

Capítulo 1 - Conjuntos Algebraicos Afines

1.1 Preliminares Algebraicos

Definiciones y Teoremas:

Definición 1: Un dominio entero (integral) es un anillo en donde la ley de cancelación se cumple, es decir, no hay divisores de cero. De forma corta, hablamos de "dominio".

Definición 2: Un campo (no cuerpo) es un anillo en donde todo elemento menos el cero es una unidad.

Definición 3: Cualquier dominio R posee un campo de fracciones K , es decir, un campo que contiene R como un subanillo.

Definición(es) 4: Para un anillo R , $R[X]$ denota el anillo de polinomios en R . El grado de un polinomio no nulo $\sum a_i X^i$ es el entero más grande d que acompaña al *término principal*. Un polinomio es *mónico* si el término principal es 1.

(*) El anillo de polinomios en n variables sobre R se denota $R[X_1, \dots, X_n]$

Definición 5: Denominamos a un polinomio F *homogeneo* o una *forma* de grado d , si todos los coeficientes a_i son nulos excepto para los monomios de grado d . (Todos los monomios poseen grado d).

(*) Todo polinomio F se puede expresar como $F = F_0 + F_1 + \dots + F_d$, donde F_i es la *forma* de grado i . Si $F_d \neq 0$, $\deg F = d$.

Definición 6: El anillo $R[X_1, \dots, X_n]$ es canonicamente isomorfo a $R[X_1, \dots, X_{n-1}][X_n]$

Definición 7: Un elemento $a \in R$ se dice irreducible si no es una unidad o el cero, y para cualquier factorización $a = bc$, $b, c \in R$, entonces b o c es una unidad. (Recordar que irreducible implica primo, pero no al revés!).

Definición 8: Un dominio es un *Dominio de Factorización Única* (DFU/UDF) si cada elemento en R puede ser factorizado de forma única. Ver directamente que $R[X]$ es un UDF para R UFD (parte del lema de Gauss).

Definición 9: Un *ideal* es propio si $I \neq R$. Un ideal es *maximal* si no está contenido en otro ideal propio. Un ideal es *primo* si es un ideal I tal que si $ab \in I$, entonces $a \in I$ o $b \in I$.

Definición 10: Un ideal es *finitamente generado* si es generado por un conjunto finito $S = \{f_1, \dots, f_n\}$, para esto denotamos $I = (f_1, \dots, f_n)$. Un ideal es principal si es generado por un elemento. Un dominio en donde cada ideal es principal se denomina *dominio ideal principal* (DIP/PID) (pensar en \mathbb{Z} , $\mathbb{Z}[X]$, $k[X]$ para cualquier campo k , pero no en $R[X_1, \dots, X_n]$ para $n \geq 2$.)

Definición 11: Cada DIP es un *Dominio de Factorización Única* (DFU/UDF). Un ideal $I = (a)$ principal en un UFD es primo si y solo si a es irreducible (o no nulo).

Definición 12: Sea R dominio. La *característica* de R , $\text{char } R$, es el entero más pequeño p tal que $1 + \dots + 1$ p veces $= 0$

Definición 12: Sea R anillo, $a \in R$, $F \in R[X]$, a es una raíz de F , entonces $F = (X - a)G$ para un único $G \in R[X]$. Un campo k es *algebraicamente cerrado* si para cualquier polinomio no constante $F \in k[X]$ posee una raíz en k

1.1

(a) Sean $F = \sum_{i=0}^n a_i f_i(X_1, \dots, X_n)$ y $G = \sum_{j=0}^m b_j g_j(X_1, \dots, X_n)$ polinomios homogéneos donde $\deg f_i = r$ y $\deg g_j = s$ para todo i, j . Luego:

$$F \cdot G = \sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_i b_j \right) (f_i g_j)(X_1, \dots, X_n)$$

