Universidad de Valladolid
Facultad de Ciencias

TRABAJO DE FIN DE GRADO

GRADO EN MATEMÁTICAS

Morfismos de variedades y género de curvas regulares

Autor: Paula Hernamperez Manso

Tutor: Manuel Mariano Carnicer Arribas

Índice general

Introducción

Este trabajo surge con la intención de completar y ampliar la materia impartida en la asignatura de "Curvas Algebraicas", situada dentro del Grado en Matemáticas, con la intención de presentar el concepto de género de una curva algebraica. Muy pronto, a la vista de los conceptos que hay que introducir para llegar a la definición de género de una curva, adquiere también el objetivo de desarrollar una introducción a la Geometría Algebraica, presentando los objetos habituales en una primera aproximación a este campo, las variedades algebraicas y las aplicaciones que relacionan estos objetos, los morfismos de variedades. A partir de los morfismos, se tienen la presentación y estudio de los conceptos de aplicación racional y aplicación birracional. En este trabajo nos hemos limitado a la definición de género en el caso de curvas regulares, ya que hacerlo en el caso general nos obligaba al estudio de la desingularización de curvas, lo cual ampliaría más de lo conveniente su extensión.

Con el punto de vista de una introducción a la Geometría Algebraica, y para potenciar el aspecto geométrico y reducir las situaciones patológicas, trabajamos siempre con un cuerpo algebraicamente cerrado y de característica cero, aunque en algunas ocasiones recalcaremos en el enunciado de algún resultado estas propiedades para resaltar que ese resultado en concreto no sería cierto en otro caso. Organizamos el trabajo dividiéndolo en tres capítulos.

En el primero de los capítulos hemos realizado un resumen de algunas de las nociones de los resultados estudiados durante la citada asignatura de "Curvas Algebraicas", todos ellos generalizados a cualquier dimensión. De este modo, introducimos las nociones de variedades afines y proyectivas en un espacio n-dimensional así como algunas de sus propiedades y enunciamos el *Teorema de los Ceros de Hilbert* tanto en su versión afín como proyectiva. En estas secciones no hemos incluido demostraciones pues casi todas ellas han sido realizadas en las clases impartidas por el profesor responsable de la asignatura. Sí hemos introducido demostraciones en las dos últimas secciones, en las que nos centramos en los conceptos de funciones racionales, que no fueron estudiados con tanto detalle en su momento, y de variedades en su definición general como abierto de una variedad proyectiva. Con la presentación de estas variedades concluimos el capítulo.

El segundo capítulo gira en torno a los morfismos entre variedades. Empezamos con su definición y después damos dos ejemplos de morfismos entre variedades, las aplicaciones polinómicas entre variedades afines y las aplicaciones regulares entre variedades, que nos serán muy útiles a la hora de desarrollar la última sección de este capítulo en la que tratamos la noción de dimensión de una variedad. Para esto, nos servirá de especial ayuda la aplicación regular conocida como el *embebimiento de Veronese*. En este capítulo añadimos también la aplicaciones racionales y birracionales que se construyen a partir de morfismos y que nos harán falta para el último capítulo del trabajo.

En el tercer y último capítulo tratamos con uno de los temas mencionados en la asignatura de "Curvas algebraicas" pero que no se llegaron a estudiar en profundidad por falta de tiempo. Para ello, nos centramos en las variedades de dimensión uno regulares, las curvas regulares, y definimos el concepto de *género de una curva regular* a través del *Teorema de Riemann*. Para ello, damos unos resultados de curvas planas e introducimos el concepto de divisor de una curva, de divisor asociado a una función racional y de equivalencias lineal de divisores.

Aunque el trabajo se centra en la Geometría Algebraica, ha sido necesario introducir resultado propios de otras ramas que no se han estudiado en el grado. Estos resultados se han recogido en dos apéndices al final del trabajo. En el primero de ellos tenemos los relacionados con el Álgebra Conmutativa, es decir, relacionados con anillos, ideales y módulos. El segundo gira en torno a las extensiones de cuerpos, concretamente, en torno a las extensiones trascendentes y las bases de trascendencia.

Capítulo 1

Variedades algebraicas

1.1. Variedades afines

Sea k un cuerpo algebraicamente cerrado y de característica 0. Denotamos por $k[x_1,..,x_n]$ al anillo de polinomios en n variables sobre k, y por $\mathbb{A}^n$ al producto cartesiano de n copias de k, un espacio afín

Definición 1 *Dado $S \subset k[X_1,...,X_n]$, definimos $V(S)$ como el conjunto de puntos $p = (x_1,...,x_n) \in \mathbb{A}^n$ tales que $f(x_1,...,x_n) = 0$ para todo $f \in S$.*

Definición 2 *Si $X \subset \mathbb{A}^n$ decimos que X es un* conjunto algebraico *si existe $S \subset k[X_1,...,X_n]$ tal que $V(S) = X$.*

Propiedades de los conjuntos algebraicos:

1. Si $S \subset R$ entonces $V(S) \supset V(R)$.
2. Si I_s es el ideal generado por el conjunto $S \subset k[X_1,...,X_n]$, $V(S) = V(I_s)$.
3. $V(k[X_1,...,X_n]) = \emptyset$.
4. $V(0) = \mathbb{A}^n$.
5. Si $\{I_\alpha\}_{\alpha\in A}$ es una familia cualquiera de ideales de polinomios, entonces $V(\cup_{\alpha\in A} I_\alpha) = \cap_{\alpha\in A} V(I_\alpha)$.
6. Si I, J son ideales del anillo de polinomios, $V(I \cap J) = V(IJ) = V(I) \cup V(J)$.
7. $V(I) = V(Rad(I))$ donde $Rad(I)$ representa al ideal radical del ideal I.

Nota: A la vista de las propiedades 5 y 6, los conjuntos algebraicos son los cerrados de una topología sobre $\mathbb{A}^n$. A esta topología se la conoce como *topología de Zariski*.

Nota: Si $S = \{f_1,..., f_r\}$ en vez de escribir $V(S)$, escribimos $V(f_1,..., f_r)$. Si r=1, decimos que $V(f)$ son los ceros del polinomio f.

Definición 3 *Definimos el ideal del conjunto $X \subset \mathbb{A}^n$, y lo representamos por* I(X)*, como el conjunto de polinomios $f \in k[X_1,...,X_n]$ que verifican $f(x_1,...,x_n) = 0$ para todo punto $(x_1,...,x_n) \in X$.*

Nota: Con esta definición es obvio que el ideal de un conjunto es un ideal.

Propiedades:

1. $I(\emptyset) = k[X_1,...,X_n]$
2. Si k es infinito, $I(\mathbb{A}^n) = \{0\}$
3. Si $X \subset Y$ entonces $I(X) \supset I(Y)$
4. $X \subset V(I(X))$
5. $S \subset I(V(S))$
6. Si X es algebraico, $X = V(I(X))$
7. $I(X) = I(V(I(X)))$
8. $I(X)$ es radical

Proposición 1 *Todo conjunto algebraico V tiene un conjunto finito de polinomios $f_1,...,f_r$ de modo que $V = V(f_1,...,f_r)$.*

Definición 4 *$V \subset \mathbb{A}^n_k$ decimos que es un* conjunto algebraico irreducible *si para todo par de conjuntos algebraicos $V_1, V_2 \subset \mathbb{A}^n_k$ tal que $V = V_1 \cup V_2$ se verifica que $V = V_1$ o $V = V_2$.*

Definición 5 *Llamamos* variedades afines *a los conjuntos algebraicos irreducibles.*

Proposición 2 *Un conjunto algebraico V es irreducible si y sólo si $I(V)$ es un ideal primo.*

Demostración: Ver [2], capítulo 1, sección 5.

Teorema 1 (de los ceros de Hilbert) *Sea $I \subset k[X_1,...,X_n]$ un ideal cualquiera. Entonces, si k es algebraicamente cerrado, $I(V(I)) = Rad(I)$.*

Demostración: Ver [2], capítulo 1, sección 7.

Del resultado anterior es inmediato deducir que toda familia de conjuntos algebraicos afines tiene un elemento minimal, puesto que si $I \subset J$ son dos ideales, entonces $V(J) \subset V(I)$ y viceversa, se invierten las contenciones.

Teorema 2 *Sea V un conjunto algebraico de $\mathbb{A}^n$. Entonces, existen $V_1,...,V_m$ variedades afines tales que $V = V_1 \cup ... \cup V_m$ y $V_i \not\subset V_j$ para cada par de i, j. Además, estos V_i son únicos.*

Demostración: Ver [2], capítulo 1, sección 5.

Definición 6 *Sea V un conjunto algebraico y sean $V_1,...,V_m$ las únicas variedades afines tales que $V = V_1 \cup ... \cup V_m$ y $V_i \not\subset V_j$ para cada par de i, j. Llamaremos a esas variedades afines las* componentes irreducibles *de V.*

Proposición 3 *Sean $I, J \subset k[X_1,...,X_n]$ dos ideales. Entonces, I y J son comaximales si y solamente si $V(I) \cap V(J) = \emptyset$.*

Demostración: Supongamos que I y J son comaximales. Entonces, si existiera $p \in V(I) \cap V(J)$ entonces, para todo polinomio $f \in I$, $f(p) = 0$ y para todo polinomio $g \in J$, $g(p) = 0$. Entonces, si $h \in k[X_1,...,X_n]$ es un polinomio cualquiera, existirán $f' \in I$ y $g' \in J$ con $h = f' + g'$, pero entonces $h(p) = f'(p) + g'(p) = 0$, de lo que deducimos que $p \in V(k[X_1,...,X_n]) = \emptyset$, lo cual es absurdo.

Supongamos que $V(I) \cap V(J) = V(I \cup J) = \emptyset$. Entonces, todo ideal que contenga a I y J, en particular $I + J$ coincidirá con el anillo $k[X_1,...,X_n]$.

Definición 7 *Sea X un conjunto algebraico. Llamamos al cociente* $A(X) = \dfrac{k[X_1,\ldots,X_n]}{I(X)}$ anillo de coordenadas *de X.*

Nota: Si V una variedad afín, entonces $I(V)$ es un ideal primo y, por tanto, el anillo de coordenadas es un dominio.

Nota: al anillo de coordenadas también se le conoce como *álgebra de coordenadas*

Sea A un conjunto cualquiera, denotamos por $J(A,k)$ a todas las funciones definidas en A con llegada en k. El conjunto $J(A,k)$ tiene estructura de anillo con la suma y producto de funciones habitual.

Definición 8 *Si X es un conjunto algebraico, decimos que una función $f \in J(X,k)$ es una* función polinómica *si existe un polinomio $P \in k[X_1,\ldots,X_n]$ tal que $f(x_1,\ldots,x_n) = P(x_1,\ldots,x_n)$ para cada punto $(x_1,\ldots,x_n) \in X$.*

El conjunto de funciones polinómicas constituye un subanillo de $J(X,k)$. Denotaremos a ese anillo por $F(X)$.

Dos polinomios P, Q dan lugar a la misma función polinómica si y sólo si $P - Q \in I(X)$.

Si consideramos el homeomorfismo $k[X_1,\ldots,X_n] \longrightarrow F(X)$, que relaciona cada polinomio con su correspondiente función restringida a V, tenemos un homeomorfismo de anillos sobreyectivo cuyo núcleo es el ideal $I(X)$, con lo que el anillo de coordenadas $A(X)$ es isomorfo a $F(X)$.

En adelante interpretaremos a los elementos de $A(X)$ como funciones polinómicas o como clases de equivalencia de un cociente según nos convenga.

Proposición 4 *Sea I un ideal de $k[X_1,\ldots,X_n]$ y sea $\pi : k[X_1,\ldots,X_n] \longrightarrow \frac{k[X_1,\ldots,X_n]}{I}$ la aplicación de paso al cociente. Entonces:*

(1) la imagen por π de todo ideal J de $k[X_1,\ldots,X_n]$ que contenga a I es un ideal de $\frac{k[X_1,\ldots,X_n]}{I}$ y la contraimagen de cualquier ideal J' de $\frac{k[X_1,\ldots,X_n]}{I}$ es un ideal de $k[X_1,\ldots,X_n]$ que contiene a I.

(2) existe una biyección entre los ideales de $k[X_1,\ldots,X_n]$ que contienen a I y los de $\frac{k[X_1,\ldots,X_n]}{I}$. Esta biyección está inducida por π.

(3) si J' es un ideal de $\frac{k[X_1,\ldots,X_n]}{I}$ y J su correspondiente ideal de $k[X_1,\ldots,X_n]$. Entonces, J' es radical, primo o maximal si y solamente si J lo es.

(4) existe una biyección entre los subconjuntos algebraicos de $V(I)$ y los ideales radicales de $\frac{k[X_1,\ldots,X_n]}{I}$. Si J' es un ideal radical de $\frac{k[X_1,\ldots,X_n]}{I}$ denotaremos por $V(J')$ a su correspondiene subconjunto algebraico de $V(I)$.

(5) si J es un ideal de $k[X_1,\ldots,X_n]$ de generación finita y J' es su correspondiente ideal de $\frac{k[X_1,\ldots,X_n]}{I}$, entonces, J' también es de generación finita.

(6) $\frac{k[X_1,\ldots,X_n]}{I}$ es noetheriano.

Demostración: (1) ambas afirmaciones son inmediatas.

(2) la biyección es la dada por π en (1).

(3) Sean $F, G \in k[X_1,\ldots,X_n]$. Para ver la parte de ideales radical basta con darse cuenta de que, $F^r \in J$ si y solo si $F^r + I = (F+I)^r \in J'$ par cualquier r. Para la parte de ideales primos, hay que fijarse en que $FG \in J$ si y solamente si $(F+I)(G+I) = FG+I \in J'$. Y para la parte de ideales maximales basta con fijarse en que F no es una unidad en $k[X_1,\ldots,X_n]$ si y solamente si $F+I$ no lo es en $\frac{k[X_1,\ldots,X_n]}{I}$.

(4) Si J es un ideal radical de $k[X_1,...,X_n]$ que contiene a I, entonces $V(J) \subset V(I)$ es un subconjunto algebraico. Además, si J es radical, por (3) tenemos que su correspondiente ideal J' en $\frac{k[X_1,...,X_n]}{I}$ también lo es. Entonces, juntando (2) y el teorema de los ceros de Hilbert concluimos.

(5) Sea $J = (F_1,...,F_s)$ con $F_i \in k[X_1,...,X_n]$ unos generadores. Entonces, es inmediato el ver que $J' = (F_1 + I,...,F_s + I)$.

(6) Inmediato aplicando (5).

1.2. Variedades proyectivas

Consideramos ahora el espacio proyectivo $\mathbb{P}^n_k$, al que nos referiremos simplemente como $\mathbb{P}^n$, con coordenadas homogéneas $(X_0;...;X_n)$.

Definición 9 *Un ideal $J \subset k[X_0,...,X_n]$ decimos que es* homogéneo *si tiene una base de generadores formada por polinomios homogéneos.*

Proposición 5 *Un ideal $J \subset k[X_0,...,X_n]$ es homogéneo si y sólo si para todo $F = \sum_{i=0}^d F_i \in J$, con $gr(F_i) = i$ homogéneos, se tiene $F_i \in J$.*

Demostración: Ver [2], capítulo 4, sección 2.

Nota: puesto que los puntos de $\mathbb{P}^n$ no tienen una expresión única si no que si $p \in \mathbb{P}^n$ es un punto con $p = (x_1;...;x_n)$, y $\lambda \in k$, $\lambda \neq 0$, también podemos escribir $p = (\lambda x_1;...;\lambda x_n)$, en general, no tiene sentido hablar de los ceros de un polinomio $F \in k[X_0,...,X_n]$, solamente en los casos en los que F sea un polinomio homogéneo de grado g tendrá sentido, pues si $F(x_0,...,x_n) = 0$, entonces $F(\lambda x_1,...,\lambda x_n) = \lambda^g F(x_0,...,x_n) = 0$.

Proposición 6 *Sea J un ideal homogéneo y sean $F_1,...,F_s$ y $G_1,...,G_r$ dos conjuntos de generadores de J formadas por polinomios homogéneos. Entonces, se tiene*

$$\{p \in \mathbb{P}^n : F_i(p) = 0, i = 1,...,s\} = \{q \in \mathbb{P}^n : G_j(q) = 0, j = 1,...,r\}.$$

Demostración: Basta con demostrar una contención pues la otra es análoga.

Sea $p \in \{p \in \mathbb{P}^n : F_i(p) = 0 \text{ para todo } i = 1,...,s\}$. Como para todo $j = 1,..,r$ tenemos que el polinomio $G_j \in (F_1,...,F_s)$, podemos escribir $G_j = H_1^j F_1 + ... + H_s^j F_s$, para ciertos polinomios H_k^j, $k = 1,...,s$. Luego $G_j(p) = H_1^j(p)F_1(p) + ... + H_s^j(p)F_s(p) = 0$.

Definición 10 *Sea $J \subset k[X_0,...,X_n]$ un ideal homogéneo y $F_1,...,F_s$ un conjunto de generadores homogéneos de J. Denotamos por $V_h(J) = \{p \in \mathbb{P}^n : F_i(p) = 0$ para todo $i = 1,...,s\}$. A este conjunto lo llamaremos* conunto de ceros del ideal.

Definición 11 *Decimos que un conjunto $X \subset \mathbb{P}^n$ es un* conjunto algebraico proyectivo *si existe un ideal homogéneo J tal que $V_h(J) = X$.*

Definición 12 *Sea $F \in k[X_1,...,X_n]$ un polinomio cualquiera. Podemos escribir $F = F_1 + ... + F_d$ donde cada F_i es un polinomio homogéneo de grado i. Entonces, definimos el conjunto $V_h(F)$ como*

$$V_h(F) = V_h(F_1,...,F_d).$$

Lema 1 *Dado un ideal homogéneo $J \subset k[X_0,...,X_n]$, se verifica que $V_h(J) = \emptyset$ si y solamente si existe un entero $s > 0$ tal que J contiene al ideal I_s formado por todos los polinomios homogéneos de grado s.*

Demostración: Ver [5], capítulo 1, sección 4, subsección 1.

Nota: Con la notación del apartado anterior, fijémonos que si $I_0 = (1) \subset J$, entonces $V_h(J) = \emptyset$, e $I_s \subset J$ para todo $s > 0$.

Nota: Los conjuntos algebraicos proyectivos cumplen propiedades similares a las de los conjuntos algebracicos. Más concretamente, cumplen las mismas propiedades enunciadas tras la definición 2 (cambiando el espacio afín por el proyectivo y $k[X_1, ..., X_n]$ por $k[X_0, ..., X_n]$) a excepción de la 3, como se ha podido ver en el lema 1.

Nota Los conjuntos algebraicos proyectivos son los cerrados de una topología en $\mathbb{P}^n$ llamada topología de Zariski.

Definición 13 *Sea $X \subset \mathbb{P}^n$. Definimos el ideal de X como el ideal generado por los polinomios homogéneos que se anulan en todo punto de X y tal que denotaremos por $I_h(X)$.*

Proposición 7 *Sea $X \subset \mathbb{P}^n$. $I_h(X)$ es un ideal homogéneo.*

Nota: El ideal $I_h(X)$ cumple propiedades similares a las de los ideales $I(Y)$ generados por un jununto $Y \subset \mathbb{A}^n$. Concretamente, cumplen las propiedades 2 a 8 según están enunciadas tras la definición 3, cambiando $k[X_1, ..., X_n]$ por $k[X_0, ..., X_n]$ y el espacio afín por el proyectivo.

Definición 14 *Sea $F \in k[X_0, ..., X_n]$ un polinomio homogéneo no nulo. Llamaremos* hipersuperficie *de $\mathbb{P}^n$ a $V_h(F)$. Diremos que la hipersuperficie es de grado m cuando $m = gr(F)$. A las hipersupeorficies de grado 1 las llamaremos* hiperplanos.

Teorema 3 (Teorema de los ceros de Hilbert proyectivo:) *Sea k algebraicamente cerrado $J \in k[X_0, ..., X_n]$ un ideal homogéneo. Entonces:*

1. *$V_h(J) = \emptyset$ si y solamente si $I_s \subset J$ para algún $s > 0$.*
2. *si $V_h(J) \neq \emptyset$, $I_h(V_h(J)) = Rad(J)$.*

Demostración: Ver [2], capítulo 4, sección 2.

Definición 15 *Diremos que un conjunto algebraico pruoyectivo es* irreducible *cuando no es unión de dos conjuntos algebraicos proyectivos propios.*

Proposición 8 *Los conjuntos algebraicos proyectivos son irreducibles si y sólo si su ideal es primo.*

Demostración: La prueba de este resultado sigue los mismos pasos que el resultado homólogo en el espacio afín.

Definición 16 *Llamamos* variedades proyectivas *a los conjuntos algebraicos proyectivos irreducibles.*

Proposición 9 *Sea R una familia de conjuntos algebraicos proyectivos de $\mathbb{P}^n$. Entonces, R posee un elemento minimal.*

Teorema 4 *Sea W un conjunto algebraico proyectivo de $\mathbb{P}^n$. Entonces, existen $W_1, ..., W_m$ variedades proyectivas tales que $W = W_1 \cup ... \cup W_m$ y $W_i \not\subset V_j$ para cada par de i, j. Además, estos W_i son únicos.*

Demostración: la demostración sigue los mismos pasos que la del teorema 2.

Definición 17 *Sea W un conjunto algebraico proyectivo, y sean $W_1,...,W_m$ las únicas variedades proyectivas tales que $W = W_1 \cup ... \cup W_m$ y $V_i \not\subset W_j$ para cada par de i, j. Llamaremos a esas variedades proyectivas las* componentes irreducibles *de W.*

El anillo de coordenadas para una variedad proyectiva W se define igual que el de variedades afines, como el anillo $A_h(W) = \dfrac{k[X_0,...,X_n]}{I_h(W)}$. Sin embargo, no podemos definir las funciones polinómicas igual que en el caso afín, pues como ya dijimos, si $P \in k[X_0,...,X_n]$ y $\lambda \in k$ es no nulo, $(x_0;...;x_n) = (\lambda x_0;...;\lambda x_n) \in \mathbb{P}^n$, en general no se cumple $P(x_0,...,x_n) = P(\lambda x_0,...,\lambda x_n)$. Es decir, no tiene sentido hablar de la evaluación de un polinomio en el espacio proyectivo. Sólo los elementos constantes de $A_h(W)$ se pueden considerar funciones (constantes).

Nota: al igual que en el caso afín, el anillo de coordenadas de una variedad proyectiva también es noetheriano. Para verlo basta con aplicar la porposición 26

1.3. La clausura proyectiva

En las dos secciones anteriores hemos dado dos definiciones de variedad según el espacio ambiente en el que trabajamos. Vamos a ver ahora una forma de relacionar variedades afines con proyectivas.

Identificaremos a $\mathbb{A}^n_k$ con la carta $X_0 \neq 0$. Siguiendo esta identificación, a cualquier elemento $p = (x_1,...,x_n) \in \mathbb{A}^n$ lo representaremos de igual manera, por $p = (1;x_1;...;x_n) \in \mathbb{P}^n$, cuando trabajemos en el espacio proyectivo. Se hará lo mismo con subconjuntos.

Sea $f \in k[X_1,...,X_n]$ es un polinomio cualquiera, f se puede escribir como $f = f_0 + ... + f_d$, donde cada f_i son polinomios homogéneos de grado i y donde $d = gr(f)$. Podemos "homogeneizar" f de manera que obtenemos un polinomio homogéneo $f^* \in k[X_0,...,X_n]$ que viene dado por la expresión

$$f^* = X_0^d f_0 + ... + X_0 f_{d-1} + f_d.$$

El polinomio f^* verifica que para cada punto $(x_1,...,x_n) \in \mathbb{A}^n$, $f(x_1,...,x_n) = f^*(1,x_1,...,x_n)$. Nótese que X_0 no divide a f^*.

Recordemos que tiene sentido hablar de los ceros de un polinomio homogéneos, esto es cierto en particular para los polinomios homogeneizados.

De igual manera, si $F \in k[X_0,...,X_n]$ es un polinomio cualquiera, podemos "deshomogeneizarlo", obteniendo así un polinomio $F_* \in k[X_1,...,X_n]$ que viene definido por $F_*(X_1,...,X_n) = F(1,X_1,...,X_n)$.

Nota: La operación que hemos definido como "deshomogeneizar" recibe este nombre porque normalmente se define únicamente para polinomios homogéneos. Y en este caso, la deshomogeneización y la homogeneización son operaciones inversas.

Proposición 10 *Sean $f, g \in k[X_1,...,X_n]$ y $F, G \in k[X_0,...,X_n]$ polinomios cualesquiera. Entonces:*

(1) $(f^*)_* = f$.

(2) Si F es homogéneo, $X_0^d (F_*)^* = F$ donde $d = gr(F) - gr((F_*)^*)$.

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

(4) $(F+G)_* = F_* + G_*$ *y* $(f+g)^* = X_0^r f^* + X_0^s g^*$ *donde* $r = gr(f+g) - gr(f)$ *y* $s = gr(f+g) - gr(g)$.

Definición 18 *Sea $I \subset k[X_1,...,X_n]$ un ideal cualquiera. Llamamos* ideal homogeneizado *de I al ideal generado por el conjunto $\{f^* : f \in I\}$ al que representaremos por I^*.*

Nota: el conjunto $\{f^* : f \in I\}$ no es un ideal. Para verlo basta con darse cuenta de que todos los elementos del conjunto son polinomios homogéneos pero que la suma de dos de ellos con distinto grado no lo es, luego no puede estar en el conjunto.

Proposición 11 *Sea $I \subset k[X_1,...,X_n]$ un ideal y sea $\{f_1,...,f_r\}$ un conjunto de generadores de I. Entonces, $I^* = (f_1^*,...,f_r^*)$*

Corolario 1 *Sea $I \subset k[X_1,...,X_n]$ un ideal cualquiera. I^* es un ideal homogéneo.*

Proposición 12 *Sea $J \subset k[X_0,...,X_n]$ un ideal homogéneo. Entonces, el conjunto $\{F_* : F \in J\}$ es un ideal.*

Definición 19 *Sea $J \subset k[X_0,...,X_n]$ un ideal homogéneo. Llamamos* ideal deshomogeneizado *de J al ideal $J_* = \{F_* : F \in J\}$.*

Proposición 13 *Sea $J \subset k[X_0,...,X_n]$ un ideal homogéneo y sea $\{F_1,...,F_r\}$ un conjunto de generadores homogéneos de J. Entonces $J_* = (F_{1*},...,F_{r*})$.*

Lema 2 *(1) Sean $I, J \subset k[X_1,...,X_n]$, entonces $(I \cap J)^* = I^* \cap J^*$.*

(2) Sean $I, J \subset k[X_0,...,X_n]$ ideales homogéneos, entonces $(I \cap J)_* = I_* \cap J_*$.

Demostración:

(1) Como $(I \cap J)^*$ es un ideal, basta ver que si $f \in (I \cap J)$ entonces $f^* \in I^* \cap J^*$ para deducir que $(I \cap J)^* \subset (I^* \cap J^*)$. Pero esto es evidente.

Por otro lado, sea $F \in I^* \cap J^*$. Empecemos suponiendo F homogéneo. Existen polinomios $H_1,...,H_s$ de modo que podemos escribir $F = H_1 h_1^* + ... + H_s h_s^*$ donde $h_1,...,h_s$ es una base de generadores de J. En consecuencia, $F_* = H_{1*} h_1 + ... + H_{s*} h_s \in J$. Siguiendo un razonamiento análogo se de deduce que $F_* \in I$. De esta forma, es evidente que $F = X_0^d (F_*)^* \in (I \cap J)^*$.

Supongamos ahora que $F \in I^* \cap J^*$ es un polinomio cualquiera. Para ciertos F_i polinomios homogéneos de grado i, podemos escribir F como $F = F_0 + ... + F_d$. Como I^* y J^* son polinomios homogéneos, para cada i $F_i \in I^* \cap J^*$ también. Y como hemos visto antes, esto implica que $F_i \in (I \cap J)^*$ con lo que es inmediato deducir $F \in (I \cap J)^*$.

(2) Sea $F \in I \cap J$ un polinomio. Es inmediato que $F_* \in I_*$ y $F_* \in J_*$, y por tanto F_* pertenece a su intersección.

Sea ahora $f \in I_* \cap J_*$ un polinomio. Si encontramos un polinomio $F \in I \cap J$ tal que $F_* = f$ concluiremos $I_* \cap J_* \subset (I \cap J)_*$. Existen $G \in I$ y $H \in J$ tales que $G_* = f = H_*$. Para ciertos G_i polinomios homogéneos de grado i, podemos escribir $G = G_0 + ... + G_d$. Como I es homogéneo, $G_i \in I$ y, por tanto, $G_i' = X_0^{d-i} G_i \in I$ también. Consideramos $G' = G_0' + ... + G_d' \in I$. Siguiendo el mismo razonamiento, construimos un polinomio $H' \in J$. G' y H' son polinomios homogéneos que cumplen $G'_* = G_* = H_* = H'_*$. Tenemos por lo tanto, $G' = X_0^{d_1}(G'_*)^*$ y $H' = X_0^{d_2}(G'_*)^*$. Podemos suponer, sin pérdida de generalidad, que $d_1 > d_2$, y en consecuencia $G' = X_0^{d_1-d_2} H' \in (I \cap J)$. G' es el polinomio que buscábamos.

Lema 3 *Sea $I \subset k[X_1,...,X_n]$ un ideal y $F \in k[X_0,...,X_n]$ un polinomio homogéneo. Entonces:*

(1) $F \in I^*$ si y sólo si $F_* \in I$.

(2) Si I es un ideal radical, I^* también lo es.

(3) Si I es un ideal primo, I^* también lo es.

Demostración:
(1) Si $F \in I^*$, $F_* \in (I^*)_* = I$.
Si $F_* \in I$, $(F_*)^* \in I^*$. Luego $F = X_0^d (F_*)^* \in I^*$.

(2) Sea $F \in k[X_0, ..., X_n]$ un polinomio tal que existe m de modo que $F^m \in I^*$. $(F^m)_* = (F_*)^m \in I$ y como I es radical, $F_* \in I$. Terminamos el razonamiento aplicano (1).

(3) sean $F, G \in k[X_0, ..., X_n]$ tales que $FG \in I^*$. Denotamos por $H = FG$. Queremos ver que F o G también son elementos de I^*. Como $H \in I^*$, $H_* \in I$. Por ser V irreducible, I es primo y tendremos $F_* \in I$ o $G_* \in I$ y, por lo tanto, $F \in I^*$ o $G \in I^*$, tal y como queríamos.

Proposición 14 *Si $H \in k[X_0, ... X_n]$ es homogéneo, entonces $V_h(H) \cap \mathbb{A}_k^n = V(H_*)$. En general, si J es un ideal homogéneo, $V_h(J) \cap \mathbb{A}_k^n = V(J_*)$.*

Demostración: Sea $P \in V_h(J) \cap \mathbb{A}^n$, $P = (1; x_1; ...; x_n) = (x_1, ..., x_n)$. Entonces,

$$F(P) = F(1, x_1, ..., x_n) = F_*(x_1, ..., x_n) = F_*(P) = 0.$$

Igualmente, si $p \in V(F_*) \subset \mathbb{A}^n$, $F_*(x_1, ..., x_n) = F(1, x_1, ..., x_n) = 0$.

Definición 20 *Dados $V \subset \mathbb{A}^n$ y $W \subset \mathbb{R}^n$. Denotamos por $V^* = V_h(I(V)^*)$ y a $W_* = V(J(W)_*)$. A V^* se le conoce como* clausura proyectiva *de V.*

Lema 4 *(1) Sean $V, W \subset \mathbb{P}^n$, entonces $(V \cup W)_* = V_* \cup W_*$*

(2) Sean $V, W \subset \mathbb{A}^n$, entonces $(V \cup W)^* = V^* \cup W^*$.

Demostración: Ambos resultados son inmediatos usando el lema 2.

Proposición 15 *Sean $V \subset \mathbb{A}^n$ un conjunto algebraico y $W \subset \mathbb{P}^n$ un conjunto algebraico proyectivo. Denotamos por H_∞ al hiperplano del infinito. Entonces se cumple:*

(1) $(V^*)_* = V$

(2) Si V es irreducible en $\mathbb{A}^n$, V^* también es irreducible en $\mathbb{P}^n$

(3) V^* es el menor conjunto algebraico proyectivo que contiene a V.

(4) Si $V \subsetneq \mathbb{A}^n$ es no vacío, entonces ninguna componente de V^* está contenida en ni contiene a H_∞.

(5) Si ninguna componente de W contiene ni está contenida en H_∞, entonces se cumple $W_* \subsetneq \mathbb{A}^n$ y $(W_*)^* = W$.

Demostración:
(1) Tenemos que $(V^*)_* = V(I_h(V_h(I(V)^*))_*) = V((I(V)^*)_*)$ por el lema anterior y el Teorema de los ceros. Pero como $(I(V)^*)_* = I(V)$ se concluye lo deseado.

(2) Basta con ver que $I_h(V^*)$ es irreducible. Pero como $I(V)$ es primo, en virtud del lema 3 $I(V)^*$ también lo es y además $I_h(V^*) = I_h(V_h(I(V)^*)) = I(V)^*$ por el teorema de los cerros proyectivos, concluyendo lo que queríamos.

(3) Denotaremos por $V \subset \mathbb{P}^n$ a la inclusión de $V \subset \mathbb{A}^n$.

Razonamos por reducción al absurdo. Supongamos que existe un conjunto algebraico proyectivo W tal que $V \subset W \subset V^*$. Veamos que $W = V^*$.

Sea $J = I(W)$ e $I = I(V)$. Queremos ver que $J \subset I^*$. Sea $F \in J$ un polinomio homogéneo de J arbitrario. Consideramos $f = F_*$ la deshomogeneización de F. Como $V \subset W_*$, $f \in I$ y $f^* \in I^*$. Como $F = X_0^r f^*$, concluimos que $F \in I^*$, tal y como queríamos.

(4) Podemos suponer que V es irreducible en virtud del lema 4.

Si $V^* \subset H_\infty$, entonces $V = (V^*)_* \subset (H_\infty)_* = \emptyset$

Si $H_\infty \subset V^*$, todo polinomio $f^* \in I^*$ verifica que $f^*(0, X_1, ..., X_n) = 0$, luego $f^* = X_0^s F$ para algún polinomio F, absurdo.

(5) En virtud del lema 4 podemos suponer que W es irreducible.

Si $W_* = \mathbb{A}^n$ entonces para todo polinomio $F \in I_h(W)$ $F(1, x_1, ..., x_n) = 0$. Como se verifica que $[1, x_1, ..., x_1] = [\lambda, \lambda x_1, ..., \lambda x_n]$ para todo $\lambda \in k$ no nulo, tenemos que como k es infinito todo polinomio de J a de ser nulo, con lo que $J = 0$ y $H_\infty \subset \mathbb{P}^n = W$, contra hipótesis.

Veamos ahora que $(W_*)^* = W$:

Sea $F_1, ..., F_s$ unos generadores homogéneos de $I_h(W)$, entonces $(W_*)^* = V_h((I_h(W)_*)^*)$ es el conjunto $\{p \in \mathbb{P}^n : (F_{i*})^*(p) = 0\ \forall i = 1, ..., s\}$. Pero como los F_i son homogéneos, $F_i = X_0^{d_i}(F_{i*})^*$, luego si $p \in (W_*)^*$ $F_i(p) = 0$ para todo i. Por lo tanto $(W_*)^* \subset W$.

Antes hemos demostrado $(W_*)^* \subset W$, lo que implica $I_h(W) \subset I(W_*)^*$. Veamos la otra contención:

Sea $f \in I(W_*)$, si vemos $f^* \in I_h(W)$, al ser $I_h(W)$ un ideal, deduciremos $I(W_*)^* \subset I_h(W)$.

