



FACULTADE DE MATEMÁTICAS

Traballo Fin de Grao

Dimensión y número de ecuaciones de las variedades algebraicas afines y proyectivas

Guillermo Vilar González

2019/2020

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRAO DE MATEMÁTICAS

Traballo Fin de Grao

Dimensión y número de ecuaciones de las variedades algebraicas afines y proyectivas

Guillermo Vilar González

2019/2020

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Trabajo propuesto

Área de Coñecemento: Algebra
Título: Dimensión y número de ecuaciones de las variedades algebraicas afines y proyectivas
Breve descripción do contido
<p>El concepto de dimensión es el primer invariante que se asocia a una variedad algebraica. Los puntos, curvas y superficies son variedades de dimensión 0, 1 y 2, respectivamente. En este trabajo se dará una definición topológica de la dimensión de una variedad algebraica muy natural, pero no siempre fácil de manejar, y también otras definiciones más manejables que exigen resultados de álgebra conmutativa y de teoría de cuerpos. En el caso de variedades algebraicas afines irreducibles se probará que su dimensión topológica coincide con la dimensión de Krull de su anillo de funciones regulares y con el grado de trascendencia de su cuerpo de funciones racionales.</p> <p>Siguiendo el modelo de las variedades lineales, se estudiará la relación entre la dimensión de una variedad algebraica afín o proyectiva y el número de ecuaciones que la definen.</p>
Recomendacións
Se recomienda haber cursado las materias Estructuras Algebraicas y Ecuaciones Algebraicas, y estar cursando la materia Álgebra, Números y Geometría.
Outras observacións

Índice general

Resumen	VIII
Introducción	XI
1. Extensiones trascendentes	1
1.1. Extensiones de cuerpos	1
1.2. Independencia algebraica	6
1.3. Bases de trascendencia	8
2. Dependencia entera	13
2.1. Anillos de fracciones	13
2.2. Dependencia entera	16
2.3. Lema de normalización de Noether	22
3. Variedades algebraicas afines	25
3.1. Variedades algebraicas afines. Topología de Zariski	25
3.2. Ideal de una variedad algebraica afín	26
3.3. Irreducibilidad	28
3.4. Teorema de los ceros de Hilbert	31
4. Variedades algebraicas proyectivas	37
5. Dimensión	45
5.1. Dimensión topológica. Relación con la dimensión de Krull	45
5.2. Dimensión de las K -álgebras finitamente generadas	47
5.3. El teorema algebraico fundamental	51
6. Número de ecuaciones de una variedad algebraica afín	53
6.1. Dimensión de una variedad algebraica afín dadas sus ecuaciones	53
6.2. Sistemas de parámetros de una variedad algebraica afín	57

7. Número de ecuaciones de una variedad algebraica proyectiva	61
Bibliografía	67

Resumen

El objetivo de este trabajo es el estudio de la dimensión de las variedades algebraicas afines y proyectivas y su relación con el número de ecuaciones necesario para describirlas.

La dimensión como espacio topológico de una variedad algebraica afín coincide con la dimensión de Krull de su anillo de funciones regulares. En el caso de una variedad algebraica afín irreducible de K^n , se prueba que su dimensión es igual al grado de trascendencia de su cuerpo de funciones racionales sobre K .

Siguiendo el modelo de las variedades lineales se analiza la relación entre la dimensión de una variedad algebraica afín y el número de ecuaciones que la definen. Por ejemplo, suponiendo que el cuerpo K es algebraicamente cerrado, se tiene que si V es una variedad algebraica afín irreducible de K^n y f_1, \dots, f_r son funciones regulares en V verificando que $Z(f_1, \dots, f_r) \neq \emptyset$, entonces toda componente irreducible de $Z(f_1, \dots, f_r)$ tiene dimensión $\geq \dim V - r$; por tanto $\dim Z(f_1, \dots, f_r) \geq \dim V - r$. En el caso $r = 1$, si $f_1 \neq 0$ y f_1 no es una unidad se tiene la igualdad.

