Pontificia Universidad Católica de Chile
Facultad de Matemáticas
Departamento de Matemática
Profesor: Giancarlo Urzúa – Estudiante: Benjamín Mateluna

Geometría Algebraica - MAT2824
Apuntes
06 de Marzo de 2025

Índice

Introducción

Habrán tres evaluaciones (I1, I2, I3) cada una vale un 20 % y un examen (EX) que vale un 40 %. Las fechas son, 9 de abril, 14 de Mayo, 11 de Junio y 1 de Julio respectivamente.

1. Conjuntos Algebraicos afines

1.1. Preliminares algebraicos

Sea R un anillo conmutativo con $+, \cdot$ y con $1 \neq 0$. Si R, R' son anillos, un morfismo de anillos es una función $f : R \to R'$ que respeta $+, \cdot$ y $f(1_R) = 1_{R'}$. Un dominio R es un anillo en donde $xy = xz$ implica que $y = z$ para todo $x \neq 0$.

Ejemplo $\mathbb{Z}$ es dominio, pero $\mathbb{Z}/6$ no lo es.

Un cuerpo es un dominio donde todo $x \neq 0$ tiene un inverso. Dado R dominio, existe el cuerpo de fracciones K tal que $R \subseteq K$. Dado R anillo, sea $R[x]$ el anillo de polinomios con coeficientes en R, sus elementos tienen la forma

$$f(x) = a_0 + a_1 x + \cdots + a_d x^d \ , \ a_d \neq 0$$

y decimos que f tiene grado d denotado por $gr(f)$. Se define de manera recursiva $R[x_1, \cdots, x_n] = R[x_1, \cdots, x_{n-1}][x_n]$ el anillo de polinomios en n variables. Dado $f = \alpha \cdot x_1^{\lambda_1} \cdots x_n^{\lambda_n}$ su grado se define como $gr(f) = \sum_{i=1}^n \lambda_i$, para f en general, definimos su grado como $gr(f) := max\{\text{grados de monomios}\}$. Dado $f \in R[x_1, \cdots, x_n]$ y $d = gr(f)$ entonces

$$f = F_0 + F_1 + \cdots + F_d \text{ , con } F_i \text{ homogeneos, esto es, } F_i(\lambda x_{x_1}, \cdots, \lambda x_n) = \lambda^i F(x_1, \cdots, x_n)$$

Si $f \in R[x]$ una raíz (cero) de f es un $r \in R$ tal que $f(r) = 0$.

Teorema 1. *Se tiene que r es cero si y solo si $f(x) = (x - r)g(x)$ para algún $g \in R[x]$.*

Un cero de $f(x_1, \cdots, x_n)$ es un $(a_1, \cdots, a_n) \in \mathbb{R}^n$ tal que $f(a_1, \cdots, a_n) = 0$.

Decimos que $r \in R$ es irreductible si toda descomposición $r = ab$ con $a, b \in R$ se tiene que a o b es una unidad. Un anillo R se dice dominio de factorización unica si todo elemento no nulo se puede factorizar de manera esencialmente unica en producto de irreductibles.

Lema 1.1. *Si R es dominio de factorización unica entonces $R[x]$ es dominio de factorización unica.*

Lema 1.2. *Si R es un dominio de factorización unica y K su cuerpo de fracciones. Dado $f \in R[x]$ irreductible entonces f es irreductible en $K[x]$.*

Sea R un anillo. Un ideal $I \subset R$ es tal que si $a, b \in I$ entonces $a + b \in I$ y si $r \in R$ entonces $ra \in I$. Consideramos la función $\pi : R \to R/I$ donde R/I es el anillo cociente que es conmutativo. Un ideal es maximal si y solo si R/I es cuerpo.

Teorema 2. *Sea R un dominio euclideano (se cumple algoritmo de la división) y $a, b \in R$, consideremos $mcd(a, b) = d$. Entonces existen $c, e \in R$ tales que $ac + be = d$.*

Teorema 3. *Si F es un polinomio homogeneo de grado d, entonces*

$$dF = x_1 F_{x_1} + \cdots + x_n F_{x_n}$$

donde F_{x_i} es la derivada formal con respecto a x_i.

1.2. Espacio Afín y Conjuntos Algebraicos

Definición 3.1. *Sea k un cuerpo. El espacio afín de dim n es $\mathbb{A}_k^n := k^n$ (generalmente se supondra que $k = \overline{k}$).*

Definición 3.2. *Una hipersuperficie de $\mathbb{A}_k^n$ es $V(F) = \{p \in \mathbb{A}_k^n : F(p) = 0\}$ para un $F \in k[x_1, \cdots, x_n]$.*

Ejemplos:

- Sea $k = \mathbb{R}$ consideramos la hipersuperficie $V(y^2 - x^2(x+1)) \subseteq \mathbb{A}^2_{\mathbb{R}}$ (foto)
  El punto $(0,0)$ se llama nodo.
- Veamos la hipersuperficie $V((x^3 - y^3)(y^3 - 1)(x^3 - 1)) \subseteq \mathbb{A}^2_{\mathbb{C}}$.
- La hipersuperficie $V(x^2 + y^2 - z^2) \subseteq \mathbb{A}^3_{\mathbb{R}}$ es conocida como cono (foto)
  Como en el primer ejemplo, el punto $(0,0)$ se llama nodo
- Consideremos $V(y^2 - x^3) \subseteq \mathbb{A}^2_{\mathbb{R}}$ (foto)
  En este caso, el punto $(0,0)$ no es un nodo, en este caso se llama cuspide.
- Veamos el caso de una hipersuperficie no parametrizable, esta es $V(y^2 - x(x+1)(x+\lambda))$.

Definición 3.3. *Sea $S \subseteq k[x_1, \cdots, x_n]$ un conjunto arbitrario, se define*

$$V(S) := \{p \in \mathbb{A}^n_k : F(p) = 0 \quad \forall F \in S\} = \bigcap_{F \in S} V(F)$$

y se dice que es un conjunto algebraico afín.

Propiedades de un conjunto algebraico afín:

a) Sea $I = \langle S \rangle = \left\{ \sum_{i=1}^{n} a_i s_i, a_i \in k \right\}$, entonces $V(I) = V(S)$.

> **Demostración.** *Veamos que $V(I) \subseteq V(S)$, si $p \in V(I)$, como $S \subseteq I$ se sigue que $p \in V(S)$. Para $V(S) \subseteq V(I)$ notemos que dado $f \in I$ se tiene que $f = \sum a_i s_i$, luego si $p \in V(S)$ vemos que $f(p) = \sum a_i s_i(p) = 0$.*

b) Sea $\{I_\alpha\}$ una colección de ideales, entonces $V(\bigcup_\alpha I_\alpha) = \bigcap_\alpha V(I_\alpha)$.

c) Si $I \subseteq J$ se sigue que $V(J) \subseteq V(I)$.

d) Sean $F, G \in k[x_1, \cdots, x_n]$, se tiene que $V(FG) = V(F) \cup V(G)$.

e) Tenemos las siguientes dos identidades $V(1) = \emptyset$ y $V(0) = \mathbb{A}^n_k$.
   observación: Lo anterior es valido si k es algebraicamente cerrado, de lo contrario, si consideramos $\mathbb{A}^1_{\mathbb{R}}$ vemos que $V(x^2+1) = \emptyset$.

1.3. Ideal de un conjunto

Definición 3.4. *Sea $X \subseteq \mathbb{A}^n_k$ un conjunto arbitrario. Se define el ideal de X como*

$$I(X) := \{F \in k[x_1, \cdots, x_n] : F(p) = 0 \quad \forall p \in X\}$$

observación: Notemos que si $F^m \in I(X)$ entonces $F \in I(X)$. Un ideal con esta propiedad se dice radical.

Propiedades del ideal de un conjunto:

a) Si $X \subseteq Y$ se tiene que $I(Y) \subseteq I(X)$.

b) Se tiene lo siguiente $I(\emptyset) = k[x_1, \cdots, x_n]$ y $I(\mathbb{A}^n_k) = \{0\}$. Además, si k es un cuerpo infinito, se tiene que $I(\{a_1, \cdots, a_n\}) = (x_1 - a_1, \cdots, x_n - a_n)$.

1.4. El Teorema de la Base de Hilbert

Teorema 4. *Todo conjunto algebraico corresponde a la intersección finita de hipersuperficies.*

> **Demostración.** *Sea $V(I)$ el conjunto algebraico para algún ideal $I \subseteq k[x_1, \cdots, x_n]$. Basta con probar que I es finitamente generado, en tal caso $I = (F_1, \cdots, F_r)$, entonces $V(I) = V(F_1, \cdots, F_r) = V(F_1) \cap \cdots \cap V(F_r)$.*

Teorema 5. *Si R es un anillo Noetheriano, entonces $R[X]$ es un anillo Noetheriano.*

Demostración. *Sea $I \subseteq R[X]$ un ideal. Dado $F = a_0 + a_1x + \cdots + a_dx^d$ con $a_d \neq 0$ decimos que a_d es el término líder de F denotado por $l(F)$. Sea*

$$\mathcal{J} := \{r \in R : r \text{ es término líder de algún } F \in I\} \cup \{0\}$$

Afirmamos que $\mathcal{J}$ es ideal, en efecto, sean $l(F), l(G) \in \mathcal{J}$, supongamos sin perdida de generalidad que $gr(F) \leq gr(G)$, luego

$$Fx^{gr(G)-deg(F)} + G = H$$

donde $l(H) = l(F) + l(G)$. Es claro que $r \cdot l(F) \in \mathcal{J}$ con $r \in R$. Por hipotesis existen $F_1, \cdots, F_r \in I$ tales que $\mathcal{J} = (l(F_1), \cdots, l(F_r))$. Sea $N > gr(F_i)$ para todo $1 \leq i \leq r$. Para cada $m \leq N$ definimos

$$\mathcal{J}_m := \{r \in R : r \text{ es término líder de } F \in I \text{ y } gr(F) \leq m\}$$

Notemos que los $\mathcal{J}_m$ son ideales en R, por ende, son finitamente generados, es decir $\mathcal{J}_m = (l(F_{m,j}))$. Consideremos el ideal $I' = \langle F_{m,j}, F_i \rangle$, afirmamos que $I' = I$. Claramente se tiene que $I' \subset I$. Supongamos, por contradicción, que $I' \neq I$, sea $G \in I' \setminus I$ de menor grado. Tenemos dos consideramos

a) Veamos cuando $gr(G) > N$, existen polinomios $Q_i \in R[X]$ tal que G y $\sum Q_iF_i$ tienen el mismo coeficiente líder. Luego $G - \sum Q_iF_i \in I'$ pues tiene menor grado que G, se sigue que $G \in I'$.

b) El resultado para $gr(G) \leq N$ se obtiene del mismo modo, usando esta vez los $F_{m,j}$.

Ejemplo: Sea $(0,0) \in \mathbb{A}^2_{\mathbb{R}}$, entonces $\{(0,0)\} = V(x^2 + y^2)$. Pero en $\mathbb{C}$ tenemos que $\{(0,0)\} \neq V(F)$ para ningún $F \in k[x,y]$.

1.5. Componentes Irreducibles en un Conjunto Algebraico

Definición 5.1. *Un conjunto algebraico V se dice reducible si $V = V_1 \cup V_2$ con V_i conjunto conjunto algebraico y distinto de V.*

Observación: Un punto es un conjunto algebraico irreducible, lo que implica que cualquier conjunto finito es algebraico y reducible.

Ejemplos:

- Notemos que $V(xy) = V(x) \cup V(y)$, es decir $V(xy)$ es reducible.
- Consideremos el espacio afín $\mathbb{A}^1_{\mathbb{R}}$, entonces el conjunto algebraico $V((x^2+1)x) = \{0\}$ es irrducible.

Proposición 5.1. *Un conjunto algebraico V es irrducible si y solo si el ideal $I(V)$ es primo.*

Demostración.