Como R es dominio entero, $\deg f_i g_j = \deg f_i + \deg g_j = r + s$

b) Suponer que $F = F_1 \cdot F_2$ (donde F_i ($i = 1, 2$) no es trivial al ser R dominio), sean d_1 y e_1 el mayor y menor grado respectivamente de los términos de F_1 y sean d_2 y e_2 respectivamente el mayor y menor grado de F_2 . El producto de los términos de grado d_1 de F_1 y d_2 de F_2 es no nulo y es de grado $d_1 + d_2$. Respectivamente el producto de los términos de grado e_1 de F_1 y e_2 de F_2 posee grado $e_1 + e_2$. Como F es homogéneo, $d_1 + d_2 = e_1 + e_2$. Sigue que $0 = (d_1 - e_1) + (d_2 - e_2)$, los sumandos son no-negativos, por lo que $d_1 = e_1$ y $d_2 = e_2$. Sigue que F_1 y F_2 son homogéneos.

1.2

1.3

Como R es un PID, todo ideal está generado por un elemento, entonces $P = (p)$, como es primo, $ab \in (P)$, entonces $a \in (P)$ o $b \in (P)$, esto es equivalente a que $p \mid ab$, entonces $p \mid a$ o $p \mid b$. Para ver que es irreducible, hay que ver si $p = xy$, entonces x o y es una unidad de R , supongamos que $x \in (p)$ (recordar la definición de ideal primo!)

$$\implies x = k \cdot p$$

$$\implies p = kpy$$

$$\implies 1 = ky$$

Entonces y es unidad.

b) Para probar que I es maximal, vamos a aprovechar que R es un PID, suponer que hay I tal que $P \subset I \subset R$, entonces $I = (q)$, entonces $(p) \subset (q)$ si y solo si $p = kq$. Pero entonces k o q es unidad, si k es unidad, entonces $q = k^{-1}p$ y

1.4

Sea $k = 1$, entonces $F \in k[X_1]$, entonces $F(a_1) = 0 \forall a_1 \in k$, por lo que $F = 0$

Supongamos que se cumple para $k = n - 1$ variables

Sea $k = n$. Entonces, $F = \sum F_i(a_1, \dots, a_{n-1})a_n^i = 0$, como $F_i = 0$ para (a_1, \dots, a_{n-1}) , entonces $F = 0 \forall a_1, \dots, a_n \in k$

1.5

Suponer que hay finitos polinomios mónicos irreducibles F_1, \dots, F_n , Sea $F = F_1 \dots F_n + 1$, entonces F es mónico irreducible o un producto de irreducibles, en el primer caso obtenemos una contradicción de lo que hemos supuesto, así que consideramos el segundo caso

1.6

Si k es un campo finito con elementos a_1, \dots, a_n , el polinomio $f(X) = 1 + \prod_{i=1}^n (X - a_i)$ no posee raíz en k , por lo que no es algebraicamente cerrado.

1.7

1.2 Espacio Afín y Conjuntos Algebraicos

Definiciones y Teoremas:

Definición 1: Sea k un campo cualquiera. Denotamos por $\mathbb{A}^n(k)$ al conjunto de n -tuplas con entradas en k . Denominamos este espacio como el *(n-)espacio afín*.

Definición 2: Para $F \in k[X_1, \dots, X_n]$ un punto $P \in \mathbb{A}^n(k)$ se denomina un *cero* de F si $F(P) = F(a_1, \dots, a_n) = 0$. Si F no es constante, el conjunto de ceros de F se denomina *hipersuperficie* definida por F y denotada por $V(F)$.

(*) Generalmente, si S es un conjunto de polinomios en $k[X_1, \dots, X_n]$, definimos $V(S) = \{P \in \mathbb{A}^n(k) \mid F(P) = 0 \ \forall F \in S\}$. Si $S = \{F_1, \dots, F_r\}$ escribimos $V(F_1, \dots, F_r)$.

