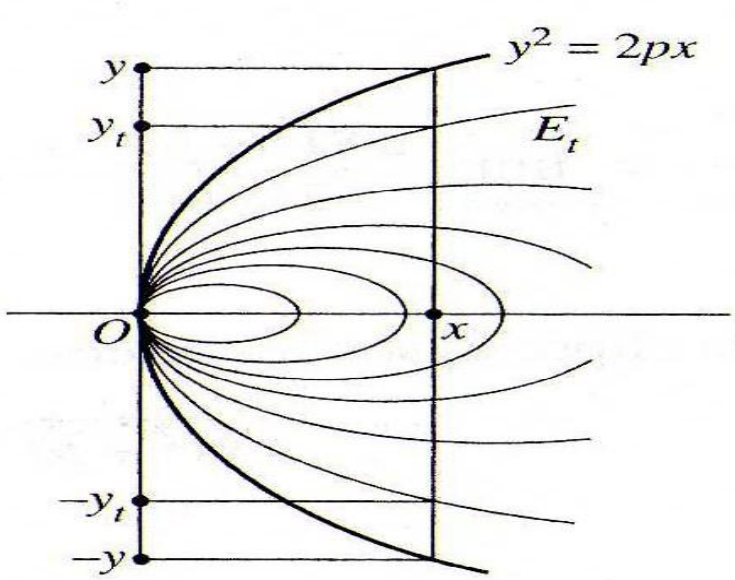
La parábola como límite de elipses:

Posemos considerar la parábola como elipse con uno de los focos en el infinito. Veámoslo usando la ecuación $y^2 = 2px$.

Definimos una familia de elipses E_t mediante sus ecuaciones:

$\dfrac{(x-a)^2}{a^2} + \dfrac{y^2}{b^2} = 1$ con $a^2 = t^2 + pt$ y $b^2 = pt$, siendo t un parámetro real positivo.

Los focos de E_t están en el eje de las x, y el primer vértice de la elipse en ese eje es el origen, que es también el vértice de nuestra parábola.



1) Como se ve en la figura, para cada x >0, si t es suficientemente grande, la elipse E_t tiene dos puntos $(x, \pm y_t)$ con y_t >0, y la parábola dada otros dos $(x, \pm y_t) = (x, \pm\sqrt{2px})$.
Afirmamos que

$$\lim_{t\to\infty}(x, \pm y_t) = (x, \pm\sqrt{2px})$$

Las elipses E_t *tienen por límite la parábola* $y^2 = 2px$

Demostración:

Probaremos que $\lim_{t\to\infty} y_t = \sqrt{2px}$, o lo que es lo mismo, $\lim_{t\to\infty} \frac{y_t^{\,2}}{2px} = 1$

Despejando $y_t^{\,2}$ en la ecuación de la elipse E_t resulta

$$y_t^2 = b^2\left(1 - \frac{(x-a)^2}{a^2}\right) = \frac{b^2(2a-x)x}{a^2} \quad \Rightarrow \quad \frac{y_t^2}{2px} = \frac{b^2(2a-x)}{2pa^2}$$

Sustituyendo ahora los valores a y b en función de t, queda:

$$\frac{y_t^2}{2px} = \frac{pt(2\sqrt{t^2+pt}-x)}{2p(t^2+pt)} = \frac{2\sqrt{t^2+pt}-x}{2(t+p)}$$

Claramente:

$$\lim_{t\to\infty}\frac{y_t^2}{2px} = \lim_{t\to\infty}\frac{2\sqrt{t^2+pt}-x}{2(t+p)} = \lim_{t\to\infty}\frac{2\sqrt{1+\frac{p}{t}}-\frac{x}{t}}{2(1+\frac{p}{t})} = 1$$

2) Los focos de la elipse E_t son los puntos $(\sqrt{t^2+pt}\pm t, 0)$ y se cumple:

▷ $\lim_{t\to\infty}(\sqrt{t^2+pt}\pm t, 0) = (\frac{p}{2}, 0)$, que es el foco de la parábola

▷ $\lim_{t\to\infty}(\sqrt{t^2+pt}\pm t, 0) = (+\infty, 0)$

Demostración:

i) Tenemos

$$\lim_{t\to\infty}(\sqrt{t^2+pt}-t) = \lim_{t\to\infty}\frac{(\sqrt{t^2+pt}-t)(\sqrt{t^2+pt}+t)}{\sqrt{t^2+pt}+t} = \lim_{t\to\infty}\frac{pt}{\sqrt{t^2+pt}+t} =$$

$$\lim_{t\to\infty}\frac{p}{\sqrt{1+\frac{p}{t}}+1} = \frac{p}{2}$$

ii) El otro límite es trivial.

3) La excentricidad de E_t es $e_t = \frac{t}{\sqrt{t^2 + pt}}$ y tal y como ya hemos comentado, pensando que una parábola es una elipse en la que uno de los focos se aleja infinitamente del otro, se cumple que $e = \frac{c}{a} \to 1$, es decir, $\lim_{t\to\infty} e_t = 1$

Demostración

Sabemos que $e = \frac{c}{a}$, así que para calcular e_t sólo tenemos que sustituir los valores de a y c en nuestro caso. Así:

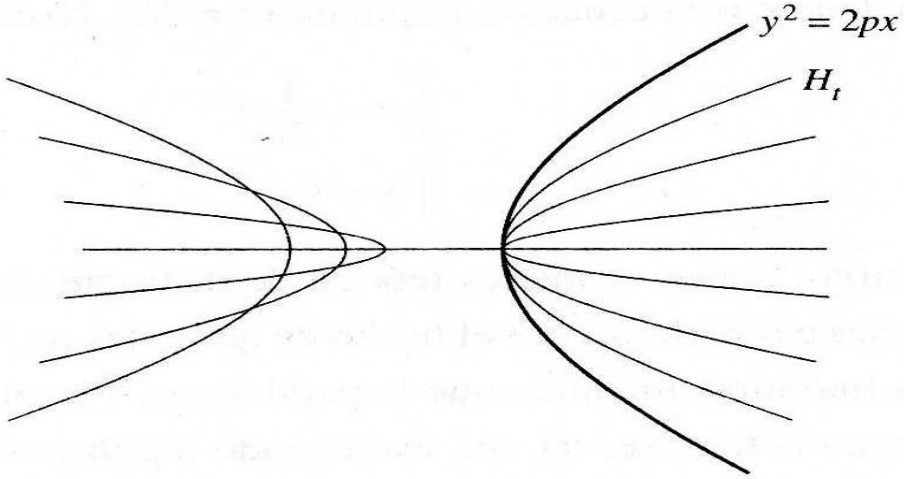
$$\lim_{t\to\infty} e_t = \lim_{t\to\infty} \frac{t}{\sqrt{t^2 + pt}} = \lim_{t\to\infty} \frac{1}{\sqrt{1 + \frac{p}{t}}} = 1$$

<u>La parábola como límite de hipérbolas:</u>

La parábola $y^2 = 2px$ puede describirse también como límite de hipérbolas. Repetiríamos toda la construcción anterior reemplazando las elipses E_t por las hipérbolas H_t de ecuación:

$$\frac{(x+a)^2}{a^2} - \frac{y^2}{b^2} = 1$$

Siendo $a = t$ y $b^2 = pt$.


$y^2 = 2px$
H_t

El teorema de Bézout

Este teorema fue publicado en el año 1776 el cual tuvo mucha importancia para el desarrollo y conocimiento de las curvas algebraicas; algunos casos especiales del teorema fueron sabidos desde el S.XVII especialmente en relación con las intersección de líneas, cónicas y cúbicas.

Teorema de Bézout: Si dos curvas algebraicas proyectivas F(x,y,z)=0 y G(x,y,z)=0 con grados m y n respectivamente, tienen mas de m.n puntos comunes entonces tienen una componente común.

Tenemos que hacer referencia a la condición necesaria y suficiente para que dos polinomios f(x) y g(x) ambos pertenecientes al DFU A[x] (anillo de polinomios) tengan un factor común no constante, para ello tiene que existir dos polinomios ψ y Φ con gr(ψ) <n y gr(Φ) <m que puedan verificar

f(x).ψ(x)=g(x).Φ (x)

además hay que tener en cuenta que dado K cuerpo A=K[$y_1 \ldots . y_r$]

con F(x) $\in$ K[$y_1 \ldots . y_r$] [x] polinomio homogéneo de grado m, G(x) $\in$ K[$y_1 \ldots . y_r$] [x] polinomio homogéneo de grado n

F(x)= $A_0 X^m + A_1 X^{m-1} + \ldots . + A_{m-1} X + A_m$ con $A_0 \in K \quad A_0 \neq 0$

G(x)= $B_0 X^n + B_1 X^{n-1} + \ldots . + B_{n-1} X + B_m$ con $B_0 \in K \quad B_0 \neq 0$

Donde A_i con i =1…m son los polinomios homogéneos de grado i ó 0

B_j con j =1…n son los polinomios homogéneos de grado j ó 0 en $y_1 \ldots . y_r$

En estas condiciones se verifica que la resultante de F,G , definida por $R_{F,G}(y_1 \ldots y_r)$ es un polinomio homogéneo de grado m.n ó 0. (determinante de las componentes de cada uno de los polinomios)

Por tanto teniendo en cuenta estos dos lemas anteriores podemos hacer la demostración del teorema,

Demostración

Supongamos que F, G tienen m.n + 1 puntos comunes $P_1, P_2, \ldots P_{mn+1}$ y sean L_{ij} rectas que unen dos puntos comunes es decir, L_{ij} recta que une P_i con P_j

Consideramos un punto P que no pertenece ni a la curva F ni a la curva G ni a ninguna de las rectas L_{ij} .

Haremos un cambio de coordenadas de manera que este punto sea P =(0,0,1).

Las ecuaciones de las curvas quedarán de la siguiente forma:

F(x_0, x_1, x_2)= $A_0 X_2^m + A_1 X_2^{m-1} + \ldots . + A_m$ con A_i i =1,2…m

Es un polinomio homogéneo en X_0, X_1 de grado i ó 0.

G(x_0, x_1, x_2)= $B_0 X_2^n + B_1 X_2^{n-1} + \ldots . + B_n$ con B_j j =1,2…n

Es un polinomio homogéneo en X_0, X_1 de grado j ó 0, con $A_0, B_0 \in K$ $A_0, B_0 \neq 0$

Por el lema nombrado anteriormente que dice que F y G poseen una componente común si y solo si $R_{F,G}\ \ x_0, x_1\ = 0$ por tanto tendremos que demostrar que $R_{F,G}\ \ x_0, x_1\ = 0$

Supongamos que $R_{F,G}\ \ x_0, x_1\ \neq 0$, el lema previo nos dice que la resultante es un polinomio homogéneo de grado m.n; sea P_i =(c_0, c_1, c_2) un punto común de F y G sustituyendo en F ,G $x_0 = c_0$ y $x_1 = c_1$ tenemos que

F(c_0, c_1, c_2)= $A_0 X_2^m + A_1 X_2^{m-1} + ... + A_m$

G(c_0, c_1, c_2)= $B_0 X_2^n + B_1 X_2^{n-1} + ... + B_n$

c_2 es raíz de F(c_0, c_1, c_2) y G(c_0, c_1, c_2) tiene la componente común $x_2 - c_2$, luego la resultante $R_{F,G}\ \ c_0, c_1\ = 0$

Supongamos P_i , P_j son puntos comunes a F y G,

P_i =(c_0, c_1, c_2) y P_j =(d_0, d_1, d_2)

P no pertenece a la recta L_{ij}

$$\det \begin{pmatrix} c_0 & c_1 & c_2 \\ d_0 & d_1 & d_2 \\ 0 & 0 & 1 \end{pmatrix} \neq 0 \qquad \det \begin{pmatrix} c_0 & c_1 \\ d_0 & d_1 \end{pmatrix} \neq 0$$

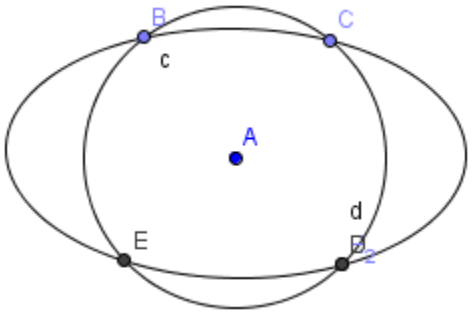
(c_0, c_1) , (d_0, d_1) son soluciones distintas del polinomio homogéneo $R_{F,G}\ \ x_0, x_1\ $ =0

(para que fuesen la misma solución (d_0, d_1) = λ (c_0, c_1) = $\lambda c_0, \lambda c_1$ con lo cual

$$\det\begin{pmatrix} c_0 & c_1 \\ d_0 & d_1 \end{pmatrix} = \det\begin{pmatrix} c_0 & c_1 \\ \lambda c_0 & \lambda c_1 \end{pmatrix}$$

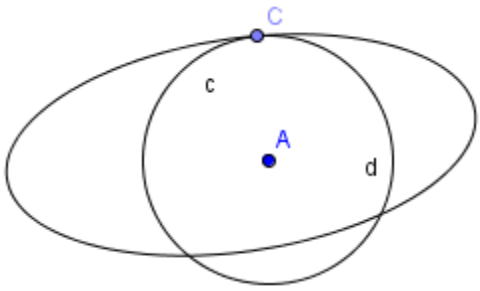
Luego $R_{F,G}\ x_0, x_1 = 0$ es un polinomio homogéneo de grado m.n con m.n+1 soluciones distintas entonces ya tenemos que $R_{F,G}\ x_0, x_1 = 0$.

Aquí podemos observar algunas ilustraciones y ejemplos del Teorema que son elipses de grado 2.Según el Teorema de Bézout el número de puntos de intersección debe se 2x2=4

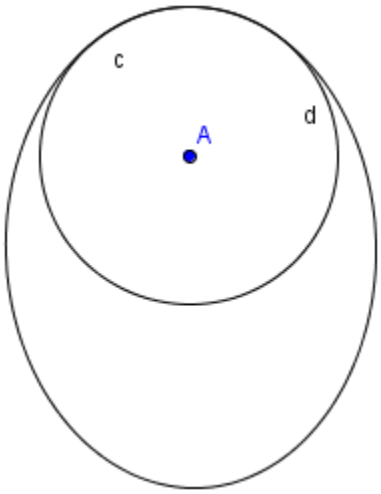


En este caso hay cuatro puntos de intersección.