- $\Rightarrow$ | *Supongamos que $I(V)$ no es primo, entonces existen F_1, F_2 polinomios tales que $F_1 \cdot F_2 \in I(V)$ y $F_1, F_2 \notin I(V)$. Afirmamos que $V = (V \cap V(F_1)) \cup (V \cap V(F_2))$. Sea $p \in V$, entonces $F_1(p) \cdot F_2(p) = 0$ lo que implica que $p \in (V \cap V(F_1)) \cup (V \cap V(F_2))$, además $V \cap V(F_i) \neq V$ ya que existe q_i tal que $F_i(q_i) \neq 0$.*
- $\Leftarrow$ | *Supongamos que V es reducible. Luego $V = V_1 \cup V_2$ con $V_i \neq V$. Entonces existe un polinomio F_i tal que $F_i(p) = 0$ para todo $p \in V_i$, pero no para todo punto en V. Notemos que $F_1 \cdot F_2 \in I(V)$, sin embargo, $F_i \notin I(V)$.*

Definición 5.2. *Una variedad afín V es un conjunto algebraico afín irreducible.*

Lema 5.1. *Sea R un anillo, las siguientes afirmaciones son equivalentes:*

a) R es Noetheriano.

b) Si $\mathcal{C}$ es una colección no vacía de ideales en R, entonces $\mathcal{C}$ tiene un elemento maximal, es decir, existe $I \in \mathcal{C}$ que no está contenido en otro ideal de $\mathcal{C}$.

c) *Toda cadena ascendente de ideales en R se estabiliza.*

Demostración.

- *(a) $\Rightarrow$(b) | Necesitamos usar el axioma de elección. Sea $\mathcal{C}$ una colección de ideales en R, para cada subconjunto no vacío de $\mathcal{C}$ elegimos un ideal. Sea I_0 el ideal escogido para $\mathcal{C}$, definimos el conjunto*

$$\mathcal{C}_1 := \{I \in \mathcal{C} : I_0 \subset I\}$$

Si $\mathcal{C}_1 = \emptyset$ entonces I_0 es el ideal maximal. Si no, repetimos el proceso. Sea $I \in \mathcal{C}_1$ el escogido, definimos

$$\mathcal{C}_2 := \{I \in \mathcal{C}_2 : I_1 \subset I\}$$

Es suficiente demostrar que existe n tal que $\mathcal{C}_n = \emptyset$. Sea $I = \bigcup_{n=0}^{\infty} I_n$ es ideal, además, notemos que $I_n \subset I_{n+1}$. Como R es Noetheriano, entonces $I = (f_1, \cdots, f_m)$, luego existe r tal que $f_1, \cdots, f_m \in I_r$, lo que implica que $I \subseteq I_r$ y por lo tanto $I = I_r$ se sigue que $I_r = I_s$ para todo $s > r$, lo cual es una contradicción.

- *(b) $\Rightarrow$(c) | Basta tomar $\mathcal{C}$ como nuestra colección de ideales en R, luego, existe un elemento maximal.*

- *(c) $\Rightarrow$(a) | Sea $I \subseteq R$ un ideal. Si $I = (0)$ estamos listos, de lo contrario, sea $f_1 \in I$, entonces $(f_1) \subseteq I$. Supongamos que $I \setminus (f_1) \neq \emptyset$, sea $f_2 \in I \setminus (f_1)$, de esta manera construimos una cadena ascendente de ideales*

$$(f_1) \subset (f_1, f_2) \subset \cdots \subset (f_1, \cdots, f_n) \subset \cdots$$

para algun N la cadena se estabiliza y por ende $(f_1, \cdots, f_N) = I$.

Proposición 5.2. *Cualquier colección de conjuntos algebraicos $\{V_i\}_{i \in I}$ en $\mathbb{A}_k^n$ tiene un elemento minimal.*

Demostración. *Dada $\{V_i\}_{i\in I}$ obtenemos una colección $\mathcal{C} = \{I(V_i)\}_{i \in I}$ de ideales en $k[x_1, \cdots, x_n]$, el cual es Noetheriano. Luego $\mathcal{C}$ tiene un elemento maximal, digamos $I(V_*)$, afirmamos que V_* es el elemento minimal, de lo contrario, existe $V_i \subseteq V_*$ entonces $I(V_*) \subseteq I(V_i)$.*

Teorema 6. *Sea $V \subseteq \mathbb{A}_k^n$ un conjunto algebraico. Entonces existen unicos conjuntos algebraicos irreducibles $V_1, \cdots, V_m$ tales que*

$$V = \bigcup_{i}^{m} V_i \quad y \quad V_i \not\subset V_j \quad \forall i \neq j$$

Demostración. *Sea $\mathcal{C} = \{V \subseteq \mathbb{A}_k^n$ conjunto algebraico : V no es unión finita de irreducibles$\}$. Si $\mathcal{C}$ es vacío estamos listos. Si no lo es, sea $V \in \mathcal{C}$ minimal. Tenemos que V no es irreducible, entonces $V = V_1 \cup V_2$ con $V_i \subset V$, lo que implica que algún $V_i \in \mathcal{C}$ lo cual es una contradicción.*

Sea $V = \bigcup_{i=1}^m V_i$ con V_i irreducibles, asumir que $V_i \not\subset V_j$ para todo $i \neq j$. Digamos que

$$\bigcup_{i=1}^{m} V_i = \bigcup_{j=1}^{s} W_j \quad con \quad V_i \not\subset V_j \quad y \quad W_i \not\subset W_j \quad y \quad V_i, W_j \neq \emptyset$$

Notemos que $V_1 = V_1 \cap V = \bigcup_{j=1}^{s} (V_1 \cap W_j)$, como V_1 es irreducible, existe unico j tal que $V_1 = V_1 \cap W_j$, es decir, $V_1 \subseteq W_j$. Por otro lado, existe unico i tal que $W_j \subseteq V_i$, lo que implica que $V_1 \subseteq V_i$ entonces $i = 1$ y así $V_1 = W_j$.

1.6. Conjuntos Algebraicos del Plano

Lema 6.1. *Si $f, g \in k[x, y]$ no tienen factores en común, entonces $V(f, g)$ es un conjunto finito.*

Demostración. *Recordemos que $k(x)[y]$ es dominio euclideano. Por lema de gauss, f, g no tienen factores en común en $k(x)[y]$, entonces existen $a, b \in k(x)[y]$ tal que $af + bg = 1$. Existe $r(x)$ tal que*

$$raf + rbg = r$$

es una ecuación en $k[x, y]$. Sea $(p, q) \in V(f, g)$, evaluando en la ecuación anterior vemos que

$$0 = raf(p, q) + rbg(p, q) = r(p)$$

por lo tanto la cantidad de valores posibles de p es finita. Haciendo lo mismo para y obtenemos que q solo puede tomar una cantidad finita de valores.

Corolario 6.1. *Si $f \in k[x, y]$ es irreducible con $|V(f)| = \infty$ entonces $I(V(f)) = (f)$ y $V(f)$ es irreducible.*

Demostración. *Si $g \in I(V(f))$, entonces $|V(f, g)| = \infty$, luego, f y g tienen factores en común, como f es irreducible, entonces f divide a g lo que implica que $g \in (f)$. La otra contención es directa.*

Por otro lado, notemos que (f) es primo, pues f es irreducible, así, $V(f)$ es irreducible.

Corolario 6.2. *Supongamos que k es infinito, entonces los conjuntos algebraicos irreducibles de $\mathbb{A}_k^2$ son: $\emptyset$, $\mathbb{A}_k^2$, un punto y los conjuntos $V(f)$ con f irreducible y $|V(f)| = \infty$.*

Demostración. *Sea V un conjunto algebraico irreducible. Si $|V| < \infty$ entonces $V = \emptyset$ o V es un punto. Si $I(V) = (0)$ entonces $V = \mathbb{A}_k^2$. Supongamos que $|V| = \infty$ y que $(0) \subset I(V) \subset k[x, y]$. Como $I(V)$ es primo, existe un polinomio no constante e irreducible tal que $f \in I(V)$.*

Si $g \in I(V)$ y $g \notin (f)$, entonces $V \subset V(f, g)$, por la proposición, esto es una contradicción. De este modo, $I(V) = (f)$. Afirmamos que $V(f) = V$, en efecto, tenemos que $V = V(I(V)) = V(f)$.

Corolario 6.3. *Supongamos que $k = \overline{k}$. Sea $f \in k[x, y]$ y sea $f = \prod_{i=1}^{m} f_i^{\alpha_i}$ con f_i irreducible. Entonces*

$$V(f) = \bigcup_{i=1}^{m} V(f_i)$$

es su descomposición en irreducibles y además $I(V(f)) = (f_1, \cdots, f_m)$.

Demostración. *Como f_i, f_j son coprimos no hay inclusiones entre $V(f_i)$ y $V(f_j)$, de lo contrario si existen $i \neq j$ tales que $V(f_i) \subset V(f_j)$, entonces*

$$(f_i) = I(V(f_i)) \supset I(V(f_j)) = (f_j)$$

lo cual es una contradicción. Luego,

$$I(V(f)) = I\left(\bigcup V(f_i)\right) = \bigcap I(V(f_i)) = \bigcap (f_i) = (f_1 \cdots f_m)$$

1.7. Nullstellensatz de Hilbert

En general supondremos que $k = \overline{k}$, a no ser que se diga lo contrario.

Teorema 7. *Sea $I \subset k[x_1, \cdots, x_n]$ un ideal, entonces $V(I) \neq \emptyset$.*

Demostración. *Podemos suponer que I es maximal. En efecto, recordemos que todo ideal esta contenido en un ideal maximal, digamos M, entonces $V(M) \subseteq V(I)$. $\{\}$Como I es maximal, esto equivale a que $k[x_1, \cdots, x_n]/I \supset k$ es cuerpo. Como k es algebraicamente cerrado, podemos asumir que $k[x_1, \cdots, x_n]/I = k$.*

Así, cada variable x_i puede ser identificada por un elemento en k digamos a_i, lo que implica que $x_i - a_i$ es igual 0 bajo el cociente, se sigue que $x_i - a_i \in I$, luego $I = (x_1 - a_1, \cdots, x_n - a_n)$. (Mejorar escritura)

De la demostración surge una pregunta, ¿Por que $k[x_1, \cdots, x_n]/I = k$? El siguiente lema lo responde

Lema 7.1. *(Lema de Zariski) Sea $K \subset L$ una extensión de cuerpo tal que L es finitamente generado como k-algebra. Entonces L es finitamente generado como k-módulo.*

Exploraremos una demostración menos general del teorema anterior, pero sin usar lema de Zariski. Para ello supongamos que $k = \mathbb{C}$.

Demostración. *Del mismo modo, supongamos que $I \subset k[x_1, \cdots, x_n]$ es un ideal maximal, luego $L := k[x_1, \cdots, x_n]/I$ es cuerpo, consideramos el morfismo canónico*

$$\begin{tikzcd} \mathbb{C}[x_1, \cdots, x_n] \arrow[r, "\pi"] & L \\ \mathbb{C}[x_i] \arrow[u, "i"] \arrow[ur, "\pi_i := \pi\big|_{\mathbb{C}[x_i]}"'] & \end{tikzcd}$$

Afirmamos que $ker(\pi_i) = (0)$ o $ker(\pi_i) = (x_i - a_i)$ para algún $a_i \in \mathbb{C}$. En efecto, si $ker(\pi_i) \neq (0)$, entonces $(0) \subset ker(\pi_i) \subset \mathbb{C}[x_i]$, donde la segunda contención es estricta, de lo contrario, $1 \in I$ y entonces $I = k[x_1, \cdots, x_n]$. Sea $f \in ker(\pi_i)$, entonces como $\mathbb{C}$ es algebraicamente cerrado, existe $(x_i - a_i)$ factor de f tal que $\pi_i(x_i - a_i) = 0$.