Propiedades: Se cumplen las siguientes propiedades:

- (1) Si I es el ideal en $k[X_1, \dots, X_n]$ generado por S , entonces $V(S) = V(I)$, por lo que cada conjunto algebraico es igual a $V(I)$ para algún ideal I .
- (2) Si $\{I_\alpha\}$ es cualquier colección de ideales, entonces $V(\bigcup_\alpha I_\alpha) = \bigcap_\alpha V(I_\alpha)$, por lo que cualquier colección de conjuntos algebraicos es un conjunto algebraico.
- (3) Si $I \subset J$, entonces $V(I) \supset V(J)$.
- (4) $V(FG) = V(F) \cup V(G)$ para polinomios F, G cualquiera; $V(I) \cup V(J) = V(\{FG \mid F \in I, G \in J\})$; por lo que cualquier unión finita de conjuntos algebraicos es un conjunto algebraico.
- (5) $V(0) = \mathbb{A}^n(k)$; $V(1) = \emptyset$; $V(X_1 - a_1, \dots, X_n - a_n) = \{a_1, \dots, a_n\}$ para todo $a_i \in k$. Entonces, cualquier subconjunto finito de $\mathbb{A}^n(k)$ es un conjunto algebraico.

1.8

Sea $\mathbb{A}^1(k)$, entonces estamos en $k[X_1]$, por lo que estamos en un PID. Sea el ideal (F) .

- a) Si $F = 0$, trivialmente, $V(0) = \mathbb{A}^1(k)$
- b) Si F es no nulo, entonces por el teorema fundamental del álgebra, $f(X)$ posee a lo más n soluciones diferentes, por lo que $V(p) = \{P \in \mathbb{A}^n \mid F(P) = 0\} = \{a_1, \dots, a_n\}$

1.9

Sea el ideal I_p de polinomios que se anulan en p , es decir $I_p = (X_1 - a_1, \dots, X_n - a_n)$. Si k es finito, un punto cualquiera (a_1, \dots, a_n) puede ser de k^n formas diferentes, por lo que cada subconjunto de $\mathbb{A}^n(k)$ es finito. Dado cualquier conjunto finito de puntos: p_1, \dots, p_j , si I_{p_i} es el ideal de polinomios anulándose en p_i , entonces cada conjunto finito está definido como $V(I_1) \cup \dots \cup V(I_j) = v(I_1, \dots, I_j)$.

1.10

Sea $\mathbb{Z} \subset \mathbb{R}$, sean la colección de conjuntos algebraicos de $\mathbb{A}^1(\mathbb{R})$, de la forma $V(X - k)$: $\{V(X - k)\}_{k \in \mathbb{Z}}$, esta colección es contable, luego $\bigcup_{k \in \mathbb{Z}} V(X - k)$ no es algebraica. (Cada subconjunto debe ser finito)

1.11

a) $\{(t, t^2, t^3) \in \mathbb{A}^3(k) \mid t \in k\}$. El conjunto corresponde a las soluciones simultáneas de $y = x^2$ y $z = x^3$, es decir el conjunto $V(y - x^2) \cap V(z - x^3) = V(x^2 - y, x^3 - z)$

b) $\{(\cos t, \sin t) \in \mathbb{A}^2(\mathbb{R}) \mid t \in \mathbb{R}\}$. El conjunto corresponde a las soluciones de la ecuación $X^2 + Y^2 = 1$, entonces $V(X^2 + Y^2 - 1)$ es conjunto algebraico.

c) $\{(r, \theta) \in \mathbb{A}^2(\mathbb{R}) \mid r = \sin \theta\}$. Por coordenadas polares, $x = r \cos \theta$, $y = r \sin \theta$, entonces $x = \sin \theta \cos \theta$; $y = \sin^2 \theta$. Estas ecuaciones cumplen: $y = 1 - \cos^2(\theta) \implies \cos \theta = \sqrt{1 - y}$.

Entonces: $x = \sqrt{y} \sqrt{1 - y} \implies x^2 = y(1 - y) \implies x^2 = y - y^2 \implies V(x^2 + y^2 - y)$

1.12

Sea $L : V(Y - (aX + b))$, entonces $Y = aX + b$, sea $F \in k[X, Y]$, por lo que $F(X, Y)$, reemplazando $Y = aX + b$, se obtiene $F(X, aX + b)$, por lo que tenemos una ecuación en una variable. Por el teorema fundamental del álgebra, hay a lo más n soluciones diferentes.

