Álgebra conmutativa y geometría algebráica

Eduardo Paluzo

Universidad de Sevilla
Versión de 8 de enero de 2017

Índice general

Introducción

Se pretende hacer un compendio de la teoría dada en la asignatura de **Álgebra conmutativa y geometría algebráica**.

Bibliografía principal:

- Fulton, W. Algebraic Curves (Curve book)
- Atiyah Macdonald , An introduction to Commutative Algebra

La evalucación continua consistirá en una serie de trabajos (70) y un examen final (30).

Horarios de tutorías:

- L,M $\rightarrow$ 9:00 - 11:00 y J $\rightarrow$ 15:30 - 17:30 mcferfer@us.es
- M,X,J 10:30 - 13:30 soto@us.es

Parte I

Impartida por MªCruz

Capítulo 1

Conjuntos algebraicos afines

1.1. Preliminares algebraicos

Definición 1.1.1. Un **anillo** es un conjunto A dotado de dos operaciones binarias, que llamaremos suma (+) y producto (·) que verifican:

1. $(A, +)$ Grupo abeliano.
2. Propiedad asociativa del producto: $a(bc) = (ab)c$
3. Propiedad distributiva del producto respecto de la suma: $a(b + c) = ab + ac$
4. Existencia de elemento neutro para el producto: 1_A tal que $1_A \cdot a = a, \forall a, b, c \in A$

   Algunos ejemplos de anillos:

- $A = \{0\}$ es un anillo.
- $\mathbb{Z}$ el anillo de los enteros.
- $k[x]$ el anillo de los polinomios con coeficiente en un cuerpo k.
- $A[x]$ el anillo de los polinomios con coeficientes en un anillo A.

Definición 1.1.2. Un subconjunto $I \subseteq A$ de un anillo A se llama **ideal** si $(I, +)$ subgrupo de $(A, +)$ y $\forall a \in A, \forall b \in I$ entonces $ab \in I$

Definición 1.1.3. Sea $I \subseteq A$ un ideal, se llama **anillo cociente** de A por I al conjunto cociente A/I dado por el cociente de A respecto de la siguiente relación de equivalencia en A: $a, b \in A, a \sim b \Leftrightarrow a - b \in I$

Denotaremos $[a] = \bar{a} = a + I$ a la clase de equivalencia de $a \in A$ respecto de la relación de equivalencia anterior.

A/I es anillo con las operaciones + y · naturales:

- $\bar{a} + \bar{b} = \overline{a+b}$
- $\bar{a} \cdot \bar{b} = \overline{ab}, \forall \bar{a}, \bar{b} \in A \backslash I$

Más ejemplos de anillos:

- Sea $m \in \mathbb{Z}, < m >= \{am : a \in \mathbb{Z}\} \subseteq \mathbb{Z}$ ideal. $\mathbb{Z}/m\mathbb{Z}$ anillo cociente.

Definición 1.1.4. Un elemento $a \in A$ se llama **divisor de cero** si $\exists b \neq 0, b \in A$ tal que $ab = 0$.

Definición 1.1.5. Un anillo $A \neq 0$ es un **dominio de integridad** si no tiene divisores de cero distintos del cero. Un dominio de integridad en el que todo elemento no nulo tiene inverso se llama **cuerpo**.

Definición 1.1.6. Un ideal $I \subseteq A$ es **propio** si $I \neq A$.

Definición 1.1.7. Un ideal $I \subseteq A$ es **primo** si es propio y $\forall a, b \in A$, si $ab \in I \Rightarrow a \in I$ o $b \in I$.

Definición 1.1.8. Un ideal $I \subseteq A$ es **maximal** si es propio y $\nexists J$ ideal propio tal que $I \subseteq J, I \neq J$.

Proposición 1.1.1. *Sea $I \subseteq A$ ideal, entonces:*

1. *I primo $\Leftrightarrow A/I$ es dominio de integridad.*
2. *I maximal $\Leftrightarrow A/I$ es cuerpo.*

Ejemplo:

- $\mathbb{Z}/m\mathbb{Z}$ es dominio de integridad $\Leftrightarrow m = 0$ y m primo. ($< m >$ primo o cero).
- $\mathbb{Z}/m\mathbb{Z}$ es cuerpo $\Leftrightarrow m$ primo. ($< m >$ maximal)

Definición 1.1.9. Sea $a \in A$, se dice que a es una **unidad** si $\exists b \in A$ tal que $ab = 1_A$ y notaremos $a^{-1} = b$

Definición 1.1.10. Un elemento $a \in A$ se llama **irreducible** si no es 0 ni unidad y $\forall b, c \in A$ tal que $a = bc \Rightarrow b$ unidad o c unidad.

Definición 1.1.11. Un **dominio de factorización única** es un dominio de integridad tal que todo elemento no nulo de A se puede escribir como producto de elementos irreducibles y unidades. Además, esta factorización es única, salvo producto por unidades y el orden de los factores.

Ejemplos:

- $\mathbb{Z}, k[x]$

Definición 1.1.12. Sea A un dominio de integridad, se llama **cuerpo de fracciones** de A al conjunto cociente de $A \times (A \backslash \{0\})$ respecto de la siguiente relación de equivalencia:

- $(a,b),(c,d) \in A \times (A\backslash\{0\})$, $(a,b) \sim (c,d) \Leftrightarrow ad = bd$ en A.

Denotaremos $\frac{a}{b}$ a la clase de equivalencia de (a,b).
Denotaremos $Q(A) = \frac{A \times (A\backslash\{0\})}{\sim}$

Proposición 1.1.2. *$Q(A)$ con las operaciones + y $\cdot$ siguientes es un cuerpo:*

- $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$
- $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$

Ejemplo:

- $A = \mathbb{Z} \Rightarrow Q(\mathbb{Z}) = \mathbb{Q}$
- $A = k[x] \Rightarrow Q(k[x]) = k(x) = \{\frac{f}{g} : f,g \in k[x], g \neq 0\}$

Lema 1.1.1. ***Lema de Gauss*** *Sea A un dominio de factorización única y $f,g \in A[x]$. Entonces, $c(fg) = c(f)c(g)$.*

Definición 1.1.13. El **contenido** de f , $c(f)$, es el máximo comun divisor de los coeficientes de f.

Corolario 1.1.1. *Si A es dominio de factorización única y $f \in A[x]$ entonces f es irreducible en $A[x] \Leftrightarrow f$ es irreducible en $K[x]$, donde $K = Q(A)$.*

Definición 1.1.14. Sea A anillo y $B \subseteq A$, diremos que B es **subanillo** de A si $(B,+)$ es subgrupo abeliano de $(A,+)$, $1_A \in B$, y B es cerrado para el producto ($ab \in B, \forall a,b \in B$).

Definición 1.1.15. Un ideal $I \subseteq A$ se dice que está **generado por un conjunto** $S \subseteq A$ si $I =< S >:= \{\sum_{i=1}^{r} a_i s_i : s_i \in S, a_i \in A, r \in \mathbb{N}, i = 1,\ldots,r\}$

Definición 1.1.16. Un ideal es **principal** si está generado por un único elemento.

Definición 1.1.17. Un dominio de integridad en el que todo ideal es principal se llama **dominio de ideales principales**.

Ejemplos:

- $\mathbb{Z}, k[x]$ con k cuerpo.
- $k[x_1, \ldots, x_n]$ $(n \leq 2)$ es dominio de factorización única, pero no es dominio de ideales principales.

Nota 1.1.1. *Si A es dominio de ideales principales, entonces A es dominio de factorización única.*

Definición 1.1.18. Sea $f : A \to B$ una aplicación entre anillos, se dice que f es un **morfismo de anillos** si:

1. $f(a+b) = f(a) + f(b), \forall a, b \in A$ (f morfismo de grupos abelianos).
2. $f(ab) = f(a)f(b), \forall a, b \in A$.
3. $f(1_A) = 1_B$.

   Ejemplo:

- id:$A \to A$ es un morfismo de anillos.
- $I \subseteq A$ ideal, $\pi : A \to A/I, a \to \bar{a}$ es un morfismo de anillos.

Proposición 1.1.3. *Si $f : A \to B$ es morfismo de anillos y $J \subseteq B$ es un ideal $\Rightarrow f^{-1}(J)$ es un ideal de A.*

En particular, el núcleo de f, $ker(f) := f^{-1}(0)$ es un ideal.

Nota 1.1.2. *Un homomorfismo es inyectivo si y sólo si el núcleo es 0.*

Operaciones con ideales:

- La intersección de ideales es un ideal.
- La unión de ideales **NO** es en general un ideal. La unión infinita de ideales encajados sí es un ideal.
- La suma de ideales es el ideal generado por la unión.
- El producto de dos ideales $I, J \subseteq A$ es el ideal

$$IJ := < \{ab : a \in I, b \in J\} > = \{\sum_{i=1}^{r} a_i b_i : a_i \in I, b_j \in J, r \in \mathbb{N}, i, j = 1, \ldots, r\}$$

Cuestión(Entrega antes de la clase del viernes 30 Sept.): Sea k un cuerpo infinito, $F \in k[x_1, \ldots, x_n]$. Supongamos que $F(a_1, \ldots, a_n) = 0, \forall (a_1, \ldots, a_m) \in k^n$. Hay que probar que $F = 0$.

Cuestión: Sea k un cuerpo, $F \in k[x_1, \ldots, x_n], a_1, \ldots, a_n \in k$. Probar:

1. $F = \sum \lambda_{(i)} (x_1 - a_1)^{i_1} \ldots (x_n - a_n)^{i_n}$
2. Si $F(a_1, \ldots, a_n) = 0$, probar $F = \sum_{i=1}^{n} (x_i - a_i) G_i$ con $G_i \in k[x_1, \ldots, x_n]$

   Problemas 1.4 y 1.7 Fulton.

1.2. El espacio afín y los conjuntos algebraicos

Sea k cuerpo, se denotará $\mathbb{A}^n = \mathbb{A}^n(k)$ al espacio afín de dimensión n sobre el cuerpo k, cuyos elementos son del tipo $(a_1, \ldots, a_n)$, $a_i \in k$.

Definición 1.2.1. Un **conjunto algebraico afín** es el conjunto de puntos del espacio afín, $\mathbb{A}^n$, que es solución de un sistema de ecuaciones polinómicas. Es decir, es un conjunto de la forma:

$$V(S) := \{p = (a_1, \ldots, a_n) \in \mathbb{A}^n | f(a_1, \ldots, a_n) = 0, \forall f \in S\}$$

Para cierto $S \subseteq k[x_1, \ldots, x_n]$

Ejemplo:

- $S = \{0\} \Rightarrow V(S) = \mathbb{A}^n$ es un conjunto algebraico.
- $S = k[x_1, \ldots, x_n] \Rightarrow V(S) = 0$
- S es un conjunto finito de polinomios de grado 1 $\Rightarrow V(S)$ variedad lineal afín.
- $S = \{f\}$ con grado(f) = 2 $\Rightarrow V(S)$ es una hipercuádrica lugar afín.

Nota 1.2.1. *Si $S = \{f\}, f \neq 0$ diremos que $V(S)$ es una hipersuperficie. En particular, si $n = 2 \rightarrow V(f)$ se llama una curva plana afín.*

Nota 1.2.2. $S \subseteq k[x_1, \ldots x_n]$, $V(S) = \bigcap_{f \in S} V(f)$

Propiedades

1. $I =< S >\subseteq k[x_1, \ldots, x_n] \Rightarrow V(I) = V(S)$. Luego, todo conjunto algebraico es de la forma $V(I)$ para algún ideal.
2. $\{I_\alpha\}_{\alpha \in A}$ familia de ideales $\Rightarrow V(\bigcup_{\alpha \in A} I_\alpha) = \bigcap_{\alpha \in A} V(I_\alpha)$; En particular, $V(< \cup_\alpha I_\alpha >) = \cap_\alpha V(I_\alpha)$.
3. $I \subseteq J \Rightarrow V(J) \subseteq V(I)$
4. $V(fg) = V(f) \cup V(g)$. Sean $I, J \subseteq k[x_1, \ldots, x_n]$ ideales $\Rightarrow V(IJ) = V(I \cap J) = V(I) \cup V(J)$
5. $V(0) = \mathbb{A}^n, V(k[\vec{x}]) = \emptyset$
6. Si $p = (a_1, \ldots, a_n) \in \mathbb{A}^n, V(x_1 - a_1, \ldots, x_n - a_n) = \{p\}$.

Demostración 1. $\boxed{3}$. *Es obvio pues en J hay más polinomios que en I y, por tanto, todo punto solución de $\{f = 0 : f \in J\}$ es también solución de $\{f = 0 : f \in I\}$.* □

$\boxed{1}$. $S \subseteq I \Rightarrow V(I) \subseteq V(S)$

$\boxed{\supseteq}$ *Sea* $p \in V(S) \Rightarrow f(p) = 0, \forall f \in S$. *Hay que probar que* $f(p) = 0, \forall f \in I$. *Sea* $f \in I =< S >\Rightarrow \exists g_1, \ldots, g_r \in S, \exists h_1, \ldots, h_r \in k[\vec{x}] | f = \sum h_i g_i \Rightarrow f(p) = \sum h_i(p) g_i(p) = 0 \Rightarrow p \in V(I)$ $\square$

$\boxed{4}$. $(IJ \subseteq I) \wedge (IJ \subseteq J) \Rightarrow (V(I) \subseteq V(IJ)) \wedge (V(J) \subseteq V(IJ)) \Rightarrow V(I) \cup V(J) \subseteq V(IJ)$.

$\boxed{\supseteq}$ $P \in V(IJ)$. *Supongo* $P \notin V(I)$, *hay que probar que* $P \in V(I) \cup V(J)$. $\exists f \in I$ *tal que* $f(P) \neq 0$. *Sea* $g \in J$ *cualquiera, entonces* $fg \in IJ \Rightarrow (fg)(P) = f(P)g(P) = 0 \Rightarrow g(P) = 0 \Rightarrow P \in V(J)$ $\square$

Corolario 1.2.1. $\{V(I) : I \subseteq k[x_1, \ldots, x_n]$ *ideal* $\}$ *es la familia de cerrados de una topología en* $\mathbb{A}^n$, *que llamaremos topología de Zariski en* $\mathbb{A}^n$.

Ejercicio 1.3. Sea R un dominio de ideales principales, sea p ideal primo, $0 \neq p \subset R$.

1. Probar que p está generado por un elemento irreducible.

2. Probar que p es maximal.

   Solución:

1. $\exists a \in R$ tal que $p =< a >$ por ser R DIP. Reducción al absurdo: $a = bc$ con b, c no unidades $\Rightarrow b \in p \vee c \in p$.

   Si $b \in p =< a >\Rightarrow \exists d \in R$ tal que $b = da = dbc \Rightarrow dc = 1$. Luego, d y c unidades $\rightarrow\leftarrow$

2. Reducción al absurdo. Si p no es maximal $\Rightarrow$ $\exists q$ ideal, $p \subset q \subset R$, $q =< b >$. b unidad ya que $q \neq R$. $a \in< b >\Rightarrow a = cb$ para cierto $c \in R$, $\Rightarrow$ c unidad (a irreducible) $\Rightarrow b = c^{-1}a$ y $p =< a >=< b >= q$

Ejercicio 1.5. Sea k un cuerpo cualquiera. Probar que existe un número infinito de polinomios mónicos irreducibles en $k[x]$.

<u>*Solución:*</u>

Sean $F_1, \ldots, F_n$ todos los polinomios mónicos irreducibles de $k[x]$. Sea $F = 1 + F_1 \cdots F_n$, como $F_i | \prod F_j$ y $F_i \not| 1 \Rightarrow F_i \not| F \Rightarrow F$ irreducible.

Ejercicio 1.6. Probar que cualquier cuerpo algebraicamente cerrado (Todos los polinomios no constantes tienen al menos una raíz) es infinito.

<u>*Solución:*</u>

Si k fuera finito $\Rightarrow \{X - a : a \in k\}$ también sería finito, y entraría en contradicción con el ejercicio anterior.

Ejercicio 1.8. Probar que los conjuntos algebraicos de $\mathbb{A}^1(k)$ son $\mathbb{A}^1$ y los conjuntos finitos de puntos de $\mathbb{A}^1$.

<u>*Solución:*</u>

$I \subseteq k[x]$ ideal $\Rightarrow_{(k[x] \text{ DIP })} I =< f >$ para cierto $f \in k[x]$.

$V(f)$ es $\mathbb{A}^1$ si $f = 0$, y si $f \neq 0$ entonces serían las raíces del polinomio que no pueden ser más que el grado del polinomio.

Ejercicio 1.9. Si k cuerpo finito, entonces todo conjunto de $\mathbb{A}^n$ es algebraico.

Solución:

Como k es finito, entonces $\mathbb{A}^n$ es finito, y entonces todo subconjunto de $\mathbb{A}^n$ es finito. Como de las propiedades (5) y (4), los puntos y la unión de conjuntos algebraicos son algebraicos, entonces todo conjunto finito de puntos es algebraico.

Ejercicio 1.10. Ejemplo de conjunto infinito numerable de conjuntos algebraicos que no sea conjunto algebraico.

Solución:

En $\mathbb{A}^1(k)$ si $\mathbb{Q} \subseteq k$, $\mathbb{Z}$ es un ejemplo.

Ejercicio 1.11 Probar que los siguientes conjuntos son algebraicos:

1. $\{(t, t^2, t^3) : t \in k\} \subseteq \mathbb{A}^3(k)$
2. $\{(cos(t), sin(t)) : t \in \mathbb{R}\} \subseteq \mathbb{A}^2(\mathbb{R}$
3. El conjunto de puntos de $\mathbb{A}^2(\mathbb{R})$ con coordenadas polares (r, θ) tales que $r = sen(\theta)$.

Solución:

1. $V(y - x^2, z - x^3)$
2. $V(x^2 + y^2 - 1)$
3. $x = rcos(\theta), y = rsin(\theta)$, entonces $x^2 + y^2 - y = 0$. (Elevando cuadrado y sumando).

Ejercicios 1.14,1.15: Entregar 30 Septiembre

1.3. El ideal de un conjunto de puntos en $\mathbb{A}^n$

Definición 1.3.1. Sea $X \subseteq \mathbb{A}^n$ un conjunto cualquiera, el conjunto $I(X) := \{f \in k[x_1, \ldots, x_n] : f(p) = 0, \forall p \in X\}$ es un ideal de $k[x_1, \ldots, x_n]$ que llamaremos **ideal de** X.

Propiedades:

1. Si $X \subseteq Y \Rightarrow I(Y) \subseteq I(X)$
2. $I(\emptyset) = k[x_1, \ldots, x_n]$, si k infinito, $I(\mathbb{A}^n) =< 0 >= 0$

3. $I(\{(a_1,\ldots,a_n)\}) =< x_1 - a_1,\ldots,x_n - a_n >$
4. $S \subseteq IV(S), \forall S \subseteq k[x]; \forall X \subseteq \mathbb{A}^n, X \subseteq VI(X)$
5. $IVI(X) = I(X); VIV(S) = V(S)$
6. $I(X)$ es radical
7. $I(X \cup Y) = I(X) \cap I(Y)$

Demostración 2. $\boxed{1}$. *$X \subseteq Y$. Sea $f \in I(Y) \Leftrightarrow f(p) = 0, \forall p \in Y \Rightarrow f(p) = 0, \forall p \in X \Leftrightarrow f \in I(X)$* $\square$

$\boxed{3}$. *$S \subseteq IV(S), S \subseteq k[\vec{x}]$. Sea $f \in S$, hay que probar que $f(p) = 0, \forall p \in V(S) \Rightarrow$ se tiene.* $\square$

$\boxed{4}$. *$IVI(X) = I(X)$, por (3), tenemos $\boxed{\supseteq}$, hay que probar $\boxed{\subseteq}$. Sea $f \in IVI(X) \Rightarrow f(p) = 0, \forall p \in VI(X)(\supseteq X) \Rightarrow f \in I(X)$. (La otra igualdad es análoga).* $\square$

$\boxed{5}$. *$I(X) = \{f \in k[\vec{x}] : f(p) = 0, \forall p \in X\} \subseteq \sqrt{I(X)}$. Sea $f \in \sqrt{I(X)} \Rightarrow \exists m \geq 0$ tal que $f^m \in I(X) \Rightarrow f^m(p) = 0, \forall p \in X \Rightarrow f(p) = 0, \forall p \in X \equiv f \in I(X)$* $\square$

$\boxed{6}$. *$I(X \cup Y) = I(X) \cap I(Y)$. $(X \subseteq X \cup Y) \wedge (Y \subseteq X \cup Y) \Rightarrow (I(X \cup Y) \subseteq I(X)) \wedge (I(X \cup Y) \subseteq I(Y))$.*

Sea $f \in I(X) \cap I(Y) \Rightarrow f(p) = 0 \Rightarrow f(p) = 0 \forall p \in X \cup Y$.

Definición 1.3.2. Dado un ideal $I \subseteq A$, se llama **radical** de I al conjunto $\sqrt{I} := \{a \in A : \exists m \geq 0, a^m \in I\}$. Un ideal $J \subseteq A$ se llama radical si $J = \sqrt{J}$.

Ejercicio 1.16 $V = W \Leftrightarrow I(V) = I(W)$
Solución:
$\boxed{\Leftarrow}$ $I(V) = I(W) \Rightarrow V = VI(V) = VI(W) = W$
Ejercicio 1.17 Sea $V \subseteq \mathbb{A}^n$ conjunto algebraico, $p \notin V$.

1. Probar que existe un polinomio $F \in k[x_1,\ldots,x_n]$ tal que $F(Q) = 0, \forall Q \in V$ pero $F(p) = 1$.
2. Sean $P_1,\ldots,P_r \in \mathbb{A}^n$ distintos, $P_i \notin V$. Probar que existen $F_1,\ldots,F_r \in k[\vec{x}]$ tales que $F_i(P_j) = 0$ si $i \neq j$, y $F_i(P_i) = 1$.
3. $a_{ij} \in k, i \leq i, j \leq r$, hay que probar que existe $G_i \in I(V)$ tal que $G_i(P_J) = a_{ij}, \forall i, j$

Solución:

1. Sea $G \in I(V) - I(V \cup \{P\}) \Rightarrow G(Q) = 0, \forall Q \in V, G(p) = a \neq 0 \Rightarrow F = \frac{G}{a}$
2. Sea $W_i = V \cup P_1 \cup \cdots \cup P_{i-1} \cup P_{i+1} \cup \cdots \cup P_r$. $W_i \neq W_i \cup \{P_i\}$. $I(W_i) \neq I(W_i \cup \{P_i\}) \Rightarrow \exists F_i \in I(V)$ tal que $F_i(P_i) = 1, F_i(P_j) = 0, \forall j \neq i$.
3. Usando ayuda y apartado anterior.

Ejercicio 1.18 Sea $I \subseteq R$ ideal. Si $a^n \in I, b^m \in I$, hay que probar que $(a+b)^{n+m} \in I$.
<u>*Solución:*</u>
$\sum_{k=0}^{n+m} \binom{n+m}{k} a^k b^{n+m-k}$, se tiene $k \geq n \Rightarrow a^k \in I$ o bien $n+m-k \geq m \Rightarrow b^{m+n} \in I$.
$\sqrt{I}$ ideal. $0 \in \sqrt{I}$. Sean $a, b \in \sqrt{I} \Rightarrow a^n, b^m \in I$, por lo anterior $(a-b)^{n+m} \in I \Rightarrow a - b \in \sqrt{I}$.
$a \in A, b \in \sqrt{I} \Rightarrow a^n b^m \in I \Rightarrow ab \in \sqrt{I}$.
Todo ideal primo es radical. Sea J un ideal primo de A, $J \subseteq \sqrt{J}$. Sea $a \in \sqrt{J} \Rightarrow a^m \in J \Rightarrow a \in J \vee a^{m-1}$, y por inducción $a \in J$, luego J es radical.
Ejercicio 1.19 $I =< x^2+1 >\subseteq \mathbb{R}[x]$ es primo, luego radical. Pero, $I \neq I(X), \forall X \subseteq \mathbb{A}^1(\mathbb{R})$.
<u>*Solución:*</u>
$\frac{\mathbb{R}[x]}{<x^2+1>} \cong \mathbb{C}$ cuerpo $\Rightarrow I$ maximal $\Rightarrow I$ primo $\Rightarrow I$ radical.
Reducción al absurdo: Si $I = I(X) \Rightarrow V(I) = VI(X) \Rightarrow IV(I) = I(X), I(\emptyset) = \mathbb{R}[x] \neq I$.
Cuestiones a entregar 1.20,1.21

1.4. El teorema de la base de Hilbert

Sea k cuerpo.

Teorema 1.4.1. *Sea $V \subseteq \mathbb{A}^n$ conjunto algebraico cualquiera, entonces V es intersección finita de hipersuperficies.*

Demostración 3. *Sabemos que $V = V(I)$ para algún ideal $I \subseteq k[x_1, \ldots, x_n]$. En particular,* $\boxed{\textit{si todo ideal de } k[x_1,\ldots,x_n] \textit{ es finitamente generado}}$ *$\Rightarrow I =< f_1, \ldots, f_r >$ para cierto $f_i \in k[\vec{x}] \Rightarrow V = V(I) = V(f_1, \ldots, f_n) = V(f_1) \cap V(f_2) \cap \cdots \cap V(f_r)$.* □

Nota 1.4.1. *El contenido recuadrado en la demostración se demostrará más adelante.*

Definición 1.4.1. Un anillo A se dice **Noetheriano** si todo ideal de A es finitamente generado.

Ejemplos: cuerpos, dominios de ideales principales.

Teorema 1.4.2. ***de la base de Hilbert***. *Si R es un anillo Noetheriano $\Rightarrow R[x]$ es Noetheriano.*

Demostración 4. *Sea $I \subseteq R[x]$ ideal cualquiera, hay que probar que I es finitamente generado. Sea $J = \{$(coeficientes líderes) $cl(f) : f \in I\}$, sean $cl(f), cl(g), f, g \in I$. Sea $m = deg(f), n = deg(g), n \leq m, h = x^{m-n}g - f \in I$ y $J \ni cl(h) = cl(g) - cl(f)$.*
$J \subseteq R$ ideal $\Rightarrow_{(R \text{ Noether })} J =< a_1, \ldots, a_r >$, $a_i = cl(f_i)$ para cierto $f_i \in I$.
Sea $N = max\{deg(f_i)\}$, para cada $m \leq N$, definimos $J_m = \{cl(f) : f \in I \wedge deg(f) \geq m\}$, entonces cada ideal $J_m \subseteq R \Rightarrow \exists\{f_{mj}\}_{j \in \Lambda_m}$ finitos que genera a J_m. $f_{mj} \subset I$.

$I' = < f_1, \ldots, f_r, f_{mj}, m \geq N, j \in \Lambda_m >$. Veamos que $I = I'$. (Λ_m es finito)

$I' \subseteq I$ es obvio porque $f_i, f_{mj} \in I$. La contención contraria se demuestra por reducción al absurdo. $I' \subset I \Rightarrow$ sea $g \in I \backslash I'$ de grado mínimo.

Si $deg(g) > N$, como $cl(g) \in J \Rightarrow cl(g) = \sum_{i=1}^{r} b_i a_i, b_i \in \mathbb{R}$, entonces puedo tomar $g - \sum h_i f_i$ con $cl(h_i) = b_i$.
$deg(h_i) = \underbrace{deg(g)}_{>N} - \underbrace{deg(f_i)}_{\leq N}$. $deg(g - \sum h_i f_i) < deg(g) \Rightarrow_{(g \text{ de grado mínimo}} g - \sum h_i f_i \in I' \Rightarrow g \in I' \rightarrow\leftarrow$.

Luego $I = I'$ es finitamente generado. $\square$

Corolario 1.4.1. *R Noetheriano $\Rightarrow R[x_1, \ldots, x_n]$ Noetheriano.*

Demostración 5. *Por inducción usando el teorema.*
$\boxed{n = 1}$ *Se aplica el teorema.*
$\boxed{n \rightarrow n+1}$ $R[x_1, \ldots, x_n] \cong P[x_1, \ldots, x_{n-1}][x_n]$

Corolario 1.4.2. *Si k es cuerpo $\Rightarrow k[x_1, \ldots, x_n]$ es Noetheriano.*

Corolario 1.4.3. *$\mathbb{Z}[x_1, \ldots, x_n]$ es Noetheriano*

Cuestión a entregar el viernes 7 de octubre: Problema 1.22.

1.5. Componentes irreducibles de un conjunto algebraico

Sea $V \subseteq \mathbb{A}^n$ un conjunto algebraico.

Definición 1.5.1. Se dice que V es **irreducible** si no existen V_1, V_2 conjuntos algebraicos tales que $V = V_1 \cup V_2$, $V_i \subset V$ con $V_i \neq V$.

Proposición 1.5.1. *$V \subseteq \mathbb{A}^n$ es irreducible $\Leftrightarrow I(V) \subset k[x_1, \ldots, x_n]$ es ideal primo.*

Demostración 6. $\boxed{\Rightarrow}$

Lo demostramos por reducción al absurdo. Supongamos que $I(V)$ no es primo. Entonces, $\exists f, g \in k[\vec{x}]$ tal que $fg \in I(V)$ pero $f \notin I(V) \wedge g \notin I(V)$. $V \subseteq VI(V) \subseteq V(fg) = V(f) \cup V(g)$.

Como $V \subseteq V(f) \cup V(g) \Rightarrow V = V \cap (V(f) \cup V(g)) = [V \cap V(f)] \cup [V \cap V(g)]$, entonces como V es irreducible se tendrá que $V = V \cap V(f)$ o que $V = V \cap V(g)$, lo demostramos para el primer caso, el otro es análogo.

Si $V = V \cap V(f) \Rightarrow V \subseteq V(f) \Rightarrow f \ni IV(f) \subseteq I(V) \rightarrow\leftarrow$

$\boxed{\Leftarrow}$

$\exists V_1, V_2 \subset V, V = V_1 \cup V_2 \Rightarrow I(V) \subset_{estrictamente} I(V_1) \cap I(V_2) \wedge I(V) = I(V_1 \cup V_2) = I(V_1) \cap I(V_2) \rightarrow\leftarrow$. $\square$

Lema 1.5.1. *Sea A un anillo Noetheriano y sea $S \neq \emptyset$ un conjunto de ideales de A. Entonces existe un ideal en S que es maximal en S respecto del orden parcial dado por la inclusión.*

Demostración 7. *Se demuestra por reducción al absurdo. Supongamos que $S \neq \emptyset$ no tiene elementos maximales como $f \neq \emptyset \Rightarrow \exists I_1 \in S$ ideal que no es maximal en $S \Rightarrow \exists I_2 \in S, I_1 \subset I_2$. Por inducción se construye una cadena de ideales infinita en S:*

$$I_1 \subset I_2 \subset \dots$$

$\Rightarrow I = \cup_{n \geq 1} I_n \subseteq A$ ideal (Noetheriano) $\Rightarrow I$ es finitamente generado.
Cada $a_i \in I = \cup I_n \Rightarrow \exists m_i \geq 1$ tal que $a_i \in I_{m_i} \Rightarrow a_1, \dots, a_r \in I_m$ si $m = max(m_i)$.
$I_m \subseteq I_{m+1} \cdots \subseteq I$, $I_m =< a_1, \dots, a_r >= I = I_{m+1} = \cdots \rightarrow\leftarrow$

Corolario 1.5.1. *Todo conjunto $S \neq \emptyset$ de conjuntos algebraicos de $\mathbb{A}^n$ posee un elemento minimal respecto de la inclusión.*

Demostración 8. *Basta aplicar el lema anterior a $S' = \{I(V) : V \in S\}$.*

Teorema 1.5.1. *Todo conjunto algebraico $V \subseteq \mathbb{A}^n$ se puede escribir de forma única como $V = V_1 \cup \cdots \cup V_r$, con V_i irreducible, $V_i \not\subset V_j, \forall i \neq j$*

Demostración 9. *Se demuestra por reducción al absurdo. Supongamos que existen conjuntos algebraicos que no pueden escribirse de esta forma.*

$S = \{V \subseteq \mathbb{A}^n$ conjunto algebraico que no se escriben de esta forma$\} \neq \emptyset \Rightarrow \exists V \in S$ minimal respecto de la inclusión.

En particular, $V \in S \Rightarrow V$ reducible $\Rightarrow \exists V_1, V_2 \subset V$ tales que $V = V_1 \cup V_2$, como V es minimal en S, eso significa que $V_1, V_2 \notin S \Rightarrow$

$$V1 = W_1 \cup \cdots \cup W_r \text{ con } W_i \not\subset W_j, \forall i \neq j$$

$$V = W'_1 \cup \cdots \cup W'_s \text{ con } W'_i \not\subset W'_j, \forall i \neq j$$

Entonces, $V = W_1 \cup \cdots \cup W_r \cup W'_1 \cup \cdots \cup W'_s$ Si algún $W_i \subset W'_{j(i)}$ o bien $w'_j \subseteq W_{i(j)}$ se quita el menor. $V \notin S \rightarrow\leftarrow$.

Falta probar la unicidad: $V = W_1 \cup \cdots \cup W_r = W'_1 \cup \cdots \cup W'_s$, cada W_i, W'_j irreducible, y tales que $W_i \not\subset W_j, W'_i \not\subset W'_j, \forall i \neq j$. Entonces, como $W_i \subseteq V = \cup_j W'_j \Rightarrow W_i = \cup_{j=1}^s (W_i \cap W'_j)$, W_i es irreducible, entonces existe $j(i)$ tal que $W_i = W_i \cap W'_{j(i)} \Rightarrow W_i \subseteq W'_{j(i)} \subseteq W_{i(j(i))}$. Análogamente, $W'_j \subseteq W_{i(j)} \Rightarrow W_i = W_j j(i)'$, con lo cual, $r = s$ y $W_i = W'_{j(i)}, i = 1, \dots r$.

Problema 1.23: *Dar un ejemplo de colección S de ideales en un anillo Noetheriano tal que ningún elemento maximal sea ideal maximal.*

Solución:

Sea el anillo $A = k[x, y]$ con k cuerpo. $S = \{< x^m >, m \geq 1\}, < x^{m+1} >\subset< x^m >$, pero estrictamente contenido. Entonces, el único elemento maximal de S es $< x >$ que no es ideal maximal ya que $< x >\subset< x, y >\subset A$.

Problema 1.24: *Todo ideal propio J de un anillo Noetheriano está contenido en un ideal.*
Solución:
Basta aplicar el lema 1.5.1 a $S = \{I \subset A \text{ ideal } : J \subseteq I\}$.

Cuestión a entregar el viernes 7 de octubre: Escribir la sección 1.6: Subconjuntos algebraicos en el plano.

1.6. Subconjuntos algebraicos en el plano

Encontremos todos los subconjuntos algebraicos del espacio afín $\mathbb{A}^2(k)$. Por el *teorema 1.5.1* es suficiente encontrar los conjuntos algebraicos irreducibles.

Proposición 1.6.1. *Sean F y G polinomios, ambos en $k[X,Y]$ sin factores comunes. Entonces $V(F,G) = V(F) \cap V(G)$ es un conjunto finito de puntos.*

Demostración 10. *F y G no tienen factores comunes en $k[X][Y]$, así que tampoco tienen factores comunes en $k(X)[Y]$ (Son isomorfos). $k(X)[Y]$ es un dominio de ideales principales (de hecho, fue uno de los ejemplos que dimos en clase), $gcd(F,G) = 1$ en $k(X)[Y]$, así que existen $R, S \in k(X)[Y]$ tales que $RF + SG = 1$ por el teorema de Bézout.*

Sea $D \in k[X]$ un polinomio no nulo tal que $DR = A$, $DS = B \in k[X,Y]$. Entonces $AF + BG = D$.