Los resultados para variedades algebraicas afines se extienden a variedades algebraicas proyectivas, y además podemos afirmar que si el número de ecuaciones es menor o igual que la dimensión de la variedad, entonces la variedad no es vacía.

Abstract

The aim of this work is to study the dimension of the affine and projective algebraic varieties and its relation to the number of equations needed to describe the variety.

The dimension as a topological space of an algebraic affine variety coincides with the Krull dimension of its ring of regular functions and it is proved that if V is an irreducible affine algebraic variety of K^n , its dimension equals to the transcendence degree of its field of rational functions over K .

Following the model of linear algebra, the relationship between the dimension of an affine algebraic variety and the number of equations that define it is analyzed. For example, for an algebraically closed field K , in the case of an irreducible affine algebraic variety V , if f_1, \dots, f_r are regular functions on V and $Z(f_1, \dots, f_r) \neq \emptyset$, then all irreducible components of $Z(f_1, \dots, f_r)$ have dimension $\geq \dim V - r$; thus, $\dim Z(f_1, \dots, f_r) \geq \dim V - r$. For $r = 1$, if f_1 is not zero or a unit, we have equality.

The results for affine algebraic varieties extend to projective algebraic varieties and we can also affirm, in favorable cases, that the varieties obtained are not empty.

Introducción

El tamaño de las variedades algebraicas afines o proyectivas se mide asignándoles una dimensión. Los puntos, las curvas y las superficies son variedades algebraicas de dimensión 0, 1 y 2, respectivamente. El concepto de dimensión es el primer invariante que se asocia a una variedad algebraica. En este trabajo damos la definición topológica de dimensión de una variedad algebraica, que es muy natural pero no siempre fácil de utilizar, y que coincide con la dimensión de Krull del anillo de funciones regulares de la variedad. En el caso de variedades algebraicas afines irreducibles probamos que la dimensión de la variedad coincide con el grado de trascendencia de su cuerpo de funciones racionales; a partir de esta última caracterización de la dimensión vamos a obtener propiedades sobre la dimensión de las variedades algebraicas afines y proyectivas y su relación con el número de ecuaciones que las definen.

El método de demostración utilizado en este trabajo para el estudio de la dimensión de una variedad algebraica y el número de ecuaciones que la definen es geométrico y está estrechamente relacionado con la teoría de ideales y el número de generadores de un ideal. Los resultados obtenidos sobre el número de ecuaciones de una variedad se pueden trasladar a K -álgebras finitamente generadas que sean un dominio, para obtener teoremas como el teorema del ideal principal de Krull o el teorema del ideal principal de Krull generalizado. Estos dos teoremas de álgebra conmutativa son ciertos en anillos noetherianos y son complicados de probar con métodos algebraicos.

En el capítulo 1, dada una extensión de cuerpos E/K se estudian los conceptos de elementos algebraicamente independientes y de base de trascendencia y se prueba que toda extensión de cuerpos tiene una base de trascendencia; en particular si la extensión es finitamente generada entonces tiene una base de trascendencia finita. Se prueba también que si una extensión E/K tiene una base de trascendencia finita entonces cualquier otra base de trascendencia es finita y tiene el mismo número de elementos; este número se denomina grado de trascendencia E sobre K y lo denotaremos por $\text{tr deg}_K(E)$.

Para las demostraciones de este capítulo hemos utilizado el libro de Lang [4] y hemos ampliado sus demostraciones utilizando a veces las notas del curso de Milne de teoría

de cuerpos [6] y desarrollando otras demostraciones que nos permitieron describir estos conceptos con claridad.

En el capítulo 2 estudiamos las propiedades más importantes de la localización de anillos y de extensiones de anillos enteras que necesitamos en el capítulo 5 para el estudio de la dimensión de las K -álgebras finitamente generadas, para un cuerpo K cualquiera. También probamos el lema de normalización de Noether que afirma que si $A = K[x_1, \dots, x_n]$ es una K -álgebra finitamente generada que es un dominio entero y el grado de trascendencia de $K(x_1, \dots, x_n)$ sobre K es d , entonces existen elementos $y_1, \dots, y_d \in A$ que son algebraicamente independientes sobre K y tales que A es entera sobre $K[y_1, \dots, y_d]$.