Tenemos que $I(W_*) = I(V(I_h(W)_*)) = Rad(I_h(W)_*)$, luego existe m tal que $f^m \in I(W)_*$. Por tanto, existirá t tal que $X_0^t(f^m)^* = X_0^t(f^*)^m \in I_h(W)$. Pero como W es irreducible, se cumple que $X_0 \in I_h(W)$ o $f^* \in I_h(W)$. Sin embargo, no puede ocurrir $X_0 \in I_h(W)$, pues $H_0 \not\subset W$, con lo que deducimos lo deseado.

Nota: Hemos visto que si $V \subset \mathbb{A}^n$, la clausura para la topología de Zariski en $\mathbb{P}^n$ coincide con V^* y que si $V \subset \mathbb{A}^n$ y $W \subset \mathbb{P}^n$ son dos variedades afín y proyectiva respectivamente, entonces, V^* y W_* también son dos variedades proyectiva y afín respectivamente. Sólo nos queda por ver lo que ocurre con las componentes irreducibles de un conjunto algebraico.

Proposición 16 *Sea V un conjunto algebraico de $\mathbb{A}^n$ cuyas componentes irreducibles son $V_1, ..., V_s$. Entonces, la clausura proyectiva de V, V^*, es un conjunto algebraico proyectivo de $\mathbb{P}^n$ con componentes irreducibles $V_1^*, ..., V_s^*$.*

Demostración: basta con juntar el lema 4 y el apartado 2 de la proposición 15.

1.4. Funciones racionales

Para estudiar tanto las variedades afines como las proyectivas utilizaremos unos objetos, el primero de ellos, el que definiremos en esta sección, es el cuerpo de funciones racionales.

Definición 21 *Sea V una variedad afín y sea $A(V)$ su anillo de coordenadas. Como ya se dijo, $A(V)$ es un dominio, luego se puede construir su cuerpo de fracciones al que denotaremos por $k(V)$ y al que llamaremos* cuerpo de funciones racionales *de V. A los elementos de $k(V)$ los llamaremos* funciones racionales.

En el cuerpo de fracciones $k(V)$ dos fracciones $\frac{a}{b}$ y $\frac{c}{d}$ definen la misma función racional si y solo si $ad = cd$.

Si tenemos $f \in k(V)$ una función racional, podemos ver a f como una función definida en un subconjunto de V con valores en k. La función f se puede considerar como tal en los punto $p \in V$ tales que existan funciones $a, b \in A(V)$ con $b(p) \neq 0$ y $f = \frac{a}{b}$. Al conjunto de puntos en los que f está bien definida lo denotaremos por $D(f)$.

Nota: las funciones a y b mencionadas antes no tienen por qué ser únicas. Evidentemente, puede existe otra fracción $\frac{c}{d}$ con $d(p) \neq 0$, pero $f = \frac{c}{d}$ solamente si $ad = cb$, y por tanto $\frac{a(p)}{b(p)} = \frac{c(p)}{d(p)}$, con lo que f está bien definida como función.

Definición 22 *Sea W una variedad proyectiva y sea $A_h(W)$ su anillo de coordenadas. Igual que en el caso afín, $A_h(W)$ es un dominio y se puede construir su cuerpo de fracciones al que denotaremos por $k_h(W)$.*

Al contrario que en el caso afín, no todos los elementos de $k_h(W)$ son funciones. Si tomamos dos polinomios homogéneos del mismo grado g, $G, H \in k[X_0, ..., X_n]$, con $H \neq 0$, entonces $F = \frac{G}{H}$ sí es una función definida en un subconjunto de W, ya que si $p \in W$ es un punto que no anula al polinomio H, entonces $F(\lambda p) = \frac{G(\lambda p)}{H(\lambda p)} = \frac{\lambda^g G(p)}{\lambda^g H(P)} = \frac{G(p)}{H(p)} = F(p)$ para todo $\lambda \in k$ no nulo. En consecuencia, si $H \notin I_h(W)$, la fracción $\frac{G+I_h(W)}{H+I_h(W)} \in k_h(W)$ sí representa una función definida en un subconjunto de W.

Al igual que en el caso afín, si tenemos $F, G, F', G' \in k[X_0, ..., X_n]$ dos pares de polinomios homogéneos con $gr(F) = gr(G)$ y $gr(F') = gr(G')$, y $G, G' \notin I_h(W)$, entonces $\frac{F+I_h(W)}{G+I_h(W)}$ y $\frac{F'+I_h(W)}{G'+I_h(W)}$ definen la misma función en un punto $p \in W$ tal que G y G' no se anulan en él, solamente si $FG' = F'G$ en $I_h(W)$, por lo tanto $\frac{F+I_h(W)}{G+I_h(W)}(p) = \frac{F'+I_h(W)}{G'+I_h(W)}(p)$.

A la vista de esto, tenemos que una función z como las descritas, está unívocamente definida como función y que además el subconjunto de W en el que está definidas es el abierto formado por todos los puntos $p \in W$ en los que existe algún par de polinomios $F, G \in k[X_0, ..., X_n]$ homogéneos y del mismo grado, de modo que $z = \frac{F+I_h(W)}{G+I_h(W)}$ y $G(p) \neq 0$. A este abierto lo denotaremos por $D(z)$.

Definición 23 *Sea W una variedad proyectiva. A los elementos $z \in k_h(W)$ que se puedan escribir como $z = \frac{F+I_h(W)}{G+I_h(W)}$ donde $F, G \in k[X_0, ..., X_n]$ son dos polinomios homogéneos del mismo grado con $G \notin I_h(W)$ los llamaremos* funciones racionales *y al conjunto de las funciones racionales lo denotaremos por $k(W)$.*

Si $z \in k(W)$, y expresamos z como $\frac{F}{G}$ en todos los puntos de W en los que G no se anula, entonces podemos expresar z^{-1} como $\frac{G}{F}$ en todos los puntos de W en los que F no se anula.

Proposición 17 *$k(W)$ es un subcuerpo de $k_h(W)$.*

Demostración: Basta con ver que si $z, w \in k(W)$, con $w \neq 0$, entonces $(z - w), (zw^{-1}) \in k(W)$. Sean $F, G, F', G' \in k[X_0, ..., X_n]$ dos pares de polinomios homogéneos con grados $gr(F) = gr(G)$ y $gr(F') = gr(G')$ y con $G, G' \notin I_h(W)$ tales que $z = \frac{F+I_h(W)}{G+I_h(W)}$, $w = \frac{F'+I_h(W)}{G'+I_h(W)}$.

Se verifica $z - w = \frac{FG'-G-F'+I_h(W)}{GG'+I_h(W)} \in k(W)$, pues al ser F, F', G, G' homogéneos, si $FG' - GF' \neq 0$, $FG' - GF'$ y GG' son homogéneos y del mismo grado y $GG' \notin I_h(W)$, y si $FG' - GF' = 0$, $0 \in k(W)$.

Por otra parte, tenemos que $F \notin I_h(W)$, pues $w \neq 0$, y por tanto $w^{-1} = \frac{G'+I_h(W)}{F'+I_h(W)} \in k(W)$, y también $zw^{-1} = \frac{FG'+I_h(W)}{GF'+I_h(W)} \in k(W)$ pues FG' y GF' son homogéneos del mismo grado y $GF' \notin I_h(W)$.

Definición 24 *Dada $z \in k(V)$ una función racional de una variedad (afín o proyectiva) V, llamaremos* cero *de de z a todo punto $p \in D(z)$ tal que z se anule en p como función de $D(z) \subset V$ en k. Llamaremos* polo *de z a todo punto $p \notin D(z)$.*

En lo que queda de sección vamos a ilustrar la relación existente entre el cuerpo de funciones de una variedad afín y el de su clausura proyectiva.

Notación: De aquí en adelante hasta el final de la sección representaremos como $\overline{F}$ las clases $F + I(V)$.

Proposición 18 *Sean* $V \in \mathbb{A}^n$ *una variedad afín y* $F, G \in k[X_0, ..., X_n]$ *polinomios tales que* $\overline{F} = \overline{G}$ *en* $A(V*)$. *Entonces,* $\overline{F_*} = \overline{G_*}$ *en* $A(V)$.

Demostración: Como $\overline{F} = \overline{G}$ en $A(V*)$, $F - G \in I(V)^*$, es decir $(F-G)_* = F_* - G_* \in I(V)$ y por lo tanto $\overline{F_*} = \overline{G_*}$ en $A(V)$, como queríamos.

Proposición 19 *Sean* $V \in \mathbb{A}^n$ *una variedad afín y* $f, g \in k[X_1, ..., X_n]$ *polinomios con* $gr(f) = gr(g)$ *y* $\overline{f} = \overline{g}$ *en* $A(V)$. *Entonces,* $\overline{f^*} = \overline{g^*}$ *en* $A(V^*)$.

Demostración: Como $\overline{f} = \overline{g}$ en $A(V)$, $f - g \in I(V)$, es decir $(f-g)^* = f^* - g^* \in I(V)^*$ por ser f y g del mismo grado, luego $\overline{f^*} = \overline{g^*}$ en $A(V^*)$, como queríamos.

Proposición 20 *Sea* $V \in \mathbb{A}^n$ *una variedad afín. Entonces, los cuerpos de funciones* $k(V)$ *y* $k(V^*)$ *son isomorfos. Además, las funciones de* $k(V)$ *vienen dadas por las restricciones de las funciones de* $k(V^*)$ *a* V.

Demostración: Consideramos la aplicación $\phi : k(V^*) \longrightarrow k(V)$ dada por $\phi(\frac{\overline{F}}{\overline{G}}) = \frac{\overline{F_*}}{\overline{G_*}}$ para toda escritura válida $\frac{\overline{F}}{\overline{G}}$ de un elemento de $k(V^*)$.

ϕ está bien definida en virtud de la proposición 18 y de que si tenemos dos escrituras $z = \frac{\overline{F}}{\overline{G}} = \frac{\overline{H}}{\overline{E}}$ de un elemento $z \in k(V^*)$ entonces $FE - HG \in I(V)^*$, es decir, $F_*E_* - H_*G_* \in I(V)$, por lo tanto $\phi(\frac{\overline{F}}{\overline{G}}) = \frac{\overline{F_*}}{\overline{G_*}} = \frac{\overline{H_*}}{\overline{E_*}} = \phi(\frac{\overline{H}}{\overline{E}})$ en $k(V)$.

Veamos que ϕ es un morfismo: sean $\frac{\overline{F}}{\overline{G}}, \frac{\overline{F'}}{\overline{G'}}$ dos elementos de $k(V^*)$.

$\phi(\frac{\overline{F}}{\overline{G}} + \frac{\overline{F'}}{\overline{G'}}) = \phi(\frac{\overline{FG'+GF'}}{\overline{GG'}}) = \frac{\overline{F_*G'_*+G_*F'_*}}{\overline{G_*G'_*}} = \frac{\overline{F_*}}{\overline{G_*}} + \frac{\overline{F'_*}}{\overline{G'_*}} = \phi(\frac{\overline{F}}{\overline{G}}) + \phi(\frac{\overline{F'}}{\overline{G'}})$.

$\phi(\frac{\overline{F}}{\overline{G}}\frac{\overline{F'}}{\overline{G'}}) = \phi(\frac{\overline{FF'}}{\overline{GG'}}) = \frac{\overline{F_*F'_*}}{\overline{G_*G'_*}} = \frac{\overline{F_*}}{\overline{G_*}}\frac{\overline{F'_*}}{\overline{G'_*}} = \phi(\frac{\overline{F}}{\overline{G}})\phi(\frac{\overline{F'}}{\overline{G'}})$.

Veamos ahora que ϕ es inyectiva: supongamos que $\phi(\frac{\overline{F}}{\overline{G}}) = \phi(\frac{\overline{F'}}{\overline{G'}})$, eso implica que $\frac{\overline{F_*}}{\overline{G_*}} = \frac{\overline{F'_*}}{\overline{G'_*}}$, luego $FG' - GF' \in I(V)^*$, lo que implica que $\frac{\overline{F}}{\overline{G}} = \frac{\overline{F'}}{\overline{G'}}$.

Por último, sólo nos queda ver que ϕ es sobreyectiva: Sean $\frac{\overline{f}}{\overline{g}} \in k(V)$, siendo f y g dos representantes de $\overline{f}$ y $\overline{g}$. Sea $D = gr(f)$ y $d = gr(g)$, si $D \geq d$ tomaremos $F = f^*$ y $G = X_0^{D-d}g^*$, en caso contrario, tomaremos $F = X_0^{d-D}f^*$ y $G = g^*$, entonces $\phi(\frac{\overline{F}}{\overline{G}}) = \frac{\overline{f}}{\overline{g}}$.

Veamos ahora que si $\frac{\overline{F}}{\overline{G}} \in k(V^*)$, entonces $\frac{\overline{F}}{\overline{G}} = \phi(\frac{\overline{F}}{\overline{G}})$ en V. Sea $p = (p_1, ..., p_n) \in V$, entonces $\frac{\overline{F}}{\overline{G}}(1; p_1; ....; p_n) = \frac{\overline{F}(1;p_1;...;p_n)}{\overline{G}(1;p_1;...;p_n)} = \frac{\overline{F_*}(p)}{\overline{G_*}(p)} = \frac{\overline{F_*}}{\overline{G_*}}(p) = \phi(\frac{\overline{F}}{\overline{G}})(p)$, como queríamos.

Nota: Como $k(V)$ y $k(V^*)$ son isomorfos a veces diremos que son iguales, de modo que un elemento $z \in \Gamma(V) \subset k(V)$ se puede representar de dos formas, como $z = F + I(V)$ en el caso afín, o como $z = \frac{F^*+I(V)}{X_0^d+I(V)}$, donde $d = gr(F)$, en el caso proyectivo. Es inmediato comprobar que ambas expresiones coinciden en todo punto de V.

1.5. Variedades

En esta sección trabajaremos con la topología de Zariski de $\mathbb{P}^n$.

A continuación vamos a dar una definición de variedad más amplia a las dos dadas en las primeras secciones del capítulo.

Definición 25 *Llamaremos* variedad *a todo conjunto abierto X no vacío de alguna variedad proyectiva V.*

Nota: En ocasiones se toma como definición de variedad una más general, en este caso a la definición que hemos dado aquí se le conoce como *variedad cuasi-proyectivas.*
Nota: Con esta definición es claro que las variedades proyectivas son variedades pues basta tomar $X = V$.
Nota: Las variedades afines también son variedades pues si V es una variedad afín, V^* es una variedad proyectiva y como $\mathbb{A}^n$ es un abierto de $\mathbb{P}^n$ y $V = V^* \cap \mathbb{A}^n$, V es un abierto de la variedad proyectiva V^*, es decir, una variedad

Proposición 21 *Sea V una variedad proyectivo. Entonces, toda variedad $X \subset V$ es densa en V.*

Demostación: Si alguna variedad X no fuera densa en V existiría U un abierto no vacío de V con $U \cap X = \emptyset$. LLamemos $Z = V \setminus U$ y $Z' = V \setminus X$, dos cerrados de X. Entonces, $Z \cup Z' = V$ pues si $v \in V$ y $v \notin Z \cup Z'$, entonces, $v \in U \cap X$. Pero V es irreducible, luego $Z = V$ o $Z' = V$, de lo que deducimos que $U = \emptyset$ o $X = \emptyset$, contra hipótesis.

Definición 26 *Si $U \subset X$ es un conjunto abierto, U será también abierto de V, con lo que también será una variedad. Decimos que U es una* subvariedad abierta *de X.*

Definición 27 *Si $Y \subset X$ es un subconjunto cualquiera, decimos que Y es* irreducible *si no es unión de dos cerrados propios.*

Proposición 22 *Si Y es un conjunto cerrado de $X \subset V$ e $\overline{Y}$ es su clausura en V, entonces $Y = X \cap \overline{Y}$.*

Demostración: Este es un resultado de topología general.

Si F es un cerrado en V, F es un conjunto cerrado de $\mathbb{P}^n$ por serlo V, es decir, un conjunto algebraico.

Proposición 23 *Sean V una variedad proyectiva e Y un conjunto cerrado e irreducible en una variedad $X \subset V$. Entonces, si $\overline{Y}$ es la clausura de Y en V, $\overline{Y}$ es irreducible en V.*

Demostración: Razonaremos por reducción al absurdo. Supondremos que $\overline{Y}$ no es irreducible y veamos que entonces Y tampoco lo es. Si $\overline{Y}$ no es irreducible en V, existirán A y B, cerrados de V, tales que $\overline{Y} = A \cup B$ y $A \neq \overline{Y}$, $B \neq \overline{Y}$.
Tomamos $A' = A \cap X$ y $B' = B \cap X$, cerrados en X.
Veamos que $Y = A' \cup B'$: por la proposición 22, sabemos que

$$Y = \overline{Y} \cap X = (A \cup B) \cap X = (A \cap X) \cup (B \cap X) = A' \cup B'$$

tal y como queríamos.
Por últimos, si vemos que $A' \neq Y$ y que $B' \neq Y$ llegaremos a la contradicción deseado. Razonaremos con A', el razonamiento con B' es análogo:
Si $A' = Y$, en particular, $Y \subset A' = A \cap X \subset A \subset \overline{Y}$. Tendríamos, pues, un cerrado A cumpliendo $Y \subset A \subset \overline{Y}$, de lo que se deduce que $A = \overline{Y}$, en contra de la hipótesis.

Puesto que Y es un abierto de $\overline{Y}$, que es una variedad proyectiva, es una variedad y tiene sentido la siguiente definición.

Definición 28 *Un conjunto cerrado $Y \subset X$ irreducible se dice que es una* subvariedad cerrada *de X.*

Nota: Otra forma de ver que las variedades afines son variedades es teniendo en cuenta la definición anterior y que $\mathbb{A}^n$ es un abierto de $\mathbb{P}^n$, pues es evidente que las variedades afines son subvariedades cerradas de $X = \mathbb{A}^n$, y por tanto variedades.

Proposición 24 *Las variedades son irreducibles.*

Demostración: Si X es una variedad, su clausura $\overline{X}$ será una variedad proyectiva, luego irreducible. Supongamos que $X = Z \cup Z'$ donde Z y Z' son dos cerrados de X. Entonces, $\overline{Z}, \overline{Z'}$ son dos cerrados de $\overline{X}$ y además $\overline{Z} \cup \overline{Z'} = \overline{X}$. Pero como $\overline{X}$ es irreducible, necesariamente $\overline{Z} = \overline{X}$ o $\overline{Z'} = \overline{X}$, de lo que se deduce que $Z = X$ o $Z' = X$, luego X es irreducible.

Proposición 25 *Sea X una variedad y sea Y un cerrado de X. Entonces, Y es irreducible si y solamente si el cerrado de $\mathbb{P}^n$ $\overline{Y}$ es irreducible.*

Demostración: Si Y es irreducible en X, y $Z \cup Z' = \overline{Y}$ donde Z y Z' son dos cerrados de $\overline{Y}$, entonces $Z \cap Y$ y $Z' \cap Y'$ serán dos cerrados de Y cuya unión será Y, podemos suponer entonces que $Z \cap Y = Y$, entonces $\overline{Z \cap Y} = Z = \overline{Y}$ y por tanto $\overline{Y}$ es irreducible.

Si ahora $\overline{Y}$ es irreducible y Z, Z' son dos cerrados de Y cuya unión coincide con Y, entonces $\overline{Y} = \overline{Z} \cup \overline{Z'}$, con lo que podemos suponer que $\overline{Y} = \overline{Z}$. Entonces, $\overline{Z} \cap Y = Z = Y$ y por tanto Y es irreducible.

Definición 29 *Sea X una variedad. Ya vimos que $\overline{X}$ es una variedad proyectiva. Llamaremos cuerpo de fracciones de X, $k(X)$, a $k(\overline{X})$.*

Proposición 26 *Las funciones racional son continuas.*

Demostración: Sea $z \in k(X)$ una función racional de una variedad X. Entonces, $z : D_z \longrightarrow k$ donde $k = \mathbb{A}$ se considera con la topología de Zariski, y en este caso, los cerrados de k son el total, el vacío y los conjuntos finitos. Queremos ver que la contraimagen de un cerrado por z es cerrado de D_z, y a vista de lo anterior, basta con probarlo para los conjuntos unipuntuales.

Además, si tenemos un recubrimiento de D_z, el ver que la contraimagen de un punto es un cerrado de D_z es equivalente a ver que lo es en cada uno de los abiertos del recubrimiento. Sabemos que D_z es la unión de los abiertos $X \setminus V_h(G)$ donde $\frac{F}{G}$ es una expresión que define a la función. Trabajaremos, por tanto con este recubrimiento y trabajaremos con cada uno de sus abiertos.

Sea $\lambda \in k$ cualquiera. Entonces, $\frac{F(p)}{G(p)} = \lambda$ si y solamente si $F(p) - \lambda G(p) = (F - \lambda G)(p) = 0$, es decir, si $p \in V_h(F - \lambda G)$. Luego la imagen de todo punto es un cerrado.

Asociado a las variedades tenemos lo que hemos llamado cuerpo de funciones racionales, vamos a definir ahora un segundo objeto que nos resultará de utilidad para el estudio de las variedades.

Definición 30 *Sea X una variedad y sea $p \in X$ un punto cualquiera. Definimos el* anillo local *de X y lo denotamos como $O_p(X)$ como el conjunto de funciones racionales de X definidas en p. Es decir,*

$$O_p(X) = \{z \in k(X) : p \in D(z)\}.$$

Nota: como $k(X) = k(\overline{X})$ entendiendo que una función racional z tiene dominio $D_{\overline{X}}(z)$ como elemento de $k(\overline{X})$ y dominio $D_X(z) = D_{\overline{X}}(z) \cap X$, también se tiene $O_p(X) = O_p(\overline{X})$ para todo punto $p \in X \subset \overline{X}$.

Proposición 27 *Sea X una variedad cualquiera. Para todo punto $p \in X$, el anillo local $O_p(X)$ es un subanillo de $k(X)$.*

Demostración: Sea $p \in X$, es evidente que $O_p(X) \subset k(X)$.Sean $\frac{F}{G}, \frac{F'}{G'} \in O_p(X)$ cualesquiera, veamos que el producto y la diferencia de dos elementos del anillo local da otro elemento del mismo:

Se verifica $\frac{F}{G}\frac{F'}{G'} = \frac{FF'}{GG'}$. Como $G(p) \neq 0$ y $G'(p) \neq 0$, $(GG)(p) \neq$. Además, para el caso proyectivo, $gr(F) = gr(G)$ y $gr(F') = gr(G')$, luego $gr(FF') = gr(GG')$. Por tanto, $\frac{F}{G}\frac{F'}{G'} \in O_p(X)$.

Se tiene $\frac{F}{G} - \frac{F'}{G'} = \frac{FG'-F'G}{GG'}$. Si $FG' - GF' = 0$, $\frac{F}{G} - \frac{F'}{G'} = 0 \in O_p(X)$. Nuevamente $(GG')(p) \neq 0$. En el caso proyectivo, si $FG' - GF' \neq 0$, por ser F, G, F' y G' polinomios homogéneos, entonces tenemos también que $gr(FG' - GF') = gr(FG') = gr(F'G) = gr(GG')$.

Proposición 28 *El anillo local $O_p(X)$ de una variedad X en un punto $p \in X$ posee un único maximal $M_p(X) = \{z \in O_p(X) : z(p) = 0\}$.*

Demostración: Veamos que $M_p(X)$ es un ideal, y que todo elemento de $O_p(X)$ que no esté en $M_p(X)$ es una unidad:

Empecemos viendo que $M_p(X)$ es un ideal. Sea $z \in M_p(X)$ y $w \in O_p(X)$, entonces $xw(p) = 0$, luego $zw \in M_p(X)$. Sean ahora $z, w \in M_p(X)$, entonces $(z + w)(p) = z(p) + w(p) = 0 + 0 = 0$, luego $z + w \in M_p(X)$. Es decir, $M_p(X)$ es un ideal.

Veamos que si $z \in O_p(X)$, $z \notin M_p(X)$, entonces z es una unidad. $z(p) \neq 0$, luego para cada par $F, G \in A(X)$ tal que z se pueda representar como $z = \frac{F}{G}$, se tiene que $F(p) \neq 0$, con lo que z tiene inverso y vendrá determinado por las fracciones $z^{-1} = \frac{G}{F}$.

Nota: Es evidente que si X es un variedad y $z \in k(X)$ es una función racional, z está definida en un punto $p \in X$ si y solamente si $z \in O_p(X)$. Y p será un cero de z si y solamente si z no es una unidad de $O_p(X)$.

Nota: en álgebra conmutativa se conoce como anillo local a todo anillo con un único ideal maximal.

Proposición 29 *Sea X una variedad, entonces $K(X)$ es el cuerpo de fracciones de $O_p(X)$ para todo $p \in X$.*

Demostración: Sea $\frac{z}{w}$ un elemento del cuerpo de fracciones de $O_p(X)$ con $z, w \in O_p(X)$ y $w \neq 0$. Como $z, w \in k(X)$, $\frac{z}{w} = zw^{-1} \in k(X)$.

Sea ahora $z \in k(X)$ una función racional cualquiera. Existirán polinomios F, G homogéneos y del mismo grado tal que $G \notin I_h(\overline{X})$ y tal que $z = \frac{F+I(\overline{X})}{G+I(\overline{X})}$. Sea $m = gr(F)$ y $L \neq 0$ un polinomio homogéneo de grado 1 tal que $L(p) \neq 0$, entonces $L \notin I(\overline{X})$. Llamaremos entonces $z' = \frac{F+I(\overline{X})}{L^m+I(\overline{X})}$ y $w' = \frac{L^m+I(\overline{X})}{G+I(\overline{X})}$. Las fracciones z' y w' son dos funciones racionales de $k(X) = k(\overline{X})$ que además están definidas en p, luego $z', w' \in O_p(X)$ y, por tanto $z = \frac{z'}{w'}$ es un elemento del cuerpo de fracciones de $O_p(X)$.

Nota: aunque ya lo habíamos mencionado antes, la proposición siguiente demuestra que $D(z)$ es un abierto.

Proposición 30 *Sea W una variedad proyectiva y sea $z \in k(W)$ una función racional cualquiera. Entonces, el conjunto de polos de z es un subconjunto algebraico de W.*

Demostración: Consideramos J el ideal generado por todos los $G \in k[X_0, ..., X_n]$ homogéneos tales que $G \notin I_h(W)$ y tales que exista $F \in k[X_0, ..., X_n]$ homogéneo y del mismo grado que G cumpliendo $z = \frac{F+I_h(W)}{G+I_h(W)}$. Veamos que el conjunto de polos de z viene dado por $V_h(J)$.

Sea $p \in V_h(J)$, entonces todo par de polinomios F, G tales que cumplen los requisitos para poder expresar z como $z = \frac{F+I_h(W)}{G+I_h(W)}$ cumple que $G(p) = 0$, es decir, $p \notin D(z)$, como queríamos.

De igual forma, si $q \in W$ es un punto tal que $q \notin D(z)$ no existen polinomios F, G homogéneos del mismo grado con $G \notin I_h(W)$ tales que $z = \frac{F+I_h(W)}{G+I_h(W)}$ y que $G(p) \neq 0$. Por lo tanto, $G(p) = 0$ para todo $G \in J$, es decir, $q \in V_h(J)$.

Corolario 2 *Sea X una variedad y sea $z \in k(X)$ una función racional cualquiera. Entonces, el conjunto de polos de z es un cerrado de X.*

Demostración: Como $k(X) = k(\overline{X})$, y el abierto de definición de $z \in k(X)$ es $D_X(z) = D_{\overline{X}}(z) \cap X$, y en virtud de la proposición 30 el conjunto de polos de $z \in k(\overline{X})$ es un cerrado V de $\overline{X}$, el conjunto de polos de z será $V \cap X$, un cerrado de X.

Proposición 31 *Sea V una variedad afín, entonces $\cap_{p \in V} O_p(V) = A(V)$.*

Demostración: Es inmediato comprobar que $A(V) \subset \cap_{p \in V} O_p(V)$.

Sea ahora $z \in \cap_{p \in V} O_p(V)$, entonces, para cada $p \in V$, existen $f_p, g_p \in A(V)$ tales que $z = \frac{f_p}{g_p}$ y $g_p(p) \neq 0$. Sea $G_p \in k[X_1, ..., X_n]$ un representante de g_P. Consideramos el ideal $I = (\{G_p\}_{p \in V})$. En virtud del teorema de la base de Hilbert, existe $\{G_1, ..., G_s\}$ un conjunto finito de generadores de I. Podemos suponer que existen $p_1, ..., p_s \in V$ tales que $G_{p_i} = G_i$, pues de no ser así, al ser I una familia finitamente generada, podríamos poner a g_i como una combinación finita de elementos de $\{G_p\}_{p \in V}$ y tomaríamos estos como generadores del ideal. Denotamos por f_i a f_{p_i}.

Si $q \in V$ es un punto cualquiera de la variedad, $G_q = h_1 G_1 + ... + h_s G_s$ para ciertos $h_i \in k[X_1, ..., X_n]$, luego no puede ocurrir que para todo i $G_i(q) = 0$, pues entonces $G_q(q) = 0$. Es decir, $\cup_{i=1,...,s} P(G_i) = V$ cuando $P(G_i)$ representa los puntos de V donde no se anula G_i.

Veamos ahora que $V(I + I(V)) = \emptyset$: si existiera $q \in V(I + I(V))$, para todo polinomio $f \in I(V)$ y para todo $i = 1, ..., s$ $f(q) = 0$ y $G_i(q) = 0$. Sin embargo, $\cup_{i=1,...,s} D(G_i) = V$, luego para todo $p \in V$ existe i tal que $G_i(p) \neq 0$. Con lo que q no puede existir.

Como $V(I + I(V)) = \emptyset$, se tiene que $1 \in Rad(I + I(V))$ con lo que $1 \in I + I(V)$, pues si J es un ideal cualquiera y $1 \in Rad(J)$, $1^n = 1 \in J$ para algún n. Por tanto, existen $H_1, ..., H_s \in k[x_1, ..., x_n]$ tales que $1 = \overline{H_1} g_1 + ... + \overline{H_s} g_s$.

Por último, tenemos que

$$z = z(H_1 g_1 + ... + H_s g_s + I(V)) = \frac{f_1}{g_1} \overline{H_1} g_1 + ... + \frac{f_s}{g_s} \overline{H_s} g_s = f_1 \overline{H_1} + ... + f_s \overline{H_s} \in A(V),$$

tal y como queríamos.

Proposición 32 *Sea W una variedad proyectiva, entonces $\cap_{p \in W} O_p(W) = k$.*

Demostración: Es inmediato comprobar que $k \subset \cap_{p \in W} O_p(W)$.

Sea ahora $z \in \cap_{p \in W} O_p(W)$. Como en la demostración anterior, para cada $p \in W$, existen polinomios $F_p, G_p \in k[X_0, ..., X_n]$ tales que $z = \frac{F_p+I_h(W)}{F_p+I_h(W)}$ y $G_p(p) \notin I_h(W)$. Consideramos también el ideal $J = (\{G_p\}_{p \in W})$. Al igual que antes, virtud del teorema de la base de Hilbert, existe $\{G_1, ..., G_t\}$ un conjunto finito de generadores de J y suponer que existen $p_1, ..., p_t \in V$ tales que $G_{p_i} = G_i$. Denotaremos por F_i a F_{p_i}.

Siguiendo el mismo razonamiento que en la demostración anterior, deducimos que para todo $p \in W$ existe i tal que $G_i(p) \neq 0$, y de aquí deducimos que $V_h(J + I_h(W)) = \emptyset$.

En virtud del lema 1, existe $s > 0$ tal que $I_s \subset J + I_h(W)$. Entonces, si tomamos $P \in I_s + I_h(W)$, podemos escribir $P = G_1 H_1 + ... + G_t H_t + I_h(W)$. Por tanto, $zP = F_1 H_1 + ... + F_t G_t + I_h(W)$ que es nuevamente un elemento de $I_s + I_h(W)$, es decir, $zI_s + I_h(W) \subset I_s + I_h(W)$, y reiterando el razonamiento, tenemos que para todo entero $q > 0$, $z^q I_s + I_h(W) \subset I_s + I_h(W)$. En particular, $X_0^s \in I_s$, luego

$\overline{X_0^s}z^q \in I_s + I_h(W) \subset A_h(W)$. Como consecuencia inmediata, tenemos que $A_h(W)[z]$ es un subanillo de $\overline{X_0^{-s}}A_h(W)$ ya que si $\sum_{i=0}^{d} a_i z^i \in A_h(W)[z]$, se verifica la igualdad $a_i z^i = a_i \overline{X_0^s} z^i \overline{X_0^{-s}}$ donde $a_i, \overline{X_0^s}z^i \in A_h(W)$. Además, por definición, $\overline{X_0^{-s}}A_h(W)$ es un módulo de generación finita del anillo $A_h(W)$, y como $A_h(W)$ es un anillo noetheriano en virtud del lema 26, aplicando la proposición 81, concluimos que $\overline{X_0^{-s}}A_h(W)$ también es un módulo noetheriano y como $A_h(W)[z]$ es un submódulo suyo, aplicando la proposicion 78, concluimos que $A_h(W)[z]$ es un módulo de $A_h(W)$ de generación finita.

Como $A_h(W)[z]$ es de generación finita, existen polinomios $P_1,...,P_r \in A_h(W)[Y]$ de modo que $A_h(W)[z] = \sum_{i=1}^{r} P_i(z)A_h(W)$. Es decir, si m es un entero mayor que el grado de P_i como polinomio en Y para todo i, $z^m \in A_h(W)[z]$ y existen elementos $a_1,...,a_r \in A_h(W)$ cumpliendo $z^m = a_1P_1(z)+...+a_rP_r(z) = 0$. Equivalentemente, el polinomio $\phi(Y) = Y^m - a_1P_1(Y) - ... - a_rP_r(Y)$ es un polinomio mónico de $A_h(W)$ que se anula en z. Escribamos $\phi(Y) = Y^m \sum_{i=0}^{m-1} b_i Y^i$ para ciertos $b_i \in A_h(W)$

Ahora bien, si escribimos $z = \frac{F+I_h(W)}{G+I_h(W)}$ para $F, G \in k[X_0,...,X_n]$ del mismo grado y con $G \notin I_h(W)$ y $b_i = B_i + I_h(W)$ donde $B_i \in k[X_0,...,X_n]$, tenemos que $\frac{F^m}{G^m} + \sum_{i=0}^{m-1} B_i \frac{F^i}{G^i} \in I_h(W)$, y si multiplicamos la expresión por G^m, nos queda que $F^m + \sum_{i=0}^{m-1} B_i F^i G^{m-i} \in I_h(W)$, luego todas las partes homogéneas de la expresión estarán en $I_h(W)$. En particular, si nos fijamos en la parte homogéneas de grado m, tenemos que $F^m + \sum_{i=0}^{m-1} B_i^0 F^i G^{m-i} \in I_h(W)$ donde B_i^0 representa la parte homogénea de grado 0 de B_i, un elemento de k. Sacando factor común a G^m, tenemos que $G^m(\frac{F^m}{G^m} + \sum_{i=0}^{m-1} B_i^0 \frac{F^i}{G^i}) \in I_h(W)$ y como $G \notin I_h(W)$ G^m tampoco lo estará, con lo que, necesariamente, $\frac{F^m}{G^m} + \sum_{i=0}^{m-1} B_i^0 \frac{F^i}{G^i} \in I_h(W)$, es decir, $z^m + \sum_{i=0}^{m-1} B_i^0 z^i = 0$.

Hemos encontrado, por tanto, un polinomio con coeficientes en k en el que z se anula, es decir, z es algebraico sobre k. Sin embargo, k es algebraicamente cerrado por hipótesis, con lo que $z \in k$, como queríamos.

Definición 31 *Llamaremos* anillo de las funiciones regulares *al anillo* $\Gamma(X) \cap_{p \in X} O_p(X)$ *y a sus elementos los llamaremos* funciones regulares.