Si $(a,b) \in V(F,G)$, entonces $D(a) = 0$. Pero, D tiene una cantidad finita de raíces. Esto prueba que solo una cantidad finita de coordenadas de X pertenecen a $V(F,G)$. Análogamente para las coordenadas Y se aplica el mismo razonamiento en $k(Y)[X]$, y eso implica que solo puede haber una cantidad finita de puntos. □

Corolario 1.6.1. *Si F es un polinomio irreducible en $k[X,Y]$ tal que $V(F)$ es infinito, entonces $I(V(F)) = F$, y $V(F)$ es irreducible.*

Demostración 11. *Si $G \in I(V(F))$, F divide a G,ésto es claro pues tienen raíces comunes pero F es irreducible. Por lo tanto, se tiene que $G \in < F >$ entonces $V(F,G)$ es infinito ($V(F) \subset V(G) \Rightarrow V(F,G) = V(F) \Rightarrow$ infinito.Por la proposición anterior tienen factores comunes, y $I(V(F)) \subset < F >$. Además, $< F > \subset I(V(F))$, y por la proposición 1.5.1, $V(F)$ es irreducible. ($< F >$ es ideal primo al ser F irreducible).* □

Nota 1.6.1. *La proposición 1.5.1 dice que $V(F)$ es irreducible si y sólo si $< F >$ es ideal primo.*

Corolario 1.6.2. *Supongamos que k es infinito. Entonces los subconjuntos algebraicos irreducibles de $\mathbb{A}^2(k)$ son: $\mathbb{A}^2(k), \emptyset$, puntos, y curvas planas irreducibles $V(F)$, donde F es un polinomio irreducible y $V(F)$ es infinito.*

Demostración 12. *Sea V un conjunto algebraico irreducible en $\mathbb{A}^2(k)$. Tenemos los siguientes casos:*

- *V es finito.*
- $I(V) = 0$
- *Si $\exists F$ polinomio no constante. Como $I(V)$ es primo (pues V es irreducible), podemos considerar que F es irreducible, pues en caso contrario podríamos tomar el factor irreducible de F que pertenezca a $I(V)$. $I(V) =< F >$ pues si $G \in I(V)$ y $G \notin< F >$, entonces $V \subset V(F, G)$ que es finito por la proposición 1.6.1.*

□

Corolario 1.6.3. *Sea k algebraicamente cerrado, F un polinomio no constante en $k[X, Y]$. Sea $F = F_1^{n_1} \cdots F_r^{n_r}$ la descomposición de F en factores irreducibles. Entonces $V(F) = V(F_1) \cup \cdots \cup V(F_r)$ es la descomposición de $V(F)$ en componentes irreducibles, y $I(V(F)) =< F_1 \cdots F_r >$.*

Demostración 13. *$F_i \not| F_j, \forall i \neq j$, así que no hay relaciones de inclusión entre $V(F_i)$. Se tiene que $I(\cup_i V(F_i)) = \cap_i I(V(F_i)) = \cap_i < F_i >$. Como cualquier polinomio es divisible por cada F_i, también lo será por $F_1 \cdots F_r$, $\cap_i < F_i >=< F_1 \cdots F_r >$. Notar que $V(F_i)$ es infinito para cada i, ya que k es algebraicamente cerrado como se demostró en el problema 1.14.* □

1.6.1. Problemas

Problema 1.30: Sea $k = \mathbb{R}$.

1. Prueba que $I(V(X^2 + Y^2 + 1)) =< 1 >$.
   <u>*Solución:*</u>

   $X^2 + Y^2 + 1$ es irreducible en $\mathbb{R}$, y además no existe $(a, b) \in \mathbb{A}^2(\mathbb{R})$ tale que $a^2 + y^2 + 1 = 0 \Rightarrow V(X^2 + Y^2 + 1) = \emptyset$. Y se tiene $I(\emptyset) =< 1 >= k[X, Y]$

2. Prueba que cada subconjunto algebraico de $\mathbb{A}^2(\mathbb{R})$ es igual a $V(F)$ para algún $F \in \mathbb{R}[X, Y]$.
   <u>*Solución:*</u>

   Los subconjuntos algebraicos irreducibles de $\mathbb{A}^2(\mathbb{R})$ por el *corolario 1.6.2* son: $\mathbb{A}^2, \emptyset$ y curvas planas. Las curvas planas cumplen lo que nos piden. $\mathbb{A}^2 = V(\emptyset)$, y $\emptyset = V(k[X, Y])$.

   Los subconjuntos algebraicos no irreducibles se pueden descomponer en unión de subconjuntos algebraicos irreducibles, y por el *corolario 1.6.3*, el producto de los polinomios que generan dichos subconjuntos irreducibles cumple lo pedido.

Nota 1.6.2. *$V(F) = V(F_1, \ldots, F_r), F = \sum F_i^2$ si $F = 0 \Rightarrow$ todos los $F_i = 0$.*

Problema 1.31:

1. Encuentra los componentes irreducibles de $V(Y^2 - XY - X^2Y + X^3)$ en $\mathbb{A}^2(\mathbb{R})$, y también en $\mathbb{A}^2(\mathbb{C})$.
   <u>*Solución:*</u>
   $Y^2 - XY - X^2Y + X^3 = (X-Y)(X^2-Y)$ en $\mathbb{A}^2(\mathbb{R}) \Rightarrow V(Y^2 - XY - X^2Y + X^3) = V(X-Y) \cup V(X^2-Y)$.
   $Y^2 - XY - X^2Y + X^3 = (X-Y)(X+\sqrt{Y})(X-\sqrt{Y})$ en $\mathbb{A}^2(\mathbb{C}) \Rightarrow V(Y^2 - XY - X^2Y + X^3) = V(X-Y) \cup V(X-\sqrt{Y}) \cup V(X+\sqrt{Y})$.

2. Haz lo mismo para $V(Y^2 - X(X^2-1))$, y para $V(X^3 + X - X^2Y - Y)$.
   - En $\mathbb{A}^2(\mathbb{R})$:
     - $Y^2 - X(X^2-1) = (Y+\sqrt{X^3+X})(Y-\sqrt{X^3+X}) \Rightarrow V(Y^2 - X(X^2-1)) = V(Y+\sqrt{X^3+X}) \cup V(Y-\sqrt{X^3+X})$
     - $X^3 + X - X^2Y - Y = (X^2+1)(X-Y) \Rightarrow V(X^3 + X - X^2Y - Y) = V(X^2+1) \cup V(X-Y)$
   - En $\mathbb{A}^2(\mathbb{C})$:
     - $X^3 + X - X^2Y - Y = (X-i)(X+i)(X-Y) \Rightarrow V(X^3 + X - X^2Y - Y) = V(X-i) \cup V(X+i) \cup V(X-Y)$

1.7. El teorema de los ceros (Nullstellensatz) de Hilbert

Sea k cuerpo algebraicamente cerrado (ejemplo $\mathbb{C}$).

Teorema 1.7.1. ***debil de los ceros.*** *Sea $I \subset k[\vec{x}]$ ideal propio, entonces $V(I) \neq \emptyset$.*

Demostración 14. *Existe $m \subset k[\vec{x}]$ ideal maximal tal que $I \subseteq m \Rightarrow V(m) \subseteq V(I)$. Basta probar que $V(m) \neq \emptyset$. Como m es maximal, se tiene que $\frac{k[\vec{x}]}{m}$ es un cuerpo.*

$k \subseteq L = \frac{k[\vec{x}]}{m}$ extensión de cuerpos. $\boxed{\text{Supongamos que } k = L}$ $\Rightarrow \forall i = 1, \ldots, n$, se tiene que $\bar{x}_i = \bar{a}_i$ en $L, a \in k$.

$\Rightarrow \underbrace{< x_1 - a_1, \ldots, x_n - a_n >}_{maximal} \subseteq m \Rightarrow m =< x_1 - a_1, \ldots, x_n - a_n > \Rightarrow V(m) = V(x_1 - a_1, \ldots, x_n - a_n) = \{(a_1, \ldots, a_n)\} \neq \emptyset$

Nota 1.7.1. *La suposición en el recuadro queda pendiente de probar.*

Teorema 1.7.2. ***de los ceros.*** *k algebraicamente cerrado, $I \subseteq k[x_1, \ldots, x_n]$ ideal $\Rightarrow IV(I) = \sqrt{I}$*

Demostración 15.
- *$\sqrt{I} \subseteq I(V(I))$ (ejercicio)*

$\boxed{\subseteq}$ Sea $f \in IV(I)$, hay que probar que $\exists m \geq 1$ tal que $f^m \in I$. Si $I =< f_1, \ldots, f_r >$, f se anula en todo punto que sea cero común de $f_1, \ldots, f_r$. Si consideramos otro ideal $J =<$

$f_1, \dots, f_r, f \underbrace{x_{n+1} - 1}_{h} > \subseteq k[x_1, \dots, x_n, x_{n+1}]$ *ideal.* $\forall P \in V(f_1, \dots, f_r) \Rightarrow f(P) = 0 \Rightarrow h(P) = -1 \neq 0$. *Por tanto* $V(I) = \emptyset \Rightarrow_{\text{teo. ceros débil}} J = k[x_1, \dots, x_{n+1}] \Leftrightarrow 1 \in J$.

$\Rightarrow 1 = g_1 f_1 + \dots + g_r f_r + g_{r+1}(f x_{n+1} - 1)$. *Podemos hacer el cambio* $x_{n+1} = \frac{1}{y}$, *y así obtenemos :*

$$1 = \sum_j g_j(x_1, \dots, x_n, \frac{1}{y}) f_j(x) + g_{r+1}(x_1, \dots, x_n, \frac{1}{y})(f\frac{1}{y} - 1)$$

Tomo $N \geq 1$ *suficientemente grande tal que* $y^{N-1} g_j(x_1, \dots, x_n, \frac{1}{y}) \in k[x_1, \dots, x_n, y]$

$$y^N = \sum_j g'_j(\vec{x}, y) f_j(\vec{x}) + g'_{r+1}(\vec{x}, y)(f - y)$$

$\Rightarrow f^N = \sum g'_j(\vec{x}, f(\vec{x})) f(x) \in I$ □

Corolario 1.7.1. *Existe una correspondencia biyectiva entre ideales radicales de* $k[\vec{x}]$ *y conjuntos algebraicos de* $\mathbb{A}^n$.

$$\{I \subseteq k[\vec{x}] \text{ ideal } : I = \sqrt{I}\} \leftrightarrow \{v \subseteq \mathbb{A}^n \text{ conjunto algebraico }\}$$
$$I \rightarrow_V V(I)$$
$$I(X) \leftarrow_I X$$

Demostración 16. *X conjunto algebraico* $\Rightarrow VI(X) = X$ *(propiedad ya vista)* $\Rightarrow V \circ I = id$.
I ideal radical $\Rightarrow IV(I) = \sqrt{I} = I \Rightarrow I \circ V = id$.
Entonces se deduce que I y V son biyectivas y una es la inversa de la otra.

Corolario 1.7.2. *Esta correspondencia lleva ideales primos en conjuntos algebraicos irreducibles y viceversa.*

Corolario 1.7.3. *Esta correspondencia lleva ideales maximales en puntos y viceversa.*

Corolario 1.7.4. *Esta correspondencia lleva ideales principales en hiperespacios y viceversa.*

Corolario 1.7.5. *Si V es una hipersuperficie, i.e,* $V = V(f)$ *para* $f \in k[\vec{x}] \backslash k$ *y sea* $f = \prod_{j=1}^r f_j^{m_j}$ *su descomposición en factores irreducibles entonces* $V(f) = V(f_1) \cup \dots \cup V(f_r)$ *es su descomposición en componentes irreducibles.*

Corolario 1.7.6. *Sea k algebraicamente cerrado e* $I \subseteq k[x_1, \dots, x_n]$ *ideal, encontes* $V(J)$ *finito si y solo si* $\frac{k[x_1, \dots, x_n]}{I}$ *es un k- espacio vectorial de dimensión finita. Además, en tal caso,* $\#V(J) \leq dim_k(\frac{k[\vec{x}]}{I})$

Demostración 17. *$\#V(I) \leq dim_k(\frac{k[\vec{x}]}{I})$. Sean $P_1,\ldots,P_r \in V(J)$ distintos $\Rightarrow \exists f_1,\ldots,f_r \in k[\vec{x}$ tales que*

$$f_j(P_j) = \begin{cases} 1 \text{ si } i = j \\ 0 \text{ si } i \neq j \end{cases}$$

Veamos que $\bar{f}_1,\ldots,\bar{f}_r \in \frac{k[\vec{x}]}{J}$ son k- linealmente independientes.

Supongamos que $\exists \lambda_1,\ldots,\lambda_r \in k$ tales que $\sum \lambda_i \bar{f}_i = 0$ en $\frac{k\vec{x}}{J} \Rightarrow \sum \lambda_i f_i \in J \Rightarrow \sum_{i=1}^{r} \lambda_i f_i(P_j) = 0, \forall j = 1,\ldots,r$, luego $\bar{f}_1,\ldots,\bar{f}_r$, linealmente independientes en $\frac{k[\vec{x}]}{J} \Rightarrow dim\frac{k[\vec{x}]}{J} \geq r$.

Si $V(J)$ es infinito $\Rightarrow dim\frac{k[\vec{x}]}{J} \geq r, \forall r \in \mathbb{N} \Rightarrow dim\frac{k[\vec{x}]}{J} = \infty$.

Si $V(J)$ tiene exactamente r puntos $\Rightarrow dim\frac{k[\vec{x}]}{J} < \infty \Rightarrow V(J)$ finito.

Supongamos ahora que $V(J) = \{P_1,\ldots,P_r\}$ es finito, $P_i = (a_{1i},\ldots,a_{ni})$.

Sea $f_j = \prod_{i=1}^{r}(x_j - a_{ji}) \Rightarrow f_j(P_i) = 0, \forall i,j, i = 1,\ldots,r, j = 1,\ldots,n \Rightarrow f_j \in IV(J) =_{k\ alg.cerrado} \sqrt{J} \Rightarrow \exists m_j \geq 0$ tal que $k[x_j] \ni f_j^m \in J$, $f_j^{m_j} = x_j^{l_j} +$ términos de menor grado en $x_j \Rightarrow \bar{x}_j^{l_j}=$ clase de suma finita de términos de $k[x_j]$ y grado $\leq l_j - 1 \Rightarrow \{\prod_{j=1}^{n} x_j^{\bar{k}_j} : 0 \leq k_j \leq l_j, \forall j = 1,\ldots,n\}$ sistema generador del k-espacio vectorial $\frac{k[\vec{x}]}{J} \Rightarrow \frac{k[\vec{x}]}{J}$ tiene dimensión finita.

Ejercicio 1.12: $C \subseteq \mathbb{A}^2$ curva, $L \not\subset C, L \subseteq \mathbb{A}^2$ recta. $C = V(F), f \in k[x,y]$. Hay que probar que $C \cap L$ conjunto finito de cardinal $\leq n = deg(f)$.

<u>*Solución:*</u>

$L = V(y - (ax+b)) \Rightarrow L \cap C = V(y - (ax+b), f(x,y)) \Rightarrow 0 \neq_{L \not\subset C} f(x, ax+b) \in k[x]$, tiene grado $\leq m \Rightarrow$ existen a lo más m posibles valores de x tal que $f(x) = 0$.

Ejercicio 1.13: (a) $\{(x,y) \in \mathbb{A}^2(\mathbb{R}) : y = sin(x)\}$, hay que probar que no es un conjunto algebraico.

<u>*Solución:*</u>

Si fuera algebraico, entonces sería $C = V(S), S \subseteq k[x_1 \ldots, x_n]$. $C \cap V(y) = \{(\pi k, 0) : k \in \mathbb{Z}\} \subseteq L = V(y)$ recta afin. Dicho conjunto es infinito y distinto del total, entonces no es conjunto algebraico, y la intersección de algebraicos debería ser algebraica.

Ejercicio 1.25: Probar que $V(y - x^2) \subseteq \mathbb{A}^2(\mathbb{C})$ es irreducible e $IV(y - x^2) =< y - x^2 >$.

<u>*Solución:*</u>

Nota 1.7.2. *Sabemos que dado un conjunto algebraico, era irreducible si y solo si $I(V)$ era ideal primo.*

Basta ver que $IV(y - x^2) =< y - x^2 >$ y que es primo. $V(y - x^2) = \{(t, t^2) : t \in \mathbb{C}\}$. $\supseteq$ la tenemos ya, probamos la contraria. Sea $f \in IV(y - x^2) \Rightarrow f(t, t^2) = 0, \forall t \in \mathbb{C}$. Por otro lado, $f = q(x,y)(y - x^2) + r(x) \Rightarrow r(t) = 0, \forall t \in \mathbb{C} \Rightarrow r = 0 \Rightarrow f = q(y - x^2) \in < y - x^2 >$, y se tiene la igualdad.

Falta ver que es ideal primo, $\frac{k[x,y]}{<y-x^2>} \cong k[x]$, $k[x] \to \frac{k[x,y]}{<y-x^2>}$ es isomorfismo. La sobreyectividad se tiene porque $f(\bar{x}, y) = f(\bar{x}, x^2), f(x, x^2) = g(x) \in k[x]$.

1.8. Módulos; Condiciones de finitud

Sea $\mathbb{A}$ anillo conmutativo y con elemento unidad.

Definición 1.8.1. Un **A-módulo** M es un grupo abeliano $(M, +)$ dotada de una operación $\cdot : A \times M \to M$, que verifica:

1. $(a + b)m = am + bm, \forall a, b \in A, \forall m \in M$.
2. $a(m + m') = am + am', \forall a \in A, \forall m, m' \in M$.
3. $a(bm) = (ab)m$.
4. $1_A m = m, \forall m \in M$.

Ejemplo:

- Si $A = \mathbb{Z}$, entonces un $\mathbb{Z}-$módulo es lo mismo que un grupo abeliano $a \in \mathbb{Z}, m \in M, am = m + \cdots + m$.
- $A = k$ cuerpo, entonces un $k-$módulo es lo mismo que un k-espacio vectorial.
- Un anillo A también es un $A-$módulo.

Definición 1.8.2. Si M es un $A-$módulo, un subgrupo abeliano $N \subset M$ es un **submódulo** si $am \in N, \forall a \in A, \forall m \in N$.

Ejemplo:
Los submódulos de un anillo A son sus ideales.

Definición 1.8.3. Sea M un $A-$ módulo, diremos que un submódulo $N \subset M$ es **finitamente generado** ($f.g.$) si $\exists m_1, \ldots, m_r \in N$ tales que $N = Am_1 + \cdots + Am_r$ (es decir, $\forall n \in N, \exists a_1, \ldots, a_r \in A$ tales que $n = \sum_{i=1}^{r} a_i m_i$).

Sea $R \subset S$ una extensión de anillos, se pueden considerar ciertas condiciones de finitud de R sobre S. (S es un $R-$módulo).

- S se dice $R-$ **álgebra** $f.g.$ si $\exists v_1, \ldots, v_n \in S$ tales que $S = R[v_1, \ldots, v_n]$. Es decir, $\exists \varphi : R[x_1, \ldots, x_n] \to S$ sobreyectivo (morfismo), $f(x_1, \ldots, x_n) \to f(v_1, \ldots, v_n)$. Por el primer teorema de isomorfía $\frac{R[x_1, \ldots, x_n]}{ker\varphi} \cong Im\varphi = S$. (No es lo mismo que un anillo de polinomios).
- ¿Es S un $R-$ módulo finitamente generado?

- Si $R = k \subset S = L$ es extensión de cuerpos y L es una $k-$álgebra $f.g.$, se dice que L es una extensión finitamente generada de k.

$$v_i \in L, L = k[v_1, \dots, v_r] = k(v_1, \dots, v_r)$$

- Una extensión $k \subset L$ de cuerpos se dice que es $f.g.$ si $\exists v_1, \dots, v_m \in L$ tales que $L = k(v_1, \dots, v_n)$.

Ejemplos:

- A anillo, $S = A[x]$; $A \subset S$, y podemos ver que tomando φ la propia inclusión se tiene que S es una $A-$álgebra $f.g.$.
  No es un $A-$módulo finitamente generado. Reducción al absurdo: $\exists f_1, \dots, f_r \in A[x]$ tal que $S = Af_1 + \cdots + Af_r, \forall f \in S \Rightarrow deg(f) \leq max\{deg(f_i)\} \rightarrow\leftarrow$.
- $k \subseteq k(x)$ es una extensión de cuerpos f.g. pero no es una $k-$álgebra finitamente generada, aunque sí es un k-álgebra por el hecho de contener el anillo k.
- Un ejemplo de k-álgebra finitamente generada es $\frac{R[x_1,\dots,x_n]}{I} = R[\bar{x}_1, \dots, \bar{x}_n]$

Cuestión a entregar viernes 14 Octubre: Ejercicios 1.44, 1.45.

Sea $R \subset S$ una extensión de anillos tal que S sea $R-$ módulo finitamente generado. ¿Es S una $R-$álgebra finitamente generada?

Sí, $S = \sum Rv_i \subset R[v_1, \dots, v_n] \subseteq S \Rightarrow S = R[v_1, \dots, v_n]$.
$R[v_1, \dots, v_n] = \{\sum r_\alpha v_1^{\alpha_1} \cdots v_n^{\alpha_n} : r_\alpha \in R\}$.

1.9. Elementos enteros y dependencia entera

Sea $R \subset S$ extensión de anillos.

Definición 1.9.1. Un elemento $s \in S$ es **entero** sobre R si $\exists 0 \neq f \in R[x]$ mónico tal que $f(s) = 0$.

Nota 1.9.1. *Si R y S son cuerpos, un elemento $s \in S$ entero sobre R es lo mismo que un elemento algebraico sobre R.*

Ejemplo:
Sea $r \in \mathbb{Q}$ tal que r sea entero sobre $\mathbb{Z}$.
$r = \frac{a}{b}, gcd(a, b) = 1$.
$r^n + a_{n-1}r^{n-1} + \dots, a_0 = 0$ en $\mathbb{Q}, a_i \in \mathbb{Z} \Rightarrow a^n = -a_{n-1}ba^{n-1} + \dots, a_0b^n = 0 = b[a_{n-1}a^{n-1} + \cdots + a_0b^{n-1}] \Rightarrow b|a^n \Rightarrow b = 1 \vee b = -1$.
Luego, $r = \frac{a}{b} \in \mathbb{Z}$.

Proposición 1.9.1. *$R \subset S$ anillos, $v \in S$. Son equivalentes:*

1. *v entero sobre R.*

2. *$R[v]$ es un $R-$módulo finitamente generado.*

3. *$\exists R' \subseteq S$ subanillo de S tal que $R[v] \subseteq R'$ y R' es un $R-$módulo finitamente generado.*

Demostración 18. $\boxed{1 \Rightarrow 2}$ $\exists n \geq 1, v^n + a_{n-1}v^{n-1} + \cdots + a_0 = 0, a_i \in R \Rightarrow v^m = -\sum_{i=0}^{n-1} a_i v^i$.

$R[v] = \{\sum_{m=0}^{k} a_m v^m : a_i \in R, i = 0, \ldots, k\} = Rv^0 + Rv + \cdots + Rv^{n-1}$ *$R-$módulo.*

$\boxed{2 \Rightarrow 3}$ $R' = R[v]$.

$\boxed{3 \Rightarrow 1}$ $R[v] \subset R' \subset S$, *$R'$ es un $R-$módulo finitamente generado.* $R' = Rv_1 + \cdots + Rv_n$, $v_i \in R'$.

$v \in R' \Rightarrow v \cdot v_i \in R' \Rightarrow \sum_{j=1}^{n} \delta_{ij} v_j = v \cdot v_i = \sum_{j=1}^{n} a_{ij} v_j \Rightarrow \sum_{j=1}^{n} (\delta_{ij} v \cdot v - a_{ij}) v_j = 0 \Rightarrow (Iv - A)(v_1 \cdots v_n)' = 0 \Rightarrow \underbrace{det(IV - A)}_{\in R[v] \subset R}(v_1 \cdots v_n)' = \vec{0} \Rightarrow_{I_{R'} = \sum b_i v_i} det(IV - A) = 0 \Rightarrow$ *v es entero sobre R*

Nota 1.9.2. *δ es la delta que vale 1 o 0, kronickle.*

Ejercicios viernes 14 Oct: 1.38,1.44,1.45,1.49,1.50.
$R \subset S, v \in S$, v entero sobre $R \Leftrightarrow R[v]$ es $R-$módulo finitamente generado.
Ejemplo:
$R = \mathbb{Z} \subset S = R, v = \sqrt{2}$ es entero sobre $\mathbb{Z}$, ya que $v^2 - 2 = 0$, de lo que se deduce que $\mathbb{Z}[\sqrt{2}]$ es $\mathbb{Z}-$módulo, grupo abeliano, finitamente generado. En concreto $\mathbb{Z}[\sqrt{2}] = \mathbb{Z} \cdot 1 + \mathbb{Z}\sqrt{2}$.

Corolario 1.9.1. *Sea $R \subset S$ extensión de anillos $\Rightarrow$ el conjunto R' de los elementos de S que son enteros sobre R es un subanillo de S que contiene a R.*

Demostración 19. *Todo elemento $r \in R$ es entero sobre R ya que $f = x - r \in R[x]$ es mónico no nulo y $f(r) = 0 \Rightarrow R \subseteq R' \subseteq S$.*

Hay que probar que $\forall a, b \in R'$ se cumple $a - b \in R'$, $ab \in R'$.

Como a es entero sobre $R \Rightarrow R[a]$ es un $R-$módulo finitamente generado, y análogo para b. Si es b es entero sobre R, entonces b es entero para $R[a] \Rightarrow R[a, b]$ es $R[a]-$módulo finitamente generado $\Rightarrow R[a, b]$ es $R-$módulo finitamente generado.

$a - b, ab \in R[a, b] \Rightarrow R[a - b], R[ab] \subset R[a, b] \subset S \Rightarrow a - b, ab$ enteros sobre R, es decir, $a - b, ab \in R'$.

1.10. Extensiones de cuerpos

Sea $k \subset L$ extensión de cuerpos finitamente generado, $L = k(v_1, \ldots, v_n)$, para ciertos $v_i \in L$.

Si $n = 1$, $L = k(v) = \{\frac{f(v)}{g(v)} : f, g \in k[x], g(v) \neq 0\}$.

Sea $\varphi : k[x] \to L, f(x) \to f(v)$ morfismo de anillos. Por el primer teorema de isomorfia se tiene $\frac{k[x]}{ker\varphi} \cong k[v] \subseteq L$.

Caso 1: $ker\varphi = 0 \Rightarrow k[x] \cong k[v] \neq k(v) = L$, porque $k[x] \neq k(x)$. Entonces L no es una $k-$álgebra finitamente generada, y tampoco es $k-$espacio vectorial de dimensión finita, y v no es algebraico sobre k.

Caso 2: $ker\varphi \neq 0 \Rightarrow ker\varphi =< f >$, omo $k[v]$ es dominio de integridad, es un ideal primo $\Rightarrow f \in k[x]$ irreducible $\Rightarrow ker\varphi =< f >$ maximal (Por un ejercicio anterior). Entonces, $\frac{k[x]}{ker\varphi}$ es un cuerpo, luego $k[v]$ también es un cuerpo $\Rightarrow k(v) = k[v] = L$ es $k-$álgebra finitamente generada.

Por otro lado, como $f \in ker\varphi \Rightarrow f(v) = 0$, como k es un cuerpo, puedo suponer $f \neq 0$ mónico, y se tiene que v es entero (algebraico) sobre k.

Nota 1.10.1. *$k(v)$ cuerpo de fracciones, menor cuerpo que lo contiene.*

Entonces por la proposición anterior, se tiene que L es $k-$módulo finitamente generado, es decir, $k-$espacio vectorial de dimensión finita.

De manera más general tenemos lo siguiente:

Proposición 1.10.1. ***(Zariski)*** *Sea $k \subset L$ extensión de cuerpos y L es una $k-$álgebra finitamente generada $\Rightarrow$ L es un $k-$espacio vectorial de dimensión finita y, por tanto, L es algebraico sobre k. ($k \subset L$ extensión algebraica).*

Demostración 20. *Se demuestra por inducción, $L = k[v_1, \ldots, v_n]$ $k-$álgebra finitamente generada por $v_1, \ldots, v_n \in L$.*

Por el razonamiento anterior lo tenemos probado para $n = 1$, lo suponemos cierto para $n - 1$, y lo probamos para n.

$L = k[v_1, \ldots, v_n] = k'[v_2, \ldots, v_n]$ con $k' = k(v_1)$. Como L es $k'-$ álgebra finitamente generada, se tiene que L es un $k'-$espacio vectorial de dimensión finita.

Por otro lado, si consideramos $k' = k(v_1])$, $k \subset k'$ es una extensión. Si v_1 es algebraico sobre k, entonces k' es $k-$ espacio vectorial de dimensión finita.

Por ambas cosas, se tendrá que L es $k-$espacio vectorial de dimensión finita.

Supongamos que v_1 no es algebraico sobre k. Entonces, $k' = k(v_1) \cong k(x)$.

Como $(k'(v_i) \subset)L$ es $k'-$espacio vectorial de dimensión finita. Entonces, $v_2, \ldots, v_n$ son enteros, y por tanto, algebraicos sobre $k' = k(v_1) \Rightarrow (v_i)^{n_i} + a_{in}(v_1)^{n_i-1} + \cdots = 0, a_{ij} \in k' = k(v) \Rightarrow \exists b \in k[v_1]$ tal que $ba_{ij} \in k[v_1] \Rightarrow (bv_i)^{n_i} + a_{in_i}b(bv_i)^{n_i-1} + \cdots = 0 \Rightarrow bv_i$ enteros sobre $k[v_1]$.

$\Rightarrow k[v_1, bv_2, \ldots, bv_n] = k'[bv_2, \ldots, bv_n]$ es $k[v_1]-$módulo finitamente generado. $\forall f \in k[v_1, \ldots, v_n] = L, \exists N \geq 0$ tal que $b^N f \in k[v_1, bv_2, \ldots, bv_n]$ esentero sobre $k[v_1]$. Como en particular, $k(v_1) \subset L$, entonces $\forall g \in k(v_1) \cong k(x), \exists N \geq 0$ tal que $b^N g$ es entero sobre $k[v_1] \cong k[x]$, por dos ejercicios propuestos (1.44,1.45), ésto no es posible. $\square$

Demostración del teorema débil de los ceros de Hilbert:

$I \subset m \subseteq k[\vec{x}]$, m ideal maximal $\Rightarrow v(m) \subseteq V(I)$. Hay que probar que $v(m) \neq \emptyset$.

Se considera la extensión $k \subseteq L = \frac{k[x_1,\ldots,x_n]}{m}$.

Si $k = L \Rightarrow \forall i = 1, \ldots, n, \bar{x}_i = \bar{a}_i, a_i \in k \Rightarrow x_i - a_i \in m \Rightarrow < x_1 - a_1, \ldots, x_n - a_n > \subseteq m$, es un ideal maximal pues $\frac{k[\vec{x}]}{<x_1-a_1,\ldots,x_n-a_n>} \cong k \Rightarrow m = < x_1 - a_1, \ldots, x_n - a_n > \Rightarrow v(m) = \{(a_1, \ldots, a_n)\} \neq \emptyset$.

Hay que probar que $k = L$, $k \subseteq L = \frac{k[x_1,\ldots,x_n]}{m}$ cuerpo y k-álgebra finitamente generada $\xrightarrow{\text{Prop}} k \subseteq L$ extensión algebraica. k algebraicamente cerrado $\Rightarrow L = k$.

Problema 1.25: (b) $V(y^4 - x^2, y^4 - x^2y^2 + xy^2 - x^3)$

<u>*Solución:*</u>

$(y^2 - x)(y^2 + x)$.

Si $x = y^2 \rightarrow y^4 - y^6 + y^4 - y^6 = 0 \rightarrow (y = 0 \rightarrow x = 0 \rightarrow (0,0))$ ó $(y = + - 1 \rightarrow x = 1(1, + - 1))$.

$x = -y^2$ no añade ninguna condición.

$W = V(x + y^2) \cup \{(1,1)\}\{(1,-1)\}$ tres componentes irreducibles.

Problema 1.26: *Probar que $F = y^2 + x^2(x-1)^2$ es irreducible en $\mathbb{R}[x,y]$, pero $V(F)$ es reducible.*

<u>*Solución:*</u>

$F = (y - ix(x-1))(y + ix(x-1))$ factorización en $\mathbb{C}[x,y]$, es un dominio de factorización única, y vemos que eso implica que es irreducible en $\mathbb{R}[x,y]$ pues multiplicando por escalares, mantenemos algún elemento complejo.

$y^2 + x^2(x-1)^2 = 0 \Rightarrow y = 0 \wedge [x = 0 \vee x = 1] \Rightarrow V(F) = \{(0,0), (1,0)\}$.

Problema 1.27: *Sean $V, W \subseteq \mathbb{A}^n$ conjuntos algebraicos, $V \subseteq W$. Probar que cada componente irreducible de V está contenida en una componente irreducible de W.*

<u>*Solución:*</u>

$V_i \subseteq W \Rightarrow V_i = (V_i \cap W_i) \cup \cdots \cup (V_i \cap W_r) \Rightarrow V_i = V_i \cap W_i \vee V_i = \cup_{j=2}^{r}(V_i \cap W_j) \Rightarrow \exists j | v_i = W_j \cap V_i \Rightarrow V_i \subseteq W_j$.

Problema 1.28: Si $V = V_1 \cup \cdots \cup V_r$ es la descomposición de V en conjuntos algebraicos irreducibles hay que probar que $V_i \not\subset \cup_{j \neq i} V_j$.

<u>*Solución:*</u>

Reducción al absurdo: Si $V_i \subseteq \cup_{j \neq i} V_j \Rightarrow \exists j \neq i | V_i \subseteq V_j \rightarrow\leftarrow$.

Problema 1.29: k infinito $\Rightarrow \mathbb{A}^n(k)$ irreducible.

<u>*Solución:*</u>

$I(\mathbb{A}^n) = \{F \in k[\vec{x}] | F(a_1, \ldots, a_n) = 0\}$ pero por un problema $F = 0 \Rightarrow = < 0 >$ que es primo, y se tiene que $\mathbb{A}^n$ irreducible.

Problema 1.32:

<u>*Solución:*</u> $I = < x^2 + 1 > \subset R[x], V(I) = \emptyset$.

$J =< x^2(x-1)^2 + y^2 >\subseteq \mathbb{R}[x,y]$ primo, $V(J) = \{(0,0)\} \cup \{(1,0)\}$ reducible.

Problema 1.33: *(a) Descomponer $V(x^2+y^2-1, x^2-z^2-1) \subseteq \mathbb{A}^3(\mathbb{C})$.*

<u>*Solución:*</u>

(a) $f - g = (y-iz)(y+iz) \Rightarrow W = V(y+iz, x^2-z^2-1) \cup V(y-iz, x^2-z^2-1)$. Para ver que es irreducible, como estamos en un cuerpo algebraicamente cerrado, basta ver que $IV(\cdot) = \sqrt{< y+iz, x^2-z^2-1 >}$.

$\frac{\mathbb{C}[x,y,z]}{<y+iz,x^2-z^2-1>} \sim \frac{\mathbb{C}[x,z]}{<x^2-z^2-1>}$ ddi. Lo prueba el ejercicio siguiente.

Problema 1.34: *Sea R un dominio de factorización única:*

1. *Probar que un polinomio mónico de grado 2 o 3 en $R[X]$ es irreducible si y sólo si no tiene raices en R.*

2. El polinomio $x^2 - a$ en $R[x]$ es irreducible $\Leftrightarrow a = b^2$ para algún $b \in R$.

<u>*Solución:*</u>

1. $f \in R[x], deg(f) = 2 \vee deg(f) = 3, f$ mónico. f reducible $\Rightarrow f = (cx+d)g$ con g de grado 1 o 2. $\Rightarrow$ el coeficiente lider de g b, $cb = 1 \Rightarrow c$ unidad en $R \Rightarrow x = c^{-1}d \in R$ y es raíz de f.

   f tiene raíz $a \in R \Rightarrow f(a) = 0, f = q(x-a) + r \Rightarrow r = 0 \Rightarrow f = q(x-a)$ y por lo tanto, es reducible.

2. $\exists b \in R$ tal que $b^2 - a = 0$

Problema 1.37: Sea k un cuerpo, $F \in k[x]$ polinomio de grado $n > 0$. Hay que probar que $\{\bar{1}, \ldots, \bar{X}^{n-1}\}$ base de $\frac{k[\vec{x}]}{<F>}$.

