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 $F = a_0 + a_1 x + \cdots + a_d x^d$ 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 $\sum Q_i F_i$ tienen el mismo coeficiente líder. Luego $G - \sum Q_i F_i \in I'$ pues tiene menor grado que G, se sigue que $G \in I'$.

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 $\mathbb{A}^2_k$ son: $\emptyset$, $\mathbb{A}^2_k$, 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 $V = \mathbb{A}^2_k$. 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*

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

  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 $V((x - y, y - x^2)) = \{(0, 0), (1, 1)\}$

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

- 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

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.