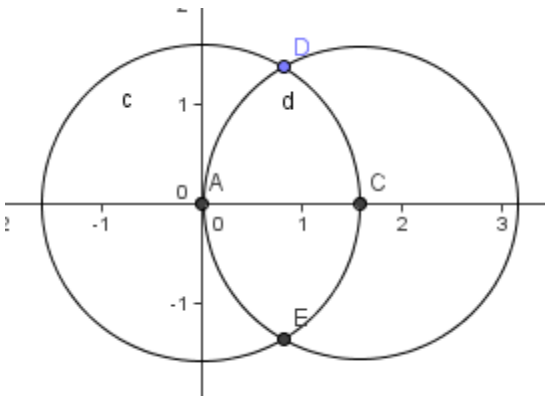
En el caso 2, la intersección de la tangente tiene multiplicidad dos y también en este caso son cuatro los puntos de intersección.



En la figura tres vemos que en la intersección no solo tenemos un punto y un tangente para las dos elipses sino una curvatura común,



En este caso el plano proyectivo los dos círculos tienen cuatro puntos según los requisitos del teorema



Hay muchas posibilidades que existen con respecto a estas figuras que se verifica el teorema en el plano descriptivo complejo

Virginia López Agudo

El Teorema de Bézout y sus aplicaciones

Ana Rodríguez Villares

- *Índice*

El teorema de Bézout y sus aplicaciones

1. Étienne Bézout

Etienne Bézout fue un matemático francés nacido en Nemours en 1730. Hijo de Pierre Bézout y Jeanne-Hélène Filz, de acuerdo con las costumbres sociales de la época, debía seguir el camino profesional de su padre. Sin embargo, interesado en los resultados obtenidos por el matemático y físico Leonard Euler, decidió finalmente orientar su carrera profesional al extenso campo de las matemáticas.
De ésta manera, su primera publicación, *Dynamique*, tuvo lugar en 1756. Éste

echo se repitió en los años posteriores gracias a la elaboración de varios escritos como *Différentielles Quantité* y *Rectificación des Courbes*.
A continuación, en 1758 fue elegido miembro de la Academia de la Marina y de Academia de las Ciencias Francesas y en 1763 Étienne François de Choiseul le nombró instructor de los Guardias de la Marina.
Con el objetivo de enseñar a sus alumnos toda la matemática elemental conocida hasta el momento con un especial énfasis en navegación y mecánica, escribió en cuatro volúmenes *Cours de mathématiques á l'uso des Gardes du Pavillon et de la* Marina.
En 1768, como consecuencia de la muerte de Camus, fue nombrado examinador del Cuerpo de Artillería y siguiendo la misma dinámica que en años anteriores, redactó en seis volúmenes *Cours complet de mathématiques à l'uso de la Marine et de l'artillería* que resultó ser uno de los textos más exitosos de la época usado por estudiantes que pretendían acceder a la Escuela Politécnica.
También fue el autor de *Théoie générale de ecuaciones algebraicas*, una obra que contenía muchos resultados novedosos y de importancia acerca de la teoría de eliminación y funciones simétricas de las raíces de una ecuación. Además, usó los determinantes en un artículo de la *Historie de l'Académie Royale*, sin estudiar en profundidad la teoría general. Además, proporcionó a un resultado similar a la *regla de Cramer* y enunció el *teorema de Bézout*.
Finalmente, Étienne murió en territorio francés Avon, en 1783.

2. El siglo XVIII y las matemáticas

El siglo XVIII se caracterizó por el florecimiento de numerosas disciplinas así como de conceptos matemáticos. Durante éste periodo, a diferencia del siglo XVII, los matemáticos europeos tenían un carácter más cuantitativo y con mayor aplicación física. En ésta etapa de las matemáticas, el Cálculo y sus diversas aplicaciones a la mecánica tuvieron una especial importancia, destacando así grandes figuras como Leibniz, los hermanos Bernoulli, Jacques y Jean, Euler, Lagrange y Laplace entre otros. El carácter aplicado que predominó en el siglo anterior se amplió especialmente durante ésta época, hecho que coincidió con una demanda creciente hacia el uso de las ciencias en la vida social, es decir, los influjos de la economía, las técnicas o la vida social influyeron en la práctica matemática. Asimismo, fue un siglo de un gran desarrollo matemático conectado a la evolución de las ciencias llamadas naturales. En menos de dos siglos, los matemáticos europeos lograron sobrepasar con creces los límites de toda la producción matemática de la Antigüedad, lo cual fue decisivo para el progreso de la cultura y la sociedad occidental teniendo en cuenta que asimismo hubo un destacable progreso cualitativo con una profundidad en los métodos así como la creación de nuevos conceptos y disciplinas matemáticas.
Es destacable, el cambio de papeles del álgebra y la geometría pues el dominio en métodos y criterios de rigor basado en la geometría durante la Antigüedad quedo en un segundo plano al otorgarle mayor relevancia al algebra.
En cuanto al Análisis se basaba en el Cálculo a pesar de la enorme oscuridad lógica. En éste campo y periodo, es destacable el matemático suizo Leonhard Euler

como uno de los autores más prolíficos de todas las épocas que abarcó diversos campos como: las ecuaciones diferenciales, la geometría analítica y diferencial de curvas y superficies, así como las series y el cálculo de variaciones. En relación a la física, Euler destacó por la aplicación del Cálculo a la mecánica tradicionalmente geométrica, el estudio de la propagación del sonido, la perturbación de los cuerpos celestes en la orbita de un planeta, la descripción mediante ecuaciones diferenciales del movimiento de un fluido.
Gracias a Euler, los resultados de Newton y Leibniz se integraron armónicamente al Análisis. La obra que esencialmente realizó ésta ampliación del Cálculo Infinitesimal fue *Introductio in analysin infinitorum* publicada en 1748, y ello fue gracias al establecienciento de función como concepto central de éste nuevo Análisis. Éste hecho tuvo una especial repercusión de tal forma que en la consideración de varios problemas clásicos, Leibniz, Jacques y Jean Bernoulli, L'Hôpital, Huygens y Pierre Varignon usaron funciones conocidas y construyeron muchas otras de mayor complejidad.
Mencionar finalmente, la notable participación de Francia en las matemáticas de la segunda mitad del siglo XVIII, con Jean D'Alembert, Alexis Claude Clairaut y Étienne Bézout, así como por la presencia de de personalidades vinculadas o afectadas por la Revolución Francesa.

3. Conceptos previos

Con el fin de facilitar la comprensión del teorema de Bézout y de su correspondiente demostración, vamos a señalar algunos conceptos y teoremas previos.
Consideremos los polinomios $f(x) = a_0 \cdot X_n + a_1 \cdot X_{n-1} + \dots + a_n$ con $a_0 \neq 0$ y grado n, y $g(x) = b_0 \cdot X_m + b_1 \cdot X_{m-1} + \dots + b_m$ con $b_0 \neq 0$ y grado m; ambos con coeficiente en un
dominio de factorización única.
A continuación, veamos el enunciado y la correspondiente demostración de un lema, cuya aportación nos será de gran utilidad en lo sucesivo.
La condición necesaria y suficiente para que f(x) y g(x) posean un factor en común no constante es que existan los polinomios $\Phi(x)$, $\Psi(x)$ con grado $\Phi(x) < n$ y grado $\Psi(x) < m$, tal que se verifique que $\Psi(x) \cdot f(x) = \Phi(x) \cdot g(x)$

Otra condición necesaria y suficiente para que f(x) y g(x) posean un factor común no constante es $R_{f,g} = 0$
Sea $\mathbb{K}$ un cuerpo, $A = \mathbb{K}[Y_1, \dots, Y_r]$.
Sea $F(x) \in A[X]$, un polinomio homogéneo de grado m
$F(x) = A_0 \cdot X_m + \dots + A_{m-1} \cdot X + A_m$ con $A_0 \in \mathbb{K}$, $A_0 \neq 0$, A_i polinomios homogéneos en $Y_1, \dots, Y_r$ de grado i ó 0.
Sea $G(x) \in A[X]$, un polinomio homogéneo de grado n
$G(x) = B_0 \cdot X_n + \dots + B_{n-1} \cdot X + B_m$ con $B_0 \in \mathbb{K}$, $B_0 \neq 0$, B_j polinomios homogéneos en $Y_1, \dots, Y_r$ de grado j ó 0.
Bajo éstas condiciones se verifica que
$R_{F,G}(Y_1, \dots, Y_r)$ es un polinomio homogéneo de grado $m \cdot n$ ó 0.

4. Aplicaciones

Existen diversas aplicaciones del Teorema de Bézout, todas ellas orientadas al campo de la Geometría Algebraica Proyectiva. Veamos algunos casos particulares:

- *Todo par de curvas se cortan en al menos un punto.*
- *Toda curva plana proyectiva lisa C es irreducible.*

Sea $C = \{[x, y, z] \in P_2 : F(x, y, z)\}$, y supongamos que C es reducible. Sean $F(x, y, z) = G(x, y, z) \cdot H(x, y, z)$ con G y H polinomios homogéneos de grado > 0. Teniendo en cuenta que todo par de curvas se cortan en al menos un punto, definimos $P = [x_0, y_0, z_0]$ perteneciente a la intersección de las curvas definidas por H(x, y, z) y por G(x, y, z). Entonces P es un punto singular de C, luego C no puede ser lisa.

- *Estudio de las componentes de una curva plana.*

Sea $C \equiv p(x,y) = 0$ una curva plana de grado n y $p \in C$ un punto racional no singular. Si C es reducible entonces una de sus componentes es una curva C' de grado menor que n que pasa por p (que es racional y no singular). C' es una curva que corta a C en p con multiplicidad infinita. Toda curva de grado menor que n que corte a C en p con multiplicidad mayor que $n \cdot (n-1)$ contiene, por el teorema de Bezout, una componente de C.

- *Probar que si una cónica tiene un punto singular entonces no es irreducible.*

Consideramos una recta que pase por dicho punto singular y por otro cualquiera de la cónica. La multiplicidad de corte de la recta y la cónica será de, al menos, 3, y por el Teorema de Bézout concluimos que la recta es una componente de la cónica.

- *El grado de una curva plana V es el máximo número n tal que existe una recta que corta a V en n puntos distintos.*

- *Componentes de una cónica*

- *Dos rectas se cortan en un punto.*

- *Dos cónicas se cortan en cuatro puntos.*

- *Cinco puntos determinan una cónica*

- *Existen 3264 cónicas no degeneradas tangentes a cinco cónicas dadas en posición general.*

- *Cada recta intersecta a una cúbica no singular en al menos tres puntos.*

6. Bibliografía.

[1] Apuntes de clase correspondientes al año académico 2008/2009.

[2] Curvas algebraicas. William Fulton. Editorial Reverté.
[3] Homenaje a Joaquín Aregui Fernández. Contribuciones matemáticas. Editorial Complutense S.A.
[4] Álgebra. Enrique Navarro, Enrique Ponsoda, Rafael Company. Universidad Politécnica de Valencia.
[5] Memorias de la Real Academia de Ciencia Exactas, Físicas y Naturales de Madrid.
[6] Introducción a la geometría superior. Sr D. Hose Echegaray.
[7] Páginas webs
http://www.cimm.ucr.ac.cr/aruiz/libros/Historia%20y%20Filosofia/Parte5/Cap17/Parte01_17.htm
www.wikipedia.es

El espectro primo de un anillo

TOPOLOGÍA DE ZARISKI

Alberto Martínez Marín, María López Martín, Luis Martínez Anoz, Susana Moreno Espinosa
27/12/2010

INTRODUCCIÓN

La topología de Zariski se define inicialmente para variedades algebraicas. Dada una variedad algebraica se considera la topología en ella dada por una base de cerrados formada por sus subvariedades algebraicas irreducibles.

Ejemplo:
En

la variedad dada por X=0 tiene como base de cerrados los puntos (0, Y). Así en general los cerrados son conjuntos finitos de puntos de la recta y los abiertos son los complementarios de los conjuntos finitos de puntos.

Pasemos ahora a definir la topología de Zariski en los conjuntos $X_A = Spec(A)$, paso a paso.

APLICACIÓN V

Consideremos un anillo A conmutativo y con identidad, y denotemos por el conjunto de todos los ideales primos de A . Definamos una aplicación V entre el retículo de las partes del anillo A y el conjunto de las partes X_A

del modo siguiente: para cada subconjunto S de A , $V(S)$ es el conjunto de ideales primos del anillo A , que contienen a S .
La aplicación V verifica las siguientes propiedades:

PROPIEDADES DE LA APLICACIÓN V

1. Dados S, S' subconjunto de A , si S' contiene a S , entonces $V(S)$ contiene a $V(S')$.

Demostración:

Evidentemente, si $p \in V(S')$, p es un ideal primo que contiene a S' , y por tanto a S , luego $p \in V(S)$.

2. Si $S \subseteq A$ y es el ideal engendrado por S , entonces $V(S) = V($

3. Si $\{ \quad \}_{i\,i}$
es una familia arbitraria de subconjuntos de A , entonces

V(

4 Si U, U' son dos ideales del anillo A , entonces

$V(U \cap U') = V(U \cdot U') = V(U) \cup V(U')$.

TOPOLOGÍA ESPECTRAL O TOPOLOGÍA DE ZARISKI

En el conjunto , de ideales primos del anillo A , queda definida una topología, , llamada Topología Espectral o Topología de Zariski, cuyos cerrados son los conjuntos elementos de $\mathrm{Im}V$
.
Efectivamente: el conjunto

$\mathrm{Im}(V) = \{ V(S) \in \quad / S \subseteq A \}$

satisface los axiomas de los conjuntos cerrados de una topología :

(a) El conjunto ϕ , y el total , pertenecen a $\mathrm{Im}V$

(b) La intersección finita, o infinita de elementos de $\mathrm{Im}V$, es un elemento de $\mathrm{Im}V$.

Es un corolario trivial de la propiedad 3.

(c)La unión finita de elementos de $\mathrm{Im}V$ es un elemento de $\mathrm{Im}V$
.

Es una consecuencia de la propiedad 4 y 2.

El espacio topológico (, recibe el nombre de Espectro Primo del anillo A , y lo designamos por $Spec(A)$.

APLICACIÓN I

Sea E un subconjunto de , denotaremos por $I(E)$, al conjunto de puntos de A que pertenecen a todos los ideales de E .

Claramente, $I(E)$ es un ideal del anillo A , el ideal intersección del conjunto de ideales que pertenecen a E.
.
Queda así definida una aplicación:
I que hace corresponder a cada E , el ideal de $P(A)$, $I(E)$.

Propiedades de I

(i) Si E *está contenido en E' entonces* , $I(E)$ contiene a $I(E')$.
U
(*ii*) Si F= { } $_i$

es una familia arbitraria de subconjuntos entonces:

$I(U\,Ei) = \cap\, I(\,Ei)$.

iii)Si E,E' son subconjuntos de X_A
:
$I(E \cap E') \supseteq I(E) + I(E')$.

Demostración:

Se sigue trivialmente de la propiedad (i) , y de que $I(E \cap E')$ es un ideal.

$(iv)\ I(\phi) = A.$
$I(X_A) = \eta\, A =$nilradical de A .