<u>*Solución:*</u>

Puedo suponer F mónico ya que $< F >=< cF >, \forall c \in k$.

$\bar{F} = \bar{0}$ en $A \Rightarrow \bar{X}^n = \bar{X}^n = -a_{n-1}x^{n-\bar{1}} - \cdots - a_0$ k espacio vectorial generado por B.

Por inducción, todas las potencias de $\bar{X}$ se pueden expresar de esa manera.

Veamos que son linealmente independientes: Supongo $\exists \lambda_i \in k$ tal que $\sum_{i=0}^{n-1} \lambda_i \bar{x}^i = \bar{0}$ en $A \Rightarrow \sum_{i=0}^{n-1} \lambda_i x^i \in< F >\Rightarrow \sum_{i=0}^{n-1} \lambda_i x^i = FQ \rightarrow\leftarrow\Rightarrow \lambda_i = 0, \forall i$.

Capítulo 2

Variedades afines

Suponemos que k es un cuerpo algebraicamente cerrado.

Definición 2.0.1. Si $V \subseteq \mathbb{A}^n$ es un conjunto algebraico irreducible, diremos que V es una **Variedad (afín)**.

2.1. Anillo de coordenadas de una variedad

Definición 2.1.1. Se llama **anillo de coordenadas** de V a $\Gamma(V) := \frac{k[x_1,\ldots,x_n]}{I(V)}$ es un dominio de integridad.

Sea $F(V,k) = \{f : V \to k : f \text{ función } \} \supseteq k$ (funciones constantes).
$(F(V,k), +, \cdot)$ es un anillo.

$$f, g : V \to k$$
$$f + g : V \to k$$
$$(f+g)(P) = f(P) + g(P)$$
$$fg : V \to k$$

Definición 2.1.2. $f \in F(V,k)$ se llama función polinómica (o regular) si existe un polinomio $F \in k[x_1,\ldots,x_n]$ tal que $f(P) = F(P), \forall P \in V$.

Nota 2.1.1. *El conjunto de las funciones polinómicas de V en k es un subanillo sobre k.*

$$\varphi : k[x_1,\ldots,x_n] \to F(V,k)$$
$$f \to (\varphi(f) : V \to k)$$

$$P \to f(P)$$

$Im\varphi =$ Funciones polinómicas de V en k.

Veamos cual es el núcleo de φ. $\varphi(f) = 0 \Leftrightarrow f(P) = 0, \forall p \in V \Leftrightarrow f \in I(V) \Rightarrow ker\varphi = I(V)$.

Por el primer teorema de isomorfía tenemos:

$$\Gamma(V) = \frac{k[\vec{x}]}{I(V)} \cong Im\varphi$$

Ejercicio propuesto 21 de Octubre: 2.2

Ejemplo:

1. $V = \mathbb{A}^n$, $I(V) = 0, \Gamma(V) = k[x_1, \ldots, x_n]$.
2. $V = \{P\}, I(V) =< x_1 - a_1, \ldots, x_n - a_n >\Rightarrow \Gamma(V) \cong k$.
3. $V = V(y - (ax + c)) \subseteq \mathbb{A}^2, \Gamma(V) = \frac{K[x,y]}{<y-(ax+c)>} \cong k[x] = \Gamma(\mathbb{A}^n)$

Problema 2.3: Sea $W \subseteq V$ subvariedad de la variedad V y sea $I_V(W) \subseteq \Gamma(V)$ ideal correspondiente a W, es decir, $I_V(W) = \{f \in \Gamma(V) : f(P) = 0, \forall p \in W\}$.

(a) Probar que toda función polinómica en V se restringe a una en W.

(b) Probar que la aplicación $\Gamma(V) \to \Gamma(W)$ es un morfismo sobreyectivo con núcleo $I_V(W)$.

Solución:

(a) f función pol. en $V \Rightarrow \exists F \in k[x_1, \ldots, x_n], f(P) = F(P), \forall P \in V \Rightarrow f_{|W}$ es función polinómica de V en k.

(b) Se restringe como en el apartado anterior. $f \to f_{|w}$.

Hay que ver que es sobreyectivo. Sea $g \in \Gamma(W) \Rightarrow \exists G \in k[x_1, \ldots, x_n]$ tal que $g(P) = G(P), \forall P \in V$.

Sea $\tilde{g} : W \to k, \tilde{g}(P) \to G(P), \forall P \in W$, es claro que $\tilde{g}_{|V} = g : V \to k$. Luego, el morfismo ψ es sobreyectivo.

$ker\psi = \{f \in \Gamma(V) : f_{|W} = 0\} = I_V(W) \xrightarrow{1^{o}\text{ Teo iso}} \frac{\Gamma(V)}{I_V(W)} \cong \Gamma(W)$.

Problema 2.4: $V \subseteq \mathbb{A}^n$ variedad. Son equivalentes:

1. V es un punto.
2. $\Gamma(V) = k$
3. $dim_k\Gamma(V) < \infty$

Solución:

$\boxed{1 \Rightarrow 2}$ Obvio, las únicas funciones de $\{P\} \to k$ son las constantes.

$\boxed{2 \Rightarrow 3}$ $\Gamma(V) = k \Rightarrow dim_k\Gamma(V) = 1 < \infty$.

$\boxed{3 \Rightarrow 1}$ $dim_k(\Gamma(V)) < \infty, dim_k(\Gamma(V)) = dim_k\frac{k[\vec{x}]}{I(V)}$, $V = V(I(V))$, y ya teniamos por una prop. anterior que : $\#V(I) \leq dim_k\frac{K[\vec{x}]}{I}$.

2.2. Aplicaciones polinómicas entre variedades

Definición 2.2.1. Sean $V \subseteq \mathbb{A}^n$, $W \subseteq \mathbb{A}^m$ variedades afines, una aplicación $\varphi : V \to W$ se llama **aplicación polinómica** si existen $f_1, \ldots, f_n \in \Gamma(V)$ tales que $\varphi(P) = (f_1(P), \ldots, f_m(P))$.

Dada una aplicación $\varphi : V \to W$ polinómica, φ induce el morfismo:

$$\tilde{\varphi} : \Gamma(W) \to \Gamma(V), f \to \tilde{\varphi}(f) = f \circ \varphi$$

Es morfismo de K-álgebra, es decir, es un morfismo de anillos y $\tilde{\varphi}(\lambda) = \lambda, \forall \lambda \in k$.

Proposición 2.2.1. *Sean $V \subseteq \mathbb{A}^n, W \subseteq \mathbb{A}^n$ variedades. Existe una correspondencia biyectiva entre las aplicaciones polinómicas $\varphi : V \to W$ y los morfismos de k-álgebras $\alpha : \Gamma(W) \to \Gamma(V)$.*

$$\varphi : V \to W \text{ polinómica } \longrightarrow \underbrace{\tilde{\varphi} : \Gamma(W) \to \Gamma(V)}_{\tilde{\varphi}(\bar{f}) = f \bar{\circ} \varphi}$$

$$\alpha : \Gamma(W) \to \Gamma(V)$$

$$\varphi_\alpha : V \to W$$

Demostración 21. *Hay que probar que $\tilde{\varphi}$ bien definida y morfismo de k-álgebra dada $\varphi : V \to W$, y que φ está bien definida y aplicación polinómica dada $\alpha : \Gamma(W) \to \Gamma(V)$.*

$\tilde{\varphi}_\alpha = \alpha$.

$\varphi_{\tilde{\varphi}} = \varphi$.

Para ver que $\tilde{\varphi}$ está bien definida basta probar que si $f \in k[y_1, \ldots, y_m], f \in I(W)$, entonces $f \circ \varphi \in I(V)$.

$f(P') = 0, \forall P' \in W, \forall P \in V, \varphi(P) \in W \Rightarrow f(\varphi(P)) = 0, \forall p \in V \Rightarrow f \circ \varphi \in I(V)$.

Por otro lado, sea $\alpha : \Gamma(W) \to \Gamma(V)$ morfismo de k-álgebras, $\bar{y}_i \to \alpha(\bar{y}_i) = \bar{g}_i$, $g_i \in k[x_1, \ldots, x_n]$.

$\varphi_\alpha : V \to W$, $P \to (g_1(P), \ldots, g_m(P)) \in \mathbb{A}^m$, *hay que probar que* $\varphi_\alpha(P) \in W$.

Sea $\psi_\alpha : \mathbb{A}^n \to \mathbb{A}^m$ sí está bien definido. Hay que probar que $\psi_\alpha(P) \in W, \forall P \in V$.

α bien definida, entonces $\forall f \in I(W), \bar{f} = \bar{0}$ en $\Gamma(W) \Rightarrow \overline{f(g_1(x), \ldots, g_m(x))} = \alpha(\bar{f}) = \bar{0}$ en $\Gamma(V)$, $\Rightarrow f(g_1(x), \ldots, g_m(x)) \in I(V) \Rightarrow \forall P \in V, f(g_1(P), \ldots, g_m(P)) = 0, \forall f \in I(W)$. Luego $\psi_\alpha(P) \in VI(W) = W$, que es lo que queríamos probar.

$\psi_\alpha(V) \subseteq W \Rightarrow \varphi_\alpha = \psi_{\alpha|V} : V \to W$ *bien definida y polinómica.*

$\tilde{\varphi}_\alpha = \alpha$:

$$y_i \bar{\circ} \varphi_\alpha = \bar{g}_i$$

LLevan los representantes de las clases al mismo sitio. Las composiciones se tienen de manera trivial.

Nota 2.2.1. *$\varphi : V \to W, \psi : W \to T$ aplicación polinómica. Entonces $\psi \circ \varphi : V \to T, \psi \tilde{\circ} \varphi = \tilde{\varphi} \circ \tilde{\psi}$.*

Demostración: Sea $\bar{f} \in \Gamma(T), \psi \circ \tilde{\varphi}(\bar{f}) = f \circ (\psi \circ \varphi) = (f \circ \psi) \circ \varphi = \tilde{\varphi}(f \circ \psi) = (\tilde{\varphi} \circ \tilde{\psi})(f)$.

$\varphi_{\beta \circ \alpha} = \varphi_\alpha \circ \varphi_\beta$.

Corolario 2.2.1. $V \sim W \Leftrightarrow \Gamma(V) \sim \Gamma(W)$

Demostración 22. $\varphi : V \to W, \psi : W \to V$ *aplicaciones polinómicas tales que* $\varphi \circ \psi = id_W, id_V = \psi \circ \varphi \Rightarrow \varphi \tilde{\circ} \psi = id_{\Gamma(W)}, \psi \tilde{\circ} \varphi = id_{\Gamma(V)}$. $\tilde{\varphi}$: *isometría entre* $\Gamma(W)$ *y* $\Gamma(V)$.

Ejercicio 1.47: $R \subset S$ (No necesariamente dominio de integridad). R-álgebra finitamente generada. Probar que S es R-módulo finitamente generado si y sólo si S entero sobre R.

Solución:

$\boxed{\Rightarrow}$ $S = R[a_1, \ldots, a_n]$ es R-módulo finitamente generado. $R[a_i] \subseteq S, \exists R' = S, R[a_i] \subseteq R'$ y R' es R-módulo finitamente generado. Por lo tanto por la implicación $\boxed{3 \Rightarrow 1}$, se tiene a_i entero sobre R, $\forall i$, R entero sobre R', entonces $R[a_1, \ldots, a_n]$ entero sobre R por ser el menor anillo que contiene a R y a todos los a_i, $i = 1, \ldots, n$.

$\boxed{\Leftarrow}$ S entero sobre $R \subseteq R[a_1] \subseteq \cdots \subseteq S_{n-1} = R[a_1, \ldots, a_{n-1}] = R[a_1, \ldots, a_{n-2}][a_{n-1}] \subseteq R[a_1, \ldots, a_n] = S = S_{n-1}[a_n]$.

S entero sobre $S_{n-1} \Rightarrow S_n = S$ es S_m-módulo finitamente generado.

$S_i = S_{i-1}[a_i]$ entero sobre $S_{i-1} \Rightarrow S_i$ es S_{i-1}-mód f.g. Por la transitividad de módulo finitamente generado demostrado en el apartado a del *ejercicio 1.45* tenemos S es R-módulo finitamente generado.

2.3. Funciones racionales y anillos locales

Sea $V \subseteq \mathbb{A}^n$ variedad con $V \neq \emptyset$. Entonces $\Gamma(V)$ es un dominio de integridad.

Definición 2.3.1. $k(V) := Q(\Gamma(V)) = \{\frac{f}{g} : f, g \in \Gamma(V), g \neq 0\}$ se llama el **cuerpo de las funciones racionales en** V. A sus elementos los llamaremos **funciones racionales en** V.

Definición 2.3.2. Se dice que una función racional $f \in k(V)$ está definida en $P \in V$ si $\exists g, h \in \Gamma(V)$ tales que $f = \frac{g}{h}$ y $h(P) \neq 0$.

Ejemplo:

$W = V(xy - zt) \subseteq \mathbb{A}^4(\mathbb{C}), f = \frac{x}{z}, P = (0, 2, 0, 1)$. Veamos que f sí está definido en P.

$xy - zt = 0$ en $\Gamma(V) = \frac{k[x,y,z,t]}{<xy-zt>}$.

En $k(V), f = \frac{x}{z} = \frac{t}{y}, y(P) = 2, t(P) = 1 \Rightarrow f$ está definida en P y $f(P) = \frac{1}{2}$.

Definición 2.3.3. Sea $f \in k(V)$ definido en P se llama valor de f en P a $\frac{g(P)}{h(P)}$ donde $f = \frac{g}{h}$ con $h(P) \neq 0, f, g \in \Gamma(V)$.

Nota 2.3.1. *El valor de f en un punto P en el que está definido está bien definido. Si $\frac{g}{h} = \frac{g'}{h'}$ en $k(V) \Leftrightarrow gh' = hg'$ en $\Gamma(V) \Rightarrow g(P')h'(P') = h(P')g'(P), \forall P' \in V \Rightarrow \frac{g(P)}{h(P)} = \frac{g'(P)}{h'(P)}$ si $h(P), h'(P) \neq 0$.*

Definición 2.3.4. Sea $f \in k(V), P \in V$ se dice que P es un **polo de** f si f no está definida en P.

Nota 2.3.2. *Si $f = \frac{g}{h} \in k(V), P \in V$ y $h(P) = 0 \wedge g(P) \neq 0 \Rightarrow P$ es polo de f.*

Demostración 23. *Reducción al absurdo: Si $\exists g', h' \in \Gamma(V)$ tales que $h'(P) \neq 0$ y $f = \frac{g'}{h'} = \frac{g}{h}$ en $k(V) \Rightarrow g'h = gh'$ en $\Gamma(V) \Rightarrow 0 = g'(P)h(P) = g(P)h'(P) \neq 0 \rightarrow\leftarrow$.* □

Ejemplo:
$f = \frac{x}{z} = \frac{t}{y}$ en $k(W), W = V(xy - zt), \forall P \in W \backslash V(z, y), f$ definida en P.
Sea $P \in V(z, y) \subseteq W$.
Si $P = (x_0, 0, 0, t_0)$, si $x_0 \neq 0$, por la observación P es polo de f.
Si $t_0 \neq 0$, por la observación P es polo de f.
El conjunto de los polos de f está contenido en $V(z, y)$, y contiene a todos los puntos cuya primera o última coordenada es cero, es decir, contiene a $V(x, y) \backslash \{(0, 0, 0, 0)\}$
¿ Es $(0, 0, 0, 0)$ un polo de f?
Sí, porque el conjunto de los polos es un conjunto algebraico W'. Lo vemos por reducción al absurdo: $W' = V(z, y) \backslash \{(0, 0, 0, 0)\} \Rightarrow V(z, y) = W' \cup \{(0, 0, 0, 0\}$, pero $V(z, y)$ es irreducible, entonces $W' = V(z, y)$, por lo tanto contiene al cero.

Proposición 2.3.1. *Sea $f \in k(V) \Rightarrow$ el conjunto de los polos de f es subconjunto algebraico.*

Demostración 24. *Sea $J_f = \{G \in k[x_1, \ldots, x_n] : \bar{G} \cdot f \in \Gamma(V)\}$, hay que ver que J_f es un ideal que contiene a $I(V)$.*

- $0 \in J_f$
- $G, G' \in J_f \Rightarrow \bar{G}f, \bar{G}'f \in \Gamma(V) \Rightarrow (G \bar{-} G')f \in \Gamma(V) \Rightarrow G - G' \in J_f$
- $G \subset J_f, F \in k[\vec{x}] \rightarrow GF \in J_f$.

$V(I_f) = \{P \in \mathbb{A}^n : G(P) = 0, \forall 0 \in k[x_1, \ldots, x_n], \bar{G}f \in \Gamma(V)\}$.
$I(V) \subseteq J_f \Rightarrow V(J_f) \subseteq VI(V) = V$.
f definido en $P \Leftrightarrow \exists g, h \in \Gamma(V), f = \frac{g}{h}, h(P) \neq 0 \Leftrightarrow \exists h \in \Gamma(V), hf \in \Gamma(V), h(P) \neq 0 \Leftrightarrow \exists H \in k[x_1, \ldots, x_n], \bar{H}f \in \Gamma(V)$ tal que $H(P) \neq 0 \Leftrightarrow P \notin V(J_f)$.
$V(J_f) \subseteq$ Polos de f.
Si P polo de $f \Rightarrow \nexists H$ tal que $\bar{H}f \in \Gamma(V)$. □

Definición 2.3.5. Sea $P \in V$, se define **el anillo local de** V **en** P como el conjunto :

$$O_P(V) := \{f \in k(V) : f \text{ está definido en } P\}$$

Nota 2.3.3. *$O_P(V)$ es anillo, $k \subseteq \Gamma(V) \subseteq O_p(V) \subseteq k(V)$.*

Comprobemos que es anillo:

1. *$1 \in O_p(V)$*
2. *$f, g \in O_p(V) \Rightarrow f = \frac{G}{H}, g = \frac{G}{H'}, F, G, H, H' \in \Gamma(V), H(P), H'(P) \neq 0$. $f - g \in (V)$ y $HH'(P) \neq 0 \Rightarrow f - g \in O_p(V)$.*
3. *Análogo para el producto.*

Definimos $m_P = \{f \in O_P(V) : f(P) = 0\} \subseteq O_p(V)$ es un ideal y además maximal. Si $f \notin m_P \Rightarrow f$ es una unidad. Se tiene que $f(P) \neq 0, f \in O_P(V), \exists g, h \in \Gamma(V), f = \frac{g}{h}, h(P) \neq 0 \Rightarrow g(P) \neq 0$. Entonces $\frac{h}{g} = f^{-1} \in O_p(V) \Rightarrow f$ es unidad en $\Gamma(V)$.

Además, m_P no contiene unidades. Se razona por reducción al absurdo, pues si no, $m_P = O_p$, y podríamos tomar $1 \in O_p, 1 \notin m_P$. Luego m_P es el conjunto de los elementos no unidades $m_P = \{f \in O_P(V) : f \text{ no unidades }\}$.

Proposición 2.3.2. *Si R es un anillo. Son equivalentes:*

1. *R tiene un único ideal maximal y éste contiene a todos los ideales propios.*
2. *El conjunto de los elementos de R que no son unidades es un ideal.*

Demostración 25. $\boxed{1 \Rightarrow 2}$ *Sea m ese ideal maximal. Si $a \in R$ es unidad, entonces $< a >= R \Rightarrow a \notin m$. Si $a \in R$ no es unidad $\Rightarrow < a > \neq R \Rightarrow < a > \subseteq m \Rightarrow a \in m \Rightarrow a \in m \Leftrightarrow a$ no unidad.*

$\boxed{2 \Rightarrow 1}$ *Sea $m = \{a \in R : a \text{ no es unidad }\}$ es ideal propio.*

Sea $J \subset R$ ideal propio $\Rightarrow J$ no contiene unidades $\Rightarrow J \subseteq m$. En particular, m es el único maximal. □

Si R verifica (1) (y, por tanto (2)) se dice que R es un anillo local.

Proposición 2.3.3. *$O_P(V)$ es un anillo local Noetheriano.*

Demostración 26. *Hay que probar que si $J \subseteq O_P(V)$ ideal $\Rightarrow J$ es finitamente generado.*

En primer lugar, vamos a probar la inclusión

$$i : \Gamma(V) \to O_P(V)$$

$J' = i^{-1}(J) = J \cap \Gamma(V)$ es un ideal de $\Gamma(V) = \frac{k[x_1, \ldots, x_n}{I(V)}$ es Noetheriano $\Rightarrow J'$ es un ideal finitamente generado, es decir, $\exists f_1, \ldots, f_r \in \Gamma(V)$ tales que $J' =< f_1, \ldots, f_r > \subseteq \Gamma(V)$.

Veamos que $J =< f_1, \ldots, f_r > \subseteq O_P(V)$. Sea $f \in J \Rightarrow \exists h \in \Gamma(V)$ tal que $fh \in \Gamma(V) \cap J = J', h(P) \neq 0$. Por lo tanto, $\exists h_1, \ldots, h_r \in \Gamma(V)$ tales que $fh = h_1 f_1 + \cdots + h_r f_r$ en $\Gamma(V)$. Entonces, $f = \underbrace{\frac{h_1}{h}}_{\in O_P(V)} f_1 + \cdots + \frac{h_r}{h} f_r \in < f_1, \ldots, f_r > \subseteq O_P(V)$. Luego, $J \subseteq < f_1, \ldots, f_r > \subseteq O_P(V) \Rightarrow_{(f_i \in J')} J =< f_1, \ldots, f_r >$

Problema 2.17: Sea $V = V(y^2 - x^2(x+1)) \subseteq \mathbb{A}^2, \bar{x}, \bar{y} \in \Gamma(V) = \frac{k[x,y]}{<y^2 - x^2(x+1)>}$ (Que es asi porque $I(V) = IV(\cdot) = \sqrt{(\cdot)} =< y^2 - x^2(x+1) >$). Sea $f = \frac{y}{x}$ encontrar los polos de f y de f^2.

<u>*Solución:*</u>

$P = (x_0, y_0) \in V, \bar{y}^2 = \bar{x}^2(x \bar{+} 1)$ en $\Gamma(V)$.

Si $x_0 \neq 0 \to x(P) \neq 0 \Rightarrow P$ no es polo.

En $k(V), \frac{\bar{y}}{\bar{x}} = \frac{\bar{x}((x\bar{+}1)}{\bar{y}}$.

Si $y_0 \neq 0 \to f$ definida en P. Luego f está definida en $V \backslash \{(0,0)\}$ ¿Está f definida en $(0,0)$? Por la siguiente proposición, tenemos: $f \in \Gamma(V) \Rightarrow f = \frac{y}{x} = \bar{h} \in \Gamma(V) \Rightarrow y = hx$ en $\Gamma(V) \Rightarrow y - hx \in I(V) =< y^2 - x^2(x+1) >\Rightarrow (y - hx) = g(y^2 - x^2(x+1))$ si $x = 0$, entonces $y = g(0, y)g^2 \to\leftarrow$.

Los de f^2:

$f^2 = \frac{y^2}{x^2} = x + 1 \in \Gamma(V)$, no tiene polos.

Proposición 2.3.4. $\cap_{P \in V} O_P(V) = \Gamma(V)$. *Es decir, las únicas funciones racionales en V definidas en todo punto de V son las funciones polinómicas.*

Demostración 27. $\boxed{\supseteq}$ *Es obvia.*

$\boxed{\subseteq}$ *Sea* $f \in \cap_{p \in V} O_P(V) \Rightarrow f$ *no tiene polos* $\Rightarrow V(J_f) = \emptyset \Rightarrow_{k \text{ al.cerr} \Rightarrow \text{ ceros débil}} J_f =< 1 >= k[x_1, \ldots, x_n] = \{G \in k[\vec{x}] : \bar{G}f \in \Gamma(V)\} \Rightarrow \bar{1}f = f \in \Gamma(V)$. □

Problema 2.18: Se considera $O_P(V)$, hay que probar que existe una correspondencia natural biyectiva entre los ideales primos de $O_P(V)$ y las subvariedades de V que pasan por P.

$$\{J \subseteq O_P(V) : J \text{ ideal primo } \} \leftrightarrow \{W \subseteq V \text{ subvariedades } : P \in W\}$$

<u>*Solución:*</u>

$J \to V(J) = \{P \in V : f(P) = 0, \forall f \in J\}$ es una subvariedad.

Y hay que probar que $W \to I(W) = \{f \in O_P(V) : f(Q) = 0 \, \forall Q \in W\}$.

$J \subseteq O_P(V)$ es un ideal primo $\Rightarrow i^{-1}(J) = J \cap \Gamma(V)$ ideal primo $\Rightarrow V(J) = V(J') \subseteq V$ subvariedad. $V(J) = V(J')$ por la prueba de que $O_P(V)$ es Noetheriano.

Por otro lado, como J ideal primo $\Rightarrow J \subset O_P(V)$ propio $\Rightarrow J \subseteq m_P \Rightarrow \{P\} = V(m_P) \subseteq V(J) \Rightarrow P \in V(I)$.

Si $W \subseteq V$ subvariedad, $P \in W \Leftrightarrow I(W) \subseteq I(P) = \{f \in O_P(V) : f(P) = 0\} = m_P$.

$I_V(W) = \{f \in \Gamma(V) : f(Q) = 0, \forall Q \in W\} \subseteq \Gamma(V)$ ideal primo. Hay que probar que $I'(W)$ es primo.

Tenemos que $I'(W) \cap \Gamma(V) = I_V(W)$ es primo. Sea entonces $\underbrace{f, g \in O_P(V)}_{h_1 f, h_2 g \in \Gamma(V), h_i \in \Gamma(V)}$ tales que $fg \in I'(W) \Rightarrow (h_1 f)(h_2 g) \in I'(W) \cap \Gamma(V) \Rightarrow_{\text{Primo}} h_1 f \in I'(W) \vee h_2 g \in I'(W) \Rightarrow f \in I'(W) \vee g \in I'(W)$, pues $\frac{1}{h_i} \in O_p(V)$, y podemos multiplicar por ellos.

Problema 2.21: Sea $\varphi : V \to W$ aplicación polinómica entre variedades afines. Supongamos que $P \in V, Q = \varphi(P) \in W$. Probar que existe un único $\psi : O_Q(W) \to O_P(V)$ tal que $\psi(f) = \tilde{\varphi}(f), \forall f \in \Gamma(W) \subseteq O_Q(W)$.

Solución:

$\psi(\frac{f}{1}) = \tilde{\varphi}(f) = f \circ \varphi$. Para que sea morfismo, $\psi(\frac{1}{1}) = 1$.

Sea $g \in \Gamma(W), g(Q) \neq 0, \frac{1}{g} \in O_P(W)$.

$$\frac{1}{1} = \psi(\frac{1}{1}) = \psi(\frac{g}{g}) = \psi(\frac{1}{g})\psi(\frac{g}{1}) \Rightarrow \psi(\frac{1}{g}) = \frac{1}{g \circ \varphi}$$

Por tanto, debe ser $\psi(\frac{f}{g}) = \frac{f \circ \varphi}{g \circ \varphi}, \forall \frac{f}{g} \in O_Q(W)$.

$\psi(h) = h \circ \varphi, \forall h \in O_Q(W)$, si existe debe estar así definido, pero hay que demostrar que está bien definido.

Hay que ver que tomando dos clases distintas se tiene que tenemos la misma imagen. Y también que es una aplicación de $O_Q(W)$ a $O_Q(V)$.

Si $\frac{f}{g} = \frac{f'}{g'}$ en $O_Q(W) \subseteq k(W) \Leftrightarrow fg' = gf'$ en $\Gamma(W) \Rightarrow \tilde{\varphi}(fg') = \tilde{\varphi}(gf') \Rightarrow (f \circ \varphi)(g' \circ \varphi) = (g \circ \varphi)(f' \circ \varphi) \Rightarrow \frac{f \circ \varphi}{g \circ \varphi} = \frac{f' \circ \varphi}{g' \circ \varphi}$ en $k(V)$, y como $\frac{f}{g} \in O_Q(W) \Rightarrow \exists f_1, g_1 \in \Gamma(W) / g_1(Q) \neq 0 \Rightarrow f_1 \circ \varphi, g_1 \circ \varphi \in \Gamma(V), (g_1 \circ \varphi)(P) = g_1(Q) \neq 0$.

Y tenemos que $\frac{f \circ \varphi}{g \circ \varphi} \in O_P(V)$.

Nota 2.3.4. *$\tilde{\varphi}$ no tiene por qué extenderse a un morfismo $k(W) \to k(V)$.*

Ejemplo: *$\varphi : \mathbb{A}^1 \to \mathbb{A}^2$, tal que $t \to (t^2, t^3)$. $Im\varphi = V(y^2 - x^3)$. $\tilde{\varphi} : \Gamma(\mathbb{A}^2) = k[x,y] \to \Gamma(\mathbb{A}^1) = k[t]$.*

$k(\mathbb{A}^2) = Q(\Gamma(\mathbb{A}^2)) = k(x,y) \ni \frac{1}{y^2 - x^3}$, $\nexists \psi : k(x,y) \to k(t)$ tal que $\psi_{|k[x,y]} = \tilde{\varphi}$. R.A. si $\exists \psi \Rightarrow \psi(\frac{f}{g}) = \frac{f \circ \varphi}{g \circ \varphi}$.

Para $g = y^2 - x^3$ tal que $g \circ \varphi = g(t^2, t^3) = 0$ en $k[t]$.

Nota 2.3.5. *$\tilde{\varphi} : O_Q(W) \to O_P(V), h \to h \circ \varphi$. $\tilde{\varphi}(m_Q(W)) \subseteq m_P(V)$.*

Sea $g \in m_Q(W)$, y hay que probar que $\tilde{\varphi}(g) \in m_P(V)$.

$\tilde{\varphi}(g)(P) = (g \circ \varphi)(P) = g(\varphi(P)) = 0$

Problema 2.22: $T : \mathbb{A}^n \to \mathbb{A}^n$, cambio de coordenadas es una afinidad, que es lo mismo que una aplicación polinómica biyectiva donde todos los polinomios tienen grado 1. La inversa de una afinidad es una afinidad. Hay que probar que $\tilde{T}$ es un isomorfismo.

Solución:

T isomorfismo $\Rightarrow \tilde{T}$ isomorfismo de $\Gamma(\mathbb{A}^n)$ y $\tilde{T}^{-1} = \widetilde{T^{-1}}$, y por el ejercicio anterior, inducen de manera única morfismos entre los anillos locales.

DIAGRAMA

Por la unicidad en el ejercicio anterior, se tiene que $\tilde{T}^{-1} \circ \tilde{T} = id_{O_Q(\mathbb{A}^n)}$.

Análogamente, $\tilde{T} \circ \widetilde{T^{-1}} = id_{O_P(\mathbb{A}^n)}$. Luego, $\tilde{T} : O_Q(\mathbb{A}^n) \cong O_P(\mathbb{A}^n)$.

2.4. Anillos de valoración discreta

Proposición 2.4.1. *Sea R un dominio de integridad que no sea cuerpo. Son equivalentes:*

1. *R es Noetheriano, local y con ideal maximal principal.*
2. $\exists t \in R$ *irreducible tal que* $\forall z \in R\backslash\{0\}, \exists! u$ *unidad,* $\exists! n \geq, z = ut^n$.

Demostración 28. $\boxed{1 \Rightarrow 2}$ *Sea* $m =< t >$ *el único ideal maximal de P. Veamos que t es irreducible.*

R.A. Si $t = rs$ *con s y r no unidades* $\Rightarrow < t >= m \subset < r > \neq R \rightarrow\leftarrow$.

(si $< t >=< r > \Rightarrow r = ts' = rss', s$ *unidad).*

Unicidad: Supongamos $t^n u = t^m v$, $u, v \in R$ *unidades,* $n, m \geq 0$. $\Rightarrow_{(Prop.\ canc.\ ddin \geq m)}$ $t^{n-m}u = v \Rightarrow t^{n-m} = vu^{-1}$ *es unidad* $\Rightarrow n = m$, *t irreducible, y por lo tanto no es unidad.*

Sea $z \in R, z \neq 0$*:*

1. *Si z es unidad* $\Rightarrow z = zt^0$.
2. *Si z no es unidad* $\Rightarrow < z > \subseteq m =< t >, z = tz_1, z_1 \in R$.

Reiterando el proceso construimos $z_i = tz_{i+1}$.

$$(z) \subseteq (z_1) \subseteq \cdots \subseteq (z_i) \subseteq \cdots$$

Esta cadena sería estrictamente creciente si ningún z_i *fuera unidad, y esto contradice a que R es Noetheriano.*

Por tanto $\exists n \geq 0$ *tal que* $< z_n >=< z_{n+1} > \Rightarrow z_{n+1} = vz_n$ *para algún* $v \in R \Rightarrow vt = 1 \Rightarrow t$ *unidad* $\rightarrow\leftarrow$.

Por tanto, $\exists n \geq 0$ *tal que* z_n *es unidad* $\Rightarrow z = tz1 = \cdots t^n z_n$ *unidad.*

$\boxed{2 \Rightarrow 1}$ $\exists t \in R$ *irreducible tal que* $\forall z \in R, z = ut^n, u$ *unidad,* $n \in \mathbb{N}$.

Sea $m =< t > \subseteq R$. *Veamos que* $m = \{z \in R : z \text{ no unidad }\}$ *(*$\Rightarrow$ *R local y* $m =< t >$ *su único ideal maximal).*

Sea $z \in R$, *si z unidad* $\Rightarrow z \notin m$ *(*$m \neq R$*).*

Si $z = ut^n$ *no es unidad* $\Rightarrow n \geq 1 \Rightarrow z = ut^n \in < t >= m$.

Veamos que R es DIP ($\Rightarrow$ *R Noetheriano).*

Sea $J \subseteq R$ *ideal y sea* $z = ut^n \in J$ *tal que n sea mínimo* $\Rightarrow J =< t^n > \Rightarrow$ *R es DIP.* □

Ejemplo:

- $$[x] = \{\sum_{m=0}^{\infty} a_m x^m : a_i \in k\}$$

  $a_0 + a_1 x + \cdots = f \in k[x]$ unidad $\Leftrightarrow a_0 \neq 0$. Entonces f no es unidad si $a_0 = 0$ $\Leftrightarrow f = xg, g \in k[X] \Leftrightarrow f \in < x >$.

$m =< x >= \{f \in k[x] : f$ no unidad $\}$ es el único maximal de $k[x]$ (anillos local).
Toda serie $f = a_n x^n + a_{n+1}x^{n+1} + \cdots = x^n(a_n + a_{n+1}x + \dots)$
Probemos:

$$a_0 + a_1 x + \cdots = f \in k[x] \text{ unidad } \Leftrightarrow a_0 \neq 0$$

Demostración 29. $g = b_0 + b_1 x + \cdots, fg = b_0 a_0 + (a_0 b_1 + b_0 a_1)x + \cdots \sum a_i b_j x^k + \cdots$.
$fg = 1 \Rightarrow a_0 \neq 0$ y $b_0 = a_0^{-1}, b_k = -\frac{1}{a_0}(\sum a_i b_j)$.

Definición 2.4.1. Un anillo R que sea dominio de integridad, no cuerpo y que cumple alguna de las dos propiedades anteriores, se llama **anillo de valoración discreta** (AVD). Un elemento $t \in R$ irreducible como en (2) se llama un **parámetro de uniformización** de R.

Definición 2.4.2. Sea $k = Q(R)$ el cuerpo de fracciones de R, podemos definir la siguiente **función orden**: $ord : k \to \mathbb{Z} \cup \{\infty\}$, que asocia a $f = ut^n \to n$, donde n se denomina el orden de f.

