



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

<b>Introducción</b>	<b>3</b>
<b>1. Conjuntos Algebraicos afines</b>	<b>4</b>
1.1. Preliminares algebraicos . . . . .	4
1.2. Espacio Afín y Conjuntos Algebraicos . . . . .	4
1.3. Ideal de un conjunto . . . . .	5
1.4. El Teorema de la Base de Hilbert . . . . .	5
1.5. Componentes Irreducibles en un Conjunto Algebraico . . . . .	6
1.6. Conjuntos Algebraicos del Plano . . . . .	7
1.7. Nullstellensatz de Hilbert . . . . .	8
1.8. Modulos y Condiciones de Finitud . . . . .	11
1.9. Elementos Integrales . . . . .	11
<b>2. Variedades Afines</b>	<b>14</b>
2.1. Anillo de Coordenadas . . . . .	14
2.2. Aplicaciones Polinomiales . . . . .	14
2.3. Cambio de Coordenadas . . . . .	14
2.4. Funciones Racionales y Anillos Locales . . . . .	14
2.5. Anillos de Evaluación Discreta . . . . .	15
2.6. Formas . . . . .	16
2.7. Producto Directo de Anillos . . . . .	16
2.8. Operando con Ideales . . . . .	17
2.9. Ideales de un Número Finito de Puntos . . . . .	17
2.10. Modulos Cociente y Secuencias Exactas . . . . .	18
2.11. Modulos Libres . . . . .	18
<b>3. Propiedades Locales de Curvas Planas</b>	<b>20</b>

## 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  $f : R \rightarrow R'$  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

$$f(x) = a_0 + a_1x + \cdots + a_dx^d, \quad a_d \neq 0$$

y decimos que  $f$  tiene grado  $d$  denotado por  $gr(f)$ . Se define de manera recursiva  $R[x_1, \dots, x_n] = R[x_1, \dots, x_{n-1}][x_n]$  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  $f \in R[x_1, \dots, x_n]$  y  $d = gr(f)$  entonces

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

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

Decimos que  $r \in R$  es irreducible 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 única si todo elemento no nulo se puede factorizar de manera esencialmente única en producto de irreducibles.

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

**Lema 1.2.** *Si  $R$  es un dominio de factorización única y  $K$  su cuerpo de fracciones. Dado  $f \in R[x]$  irreducible entonces  $f$  es irreducible 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  $\pi : R \rightarrow R/I$  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 euclideo (se cumple algoritmo de la división) y  $a, b \in R$ , consideremos  $\text{mcd}(a, b) = d$ . Entonces existen  $c, e \in R$  tales que  $ac + be = d$ .*

**Teorema 3.** *Si  $F$  es un polinomio homogéneo 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 supondrá que  $k = \bar{k}$ ).*

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

**Ejemplos:**

- Sea  $k = \mathbb{R}$  consideramos la hipersuperficie  $V(y^2 - x^2(x+1)) \subseteq \mathbb{A}_{\mathbb{R}}^2$  (foto)  
El punto  $(0,0)$  se llama nodo.
- Veamos la hipersuperficie  $V((x^3 - y^3)(y^3 - 1)(x^3 - 1)) \subseteq \mathbb{A}_{\mathbb{C}}^2$ .
- La hipersuperficie  $V(x^2 + y^2 - z^2) \subseteq \mathbb{A}_{\mathbb{R}}^3$  es conocida como cono (foto)  
Como en el primer ejemplo, el punto  $(0,0)$  se llama nodo
- Consideremos  $V(y^2 - x^3) \subseteq \mathbb{A}_{\mathbb{R}}^2$  (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  $S \subseteq k[x_1, \dots, x_n]$  un conjunto arbitrario, se define

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

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  $F, G \in k[x_1, \dots, x_n]$ , se tiene que  $V(FG) = V(F) \cup V(G)$ .
- e) Tenemos las siguientes dos identidades  $V(1) = \emptyset$  y  $V(0) = \mathbb{A}_k^n$ .

**observación:** Lo anterior es valido si  $k$  es algebraicamente cerrado, de lo contrario, si consideramos  $\mathbb{A}_{\mathbb{R}}^1$  vemos que  $V(x^2 + 1) = \emptyset$ .

### 1.3. Ideal de un conjunto

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

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

**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  $I(\emptyset) = k[x_1, \dots, x_n]$  y  $I(\mathbb{A}_k^n) = \{0\}$ . Además, si  $k$  es un cuerpo infinito, se tiene que  $I(\{a_1, \dots, a_n\}) = (x_1 - a_1, \dots, x_n - a_n)$ .