Demostración:

La primera afirmación es inmediata y pasemos a demostrar que $I(X_A)$ es el nilradical del anillo A .

$I(X_A)$ es la intersección de todos los ideales primos del anillo A y el nilradical de A , $\eta(A)$, es el ideal formado por los elementos de A que son nilpotentes y se demuestra que estos ideales coinciden..

COMPOSICIÓN DE I y V

Las aplicaciones, composición de I, V :

$\Psi = VI: \ P(X_A) \to P(X_A)$

$\Phi = IV: \ P(X_A) \to P(X_A)$

Verifican las propiedades siguientes:

(i) Dado $E \subseteq X_A : E \subseteq \psi(E)$

.

(i') Dado $S \subseteq A$: $S \subseteq \Phi(S)$.

Demostración:

Sea $f \in S$, como $S \subseteq p$, $\forall p \in V(S)$, entonces $f \in p$, $\forall p \in V(S)$, luego $f \in I(V(S))$.

(ii) $\Phi \cdot I = I \cdot \psi = I$

Es decir, $I V I = I$

Demostración:

Dado $E \subseteq X_A$, por (i) , $E \subseteq V I(E)$, aplicando I :

$I(E) \supseteq I(V I(E))$. Por otra parte, $I(E) \subseteq A$ y por (i') :

$I(E) \subseteq I V(I(E))$.

(ii') $\psi \cdot V = V \cdot \Phi = V$

Es decir, $I V I = V$.

Demostración:

Dado $S \subseteq A$, por (i') : $S \subseteq I V(S)$ y aplicando V , $V(S) \supseteq V(I V(S))$. Recíprocamente, como $V(S) \subseteq X_A$, aplicamos (i) : $V(S) \subseteq V I(V(S))$.

(iii) Dado $E \subseteq X_A$, E es un elemento de la imagen de la aplicación V si y solo si, $\psi(E) = E$.

Demostración:

E s consecuencia inmediata (ii') , ya que $E \in \mathrm{Im}V$, si y solo si, existe

$S \subseteq A: E = V(S) = \psi\ (V(S)) = \psi\ (E)$

(iii') Dado $S \subseteq A$, S es un elemento de la imagen de la aplicación I , si y solo si, $\Phi(S) = S$.

Demostración:

Se sigue de (ii) , puesto que $S \in \mathrm{Im}I$ si y solo si, existe : $E \subseteq X_A : S = I\ E = \Phi \cdot I\ E = \Phi\ S$.

(iv) Las aplicaciones ψ , Φ son idempotentes.

Demostración:

En efecto, basta aplicar las propiedades (ii) , ó (ii') , para conseguir:

$\psi^2 = \psi \cdot \psi = \psi \qquad \Phi^2 = \Phi \cdot \Phi = \Phi$.

TEOREMA DE LOS CEROS DE HILBERT

Dado U ideal del anillo A , U es un ideal radical, si y solo si U pertenece al conjunto imagen de la aplicación I .

En general, $I\ (V(U)) = rad(U)$.

Demostración:
Como por definición, $rad(U)$ es la intersección de los ideales primos que contienen a U , entonces

I(V(Y)) = rad(U)

Teniendo en cuenta (iii') de la **composición de *I* y *V*** queda concluida la demostración. Es decir, $U = rad(U)$ si y solo si $U \in \mathrm{Im}I$.

* Obsérvese que el radical del ideal U , $rad(U)$, puede también expresarse como el conjunto de elementos nilpotentes del anillo cociente A/U .

Este resultado se sigue inmediatamente de aplicar, al anillo cociente A/U , lo visto en la demostración de (iv) de **propiedades de *I*** donde aseguramos que la intersección de ideales primos de un anillo coincide con el conjunto de elementos nilpotentes de dicho anillo.

TEOREMA

La aplicación $\Psi = VI: \ P(X_A) \to P(X_A)$ es un operador de adherencia de la topología de Zariski en $Spec(A)$.

Demostración

Veamos primeramente que Ψ es un operador de adherencia sobre X_A , es decir que verifica las

propiedades siguientes:

(a) $\Psi(\phi) = \phi$.

(b) $E \subset \Psi(E), \forall E \subseteq X_A$.

(c) $\Psi(E \cup E') = \Psi(E) \cup \Psi(E'), \forall E, E' \in P(X_A)$.

(d) $\Psi(\Psi(E)) = \Psi(E)$.

En efecto ,utilizando las propiedades , de las aplicaciones I , V , tenemos lo siguiente:

(a) $\Psi(\phi) = VI(\phi) = V(A) = \phi$.

(b) : $\forall E \subseteq X_A : E \subset VI\, E = \Psi\, E$.

(c) $\Psi(E \cup E') = VI(E \cup E') = V(I(E) \cap I(E')) = VI(E) \cup VI(E') = \Psi(E) \cup \Psi(E')$.

(d) $\Psi(\Psi(E)) = \Psi(E), \ \forall E \subseteq X_A$.

Además Ψ es el operador de adherencia de la topología de Zariski sobre X_A , es decir , para cada $E \subseteq X_A$, $\Psi(E)$ =clausura de E en el espacio topológico $Spec(A)$.

$E \subset \Psi(E) = V(I(E))$, y este último es un cerrado de la topología T_Z , luego

$cl(E) \subseteq VI(E)$. Recíprocamente , sea E' un cerrado en la topología T_Z tal que

$E \subseteq E' \subseteq VI(E)$, entonces $E' \in \mathrm{Im} V$, es decir $E' = VI(E')$ y tenemos la cadena de contenidos

$E \subseteq VI(E') \subseteq VI(E)$, aplicando VI y simplificando nos queda lo que queríamos demostrar.

Definición

Dado un elemento f del anillo A , podemos considerar el complementario de $V((f))$ en X_A , siendo (f) el ideal formado por los múltiplos de A del elemento f . A este subconjunto de X_A lo denotamos X_f , con lo que :

$$X_f = \{ p \in X_A / f \notin p \}$$

Para simplificar la notación : $V((f)) = V(f)$.

BASE DE LA TOPOLOGÍA DE ZARISKI

Dado el espacio topológico $Spec\, A = (X_A, T_Z)$, el conjunto:

$B_Z = \{ X_f \subseteq X_A / f \in A \}$ es una base de abiertos de la topología T_Z .

Demostración

a) $B_Z \subset T_Z$

En efecto ,para cada $f \in A$, X_f es el complementario del conjunto $V(f)$ que es un cerrado de T_Z , luego $X_f \in T_Z$.

b) $\forall G \epsilon \ \ TZ - \phi$, y $\forall p \in G$ existe un f tal que $p \in X_f \subseteq G$.

Sea $G \in T_Z$: $\exists S \subseteq G = X - V(S)$.

Si $p \in G, p \notin V(S)$, es decir p no contiene a S , luego existe $f \in S$ y $f \notin p$.

Además si $f \in S$, como $X_f = X - V(f)$, X_f contiene a $G = X_A - V(S)$; y si

$f \notin p$ entonces $p \notin V(f)$ es decir $p \in X_A - V(f) = X_f$. Por lo tanto :

$p \in X_A - V(f) = X_f$ que está contenido en $X_A - V(S) = G$.

INTERSECCIÓN DE ABIERTOS

Dados f , $g \in A$ se verifica $X_f \cap X_g = X_{fg}$.

Demostración:

$$X_f \cap X_g = (X_A - V(f)) \cap (X_A - V(g)) = X_A - (V(f) \cup V(g)) = X_A - V(fg) = X_{fg}$$

En la demostración se ha tenido en cuenta las propiedades de la aplicación V y el hecho de que el ideal producto $(f)(g)$ es precisamente (fg) .

TEOREMA

$X_f = \phi$ si y solo si el elemento f es nilpotente en A .

.

TEOREMA

Dado $f \in A$, $X_f = X_A$ si y solo si f es una unidad de A .

Demostración

En efecto:

$X_f = X_A$, si y solo si $V(f) = \varnothing$ y esto quiere decir que ningún ideal primo del anillo A , contiene a

f en particular, ningún ideal maximal contiene a f y por lo tanto f es una unidad de A .

TEOREMA

Dados f , $g \in A, X_f = X_g$, si y solo si el ideal radical de (f) coincide con el ideal radical de (g) .

Demostración

Si $X_f = X_g$, $X_A - V(f) = X_A - V(g)$, con lo que $V(f) = V(g)$, entonces, aplicando I ,

$I(V(f)) = I(V(g))$, y por lo tanto $rad(f) = rad(g)$.

Recíprocamente, si $rad(f) = rad(g)$, aplicamos V y $V(rad(f)) = V(rad(g))$, es decir

$V(I\,V(f)) = V(I\,V(g))$,luego $V(f) = V(g)$, es decir, tomando

complementarios, $X_f = X_g$.

TEOREMA

Para cada $f \in A$, X_f es un compacto en el espacio topológico $Spec(A)$.

En particular, X_A es un conjunto compacto.

Demostración:

Es suficiente para la demostración, considerar un recubrimiento de X_f , con abiertos básicos de T_Z . .

TEOREMA

Es equivalente que un conjunto G pertenezca a T_Z y sea un compacto a que existan un número finito de elementos de B_Z cuya unión sea el conjunto G .

.

NOTA IMPORTANTE

Nótese que un ideal primo p del anillo A , se considera a su vez como un punto del conjunto X_A .

Teniendo en cuenta esto, tenemos las siguientes propiedades.

PROPIEDADES DEL ESPACIO TOPOLÓGICO X_A

Dado el espacio topológico $Spec(A) = (X_A, T_Z)$ y $p \in X_A$, un ideal primo del anillo A , se verifican las siguientes propiedades:

1. El conjunto unitario $\{p\}$ es un cerrado en $Spec(A)$, se dice que p es un punto cerrado, si y solo si, p es un ideal maximal de A.

2. La clausura de $\{p\}$ es $V(p)$

3. Dado $p' \in X_A$, $p' \in cl(\{p\})$ si y solo si $p \subseteq p'$.

Demostración:

Es una consecuencia inmediata de la propiedad 2

4. El espacio topológico $Spec(A)$ es un espacio T_0 .

Esto significa que si p, p' son dos puntos distintos de X_A , entonces o existe un entorno de p que no contiene a p' o existe un entorno de p' que no contiene a p.

Demostración:

Se obtiene de forma directa de la propiedad 3 aplicando la definición de clausura cuando p es distinto de p'.

NOTA IMPORTANTE

Hemos señalado que el espacio topológico $Spec(A)$ es un espacio T_0 , pero lo más importante de éste Espacio es que no es un espacio Hausdorff (T_2) (no es separable).

Ejemplo:

Sea $A = \underline{\mathbb{Z}}$

Entonces $Spec(A) = \{(p)\ p, primo\}$

DEFINIMOS LA APLICACIÓN $V : P(\underline{\mathbb{Z}}) \to P(X_Z)$

$B \in \underline{\mathbb{Z}}$, B ={Conjunto de enteros} $\to V(B) =$ { conjunto de primos que dividen al máximo común divisor de los elementos de B }.

$V(\{2,3,4\}) = \varnothing$

$V(\{2,4\}) = V((2)) = \{(2)\}$

LOS CERRADOS DE X_Z

Son los subconjuntos finitos y el total (las imágenes son finitas pues vienen del m.c.d).

.

VARIEDAD DEFINIDA POR EL IDEAL SUMA

Definición: Sea X_j una familia de ideales de un anillo A, que puede ser infinita, definimos la suma de ideales $\Sigma_j X_j$ como el conjunto de todas las sumas $\Sigma_i x_i$ donde cada $x_i \in X_j$ y todos los x_i son cero salvo un numero finito de ellos.

Propiedad: El ideal suma es el menor ideal que contiene a todos los ideales X_j.

Caso particular para dos ideales

Sean X y X' dos ideales del anillo A el ideal suma será el conjunto:
$\{ x+x' / x \in X \text{ y } x' \in X' \}$.

Si consideramos X y X` ideales del anillo R_n , por tanto son de la siguiente forma:

$X= R_n(f_1, \ldots, f_s)$, $X'= R_n(g_1, \ldots, g_r)$, y los elementos del ideal suma serán de la forma:

$X+X'= R_n(f_1, \ldots, f_s, g_1, \ldots, g_r)$.

Definición: Sean X, X' dos ideales de un anillo R, decimos que X y X' son comaximales en R si X+X'=R.

Proposición: Sean X, X' ideales de R_n, entonces:

$V(X+X') = V(X) + V(X')$

La variedad definida por el ideal suma es la intersección de las variedades definidas por cada uno de los dos ideales.

Demostración: para demostrarlo, comprobaremos los dos contenidos.

$\subset$) Sabemos que: $X \subset X+X'$ y $X' \subset X+X'$

Por tanto $V(X+X') \subset V(X)$ y $V(X+X') \subset V(X')$
por lo que $V(X+X') \subset V(X) \cap V(X')$.

$\supset$) Sea ($f_1, \ldots, f_s$) una base de X, y ($g_1, \ldots, g_r$) una base de X'. Si P es un elemento de $V(X) \cap V(X')$, entonces $f_i(P) = 0$, para i = 1, ….., s y $g_j(P) = 0$, para j = 1, ….., r. Por la definición de ideal suma, tenemos que
($f_1, \ldots, f_s, g_1, \ldots, g_r$) es base del ideal suma X+X'.

Tenemos por tanto que P anula a todos los polinomios de la base de X+X', por lo que queda demostrado que $V(X) \cap V(X') \subset V(X+X')$.

Algunos ejemplos

Ejemplo1:

Consideramos el anillo y los ideales:

X= (+ + -25 , + -16) y X'= (-3)

En este caso la variedad definida por el ideal X vendría dada por las soluciones

 = 3 y = -3.

Mientras que la variedad definida por X' vendría dada por las soluciones de la siguiente ecuación:

-3=0

De donde resulta, = 3.

Por tanto, la variedad definida por el ideal suma, seria la intersección de ambas variedades, de tal forma que la variedad definida por el ideal suma es el plano

x3=3.

Para comprobarlo, calculamos el ideal suma que seria el siguiente:

(+ + -25 , + -16 , -3)

De tal forma que la variedad definida por el ideal suma seria:

= 3.

Así, la variedad definida por el ideal suma coincide con la intersección de las variedades definidas por cada uno de los ideales.

Ejemplo2:

Consideramos el anillo R_3 y los ideales:
X=R_3(- +1) ; X'= R_3(,) y X''=R_3(+1)

La suma de estos tres ideales será el ideal:

X=R_3(- +1, , +1)

La variedad definida por este ideal es el conjunto de puntos de que son solución del siguiente sistema:

- +1=0

= = 0

+1 = 0

Es decir, es el punto (0,0,-1)

Por otra parte:

- La variedad definida por X es el conjunto de puntos de la parábola - +1=0

- La variedad definida por X' es el eje

- La variedad definida por X'' es el plano = -1

Por lo que la intersección de estas tres variedades es el punto (0,0,-1) que coincide con la variedad del ideal suma.