Problema 2.23: La función $ord : k \to \mathbb{Z} \sqcup \{\infty\}$ no depende del parámetro de uniformización.
Solución:
$m =< t >=< s >$, es decir, s y t dos parámetros de unif. $\Rightarrow s = vt$ con v unidad.
Sea $f \in k$ tal que $f = t^n u = s^m u'$ con u, u' unidades en $R \Rightarrow t^n u = v^m t^m u'$. Si $n \geq m \Rightarrow t^{n-m} = v^m u' u^{-1}$ unidad de $R \Rightarrow n = m$.
Problema 2.24a: Sea $V = \mathbb{A}^1, \Gamma(V) = k[x], K = k(v) = k(x)$. Probar que $O_a(V)$ es un anillo de valoración discreta con parámetro de uniformización $(x - a), a \in k$.
Solución:
$Q_a(V) = \{\frac{g}{h} = f \in k(x) : f$ definida en $a\}$. Vimos que $O_a(\mathbb{A}^1)$ es Noetheriano y anillo local con ideal maximal $m_a(\mathbb{A}^1) = \{f \in O_a(\mathbb{A}^1) : f(a) = 0\}$. $\frac{g}{h}(a) = \frac{g(a)}{h(a)} = 0 \Leftrightarrow g(a) = 0 \Leftrightarrow g \in < x - a > \subseteq k[x] = \Gamma(V)$.
Por tanto, $m_a(\mathbb{A}^1) =< x - a > \subseteq O_a(\mathbb{A}^1)$. Por lo tanto, es un parámetro de uniformización.
Problema 2.24b: Probar que $O_\infty := \{\frac{F}{G} : F, G \in k[x], G \neq 0, deg(G) \geq deg(F)\} \subseteq k(x)$.
Solución:
Unidades de O_∞ son de la forma $\frac{F}{G}$, $deg(F) = deg(G)$. Las no unidades son: $\{\frac{F}{G} : deg(G) > deg(F)\} =: m$. Si m es ideal $\Rightarrow O_\infty$ es local y m su único maximal.
$\frac{F_1}{G_1}, \frac{F_2}{G_2} \to \frac{F_1}{G_1} - \frac{F_2}{G_2} \in m$. Es facil ver que es un ideal.
Si $\frac{F}{G} \in O_\infty$ con $m = deg(F) \leq deg(G) = n \Rightarrow u = \frac{x^{n-m}F}{G}$ es unidad $\Rightarrow \frac{F}{G} = u\frac{1}{x^{n-m}} = u(\frac{1}{x})^{n-m}$, y $\frac{1}{x}$ es irreducible (En apuntes).

La unicidad se prueba fácilmente. Luego, O_∞ es anillo de valoración discreta con parámetro de uniformización $\frac{1}{x}$.

Problema 2.26: Sea R un dominio de valoración discreta (que en particular implica dominio de integridad), $k = Q(R)$, sea $m \subseteq R$ su ideal maximal.

1. Si $z \in k, z \notin R \Rightarrow z^{-1} \in m$.

2. Supongamos $R \subset S \subset K$, y S es también DVR. Supongamos que el ideal maximal $m' =< s >= Ss$ de S contiene a $m =< t >= Rt$. Probar que $S = R$.

Solución:

1. $z = ut^n, n \in \mathbb{Z}$. Si $n \geq 0 \Rightarrow z = ut^n \in R$, por lo tanto $n < 0$ si $z \notin R$, $n \leq -1 \Rightarrow z^{-1} = u^{-1}t^{-n} \in m$.

2. $t \in < s >$, con lo cual $t = sv$. $\forall z \in k, z?ut^m, m \in \mathbb{Z} \Rightarrow$ en particular $s = ut^m \Rightarrow t = ut^m v \Rightarrow m = 0$ y $t = uv$ unidad en $S \rightarrow\leftarrow$, o bien $m \geq 1 \Rightarrow 1 = ut^{m-1}v \Rightarrow m = 1, v$ unidad de R.

   $\Rightarrow t = sv \Rightarrow t$ irreducible en S y $< s >=< t >$, entonces $s = tv^{-1} \in R$.

   Sea z unidad de $S \subset K$ tal que $z \notin R$, y por (a) $z^{-1} \in m \subseteq m' \subset S \rightarrow\leftarrow$.

   Toda unidad de S está en R.

   $\forall z \in S, z = u's^m = u'(ut)^m = u'u^m t^m \in R$.

2.5. Formas

Sea R un dominio. Si $F \in R[X_1, \ldots, X_{n+1}]$ es una forma, definiremos $F_* \in R[X_1, \ldots, X_n]$ por $F_* = F(X_1, \ldots, X_n, 1)$. Recíprocamente, para todo polinomio $f \in R[X_1, \ldots, X_n]$ de grado d, que se puede escribir de la siguiente manera: $f = f_0 + f_1 + \cdots + f_d$, donde f_i es una forma de grado i, definiremos $f^* \in R[X_1, \ldots, X_{n+1}]$ por

$$f^* = X_{n+1}^d f_0 + X_{n+1}^{d-1} f_1 + \cdots + f_d = X_{n+1}^d f(X_1/X_{n+1}, \ldots, X_n/X_{n+1})$$

f^* es una forma de grado d.

Proposición 2.5.1. *Se tiene que:*

1. $(FG)_* = F_* G_*; (fg)^* = f^* g^*$.

2. *Si r es la mayor potencia de X_{n+1} que divide a F, entonces $X_{n+1}^r (F_*)^* = F$; $(f^*)_* = f$.*

3. $(F+G)_* = F_* + G_*; X_{n+1}^t (f+g)^* = X_{n+1}^r f^* + X_{n+1}^s g^*$*, donde $r = gr(g), s = gr(f)$, y $t = r + s - gr(f+g)$.*

Demostración 30. 1. *$F \in R[X_1, \dots, X_{n+1}], G \in R[X_1, \dots, X_{m+1}]$. Por lo tanto, $F = \sum_i^{n+1} \lambda_i X_i^d$, donde d es el grado de la forma, y $G = \sum_k^{m+1} \beta_k X_k^e$,donde e es el grado de la forma G, con $\lambda_i, \beta_k \in R$. Entonces tenemos $F_* = \sum_i^n \lambda_i X_i^d + \lambda_{n+1}$, y $G_* = \sum_k^m \beta_k X_k^e + \beta_{m+1}$. Finalmente, $(FG)_* = (\sum_{i,k} \lambda_i \beta_k X_i^d X_k^e)_* =$*

$\sum_{i,k} \lambda_i \beta_k X_i^d X_k^d + \lambda_{n+1}\beta_{m+1}$,pues la variable que se hace 1 es aquella que tiene como coeficiente los más altos en subíndice de cada una de las formas. Por otro lado, $F_* G_* = (\sum_i^n \lambda_i X_i^d + \lambda_{n+1})(\sum_k^m \beta_k X_k^e + \beta_{m+1}) = \sum_{i,k} \lambda_i \beta_k X_i^d X_k^e + \lambda_{n+1}\beta_{m+1}$, y tenemos la igualdad.

Ahora tenemos que probar que $(fg)^* = f^* g^*$. $f \in R[X_1, \dots, X_n], g \in R[X_1, \dots, X_m]$, f y g se pueden escribir de la siguiente forma: $f = f_0 + \cdots + f_d, g = g_0 + \cdots + g_e$.

$$f^* = X_{n+1}^d f_0 + X_{n+1}^{d-1} f_1 + \cdots + f_d$$

$$g^* = X_{m+1}^e g_0 + X_{m+1}^{e-1} g_1 + \cdots + g_e$$

$$f^* g^* = \sum_{i,j} X_{n+1}^{d-i} X_{m+1}^{e-j} f_i g_j = (fg)^*$$

□

Nota 2.5.1. *Hay que notar que en la expresión $F_* G_*$, así como en $(FG)_*$, algunos sumandos del sumatorio presentan X_{n+1} y por lo tanto se hace 1, es decir, hay sumandos que solo tienen una variable y no el producto de dos.*

2. *$F = \sum_i^{n+1} \lambda_i X_i^d \Rightarrow F_* = \underbrace{\sum_i^n \lambda_i X_i^d}_{\text{Cada sumando se denota } f_i} + \underbrace{\lambda_{n+1}}_{f_0}$. Por lo tanto, $(F_*)^* = \sum_i X_{n+1}^{n-i} f_i \Rightarrow X_{n+1}^r (F_*)^* = F$.* □

3. *Primero hay que probar que $(F+G)_* = F_* + G_*$: $F + G = \sum_{i,k} \lambda_i X_i^d + \beta_k X_k^e \Rightarrow (F + G)_* = \sum_i^{max(m,n)} (\lambda_i X_i^d + \beta_i X_i^e) + (\lambda_{n+1} + \beta_{m+1}) = \sum_i \lambda_i X_i^d + \lambda_{n+1} + \sum_k \beta_k X_k^e + \beta_{n+1} = F^* + G^*$.*

   Nota 2.5.2. *En el sumatorio consideramos que si X_j no está definido para algún j, entonces X_j vale 0.*

   Falta probar que $f^* + g^* = (f+g)^*$:

   Nota 2.5.3.
   - *El grado de f^* es el mismo que el de f, pues al homogeneizar se convierte en una suma de formas todas del grado de f.*
   - *El grado de $f + g$ coincide con el grado de $(f+g)^*$. La demostración es trivial.*
   - *El grado de $f + g$ es el $max(r, s)$.*

Teniendo en cuenta la nota, es facil ver que

$$\underbrace{\underbrace{X_{n+1}^{r} \underbrace{f^{*}}_{\text{Tiene grado } s}}_{\text{Tiene grado } r\cdot s} + \underbrace{X_{n+1}^{s} \underbrace{g^{*}}_{\text{Tiene grado } r}}_{\text{Tiene grado } r\cdot s}}_{\text{Tiene grado } r\cdot s}$$

Y si analizamos:

$$\underbrace{\underbrace{X_{n+1}^{t}}_{t=r+s-max(r,s)} \underbrace{(f+g)^{*}}_{\text{Tiene grado } max(r,s)}}_{\text{Tiene grado } r\cdot s}$$

Y finalmente, tenemos la igualdad.

Corolario 2.5.1. *Salvo potencias de X_{n+1}, la descomposición en factores de una forma $F \in R[X_1, \ldots, X_{n+1}]$ es la misma que la descomposición en factores de $F_* \in R[X_1, \ldots, X_n]$. En particular, si $F \in k[X, Y]$ es una forma, y k es algebraicamente cerrado, entonces F descompone en producto de factores lineales.*

Demostración 31. *La primera afirmación se tiene de (1) y (2) de la proposición anterior. Si $F = F_1F_2$, entonces se tiene que $F_* = F_{1*}F_{2*}$, y por (2), tenemos que homogeneizando, es decir, multiplicando por potencias de X_{n+1} tendríamos la misma factorización.*

Para la segunda afirmación, tomamos la mayor potencia de Y que divida a F, teniendo $F = Y^r G$, es decir, Y no divide a G y, por lo tanto, $G \in k[X]$. Entonces $F_* = G_* = c\prod(X - \lambda_i)$, pues k es un cuerpo algebraicamente cerrado, así que factoriza en factores lineales. Finalmente, solo queda deshacer la deshomogeneizaciónquedando $F = cY^r \prod(X - \lambda_i Y)$ □

2.6. Módulos cociente y sucesiones exactas de módulos

Sea R un anillo, M, N R-módulos.

Definición 2.6.1. Una aplicación $\varphi : M \to N$ es un **(homo)morfismo de R-módulos** es un morfismo de grupos abelianos tal que $\varphi(am) = a\varphi(m), \forall a \in R$.

Nota 2.6.1. *$ker(\varphi) = \{m \in M : \varphi(m) = 0\} \subseteq M$ sub-R-módulo. Es decir, es subgrupo abeliano de M por ser φ morfismo de grupos abelianos. Basta ver que $\forall m \in ker(\varphi), \forall a \in R \Rightarrow \varphi(am) = a \underbrace{\varphi(m)}_{=0} = 0 \Rightarrow am \in ker\varphi$.*

Nota 2.6.2. *$Im\varphi \subseteq N$ sub-R-módulo. Es subgrupo abeliano por ser φ morfismo de grupos abelianos. $\forall a \in R, m' \in Im\varphi \exists m \in M$ tal que $\varphi(m) = m' \Rightarrow am' = a\varphi(m) = \varphi(am) \in Im\varphi$.*

Nota 2.6.3. *φ es inyectivo $\Leftrightarrow ker\varphi = 0$, φ sobreyectivo $\Leftrightarrow Im\varphi = N$.*

Definición 2.6.2. Un **isomorfismo de R-módulos** es un morfismo biyectivo de R-módulos.

Definición 2.6.3. Dada una sucesión de R-módulos y morfismos de la forma siguiente:

$$M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} M_3$$

diremos que es exacta (en M_2) si se verifica que $ker\varphi_2 = Im\varphi_1$

Ejemplo:
k cuerpo,

$$k^n \xrightarrow{i} k^{n+m} \xrightarrow{\pi} K^m$$

$$(a_1, \dots, a_n) \to (a_1, \dots, a_n, 0, \dots, 0) | (a_1, \dots, a_n, b_1, \dots, b_m) \to (b_1, \dots, b_m)$$

Nota 2.6.4.
- *Si $M_3 = 0$, $M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} 0$, $ker\varphi_2 = M_2$. Esta sucesión es exacta $\Rightarrow Im\varphi_1 = M_2 \Leftrightarrow \varphi_1$ sobreyectiva.*
- *Si $M_1 = 0, M_2, M_3 \neq 0$ la sucesión es exacta si y sólo si φ_2 inyectiva.*

Definición 2.6.4. Diremos que una **sucesión** de R-módulos y morfismos:

$$\cdots M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} \cdots \to M_{n-1} \xrightarrow{\varphi_{n-1} M_n \cdots}$$

es **exacta** si y sólo si $ker\varphi_{i+1} = Im\varphi_i, \forall i$.

Definición 2.6.5. Llamaremos **sucesión exacta corta** a las sucesiones exactas que son de la forma:

$$0 \to N \xrightarrow{\psi} M \xrightarrow{\varphi} P \to 0$$

Nota 2.6.5. *Esta sucesión es exacta si y sólo si:*

- *ψ inyectiva.*
- *φ sobreyectiva.*
- *$ker\varphi = Im\psi$.*

El ejemplo anterior podemos generalizarlo.

2.6.1. Módulos cocientes

Sea $N \subseteq M$ sub-R-módulo, entonces el grupo abeliano cociente $\frac{M}{N}$ R-módulo con el siguiente producto por escalares de R.

$$a\bar{m} := a\bar{m}, \forall a \in R, \forall m \in M$$

donde $\bar{m} \in \frac{M}{N}$.

La proyección natural $\pi : M \to \frac{M}{N}$ es morfismo de R-módulos. Lleva m a $\bar{m}$.

Ejemplo:

Si $N \subseteq M$ sub-R-módulo, entonces $0 \to N \xrightarrow{i} M \xrightarrow{\pi} \frac{M}{N} \to 0$ es sucesión exacta corta.

Proposición 2.6.1. *Sean V_1, V_2, V_3, V_4 k-espacios vectoriales de dimensión finita. Entonces:*

1.
$$Si\ 0 \to V_1 \xrightarrow{\varphi_1} V_2 \xrightarrow{\varphi_2} V_3 \to 0$$
es sucesión exacta corta. Entonces, $dimV_2 = dimV_2 + dimV_3$.

2.
$$Si\ 0 \to V_1 \xrightarrow{\varphi_1} V_2 \xrightarrow{\varphi_2} V_3 \xrightarrow{\varphi_2} \to 0$$
Entonces, $dimV_1 - dimV_2 + dimV_3 - dimV_4 = 0$.

Demostración 32. *1. $\varphi_2 : V_2 \to V_3$ aplicación k-lineal. Fijando bases B_i de V_i, $i = 1, 2 \Rightarrow$ $\varphi_2(v)^t_{B_3} = Av^t_{B_2}$ donde $A = M_{B_1,B_2}(\varphi)$ matriz $m_2 \times m_3$.*

$dimV_2 = m_2, dimV_3 = m_3$, $ker\varphi_2 = Ax^t = 0, Im\varphi_2 =< v_1, \dots, v_{m_3} >$, $A = [x^t_1|\dots|x^t_{m_3}]$.

Entonces, $dim(Im\varphi_2) = rango(A)$,

$dim(ker\varphi_2) = dimV_2 - rango(A) \Rightarrow dim\underbrace{(Im\varphi_2)}_{V_3} + dim\underbrace{(ker\varphi_2)}_{\sim V_1} = dimV_2$

2. *Tenemos dos sucesiones exactas:*

$$0 \to V_1 \xrightarrow{\varphi_1} V_2 \xrightarrow{\varphi_2} W \to 0$$

$$0 \to W \xrightarrow{i} V_3 \xrightarrow{\varphi_3} V_4 \to 0$$

Con lo que aplicando el apartado 1, tenemos:

$$dimV_1 - dimV_2 + dimW = 0$$

$$dimW - dimV_3 + dimV_4 = 0$$

que restando se obtiene:

$$dimV_1 - dimV_2 + dimV_3 - dimV_4 = 0$$

□

Ejemplo (ej 2.48):
$\varphi : M \to M'$ morfismo de R-módulos.

$$0 \to ker\varphi \xrightarrow{i} M \xrightarrow{\varphi} Im\varphi \to 0$$

es una sucesión exacta. $Imi = i(ker\varphi) = ker\varphi$.
Ejercicio 2.49:
(a) $N \subseteq M$ submódulo $\pi : M \to \frac{M}{N}$.
Sea $M \to M'$ morfismo de R-módulos y $\varphi(N) = 0$, hay que probar que existe un único $\bar{\varphi} : \frac{M}{N} \to M'$ tal que $\bar{\varphi} \circ \pi = \varphi \Rightarrow (\bar{\varphi} \circ \pi)(m) = \varphi(m) = \varphi(\bar{m}), \forall m \in M$.
<u>*Solución:*</u>
$\bar{\varphi}$ bien definida.
Si $\bar{m} = \bar{m'} \Rightarrow m - m' \in N \Rightarrow \varphi(m - m') \in \varphi(N) = 0 \Rightarrow \varphi(m - m') = 0 = \varphi(m) - \varphi(m') = \varphi(\bar{m}) - \varphi(\bar{m'})$.
(b) Si $P \subseteq N \subseteq M$ sub-R-módulo, entonces existe $\frac{M}{P} \to \frac{M}{N}$ y $\frac{M}{P} \to \frac{M}{P}$, veamos que es exacta $0 \to \frac{N}{P} \to \frac{M}{P} \to \frac{M}{N} \to 0$.
<u>*Solución:*</u>

$$0 \to \frac{N}{P} \xrightarrow{iny.} \frac{M}{P} \xrightarrow{Sobr.} \frac{M}{N} \to 0$$

$ker\pi = \{m + P : m + N = 0\}, Im(i) = \{n + P : n \in N\} \Rightarrow$ exacta en $\frac{M}{P}$.
$\frac{M/P}{N/P} \sim M/N$.

2.7. Operaciones con ideales

Sean $I, J \subseteq R$ ideales:

- $I + J = \{a + b : a \in I, b \in J\}$ ideal suma de I y J.
- $IJ = < ab : a \in I, b \in J > = \{\sum_{i=1}^{r} a_i b_i : a_i \in I, b_i \in J, 1 \leq r \in \mathbb{N}\}$
- $I^n = I \cdots I \neq < a^n : a \in I >$, si no $I^n = < a_1 \cdots a_n : a_i \in I >$.

Ejemplo: $I = < x, y > \subseteq k[x, y], I^2 = < x^2, y^2, xy >$. $\boxed{\subseteq}$ $f = ax, by, g = cx + dy \Rightarrow fg = acx^2 + (ad + bc)xy + bdy^2$. Los generadores de I^2 son todas de esta forma y está en $< x^2, xy, y^2 > \Rightarrow I^2 \subseteq < x^2, xy, y^2 >$.

Lema 2.7.1.
- *$IJ \subseteq I \cap J$*
- *Si $I + J = R$ (I y J maximales), entonces $I \cap J = IJ$*
- *$(I_1 + I_2)J = I_1 J + I_2 J$.*

Demostración 33. *(1) es obvio.*
(3) $I_i \subseteq I_1 + I_2 \Rightarrow I_i J \subseteq (I_1 + I_2)J \Rightarrow I_1 J + I_2 J \subseteq (I_1 + I_2)J$.

Para ver que $(I_1+I_2)J \subseteq I_1J + I_2J$ basta probar que los generadores del primero está en el segundo.

Sea $(a_1+a_2)b$ con $a_i \in I_i, b \in J$, $a_1b + a_2 \in I_1J + I_2J$.

(2) $(I \cap J) = R(I \cap J) = (I+J)(I \cap J) = \underbrace{I \underbrace{(I \cap J)}_{\subseteq J}}_{\subseteq IJ} + \underbrace{J \underbrace{(I \cap J)}_{\subseteq J}}_{\subseteq IJ} \subseteq IJ.$

Problema 2.39: Apartado b, $(I_1 \cdots I_N)^n = I_1^n \cdots I_N^n$.

Solución:

Hay que ver que los generadores de uno están contenidos en los del otro y el recíproco.

$I_1 \cdots I_N := < a_1 \cdots a_N : a_I \in I_i >$, $(I_1 \cdots I_N)^n = < b_1 \cdots b_n : b_i \in I_i > = < (a_1^{(1) \cdots a_N^{(1)}}) \cdots (a_1^{(n)} \cdots a_N^{(n)}) : a_i^{(j)} \in I_i > = I_1^n \cdots I_N^n$.

Problema 2.40: $I + J = R$, hay que probar que $I + J^2 = R$. (b) $I_1, \dots, I_N \subseteq R$ ideales, I_i y $J_i := \cap_{I \neq j} I_i$ comaximales $\Rightarrow I_1^n \cap \cdots \cap I_N^n = (I_1 \cdots I_N)^n = (I_1 \cap \cdots \cap I_n)^n$

Solución:

$$J = RJ = (I+J)J = IJ + J^2 \subseteq I + J^2$$
$$I \subseteq I + J^2$$
$$\Rightarrow R = I + J \subseteq I + J^2$$

Hay que probar que $I^n + J^m = R, \forall n, m \geq 1$.

Supongo que $I^n + J^m = R$, hay que probar $I^{n+1} + J^m = R$. $I^n = RI^n = (I+J)I^n = I^{n+1} + JI^n \subseteq I^{n+1}J^n \Rightarrow I^n + J^n \subseteq I^{n+1} + J^n$.

(b) $N = 2 \to I_1^n \cap I_2^n = I_1^n I_2^n = (I_1 I_2)^n = (I_1 \cap I_2)^n$. $I_1 + I_2 = R \Rightarrow I_1^n + I_2^n = R$.

Supongo cierto para N y lo veremos para $N+1$ ideales.

$I_1, \dots, I_{N+1}$ ideales tales que $I_i + \cap I_j = R$, hay que probar que $I_1^n \cap \cdots \cap I_{N+1}^n = (I_1 \cdots I_{N+1})^n = (I_1 \cap \cdots \cap I_{n+1})^n$.

$I_i + \underbrace{\cap_{j \neq i,k} I_j}_{\supseteq \cap_{I \neq j} I_j} = R \Rightarrow I_1^n \cap \cdots \cap I_n^n = (I_1 \cap \cdots \cap I_N)^n$ quitando el elemento $k-$ésimo.

$I_1^n \cdots I_{N+1}^n = I_k^n (\prod_{j \neq k} I_j)^n = \cap I_j^n$

Problema 2.41: Sean $I, J \subseteq R$ ideales, $I = < a_1, \dots, a_r >$ finitamente generado. $I \subset \sqrt{J}$. Hay que probar que $I^n \subset J$ para algún n.

Solución:

$a_i \in I \Rightarrow \exists n_i$ tal que $a_i^{n_i} \in J$, nos basta que $I^n = < a_1^{k_i} \cdots a_r^{k_r} : \sum k_i = n >$, tomamos $n = \sum n_i$.

Problema 2.42: (a) $I \subseteq J \subseteq R$ ideales, $\exists \varphi : R/I \to R/J$ homomorfismo natural de anillos sobreyectivo. $r + I \to \varphi(r+I) = r + J$.

(b) $\underbrace{I \subseteq}_{\text{ideal}} R \underbrace{\subseteq}_{\text{subanillo}} S$. Notaremos $IS =< I >\subseteq S$ ideal generado por I en S. $\exists \psi$: $R/I \to S/IS$ homomorfismo natural. $r + I \to \varphi(r + I) = r + IS$.

Solución:

(a) Bien definida:

$r + I = r' + I \Rightarrow r - r' \in I \subseteq J \Rightarrow r + J = r' + J$.

Sea $r + J \in R/J$ cualquiera, $r \in R \Rightarrow \varphi(r + I) = r + J$.

Nota 2.7.1. *$ker\varphi = J/I \subseteq R/I$. Luego, φ no inyectivo si $I \neq J$.*

(b)

Bien definido porque $I \subseteq IS$. Es homomorfismo trivial.

Ejemplo: $I =< x >\subseteq R = k[x] \subseteq S = k(x), IS =< x >=< 1 >= k(x) \Rightarrow S/IS = 0, \psi : \frac{k[x]}{<x>} \to 0$ no inyectivo.

Ejemplo: $I =< x >\subseteq R = k[x] \subseteq S = k[x, y]$, $\psi : \frac{k[x]}{<x>} \to \frac{k[x,y]}{<x>}$ no sobreyectiva pues $\bar{y} \notin Im\psi$, reducción al absurdo: $f(x) \in k[x], \bar{f} = \bar{y}, f - y \in< x >\to\leftarrow$.

Problema 2.43:

Solución:

Sea $\frac{f}{g} \in m, f, g \in k[x]$ tales que $f(P) = 0, g(P) \neq 0 \Rightarrow \frac{f}{g} = \frac{1}{g} f = IO$.

$\frac{x_i}{1} \in m \Rightarrow IO \subseteq m$.

En particular, se deduce que $m^r = I^r O, \forall r \geq 1$.

Problema 2.44:

Solución:

Por un ejercicio anterior, tenemos que existe un único homomorfismo $\tilde{i} : O_p(\mathbb{A}^n) \to O_p(v)$ único homomorfismo que extiende el del enunciado, que lleva $\frac{f}{g} \to \frac{\bar{f}}{\bar{g}}$.

$\varphi(\frac{f}{g} + JO_p(\mathbb{A}^n)) = \tilde{i}(\frac{f}{g}) + J'O_p(V)$.

$\frac{f}{g} - \frac{f'}{g'} \in IO_p(\mathbb{A}^n) \Leftrightarrow g'f - gf' \in J \Leftrightarrow g'f - gf' + I \in J/I = \pi(J) = J' \underbrace{\Leftrightarrow}_{\frac{1}{gg'} \in O_p(V)} \frac{\bar{f}}{\bar{g}} - \frac{\bar{f}'}{\bar{g}'} \in J'O_p(V)$, luego está bien definido e inyectivo. Y es homomorfismo por serlo $\tilde{i}$.

φ sobreyectiva es claro pues todo elementos de $\frac{O_p(V)}{JO_p(V)}$ es de la forma $\frac{\bar{f}}{\bar{g}} + J'O_p(V)$.

Problema 2.45:

Solución:

$\boxed{\Rightarrow}$ $V(I) \cap V(J) = V(I + J) = V(1) = \emptyset$

$\boxed{\Leftrightarrow}$ Por el teorema débil de los ceros de Hilbert.

Problema 2.46:

Solución:

$n = 1$ $\frac{k[x,y]}{<x,y>} \cong k \Rightarrow dim_k k = 1$. $I^n =< x^n, x^{n-1}y, \ldots, xy^{n-1}, y^n >$, $\frac{k[x,y]}{I} \cong \{f \in k[x, y]$ de grado $\leq n - 1\}$ como $k-$espacio vectorial. Una base será todos los monomios de grado menor o igual que $n - 1$.

Problema 2.49:

$P \subseteq N \subseteq M$ R-módulos. $0 \to N/P \to M/P \Rightarrow M/N \to 0$ s.e.c.

(c) $V \subseteq W \subseteq V, dim_k(V/U) < \infty, dim(V/W) + dim(W/U)$.

$0 \to W/U \to V/U \to V/W \to 0$ es s.e.c de k-espacio vectorial $\Rightarrow$ por la prop.7 $dim(V/U) = dim(W/U) + dim(V/W)$.

(d) O anillo local con m ideal maximal, existe una sucesión exacta corta de la forma:

$$0 \to m^n \to O/m^{n+1} \to O/m^n \to 0$$

Con $P = m^{n+1} \subseteq N = m^n \subseteq M = O$ son $O-$módulos. Por (b) se tiene que la sucesión anterior es s.e.c.

Problema 2.50: R anillo de valoración discreta, $R \to R/m$, m ideal maximal.(a) Probar que $dim_k(m^n/m^{n+1}) = 1$.(b) $dim_k(R/m^n) = n, \forall n > 0$.

Solución:

(a) $m =< t >$, veamos que $\{t^n + n^{n+1}\}$ es base de m^n/m^{n+1}. Sea $0 \neq b \in m^n =< t^n >, ord(b) \geq n \Rightarrow_{2,30} \exists! \lambda_0, \ldots, \lambda_n \in k, z_n \in R$ tales que $b = \sum_{i=0}^{n} \lambda_i t^i + z_n t^{n+1} \Rightarrow b = \lambda_n t^n + z_n t^{n+1} \Rightarrow b + m^{n+1} = \lambda_n t^n + m^{n+1}$. Es lo mismo que decir que es una base, así que $dim(m^n/m^{n+1}) = 1$.

(b) Se puede hacer tomando $\{1 + m^n, \ldots, t^{n-1} + m^n\}$ base. O también, usando la sucesión exacta corta:

$$0 \to m^n/m^{n+1} \to O/m^{n+1} \to R/m^n \to O$$

Así que $dim(R/m^{n+1}) = 1 + dim(R/m^n)$, usando que el caso base es $dim_k(R/m) = 1$, y por inducción $dim(R/m^n) = n$.

2.8. Ideales con un número finito de ceros

k cuerpo algebraicamente cerrado. Sea $I \subseteq k[x_1, \ldots, x_n]$ tales que $V(I) = \{P_1, \ldots, P_N\} \subseteq \mathbb{A}^n$.

$O_{P_i}(\mathbb{A}^n) = \{\frac{f}{g} : f, g \in k[x], g(P_i) \neq 0\} := O_i$.

Proposición 2.8.1. *Se tiene el siguiente isomorfismo natural de anillos* $\varphi : \frac{k[x_1,\ldots,x_n]}{I} \to \frac{O_1}{IO_1} \times \cdots \times \frac{O_N}{IO_N}$.

Demostración 34. *Libro, página 27.*

Corolario 2.8.1. $dim \frac{k[\vec{x}]}{I} = dim(\prod_{i=1}^{N} \frac{O_i}{IO_i}) = \sum dim \frac{O_i}{IO_i}$

Corolario 2.8.2. *Si* $V(I) = \{P\}$, *entonces* $\frac{k[\vec{x}]}{I} \cong \frac{O_P(\mathbb{A}^n}{IO_P(\mathbb{A}^n}$.

Problema 2.47:

Se tiene que R es una k-álgebra finitamente generada, lo que implica que es isomorfo a $k[x_1, \ldots, x_n]/I$. Como $dim_k R < \infty$, $V(I)$ es finito, y podemos aplicar la proposición anterior.

Parte II

Impartida por J. Soto

Capítulo 3

Propiedades locales de curvas planas

3.1. Puntos múltiples y lineas tangentes

Sabemos que el conjunto de las curvas planas se puede identificar con hipersuperficies de $\mathbb{A}^2$, que a su vez se puede poner en correspondencia biunívoca con ideales generados por un único elemento $I =< F >$, con F irreducible.

Definición 3.1.1. Una curva es la clase de un polinomio F no constante, módulo la multiplicación por constantes de $k[x, y]$.

Definición 3.1.2. Sea $F \in k[x, y]$ una curva , y (como $k[x, y]$ DFU) $F = \prod_{i=1}^{l} F_i^{e_i}$ su factorización en factores irreducibles. Llamamos componentes irreducibles de F a los F_i y e_i las multiplicidades.

Nota 3.1.1. $V(F) = V(F_1) \cup \cdots \cup V(F_e)$

Nota 3.1.2. *Si F es irreducible, entonces $V(F)$ es una variedad afín. Llamaremos $\Gamma(F) = \Gamma(V(F)) = k[x, y]/ < F >$. $O(F) = Q(\Gamma(F))$ conjunto de las funciones racionales de F. $O_P(F)$ el conjunto de las funciones racionales definidas en P.*

Ejemplos:

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

Definición 3.1.3. Sea F una curva y $P = (a, b) \in F$. Decimos que P es **simple** si $\frac{\partial F}{\partial x}(P) \neq 0$ ó $\frac{\partial F}{\partial y}(P) \neq 0$. En caso contrario, se llama **singular**.

Definición 3.1.4. Si P es simple, la recta $\frac{\partial F}{\partial x}(P)(x-a) + \frac{\partial F}{\partial y}(P)(y-b) = 0$ se llama la **recta tangente**.

Definición 3.1.5. Sea F una curva , y $P = O = (0,0)$. F se puede escribir como $F = F_m + F_{m+1} + \cdots + F_n$ formas de grado i, $F_m \neq 0$. Se define la multiplicidad de F en P como $m_P(F) = m$.

Nota 3.1.3. $P \in F \Leftrightarrow m_P(F) > 0$.

Nota 3.1.4. *El punto $P \in F$ es simple (ó regular) si y sólo si $m_P(F) = 1$.*

Demostración 35. $\boxed{\Rightarrow}$ *$P \in F$ simple. $F = F_1 + F_2 + \cdots = (aX + bY) +$ formas de grado superior . Sabemos que $\frac{\partial F}{\partial X}(0,0)$ ó $\frac{\partial F}{\partial Y}$ son no nulas. $\frac{\partial F}{\partial X}(0,0) = a$, $\frac{\partial F}{\partial Y}(0,0) = b \Rightarrow F_1 \neq 0 \Rightarrow m_P(F) = 1$.*
$\boxed{\Leftrightarrow}$ *Trivial* □

Si P es simple, F_1 es exactamente la recta tangente a F en P.

Definición 3.1.6. Sea $P = O = (0,0)$, F una curva y

$$F = F_m + \cdots + F_n, , \text{descomposición en formas } f_n \neq 0$$

Entonces, $F_m = \prod_i L_i^{r_i}$, y llamamos a cada L_i recta tangente con multiplicidad r_i.

Ejemplos:

- $F = Y - X^2$, la recta tangente es $Y = 0$.
- $F = Y^2 - X^3$, la recta tangente es $Y = 0$ con multiplicidad 2.
- $F = Y^2 - X^3 - X^2 = \underbrace{Y^2 - X^2}_{F_2=(X+Y)(X-Y)} - X^3$, hay dos rectas tangentes.

Definición 3.1.7. Si $F = F_m + \cdots + F_n$ tiene $m > 1$ tangentes distintas. Se llama punto **múltiple** o singular ordinario, y si $m = 2$ se llama **nodo**. Si tiene exactamente una tangente de multiplicidad $m > 1$, se llama una **cúspide**.

Proposición 3.1.1. *Sea $F = \prod F_i^{e_i}$, descomposición en factores irreducibles, $P = O = (0,0)$. Entonces $m_P(F) = \sum e_i \cdot m_P(F_i)$.*

Demostración 36. *Idea: $F_i = F_{m_i}^{(i)} + \cdots F_{n_i}^{(i)}$, $m_P(F_i) = m_i$. $F = \prod F_i^{e_i} = (F_{m_1}^{(1)})^{e_1} \cdots (F_{m_l}^{(l)})^{e_l} +$ elementos de grado superior. Por lo tanto, la multiplicidad es la suma $m_P(F) = e_1 m_1 + \cdots + e_l m_l$* □

Corolario 3.1.1. *Sea $P = O = (0,0) \in F$. P es simple si y sólo si P pertenece a exactamente una componente irreducible de F, F_i. Además, F_i es una componente simple $(e_i = 1)$. P es simple en F_i.*

Definición 3.1.8. Sea $P = (a, b)$ y sea F una curva. Sea T la traslación que lleva $O = (0, 0)$ en $P = (a, b)$. $T : \mathbb{A}^2 \to \mathbb{A}^2$, donde $T = (X + a, Y + b)$. La curva trasladada es $F^T = F(X + a, Y + b)$, y la multiplicidad $m_P(F) = m_O(F^T)$.