Nota: Si X es una variedad y $U \subset X$ es una subvariedad abierta, como U es denso en X, $\overline{U} = \overline{X}$ y con ellos $k(U) = k(X)$ y $O_p(U) = O_p(X)$ para todo $p \in U \subset X$.

El anillo de funciones regulares es el último objeto que definiremos asociado a las variedades. A continuación daremos una serie de resultados asociados a estos objetos y que utilizaremos más adelante.

Proposición 33 *Sea X una variedad y sea $z: X \longrightarrow k$ una función. Entonces, z es una función regular de $\Gamma(X)$ si y solamente si para todo punto $p \in X$ existe un abierto $U \subset X$ que contiene a p y una función regular $w \in \Gamma(U)$ de modo que $z = w$ como funciones definidas en U.*

Demostración: Supongamos que z es una función regular de $\Gamma(X)$. Entonces, basta con tomar $U = X$.

Veamos ahora la otra implicación. Sea $p \in X$ un punto cualquiera. Existirá un abierto U_p de X que contiene a p y una función racional $w_p \in \Gamma(U_p)$ tal que $z = w_p$ en U. Existirán también $F_p, G_p \in k[X_0,...,X_n]$ polinomios homogéneos del mismo grado tal que G_p no se anula en p y tales que $w_p = \frac{F_p + I_h(\overline{U_p})}{G_p + I_h(\overline{U_p})}$.

Sea $q \in X$, $q \neq p$ otro punto. Igual que antes existirán un entorno abierto $U_q \subset X$ de q, una función racional $w_q \in \Gamma(U_q)$ con $w_q = z$ en U_q y polinomios $F_q, G_q \in k[X_0,...,X_n]$ homogéneos, del mismo grado con $G_q(q) \neq 0$ y con $W_q = \frac{F_q + I_h(\overline{U_q})}{G_q + I_h(\overline{U_q})}$.

Si vemos que $w_q = w_p$ tendremos que $q \in D(w_p)$ y con ellos que $X \subset D(w_p)$ y que $z = w_p$ como funciones definidas en todo X, es decir, $z \in \Gamma(X)$.

Teniendo en cuenta que $\overline{U_p} = \overline{U_q} = \overline{X}$, para ver que $\frac{F_p+I_h(\overline{U_p})}{G_p+I_h(\overline{U_p})} = \frac{F_q+I_h(\overline{U_q})}{G_q+I_h(\overline{U_q})}$ necesitamos ver $F_qG_p - F_pG_q \in I_h(X)$. Tenemos que el polinomio homogéneo $F_qG_p - F_pG_q$ se anula en el abierto $U_q \cap U_p \cap D(w_q) \cap D(w_p)$ de X ya que en este abierto $w_p = z = w_q$. Como $F_qG_p - F_pG_q$ es un polinomio que se anula en un abierto denso de X, se anulará en todo X.

Lema 5 *Sean $q, p_1, ..., p_s \in \mathbb{P}^n$ puntos cuales quiera. Existen, existe un polinomio homogéneo de grado 1 en $k[X_0, ..., X_n]$ que se anula en q pero no en $p_1, ..., p_s$.*

Demostración: Supongamos que $n = 1$. Denotemos por $q = (A; B)$ y por $p_i = (a_i; b_i)$. Buscamos un polinomio $L(X_0, X_1) = \lambda_0 X_0 + \lambda_1 X_1$ tal que $L(q) = \lambda_0 A + \lambda_1 B = 0$. Como podemos suponer $B \neq 0$, deducimos que $\lambda_1 = -\frac{A}{B}\lambda_0$. Para que $L(p_i) \neq 0$ para todo i necesitamos que $\lambda_0 \neq -\frac{a_i B}{Ab_i}$ para todo $i = 1, ..., s$ con $b_j \neq 0$ pero como $s < card(k)$ existe un elemento de k verificando esta ecuación.

Razonemos ahora por inducción sobre la dimensión del espacio proyectivo y supongamos que el enunciado es cierto para puntos en $\mathbb{P}^{n-1}$ y demostrémoslo en dimensión n:

Denotemos por $q = (q_0; ...; q_n)$ y por $p_i = (p_0^i; ...; p_n^i)$ para $i = 1, ..., s$. Como no puede ocurrir $q_k = 0$ para todo $k = 0, ..., n$ podemos suponer que al menos $q_k \neq 0$ para algún $k < n$ de modo que si denotamos por $q' = (q_0; ...; q_{n-1})$, $q' \neq 0$ y por tanto $q' \in \mathbb{P}^{n-1}$. De igual manera, denotamos por $p_i' = (p_0^i; ...; p_{n-1}^i)$. Se verifica que $p_i' = 0$ si y solo si $p_i = (0; ...; 0; 1)$.

Empecemos suponiendo que $p_i' \neq 0$ para todo $i = 1, ..., s$. Entonces, $p', q_1', ..., q_s' \in \mathbb{P}^{n-1}$ luego, por la hipótesis de inducción, existirá un polinomio homogéneo $L \in k[X_0, ..., X_{n-1}] \subset k[X_0, ..., X_n]$, de grado 1 de modo que $L(q') = L(q) = 0$ y tal que $L(p_i') = L(p_i) \neq 0$ para todo $p = 1, ..., s$. El polinomio L es el polinomio que buscábamos.

Supongamos ahora que para algún j $p_j' = 0$, por ejemplo, $j = s$. Siguiendo el razonamiento anterior, existe L un polinomio homogéneos y de grado 1 en $k[X_0, ..., X_n]$ de modo que $L(q) = 0$ y $L(p_i) \neq 0$ para $i = 1, ..., s-1$.

Sabemos que para algún $k < n$ $q_k \neq 0$. Consideremos ahora los puntos $(q_k; q_n), (0; 1) \in \mathbb{P}^1$. Por hipótesis de inducción, existirá un polinomio homogéneo de grado 1 $L' \in k[X_k, X_n] \subset k[X_0, ..., X_n]$, verificando que $L'(q_k, q_n) = L'(q) = 0$ y $L'(0, 1) = L'(p_s) \neq 0$.

Consideremos por último el polinomio homogéneo de grado 1 $L'' = L + \lambda L' \in k[X_0, ..., X_n]$. Este polinomio se anula en q independientemente de λ. Para que $L''(p_s) \neq 0$ hemos de exigir que $\lambda \neq 0$ y para que $L''(q_i) \neq 0$ para $i = 1, ..., s-1$ necesitamos que $\lambda \neq -\frac{L(p_i)}{L'(p_i)}$ para todo i con $L'(p_i) \neq 0$. Pero estas son s condiciones sobre λ, y como k es infinito, este λ sí que existe. Por tanto, L'' es el polinomio que buscábamos.

Proposición 34 *Sea $I \subset k[X_1, ..., X_n]$ un ideal con $V(I) = \{p_1, ..., p_m\}$ un conjunto finito. Denotemos por $O_i = O_{p_i}(\mathbb{A}^n)$. Existe un isomorfismo entre $\frac{k[X_1,...,X_n]}{I}$ y el producto cartesiano $\Pi_{i=1}^m \frac{O_i}{IO_i}$.*

Demostración: Sea $I_i = I(p_i)$, entonces $I \subset I_i$ para todo i. Denotemos por $R = \frac{k[X_1,...,X_m]}{I}$ y por $R_i = \frac{O_i}{IO_i}$. Entonces, podemos ver $k[X_1, ..., X_n] \subset O_i$, esta inclusión induce un morfismo $\phi_i : R \longrightarrow R_i$ y a su vez, todos estos morfismos inducen otro $\phi : R \longrightarrow \Pi_{i=1}^m R_i$ que lleva cada elemento $r \in R$ a la m-upla $(\phi_1(r), ..., \phi_n(r))$.

Por otra parte, en virtud del teorema de los ceros de Hilbert, $Rad(I) = I(\{p_1, ..., p_m\}) = \cap_{i=1}^m I_i$, luego, en virtud de la proposición 72 $(\cap_{i=1}^m I_i)^d \subset I$ para algún entero d.

Es evidente que para todo i $V(I_i) \cap V(\cap_{j \neq i} I_j) = \{p_i\} \cap \{p_j\}_{j \neq i} = \emptyset$, luego, en virtud de la proposición 3 I_i y $\cap_{j \neq i} I_j$ son comaximales, y aplicando la proposición 71, tenemos que

$$\cap_{j=1}^m I_j^d = (I_1 ... I_m)^d = (I_1 \cap ... \cap I_m)^d \subset I.$$

En virtud del lema 5, podemos tomar $F_i \in k[X_1, ..., X_n]$ con $F_i(p_i) = 1$ y $F_i(p_j) = 0$ cuando $j \neq i$. Notemos que $F_i^d \in I_j^d$ para todo $j \neq i$ Definimos $E_i = 1 - (1 - F_i^d)^d$. Como F_i^d divide a E_i, $E_i \in I_j^d$ si

$j \neq i$. También se verifica que $1-\sum_{i=1}^m E_i \in \cap_{j=1}^m I_j^d \subset I$ pues $E_i(p_i)=1$ y $E_i(q_i)=0$ si $j\neq i$. También se verifica $E_i - E_i^2 = E_i(1-F_i^d)^d \in (\cap_{j\neq i} I_j^d)I_i^d \subset I$ ya que $(\cap_{j\neq i} I_j^d)I_i^d \subset (\cap_{j=1}^m I_j^d) \subset I$. De igual forma $E_iE_j \in \cap_{k=1}^m I_k^d \subset I$.

Si denotamos por $e_i = E_i + I \in R$, hemos probado las siguientes igualdades: $e_i^2 = e_i$, $e_ie_j = 0$ si $i\neq j$ y $\sum_{i=1}^m e_i = 1$.

Veamos que si $G \in k[X_1,...,X_n]$ y $G(p_i)=1$ existe $t\in R$ tal que $tg = e_i$ donde $g = G+I$. Para ello tomamos $H = 1-G$ y consideramos el polinomio $(1-H)(E_i + HE_i + ... + H^{d-1}E_i) = E_i - H^dE_i$. Como $H \in I_i$, $H^dE_i \in I$ pues $H\in I_i$ y $E_i \in I_j^d$ para todo $j\neq i$, con lo que $H^dE_i \in \cap_{j=1}^m I_j^d \subset I$, y por tanto $g(e_i + he_i + .. + h^{d-1}e_i) = e_i$, como queríamos.

En general, si $p=(p_1,...,p_n)\in \mathbb{A}^n$ es un punto cualquiera, $O_p(\mathbb{A})^n$ es el conjunto de fracciones $\frac{P}{Q}$ con $P,Q \in k[X_1,...,X_n]$ y tal que $Q(p)\neq 0$. Entonces, si para algún polinomio $F \in k[X_1,...,X_n]$, $\phi_i(F+I) = 0$ entonces, $F + IO_i = 0$, es decir, existen polinomio $H_1,...,H_s$ que generan I y elementos $\frac{A_1}{M_1},...,\frac{A_s}{M_s} \in O_i$ con $F = \sum_{k=1}^s \frac{A_k}{M_k}H_k$, e igualando denominadores tenemos que $F = \frac{T}{G}$ donde $T\in A$ pues $H_k \in I$ para todo $k=1,...,s$ y $G(p_i)\neq 0$, pues como $\frac{A_k}{M_k} \in O_i$, $M_k(p_i)\neq 0$ para todo $k=1,...,s$. Entonce, $FG = A \in I$.

Veamos ahora que ϕ es un isomorfismo. Empecemos por ver que es inyectiva: si $\phi(f)=0$ para algún $f\in R$, existirá $G_i \in k[X_1,...,X_n]$ con $G_i(p_i)\neq 0$ y con $G_iF \in I$ donde F es un representante de f. Existen, entonces, elementos $t_i \in R$ con $t_ig_i = e_i$ donde $g_i = G_i + I$ y por lo tanto,

$$f = 1f = \sum e_if = \sum t_ig_if = 0.$$

Veamos ahora que es sobreyectiva: como $E_i(p_i)=1$, $\phi(e_i)$ es una unidad en R_i, pues en R_i las unidades son las clases de polinomios que no se anulan en p_i. También tenemos que

$$\phi_i(e_i)\phi_i(e_j) = \phi_i(e_ie_j) = \phi_i(0) = 0$$

si $i\neq j$ y que $\phi_i(e_j) = 0$ si $i \neq j$. Por lo tanto

$$\phi_i(e_i) = \sum \phi_i(e_j) = \phi(\sum e_j) = \phi(1) = 1.$$

Tomemos $z \in \Pi_iR_i$, que podremos escribir como $z = (\frac{A_1}{S_1} + IO_1,...,\frac{A_m}{S_m} + IO_m)$. Existirán polinomios $T_1,...,T_s \in k[X_1,...,X_n]$ con $T_iS_i + I = E_i + I$. Entonces, $\frac{A_i}{S_i} + IO_i = A_iT_i + IO_i$ si y solamente si $\frac{A_i - A_iS_iT_i}{S_i} = \frac{A_i - A_iE_i}{S_i} = \frac{A_i(E_i - E_i^2)}{S_iE_i} \in IO_i$, lo cual es cierto pues $\frac{A_i}{S_iE_i} \in R_i$ y $E_i - E_i^2 \in I$.

Entonces,

$$\phi_i(\sum_{j=1}^m A_jT_jE_j + I) = \sum_{j=1}^m A_jT_jE_j + IO_i = \sum_{j=1}^m \frac{A_jT_jE_jE_i}{E_i} + IO_i =$$

$$= \frac{A_iT_iE_i^2}{E_i} + IO_i = A_iT_i + IO_i = \frac{A_i}{S_i} + IO_i$$

y por tanto $\phi(\sum_{j=1}^m T_jA_jE_j + I) = z$ y concluimos.

Corolario 3 *Con la notación de la proposición 34,* $dim(\frac{k[X_1,...,X_n]}{I}) = \sum_{i=1}^m dim(\frac{O_i}{IO_i})$.

Lema 6 *Sea V una variedad afín, $p\in V$ un punto cualquiera e I un ideal de $\Gamma(V)$. Sea $\frac{a}{b} \in O_p(V)$. Entonces, $\frac{a}{b} \in IO_p(V)$ si y solamente si existe un elemento $t\in\Gamma(V)$ con $t(p)\neq 0$ y con $at \in I$.*

Demostración: Si existe el elemento t del enunciado, $\frac{a}{b} = \frac{at}{bt} = at\frac{1}{bt}$ y como $t(p)\neq 0$, $at\in I$ y $\frac{1}{bt} \in O_p(V)$.

Si $\frac{a}{b} \in IO_p(V)$, existirán $h_1,...,h_s \in I$ y $\frac{a_1}{b_1},...,\frac{a_s}{b_s} \in O_p(V)$ con $\frac{a}{b} = sum_{i=1}^s h_i\frac{a_i}{b_i}$ y poniendo denominadores comunes, tendremos que $\frac{a}{b} = \frac{r}{t}$ con $r\in I$ y $t(p)\neq 0$. Entonces, $at = br \in I$.

Proposición 35 *Sea $V \subset \mathbb{A}^n$ una variedad afín. Sea $I = I(V)$ el ideal de V y $p \in V$ un punto, y sea $J \subset k[X_1, ..., X_n]$ un ideal que contiene a I. Llamemos J' a $\frac{J}{I} \subset \frac{k[X_1,...,X_n]}{I}$. Entonces, existe un isomorfismo entre $\frac{O_p(\mathbb{A}^n)}{JO_p(\mathbb{A}^n)}$ y $\frac{O_p(V)}{J'O_p(V)}$ y $\frac{O_p(\mathbb{A}^n)}{IO_p(\mathbb{A}^n)}$ es isomorfo a $O_p(V)$.*

Demostración: Si probamos que $\frac{O_p(\mathbb{A}^n)}{JO_p(\mathbb{A}^n)}$es isomorfo a $\frac{O_p(V)}{J'O_p(V)}$, basta con tomar $J = I$ para ver que $\frac{O_p(\mathbb{A}^n)}{IO_p(\mathbb{A}^n)}$ y $O_p(V)$ son isomorfos, pues $J' = 0$ y el cociente de un anillo por el ideal 0 es siembre isomorfo al anillo.

Veamos ahora que $\frac{O_p(\mathbb{A}^n)}{JO_p(\mathbb{A}^n)}$ es isomorfo a $\frac{O_p(V)}{J'O_p(V)}$. Definimos una aplicación entre $O_p(\mathbb{A}^n)$ y $\frac{O_p(V)}{J'O_p(V)}$ que envíe a cada elemento $\frac{P}{Q} \in O_p(\mathbb{A}^n)$ al elemento $\frac{P+I(V)}{Q+I(V)} + J'O_p(V)$. Veamos que el núcleo de esta aplicación es $JO_p(\mathbb{A}^n)$: si $\frac{P+I(V)}{Q+I(V)} \in J'O_p(V)$, en virtud del lema anterior, existe $\alpha \in \Gamma(V)$ y con $\alpha(p) \neq 0$ de modo que $\alpha(P + I(V)) \in J'$, es decir, para algún polinomio $A \in k[X_1, ..., X_n]$ con $A + I(V) = \alpha$ que no se anula en p, $AP + I(V) \in J'$, pero por definición de J', esto sólo ocurre si $AP \in J$ y, nuevamente por el lema anterior, esto ocurre si y solamente si $\frac{P}{Q} \in JO_p(\mathbb{A}^n)$

Capítulo 2

Aplicaciones entre variedades

2.1. Morfismos entre variedades

En esta sección se trabajará con la topología de Zariski y X e Y denotarán dos variedades cualesquiera, salvo que se indique lo contrario.

En el capítulo anterior estudiamos las variedades, procedemos ahora a estudiar las aplicaciones que relacionan dos variedades, los morfismos entre variedades.

Definición 32 *Una aplicación $\varphi : X \longrightarrow Y$ se dice que es un* morfismo *entre las variedades X e Y, si:*

1. *φ es continua.*
2. *Para toda subviariedad abierta $U \subset Y$, si denotamos por $Z = \varphi^{-1}(U)$ y $f \in \Gamma(U)$, entonces $f \circ \varphi \in \Gamma(Z)$.*

Definición 33 *Un isomorfismo entre variedades es un morfismo biyectivo cuya inversa es también un morfismo.*

Proposición 36 *Sean X, Y dos variedades cuales quiera, y sea $\varphi : X \longrightarrow Y$ un isomorfismo. Entonces, φ induce isomorfismos de anillos entre $k(X)$ y $k(Y)$, entre $\Gamma(X)$ y $\Gamma(Y)$ y entre $O_p(X)$ y $O_{\varphi(p)}(Y)$.*

Demostración: Definamos la aplicación $\overline{\varphi} : k(Y) \longrightarrow k(X)$ como $\phi(z) = z \circ \varphi$ para todo $z \in k(Y)$.

La aplicación $\overline{\varphi}$ está bien definida y es un morfismo de anillos pues si $\lambda \in k$, $\lambda \neq 0$, y $z, w \in k(Y)$ son funciones racionales cuales quiera, tenemos $\overline{\varphi}(z+w) = (z+w)\circ\varphi = z\circ\varphi + w\circ\varphi = \overline{\varphi}(z)+\overline{\varphi}(w)$ y $\overline{\varphi}(\lambda z) = (\lambda z)\circ\varphi = \lambda(z\circ\varphi) = \lambda\overline{\varphi}$. Además es biyectiva, y su inversa viene dada por $\overline{\varphi}^{-1}(w) = w\circ\varphi^{-1}$ para todo $w \in k(Y)$. Luego $\overline{\varphi}$ es un isomorfismo.

Para ver que los anillos $O_p(X)$ y $O_{\varphi(p)}(Y)$ son isomorfos nos fijamos en que $O_p(X) \subset k(X)$ y en que $O_{\varphi(p)}(Y) \subset k(Y)$. Por tanto, si $\overline{\varphi}$ se restringe a una biyección entre $O_{\varphi(p)}(Y)$ y $O_p(X)$ concluiremos. Evidentemente esto es cierto, pues $z \in k(Y)$ está bien definida en $\varphi(p) \in Y$ si y solamente si $\overline{\varphi}(z) = z\circ\varphi \in k(X)$ está bien definida en $p \in X$.

Por último, para ver que $\Gamma(X)$ y $\Gamma(Y)$ son isomorfos, nos fijamos en que $\Gamma(X) = \cap_{p\in X} O_p(X)$ y que $\Gamma(Y) = \cap_{q\in Y} O_q(Y) = \cap_{p\in X} O_{\varphi(p)}(Y)$ y como $O_p(X)$ y $O_{\varphi(p)}(Y)$ son isomorfos, se concluye lo deseado.

Definición 34 *Una variedad isomorfa a una variedad afín (resp. variedad proyectiva) se llama* variedad afín *(resp.* variedad proyectiva*).*

Con la anterior ya hemos dado dos definiciones de variedad afín (resp. proyectiva). Nos referiremos a la definición dada en la sección "Variedades afines"(resp. "Variedades proyectivas") cuando digamos que “un conjunto $X \subset \mathbb{A}^n$ es una variedad afín"(resp. “un conjunto $X \subset \mathbb{P}^n$ es una variedad proyectiva"). Si simplemente decimos que "X es una variedad afín (res. proyectiva)"nos estemos refiriendo a la definición dada en esta sección.

Lema 7 *Sea Z una variedad y sea $Z' \subset Z$ una subvariedad (abierta o cerrada). Entonces, si $\alpha \in \Gamma(Z)$ es una función regular de Z, la restricción de α a Z' es una función regular de Z'.*

Demostración: Si Z' es una subvariedad abierta. El que $\alpha \in \Gamma(Z)$ implica que $\alpha \in k(Z)$ y que $Z \subset D(\alpha)$, pero como Z' es abierto, $k(Z) = k(Z')$ y $Z' \subset Z \subset D(\alpha)$ y por tanto $\alpha \in \Gamma(Z')$.

Supongamos que $Z' \subset Z \subset \mathbb{A}^n$ son cerrados. Entonces existirá $A \in k[X_1, ..., X_n]$ con $\alpha = A + I(Z)$. Llamemos $\beta = A + I(Z')$. Si vemos α y β como funciones, $\alpha(y) = A(y) = \beta(y)$ cuando $y \in Z'$ puesto que $I(Z) \subset I(Z')$, luego $\alpha = \beta$ en Z', y por tanto la restricción de α a Z' es una función regular de Z'.

Supongamos por último que Z es una variedad y Z' una subvariedad cerrada de Z. Llamemos $Z_i = Z \cap A_i$ y $Z'_i = Z' \cap A_i$ donde A_i es una carta afín. Como Z_i es abierto de Z, $\alpha \in \Gamma(Z_i)$ y como $Z'_i \subset Z_i$ es un cerrado de un afín, $\alpha \in \Gamma(Z'_i)$. Entonces, para todo $p \in Z'$ existe un abierto Z'_i que contiene a p y tal que $\alpha \in \Gamma(Z'_i)$. Por tanto, basta con aplicar la proposición 33.

Proposición 37 *Sean X, Y dos variedades, y sean $X' \subset X$ e $Y' \subset Y$ dos subvariedades (abiertas o cerradas). Entonces la restricción de cualquier morfismo $\varphi : X \longrightarrow Y$ que cumpla $\varphi(X') \subset Y'$ a X' y Y' es también un morfismo.*

Demostración: Este resultado es equivalente a dos casos particulares. Uno el caso $X = X'$ y otro el caso $Y = Y'$. Una vez demostrados estos dos casos tendremos que aplicando el primero de ellos, $\varphi : X \longrightarrow Y'$ será un morfismo y aplicando después el segundo, concluiremos lo deseado. Empecemos viendo que $\varphi' : X \longrightarrow Y'$ cuando $\varphi(X) \subset Y'$ es un morfismo.

La aplicación φ' es evidentemente continua pues Y' tiene la topología de subespacio de Y.

Tomemos ahora $U \subset Y'$ un abierto, existirá por tanto $V \subset Y$ un abierto con $U = V \cap Y'$. Sea $g \in \Gamma(U)$ una función regular. Existirán entonces F, G polinomios homogéneos del mismo grado con $G \notin I(\overline{U})$ de modo que $g = \frac{F + I_h(\overline{U})}{G + I_h(\overline{U})}$. Como $U \subset V$, $G \notin I(\overline{V})$, con lo que podemos definir la función racional $h = \frac{F + I_h(\overline{V})}{G + I_h(\overline{V})}$. Entonces, $h = g$ en el abierto $U \cap D(G)$ de U, es decir, un denso de $\overline{U}$, y por tanto, $h = g$ en U.

Por otra parte, como φ es morfismo, sabemos que $h \circ \varphi \in \Gamma(\varphi^{-1}(V))$, pero como tenemos que $\varphi^{-1}(V) = \varphi'^{-1}(U)$ y $g = h$ en U, concluimos que $g \circ \varphi' \in \Gamma(\varphi'^{-1}(U))$ como queríamos.

Hemos probado que $\varphi : X \longrightarrow Y'$ es un morfismo. Veamos ahora que la restricción $\varphi'' : X' \longrightarrow Y$ también lo es.

La restricción de φ es evidentemente continua pues X' tiene la topología de subespacio de X.

Sea U un abierto de Y, y sea $g \in \Gamma(U)$. Queremos ver que $g \circ \varphi'' \in \Gamma(\varphi''^{-1}(U))$.

Tenemos que $g \circ \varphi''$ coincide con la restricción de $g \circ \varphi$ al cerrado de $\varphi^{-1}(U)$, $\varphi^{-1}(U) \cap X'$. Denotemos por $Z = \varphi^{-1}(U)$, por $Z' = \varphi^{-1}(U) \cap X'$ y por $\alpha = g \circ \varphi$. Concluimos lo deseado aplicando el lema 7.

Proposición 38 *Sean X, Y dos variedades y $\phi : X \longrightarrow Y$ una aplicación. Si $\{X_\alpha\}_{\alpha \in A}$ y $\{Y_\alpha\}_{\alpha \in A}$ son dos recubrimientos por abiertos de X e Y respectivamente, tales que $\phi(X_\alpha) \subset Y_\alpha$. Entonces, ϕ es un morfismo si y solamente si las restricciones de ϕ, $\phi_\alpha : X_\alpha \longrightarrow Y_\alpha$ son morfismos.*

Demostración: Un resultado de topología general es que ϕ es contínua si y solamente sí ϕ_α es contínua para todo α por ser $\{X_\alpha\}_{\alpha \in A}$ un recubrimiento de X.

Supongamos que los ϕ_α son morfismos. Sea V un abierto de Y y tomemos $V_\alpha = V \cap Y_\alpha$. Denotemos por $Z = \phi^{-1}(V) = \phi^{-1}(\cup_{\alpha\in A} V_\alpha) = \cup_{\alpha\in A}\phi^{-1}(V_\alpha)$ un abierto de X. Denotemos por $z_\alpha = Z \cap X_\alpha$ abiertos de X.

Veamos que $Z_\alpha \subset \phi^{-1}(V_\alpha)$: sea $p \in Z\alpha \subset X_\alpha$ y sea $q = \phi(p) \in V_\alpha \cap \phi(X) \subset V_\alpha$. Entonces el punto $p \in \phi^{-1}(q) \subset \phi^{-1}(V_\alpha)$.

Sea $g \in \Gamma(V) = \Gamma(\cup_{\alpha\in A} V_\alpha) \subset \Gamma(V_\alpha)$ para todo $\alpha \in A$. Sabemos que $g\circ\phi$ restringido a X_α coincide con $g \circ \phi_\alpha \in \Gamma(\phi^{-1}(V_\alpha))$ y como $Z_\alpha \subset \phi^{-1}(V_\alpha)$, tenemos que $g \circ \phi_\alpha \in \Gamma(Z_\alpha)$.

Denotamos por $z = g\circ\phi$ y por $w_\alpha = g\circ\phi_\alpha$. Entonces, tenemos Z una variedad, Z_α abiertos que recubren Z y w_α funciones racionales de X_α que coinciden con z en cada $Z_\alpha \subset X_\alpha$. Luego basta con aplicar la proposición 33 para concluir que $z \in \Gamma(Z)$.

Supongamos ahora que ϕ es un morfismo. Ver que las restricciones de ϕ a X_α e Y_α son morfismos es consecuencia inmediata de la proposición 37.

Lema 8 *Sea A un anillo que además es un dominio, y sea K su cuerpo de fracciones. Sean $P \in A[X]$ y $Q \in K[X]$ dos polinomios que verifican la igualdad $P(X) = (aX-1)Q(X)$ para algún $a \in A$. Entonces, $Q \in A[X]$ también.*

Demostración: Podemos escribir $P(X) = \sum_{i=0}^{n} a_i X^i$ y $Q(X) = \sum_{i=0}^{n-1} b_i X^i$ donde $a_i \in A$ y $b_i \in K$. Fijándonos en la igualdad $P(X) = (aX-1)Q(X)$ y fijándonos en las partes homogéneas de ambos lados tenemos las siguientes igualdades:

$$a_0 = b_0,$$
$$a_1 = ab_0 - b_1,$$
$$\ldots$$
$$a_{n-1} = ab_{n-2} - b_{n-1},$$
$$a_n = ab_{n-1}.$$

Como $b_0 = a_0$, $b_0 \in A$ y podemos aplicar una inducción para $i = 1, \ldots, n-1$ a las expresiones $a_i = ab_{i-1} - b_i$ para ver que si $b_{i-1} \in A$, entonces $b_i = ab_{i-1} - a_i \in A$. Por tanto, $Q \in A[X]$ también.

Proposición 39 *Sea V una variedad afín, y $f \in \Gamma(V)$ no nulo. Sea $V_f = \{p \in V : f(p) \neq 0\}$, una subvariedad abierta de V. Entonces.*

(1) $\Gamma(V_f) = \Gamma(V)[\frac{1}{f}] = \{\frac{g}{f^n} : g \in \Gamma(V),\ n \in \mathbb{Z}\}$.

(2) *V_f es una variedad afín.*

Demostración: (1) Veamos primero que $\Gamma(V_f) \subset \Gamma(V)[\frac{1}{f}]$: sean $z \in \Gamma(V_f)$ y $F \in k[X_1, \ldots, X_n]$ tal que $F = f + I(V)$. El conjunto de polos de z es $V(J_z)$, donde $J_z = \{g \in k[X_1, \ldots, X_n] : \overline{g}z \in A(V)\}$. $V(J_z) \subset V(F)$, luego $Rad(F) \subset Rad(J_z)$ en virtud del teorema de los ceros, es decir, para todo elemento $h \in Rad(F)$ existe m tal que $h^m \in (J_z)$, en particular, existe m tal que $F^m \in J_z$. Por lo tanto, $\overline{F^m}z = f^m z \in \Gamma(V)$ y si denotamos por $H = f^m z$, tenemos que $z = \frac{H}{f^m} \in \Gamma(V)[\frac{1}{f}]$ tal y como queríamos.

Veamos que $\Gamma(V)[\frac{1}{f}] \subset \Gamma(V_f)$: Es evidente que $V_f \subset V$ y por tanto $\Gamma(V) \subset \Gamma(V_f)$. Además, como se verifica que una fracción $\frac{g}{h} \in \Gamma(V_f)$ si y solo si para todo $p \in V$ tal que $f(p) \neq 0$ se tiene también que $h(p) \neq 0$, es trivial que $\frac{1}{f} \in \Gamma(V_f)$. Juntando ambas observaciones concluimos que $\Gamma(V)[\frac{1}{f}] \subset \Gamma(V_f)$.

(2) Tomemos $F \in k[X_1, \ldots, X_n]$ con $F + I(V) = f$. Definimos el $I' \subset k[X_1, \ldots, X_n, X_{n+1}]$ como el ideal generado por $I(V)$ y por $X_{n+1}F - 1$. Definamos también $V' = V(I')$, una variedad afín de $\mathbb{A}^{n+1}$.

Consideremos ahora un morfismo de anillos $\phi : k[X_1,...,X_{n+1}] \longrightarrow \Gamma(V_f)$ dado por $\phi(X_{n+1}) = \frac{1}{f}$ y por $\phi(X_j) = X_j + I(V)$ para $j = 1,...,n$. La aplicación ϕ está bien definida en virtud del apartado anterior. Además, ϕ es sobreyectiva pues cualquier elemento de $\Gamma(V')$ se puede ver como un polinomio $P = \sum a_i \frac{1}{f^i}$ en $\Gamma(V)[\frac{1}{f}]$, que será la imagen por ϕ de $Q = \sum A_i X_{n+1}^i \in k[X_1,...,X_{n+1}]$ donde $a_i = A_i + I(V)$.

La aplicación ϕ también verifica que $Ker(\phi) = I'$: obviamente $I' \subset Ker(\phi)$ pues si $g \in I(V)$ entonces $\phi(g) \in \Gamma(V)$ es 0 y también $\phi(X_{n+1}F - 1) = \frac{1}{f}f - 1 = 0$. Veamos que $Ker(\phi) \subset I'$. Tomemos $P \in K[X_1,...,X_{n+1}]$ un elemento del núcleo de ϕ, es decir, $P(X_1 + I(V),...,X_n + I(V), \frac{1}{f}) = 0$.

Podemos descomponer ϕ en dos aplicaciones α y β dadas por

$$\alpha(R(X_1,...,X_{n+1})) = R(X_1 + I(V),...,X_n + I(V), X_{n+1}) \in \Gamma(V)[X_n + 1]$$

para todo polinomio $R \in k[X_1,...,X_{n+1}]$, y por $\beta(S(X_{n+1})) = S(\frac{1}{f})$ para todo $S \in \Gamma(V)[X_{n+1}]$ de modo que $\phi = \beta \circ \alpha$. Tenemos entonces que $P \in Ker(\phi)$ si y solamente si $\alpha(P) \in Ker(\beta)$.

De $\phi(P) = 0$ deducimos entonces que si $\alpha(P) \neq 0$, $\frac{1}{f}$ es un cero del polinomio $\alpha(P) \in K(V)[X_{n+1}]$, es decir, existe $Q \in K(V)[X_{n+1}]$ verificando $\alpha(P)(X_{n+1}) = (X_{n+1} - \frac{1}{f})Q(X)$ y multiplicando por $\frac{f}{f}$ al segundo miembro de la igualdad, y aplicando el lema 8 concluimos que $Q' = \frac{Q}{f} \in \Gamma(V)[X_{n+1}]$, y por tanto $\alpha(P)(X_{n+1}) = (X_{n+1}f - 1)Q'(X_{n+1}) \in (X_{n+1}f - 1) \subset \Gamma(V)[X_{n+1}]$.

Ahora, si $\alpha(P) = 0$ significa que si escribimos $P(X_1,...,X_{n+1}) = \sum P_i(X_1,...,X_n)X_{n+1}^i$ para ciertos polinomios $P_i \in k[X_1,...,X_n]$, entonces $P_i \in I(V)$ para todo i y, por lo tanto, P es un elemento de I'. Y si $\alpha(P) \in (X_{n+1}f - 1)$ entonces $P \in (X_{n+1}F - 1)$, y por tanto en I'. Como queríamos.

La aplicación ϕ induce entonces un isomorfismo de anillos $\tilde{\phi} : \Gamma(V') \longrightarrow \Gamma(V_f)$.

Consideremos ahora la proyección de $\mathbb{A}^{n+1}$ en $\mathbb{A}^n$ a la que denotaremos por Pr. Veamos que $Pr(V') \subset V_f$. Sea $p = (x_1,...,x_{n+1}) \in V'$ un punto, entonces $(x_1,...,x_n) \in V$ y $x_{n+1}F(x_1,...,x_n) - 1$ es nulo, es decir $Pr(p) \in V$ y $f(Pr(p)) \neq 0$, pues si no $x_{n+1}f(Pr(p)) - 1 = -1 \neq 0$. Es decir $Pr(p) \in V_f$. Aplicando la proposición 37 concluimos que Pr induce un morfismo de variedades $\varphi : V' \longrightarrow V_f$.