1.13

(a) $\{(x, y) \in \mathbb{A}^2(\mathbb{R}) \mid t \in k\}$

Se tiene que la curva $y = \sin x$ y la recta $y = 0$ poseen infinitos puntos de intersección, esto no pasa con los conjuntos algebraicos. Ver que la unión de los conjuntos algebraicos descritos por las soluciones $a + 2\pi k$ no es conjunto algebraico. (ver ejercicio 1.10)

(b) $\{(z, w) \in \mathbb{A}^2(\mathbb{C}) \mid |z|^2 + |w|^2 = 1\}$, donde $|x + iy|^2 = x^2 + y^2$ para $x, y \in \mathbb{R}$

Sea $|z|^2 + |w|^2 = 1$, finando $z = 0$, entonces $|w|^2 = 1$, llevando w a coordenadas polares se obtiene que $|r \operatorname{cis} \theta|^2 = 1$, entonces $|\operatorname{cis} \theta| = 1/r^2$, entonces nos encontramos en un círculo, por lo que existen infinitas soluciones para θ .

$\{(\cos t, \sin t, t) \in \mathbb{A}^3(\mathbb{R}) \mid t \in \mathbb{R}\}$

Se tiene que esta es la hélice, los puntos de la forma $(\cos 2k\pi, \sin 2k\pi, 2k\pi)$ poseen infinitos puntos de intersección con la hélice.

1.14

Sea $n \geq 1$, como k es algebraicamente cerrado, el polinomio $F(1, \dots, 1, X_n)$ posee solamente soluciones finitas por el teorema fundamental del álgebra. por lo que el subconjunto:

$$\{(1, \dots, 1, a_n) \mid f(1, \dots, 1, a_n) \neq 0\} \subset \mathbb{A}^k - V(F)$$

es infinito, entonces $\mathbb{A}^k - V(F)$ lo es. Luego, sea $n \geq 2$, se cumple que para todo $a_1, a_2, \dots, a_{n-1} \in k$, el polinomio $F(a_1, a_2, \dots, a_{n-1}, X_n)$ posee al menos una raíz por el teorema fundamental del álgebra. por lo que $V(F)$ es finito. (no confundir los a_1, \dots, a_{n-1} , como valores fijos, notar el *para todo* al comienzo.)

1.15

Sea $F \in I(V)$ tal que $F(a_1, \dots, a_n) = 0$ y $G \in I(W)$ tal que $G(b_1, \dots, b_m) = 0$. Se definen:

$$\begin{aligned} F &= F'[X_1, \dots, X_n, X_{n+1}, \dots, X_m] \\ G &= G'[X_1, \dots, X_n, X_{n+1}, \dots, X_m] \end{aligned}$$

polinomios que les faltan algunas variables y que esto permite que aún sigan anulándose en los puntos anteriores; entonces:

$$V \times W = F(F' \cdot G')$$

1.3 El Ideal de un Conjunto de Puntos

Definiciones y Teoremas:

Definición 1: Para cualquier subconjunto X de $\mathbb{A}^n(k)$, se tiene que el conjunto de polinomios que se anulan en X forman un ideal en $k[X_1, \dots, X_n]$; este se denota como $I(X)$ y se define como:

$$I(X) = \{F \in k[X_1, \dots, X_n] \mid F(a_1, \dots, a_n) = 0 \quad \forall (a_1, \dots, a_n) \in X\}$$

Propiedades:

(6) Si $X \subset Y$, entonces $I(X) \supset I(Y)$.

(7) $I(\emptyset) = k[X_1, \dots, X_n]$; $I(\mathbb{A}^n(k)) = (0)$ si k es un campo infinito; $I(\{(a_1, \dots, a_n)\}) = (X_1 - a_1, \dots, X_n - a_n)$ para $a_1, \dots, a_n \in k$.

(8) $I(V(S)) \supset S$ para cualquier conjunto S de polinomios; $V(I(X)) \supset X$ para cualquier conjunto X de puntos.