Volviendo a la demostración del teorema. Tenemos dos consideramos

- *$ker(\pi_i) = (x_i - a_i)$ para todo i. Entonces $(x_1 - a_i, \cdots, x_n - a_n) \subseteq I$. Como $(x_1 - a_i, \cdots, x_n - a_n)$ es ideal maximal e I es propio se obtiene el resultado.*

- *Existe i tal que $ker(\pi_i) = (0)$, entonces π_i es inyectiva, como L es cuerpo $\mathbb{C}(x_i)$ se incrusta en L.*

$$\begin{tikzcd} \mathbb{C}[x_i] \arrow[r, "\pi_i"] \arrow[d, "i"'] & L \\ \mathbb{C}(x_i) \arrow[ur, "i_L"'] & \end{tikzcd}$$

Es decir $\mathbb{C}(x_i) \subseteq L$. Notemos que L es un espacio vectorial numerable, a saber, la base corresponde a todos los monomios. Notemos que el siguiente conjunto es linealmente independiente

$$S := \left\{ \frac{1}{x_i - a_i} : a \in \mathbb{C} \right\}$$

Notemos que si $\sum_{j=1}^{m} \frac{\lambda_j}{x_i - a_j} = 0$ entonces multiplicando por $(x_i - a_1) \cdots (x_i - a_m)$ y evaluando se tiene que $\lambda_j = 0$ para todo j. Esto es una contradicción pues S es no numerable.

Teorema 8. *(Teorema de Nullstellensatz) Sea $I \subset k[x_1, \cdots, x_n]$, entonces $I(V(I)) = \sqrt{I}$.*

Demostración.

- *$\supseteq$ | Sea $f \in \sqrt{I}$, entonces $f^n \in I$ para algún n. Luego $f^n(p) = 0$ para todo $p \in V(I)$, entonces $f(p) = 0$ para todo $p \in V(I)$ lo que implica que $f \in I(V(I))$.*

- *$\subseteq$ | (Truco de Rabinowitsch) Sea $f \in I(V(I))$ y digamos que $I = (f_1, \cdots, f_m)$. Definimos el ideal $J := (f_1, \cdots, f_m, x_{n+1}f - 1) \subseteq k[x_1, \cdots, x_{n+1}]$. Supongamos que $(a_1, \cdots, a_n, a_{n+1}) \in V(J)$, entonces $(a_1, \cdots, a_n) \in V(I)$ se sigue que $f(a_1, \cdots, a_n) = 0$, esto resulta en una contradicción. Concluimos que $V(J) = \emptyset$.*

  Por el teorema anterior y como k es algebraicamente cerrado tenemos que $J = k[x_1, \cdots, x_{n+1}]$, entonces existen $\{g_i\}_{i=1}^{m+1} \subseteq k[x_1, \cdots, x_n]$ tales que

$$g_1 f_1 + \cdots + g_m f_m + g_{m+1}(x_{n+1}f - 1) = 1$$

tomando $x_{n+1} = 1/f$ *obtenemos*

$$g_1(x_1, \cdots, x_n, 1/f)f_1 + \cdots + g_m(x_1, \cdots, x_n, 1/f)f_m = 1$$

existe $n \in \mathbb{N}$ *tal que* $f^n \in I$.

Corolario 8.1. *Hay una correspondecia uno a uno entre puntos en* $\mathbb{A}_k^n$ *e ideales maximales.*

Corolario 8.2. *Las variedades afines en* $\mathbb{A}_k^n$ *estan en correspondecia uno a uno con los ideales primos.*

Corolario 8.3. *Las hipersuperficies irreducibles en* $\mathbb{A}_k^n$ *se corresponden uno a uno con polinomios irreducibles en* $k[x_1, \cdots, x_n]$.

Corolario 8.4. *Sea* $I \subseteq k[x_1, \cdots, x_n]$ *un ideal. Entonces* $V(I)$ *es un conjunto finito de puntos si y solo si como* k*-espacio vectorial* $k[x_1, \cdots, x_n]/I$ *tiene dimensión finita.*

Demostración.

- $\Leftarrow |$ *Sean* $p_1, \cdots, p_r \in V(I) \subseteq \mathbb{A}_k^n$. *Consideramos* $F_1, \cdots, F_r \in k[x_1, \cdots, x_n]$ *tales que* $F_i(p_j) = 0$ *para todo* $i \neq j$ *y* $F_i(p_i) = 1$. *Sea* $\overline{F_i}$ *la imagen de* F_i *en el cociente* $k[x_1, \cdots, x_n]/I = R$.

  Afirmamos que el conjunto $\{F_1, \cdots, F_r\}$ *es linealmente independiente en* R. *En efecto, si*

  $$\sum_{i=1}^{r} \lambda_i \overline{F_i} = 0 \quad \text{con} \quad \lambda_i \in k$$

  entonces $\sum \lambda_i \overline{F_i} \in I$, *evaluando en* p_i *vemos que* $\lambda_i = 0$ *para todo* i, *lo que prueba la afirmación. Así,* $r \leq dim_k R$.

- $\Rightarrow |$ *Digamos que* $V(I) = \{p_1, \cdots, p_r\}$ *y* $p_i = (a_{i1}, \cdots, a_{in})$. *Definimos*

  $$F_j := \prod_{i=1}^{r} (x_j - a_{ij})$$

  Luego $F_j \in I(V(I))$, *por Nullstellensatz, se tiene que* F_j^N *para algún* N, *así,* $\overline{F_j}^N = 0$ *en* R, *es decir,* $p(x_j) + x_j^{rN} = 0$, *con* $gr(p_j) < rN$ *entonces* $dim_k R < \infty$.

Ejemplos:

- Consideremos los polinomios $x - y, y - x^2 \in k[x, y]$, se sigue $V((x - y, y - x^2)) = \{(0, 0), (1, 1)\}$

  $$dim_k \left(k[x, y] \Big/ (x - y, y - x^2) \right) = dim_k \left(k[x] \Big/ (x - x^2) \right) = dim_k \left(k \oplus kx \right) = 2$$

- Notemos que $V(x - y - 1, x - y) = \emptyset$ y por otro lado

  $$k[x, y] \Big/ (x - y, x - y - 1) = k[x, y] \Big/ (1) = (0)$$

  así $dim_k R = 0$.

- Veamos que $V(y, x - y^3) = \{(0, 0)\}$, entonces

  $$dim_k \left(k[x, y] \Big/ (y, x^3 - y) \right) = dim_k \left(k[x] \Big/ (x^3) \right) = 3$$

- El conjunto $V(my - x, y - x^2)$ tiene dos puntos de intersección para todo $m \neq 0$,

  $$dim_k \left(k[x, y] \Big/ (my - x, y - x^2) \right) = dim_k \left(k[x] \Big/ (mx^2 - x) \right) = 2$$

  pero si $m = 0$, vemos que $dim_k R = 1$.

1.8. Modulos y Condiciones de Finitud

Sea R un anillo, se dice que M es un R-módulo, si M es un grupo conmutativo y si viene con producto escalar, es decir, una función de $R \times M$ a M, se denota por $a \cdot m$ que satisface lo siguiente

- $(a+b)m = am + bm$ para todo $a, b \in R$ y $m \in M$.
- $a(m+n) = am + an$ para todo $a \in R$ y $m, n \in M$.
- $(ab)m = a(bm)$ para todo $a, b \in R$ y $m \in M$.
- $1_R \cdot m = m$ para todo $m \in M$

Un subgrupo de N de un R-módulo M se dice un submodulo si N es un R-módulo con el mismo producto escalar. Dado $S \subseteq M$, definimos el generado de S por

$$\langle S \rangle := \left\{ \sum r_i s_i \ \mid \ r_i \in R, s_i \in S \right\}$$

de hecho corresponde al submódulo de M mas pequeño que contiene a S. Decimos que M es finitamente generado si existe $S \subseteq M$ tal que $\langle S \rangle = M$.

Sea $R \subseteq S$ anillos. Decimos que S es modulo finito sobre R, si es finitamente generado como R-módulo.

Sean $v_1, \cdots, v_n \in S$. Sea $\varphi : R[x_1, \cdots, x_n] \to S$ el morfismo de anillo que manda x_i a v_i. La imagen de φ se denota por $R[v_1, \cdots, v_n]$ y corresponde a un subanillo de S que contiene a R y $v_1, \cdots, v_n$, además, es el subanillo mas pequeño con esta propiedad. Decimos que S es un algebra finita sobre R si $S = R[v_1, \cdots, v_n]$ para algunos $v_1, \cdots, v_n \in S$.

Sean $K \subset L$ cuerpos. Sean $v_1, \cdots, v_n \in L$ y consideremos $K(v_1, \cdots, v_n)$ el cuerpo de fracciones de $K[v_1, \cdots, v_n]$. Al igual que antes, corresponde al menor subcuerpo de L que contiene a K y $v_1, \cdots, v_n$. El cuerpo L se dice una extensión finitamente generada de K si $L = K(v_1, \cdots, v_n)$ para algunos $v_1, \cdots, v_n \in L$.

1.9. Elementos Integrales

Definición 8.1. *Sean $R \subset S$ dominios enteros. Decimos que un elemento $v \in S$ es integral sobre R si*

$$v^n + r_{n-1}v^{n-1} + \cdots + r_1 v + r_0 = 0$$

para algunos $r_i \in R$ y $n \in \mathbb{N}$.

Proposición 8.1. *Sean $R \subset S$ dominios enteros, $v \in S$. Son equivalentes las siguientes afirmaciones*

a) v es integral sobre R.

b) $R[v]$ es un R-modulo finitamente generado.

c) Existe un subanillo $R' \subset S$ con $R[v] \subset R'$ y R' un R-modulo finitamente generado sobre R.

Demostración.

- *(a) $\Rightarrow$(b) | Existe un polinomio monico $f \in R[x]$ tal que $f(v) = 0$, luego el $R[v]$ se puede generar por finitos elementos.*
- *(b) $\Rightarrow$(c) | Basta tomar $R' = R[v]$.*
- *(c) $\Rightarrow$(a) | Existe R' tal que $R \subset R[v] \subset R' \subset S$. Con R, $R[v]$, R' finitamente generados como R-modulos. Sean $w_1, \cdots, w_n$ generadores de R'. Sabemos que*

$$v \cdot w_i = a_{i1}w_1 + \cdots + a_{in}w_n$$

luego tenemos el sistema

$$\begin{aligned}
&(a_{11} - v)w_1 + a_{12}w_2 + \cdots + a_{1n}w_n = 0 \\
&a_{21}w_1 + (a_{22} - v)w_2 + \cdots + a_{2n}w_n = 0 \\
&\vdots \\
&a_{n1}w_1 + a_{n2}w_2 + \cdots + (a_{nn} - v)w_n = 0
\end{aligned}$$

Como $R \subset S$ son dominios, podemos verlo dentro del cuerpo de fracciones, entonces tiene sentido calcular el determinante de la matriz asociada al sistema de ecuaciones. Por otro lado, $(w_1, \cdots, w_n)$ es una solución no trivial del sistema y por lo tanto el determinante de la matriz asociada es 0, lo que implica que v es integral sobre R.

Corolario 8.5. *Sean $R \subseteq S$ dominios. Entonces los elementos integrales sobre R forman un anillo.*

Demostración. *Sean $a, b \in S$ elementos integrales sobre R. Notemos que*

$$R \subseteq R[a+b] \subseteq R[a,b] \quad y \quad R \subseteq R[ab] \subseteq R[a,b]$$

Como a y b son elementos integrales sobre R, $R[a]$ y $R[b]$ son finitamente generados por $\{1, a, a^2, \cdots, a^{n-1}\}$ y $\{1, b, b^2, \cdots, b^{n-1}\}$. Es claro que $R[a,b]$ es generado por $\{a^i b^j : 0 \leq i \leq n-1, \ 0 \leq j \leq m-1\}$. Por la proposición se sigue que $a+b$ y ab son elementos integrales sobre R.