El morfismo φ es una biyección pues si $(x_1,...,x_{n+1}) \in V_f$, entonces x_{n+1} y $f(x_1,...,x_n)$ son no nulos, pues si $f(x_1,...,x_n) = 0$, $f \notin I'$, lo cual es absurdo puesto que $f \in I(V)$. Tenemos entonces que $\varphi^{-1}(x_1,...,x_n) = (x_1,...,x_n, \frac{1}{f(x_1,...,x_n)}) \in V'$. Y si $\varphi(x_1,...,x_{n+1}) = \varphi(y_1,...,y_{n+1})$ para dos puntos cuales quiera $(x_1,...,x_{n+1}), (y_1,...,y_{n+1}) \in V'$, necesariamente $(x_1,...,x_n) = (y_1,...,y_n)$ y

$$x_{n+1}F(x_1,...,x_n) - 1 = x_{n+1}F(y_1,...,y_n) - 1 = y_{n+1}F(y_1,...,y_n) - 1,$$

con lo que también $x_{n+1} = y_{n+1}$.

El morfismo φ induce un morfismo de anillos $\tilde{\varphi} : \Gamma(V_f) \longrightarrow \Gamma(V')$. Veamos que $\tilde{\varphi} = \tilde{\phi}^{-1}$: Dado $P \in k[X_1,...,X_{n+1}]$, $(\tilde{\varphi} \circ \tilde{\phi})(P + I') = \tilde{\varphi}(P(X_1 + I(V),...,X_n + I(V), \frac{1}{f(X_1,...,X_n)}))$. Tomando entonces $(x_1,...,x_{n+1}) \in V'$ un punto, $(\tilde{\varphi} \circ \tilde{\phi})(P + I')(x_1,...,x_{n+1}) = P(x_1,...,x_n, \frac{1}{f(x_1,...,x_n)}) = P(x_1,...,x_{n+1})$ ya que $x_{n+1}f(x_1,...,x_n) - 1 = 0$ para todo $(x_1,...,x_{n+1}) \in V'$.

Veamoa ahora que φ^{-1} es una aplicación contínua: Sea $Z = V(g) \cap V'$ un cerrado de V' con $g \in k[X_1,...,X_{n+1}]$, entonces $\varphi(W) = V(F^k G(X_1,...,X_n, \frac{1}{F(X_1,...,X_n)})) \cap V_f$, un cerrado de V_f.

Si vemos que φ^{-1} es un morfismo, habremos visto que φ es un isomorfismo entre una variedad afín V' y V_f y habremos terminado. Para ver que φ^{-1} es un morfismo, tenemos que ver que para cada abierto U de V', y para cada $g \in \Gamma(U)$, se cumple que $g \circ \varphi^{-1} \in \Gamma(\varphi(U))$.

Empecemos fijándonos que si $h \in \Gamma(V')$, $h \circ \varphi^{-1} = \tilde{\phi}(h)$. Lo cual es cierto si y solamente si $h \circ \varphi^{-1} \circ \varphi = \tilde{\phi}(h) \circ \varphi$ puesto que φ es una biyección, pero $h \circ \varphi^{-1} \circ \varphi = h$ y $\tilde{\phi}(h) \circ \varphi = \tilde{\varphi} \circ \tilde{\phi} \circ h = h$.

Como $g \in \Gamma(U)$, para cada $p \in U$ existirán $F_p, G_p \in k[X_1,...,X_{n+1}]$ polinomios homogéneos del mismo grado con $G_p(p) \neq 0$ tal que, si vemos U como una subvariedad abierta de la variedad V', $g = \frac{F_p + I_h(\overline{U})}{G_p + I_h(\overline{U})}$, en los puntos de V' que no anulen a G_p, pero como U es un abierto, es denso, luego

$\overline{U} = V'$, con lo que $F_p + I_h(\overline{U}), G_p + I_h(\overline{U}) \in \Gamma(V')$,pues V' es afín. Tiene sentido entonces considerar $\tilde{\phi}(F_p + I_h(V')), \tilde{\phi}(G_p + I_h(V')) \in \Gamma(V_f) \subset k(V_f)$. Como $k(V_f)$ es un cuerpo, $\frac{\tilde{\phi}(F_p+I_h(V'))}{\tilde{\phi}(G_p+I_h(V'))} \in k(V_f)$.

Tomando U_p el abierto dado por los puntos $q \in V_f$ tales que $\tilde{\phi}(G_p + I_h(V'))(q) \neq 0$, obviamente $\frac{\tilde{\phi}(F_p+I_h(V'))}{\tilde{\phi}(G_p+I_h(V'))} \in \Gamma(U_p)$ y $\varphi(p) \in U_p$ pues $\tilde{\phi}(G_p + I_h(V'))(\varphi(p)) = \tilde{\varphi} \circ \tilde{\phi} \circ G_p(p) = G_p(p) \neq 0$.

Además, $g \circ \varphi^{-1} = \frac{\tilde{\phi}(F_p+I_h(V'))}{\tilde{\phi}(G_p+I_h(V'))}$ en U_p pues si $q \in U_p \subset V_f$, tenemos las igualdades

$$\frac{\tilde{\phi}(F_p + I_h(V'))}{\tilde{\phi}(G_p + I_h(V'))}(q) = \frac{(F_p + I_h(V')) \circ \varphi^{-1}}{(G_p + I_h(V')) \circ \varphi^{-1}}(q) = \frac{F_p + I_h(V')}{G_p + I_h(V')}(\varphi^{-1}(q)) = g \circ \varphi^{-1}(q)$$

ya que $G_p \circ \varphi^{-1}(q) = (G_p + I_h(V')) \circ \varphi^{-1}(q) = \tilde{\phi}(G_p + I_h(V'))(q) \neq 0$, ya que $q \in U_p$.

Por lo tanto, concluimos lo deseado aplicando la proposición 33.

Terminamos esta sección con un resultado que necesitaremos más adelante y unos lemas previos que necesitaremos para su demostración.

Lema 9 *Sea $V \subset \mathbb{A}^n$ una variedad afín y sean p, q puntos del espacio afín que no pertenecen a V. Entonces, existe un polinomio $F \in k[X_1, ..., X_n]$ que no se anula ni en p ni en q pero con $P \in I(V)$.*

Demostración: Empecemos viendo que existe un polinomio $Q \in k[X_1, ..., X_n]$ que se anula en V pero no en q. De esta forma, si $Q(p) \neq 0$ tomaremos $F = Q$. En caso contrario, también existirá $P \in I(V)$ pero con $P(p) \neq 0$, si $P(q) = 0$ también, bastará con tomar $F = P + Q$.

Si no existiera dicho polinomio Q, tendríamos que $I(V) = I(V \cup \{q\})$, pero entonces

$$V = V(I(V)) = V(I(V \cup \{q\})) \supset V \cup \{q\},$$

lo cual es absurdo, pues $q \notin V$.

Lema 10 *Sea X una variedad y sean $p, q \in X$ dos puntos de la variedad distintos entre sí. Entonces, existe una subvariedad afín $U \subset X$ que contiene tanto a p como a q.*

Demostración: Como X es un abierto y $\overline{X}$ es un cerrado, $Z = \overline{X} \setminus X$ es un cerrado que no contiene a p ni a q. Sea A cualquier carta de $\mathbb{P}^n$ y tomemos $V = \overline{X} \cap A$ y $T = Z \cap A$. Entonces, por el lema 9 tenemos que existe un polinomio $P \in I(T)$ pero que no se anula ni en p ni en q, y por lo tanto, $P + I(V) \in \Gamma(V)$ es una función regular, de lo que deducimos que, según la notación de la proposición 39, U=$V_{P+I(V)}$ es una variedad afín que contiene a p y a q y que además está contenida en X por ser un abierto de $\overline{X}$.

Lema 11 *Sea X una variedad, y sean p, q puntos distintos de X. Entonces, existe una función racional $f \in k(X)$ con $f \in O_p(X) \cap O_q(X)$ y tal que $f(p) = 0$, pero $f(q) \neq 0$.*

Demostración: Podemos suponer que $X \subset \mathbb{A}^n$ es una variedad afín, pues en virtud de la proposición 10 sabemos que existe una subvariedad afín $V \subset X$ que es entorno de p y q y tendremos que $k(\overline{V}) = k(\overline{X}) = k(X)$.

Sea pues, $X \subset \mathbb{A}^n$ una variedad afín. En virtud del lema 5 existe un polinomio homogéneo L de grado 1 que se anule en p pero no en q. Entonces, $L \notin I(X)$ y $f = L + I(X) \in k(X)$ es una función racional. Obviamente $f \in O_p(C) \cap O_q(C)$ y $f(p) = 0$ pero $f(q) \neq 0$, como queríamos.

Lema 12 *Sea $\phi : X \longrightarrow Y$ un morfismo entra las variedades X e Y. Supongamos que $\phi(X)$ es denso en Y. Entonces, el morfismo de anillos $\overline{\phi} : \Gamma(Y) \longrightarrow \Gamma(X)$ que induce ϕ entre estos anillos y que viene dado por $\overline{\phi}(z) = z \circ \phi$ para todo $z \in \Gamma(Y)$ es inyectivo.*

Demostración: Sean $z, w \in \Gamma(Y)$ dos funciones racionales. Supongamos que $\overline{\phi}(z) = \overline{\phi}(w)$, es decir, si $y \in Im(\phi) \subset Y$ se cumple que $z(y) = w(y)$. Tenemos pues, que z y w son dos funciones contínuas definidas de Y en k y que coinciden en un denso de Y.

Por otro lado, $z = w$ en todo Y si y solo si $FQ - PG = 0$ en $\overline{Y}$ cuando $z = \frac{F+I_h(\overline{Y})}{G+I_h(\overline{Y})}$ y $w = \frac{P+I_h(\overline{Y})}{Q+I_h(\overline{Y})}$. Sabemos que es cierto en un denso de $\overline{Y}$ y como $FQ - PG = 0$ define un cerrado de $\overline{Y}$ que contiene a un denso, es inmediato que $z = w$ en todo Y.

Proposición 40 *Sea H_∞^n el hiperplano del infinito de $\mathbb{P}^n$ para la carta $x_n \neq 0$. Entonces:*

(1) La aplicación $i : \mathbb{P}^{n-1} \longrightarrow H_\infty^n$ que envía un punto $(x_0;...;x_{n-1}) \in \mathbb{P}^{n-1}$ al punto $(x_0;...;x_{n-1};0)$ es un isomorfismo.

(2) Si $V \subset \mathbb{P}^n$ es una variedad con $V \subset H_\infty^n$, entonces, V es isomorfa a alguna variedad de $\mathbb{P}^{n-1}$.

(3) Toda variedad es isomorfa a alguna variedad $V \subset \mathbb{P}^n$ para algún n de modo que V no está contenida en ningún hiperplano de $\mathbb{P}^n$.

Demostración:

(1) La aplicación i es evidentemente biyectiva y tanto i como su inversa son contínuas por tratarse de la inclusión y su inversa la proyección. Sea $U \subset H_\infty^n$ un abierto, y $g \in \Gamma(U)$ una función regular, entonces, existirán $F, G \in k[X_0,...,X_n]$ con $G(U) \neq 0$, $gr(F) = gr(G)$ y $g = \frac{F+I_h(H_\infty^n)}{G+I_h(H_\infty^n)}$. Es evidente, entonces, que $g \circ i = \frac{F(X_0,...,X_{n-1},0)+I_h(\mathbb{P}^{n-1})}{G(X_0,...,X_{n-1},0)+I_h(\mathbb{P}^{n-1})}$ es una función regular de $\Gamma(i^{-1}(U))$ pues $F(X_0,..,X_{n-1},0)$ y $G(X_0,...,X_{n-1},0)$ son polinomios de $k[X_0,...,X_{n-1}]$ del mismo grado, y $G(X_0,...,X_{n-1},0)$ no es nulo pues $G \notin I_h(H_\infty^n)$.

De igual forma, si $V \subset \mathbb{P}^{n-1}$ es un abierto y $h \in \Gamma(V)$, existirán $P, Q \in k[X_0,...,X_{n-1}] \subset k[X_0,...,X_n]$ con $Q \neq 0$ y $gr(P) = gr(Q)$ que verifican $h = \frac{P+I_h(\mathbb{P}^{n-1})}{Q+I_h(\mathbb{P}^{n-1})}$. Entonces, $h \circ i^{-1} = \frac{F+I_h(H_\infty^n)}{G+I_h(H_\infty^n)}$, que es, evidentemente, una función regular en H_∞^n.

(2) Sea $W = i^{-1}(V)$ una variedad de $\mathbb{P}^{n-1}$. Aplicando la proposición 37 es inmediato el ver que V y W son isomorfas.

(3) Sea H un hiperplano de $\mathbb{P}^m$. Si vemos que H es isomorfo a H_∞^m, aplicando (2) tendremos que cualquier variedad contenida en H es isomorfa a otra de $\mathbb{P}^{m-1}$. Iterando el razonamiento, si para todo n la variedad está contenida en algún hiperplano de $\mathbb{P}^n$, razonamos con $n = 0$ y concluímos que la variedad es el vacío.

Veamos que H es isomorfo al hiperplano del infinito. El hiperplano H vendrá dado por la anulación de un polinomio homogéneo de grado 1, L. Como $L \neq 0$, ha de aparecer alguna coordenada X_i en la expresión de L, supongamos que aparece X_0. Consideremos la aplicación $\mathbb{P}^n \longrightarrow \mathbb{P}^n$ que envía cada punto $(x_0;...;x_n)$ al punto $(L(x_0,...,x_n);x_1;...;x_n)$. Esta aplicación es evidentemente un isomorfismo (un caso más general se detallará en el lema 14) que se restringe a otro entre H y H_∞^n nuevamente por la proposición 37, como queríamos.

2.2. Aplicaciones polinómicas

Definición 35 *Sean $V \subset \mathbb{A}^n$ y $W \subset \mathbb{A}^m$ variedades afines. Una función $\varphi : V \longrightarrow W$ se llama* aplicación polinómica *si existen polinomios $T_1,...,T_m \in K[X_1,...,X_n]$ tales que para cada $(x_1,...,x_n) \in \mathbb{A}^n$, $\varphi(x_1,...,x_n) = (T_1(x_1,...,x_n),...,T_m(x_1,...,x_n))$.*

Una aplicación polinómica $\varphi : V \longrightarrow W$ induce un homeomorfismo $\widetilde{\varphi} : J(W,k) \longrightarrow J(V,k)$ donde $\widetilde{\varphi}(f) = f \circ \varphi$. Como φ es polinómica, $\varphi(A(W)) \subset A(V)$, podemos restringir la aplicación anterior al homeomorfismo (que denotaremos igual) $\widetilde{\varphi} : A(W) \longrightarrow A(V)$.

Proposición 41 *Sean $V \subset \mathbb{A}^n$ y $W \subset \mathbb{A}^m$ variedades afines. Existe una biyección entre las aplicaciones polinómicas $\varphi : V \longrightarrow W$ y los homeomorfismos $\widetilde{\varphi} : A(W) \longrightarrow A(V)$. Toda aplicación polinómica φ es la restricción de otra aplicación polinómica de $\mathbb{A}^n$ en $\mathbb{A}^m$.*

Demostración: Ya hemos visto cómo de una aplicación polinómica $\varphi : V \longrightarrow W$ se obtiene otro $\widetilde{\varphi} : A(W) \longrightarrow A(V)$. Veamos ahora cómo a partir de $\widetilde{\varphi}$ podemos contruir una aplicación polínómica $T_{\widetilde{\varphi}}$ y que además $T_{\widetilde{\varphi}} = \varphi$.

Sean $T_1, ..., T_m \in k[X_1, ..., X_n]$ polinomios tales que $T_i = \widetilde{\varphi}(Y_i + I(W))$. Tenemos así una aplicación polinómica $T = (T_1, ..., T_m) : \mathbb{A}^n \longrightarrow \mathbb{A}^m$. Si vemos que $T(V) \subset W$, tendremos la aplicación polinómica $T_{\widetilde{\varphi}} = T\mid_V$ que buscábamos pues si $p \in V$

$$T_{\widetilde{\varphi}} = (T_1(p), ..., T_m(p)) = (\widetilde{\varphi}(Y_1)(p), ..., \widetilde{\varphi}(Y_m)(p)) = \varphi(p).$$

Para ver que $T(V) \subset W$ primero vamos a ver que $\widetilde{T}(I(W)) \subset I(V)$: Sea $P \in k[Y_1, ..., Y_m]$ un polinomio, $\widetilde{T}(P) = P \circ T = P(T_1, ..., T_m) = P(\widetilde{\varphi}(Y_1 + (I(W)), ..., \widetilde{\varphi}(Y_m + I(W))))$, como $\widetilde{\varphi}$ es un homeomorfismo, tenemos también la igualdad

$$\widetilde{T}(P) = \widetilde{\varphi}(P(Y_1 + I(W), ..., Y_m + I(W))) = \widetilde{\varphi}(P + I(W)).$$

Además, si $P \in I(W)$, $P + I(W) = 0$, luego $\widetilde{T}(P) = 0$, es decir $\widetilde{T} \subset I(V)$.

Veamos por últimos que $T(V) \subset W$: sea $p \in V$, $T(p) \in W$ si y sólo si para todo $P \in I(W)$ $P(T(p)) = 0$. Pero como $\widetilde{T}(I(W)) \subset I(V)$, $P(T(p)) = \widetilde{T}(P)(p) = 0$, tal y como queríamos.

Proposición 42 *Sean X e Y dos variedaes afines. Existe una biyección entre morfismos $\varphi : X \longrightarrow Y$ y morfismos de anillos $\alpha : \Gamma(Y) \longrightarrow \Gamma(X)$. Si $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^n$, un morfismo de X en Y coincide con una aplicación polinómica.*

Demostración: Podemos suponer que $X \subset \mathbb{A}^n$ e $Y \subset \mathbb{A}^m$ son variedades afines.

Ahora, dado un morfismo $\varphi : X \longrightarrow Y$, podemos construir una aplicación $\widetilde{\phi} : \Gamma(Y) \longrightarrow \Gamma(X)$ definida como $\widetilde{\phi}(f) = f \circ \phi$ para todo $f \in \Gamma(Y)$. Veamos que $\widetilde{\phi}$ es un morfismo de anillos. Sean $f, g \in \Gamma(Y)$ dos funciones cualesquiera. Entonces:

$\widetilde{\phi}(f + g) = (f + g) \circ \phi = f \circ \phi + g \circ \phi = \widetilde{\phi}(f) + \widetilde{\phi}(g)$.

$\widetilde{\phi}(fg) = (fg) \circ \phi = (f \circ \phi)(g \circ \phi) = \widetilde{\phi}(f)\widetilde{\phi}(g)$.

Ya vimos en la proposición 41 que todo morfismo $\alpha : \Gamma(Y) \longrightarrow \Gamma(X)$ viene dada de forma única por una aplicación polinómica $T_\alpha : X \longrightarrow Y$ que viene dada por $T_\alpha(f) = (T_1, ..., T_m)$ donde, para cada i, $T_i = \widetilde{\phi}(Y_i + I(Y))$. Veamos que $T_{\widetilde{\phi}} = \phi$:

Sea $a \in X$ y $b = \phi(a) \in Y$. Entonces

$$\begin{aligned} T_{\widetilde{\phi}}(a) &= (\widetilde{\phi}(Y_1 + I(Y)), ..., \widetilde{\phi}(Y_m + I(Y)))(a) = \\ &= ((Y_1 + I(Y))(\phi(a)), ..., (Y_m + I(Y))(\phi(a))) = \\ &= ((Y_1 + I(Y))(b), ..., (Y_m + I(Y))(b)) = (b_1, ..., b_m) = b, \end{aligned}$$

tal y como queríamos.

2.3. Aplicaciones regulares

Definición 36 *Sea X una variedad y sea $\phi : X \longrightarrow \mathbb{A}^m$ una aplicación. Diremos que ϕ es una* aplicación regular *entre la variedad X y un espacio afín si existen funciones regulares $z_1, ..., z_m \in \Gamma(X)$ con $\phi = (z_1, ..., z_m)$*

Definición 37 *Sean X, Y dos variedades, $Y \subset \mathbb{P}^m$, y sea $\phi : X \longrightarrow Y$ una aplicación. Diremos que ϕ es una* aplicación regular *entre las variedades X e Y si para cada punto $x \in X$ existe un entorno abierto U de x tal que alguna carta A_i de $\mathbb{P}^m$ contenga a $\phi(U) \subset Y$ e, identificando A_i con el espacio afín $\mathbb{A}^m$, la restricción $\phi : U \longrightarrow A_i$ es una aplicación regular entre la variedad U y un espacio afín.*

En la definición anterior fijamos una carta A_i que contiene a $f(x)$, pero este punto puede estar contenido en otra carta A_j de modo que para algún otro entorno $U' \subset X$, $f : U' \longrightarrow A_j$ también sea una aplicación regular. De esta forma, si $f : U \longrightarrow A_i$ viene dada por funciones regulares $z_1, ..., z_m$, se tiene que $\frac{z_k}{z_j}$ es también una función regular para todo $k = 1, ..., m$, $k \neq j$, $k \neq i$ y también lo es $\frac{1}{z_j}$, con lo que podemos definir $f : U' \longrightarrow A_j$ como $f = (\frac{z_1}{z_j}; ...; \frac{1}{z_j}; ...; \frac{z_m}{z_j})$ donde $\frac{1}{z_j}$ está en la posición i y $\frac{z_j}{z_j}$ no aparece.

Si $U \subset X$ es una subvariedad abierta tal que $f : U \longrightarrow A_0$ define una aplicación regular, f vendrá dada por funciones regulares $z_1, ..., z_m$. Podemos escribir $z_i = \frac{F_i + I_h(\overline{X})}{G_i + I_h(\overline{X})}$ para $F_i, G_i \in k[X_0, ..., X_m]$ polinomios homogéneos del mismo grado y con $G_i \notin I_h(\overline{X})$. Igualando denominadores tenemos que $z_i = \frac{H_i + I_h(\overline{X})}{G + I_h(\overline{X})}$. Entonces, tenemos que $f = (G; H_1; ...; H_m)$ es una expresión para $f : X \longrightarrow Y$.

Si tenemos expresiones similares para f en otros abiertos U' de X y en otras cartas A_j, siguiendo los mismos pasos que antes obtendríamos otras expresiones para la aplicación f definida entre X e Y. Necesitamos, pues, ver cuándo dos expresiones definidas entre X e Y dan lugar a la misma aplicación:

Proposición 43 *Dadas $f, g : X \longrightarrow Y$ dos aplicaciones definidas por $f(x) = (F_0(x); ...; F_m(x))$ y por $g(x) = (G_0(x); ...; G_m(x))$ para todo punto $x \in X$ donde $F_i, G_i \in \Gamma(\overline{X})$ definen la misma aplicación entre X e Y, si y solamente si $F_iG_j = F_jG_i$ en X para todo par de índices i, j.*

Demostración: Supongamos que f y g definen la misma aplicación, entonces, para todo punto $x \in X$ $(F_0(x); ...; F_m(x)) = (G_0(x); ...; G_m(x))$, es decir $F_i(x) = \lambda G_i(x)$ para todo $i = 0, ..., m$ y para algún $\lambda \in k$ no nulo, luego, ver que $F_iG_j = F_jG_i$ en X es trivial.

Veamos ahora la otra implicación. Se tiene que $(F_0; ...; F_m) = (1; \frac{F_1}{F_0}; ...; \frac{F_m}{F_0})$ y $(G_0; ...; G_m) = (1; \frac{G_1}{G_0}; ...; \frac{G_m}{G_0})$ definido en los puntos de X donde F_0 y G_0 no se anulen respectivamente. Entonces, $\frac{F_k}{F_0} = \frac{G_k}{G_0}$ como funciones regulares si y solo si $F_kG_0 = F_0G_k$ en X, lo cual es cierto. Si en vez de mirar en la carta A_0, miramos en cualquier otra carta A_j tendremos que $F_kG_j = F_jG_k$ en X también, luego, como f y g coinciden en un cada carta de Y definen la misma aplicación entre X e Y.

A la vista de lo anterior, también es posible definir función regular como en la siguiente definición.

Definición 38 *Sea X una variedad de $\mathbb{P}^n$ y sea $\phi : X \longrightarrow \mathbb{P}^m$ una aplicación. Diremos que ϕ es una* aplicación regular *si para cada punto $x \in X$ existen $F_0, ..., F_m \in k[X_0, ..., X_n]$ polinomios homogéneos del mismo grado tales que para algún i $F_i(x) \neq 0$ y tales que $\phi(x) = (F_0(x); ...; F_m(x))$.*

Proposición 44 *Las aplicaciones regulares entre variedades son de hecho morfismos entre variedades.*

Demostración: Sean X, Y dos variedades, y sea $\phi : X \longrightarrow Y$ una aplicación regular entre variedades. Como para todo $x \in X$ existe un entorno $U_x \subset X$ abierto de modo que para algún i $\phi : U_x \longrightarrow A_i \subset \mathbb{A}^m$ es una aplicación regular, fijándonos en que los U_x recubren X y que los A_i recubren Y, si vemos que el enunciado es cierto para aplicaciones para el caso afín habremos terminado.

Sea $\phi : X \longrightarrow \mathbb{A}^m$ una aplicación regular. Empecemos suponiendo que X es una variedad afín. Existen $z_1, ..., z_m \in \Gamma(X)$ tales que $\phi = (z_1, ..., z_m)$. Como X es afín, podemos escribir $Z_i = T_i + I(X)$ para algún polinomio $T_i \in k[X_1, ..., X_n]$.

Sea $U \subset \mathbb{A}^m$ un abierto y sea $g \in \Gamma(U)$, entonces, para todo punto $p \in U$ existen polinomios $F, G \in k[Y_1, ..., Y_m]$ con $g = \frac{F+I(\mathbb{A}^m)}{G+I(\mathbb{A}^m)}$ y con $G(p) \neq 0$.

Entonces, para todo punto $x \in \phi^{-1}(U)$ existen polinomio $F, G \in k[Y_1, ..., Y_m]$ con $G(\phi(x)) \neq 0$ tales que $F(T_1, ..., T_m), G(T_1, ..., T_m) \in k[X_1, ..., X_n]$ y $g \circ \phi(x) = \frac{F(T_1(x),...,T_m(x))}{G(T_1(x),...,T_m(x))}$. Luego $g \circ \phi \in \Gamma(\phi^{-1}(U))$.

Si X es una variedad no necesariamente afín, las restricciones $\phi_i : X \cap A_i \longrightarrow \mathbb{A}^m$ donde A_i son las cartas de $\mathbb{P}^n$ son aplicaciones entre variedades afines y el espacio afín.

Como $X \cap A_i \subset X$, se tiene que $\Gamma(X) \subset \Gamma(X \cap A_i)$, luego si ϕ es una aplicación regular, ϕ_i también lo es, y como hemos visto, esto implica que ϕ_i es un morfismo para todo i. Como los $X \cap A_i$ recubren X, podemos aplicar la proposición 38 para concluir que ϕ también es un morfismo.

A continuación daremos dos ejemplos de aplicaciones regulares que nos serán de utilidad más adelante:

Ejemplo 1: **Proyección de centro un espacio lineal.** Sea $E \subset \mathbb{P}^n$ un espacio lineal de dimensión d. E vendrá dado por la anulación de unos polinomios homogéneos de grado 1 $L_1, ..., L_{n-d}$. Definimos la proyección de centro el espacio lineal E como la proyección $\Pi : \mathbb{P}^n \longrightarrow \mathbb{P}^{n-d-1}$ que viene dada por $\Pi(p) = (L_1(p); ...; L_{n-d}(p))$. Esta aplicación es regular en $\mathbb{P} \setminus E$ ya que fuera de E no se pueden anular todos los L_i a la vez. En particular, si X es una variedad de $\mathbb{P}^n$ disjunta de E, la aplicación restricción de Π, $\Pi : X \longrightarrow \mathbb{P}^{n-d-1}$ es una aplicación regular.

Ejemplo 2: **El embebimiento de Veronese.** Consideremos todos los polinomios homogéneos de grado m en $k[X_0, ..., X_n]$. El conjunto de estos polinomios genera un espacio lineal de dimensión $\binom{m+n}{m}$. Consideremos ahora el espacio de hipersuperficies correspondientes a la anulación de estos polinomios de grado m. Como dos de estos polinomios F, G dan la misma hipersuperficie si y solo si existe un elemento $\lambda \in k$ tal que $F = \lambda G$, podemos ver el espacio de hipersuperficies como el espacio de puntos del espacio proyectivo $\mathbb{P}^N$ con $N = \binom{m+n}{m} - 1$. De esta forma, fijado un orden para los $\binom{m+n}{m}$ monomios homogéneos de grado m que se pueden formar en $k[X_0, ..., X_n]$, podremos representar las hipersuperficies por los puntos de $\mathbb{P}^N$ de coordenadas $\gamma_{i_0,...,i_n}$ con $\sum_{j=0}^n i_j = m$ donde una hipersuperficie se escribe como $\sum \gamma_{i_0,...,i_n} X_0^{i_0} ... X_n^{i_n}$, es decir, como la suma de todos los posibles monomios de grado m multiplicados por sus correspondientes coordenadas.

Definimos ahora la aplicación $\gamma_m : \mathbb{P}^n \longrightarrow \mathbb{P}^N$ definida como $\gamma_m(u_0, ..., u_n) = (\gamma_{i_0,...,i_n} = u_0^{i_0} ... u_n^{i_n})$ ordenadas las coordenadas en $\mathbb{P}^N$ según el orden prefijado. Esta aplicación es una aplicación regular puesto que si para algún $u = (u_0, ..., u_n) \in \mathbb{P}^n$ $\gamma_m(u) = 0$, necesariamente las coordenadas $\gamma_{0,...,m,..,0} = 0$ donde $m = i_j$ para todo $j = 0, ..., n$, es decir, $u_j^m = 0$ para todo j, y esto implica que $u = 0 \in \mathbb{P}^n$, lo cual es absurdo. A esta aplicación γ_m la llamamos el m-ésimo *embebimiento de Veronese.*

Vimos que las aplicaciones regulares son morfismos, luego, en particular, el embebimiento de Veronese lo es. Vamos a ver a continuación que es de hecho un isomorfismo en su imagen.

Consideremos S el conjunto de puntos $\gamma = (\gamma_{i_0,...,i_n}) \in \mathbb{P}^N$ que para todo k natural verifiquen $\gamma_{i_0^1,...,i_n^1} ... \gamma_{i_0^k,...,i_n^k} = \gamma_{j_0^1,...,j_n^1} ... \gamma_{j_0^k,...,j_n^k}$ si $i_l^1 + ... + i_l^k = j_l^1 + ... + j_l^k$, para $l = 0, ..., n$. Es inmediato comprobar que los puntos de la imagen del embebimiento de Veronese cumple estas condiciones y por tanto es un subconjunto de S. Denotemos por $A_{i_0,...,i_n}$ las cartas de $\mathbb{P}^N$ que vienen dadas por $\gamma_{i_0,...,i_n} \neq 0$ y tomemos $S_{i_0,...,i_n} = S \cap A_{i_0,...,i_n}$. Veamos que $S = S_{m,0,...,0} \cup ... \cup S_{0,...,0,m,0,...,0} \cup ... \cup S_{0,...,0,m}$. Por simplificar la notación, representaremos las n-úplas $(0, ..., 0, m, 0, ..., 0)$ donde m está en la posición t, por simplemente t. Sea $\gamma \in S$, como $\gamma = (\gamma_{i_0,..,i_n}) \neq 0$ para alguna n-úpla $(i_0, ..., i_n)$ $\gamma_{i_0,...,i_n} \neq 0$, y como $i_0 + ... + i_n = m$ existirá j con $i_j \neq 0$. Consideremos entonces, el producto de m copias de $\gamma_{i_0,...,i_n}$ al que denotaremos por Γ. Entonces, como $\gamma \in S$, se cumple la igualdad $\Gamma = (\gamma_0 ... \gamma_0) ... (\gamma_t ... \gamma_t) ... (\gamma_n ... \gamma_n)$ donde los γ_t aparecen i_t veces en el producto. Entonces, si cada elemento γ_t que aparece en el producto fuera nulo, necesariamente $\gamma_{i_0,...,i_n} = 0$, lo cual es absurdo. Por tanto, todos los γ_t que aparecen son no nulos, en particular aquél con $t = j$, con lo que $\gamma \in S_j$.

Definamos ahora aplicaciones regulares $pr_t : S_t \longrightarrow \mathbb{P}^n$ donde

$$pr_t(\gamma) = (\gamma_{1,0,\dots,0,m-1,0,\dots,0}; \gamma_{0,1,0,\dots,0,m-1,0,\dots,0}; \dots; \gamma_t; \dots; \gamma_{0,\dots,0,m-1,0,\dots,0,1}).$$

Como estas aplicaciones son regulares, son morfismos que en virtud de la proposición 38 podemos extender a otro morfismo pr de S en $\mathbb{P}^n$ si y solamente si para todo $\gamma \in S_t \cap S_{t'}$, se cumple que $pr_t(\gamma) = pr_{t'}(\gamma)$. Para verlo, supongamos $t = 0$ y $t' = n$ por simplicidad y empecemos viendo que si γ_0 y γ_n no son nulos, entonces $\gamma_{m-1,0,\dots,0,1} \neq 0$. Como antes, consideremos el producto de m copias de $\gamma_{m-1,0,\dots,0,1}$ y denotémoslo por Γ, nuevamente, $\Gamma = \gamma_0 \dots \gamma_0 \gamma_n$ donde γ_0 aparece $m-1$ veces y γ_n solamente una vez. Por tanto $\gamma_{m-1,0,\dots,0,1}$ es no nulo. Entonces, si denotamos por u_j a la coordenada j-ésima de pr_0 y por v_j a la de pr_n, $j = 0, \dots, n$, tenemos que $u_j \gamma_0 = v_j \gamma_{m-1,0,\dots,0,1}$ para todo j, y como γ_0 y $\gamma_{m-1,0,\dots,0,1}$ son constantes de k no nulas, concluimos que $pr_0(\gamma) = pr_n(\gamma)$.

Veamos, por último, que $pr = \gamma_m^{-1}$ y deduciremos que el embebimiento de Veronese es un isomorfismo con su imagen. Sea $\gamma \in \mathbb{P}^N$, supongamos que $\gamma \in S_0$, entonces

$$pr(\gamma) = (\gamma_0; \gamma_{m-1,1,0,\dots,0}; \dots; \gamma_{m-1,0,\dots,0,1}) = (u_0; \dots; u_n).$$

Ahora, $\gamma_m(u_0, \dots, u_n) = \Gamma = (\Gamma_{i_0,\dots,i_n} = u_0^{i_0} \dots u_n^{i_n})$, luego $\Gamma_{i_0,\dots,i_n} = \gamma_0^{i_0} \gamma_{m-1,1,0,\dots,0}^{i_1} \dots \gamma_{m-1,0,\dots,0,1}^{i_n}$. Veamos que $\Gamma_{i_0,\dots,i_n} = \gamma_{i_0,\dots,i_n}$. Como estamos trabajando en el espacio proyectivo $\mathbb{P}^N$, basta con ver que $\gamma_{i_0,\dots,i_n} \gamma_0^{m-1} = \Gamma_{i_0,\dots,i_n}$ para toda n-upla $(i_0, \dots, i_n)$. Entonces, como $\gamma \in S$,

$$\gamma_0^{i_0} \gamma_{m-1,1,0,\dots,0}^{i_1} \dots \gamma_{m-1,0,\dots,0,1}^{i_n} = \gamma_{i_0,\dots,i_n} \gamma_0^{m-1}$$

si y solamente si $i_0 m + i_1(m-1) + \dots + i_n(m-1) = i_0 + \sum_{j=1}^n i_j(m-1) = m(m-1) + i_0$ y si $i_j = i_j$ para $j = 1, \dots, n$, lo cual es evidentemente cierto.