Para la realización del capítulo 2 se ha utilizado el libro de Atiyah [1] y las notas de álgebra conmutativa de Milne [5].

En los capítulos 3 y 4 se estudian algunos conceptos de variedades algebraicas afines y de variedades algebraicas proyectivas. Si $K[X_1, \dots, X_n]$ es el anillo de polinomios se define una variedad algebraica afín V de K^n como el conjunto de ceros de un conjunto finito de polinomios de $K[X_1, \dots, X_n]$. Las variedades algebraicas afines de K^n verifican los axiomas de los cerrados de una topología en K^n que se llama topología de Zariski. Con esta topología toda variedad algebraica afín V no vacía se puede escribir de forma única (salvo permutación) como $V = V_1 \cup \dots \cup V_r$, donde V_i es una variedad algebraica afín irreducible y $V_i \not\subset V_j$, para $i \neq j$. Los conjuntos V_i se dice que son las componentes irreducibles de V .

Si V es una variedad algebraica afín, se llama anillo de funciones regulares o polinómicas en V y se denota por $\Gamma(V)$ al conjunto de aplicaciones $f: V \rightarrow K$ tales que existe un polinomio $F \in K[X_1, \dots, X_n]$ tal que $f(P) = F(P)$, para cada $P \in V$; si V es irreducible, entonces $\Gamma(V)$ es una K -álgebra finitamente generada que es un dominio entero y su cuerpo de fracciones, que se denota por $K(V)$, se llama cuerpo de funciones racionales. Si V y W son variedades algebraicas afines y $W \subset V$, entonces W se puede escribir como el conjunto de ceros de un conjunto finito de funciones regulares en V , es decir $W = Z(f_1, \dots, f_r)$ donde $f_i \in \Gamma(V)$, para $i = 1, \dots, r$. Si el cuerpo K es algebraicamente cerrado, el teorema de los ceros de Hilbert permite establecer una biyección decreciente entre el conjunto de ideales radicales de $\Gamma(V)$ y el conjunto de variedades algebraicas de K^n contenidas en V ; esta biyección establece un diccionario álgebra-geométrico entre estos dos conjuntos, donde los ideales primos de $\Gamma(V)$ corresponden a las variedades algebraicas irreducibles contenidas en V , los ideales maximales de $\Gamma(V)$ a los conjuntos con un solo punto de V y los ideales primos minimales de $\Gamma(V)$ a las componentes irreducibles de V .

Una variedad algebraica proyectiva de $\mathbb{P}^n(K)$ es el conjunto de ceros de un conjunto finito de polinomios homogéneos de $K[X_0, \dots, X_n]$. Las variedades algebraicas proyectivas

son los cerrados de una topología en $\mathbb{P}^n(K)$ llamada topología de Zariski. Igual que en el caso afín, toda variedad algebraica proyectiva es unión de sus componentes irreducibles. Si V es una variedad algebraica proyectiva, el cono de V es la variedad algebraica afín $C(V) = \{(x_0, \dots, x_n) \in K^{n+1} \mid (x_0 : \dots : x_n) \in V\} \cap \{(0, \dots, 0)\}$. El concepto de cono permite relacionar un problema proyectivo con su problema análogo afín.

Para la elaboración de los capítulos 3 y 4 hemos utilizado fundamentalmente el libro de Fulton [2] y el libro de Perrin [8].

El capítulo 5 se dedica al estudio de la dimensión de las variedades algebraicas afines. La dimensión de un espacio topológico X es el supremo de las longitudes de todas las cadenas

$$X_0 \subsetneq X_1 \subsetneq \dots \subsetneq X_n$$

de cerrados irreducibles de X . La dimensión de Krull de un anillo es el supremo de las longitudes de las cadenas de ideales primos de A y como consecuencia de la biyección decreciente entre cerrados irreducibles de V e ideales primos de $\Gamma(V)$, la dimensión de una variedad algebraica afín coincide con la dimensión de Krull de su anillo de funciones regulares.