Proposición: La intersección finita o infinita de variedades algebraicas de es una variedad algebraica de .

Demostración:

Sea V_i una familia que puede ser finita o infinita de variedades de , entonces, para cada i existe un U_i ideal del anillo de polinomio R_n, tal que V_i es la variedad definida por el ideal U_i, es decir $V_i = V(U_i)$. Veamos entonces que

$\cap = V(\sum)$ siendo $\sum$

el ideal suma de la familia de ideales U_i según la definición anterior.
Tenemos por tanto que si x es un elemento de $\cap$

entonces $x \in V_i = V(U_i)$
para todo i, luego f(x)=0 para todo f perteneciente a U_i, y esto ocurre para todo i.

Así, tenemos que f(x)=0 para todo $f \in U_i$, para todo i, luego $x \in V(\sum)$

Recíprocamente, cada U_i está contenido en el ideal suma,

$V(\sum)$ está contenido en cada $V(U_i)$ y por lo tanto
Está en la intersección.

Así, teniendo en cuenta que dada una familia de ideales U_i del anillo R_n, el ideal

suma es un ideal de R_n, y $V(\sum)$

es una variedad algebraica del espacio afín .

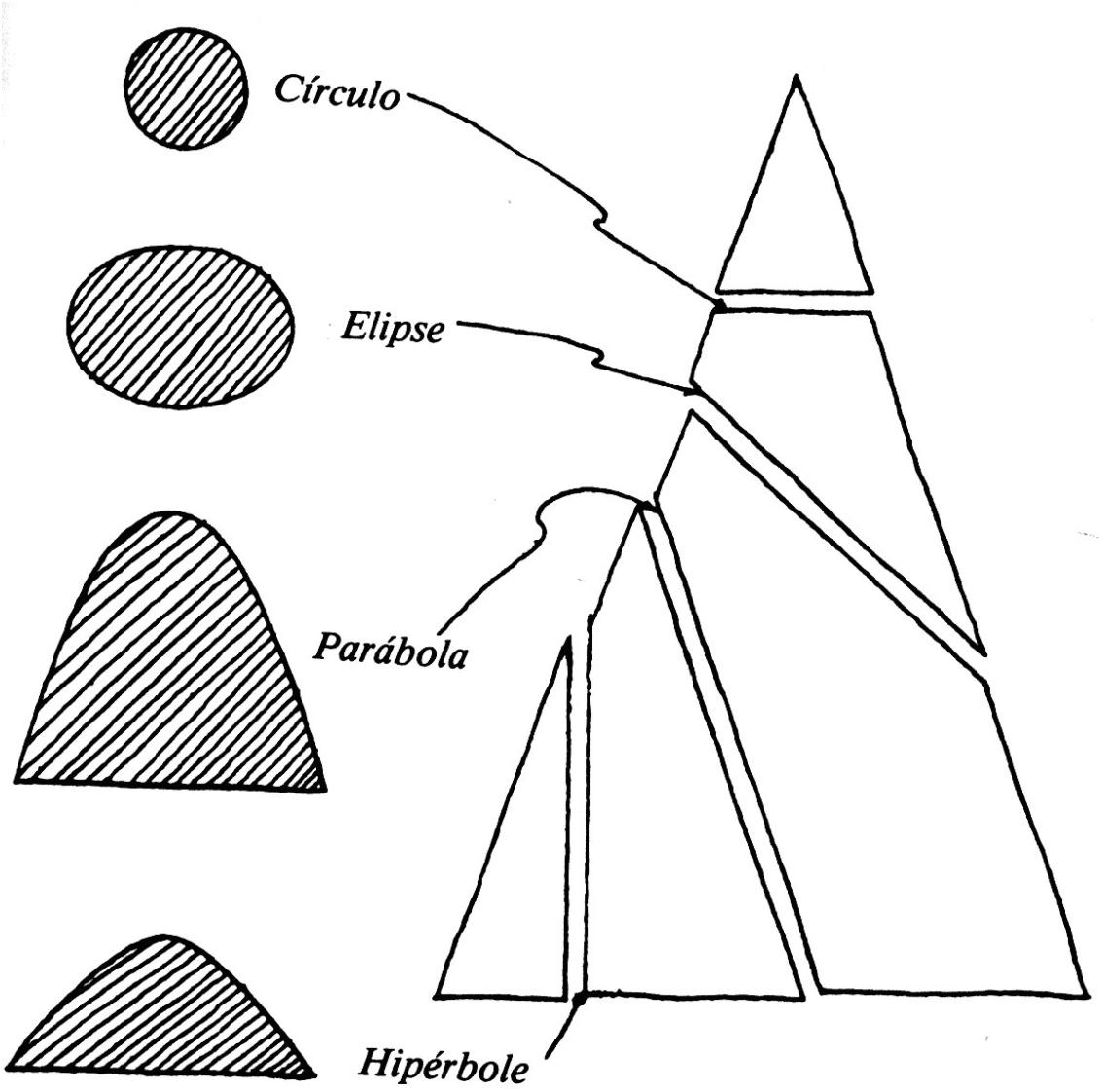
Como ya hemos demostrado que la intersección de variedades es igual a la variedad de la suma, se tiene que la intersección de variedades de es otra variedad de

La Circunferencia y la Elipse

Ricardo Laorga Victoria Llorente Lucía Martín

Capítulo 1
Introducción

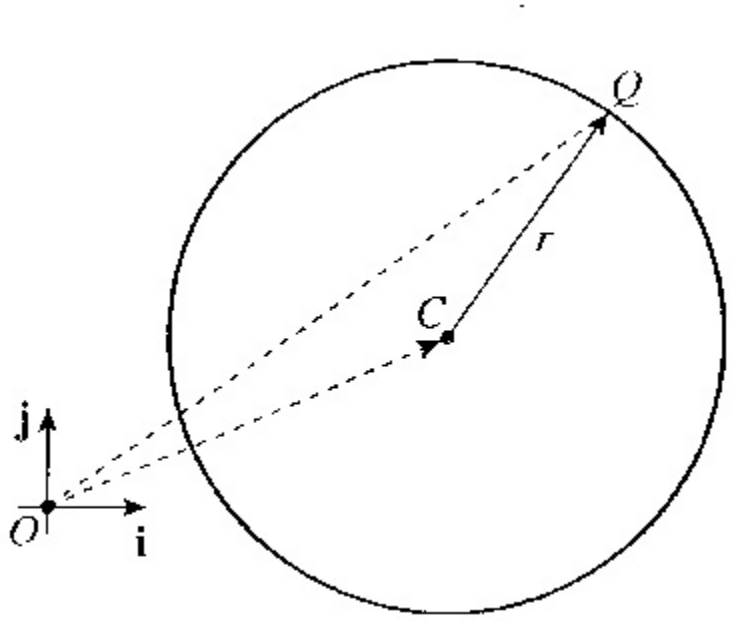
Situémonos en el plano real R_2. Las figuras más sencillas que nos encontramos (sin contar los puntos) son las rectas, las cuales, como ya sabemos, se representan mediante ecuaciones lineales o de primer grado. Después de ellas, y según su grado de dificultad, encontramos las curvas planas denominadas cónicas, las cuales pueden ser degeneradas (punto doble, recta doble o dos rectas) o no degeneradas (circunferencia y elipse, hipérbola y parábola). Normalmente
al hablar de cónicas, nos estamos refiriendo a las no degeneradas.
Con las definiciones geométricas originales de estas curvas veremos que al representarlas encontramos ecuaciones cuadráticas, esto es, de segundo grado. Recíprocamente, si partimos de una ecuación de segundo grado siempre
obtenemos una cónica.
Otra cosa curiosa es que estas curvas se obtienen todas como cortes de un cono doble con un plano y, además, son las únicas que se obtienen haciendo esto. Por esto reciben el nombre de cónicas.
En nuestro caso, nos centraremos en la elipse y en la circunferencia. Veremos sus definiciones clásicas, sus ecuaciones y sus invariantes, todo ello con ejemplos.
Por último y como anexo, veremos la aplicación de la geometría proyectiva al reconocimiento de los distintos tipos de cónicas y, además, las figuras correspondientes
a la circunferencia y a la elipse en el espacio R_3: la esfera y el elipsoide.



Capítulo 2
La circunferencia

2.1. Definición

La circunferencia es el lugar geométrico de todos los puntos Q del plano que equidistan de uno dado C. El punto C se llama centro y la distancia r = dist(Q;C) se llama radio.



Ejemplo 1

Encontrar el centro C y el radio r de una circunferencia que pase por los puntos P = (4; 4), Q = (6; 0) y R =(— –)

¿Cuántas de tales circunferencias hay?

Empecemos buscando el centro C.

Por la definición de la circunferencia, tiene que equidistar de P y Q, luego tiene que estar en la mediatriz de P y Q, m_1. Hallemos tal mediatriz:

La mediatriz pasa por el punto medio de P y Q,

M_1 =(5,2)

y es perpendicular a

PQ = (1;-2), así,
$v_1 = (2; 1)$
luego tiene de ecuación:
m_1 :

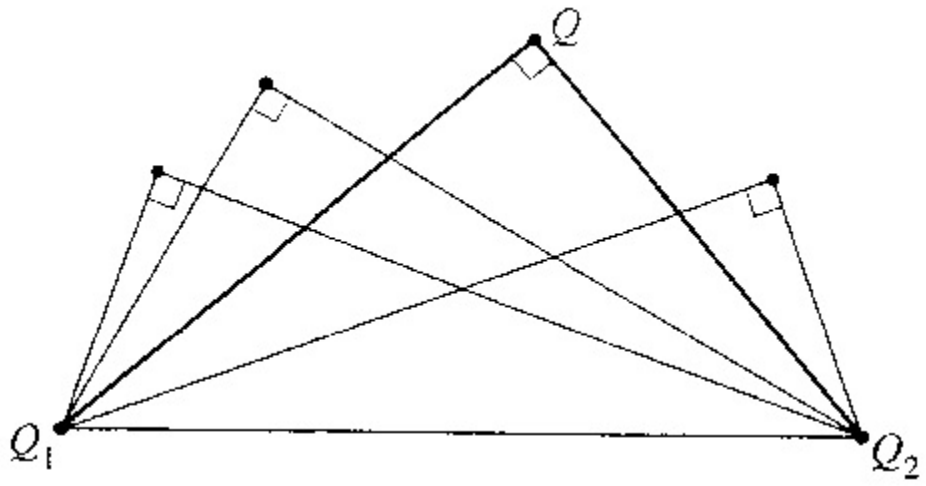
x = 2□ + 5
y = 1□ + 2
y despejando □
m_1 : x - 2y = 1
Análogamente, el centro tiene que estar en la mediatriz de Q y R, m_2.
Tras cálculos . . .
m_2 : x - 7y = 1
2.2. ECUACIÓN IMPLÍCITA 9
Luego C está en m_1 y en m_2:

Esto es,
C = (1; 0)
Ahora veamos el radio r:
:
r = 5

_
Como conclusión, hay una única circunferencia que pasa por P, Q y R, y tiene de ecuación
+ = 25

Ejemplo 2

Sean Q_1 y Q_2 dos puntos dados del plano. Determinar el lugar geométrico de todos los puntos Q desde los que Q_1 y Q_2 se ven desde un ángulo recto.
Sean $Q_1 = (a_1; b_1)$, $Q_2 = (a_2; b_2)$ y Q = (x; y), el hecho de que Q_1 y Q_2 se vean bajo un ángulo recto desde Q 10

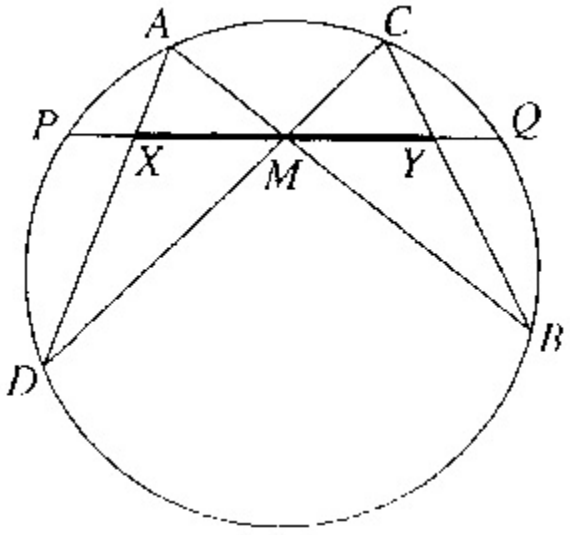


Por tanto, el lugar geométrico buscado es la circunferencia que pasa por Q_1 y Q_2 y tiene de centro el punto medio de esos dos puntos.X

Ejemplo 3

Se considera una cuerda, PQ, de una circunferencia, y otras dos cuerdas, AB y CD, que pasan por el punto medio, M, de la primera. Demostrar que estas dos cuerdas determinan un segmento, XY , en la primera cuyo punto

medio es M.
Elegimos



Elegimos el sistema de referencia con centro el punto M,.
Como M es el punto medio de la cuerda PQ, resulta que el centro de la circunferencia está en el eje de las y, luego tiene coordenadas (0; β), y la ecuación de la circunferencia es

=

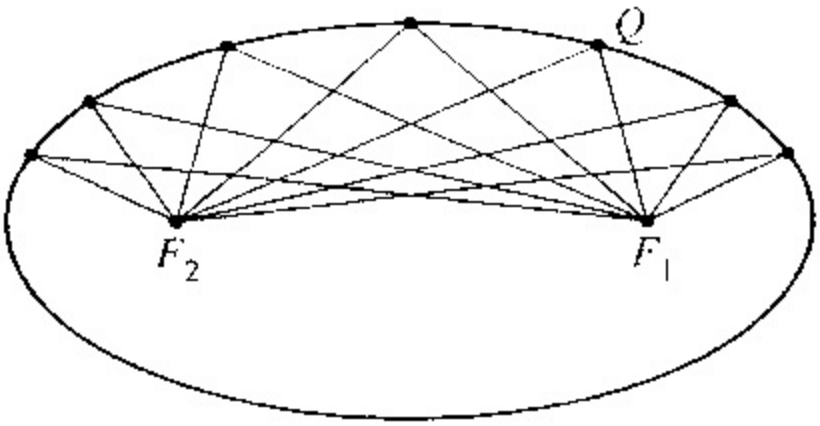
En esta situación, X = (k; 0), y decir que M es el punto medio del segmento XY equivale a ver que Y = (-k; 0). Para confirmar esto, calcularemos las coordenadas de todos los puntos involucrados a partir de A = (a; a') y C = (c; c').
Por la construcción, es claro que B = t(a; a'), y calculamos t usando que B está en la circunferencia. Operando,obtenemos la solución deseada.