Veamos ahora que si $(u_0; \dots; u_n) \in \mathbb{P}^n$, suponiendo que $\gamma_m(u_0, \dots, u_n) = (\gamma_{i_0,\dots,i_n} = u_0^{i_0} \dots u_n^{i_n}) = \gamma$, y que $u_0 \neq 0$, entonces $pr(\gamma) = (u_0; \dots : u_n)$. Como $u_0 \neq 0$, $\gamma_0 \neq 0$ y

$$pr(\gamma) = pr_0(\gamma) = (u_0^m; u_1 u_0^{m-1}; \dots; u_n u_0^{m-1}) = (u_0; \dots; u_n) \in \mathbb{P}^n.$$

Definición 39 *Sea $\phi : X \longrightarrow \mathbb{P}^n$ una aplicación regular. El subconjunto de $X \times \phi(X)$ dado por los puntos $(x, \phi(x))$ se llama* grafo *de ϕ y lo denotaremos $Graf(\phi)$.*

Lema 13 *El grafo de una aplicación regular es cerrado para la topología producto de la topología de Zariski.*

Demostración: Sea $i : \mathbb{P}^n \longrightarrow \mathbb{P}^n$ la aplicación regular identidad y consideremos la aplicación $(\phi, i) : X \times \mathbb{P}^n \longrightarrow \mathbb{P}^n \times \mathbb{P}^n$ dado por $(\phi, i)(x, p) = (\phi(x), p)$. $Graf(\phi)$ es la imagen inversa de $Graf(i)$ por la aplicación (ϕ, i), luego si vemos que $Graf(i)$ es cerrado concluiremos lo deseado.

$Graf(i)$ viene dado por los pares $(x, y) \in \mathbb{P}^n \times \mathbb{P}^n$ cumpliendo $x = y$, luego un cerrado.

Proposición 45 *La imagen de una variedad a través de una aplicación regular es un conjunto cerrado.*

Demostración: Sea $\phi : X \longrightarrow \mathbb{P}^n$ una aplicación regular, sea $Graf(\phi)$ su grafo. Denotemos por $p : X \times \mathbb{P}^n \longrightarrow \mathbb{P}^n$ a la proyección dada por $p(x, y) = y$. Es evidente que $\phi(X) = p(Graf(\phi))$, luego $\phi(X)$ es un cerrado.

Definición 40 *Sean V y W dos variedades afines de $\mathbb{A}^n$ y $\mathbb{A}^m$ respectivamente,y sea $\phi : V \longrightarrow W$ una aplicación regular. Diremos que ϕ es una* aplicación finita *si $\phi(V)$ es denso en W y $\Gamma(V)$ es entera sobre $\Gamma(W)$.*

Nota: en el lema 12 vimos que $\overline{\phi} : \Gamma(W) \longrightarrow \Gamma(V)$ es inyectiva. Es de esta forma que vemos $\Gamma(W)$ como $\Gamma(V)$-módulo y la condición de que $\Gamma(V)$ sea entera sobre $\Gamma(W)$ tiene sentido.

Definición 41 *Sean X, Y dos variedades de $\mathbb{P}^n$ y $\mathbb{P}^m$. Diremos que $\phi : X \longrightarrow Y$ es una* aplicación finita *si todo punto $y \in Y$ tiene un entorno abierto V que sea una variedad afín tal que $U = \phi^{-1}(V)$ es a su vez una variedad afín y tal que la restricción $\phi : U \longrightarrow V$ es una aplicación finita entre variedades afines.*

Lema 14 *Sea $L \in k[X_0, ..., X_n]$ un polinomio homogéneo de grado 1 y V una variedad. Sea U el abierto de $\mathbb{P}^n$ dado por los puntos que no anulan a L. Entonces, para toda función racional $z \in \Gamma(V)$ existe un polinomio $G \in k[X_0, ..., X_n]$ de grado d de modo que $z = \frac{G}{L^d}$.*

Demostración: Tomemos para $i = 1, ..., n$ $L_i = \sum_{j=0}^n l_j^i X_j$ polinomios homogénes de grado 1 de modo que si $L = \sum_{j=0}^n l_j^0 X_j$ la matriz dada por los l_j^i tiene determinante no nulo.

Definamos la aplicación regular $F : \mathbb{P}^n \longrightarrow \mathbb{P}^n$ que viene dada por $F = (L_0; ...; L_n)$, donde $L_0 = L$. Como F es biyectiva por la condición de que el determinante de la matriz de elementos l_j^i sea no nulo y como los L_i son todos formas lineales tenemos que el inverso de F también vendrá dado por polinomios homogéneos de grado 1, es decir, otra aplicación regular. De lo que concluimos que F es un isomorfismo.

Tenemos que $F(U)$ es la carta dada por la expresión $y_0 \neq 0$ donde y_0 es la primera coordenada homogénea en la imagen de F, una carta afín a la que denotaremos por $V = F(U)$. Entonces la restricción $F : U \longrightarrow V$ es un isomorfismo entre variedades.

Sea $z \in \Gamma(V)$, y denotemos por $w = z \circ F^{-1}$. Como F induce un isomorfismo entre $\Gamma(U)$ y $\Gamma(V)$, sabemos que $w \in \Gamma(U) \subset k(U)$. Vimos que existe un polinomio $H \in k[Y_0, ..., Y_n]$ de grado d de modo que $w = \frac{H}{Y_0^d}$ ya que $I_h(\overline{U}) = I_h(\mathbb{P}^n) = 0$. Entonces, $w \circ F = z = \frac{H(L_0, ..., L_n)}{L_0^d} = \frac{G}{L^d} \in \Gamma(V)$, como queríamos.

Teorema 5 *Sea W una variedad proyectiva de $\mathbb{P}^n$ disjunta de un espacio lineal $E \subset \mathbb{P}^n$ de dimension d. Entonces, la proyección de centro E $\Pi : W \longrightarrow \Pi(W)$ define una aplicación finita con su imagen.*

Demostración: Sean $L_1, ..., L_{n-d}$ las formas lineales que definen a E, y sea $\Pi : W \longrightarrow \mathbb{P}^{n-d-1}$ a proyección de centro E definida para cada punto $x \in W$ como $\Pi(x) = (L_1(x); ...; L_{n-d}(x)) = (y_1; ...; y_{n-d})$, un elemento de $\mathbb{P}^{n-d-1}$. Si denotamos cada $n-d-1$ cartas afines de $\mathbb{P}^{n-d-1}$ definidas por $y_i \neq 0$ por A_i, definimos $U_i = \Pi^{-1}(A_i) \cap W$. U_i es un conjunto abierto de W, ya que la proyección es continua, y un conjunto afín de $\mathbb{A}^n$ en la carta $x_i \neq 0$.

Como los U_i recubren W, trataremos de ver que $\Pi : U_i \longrightarrow A_i \cap \Pi(W)$ es una aplicación finita entre variedades afines: sea $g \in \Gamma(U_i)$, g será de la forma $g = \frac{G(X_0, ..., X_n) + I_h(W)}{L_i^m + I_h(W)}$ en virtud del lema 14 donde G es un polinomio homogéneo de grado m. Consideremos $\pi : W \longrightarrow \mathbb{P}^{n-d}$ dada por $\pi(x) = (L_1^m(x); ...; L_{n-d}^m(x); G(x)) = (z_1; ...; z_{n-d+1}) \in \mathbb{P}^n$. π es una aplicación regular, pues el punto $(0; ...; 0) \notin \mathbb{P}^n$ y, en virtud de la proposición 45, $\pi(W)$ es un cerrado de $\mathbb{P}^{n-d}$, es decir, un conjunto algebraico, luego existen polinomios $F_1, ..., F_s \in k[Z_1, ..., Z_{n-d+1}]$ de modo que $\pi(W) = V_h(F_1, ..., F_s)$.

Ahora bien, como W es disjunto de E, los polinomios L_i no se anulan a la vez en W, con lo que el punto $(0; ...; 0; 1) \in \mathbb{P}^{n-d}$ no pertenece a $\pi(W)$. En consecuencia, el sistema de ecuaciones

$$Z_1 = ... = Z_{n-d} = F_1(Z_1, ..., Z_{n-d+1}) = ... = F_s(Z_1, ..., Z_{n-d+1}) = 0$$

no tiene solución, es decir, el conjunto algebraico $V_h(Z_1, ..., Z_{n-d}, F_1, ..., F_s) \subset \mathbb{P}^n$ es el conjunto vacío, y en virtud del lema 1, existe $r > 0$ tal que $(Z_1^r, ..., Z_{n-d+1}^r) \subset (Z_1, ..., Z_{n-d}, F_1, ..., F_s)$. En particular, $Z_{n-d+1}^r \subset (Z_1, ..., Z_{n-d}, F_1, ..., F_s)$, por lo tanto, existirán polinomios $G_j, H_k \in k[Z_1, ..., Z_{n-d+1}]$ tales que $Z_{n-d+1}^r = \sum_{j=1}^{n-d} Z_j G_j + \sum_{k=1}^s F_k H_k$. Como en $\pi(W)$ $F_k = 0$, aplicando un argumento sobre el grado de la expresión anterior, concluimos que el polinomio $\phi(Z_1, ..., Z_{n-d}) = Z_{n-d+1}^r - \sum_{j=1}^{n-d} Z_j G_j^{(r-1)}$ se anula en $\pi(W)$ cuando $G_j^{(r-1)}$ represente a la parte homogénea de grado $r-1$ de G_j. Además, podemos ver al polinomio homogéneo ϕ como un polinomio en Z_{n-d+1}, de grado r, y que es mónico, y podemos reescribirlo como $\phi(Z_{n-d+1}) = Z_{n-d+1}^r + \sum_{j=0}^{r-1} B_j(Z_1,\ldots,Z_{n-d})Z_{n-d+1}^j$ para ciertos polinomios homogéneos B_j de grado $r-j$. Por último, si consideramos $\phi\circ\pi$ y dividimos a esta aplicación por L_i^{mr} tenemos que $g^r + \sum_{j=0}^{r-1} B_j(L_1^m,\ldots,L_{n-d}^m)g^j \frac{1}{L_i^{(r-j)m}} = 0$ en W, y como B_j son homogéneos de grado $r-j$, $\frac{B_j(L_1^m,\ldots,L_{n-d}^m)}{L_i^{(r-j)m}} = B_j(L_1^m,\ldots,1,\ldots,L_{n-d}^m)$. Luego $g^r + \sum_{j=0}^{r-1} B_j(Y_1^m,\ldots,1,\ldots,Y_{n-d}^m)g^j = 0$ en $A_i \cap \Pi(W)$ es decir, g es entero sobre $\Gamma(A_i\cap\Pi(W))$ ya que $B_j(Y_1^m,\ldots,1,\ldots Y_{n-d}^m)$ está bien definida en todos los puntos $(Y_1^m,\ldots,Y_{n-d}^m)$ tales que $Y_i = L_i(x)$, $x\in W$, con $L_i(x) = 1 \neq 0$, teniendo en cuenta que si $L_i(x)\neq 1$, $x' = \frac{x}{L_i(x)} = x \in W$ y que $L_i(x') = 1$.

Proposición 46 *Sea $X \subset \mathbb{P}^n$ una variedad y sean $F_0,\ldots,F_s \in k[X_0,\ldots,X_n]$ polinomios homogéneos del mismo grado m de modo que para todo $x\in X$ existe i tal que $F_i(x)\neq 0$. Entonces, la aplicación dada por $\phi(x) = (F_0(x),\ldots,F_s(x))$ es una aplicación finita.*

Demostración: Consideremos el m-ésimo embebimiento de Vernose $\gamma_m : \mathbb{P}^n \longrightarrow \mathbb{P}^N$ donde $N = \binom{m+n}{m} - 1$. Podemos ver los polinomios F_i como formas lineales dentro de $\mathbb{P}^N$ de la siguiente forma: si $F = \sum_j a_j X_0^{m_0^j}\ldots X_n^{m_n^j}$ es un polinomio homogéneo de grado m, entonces, $\sum_k m_k^j = m$ y $F = \sum a_j \gamma_{m_0,\ldots,m_n}$ es una forma lineal L en $\mathbb{P}^n$. Representemos por L_i las formas lineales correspondientes a los polinomios F_i.

Si denotamos por $\Pi = (L_1;\ldots;L_s)$ se verifica que $\phi = \Pi\circ\gamma_m$, pues si $p = (x_0;\ldots;x_n)\in\mathbb{P}^n$, entonces, $\gamma_m(p) = (\gamma_{i_0,\ldots,i_n} = x_0^{i_0}\ldots x_n^{i_n})$ y por tanto

$$\Pi\circ\gamma_m(p) = (L_1(\gamma_{i_0,\ldots,i_n} = x_0^{i_0}\ldots x_n^{i_n});\ldots;L_s(\gamma_{i_0,\ldots,i_n} = x_0^{i_0}\ldots x_n^{i_n})) =$$

$$= (F_1(x_0,\ldots,x_n);\ldots;L_s(x_0,\ldots,x_n)) = \phi(p)$$

y como γ_m es un isomorfismo, basta con aplicar el teorema 5 para concluir lo deseado.

2.4. Aplicaciones racionales y birracionales

Definición 42 *Si X e Y son dos variedades y U_1, U_2 son dos subvariedades abiertas de X, diremos que dos morfismos $f_1 : U_1 \longrightarrow Y$ y $f_2 : U_2 \longrightarrow Y$ son equivalentes si las restricciones de ambos morfismos al abierto $U_1\cap U_2$ coinciden. Esta relación es de equivalencia y llamaremos* aplicacion racional *a cada clase de equivalencia.*

Las aplicaciones racionales son aplicaciones entre variedades X e Y cuyos dominios de definición son la unión de todas las subvariedades abiertas $U\subset X$ tales que $f : U \longrightarrow Y$ pertenece a la clase de equivalencia.

En consecuencia, en toda aplicación racional existe un morfismo $f : U \longrightarrow Y$ definido en todo el dominio de la aplicación racional, la subvariedad U. En este caso, el resto de morfismos que están en la misma clase de equivalencia que f son restricciones de f a alguna subvariedad abierta de U. A la vista de esto, las aplicaciones racionales se pueden definir también como morfismos entre variedades X e Y cuyo dominio de definición sea una subvariedad a bierta de U no se puede extender a otra subvariedad de X que conga a U.

Proposición 47 *Sea $F : X \longrightarrow Y$ una aplicación racional entre las variedades X e Y.Entonces:*

(1) Si $F(X)$ es denso en Y, F induce un morfismo $\overline{F} : k(Y) \longrightarrow k(X)$.

(2) Sean $p\in X$ y $q\in Y$ dos puntos de modo que $O_p(X)$ domina a $\overline{F}(O_q(Y) \subset O_p(X)$. Entonces, $p\in D(F)$ y $F(p) = q$.

Demostración: (1) Sea $F : U \longrightarrow V$ un morfismo que represente a F con $U \subset X$ y $V \subset Y$ abiertos afines. Sabemos que F induce un morfismo $\overline{F} : \Gamma(V) \longrightarrow \Gamma(U)$ que es inyectivo como vimos en el lema 12. Podemos, por tanto, extender $\overline{F}$ a $k(V)$ y $k(U)$ de la siguiente forma, si $z \in k(V)$, entonces $z = \frac{g}{h}$ con $g, h \in \Gamma(V)$ y $h \neq 0$, definimos, entonces $\overline{F}(z) = \frac{\overline{F}(g)}{\overline{F}(h)}$ que será un elemento de $k(U)$ pues $k(U) = Frac(\Gamma(U))$ y $\overline{F}(h) \neq 0$ al ser $h \neq 0$. Como $k(V) = k(Y)$ y $k(U) = k(X)$ necesitamos ver que no depende de los abiertos afines que elijamos para definir el morfismo. Sea $G : U' \longrightarrow V'$ otro morfismo que represente a f con $U' \subset X$ y $V' \subset Y$ abiertos afines. Entonces, $F(p) = G(p)$ para todo punto $p \in U \cap U'$, por tanto, si $z = \frac{P+I_h(\overline{Y})}{Q+I_h(\overline{Y})}$ con P, Q polinomio del mismo grado y $Q(p) \neq 0$ para $p \in F^{-1}(U \cap U') \subset Y$, entonces $\frac{P \circ F+I_h(\overline{X})}{Q \circ F+I_h(\overline{X})} = \frac{P \circ G+I_h(\overline{X})}{Q \circ G+I_h(\overline{X})}$ en $U' \cap U$, un denso de $\overline{X}$, luego son iguales en todo X.

(2) Tomemos entornos afines $V \subset X$ y $W \subset Y$ de p y q respectivamente. Podemos escribir $\Gamma(W)$ como $k[y_1, ..., y_m]$. Entonces, $\overline{F}(y_i) \in k(V)$, con lo que existen $a_i, b_i \in \Gamma(V)$ y $\overline{F}(y_i) = \frac{a_i}{b_i}$. Como $y_i \in \Gamma(W) \subset O_q(Y)$ y $\overline{f}(O_q(Y)) \subset O_p(X)$, $\overline{f}(y_i) = \frac{a_i}{b_i} \in O_p(X)$ y por tanto $b_i(p) \neq 0$.

Tomemos $b = b_1 ... b_m$, entonces $\overline{F}(\Gamma(W)) \subset \Gamma(V)[\frac{1}{b}] = \Gamma(V_b)$ como en la proposición 39. Tenemos entonces un morfismo $\overline{F} : \Gamma(W) \longrightarrow \Gamma(V_b)$ que en virtud de la proposición 42 induce un morfismo $f : V_b \longrightarrow W$. Como V_b es el conjunto de puntos de V que no se anulan en b, $p \in U_b$, y como este morfismo f es un representante de F, $p \in D(F)$.

Por otra parte, $\overline{F}(m_q) \subset m_p$, es decir, la imagen por $\overline{F}$ de toda función racional que se anule en q se anula en p. Entonces, si $F(p) = t \neq q$, tomamos z es una función racional de $k(Y)$ que se anula en q pero no en t y tendremos $\overline{F}(z)(p) = s(t) \neq 0$, lo cual es imposible. Por lo tanto, $F(p) = q$.

Proposición 48 *Sean X e Y dos variedades afines y sea $F : X \longrightarrow Y$ una aplicación racional cuya imagen es densa en Y. Entonces, la aplicación $\overline{F} : \Gamma(Y) \longrightarrow \Gamma(X)$ que induce F no es inyectiva.*

Demostración: Como $F(X)$ no es denso, existirá un abierto $U \subset Y$ con $U \cap F(X) = \emptyset$. Como U es un abierto para la topología de subespacio de Y, existirá $V \subset \mathbb{A}^m$ un abierto con $U = V \cap Y$.

Como el complementario de un abierto es un cerrado, existirán polinomios $P_1, ..., P_s \in k[Y_1, ..., Y_m]$ con $\mathbb{A}^m \setminus V = V(P_1, ..., P_s)$. Como U es no vacío, $Y \not\subset V(P_1, ..., P_s)$, es decir, existirá i con $P_i \notin I(Y)$. Es decir, $p_i = P + I(Y) \subset \Gamma(Y)$ es no nulo.

Por otra parte, como $F(X) \cap U = \emptyset$, $F(X) \cap V = \emptyset$, con lo que $F(X) \subset V(P_1, ..., P_s) \subset V(P_i)$, luego $\overline{F}(p_i) = 0$ en X pese a que $p_i \neq 0$, luego $\overline{F}$ no puede ser inyectiva.

Nota: en la proposición 38 vimos que morfismos que coinciden en la intersección de sus abiertos de definición podían extenderse a un morfismo definido en la unión de todos los abiertos.

Definición 43 *Una aplicación racional $f : X \longrightarrow Y$ diremos que es una* aplicación birracional *si para algún abierto $U \subset X$ y para algún abierto $V \subset Y$ existe un representante de f que sea un isomorfismo entre U y V.*

Definición 44 *Dadas dos variedades X, Y, diremos que son* birracionalmente equivalentes *si existe una aplicación birracional entre ellas.*

Proposición 49 *Sean X, Y dos variedades. X e Y son birracionalmente equivalentes si y solo si $k(X)$ y $k(Y)$ son isomorfos.*

Demostración: Supongamos que X e Y son birracionalmente equivalentes. Existirán $U \subset X$ y $V \subset Y$ abiertos con $k(U)$ y $k(V)$ isomorfos. Concluimos lo deseado fijándonos en que $k(U) = k(X)$ y que $k(V) = k(Y)$.

Supongamos ahora que $k(X)$ y $k(Y)$ son isomorfos. Entonces $\Gamma(X)$ son los polinomios $k[X_1, ..., X_n]$ módulo el ideal $I(X)$. Pongamos $\Gamma(X) = K[x_1, ..., x_n]$ donde $x_i = X_i + I(X)$. Entonces, $\phi(x_i) = \frac{a_i}{b_i}$

para $a_i, b_i \in \Gamma(Y)$. Tomemos $b = b_1...b_n \in \Gamma[Y]$, de esta forma, $\Gamma(Y_b) = \Gamma(y)[\frac{1}{b}]$ y es evidente que $\phi(\Gamma(X)) \subset \Gamma(Y_b)$, con la notación de la proposición 39. Como ϕ es un isomorfismo, existirá también $d \in \Gamma(X)$ con $\phi^{-1}(\Gamma(Y)) \subset \Gamma(X_d)$. Entonces, la restricción de $\phi : \Gamma((X_d)_{\phi^{-1}(b)}) \longrightarrow \Gamma((Y_b)_{\phi(d)})$ es un isomorfismo. Y en virtud de la proposición 36 tenemos que los abiertos $(X_d)_{\phi^{-1}(b)}$ y $(Y_b)_{\phi(d)}$ son isomorfos, y por tanto, ϕ es una aplicación birracional.

Proposición 50 *Sea $f : X \longrightarrow Y$ una aplicación birracional entre las variedades X e Y. Entonces, la imagen de f es un denso de Y.*

Demostración: Como f birracional existen $U \subset X$ y $V \subset Y$ en los que f define un isomorfismo, entonces, la imagen de f contiene a $f(U) \subset V$, abierto de un abierto de Y, luego un abierto de Y y por tanto denso en Y. Es decir, la imagen de f contiene un denso de Y, luego es densa.

2.5. Dimensión de una variedad

Proposición 51 *Sea X una variedad de $\mathbb{P}^n$ entonces $k(X) : k$ es una extensión de cuerpos con grado de trascendencia finito.*

Demostración: Sabemos que $(\overline{X})_*$ es una variedad afín y que $k(X) = k(\overline{X}) = K((\overline{X})_*)$. Es decir, $k(X) = Frac(\frac{k[X_1,...,X_n]}{I((\overline{X})_*)}) = Frac(k[\overline{X_1},...,\overline{X_n}]) = k(\overline{X_1},...,\overline{X_n})$. Luego evidentemente $k(X) : k(\overline{X_1},...,k(\overline{X_n}))$ es algebraica y por tanto el grado de trascendencia de la extensión $k(X) : k$ es como mucho n, es decir, finito.

Definición 45 *Sea X una variedad. Definiremos la* dimensión *de la variedad X como el grado de trascendencia de la extensión de cuerpos $k(X) : k$ y lo denotaremos por $dim(X)$.*

Proposición 52 *La dimensión de $\mathbb{P}^n$ como variedad es n.*

Nota: En la demostración de la proposición 51 hemos visto que si X es una variedad de $\mathbb{P}^n$ entonces la dimensión de X es $dim(X) \leq n$.

Definición 46 *Sea W un conjunto algebraico (afín o proyectivo). Definimos la dimensión de W como la mayor dimensión de sus componentes irreducibles.*

Nota: Sea $U \subset X$ una subvariedad abierta de X, entonces $dim(U) = dim(X)$ pues $k(U) = k(X)$.

Teorema 6 *Sean W y V dos conjuntos algebraicos proyectivos (resp. variedades) con $W \subset V$, entonces $dim(W) \leq dim(V)$. Si además V es irreducible, W es cerrado en V y $dim(W) = dim(V)$ entonces $W = V$.*

Demostración: Supongamos que ambas afirmaciones son ciertas para W, V conjuntos algebraicos afines y consideremos los conjuntos algebraicos afines $\overline{V}_*$ y $\overline{W}_*$. En el caso de que V, W conjuntos algebraicos proyectivos, V y W ya serán cerrados en $\mathbb{P}^n$ con lo que no hace falta tomar su clausura, sí es necesario en el caso en el que trabajemos con variedades, sin embargo, como $\overline{V} = V$ y $\overline{W} = W$ cuando trabajamos con conjuntos algebraicos proyectivos las siguientes afirmaciones serán ciertas para ambos casos (algunas de ellas quizás triviales para conjuntos algebraicos).

Los conjuntos $\overline{V}_*$ y $\overline{W}_*$ se pueden ver como subvariedades abiertas de $\overline{V}$ y $\overline{W}$ respectivamente, luego $k(\overline{V}_*) = k(\overline{V}) = k(V)$ y $k(\overline{W}_*) = k(\overline{W}) = k(W)$. Por tanto, es evidente que $dim(W) \leq dim(V)$ y como si V es irreducible, $\overline{V}_*$ también lo será, tendremos también que $\overline{V} = (\overline{V}_*)^* = (\overline{W}_*)^*$. Por otra parte, $\overline{W}$ no tiene por qué coincidir con $(W_*)^*$ al no ser W irreducible, pero sí tenemos que

$\overline{V} = (\overline{W}_*)^* \subset \overline{W}$, de lo que deducimos $\overline{W} = \overline{V}$. Entonces, $V = \overline{W}$ esta vez tomando la clausura de W en V, pero como W es cerrado en V, concluimos que $V = W$.

Veamos ahora que el resultado es cierto para V, W conjuntos algebraicos afines. Como la dimensión de V y W es la mayor de las de sus componentes homogéneas, podemos suponer que V y W son irreducibles. Sea $m = dim(V)$, entonces, cualquier conjunto formado por $m+1$ elementos de $\Gamma(V) \subset k(V)$ será algebraicamente dependientes, y en particular, lo será el formado por los elementos $x_1 = X_1 + I(V), ..., x_{m+1} = X_{m+1} + I(V)$ (podemos suponer $m < n$, si no prodríamos ver $W \subset V \subset \mathbb{P}^{n+1}$) son algebraicamente dependientes, es decir, existe un polinomio $P \in k[T_1, ..., T_{m+1}]$ tal que $P(x_1, ..., x_{m+1})$ se anula en V, y como $W \subset V$, también se anula en W. Es decir, todo subconjunto de $m+1$ elementos $y_1 = X_1 + I(W), ..., y_n = X_n + I(W)$ es algebraicamente dependietes como elementos de $k(W) = k(y_1, ..., y_n)$. En el teorema 13 vimos que podemos tomar una base de trascendencia a partir de los elementos $y_1, ..., y_n$ (esta base puede ser vacía si $k(W) : k$ fuera una extensión algebraica), y hemos visto entonces, que esta base de trascendencia ha de tener a lo sumo m elementos, y por tanto, $dim(W) \leq m = dim(V)$.

Supongamos ahora que $dim(V) = dim(W) = m$. Existen, por tanto, m elementos de $y_1, ..., y_n$ que son algebraicamente independientes como elementos de $k(W) = k(y_1, ..., y_n)$, pongamos $y_1, ..., y_m$, entonces, $x_1, ..., x_m$ son algebraicamente independientes como elementos de $k(V) = k(x_1, ..., x_n)$, pues si para algún $P \in k[T_1, ..., T_n]$, $P(x_1, ..., x_m) = 0$ en V, también se anulará en W, es decir, $P(y_1, ..., y_n) = 0$, pero esto implica que $P = 0$.

Sea $u \in \Gamma(V)$ con $u \neq 0$ pero con $u = 0$ en X. El conjunto $\{x_1, ..., x_m, u\}$ es algebraicamente dependiente pues $\{x_1, ..., x_m\}$ es una base de trascendencia de $k(V)$, por lo tanto, existe un polinomio $a \in k[x_1, ..., x_m][U]$ no nulo que podemos suponer irreducible con $a(x_1, ..., x_m)(u) = 0$. Como $a(x_1, ..., x_m)$ es irreducible, si escribimos $a(x_1, ..., x_n)(U) = \sum_{k=0}^{d} a_k(x_1, ..., x_m)U^k$, necesariamente $a_0(x_1, ..., x_m)$ es no nulo en Y.

Ahora bien, como $u = 0$ en W, $a(y_1, ..., y_m)(u) = a_0(y_1, ..., y_m) = 0$ en W. Pero $x_1, ..., x_n$ eran algebraicamente independientes en W, luego $a_0 \equiv 0$ en todo $\mathbb{A}^n$ contra hipótesis.

Es decir, si $u \in \Gamma(V)$ es tal que $u = 0$ en W, $u = 0$ en V, y por tanto, $I(W) \subset I(V)$, de lo que deducimos $V \subset W$ y concluimos $V = W$.

Lema 15 *Sea $\phi : X \longrightarrow Y$ una aplicación finita entre variedades. Entonces, $dim(X) = dim(Y)$.*

Demostración: podemos suponer que X e Y son variedades afines contenidas en $\mathbb{A}^n$ y $\mathbb{A}^m$ respectivamente. Como ϕ es una aplicación regular, es un morfismo en virtud de la proposición 44. Además, $\phi(X)$ es denso en Y, luego podemos aplicar el lema 12. Sea $\overline{\phi}$ el morfismo de anillos inyectivo del lema.

Sea ahora $z \in k(Y)$ una función racional. Existirán por tanto $f, g \in \Gamma(Y)$ funciones regulares con $g \neq 0$ de modo que $z = \frac{f}{g}$. Como $\overline{\phi}$ es inyectiva $g \circ \phi \neq 0$ y por tanto, $z \circ \phi = \frac{f \circ \phi}{g \circ \phi}$ es una función racional de $k(X)$. Definimos así una $k(Y)$-álgebra que nos permite ver $k(Y) \subset k(X)$. Veamos que esta es en realidad una extensión de cuerpos algebraica.

Si $z = \frac{f}{g}$ como antes, sabemos que $f, g \in \Gamma(X)$ son enteros sobre $\Gamma(Y)$ y por consiguiente, algebraicos sobre $k(Y) \supset \Gamma(Y)$. Como f es algebraico sobre $k(Y)$ también lo es su inverso $\frac{1}{f}$ y como el producto de dos elementos algebraicos también es algebraico, tenemos que $\frac{f}{g} = z$ es algebraico sobre $k(Y)$ y por consiguiente, la extensión es algebraica.

Hemos visto que la extensión es algebraica, por tanto, ambos cuerpos tienen el mismo grado de trascendencia sobre k, es decir, X e Y tienen la misma dimensión

Teorema 7 *Sea W una variedad proyectiva y sea $F \in k[X_0, ..., X_n]$ un polinomio homogéneo que no es idénticamente nulo en W. Entonces, $dim(V_h(F) \cap W) = dim(W) - 1$.*

Demostración: Empecemos fijándonos en que para todo conjunto algebraico podemos encontrar un polinomio $G \neq 0$ del grado m que deseemos. Para ello basta con tomar un elemento del conjunto algebraico y considerar una forma lineal L que no se anule en dicho punto y tomar $G = L^m$.

Tenemos ahora $F \neq 0$ en W, denotaremos por $W_F \subset W$ a $V_h(F) \cap W$. En virtud del teorema 6 $dim(W_F) < dim(W)$ por ser W irreducible. Tomamos $W^0 = W$, W^1 una componente irreducible de W_F y $F_0 = F$. Por el mismo resultado, $dim(W^1) < dim(W^0)$. Buscamos ahora F_1 del mismo grado de F_2 tal que $F_2 \neq$ en W^1. Llamamos $W^2 = V_h(F) \cap W^1$. $dim(W^2) \leq dim(W^1)$ por el teorema 6.

Iterando el razonamiento conseguimos una cadena de variedades proyectivas W^i y una sucesión de polinomios F_i verificando la cadena $W^0 \supset W^1 \supset ...$ con W^i una componente irreducible de $V_h(F_{i-1}) \cap W^{i-1}$ y con $dim(W^{i+1}) < dim(W^i)$.

En virtud del teorema 6 $dim(W^{i+1}) < dim(W^i)$, luego si $dim(W) = m$, $W^{m+j} = \emptyset$ para $j > 0$ y para todo $x \in W$ existe $i < m+1$ tal que $F_i(x) \neq 0$, pues de no ser así, existiría $x \in W^i$ para todo $i = 0, ..., m$ y tomando F_m del mismo grado que los demás y que se anule en x y consideramos $W^{m+1} = V_h(F^m) \cap W^m$ que no sería un conjunto vacío pues $x \in W^{m+1}$.

Consideramos ahora la aplicación $\phi : W \longrightarrow \mathbb{P}^m$ dada por $\phi(x) = (F_0(x); ...; F_m(x))$. En virtud de la proposición 46 $W \longrightarrow \phi(W)$ es una aplicación finita, por lo tanto, en virtud del lema 15, $dim(X) = dim(\phi(W)) = m$ y como $\phi(W) \subset \mathbb{P}^m$ es un cerrado por la proposición 45, es decir, un conjunto algebraico, con lo que $\phi(W) = \mathbb{P}^m$ en virtud del teorema 6.

Supongamos ahora que $dim(V_h(F)) < m-1$, entonces $W^m = \emptyset$ y como antes $F_0, ..., F_{m-1}$ no tienen ceros en común en W, luego $(0; ...; 0; 1) \notin \phi(W)$, en contra de que $\phi(W) = \mathbb{P}^m$.

Corolario 4 *Si X es una variedad y $F \in k[X_0, ..., X_n]$ un polinomio homogéneo que no es idénticamente nulo en X. Entonces, $dim(V_h(F) \cap X) = dim(X) - 1$.*

Demostración: Sabemos que $\overline{X}$ es una variedad proyectiva que contiene a X, y como F no es nulo en X, no será nulo en $\overline{X}$ tampoco, y además $dim(X) = dim(\overline{X})$. Por otra parte, $V_h(F) \cap X$ es un abierto de $V_h(F) \cap \overline{X}$ y por tanto $dim(V_h(F) \cap X) = dim(V_h(F) \cap \overline{X}) = dim(\overline{X}) - 1 = dim(X) - 1$.

Corolario 5 *La dimensión de una variedad proyectiva W se puede definir como el máximo entero m tal que tal que existe una cadena $\emptyset \subsetneq V_1 \subsetneq ... \subsetneq V_n \subsetneq W$ de longitud m de subvariedades irreducibles $V_i \subset W$.*

Corolario 6 *Sean $F_1, ..., F_s \in k[X_0, ..., X_n]$. La dimensión de $V_h(F_1, ..., F_s)$ es mayor o igual que $n-s$.*

Corolario 7 *Sea $V_h(F)$ con $F \in k[X_0, ..., X_n]$ un polinomio homogéneo no nulo, una hipersuperficie. Entonces, $dim(V_h(F)) = n-1$.*

Proposición 53 *Sea W una variedad proyectiva de dimensión 0. Entonces, W consta de un único punto.*

Demostración: Como los puntos son variedades de dimensión 0, si W constara de más de un punto, tendríamos que para cualquier $p \in W$ $\{p\} \subsetneq W$, con lo que $dim(W) \geq 1$.

Definición 47 *A las variedades proyectivas de dimensión 1 las llamaremos* curvas.

Proposición 54 *Sea C una curva y sea $z \in k(C)$, $z \notin k$. Entonces $k(C)$ es algebraico sobre el cuerpo de fracciones de $k[z]$, $k(z)$.*

Demostración: Como el grado de trascendencia de la extensión $k(C) : k$ es 1, podemos tomar $t \in k(C)$ tal que $k(C)$ sea algebraico sobre $k(t)$, entonces, z será algebraico sobre $k(t)$, es decir, quitando denominadores, existe un polinomio $P \in k[Z, T]$ tal que $P(z, t) = 0$. Como k es algebraicamente cerrado, como el conjunto de elementos algebraicos de un cuerpo algebraicamente cerrado es el propio cuerpo, tenemos que z no es algebraico sobre k y por tanto no puede existir ningún polinomio de una variable con coeficientes en k que se anule en z, y por tanto, T aparece en P, y como $P(z,t)=0$ deducimos que t es algebraico sobre $k(z)$. Ahora, como $k(z,t)$ es el menor cuerpo que contiene a $k(z)$ y a t y t es algebraico sobre $k(z)$, como el cuerpo de elementos algebraicos de de $k(x,t)$ sobre $k(x)$ es un subcuerpo de $k(x,t)$ que contiene a $k(x)$ ha de ser el propio $k(z,t)$, es decir, $k(z,t)$ es algebraico sobre $k(x)$. Por últimos, teniendo en cuenta que $k(C)$ es algebraico sobre $k(z,t)\supset k(t)$, concluimos que $k(C)$ es algebraico sobre $k(z)$.