Un teorema muy importante en este capítulo y que utilizaremos además en el estudio del número de ecuaciones de una variedad es el siguiente: si V es una variedad algebraica afín irreducible de K^n y $f \in \Gamma(V)$, $f \neq 0$ es tal que f no es una unidad de $\Gamma(V)$, y \mathfrak{p} es un ideal primo de $\Gamma(V)$ minimal entre los ideales primos de $\Gamma(V)$ que contienen a $\langle f \rangle$, se tiene

$$\text{tr deg}_K \Gamma(V)/\mathfrak{p} = \text{tr deg}_K K(V) - 1.$$

donde $\text{tr deg}_K \Gamma(V)/\mathfrak{p}$ es el grado de trascendencia del cuerpo de fracciones de $\Gamma(V)/\mathfrak{p}$ sobre K . Este resultado es un resultado estándar en Algebra Commutativa válido para K -álgebras finitamente generadas que son un dominio entero (véase por ejemplo el libro de Kunz [3]). La demostración que se da aquí es bastante sencilla y geométrica y utiliza básicamente el lema de normalización de Noether y las propiedades de las normas de los elementos de una extensión de cuerpos. Esta prueba es de J. Tate. Como corolario se obtiene que si V es una variedad algebraica irreducible de K^n y \mathfrak{p} es un ideal primo minimal de $\Gamma(V)$, $\mathfrak{p} \neq \{0\}$, entonces

$$\text{tr deg}_K \Gamma(V)/\mathfrak{p} = \text{tr deg}_K K(V) - 1,$$

y aplicando este último resultado queda probado el teorema fundamental de este capítulo, que afirma que si V es una variedad algebraica afín irreducible de K^n entonces la dimensión de V coincide con el grado de trascendencia de la extensión $K(V)/K$; en particular, la dimensión de una variedad algebraica afín es finita.

Para el desarrollo del capítulo 5 hemos utilizado fundamentalmente las notas de Milne de álgebra conmutativa [5].

En el capítulo 6 se analiza el número de ecuaciones de una variedad algebraica afín. Sabemos que una variedad lineal no vacía de un espacio afín de dimensión n que se describe por un sistema de ecuaciones lineales de rango r tiene dimensión $n - r$ y que cualquier variedad lineal de dimensión d se puede describir por $n - d$ ecuaciones. Para variedades algebraicas los conceptos correspondientes son más difíciles de probar y en general no tenemos estas igualdades, pero tenemos aproximaciones.

En el caso de una variedad lineal, su dimensión como espacio topológico coincide con su dimensión como variedad lineal, es decir con la dimensión de su subespacio dirección y se puede calcular su dimensión de la forma usual conocidas sus ecuaciones lineales.

Se comprueba que si V es una variedad algebraica afín irreducible de dimensión n y $f \in \Gamma(V)$, $f \neq 0$ y no es una unidad, entonces las componentes irreducibles de $Z(f)$ tienen dimensión $n - 1$, luego $\dim Z(f) = n - 1$. La traducción de este resultado a álgebra conmutativa es el teorema del ideal principal de Krull. A partir de este teorema, mediante un razonamiento por inducción, se prueba que si V es una variedad algebraica afín irreducible de dimensión n , $f_1, \dots, f_r \in \Gamma(V)$ y W es una componente irreducible de $Z(f_1, \dots, f_r)$, entonces $\dim W \geq n - r$. Así, cuando $Z(f_1, \dots, f_r) \neq \emptyset$, $\dim Z(f_1, \dots, f_r) \geq n - r$. Este resultado corresponde en álgebra conmutativa al teorema de ideal de Krull generalizado. Recíprocamente, si $\Gamma(V)$ es un anillo factorial y W es una subvariedad de V , $\dim W = n - 1$, entonces existe $f \in \Gamma(V)$ tal que $W = Z(f)$. En el caso general solo tenemos el siguiente resultado: si V una variedad algebraica afín irreducible de dimensión n y W es una subvariedad de algebraica afín irreducible de dimensión $n - r \geq 1$, entonces existen $f_1, \dots, f_r \in \Gamma(V)$ tales que W es una componente irreducible de $Z(f_1, \dots, f_r)$ y todas las componentes irreducibles de $Z(f_1, \dots, f_r)$ son de dimensión $n - r$.