Capítulo 3

La elipse

3.1. Definición

La elipse es el lugar geométrico de los puntos Q cuya suma de distancias a dos puntos dados, F_1 y F_2, es constante (y mayor que la distancia entre ambos

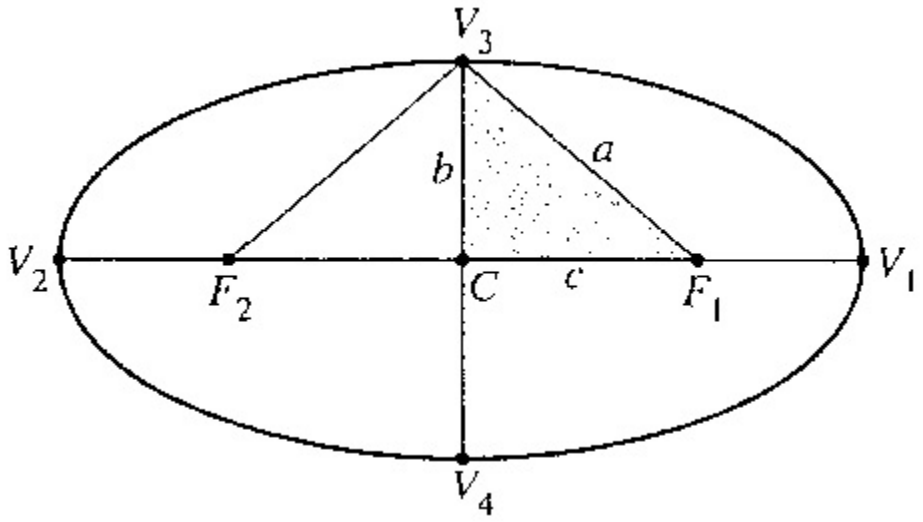


3.2. Invariantes de la elipse

Los puntos F_1 y F_2 se denominan focos, y la suma constante de distancias se suele denotar

$k = dist(Q; F_1) + dist(Q; F_2)$

La distancia focal es la longitud del segmento que une los focos. El punto medio de ese segmento es el centro de la elipse C = – +–



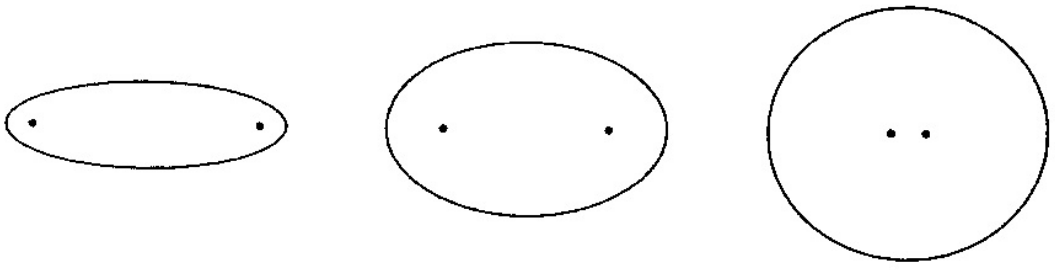
Así, la distancia c de un foco al centro es la mitad de la distancia focal.
Los dos ejes de la elipse son la recta que une los focos y su mediatriz respecto de estos; ambos ejes pasan por el centro. Los vértices (V_1, V_2, V_3 y V_4) son los cuatro puntos de la elipse que se encuentran en los ejes.
Las distancias de los vértices al centro, $a = dist(V_1;C) = dist(V_2;C)$ y $b = dist(V_3;C) = dist(V_4;C)$, son los dos semiejes.
Todos estos datos están ligados por las dos relaciones siguientes:
$k = 2a$ y
Demostración
Por la definición de la elipse y la simetría de la figura:
$k = dist(V_1; F_1) + dist(V_1; F_2)$
$= dist(V_1; F_1) + (dist(V_1;C) + dist(C; F_2))$
$= dist(V_1; F_1) + (dist(V_1;C) + dist(C; F_1))$
$= (dist(V_1; F_1) + dist(F_1;C)) + dist(V_1;C)+$
$= dist(V_1;C) + dist(V_1;C) = 2a$
y, por otra parte

$2a = k = dist(V_3; F_1) + dist(V_3; F_2) = 2dist(V_3; F_1)$
de modo que $a = dist(V_3; F_1)$ y, por el “Teorema de Pitágoras”,

3.3. ECUACIÓN IMPLÍCITA 15

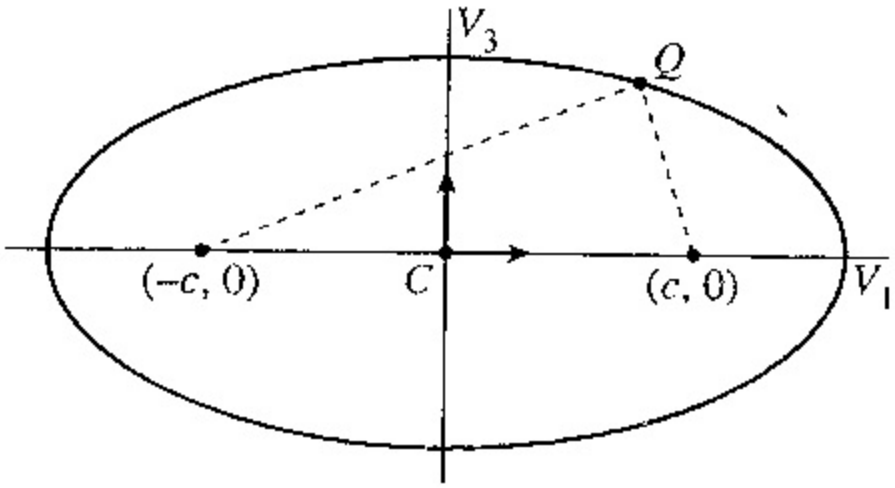
Se llama excentricidad de la elipse al coeficiente $e =$ –

.Como $c < a$,
tenemos
$0 \leq e < 1$
Este coeficiente expresa cuán lejos está la elipse de ser una circunferencia.
En particular, la elipse será una circunferencia cuando $e = 0$.



3.3. Ecuación implícita

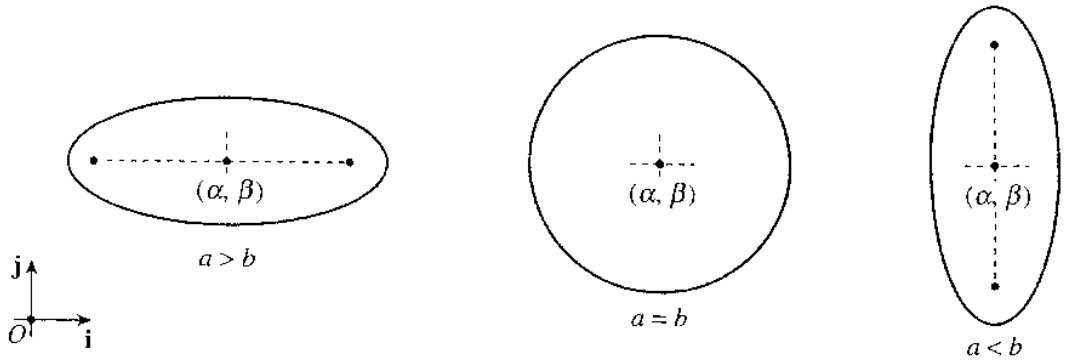
Para obtener la ecuación implícita de una elipse de una forma sencilla, haremos una elección conveniente de la referencia ortonormalCV_1 ___ De este modo, tenemos:
$\overline{C}$ = (0; 0); F_1 = (c; 0); F_2 = (-c; 0)



con lo que la ecuación resulta ser

—+—=1

Distintos tipos de elipses



$$\frac{(x-\alpha)^2}{a^2}+\frac{(y-\beta)^2}{b^2}=1$$

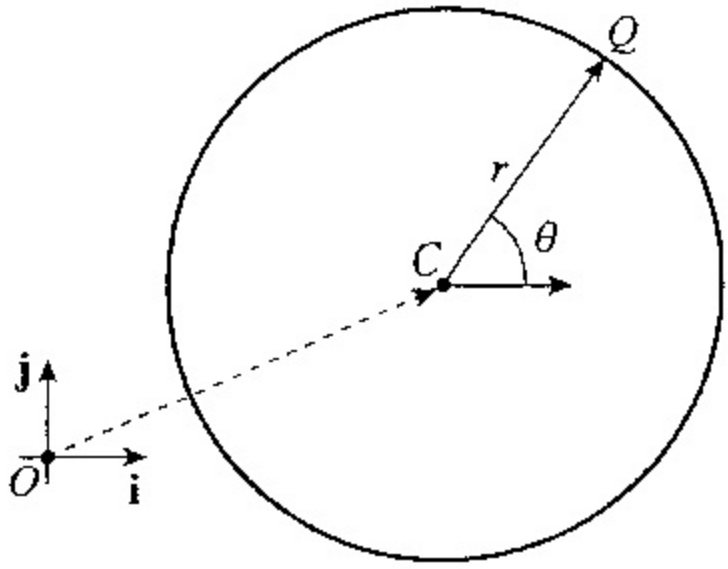
Capítulo 4
Ecuaciones paramétricas

Para encontrar las ecuaciones paramétricas de la circunferencia y de la elipse, necesitaremos la conocida fórmula de la identidad trigonométrica:

$\cos^2 \Phi\_ + \text{sen}^2 \Phi\_ = 1$

Ecuaciones paramétricas de la circunferencia de centro (α_; β_) y radio r:

x = α_ + r cos Φ_
y = β_ + r sin _Φ



Ecuaciones paramétricas de la elipse de centro (α_; β_) y semiejes a, b:

x = α_+ a cos Φ_
y = β_ + b sin Φ_

Demostración

Se comprueba fácilmente que estas ecuaciones verifican la ecuación implícita

de la elipse de centro el punto (α_; β_) y semiejes a, b > 0.

Apéndice A
Geometría proyectiva

Vamos a ver cómo la geometría proyectiva nos puede ayudar a distinguir los tipos de cónicas a partir de una ecuación de segundo grado.

Sea en R^2 la cónica de ecuación

$aX^2 + bXY + cY^2 + dX + eY + f = 0$

Homogeneizamos y cortamos con la recta del infinito (z = 0):

$Ax^2 + bxy + cy^2 + dxz + eyz + fz^2 = 0$
$z = 0$

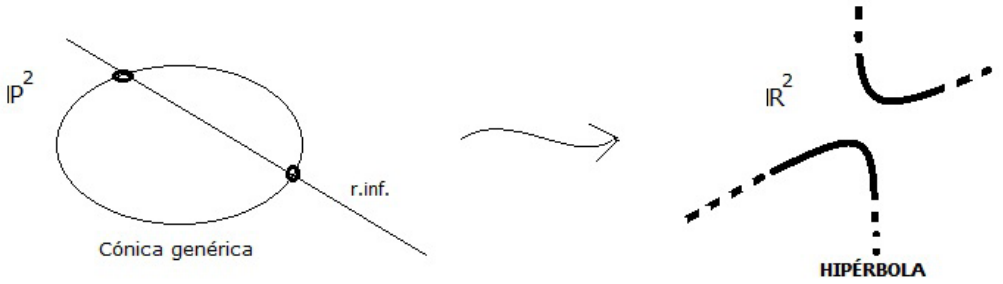
y nos queda

$ax^2 + bxy + cy^2 = 0$

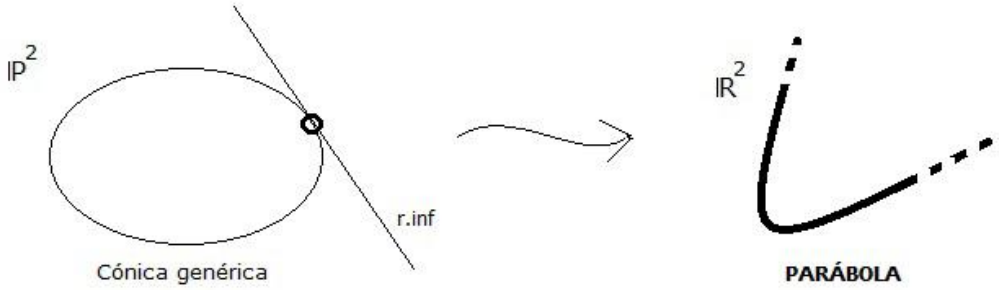
Llamando $D = b^2 - 4ac$

Y así, tenemos tres casos:

D > 0: Hay dos soluciones reales en la ecuación, luego la cónica corta a la recta del
infinito en dos puntos reales y distintos. Es una hipérbola.

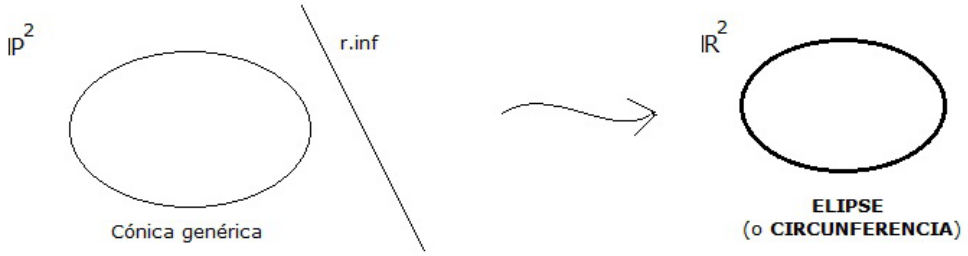


D = 0: Hay una solución real, luego la cónica corta a la recta del infinito en un solo punto real. Es una parábola.



D < 0: No hay soluciones reales, luego la cónica no corta a la recta del

infinito en ningún punto real. Es una elipse.