Ejemplo:
Sea $Y - X^2 \ni (1, 1)$. $m_{(1,1)}F = m_{(0,0)}F^T = 1$, con $F^T = F(X + 1, Y + 1) = (Y + 1) - (X + 1)^2 = Y - X^2 - 2X$.

En la situación anterior, $G = F^T = G_m + \cdots + G_n$, $G_m = \prod L_i^{r_i}$, $L_i = \alpha_i X + \beta_i Y$, y las rectas tangentes a F en P son $\alpha_i(X - a) + \beta_i(Y - b)$ con multiplicidad r_i.

Problema 3.5: Probar que $m_P(F)$ es el menor entero m tal que para algún $i + j = m$, $\frac{\partial^m F}{\partial x^i \partial y^j}(P) \neq 0$. Encuentra una descripción para la forma lider de F en P en término de sus derivadas.

Solución: Supongamos $P = (0, 0)$. $F = F_m + \cdots + F_n$, sabemos que existen $i + j = m$ de manera que $F_m = aX^iY^j + \cdots$. Y se tiene que $\frac{\partial^m F}{\partial x^i \partial y^j}(P)(0, 0) = a$. El resto trivial.

Problema 3.3: Sea F una curva $deg(F) = n$. Si F tiene un punto P de multiplicidad n. Entonces F es la unión de n rectas (no necesariamente distintas).

Solución:

Sea $F = F_m + \cdots + F_n$ descomposición en formas. Consideramos que P es el origen. n es el grado y m es $m_p(P)$. $m = n \Rightarrow F$ es una forma de grado n, por lo tanto factoriza como producto de formas lineales. $F = F_n = \prod_{i=1}^{k} L_i^{r_i}$ con $r_1 + \cdots + r_k = n$. Por lo tanto, F es la unión de las rectas L_i con multiplicidad i.

3.2. Multiplicidad y anillo local

El objetivo de esta sección es poder leer $m_P(F)$ en $O_p(F)$. Notación: Sea F una curva, y $\Gamma(F) = k[x, y]/ < F >$, si $G \in k[x, y]$ denotamos por $g = G+ < F >\in \Gamma(F)$ y cuando haga falta, $g/1 \in O_p(F)$.

Teorema 3.2.1. *Sea F una curva, y P un punto de F. P es un punto simple si y sólo si $O_P(F)$ es un anillo de valoración discreta. En este caso, si L es una recta que pasa por P y no es tangente a F (en P), entonces $l/1$ (la imagen de $l = L+ < P >$ en $O_P(F)$) es un parámetro de uniformización de $O_P(F)$.*

Demostración 37. $\boxed{\Rightarrow}$ *Cambio de coordenadas convirtiendo $P = O = (0, 0)$, $L = x$ y que la tangente (al ser P punto simple, es único) a F en P tenga ecuación $y = 0$. Sabemos que $O_P(F) \cong O_P(\mathbb{A}^2)/FO_P(\mathbb{A}^2)$, veamos cual es el ideal maximal de $O_P(F)$ que denotaremos por m_P, el ideal maximal m de $O_P(\mathbb{A}^2)$ es $< x/1, y/1 >$, y por lo tanto, $m_P =< x/1, y/1 >$ y lo que tenemos que probar es que $m_P =< x >$. Consideramos $F = Y+$ términos de grado mayor que 1. Entonces, se puede escribir $F = YG - X^2H$, donde $G = 1 + \cdots , H \in k[x]$. $G(P) \neq 0$, por lo tanto podemos tomar $yg - x^2h$ en $\Gamma(F) = k[x, y]/ < F >$, y en ese ambiente,*

$yg - x^2h = 0$, y podemos despejar, tomando $yg = x^2h \Rightarrow \frac{y}{1}\frac{g}{1} = \frac{x^2}{1}\frac{h}{1}$ en $O_P(F) \ni \frac{1}{g}$, pues $g \neq 0$, y queda $\frac{y}{1} = \frac{x^2}{1}\frac{h}{1}\frac{1}{g}$ y se tiene que $m_p =< \frac{x}{1}, \frac{y}{1} >=< x >$. □

Ejemplo: $y = x^2$, $p = (0,0)$, y se tiene que $y = x^2$ en $\Gamma(F)$ y por tanto, $y/1 = x^2/1$ en $O_P(F)$. Entonces, $m_p < \frac{x}{1}, \frac{y}{1} >=< \frac{x}{1} >$

Nota 3.2.1. *Si el ideal maximal está generado por un solo elemento, es un anillo de valoración discreta.*

Nota 3.2.2. *El orden está relacionado a la recta tangente, la caracteriza.*

Corolario 3.2.1. *Sea P un punto simple de F, (F irreducible) y L una recta que pasa por P. Entonces $ord_P^F(l) = 1$ si y sólo si L no es tangente a F en P. Y $ord_P^F(l) > 1$ si y sólo si L tangente a F en P.*

Demostración 38. *Usando el mismo cambio de coordenadas del teorema anterior. $Y = 0$ es la recta tangente, y L no tangente tiene ecuación $X = 0$. Entonces $ord_P^F(x/1) = 1, ord_P^F(y/1) = ord_P^F(\frac{x^2}{1}\frac{h}{1}\frac{1}{g}) = ord_P^F(x^2) + ord_P^F(\frac{h}{g}) \geq 2$.* □

Nota 3.2.3. *En general, si F no es irreducible, no tiene sentido hablar de ord_P^F (ni si quiera está definillo el anillo local). Pero si $P \in F$ es simple, entonces P pertenece a exactamente una componente irreducible, y definimos $ord_P^F(L) := ord_P^{F_i}(L)$.*

Teorema 3.2.2. *F una curva irreducible, P un punto. Para n suficientemente grande,*

$$m_P(F) = dim_k(m_P^n/m_P^{n+1}),$$

donde m_P es el ideal maximal de $O_P(F)$.

Demostración 39. *Sea $P = (0,0)$, $O = O_P(F)$, y denotamos $m_P(O_P(F)) = m$, $m' = m_P(F)$. La sucesión de espacios vectoriales:*

$$0 \to m^n/m^{n+1} \to \underbrace{O/m^{n+1} \to O/m^n \to 0}_{(*1)}$$

es exacta. Veamos que es exacta:

$O \to O/m^n \to 0$, $m^{n+1} \subset m^n$, y por lo tanto está contenido en el núcleo, luego $(*1)$ es trivialmente exacta. Ver demostración en la sección 2.9. Son subespacios de dimensión finita, y por lo tanto, $dim(m^n/m^{n+1}) = dim_k(O/m^{n+1}) - dim_k(O/m^n)$.

Queremos calcular $dim_k(O/m^n)$ para $n >> 0$.

Observamos que es suficiente demostrar que para $n >> 0$, $dim(O/m^n) = n \cdot m' + s$ con s constante. En ese caso, $dim_k(m^n/m^{n+1}) = (n+1)m' + s - (nm' + s) = m'$. Por la sección 2.9 y el problema 2.44. Tenemos:

$O_P/m^n = O_p(F)/m^n \cong O_P(F)/I^n O_P(F) \cong O_P(\mathbb{A}^2)/ < I^n, F > O_P(\mathbb{A}^2) \cong k[X,Y]/ < I^n, F >$, con $I =< X, Y >\subseteq k[X,Y]$. (La última isomorfía se tiene por tener una cantidad finita de puntos).

$F = F_{m'} + \dots$, si tomamos $G \in I^{n-m'} \Rightarrow FG \in I^n$. Consideramos $k[X,Y]/ < I^n, F >$, es dificil calcularlo, pero sí conocemos $k[X,Y]/I^n$ que está contenido en el otro. Y podemos construir la siguiente sucesión exacta:

$$k[X,Y]/I^{n+m'} \xrightarrow{\psi} k[X,Y]/I^n \xrightarrow{\varphi} k[X,Y]/ < I^n, F > \to 0$$

$\varphi(G + I^n) = G+ < I^n, F >$, y $\psi(G + I^{n-m'}) = GF + I^n$
Para probar que es exacta, hay que probar:

- *φ es sobreyectiva (Que lo tenemos).*
- *ψ inyectiva: $\psi(H + I^{n-m'}) = \underbrace{HF}_{\text{Todo monomio de } HF \text{ tiene grado } \geq n(*2)} + I^n = 0 + I^n$, $(*2)$ implica que todo monomio de H tiene grado $\geq n - m'$, y por lo tanto es 0 en el cociente por $I^{n-m'}$.*
- *$im\psi = ker\varphi$*
  $\boxed{\subseteq}$ Es equivalente a que $\varphi \circ \psi = 0$, y es trivial, pues $\varphi \circ \psi(G + I^{n-m}) = \varphi(GF + I^n) = GF+ < I^n, F >= \bar{0}$.
  $\boxed{\supseteq}$ $H + I^n$ tal que $\varphi(H + I^n) = 0 \Leftrightarrow H+ < I^n, F >= 0 \Leftrightarrow H \in< I^n, F >\Leftrightarrow H = A + BF$, donde $A \in I^n$. Tomamos $\psi(B + I^{n-m}) = BF + I^n = A + BF + I^n = H + I^n$

Por lo tanto, podemos tomar $dim_k k[X,Y]/ < I^n, F >= dim_k k[X,Y]/I^n - dim_k k[X,Y]/I^{n-m} = \frac{n(n+1)}{2} - \frac{(n-m)(n-m+1}{2} = nm - \underbrace{\frac{m(m+1)}{2}}_{cte=s}$ □

Corolario 3.2.2. *El recíproco del teorema 1.*

Demostración 40. *Por el problema 2.50, si $O_P(F)$ es AVD, entonces $dim_k(m^n/m^{n+1}) = 1$, y por el teorema 2, $m_P(F) = 1$ y se tiene que P es simple.* □

Nota 3.2.4. *Cuando hablamos de n suficientemente grande, basta que sea mayor o igual que $m_P(F)$.*

Problema 3.13: Con la notación del teorema, $m = m_P(F)$. Hay que probar que $dim_k(m^n/m^{n+1}) = n + 1$ para $0 \leq n < m_P(F)$. En particular, el punto P es simple si y sólo si $dim_k(m/m^2) = 1$, y no es simple si es mayor o igual que 2.

<u>Solución:</u>

$n \leq m'$, el ideal $< I^n, F >=< I^n >$, y así, $O/m^n \cong k[X,Y]/ < I^n, F >= k[X,Y]/ < I^n >$. Y tenemos,

$$0 \to m^n/m^{n+1} \to O/m^{n+1} \to O/m^n \to 0,$$

$d = \frac{(n+1)(n+2)}{2} - \frac{n(n+1)}{2} = n + 1.$

3.3. Número de intersección

Como la definición de número de intersección es poco intuitiva, se dará una serie de propiedades que justifiquen la definición.

1. $I(P, F \cap G) \in \mathbb{Z}_{\geq 0}$ para cualesquiera curvas F, G que se intersequen propiamente en P (i.e. que no tengan ninguna componente (irreducible) común sobre P). $I(P, F \cap G) = \infty$ si no se intersecan propiamente en P.

2. $P \notin F \cap G \Leftrightarrow I(P, F \cap G) = 0$. $I(P, F \cap G)$ sólo depende de las componentes irreducibles de F y G que pasan por P. En particular, si F, G son constantes no nulas $I(P, F \cap G) = 0$.

3. Si T es un cambio de coordenadas con $T(Q) = P$, $I(P, F \cap G) = I(Q, F^T \cap G^T)$.

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

5. $I(P, F \cap G) \geq m_P(F) \cdot m_P(G)$. E igualdad si y solo si F y G no poseen tangentes comunes en P. En particular, $I(P, F \cap G) = 1$ si y sólo si P es simple para F y G y las tangentes son distintas.

6. $F = \prod F_i^{r_i}$, $G = \prod G_j^{s_j}$, entonces $I(P, F \cap G) = \sum r_i s_j I(P, F_i \cap G_j)$.

7. $I(P, F \cap G) = I(P, F \cap (G + AF)), \forall A \in k[x, y]$. Es decir, $I(P, F \cap G)$ sólo depende de la imagen de G en $\Gamma(F) = k[x, y]/ < F >$.

Teorema 3.3.1. *Existe un único número definido para P, F, G arbitrarios que verifica las propiedades (1-7) y viene dado por $I(P, F \cap G) = dim_k O_P(\mathbb{A}^2)/ < F/1, G/1 >$.*

Demostración 41. $\boxed{\text{Unicidad}}$ *Queremos probar que las propiedades (1-7) determinan unívocamente $I(P, F \cap G)$. Por la propiedad 3, podemos suponer que $P = (0, 0)$. Por la propiedad 1, el caso $I(P, F \cap G) = \infty$ está determinado. Por la propiedad 2, $I(P, F \cap G) = 0$ está determinado.*

Procedemos a demostrar el resto de casos por inducción (fuerte): suponemos que $I(P, F \cap G) = n$ y la hipótesis es que $I(P, A \cap B)$ está unívocamente determinado para cualesquiera A, B con $I(P, A \cap B) < n$.

Sean $r = deg(F(X, 0))$ y $s = deg(G(X, 0))$. Podemos suponer por la propiedad 4 que $r \leq s$. Si $r = 0$, entonces $y | F(X, Y) \Rightarrow F = Y \cdot H$. Por la propiead 6, $I(P, F \cap G) = I(P, Y \cap G) + I(P, H \cap G)$. Ponemos $G(X, 0) = X^m(a_0 + a_1 X + \cdots)$, y ocurre por la propiedad 7 que $I(P, Y \cap G) = I(P, Y \cap G(X, 0)) =_{P,6} \underbrace{I(P, Y \cap X^m)}_{=m \underbrace{I(P, Y \cap X)}_{P,5} = m} + \underbrace{I(P, Y \cap (a_0 + a_1 X + \cdots))}_{=0}$. Y llegamos a la conclusión de que $I(P, F \cap G) = I(P, Y \cap G) + I(P, H \cap G) = \underbrace{m}_{>0} + \underbrace{I(P, H \cap G)}_{<I(P, F \cap G)}$, y se aplica inducción.

Si $r > 0$, podemos suponer que $F(X,0)$ y $G(X,0)$ son mónicos. Definimos $H := G - X^{s-r}F$, y sabemos por la propiedad 7 que $I(P, F\cap G) = I(P, G - X^{s-r}F \cap F)$, y H tiene grado estrictamente menor que G, $deg(H(X,0)) < s$. Se repite el proceso hasta caer en el caso $r = 0$, intercambiando si es necesario el orden.

$\boxed{\text{Existencia}}$ Definimos $I(P, F\cap G) = dim_k O_P(\mathbb{A}^2)/ < f, G >$. La propiedad 4 se cumple porque no importa el orden en el ideal. La propiedad 7 se tiene sustituyendo G por AF. La propiedad 2 se tiene porque si $p \notin G\cap F \Rightarrow p \notin F \vee p \notin G \Rightarrow$ (por ejemplo no está en F), entonces F una unidad y $< F, G >= O_P(\mathbb{A}^2)$ y $I(P, F\cap G) = 0$. Sólo depende de las componentes irreducibles que pasan por P, $F = F_1F_2$ con $p \notin F_2$. $O_P(\mathbb{A}^2) \ni F = F_1 \underbrace{F_2}_{Unidad}$.

La propiedad 3 también es evidente, pues si T es un cambio de coordenadas, induce un isomorfismo de anillos locales $T : O_Q(\mathbb{A}^2) \to O_P(\mathbb{A}^2)$, $\frac{H}{L} \to \frac{H^T}{L^T}$, entonces $O_P(\mathbb{A}^2)/ < F, G >\cong O_Q(\mathbb{A}^2)/ < F^T, G^T >$. Podemos a partir de ahora usar $P = (0,0)$.

Demostremos la propiedad 1, supongamos que F y G tienen una componente común sobre P, existe H tal que $H(P) = 0$ tal que $H|F$ y $H|G$. Eso quiere decir que $< F, G >\subseteq< H >$. Y por tanto, $< F/1, G/1 >\subseteq< H/1 >$ como ideales de $O_P(\mathbb{A}^2)$. Y tenemos la siguiente sucesión exacta de anillos, por lo tanto de espacios vectoriales:

$$O_P(\mathbb{A}^2)/ < F, G >\to O_P(\mathbb{A}^2)/ < H >\to 0$$

Y se tiene que $dim_k O_P(\mathbb{A}^2)/ < F, G >\geq dim_k \underbrace{O_P(\mathbb{A}^2)/H}_{\cong O_P(H)} =_{O_P(H)\supset\Gamma(H)}= \infty$, por el corolario 4 del Nulstellenstaz. Se usa que H tiene un conjunto infinito de puntos, pues no es constante.

Si F y G no tienen componentes comunes sobre P, entonces $dim_k(O_P(\mathbb{A}^2)/ < F, G >) = dim_k(k[x,y]/ < F, G >) < \infty$.

Demostremos la propiedad 6, basta con probar $I(P, F\cap GH) = I(P, F\cap G) + I(P, F\cap H)$. Tenemos que $< F, GH >\subseteq< F, G >$ (denotemos $O = O_P(\mathbb{A}^2)$), entonces necesitamos la sucesión exacta:

$$0 \to O/ < F, H >\xrightarrow{\psi} O/ < F, GH >\xrightarrow{\varphi} O/ < F, G >\to 0$$

$\varphi(t+ < F, GH >) = t+ < F, G >$ bien definida y sobreyectiva.

$\psi(t+ < F, H >) = tG+ < F, GH >$. Hay que ver que ψ es inyectiva y que $Im\psi = ker\varphi$.

Veamos que ψ inyectiva:

$\psi(t+ < F, H >) = 0+ < F, GH >\Rightarrow tG = uF + vGH$, donde $u, v \in O$. Existe un polinomio $S \in k[x,y]$, $S(P) \neq 0$, así que $Su = A \in k[x,y]$, $sv = B \in k[x,y]$ y $st = C \in k[x,y]$, entonces $stG = SuF + SvGH \Rightarrow CG = AF + BGH \Rightarrow G(C - BH) = AF$ en $k[x,y]$. Como F y G no tiene componentes comunes, entonces $F|(C - BH) \Rightarrow C - BH = DF \Rightarrow C = DF + BH$, dividimos por S y tenemos $t = C/S = (D/S)F + (B/S)H \Rightarrow \bar{t} = 0$.

Falta ver que $im\psi = ker\varphi$:

$\boxed{\subseteq}$ *$\varphi \circ \psi = 0$, y se tiene porque $\varphi \circ \psi(t+ < F, H >) = \varphi(tG+ < F, GH >) = tG+ < F, G >= 0$.* $\boxed{\supseteq}$ *Sea $z+ < F, GH >\in ker\varphi \Rightarrow z+ < F, G >= 0 \Rightarrow z = uF + vG \Rightarrow \psi(v+ < F, H >) = vG+ < F, GH >= z+ < F, GH >$.*

Falta probar la propiedad 5, $I(P, F \cap G) \geq m_P(F)m_P(G)$, y se da la igualdad si y sólo si F y G no tienen tangentes comunes en P.

Llamamos $m = m_P(F), n = m_P(G), O = O_P(\mathbb{A}^2)$, y consideramos $I =< x, y >\subseteq k[X, Y]$.

Sabemos que $< F, G >\subseteq< I^{m+n}, F, G >$, entonces tiene sentido considerar

DIAGRAMA PÁGINA 54

donde φ, π, α son los homomorfismos naturales y ψ se define por $\psi(A + I^n, B + I^m), = \psi(\bar{A}, \bar{B}) = AF \bar{+} BG = AF + BG + I^{m+n}$.

Hay que ver que la sucesión de arriba es exacta, para ello hay que probar que $ker\varphi = Im\psi$:

$\boxed{\supseteq}$ $\Leftrightarrow \varphi \circ \psi = 0$.

$\boxed{\subseteq}$ *$H + I^{m+n}$ tal que $\varphi(\bar{H}) = \bar{0} \Leftrightarrow H \in< I^{n+m}, F, G >\Leftrightarrow H = H_1 + AF + BG, H_1 \in I^{n+m}, \psi(A + I^n, B + I^m) = AF + BG + I^{m+n} = (AF + BG + H_1) + I^{n+m}$.*

Por lo tanto el diagrama es exacto.

$dim(ker\varphi) = dim(Im\psi) \leq dim(k[X, Y]/I^n) + dim(k[X, Y]/I^m)$, y se da la igualdad si y sólo si ψ es inyectiva.

$dim(k[X, Y]/ < I^{n+m}, F, G >= dim(k[X, Y]/I^{m+n}) - dim(ker\varphi)$.

$dim(O_P(\mathbb{A}^2)/ < F, G >\geq_{(*1)} dim(O/ < I^{n+m}, F, G >) = dim(k[X, Y]/ < I^{m+n}, F, G >= dim(k[X, Y]/I^{n+m}) - dim(ker\varphi) \geq_{(*2)} dim(k[X, Y]/I^{n+m}) - dim(k[X, Y]/I^n) - dim(k[X, Y]/I^m) = m \cdot n$.

Falta ver cuándo se da la igualdad. Se da si π es isomorfismo, que da la igualdad $(*1)$, o de manera equivalente si y sólo si $I^{n+m} \subset< F, G >$, y se tiene $(*2)$ si y sólo si ψ es inyectiva. (Ejercicio) □

Lema 3.3.1. *En las condiciones anteriores:*

1. *F, G no tienen tangentes comunes en P, entonces $I^t \subset< F, G > O$ para todo $t \geq m + n - 1$.*

2. *ψ es inyectiva si y sólo si F, G no tienen tangentes comunes en P.*

Demostración 42. *Ejercicio.*

Ejemplo:

$F = X^2 - Y^3$, tiene dos ramas.

Tomamos $G = X$. $I(P, F \cap G) = I(P, X^2 - Y^3 \cap X) = I(P, Y^3 \cap X) = 3I(P, Y \cap X) = 3$, porque no tienen tangentes comunes.

Tomamos ahora la horizontal. $I(P, F \cap H) = I(P, X^2 - Y^3 \cap Y) = I(P, X^2 \cap Y) = 2$.

Ejemplo:

$I(P, E \cap F)$, donde $E = (X^2 + Y^2)^2 + 3X^2Y - Y^3$, y $F = (X^2 + Y^2)^3 - 4X^2Y^2$.

Las tangentes de E:

$E_3 = (3X^2 - Y^2)Y = Y(\sqrt{3}X - Y)(\sqrt{3} + Y)$ tomando los monomios de menor grado.

$F_4 = X^2Y^2$.

Por lo tanto que la multiplicidad va a ser mayor que $3 \cdot 4 = 12$.

$I(P, E \cap F) = I(P, F - (X^2 + Y^2)E \cap E) = I(P, -4X^2Y^2 - (X^2 + Y^2)Y(3X^2 - Y^2) \cap (X^2 + Y^2)^2 + (3X^2 - Y^2)Y) = I(P, Y(-4X^2Y - (X^2 + Y^2)(3X^2 - Y^2) \cap E) = I(P, Y \cap (X^2 + Y^2)^2 + (3X^2 - Y^2)Y) + I(P, H_3 \cap H_2) = I(P, Y \cap X^4) + 3 \cdot 2 =$ ... En el Fulton.

Ejercicio: Demostrar las propiedades 8 y 9.

Capítulo 4

Variedades proyectivas

4.1. Conjuntos algebraicos proyectivos

Definición 4.1.1. Dado un polinomio $F \in k[X_1, \ldots, X_{n+1}]$ y $P = [a_1 : \cdots : a_{n+1}] \in \mathbb{P}^n$, decimos que $F(P) = 0$ si $F(b_1, \ldots, b_{n+1}) = 0$ para toda elección $[b_1 : \cdots : b_{n+1}] = [a_1 : \cdots : a_{n+1}]$.

Nota 4.1.1. *Es equivalente a que $F(\lambda a_1, \ldots, \lambda a_{n+1}) = 0, \forall \lambda$.*

Nota 4.1.2. *Sea $F = F_m + \cdots + F_n$ la descomposición en formas de F. $F(P) = 0 \Leftrightarrow F_m(P) = \cdots = F_n(P) = 0$.*

Demostración 43. *Sea $P = [a_1 : \cdots : a_{n+1}]$, $F(\lambda a_1, \ldots, \lambda a_{n+1}) = 0 \forall \lambda \in K^*$. Sea λ una variable, consideramos el polinomio $G(\lambda) = F(\lambda, \ldots, \lambda a_{n+1}) = F_m(\lambda a_1, \ldots, \lambda a_{n+1}) + \cdots + F_n(\lambda a_1, \ldots, \lambda a_{n+1}) = \lambda^m F_m(a_1, \ldots, a_{n+1}) + \cdots + \lambda^n F_n(a_1, \ldots, a_{n+1})$, pero $F(P) = 0 \Leftrightarrow G(\lambda) = 0 \Leftrightarrow F_i(a_1, \ldots, a_{n+1}) = 0 \Leftrightarrow F_i(\mu a_1, \ldots, \mu a_{n+1}) = 0, \forall \mu \in K^* \Leftrightarrow F_i(P) = 0$.*

Definición 4.1.2. Sea $S \subseteq K[X_1, \ldots, X_{n+1}]$, se denota $V(S)$

$$V(S) = \{P : F(P) = 0, \forall F \in S\}$$

y se llama el conjunto algebraico proyectivo definido por S.

Proposición 4.1.1. *Si $I =< S >$, entonces $V(I) = V(S)$. Más aún, $I =< F^{(1)}, \ldots, F^{(r)} >$, entonces $V(I) = V(< \{F_j^{(i)}\} >)$ donde $F^{(i)} = F_{m_1}^{(i)} + \cdots + F_{n_i}^{(i)}$, suma de formas homogéneas.*

Demostración 44. *$S \subseteq I \Rightarrow V(I) \subset V(S)$. Recíprocamente, $P \in V(S), H \in I \Rightarrow H_1, \ldots, H_r \in S$ tal que $H = A_1 H_1 + \cdots + A_s + H_s$.*

$H(P) = A_1(P)H_1(P) + \cdots A_s(P)H_s(P) = 0$, suma de ceros, luego $H(P) = 0, \forall H \in I \Rightarrow P \in V(I)$.

Veamos que $V(< F^{(1)}, \ldots, F^{(r)} >) = V(< F_j^{(i)} >)$. $P \in V(< F^{(1)}, \ldots, F^{(r)} >) \Leftrightarrow F^{(i)}(P) = 0, i = 1, \ldots, r \Leftrightarrow F^{(i)}(P) = 0, i = 1, \ldots, r$ y $j = m_i, \ldots, n_i \Leftrightarrow P \in V(< F_j^{(i)} >)$. Puedo pensar que I está generado por formas.

Ejemplo: $V(< Y-X^2, X^2Y-Y^4, Y^4+Z^4 >) = V(< \{Y, X^2, X^2Y, Y^4, Y^4+Z^4\} >)$.

Definición 4.1.3. Sea $\mathbb{X} \subset \mathbb{P}^n$. Se llama el ideal de $\mathbb{X}$ a $I(\mathbb{X}) = \{F \in K[X_1, \ldots, X_{n+1}]$ tal que $F(P) = 0, \forall P \in \mathbb{X}\}$.

Nota 4.1.3. *$I(\mathbb{X})$ es un ideal y verifica que $\forall F \in I = I(X)$, si $F = F_m + \cdots + F_n, F_i \in I, i = m, \ldots, n$.*

Definición 4.1.4. Un ideal homogéneo es un ideal $I \subset K[X_1, \ldots, X_{n+1}]$ con esa propiedad, es decir, si $F = \sum F_i \in I \Leftrightarrow F_i \in I$.

Proposición 4.1.2. *Sea I un ideal de $K[X_1, \ldots, X_{n+1}]$, entonces I es homogéneo si y sólo si I tiene un sistema de generadores homogéneos.*

Demostración 45. $\boxed{\Rightarrow}$ *Si $I =< F^{(1)}, \ldots, F^{(r)} >\Rightarrow I =< F_j^{(i)} >$.*

$\boxed{\Leftarrow}$ *Sea $I =< G_1, \ldots, G_s >, G_i$ homogéneos. Tomamos $F \in I$ arbitrario, $F = F_m + \cdots + F_n$, demostremos que $F_n \in I$. $F = A_1G_1 + \cdots + A_sG_s$, puedo suponer que el grado de los G_i es menor o igual que n, pues si alguno tiene grado mayor y es homogéneo va a cancelar. También podemos suponer que $deg(A_i) \leq n - deg(G_i)$. $F_n = (A_1G_1 + \cdots + A_sG_s)_n = \sum A_{in-d_i}G_i$ con $d_i = deg(G_i), A_i = \sum A_{ij}$, por lo tanto $F_n \in I$.* $\square$

Corolario 4.1.1.

$$\{\textit{ Conjuntos algebraicos } \mathbb{X} \subset \mathbb{P}^n\}$$

$$I \downarrow \quad \uparrow V$$

$$\{\textit{ Ideales homogéneos de } K[X_1, \ldots, X_{n+1}]\}$$

Ejercicio: Denotamos I, J ideales homogéneos, $\mathbb{X}, \mathbb{Y}$ conjuntos algebraicos proyectivos.

1. $I =< S >\Rightarrow V(I) = V(S)$.
2. $V(\cup_i I_i) = V(\sum I_i) = \cap_i V(I_i)$.
3. $I \subset J \Rightarrow V(I) \supset V(J)$.
4. F, G son formas, entonces $V(F \cdot G) = V(F) \cup V(G)$. Por tanto, $V(I) \cup V(J) = V(\{FG : F \text{ forma } \in I, G \text{ forma } \in J\})$.
5. $V(< 0 >) = \mathbb{P}^n$. $V(< 1 >) = V(K[X_1, \ldots, X_{n+1}]) = \emptyset$. $V(< X_1, \ldots, X_{n+1} >) = \emptyset$, $< X_1, \ldots, X_{n+1} >$ es el ideal irrelevante. Sea $P \in \mathbb{P}^n, [a_1 : \cdots : a_{n+1}] = P = V(\{a_iX_j - a_jX_i\})$(, todos los menores de orden 2).
6. $\mathbb{X} \subseteq \mathbb{Y} \Rightarrow I(\mathbb{Y}) \subset I(\mathbb{X})$.
7. $I(\emptyset) =< 1 >= k[X_1, \ldots, X_{n+1}]$

8. $I(V(S)) \supset S, V(I(\mathbb{X})) \supset \mathbb{X}$

9. $V(I(V(S))) = V(S), I(V(I(\mathbb{X}))) = I(\mathbb{X})$.

10. $I(\mathbb{X})$ es homogéneo y radical.

Lema 4.1.1. *Sea I un ideal homogéneo, I es primo si y sólo si $FG \in I, F, G$ formas, entonces $F \in I$, ó $G \in I$.*

Demostración 46. $\boxed{\Rightarrow}$ *Trivial.*

$\boxed{\Leftarrow}$ *¿I primo? $F, G \in K[X_1, \dots, X_{n+1}]$, supongo que $FG \in I$, pero $F \notin I, G \notin I$. $F = \sum_{i=0}^{n} F_i, G = \sum_{j=0}^{m} G_j \Rightarrow \exists r =$ máximo grado de la formas de F, tal que $F_r \notin I, F_r \neq 0$, y $s =$ máximo grado de las formas de G, tales que $G_s \notin I, G_s \neq 0$. Consideremos la forma $(F \cdot G)_{r+s} = F_0 G_{r+s} + F_1 G_{r+s-1} + \underbrace{\cdots + F_r G_s}_{\neq 0} + F_{r+1} G_{s-1} + \cdots + F_{r+s} G_0$. Tenemos dos casos posibles, $F_l G_h$, con $(l, h) = (r, s)$ ó $(l > r) \vee (h > s)$, en este último puede ser 0 o pertenecer al ideal.*

Como I es homogéneo, $(\underbrace{\underbrace{FG}_{H}}_{\in I}{}_{+F_rG_s})_{r+s} \in I \Rightarrow F_r G_s \in I$, que al ser primo para las formas, $F_r \in I \vee G_s \in I \rightarrow\leftarrow$. □

Definición 4.1.5. Un conjunto algebraico proyectivo se llama irreducible si y sólo si no es unión de dos subconjuntos propios, es decir , si $\mathbb{X} = \mathbb{X}_1 \cup \mathbb{X}_2 \Rightarrow \mathbb{X} = \mathbb{X}_1$ ó $\mathbb{X} = \mathbb{X}_2$.

Proposición 4.1.3. *Sea $\mathbb{X}$ conjunto algebraico proyectivo irreducible si y sólo si $I(\mathbb{X})$ es primo. Todo conjunto algebraico proyectivo se descompone de forma única (salvo orden) en conjuntos algebraicos proyectivos irreducibles, que se llaman las componentes irreducibles de $\mathbb{X}$.*

Demostración 47. *Misma demostración que en el caso afín.*

Definición 4.1.6. Dado V un conjunto algebraico proyectivo, no vacío. Se llama el cono afín de V a

$$C(V) = V_a(I(V)) = \{(a_1, \dots, a_{n+1}) \in \mathbb{A}^{n+1} : [a_1 : \cdots : a_{n+1}] \in \mathbb{X}\} \cup \{\vec{0}\}$$

Proposición 4.1.4. *Sea $V \neq \emptyset$ conjunto algebraico proyectivo, $I_a(C(V)) = I_p(V)$. Si I es homogéneo, $V_p(I) \neq \emptyset$, entonces $C(V_p(I)) = V_a(I)$.*

Teorema 4.1.1. *(Nullstellensatz) I homogeneo $\subseteq k[X_1, \dots, X_{n+1}]$.*

1. *$V_p(I) = \emptyset \Leftrightarrow$ existe una potencia $N >> 0$ tal que I contiene todas las formas de grado N.*

2. *$V_p(I) \neq \emptyset$, $I_p(V_p(I)) = radI$.*

Demostración 48. 1. $V_p(I) = \emptyset \Leftrightarrow V_a(I) \subset \{(0,\dots,0)\} \Leftrightarrow \underbrace{I_a(V_a(I))}_{radI} \supset \underbrace{I_a(\{0,\dots,0\})}_{<X_1,\dots,X_{n+1}>} \Leftrightarrow$ $\exists N >> 0$ *tal que* $< X_1,\dots,X_{n+1} >^N \subseteq I$.

2. $V_p(I) \neq \emptyset$, $I_p(V_p(I)) = I_a(C(V_p(I))) = I_a(V_a(I)) = radI$ □

Corolario 4.1.2. *I un ideal radical de* $k[X_1,\dots,X_{n+1}]$ *homogéneo tal que* $V_p(I) \neq \emptyset$ *(i.e.* $I \neq < X_1,\dots,X_n >$*), entonces,* $I(V(I)) = I$.

Corolario 4.1.3. *I homogéneo y primo,* $I \neq < X_1,\dots,X_n > \Rightarrow V(I)$ *es irreducible.*

Corolario 4.1.4. *Existe una correspondencia biyectiva entre:*

$$\{\textit{Ideales primos homogéneos distintos del ideal irrelevante}\}$$
$$\updownarrow$$
$$\{\textit{Conjuntos algebraicos proyectivos irreducibles}\} = \{\textit{Variedades proyectivas}\}$$

Corolario 4.1.5. *F un polinomio homogéneo no constante,* $F = F_1^{r_1}\dots F_s^{r_s}$, F_i *formas,* $V(F) = V(F_1) \cup \dots \cup V(F_s)$, $I(V(F)) =< F_1,\dots,F_s >$*. En particular,*

$$\{\textit{Polinomios homogéneos irreducibles no constantes}\}$$
$$\updownarrow$$
$$\{\textit{hipersuperficies irreducibles de } \mathbb{P}^n\}$$

Definición 4.1.7. V variedad, $V \neq \emptyset, V \subseteq \mathbb{P}^n$, definimos $\Gamma_h(V) = k[X_1,\dots,X_{n+1}]/I(V)$ (dominio) como el anillo de coordenadas de V. Dado un polinomio $f \in \Gamma(V), f = F + I(V)$, donde $F \in k[X_1,\dots,X_{n+1}]$, diremos que f es una forma si F es una forma.

Ejemplo: $x^2 - y^3 = X^2Z + I(V)$, con $R[X,Y,Z]/ < X^2Z - Y^3, X >$, a pesar de no tener forma de homogéneo en el cociente, si vemos de donde proviene, sí lo es.