Proposición 55 *Sean C y C' dos curvas y sea $F: C\longrightarrow C'$ una aplicación racional. Entonces:*

(1) O $F(C)$ es denso en C' o F es constante.

(2) Si F no es constante, $k(C):\overline{F}(k(C'))$ es una exensión algebraica finita.

Demostración: (1) Es evidente que si F es constante, $F(C)$ no es denso.

Supongamos que C y C' son curvas planas afines. Si $F(C)$ no es denso, en virtud de la proposición 48, existe $T\in k[X_1,X_2]$ con $t=T+I(C')\neq 0$ pero con $\overline{F}(t)=0$, es decir, $T\circ F\in I(C)$. Entonces, $F(C)\subset V(T)\cap C'$ y por tanto, $dim(F(C))\leq dim(V(T)\cap C')=0$ en virtud de el teorema 6 y del teorema 7. Entonces, aplicando la proposición 53, concluimos que $F(C)$ es un conjunto finito.

Pongamos que $F(C)=\{p_1,...,p_t\}\subset C'$ con $t\geq 2$ y consideremos lo abiertos $U_1=C'\setminus\{p_2,...,p_t\}$ y $U_t=C'\setminus\{p_1,...,p_{t-1}\}$. Entonces, $V_1=F^{-1}(U_1)$ son los puntos de C cuya imagen es p_1 y $V_t=F^{-1}(U_t)$ son los puntos de C cuya imagen es p_t y como $p_1,p_t\in F(C)$ ninguno de lo abiertos V_1 ni V_t son vacíos, luego $V_1\cap V_t\neq\emptyset$ pero esto es imposible, pues un punto no puede tener dos imágenes.

Ahora que hemos visto el resultado par curvas planas afines, supongamos C y C' curvas planas proyectivas. Podemos ver F como un morfismo $F: D(F)\longrightarrow C'$ definido en un abierto $D(F)\subset C$. Si $F(C)$ no es denso en C', existe un abierto afín U con $p\in U\subset D(F)\subset C$. Tomemos $q\in C$ con $F(q)=p$. Entonce, $q\in F^{-1}(U)$ y $F^{-1}(U)\subset D(f)\subset C$, luego, por ser F un morfismo continuo y U un abierto, $F^{-1}(U)$ es un abierto que contiene a q. Entonces, existirá V un abierto afín con $q\in V\subset F^{-1}(U)$. Además, $F(V)\subset U$.

Consideremos la restricción $F: V\longrightarrow U$ entre variedades afines. Como $F(V)\subset F(C)$, $F(V)$ no puede ser denso en U, luego la restricción de F ha de ser constante.

Por otra parte, el conjunto de puntos de $D(F)$ que tienen a p por imagen es un cerrado de C que contiene a V, puesto que $q\in V$, $F(q)=p$ y F es constante en V, luego, por continuidad y porque V es un abierto denso de C, el conjunto de puntos de $D(F)$ cuya imagen es p ha de ser todo C, y por tanto F es constante.

(2) Como $F(C)$ es denso, podemos aplicar la proposición 47 y deducimos que F induce un morfismo $\overline{F}: k(C)\longrightarrow k(C')$. Veamos que $\overline{F}$ es inyectiva: si $z\in Ker(\overline{F})$, entonces para todo $p\in C$, $z(F(p))=0$ pues $z\circ F=0$, es decir, z se anula en un denso de C', luego $z=0$ en todo C' en virtud de la proposición 26.

Como $\overline{F}$ es inyectiva, $k(C')$ es isomorfo a su imagen por $\overline{F}$, luego el grado de trascendencia de $k(C):k$ es el mismo que el de $\overline{F}(k(C')):k$, es decir, 1, que es el mismo que el de $k(X):k$. Por tanto, si $x\in\overline{F}(k(C'))$ es un elemento algebraicamente independiente sobre k, será una base de trascendencia, y como $\overline{F}(k(C'))\subset k(C)$, $x\in k(C)$ será también algebraicamente independiente sobre k como elemento de $k(C)$, luego también será una base de trascendencia de $k(C)$ sobre k y por tanto, si $y\in k(C)$, $x\neq y$, y será algebraico sobre $k(x)\subset\overline{F}(k(C'))$, luego también será algebraico sobre $\overline{F}(k(C'))$. Es decir, la extensión $k(C):\overline{F}(k(C'))$ es algebraica.

Ahora bien, si pensamos en cualquier abierto afín de C, su cuerpo de fracciones coincidirá con el de C y tendremos que $k(C)=Frac(\frac{k[X_1,...,X_n]}{I})=k(X_1+I,...,X_n+I)$ para algún ideal I, luego está generado finitamente como k-álgebra. Además, como $k\subset\overline{F}(k(C))\subset k(C')$, $k(C)$ y la extensión $k(C):\overline{F}(k(C'))$ es algebraica, es inmediato que la extensión es también finita.

Capítulo 3

El género

3.1. Curvas y curvas planas

Proposición 56 *Sea C una cuerva y $k(C)$ su cuerpo de fracciones. Entonces, si k tiene característica 0, existen $x, y \in k(C)$ con $x \notin k$ de modo que $k(x, y) = k(C)$.*

Demostración: Como C tiene dimensión 1, existe un elemento $x \in k(C)$, $x \notin k$, tal que $k : k(x)$ es una extensión algebraica. Basta, por tanto, con aplicar el teorema del elemento primitivo.

Definición 48 *A las curvas de $\mathbb{P}^2$ las llamaremos* curvas planas. *Si la curva es una variedad afín la llamaremos* curva plana afín.

Proposición 57 *Toda curva plana es una hipersuperficie.*

Demostración: Sea C una curva plana, supongamos que $C \subset \mathbb{A}^2$ es una variedad afín. Entonces, $I(C) \neq 0$, pues si no $C = \mathbb{A}^2$ tendría dimensión 2, entonces, existe $F \in I(C)$, $F \neq 0$. Si F fuera constante, sería una unidad en $k[X_1, X_2]$, es decir $I(C) = (1)$ y $C = \emptyset$. Como F no constante, podemos escribir $F = F_1 \ldots F_s$ donde F_j son factores irreducibles de F. Ahora bien, como C es irreducible, $I(C)$ es primo,luego existirá i con $F_i \in I(C)$.

Veamos que $I(C) = (F_i)$: evidentemente $(F_i) \subset I(C)$. Para ver la otra contención supongamos que existe $G \in I(C)$ pero con $G \notin (F_i)$. En virtud del teorema 7, $V(F_i) \subset \mathbb{A}^2$ tiene dimensión 1 y como $G \notin (F_i)$, $G \neq 0$ en $V(F_i)$ y por tanto $V(G, F)$ tiene dimensión 0. Sin embargo $C \subset V(G, F)$, luego C tiene dimensión 0, contra hipótesis. Por tanto, $I(C) = (F_i)$, y $C = V(F_i)$ es una hipersuperficie de $\mathbb{A}^2$.

Supongamos ahora que C es una curva plan proyectiva. Entonces, consideremos C_* la curva plana proyectiva afín en una carta adecuada para que $C_* \neq \emptyset$. Entonces $C_* = V(f)$ será un hipersuperficie y como las curvas son irreducibles, $C = (C_*)^* = V_h(f^*)$ será una hipersuperficie de $\mathbb{P}^2$.

Definición 49 *Sea C una curva plana y sea H el polinomio que la define. Diremos que C es una* curva irreducible *si el polinomio H lo es, es decir, cuando es un cerrado irreducible.*

Proposición 58 *Toda cuerva es birracionalmente equivalente a una curva plana.*

Demostración: Sea C una curva en $\mathbb{P}^n$ y sea $k(C)$ su cuerpo de fracciones. En virtud de la proposición anterior, existirán $x, y \in k(C)$ con $k(C) = k(x, y)$.

Consideremos la aplicación $\varphi : k[X, Y] \longrightarrow k[x, y] \subset k(C)$ y denotemos por $I = Ker(\varphi)$. El ideal I es un ideal primo, luego $V = V(I) \subset \mathbb{A}^2$ es una variedad afín con $\Gamma(V) = \frac{k[X,Y]}{I}$ isomorfo a $k[x, y]$

puesto que φ es sobreyectiva. Por lo tanto, $K(V) = Frac(\Gamma(V))$ y $k(C) = k(x, y) = Frac(k[x, h])$ son isomorfos, y como el cuerpo de fracciones de $V^* \subset \mathbb{P}^2$ cumple $k(V) = k(V^*)$, también se tienen las igualdades $dim(V^*) = dim(V) = dim(C) = 1$, es decir, V^* es una curva plana. Aplicando la proposición 49 concluimos.

Definición 50 *Sea $p \in C$ un punto cualquiera. Diremos que p es un punto* regular, simple *o* no singular *si $O_p(C)$ es un anillo de valoración discreto.*

Definición 51 *A todo punto $p \in C$ que no es regular se le conoce como* singular.

Definición 52 *A las curvas cuyos puntos son todos regulares se las llama* curvas regulares.

Proposición 59 *Sea C una curva regular, y sea $z \in k(C)$ una función racional. Entonces, un punto $p \in C$ es un cero de z si y sólo si p es un polo de z^{-1}.*

Demostración: Como C es una curva regular, $O_p(C)$ es un anillo de valoración discreta cuyo cuerpo de fracciones es $k(C)$, y por lo tanto, existe $t \in O_p(C)$ tal que $z = vt^n$ con $v \in O_p(C)$ una unidad y n un número entero. Es decir, $n \geq 0$ si y solamente si $z \in O_p(C)$ y $n \leq 0$ si y solamente si $\frac{v}{t^{-n}} = z^{-1} \in O_p(C)$. En consecuencia, si z no es una unidad, o bien $z \in O_p(C)$ o bien $z^{-1} \in O_p(C)$.

Ahora bien, si p es un cero de z, significa que $z \in O_p(C)$ no es una unidad, si y solamente si $z^{-1} \notin O_p(C)$, es decir, p es un polo de z^{-1}.

Proposición 60 *Sea C una curva regula. El conjunto de ceros de una función racional de C es un subconjunto algebraico proyectivo de C.*

Demostración: Es inmediato juntando los resultados de las proposiciones 30 y 59.

Definición 53 *Dada $z \in k(C)$ y p un cero de z, llamaremos* orden *de z en p, y lo denotaremos por $ord_p(z)$ al orden de z en $O_p(z)$. Si p es un polo de z, p será un cero de z^{-1} y definimos el* orden *de z en p como $ord_p(z) = -ord_p(z^{-1})$.*

Nota: La definición de orden $ord_p(z)$ anterior corresponde con el orden que se puede definir en $k(C)$ como cuerpo de fracciones de $O_p(C)$ con lo que es compatible con el producto de elementos del cuerpo.

Teorema 8 *Sea C una curva y sea A un anillo de valoración discreta con $k(C) \not\subset A$ pero $k \subset A$. Sea $L = Frac(A)$ el cuerpo de fracciones de A. Supongamos que L contiene a $k(C)$. Entonces, existe un único punto $p \in C$ tal que A domina a $O_p(C)$.*

Demostración: Denotemos por m al maximal de A. Empecemos viendo que a lo sumo existe un único punto p con $m_p \subset m$. Para ello, supongamos que existen dos puntos $p, q \in C$ distintos con $m_p \subset m$ y $m_q \subset m$. Entonces, en el lema 11 vimos que existe $f \in k(C)$ con $f \in m_p$ y con $f \notin O_q(C)$, es decir, $\frac{1}{f} \in O_q(C)$. Luego, $f \in m$, es decir, f no es una unidad en A. Entonces $ord(f) > 0$ en L y por tanto $ord(\frac{1}{f}) < 0$. Sin embargo $\frac{1}{f} \in O_q(C) \subset k(C) \subset L$ tiene orden $ord(\frac{1}{f}) \geq 0$, lo cual es absurdo.

Veamos ahora que efectivamente existe el punto p del enunciado. En virtud de la proposición 40 podemos suponer que $C \cap A_i \neq \emptyset$ cuando A_i es un carta afín de $\mathbb{P}^n$ para todo $i = 0, ..., n$. Entonces, $A_h(C) = \frac{k[X_0,...,X_n]}{I_h(C)} = k[x_0, ..., x_n]$ donde $x_i = X_i + I_h(C)$. Además, como $C \cap A_i \neq \emptyset$ tenemos que $x_i \neq 0$ para todo i.

Es claro que $\frac{x_i}{x_j} \in k(C)$, luego podemos ver el orden de estas funciones racionales dentro de L. Tomemos $N = max_{i,j}(ord(\frac{x_i}{x_j}))$. Supongamos que $N = ord(\frac{x_1}{x_0})$. Entonces, para $i = 1, ..., n$ se verifica que $ord(\frac{x_i}{x_0}) = ord(\frac{x_1}{x_0}\frac{x_i}{x_1}) = N - ord(\frac{x_i}{x_1}) \geq 0$. Por tanto, para $i = 1, ..., n$ las funciones racionales $\frac{x_i}{x_0}$ son de hecho elementos de A.

Si tomamos C_* la curva deshomogeneizada de C por la carta A_0, podemos identificar el anillo $\Gamma(C_*) = A(C_*)$ con $k[\frac{x_1}{x_0}, ..., \frac{x_n}{x_0}]$ y como $\frac{x_i}{x_0} \in A$, es inmediato que $\Gamma(C_*) \subset A$. Tiene sentido,por tanto considerar el ideal primo de $\Gamma(C_*)$ $J = \Gamma(C_*) \cap m$.

Consideremos la subvariedad $V = V(J)$ de C_*, como en la proposición 4. Si $V = C_*$ tendríamos que $J = 0$ y todo elemento no nulo de $\Gamma(C_*)$ es una unidad de A, pero entonces $k(C) \subset A$, contra hipótesis.

Tenemos, por tanto, que $V \subsetneq C_*$, por un razonamiento con las dimensiones de ambas variedades afines, deducimos que V consta de un único punto $p \in V \subset C$. Como $m_p = I(V) = I(V(J)) = J$ concluimos que $m_p \subset m$ y p es el punto que buscábamos.

Corolario 8 *Sean C una curva plana, C' una curva y $f : C' \longrightarrow C$ una aplicación racional. Entonces, f está definida en todo punto regular de C'. Además, si C' es regular, f será un morfismo.*

Demostración: en virtud de la proposición 55, $f(C')$ es denso en C o un punto. Si $f(C')$ es un punto, entonces todo morfismo que represente a f se extiende a todos los puntos regulares de C' fácilmente.

Supongamos que $f(C')$ es denso en C, entonces, $\overline{F} : k(C) \longrightarrow \overline{k(C')}$ induce una extensión de cuerpos algebraica finita como vimos en la proposición 55.

Sea $p \in C$ un punto simple y denotemos por $R = O_p(C')$ y por $L = k(C)$. Notemos que el cuerpo $L = Frac(R)$ y que $k \subset R$. Entonces, si $k(C) \subset R \subset L$, como $L : k(C)$ es algebraica finita, entonces R es un cuerpo, lo cual no es cierto. Tenemos entonces que $k(C) \not\subset R$, y el teorema 8 garantiza que existe un único punto $q \in C$ de modo que $R = O_p(C')$ domina a $O_q(C)$, y aplicando la proposición 47 concluimos que p pertenece al dominio de F.

3.2. Índice de intersección

Todas las dimensiones consideradas en esta sección son las dimensiones de cocientes vistos como k-espacios vectoriales.

Sea C una curva regular y $F \in k[X_0, X_1, X_2]$ un polinomio homogéneo. Vamos a definir para cada $p \in C$ un número $m_p(F)$ que sea nulo excepto para un número finito de puntos.

En virtud de la proposición 58 tenemos que existe C' una curva plana birracionalmente equivalente a C. Llamemos $t : C \longrightarrow C'$ a la aplicación birracional y $T : k(C') \longrightarrow k(C)$ el isomorfismo de anillos que induce t según la proposición 49. Podemos suponer que C' es una curva plana proyectiva pues si no lo es basta componer t con la inclusión $i : C' \longrightarrow C'^*$, es inmediato comprobar que $i \circ t$ será también una aplicación birracional. Como C es regular, en virtud de la proposición 8 t está definida en todo punto de C.

Supongamos que $t(p) \in C'$ tiene su primera coordenada no nula, es decir, pertenece a la carta A_0. Entonces, podemos ver $F_* \in k(C'_*) = k(C')$ deshomogeneizando con respecto a A_0, luego $T(F_*) \in k(C)$ y como C es regular, tenemos definido un orden en $O_p(C)$ que sabemos extender a los elementos de $k(C)$. Tomemos $m_p(F) = ord_p(T(F_*))$.

Comprobemos que $m_p(F)$ no depende de la carta en la que hayamos visto a $t(p)$. Si $t(p)$ perteneciera a $A_i \cap A_j$ y F_{*i} y F_{*j} son las dehomogeneizaciones de F respecto a A_i y A_j respectivamente, entonces $F_{*i} = \frac{F+I_h(C')}{X_i^d+I_h(C')}$ y $F_{*j} = \frac{F+I_h(C')}{X_j^d+I_h(C')}$ si los vemos en $k(C')$, por lo tanto, si denotamos por $a_{ij} = \frac{X_i+I_h(C')}{X_j+I_h(C')}$, se cumple que $F_{*i}a = F_{*j}$, luego $T(F_{*i})T(a) = T(F_{*j})$ y como $ord_p(T(a)) = 0$ pues a es una unidad concluimos.

El ver que $m_p(F)$ es nulo para casi todo punto de C lo veremos en la siguiente sección.

Definición 54 *Sean F, G polinomios de $k[X_1, X_2]$ y sea $p \in \mathbb{A}^2$. Se define el* índice de intersección *de F y G (o de las curvas planas que definen su anulación) en p como el número $I_p(F,G) = dim(\frac{O_p(\mathbb{A}^2)}{(F,G)})$ donde consideramos la dimensión como k-espacio vectorial cociente.*

Propiedades:

1. $I_p(F,G)$ es un entero no negativo cuando F y G se cortan en p. E $I_p(F,G) = \infty$ si F y G tienen alguna componente homogénea en común que se anule en p.

2. $I_p(F,G) = 0$ si y solamente si $p \notin F \cap G$. El número de intersección depende sólo de las componentes irreducibles de F y G que pasen por p.

3. Si T es un cambio de coordenadas en el plano afín con $T(q) = p$, entonces $I_p(F,G) = I_q(T(F), T(G))$.

4. $I_p(F,G) = I_p(G,F)$.

5. $I_p(F,G) \geq m_p(f)m_p(g)$. La igualdad se cumple si y solo si F y G no tienen tangenetes comunes en p.

6. Si $f = \pi f_i$ y $g = \pi g_i$, y F_i y G_i representan las curvas resultantes de la anulación de f_i y g_i respectivamente, entonces $I_p(F,G) = \sum_i I_p(F_i, G_i)$.

7. $I_p(F,G) = I_p(F, G + HF)$ cuando $H \in k[X_1, X_2]$.

Proposición 61 *El índice de intersección es el único número definido para todo par de curvas planas y todo punto $p \in \mathbb{A}^2$ que satisface las siete propiedades anteriores.*

Demostración: Ver [2], capítulo 3, sección 3.

Nota: el índice de intersección lo hemos definido para curvas planas afines, sin embargo, si $F, G \in k[X_0, X_1, X_2]$ son polinomios homogéneos que definen curvas planas proyectivas, entonces, podemos considerar las deshomogeneizaciones F_* y G_* en las cartas A_0, A_1, A_2 que contengan al punto $p \in \mathbb{P}^n$. Entonces, podemos ver a F y G dentro de $O_p(\mathbb{P}^2)$ si representamos a estos polinomios como $\frac{F}{X_i^{d_F}}$ y $\frac{G}{X_i^{d_G}}$ donde $X_i \neq 0$ es una carta que contiene a p y si consideramos las deshomogeneizaciones F_*, G_* en esa misma carta, entonces $\frac{O_p(\mathbb{P}^2)}{(\frac{F}{X_i^{d_F}}, \frac{G}{X_i^{d_G}})} = \frac{O_p(\mathbb{A}^2)}{(F_*, G_*)} = I_p(F_*, G_*)$ cometiendo el abuso de notación de identificar a un polinomio con su curva plana correspondiente. Como el índice de intersección solo depende del punto y de las componentes de las curvas que pasan por el punto, $I_p(F_*, G_*)$ no depende de la carta en la que veamos a F_* y G_* y por tanto podemos extender la definición de índice de intersección al caso no afín también.

Lema 16 *Sea $I \subset k[X_1, ..., X_n]$ un ideal de modo que $V(I)$ consta de un único punto. Entonces, $dim(\frac{k[X_1,...,X_n]}{I})$ es finito.*

Demostración: sea $V(I) = \{p\}$ con $p = (p_1, ..., p_n)$, entonces $Rad(I) = (X_1 - p_1, ..., X_n - p_n)$, es decir, para cada $i = 1, ..., n$ existe N_i con $(X_i - p_i)^{N_i} \in I$. Como $p_i \in k$, $(T - p_i)^{N_i}$ es un polinomio de $k[T]$ cuya clase en V se anula en X_i. Por tanto, el cociente $\frac{k[X_1,...,X_n]}{I}$ está generado como k-espacio vectorial por las potencias de X_i $X_i^0, X_i, ..., X_i^{N_i - 1}$ para todo $i = 1, ..., n$ y por tanto, la dimensión de $\frac{k[X_1,...,X_n]}{I}$ es finita.

Lema 17 *Sea C una curva plana y C' una curva regular. Sea $f : C' \longrightarrow C$ una aplicación birracional no constante entre ambas curvas y sea $G \in k[X_0, X_1, X_2]$ un polinomio homogéneo no nulo en C. Entonces, para todo $p \in C \cap V_h(G)$ existen abiertos afines $U \subset C$ y $V \subset C'$ tales que:*

1. $V_h(G) \cap U = \{p\}$.

2. *para alguna carta A_i que contiene a p, la deshomogeneización $g = G_*$ con respecto a esa carta cumple $g \in \Gamma(U)$.*

3. *si $q \in C'$ y $f(q) = p$, entonces $q \in V$.*

4. $f(V) \subset U$.

Demostración: Empecemos fijándonos en que como C' es regular, f es un morfismo definido en todo C'. Como $V_h(G) \cap C$ es un cerrado estrictamente contenido en C, ha de tener dimensión 0, es decir, es un conjunto finito. Pongamos $V_h(G) \cap C = \{p_0, p_1, ..., p_s\}$ y como $p \in V_h(G) \cap C$, supongamos $p = p_0$.

Tomemos $A = C \setminus \{p_1, ..., p_s, p_\infty\}$ con p_∞ el punto del infinito de una carta A_i que fijamos y que contenga a p. Entonces, A es una subvariedad abierta de C que contiene a p. Vimos, que entonces existe $U \subset A$ un abierto afín de A que contiene a p.

Obviamente $V_h(G) \cap U = \{p\}$, y además, como $p_\infty \notin U$, podemos ver $g \in \Gamma(U)$, luego el abierto U cumple las condiciones que pedíamos.

Consideremos ahora $B = f^{-1}(U) \subset C'$ un abierto no necesariamente afín. El conjunto $f^{-1}(q)$ es un cerrado de B contenido estrictamente en C', luego, como antes, $f^{-1}(q) = \{q_1, ..., q_r\}$. Sabemos que existe $L \in k[X_0, X_1, X_2]$ un polinomio homogéneo de grado 1 que no se anula en $\{q_1, ..., q_r\}$. Entonces, $S = \overline{C'} \setminus V_h(L)$ es un abierto afín de $\overline{C'}$, pues, razonando como en el lema 14, existe un isomorfismo ϕ de $\mathbb{P}^2$ en sí mismo que envía un punto cualquiera x al punto $(L_0(x); L_1(x); L_2(x))$ donde $L_0 = L$ y cuya restricción da un isomorfismo entre la carta A_0 y el conjunto de puntos de $\mathbb{P}^2$ que no anulan a L, y entonces $\phi(\overline{C}) \cap A_0$ es una variedad afín cuya contraimagen coincide con S.

Como C' es un abierto de $\overline{C'}$, B es un abierto de $\overline{C'}$, y existen polinomio $F_1, ..., F_t \in k[X_0, X_1, X_2]$ homogéneos con $B = \overline{C'} \setminus V_h(F_1, ..., F_t)$. También vimos que estos $F_1, ..., F_t$ generan funciones regulares $f_1, ..., f_t \in \Gamma(S)$ donde $f_i = \frac{F_i}{L^{d_i}}$. Como S es afín, S_{f_1} también lo será, y también lo será $V = (...(S_{f_1})_{f_2} ...)_{f_t}$.

Entonces, V es un abierto afín de puntos de S que no se anulan en $F_1, ..., F_s$, es decir es el abierto $V = B \cap S \subset f^{-1}(U)$, luego $f(V) \subset U$ y además, si $q \in X$ es tal que $f(q) = p$, entonces $q = q_i$ para algún $i = 1, ..., r$ y $q \in f^{-1}(U)$ pues $p \in U$, por tanto, como L no se anula en q_i para ningún i, $q \in S$ y también $q \in B$. En consecuencia, $q \in V$.

Lema 18 *Sean $W \subset V$ dos espacios vectoriales y sea $T : V \longrightarrow V$ una forma lineal inyectiva tal que $T(W) \subset W$. Supongamos que la dimensión de los cocientes $\frac{V}{W}$ y $\frac{W}{T(W)}$ es finita. Entonces, $\frac{V}{T(V)}$ y $\frac{W}{T(W)}$ tienen la misma dimensión.*

Demostración: Como $\frac{V}{W}$ y $\frac{W}{T(W)}$ tienen dimensión finita,

$$dim(\frac{V}{T(W)}) = dim(\frac{V/W}{W/T(W)}) = dim(\frac{V}{W}) - dim(\frac{W}{T(W)})$$

también es finita. Esto garantiza que todos los cocientes que vamos a considerar a continuación y que estarán contenidos en $\frac{V}{T(W)}$ tienen dimensión finita, permitiéndonos realizar las operaciones indicadas.

Definimos $T' : V \longrightarrow \frac{V}{T(W)}$ como $T'(v) = T(v) + T(W)$ otra forma lineal. Entonces, $v \in Ker(T')$ si y solo si $T(v) \subset T(W)$, y como T es inyectiva esto ocurre si y solamente si $v \in W$. Como $T(W) \subset W$, la restricción de esta biyección induce una forma lineal $T'' : \frac{V}{T(W)} \longrightarrow \frac{V}{T(W)}$ con $Ker(T'') = \frac{W}{T(W)}$.

Como T'' es una forma lineal, $dim(\frac{V}{T(W)}) = dim(Ker(T'')) + dim(Im(T'')) = dim(\frac{W}{T(W)}) + dim(\frac{T(V)}{T(W)})$ y por tanto $dim(\frac{W}{T(W)}) = dim(\frac{V}{T(W)}) - dim(\frac{T(V)}{T(W)}) = dim(\frac{\frac{V}{T(W)}}{\frac{T(V)}{T(W)}}) = dim(\frac{V}{T(V)})$.

Lema 19 *En las condiciones del lema 17 $\overline{f}: k(C) \longrightarrow k(C')$ verifica que $\overline{f}(\Gamma(U)) \subset (\Gamma(V))$ y además la dimensión como k-espacio vectorial de $\frac{\Gamma(V)}{\overline{f}(\Gamma(U))}$ es finita.*

Demostración: Como C' es regular, f es un morfismo definido en todo C' y como U y V son abiertos con $f(V) \subset U$, es evidente que la restricción $f: V \longrightarrow U$ es un morfismo, y por definición, $f(\Gamma(U)) \subset \Gamma(f^{-1}(U)) \subset \Gamma(V)$.

Como U y V son afines, existen $y_1,..,y_m \in \Gamma(U)$ con $\Gamma(U) = k[y_1,...,y_m]$ y $k(U) = k(y_1,...,y_m)$. Como el grado de trascendencia de $k(C) : k$ es 1, existe j de modo que $\{y_j\}$ es una base de trascendencia de $k(C)$ sobre k. De igual modo, existen $x_1,...,x_n \in \Gamma(V)$ de modo que $\Gamma(V) = k[x_1,...,x_n]$ y $k(V) = k(x_1,...,x_n)$.

Como f es un morfismo e $y_j \in \Gamma(U)$, $\overline{f}(y_j) \in \Gamma(V) \subset k(V)$. Si $\overline{f}(y_j)$ no fuera trascendente sobre k, existiría un polinomio $P \in k[T]$ no nulo con $P(\overline{f}(y_j)) = 0$, pero $P(\overline{f}(y_j)) = \overline{f}(P(y_j)) = 0$ y como $\overline{f}$ es una biyección entre $k(C)$ y $k(C')$, y $P(y_j) \in k(C)$, esto ocurre solo si $P(y_j) = 0$, pero entonces $P = 0$ contra hipótesis. Como $\overline{f}(y_j)$ es trascendente y el grado de trascendencia de $k(V) : k$ es 1, $\{\overline{f}(y_j)\}$ es una base de trascendencia. Por tanto, cada x_i ha de ser algebraico sobre $k(y_j)$, es decir, existirán polinomio $P_i(T) = \sum_{k=0}^{d_i} \alpha_k^i T^k$ no nulos con $\alpha_k^i \in k[\overline{f}(y_j)]$ que se anulan en x_i.

Quitando denominadores en P_i, obtenemos un polinomio $S_i(T) = \sum_{k=0}^{d_i} \beta_k^i T^k$ con $\beta_k^i \in k[\overline{f}(y_j)]$ no nulo y que se anula en x_i. Viendo $\beta_k^i \in k[T]$, tenemos que si $\beta_k^i(0) = 0$, podríamos dividir a S_i entre $\overline{f}(y_j)$ y obtendríamos otro polinomio $S_i' = \frac{S_i}{\overline{f}(y_j)}$ que también se anularía en x_i. Podemos suponer, por tanto, que algún $\beta_k^i(0) \neq 0$.

Como $x_i, \overline{f}(y_j) \in \Gamma(V)$, $S_i \in \Gamma(V)[T]$ y $S_i(x_i) \in \Gamma(V)$, y como $\overline{f}(\Gamma(U)) \subset \Gamma(V)$, $S_i(x_i) + \overline{f}(\Gamma(U))$ es un elemento de $\frac{\Gamma(V)}{\overline{f}(\Gamma(U))}$, es decir, $\beta_k^i + \overline{f}(\Gamma(U)) = 0$ en $\frac{\Gamma(V)}{\overline{f}(\Gamma(U))}$. Sin embargo, $\beta_k^i + \overline{f}(\Gamma(U)) = \beta_k^i(0)$, pues $\overline{f}(y_j) \in \overline{f}(\Gamma(U))$, es decir, $\beta_k^i + \overline{f}(\Gamma(U))$ son elementos del cuerpo k no todo ellos nulos. Por lo tanto, $S_i(x_i) + \overline{f}(\Gamma(U)) = \sum_{k=0}^{d_i} \beta_k^i x_i^k + \overline{f}(\Gamma(U)) = \sum_{k=0}^{d_i} \beta_k^i(0)(x_i^k + \overline{f}(\Gamma(U))) = 0$ donde las potencias de x_i correspondientes a los $\beta_k^i(0) \neq 0$ sí aparecen. En particular, si $x_i^{h_i}$ es la mayor potencia que aparece, $\beta_{h_i}^i$ tiene inverso en k, luego para, cada $i = 1,...,n$, tenemos un polinomio mónico de $k[T]$ cuya clase en $\overline{f}(\Gamma(U))$ se anula en x_i. Por tanto $\frac{\Gamma(V)}{\overline{f}(\Gamma(U))} = \frac{k[x_1,...,x_n]}{\overline{f}(\Gamma(U))} = k[x_1 + \overline{f}(\Gamma(U)),...,x_n + \overline{f}(\Gamma(U))]$ está finitamente generado como k-espacio vectorial por las potencias las potencias de x_i, $x_i^0,...,x_i^{h_i}$, para todo i, luego el cociente tiene dimensión finita.

Lema 20 *Sea X una variedad y U un abierto afín de X. Sea $g \in \Gamma(U)$ una función regular tal que el conjunto de puntos de U que se anulan en g es el conjunto $\{p_1,...,p_s\}$, un conjunto finito. Entonces, $\sum_{i=1}^s dim(\frac{O_{p_i(X)}}{(g)O_{p_i(X)}}) = dim(\frac{\Gamma(U)}{(g)\Gamma(U)})$.*

Demostración Como U es afín, $\Gamma(U) = \frac{k[X_1,...,X_n]}{I}$ apara algún ideal I, y como $g \in \Gamma(U)$, existirá $P \in k[X_1,...,X_n]$ con $g = P + I$. Entonces, $\frac{\Gamma(U)}{(g)\Gamma(U)} = \frac{k[X_1,...,X_n]}{(P,I)}$ y como los ceros de g en U son los ceros de (P,I), vimos en la proposición 34 que $\frac{k[X_1,...,X_n]}{(P,I)} = \Pi_{i=1}^s \frac{O_{p_i}(\mathbb{A}^n)}{(P,I)O_{p_i}(\mathbb{A}^n)}$ y como en virtud de la proposición 35 $\frac{O_{p_i}}{(P,I)O_{p_i}(\mathbb{A}^n)} = \frac{O_{p_i}(U)}{(g)O_{p_i}(U)}$, concluimos que

$$dim(\frac{\Gamma(U)}{(g)\Gamma(U)}) = dim(\frac{k[X_1,...,X_n]}{(P,I)}) = \sum_{i=1}^s dim(\frac{O_{p_i}(\mathbb{A}^n)}{(P,I)O_{p_i}(\mathbb{A}^n)}) = \sum_{i=1}^s dim(\frac{O_{p_i}(\mathbb{A}^n)}{(g)O_{p_i}(U)}).$$

Lema 21 *En las condiciones del lema 17, $I_p(V(G),C) = dim(\frac{\Gamma(V)}{(\overline{f}(g))\Gamma(V)})$*

Demostración: Empecemos viendo que $\frac{\overline{f}(\Gamma(U))}{\overline{f}(g)\overline{f}(\Gamma(U))}$ tiene dimensión finita como k-espacio vectorial: como f es birracional, $Im(f)$ es denso en C, luego $\overline{f}$ es un inyectiva y con ello un isomorfismo en la imagen. Por tanto, $dim(\frac{\overline{f}(\Gamma(U))}{\overline{f}(g)\overline{f}(\Gamma(U))}) = dim(\frac{\Gamma(U)}{(g)\Gamma(U)}) = \frac{k[X_1,...,X_n]}{(P,I)}$ donde I es el ideal de la variedad afín contenida en $\mathbb{A}^n$ a la que es isomorfa U y P es un polinomio de $k[X_1,...,X_n]$ cuya clase en $\Gamma(U)$ es g. Ahora bien, los ceros del ideal (P,I) son los ceros de g en U, es decir, únicamente el punto p, y por tanto, $dim(\frac{\overline{f}(\Gamma(U))}{\overline{f}(g)\overline{f}(\Gamma(U))}) = dim(\frac{k[X_1,...,X_n]}{(P,I)})$ es finito.