Es conocido que en general, una variedad algebraica afín de K^n no se puede describir mediante $n - \dim V$ ecuaciones. Las variedades algebraicas V de K^n que se pueden describir por $n - \dim V$ ecuaciones se dice que son variedades intersección completa. El capítulo V del libro de Kunz [3] estudia cuando una variedad algebraica es intersección completa.

En el capítulo 7 se prueban para variedades algebraicas proyectivas resultados similares a los obtenidos para variedades algebraicas afines. En el caso de una variedad lineal proyectiva, su dimensión como espacio topológico coincide con su dimensión como variedad lineal proyectiva y por tanto se puede calcular su dimensión de la forma usual, conocidas sus ecuaciones lineales homogéneas. Para probar los resultados similares a los del caso afín sobre el número de ecuaciones de una variedad algebraica proyectiva, utilizamos el concepto de cono de una variedad algebraica proyectiva. En el caso proyectivo se puede afirmar

además que si el número de ecuaciones es menor o igual que la dimensión de la variedad, entonces la variedad no es vacía.

Para la realización de los capítulos 6 y 7 hemos utilizado el libro de Perrin [8] y las notas del curso de geometría algebraica de Milne [7]. Tanto el libro de Perrin como las notas de Milne trabajan con variedades algebraicas más generales que son espacios anillados localmente isomorfos a variedades algebraicas afines. En nuestras demostraciones no hemos utilizado los conceptos relativos a teoría de haces.

Agradecimientos

Muchas gracias a mi tutora María Jesús Vale Gonsalves por ayudarme en todo momento durante la realización de este trabajo, y a mis padres por haberme dado la posibilidad de estudiar esta carrera.

Capítulo 1

Extensiones trascendentes

Si K es un cuerpo denotaremos por $K[X_1, \dots, X_n]$, el anillo de polinomios en las variables X_1, \dots, X_n , sobre K . Dada una extensión de cuerpos E/K vamos a definir el concepto de elementos algebraicamente independientes sobre K , de base de trascendencia de E sobre K y probar que si $E = K(\Gamma)$ entonces existe una base de trascendencia A de E/K tal que $A \subset \Gamma$; en particular si la extensión E/K es finitamente generada, entonces tiene una base de trascendencia finita. Definiremos también el concepto de grado de trascendencia de una extensión de cuerpos.

1.1. Extensiones de cuerpos

Definición 1.1. Un cuerpo E que contiene un cuerpo K se dice que es un cuerpo extensión de K , se denota por E/K y se dice que E/K es una extensión de cuerpos. Si E/K es una extensión de cuerpos, entonces E es un espacio vectorial sobre K y se llama grado de E sobre K a la dimensión de E como espacio vectorial sobre K ; el grado de la extensión E/K se denota por $[E : K]$.

Definición 1.2. Sea E/K una extensión de cuerpos y $S \subset E$. Se llama *subanillo* de E generado por K y S al menor subanillo de E que contiene a K y a S y que denotaremos por $K[S]$. Si $S = \{\alpha_1, \dots, \alpha_n\}$ denotaremos $K[S]$ por $K[\alpha_1, \dots, \alpha_n]$.

Definición 1.3. Sea A un anillo. Una A -álgebra es un anillo B junto con un homomorfismo de anillos $i_B : A \rightarrow B$. Si B y C son A -álgebras se dice que la aplicación $f : B \rightarrow C$ es un homomorfismo de A -álgebras, si f es un homomorfismo de anillos y $f(i_B(a)) = i_C(a)$.