### 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  $I \subseteq k[x_1, \dots, x_n]$ . Basta con probar que  $I$  es finitamente generado, en tal caso  $I = (F_1, \dots, F_r)$ , entonces  $V(I) = V(F_1, \dots, F_r) = V(F_1) \cap \dots \cap V(F_r)$ .

**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 pérdida 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 hipótesis existen  $F_1, \dots, F_r \in I$  tales que  $\mathcal{J} = (l(F_1), \dots, l(F_r))$ . 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

- Veamos cuando  $gr(G) > N$ , existen polinomios  $Q_i \in R[X]$  tal que  $G$  y  $\sum Q_i F_i$  tienen el mismo coeficiente líder. Luego  $G - \sum Q_i F_i \in I'$  pues tiene menor grado que  $G$ , se sigue que  $G \in I'$ .
- El resultado para  $gr(G) \leq N$  se obtiene del mismo modo, usando esta vez los  $F_{m,j}$ .

**Ejemplo:** Sea  $(0,0) \in \mathbb{A}_{\mathbb{R}}^2$ , 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 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  $\mathbb{A}_{\mathbb{R}}^1$ , entonces el conjunto algebraico  $V((x^2 + 1)x) = \{0\}$  es irreducible.

**Proposición 5.1.** Un conjunto algebraico  $V$  es irreducible 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:

- $R$  es Noetheriano.
- 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

$$\mathcal{C}_2 := \{I \in \mathcal{C}_1 : I \subset I\}$$

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  $I = (f_1, \dots, f_m)$ , luego existe  $r$  tal que  $f_1, \dots, f_m \in I_r$ , 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

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

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

**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  $k[x_1, \dots, x_n]$ , 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  $V_1, \dots, V_m$  tales que

$$V = \bigcup_{i=1}^m V_i \quad \text{y} \quad V_i \not\subseteq V_j \quad \forall i \neq j$$

**Demostración.** Sea  $\mathcal{C} = \{V \subseteq \mathbb{A}_k^n \text{ conjunto algebraico} : V \text{ no es unión finita de irreducibles}\}$ . 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  $V_i \not\subseteq V_j$  para todo  $i \neq j$ . Digamos que

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

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 euclideo. 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  $k = \bar{k}$ . 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  $I(V(f)) = (f_1, \dots, f_m)$ .

**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,

$$I(V(f)) = I\left(\bigcup_{i=1}^m V(f_i)\right) = \bigcap_{i=1}^m I(V(f_i)) = \bigcap_{i=1}^m (f_i) = (f_1 \cdots f_m)$$

## 1.7. Nullstellensatz de Hilbert

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

**Teorema 7.** Sea  $I \subset k[x_1, \dots, x_n]$  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  $k[x_1, \dots, x_n]/I \supset k$  es cuerpo. Como  $k$  es algebraicamente cerrado, podemos asumir que  $k[x_1, \dots, x_n]/I = k$ .

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  $I = (x_1 - a_1, \dots, x_n - a_n)$ . (Mejorar escritura)



De la demostración surge una pregunta, ¿Por que  $k[x_1, \dots, x_n]/I = k$ ? 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  $k$ -álgebra. 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  $I \subset k[x_1, \dots, x_n]$  es un ideal maximal, luego  $L := k[x_1, \dots, x_n]/I$  es cuerpo, consideramos el morfismo canónico

$$\begin{array}{ccc} \mathbb{C}[x_1, \dots, x_n] & \xrightarrow{\pi} & L \\ \uparrow i & \nearrow \pi_i := \pi|_{\mathbb{C}[x_i]} & \\ \mathbb{C}[x_i] & & \end{array}$$

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  $I = k[x_1, \dots, x_n]$ . 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  $(x_1 - a_1, \dots, x_n - a_n) \subseteq I$ . Como  $(x_1 - a_1, \dots, x_n - a_n)$  es ideal maximal e  $I$  es propio se obtiene el resultado.
- Existe  $i$  tal que  $\ker(\pi_i) = (0)$ , entonces  $\pi_i$  es inyectiva, como  $L$  es cuerpo  $\mathbb{C}(x_i)$  se incrusta en  $L$ .

$$\begin{array}{ccc} \mathbb{C}[x_i] & \xrightarrow{\pi_i} & L \\ \downarrow i & \nearrow i_L & \\ \mathbb{C}(x_i) & & \end{array}$$