Definición 8.2. *Sean $R \subseteq S$ dominios. Decimos que S es integral sobre R si todo $s \in S$ es integral sobre R.*

Además, R es un dominio integralmente cerrado si ningún $z \in Frac(R) \setminus R$ es integral.

Ejemplos:

- Consideremos $\mathbb{Z} \subseteq \mathbb{Q}$, sea $p/q \in \mathbb{Q}$ con p y q coprimos. Si tenemos la expresión

$$\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_1\left(\frac{p}{q}\right) + a_0 = 0$$

  Por teorema de la raiz racional, q debe dividir a 1, luego $q = 1$ lo que implica que $p/q \in \mathbb{Z}$. Concluimos que Z es integralmente cerrado.

- Veamos el conjunto algebraico $V(y^2 - x^3) \subseteq \mathbb{A}_k^2$ con $k = \overline{k}$. Vemos el anillo

$$R = \frac{k[x,y]}{(y^2 - x^3)}$$

  que es un dominio, pues $(y^2 - x^3)$ es irreducible. Dentro de $R \subseteq Frac(R)$, vemos que se cumple la relación $y^2 = x^3$, que dentro del cuerpo de fracciones es equivalente a

$$\left(\frac{y}{x}\right)^2 - x = 0$$

  notemos que $\frac{y}{x} \notin R$ y que $x \in R$. Por lo tanto R no es integralmente cerrado.

- Sea $V(y - x^2) \subseteq \mathbb{A}_k^2$. Vemos el anillo

$$R = \frac{k[x,y]}{(y - x^2)}$$

  por demostrar, R es integralmente cerrado. Consideremos la función $\varphi : \mathbb{A}_k^1 \to \mathbb{A}_k^2$ dada por $\varphi(t) = (t, t^2)$. Notemos que $Im(\varphi) = V(y - x^2)$. La función φ induce el isomorfismo

$$\begin{aligned}
\frac{k[x,y]}{(y - x^2)} &\to k[t] \\
x &\to t \\
y^2 &\to t^2
\end{aligned}$$

  Como $k[t]$ es DFU, se sigue que R es integralmente cerrado.

Vamos a estudiar un caso particular del lema de Zariski. Sea k un cuerpo e $I \subseteq k[x]$ un ideal maximal, entonces $k[x]/I = L$ es un cuerpo. Tenemos dos casos, $I = (0)$ ó $I = (f(x))$. Si $I = (0)$ entonces $k[x]$ es cuerpo, esto es una contradicción. Por otro lado escribimos

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

pero en L se tiene que $f(x) = 0$, luego, L es generado como k módulo por $\{1, x, \cdots, x^{n-1}\}$.

Veamos cuando $k[x, y]/I = L$ donde k es un cuerpo e $I \subseteq k[x, y]$ es un ideal maximal. Si $x \in I$ o $y \in I$ podemos reducir al caso anterior. Entonces L es finitamente generado por potencias de x e y.

Pensaremos en $k(x)$ como los cocientes de polinomios en una variable modulo I, luego

$$k \subset k(x) \subset k(x)[y] = L$$

donde la igualdad $k(x)[y] = L$ se debe a que la inversa de un polinomio en $k(x)$ en realidad se escribe como combinación de potencias de x e y. Además, por el caso anterior, $k(x)[y]$ es finitamente generado como $k(x)$ módulo.

Tenemos dos casos:

- Caso 1: La extensión $k \subset k(x)$ es finita. Esto implica que la extensión $k \subseteq L$ es finita, basta tomar el producto de los generadores.
- Caso 2: Se tiene la siguiente igualdad

  $$k(x) = \left\{ \text{cocientes } \frac{p(x)}{q(x)} \right\}$$

  En L se debe cumplir la relación $y^m = a_{m-1}y^{m-1} + \cdots + a_1 y + a_0$ con $a_i \in k(x)$. Tomar $a \in k[x]$ tal que a^m limpie los denominadores, luego

  $$(ay)^m = b_{m-1}(ay)^{m-1} + \cdots + b_1(ay) + b_0$$

  con $b_i \in k[x]$. Se sigue que ay es integral sobre $k[x]$. Sea $z \in L$, luego para N suficientemente grande $a^N z$ es integral sobre $k[x]$, ya que

  $$\begin{aligned} a^N z &= a^N f(x, y) \\ &= a^N (c_0 + c_1 y + \cdots + c_M y^M) \\ &= c_0' + c_1'(ya) + \cdots + c_M'(ya)^M \end{aligned}$$

  donde $c_i' \in k[x]$. Como $k[x]$ es DFU, $a = p_1 \cdots p_s$ su factorización en irreducibles, sea p_{s+1} un irreductible distinto de p_i, tomando $z = \frac{1}{p_{s+1}}$ resulta que $a^N z$ es integral, lo cual es una contradicción.

Lema 8.1. *(Lema de Zariski) Sean $K \subseteq L$ y L es finitamente generado como K algebra, entonces L es finitamente generado como K modulo, es decir, como espacio vectorial.*

2. Variedades Afines

De ahora en adelante k será un cuerpo algebraicamente cerrado. A un conjunto algebraico afín irreducible lo llamamos variedad afín, o simplemente variedad.

2.1. Anillo de Coordenadas

Definición 8.3. *Sea $V \subseteq \mathbb{A}_k^n$ una variedad no vacía. Definimos*

$$\Gamma(V) := \frac{k[x_1, \cdots, x_n]}{I(V)}$$

y lo llamamos el ***anillo de coordenadas de*** *V y los elementos de $\Gamma(V)$ les decimos* ***funciones regulares****.*

Observación: El anillo de coordenadas de V es un dominio, ya que $\mathbb{I}(V)$ es un ideal primo de $k[x_1, \cdots, x_n]$. Por otro lado, dado $f, g \in k[x_1, \cdots, x_n]$ entonces f, g determinan la misma función si y solo si $f - g \equiv 0$ en V, es decir, $f - g \in \mathbb{I}(V)$. De este modo tenemos dos maneras de ver los elementos de $\Gamma(V)$; como una función de V, o como clase de equivalencia de polinomios.

2.2. Aplicaciones Polinomiales

Definición 8.4. *Sean $V \subseteq \mathbb{A}_k^n$ y $W \subseteq \mathbb{A}_k^m$ variedades. Una aplicación $\varphi : V \to W$ se dice* ***aplicación polinomial*** *si existen $f_i \in k[x_1, \cdots, x_n]$ tales que*

$$\varphi(a) = \varphi(a_1, \cdots, a_n) = (f_1(a), \cdots, f_m(a))$$

Proposición 8.2. *Sean $V \subseteq \mathbb{A}_k^n$ y $W \subseteq \mathbb{A}_k^m$ variedades. Entonces hay una correspondecia uno a uno entre las funciones polinomiales $\varphi : V \to W$ y los homomorfismos $\tilde{\varphi} : \Gamma(W) \to \Gamma(V)$.*

Demostración.

- *Dada $\varphi : V \to W$ una aplicación polinomial, sean $f_i \in k[x_1, \cdots, x_n]$ tales que $\varphi = (f_1, \cdots, f_m)$. Definimos $\tilde{\varphi} : \Gamma(W) \to \Gamma(V)$ dada por*

$$\tilde{\varphi}(f) := f \circ \varphi = f(f_1, \cdots, f_m)$$

  Veamos que esta bien definida, en efecto, sea $f \in \mathbb{I}(W)$, entonces $g \circ \varphi \equiv 0$ en V, luego $g \circ \varphi \in \mathbb{I}(V)$. Claramente $\tilde{\varphi}$ es homomorfismo.

- *Sea $\tilde{\varphi} : \Gamma(W) \to \Gamma(V)$ un homomorfismo. Sean $f_i \in k[x_1, \cdots, x_n]$ tales que $\tilde{\varphi}(y_i) = f_i$, definimos la aplicación polinomial $\varphi := (f_i, \cdots, f_m)$, por la discusión anterior φ esta bien definida y además la función inducida por φ es la misma que $\tilde{\varphi}$.*

Definición 8.5. *Una aplicación polinomial se dice* ***isomorfismo*** *si tiene inversa que también es una aplicación polinomial.*

Observación: Por la proposición anterior una aplicación polinomial es isomorfismo si y solo si el homomorfismo inducido es isomorfismo de anillos. Luego, dos variedades son isomorfas si y solo si sus anillos de coordenadas son isomorfos.

2.3. Cambio de Coordenadas

Definición 8.6. *Un* ***cambio de coordenadas afín*** *en $\mathbb{A}_k^n$ es una aplicación polinomial $\varphi = (f_1, \cdots, f_n) : \mathbb{A}_k^n \to \mathbb{A}_k^n$ tal que $gr(f_i) = 1$ y φ es biyectiva.*

2.4. Funciones Racionales y Anillos Locales

Definición 8.7. *Sea $V \subseteq \mathbb{A}_k^n$ una variedad no vacía. Definimos el* ***cuerpo de funciones racionales*** *en V como $k(V) := Frac(\Gamma(V))$. Un elemento en $k(V)$ se dice* ***función racional*** *en V.*

Notemos que $f \in k(V)$ no es necesariamente una función $f : V \to \mathbb{A}^1_k$. Consideremos $V = \mathbb{V}(xw - yz) \subseteq \mathbb{A}^4_k$ y $f = \frac{x}{y}$, luego, no es posible evaluar en los puntos de la forma $(a, 0, b, 0)$.

Definición 8.8. *Sea $V \subseteq \mathbb{A}^n_k$ una variedad no vacía. Sea f una función racional de V y $p \in V$, decimos que f esta definida en p si para algunos $a, b \in \Gamma(V)$ se tiene que $f = \frac{a}{b}$ y $b(p) \neq 0$.*

Observación: Si $\Gamma(V)$ es DFU entonces la expresión a/b es esencialmente única y por lo tanto f esta definida en p si y solo si $b(p) \neq 0$.

Definición 8.9. *Sea $V \subseteq \mathbb{A}^n_k$ una variedad no vacía. Sea $p \in V$, definimos*

$$\mathcal{O}_p(V) := \{f \in k(V) : f \text{ está definida en } p\}$$

*se dice que $\mathcal{O}_p(V)$ es el **anillo local** de V en p.*

Observación: Notemos que $\mathcal{O}_p(V)$ es un subanillo de $k(V)$ que contiene $\Gamma(V)$, en otras palabras $k \subseteq \Gamma(V) \subseteq \mathcal{O}_p(V) \subseteq k(V)$.
Este anillo tiene la propiedad de que tiene un único ideal maximal, a saber, $m_p(V) = \{f \in \mathcal{O}_p(V) : f(p) = 0\}$. Un anillo con esta propiedad se dice **anillo local**.

Definición 8.10. *El conjunto de puntos $p \in V$ donde una función racional f no está definida se llama el **conjunto de polos** de f.*

Proposición 8.3.

a) El conjunto de polos de una función racional es un subconjunto algebraico de V.

b) $\Gamma(V) = \bigcap_{p \in V} \mathcal{O}_p(V)$.

Demostración.

a) Sea $f \in k(V)$. Consideramos

$$J_f := \{G \in k[x_1, \cdots, x_n] : \overline{G} f \in \Gamma(V)\}$$

donde $\overline{G}$ es la clase de G en $\Gamma(V)$. Es claro que J_f es un ideal en $k[x_1, \cdots, x_n]$ que contiene a $I(V)$. Veamos que $V(J_f) = \{$polos de $f\}$.

Supongamos que $p \notin V(J_f)$, entonces existe $G \in J_f$ tal que $G(p) \neq 0$. Tenemos que $\overline{G} f = \overline{H} \in \Gamma(V)$, en $k(V)$ se tiene que $f = \frac{H}{G}$, entonces p no es polo de f.