Obsérvese que si B es una A -álgebra, entonces B es anillo y además un A -módulo con la operación $ab = i_B(a)b$, para cada $a \in A$ y $b \in B$; se dice B es un A -módulo *vía* i_B . Si $f : B \rightarrow C$ es un homomorfismo de A -álgebras, entonces f es un homomorfismo de anillos

y además de A -módulos, donde B es un A -módulo vía i_B y C es un A -módulo vía i_C , puesto que

$$f(ab) = f(i_B(a)b) = f(i_B(a))f(b) = i_C(a)f(b) = af(b).$$

Lema 1.4. *Sea E/K una extensión de cuerpos y $S \subset E$. El subanillo $K[S]$ es la intersección de todos los subanillos de E que contienen a K y a S y está formado por los elementos que se pueden expresar como sumas finitas de la forma*

$$\sum a_{i_1 \dots i_n} \alpha_1^{i_1} \dots \alpha_n^{i_n}, \quad a_{i_1 \dots i_n} \in K, \quad \alpha_1, \dots, \alpha_n \in S, \quad i_1, \dots, i_n \in \mathbb{N}$$

Por tanto, $K[\alpha_1, \dots, \alpha_n]$ está formado por los elementos de E que pueden expresarse como polinomios en los α_i con coeficientes en K . Esto quiere decir que el homomorfismo de K -álgebras

$$\begin{aligned} \varphi : K[X_1, \dots, X_n] &\rightarrow K[\alpha_1, \dots, \alpha_n] \\ F(X_1, \dots, X_n) &\rightsquigarrow F(\alpha_1, \dots, \alpha_n), \end{aligned}$$

es sobreyectivo.

Demostración. Sea R el conjunto formado por tales elementos. Claramente R es un subanillo de E que contiene a K y a S y que está contenido en todo subanillo que contiene a K y a R . Por tanto, $R = K[S]$. \square

Definición 1.5. Un anillo A es un dominio entero si no es el anillo cero y si $ab = 0$ en A , entonces $a = 0$ o $b = 0$.

Lema 1.6. *Sea R un dominio entero que contiene un cuerpo K como subanillo. Si R considerado como espacio vectorial sobre K tiene dimensión finita, entonces R es un cuerpo.*

Demostración. Sea $a \neq 0$ un elemento de R , veamos que tiene un inverso en R . Por ser R un dominio entero, la aplicación

$$\begin{aligned} \varphi_a : R &\rightarrow R \\ x &\rightsquigarrow ax, \end{aligned}$$

es una aplicación K -lineal que es inyectiva por ser R un dominio entero. Dado que R es un espacio vectorial de dimensión finita sobre K , φ_a es sobreyectiva. En particular, existe un elemento $b \in R$ tal que $ab = 1$. \square

Definición 1.7. Sea E/K una extensión de cuerpos y $S \subset E$. Se llama *subcuerpo* de E generado por K y S al menor subcuerpo de E que contiene a K y a S y que denotaremos por $K(S)$. Si $S = \{\alpha_1, \dots, \alpha_n\}$, denotaremos $K(S)$ por $K(\alpha_1, \dots, \alpha_n)$.

Lema 1.8. Si E/K es una extensión de cuerpos y $S \subset E$, el cuerpo $K(S)$ es la intersección de todos los subcuerpos de E que contienen a K y a S y está formado por los elementos de E que son producto de un elemento de $K[S]$ y el inverso de un elemento no nulo de $K[S]$; en particular expresaremos los elementos de $K(\alpha_1, \dots, \alpha_n)$ como cociente de dos polinomios en los α_i con coeficientes en K .

Demostración. El conjunto de elementos de E que son producto de un elemento de $K[S]$ y el inverso de un elemento no nulo de $K[S]$ es un cuerpo. En efecto, sean $F_1, F_2, G_1, G_2 \in K[S]$ y $G_1 \neq 0$ y $G_2 \neq 0$, se tiene

$$\begin{aligned} F_1 G_1^{-1} - F_2 G_2^{-1} &= (F_1 G_2 - F_2 G_1) (F_2 G_2)^{-1}, & (F_1 G_1^{-1}) (F_2 G_2^{-1}) &= (F_1 F_2) (G_1 G_2)^{-1} \\ (F_1 G_1^{-1})^{-1} &= G_1 F_1^{-1}. \end{aligned}$$

Además, es un subcuerpo de E que contiene a K y a S y que está contenido en todo subcuerpo de E que contiene a K y a S . \square

Observación 1.9. Sea E/K una extensión de cuerpos y $S \subset E$. Si $K[S]$ es un espacio vectorial sobre K de dimensión finita, entonces por el lema 1.6, $K[S]$ es un cuerpo y en este caso $K[S] = K(S)$.