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

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

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  $I \subset k[x_1, \dots, x_n]$ , 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  $I = (f_1, \dots, f_m)$ . Definimos el ideal  $J := (f_1, \dots, f_m, x_{n+1}f - 1) \subseteq k[x_1, \dots, x_{n+1}]$ . Supongamos que  $(a_1, \dots, a_n, a_{n+1}) \in V(J)$ , entonces  $(a_1, \dots, a_n) \in V(I)$  se sigue que  $f(a_1, \dots, a_n) = 0$ , esto resulta en una contradicción. Concluimos que  $V(J) = \emptyset$ .

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

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

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

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

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

**Corolario 8.1.** Hay una correspondencia 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 correspondencia 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  $k[x_1, \dots, x_n]$ .

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

### Demostración.

- $\Leftarrow$  | Sean  $p_1, \dots, p_r \in V(I) \subseteq \mathbb{A}_k^n$ . Consideramos  $F_1, \dots, F_r \in k[x_1, \dots, x_n]$  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  $k[x_1, \dots, x_n]/I = R$ .

Afirmamos que el conjunto  $\{F_1, \dots, F_r\}$  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  $V(I) = \{p_1, \dots, p_r\}$  y  $p_i = (a_{i1}, \dots, a_{in})$ . 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  $\text{gr}(p_j) < rN$  entonces  $\dim_k R < \infty$ .

### Ejemplos:

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

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

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

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

así  $\dim_k R = 0$ .

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

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

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

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

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

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

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

## 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

$$v^n + r_{n-1}v^{n-1} + \dots + r_1v + r_0 = 0$$

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  $w_1, \dots, w_n$  generadores de  $R'$ . Sabemos que

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

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  $R \subseteq S$  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,  $(w_1, \dots, w_n)$  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  $\{1, a, a^2, \dots, a^{n-1}\}$  y  $\{1, b, b^2, \dots, b^{m-1}\}$ . 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  $z \in \text{Frac}(R) \setminus R$  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 raíz racional,  $q$  debe dividir a 1, luego  $q = 1$  lo que implica que  $p/q \in \mathbb{Z}$ . Concluimos que  $\mathbb{Z}$  es integralmente cerrado.

- Veamos el conjunto algebraico  $V(y^2 - x^3) \subseteq \mathbb{A}_k^2$  con  $k = \bar{k}$ . 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  $R \subseteq \text{Frac}(R)$ , 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  $\varphi : \mathbb{A}_k^1 \rightarrow \mathbb{A}_k^2$  dada por  $\varphi(t) = (t, t^2)$ . Notemos que  $\text{Im}(\varphi) = V(y - x^2)$ . La función  $\varphi$  induce el isomorfismo

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

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

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

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

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  $y^m = a_{m-1}y^{m-1} + \cdots + a_1y + a_0$  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

$$\begin{aligned} a^N z &= a^N f(x, y) \\ &= a^N (c_0 + c_1 y + \cdots + c_M y^M) \\ &= c'_0 + c'_1(ay) + \cdots + c'_M(ay)^M \end{aligned}$$

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 irreducible 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

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

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  $I(V)$  es un ideal primo de  $k[x_1, \dots, x_n]$ . Por otro lado, dado  $f, g \in k[x_1, \dots, x_n]$  entonces  $f, g$  determinan la misma función si y solo si  $f - g \equiv 0$  en  $V$ , es decir,  $f - g \in I(V)$ . 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  $\varphi : V \rightarrow W$  se dice **aplicación polinomial** si existen  $f_i \in k[x_1, \dots, x_n]$  tales que

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

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

#### Demostración.

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

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

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

- Sea  $\tilde{\varphi} : \Gamma(W) \rightarrow \Gamma(V)$  un homomorfismo. Sean  $f_i \in k[x_1, \dots, x_n]$  tales que  $\tilde{\varphi}(y_i) = f_i$ , definimos la aplicación polinomial  $\varphi := (f_1, \dots, f_m)$ , por la discusión anterior  $\varphi$  esta bien definida y además la función inducida por  $\varphi$  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  $\varphi = (f_1, \dots, f_n) : \mathbb{A}_k^n \rightarrow \mathbb{A}_k^n$  tal que  $gr(f_i) = 1$  y  $\varphi$  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  $k(V) := \text{Frac}(\Gamma(V))$ . Un elemento en  $k(V)$  se dice **función racional** en  $V$ .