Nota 4.1.4. $f + I(V)$ *forma de grado i si existe* $F = F_i$ *tal que* $f = F + I(V)$. $f = F + I(V) = G + I(V)$*, pero* $F = F_1 + F_2, F_1 \notin I(V), F_2 \in I(V), G = G_1 + G_2, G_1 \notin I(V), G_2 \in I(V)$*, pueden tener grados distintos F y G. Si* $F = +I(V) = G + I(V)$*, se tiene* $F - G \in I(V) \Rightarrow F - G = H = \sum H_i \in I(V)$*. Podemos escribir que* $F = G + \sum H_i$*, si tomamos la forma de mayor grado de F que llamamos* F_n*, se cumple que* $F_n = G_n + H_n$*, si* $G_k \neq 0$, $k > n$*, entonces* $G_k \in I(V)$*. Por lo tanto, el grado de una forma está bien definido.*

Ejemplo: $k[X,Y,Z]/ < X - Y >$, y sea $Z^{10} + Z^9X + Z^9Y$ y Z^{10} en el cociente son iguales.

Proposición 4.1.5. *Todo elemento f de* $\Gamma_h(V)$ *se descompone en suma única (salvo orden) de formas.*

Demostración 49. *Existencia:* $f \in \Gamma_h(V) = f_n + \cdots + f_m, f_i$ *de grado i.* $F = F_n + \cdots + F_m + I(V)$.

Unicidad: $f = \sum f_i = \sum g_i \Rightarrow \sum f_i - \sum g_i = 0 \Leftrightarrow \sum F_i - \sum G_i \in I(V)$, *pero* $I(V)$ *es homogéneo, así que podemos escribirlo como* $\sum(F_i - G_i)$, *por lo tanto,* $F_i - G_i \in I(V) \Rightarrow f_i = g_i$.

Nota 4.1.5. $\Gamma_h(V)$ *no se puede interpretar, en genera, como funcionesd* $V \to k$.

Ejemplo: $\mathbb{C}[X,Y,Z]/ < X^2Z - Y^3 >$, $f = X^2 + I = x^2$. Tomamos el punto $[1,1,1] = [2,2,2] \in V, f([1,1,1]) = 1 \neq 4 = f([2,2,2])$.

Definición 4.1.8. $k_h(V) =$ anillo de fracciones de $\Gamma_h(V)$.

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

f_i es de grado i si $f_i = F_i + I(V)$ con F_i de grado i.

Nota 4.1.6. $k \subset k(V) \subset k_h(V)$, *pero en general* $\Gamma_h(V) \not\subseteq k(V)$.

Definición 4.1.9. Dado $z = \frac{f}{g} \in k(V)$, decimos que z está definida en P si $g(P) \neq 0$, i.e, $g = G + I(V), G(P) \neq 0$.

$$O_p(V) = \{z = \frac{f}{g} \in k(V) : z \text{ está definido en } P\}$$

$O_p(V)$ es anillo local, con ideal maximal

$$m_p = \{z = f/g \in O_P(V) \text{ con } f(P) = 0, i.e, f = F + I(V), F(P) = 0\}$$

Nota 4.1.7. $z(P)$ *sí está bien definido en* $O_p(V)$ *i.e,* $z = f/g = f'/g'$, $P = [\vec{u}] = [\vec{v}]$.

$$z(P) = f(\vec{u})/g(\vec{u}) = \frac{f'(\vec{v})}{g'(\vec{v})}$$

Si $T : \mathbb{A}^{n+1} \to \mathbb{A}^{n+1}$ es un cambio (lineal) de coordenadas (base). T induce un cambio de coordenadas proyectivo.

Ejemplo: $T : \mathbb{A}^3 \to \mathbb{A}^3$, con T con matriz [T] [1,1 |] [1,1 |] [|1]

El cambio de base sería [T][X' Y' Z']' = [X Y Z]'. Si V es un conjunto algebraico, $V^T = T^{-1}(V)$ también es un conjunto algebraico, $V = V(I)$,

$$V^T = T^{-1}(V) = V(F_1^T, \ldots, F_r^T >) =< F_1 \circ T, \ldots, F_r \circ T >=< F_1(T_1, \ldots, T_{n+1}), \ldots, F_r(T_1, \ldots, T_{n+1}) >$$

donde $T_i = T(X_i)$.

Ejemplo: $V = V(X^2Z - Y^3), V^T((X' + Y')^2Z' - (X' - Y')^3)$.

Proposición 4.1.6. *Si T es un cambio de coordenadas proyectivo, con $T(Q) = P$, entonces T induce isomorfismos ,*

$$T : k[X_1, \ldots, X_{n+1}] \to k[X'_1, \ldots, X'_{n+1}]$$
$$T : \Gamma_h(V) \to \Gamma_h(V^T)$$
$$T : k(V) \to k(V^T)$$
$$T : O_p(V) \to O_Q(V^T)$$

Sustitución.

4.2. Variedades proyectivas y afines

Recordamos: $\varphi_{n+1} : \mathbb{A}^n \to \mathbb{P}^n$, que manda $(a_1, \ldots, a_n) \mapsto [a_1 : \cdots : a_n : 1]$.

Dado un polinomio $F \in k[X_1, \ldots, X_n]$, definimos $F^* = X_{n+1}^{degF} F(X_1/X_{n+1}, \ldots, X_n/X_{n+1}) \in k[X_1, \ldots, X_{n+1}]$. F^* es homogéneo.

Ejemplo: $F = X^2 - Y^3, F^* = Z^3((X/Z)^2 - (Y/Z)^3) = X^2Z - Y^3$

Definición 4.2.1. Sea $I \subset k[X_1, \ldots, X_n]$,

$$I^* =< F^* | F \in I >$$

Ejercicio 4.20

Nota 4.2.1. *I^* es un ideal homogéneo.*

Definición 4.2.2. Sea $I \subset k[X_1, \ldots, X_n]$, $V \subset \mathbb{A}^n$, $V = V(I)$, definimos $V^* = V_p(I^*)$

Ejemplo: En el caso de hipersuperficies, $V = V(F) \Rightarrow V^* = V(F^*)$, ejercicio 4.19.

Definición 4.2.3. Sea $F \in k[X_1, \ldots, X_{n+1}]$, F homogéneo, $F_* = F(X_1, \ldots, X_n, 1)$. I homogéneo, $I \subseteq k[X_1, \ldots, X_{n+1}]$, $I_* =< F_* | F_* \in I >$. $V = V(I)$ conjunto algebraico proyectivo, $V_* = V_a(I_*)$.

Definición 4.2.4. V^* se llama la clausura proyectiva de V.

Lema 4.2.1.

1. *$V \subset \mathbb{A}^n, \varphi_{n+1}(V) = V^* \cap U_{n+1}$ y $(V^*)_* = V$.*
2. *$V \subset W \subseteq \mathbb{A}^n, V^* \subseteq W^* \subseteq \mathbb{P}^n$.*
3. *$V \subseteq W \subseteq \mathbb{P}^n \Rightarrow V_* \subseteq W_* \subseteq \mathbb{A}^n$.*
4. *$V \subseteq \mathbb{A}^n$ irreducibles, entonces V^* es irreducible.*
5. *$V = \cup V_i$, es descomposición en componentes irreducibles, entonces $V^* = \cup V_i^*$ es descomposición en componentes irreducibles.*

6. V^* *es el menor conjunto algebraico proyectivo que contiene a* $\varphi_{n+1}(V)$, *y por eso se llama clausura proyectiva.*

7. $\emptyset \neq V \subseteq \mathbb{A}^n$, *entonces* V^* *no está contenida en* H_∞, *ni contiene a* H_∞.

8. $V \subseteq \mathbb{P}^n$ *tal que ninguna componente irreducible de* V *está en o contiene a* H_∞, *etnonces* $V_* \subset \mathbb{A}^n$, *pero* $V_* \neq \mathbb{A}^n$ *y* $(V_*)^* = V$.

Proposición 4.2.1. *Existe una correspondencia biyectiva entre*

$$\{\text{Variedades afines distintas del vacío de } \mathbb{A}^n\}$$

$$V^* \updownarrow V_*$$

$$\{\text{ Variedades proyectivas no contenidas en } H_\infty\}$$

Demostración 50. ***Ejercicio***, *en esencia el ejercicio 4.22.*

Nota 4.2.2. $A = k[X_1, \dots, X_n], B = k[X_1, \dots, X_{n+1}]$, *si partimos de un polinomio* $F \in A$, $(F^*)_* = F$, *ya que* $F^* = X_{n+1}^{deg(F)} F(\frac{X_1}{X_{n+1}, \dots, \frac{X_n}{X_{n+1}}})$.

$F \in B, (F_*)^* X_{n+1}^r = F$, *donde* r *es tal que* $F = X_{n+1}^r F'$ *con* $X_{n+1} \not| F'$.

Nota 4.2.3.

$$\mathbb{A}^n \to \mathbb{P}^n$$

$$p \in V \to V^* \ni \varphi_{n+1}(P)$$

$$O_P(V) \quad O_P(V^*)$$

Teorema 4.2.1. *Sea* $V \subset \mathbb{A}^n$ *una variedad afín,* $P \in V$. *Se tienen isomorfismos naturales:*

1. $k(V^*) \cong k(V)$

2. $O_{\varphi_{n+1}(P)}(V^*) \cong O_P(V)$

Demostración 51.

$$\Gamma(V) \stackrel{\alpha}{\leftarrow} \Gamma_h(V^*)$$

$$f_* = F_* + I(V) \leftarrow f = F + I(V^*)$$

Comprobemos que α *está bien definido.* $f = F + I(V^*) = G + I(V^*) \Leftrightarrow F - G \in I(V^*) \Rightarrow (F - G)_* \in I(V) \Rightarrow F_* + I(V) = G_* + I(V)$.

DIAGRAMA

Si $f \neq 0$, *entonces* $\tilde{\alpha}(f) = f_*/1$ *es una unidad.* $\bar{\alpha}(\frac{f}{g}) = \tilde{\alpha}(f) \cdot \tilde{\alpha}(g)^{-1} = \frac{f_*}{g_*}$, *por lo tanto, está bien definido.*

$\bar{\alpha}(\frac{f}{g}) = 0/1 \Rightarrow f_* = 0$ *en* $k(V)$, *por lo tanto también lo es en* $\Gamma(V)$, *y eso implica que* $F_* \in I(V)$, *entonces* $F \in I(V^*) \Rightarrow \frac{f}{g} = \frac{0}{1}$ *en* $k(V^*)$, *así que tenemos la inyectividad.*

Sea $h_1/h_2 \in k(V), h_1 = H_1 + I(V), h_2 = H_2 + I(V)$, consideremos $\bar{H}_1^*, \bar{H}_2^*$, entonces $\frac{\bar{H}_1^*}{\bar{H}_2^*}X_{n+1}^a$, de manera que tienen mismo grado, y habita en $\wr(V^*)$, y entonces $\alpha(\frac{\bar{H}_1^*}{\bar{H}_2^*}X_{n+1}^a) = \frac{h_1}{h_2}$, así que es sobreyectiva.

El apartado 2 es consecuencia de 1, pues DIAGRAMA . La restricción es trivialmente un isomorfismo.

Corolario 4.2.1. $\mathbb{P}^n = \cup_{i=1}^{n+1} U_i$ *con* $U_i : x_i \neq 0$. *Sea* $P \in U_i \cap U_j$, *entonces* $O_{\varphi_i^{-1}(P)}(\underbrace{V \cap U_i}_{V_{*i}}) = O_P(V) = O_{\varphi_j^{-1}(P)}(\underbrace{V \cap U_J}_{V_{*j}})$

Ejemplo: $q = [1:1:1] \in X^2Z - Y^3, O_q(V), V = V(X^2Z - Y^3)$,
$P \in U_1, V_{*1}, O_{(1,1)}(V_1), V_1 = V(Z - Y^3)$.
$P \in U_2, V_{*2}, O_{(1,1)}(V_2), V_2 = V(X^2Z - 1)$.
$P \in U_3, V_{*3}, O_{(1,1)}(V_3), V_3 = V(X^2 - Y^3)$.
Estos espacios son isomorfos por el teorema. Comprobemos:

$O_{(1,1)}(V_1) = O_{(0,0)}(V_1'), V_1' : (Z+1) - (Y+1)^3 = Z + 1 - (Y^3 + 3Y^2 + 3Y + 1) = Y^3 + 3Y^2 + 3Y + Z = H$, $\Gamma(H) = k[Y,Z]/H = k[Y]$, por lo tanto, $k(V_1') = k(Y) \supset O_{(0,0)}(V_1')$.

$O_{(1,1)}(V_2) = O_{(0,0)}(V_2')$, con $V_2' = V((X+1)^2(Z+1)^2 - 1) = V((X^2+2X+1)(Z+1) - 1) = V(X^2Z + 2XZ + Z + X^2 + 2X)$. Se tiene $\Gamma(V_2) = k[X,Z]/ < Z(X^2 + 2X + 1) + X^2 + 2X >$ en el anillo local, $O_{(0,0)}(V_2)$, $Z(X^2 + 2X + 1) = -(X+2)X$, $Z = UX$.

Nota 4.2.4. $m_P(V) = dim(\frac{m'^n}{m'^{n+1}}) = m_{\varphi^{-1}(P)}(\varphi^{-1}(V \cap U_i)), n >> 0, m'$ *ideal maximal de* $O_p(V)$

Capítulo 5

Curvas proyectivas planas

Definición 5.0.1. Una curva proyectiva plana es una clase de equivalencia

$\{$polinomios homogeneos de $k[X,Y,Z]\}/\sim$, donde $F \sim G \Leftrightarrow \exists \lambda \neq 0$ tal que $F = \lambda G$.

Nota 5.0.1. *$P \in F$ y $P \in U_i$, sabemos que $O_P(F) = O_{\varphi_i^{-1}(P)}(F_{*i})$.*

Definición 5.0.2. $m_P(F) = m_{\varphi_i^{-1}(P)}(F_{*i})$ para cualquier carta $P \in U_i$.

Nota 5.0.2. *$m_P(F)$ no depende de la carta U_i y es invariante por cambio de coordenadas proyectivas.*

Ejemplo: $(X^2+Y^2)^3 - 4X^2Y^2Z^2 = F, P = [0:0:1], F_* = F(X,Y,1) = (X^2+Y^2)^3 - 4X^2Y^2$, entonces $m_P(F) = 2$.

Igual que en el caso afín:

$$P \text{ simple} \Leftrightarrow m_P(F) = 1$$

$$P\text{múltiple, singular} \Leftrightarrow m_P(F) > 1$$

Lema 5.0.1. *P es múltiple para $F \Leftrightarrow F(P) = \partial_X F(P) = \partial_Y F(P) = \partial_Z F(P) = 0$.*

Demostración 52. *$F(\lambda X, \lambda Y, \lambda Z) = \lambda^d F(X,Y,Z)$, con $d = deg(F)$. Derivamos respecto a λ, $D(F(\lambda X, \lambda Y, \lambda Z)) = \partial_X F \cdot \frac{d\lambda X}{d\lambda} + \partial_Y F \cdot \frac{d\lambda Y}{d\lambda} + \partial_Z F \cdot \frac{d\lambda Z}{d\lambda} = d\lambda^{d-1}F(X,Y,Z)$.*

Obtenemos: $X\partial_X F + Y\partial_Y F + Z\partial_Z F = d\lambda^{d-1}F(X,Y,Z) = dF(X,Y,Z)$

Supongamos $P = [a:b:1]$, P es múltiple $\Leftrightarrow$ (a,b) es múltiple para $F_*(X,Y) = F(X,Y,1) \Leftrightarrow F_*(a,b) = 0 = F(a,b,1), \underbrace{\partial_X F_*(a,b)}_{\partial_X F(a,b,1)} = 0, \underbrace{\partial_Y F_*(a,b)}_{\partial_Y F(a,b,1)} = 0$. Así que tenemos que $F(a,b,1) = 0, \partial_X F(a,b,1) = 0, \partial_Y F(a,b,1) = 0, \partial_Z F(a,b,1) = 0$.

Si la última coordenada de P es 0, podemos reducir al caso anterior permutando las variables.

Además, si P es simple, tiene una única recta tangente que es $X\partial_X F(P) + Y\partial_Y F(P) + Z\partial_Z F(P) = 0$. $\square$

Ejemplo: $F = XY^4 + YZ^4 + XZ^4$, los puntos singulares tienen de ecuaciones $XY^4 + YZ^4 + XZ^4 = 0, Y^4 + Z^4 = 0, 4XY^3 + Z^4 = 0, 4YZ^3 + 4XZ^3 = 0$.

Si $Z = 0 \Rightarrow Y = 0 \Rightarrow [1 : 0 : 0]$.

Si $Z \neq 0$ lo evaluamos $Z = 1 \Rightarrow XY^4 + Y + X = 0, Y^4 + 1 = 0, 4XY^3 + 1 = 0, Y + X = 0 \Rightarrow$ no tiene solución.

Deshomogeneización por cualquier recta:

Sea $L : a_1X_1 + \cdots + a_{n+1}X_{n+1} = 0$, y $P = [P_1 : \cdots : P_{n+1}] \notin L$, entonces $\tilde{P} = [\frac{P_1}{L(P)} : \cdots : \frac{P_{n+1}}{L(P)}]$, y se tiene que $L(\tilde{P}) = 1$, así que podemos quitar una coordenada, pues podemos escribir $\tilde{P} = [\frac{P_1}{L(P)} : \cdots : \frac{1}{a_{n+1}}(L(P) - \sum(a_i \frac{P_i}{L(P)}))]$, es decir, la última coordenada depende de las demás, y podemos quitarla.

Dados $P_1, \ldots, P_r$ existe una recta proyectiva que no pasa por ninguno. Entonces, si tenemos $O_{P_1}(\mathbb{P}^2), \ldots, O_{P_2}(\mathbb{P}^2)$, y a ellos pertenece $\frac{F}{L^{degF}}$, pero depende de la L escogida.

Nota 5.0.3. $\frac{F}{L^{degF}} = \underbrace{\frac{L'^{degF}}{L^{degF}}}_{Unidad} \frac{F}{L'^{degF}}$

Definimos $F_* = \frac{F}{L^{degF}}$ como la deshomogeneización respecto de la recta L. Y coincide con la deshomogeneización respecto de la última variable. Y así, tiene sentido definir en $\mathbb{P}^n$ a $I(P, F \cap G) = O_P(\mathbb{P}^2)/ < F/L^{degF}, G/L^{degG} >$.

Nota 5.0.4. *Sea* $¶_1, \ldots, P_r \in \mathbb{P}^2$.

- *Existe una recta L tal que $P_i \notin L$, $i = 1, \ldots, r$.*
- *F forma de grado d, $F \in k[X, Y, Z]$, $F/L^d \in O_{p_i}$.*
- *Si L' es otra recta, $P_i \notin L'$, $F/L'^d \in O_{p_i}(\mathbb{P}^2)$ y $F_* = F/L^d = F/L'^d u$ en $O_{p_i}(\mathbb{P}^2)$.*

En el caso particular $L = Z$:

$$F_* = F/Z^d \in k(\mathbb{P}^2) \xrightarrow{\alpha} k(\mathbb{A}^2)$$

$$\alpha(\frac{F(X,Y,Z)}{Z^d}) = F(X,Y,1)/1^d = F_*$$

Sea F una curva irreducible, $P \in F$. Si P es un punto simple, $O_P(F)$ es un anillo de valoración discreta (porque $O_P(F) \cong O_{\varphi_i^{-1}(P)}(F_{*i})$ para toda carta $U_i \ni P$).

Se define el orden:

$$ord_P^F(G) = ord_P^F(G/H) = ord_{\varphi_i^{-1}}^{F_{*i}}(G_{*i}) \text{ para } U_i \ni P$$

, donde H es cualquier forma del mismo grado que G y $H(P) \neq 0$.

$= ord_P^F(\bar{G}_*)$, G_* es la deshomogeneización en $O_P(\mathbb{P}^2)$ y $\bar{G}_*$ la imagen de G_* en $O_P(\mathbb{P}^2)/FO_P(\mathbb{P}^2) = O_P(F)$.

Definición 5.0.3. $I(P, F\cap G) = dim_k(O_P(\mathbb{P}^2)/ < F_*, G_* >)$

Nota 5.0.5. *No es completamente trivial que no depende de la deshomogeneización. Si tenemos* L, L' *tales que* $P \notin L$ *y* $P \notin L'$, *entonces* $dim_k(O_P(\mathbb{P}^2)/ < F/L^{degF}, G/L^{degG} >= dim_k O_P(\mathbb{P}^2/ < F/l'^{degF}, G/L'^{degF} >$.

Corolario 5.0.1.

1. $I(P, F\cap G) \geq 0$ *para todos* $P, F, G; F$ *y* G *con intersección propia.* $I(P, F\cap G) = \infty$ *para todos* $P, F, G; F$ *y* G *sin intersección propia.*
2. $I(P, F\cap G) = 0 \Leftrightarrow P \notin F\cap G$. $I(P, F\cap G)$ *depende sólo de las componentes irreducibles de* F *y* G *que pasan por* P.
3. *Si* T *es un cambio de coordenadas proyectivo, con* $T(Q) = P$, $I(P, F\cap G) = I(Q, F^T \cap G^T)$.
4. $I(P, F\cap G) = I(P, G\cap F)$.
5. $I(P, F\cap G) \geq m_P(F)\cdot m_P(G)$; *y se da la igualdad* $\Leftrightarrow$ F *y* G *no tienen tangentes comunes en* P, *donde la recta* L *es tangente a* F *en* P, *si* $I(P, F\cap L) > m_P(F)$.
6. $F = \prod F_i^{r_i}, G = \prod G_j^{s_j}$, *entonces* $I(P, F\cap G) = \sum r_i s_j I(P, F_i \cap G_j)$.
7. $I(P, F\cap G) = I(P, F\cap G + AF)$ *donde* $A \in k[X, Y, Z]$ *forma de grado* $deg(G) - deg(F)$.
8. *Si* P *es simple para* F, *entonces* $I(P, F\cap G) = ord_P^F(G)$.

Ejercicio: Sean F, G curvas planas proyectivas; si no tienen componentes comunes. Entonces tienen un número finito de puntos de intersección. Idea: Reducir al caso afín.

Ejemplo: Sea $F = X^2Y^3 + X^2Z^3 + Y^2Z^3$. Cálculo de puntos singulares.

$sing(F) = ...$ Se resuelve el sistema:

$$X^2Y^3 + X^2Z^3 + Y^2Z^3 = 0$$

$$2XY^3 + 2XZ^3 = 0$$
$$3X^2Y^2 + 2YZ^3 = 0$$
$$3X^2Z^2 + 3Y^2Z^2 = 0$$

Obteniendo: Si $z = 0 \to P_1 = [1 : 0 : 0], P_2 = [0 : 1 : 0]$, si $z \neq 0 \to P_3 = [0 : 0 : 1]$. Obtenemos sus multiplicidades:

- Como $P_1 \in U_1$, deshomogeneizamos por la X, $F_1 = Y^3 + Z^3 + Y^2Z^3 \Rightarrow m_{p_1}(F) = m_{(0,0)}(F_1) = 3$.
- Como $P_2 \in U_2$, deshomogeneizamos por Y, $F_2 = X^2 + X^2Z^3 + Z^3$, $m_{p_2}(F_2) = 2$.

- Como $P_3 \in U_3$, deshomogeneizamos por Z, $F_3 = X^2Y^3 + X^2 + Y^2$, $m_{p_3}(F_3) = m_{(0,0)}(F_3) = 2$.

Sea $F = Y^2Z - X(X-2Z)(X+Z)$ y $G = Y^2 + X^2 - 2XZ$. Calcular los puntos de intersección, y sus números de intersección. (Irreducible, se puede ver homogeneizando alguna de las variables).

$F \cap G$: Consideramos $Y = 0$ y luego cuando $Y = 1$. Si $Y = 0$, se tiene que $-X(X-2Z)(X+Z) = 0$ y $X^2 - 2X = 0$, quedando así $P_1 = [0:0:1], P_2 = [2:0:1]$, que son solución de F y G. Ahora veamos si $Y = 1$, obtenemos $Z - X(X-2Z)(X+Z) = 0$, y $1 + X^2 - 2XZ = 0$, obteniendo del sistema $Z = X/-2, X = +-i\frac{\sqrt{2}}{2}$, obteniendo así dos puntos más P_3 y P_4.

Falta calcular los números de intersección.

$P_1 \subset U_3, Z = 1$, $I(P_1, F \cap G) = I(0, F_* \cap G_*) = I(0, Y^2 - X(X-2)(X+1) \cap Y^2 + X^2 - 2X) = I(0, Y^2 - X(X-2)(X+1) \cap Y^2 + X(X-2)) = I(0, F_* + (X+1)G_* \cap G_*) = I(0, \underbrace{Y^2 + (X+1)Y^2}_{Y^2 \underbrace{(X+2)}_{unidad, O_P(\mathbb{A})=Y^2}} \cap Y^2 + X(X-2)) = I(0, Y^2 \cap Y^2 + X(X-2)) = I(0, Y^2 \cap X(X-2)) = 2$

P_2, consideramos en U_3 el punto $(2,0)$. $I((2,0), F_* \cap G_*) \underbrace{=}_{T(X,Y)=(X+2,Y)} I(0, F_*(X+2,Y) \cap G_*(X+2,Y)) = I(0, Y^2 - (X+2)X(X+3) \cap Y^2 + X(X+2)) = I(0, H_1 \cap H_2) = I(0, H_1 + (X+3)H_2 \cap H_2) = I(0, Y^2(X+4) \cap H_2 - Y^2) = I(0, Y^2 \cap X(X+2)) = I(0, Y^2 \cap X) = 2$.

Por el teorema de Bézout, $deg(F)deg(G) = \sum_{i=1}^{4} I(P_i, F \cap G) \Rightarrow I(P_3, F \cap G) = 1, I(P_4, F \cap G) = 1$.

5.1. Teorema de Bézout

Teorema 5.1.1. *Sean F, G dos curvas proyectivas planas sin componentes comunes. Entonces*

$$\sum_P I(P, F \cap G) = degF \cdot degG$$

Corolario 5.1.1. *Si F, G no tienen componentes comunes, entonces*

$$\sum_P m_P(F) \cdot m_P(G) \leq deg(F) \cdot deg(G)$$

Corolario 5.1.2. *Si el grado de F es m y el grado de G es n y se cortan en un número de puntos igual a $m \cdot n$, entonces se cortan en exáctamente en mn puntos y todos los puntos de corte son simples.*

Corolario 5.1.3. *Si F y G tienen más de mn puntos comunes, entonces tienen una componente común.*

Ejercicios 5.20,5.21,5.22

5.2. Sistemas lineales de curvas

Se pretende estudiar todas las curvas proyectivas planas de grado d. Hay exáctamente $N = \frac{(d+1)(d+2)}{2} = dim(V(d,3))$, monomios de grado d en X, Y, Z, y fijamos un orden.

$$M_1, \ldots, M_N$$

Nota 5.2.1. *Existe una biyección entre curvas proyectivas de grado d y el conjunto de puntos proyectivos de* $\mathbb{P}^{N-1}$. *Que lleva* $a_1M_1 + \cdots + a_NM_N \leftrightarrow [a_1 : \cdots : a_N]$.

Ejemplo: Sea $aX^2 + bXY + cXZ + dY^2 + eYZ + fZ^2$, y se identifica con el punto $[a : b : c : d : e : f] \in \mathbb{P}^5$.

Lema 5.2.1.

1. *El conjunto de curvas de grado d que pasan por un punto P es un hiperplano de* $\mathbb{P}^{d(d+3)/2}$.
2. *Si* $T : \mathbb{P}^2 \to \mathbb{P}^2$ *es un cambio de coordenadas proyectivo, entonces* $F \mapsto F^T$ *es un cambio de coordenadas.*

Demostración 53.

1. *Sea* $P = [a : b : c]$, *y consideramos la curva* $U_1M_1 + \cdots + U_NM_N$, *el punto P pertenece a la curva si y sólo si* $U_1M_1(a,b,c) + \cdots + U_NM_N(a,b,c) = 0$, *que es un hiperplano.*
2. $T : \mathbb{P}^2 \to \mathbb{P}^2$, $T = (T_1, T_2, T_3)$, *polinomio de grado 1. Entonces,* $M_i^T = M_i(T_1, T_2, T_3) = \sum_j \lambda_{i,j} M_j$.

   La transformación $F \mapsto F^T$, *mandamos* $[a_1 : \cdots : a_N] \mapsto (\lambda_{ij})$, *invertible porque T tiene inversa.*

□

Sea $V(d, r_1P_1, \ldots, r_nP_n)$ el conjunto de curvas de grado d tales que la multiplicidad de la curva en el punto P_i es mayor o igual que r_i.

Teorema 5.2.1.

1. $V(d, r_1P_1, \ldots, r_nP_n)$ *es una variedad proyectiva de dimensión mayor o igual que* $\frac{d(d+3)}{2} - \sum \frac{r_i(r_i+1)}{2}$.
2. *Si* $d \geq (\sum r_i) - 1$, *entonces se da la igualdad.*

Demostración 54. *1. Consideramos $V(d, rP)$. Tomo T un cambio de coordenadas de manera que, $p = [0:0:1]$ y por tanto, $F = \sum F_i(X,Y)Z^{d-i}$. $m_P(F) \geq r \Leftrightarrow m_0(F_*) \geq r \Leftrightarrow F_0 = \cdots = F_{r-1} = 0$, por lo tanto, $V(d, rP) = \{U_1 = \cdots = U_{r(r+1)/2} = 0\}$, y eso implica que $dim(V(d; rP) = dim\{U_1 = \cdots = U_{r(r+1)/2} = 0\} = \frac{d(d+3)}{2} - \frac{r(r+1)}{2}$.*

$V(d, r_1P_1, r_2P_2) = V(d, r_1P_1) \cap V(d, r_2P_2)$, entonces $dim(d, r_1P_1, r_2P_2) \geq \frac{d(d+3)}{2} - \frac{r_1(r_1+1)}{2} - \frac{r_2(r_2+1)}{2}$, y se itera el argumento para la generalización. □

Ejercicio 5.17

Parte III

Problemas a entregar

Capítulo 6

Problemas a entregar

6.1. Problemas 30 de Septiembre

6.1.1. Problema 1.4

Sea** k **un cuerpo infinito,** $F \in k[x_1, \ldots, x_n]$**. Supongamos que** $F(a_1, \ldots, a_n) = 0, \forall (a_1, \ldots, a_m) \in k^n$**. Hay que probar que** $F = 0$**.

Solución:

Demostramos por reducción al absurdo:

Supongamos que $F \neq 0$, entonces existiría algún $(a_1, \ldots, a_n) \in k^n$ tal que $F(a_1, \ldots, a_n) \neq 0$. Sea $n = 1$ con $F \neq 0$. El grado de F es mayor o igual al número de raíces de F. Como el grado es finito, las raíces son finitas. Luego, como k es un cuerpo infinito, tiene elementos que no son raíces de F, lo que entra en contradicción con que $F(a) = 0, \forall a \in k$.

Suponemos que es cierto para cualquier $m \leq n-1$. Sea $n \geq 2$, entonces $F = \sum_{i=1}^{n} F_i x_n^i$, donde $F_i \in k[x_1, \ldots, x_{n-1}]$, como $F \neq 0$ entonces se tiene que existe F_i tal que $F_i \neq 0$. Por la hipótesis de inducción existirá $a_1, \ldots, a_{n-1}$ tal que $F_i(a_1, \ldots, a_{n-1}) \neq 0$. Por lo tanto, $F(a_1, \ldots, a_{n-1}, x_n)$ es un polinomio en $k[x_n]$, y como demostramos antes para $n = 1$, debe existir a_n tal que $F(a_1, \ldots, a_{n-1}, a_n) \neq 0$.

6.1.2. Problema 1.7

Sea** k **un cuerpo,** $F \in k[x_1, \ldots, x_n], a_1, \ldots, a_n \in k$**. Probar:

1. $F = \sum \lambda_{(i)}(x_1 - a_1)^{i_1} \ldots (x_n - a_n)^{i_n}, \lambda_{(i)} \in k$
2. ***Si** $F(a_1, \ldots, a_n) = 0$**, probar** $F = \sum_{i=1}^{n}(x_i - a_i)G_i$ **con** $G_i \in k[x_1, \ldots, x_n]$*

Solución:

1. Se demuestra por inducción. Sea $n = 1$, $F \in k[x_1]$, por el algoritmo de la división en $k[x_1]$ se tiene $F = \sum \lambda_{(i)}(x_1 - a_1)^i$, con $\lambda_{(i)} \in k$. Se supone cierpo para $n = r$. Sea $F \in k[x_1, \ldots, x_{r+1}]$ ($k[x_1, \ldots, x_{r+1}]$ es isomorfo a $k[x_1, \ldots, x_r][x_{r+1}]$), entonces se tiene por el algoritmo de la división en $k[x_1, \ldots, x_r][x_{r+1}]$ que:

$$F = \sum G_{(i)}(x_{r+1} - a_{r+1})^i, \text{ con } G_{(i)} \in k[x_1, \ldots, x_r]$$

Como era cierto para r, aplicándolo a cada $G_{(i)}$, se tiene:

$$F = \sum \lambda_{(i)}(x_1 - a_1)^{i_1} \cdots (x_{r+1} - a_{r+1})^{i_{r+1}} \text{ con } \lambda_{(i)} \in k$$

2. Por el apartado 1, sabemos que $F = \sum \lambda_{(i)}(x_1 - a_1)^{i_1} \ldots (x_n - a_n)^{i_n}$, con $\lambda_{(i)} \in k$. Como $F(a_1, \ldots, a_n) = 0$, se tiene en particular para $i_j = 0 \forall j = 1, \ldots, n$ que $\lambda_{(i)} = 0$. Por lo tanto, $\exists j$ tal que $i_j \neq 0$, y esto último implica que podemos sacar el factor $(x_j - a_j)$ y reagrupar la suma, quedando

$$F = \sum_{i=1}^{n} (x_i - a_i) G_i \text{ con } G_i \in k[x_1, \ldots, x_n]$$

6.1.3. Problema 1.14

Sea** F **un polinomio no constante,** $F \in k[x_1, \ldots, x_n]$**,** k **algebraicamente cerrado. Prueba que** $\mathbb{A}^n \backslash V(F)$ **es infinito si** $n \geq 1$**, y** $V(F)$ **es infinito si** $n \geq 2$**. Concluye que el complementario de cualquier conjunto algebraico es infinito.

Solución:

k es algebráicamente cerrado, es decir, todo polinomio tiene al menos una raíz. k es infinito, y eso implica que $\mathbb{A}^n$ tambien lo es. Supongo que $\mathbb{A}^n \backslash V(F)$ es finito, y tomo $f \in k[x_1, \ldots, x_n]$ tal que $V(f) = \mathbb{A}^n(k) \backslash V(F)$. Añado entonces los elementos del conjunto algebraico $V(F)$ a $V(f) \Rightarrow V(f) \cap V(F) = V(fF) = \mathbb{A}^n(k)$. Pero hemos visto en una de las propiedades de los conjuntos algebraicos que $V(fF) = \mathbb{A}^n(k) \Leftrightarrow fF = 0$, luego $(f = 0) \vee (F = 0)$ lo cual es imposible, pues F no es constante, y $f \neq 0$.

¿$V(F)$ es infinito? Tomamos, $F(a_1, \ldots, a_{n-1}, x) \in k[x]$, como k es infinito y algebraicamente cerrado, tenemos que para cada elemento de la forma $a_1, \ldots, a_{n-1}$ existirá $a \in k$ en el que F se anula. La cantidad de elementos de la forma $a_1, \ldots, a_{n-1}$ es infinito, así que $V(F)$ es infinito.

Como $\mathbb{A}^n \backslash V(F)$ es infinito siendo $V(F)$ infinito, se tiene la finitud de los complementarios.