Definición 1.10. Sea E/K una extensión de cuerpos. Se dice que E es de generación finita sobre K si existen elementos $\alpha_1, \dots, \alpha_n \in E$ tales que $E = K(\alpha_1, \dots, \alpha_n)$.

Definición 1.11. Sea E/K una extensión de cuerpos y sea $\alpha \in E$. Se dice que α es *algebraico* sobre K si el homomorfismo de K -álgebras

$$\begin{aligned} \varphi_\alpha: K[X] &\rightarrow E \\ F(X) &\rightsquigarrow F(\alpha) \end{aligned}$$

tiene núcleo distinto de $\{0\}$. Se dice que α es *trascendente* sobre K si φ_α es inyectivo. Si $\alpha \in E$ es trascendente sobre K entonces el homomorfismo φ_α se factoriza por $K[\alpha]$ y el homomorfismo inducido que denotaremos también por $\varphi_\alpha: K[X] \rightarrow K[\alpha]$ es un isomorfismo que se extiende a un isomorfismo de cuerpos $\overline{\varphi}_\alpha: K(X) \rightarrow K(\alpha)$, donde $K(X)$ es el cuerpo de fracciones de $K[X]$.

Ejemplos 1.12. Los números $i \in \mathbb{C}$ y $\sqrt{2} \in \mathbb{R}$ son algebraicos sobre \mathbb{Q} . Liouville demostró en 1844 que e es trascendente sobre \mathbb{Q} . Lindemann demostró en 1882 que π es trascendente sobre \mathbb{Q} .

Definición 1.13. Se dice que la extensión de cuerpos E/K es finita si E es un espacio vectorial de dimensión finita sobre K . Se llama grado de la extensión finita E/K , y se denota por $[E : K]$, a la dimensión de E como espacio vectorial sobre K .

Definición 1.14. Sea E/K una extensión de cuerpos y sea α un elemento algebraico sobre K . Se llama polinomio irreducible de α sobre K al polinomio con coeficientes en K mónico que genera el núcleo de φ_α ; lo denotaremos por $\text{Irr}(\alpha, K, X)$.

Dado que el núcleo de φ_α es un ideal primo, $\text{Irr}(\alpha, K, X)$ es un polinomio irreducible. Además, $K[\alpha]$ es un cuerpo y entonces $K[\alpha] = K(\alpha)$ y se tiene que $[K(\alpha) : K]$ es igual al grado del polinomio $\text{Irr}(\alpha, K, X)$.

Definición 1.15. Se dice que la extensión de cuerpos E/K es algebraica si todo elemento de E es algebraico sobre K . Se dice que E/K es trascendente si existe un elemento en E que es trascendente sobre K .

Proposición 1.16. Si $E = K(\alpha_1, \dots, \alpha_n)$ y $\alpha_1, \dots, \alpha_n$ son algebraicos sobre K , entonces E/K es finita.

Proposición 1.17. Una extensión de cuerpos E/K es finita si, y solo si, E/K es algebraica y E es de generación finita sobre K .

Proposición 1.18. Sea E/F y F/K extensiones de cuerpos. Se tiene E/K es algebraica si, y solo si, E/F es algebraica y F/K es algebraica.

La extensión \mathbb{C}/\mathbb{R} es algebraica, puesto que $\dim_{\mathbb{R}} \mathbb{C} = 2$; además $\mathbb{C} = \mathbb{R}[i] = \mathbb{R}(i)$. La extensión \mathbb{C}/\mathbb{Q} es trascendente.

Definición 1.19. Si $A \in M_n(K)$ se llama polinomio característico de A y se denota por $P_A(X)$ al polinomio $\det(A - XI)$. Si V es un espacio vectorial de dimensión finita sobre el cuerpo K y f es un endomorfismo de V , se llama polinomio característico de f al polinomio característico de la matriz asociada a f respecto a una base cualquiera de V .