Apéndice B
Esferas y elipsoides

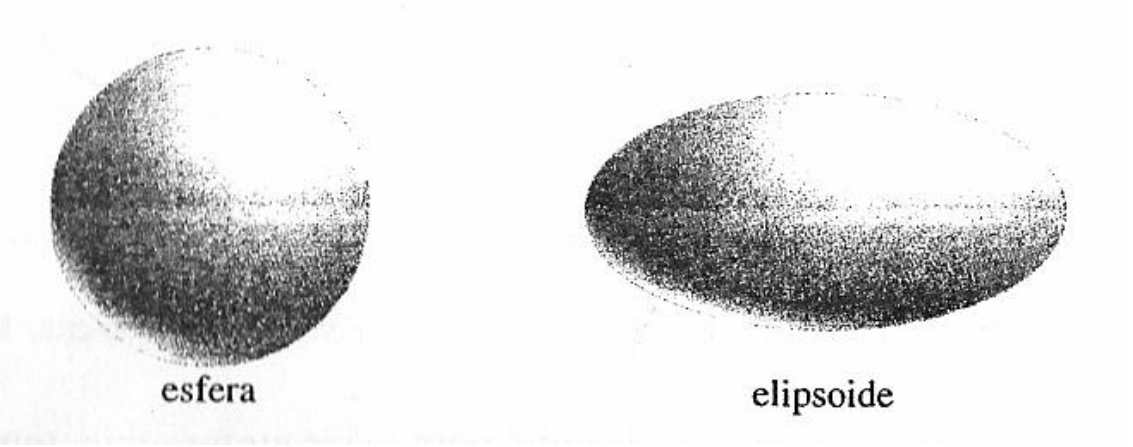
Las figuras que en el espacio corresponden a las circunferencias y elipses del plano son las esferas y los elipsoides.También pueden definirse como lugares geométricos:

_ Una esfera es el lugar geométrico de los puntos del espacio cuya distancia a uno dado es constante. El punto dado es el centro, y la distancia constante es el radio. La ecuación de una esfera de centro (α_; β_;γ) y radio r es:

$(x- \alpha)^2 + (y- \beta)^2 + (z- \gamma)^2 = r^2$

_
Un elipsoide es el lugar geométrico de los puntos del espacio cuya suma de distancias a dos puntos dados es constante. Los dos puntos dados son los focos, y el punto medio de ellos es el centro. La ecuación de un elipsoide de centro el origen y focos en un semieje coordenado es del tipo:

—+—+—=1



Curvas Algebraícas

Variedades definidas por los ideales intersección y producto. Ideal de una variedad. Teorema de los ceros de Hilbert

Francisca Muñoz Rodríguez

Jesús del Pico Iglesias

Santiago Ruiz Encinas

Estrella López Romero

Variedades definidas por los ideales intersección y producto

Proposición 2.7.1.:

Dado A, anillo conmutativo y unitario, la intersección de una familia cualquiera $X_{i\ i}$, de ideales de A, es un ideal de A.

Así los ideales de A forman un retículo completo respecto a la inclusión.

El producto de dos ideales X, Y en A es el ideal XY generado por todos los productos xy donde $x \in X$ e $y \in Y$. Es el conjunto de todas las sumas finitas $\sum x_i y_i$, donde cada $x_i \in X$ y cada $y_i \in Y$.

Análogamente se define el producto de cualquier familia finita de ideales.

Observación:

En particular las potencias X^n, $n > o$ de un ideal X quedan definidas.

Por convenio $X^0 = (1)$.

Así X^n, $n > 0$, es el ideal generado por todos los productos $x_1 x_2 \dots x_n$ en los que cada factor $x_i \in X$.

Observación:

Dados X, Y ideales del anillo A, se verificara que el ideal intersección de X e Y contiene al ideal producto XY.

Proposición 2.7.2:

Dados U, U' ideales del anillo de polinomios R_n, la variedad definida por el ideal producto UU' es igual a la variedad definida por el ideal intersección $U \cap U'$ e igual a la unión de las variedades definidas por cada uno de los factores U, U'. Es decir:

$$V(UU') = V(U \cap U') = V(U) \cup V(U')$$

Demostración:

$\subseteq$

$$\left.\begin{array}{l} U \supset U \cap U' \supset UU' \\ U' \supset U \cap U' \supset UU' \end{array}\right\} \Rightarrow \left\{\begin{array}{l} V(U) \subset V(U \cap U') \subset V(UU') \\ V(U') \subset V(U \cap U') \subset V(UU') \end{array}\right\}$$

$$\underline{V(U) \cup V(U') \subset V(U \cap U') \subset V(UU')}$$

$\supseteq$

Si demostramos que $V(UU') \subset V(U) \cup V(U')$ tenemos que $V(UU') = V(U) \bigcup V(U')$ y como $V(U \cap U') \subset V(U) \bigcup V(U') \subset V(UU')$, tendrá que ser igual y tendremos que $V(U) \bigcup V(U') = V(U \cap U') = V(UU')$

Vamos a demostrar que $V(UU') \subset V(U) \cup V(U')$ por reducción al absurdo:

Sea p $\notin V(U) \bigcup V(U')$, luego $\left\{\begin{array}{l} p \notin V(U),\ \exists f \in U,\ f(p) \neq 0 \\ p \notin V(U'),\ \exists g \in U',\ g(p) \neq 0 \end{array}\right\}$

$fg \in UU'$ luego $fg(p) = f(p)g(p) \neq 0$ luego $p \notin V(UU')$.

Ejemplo 1:

Consideramos los ideales del anillo R_2, $U = R_2(x_1)$, $U' = R_2(x_2)$.

Tenemos que $UU' = U \cap U' = R_2(x_1 x_2)$ y la variedad definida por este ideal serian los puntos $(x_1, x_2) \in C^2 / x_1 x_2 = 0 \Rightarrow x_1 = 0 \text{ó} x_2 = 0$. Por tanto,

$$V(R_2(x_1 x_2)) = V(U) \bigcup V(U')$$

En general, dados U, U' ideales de un anillo A: $U \cap U' \neq UU'$

Sea A=R_2, $U = R_2(x_1) = U'$, entonces $U \bigcap U' = R_2(x_1)$ contiene y es distinto a $U U' = R_2(x^2_1)$ *pues* $x_1 \notin R_2(x^2_1)$. Sin embargo la variedad que definen es la recta $x_1 = 0$.

Ejemplo 2:

Sea $U = R_2(x_1, x_2), \qquad U' = R_2(x_1).$

$U \cap U' = R_2(x_1) \neq UU' = R_2(x_1^2, x_1 x_2).$

Las variedades definidas por estos ideales coinciden, es la recta $x_1 = 0.$

Corolario 2.7.3:

La unión finita de variedades de $\mathbb{K}^n$. es una variedad de $\mathbb{K}^n$.

Ideal de una variedad. Teorema de los ceros de Hilbert

Definición:

Sea E un subconjunto del especio afín $\mathbb{A}^n$, denotaremos por $I(E)$, al conjunto de polinomios de R_n que se anulan en cualquier punto de E, es decir:

$$I(E) = \{ f \in R_n / f(x) = 0, \forall x \in E \}$$

En particular, si V_0 es una variedad algebraica de $\mathbb{A}^n$, llamaremos Ideal de la variedad V_0 al conjunto de los polinomios de R_n que se anulan en todos los puntos de V_0, es decir, al conjunto $I(V_0)$

3.1.2. Se define la aplicación I: $P(C^n)$ ------- > $J(R_n)$ como aquella que hace corresponder a cada $E \in P(C^n)$ el ideal de R_n, I(E). Esta aplicación verifica:

3.1.2. (1)

Si E, E' Є P (C^n) y E' contiene a E entonces I(E) contiene a I(E').

3.1.2. (2)

Si $F = \{E_i\}_i$ es una familia de subconjuntos de C^n, entonces: $I(UE_i) = \bigcap I(E_i)$

Demostración: En efecto: si f es un polinomio de R_n que pertenece a $I(UE_i)$, entonces como E_i contiene a cada E_i, f(x)=0 para todo x de E_i y para todo i, luego $f \in I(E_i)$ para todo i, es decir $f \in \bigcap I(E_i)$. Recíprocamente si $f \in I(E_i)$ para todo i entonces dado un elemento arbitrario x de UE_i existe un elemento E_j de la familia F tal que $x \in E_j$, luego f(x)=0 y por lo tanto $f \in I(UE_i)$.

3.1.2. (3)

Si V_0 es la variedad definida por el ideal U_0 de R_n, entonces el ideal de la variedad V_0 contiene al ideal U_0.

Demostración: Basta tener en cuenta que si $f \in U_0$ entonces f(x)=0 para todo s elemento de $V(U_0)=V_0$, por lo que f es un elemento de $I(V_0)$.

3.1.2. (4)

Si UϵIm(I) entonces el radical del ideal U coincide con U.

Demostración: El radical de un ideal U contiene al ideal, trivialmente. Recíprocamente si f$\epsilon\sqrt{U}$ entonces existe mϵN: $f^m(x)=0$, para todo xϵE.

Teniendo en cuenta que C es cuerpo y por tanto dominio de integridad, resulta que existe algún factor que es cero, así f(x)=0, xϵE y f es un elemento de I(E)=U.

Teniendo en cuenta que Im(I) está contenida en $J(R_n)$ y que Im(V) está contenida en $P(C^n)$, podemos considerar la composición de aplicaciones:

V*I: $P(C^n)$ ------- > $P(C^n)$

I*V: $J(R_n)$ -------- > $J(R_n)$

verificándose:

3.1.2. (5)

Dado Uϵ $J(R_n)$: I(V(U)) contiene a U.

3.1.2. (6)

Dado Eϵ $P(C^n)$: V(I(E)) contiene a E.

3.1.2. (7)

Dado Eϵ $P(C^n)$: V(I(E))=E si y solo si E es una variedad de C^n.

Demostración: En efecto, I(E) es un ideal de R_n y por tanto V(I(E))=E es una variedad. Recíprocamente, teniendo en cuenta 3.1.2. (5), veamos la otra inclusión: si E es una variedad existe U ideal de R_n tal que E=V(U), y por 3.1.2. (6), I(E) contiene a U, aplicando 2.5.3. (1) V(U)=E contiene a V(I(E)).

3.1.2. (8)

I(V(U))=U si y solo si UϵIm(I).

Demostración: Evidentemente si U= I(V(U)), U es un elemento de la imagen de la aplicación I. Recíprocamente tenemos por 3.1.2. (6) que siempre se verifica una inclusión. Si UεIm(I) existe E de $P(C^n)$: U=I(E), aplicando 3.1.2. (5) V(U) contiene a E, y por 3.1.2. (1), I(E)=U contiene a I(V(U)).

3.1.3. Subvariedades:

El espacio afín C^n es un espacio topológico, con la topología de Zariski, en la que los conjuntos cerrados son las variedades algebraicas de C^n. (2.7.4.). Podemos por tanto considerar la topología inducida en cada variedad V de C^n.

Si las subvariedades de una variedad V son las variedades algebraicas de C^n contenidas en V, entonces los subconjuntos cerrados de V son precisamente las subvariedades de V: dado D cerrado de V, existe D' cerrado en C^n, es decir, D' variedad de C^n tal que D=D' contenido en V, y por 2.6.3., D es una variedad de C^n, y contenida en V, luego D es una subvariedad de V.

3.1.4.

Si E es cualquier subconjunto de C^n, entonces la clausura de E es la menor variedad algebraica conteniendo a E.

Demostración: Si V' es una variedad de C^n y V' contiene a E entonces, por 3.1.2. (1), I(E) contiene a I(V'), y por 3.1.2. (7) V'=V(I(V')).

Aplicando ahora 2.5.3. (1), V' contiene a V(I(E)) que a su vez contiene a E (3.1.2. (5)). Luego V(I(E)) es un cerrado de C^n, pues es una variedad, y además está contenida en cualquier otra variedad que contenga a E. Por lo tanto: clausura(E)= V(I(E)).

3.1.5.

Dadas las variedades V_1 y V_2 en C^n, si $V_1 \neq V_2$ entonces $I(V_1) \neq I(V_2)$.

Como consecuencia: una cadena estrictamente descendente: $V_1 > V_2 > \ldots > V_i > \ldots$ de variedades de C^n, le corresponderá una cadena estrictamente ascendente de ideales de polinomios de R_n, que será necesariamente finita pues R_n es un anillo noetheriano; siendo dicha cadena: $I(V_1) > I(V_2) > \ldots > I(V_i) > \ldots$

Para la obtención de este resultado hemos tenido en cuenta 3.1.2. (1) y 3.1.5.

Esta propiedad especial de las variedades muestra que cualquier variedad, con la topología de Zariski, es un espacio cuasicompacto.

3.1.6. Definición: Variedades irreducibles

Una variedad V definida sobre C será REDUCIBLE sobre C si puede descomponerse en la suma de las variedades V_1 y V_2, las cuales están definidas sobre C y son subconjuntos propios de C.

Si tal descomposición no existe entonces la variedad V se dice que es IRREDUCIBLE.

Nota1: Dada una variedad V descompuesta como suma finita de variedades irredundante $V_1, V_2, \ldots, V_n$. Se dice que esta descomposición es irreducible si $V_i \not\subset V_j$ para i, j= 1, …, n y j $\neq$ i

Demostración:

Si la descomposición de V no es irredundante entonces sea por ejemplo V_1 superflua.

Luego: $V_1 \subset \bigcup_{i=2}^{n} V_i, V_1 = \bigcup_{i=2}^{n} (V_i \cap V_1)$

Como V_1 es irreducible entonces $V_1 = V_i \cap V_1$ para algún i $\neq$ 1 y por consiguiente $V_1 \subset V_i$ para algún i $\neq$ 1

3.1.6 (1) Teorema

Una variedad V de C^n es irreducible $\Leftrightarrow$ I (V) es primo

Demostración:

($\Rightarrow$) Sean $f_1, f_2 \in R_n$ polinomios tales que $f_1, f_2 \notin I(V)$. Y consideremos los conjuntos:

$$W_1 = \{x \in V / f_1(x) = 0\} = V(R_n(f_1)) \cap V$$

$$W_2 = \{x \in V / f_2(x) = 0\} = V(R_n(f_2)) \cap V$$

que son subvariedades de V. Además cada $W_i, i = 1,2$ es distinto de V puesto que si coincidieran entonces $f_i \in I(V)$ contra la hipótesis.

a) Supongamos que $W_i \neq \varnothing$ para algún $i = 1,2$ luego $W_1 \cup W_2 \subset V$ y $W_1 \cup W_2 \neq V$ pues V es irreducible. Por tanto, $\exists x \in V / x \notin W_1, x \notin W_2$, es

decir,

$\exists x \in V \,/\, f_1(x) \neq 0,\, f_2(x) \neq 0 \Rightarrow \exists x \in V \,/\, f_1(x) \cdot f_2(x) \neq 0 \Rightarrow f_1(x) \cdot f_2(x) \notin I(V) \Rightarrow$ I(V) es primo.

b) Supongamos que $W_i = \varnothing, i = 1,2$ entonces

$\forall x \in V \,/\, x \notin W_1, x \notin W_2 \Rightarrow f_1(x) \neq 0,\, f_2(x) \neq 0 \Rightarrow f_1(x) \cdot f_2(x) \neq 0 \Rightarrow f_1 \cdot f_2 \notin I(V)$

($\Leftarrow$) Supongamos ahora que I(V) es un ideal primo y tenemos que ver que V es irreducible. Entonces supongamos que sea V reducible. En consecuencia, $\exists V_1, V_2 \,/\, V_1 \cup V_2 = V$ y tal que una de las dos variedades, por ejemplo V_2 cumple que $V_2 \neq V$. Aplicando lo demostrado anteriormente como 3.1.2 (2) (que decía que si F={ E_i $_i$} es una familia de subconjuntos de C^n entonces $I(\bigcup_i E_i) = \bigcap_i I(E_i)$)

entonces tendremos que $I(V) = I(V_1) \cap I(V_2)$ y por el 3.1.5 sabemos que I(V) $\not\subset I(V_2)$.