(9) $V(I(V(S))) = V(S)$ para cualquier conjunto S de polinomios y $V(I(V(I(X)))) = I(X)$ para cualquier conjunto X de puntos. Entonces, si V es un conjunto algebraico, $V = V(I(V))$ y si I es el ideal de un conjunto algebraico, $I = I(V(I))$.

(*) Si $I = I(X)$ con X conjunto algebraico, entonces si $F^n \in I$ para algún entero $n > 0$, entonces $F \in I$.

Definición 2: Se define el *radical* de un ideal como:

$$\text{Rad}(I) = \{a \in R \mid a^n \in I, \text{ para algún } n \in \mathbb{N}\}$$

Se tiene que $\text{Rad}(I)$ es un ideal conteniendo I . Un ideal I se dice *ideal radical* si $I = \text{Rad}(I)$.

Propiedad 3: $I(X)$ es ideal radical para cualquier $X \in \mathbb{A}^n(k)$.

Ejercicios:

1.16

\implies) Supongamos que $V = W$. Luego, sease $f \in I(V)$, entonces para $p \in V$, $f(p) = 0$, pero $p \in W$ también, por lo que $f \in I(W)$. La igualdad se obtiene argumentando del mismo modo para $I(W)$.

\impliedby) Supongamos que $I(V) = I(W)$. Sea $p \in V$, por suposición hay $f \in I(V)$ tal que $f(p) = 0$, luego, $f \in I(W)$ también, entonces $p \in W$. Del mismo modo, la igualdad se obtiene cambiando en el argumento $I(V)$ por $I(W)$ de orden.

1.17

(a) Sea $f \in I(V)$, se puede definir F como $F(X_1, \dots, X_n) = \frac{f(X_1, \dots, X_n)}{f(P)}$

(b) Para cada punto, podemos definir un polinomio igual que en la parte (a) tal que solamente se anule en los demás puntos menos uno, formalmente:

Para todo elemento en $\{1, \dots, r\}$, se define el conjunto algebraico $V_i = \{P_1, \dots, P_{i-1}, P_{i+1}, \dots, P_r\}$, se define el polinomio que se anula en todos los conjuntos de la forma V_j : $G_i(V_i)$, pero que $G_i(P_i) \neq 0$, entonces:

$$F = \frac{G_i}{G_i(P_i)}$$

(c) Considerar P_1, \dots, P_r como antes, queremos construir una función tal que $G_i(P_j) = a_{ij}$ para todo i, j , para esto nos aprovechamos de la sumatoria:

$$G_i = \sum_j a_{ij} F_j$$

Directamente podemos ver que $F_j(P_i)$ se anula si $j \neq i$, por lo que $G_i = a_{ij}$

1.18

(a) Sea

$$(x + y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^{n+m-k} y^k$$

Se tiene que para todo $0 \leq k \leq m$, el grado que de x es $\geq n$ y para todo $m \leq k \leq n+m$, todo grado y es $\geq m$, por lo que cada monomio de la sumatoria pertenece a I y a consecuencia, la sumatoria en sí.

(b) Sea $a + b \in R$, donde $a^n \in I$ y $b^m \in I$

- $(a + b)^{n+m} \in I \implies a + b \in \text{Rad } I$
- $(ab)^{nm} = (a^n)^m \cdot (b^m)^n \in I \implies ab \in \text{Rad } I$
- Sea $x \in R$ y $a \in \text{Rad } I \implies (ax)^n = a^n x^n \in I \implies ax \in \text{Rad } I$

(c) Hay que probar $\text{Rad } I = \text{Rad}(\text{Rad } I)$

\subset) Sea $x \in \text{Rad } \text{Rad } I \iff x^n \in \text{Rad } I \iff (x^n)^n \in I \implies x \in \text{Rad } I$

⊃) Sea $x \in \text{Rad } I \iff x^n \in I \iff (x^n)^n \in I \implies x^n \in \text{Rad } I \implies x \in \text{Rad Rad } I$

(d) Sea P ideal primo.