Nota 6.1.1. *Teniamos dos posibilidades, quitar un conjunto finito de puntos a un conjunto infinito, que claramente es infinito; y quitar infinitos puntos a otro conjunto infinito, que hemos demostrado que en este caso es infinito.*

6.1.4. Problema 1.15

Sea $V \subset \mathbb{A}^n(k), W \subset \mathbb{A}^m(k)$***, conjuntos algebraicos. Prueba que***

$$V \times W = \{(a_1, \ldots, a_n, b_1, \ldots, b_m) | (a_1, \ldots, a_n) \in V, (b_1, \ldots, b_m) \in W\}$$

es un conjunto algebraico en $\mathbb{A}^{n+m}(k)$***. Se llama producto de V y W.***
Solución:

Sabemos que un conjunto algebraico se puede expresar como conjunto algebraico de un ideal, por ello tomamos $V = V(I)$ y $W = V(J)$, con $I \subset k[x_1, \ldots, x_n]$ y $J \subset k[x_1, \ldots, x_m]$ ideales. Construimos dos ideales a partir de I y J, de manera que:

$$V(I') = \{(a_1, \ldots, a_n, 0, \ldots, 0) | (a_1, \ldots, a_n) \in V(I)\} \subset \mathbb{A}^{n+m}$$
$$V(J') = \{(0, \ldots, 0, b_{n+1}, \ldots, b_{n+m}) | (b_{n+1}, \ldots, b_m \in V(J)\} \subset \mathbb{A}^{n+m}$$
$$I' + J' = \{f + g | f \in I', g \in J'\}, I' \cap J' = \emptyset$$

Luego tenemos que $V(I' + J') = V \times W$, y como $V(I' + J')$ es un conjunto algebraico, $V \times W$ tambien lo es.

6.1.5. Problema 1.20

Demuestra que para cualquier ideal I ***en*** $k[x_1, \ldots, x_n], V(I) = V(\sqrt{I})$***, y*** $\sqrt{I} \subset I(V(I))$
Solución:

$$V(I) = V(\sqrt{I})$$

$\boxed{\subseteq}$ $a \in V(I) \Rightarrow f(a) = 0 \forall f \in I \Rightarrow f^m(a) = 0 \forall f \in I \Rightarrow f \in \sqrt{I} \Rightarrow a \in \sqrt{I}$.
$\boxed{\supseteq}$ $a \in V(\sqrt{I}) \Rightarrow f(a) = 0 \forall f \in \sqrt{I} \Rightarrow a \in V(I)$. La última implicación se debe a que $I \subseteq \sqrt{I}$, ya que por definición $I \ni f = f^1 \Rightarrow f \in \sqrt{I}$.

6.1.6. Problema 1.21

Prueba que $I = (x_1 - a_1, \ldots, x_n - a_n) \subset k[x_1, \ldots, x_n]$ ***es un ideal maximal, y que el homomorfismo natural*** $\varphi : k \to k[x_1, \ldots, x_n]/I$ ***es un isomorfismo.***
Solución:

Si I no fuera maximal, existiría un ideal J tal que $I \subset J \subset k[x_1, \ldots, x_n]$. $I =< x_1 - a_1, \ldots, x_n - a_n >$. Sea $f \in J$ tal que $f \notin I$, entonces f no debería poder expresarse como combinación de elementos del tipo $x_i - a_i$, pero eso entra en contradicción con el problema 1.7.

Hay que probar que φ es un isomorfismo, es decir, que es un homomorfismo biyectivo. Como I es un ideal maximal, se tiene que A/I es un cuerpo, y sabemos que todo homomorfismo entre cuerpos es inyectivo. Falta probar que es sobreyectivo, pero es trivial que todo elemento de A/I tiene anti-imagen por φ.
$\sqrt{I} \subseteq I(V(I) \Rightarrow I(V(I)) = I(V(\sqrt{I})) \supset \sqrt{I}$.

6.2. Problemas 7 Octubre

6.2.1. Problema 1.22

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

1. ***Prueba que cada ideal** J' **de** R/I**,**$\pi^{-1}(J') = J$ **es un ideal de** R **que contiene a** I**, y para cada ideal** J **de** R **que contiene a** I**,** $\pi(J) = J'$ **es un ideal de** R/I**. Esto construye una correspondencia natural uno a uno entre ideales de** R/I **e ideales de** R **que contienen** I**.***

2. ***Prueba que** J' **es radical si y solo si** J **es radical. Análogamente para ideales primos y maximales.***

3. ***Prueba que** J' **está finitamente generado si** J **lo está. Concluye que** R/I **es Noetheriano si** R **lo es. Cualquier anillo de la forma** $k[X_1, \ldots, X_n]/I$ **es Noetheriano.***

Solución:

$$\pi : R \to R/I$$
$$a \mapsto a + I$$

1. Como J' es un ideal, se cumple que $\forall a \in R/I$, $\forall b \in J'$, $ab \in J'$. π es sobreyectiva, asi que tiene sentido que hablemos de anti-imagen, lo que nos lleva a $J \ni \pi^{-1}(ab) = \underbrace{\pi^{-1}(a)}_{\in R}\underbrace{\pi^{-1}(b)}_{\in J} \Rightarrow J$ ideal. ¿$I \subset J$? Supongamos que existe $a \in I$ tal que $a \notin J$, y sea $b \in J$. Entonces $J \ni ab \in I$, pues I y J son ideales, $\to\leftarrow$. Como π es homomorfismo, mantiene las operaciones y sigue siendo subgrupo respecto la suma.

   Finalmente, $I \subset J \subset R$ ideal, sean $a \in R$, $b \in J$, $ab \in J \Rightarrow \pi(ab) = \underbrace{\pi(a)}_{\in R/I}\underbrace{\pi(b)}_{\in J'} \in J'$, entonces J' ideal.

2. Tenemos por hipótesis $\sqrt{J'} = J'$. Recordemos que $\sqrt{J} = \{a \in R : a^m \in J, m > 0\}$. $J \subset \sqrt{J}$ por la propiedad probada en clase, demostremos la contención contraria.

$a \in \sqrt{J} \Rightarrow \pi(a) \in \sqrt{J'} \Rightarrow \pi(a) \in J' \Rightarrow a \in J$. La implicación contraria la tenemos de manera análoga.

J' ideal primo $\Leftrightarrow$ J ideal primo. Sea J primo, $a \cdot b \in J' \Rightarrow \pi^{-1}(ab) \in J \Rightarrow \pi^{-1}(a)\pi^{-1}(b) \in J \Rightarrow \pi^{-1}(a) \vee \pi^{-1}(b) \in J$ pues J es primo $\Rightarrow (a' \in J) \vee (b \in J')$. La implicación contraria es análoga.

J' ideal maximal $\Leftrightarrow$ J ideal maximal. Sea J' ideal maximal, entonces no existe ningún ideal que lo contenga contenido en R/I. Supongo que existe L ideal tal que $J \subset L \subset R \Rightarrow$ ¿$J' \subset L' = \pi^{-1}(L)$? $a \in J' \Rightarrow \pi^{-1}(a) \in J \Rightarrow \pi^{-1}(a) \in L \Rightarrow a \in L' \Rightarrow J' \subset L' \rightarrow\leftarrow$. La implicación contraria es análoga.

3. Hay que probar que J finitamente generado implica que J' es finitamente generado. Como J es finitamente generado, entonces $\exists f_i, i = 1, \ldots, n$ tales que $J =< f_1, \ldots, f_n >$, y tales que $\forall f \in J, f = \sum \lambda_i f_i, \lambda_i \in \mathbb{R}$. Por lo tanto, sea $g \in J'$, como π es sobreyectiva, g tiene anti-imagen en J, es decir, $\pi^{-1}(g) \in J \Rightarrow \pi^{-1}(g) = \sum \lambda_i f_i \rightarrow \forall g \in J', g = \pi(\sum \lambda_i f_i) = \sum \lambda_i \underbrace{\pi(f_i)}_{\in J'}$.

Nota 6.2.1. *Al tomar $\pi^{-1}(a)$ nos referimos a tomar un representante del conjunto.*

6.3. Problemas 14 de Octubre

6.3.1. Problema 1.38

Sea $R = k[x_1, \ldots, x_n]$, k algebraicamente cerrado, $V = V(I)$. Prueba que hay una correspondencia biyectiva entre subconjuntos algebraicos de V e ideales radicales en $k[x_1, \ldots, x_n]/I$, y que conjuntos algebraicos irreducibles tienen correspondencia con ideales primos. Así como los puntos a ideales maximales.

Solución:

Por el *corolario 1.7.1* existe una correspondencia biyectiva entre ideales radicales y conjuntos algebraicos. Es la correspondencia dada por las aplicaciones I y V.

Por el *teorema de los ceros* tenemos que en k algebraicamente cerrado, $IV(I) = \sqrt{I}$. Pretendemos unir ambos resultados al *problema 1.22*, y así demostrar lo que nos piden.

Sea π el homomorfismo natural que se define en el *problema 1.22*, es decir $\pi : R \rightarrow R/I$. Sea J un ideal que contiene a I, entonces se tiene que $V(J) \subset V(I)$, es decir, todo subconjunto algebráico de V es de esa forma con ideales que contienen a I. Así que tenemos las mismas condiciones que el *problema 1.22*, y podemos decir que $\pi(I(V(J)) \xrightarrow{\pi} J'$ es radical, pues por el *teorema de los ceros* tenemos que $I(V(J)) = \sqrt{J}$, y por tanto, $J' = \sqrt{J'}$ por aplicación directa del problema. Así que tenemos la composición de correspondencias biyectivas, obteniendo la correspondencia biyectiva que deseabamos.

Demostremos la correspondencia entre conjuntos algebraicos irreducibles e ideales primos. Sea V un conjunto algebraico irreducible, $I(V)$ es un ideal primo, si aplicamos π tenemos por el problema ya mencionado que se hereda la propiedad "primo" de los ideales.

De manera análoga, tenemos que la correspondencia biyectiva lleva puntos en ideales maximales (*Corolario 1.7.3*).

6.3.2. Problema 1.44

Prueba que $L = K(X)$ ***(el cuerpo de funciones racionales en una variable) es una extensión de cuerpos finitamente generada de*** K***, pero*** L ***no es un k-álgebra finitamente generada sobre*** K***.***

Solución:

Recordemos los conceptos clave para el ejercicio:

L es una **extensión finitamente generada** de K si $L = k(v)$ para un cierto $v \in L$.

L es un **k-álgebra finitamente generada** sobre K si $L = K[v] = \{\sum a_{(i)}v^i | a_{(i)} \in K\}$ para algún $v \in L$.

Demostremos el primer aserto, el cuerpo de funciones racionales en una variable es el cuerpo de fracciones del dominio de integridad K, y es claro que es una extensión, falta ver que es finitamente generada. $L = k(x) = \{\frac{f}{g} : f, g \in k[x], g \neq 0\}$, si tomamos cualquier α, $L = \{\frac{f(\alpha)}{g(\alpha)} : f, g \in k[\alpha], g(\alpha) \neq 0\}$.

Ahora, supongamos que L es un k-álgebra finitamente generada, entonces $\exists f_1, \ldots, f_r$ tales que $k(x) = k[f_1, \ldots, f_r]$. La contención $\boxed{\supseteq}$ se tiene de manera trivial. Veamos la contención contraria: Sea $\frac{f}{g} \in K(x)$, elemento cualquiera. Si estuvieran generados por $f_1, \ldots, f_r$, tomando $h \in k[x]$ el mínimo común múltiplo de los denominadores de los generadores, $\frac{f}{g} \cdot h^n$ debe pertenecer a $K[x]$ para algún n. Pero siempre podemos tomar $f = 1$ y $g = c$ con c tal que $c \not| h$ y, por lo tanto, no está generado por ellos y no tenemos la contención.

6.3.3. Problema 1.45

Sea R ***un subanillo de*** S***,*** S ***un subanillo de*** T***.***

1. Si $S = \sum Rv_i, T = \sum Sw_j$, prueba que $T = \sum Rv_iw_j$.
2. Si $S = R[v_1, \ldots, v_n], T = S[w_1, \ldots, w_m]$, prueba que $T = R[v_1, \ldots, v_n, w_1, \ldots, w_m]$
3. Si R, S, T son cuerpos, y $S = R(v_1, \ldots, v_n)$, $T = S(w_1, \ldots, w_m)$, prueba que $T = R(v_1, \ldots, v_n, w_1, \ldots, w_m)$.

Solución:

1. $\sum Sw_j = \sum(\sum Rv_i)w_j = \sum Rv_i w_j$.

2. $R[v_1, \dots, v_n][w_1, \dots, w_m] \cong R[v_1, \dots, v_n, w_1, \dots, w_m]$.

3. $R(v_1, \dots, v_n) = \{\frac{f(v_1,\dots,v_n)}{g(v_1,\dots,v_n)} : f, g \in R[x_1, \dots, x_n], g(v_1, \dots, v_n) \neq 0\}, S(w_1, \dots, w_m) = \{\frac{f(w_1,\dots,w_m)}{g(w_1,\dots,w_w)} : f, g \in S[x_1, \dots, x_m], g(w_1, \dots, w_m) \neq 0\} = \{\frac{f(v_1,\dots,v_n,w_1,\dots,w_m)}{g(v_1,\dots,v_n,w_1,\dots,w_w)} : f, g \in R[x_1, \dots, x_n, y_1, \dots, y_m], g(v_1, \dots, v_n, w_1, \dots, w_m) \neq 0\} = R(v_1, \dots, v_n, w_1, \dots, w_m)$

6.3.4. Problema 1.49

Sea** K **un cuerpo,** $L = K(X)$ **el cuerpo de las funciones racionales en una variable sobre** K**. Probar:

1. ***Que cualquier elemento de** L **que sea entero sobre** $K[X]$ **está en** $K[X]$**.***

2. ***Que no existe ningún elemento no nulo** $F \in K[X]$ **tal que cada** $z \in L, F^n z$ **es entero sobre** $K[X]$ **para algún** $n > 0$**.***

Solución:

1. Sea $z \in L$, z entero sobre $K[X]$, entonces existe un polinomio mónico que se anula en z. Es decir, tenemos $z^n + a_1 z^{n-1} + \dots = 0$. Como $z \in L = K(X) \Rightarrow z = \frac{f}{g}$, tomamos f y g primos relativos. $(\frac{f}{g})^n + a_1(\frac{f}{g})^{n-1} + \dots = 0 \Rightarrow f^n + a_1 f^{n-1} g + \dots = 0 \Rightarrow f^n = g(a_1 f^{n-1} + \dots) \Rightarrow g|f \Rightarrow z \in K[X]$.

2. Sea $z = \frac{1}{G}$ donde G es un polinomio irreducible que no divide a F. Para cualquier F existe G que cumpla esas condiciones, por lo tanto, no existe F que cumpla lo pedido. Además, aplicando el *ejercicio 1.44* pues no pertenece $F^n z$, y si no pertenece no puede ser entero.

6.3.5. Problema 1.50

Sea** K **un subcuerpo de un cuerpo** L**.

1. ***Prueba que el conjunto de los elementos de** L **que son algebraicos sobre** K **es un subcuerpo de** L **que contiene a** K**.***

2. ***Supón que** L **es** K**-módulo finitamente generado, y** $K \subset R \subset L$**. Prueba que** R **es un cuerpo.***

Solución:

1. La proposición y corolario de la sección 1.9 se pueden extender a cuerpos y la demostración de este ejercicio sería inmediata, pero procederemos con otra estrategia. Sea $v \in L$ algebraico sobre K, entonces existe un polinomio mónico $v^n + a_1 v^{n-1} + \cdots + a_n = 0$, si $a_n \neq 0$, entonces tendríamos $-a_n = v(v^{n-1}a_1 + \dots)$, por lo tanto, $v|a_n$, de ahí se deduce la contención $K \subset T$,

   con $T = \{$ elementos de L algebraicos sobre $K\}$.

2. Como L es K-módulo finitamente generado, tenemos $L = \sum K l_i$ con $l_i \in L$, es decir, todos los elementos de L serán combinaciones de elementos de L y K, y como R está contenido en L, sus elementos también estarán expresados de la misma manera y, por lo tanto, hereda las propiedades de los cuerpos de L.

Nota 6.3.1. *Un elemento es algebraico en un cuerpo si es raiz de un polinomio con coeficientes en el cuerpo.*

6.4. Problemas 20 de Octubre

6.4.1. Problema 2.2

Sea $V \subset \mathbb{A}^n$ una variedad afin. Una subvariedad de V es una variedad $W \subset \mathbb{A}^n$ que está contenida en V. Prueba que existe una correspondencia biyectiva entre subconjuntos algebraicos (respectivamente subvariedades y puntos) de V e ideales radicales (respectivamente ideales primos e ideales maximales) de $\Gamma(V)$.

Solución:

Este problema se resuelve por aplicación directa del *problema 1.38*. Por dicho problema sabemos que existe una correspondencia uno a uno entre subconjuntos algebraicos (las variedades son casos particulares) e ideales radicales de $k[\vec{x}]/I$, que es lo primero que tenemos que demostrar.

Por otro lado, por el mismo problema sabemos que conjuntos algebraicos irreducibles tienen correspondencia biyectiva con ideales primos, y una subvariedad es un subconjunto algebraico irreducible.

Además, también sabemos que los puntos tienen una correspondencia biyectiva con ideales maximales.

Todo fue demostrado en el *problema 1.38*, pues $\Gamma(V) = \frac{k[x_1,\dots,x_n]}{I(V)}$.

6.4.2. Problema 2.7

Si $\varphi : V \to W$ es una aplicación polinómica, y X es un subconjunto algebraico de W, prueba que $\varphi^{-1}(X)$ es un subconjunto algebraico de V. Si $\varphi^{-1}(X)$ es irreducible, y X está contenido en la imagen por φ. Probar que X es irreducible. Ésto da un test para la irreducibilidad.

Solución:

Como X es un conjunto algebraico, $X = V(I)$ con I un ideal contenido en $\Gamma(W)$. Sea $f \in I$, entonces $\tilde{\varphi}(f) \in \Gamma(V)$, además, $\tilde{\varphi}(I) = J$ con J ideal, formado por la imagen de los polinomios de I por $\tilde{\varphi}$. Por lo tanto, $X = V(I) \Rightarrow \varphi^{-1}(X) = V(J)$, es decir, un subconjunto algebraico de V.

Ahora, si φ^{-1} es irreducible y X está contenido en la imagen de φ, tenemos que $k[V]/J \cong K[W]/I$ (pues φ es biyectiva al ser sobreyectiva y $\varphi(\varphi^{-1}(X)) \subset X$)$\Rightarrow k[W]/I$ es un dominio de integridad si y sólo si $k[V]/J$ lo es, y de ahí se deduce la irreducibilidad.

6.4.3. Problema 2.9

Sea $\varphi : V \to W$ una aplicación polinómica de variedades. Sean $V' \subset V, W' \subset W$ subvariedades. Supón que $\varphi(V') \subset W'$. Probar que $\tilde{\varphi}(I_W(W')) \subset I_V(V')$. Probar también que la restricción de φ da una aplicación polinómica de V' a W'.

Solución:

Sabemos que $I_W(W') = \{f \in \Gamma(W) : f(P) = 0, \forall p \in W'\}$, de manera análoga $I_V(V') = \{f \in \Gamma(V) : f(p) = 0, \forall p \in V'\}$. Hay que probar que $\tilde{\varphi}(I_W(W')) \subset I_V(V')$, sabiendo que $\varphi(V') \subset W'$. Sabemos del *problema 2.3* que toda aplicación polinómica en una variedad, restringe en una subvariedad suya.

Basta probar que dado $f \in I_W(W')$, se cumple que $f \circ \varphi \in I_V(V')$.

$f(P') = 0, \forall P' \in W'$, y $\forall P \in V', \varphi(P) \in W' \Rightarrow f(\varphi(P)) = 0, \forall p \in V' \Rightarrow f \circ \varphi \in I_V(V')$.

Ahora tenemos que probar que la restricción de φ da una aplicación polinómica de V' a W'. φ es una función polinómica de V en W, entonces $\exists F \in k[x_1, \ldots, x_n], \varphi(P) = F(P), \forall P \in V$, por el *problema 2.3* podemos restringirlo a V' y seguiría siendo aplicación polinómica, y como $\varphi(V') \subset W'$, tenemos que $\varphi_{|V'} : V' \to W'$ es una aplicación polinómica.

6.4.4. Problema 2.12

Sea $\varphi : \mathbb{A}^1 \to V = V(Y^2 - X^3) \subset \mathbb{A}^2$ definida por $\varphi(t) = (t^2, t^3)$. Probar que, a pesar de ser φ una aplicación polinómica uno a uno, φ no es un isomorfismo.

Solución:

Por la *proposición 2.2.1*, sabemos que dos variedades son isomorfas si y sólo si sus anillos de coordenadas lo son. Luego, ¿$\Gamma(\mathbb{A}^1) \cong \Gamma(V)$?

$$\varphi : \mathbb{A}^1 \to V$$
$$t \to (t^2, t^3)$$
$$\tilde{\varphi} : \underbrace{\Gamma(V)}_{k[T^2,T^3]} \to \underbrace{\Gamma(\mathbb{A}^1)}_{k[T]}$$
$$f = f(t) \to f(t^2, t^3)$$

Luego, tenemos que $\Gamma(V) = k[T^2, T^3] \subset K[T] = \Gamma(\mathbb{A}^1)$, que claramente no son isomorfos.

***Sea** $\varphi : \mathbb{A}^1 \to V = V(Y^2 - X^2(X+1))$ **definida por** $\varphi(t) = (t^2 - 1, t(t-1))$. **Prueba que** φ **es biyectiva excepto para** $\varphi(\pm 1) = (0, 0)$.*

Solución:

Es claro que la inyectividad falla para los valores 1 y -1, así que quitemos esos puntos del dominio y veamos la biyectividad.

Es equivalente a ver que $\Gamma(\mathbb{A}^1) \cong k[x] = \Gamma(V) = \frac{k[x,y]}{V(Y^2 - X^2(X+1))}$. Debido a que X e Y están al cuadrado teníamos el problema con los valores ± 1, pero sin ellos podemos expresar Y en función de X, y con ello tenemos el isomorfismo. Por lo tanto, φ es biyectiva.

6.5. Problemas 28 de Octubre

6.5.1. Problema 2.35

(a) Probar que existen** $d+1$ **monomios de grado** d **en** $R[X,Y]$**, y** $\frac{(d+1)(d+2)}{2}$ **monomios de grado** d **en** $R[X,Y,Z]$**.

Solución:

Primero tenemos que ver que existen $d+1$ monomios de grado d en $R[X,Y]$, es decir, elementos del tipo X^iY^j tales que $i+j=d$. Es claro que hay $d-1$ valores distintos de d para el índice j para el que $j\neq 0$, y luego queda sumar los dos casos que faltan de tener monomios del tipo X^d e Y^d.

Ahora tenemos que probar que existen $\frac{(d+1)(d+2)}{2}$ monomios de grado d en $R[X,Y,Z]$, es decir, $X^iY^jZ^k$ tales que $i+j+k=d$ con $i,j,k\in\{0,\dots,d\}$. Sea $F\in R[X,Y,Z]$ que sea un monomio. Entonces tenemos que $F*\in R[X,Y]$ también es un monomio, y existen $d+2$ posibles, pues hay que contemplar el caso X^0Y^0, ahora, homogeneizando, tendríamos $d+1$ valores para la potencia de Z. Por lo tanto, si construyeramos una tabla con los valores que obtenemos, solo nos quedamos con la mitad de ellos, quedando $\frac{(d+1)(d+2)}{2}$ monomios. También podemos verlo como el combinatorio $\binom{d+1}{2}$.

(b) Sea** $V(d,n)=\{$ **formas de grado** d **en** $k[X_1,\dots,X_n]\}$**,** k **un cuerpo. Probar que** $V(d,n)$ **es un espacio vectorial sobre** k**, y que los monomios de grado** d **constituyen una base.** $dimV(d,1)=1; dimV(d,2)=d+1, dimV(d,3)=\frac{(d+1)(d+2)}{2}$**.

Solución:

Hay que ver que $V(d,n)$ es un espacio vectorial. La demostración es muy sencilla:

Para ello basta ver que $\forall\lambda,\mu\in k,\forall f_1,f_2\in V(d,n)$ se tiene que $\lambda f_1+\mu f_1\in V(d,n)$, que es trivial pues las formas de mismo grado al sumarlas mantienen el grado, y el producto por escalares no afecta al grado.

Veamos que los monomios de grado d forman base:

Sea $f=X_1^{i_1}\cdot X_n^{i_n}$ tal que $\sum_{j=1}^n i_j=d$ un monomio de grado d. Es claro que la suma de monomios es sistema generador pues las formas pueden expresarse como suma de monomios del mismo grado. Basta ver que forman base, es decir, la independencia lineal, que se tiene por la independencia de las X_i.

(c) Sean** $L_1,L_2,\dots$ **y** $M_1,M_2,\dots$ **sucesiones de formas lineales en** $k[X,Y]$**, y supóngase que es** $L_i=\lambda M_j,\lambda\in k$**. Sea** $A_{ij}=L_1L_2\cdots L_iM_1M_2\cdots M_j, i,j\geq 0$**. Probar que** $\{A_{ij}|i+j=d\}$ **forma una base de** $V(d,2)$**.

Solución:

Cada A_{ij} es un monomio de grado d, y por el apartado anterior sabemos que forman base, pues hay $d+1$ elementos A_{ij} distintos.

6.5.2. Problema 2.37

¿Cuáles son las identidades para la suma y el producto en el anillo $\prod R_i$***?¿Es la aplicación*** φ ***de*** R_i ***a*** $\prod R_j$ ***que lleva a*** a_i ***a*** $(0,\ldots,a_i,\ldots,0)$ ***un homomorfismo de anillos?***

Solución:

El elemento neutro para la suma es $(0,\ldots,0)$, mientras que el elemento identidad para el producto es $(1,\ldots,1)$.

La aplicación no es un homomorfismo de anillos, pues:

- $\varphi(a_i+b_i)=(0,\ldots,a_i+b_i,0,\ldots,0)=\varphi(a_i)+\varphi(b_i)$.
- $\varphi(a_ib_i)=(0,\ldots,a_ib_i,0,\ldots,0)=\varphi(a_i)\varphi(b_i)$.
- $\varphi(1_{R_i})\neq 1_{\prod R_j}$

6.5.3. Problema 2.38

Probar que si $k\subset R_i$***, y cada*** R_i ***es de dimensión finita sobre*** k***, entonces*** $dim(\prod R_i)=\sum_i dim(R_i)$***.***

Solución:

Para probar esto simplemente vamos a formar una base y contar los elementos que tiene:

$$\lambda_1(a_1,0,\ldots,0)+\cdots+\beta_{dimR_1}(a_{dimR_1},0,\ldots,0)+\cdots+\beta_1(0,\ldots,0,b_1)+\cdots+\beta_{dimR_n}(0,\ldots,0,b_{dimR_n})$$

Es claro que hay $\sum dimR_i$ sumandos, y forma base porque está formada por la suma disjunta de bases de cada R_i.

6.6. Problemas 4 de Octubre

6.6.1. Problema 2.28

Una función φ de K sobre $\mathbb{Z} \cup \infty$, que satisfaga:

- $\varphi(a) = \infty \Leftrightarrow a = 0$.
- $\varphi(ab) = \varphi(a) + \varphi(b)$
- $\varphi(a + b) \geq min(\varphi(a), \varphi(b))$

Se llamará una función de orden sobre el cuerpo K. Probar que $R = \{z \in K : \varphi(z) \geq 0\}$ es un anillo de valoración discreta cuyo ideal maximal es $m = \{z : \varphi(z) > 0\}$, y cuyo cuerpo cociente es K. Recíprocamente, probar que si R es un anillo de valoración discreta con cuerpo de fracciones K, entonces la función orden es una función orden sobre K. Dar un anillo de valoración discreta con cuerpo cociente K es lo mismo que definir una función orden sobre K.

Solución:

Para probar que R es un anillo de valoración discreta, tenemos que ver que se cumple:

1. R anillo.
2. M ideal maximal.
3. Unicidad de M como ideal maximal.
4. R Noetheriano.

1. R anillo:

a) $(R, +)$ grupo abeliano. Es trivial comprobarlo, pues los elementos de R son elementos de K, así que cumplen las propiedades de grupo. Además, la suma es una operación interna para R, pues si $a \in R, b \in R \Rightarrow \varphi(a + b) \geq 0 \Rightarrow a + b \in R$.

b) $a(bc) = (ab)c$ se cumple. Pues son elementos de K

c) $a(b + c) = ab + ac$ también se cumple. Pues son elementos de K.

d) $1 \in R$, pues $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) + \varphi(1) \Rightarrow \varphi(1) = 0 \geq 0$.

2. M ideal maximal.

Primero comprobemos que es un ideal: es subgrupo de $(R, +)$, y es cerrado para el producto: $a \in R, b \in M \Rightarrow \varphi(ab) = \underbrace{\varphi(a)}_{\geq 0} + \underbrace{\varphi(b)}_{>0} > 0$.

Veamos que es maximal, pero para eso basta ver que el único elemento de R que no está en M, es aquel que tiene imagen por φ igual a 0, es decir, las unidades de R. Aplicando el lema de la sección de funciones racionales y anillos locales, eso implica que R posee un ideal maximal único que contiene a todo ideal propio de R.

3. Se tiene del apartado anterior.

4. R Noetheriano: Como existe M ideal maximal que contiene a todos los ideales propios. Podemos construir una cadena ascendente de ideales, de manera que se estabiliza en M, y eso implica que R es Noetheriano. También se puede deducir porque K es el menor cuerpo que contiene a R, y es algebraicamente cerrado y, por lo tanto, R es finitamente generado.

La función *ord* es una función de orden sobre K:

$$ord(0) = ord(ut^n, \text{ para cualquier } n) = \infty$$

$$ord(ab) = ord(a) + ord(b) = ord(ut^n ut^m) = ord(ut^{n+m}) = n + m$$

$$ord(a+b) = ord(ut^n + ut^m) = ord(ut^m(t^{n-m} + 1)) = ord(ut^m) + ord(t^{n-m} + t^0) = m + ord(t^{n-m} + 1) \geq m = min(ord(a), ord(b))$$

6.6.2. Problema 2.29

Sea** R **un anillo de valoración discreta con cuerpo de fracciones** K**, y se designa con ord, la función orden de** K**.

1. ***Si** $ord(a) < ord(b)$**, probar que** $ord(a+b) = ord(a)$**.***
2. ***Si** $a_1, \dots, a_n \in K$**, y para algún i,** $ord(a_i) < ord(a_j), \forall i \neq j$**, entonces** $a_1 + \cdots + a_n \neq 0$**.***

Solución:

1. $ord(a) = n, ord(b) = m, n < m \Rightarrow ord(a+b) = ord(ut^n + ut^m) = ord(ut^n(1 + t^{m-n})) = ord(ut^n) + ord(\underbrace{1 + t^{m-n}}_{(*)}) = n.$

   $(*) 1 + t^{m-n} = ut^s$ para un cierto s, y t no unidad $\Rightarrow t^s | (1 + t^{m-n}) \Rightarrow s = 0$

2. Si $ord(a_i) < ord(a_j), \forall j \neq i \Rightarrow ord(a_i) < ord(\sum_{j \neq i} a_j) \Rightarrow ord(\underbrace{a_1 + \cdots + a_n}_{ut^s}) = ord(a_i + \sum_{j \neq i} a_j) = ord(a_i) \Rightarrow s = ord(a_i) \Rightarrow ut^s \neq 0 \Rightarrow a_1 + \cdots + a_n \neq 0.$

6.6.3. Problema 2.30

Sea** R **un AVD cuyo ideal maximal sea** M**, y cuerpo de fracciones** K**, y supóngase que un cierto cuerpo** k **es un subanillo de** R**,y que la composición** $k \to R \to R/M$ **es un isomorfismo de** k **con** R/M**. Verificar las siguientes afirmaciones:

1. ***Para todo** $z \in R$**, existe un número** $\lambda \in k$**,único, tal que** $z - \lambda \in M$**.***

2. ***Sea** t **un parámetro de uniformización para** R**,** $z \in R$**. Entonces para todo** $n \geq 0$ **existen** $\lambda_0, \lambda_1, \ldots, \lambda_n \in k$ **y** $z_n \in R$ **tales que** $z = \lambda_0 + \lambda_1 t + \cdots + \lambda_n t^n + z_n t^{n+1}$**, y son únicos.***

Solución:

1. $k \xrightarrow{i} R \xrightarrow{\pi} R/M$, y denotamos $\varphi = i \circ \pi$. Como φ es biyectiva, sabemos que π debe ser inyectiva e i debe ser sobreyectiva. Por lo tanto, sea $z \in R$ tiene sentido tomar $\pi(z)$, y debe existir $\tilde{\lambda}$ tal que $\pi(z) - \tilde{\lambda} = 0$ que es equivalente a que pertenezca a M. Empleamos la imagen inversa de φ, obteniendo $\varphi^{-1}(\pi(z) - \tilde{\lambda}) = \varphi^{-1}(0) \Rightarrow \varphi^{-1}(\pi(z)) - \underbrace{\varphi^{-1}(\lambda)}_{\lambda} = 0 \Rightarrow \lambda = \varphi^{-1}(\pi(z))$, y es único por las propiedades de las funciones empleadas.

2. Existencia: Para $n = 0$, por el apartado anterior tenemos que existe λ tal que $z = \lambda$. Suponemos cierto para n y lo probarmos para $n+1$. Como es cierto para n, tenemos:
$$z = \lambda_0 + \lambda_1 t + \cdots + \lambda_n t^n + z_n t^{n+1}$$
Podemos expresar $z_n = \lambda_{n+1} + z_{n+1} t$, por lo tanto, tenemos:
$$z = \lambda_0 + \lambda_1 t + \cdots \lambda_{n+1} t^{n+1} + z_{n+1} t^{n+2}$$
que es lo que queríamos probar.
Unicidad: Lo deducimos por reducción al absurdo, si no fueran únicos, se tendría que
$$z = \lambda_0 + \lambda_1 t + \cdots + \lambda_n t^n + z_n t^{n+1}$$
$$z = \beta_0 + \beta_1 t + \cdots + \beta_n t^n + \bar{z}_n t^{n+1}$$
Restando ambas expresiones:
$$0 = (\lambda_0 - \beta_0) + \cdots (z_n - \bar{z}_n) t^{n+1}$$
pero por el problema 2.29, sabemos que si algún sumando fuera distinto de 0, tendríamos un elemento cuyo orden minoraría los demás y la suma sería distinta de cero y llegaríamos a contradicción.

6.6.4. Problema 2.52

Sean** N, P **submódulos de un módulo** M**. Probar que el subgrupo** $N + P = \{n + p : n \in N, p \in P\}$ **es submódulo de** M**. Probar que existe un isomorfismo natural entre** $R-$**módulos de** $N/N \cap P$ **sobre** $(N+P)/P$**.

Solución:

Para probar que $N+P$ es submódulo de M basta probar que es subgrupo abeliano y que $\forall a \in N+P, \forall b \in M, ab \in N+P$.

Es claro que es subgrupo abeliano pues se verifican todas las propiedades, y se tiene que $\forall a \in N+P, a = a_N + a_P, ab = \underbrace{a_N b}_{\in N} + \underbrace{a_P b}_{\in P} \in N+P$.

Para probar que $N/N \cap P$ y $(N+P)/P$ son isomorfos aplicaremos el primer teorema de isomorfía. Sea $f : N \to (N+P)/P$, donde f es la inmersión de N en $N+P$ tomando clases en P, $ker(f) = \{a : a \in N, f(a) \in P\}$, es decir, aquellos elementos de N, que también están en P, $ker(f) = N \cap P$. Por lo tanto, tenemos el isomorfismo.

6.7. Problemas 2 de Diciembre

6.7.1. Lema

Si F y G tienen tangentes distintas en P, entonces $I^t \subset (F,G)O$ para $t \geq m+n-1$

Demostración 55. *Sean $L_1,\ldots,L_m$ las tangentes a F en P, $M_1,\ldots,M_n$ las tangentes a G en P. Sea $L_i = L_m$ si $i > m$, $M_j = M_n$ si $j > n$, y sea $A_{ij} = L_1 \cdot \cdots \cdot L_i \cdot M_1 \cdot \cdots \cdot M_j$ para todo $i, j \geq 0$, se define $A_{00} = 1$. Por el problema 2.35, apartado (c) (entregado el día 28 de Octubre), tenemos que el conjunto $\{A_{ij} : i+j = t\}$ constituye una base del espacio vectorial de todas las formas de grado t de $k[X,Y]$, que tiene dimensión $t+1$, pues los monomios del tipo X^iY^{t-i}, para $0 \leq i \leq t$ forman una base de dicho espacio.*

Por lo tanto, para demostrar que el ideal $I^t \subset (F,G)O$ basta probar que los A_{ij} que forman base pertenecen a $(F,G)O$ para todo $t = i+j \geq m+n-1$ (I^t es el ideal formado por los elementos X^t, Y^t de $K[X,Y]$). La desigualdad $i+j \geq m+n-1$ implica que o bien $i \geq m$ o que $j \geq n$.