Si p no es polo de f, entonces existen $G, H \in k[x_1, \cdots, x_n]$ tal que $f = \frac{H}{G}$ y $G(p) \neq 0$, además vemos que $\overline{G} f \in \Gamma(V)$, es decir, $p \notin V(J_f)$.

b) Una contención es clara, veamos la otra. Sea $f \in \bigcap_{p \in V} \mathcal{O}_p(V)$, entonces $V(J_f) = \emptyset$, por Nullstellensatz se sigue que $J_f = k[x_1, \cdots, x_n]$ y por ende $f = 1 \cdot f \in \Gamma(V)$.

Proposición 8.4. *$\mathcal{O}_p(V)$ es un dominio local Noetheriano.*

Demostración. *Sea $I \subseteq \mathcal{O}_p(V)$ un ideal, consideremos $I' = I \cap \Gamma(V)$. Como $\Gamma(V)$ es Noetheriano, existen $f_i \in \Gamma(V)$ tales que $I' = \langle f_1, \cdots, f_m \rangle$. Luego si $f = \frac{a}{b}$ entonces $bf = a \in I'$. Se sigue que*

$$bf = \sum a_i f_i \Rightarrow f = \sum \frac{a_i}{b} f_i$$

2.5. Anillos de Evaluación Discreta

Proposición 8.5. *Sea R un dominio que no es cuerpo. Luego, R es Noetheriano, local y su ideal maximal es principal si y solo si existe $t \in R$ irreducible tal que para todo $z \in R \setminus \{0\}$ y $z = ut^n$ para algún u unidad y $n \in \mathbb{N}_0$.*

Definición 8.11. *Sea R como antes, decimos que R es un **anillo de evaluación discreta** y lo abreviamos DVR, el elemento t se llama **parametro uniformizante**.*

Ejemplos:

- Consideremos $p \in \mathbb{A}^1_k = V$, sea $m_p(V)$ el unico ideal maximal de $\mathcal{O}_p(V)$, luego $(t) = m_p(V)$.
- Un no ejemplo. Si tomamos $p = (0,0) \in \mathbb{A}^2_k = V$ entonces $(x,y) \subseteq \mathcal{O}_p(V)$ no es principal, $\mathcal{O}_p(V)$ no es un DVR.

Definición 8.12. *Sea R un DVR, consideremos $k = Frac(R)$, entonces para todo $z \in k$ existe $n \in \mathbb{Z}$ y $u \in R$ unidad tales que $z = ut^n$, luego*

*a) n es el **orden** de z y se escribe $ord(z)$. Decimos que $ord(o) = \infty$.*

*b) Si $n < 0$, entonces z es un **polo**.*

*c) Si $n > 0$, decimos que z es un **cero**.*

*d) Si $n = 0$, z se dice **unidad**.*

2.6. Formas

Definición 8.13. *Una **forma** es un polinomio homogeneo en $R[x_1, \cdots, x_n]$, con R dominio. Recordando el capitulo 1, sección 1, $f \in R[x_1, \cdots, x_n]$ es homogeneo si $f(\lambda \overrightarrow{x}) = \lambda^n f(\overrightarrow{x})$ con $n = gr(f)$.*

Ejemplo: Sea $f = x_1^2 + x_2^2 + x_3x_4$ es una forma.

Definición 8.14. *Sea R un dominio,*

a) Sea $f \in R[x_1, \cdots, x_n]$, escribimos $f = \sum f_0 + f_1 + \cdots + f_d$ donde f_i es un polinomio homogeneo de grado i, definimos $f^* \in R[x_1, \cdots, x_{n+1}]$ como

$$f^* := x_{n+1}^d f_0 + x_{n+1}^{d-1} f_1 + \cdots + f_d = x_{n+1}^d f\left(\frac{x_1}{x_{n+1}}, \cdots, \frac{x_n}{x_{n+1}}\right)$$

*este proceso se llama **homogenización**.*

*b) Sea $F \in R[x_1, \cdots, x_{n+1}]$ una forma, definimos $F_* \in R[x_1, \cdots, x_n]$ como $F_* := F(x_1, \cdots, x_n, 1)$. Decimos que **deshomogenizamos** el polinomio.*

Proposición 8.6. *Se cumple lo siguiente*

a) $(FG)_* = F_*G_*$ y $(fg)^* = f^*g^*$.

b) Si $F \neq 0$ y r es la mayor potencia de x_{n+1} que divide F entonces $x_{n+1}^r (F_*)^* = F$. Además, $(f^*)_*$.

c) Se tiene que $(F+G)_* = F_* + G_*$. Por otro lado, sea $r = gr(g)$, $s = gr(f)$ y $t = r + s - gr(f+g)^*$ entonces $x_{n+1}^t (f+g)^* = x_{n+1}^r f^* + x_{n+1}^s g^*$.

2.7. Producto Directo de Anillos

Definición 8.15. *Sean $R_1, \cdots, R_n$ anillos, definimos $R := \prod R_i$ junto con las operaciones*

$$\begin{aligned}(a_1, \cdots, a_n) + (b_2, \cdots, b_n) &:= (a_1 + b_1, \cdots, a_n + b_n)\\ (a_1, \cdots, a_n) \cdot (b_2, \cdots, b_n) &:= (a_1 \cdot b_1, \cdots, a_n \cdot b_n)\end{aligned}$$

*y $\pi_i : R \to R_i$ son las proyecciones a cada coordenada. Decimos que R es un **anillo producto**.*

Observación: Es directo que R con las operaciones definidas es un anillo, donde $(0, \cdots, 0)$ y $(1, \cdots, 1)$ son los neutros de $+$ y $\cdot$ respectivamente.

Proposición 8.7. ***(Propiedad Universal)*** *Para todo anillo S y todo morfismo $\phi_i : S \to R_i$, existe un unico morfismo $\varphi : S \to R$ tal que*

$$\begin{tikzcd} S \arrow[r, "\varphi"] \arrow[d, "\phi_i"'] & R \arrow[dl, "\pi_i"] \\ R_i & \end{tikzcd}$$

2.8. Operando con Ideales

Definición 8.16. *Sean $I, J \subseteq R$ ideales de un anillo R. Definimos el* ***producto de ideales*** *como*

$$IJ := \langle ab : a \in I, b \in J \rangle$$

Observación: Si $I = \langle a_1, \cdots, a_n \rangle$ entonces

$$I^n = \left\langle a_1^{i_1} \cdots a_k^{i_k} : k \leq r, \sum_{j=1}^{k} i_j = n \right\rangle$$

Definición 8.17. *Sean $I, J \subseteq R$ ideales, definimos la* ***suma de ideales*** *como $I + J := \{a + b : a \in I, b \in J\}$. Decimos I, J son* ***comaximales*** *si $I + J = R$.*

Proposición 8.8. *Sean $I, J \subseteq R$ ideales, tenemos que*

a) $IJ \subseteq I \cap J$.

b) Si I, J son comaximales entonces $IJ = I \cap J$.

2.9. Ideales de un Número Finito de Puntos

Proposición 8.9. *Sea $I \subseteq k[x_1, \cdots, x_n]$ un ideal con $k = \overline{k}$. Supongamos que $|V(I)| < \infty$, digamos que $V(I) = \{p_1, \cdots, p_m\}$, entonces existe un isomorfismo natural*

$$\varphi : \frac{k[x_1, \cdots, x_n]}{I} \to \frac{\mathcal{O}_{p_1}(\mathbb{A}_k^n)}{I\mathcal{O}_{p_1}(\mathbb{A}_k^n)} \times \cdots \times \frac{\mathcal{O}_{p_m}(\mathbb{A}_k^n)}{I\mathcal{O}_{p_m}(\mathbb{A}_k^n)}$$

donde $I\mathcal{O}_{p_i}(\mathbb{A}_k^n)$ es el ideal generado por I con elementos de $\mathcal{O}_{p_i}(\mathbb{A}_k^n)$.

Demostración. *Diremos que $\mathcal{O}_i := \mathcal{O}_{p_i}(\mathbb{A}_k^n)$, $R = k[x_1, \cdots, x_n]/I$ y que $R_i := \mathcal{O}_i/I\mathcal{O}_i$. Sea I_i el ideal maximal de p_i, luego $(x_1 - p_{i1}, \cdots, x_n - p_{in}) = I_i \supset I$. Definimos $\varphi_i : R \to R_i$ donde $\varphi(f) = \varphi_i([F]_I) := [F]_{I\mathcal{O}_i}$.*

Por la propiedad universal, existe un unico morfismo $\varphi : R \to R_1 \times \cdots \times R_m$, que esta dada por $\varphi(F) = (\varphi_1(F), \cdots, \varphi_m(F))$. Afirmamos que φ es biyección. Por Nullstellensatz se sigue que

$$\sqrt{I} = \mathbb{I}(\{p_1, \cdots, p_m\}) = \bigcap_{i=i}^{m} I_i$$

entonces $\left(\bigcap_{i=i}^m I_i\right)^d \subseteq I$ para algún $d \in \mathbb{N}$. Por otro lado $\left(\bigcap_{i=i}^m I_i\right)^d = (I_1 \cdots I_m)^d = \bigcap_{i=1}^m I_i^d$, se sigue que $\bigcap_{i=i}^m I_i^d \subseteq I$.

Sean $F_i \in k[x_1, \cdots, x_n]$ tales que $F_i(p_j) = 0$ para $i \neq j$ y $F_i(p_i) = 1$, definimos $E_i = 1 - (1 - F_i^d)^d$ para $i = 1, \cdots, m$. Notemos que $E_i = F_i^d D_i$ para algún D_i, entonces $E_i \in I_j^d$ para $i \neq j$, lo que implica

- *Dado j fijo se tiene que $1 - \sum_i E_i = (1 - E_j) - \sum_{i \neq j} E_i \in I_j^d$, lo que implica que $1 - \sum_i E_i \in \bigcap_{j=1}^m I_j^d$.*
- *Para i fijo vemos que $E_i - E_i^2 = E_i(1 - F_i^d)^d \in \bigcap_{i=1}^m I_i^d$.*

Definimos $e_i := [E_i]_I \in R$, por lo anterior, cumplen que $e_i^2 = e_i$, $e_i e_j = 0$ y $\sum_i e_i = 1$.

Lema: *Si $G \in k[x_1, \cdots, x_n]$ con $G(p_i) \neq 0$ entonces existe $t \in R$ tal que $tg = e_i$ donde $g = [G]_I \in R$. En efecto, supongamos que $G(p_i) = 1$ y sea $H = 1 - G$, luego*

$$(1 - H)(E_i + HE_i + \cdots + H^{d-1}E_i) = E_i - H^d E_i$$

por ende

$$g(e_i + he_i + \cdots + h^{d-1}e_i) = e_i$$

Veamos que φ es biyección. Sea $f \in R$ tal que $\varphi(f) = 0$, luego $[F]_{I\mathcal{O}_i} = 0$, lo que implica que $F \in I\mathcal{O}_i$, entonces existe $G \in k[x_1, \cdots, x_n]$ tal que $G_i(p_i) \neq 0$ y $FG \in I$, por el lema se sigue que existe $t_i \in R$ tal que $t_i g_i = e_i$, *entonces*

$$f = \sum_i e_i f = \sum_i t_i g_i f = 0$$

por lo tanto φ *es inyectiva. Como* $E_i(p_i) = 1$ *vemos que* $\varphi(e_i)$ *es una unidad en* R_i*, como* $e_i e_j = 0$ *para* $i \neq j$ *se tiene que* $\varphi_i(e_j) = 0$ *para* $i \neq j$*. Por ende,* $\varphi_i(e_i) = \varphi_i(\sum e_j) = 1$*. Sea*

$$z = \left(\frac{h_1}{g_1}, \cdots, \frac{h_m}{g_m}\right) \in R_1 \times \cdots \times R_m$$

por el lema, existe t_i *tal que* $t_i g_i = e_i$*, tenemos que*

$$\varphi_i(g_i)\frac{h_i}{g_i} = [G_i]_i \cdot \left[\frac{H_i}{G_i}\right]_i = [H_i]_i = \varphi_i(h_i)$$

lo que implica que $\varphi_i(t_i h_i) = h_i/g_i$*. De este modo*

$$\varphi_i\left(\sum t_j h_j e_j\right) = \varphi_i(t_i h_i) = \frac{h_i}{g_i}$$

concluimos que $\varphi(\sum t_j h_j e_j) = z$ *y por lo tanto* φ *es sobreyectiva.*

Corolario 8.6.

$$dim_k\left(\frac{k[x_1, \cdots, x_n]}{I}\right) = \sum_{i=1}^{m} dim_k\left(\frac{\mathcal{O}_i}{I\mathcal{O}_i}\right)$$

2.10. Modulos Cociente y Secuencias Exactas

Sea R un anillo, sean M y V R-modulos un morfismo de grupos $\varphi : M \to V$ se dice **morfismo de R-modulos** si $\varphi(am) = a\varphi(m)$ para todo $a \in R$ y $m \in M$. Decimos que es isomorfismo cuando es biyectivo.