Sea $x \in \text{Rad } P$, por definición $x^n \in P$, como P es primo $x \in P$ o $x^{n-1} \in P$, en el primer caso directamente demostramos que $x \in P$, en el segundo caso argumentamos de forma inductiva x^{n-1} veces.

Sea $x^n \in P$, con $n \in \mathbb{N}$ minimal, entonces $x \in P$ o $x^{n-1} \in P$, en el primer caso directamente $x \in P$, en el segundo encontramos una contradicción ya que tomamos n minimal.

1.19

Para mostrar que es radical solo falta ver que es ideal primo, como el polinomio que describe $X^2 + 1$ es irreducible en $\mathbb{R}[X]$, es ideal maximal y por lo tanto primo (su discriminante es negativo), y por lo tanto $(X^2 + 1) = \text{Rad}(X^2 + 1)$. Se tiene que $V(X^2 + 1)$ no describe ningún conjunto en $\mathbb{A}^1(\mathbb{R})$, ya que \mathbb{R} no es algebraicamente cerrado.

1.20

(a)

\implies) Para $P \in V(I)$, todo $f \in I$ cumple que $f(P) = 0$, pero entonces $f^n(x) = 0$ también, es decir $f^n \in I$, esto es la definición de que $f \in \text{Rad } I$. Concluimos que $P \in V(\text{Rad } I)$.

\impliedby) Sea $P \in V(\text{Rad } I)$, entonces $\forall f \in \text{Rad } I$ tal que $f(P) = 0$, $f^n \in I$, en donde $f^n(P) = 0$, por lo que $P \in V(I)$.

(b)

Para $f \in \text{Rad } I$, hay $n \in \mathbb{N}$ tal que $f^n \in I$, por lo que f^n se anula en $V(I)$, es decir, para todo $x \in V(I)$, $f^n(x) = 0 \iff f(x) = 0 \quad \forall x \in V(I)$. Es decir, $f(x) \in I(V(I))$.

1.21

(a) Sea $\varphi : k[x_1, \dots, X_n] \rightarrow k$ el mapa de evaluación. Entonces el kernel está descrito por aquellos polinomios en donde $f(a_1, \dots, a_n) = 0 \iff (X_i - a_i) \mid f(X_1, \dots, X_n) \quad \forall i \in \{1, \dots, n\}$. Entonces $\ker \varphi \subset (X_1 - a_1, \dots, X_n - a_n)$. La otra inclusión es directa, ya que todo polinomio en I se cancela en el punto (a_1, \dots, a_n) . Es decir $\ker \varphi = (X_1 - a_1, \dots, X_n - a_n)$.

La imagen está dada por k . Ya que para todo $a \in k$ puedo definir el polinomio constante $a \in k[X_1, \dots, X_n]$. Por lo que $k[X_1, \dots, X_n]/I \cong k$.

(b) Para ver que el mapeo es isomorfismo solo basta ver que es la inversa de φ . O también ver que el kernel solo puede ser el (0) y que para toda clase de equivalencia $a + I$ puedo definir $a \in k$.

1.4 Teorema de la base de Hilbert

Teoremas y Definiciones:

Teorema 1: Cada conjunto algebraico es la intersección de un número finito de hiper superficies.

Teorema 2 (Teorema de la base de Hilbert): Si R es un anillo noetheriano, entonces $R[X_1, \dots, X_n]$ es noetheriano.

Corolario 3: $k[X_1, \dots, X_n]$ es noetheriano para todo campo k .

Ejercicio:

1.22 Sea I un ideal en un anillo R , $\pi : R \rightarrow R/I$ el homomorfismo natural.

(a) Mostrar que cada ideal J' de R/I , $\pi^{-1}(J') = J$ es un ideal de R conteniendo I y por cada ideal J de R conteniendo I , $\pi(J) = J'$ es un ideal de R/I

Sea I un ideal en R , se define la función $\pi : \{J \subseteq R \mid I \subseteq J\} \rightarrow \{J' \subseteq S/I\}$, tal que $f(S) = S/I$, la función está bien definida.