Sin pérdida de generalidad, supongamos que $i \geq m$, entonces $A_{ij} = A_{m0}B$, donde B es una forma de grado $t = i+j-m$. COmo A_{m0} es F_m, podemos escribir $F = A_{m0} + F'$, donde todos los términos de F' son de grado mayor o igual que $m+1$, es decir, F' es un polinomio en I^{m+1},. Entonces, $A_{ij} = BF - BF'$, pues $A_{ij} = B(A_{m0} + F') - BF' = BF' - BF' + BA_{m0} = BA_{m0}$, donde cada uno de los términos de BF' tiene grado mayor o igual que $i+j+1$ (suma de los grados de B y F'). Habremos terminado si podemos probar que $I^t \subset (F,G)O$ para todo t suficientemente grande.

Este hecho es consecuencia del "teorema de los ceros": sea $V(F,G) = \{P, Q_1,\ldots,Q_s\}$, y elijamos un polinomio H tal que $H(Q_i) = 0, H(P) \neq 0$ (está definido en P), que podemos tomarlo por el problema 1.17. Se tiene que $HX, HY \in I(V(F,G))$, pues si $P = (0,0)$, ambos se anulan en él, por lo tanto por el "teorema de los ceros", se tiene que $(HX)^N, (HY)^N \in < F,G > \subset k[X,Y]$ para un cierto N. Como $H(P) \neq 0$, $\frac{1}{H} \in O$, así que $\frac{1}{H^N}(HX)^N = X^N \in (F,G)O$, luego $X^N, Y^N \in (F,G)O$, pues para Y^N se razona de manera análoga, y se tiene que $I^{2N} \subset < X^N, Y^N \subseteq (F,G)O$, ya que si $X^aY^b \in I^{2N}$, entonces $a+b \geq 2N$, y así $(a \geq N) \vee (b \geq N)$ □

Nota 6.7.1. $O = O_P(\mathbb{A}^2)$.

ψ es inyectiva si y sólo si F y G poseen tangentes distintas en P.

Demostración 56. *Supongamos que las tangentes son distintas y que $\psi(\bar{A},\bar{B}) = \overline{AF+BG} = 0$, es decir, que $AF+BG$ consta exclusivamente de términos de grado mayor o igual que $m+n$. Escribamos $A = A_r +$ términos de grado superior, $B = B_s + \ldots$, luego $AF+BG = A_rF_m + B_sG_n + \ldots$. Entonces debe ser $r+m = s+n$ y $a_rF_m = -B_sG_n$. Pero F_m y G_n no tienen factores comunes, luego F_m divide a B_s, y G_n dvide a A_r. Por lo tanto, $s \geq m, r \geq n$, y en consecuencia $(\bar{A},\bar{B}) = (0,0)$.*

Recíprocamente, si L fuese una tangente común a F y a G en P, se tendría $F_m = LF'_{m-1}$, $G_n = LG'_{n-1}$ *para ciertas formas* F'_{m-1} *y* G'_{n-1}. *Pero entonces* $\psi(\bar{G'_{n-1}}, \bar{F'_{m-1}}) = FG'_{n-1} - F'_{m-1}G$, *los grados menores cancelan, pues* $F_m G'_{n-1} = F'_{m-1}LG'_{n-1} = F'_{m-1}G_n$, *como cada término tiene grado al menos* $m+n$, *se tiene* $\psi(\bar{G'_{n-1}}, \bar{F'_{m-1}}) = 0$, *y por lo tanto* ψ *no es inyectiva.* □

6.7.2. Propiedad 8

Si P es un punto simple de F, entonces $I(P, F \cap G) = ord_P^F(G)$.

Demostración 57. *Podemos suponer que F es irreducible. Si g es la imagen de G en* $O_P(F)$, *entonces* $ord_P^F(G) = dim_k(O_P(F)/ < g >)$ *por el problema 2.50, apartado c. Como* $O_P(F)/ < g >$ *es isomorfo a* $O_P(\mathbb{A}^2)/ < F, G >$ *por el problema 2.44, y esta dimensión es* $I(P, F \cap G)$.

Nota 6.7.2.
- ***Problema 2.50:*** *Sea R un anillo de valoración discreta, si* $z \in R$ *entonces* $ord(z) = dim_k(R/ < z >)$.

6.7.3. Propiedad 9

Si F y G no poseen componentes comunes, entonces $\Sigma_P I(P, F \cap G) = dim_k(k[X, Y]/ < F, G >)$.

Demostración 58. *Como* $V(F, G)$ *es finito, por el corolario 1 de la proposición 6 de la sección 2.9, se tiene que*

$$dim_k(k[X, Y]/ < F, G >) = \sum_{i=1}^{N} dim_k(O_i/(F, G)O_i) = \sum_P dim_k(O_P(\mathbb{A}^2)/ < F, G >) =$$

$$= \sum_i I(P, F \cap G)$$

6.7.4. Problema 3.19

Una recta L es tangente a la curva F en el punto P si y sólo si $I(P, F \cap L) > m_p(F)$.

Solución:

Por la propiedad 5, tenemos que $I(P, F \cap L) \geq m_P(F) \underbrace{m_P(L)}_{=1} = m_P(F)$, y se alcanzaba la igualdad si no tenian tangentes comunes, es decir, que si la desigualdad es estricta, deben tener tangentes comunes, y al ser L una recta, ésta tiene que ser tangente a F en P.

6.8. Problemas 9 Diciembre

6.8.1. Lema

1. $V \subset \mathbb{A}^n$,entonces $\varphi_{n+1}(V) = V^* \cap U_{n+1}$ y $(V^*)_* = V$.

2. $V \subset W \subseteq \mathbb{A}^n$, entonces $V^* \subseteq W^* \subseteq \mathbb{P}^n$. Si $V \subseteq W \subseteq \mathbb{P}^n \Rightarrow V_* \subseteq W_* \subseteq \mathbb{A}^n$.

3. $V \subseteq \mathbb{A}^n$ irreducible, entonces V^* es irreducible.

4. $V = \cup_i V_i$, es descomposición en componentes irreducibles, entonces $V^* = \cup_i V_i^*$ es descomposición en componentes irreducibles.

5. V^* es el menor conjunto algebraico proyectivo que contiene a $\varphi_{n+1}(V)$, y por eso se llama clausura proyectiva.

6. $\emptyset \neq V \subseteq \mathbb{A}^n$, entonces V^* no está contenida en H_∞, ni contiene a H_∞.

7. $V \subseteq \mathbb{P}^n$ tal que ninguna componente irreducible de V está en o contiene a H_∞, entonces $V_* \subset \mathbb{A}^n$, pero $V_* \neq \mathbb{A}^n$ y $(V_*)^* = V$.

Demostración 59. 1. *$\varphi_{n+1}(V) = V^* \cap U_{n+1}$, lo demostramos por doble contención:*

$\boxed{\supseteq}$ *Los elementos de $V^* \cap U_{n+1}$ son del tipo $[x_1 : \cdots : x_n : x_{n+1}]$ con $x_{n+1} \neq 0$, esto es debido a que $\mathbb{P}^n \supset U_{n+1} = \{[x_1 : \cdots : x_{n+1}] \in \mathbb{P}^n : x_{n+1} \neq 0\}$. Por otro lado, V^* es la homogeneización de V, es decir, $V^* = V(I^*)$ con $I^* =< F^* : F \in I >$ (I^* ideal homogéneo), sabiendo que $V = V(I)$ para I un cierto ideal. Por lo tanto, tomando los representantes de la forma $[\frac{x_1}{x_{n+1}} : \cdots : \frac{x_n}{x_{n+1}} : 1]$ demostramos la inclusión.*

$\boxed{\subseteq}$ *$\varphi_{n+1}(V)$ tiene elementos del tipo $[x_1 : \cdots : x_n : 1]$, luego está contenido en U_{n+1}. Por otro lado, si $V^* = V(I^*)$, se tiene que cada polinomio $F^* \in I^*$ procede de un polinomio $F \in I$, y si evaluamos la última coordenada x_{n+1} en 1, mantienen los mismos puntos algebraicos, es decir, si $F((a_1, \ldots, a_n)) = 0$, entonces $F^*([a_1 : \cdots : a_n : 1]) = 0$, por lo tanto, aquellos elementos de V^* que tienen la última coordenada distinta de 0, proceden de elementos de V, y tenemos la contención.*

Falta probar que $(V^*)_* = V$, pero para ello basta ver que como $V = V(I)$, $V = \{P : F(P) = 0, \forall F \in I\}$, y que además, $V^* = V(I^*)$ con una definición análoga. Y por la proposición 5 de la sección 2.6 sabemos que $(F^*)_* = F$, así que tienen los mismos puntos en los conjuntos algebraicos.

2. *Sea $V = V(I), W = V(J)$ para I, J ideales. Entonces $J \subseteq I$, por lo que $J^* \subseteq I^*$, y como V invierte inclusiones, se tiene que $V(J^*) \supseteq V(I^*) \Rightarrow V \subseteq W$. De manera análoga, $J \subseteq I$, por lo que $J_* \subseteq I_*$, lo que implica que $V_* \subseteq W_*$.*

3. *Sea F una forma e $I = I(V)$, entonces $F \in I^* \Leftrightarrow F_* \in I$. Ésto se tiene ya que $F_* \in I \Leftrightarrow X_{n+1}^r(F_*)^* = F \in I^*$. Sabemos que V es irreducible si y sólo si $I(V)$ es un ideal primo, así que basta probar que I^* es primo. Entonces, $FG \in I^* \Leftrightarrow (FG)_* = F_* \cdot G_* \in I \Leftrightarrow (F_* \in I) \vee (G_* \in I) \Leftrightarrow (F \in I^*) \vee (G \in I^*)$.*

4. *Se sigue de los apartados (2), (3) y (5). Como $V = \cup_i V_i$, $V_i \subset V$, por lo que aplicando (2) tenemos que $V_i^* \subset V^*$. Por otro lado, cada V_i^* es irreducible por el apartado (3), así que $\cup_i V_i^* \subseteq V^*$. Falta ver la igualdad, pero se tiene por el apartado (5), pues V^* es el menor conjunto algebraico que contiene a $\varphi_{n+1}(V)$, por lo que es el menor que contiene a la inclusión de V en $\mathbb{P}^n$, así mismo, ésto es aplicable a cada V_i^* y V_i, así que $\cup V_i^*$ es el menor conjunto que contiene $\cup V_i$, y por lo tanto que contiene a V, y eso implica la igualdad.*

5. *Por el apartado (1), tenemos que $\varphi_{n+1}(V) \subseteq V^*$, falta probar que es el menor. Sea W un conjunto algebraico de $\mathbb{P}^n$ tal que $\varphi_{n+1}(V) \subseteq W$. Si $F \in I(W)$, como $I(W) \subseteq I(\varphi_{n+1}(V))$, entonces se tiene que $F_* \in I(V)$, por lo tanto como vimos en la demostración (3), $F = X_{n+1}^r(F_*)^* \in I(V)^* \subseteq I(V^*)$, así $I(V^*) \supseteq I(W) \Rightarrow V^* \subseteq W$.*

6. *Supongamos que V es irreducible, si no lo fuera se podría descomponer y valdría una prueba análoga. $\boxed{V^* \not\subset H_\infty}$, ya que por (1) tenemos que $\varphi_{n+1}(V) = V^* \cap U_{n+1}$ y $V \neq \emptyset$, entonces $\varphi_{n+1}(V) \neq \emptyset$, es decir, hay elementos de V^* que no están en H_∞. Si $V^* \supset H_\infty$, entonces $I^* = I(V)^* \subset I(V^*) \subset I(H_\infty) =< X_{n+1} >$. Pero como $V \neq \emptyset$, entonces existe $F \neq 0$ tal que $F \in I(V)$, por lo que $F^* \in I^*$, con $F^* \notin < X_{n+1} >$. Así que $\boxed{V^* \not\supset H_\infty}$.*

7. *Al igual que en el apartado anterior, podemos suponer que V es irreducible. Como $\varphi_{n+1}(V_*) \subset V$, basta probar que $V \subset (V_*)^*$, o que $I(V_*)^* \subset I(V)$, pues I invierte las inclusiones. Sea $F \in I(V_*)$. Entonces $F^N \in I(V)_*$ para algún N, así que $X_{n+1}^t(F^N)^* \in I(V)$ para algún t (proposición 5 (3) de la sección 2.6). Pero $I(V)$ es primo al ser V irreducible, y $X_{n+1} \notin I(V)$ ya que $V \notin H_\infty$, así que $F^* \in I(V)$.*

6.8.2. Problema 4.19

Si $I =< F >$ es el ideal de una hipersuperficie afín, probar que $I^* =< F^* >$.
<u>*Solución:*</u>

Por definición, $I^* =< F^* : F \in I >$, pero I está generado solo por F. Por lo tanto $I^* =< F^* >$.

6.8.3. Problema 4.20

Sea $V = V(Y - X^2, Z - X^3) \subset \mathbb{A}^3$**. Probar:**
(a) $I(V) =< Y - X^2, Z - X^3 >$.
(b) $ZW - XY \in I(V)^* \subset k[X, Y, Z, W]$, **pero** $ZW - XY \notin< (Y - X^2)^*, (Z - X^3)^* >$.
Solución:

(a) Sea $F \in I(V)$, entonces debe cumplir que $F(P) = 0, \forall P = (\alpha, \beta, \gamma) \in V$, es decir, $\beta - \alpha^2 = 0$, y que $\gamma - \alpha^3 = 0$. Por lo tanto, podemos escribir F como:

$$F = F_1(Y - X^2) + F_2(Z - X^3) + F_3$$

con $F_1 \in k[X, Y, Z]$, $F_2 \in k[X, Z]$ y $F_3 \in k[X]$. Como debe cumplir la relación antes mencionada, $F_3(\alpha) = 0$, para cualquier α que anule en los sumandos previos. Por lo tanto, $F \in< Y - X^2, Z - X^3 >$.

(b) Como $Z - XY = Z - X^3 - X(Y - X^2)$, se tiene que $Z - XY \in I(V)$ y, por lo tanto, $ZW - XY \in I(V)^*$. Por otro lado, si $ZW - XY \in< (Y - X^2)^*, (Z - X^3)^* >$, se debe cumplir que

$$ZW - XY = \alpha(YW - X^2) + \beta(ZW^2 - X^3)$$

para $\alpha, \beta \in k[X, Y, Z, W]$. Pero por el grado,$\beta$ debería ser 0 y α ser constante $\rightarrow\leftarrow$.

6.8.4. Problema 4.22

Supongamos que V **es una variedad en** $\mathbb{P}^n$ **y** $V \supseteq H_\infty$**. Probar que** $V = \mathbb{P}^n$ **o** $V = H_\infty$**. Si** $V = \mathbb{P}^n, V_* = \mathbb{A}^n$**, mientras que si** $V = H_\infty, V_* = \emptyset$**.**
Solución

Como $H_\infty \subset V$, entonces todos los elementos del tipo $[x_1 : \cdots : x_n : 0]$ están en V. Hay dos posibilidades, que $V \cap U_{n+1} = \emptyset$, lo que implica que $V = H_\infty$, o que $V \cap U_{n+1} \neq \emptyset$, entonces existe $P \in V$ tal que $P_{n+1} \neq 0$, el subíndice denota la coordenada de P. Por lo tanto, si $P = [y_1 : \cdots : y_{n+1}, P/P_{n+1} = [y_1/y_{n+1} : \cdots : 1] \in V$, y como H_∞ contiene todas los elementos posibles con 0 en la última coordenada, podemos obtener una base $[1 : 0 : \cdots : 0], \ldots, [0 : \cdots : 0 : 1]$ de $\mathbb{P}^n$, y así $V = \mathbb{P}^n$.

Sea $V = \mathbb{P}^n \Rightarrow V = V(< 0 >) \Rightarrow V_* = V(0) = \mathbb{A}^n$. Si $V = H_\infty$, entonces $V = V(< X_{n+1} >) \Rightarrow V_* = V(k[\vec{X}]) = \emptyset$.

6.8.5. Desigualdad del cono para $V = \emptyset$

Contraejemplo o demostración de las igualdades sobre el Cono afín asociado a una variedad proyectiva cuando V es el vacío.
Solución:
Si $V = \emptyset$, entonces $C(V) = \{(0, \ldots, 0)\}$. Por lo tanto, ¿$I_a(C(V)) = I_p(\emptyset)$? Por un lado, $I_a(C(V)) = I_a(\{(0, \ldots, 0)\}) =< X_1, \ldots, X_n >$, e $I_p(\emptyset) = k[X_1, \ldots, X_{n+1}]$.

6.9. Problemas 19 Diciembre

6.9.1. Problema 4.25

Sea $P = (x, y, z) \in \mathbb{P}^2$**.**

1. **Probar que** $\{(a, b, c) \in \mathbb{A}^3 | ax + by + cz = 0\}$ **es un hiperplano de** $\mathbb{A}^3$**.**
2. **Probar que para todo conjunto finito de puntos de** $\mathbb{P}^2$**, existe una recta que no pasa por ninguno de ellos.**

<u>*Solución:*</u>

1. Viene dado por una ecuación, y será un hiperplano si tiene dimensión $n-1$, con $n = 3$. Pero sabemos que la dimensión viene dada por $n-$número de ecuaciones. Por lo tanto, es un hiperplano.
2. Lo demostramos por reducción al absurdo. Supongamos que existe un conjunto finito de puntos $\mathcal{P} = \{p_1, \ldots, p_n\}$ tal que cada línea en $\mathbb{P}^2$ interseca con $\mathcal{P}$. Entonces algún p_i es solución de cada ecuación $aX + bY + cZ + d = 0$ con $a, b, c, d \in K$. Dada esa ecuación, supongamos que $p_i = [X_i, Y_i, Z_i]$ es una raíz. Si tomamos otro término independiente d', $aX_i + bY_i + cZ_i + d' \neq 0$. Sin embardo, debe existir j tal que p_j cumpla que $aX_j + bX_j + cZ_j + d' = 0$. Así, tomamos para cada $p \in \mathcal{P}$ su respectivo término independiente. Por lo tanto, si pudieramos tomar un $d^{(n)}$ distinto a los anteriores llegaríamos a contradicción. Supongamos que no podemos, entonces K sería finito y eso entra en contradicción con que K es un cuerpo algebraicamente cerrado, y por lo tanto, infinito.

6.9.2. Ejercicio 5.4

Sea P **un punto simple de** F**. Probar que la recta tangente a** F **en** P **es** $F_X(P)X + F_Y(P)Y + F_Z(P)Z = 0$**.**

<u>*Solución:*</u>

Sea $P = (P_1, P_2, P_3)$. Para demostrarlo, emplearemos la ecuación de la tangente en el caso afín, así como la identidad de Euler. Por la identidad de Euler, tenemos que $dF = XF_X + YF_Y + ZF_Z$, si evaluamos en P, que es un punto de la curva, se tiene que $P_3F_Z(P) = -P_1F_X(P) - P_2F_Y(P)$. Ahora, mediante la ecuación de la recta tangente en el afín, deshomogeneizando, es decir, tomando $F(X, Y, Z) \to F(X/Z, Y/Z, 1)$:

$$F_X(P)(X - \frac{P_1}{P_3}) + F_Y(P)(Y - \frac{P_2}{P_3}) = 0$$

y homogeneizando:

$$F_X(P)(X - \frac{P_1}{P_3}Z) + F_Y(P)(Y - \frac{P_2}{P_3}Z) = 0$$

Y, por lo tanto, el coeficiente de Z será $\frac{P_1 F_X(P)+P_2 F_Y(P)}{-P_3}$, que por la identidad de Euler, habíamos determinado que ésto era igual a $F_Z(P)$, y finalmente, se tiene la recta tangente.

6.9.3. Ejercicio 5.5

Sea $P = [0 : 1 : 0]$, F una curva de grado n, $F = \sum F_i(X,Z)Y^{n-i}$, F_i una forma de grado i. probar que $m_P(F)$ es el menor m tal que $F_m \neq 0$, y los factores de F_m determinan las tangentes de F en P.

Solución:

Se tiene que $F = F_0 Y^n + F_1 Y^{n-1} + \cdots + F_n$, $P \in U_2$, por lo tanto, podemos deshomogeneizar por la segunda variable, obteniendo $\tilde{F} = F_0 + \cdots + F_n$, así, como $m_P(F) = m_P(\tilde{F})$, por definición, $m_P(F) = m_P(\tilde{F}) = m$, siendo F_m la menor (en grado) forma no nula.

Como estámos en un cuerpo algebraicamente cerrado, F_m descompone en factores lineales, es decir, $F_m = \prod_{i=1}^{m} L_i$, faltaría ver que esos factores son las rectas tangentes a F en P, pero como estamos en el afín al haber deshomogeneizado, son esas.

6.9.4. Ejercicio 5.6

Para cualquier $F, P \in F$, probar que $m_P(F_X) \geq m_P(F) - 1$.

Solución: Como $XF_X = \lambda F$, y sea $F = \sum F_i$ su descomposición en formas. Y sea F_m la forma de menor grado distinta de 0. Entonces:

- Si $F_{m_X} \neq 0$, entonces tenemos $m_P(XF_X) = m_P(X) + m_P(F_X) = 1 + m_P(F_X) = m_P(F) \Rightarrow m_P(F_X) = m_P(F) - 1$.
- Si $F_{m_X} = 0$, entonces tenemos que $m_P(XF_X) = m_P(X) + m_P(F_X) > m_P(F) \Rightarrow m_P(F_X) > m_P(F) - 1$.

Juntando ambas obtenemos lo que queríamos probar.

6.9.5. Ejercicio 5.7

Probar que dos curvas planas sin componentes comunes intersecan en un número finito de puntos.

Solución:

En la sección 1.6, proposición 2, vimos que $V(F,G) = V(F) \cap V(G)$ y que con las hipótesis del problema, era finito. $V(F) \cap V(G) = \{P : f(P) = 0 = g(P), \forall f \in < F >, g \in < G >\}$.

6.9.6. Ejercicio 5.8

Sea F una curva irreducible. probar que F_X, F_Y, ó $F_Z \neq 0$. Probar que F tiene una cantidad finita de puntos múltiples.

Solución: Supongamos que todos son cero, y sea F ese polinomio. $F = F(X^k, Y^k, Z^k)$, pero estamos en un cuerpo algebraicamente cerrado, por lo tanto $F = G(X, Y, Z)^k$, y no sería irreducible.

El conjunto de los puntos múltiples es $V(F, F_X, F_Y, F_Z) \subset V(F)$. Por el ejercicio anterior, sabemos que si no tienen componentes comunes, entonces será finito. Por razones de grado, F no divide a ningún F_X, F_Y, F_Z, y al ser irreducible, tampoco lo dividen, por lo tanto, no tienen componentes comunes, además, sabemos que alguno es distinto de cero. Así que tenemos la finitud.

6.10. Problemas 9 Enero

6.10.1. Ejercicio 5.17

Sean $P_1, P_2, P_3, P_4 \in \mathbb{P}^2$ y V el sistema lineal de cónicas que pasa por estos puntos. Probar que $dim(V) = 2$, si $P_1, \ldots, P_4$ están alineados, y $dim(V) = 1$, en caso contrario.

<u>*Solución:*</u>

Sabemos que dado un punto P, las curvas de grado d que pasan por ese punto forman un hiperplano de $\mathbb{P}^{\frac{1}{2}d(d+3)}$. Por lo tanto, si tenemos 4 puntos, trabajamos con la intersección de 4 hiperplanos de dimensión 4. La fórmula de la dimensión, nos dice que dados dos variedades H_1 y H_2, se cumple que:

$$dim(H_1 + H_2) = dim(H_1) + dim(H_2) - dim(H_1 \cap H_2)$$

así que, primero trabajemos con dos de los puntos, sea H_i el hiperplano que forman las curvas de grado 2 que pasan por el punto P_i, con $i = 1, 2, 3, 4$. Entonces:

$$dim(H_1 + H_2) = 4 + 4 - dim(H_1 \cap H_2)$$

$dim(H_1 + H_2) = 5$ (ya que $H1 \neq H_2$) , obteniendo $dim(H_1 \cap H_2) = 3$, y tomamos la variedad $V_1 = H_1 \cap H_2$. De manera análoga, $V_2 = H_3 \cap H_4$. Finalmente, apliquemos la fórmula de la dimensión a V_1 y V_2, pues $V = V_1 \cap V_2$.

$$dim(V_1 + V_2) = 3 + 3 - dim(V_1 \cap V_2)$$

$dim(V_1 + V_2)$ puede ser 5 o 4, dependiendo de si están o no alineados, obteniendo así que $dim(V_1 \cap V_2) = 2$ si están alineados e igual a 1 en caso contrario.

6.10.2. Ejercicio 5.20

Buscar los puntos de intersección de los siguientes pares de curvas, y los números de intersección en dichos puntos:

1. $Y^2Z - X(X - 2Z)X + Z)$ y $Y^2 + X^2 - 2XZ$.
2. $(X^2 + Y^2)Z + X^3 + Y^3$ y $X^3 + Y^3 - 2XYZ$.
3. $Y^5 - X(Y^2 - XZ)^2$ y $Y^4 + Y^3Z - X^2Z$.
4. $(X^2 + Y^2)^2 + 3X^2YZ - Y^3Z$ y $(X^2 + Y^2)^3 - 4X^2Y^2Z^2$.

<u>*Solución:*</u>

1. Para hallar los puntos de intersección en H_∞, sea $Z = 0$, obtenemos el sitema de ecuaciones:

$$\begin{cases} X^3 = 0 \\ Y^2 + X^2 = 0 \end{cases}$$

Como la única solución del sistema es $(0,0)$, F y G no intersecan en H_∞.

Para encontrar la intersección en U_1, tomamos $Z = 1$ y obtenemos el sistema de ecuaciones

$$\begin{cases} Y^2 - X(X-2)(X+1) = 0 \\ Y^2 + X^2 - 2X = 0 \end{cases}$$

que por sustitución, se obtiene $X^3 - 4X = 0$, así que $X = 0, X = 2, X = -2$, así que se obtienen los puntos:

$$P_1 = [0:0:1], P_2 = [2:0:1], P_3 = [-2:-2^{\frac{3}{2}}i:1], P_4 = [-2:2^{\frac{3}{2}}i:1]$$

Ahora, sea $P_0 = (0,0)$

$I(P_1, F \cap G) = I(P_0, Y^2 - X(X-2)(X+1) \cap Y^2 + X^2 - 2X) = I(P_0, Y^2 - X^3 + X^2 + 2X \cap Y^2 + X^2 - 2X) = I(P_0, -X^3 + 4X \cap Y^2 X^2 - 2X) = I(P_0, X(X+2)(X-2) \cap Y^2 + X^2 - 2X) = I(P_0, X \cap Y^2 - 2X) + I(P_0, (X+2)(X-2) \cap Y^2 + X^2 - 2X) = I(P_0, X \cap Y^2 + X^2 - 2X) + \underbrace{0}_{P \notin (X+2)(X-2)} = I(P_0, X \cap Y^2) = 2$

$I(P_2, F \cap G) = I((0,2), Y^2 - X(X-2)(X+1) \cap Y^2 + X^2 - 2X) = I(P_0, Y^2 - (X+2)X(X+3) \cap Y^2 + (X+2)^2 - 2(X+2)) = I(P_0, -X^3 - 6X^2 - 8X \cap Y^2 + X^2 + 2X) = I(P_0, X(X+2)(X+4) \cap Y^2 + X^2 + 2X) = I(P_0, X \cap Y^2 + X^2 + 2X) = I(P_0, X \cap Y^2) = 2$.

Y por el teorema de Bézout, $6 = \sum_{i=1}^4 I(P_i, F \cap G) \Rightarrow I(P_3, F \cap G) = 1 = I(P_4, F \cap G)$.

2. Para calcular los puntos de intersección en U_1, consideramos $Z = 1$, y obtenemos el sistema de ecuaciones:

$$\begin{cases} X^2 + Y^2 + X^3 + Y^3 = 0 \\ X^3 + Y^3 - 2XY = 0 \end{cases}$$

Por sustitución se obtiene $(X+Y)^2 = X^2 + 2XY + Y^2 = 0$, siendo las soluciones del tipo $(\lambda, -\lambda), \lambda \in k$, para finalmente obtener $\lambda = 0$. Así que el único punto de intersección en U_1 es $P_1 = [0:0:1]$.

Ahora veamos los puntos de intersección en H_∞, consideramos $Z = 0$ y obtenemos el sistema de ecuaciones:

$$\begin{cases} X^3 + Y^3 = 0 \\ X^3 + Y^3 = 0 \end{cases}$$

Obtenemos los puntos

$$P_1 = [0:0:1], P_2 = [1:-1:0], P_3 = [1:\frac{1+\sqrt{3}i}{2}:0], P_4 = [1:-\frac{\sqrt{3}i-1}{2}:0]$$

Calculamos las intersecciones:

$I(P_1, F \cap G) = I(P_0, X^2+Y^2+X^3+Y^3 \cap X^3+Y^3-2XY) = I(P_0, X^2+Y^2+2XY \cap X^3+Y^3-2XY) = I(P_0, (X+Y)^2 \cap X^3+Y^3-2XY) = 2I(P_0, X+Y \cap XY) = 4.$

$I(P_2, F \cap G) = I((-1,0), (1+Y^2)Z+1+Y^3 \cap 1+Y^3-2XY) = I((-1,0), (1+Y^2)Z+2YZ \cap 1+Y^3-2YZ) = I(P_0, (1+(Y-1)^2)Z+2(Y-1)Z \cap 1+(Y-1)^3-2(Y-1)Z) = I(P_0, Y^2Z \cap Y^3-3Y^2-2YZ+3Y+2Z) = 2I(P_0, Y \cap 2Z) + I(P_0, Z \cap Y^3-3Y^2+3Y) = 2+1 = 3$

Así que por el teorema de Bézout, como $deg(F)deg(G) = 9$, sabemos que deben intersecar transversalmente en los otros dos puntos de intersección.

3. Comprobamos la intersección en H_∞, obteniendo el sistema:

$$\begin{cases} Y^5 - XY^4 = 0 \\ Y^4 = 0 \end{cases}$$

obteniendo $P_1 = [1:0:0]$.

Ahora calculamos los puntos de intersección en U_1, tomando $Z = 1$, así que se tiene el sistema:

$$\begin{cases} Y^5 - X(Y^2-X)^2 = 0 \\ Y^4 + Y^3 - X^2 = 0 \end{cases}$$

Y no hay soluciones distintas del 0, por lo tanto, tenemos el punto $P_2 = [0:0:1]$. Aplicamos el teorema de Bézout, $I(P_1, F \cap G) = I(P_2, F \cap G) = \frac{4 \cdot 5}{2} = 10$.

4. Comprobamos como antes $Z = 0$ y $Z = 1$, obteniendo en el primer caso los puntos $P_1 = [1:-i:0]$ y $P_2 = [1:i:0]$,y $P_3 = [0:0:1]$ en el otro caso.

Sea $G - (X^2+Y^2)F = yJ$, y $J + 3F = yH$.

$I(P_3, F \cap G) = I(P_3, F \cap (G + F(3*Y - (X^2+Y^2)))) = I(P_3, F \cap (G - (X^2+Y^2)F + 3FY)) = I(P_3, F \cap (YJ + 3FY)) = I(P_3, F \cap Y(J+3F)) = I(P_3, F \cap y^2H) = 2I(P_3, F \cap Y) + I(P, F \cap H).$

$I(P, F \cap H) = I(P_3, X^4 \cap Y) = 4$ y $I(P_3, F \cap H) = m_p(F)m_P(H) = 6$. Por lo tanto, $I(P_3, F \cap G) = 14$.

Por lo tanto, aplicamos el teorema de Bézout, obteniendo $I(P_1, F \cap G) = I(P_2, F \cap G) = 5$, pues $deg(F) \cdot deg(G) = 4 \cdot 6 = 24$.

A continuación, las comprobaciones de los sistemas algebráicos en maxima:

```
(%i1) algsys([x^3, y^2+x^2], [x,y]);
```

$$(\%o1) \quad [[x = 0, y = 0]]$$

```
(%i2) algsys([y^2-x*(x-2)*(x+1), y^2+x^2-2*x], [x,y]);
```

$$(\%o2) \quad [[x = 2, y = 0], [x = -2, y = -2^{\frac{3}{2}} \cdot i], [x = -2, y = 2^{\frac{3}{2}} \cdot i], [x = 0, y = 0]]$$

```
(%i3) algsys([x^2+y^2+x^3+y^3, x^3+y^3-2*x*y], [x,y]);
```

$$(\%o3) \quad [[x = 0, y = 0]]$$

```
(%i4) algsys([x^3+y^3, x^3+y^3], [x,y]);
```

$$(\%o4) \quad [[x = \%r1, y = \frac{\left(1+\sqrt{3}\cdot i\right)\cdot \%r1}{2}], [x = \%r2, y = -\frac{\left(\sqrt{3}\cdot i-1\right)\cdot \%r2}{2}], [x = \%r3, y = -$$

```
(%i6) algsys([y^5-x*y^4,y^4], [x,y]);
```

$$(\%o6) \quad [[x = \%r4, y = 0]]$$

```
(%i7) algsys([y^5-x*(y^2-x)^2, y^4+y^3-x^2], [x,y]);
```

$$(\%o7) \quad [[x = 0, y = 0]]$$

6.10.3. Ejercicio 5.21

Probar que toda curva proyectiva plana no-singular es irreducible. ¿Es cierto para curvas afines?

Solución:

Supongamos que F es una curva no singular del plano proyectivo, y supongamos que F es reducible, es decir, $F = GH$ con $gr(F), gr(G) > 0$. Entonces por el teorema de Bézout, existe un punto $P \in F \cap G$. Pero, entonces

$$F_{X_i}(P) = (GH)_{X_i}(P) = G(P)H_{X_i}(P) + G_{X_i}(P)H(P) = 0, i = 1, 2, 3$$

Eso implica que P es un punto singular de F, llegando a una contradicción.

Por otro lado, en $\mathbb{A}^2$, $F = (Y - X)(Y - X - 1)$ es no singular, ya que $F_X = 0 = F_y$ no tiene soluciones.

6.10.4. Ejercicio 5.22

Sea F una curva irreducible de grado n. Supongamos que $F_X \neq 0$. Aplicar el corolario 1 a F y a F_X, y concluir que $\sum m_P(F)(m_P(F) - 1) \leq n(n-1)$. En particular, F tiene a lo sumo $\frac{1}{2}n(n-1)$ puntos múltiples.

<u>*Solución:*</u>

Sea F una curva irreducible de grado n y $F_X \neq 0$. Por el ejercicio 5.6, $m_P(F_X) \geq m_P(F) - 1, \forall P \in \mathbb{P}^2$. Como $F_X \neq 0$, $deg(F_X) = n - 1$. Así que por el primer corolario del teorema de Bézout:

$$n(n-1) = deg(F)deg(F_X) \geq \sum_P m_P(F)m_P(F_X) \geq \sum_P m_P(F)(m_P(F) - 1)$$

Ahora, por el ejercicio 5.6 sabemos que si $m_P(F) \geq 2$ entonces $m_P(F_X) \geq 1$, y en ese caso $m_P(F)m_P(F_X) \geq 1$, así que:

$$n(n-1) \geq \sum_P m_P(F)(m_P(F) - 1) = \sum_{\text{P:múltiple en F}} m_P(F)(m_P(F) - 1) =$$

$$= \sum_{\text{p:múltiple en F}} 1 = \#\{P : P \text{ punto múltiple de } F\}$$

Índice alfabético