Llamemos ahora $W' = \overline{f}(\Gamma(U))$, $V' = \Gamma(V)$ y $T : V' \longrightarrow V'$ a la forma lineal inyectiva dada por $T(a) = \overline{f}(g)a$. Entonces, acabamos de ver que $\frac{W'}{T(W')}$ tiene dimensión finita y en el lema 19 vimos que $\frac{V'}{W'}$ también tiene dimensión finita. Por lo tanto, podemos aplicar el lema 18 y concluimos que $dim(\frac{\Gamma(V)}{(\overline{f}(g))\Gamma(V)}) = dim(\frac{V'}{T(V')}) = dim(\frac{W'}{T(W')}) = dim(\frac{\overline{f}(\Gamma(U))}{(\overline{f}(g))\overline{f}(\Gamma(U))})$. Y como $\overline{f}$ es un isomorfismo en la imagen, $dim(\frac{\Gamma(V)}{(\overline{f}(g))\Gamma(V)}) = dim(\frac{\Gamma(U)}{(g)\Gamma(U)})$, pero en el lema 20 vimos que $\frac{\Gamma(U)}{(g)\Gamma(U)}$ y $\frac{O_p(U)}{(g)O_p(U)}$ tienen la misma dimensión, puesto que p es el único punto de U en el que g se anula, y en la proposición 35 vimos que $\frac{O_p(U)}{(g)O_p(U)} = \frac{O_p(C)}{(g)O_p(C)} = \frac{O_p(C_*)}{(g)O_p(C_*)}$ es isomorfo a $\frac{O_p(\mathbb{A})}{(G_*,H_*)}$ donde H es el polinomio homogéneo de $k[X_0,X_1,X_2]$ que define a la curva plana C, luego sus dimensiones coinciden también, pero, por definición, la dimensión de este último espacio vectorial es el número $I_p(V_h(G),C)$.

Lema 22 *En las condiciones del lema 17, se cumple* $dim(\frac{\Gamma(V)}{\overline{f}(g)\Gamma(V)}) = \sum_{q\in f^{-1}(p)} dim(\frac{O_q(C')}{\overline{f}(g)O_q(C')})$ *y además* $dim(\frac{O_q(C')}{\overline{f}(g)O_q(C')}) = ord_q(\overline{f}(g))$.

Demostración: Como V es afín, $\Gamma(V) = \frac{k[X_1,...,X_n]}{I}$ apara algún ideal I. Como $g \in \Gamma(U)$ y f es un morfismo por ser C regular, $f(g) \in \Gamma(V)$, luego existirá $P \in k[X_1,...,X_n]$ con $\overline{f}(g) = P + I$.

Tenemos que $\frac{\Gamma(V)}{(\overline{f}(g))\Gamma(V)} = \frac{k[X_1,...,X_n]}{(P,I)}$ y como $\overline{f}(g) \neq 0$ por ser $\overline{f}$ inyectiva y $g \neq 0$ en V, el conjunto de puntos de C' que son ceros de $\overline{f}(g)$ es un cerrado de C', luego tiene dimensión 0, es decir, es un conjunto finito. Supongamos que estos puntos son los $p_1,...,p_t$. Por lo tanto, aplicando la proposición 34, $\frac{k[X_1,...,X_n]}{(P,I)} = \Pi_{i=1}^t \frac{O_{p_i}(\mathbb{A}^n)}{(P,I)O_{p_i}(\mathbb{A}^n)}$.

Por otra parte, $\frac{O_{p_i}(\mathbb{A}^2)}{(P,I)O_{p_i}(\mathbb{A}^2)} = \frac{\frac{O_{p_i}(\mathbb{A}^2)}{IO_{p_i}(\mathbb{A}^2)}}{(\overline{f}(g))O_{p_i}(C')} = \frac{O_{p_i}(C')}{(\overline{f}(g))O_{p_i}(C')}$ en virtud de la proposición 35, y por tanto $\frac{\Gamma(V)}{(\overline{f}(g))\Gamma(V)} = \Pi_{i=1}^t \frac{O_{p_i}(C')}{(\overline{f}(g))O_{p_i}(C')} = \Pi_{q\in f^{-1}(p)} \frac{O_q(C')}{(\overline{f}(g))O_q(C')}$, pues el único punto de U en el que se anula g es p y $\overline{f}(q) = 0$ si y silamente $g(f(q)) = 0$, es decir si y solamente si $f(q) = p$.

Además, como $\overline{f}(g) \subset \Gamma(V) \subset O_p(C)$, $ord_q(\overline{f}(g)) = dim(\frac{O_q(C')}{\overline{f}(g)O_q(C')})$ en virtud de la proposición 75 tomando $A = O_q(C')$ y $a = \overline{f}(g)$.

Proposición 62 *Sea C una curva plana birracionalmente equivalente a una curva proyectiva irreducible C' y $p \in \mathbb{P}^2$ un punto cualquiera. Representaremos por f a la aplicación birracional y denotaremos por H al polinomio que define C'. Sea $V_h(G)$ una curva plana que viene dada por la anulación de un polinomio no nulo $G \in k[X_0,X_1,X_2]$. Entonces,* $I_p(C',V_h(G)) = \sum_{q\in f^{-1}(p)} ord_q(\overline{f}(G_*))$ *donde G_* es la deshomogeneización de G en una carta que contenga a p.*

Demostraicón: si $p \notin V_h(G)\cap C$, sabemos que $I_p(V_h(G),C) = 0$. Por otra parte, si $p \notin C$ el conjunto de puntos $q \in C'$ con $f(q) = p$ es el vacío, pues $Im(f) \subset C$, con lo que $\sum_{q\in f^{-1}(p)} ord_q(\overline{f}(G_*)) = 0$ también, y si $p \notin V_h(G)$ pero sí en C, entonces $\overline{f}(G_*)(q) \neq p$ para todo $q \in C'$ con $f(q) = p$, luego $ord_q(\overline{f}(G_*)) = 0$ para todo q.

Si $p \in V_h(G) \cap C$, tomamos U, V como en el lema 17 y entonces, $\sum_{q \in f^{-1}(p)} ord_q(\overline{f}(g)) = dim(\frac{\Gamma(V)}{(\overline{f}(g))\Gamma(V)})$ en virtud del lema 22, pero esto es igual a $I_p(V_h(G), C)$ en virtud del lema 21.

Teorema 9 (de Bezout) *Sean $f, g \in k[X_0, X_1, X_2]$ polinomios homogéneos que definen curvas planas F y G, respectivamente. Entonces, si f y g no tienen componentes homogéneas comunes, $\sum_{p \in F \cap G} I_p(F, G)$ coincide con el producto de los grados de f y g.*

Demostración: Ver [2], capítulo 5, sección 3.

3.3. Divisores

En esta sección trabajaremos con C una curva regular.

Definición 55 *Un* 0-ciclo *es una suma formal de puntos $p \in \mathbb{P}^n$, $\sum_{p \in \mathbb{P}^n} n_p p$, donde $n_p \in \mathbb{P}^n$ y es no nulo solo para un conjunto finito de puntos.*

Definición 56 *El* grado de un 0-ciclo $D = \sum_{p \in \mathbb{P}^n} n_p p$ *es el número $gr(D) = \sum n_p$.*

Proposición 63 *La relación $\sum_{p \in \mathbb{P}^n} n_p p \geq \sum_{p \in \mathbb{P}^n} m_p p$ si y solo si $n_p \geq m_p$ para todo $p \in \mathbb{P}^n$ es una relación de orden en el conjunto de 0-ciclos.*

Definición 57 *Un 0-cilco $\sum_{p \in \mathbb{P}^n} n_p p$ se dice que es* efectivo *o* positivo *si $n_p \geq 0$ para todo $p \in \mathbb{P}^n$.*

Definición 58 *Llamamos* divisor *de C a un 0-ciclo $\sum_{p \in \mathbb{P}^n} n_p p$ tal que $p \in C$.*

Nota: Al conjunto de divisores de una curva C lo denotaremos por $Div(C)$.

En la proposición 30 vimos que los ceros y polos de una función racional $z \in k(C)$ es un subconjunto algebraico proyectivo de C, pero como C es de dimensión 1, los conjuntos de ceros y de polos han de ser de dimensión 0, es decir, finitos en virtud de la proposición 53. Por tanto, si $z \in k(C)$ solo habrá un número finito de puntos p de C de modo que $ord_p(z) \neq 0$. Esta afirmación justifica la validez de la siguiente definición:

Definición 59 *Sea $z \in k(C)$ una función racional. Definiremos el divisor de z, $div(z)$ como el 0-ciclo $\sum_{p \in C} n_p p$ donde n_p es el orden de z en p, $ord_p(z)$.*

El número $m_p(F)$ definido en la sección anterior es nulo para todos los puntos $p \in C$ salvo para un número finito pues los puntos de C' que son ceros o polos de $T(F)$ ya comentamos antes que es un conjunto finito puesto que $T(F) \in k(C)$.

Definición 60 *Sea $F \in k[X_0, X_1, X_2]$ un polinomio homogéneo. Definimos el divisor de F de C a través de la aplicación birracional $t : C \longrightarrow C'$ donde C' es una curva plana y al que representaremos por $div_t F$ como el 0-ciclo $div_t(F) = \sum_{p \in C} m_p(F) p$.*

Proposición 64 *Sea $F \in k[X_0, X_1, X_1]$ un polinomio homogéneo, denotaremos también por F a la curva plana que define, $t : C \longrightarrow C'$ una aplicación birracional y C' una curva plana que viene dada por la anulación de un polinomio $H \in k[X_0, X_1, X_2]$. Entonces, el divisor de un polinomio tiene grado $gr(H)gr(F)$.*

Demostración: El grado del divisor $div_t(F) = \sum_{p \in C} m_p(F)$ es el número $\sum_{p \in C} m_p(F)$ y, en virtud de la proposición 62 $\sum_{p \in C} m_p(F) = \sum_{q \in C'} I_q(C', F)$ y aplicando el teorema de Bezout, concluimos lo deseado.

Definición 61 *Diremos que un 0-ciclo es un* divisor principal *de la curva C si es divisor de alguna función racional de C.*

Proposición 65 *Sea $z \in k(C)$, entonces $div(z)$ es un divisor de grado 0.*

Demostración: en virtud de la proposición 58, existe $t : C \longrightarrow C'$ una aplicación birracional y C' una curva plana que viene dada por un polinomio $H \in k[X_0, X_1, X_2]$. Sea $T : k(C') \longrightarrow k(C)$ el isomorfismo que t induce. Entonces, existirán polinomios $F, G \in k[X_0, X_1, X_2]$ del mismo grado con $\frac{F+I_h(\overline{C'})}{G+I_h(\overline{C'})} \in k(C')$ y $z = T(\frac{F+I_h(C')}{G+I_h(C')})$. Como $z = T(F + I(\overline{C'}))T^{-1}(G + I(\overline{C'}))$, el orden de z en p es $ord_p(z) = m_p(F) - m_p(G)$, luego el grado del divisor de z será

$$\sum_{p \in C} ord_p(z) = \sum_{p \in C} (m_p(F) - m_p(G)) = gr(F)gr(H) - gr(G)gr(H)$$

en virtud de la proposición 64, y como $gr(F) = gr(G)$ concluimos lo deseado.

Proposición 66 *Sea $z \in k(C)$ no nulo. Entonces, los siguiente enunciados son equivalentes:*

(1) $div(z) \geq 0$.

(2) $z \in k$.

(3) $div(z) = 0$.

Demostración: Si $div(z) \geq 0$, entonces $z \in O_p(C)$ para todo $p \in C$ y como vimos en la proposición 32, $\cap O_p(C) = k$, luego $z \in k$ como queríamos.

Ver que (2) implica (3) y que (3) implica (1) es inmediato.

Definición 62 *Dados $D, D' \in Div(C)$, diremos que son* linealmente equivalentes *y lo denotaremos por $D \equiv D'$ si existe una función racional $z \in k(C)$ tal que $D = D + div(z)$.*

Proposición 67 *Sean $D, D', D_1, D_2 \in Div(C)$. Entonces:*

(1) La relación $\equiv$ definida antes es una relación de equivalencia.

(2) $D \equiv 0$ si y sólo si D es un divisor principal de C.

(3) Si $D \equiv D'$ entonces $gr(D) = gr(D')$

(4) Si $D \equiv D'$ y $D_1 \equiv D_2$, entonces $D + D_1 \equiv D' + D_2$.

(5) $D \equiv D'$ si y solamente si existen dos polinomios homogéneos de mismo grado F y F' tales que $D + div(F) = D' + div(F')$.

Demostración: Del 1 al 4 son inmediatas.

(5) Basta tener en cuenta que $\frac{F}{F'} \in k(C)$ y que toda función racional de $k(C)$ se puede expresar como una fracción de polinomios homogéneos del mismo grado.

Definición 63 *Sea $D \in Div(C)$. Denotamos por $L(D)$ al conjunto $\{0\} \cup \{z \in k(C) : div(z) + D \geq 0\}$.*

Proposición 68 *Sean $U \subset V \subset W$ tres espacios vectoriales sobre el mismo cuerpo. Entonces, si $dim(\frac{W}{U})$ es finita se verifica que $dim(\frac{W}{U}) = dim(\frac{W}{V}) + dim(\frac{V}{U})$.*

Demostraicón: Este es un resultado general de álgebra lineal.

Proposición 69 *Sean $D, D' \in Div(C)$:*

(1) $L(D)$ es un espacio vectorial. Denotaremos por $l(D)$ a su dimensión,

(2) Si $D < D'$, entonces $L(D) \subset L(D')$ y $dim(\frac{L(D')}{L(D)}) \leq gr(D'-D)$.

(3) $L(0) = k$ y, si $gr(D) < 0$, $L(D) = 0$.

(4) $L(D)$ es un espacio vectorial de dimensión finita. Además, si $gr(D) \geq 0$, $l(D) \leq gr(D)+1$.

(5) Si $D \equiv D'$, entonces $l(D) = l(D')$.

Demostración: (1) Para ver que $L(D)$ es un espacio vectorial basta con darse cuenta de que si $z, z' \in k(C)$, entonces $div(z+z') = div(z) + div(z')$ y que si $\lambda \in k$, $div(\lambda z) = div(z)$.

(2) Ver que si $D < D'$ $L(D) \subset L(D')$ es inmediato.

Veamos ahora que $dim(\frac{L(D')}{L(D)}) \leq gr(D'-D)$: como $D < D'$, podemos escribir $D' = D+p_1+...+p_s$, donde $p_i \in C$. Además, $L(D) \subset L(D+p_1) \subset ... \subset L(D+p_1+...+p_s)$, luego en virtud de la proposicion 68 es suficiente probar que $dim_k(L(D+p)/L(D)) \leq 1$ para cualquier $p \in C$.

Sea t un parámetro de uniformización de $O_p(C)$, y sea n_P el coeficiente de P en D. Definimos $\phi : L(D+p) \to k$ por $\phi(f) = (t^{n_p+1}f)(p)$; como t no es una unidad, necesariamente $t(p) = 0$, es decir, $ord_p(t) > 0$ y como $ord_p(f) \geq -n_P - 1$, tenemos que

$$ord_p(\phi(f)) = ord(t^{n_p+1}f) = (n_p+1)ord_p(t) + ord_p(f) \geq n_p + 1 + ord_p(f) \geq 0$$

, luego tiene sentido hablar de la evaluación de $t^{n_p+1}f$ en p, y con ello, ϕ está bien definida. Veamos que ϕ es una aplicación lineal con $Ker(\phi) = L(D)$: sean $f, g \in L(D+p)$ y sean $a, b \in k$, entonces $\phi(af+bg) = (t^{n_p+1}(af+bg))(p) = a(t^{n_p+1}f)(p) + b(t^{n_p+1}g)(p) = a\phi(f) + b\phi(g)$, luego es lineal. Sea ahora $h \in L(D)$, entonces $ord_p(h) + n_p > 0$, y como $ord(t) > 0$ tenemos que $ord(t^{n_p+1}h) = (n_p+1)ord_p(t) + ord_p(h) \geq n_p + 1 + ord_p(f) > 1$, con lo que $\phi(p)$ se ha de anular en p, de donde deducimos que $L(D) \subset Ker(\phi)$.

Para ver que $Ker(\phi) \subset L(D)$ basta ver que si $z \in Ker(\phi)$, el orden de z, $ord_q(z) + n_q \geq 0$ para todo punto $q \in C$ y con n_q el coeficiente de q en D. Si $q \in C$ es distinto de p comprobar lo anterior es inmediato. Para p, sabemos que $(t^{n_p+1}z)(p) = 0$, es decir, el orden de $t^{n_p+1}z$ en p cumple $ord_p(t^{n_p+1}z) = ord_p(t^{n_p+1}) + ord_p(z) = (n_p+1)ord_p(t) + ord_p(z) > 0$. Ahora bien, $t \in M_p(C)$,el maximal de $O_p(C)$, luego $t(p) = 0$, y por tanto $ord_p(t) > 0$, con lo que $ord_p(z) + n_p > -1$ como queríamos.

Por lo tanto ϕ induce una aplicación inyectiva $\phi' : \frac{L(D+p)}{L(D)} \to k$ de lo que es inmediato que $dim_k(\frac{L(D+p)}{L(D)}) \leq 1$.

(3) Usando la proposición 66 es evidente que $L(0) = k$.

Sea ahora D un divisor de grado negativo. Si $z \in L(D)$, es una función racional no nula, entonces $gr(div(z)+D) = gr(div(z)) + gr(D) = gr(D) \geq 0$, contra hipótesis.

(4) Sea $n = gr(D)$. En virtud del apartado 3 podemos suponer que $n \geq 0$. Sea $p \in C$ un punto cualquiera, denotaremos por $D' = D - (n+1)p$. $gr(D') = gr(D) - (n-1) = -1 > 0$, luego $L(D') = 0$ tal y como vimos en el apartado 3. Entonces, aplicando el apartado 2,

$$l(D) = dim(\frac{L(D)}{L(D')}) \leq gr(D-D') = gr((n+1)p) = n+1 = gr(D)+1.$$

(5) Si $D \equiv D'$, entonces $D = D' + div(w)$ para alguna función racional $w \in k(C)$. Definimos la aplicación $\phi : L(D') \longrightarrow L(D)$ dada por $\phi(z) = zw$ para todo $z \in L(D')$. ϕ está bien definida, pues si $z \in L(D')$, entonces $div(z) + div(w) + D \geq 0$. Si vemos que ϕ es una biyección, tendremos que $l(D) = l(D')$. ϕ es lineal, pues si x, z son dos funciones racionales de $L(D)$ y $a, b \in k$ constantes,

tenemos que $\phi(ax+bz) = w(ax+bz) = a(wx)+b(wz) = a\phi(x)+b\phi(z)$, luego es una aplicación lineal, además si $\phi(x) = \phi(z)$, como $k(C)$ es un cuerpo, $wx = wz$ implica que $x = z$. Sólo falta ver que ϕ es sobreyectiva, para eso basta fijarse en que w tiene inversa y que si $y \in L(D')$, $w^{-1}y \in L(D)$ y que $\phi(w^{-1}y)) = y$.

Proposición 70 *Sean D y D' dos divisores de una misma curva tales que $D \leq D'$, entonces, tenemos que $l(D') \leq l(D) + gr(D' - D)$.*

Demostración: $l(D') = l(D') - l(D) + l(D) = dim(\frac{L(D')}{L(D)}) + l(D) \leq gr(D' - D) + l(D)$ como hemos visto en el segundo apartado de la proposición 69.

Lema 23 *Sea $S \subset C$ un subconjunto, y $D = \sum_{p\in C} n_p p$ y D' dos divisores de C con $D \leq D'$. Si denotamos por $D_S = \sum_{p\in S} n_p p$ y a $L_S(D) = \{z \in L(D) : div(z)_S + D_S \geq 0\}$, entonces $L_S(D) \subset L_S(D')$ y si S es finito, entonces $dim(\frac{L_S(D')}{L_S(D)}) = gr(D'_S - D_S)$.*

Demostración: Ver que $L_S(D) \subset L_S(D')$ es inmediato.

Para ver que $dim(\frac{L_S(D)}{L_S(D')}) = gr(D'_S - D_S)$ fijémonos primero en que $L_S(D) = L(D_S)$ y, por tanto se verifica que $dim(\frac{L_S(D)}{L_S(D')}) \leq gr(D'_S - D_S)$ en virtud del apartado 2 de la proposición 69. Para ver que se tiene la igualdad razonaremos exactamente igual que en la demostración de esa proposición. Supondremos que $D' = D + p$, Fijémonos en que si $p \notin S$ entonces $D_S = D'_S$, y consideraremos la aplicación $\phi : L(D_S + p) \longrightarrow k$ dada por $\phi(f) = (t^{n_p+1}f)(p)$.

Para ver que tenemos la igualdad, necesitamos que $Ker(\phi) = L(D_S) \neq L(D_S + p)$, pues entonces necesariamente $\frac{L_S(D')}{L_S(D)} \neq 0$, y su dimensión habrá de ser no nula, como queríamos. Si $p \notin S$ sí que ocurre que $L(D_S) = L(D'_S)$, pero también $gr(D'_S - D_S) = 0$, con lo que supondremos $p \in S$.

Para ver que $Ker(\phi) \neq L(D_S + p)$ necesitamos encontrar un elemento $f \in L(D_S + p)$ con $\phi(f) \neq 0$, es decir un elemento $f \in k(C)$ con $ord_p(f) + n_p + 1 = 0$ y $ord_q(f) + n_q \geq 0$ para todo $q \in S$, $q \neq p$ de esta forma $f \in L(D_S + p)$ y $t^{n_p+1}f$ no se puede anular en p pues tiene orden 0, ya que $ord_p(t) = 1$ Como S es finito, para cada $q \in S$, en virtud del lema 5 podemos encontrar un polinomio homogéneo de grado 1, L_q que se anule en q, pero no en ningún otro punto de S, y otro polinomio homogéneo de grado 1, L, que no se anule en S. Consideraremos $f = \frac{L_p \prod_{q\in S} L_q^{n_q}}{L^{1+\sum_{q\in S} n_q}}$. Puesto que L no se anula en $S \subset C$, L tampoco se anula en C, y como tanto el numerado como el denominador tienen el mismo grado, f es el elemento de $k(C)$ que buscábamos.

3.4. El teorema de Riemann

Lema 24 *Sea $z \in k(C)$, $z \notin k$. Sea $z_0 \geq 0$ el divisor de ceros de z y n el grado de la extensión de cuerpos $[k(C) : k(z)]$. Entonces:*

(1) existe una constante τ tal que $l(Rz_0) \geq Rn - \tau$ para todo R entero no negativo.

(2) z_0 es un divisore efectivo de grado n.

Demostración:

(1) Sea $S = \{p \in C : n_p > 0\}$ donde $z_0 = \sum_{p\in C} n_p p$. Como vimos en la proposición 54 $k(C)$ es algebraico sobre $k(z)$, luego, en virtud de la proposición 82, podemos tomar una base $v_1, ..., v_m$ de $k(C)$ como $k(z)$-espacio vectorial formada por elementos enteros sobre $k(z)$, es decir, verifican $v_i^{m_i} + a_i^{m_i-1} v_i^{m_i-1} + ... + a_i^0 = 0$ para ciertos $a_i^j \in k[z^{-1}]$.

Si $p \notin S$, entonces $ord_p(a_i^j) \geq 0$, pues $a_i^j = P_i^j(z^{-1})$ con $P_i^j \in k[X]$ y $ord_p(z^{-1}) = -ord_p(z) \geq 0$. Si además $ord_p(v_i)$ es negativo, tendremos que $ord_p(v_i^{m_i}) = m_i ord_p(v_i)$ y también que

$$ord_p(a_i^j v_i^{m_i-j}) = ord_p(a_i^j) + (m_i - j) ord_p(v_i)$$

y restando la primera expresión a la segunda obtenemos que

$$ord_p(v_i^{m_i}) - ord_p(a_i^j v_i^{m_i-j}) = j ord_p(v_i) - ord_p(a_i^j) < 0,$$

lo cual es imposible en virtud de la proposición 74, viendo $k(C)$ como el cuerpo de fracciones de $O_p(C)$. En consecuencia $ord_p(v_i) \geq 0$ para todo punto $p \in S$. Además, existe un entero $t > 0$ tal que $div(v_i) + tz_0 \geq 0$ para todo $i = 1, ..., n$, pues si $p \notin S$ $ord_p(v_i) \geq 0$ y $ord_p(z_0) \geq 0$ con lo que cualquier t valdría y si $p \in S$, como S es finito pues el número de puntos tal que $n_p \neq 0$ es finito, podemos tomar t lo suficientemente grande como para que $ord_p(v_i) + tn_p$ para todo $p \in S$ y todo $i = 1, ..., n$.

Veamos ahora que $v_i z^{-j}$ son elementos linealmente independientes sobre el k-espacio vectorial $L((R+t)z_0)$ para todo entero no negativo $R \geq j$. Empecemos viendo que $v_i z^{-j} \in L((R+t)z_0)$. Hay que ver que $ord_p(v_i) - j ord_p(z) + (R+t)n_p > 0$, lo cual es cierto, pues si $p \in S$, $ord_p(z) = n_p$ y $(R-j)n_p > 0$, y si $p \notin S$, $ord_p(z) \leq 0$, con lo que $-j ord_p(z) > 0$. Para ver que son linealmente consideremos $\sum_{i,j} b_i^j v_i z^{-j} = 0$ una combinación lineal nula de los elementos $v_i z^{-j}$, esta expresión también la podemos escribir como $\sum_i P_i(z^{-1} v_i)$ donde $P_i = \sum_j b_i^j X^j \in k[X]$, y como los v_i son linealmente independientes sobre $k[z^{-1}]$, necesariamente $P_i(z^{-1}) = 0$ para todo i. Sin embargo, z^{-j} $j = 0, ..., R$ son linealmente independientes sobre k, pues de no serlo, $P_i(z^{-1}) = 0 \in k$, demuestra que z^-1 es algebraico sobre k, pero como k es algebraicamente cerrado y $z \notin k$ esto no es posible, con lo que, necesariamente, $b_i^j = 0$, tal y como queríamos.

Como existen $n(R+1)$ elementos linealmente independientes en $L((R+t)z_0)$, ha de cumplirse $l((R+t)z_0) \geq n(R+1)$. Obviamente $(R+t)z_0 > Rz_0$, luego

$$l((R+t)z_0) \leq l(Rz_0) + gr(tz_0) = l(Rz_0) + t gr(z_0),$$

es decir, $l(Rz_0) \geq l((R+t)z_0) - t gr(z_0) \geq n(R+1) - t gr(z_0) = Rn - \tau$, tomando $\tau = n - t gr(z_0)$, como queríamos.

(2) Sea $m = gr(z_0)$ y $S = \{p \in C : n_p > 0\}$. En virtud de la proposición 23, podemos tomar $w_1, ..., w_m \in L_S(0)$ tales que $\overline{w_1}, ..., \overline{w_m} \in \frac{L_S(0)}{L_S(-z_0)}$ sean una base. Veamos que $w_1, ..., w_m$ son elementos de $k(C)$ linealmente independientes sobre $k(z)$. Si no lo fueran, existirían elementos no nulos $f_1, ..., f_s \in k(z)$ tales que $\sum f_i w_i = 0$. Quitando denominadores, podemos suponer que para todo i, $f_i \in k[z]$ y podemos suponer que si $f_i = \sum_{j=0}^{d_i} f_j^i z^j$, para algún i se cumple que $f_0^i \neq 0$, pues si no $\sum f_i w_i = z \sum f_i' w_i = 0$ y trabajaríamos con los f_i' en vez de con los f_i. Escribiremos $f_i = zh_i + f_0^i$ donde $h_i = \sum_{j=1}^{d_i} f_j^i z^{j-1}$. Entonces $\sum w_i f_0^i = -z \sum w_i h_i \in L_S(-z_0)$, pues si $p \in S$, $ord_0(-z_0) = -n_p$, $ord_p(-z) = n_p$, $ord_p(w_i) \geq 0$ por ser elementos de $L_S(0)$, $ord_p(f_j^i z^j) = jn_p \geq 0$ y $ord_p(\sum w_i h_i) \geq ord_p(w_i h_i) \geq ord_p(w_i f_j^i z^j) \geq 0$ par todo par de i, j. Pero, entonces, $\sum f_0^i \overline{w_i} = 0$ aunque no todos los $f_0^i = 0$, lo cual es absurdo.

Como hemos visto que existen m elementos de $k(C)$ linealmente independientes sobre $k(z)$, tenemos que $m \leq n$.

Por otra parte, en el apartado anterior hemos visto que $l(Rz_0) \geq Rn - \tau$ para todo R positivo. Pero también se cumple $l(Rz_0) \leq gr(Rz_0) + 1 = Rm + 1$ en virtud de la proposición 69 apartado 4, y por tanto $m \geq n - \frac{\tau+1}{R}$ para todo $R > 0$, con lo que, tomando un R lo suficientemente grande, concluimos que $m \geq n$.

Teorema 10 *Dada una curva regular C, existe un entero no negativo g tal que $l(D) \geq gr(D) + 1 - g$ para todos los divisores D de C.*

Demostraicón: Denotaremos por $G(D) = gr(D) + 1 - l(D)$. Queremos encontrar una constante g tal que $G(D) \leq g$ para todo divisor D.

En virtud de la proposición 70, si $D \leq D'$, entonces $G(D) \leq G(D')$. Sea $z \in k(C)$, $z \notin k$, y sea τ la menor de las constantes que se mencionan en el lema 24. En virtud de ese mismo lema, se tiene que $G(Rz_0) = gr(Rz_0) + 1 - l(Rz_0) \leq gr(Rz_0) + 1 + \tau - Rn = \tau + 1$, donde $n = [k(C) : k(z)]$.

Como $Rz_0 \leq (R+1)z_0$, $G(Rz_0) \leq G((R+1)z_0)$ y como $G(D)$ es un número entero y τ es el menor entero tal que $G(Rz_0) \leq \tau + 1$, se verifica que para un R lo suficientemente grande $G(Rz_0) = \tau + 1$.

Sea $g = \tau + 1$. g es un número entero y como $G(0) = 0$, $g \geq 0$. En virtud de las proposiciones 67 y 69 se verifica que si $D \equiv D'$, entonces $G(D) = G(D')$.

Veamos ahora que para todo divisor D existe otro divisor D' tal que $D \equiv D'$ y $D' \leq Rz_0$ para algún entero $R \geq 0$: Si $z_0 = \sum n_p p$ y $D = \sum m_p p$, necesitamos una función racional $w \in k(C)$ tal que $m_p - ord_p(w) \leq Rn_p$ para algún R y para todo p. Sea $T = \{p \in C : m_p > 0\ ord(z^{-}1) \leq 0$ y definamos $w = \prod_{p \in T}(z^{-1} - z(p))^{m_p}$. w está bien definido y además $w \in k(C)$ pues $z^{-1} - z(p) \in k(C)$ para todo $p \in T$. Además, si $ord_p(w) \geq 0$, entonces $m_p - ord_p(w) \geq 0 \geq n_p$, y si $ord_p(w) < 0$ entonces $n_p > 0$ y para algún r se verificará la desigualdad anterior. Como el conjunto de $p \in C$ tal que $ord_p(w) > 0$ es un conjunto finito, podemos tomar R como el mayor de los r anteriores y concluimos.

Definición 64 *A la menor de las constantes g mencionadas en el teorema de Riemann se la llama el* género *de la curva C.*

Apéndice A: Anillos, módulos y dependencia entera

Anillos e ideales

En este apéndice nos referiremos siempre a anillos conmutativos y unitarios.

Definición 65 *Sea A un anillo e I, J dos ideales de A. Diremos que I y J son* ideales comaximales *si $I + J = A$.*

Proposición 71 *Sean I y J dos ideales comaximales de un anillo A. Entonces:*

(1) para todo n, m enteros, I^n y J^m son comaximales.

(2) Si $I_1, \ldots, I_m \subset A$ son ideales con I_i y $\cap_{j\neq i} I_j$ comaximales para todo i. Entonces

$$I_1^d \cap \ldots \cap I_m^d = (I_1 \ldots I_m)^d = (I_1 \cap \ldots \cap I_m)^d$$

para todo entero positivo d.

Demostración: (1) Empecemos viendo que I y J^m son comaximales. Podemos escribir $1 = x + y$ con $x \in I$ e $y \in J$, entonces $1 = 1^m = (x+y)^m = \sum_{k=0}^m a_k x^k y^{m-k}$. Entonces,$x^k y^{m-k} \in I$ para todo $k > 0$ e $y^m \in J^m$, luego $1 = x' + y'$ donde $x' \in I$ e $y' \in J^m$. Sea $a \in A$ un elemento cualquiera. Podemos escribir $a = a1 = a(x' + y') = ax' + ay'$ donde $ax' \in I$ y $ay' \in J^m$, luego I y J^m son comaximales.

Por último, para ver que que I^n y J^m son comaximales, llamamos $J' = J^m$. Hemos visto que J' e I son comaximales, luego repitiendo el razonamiento anterior es inmediato que I^n y $J' = J^m$ también lo son.

(2) Veamos que $(I_1 \cap \ldots \cap I_m)^d \subset I_1^d \cap \ldots \cap I_m^d$. Sea $x \in (I_1 \cap \ldots \cap I_m)^d$, entonces, podemos suponer $x = x_1 \ldots x_d$ donde $x_j \in I_1 \cap \ldots \cap I_m$. Entonces, $x_j \in I_i$ para todo j y todo i, luego $x \in I_i^d$ para todo i, y concluimos.

Veamos ahora que $(I_1 \ldots I_m)^d \subset (I_1 \cap \ldots \cap I_m)^d$. Sea $x \in (I_1 \ldots I_m)^d$. Entonces, podemos suponer que $x = x_1 \ldots x_d$ donde $x_i \in I_1 \ldots I_m$ para todo $i = 1, \ldots, d$, pero eso implica que $x_i \in I_j$ para todo j, es decir, $x_i \in I_1 \cap \ldots \cap I_m$, de lo que es inmediato el que $x \in (I_1 \cap \ldots \cap I_m)^d$.

Por último, tomemos que ver que $I_1^d \cap \ldots \cap I_m^d \subset (I_1 \ldots I_m)^d$. Para ello empecemos viendo el caso $d = 1$.

Si $m = 2$: podemos escribir $1 = x + y$ donde $x \in I_1$ e $y \in I_2$. Entonces, si $a \in I_1 \cap I_2$, podemos escribir $a = a1 = a(x+y) = ax + ay$ donde $ax, ay \in I_1 I_2$, luego $a \in I_1 I_2$.

Si $m > 2$: Podemos escribir $1 = x_i + y_i$ donde $x_i \in I_i$ e $y_i \in \cap_{j\neq i} I_j$ para todo $i = 1, \ldots, m$. Entonces, $1 = x_1 + y_1 = 1x_1 + y_1 = y_1 + x_1(x_2 + y_2) = y_1 + y_2 x_1 + x_1 x_2$ donde $y_1 \in \cap_{j\neq 1} I_j$, $y_2 x_1 \in \cap_{j\neq 2} I_j$ y con $x_1 x_2 \in I_1 \cap I_2$. Como $x_1 x_2 = x_1 x_2 1$, podemos escribir $1 = sum_{i=1}^m y_i$ donde $y \in \cap_{j\neq i} I_j$.

Sea ahora $a \in \cap_{j=1}^m I_j$. Entonces, $a = a1^{m-1} = \sum a x_{i_1} \ldots x_{i_{m-1}}$. Se verifica que $a x_{i_1} \ldots x_{i_{m-1}} \in I_1 \ldots I_m$ pues x_{i_1} está en $m-1$ de los m I_j, elegido uno de ellos. Entonces, x_{i_2} estará en en al menos en $m-2$

de los $m-1$ I_j excluyendo el elegido para x_{i_1}, elegimos uno de ellos y repetimos el procedimiento para cada i_j $j=1,...,m-2$. Entonces, $x_{i_{m-1}}$ estará en al menos uno de los dos I_j aún no elegido y si elegimos uno de ellos a estará en el último I_j que quede, puesto que a está en todos ellos. Por tanto, $a \in I_1...I_m$.