Sea $a + I, b + I \in S/I$ para $a, b \in S$

$$\begin{aligned}\pi(a + b) &= (a + b) + I = (a + I) + (b + I) \text{ en } S/I \\ \pi(ab) &= ab + I = (a + I)(b + I) \in S/I\end{aligned}$$

Entonces S/I es subanillo de R/I .

La función es inyectiva, si $\pi(S_1) = \pi(S_2) \iff a + I = b + I \iff a - b + I = I \iff a = b$ para $a \in S_1$ y $b \in S_2$. La función es sobreyectiva ya que siempre se puede definir para $a + I$, con a tal que $\pi(a) = a + I$.

(b) Mostrar que J' es ideal radical si y solo si J es radical. Similarmente para ideales primos y maximales.

1b) \implies Si J' es radical, entonces para todo $x + I \in R/I$, $(x + I)^n \in J'$ por lo que $x + I \in J'$, entonces $\pi^{-1}(x^n + I) = x^n \in J$, por lo que $\pi^{-1}(x + I) \in J$.

\iff Si J es radical, entonces $x^n \in J$, entonces $x \in J$, entonces $\pi(x^n) = x^n + I \in J'$, por lo que $xI \in J'$

2b) \implies Si J' es ideal primo, entonces para $ab + I \in J'$ entonces $a + I \in J'$ o $b + I \in J'$, es decir $\pi^{-1}(ab + I) = ab \in J$, entonces $a \in J$ o $b \in J$. La otra implicancia se obtiene a través del mapa inverso.

3b) Si J' es maximal, $K' = J'$ o $K' = R/I$. Si $K' = R/I$, entonces K contiene elementos no en J , entonces $K = R$. Conversamente, si $K' = J'$, entonces $K \subseteq J$, entonces $K = J$. Entonces J es maximal. La implicancia contraria se prueba de forma similar.

(c) Mostrar que si J' es finitamente generado si J lo es. Concluir que R/I es noetheriano si R es noetheriano. Cualquier anillo de la forma $k[X_1, \dots, X_n]/I$ es noetheriano.

Si J es un ideal finitamente generado en R , entonces podemos escribir

$$J = \langle x_1, x_2, \dots, x_n \rangle$$

para algunos $x_1, x_2, \dots, x_n \in R$.

Como π es un homomorfismo, tenemos

$$\pi(J) = \pi(\langle x_1, x_2, \dots, x_n \rangle) = \langle \pi(x_1), \pi(x_2), \dots, \pi(x_n) \rangle.$$

Por lo tanto, $J_0 = \pi(J)$ es finitamente generado en R/I .

Por el contrario, si J_0 es finitamente generado en R/I , entonces

$$J_0 = \langle x_1 + I, x_2 + I, \dots, x_n + I \rangle,$$

y la preimagen $J = \pi^{-1}(J_0)$ está generada por x_1, x_2, \dots, x_n , por lo que J es finitamente generado en R .

Así, J_0 es finitamente generado si y solo si J es finitamente generado.

Si R es Noetheriano, entonces todo ideal de R es finitamente generado. Como $J_0 = \pi(J)$ es finitamente generado si J lo es, se sigue que R/I también es Noetheriano.

Cualquier anillo de la forma $k[X_1, X_2, \dots, X_n]/I$ es Noetheriano porque el anillo de polinomios $k[X_1, X_2, \dots, X_n]$ es Noetheriano, y I es un ideal en ese anillo.

Así, concluimos que R/I es Noetheriano si R es Noetheriano, y cualquier anillo de la forma $k[X_1, X_2, \dots, X_n]/I$ es Noetheriano.

Componentes Irreducibles de un Conjunto Algebraico

Teoremas y Definiciones

Proposición 1: Un conjunto algebraico V es irreducible si y solo si $I(V)$ es primo

Lema 2: Sea T cualquier colección no vacía de ideales en un anillo noetheriano R . Entonces T posee un elemento maximal, es decir, hay un ideal $I \in T$ que no está contenido en cualquier otro ideal de T .