Además, $I(V_1) \cap I(V_2) \subset I(V_1 \cdot V_2)$ y por hipótesis I (V) es primo entonces I(V) $\supset I(V_1)$ y la otra inclusión es trivial, así que en consecuencia I(V)=I(V_1) y por tanto, V(I(V))=V(I(V_1)) por 3.1.2 (7) V=V_1. Luego concluimos que V es una variedad irreducible.

3.1.6 (2) Teorema: Componentes irreducibles

Cualquier variedad V puede representarse como una suma finita de variedades irreducibles V_i, es decir, $V = \bigcup_{i=1}^{n} V_i$.

Además, si en esta descomposición no se repiten los V_i entonces tal descomposición es única, salvo el orden de los V_i.

A cada una de las variedades irreducibles V_i , i=1,… n tal que cumplen lo anterior, es decir, $V = \bigcup_{i=1}^{n} V_i$ las llamamos componentes irreducibles de una variedad V.

Demostración:

a) Existencia: Siempre existe una descomposición en variedades irreducibles de toda variedad V ya que si suponemos que existe una variedad V_0 que no se descompone en irreducibles entonces V_0 es reducible por lo que $V_0 = W \bigcup W'$ siendo W y W' tales que $W, W' \subset V_0$ y $W \neq V_0, W' \neq V_0$ y la descomposición será falsa para alguna de las variedades W, W'.

Luego tenemos demostrado el teorema para una variedad V_0, así que existe una subvariedad propia V_1 de V_0 para la cual el teorema también será falso. Esta conclusión asegurará la existencia de una cadena infinita de variedades que será estrictamente decreciente ($V_0 > V_1 > V_2 > \ldots$), en contradicción con la consecuencia del 3.1.5 pues dicha cadena da lugar a la cadena de ideales del anillo de polinomios R_n siguiente: ($I(V_0) < I(V_1) < I(V_2) < \ldots$) que es infinita y por lo tanto al ser el anillo netheriano no la admite.

b) Unicidad: Supongamos que la variedad V admite la descomposición no redundante en variedades irreducibles: $V = \bigcup_{i=1}^{n} V_i$

Y sea ahora otra descomposición irredundante de V en componentes irreducibles:

$V = \bigcup_{j=1}^{m} V'_j$

Así para cada V_i, i=1,2…n tendremos que $V_i = V \bigcap V_i = \bigcup_{j=1}^{m} (V'_j \bigcap V_i)$. Y puesto que V_i es irreducible entonces $\exists j \,/\, V'_j \bigcap V_i = V_i$, es decir, $V_i \subset V'_j$, para algún j=1,.. m. Del mismo modo, cada $V'_j \subset V_s$, para algún s=1,...n. Luego $V_i \subset V'_j \subset V_s$ y por tanto que $V_i = V'_j = V_s$ pues si V_s contuviera propiamente a V_i entonces tendremos que V_s sería superflua en la descomposición dada de V y esto no puede ser ya que habíamos supuesto que la descomposición es irredundante. Luego cada una de las n variedades irreducibles V_i coincide con cada una de las m V'_j y al revés. Así habremos probado la unicidad de la descomposición.

Nota 2: El anterior razonamiento de la nota 1 es similar al que usamos para probar que: Si un conjunto finito de de ideales primos $\{ p_1, p_2, \ldots, p_n \}$ es tal que $p_j \not\subset p_i$ para i, j=1,…n y $j \neq i$, entonces p_i no es superfluo en la intersección $p_1 \bigcap p_2 \bigcap \ldots \bigcap p_n$. En efecto, si

$p_1 \cap p_2 \cap \ldots \cap p_n$ no es irredundante entonces existe un i, por ejemplo i=1 tal que $\bigcap_{i=2}^{n} p_i \subset p_1$ y p_1 es un ideal primo con lo que existirá un $i \neq 1$ tal que $p_i \subset p_1$

Proposición :

Si V es una variedad irreducible, V≠Ø, ⟶ V no es un espacio Hausdorff (T_2)

Demostración:

Sean V_1 y V_2 subconjuntos propios cerrados de V, de manera que, por ser V irreducible, $V_1 \cup V_2 \neq V$, lo que equivale a que $U_1 \cap U_2 \neq \emptyset$ con U_1, U_2 abiertos no vacios de V, por lo que V no puede ser Hausdorff. #

Proposición:

Cualquier ideal U del anillo de polinomios de R_n tal que U ∈ Im(I), admite una representación irredundante

$$U=P_1 \cap P_2 \cap \ldots \cap P_n$$

con P_i ideales primos.

Además, la descomposición es única y cada $P_i \in Im(I)$ de manera que cada variedad $V_i=V(P_i)$ son las componentes irreducibles de la variedad V(U).

Demostración:

Sea V'=V(U); como U ∈ Im(I), por 3.1.2.(8) U=I(V'); aplicando 3.1.6.(2) con $V_1, V_2, \ldots V_n$ las componentes irreducibles de la variedad V'. Por la propiedad 3.1.2.(2) tenemos que

$$U=P_1 \cap P_2 \cap \ldots \cap P_n$$

con $P_i=I(V_i) \in Im(I)$ que son ideales primos por el teorema 3.1.6.(1).

Además, la descomposición de V es irreducible, es decir $V_i \not\subset V_j$ para todo i≠j con i,j=1,…,n , y de aquí, $I(V_i)=P_i$ no contiene a $I(V_j)=P_j$ para i≠j con i,j=1, ,n , lo que muestra que $P_1 \cap P_2 \cap \ldots \cap P_n$ es irredundante.

Veamos que esa descomposición de U es única:

Sea $U=P_1' \cap P_2' \cap \ldots \cap P_h'$ otra descomposición de U irredundante de ideales primos P_j'.

Para cualquier P_i, i=1,…,n tenemos que: $P_i = U \cup P_i = \cap_{\{j=1\ldots h\}}(P_j' \cup P_i)$ contiene a $\prod_{\{j=1\ldots h\}}(P_j' \cup Pi)$

Por ser P_i un ideal primo, alguno de los h ideales $P_j' \cup P_i \subset P_i$, y como la otra inclusión siempre se da, existe j=1,…,h tal que $P_j' \subset P_i$.

Utilizando el mismo argumento, cada $P_s \subset P_j'$ para algún s=1,…,n. Tenemos pues $P_s \subset P_j' \subset P_i$, por lo que $P_s = P_j' = P_i$.

Luego, cada uno de los n ideales primos P_i coincide con uno de los h ideales P_j' y recíprocamente.

VARIEDADES DEFINIDAS POR IDEALES PRIMOS

Antes de comenzar a caracterizar los ideales primos del anillo de polinomios $\boldsymbol{R_n}$ recordemos brevemente como definíamos un ideal, y cuando decíamos que éste era primo:

Definición de ideal: Sea A anillo conmutativo y con unidad.

Diremos que I es un ideal de A si y solo si

- I está contenido en A
- Para todo x, y pertenecientes a I tenemos que x-y también está en I
- Para todo a perteneciente a A, y para todo x perteneciente a I, ax también pertenece a I

Definición de ideal primo: Sea A anillo conmutativo y con unidad.

Diremos que P ideal de A es primo cuando verifique que si a, b pertenecen a A, ab pertenece a P, a no pertenece a P, entonces b ha de pertenecer a P.

Caracterización de los ideales primos en el anillo de polinomios $\boldsymbol{R_n}$[X]:

Veamos primero que en Z, los ideales formados por los múltiplos de un número son primos ~~dicho~~ número es primo.

Por ejemplo:

- 3***Z*** es un ideal primo ya que está formado por los múltiplos de 3, numero primo
- 6***Z*** no es ideal primo ya que 6 = 2·3.

Si utilizamos este mismo argumento, en el anillo $\mathbf{R_n}$[X], tenemos la siguiente definición de los ideales primos, que además serán principales:

Definición:

Llamamos polinomio primitivo a un polinomio tal que sus coeficientes no tienen divisores comunes salvo las unidades.

Por ejemplo, en $\mathbf{R_3}$:

- $\mathbf{3x^4 + 4y^2 + 5z + 2xy^3 + xz}$ es un polinomio primitivo ya que sus coeficientes no tienen divisores comunes
- $\mathbf{3x^4 + 9xy^2 + 6xz + 24xy^3 + 15xz = 3x(x^4 + 3y^2 + 2z + 8y^3 + 5\ z)}$
  Este no es un polinomio primitivo ya que los coeficientes tienen divisor común 3 y lo podemos sacar, junto con una x, como factor común

Como consecuencia inmediata de la definición tenemos la siguiente proposición.

Proposición:

Todo polinomio **f(x)** de $\mathbf{R_1}$ se puede poner de la forma $\mathbf{c \cdot f_1(x)}$, donde $\mathbf{f_1(x)}$ es un polinomio primitivo y **c** es precisamente el máximo común divisor de los coeficientes, que lo denotamos por **c(f),** y recibe el nombre de **contenido.**

$$\mathbf{f(x) = c(f) \cdot f_1(x)}$$

Además se verifica que un polinomio f(x) es primitivo $\Longleftrightarrow$ la constante c es una unidad del cuerpo en el que estemos, en este caso **R**.

Nota: Hemos visto esta definición y sus consecuencias en $\mathbf{R_n}$ pero seguirán siendo igualmente válidas si cambiamos $\mathbf{R_n}$ por cualquier dominio de factorización Única (DFU) D y el anillo de polinomios D[X].

Lema de Gauss:

Sean **f(x), g(x)** $\in$ D[X] siendo D un DFU. Se verifica entonces que:

$c(f\cdot g) = c(f)\cdot c(g)$.

En particular, el producto de dos polinomios primitivos es un polinomio primitivo.

Demostración: Si llamamos $c_1=c(f)$ y $c_2=c(g)$ se tiene que $f(x)\cdot g(x) = (c_1\cdot c_2)f_1(x)g_1(x)$ siendo f_1 y g_1 polinomios primitivos. El lema se verificará si probamos que $f_1(x)\cdot g_1(x)$ es un polinomio primitivo, es decir, si probamos la segunda parte del mismo.

Lo haremos por reducción al absurdo:

Supongamos que esto no es cierto, es decir, existe $p \in D$ tal que divide a los coeficientes de $f_1\cdot g_1$. Pero como f_1 es primitivo debe existir un coeficiente a_i de f_1 de forma que p no lo divide y como g_1 también es primitivo, existe un coeficiente b_j de g_1 de forma que p no lo divide.

Sean a_s y b_t los coeficientes de f_1 y g_1 de menor grado que verifican lo anterior. El coeficiente de grado s-t de $f_1\cdot g_1$ es $(\ldots + a_{s-1}b_{t+1} + a_sb_t + a_{s+1}b_{t-1} + \ldots)$. Este coeficiente será múltiplo de p: $(\ldots + a_{s-1}b_{t+1} + a_sb_t + a_{s+1}b_{t-1} + \ldots) = ph = \ldots + ph_1 + a_sb_t + ph_2 + \ldots$ por lo que $a_sb_t = ph - ph_1 - ph_2 - \ldots = p(h - h_1 - h_2 - \ldots)$. Luego $p \mid a_sb_t$, teniendo que cuenta que D es DFU necesariamente se tendría que cumplir $p \mid a_s$ o $p \mid b_t$. ABSURDO.

#

<u>Lema:</u>

Sea **g(x)** un polinomio de D[X], donde D es un DFU tal que **g(x)** es primitivo, es decir sus coeficientes no tienen divisores comunes, y tal que **$g(x) \mid bf(x)$**, con $b\neq 0$ elemento de D **$g(x) \mid f(x)$.** $\Longrightarrow$

Demostración: si $g(x) \mid bf(x)$ $\Longrightarrow$ $f(x) = g(x)h(x)$ donde h(x) es un polinomio de D[X], teniendo en cuenta el lema de Gauss se cumple que $bc(f) = c(g)c(h)$. Como $c(g)$ es una unidad, ya que g es primitivo, se tiene que $b \mid c(h)$ por lo que

$$h(x) = c(h)h_1(x) = bh_2(x)$$

Sustituimos esto que acabamos de tener en la primera igualdad, y tenemos que

$bf(x) - bg(x)h_2(x) = 0$ y como $b\neq 0$ se tiene que $f(x) - g(x)h_2(x) = 0$, luego

$$f(x) = g(x)h_2(x)$$

es decir g(x) divide a f(x).

#

Teorema:

Si D es un DFU ⇨ D[X], que es el anillo de polinomios sobre D en una indeterminada, también lo es.

Demostración:La haremos en dos partes:

1) todo elemento no unidad de D[X] es producto de factores irreducibles.
2) Si p(x) es un elemento irreducible de D[X] y p(x) | f(x)·g(x) entonces p(x) | f(x) o p(x)| g(x).

1) Todo elemento no unidad de D[X] es producto de factores irreducibles.
   Demostraremos esto por inducción sobre el grado del polinomio:

   - Si gr(f) = 0 entonces f(x) = r con r∈ D, luego trivialmente r es producto de factores irreducibles.
   - Si gr(f) = n, suponiendo que todo polinomio de grado menos que n puede ser expresado como producto de factores irreducibles. f(x) se podría expresar como f(x) = c·f_1(x) siendo c = c(f) y f_1(x) primitivo.
     Veamos que f_1(x) se puede descomponer en factores irreducibles:

     - Si f_1(x) es irreducible, es trivial.
     - Si f_1(x) no es irreducible, suponemos f_1(x) = g(x)·h(x), siendo g(x), h(x)∈ D[X] no constantes y por lo tanto de grado menor que n y en consecuencia verifican la hipótesis de inducción:
       g(x) = $\prod_i g_i(x)$ y $h(x) = \prod_j h_j(x)$ siendo $g_i(x)$ y $h_j(x)$ polinomios irreducibles. Con lo que tenemos $f(x) = c\prod_{i,j} g_i h_j$.

2) Si p(x) es un elemento irreducible de D[X] y p(x) | f(x)·g(x) entonces p(x) | f(x) o p(x)| g(x).

   Razonemos según el grado de p(x).