Sea N un submodulo de un R-modulo M, en el grupo cociente M/N consideramos la operación $a\overline{m} = \overline{am}$, lo que da estructura de R-modulo y lo llamamos el **modulo cociente** de M por N.

Definición 8.18. *Sean* $\psi : M' \to M$ *y* $\varphi : M \to M''$ *morfismos de R-modulos. Decimos que la secuencia*

$$M' \xrightarrow{\psi} M \xrightarrow{\varphi} M''$$

es ***exacta*** *si* $Im(\psi) = ker(\varphi)$*.*

Proposición 8.10.

a) Sea

$$0 \longrightarrow V' \xrightarrow{\psi} V \xrightarrow{\varphi} V'' \longrightarrow 0$$

una secuencia exacta de espacios vectoriales sobre un cuerpo k de dimensión finita, entonces $dimV' + dimV'' = dimV$*.*

b) Sea

$$0 \longrightarrow V_1 \xrightarrow{\varphi_1} V_2 \xrightarrow{\varphi_2} V_3 \xrightarrow{\varphi_3} V_4 \longrightarrow 0$$

una secuencia exacta de espacios vectoriales sobre un cuerpo k de dimensión finita, entonces $dimV_4 = dimV_3 - dimV_2 + dimV_1$

2.11. Modulos Libres

Definición 8.19. *Sea R un anillo y X un conjunto. Consideramos*

$$M_X := \left\{\varphi : X \to R : \left|\varphi^{-1}(R \setminus \{0\})\right| < \infty\right\}$$

Lo dotamos de estructura de R-modulo como sigue: $(\varphi+\psi)(x) := \varphi(x)+\psi(x)$ *y* $(a\varphi)(x) := a\varphi(x)$*, donde* $\varphi, \psi \in M_X$ *y* $a \in R$*. El modulo* M_X *se dice* ***R-modulo libre*** *sobre el conjunto X.*

Observación: Si definimos $\varphi_x \in M_X$ como $\varphi_x(y) := \mathbb{1}_x(y)$, entonces todo $\varphi \in M_X$ tiene expresión unica $\varphi = \sum a_x \varphi_x$ donde $a_x = \varphi(x)$. Usualmente escribimos x en lugar de φ_x.

Proposición 8.11. *(**Propiedad Universal**) Sea $\alpha : X \to M$ una función del conjunto X a un R-modulo M, entonces α se extiende de manera unica a un morfismo de M_X a M.*

Definición 8.20. *Un R-modulo M se dice **libre** con base $m_1, \cdots, m_n \in M$, si el conjunto $X := \{m_1, \cdots, m_n\}$ y el morfismo natural de M_X a M es isomorfismo.*

3. Propiedades Locales de Curvas Planas

3.1. Puntos Multiples y Rectas Tangentes

Definición 8.21. *Sea $V = \mathbb{V}(F) \subseteq \mathbb{A}_k^2$ con F no constante y no necesariamente irreducible. Decimos que V es una **curva plana**. El **grado** de una curva es el grado de F.*

Observación: Si $F = F_1^{\alpha_1} \cdots F_r^{\alpha_r}$ con F_i irreducible entonces $V = \mathbb{V}(F_1) \cup \cdots \cup \mathbb{V}(F_r)$ es su descomposición en irreducibles. Si $\alpha_i = 1$ decimos que la componente $\mathbb{V}(F_i)$ es **simple**.

Definición 8.22. *Sea $V \subseteq \mathbb{A}_k^2$ una curva plana. Dado $p \in V = \mathbb{V}(F)$ decimos que es **no singular** si $F_x(p) \neq 0$ o $F_y(p) \neq 0$. En este caso la recta*

$$F_x(p)(x-a) + F_y(p)(y-b) = 0 \quad \text{con } p = (a,b)$$

*es la **recta tangente** en p. De lo contrario, decimos que p es **singular**.*

Definición 8.23. *Una curva plana $V \subseteq \mathbb{A}_k^2$ se dice **no singular** si todo punto es no singular.*

Ejemplo: Sea $F = y^2 - x^2 - x^3$, luego $F_x = -2x - 3x^2$ y $F_y = 2y$. Buscamos los puntos singulares, debemos resolver el sistema

$$\begin{aligned} y^2 - x^2 - x^3 &= 0 \\ -2x - 3x^2 &= 0 \\ 2y &= 0 \end{aligned}$$

Si $char(k) \neq 2, 3$, entonces $x, y = 0$. Por otro lado, si $char(k) = 2$ entonces $x = 0$ por la segunda ecuación y así, por la primera ecuación, $y = 0$. Para $char(k) = 3$ el resultado es directo. El unico punto singular es $(0,0)$.

Observación: Sea $p \in k[x,y]$ homogeneo de grado d y $k = \overline{k}$, entonces

$$p = \prod_i (x - \lambda_i y)^{\alpha_i}$$

Definición 8.24. *Sea $V \subseteq \mathbb{A}_k^2$ una curva plana. Sea $p = (0,0)$, escribimos $F = F_m + F_{m+1} + \cdots + F_n$ con $m \leq n$. La **multiplicidad** de $V = \mathbb{V}(F)$ en p es $m_p(F) := m$.*

Observación: Veamos que $p = (0,0)$ es no singular si y solo si $m_p(F) = 1$. Si $m_p(F) = 2$ decimos que p es punto doble, si $m_p(F) = 3$ es punto triple y asi.

Definición 8.25. *Sea $V \subseteq \mathbb{A}_k^2$ una curva plana. Sea $p = (0,0)$, escribimos $F = F_m + F_{m+1} + \cdots + F_n$ con $m \leq n$. Entonces*

$$F_m = \prod_i L_i^{\alpha_i}$$

*con L_i lineal y se llama **recta tangente** de V en p y α_i se dice **multiplicidad de la tangente**. Si $\alpha_i = 1$ para todo i, decimos que p es **punto multiple ordinario**.*

Definición 8.26. *Sea $V \subseteq \mathbb{A}_k^2$ una curva plana. Definimos la multiplicidad de $p = (a,b)$ en V como*

$$m_p(F) := m_{(0,0)}\left(F^T\right) \quad \text{con } F^T = F(x+a, y+b)$$

3.2. Multiplicidades y Anillos Locales

Teorema 9. *Sea V una curva plana irreducible. Entonces p un punto no singular de $V = \mathbb{V}(F)$ si y solo si $\mathcal{O}_p(V)$ es un anillo de evaluación discreta.*

En tal caso, si $L = ax + by + c$ es una recta no tangente en p, entonces su imagen en $\mathcal{O}_p(V)$ es un parametro uniformizante.

Demostración. *Supongamos que p es un punto no singular de V y L una recta que pasa por p que no es tangente a F en p. Podemos suponer que $p = (0,0)$ y que y es la recta tangente y $L = X$. Basta mostrar que x genera $m_p(V)$.*

Notemos que $m_p(V) = (x,y)$ en $\mathcal{O}_p(V)$. Escribimos $F = Y + P(x,y)$ donde $P(x,y)$ son términos de grado mayor. Luego, reescribimos $F = YG - X^2H$, donde $G = 1 + P_1(x,y)$ con $P_1(x,y)$ términos de grado mayor y $H \in k[x]$.

Entonces $yg = x^2h \in \Gamma(V)$, lo que implica que $y = x^2hg^{-1} \in (x)$, ya que $g(p) \neq 0$. Por lo tanto, $m_p(V) = (x,y) = (x)$.

La otra dirección se sigue del siguiente teorema.

La demostración del siguiente teorema se encuentra en algebraic curves de fulton.

Teorema 10. *Sea p un punto de una curva irreducible $V = \mathbb{V}(F)$. Entonces para n suficientemente grande, se tiene que*

$$m_p(F) = dim_k\left(\frac{m_p(V)^n}{m_p(V)^{n+1}}\right)$$

En particular, la multiplicidad de F en p depende solo del anillo local $\mathcal{O}_p(V)$.

Observación: Notemos que si $\mathcal{O}_p(V)$ es un DVR, entonces, $m_p(F) = 1$ lo que implica que p es no singular.

Ejemplo: Sea $(x,y) \subseteq k[x,y]$, luego

$$dim_k\left(\frac{(x,y)}{(x,y)^2}\right) = 2$$

3.3. Número de Intersecciones

Sean $V = \mathbb{V}(F), W = \mathbb{V}(G)$ curvas planas y sea $p \in \mathbb{A}^2_k$. El objetivo de esta sección es definir el número de Intersecciones de dos curvas V y W, que será denotado por $I(p, F \cap G)$. Comenzaremos listando 7 propiedades que nos gustaría que tuviese el número de intersección

(1) $I(p, F \cap G)$ es un entero no negativo para todo $F, G \in k[x,y]$ y $p \in \mathbb{A}^2$ si F, G no tienen factores en común que pasen por p, de lo contrario decimos que $I(p, F \cap G) = \infty$.

(2) $I(p, F \cap G) = 0$ si y solo si $p \notin F \cap G$. Además, $I(p, F \cap G)$ solo depende de las componentes de F, G que pasan por p.

(3) Si T es un cambio afín de coordenadas en $\mathbb{A}^2$ y $T(q) = p$ entonces $I(p, F \cap G) = I(q, F^T \cap G^T)$.

(4) $I(p, F \cap G) = I(p, G \cap F)$.

(5) $I(p, F \cap G) \geq m_p(F)m_p(G)$, con igualdad si y solo si F y G no tienen rectas tangentes en común en p.

(6) Si $F = \prod F_i^{r_i}$ y $G = \prod G_j^{s_j}$, entonces

$$I(p, F \cap G) = \sum_{i,j} r_i s_j I(p, F_i \cap G_j)$$

(7) $I(p, F \cap G) = I(p, F \cap (G + AF))$ para todo $A \in k[x,y]$.

El siguiente teorema asegura la existencia y unicidad del número de intersección, la demostración se encuentra en algebraic curves de Fulton.

Teorema 11. *Existe un único número de intersección $I(p, F \cap G)$ definido para todas las curvas planas y todos los puntos en $\mathbb{A}^2$, que satisface las siete propiedades. Además, esta dado por la fórmula*

$$I(p, F \cap G) = dim_k\left(\frac{\mathcal{O}_p(\mathbb{A}^2)}{(F,G)}\right)$$

Ejemplo: Calcular el $I(p, F \cap G)$ donde $F = (x^2+y^2)^2 + 3x^2y - y^3$ y $G = (x^2+y^2)^3 - 4x^2y^2$ y $p = (0,0)$. Reemplacemos G por $G - (x^2+y^2)F = y((x^2+y^2)(y^2-3x^2) - 4x^2y) = yE$, luego

$$I(p, F \cap G) = I(p, F \cap (G - (x^2+y^2)E)) = I(p, F \cap y) + I(p, F \cap E)$$

por la propiedad (7) y (6) respectivamente. Como $F = x^4 + yA$, entonces por la propiedad $(5),(7)$ y (6) se sigue que $I(p, F \cap y) = I(p, x^4 \cap y) = 4$.