(*) Sigue inmediatamente que cualquier colección de conjuntos algebraicos en $\mathbb{A}^n(k)$ posee un elemento minimal. Si $\{V_\alpha\}$ es una colección, tomar el elemento maximal $I(V_{\alpha_0})$ de $\{I(V_\alpha)\}$. Entonces V_{α_0} es un elemento minimal de la colección.

Teorema 3: Sea V un conjunto algebraico en $\mathbb{A}^n(k)$. Entonces hay conjuntos algebraicos irreducibles únicos V_1, \dots, V_m tal que $V = V_1 \cup \dots \cup V_m$ y $V_i \subset V_j$ para todo $i \neq j$.

(*) Los V_i se denominan los componentes irreducibles de V ; $V = V_1 \cup \dots \cup V_m$ es la descomposición de V en componentes irreducibles.

Ejercicios:

1.25

(a) Para ver esto, definimos el mapa:

$$\begin{aligned}\varphi: \mathbb{C}[X, Y] &\rightarrow \mathbb{C}[X] \\ x &\mapsto x \\ y &\mapsto x^2\end{aligned}$$

Vemos que el kernel de este mapa corresponde a $(Y - X^2)$. Si $f \in \ker \varphi$, entonces se cumple que $f(x, x^2) = 0$ si y solo si el polinomio $Y - X^2$ divide a f , entonces $f \in (Y - X^2)$. Luego, directamente $Y - X^2 \in \ker \varphi$ (verlo evaluando directamente). Entonces $\mathbb{C}[X, Y]/(Y - X^2) \cong \mathbb{C}[X]$, en donde $\mathbb{C}[X]$ es dominio (entero). Por lo que $(Y - X^2)$ es ideal primo.

(b) Ver que estamos trabajando en \mathbb{C} . Factorizaremos los polinomios uno a uno:

- $Y^4 - X^2 = (Y^2 + X)(Y^2 - X)$
- $Y^4 - X^2Y^2 + XY^2 - X^3 = Y^2(Y^2 - X^2) + X(Y^2 - X^2) = (Y^2 + X)(Y^2 - X^2) = (Y^2 + X)(Y + X)(Y - X)$

Entonces $V(Y^4 - X^2, Y^4 - X^2Y^2 + XY^2 - X^3) = V((Y^2 - X)(Y^2 + X), (Y^2 + X)(Y + X)(Y - X)) = V(Y^2 + X) \cup V((Y^2 - X)(Y + X)(Y - X))$

Ahora hay que estudiar $V((Y^2 - X)(Y + X)(Y - X)) = V(Y^2 - X) \cap V(Y + X) \cap V(Y - X)$. Para eso vemos las soluciones simultáneas de:

$$Y^2 - X = Y^2 - X^2$$

Es decir $X = 0$ o $X = 1$. Para $X = 0$ se obtiene que $Y = 0$ y para $X = 1$, también $Y = 0$.

Entonces $V((Y^2 - X)(Y + X)(Y - X)) = V(X, Y) \cup V(X - 1, Y)$

Luego, $V(Y^4 - X^2, Y^4 - X^2Y^2 + XY^2 - X^3) = V(Y^2 + X) \cup V(X, Y) \cup V(X - 1, Y)$. (El primer ideal es primo, se puede ver haciendo el mismo tipo de mapa que en (a)).

1.26

Estamos en característica 0. Supongamos que $Y^2 + X^2(X - 1)^2 \in \mathbb{R}[X, Y]$ es reducible, entonces $F = (a(X)Y + b(X))(c(X)Y + d(X)) = (a(X)c(X)Y^2 + (a(X)d(X) + b(X)c(X))Y + b(X)d(X))$.

Entonces $a(X)c(X) = 1$, por lo que son polinomios constantes y además inversos. Del coeficiente $(a(X)d(X) + b(X)c(X))$ vemos que $d(X) = b(X) = 0$ necesariamente, pero entonces $b(X)d(X) = 0$, pero esto no es posible, porque debe darnos $X^2(1 - X)^2$, por lo que es una contradicción.