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

**Definición 8.8.** Sea  $V \subseteq \mathbb{A}_k^n$  una variedad no vacía. Sea  $f$  una función racional de  $V$  y  $p \in V$ , decimos que  $f$  está 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  $f$  está definida en  $p$  si y solo si  $b(p) \neq 0$ .

**Definición 8.9.** Sea  $V \subseteq \mathbb{A}_k^n$  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

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

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

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  $G, H \in k[x_1, \dots, x_n]$  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  $J_f = k[x_1, \dots, x_n]$  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  $I' = \langle f_1, \dots, f_m \rangle$ . 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  $p \in \mathbb{A}_k^1 = V$ , sea  $m_p(V)$  el unico ideal maximal de  $\mathcal{O}_p(V)$ , luego  $(t) = m_p(V)$ .
- Un no ejemplo. Si tomamos  $p = (0, 0) \in \mathbb{A}_k^2 = V$  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  $k = \text{Frac}(R)$ , entonces para todo  $z \in k$  existe  $n \in \mathbb{Z}$  y  $u \in R$  unidad tales que  $z = ut^n$ , luego

- $n$  es el **orden** de  $z$  y se escribe  $\text{ord}(z)$ . Decimos que  $\text{ord}(0) = \infty$ .
- Si  $n < 0$ , entonces  $z$  es un **polo**.
- Si  $n > 0$ , decimos que  $z$  es un **cero**.
- Si  $n = 0$ ,  $z$  se dice **unidad**.

## 2.6. Formas

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

**Ejemplo:** Sea  $f = x_1^2 + x_2^2 + x_3 x_4$  es una forma.

**Definición 8.14.** Sea  $R$  un dominio,

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

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

este proceso se llama **homogenización**.

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

**Proposición 8.6.** Se cumple lo siguiente

- $(FG)_* = F_* G_*$  y  $(fg)^* = f^* g^*$ .
- 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,  $(f^*)_*$ .
- Se tiene que  $(F + G)_* = F_* + G_*$ . Por otro lado, sea  $r = \text{gr}(g)$ ,  $s = \text{gr}(f)$  y  $t = r + s - \text{gr}(f + g)^*$  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  $R_1, \dots, R_n$  anillos, definimos  $R := \prod R_i$  junto con las operaciones

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

y  $\pi_i : R \rightarrow R_i$  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  $(0, \dots, 0)$  y  $(1, \dots, 1)$  son los neutros de  $+$  y  $\cdot$  respectivamente.

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

$$\begin{array}{ccc} S & \xrightarrow{\varphi} & R \\ \phi_i \downarrow & \swarrow \pi_i & \\ R_i & & \end{array}$$



## 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  $I = \langle a_1, \dots, a_n \rangle$  entonces

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

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

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

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

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

$$\sqrt{I} = \mathbb{I}(\{p_1, \dots, p_m\}) = \bigcap_{i=1}^m I_i$$

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

Sean  $F_i \in k[x_1, \dots, x_n]$  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  $i = 1, \dots, m$ . 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  $G \in k[x_1, \dots, x_n]$  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  $\varphi$  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  $G \in k[x_1, \dots, x_n]$  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  $\varphi$  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

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

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  $\varphi$  es sobreyectiva.

**Corolario 8.6.**

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

## 2.10. Módulos Cociente y Secuencias Exactas

Sea  $R$  un anillo, sean  $M$  y  $V$   $R$ -módulos un morfismo de grupos  $\varphi : M \rightarrow V$  se dice **morfismo de  $R$ -módulos** 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 submódulo de un  $R$ -módulo  $M$ , en el grupo cociente  $M/N$  consideramos la operación  $a\bar{m} = \overline{am}$ , lo que da estructura de  $R$ -módulo y lo llamamos el **módulo cociente** de  $M$  por  $N$ .

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

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

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

**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  $\dim V' + \dim V'' = \dim V$ .

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  $\dim V_4 = \dim V_3 - \dim V_2 + \dim V_1$

## 2.11. Módulos Libres

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

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

Lo dotamos de estructura de  $R$ -módulo 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 módulo  $M_X$  se dice  **$R$ -módulo 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 única  $\varphi = \sum a_x \varphi_x$  donde  $a_x = \varphi(x)$ . Usualmente escribimos  $x$  en lugar de  $\varphi_x$ .

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

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

### 3. Propiedades Locales de Curvas Planas