Reemplazamos E por $E + 3F = y(5x^2 - 3y^2 + 4y^3 + 4x^2y) = yH$, así

$$I(p, F \cap E) = I(p, F \cap y) + I(p, F \cap H) = 4 + 6 = 10$$

por la propiedad $(7),(6)$ y (5). Por lo tanto $I(p, F \cap G) = 14$.

4. Variedades Proyectivas

4.1. Espacio Proyectivo

Definición 11.1. *Sea k un cuerpo tal que $k = \overline{k}$. Definimos el* ***n-espacio proyectivo*** *sobre k, denotado por $\mathbb{P}_k^n$, como*

$$\mathbb{P}_k^n := \frac{\mathbb{A}_k^{n+1} \setminus \{(0, \cdots, 0)\}}{\sim}$$

donde $x \sim y$ si y solo si existe $\lambda \in k \setminus \{0\}$ tal que $x = \lambda y$. Un elemento $p \in \mathbb{P}_k^n$ se dice ***punto*** *y un representante de la clase se llama* ***coordenada homogénea*** *para p.*

Observación: Un elemento en $\mathbb{P}_k^n$ típicamente se escribe por algún representante de la clase, y este se escribe del modo que sigue $[x_1, \cdots, x_{n+1}]$. Consideremos el conjunto

$$U_i := \{[x_1, \cdots, x_{n+1}] \in \mathbb{P}_k^n : x_i \neq 0\}$$

de este modo cada $p \in U_i$ se puede escribir de manera única como $[x_1, \cdots, x_{i-1}, 1, x_{i+1}, \cdots, x_{n+1}]$. Notemos que $\mathbb{P}_k^n = \bigcup_{i=1}^{n+1} U_i$, donde U_i puede ser vista como una copia $\mathbb{A}_k^n$. Por conveniencia nos enfocaremos en U_{n+1}.

Definición 11.2. *Sea*

$$H_\infty := \mathbb{P}_k^n \setminus U_{n+1} = \{[x_1, \cdots, x_{n+1}] \in \mathbb{P}_k^n : x_{n+1} = 0\}$$

Decimos que H_∞ es el ***hiperplano en el infinito****.*

Observación: Notemos que existe una correspondecia entre $[x_1, \cdots, x_n, 0]$ y $[x_1, \cdots, x_n]$, por lo que H_∞ puede se identificado con $\mathbb{P}_k^{n-1}$, de este modo $\mathbb{P}_k^n = U_{n+1} \cup H_\infty$ es la unión de un n-espacio afín y un conjunto que da todas las direcciones del n-espacio afín.

4.2. Conjuntos Algebraicos Proyectivos

Definición 11.3. *Un punto $p \in \mathbb{P}_k^n$ se dice* ***cero*** *de un polinomio $F \in k[x_1, \cdots, x_{n+1}]$ si $F(x_1, \cdots, x_{n+1}) = 0$ para toda coordenada homogénea $(x_1, \cdots, x_{n+1})$ de p, si es el caso, escribimos $F(p) = 0$.*

Definición 11.4. *Sea $S \subseteq k[x_1, \cdots, x_{n+1}]$, definimos*

$$\mathbb{V}(S) := \{p \in \mathbb{P}_k^n : p \text{ es cero para todo } F \in S\}$$

Observación: Al igual que en el caso de espacio afín, si I es el ideal generado por S entonces $\mathbb{V}(I) = \mathbb{V}(S)$.

Definición 11.5. *Decimos que $V = \mathbb{V}(I)$ es un* ***conjunto algebraico proyectivo*** *o conjunto algebraico en $\mathbb{P}_k^n$ si $\mathbb{V}(I) = \mathbb{V}(\{F_j^{(i)}\})$ donde $\{F_j^{(i)}\}$ es un conjunto finito de formas.*

Definición 11.6. *Dado $X \subseteq \mathbb{P}_k^n$, definimos*

$$\mathbb{I}(X) := \{F \in k[x_1, \cdots, x_{n+1}] : F(p) = 0 \text{ para todo } p \in X\}$$

el ideal $\mathbb{I}(X)$ se dice ideal de X.

Definición 11.7. *Un ideal $I \subseteq k[x_1, \cdots, x_{n+1}]$ se dice* ***homogeneo*** *si para todo $F = \sum_i F_i \in I$, con F_i una forma de grado i, entonces $F_i \in I$.*

Observación: Para todo conjunto $X \subseteq \mathbb{P}_k^n$ se tiene que $\mathbb{I}(X)$ es un ideal homogeneo.

Proposición 11.1. *Un ideal $I \subseteq k[x_1, \cdots, x_{n1}]$ es homogeneo si y solo si es generado por un número finito de formas.*

> **Demostración.** *Supongamos que I es homogeneo, luego $I = \left\langle F^{(1)}, \cdots, F^{(r)} \right\rangle$, entonces I es generado por $F_j^{(i)}$ donde $F^{(i)} = \sum_j F_j^{(i)}$.*
>
> *Sea $S = \{F^\alpha\}$ un conjunto de formas que generan I, con $gr(F^\alpha)d_\alpha$. Sea $F = F_m + \cdots + F_r \in I$ y $gr(F_i) = i$.*

Luego

$$F = \sum A^\alpha F^\alpha$$

notamos que $F_m = \sum A^\alpha_{m-d_\alpha} F^\alpha$, *entonces* $F_m \in I$ *lo que implica que* $F_i \in I$ *para* $m \leq i \leq r$.

Definición 11.8. *Un conjunto algebraico* $V \subseteq \mathbb{P}^n_k$ *es* ***reducible*** *si existen* $V_1, V_2 \subseteq \mathbb{P}^n_k$ *conjuntos algebraicos no triviales tales que* $V_i \neq V$ *y* $V = V_1 \cup V_2$. *En caso contrario, decimos que* V *es* ***irreducible***.

Observación: Al igual que en el caso afín, se tiene el resultado V es irreducible si y solo si $\mathbb{I}(V)$ es primo. Generalmente, se dice que un conjunto algebraico $V \subseteq \mathbb{P}^n_k$ irreducible es una **variedad proyectiva**.

Todo conjunto algebraico puede ser escrito de manera unica como unión de variedades proyectivas, su **componentes irreducibles**.

Definición 11.9. *Sea* $V \subseteq \mathbb{P}^n_k$ *un conjunto algebraico, definimos*

$$C(V) := \{(x_1, \cdots, x_{n+1}) \in \mathbb{A}^{n+1} : [x_1, \cdots, x_{n+1}] \in V \text{ o } (x_1, \cdots, x_{n+1}) = 0\}$$

el ***cono*** *sobre* V.

Para evitar confusiones, denotaremos por V_p, I_p a las operaciones proyectivas y por V_a, I_a a las afines.

Teorema 12. *(Nullstellensatz Proyectivo) Sea* $I \subseteq k[x_1, \cdots, x_{n+1}]$ *un ideal homogeneo, entonces*

a) $V_p(I) = \emptyset$ *si y solo si existe un entero* N *tal que* I *contiene todas las formas de grado mayor o igual que* N.

b) Si $V_p(I) \neq \emptyset$ *entonces* $I_p(V_p(I)) = Rad(I)$.

Observación:(Falta entender bien lo que dice)

Definición 12.1. *Sea* $V \subseteq \mathbb{P}^n_k$ *una variedad proyectiva no vacía, entonces* $\mathbb{I}(V)$ *es primo, luego el anillo*

$$\Gamma_h(V) = \frac{k[x_1, \cdots, x_{n+1}]}{\mathbb{I}(V)}$$

es un dominio, llamado ***anillo de coordenadas homogeneo*** *de* V. *Un elemento* $f \in \Gamma_h(V)$ *se dice* ***forma*** *de grado* d, *si existe una forma* $F \in k[x_1, \cdots, x_{n+1}]$ *de grado* d *tal que* $[F] = f$.

Proposición 12.1. *Todo elemento* $f \in \Gamma_h(V)$ *puede ser escrito de manera unica como* $f = f_0 + \cdots + F_m$, *con* f_i *una forma de grado* i.

Demostración. *Sea* $F \in k[x_1, \cdots, x_{n+1}]$ *tal que* $[F] = f$, *escribimos* $F = \sum F_i$ *entonces* $f = \sum f_i$, *donde* f_i *es una forma de grado* i. *Supongamos que* $f = \sum g_i$ *donde* $g_i = [G_i]$ *con* G_i *una forma de grado* i. *Luego*

$$F - \sum G_i = \sum (F_i - G_i) \in I$$

como $\mathbb{I}(V)$ *es homogeneo, se sigue que* $F_i - G_i \in I$ *lo que implica que* $f_i = g_i$.

Definición 12.2. *Sea* $k_h(V)$ *el cuerpo de fracciones de* $\Gamma_h(V)$ *y se le llama* ***cuerpo de funciones homogeneas*** *de* V.

Observación: Notar que, a diferencia del caso afín, ningún elemento en $\Gamma_h(V)$, a excepción de las constantes, determina una función. Sin embargo, si f, g son formas en $\Gamma_h(V)$ del mismo grado, entonces f/g definen una función, al menos donde g no es cero.

Definición 12.3. *El* ***cuerpo de funciones*** *de* V, *denotado por* $k(V)$, *se define como*

$$k(V) := \left\{ \frac{f}{g} : f, g \in \Gamma_h(V) \text{ son formas del mismo grado} \right\}$$

los elementos en $k(V)$ *se dicen* ***funciones racionales*** *en* V.

Observación: Notar que $k(V)$ es un subcuerpo de $k_h(V)$, se tiene la cadena $k \subset k(V) \subset k_h(V)$.

Definición 12.4. *Sea $V \subseteq \mathbb{P}^n_k$ una variedad proyectiva no vacía. Sea $p \in V$, decimos que $z \in k(V)$* ***esta definida*** *en p si existen formas $f, g \in \Gamma_h(V)$ del mismo grado tales que $z = f/g$ y $g(p) \neq 0$.*

Definición 12.5. *Se define*

$$\mathcal{O}_p(V) := \{z \in k(V) : z \text{ esta definida en } p\}$$

se dice el ***anillo local*** *de V en p.*

Observación: Veamos que $\mathcal{O}_p(V)$ es un subanillo de $k(V)$, es un anillo local con ideal maximal

$$m_p(V) = \{z \in \mathcal{O}_p(V) : z(p) = 0\}$$

4.3. Variedades Proyetivas y Afines

Definición 12.6. *Sea $V \subseteq \mathbb{A}^n_k$ un conjunto algebraico e $I = \mathbb{I}(V) \subseteq k[x_0, \cdots, x_{n-1}]$ definimos la* ***homogenización de*** *I como*

$$I^* := \{F^* : F \in I\} \subseteq k[x_0, \cdots, x_n]$$

Además, definimos la ***clausura proyectiva de*** *V como $V^* := \mathbb{V}(I^*) \subseteq \mathbb{P}^n_k$.*

Observación: El ideal I^* es homogeneo.

Definición 12.7. *Dado $V \subseteq \mathbb{P}^n_k$ un conjunto algebraico proyectivo e $I = \mathbb{I}(V) \subseteq k[x_0, \cdots, x_n]$, definimos la* ***deshomogenización de*** *I como*

$$I_* := \{F_* : F \in I\} \subseteq k[x_0, \cdots, x_{n-1}]$$

Adicionalmente, $V_* := \mathbb{V}(I_*) \subseteq \mathbb{A}^n_k \subseteq U_n$.

Ejemplo: Cuidado, si I es finitamente generado su homogenización no es igual a homogenizar cada uno de sus generadores y tomar el ideal generado. Sea $V = \mathbb{V}(y - x^2, z - x^3)$ que esta parametrizado por

$$\varphi(t) = (t, t^2, t^3)$$

Su ideal es $\mathbb{I}(V) = (y - x^2, z - x^3)$. Notemos que $z - xy \in I$, pero $zw - xy \notin (wy - x^2, w^2z - x^3)$.