Veamos que para todo m y todo d $(I_1...I_m)^d = I_1^d...I_m^d$. Si $x \in (I_1...I_m)^d$, entonces podemos suponer $x = x_1...x_d$ donde $x_i \in I_1...I_m$, es decir, podemos suponer $x_i = y_i^1...y_i^m$ donde $y_i^j \in I_j$ para todo i y j. Entonces, reordenando, concluimos que $x = \Pi_{j=1}^m y_1^j...y_d^j \in I_1^d...I_m^d$. Si tomamos $y \in I_1^d...I_m^d$, podemos suponer que $y = y_1...y_m$ donde $y_j \in I_j^d$. Podemos suponer por tanto que $y_j = y_1^j...y_d^j$ donde $y_i^j \in I_j$ para todo j e i. Entonces, reordenando de nuevo, deducimos que $y = \Pi_{i=1}^d y_j^1...y_j^m \in (I_1...I_m)^d$ como queríamos.

Veamos ahora el resultado para cualquier d y para $m=2$. Queremos ver que $I_1^d \cap I_2^d \subset (I_1 I_2)^d$. Llamemos $J_1 = I_1^d$ y $J_2 = I_2^d$, entonces, J_1 y J_2 son comaximales por (1), luego estamos en el caso $d=1$ y $m=2$, y por lo tanto $I_1^d \cap I_2^d = J_1 \cap J_2 \subset J_1 J_2 = I_1^d I_2^d = (I_1 I_2)^d$ como vimos antes.

Por último, razonamos por inducción sobre m. Supongamos que $I_{i_1}^d...I_{i_{m-1}}^D \subset (I_{i_1}...I_{i_{m-1}})^d$ para cualquier subconjunto de $m-1$ ideales distinto de $I_1,...,I_m$.

Vimos antes que $(I_{i_1}...I_{i_{m-1}})^d \subset I_{i_1}^d \cap ... \cap I_{i_{m-1}}^d \subset (I_{i_1} \cap ... \cap I_{i_{m-1}})^d$, luego todas estas son igualdades.

Veamos que I_i^d y $\cap_{j \neq i, j \neq k} I_j^d$ son comaximales para todo i y todo $k \neq i$. Como $\cap_{j \neq i} I_j \subset \cap_{j \neq i, j \neq k} I_j$, y $\cap_{j \neq i} I_j$ e I_j son comaximales, es inmediato el ver que I_i y $\cap_{j \neq i, j \neq k} I_j$ también son comaximales para toda k y por tanto I_i^d y $(\cap_{j \neq i, j \neq k} I_j)^d$ son comaximales para todo k. Entonces, usando la hipótesis de inducción, vimos que $(\cap_{j \neq i} I_j)^d = \cap_{j \neq i} I_j^d = (\Pi_{j \neq i} I_j)^d$. Por tanto, I_i^d y $(\cap_{j \neq i} I_j)^d = \cap_{j \neq i} I_j^d$ son comaximales por (1).

Llamemos ahora $J_j = I_j^d$ para todo $j = 1,...,m$ y como hemos visto que J_i y $\cap_{j \neq i} J_j$ son comaximales para todo i, hemos reducido el problema al caso $d=1$ que ya tratamos antes. Es decir $I_1^d \cap ... \cap I_m^d = J_1 \cap ... \cap J_m \subset J_1...J_m = I_1^d...I_m^d = (I_1...I_m)^d$ y concluimos.

Proposición 72 *Sean $I, J \subset A$ dos ideal es con I finitamente generado e $I \subset Rad(J)$ donde $Rad(J)$ representa el ideal radical de J. Entonces, existe un entero n no negativo con $I^n \subset J$.*

Demostración: Sean $x_1,...,x_m \in A$ con $I = (x_1,...,x_m)$. Como $I \subset Rad(J)$, existen enteros positivos $n_1,...,n_m$ con $x_i^{n_i} \in J$. Sea $n \geq \sum_{i=1}^m n_i$. Sea ahora $y \in I^n$, podemos suponer que $y = y_1...y_n$ donde $y_i \in I$. Entonces $y_i = \sum_{i=1}^{m_i} a_j x_j$ con $a_j \in A$, por lo tanto, $y = \sum_{i_1+...+i_m=n} a_{i_1,...,i_m} x_1^{i_1}...x_m^{i_m}$. Si todo $i_j < n_j$, $\sum i_j < n$, luego para algún j, $i_j \geq n$ y por tanto $a_{i_0,...,i_m} x_1^{i_1}...x_m^{i_m} \in J$ y con ello $y \in J$.

Definición 66 *Un anillo A se dice que es* neotheriano *si todo ideal está finitamente generado.*

Definición 67 *Sea B un anillo y A un subanillo de B de modo que ambos anillos son locales (poseen un único ideal maximal). Diremos que B domina a A si el maximal de A está contenido en el de B*

Nota: En particular, los dominios de ideales principales, y con ello los cuerpos, son noetherianos.

Teorema 11 (de la base de Hilbert) *: Si A es un anillo neotheriano, entonces $A[X]$ también es un anillo neotheriano.*

Demostración: Ver [2], capítulo 1, sección 4.

Corolario 9 *$k[X_1,...,X_n]$ es un anillo noetheriano.*

Lema 25 *Sea A un anillo neotheriano y sea S una familia no vacía de ideales de A. Entonces, S posee un elemento maximal.*

Demostración: Ver [2], capítulo 1, sección 5.

Anillos de valoración discreta

Definición 68 *Se conoce como* anillo de valoración discreta *a todo anillo que sea un dominio, neotheriano, local y cuyo maximal es un ideal principal.*

Proposición 73 *Sea A un anillo que es un dominio. Son equivalentes:*

(1) A es un anillo de valoración discreta.

(2) Existe un elemento irreducible $t \in A$ tal que para todo $x \in A$ irreducible, $x \neq 0$, se puede escribir de forma única como $x = ut^n$ con $u \in A$ una unidad y n un entero no negativo.

Demostación: Sea A un anillo de valoración discreta y sea M su maximal. Sea t un generador de M y sea $x \in A$ un elemento irreducible no nulo. $x \in M$, luego existe $x_1 \in A$ tal que $x = x_1 t$. Si x_1 es una unidad hemos terminado, si no, existirá $x_2 \in A$ tal que $x_1 = x_2 t$ y con ello $x = x_2 t^2$. Iterando el proceso, tenemos una sucesión $x_1, x_2, \ldots$ con $x_i = x_{i+1}t$. Si para todo i x_i no es una unidad, tendremos entonces una cadena de ideales $(x_1) \subsetneq (x_2) \subsetneq \ldots$ que, en virtud de el lema 25 tiene un maximal, es decir, existe n tal que $(x_n) = (x_{n+1})$, por tanto, existe una unidad v tal que $x_{n+1} = vx_n$. Esto implica que $x_n = x_{n+1}t = vx_n t$ y necesariamente $1 = vt$, pero t no es una unidad, luego ha de ocurrir que para algún j $x_j = u$ sea una unidad. Con lo que $x = ut^j$ como queríamos.

Para ver la unicidad, consideremeos $u, v \in A$ dos unidades y n, m dos enteros no negativos con $m \geq n$ y supongamos que $ut^n = vt^m$, entonces $(u - vt^{m-n})t^n = 0$, es decir $u = vt^{m-n}$ es una unidad, luego $u = v$ y $m = n$.

Para ver la otra implicación basta darse cuenta de que como todo elemento que no sea una unidad se puede escribir como $x = ut^n$ con $n \neq 0$, (t) es el conjunto de todos los elementos de A que no son una unidad, luego es el único maximal de A. Con esto hemos visto que A es un anillo local cuyo maximal es principal. Para ver que es noehtherianos, veamos que todos los ideales de A distintos del nulo han de ser de la forma (t^m) con $m \geq 0$. Sea $I \subset A$ un ideal, si I no es el total, necesariamente $I \subset (t)$. Si $a \in I$, sabemos que podemos escribir $a = ut^n$ para alguna unidad u y para $n > 0$, luego I está generado por potencias t^n tales que $vt^n \in I$ y $n > 0$. Tomamos m como el mínimo de los n, $m > 0$ y tendremos que $I = (t^m)$.

Definición 69 *Al elemento t de la proposición 73 se le conoce como* parámetro de uniformización.

Definición 70 *A la potencia n del parámetro de uniformización de la proposición 73 se le conoce como* orden *de x y lo denotaremos por $ord(x)$. Este orden no depende del parámetro de uniformización escogido pues si tenemos s y t dos parámetros de uniformización, $(s) = (t)$ son el ideal maximal del anillo local y por tanto $s = vt$ con v una unidad y si $x = us^n = uv^n t^n = wt^n$ con w una unidad.*

Esta escritura para los elementos de un anillo de valoración discreta A se puede extender a los de su cuerpo de fracciones, pues si denotamos por K a este cuerpo y $\frac{a}{b} \in K$ para ciertos $a = ut^n$ y $b = vt^m$ elementos de A, entonces $\frac{a}{b} = \frac{ut^n}{vt^m} = wt^l$ con w una unidad y l un entero no necesariamente positivo. De esta forma, si un elemento $x \in K$ se escribe como $x = wt^l$, entonces $x^{-1} = w^{-1}t^{-l}$.

Proposición 74 *Sea A un anillo de valoración discreta y sea K su cuerpo de fracciones. Entonces*

(1) si $x, y \in K$ y $ord(x) < ord(y)$ entonces $ord(x + y) = ord(x)$.

(2) si $x_1, \ldots, x_n \in K$ y existe i tal que $ord(x_i) < ord(x_j)$ para todo $j \neq i$, entonces $x_1 + \ldots + x_n \neq 0$

Demostración:

(1) Sea t un parámetro de uniformización y sean u, v elementos irreducibles de K, entonces, podemos escribir $x = ut^n$ e $y = vt^m$ con $ord(x) = n$ y $ord(y) = m$ números enteros. Entonces $x + y = t^n(u + vt^{m-n})$. Si $u + vt^{m-n}$ no fuera una unidad, existiría $w \in A$ tal que $u + vt^{m-n} = wt^r$ con $r \in \mathbb{Z}$, $r > 0$, con lo que $u = at^s$ con $a \in A$ y s un entero distinto de 0 pues $min(r, m-n) > 0$ o $u = 0$. Absurdo pues u es una unidad.

(2) Como hemos visto en el apartado anterior, $ord(\sum x_j) = ord(a_i)$. Si $ord(a_i) > 0$, entonces $\sum a_j \neq 0$. Si $ord(a_i) = 0$, a_i es una unidad pero como $ord(\sum_{j\neq i} a_j) > 0$, $\sum a_j \neq 0$ pues es la suma de una unidad y una no unidad. Si $ord(a_i) < 0$, entonces $\sum a_j \neq 0$.

Proposición 75 *Sea A un anillo de valoración discreta y m su ideal maximal. Sea $k = \frac{A}{m}$ un cuerpo. Entonces $\frac{m^n}{m^{m+1}}$ y $\frac{A}{m^n}$ son espacios vectoriales sobre k que verifican:*

(1) $dim(\frac{m^n}{m^{n+1}}) = 1$ *para todo* $n \geq 0$.

(2) $dim(\frac{A}{m^n}) = n$ *para todo* ≥ 0.

(3) *si* $a \in A$ *y* $(a) = m^n$, *entonces,* $ord(a) = n$.

(4) $ord(a) = dim(\frac{A}{(a)})$ *para todo* $a \in A$.

Demostración: (1) Si $h \in \frac{m^n}{m^{n+1}}$, entonces escribimos $h = at^n + m^{n+1}$ para algún $a \in A$ y t un parámetro de uniformización. Por otra parte, como $k = \frac{A}{m}$, si $b \in A$ existe $\lambda_b \in k$ con $b - \lambda_b \in m$. Entonces, $\lambda_a t^n - h = (\lambda_a - a)t^n - (h - at^n)$ y como $\lambda_a - a, t \in m$, $(\lambda_a - a)t^n, h - at^n \in m^{n+1}$ y por tanto $h = \lambda_a t^n + m^{n+1}$. Es decir, el elemento $t^n + m^{n+1}$ es un sistema de generadores del k-espacio vectorial $\frac{m^n}{m^{n+1}}$, luego $dim(\frac{m^n}{m^{n+1}}) = 1$.

(2) Razonemos por inducción sobre n. Si $n = 0$, $\frac{A}{m^0} = \frac{A}{(1)} = 0$, y claramente $dim(\frac{A}{m^0}) = 0$. Supongamos que $dim(\frac{A}{m^n}) = n$. Sabemos $\frac{A}{m^n} = \frac{A/m^{n+1}}{m^n/m^{n+1}}$ luego

$$dim(\frac{A}{m^{n+1}}) = dim(\frac{A}{m^n}) + dim(\frac{m^n}{m^{n+1}}) = n + 1.$$

(3) Si t es un parámetro de unifomización, $(a) = m^n = (t)^n = (t^n)$, luego $a = ut^n$ con $u \in A$ una unidad, y por tanto, $ord(a) = n$.

(4) Consecuencia inmediata de (2) y (3).

Módulos y sucesiones exactas

Definición 71 *Dado un anillo conmutativo y unitario A, llamamos* módulo *de A a todo grupo abeliano M que verifique que para cada par de elementos $n, m \in M$, cada par de elementos $a, b \in A$ y para $e \in A$ el elemento unidad del anillo, se verifica:*

$$a(x + y) = ax + ay,$$

$$(a + b)x = ax + bx,$$

$$(ab)x = a(bx),$$

$$ex = x.$$

Dos ejemplos inmediatos de A-módulos son el propio A y en general cualquier ideal de A.

Dada un conjunto finito de A-módulos M_i $i = 1,...,n$ se define su suma directa $\oplus_{i=1}^n M_i$ como el conjunto de n-uplas $(m_1,...,m_n)$ tales que $m_i \in M_i$. Como ejemplo, tenemos la suma directa de n copias de A visto como A-módulo. Denotaremos por A^n a esta suma directa.

Definición 72 *Dados A un anillo y M, N dos A-módulos, decimos que una aplicación $f : M \longrightarrow N$ es un* morfismo de A-módulos*, si para cada par de $m, n \in M$ y para cada $a \in A$ se verifica:*

$$f(m+n) = f(m) + f(n)$$

$$f(am) = af(m).$$

Si f es biyectiva y su inversa también es un morfismo de A-módulos, diremos que f es un isomorfismo

Proposición 76 *Dado un morfismo $f : M \longrightarrow N$ entre A-módulo, se tiene que el núcleo de la aplicación $Ker(f) = \{x \in M : f(M) = 0\}$ es un submódulo de N y que si denotamos por $Im(f) = f(M)$ la imagen de f, existe un isomorfimos entre $\frac{M}{Ker(f)}$ y $Im(f)$.*

Demostración: Ver [1], capítulo 2.

Definición 73 *Dadas una sucesión de A-módulos M_i y una sucesión de morfismos de A-módulos $f_i : M_{i-1} \longrightarrow M_i$ diremos que la sucesión*

$$... \longrightarrow M_{i-1} \longrightarrow M_i \longrightarrow ...$$

es exacta en M_i si $Im(f_i) = Ker(f_{i+1})$ y diremos que la sucesión es exacta si lo es en cada A-módulo M_i.

Nota: Fijémonos que una sucesión $0 \longrightarrow M_0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow 0$ es exacta si y solamente si f_1 es inyectiva, f_2 es sobreyectiva y que f_1 induce un isomorfismo entre $\frac{M_1}{Im(f_1)}$ y M_2.

Definición 74 *Dados A un anillo y M un A-módulo tal que para ciertos $x_i \in M$ se puede escribir $M = \sum x_i A$, decimos que los x_i son unos* generadores *del módulo y si M tiene un conjunto de generadores finito diremos que M es un* módulo finitamente generado.

Proposición 77 *Dado M un módulo de un cierto anillos A se verifica que M es de generación finita si y solo si M es isomorfo al cociente de A^n por algún ideal para algún entero $n > 0$.*

Demostración: Supongamos que M es de generación finita, entonces, existirán $x_1,...,x_n \in M$ unos generadores del módulo. Definimos ahora el morfismo de A-módulos $f : A^n \longrightarrow M$ como $f(a_0,...,a_n) = a_1x_1 + ... + a_nx_n$. Como obviamente $Im(f) = M$, tenemos que M es isomorfo a $\frac{A^n}{Ker(f)}$.

Supongamos ahora que existe un isomorfismo de A-módulos entre un cociente de A^n y M. Existe entonces un morfismo de A-módulos $f : A^n \longrightarrow M$ sobreyectivo. Si e_i es el vector coordenado de A^n, los elementos $e_1,...,e_n$ generan A^n y, por tanto, sus imágenes generarán M, con lo que las imágenes de los vectores coordenados forman un conjunto finito de generadores de M.

Definición 75 *Dado A un anillo, y M un A-módulo, diremos que M es un* módulo noetheriano *si el conjunto de sumbódulos de M tiene un maximal, equivalentemente, si $N_1 \subset N_2 \subset ...$ es una cadena ascendente de A-módulos con $N_i \subset M$, entonces existe j tal que $N_j = N_{j+1}$.*

Nota: Del lema 25 se deduce que A es un A-módulo noetheriano de generación finita.

Proposición 78 *Dado A un anillo y M un A-módulo. M será un módulo noetheriano si y solamente si, todo submódulo de M es un A-módulo de generación finita.*

Demostración: Supongamos que M es noetheriano. Sea N un submódulo de M y sea Σ el conjunto de todos los sumbódulos de N de generación finita como A-módulos. Como el conjunto 0 es un A-módulo contenido en todos los demás A-módulos y es obviamente de generación finita, Σ es un subconjunto no vacío del conjunto de submódulos de M, con lo que Σ tiene un elemento maximal al que denotaremos por N_0. Si N es distinto de N_0, existirá $x \in N$, $x \notin N_0$ y por tanto $N_0 + xA$ es un submódulo de N de generación finita que contiene a N_0, lo que es absurdo. En consecuencia, $N = N_0$ es de generación finita.

Supongamos ahora que todo submódulo de M es de generación finita. Consideremos M_i un conjunto de submódulos de M tales que $M_1 \subset M_2 \subset ...$ y consideremos $N = \cup M_i$. N es un submódulo de M y, por tanto, existirán $x_1, ..., x_n \in N$ generadores de N como A-módulo. Para cada $j = 1, ..., n$ existirá i_j de modo que $x_j \in M_{i_j}$, con lo que si $k > i_j$ para todo j, tendremos que $x_j \in M_k$ para todo j y con ello, deducimos que $N = M_k$ y en consecuencia, $M_{k+1} = M_k$ para todo, luego M es noetheriano.

Proposición 79 *Dada una sucesión exacta de A-módulos* $0 \longrightarrow M_0 \longrightarrow M_1 \longrightarrow M_1 \longrightarrow 0$ *que viene dada por $f_{i-1} : M_{i-1} \longrightarrow M_i$ para $i = 1, 2$. Se verifica que M_1 es noetheriano si y solo si M_0 y M_2 son noetherianos.*

Demostración: Supongamos que M_1 es noetheriano. Si tenemos una cadena ascendente de submódulos N_i de M_0 y otra de submodulos N'_i de M_2, a través de los morfismos f_0 y f_1 tendremos dos cadenas ascendentes $f_0(N_i)$ y $f_1^{-1}(N'_i)$ de submódulos de M_1. Entonces, existirá j tal que $f_0(N_{j-1}) = f_0(N_j)$ y $f_1^{-1}(N'_{j-1}) = f_1^{-1}(N'_j)$. Como f_0 es inyectiva tenemos que $N_{j-1} = N_j$, luego M_0 es noetheriano, y como f_1 es sobreyectiva, también tenemos que M_2 es noetheriano porque $N'_{j-1} = N'_j$.

Supongamos ahora que M_0 y M_1 son noetherianos. Sea N un submódulo de M_1. Si vemos que N es de generación finita, en virtud de la proposición 78 deduciremos que M_1 es noetheriano. Sea $n \in N$ un elemento cualquiera. Como M_1 es noetheriano, existirán $\alpha 1, ..., \alpha \in f_1(N)$ que generen el módulo, es decir, para ciertos $a_1, ..., a_s \in A$, podemos escribir $f(n) = \sum_{i=1}^{s} a_i \alpha$. Llamemos β_i a $f_1^{-1}(\alpha_i) \in N$, entonces, como f_i es un morfismo de A-módulos, es lineal para los elementos de A, y por tanto, $n - \sum_{i=1}^{s} a_i \beta_i \in Ker(f_1) = Im(f_0)$ por ser la sucesión exacta, es decir, existe $m \in M_0$ tal que $f_0(m) = n - \sum_{i=1}^{s} a_i \beta_i$. Ahora bien, M_0 también es noetheriano, luego existen elementos $\gamma_1, ..., \gamma_r \in f_0^{-1}(N)$ que generen el submódulo. Como $f_0(m) \in N$, $m \in f_0^{-1}(N)$, con lo que existirán $b_1, ..., b_r \in A$ tales que $m = \sum_{j=1}^{r} n_j \gamma_j$. De esta forma, se tiene que $f_0(m) = \sum_{j=1}^{r} b_j f_0(\gamma_j) = n - \sum_{i=1}^{s}$, es decir, $n = \sum_{j=1}^{r} b_j f_0(\gamma_j) + \sum_{i=1}^{s} a_i \beta_i$, de lo que deducimos que los β_i y los $f_0(\gamma)$ general N.

Proposición 80 *Dados $M_1, ..., M_n$ A-módulos noetherianos, entonces, $\oplus_{i=1}^{n} M_i$ también es noetheriano.*

Demostración: Consideremos la sucesión $0 \longrightarrow M_k \longrightarrow \oplus_{i=1}^{k} M_i \longrightarrow \oplus_{i=1}^{k-1} M_i \longrightarrow 0$ dada por la inclusión i_k y la proyección p_k. La inclusión es inyectiva y la proyección es sobreyectiva, y además $\frac{\oplus_{i=1}^{k} M_i}{Im(i_k)}$ es, evidentemente, isomorfo a $\oplus_{i=1}^{k-1} M_i$. En consecuencia, la sucesión anterior es exacta para todo $k = 2, ..., n$. Para concluir, aplicamos inducción sobre k y aplicamos la proposición 79 para deducir que para cada k, el A-módulo $\oplus_{i=1}^{k} M_i$ es noetheriano.

Proposición 81 *Dado un anillo noetheriano A, se verifica que todo A-módulo de generación finita es un módulo noetheriano.*

Demostración: Como hemos mencionado antes, A es un A-módulo noetheriano, y de la proposición 80, deducimos que A^n es noetheriano para todo entero $n > 0$. En virtud de la proposición 77 existe un ideal I de A^n de modo que M es isomorfo a $\frac{A^n}{I}$, en consecuencia, existe un morfismo $f : A^n \longrightarrow M$ sobreyectivo. Recordemos que I es un A-módulo y consideramos ahora la sucesión de A-módulos $0 \longrightarrow I \longrightarrow A^n \longrightarrow M \longrightarrow 0$ dada por la inclusión de I en A^n y por f. Esta sucesión es exacta, y de la proposición 79 deducimos que M es noetheriano.

Lema 26 *Sea A un anillo noetheriano, e I un ideal de A. Entonces, $\frac{A}{I}$ es un anillo noetheriano.*

Demostración: Tenemos que la aplicación del paso al cociente es sobreyectiva y la inclusión de I en A es inyectiva. Luego la sucesión $0 \longrightarrow I \longrightarrow A \longrightarrow \frac{A}{I} \longrightarrow 0$ es exacta y concluimos aplicando la proposición 79

Dependencia entera

Definición 76 *Sea B un anillo cualquiera y sea A un subanillo de B. Diremos que un elemento $b \in B$ es* entero *sobre A si existen elementos $a_0, ..., a_n \in A$ que cumplen la igualdad $b^{n+1} + a_n b^n + ... + a_0 = 0$.*

Definición 77 *Un anillo B es entero sobre un subanillo $A \subset B$ si cada elemento de B es entero sobre A.*

Proposición 82 *Sea A un dominio con cuerpo de fracciones k. Sea $k : K$ una extensión algebraica de cuerpos finita. Entonces, existe una base $v_1, ..., v_n$ de K como k-espacio vectorial formada por elementos enteros sobre A.*

Demostración: Sea $v \in K$ algebraico sobre k. Entonces existe un polinomio $P \in k[X]$ tal que $P(v) = 0$. Quitando denominadores en P tenemos que $a_0 + a_1 v + ... + a_n v^n = 0$ para ciertos $a_i \in A$. Si multiplicamos la expresión anterior por a_n^{n-1} tenemos $(a_0 a_n^{n-1}) + (a_1 a_n^{n-2})(a_n v) + ... + (a_n v)^n = 0$, es decir, $a_n v$ es entero sobre A. Es decir, para todo elemento de K existe un elemento $a \in A$ tal que av es entero sobre A.

Sea ahora $w_1, ..., w_n$ una base de K como k-espacio vectorial. Y sean $v_i = a_i w_i$ enteros sobre A. Como $a_i \in k$, $v_1, ..., v_n$ sigue siendo una base de K, con lo que concluimos.

Apéndice B: Extensiones de cuerpos

Extensiones algebraicas

Teorema 12 (del elemento primitivo) *Sea $K : L$ una extensión algebraica finita de cuerpos con K un cuerpo de característica cero. Entonces, existe $x \in L$ de modo que $L = K(x)$.*

Demostración: Como la extesnsión es finita, es finitamente generada, es decir, existen elementos $x_1, ..., x_s \in L$ algebraicos sobre K tales que $K(x_1, ..., x_s) = L$.

Supongamos que existen $x, y \in L$ algebraicos sobre K con $L = K(x, y)$. Sean F y G dos polinomios mónicos irreducibles de $K[X]$ con $F(x) = 0$ y $G(y)$. Sea L' el cuerpo de descomposición de F y G. En L' podemos escribir $F = \Pi_{i=1}^{n}(X - x_i)$ y $G = \Pi_{j=1}^{m}(X - y_j)$ donde para algún i y algún j, $x = x_i$ e $y = y_j$, como F y G son mónicos e irreducibles, solo un i y un j lo verifican, supongamos $i = 1 = j$. Como $L' \supset K$ y $x, y \subset L'$, concluimos que $L \subset L'$.

Sea $\lambda \in K$ de modo que la expresión en $L' \supset L$ $\lambda(x - x_i) + (y - y_j) \neq 0$ para todo par de i, j con $i \neq 1$ y $j \neq 1$. Tomemos $z = \lambda x + y$, $K' = K(z) \subset L$ y $H(X) = G(\lambda(x - X) + y) = G(z - \lambda X) \in K'[X]$. $H(x) = G(y) = 0$ pero $H(x_i) = G(\lambda(x - x_i) + y)$ y como $\lambda(x - x_i) + y \neq y_j$ para $j = 1, ..., m$, si $i \neq 1$ $H(x_i) \neq 0$ para $i \neq 1$. En consecuencia, el ideal $(H, F) = (X - x) \in K'[X]$, ya que x es el único cero que tienen en común, pues de para algún $X \neq x$ $F(X) = H(X)$, $X = x_i$ para algún $i > 1$ por ser raíz de F, pero $H(x_i) = G(\lambda(x - x_i) + y)$, que se anula si y solamente si $\lambda(x_i - x) + (y_i + y) = 0$, lo cual no es posible. Por lo tanto, $x \in K'$ y también $y \in K'$, luego $L \subset K'$.

Razonemos ahora por inducción sobre s. Supongamos que si $L = K(x_1, ..., x_{s-1})$ existen $\lambda_1, ..., \lambda_{s-1}$ de modo que $L = K(\sum_{i=1}^{s-1} \lambda_i x_i)$ y veamos que si $L = K(x_1, ..., x_s)$ existen $\lambda_1, ..., \lambda_s$ de modo que $L = K(\sum_{i=1}^{s} \lambda_i x_i)$: sea $L' = K(x_1, .., x_{s-1})$, entonces, por hipótesis de inducción, existen $\alpha_1, ..., \alpha_{s-1}$ de modo que si $w = \sum_{i=1}^{s-1} \alpha_i x_i$, $L' = K(w)$. Como $w \in K(x_1, ..., x_s)$ y $x_1, ..., x_{s-1} \in K(w) \subset K(w, x_s)$ tenemos que $K(x_1, ..., x_s) = K(w, x_s)$. Nuevamente, por hipótesis de inducción, existirán $\lambda_1, \lambda_2 \in K$ de modo que $L = K(\lambda_1 w + \lambda_2 x_s) = K(\sum_{i=1}^{s-1} \lambda_1 \alpha_i x_i + \lambda_2 x_s)$.

Extensiones trascendentes y bases de trascendencia

Definición 78 *Sea $k : K$ una extensión de cuerpos. Diremos que un subconjunto $S \in K$ es* algebraicamente independiete *sobre k o que sus elementos lo son si cuando tengamos una expresión finita del tipo $\sum_I a_I \Pi_{x \in S} x^{I_x} = 0$ donde I es un multi-índice y $a_I \in k$, entonces, necesariamente $a_I = 0$ para todo I. A los conjuntos que no son algebraicamente independientes o a sus elementos los llamaremos* algebraicamente dependientes.

Nota: Un subconjunto de K formado por elementos enteros sobre k es obviamente algebraicamente dependiente.

Es posible ordenar los subconjuntos algebraicamente independentes de K sobre k de modo que $S \leq S'$ si $S \subset S'$. Formamos así cadenas ordenadas que tendrán algún elemento maximal.

Definición 79 *Un subconjunto $S \subset K$ algebraicamente independiente sobre k y maximal se llama* base de trascendencia *de K sobre k.*

Proposición 83 *Sea $k : K$ una extensión de cuerpos y sea S una base de trascendencia de K sobre k. Entonces, la extensión $k(S) : K$ es algebraica.*

Demostración: Si la extensión no fuera algebraica, existiría $x \in K$ trascendente sobre $k(S)$. Es decir, ningún polinomio $P \in k(S)[X]$ se anula en x, por lo tanto, si tuviéramos una expresión $\sum_{j=0}^{d}(\sum_{I_j} a_{I_j} \Pi_{y\in S} y^{I_{jy}})x^j = 0$, como $\sum_{I_j} a_{I_j} \Pi_{y\in S} y^{I_{jy}} \in k(S)$ para todo j entonces, necesariamente $\sum_{I_j} a_{I_j} \Pi_{y\in S} y^{I_{jy}} = 0$ para todo j, pero como los elementos de S son algebraicamente independientes, $a_{I_j} = 0$ para todo I_j.

Ahora bien, si vemos $\sum_{j=0}^{d}(\sum_{I_j} a_{I_j} \Pi_{y\in S} y^{I_{jy}})x^j$ no como un polinomio en x si no como una expresión $\sum_J b_J x^{J_x} \Pi_{y\in S} y^{J_y}$, hemos visto que si cualquier expresión de este tipo se anula, necesariamente $b_J = 0$, luego x es un elemento algebraicamente independiente pero que no es un elemento de S, pues de serlo no sería trascendente. Sin embargo, S es maximal por hipótesis, luego este x no puede existir.

Definición 80 *Sean k y K dos cuerpo, de modo que $k : K$ es una extensión de cuerpos. Se define el* grado de trascendencia *como el menor entero n (puede ser infinito) tal que existen $x_1, ..., x_n \in K$ de modo que K es algebraico sobre $k(x_1, ..., x_n)$.*

Nota: el grado de trascendencia coincide por tanto con el menor de los cardinales de las bases de trascendencia de K sobre k. Veremos en el teorema siguiente que en realidad todas las bases de trascendencia tienen el mismo número de elementos (finito o infinito).

Teorema 13 *Sea $k : K$ una extensión de cuerpos. Entonces, todo par de bases de trascendencia de K sobre k tienen el mismo cardinal. Además, si $T \subset K$ es un tal que $K = k(T)$, y $S \subset T$ un subconjunto de T algebraicamente independiente, existe una base de trascendencia B de modo que $S \subset B \subset T$.*

Demostración: Para ver que dos bases de trascendencia siempre tienen el mismo cardinal, basta con ver que si existe una base de trascendencia con m elementos, todo subconjunto de K que sea algebraicamente independiente sonbre k tendrá cardinal como mucho m.

Sean $x_1, ..., x_m$ los elementos de una base de trascendencia. Y tomemos $w_1, ..., w_n$ elementos algebraicamente independientes. Como $x_1, ..., x_m$ son elementos de una base maximal, existe un polinomio en $m+1$ con coeficientes en k, $f \neq 0$, de modo que $f(w_1, x_1, ..., x_m) = 0$. Además, necesariamente w_1 ha de aparecer en $f(w_1, x_1, ..., x_m)$ al igual que x_i para algún i ya que $x_1, ..., x_m$ son algebraicamente independientes y también lo es w_1. Supongamos $i = 1$.

Podemos ver f como un polinomio en una variable con coeficientes en $k(w_1, x_2, ..., x_m)$, luego x_1 es algebraico sobre $k(w_1, x_2, ..., x_m)$.

Sabemos que K es algebraico sobre $k(x_1, ..., x_m)$, luego también sobre $k(w_1, x_1, ..., x_m)$. También sabemos que $k(w_1, x_1, ..., x_m)$ es algebraico sobre $k(w_1, x_2, ..., x_m)$ por serlo x_1. Por tanto, K es algebraico sobre $k(w_1, x_2, ..., x_m)$.

Supongamos que para $r < n$ K es algebraico sobre $k(w_1, ..., w_r, x_{r+1}, ..., x_m)$ Razonemos por inducción sobre r y veamos que K es algebraico sobre $k(w_1, ..., w_{r+1}, x_{r+2}, ..., x_m)$.

Como K es algebraico sobre $k(w_1, ..., w_r, x_{r+1}, ..., x_m)$, existe un polinomio f en $m+1$ variables con $f(w_{r+1}, w_1, ..., w_r, x_{r+1}, ..., x_m) = 0$. Igual que antes, necesariamente w_{r+1} ha de aparecer en la expresión, así como un x_i para $i = r+1, ..., m$. Supongamos que $i = r+1$. También esta vez podemos ver a f como polinomio en una única variable en $k(x_{r+1}, w_1, ..., w_r, x_{r+2}, ..., x_m)$ de lo que deducimos que x_{r+1} es algebraico sobre $k(w_1, ..., w_{r+1}, x_{r+2}, ..., x_m)$ y como antes, K es algebraico sobre $k(w_1, ..., w_{r+1}, x_{r+2}, ..., x_m)$.

Hemos probado, por lo tanto, que si $n \geq m$ entonces K es algebraico sobre $k(w_1, ..., w_m)$ y por tanto si $n > m$ existiría w_{m+1} de modo que $w_1, ..., w_m, w_{m+1}$ fueran algebraicamente independientes, pero como $w_{m+1} \in K$, w_{m+1} es algebraico sobre $k(w_1, ..., w_m)$, lo cual es absurdo.

Hemos probado, por tanto, que todo conjunto algebraicamente independiente ha de tener cardinal a lo sumo m. De lo que es inmediato deducir que si existe una base de trascendencia con cardinal finito, todas las bases de trascendencia tienen el mismo cardinal. Si no existiera ninguna base con cardinal finito, entonces todas las bases son infinitas.

Veamos ahora que existe una base de trascendencia B de modo que $S \subset B \subset T$. Sea $L = k(S)$, y $R = T \setminus S$, entonces $K = L(R)$. Si la extensión $K : L$ no es algebraica, existe algún elemento de T que no está en S y que es trascendente sobre L. Consideramos entonces S' el conjunto formado por dicho elemento y por los elementos de S' y repetimos el razonamiento hasta que la extensión $K : L$ sea algebraica.

Supongamos que la extensión $K : L$ es algebraica. Entonces, todo elemento $w \in K \setminus L$ es algebraico sobre L, es decir, no existen elementos de K algebraicamente independientes sobre $k(S)$. Es decir, S es la base B que buscábamos.

Bibliografía

[1] ATIYAH,M.F. / MACDONALD,I.G.: *Intrsocucción al Álgebra Conmutativa*. Editorial Reverté. 1978

[2] FULTON, W.: *Curvas algebraicas*. Editorial Reverté. 1971

[3] HARTSHORNE, R.: *Algebraic Geometry*. Springer. Graduate Texts in Mathematics. 1977

[4] LANG,S.: *Álgebra*. Aguilar. 1971

[5] SHAFAREVICH,I.R.: *Basic Algebraic Geometry. Vol. 1 (Vatieties in Proyective Space). Second Edition*. Springer-Verlag. 1994