   - Si gr(p) = 0 entonces p(x) será igual a una constante, llamémosla p, p∈ D y p | f(x)·g(x) luego p divide a todos sus coeficientes, en particular, p| c(f)·c(g) y al ser c(f), c(g)∈ D se sigue necesariamente que p divide a uno de los dos, p | c(f) o p | c (g), y en consecuencia p | c(f)f_1(x) = f(x) o p | c(g)g_1(x) = g(x).
   - Si gr(p)>0. Supongamos que p(x) no divide a f(x), construimos el conjunto:
     M={A(x)p(x) + B(x)f(x) / A(x), B(x) ∈ D[X]}
     Sea h(x) el polinomio de M no idénticamente nulo de menor grado y sea *a* el coeficiente del término de mayor grado de h(x). Sabemos que existen dos polinomios q(x) y r(x) y k∈ Z^+ de manera que

$a^k f(x) = h(x)q(x) + r(x)$ siendo $gr(r) < gr(h)$, por lo que

$a^k f(x) = (A(x)p(x) + B(x)f(x))q(x) + r(x) =$

$= A(x)p(x)\, q(x) + B(x)f(x)q(x) + r(x)$

Despejando r(x) tenemos: $r(x) = a^k f(x) - A(x)p(x)\, q(x) - B(x)f(x)q(x) =$

$= f(x)(a^k - B(x)q(x)) - p(x)(A(x)q(x))$

Asique tenemos que r(x) es un elemento del conjunto M, y como ya hemos dicho $gr(r) < gr(h)$ por lo que r(x) ha de ser necesariamente el polinomio idénticamente cero, ya que gr(h) era el mínimo de los polinomios pertenecientes a M, por lo que gr(r) = 0, y $a^k f(x) = h(x)q(x)$, o lo que es lo mismo $a^k f(x) = c(h)h_1(x)q(x)$ siendo $h_1(x)$ un polinomio primitivo tal que $h_1(x) \mid a^k f(x)$ que por el lema anterior $h_1(x) \mid f(x)$.

De manera análoga llegaríamos a que $h_1(x) \mid p(x)$, pero teníamos que p(x) es un polinomio irreducible y p(x) no divide a f(x), por lo que necesariamente $h_1(x)$ es una unidad de D[X]. Como las unidades de D[X] son sólo las unidades en D, se ha de cumplir que $h_1(x) = h$, $h \in D$ y que

$hg(x) = A(x)g(x)p(x) + B(x)g(x)f(x)$ se cumple que $p(x) \mid hg(x)$

siendo p(x) polinomio irreducible de $gr(p) > 0$ y por tanto primitivo, por lo que según el lema anterior p(x) divide a g(x).

#

Proposición:

El anillo de polinomios $\mathbf{R_n}$ es u DFU cuyas unidades o elementos inversibles son los elementos no nulos de **C**.

Demostración: Sabemos que $\mathbf{R_1} = \mathbf{C}[X]$ es un dominio euclídeo y por tanto, un DFU. Por inducción, supongamos que $\mathbf{R_{n-1}}$ anillo de polinomios sobre **C** en n-1 indeterminadas es un DFU. Entonces $\mathbf{R_n} = \mathbf{R_{n-1}}[x_n]$, con lo que se sigue que $\mathbf{R_n}$ es DFU. Además, si d es un elemento no nulo de **C** es por tanto una unidad en $\mathbf{R_n}$ ya que posee inverso y tanto d como d^{-1} están en $\mathbf{R_n}$.

Recíprocamente, si f es una unidad en $\mathbf{R_n}$ existirá f^{-1} de forma que $f \cdot f^{-1} = 1$ y al ser gr(1)=0 se tiene que cumplir que $gr(f) \cdot gr(f^{-1}) = 0$ y por tanto f y f^{-1} son elementos no nulos de **C**.

#

Una vez visto lo anterior podemos caracterizar los ideales primos y principales de $\mathbf{R_n}$:

Proposición:

Sea **f(x)** elemento de $\mathbf{R_n}$, entonces el ideal que genera $\mathbf{R_n(f)}$ es primo $\Leftrightarrow$ irreducible, invertible o nulo.

Demostración:

si f(x) es el polinomio idénticamente nulo entonces $\mathbf{R_n}(f)$ es el ideal generado por el cero, que es primo.

Si f(x) es invertible entonces sabemos que es un elemento no nulo, y por tanto f(x) = k, $\mathbf{R_n}(k) = \mathbf{R_n}$ que es así mismo ideal primo.

Si f(x) es un polinomio irreducible: sea p y q elementos de $\mathbf{R_n}(f)$, es decir $p \cdot q = h \cdot f$ siendo h perteneciente a $\mathbf{R_n}$ y supongamos que p no pertenece a $\mathbf{R_n}(f)$. Al ser p,q y h elementos de un DFU se pueden expresar como producto de factores irreducibles de manera única salvo el orden y salvo los factores unidad:

$$p_1 \cdot \ldots \cdot p_n \cdot q_1 \cdot \ldots \cdot q_m = h_1 \cdot \ldots \cdot h_s f$$

Por lo que al ser f irreducible existirá un elemento del primer término que será igual a f.

Supongamos que el termino $p_j = f \Longrightarrow p_1 \cdot \ldots \cdot p_j \cdot \ldots \cdot p_n = p_1 \cdot \ldots \cdot f \cdot \ldots \cdot p_n$, entonces p sería un elemento de $\mathbf{R_n}(f)$ lo que contradice la hipótesis. Luego necesariamente tiene que ocurrir que $q_j = f$, y con ello: $q = q_1 \cdot \ldots \cdot q_j \cdot \ldots \cdot q_n =$ $= q_1 \cdot \ldots \cdot f \cdot \ldots \cdot q_n$.

Por lo tanto q es un elemento de $\mathbf{R_n}(f)$.

Recíprocamente, supongamos que $\mathbf{R_n}(f)$ es un ideal primo:

Si f = 0 se verifica la proposición

Si f es un elemento constante y por tanto invertible, también lo tendremos

Si f es un elemento de $\mathbf{R_n}$ no constante y que f = g·h donde g y h son elementos de $\mathbf{R_n}$, entonces $g \in \mathbf{R_n}(f)$ o $h \in \mathbf{R_n}(f)$. supongamos que $g \in \mathbf{R_n}(f)$: entonces g = p·f y f = p·f·h y por ello f(ph – 1) = 0 siendo f no idénticamente nulo por tanto ph – 1 = 0, y por tanto h es una unidad de ya que $h \mid 1 \in \mathbf{R_n}$. Es decir si f= g·h, h tiene que ser una unidad, lo que lleva a que g sea divisor propio de f y por tanto f será irreducible.

#

Veamos ahora algunos ejemplos de ideales que según el teorema anterior son primos:

1) El ideal principal $\mathbf{R_2}(x^2+y^2-1)$ es un ideal primo ya que el polinomio que lo genera es un polinomio irreducible en $\mathbf{R_2}$.
2) Si consideramos el ideal generado por el polinomio x^2-y^2, no es primo ya que se puede expresar como (x-y)(x+y) y por ello es un polinomio reducible en $\mathbf{R_2}$.

Veamos otros ejemplos de variedades y sus ideales asociados:

1) Sea la variedad V_1 de $\mathbf{C^2}$, tal que está formada por los puntaos de la recta $x_2 = 0$. esta variedad es irreducible y su ideal asociado es $I(V_1) = \mathbf{R_2}(x_2)$ que es un ideal primo

2) Sea la variedad $V_2 = \{(x_1, x_2) \in \mathbf{C^2} / (x_1, x_2) = (0,0), (0,1), (0, -1)\}$. Ésta es claramente reducible, ya que el ideal generado por ella es
   $V_2 = V(\mathbf{R_2}(x_1, x_2)) \cup V(\mathbf{R_2}(x_1, x_2 -1)) \cup V(\mathbf{R_2}(x_1, x_2 +1))$

   Entonces $I(V_2) = (\mathbf{R_2}(x_1, x_2(x^2_2 -1))$ que no es un ideal primo ya que

   $x_2(x^2_2 -1)$ pertenece al ideal y sin embargo x_2 y $(x^2_2 -1)$ no pertenecen a él.

3) Sea la variedad V_3 consistente en los puntos de la parábola $x^2-y=0$. $\mathbf{V_3}$ es irreducible, el ideal generado por V_3 es $I(V_3)=\mathbf{R_2}(x^2-y)$ y es un ideal primo ya que el polinomio que lo genera es irreducible.
4) Sea V_4 la variedad generada por el punto (1,0) y los puntos de la recta de ecuación x=0. es claro que se puede expresar como unión de dos variedades. El ideal de V_4 es $I(V_4)=\mathbf{R_2}(x(x-1), yx)$ que no es primo ya que $y\cdot x \in I(V_4)$ y sin embargo, y, $x \notin I(V_4)$.
5) la variedad V que consiste en todo $\mathbf{C^n}$ es irreducible. Basta considerar el ideal definido por V: I(V) que es el ideal impropio de $\mathbf{R_n}$.
6) sea la variedad V constituida por Rn, tenemos que $V(Rn) = \phi$, ya que en Rn están los polinomios, 7, 15, 24,… de grado cero. Y ningún poto se anula en ellos ya que siempre $7 \neq 0$, $15 \neq 0$, $24 \neq 0$

Proposición:

Sea un ideal primo de $\mathbf{R_n}$ $\Rightarrow$ verifica que la variedad a dicho ideal es irreducible.

Demostración: Aplicando el teorema de los ceros de Hilbert, $I(V(p)) = \sqrt{p} = p$ y se sigue que V(p) es irreducible.

Nota: aplicando esta proposición la variedad V= Ø es una variedad irreducible por estar asociada al ideal primo $\mathbf{R_n}$.

Proposición:

Sea un ideal primo p de un anillo R de forma que contenga a la intersección de los ideales $U_1,\ldots. U_s$, p contiene a alguno de los ideales $U_1,\ldots. U_s$.

Demostración: basta tener en cuenta que el ideal producto $U_1\cdot\ldots\cdot U_s$ por estar contenido en $U_1 \cap \ldots. \cap U_s$, está contenido en el ideal primo p y consecuentemente alguno de los U_i.

#

Proposición:

Si una variedad V está contenida en la unión de las variedades $V_1,\ldots, V_s$ siendo V irreducible entonces está contenida en algunas de las variedades V_i.

Nota: esta proposición no se verifica si V no es irreducible.

Contraejemplo: la variedad formada por los puntos (0,1) y (0, -1) está contenida en la unión de os variedades sin estarlo en ninguna de las dos.

#

.

TEOREMA DE LA BASE DE HILBERT

Arturo Rodríguez Rodríguez

TEOREMA DE LA BASE DE HILBERT

CONCEPTOS PREVIOS

En lo que sigue supondremos que A es un anillo conmutativo y con unidad.

Definición: Ideal de A.

Un subconjunto no vacío I de A es un ideal de A si:

- $a, b \quad I$ se tiene $a + b \epsilon I$
- $a \epsilon I, \quad x \epsilon A$ se tiene $a \, . \, x \epsilon I$

Definición: Ideal finitamente generado

Sea $L = \{Xi\}\ ieI$. Se define el ideal generado por L como

$$(L)\ A = \{x \in A : x = \sum \quad , \ i = 1 \ldots r, \ \text{para ciertos,} \ r \in Z+, \ a_i \in A, \ Xi \epsilon L\}$$

Un ideal se dice finitamente generado cuando admite ser generado por un conjunto finito.

Definición: Anillo noetberiano.

Un anillo es noetheriano cuando todos sus ideales son finitamente generados.

Proposición.

Son

equivalentes:

- A es noetheriano
- Todo conjunto no vacío de ideales de A admite un elemento maximal.
- A cumple la siguiente condición de cadena ascendente. Si

$$\text{lo} \quad 1_1 \subseteq 1_2 \subseteq \ldots \ In \subseteq ln+1 \subseteq \ldots$$

es una cadena de ideales de A entonces existe $N \in N$ tal que $1_N = 1_{N+1} = 1_{N+2} = \ldots$

Axioma de elección (AE)

Para todo conjunto A y cada partición p de A existe un conjunto B de representantes.

Intuitivamente, AE dice que dada una colección de subconjuntos no vacíos de un conjunto, se puede tomar exactamente un elemento de cada uno de estos subconjuntos.

TEOREMA DE LA BASE DE HILBERT

Si *A* es un nillo noetheriano => *A [X]* es anillo noetheriano.

Demostración

Procedemos por reducción al absurdo. Supongamos que existe un ideal *1* de *A [X]* que no es finitamente generado.

Construimos una sucesión de polinomios del modo siguiente

- Sea E I \ {O} tal que grado( ) = min{grado(f), f E I \ {O}}
- Sea E *1* \ ( )*A[X]* tal que grado( ) = min{grado(f), *f* E *1* \ ( )*A[XI)*
- Sea E *1* \ ( )*A[X]* tal que

grado ( ) = min {grado *(f), f* E *1* \ (,)*A[XI)*

y así seguimos

Obsérvese que, como I no es finitamente generado, entonces para cada *n* EN es

1 \ (, , ... ,)*A[X]*

Nótese que en la construcción de esta sucesión estamos empleando el axioma de elección.

Para cada *n* EN denotaremos

a_n = I( ) = coeficiente principal de y d_n = grado de

Observamos que la sucesión de los grados de los polinomios elegidos es no decreciente, esto es,

$d_1 \; d_2 \; d_3$

Consideramos ahora la siguiente cadena de ideales de *A* :

= ( )*A*, = ( )*A*, ⋯,J_n = (a_2,⋯,a_n)*A*, ...

Es claro que $\subseteq J_2 \subseteq J_3 \subseteq \ldots \subseteq J_n \subseteq J_{n+1} \subseteq \ldots$ y por ser A un anillo noetheriano N ∈N tal que $n \sim N$ se tiene $J_n = J_N$.

Por tanto existen ,…, ϵ A con =∑
Construimos el polinomio g

G= - -….-

De este modo el polinomio g construido cumple

1) gϵ I\ (,…,)A[X]
2) grado (g) grado ( )

Por tanto, todo ideal de $A[X]$ es finitamente generado, por lo que $A[X]$ es noetherianoo

CONSECUENCIAS DEL TEOREMA DE LA BASE DE HiLBERT

Corolario 1

Si A es un anillo noetheriano entonces cualquier anillo de polinomios sobre A en un número finito de indeterminadas es noetheriano.

Demostración

Demostraremos el resultado por inducción sobre el número de indeterminadas.

i) Si A es un anillo noetheriano, entonces acabamos de probar que el anillo de polinomios en una indeterminada sobre A, $A[X]$ es noetheriano.

ii) Suponemos ahora que se cumple que si A es un anillo noetheriano entonces el anillo de polinomios sobre A en n -1 indeterminadas, es noetheriano.

Sea pues A un anillo noetheriano; entonces por la hipótesis de inducción

A[,…] es noetheriano. Aplicando ahora (i) (A [, …, ,] es noetheriano.

Corolario 2

Si K es un cuerpo entonces K [,…] es noetheriano.

Demostración

Por ser K un cuerpo es noetheriano ya que los cuerpos tienen solo dos ideales (O) y (1) = K , Y ambos son finitamente generados. Luego aplicando el corolario 1 tenemos el resultado.

ÍNDICE