Vamos a considerar $\mathbb{A}^n_k$ como un subconjunto de $\mathbb{P}^n_k$ mediante la biyección $\varphi : \mathbb{A}^n_k \to U_{n+1}$ dada por $\varphi(x_1, \cdots, x_n) = [x_1, \cdots, x_n, 1]$. Prontamente veremos que esta función define un isomorfismo entre ambas variedades algebraicas, con la topología de Zariski será un homeomorfismo.

Proposición 12.2. *Se cumplen las siguientes afirmaciones*

(1) Si $V \subseteq \mathbb{A}^n_k$, entonces $\varphi(V) = V^* \cap U_{n+1}$ y $(V^*)_* = V$.

(2) Si $V \subseteq W \subseteq \mathbb{A}^n_k$. Entonces $V^* \subseteq W^* \subseteq \mathbb{P}^n_k$. Se cumple lo análogo para deshomogenización.

(3) Si V es irreducible en $\mathbb{A}^n_k$, entonces V^* es irreducible en $\mathbb{P}^n_k$.

(4) Si $V = \bigcup_i V_i$ es la descomposición en irreducibles de V en $\mathbb{A}^n_k$, entonces $V^* = \bigcup_i V_i^*$ es la descomposición en irreducibles de V^* en $\mathbb{P}^n_k$.

(5) Si $V \subseteq \mathbb{A}^n_k$, entonces V^* es el conjunto algebraico mas pequeño que contiene a $\varphi_{n+1}(V)$.

(6) Si $V \subset \mathbb{A}^n_k$ es no vacío, entonces ninguna componente de V^* esta contenida o contiene a H_∞.

(7) Si $V \subseteq \mathbb{P}^n_k$ y ninguna componente de V esta contenida o contiene a H_∞ entonces $V_* \subset \mathbb{A}^n_k$ y $(V_*)^* = V$.

4.4. Espacio Multiproyectivo

Nos gustaría estudiar el producto de espacios proyectivos, esta no es una tarea tan natural como en el caso afín, pues un punto en $(x, y) \in \mathbb{P}_k^n \times \mathbb{P}_k^m$ no tienen relación entre sí. ¿Que significa que un polinomio se anule en (x, y)?

Escribiremos $k[x, y]$ como $k[x_1, \cdots, x_{n+1}, y_1, \cdots, y_{m+1}]$.

Definición 12.8. *Un polinomio $F \in k[x, y]$ se dice una **biforma de grado** (p, q), si F es una forma de grado p (resp. q) en la variable x (resp. y) con coeficientes en $k[y_1, \cdots, y_{m+1}]$ (resp. $k[x_1, \cdots, x_{n+1}]$).*

Observación: Todo polinomio $F \in k[x, y]$ puede ser escrito de manera única como $F = \sum_{p,q} F_{p,q}$ donde $F_{p,q}$ es una biforma de grado (p, q).

Ejemplo: Consideremos $\mathbb{P}_k^1 \times \mathbb{P}_k^1$ denotamos por $p \in \mathbb{P}_k^1 \times \mathbb{P}_k^1$ como $([x_0, x_1], [y_0, y_1])$, tomemos el polinomio $F = x_0^3 y_1 + y_0 x_1^3$, que es una biforma de grado $(3, 1)$.

Definición 12.9. *Sea $S \subset k[x_1, \cdots, x_{n+1}, y_1, \cdots, y_{m+1}]$ un conjunto de biformas, definimos*

$$\mathbb{V}(S) := \{(x, y) \in \mathbb{P}_k^n \times \mathbb{P}_k^m : F(x, y) = 0 \text{ para todo } F \in S\}$$

Decimos que $V \subseteq \mathbb{P}_k^n \times \mathbb{P}_k^m$ es conjunto algebraico si $V = \mathbb{V}(S)$ para algún S.

Definición 12.10. *Dado $V \subseteq \mathbb{P}_k^n \times \mathbb{P}_k^m$, definimos*

$$\mathbb{I}(V) := \{F \in k[x, y] : F(x, y) = 0 \text{ para todo } (x, y) \in V\}$$

Observación: Si se define un ideal bihomogeneo, como es natural, resulta que $\mathbb{I}(V)$ es un ideal bihomogeneo.

El resto de definiciones y resultados, presenten en los casos afín y proyectivo, se extienden de manera natural al caso multiproyectivo.

5. Curvas Planas Proyectivas

5.1. Definiciones

Definición 12.11. *Decimos que un conjunto algebrico $V \subseteq \mathbb{P}^2_k$ es una* ***curva plana proyectiva*** *si $V = \mathbb{V}(F)$ con F una forma grado d. El* ***grado de la curva*** *corresponde al grado del polinomio que la define.*

Decimos que una curva de grado 1 es una recta, una de grado 2 una cónica, de grado 3 una cúbica y de grado 4 una cuártica.

Observación: Notemos que si F es irreducible y $p \in V$ tal que $p = [x, y, 1]$ entonces $\Gamma_h(V)$ es dominio, entonces esta definido $\mathcal{O}_p(V)$. Además, se tiene un isomorfismo canónico entre $\mathcal{O}_p(V)$ y $\mathcal{O}_{(x,y)}(V)$ identificando un polinomio $F \in k[x, y, z]$ con $F_* \in k[x, y]$.

Desde este momento, supondremos que, $V = \mathbb{V}(F)$ con $F \in k[x, y, z]$ una forma.

Definición 12.12. *Sea $p \in V$, decimos que p es un punto* ***singular****, si $F_x(p) = F_y(p) = F_z = 0$.*

Observación: De la formula $dF = x_1 F_{x_1} + x_2 F_{x_2} + x_3 F_{x_3}$, deducimos que basta con que se anule en dos de las tres derivadas.

Definición 12.13. *Sea $p \in V$, definimos la* ***multiplicidad*** *de F en p, denotado por $m_p(F)$, como $m_p(F) = m_p(F_*)$.*

Observación: La multiplicidad es independiente de la carta afín escogida e invariante bajo cambio de coordenadas proyectivo.

Si V es una curva irreducible de grado d, sea L una recta tal que $p \notin L$, consideramos

$$f = \frac{F}{L^d} \in \mathcal{O}_p(V)$$

Si p es simple (no singular), es decir $m_p(V) = 1$, entonces $\mathcal{O}_p(V)$ es un DVR, denotamos por ord_p^F la función de orden en $k(V)$.

Definición 12.14. *Sean F, G dos curvas planas proyectivas cualesquiera y sea $p \in \mathbb{P}^2_k$, definimos el* ***número de intersección*** *como*

$$I(p, F \cap G) := dim_k \left(\frac{O_p(\mathbb{P}^2_k)}{(f, g)} \right)$$

Observación: De la definición de f, si L' es otra recta tal que $p \notin L'$ entonces $\frac{L'}{L}$ es una unidad en $\mathcal{O}_p(\mathbb{P}^2_k)$ y por lo tanto la definición del número de intersección es independiente de como se escoge L. Por otro lado, como en el caso afín este número cumple las mismas propiedades, con excepción de que en (7) el polinomio A debe ser una forma tal que $gr(A) = gr(G) - gr(F)$.

Definición 12.15. *Decimos que una recta L, es* ***tangente*** *a una curva V en p si $I(p, F \cap L) > m_p(F)$. Un punto multiple es* ***ordinario*** *en F si F tiene $m_p(F)$ rectas tangentes distintas en p.*

Definición 12.16. *Dos curvas F y G se dicen* ***proyectivamente equivalentes****, si existe un cambio de coordenadas proyectivo T tal que $G = F^T$.*

5.2. Sistemas Lineales de Curvas

La intención de esta sección es estudiar todas las curvas proyectivas de grado d. Una forma F de grado d con variables x, y, z tiene, por un argumento de conteo, $N = \binom{d+2}{2}$ monomios. Luego, una curva F es lo mismo que escoger $a_1, \cdots, c_N \in k$ no todos cero, además, $\lambda a_1, \cdots, \lambda a_N$ determinan la misma curva.

Por el argumento anterior tenemos una correspondecia uno a uno entre las curvas de grado d con los punto en $\mathbb{P}^{N-1}_k$.

$$\{\text{Curvas de grado d}\} \longleftrightarrow \mathbb{P}^{N-1}_k$$

Ejemplos:

- Sea $d = 1$, una recta $ax + by + cz$ corresponde a un punto $[a, b, c] \in \mathbb{P}^2_k$.

- Para $d = 2$, las cónicas $ax^2 + by^2 + cz^2 + dxy + exz + fyz$ corresponden a puntos $[a, b, c, d, e, f] \in \mathbb{P}^5_k$.

Definición 12.17. *Un sistema lineal de curvas de grado d es una subvariedad lineal de $\mathbb{P}^{N-1}_k$. Decimos que la dimensión del sistema es n, si el conjunto solución tiene dimensión n.*

Lema 12.1.

a) Sea $p \in \mathbb{P}^2_k$ un punto fijo. El conjunto de curvas de grado d que contienen a p forma un hiperplano en $\mathbb{P}^{N-1}_k$.

b) Si $T : \mathbb{P}^2_k \to \mathbb{P}^2_k$ es un cambio de coordenadas proyectivo, entonces la función $F \to F^T$ de curvas de grado d a curvas de grado d es un cambio de coordenadas proyectivo en $\mathbb{P}^{N-1}_k$

Demostración.

a) Una curva F de grado d, con $(a_1, \cdots, a_N)$ los puntos correspondientes en $\mathbb{P}^{N-1}_k$, pasa por el punto p si y solo si

$$F(p) = \sum_{i=1}^{N} a_i M_i(x, y, z) = 0$$

con M_i un monomio sin constante de grado d. Como M_i no son todos cero, los puntos $(a_1, \cdots, a_N)$ satisfacen la ecuación de un hiperplano.

b) La demostración es similar.

Proposición 12.3. *Sea $p \in \mathbb{P}^2_k$ y $r \leq d + 1$. Luego*

$$V(d; rP) := \{F \in \mathbb{P}^{N-1}_k \text{ de grado } d : mp(F) \geq r\} \subseteq \mathbb{P}^{N-1}_k$$

es un sistema lineal de dimensión

$$\frac{d(d+3)}{2} - \frac{r(r+1)}{2}$$

Demostración. *Por el segundo resultado del lema anterior, podemos suponer que $p = [0, 0, 1]$. Sea F una forma de grado d, luego el término cz^d es cero, es decir, $c = 0$, escribimos*

$$F_* = f_0 + f_1(x, y) + f_2(x, y) + \cdots + f_d(x, y)$$

como $F \in V(d; rP)$ se tiene que $f_0 = f_1 = f_2 = \cdots = f_{r-1} = 0$. Hay $\frac{r(r+1)}{2}$ coeficientes que deden ser cero. Luego la dimensión es

$$\frac{d(d+3)}{2} - \frac{r(r+1)}{2}$$

Notemos que el conjunto corresponde a la intersección de hiperplanos y por ende es un sistema lineal.

Sean $p_1, \cdots, p_n \in \mathbb{P}^2_k$ y sean $r_1, \cdots, r_n \in \mathbb{N}$. Consideramos el sistema lineal

$$V(d; r_1, p_1, \cdots, r_n p_n) := \bigcap_i V(d; r_i p_i)$$

Teorema 13. *Se tiene lo siguiente*

a) El sistema lineal $V(d; r_1, p_1, \cdots, r_n p_n)$ tiene dimensión al menos

$$\frac{d(d+3)}{2} - \sum \frac{r_i(r_i+1)}{2}$$

b) Si $d \geq (\sum r_i) - 1$, entonces

$$dim_k V(d; r_1, p_1, \cdots, r_n p_n) = \frac{d(d+3)}{2} - \sum \frac{r_i(r_i+1)}{2}$$