El polinomio característico del endomorfismo f de V no depende de la base considerada y el coeficiente de grado cero del polinomio característico de f es el determinante de f .

Definición 1.20. Sea E/K una extensión de cuerpos finita de grado n . Un elemento $\alpha \in E$ define una aplicación K -lineal

$$\begin{aligned} \alpha 1_E: E &\longrightarrow E \\ x &\rightsquigarrow \alpha x, \end{aligned}$$

y definimos la norma de α como el determinante de la aplicación $\alpha 1_E$. Se denota por $\text{Nm}_{E/K}(\alpha)$.

Ejemplos 1.21. (1) Consideremos la extensión de cuerpos \mathbb{C}/\mathbb{R} . Si $\alpha = a + bi$, entonces

$$\text{Nm}_{\mathbb{C}/\mathbb{R}}(\alpha) = a^2 + b^2 = |\alpha|^2.$$

(2) Si $a \in K$, entonces $\text{Nm}_{E/K}(a) = a^n$, siendo n el grado de la extensión E/K .

Proposición 1.22. *Sea E/K una extensión finita de cuerpos de grado n y sea $\alpha \in E$. Si $P_{\alpha 1_E}(X)$ es el polinomio característico de $\alpha 1_E$, entonces*

$$P_{\alpha 1_E}(X) = \text{Irr}(\alpha, K, X)^{[E:K(\alpha)]}.$$

Demostración. Dado que E/K es una extensión finita entonces es algebraica y de generación finita. Veamos que si $E = K(\alpha)$, entonces $P_{\alpha 1_E}(X) = \text{Irr}(\alpha, K, X)$. Consideremos el homomorfismo de anillos

$$\begin{aligned} \varphi: E &\rightarrow \text{End}_K(E) \\ x &\rightsquigarrow x 1_E \end{aligned}$$

El homomorfismo φ es inyectivo, puesto que si $(x 1_E)(y) = xy = 0$ para todo $y \in E$, entonces $x = x 1 = 0$. Por el teorema de Cayley Hamilton, que afirma que todo endomorfismo es raíz de su polinomio característico, $P_{\alpha 1_E}(\alpha 1_E) = 0$ y entonces dado que $\varphi(P_{\alpha 1_E}(\alpha)) = P_{\alpha 1_E}(\alpha 1_E) = 0$ y que φ es inyectivo $P_{\alpha 1_E}(\alpha) = 0$. Dado que el polinomio $\text{Irr}(\alpha, K, X)$ divide a $P_{\alpha 1_E}(X)$ y que $P_{\alpha 1_E}(X)$ es mónico y su grado coincide con la dimensión de E como espacio vectorial sobre K , entonces $P_{\alpha 1_E}(X) = \text{Irr}(\alpha, K, X)$.

Supongamos que $E \neq K(\alpha)$ y que $[K(\alpha) : K] = d$. Si $\{\beta_1, \dots, \beta_d\}$ es una base de $K(\alpha)$ como espacio vectorial sobre K y $\{\gamma_1, \dots, \gamma_m\}$ es una base de E como espacio vectorial sobre $K(\alpha)$, entonces $S = \{\beta_1 \gamma_1, \dots, \beta_d \gamma_1, \dots, \beta_1 \gamma_m, \dots, \beta_d \gamma_m\}$ es una base de E como espacio vectorial sobre K .

Si $\alpha \beta_i = \sum a_{ji} \beta_j$, para $i = 1, \dots, d$, entonces por el caso anterior el polinomio característico de $\alpha 1_{K(\alpha)}$ que es el polinomio característico de la matriz $A = (a_{ij}) \in M_d(K)$ coincide con el polinomio $\text{Irr}(\alpha, K, X)$. Dado que

$$\alpha \beta_i \gamma_k = \sum_{j=1}^d a_{ji} \beta_j \gamma_k$$

entonces la matriz asociada a $\alpha 1_E$ respecto a la base S es la matriz diagonal por bloques

$$\begin{pmatrix} A & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & A \end{pmatrix},$$

y entonces el polinomio característico de $\alpha 1_E$ es

$$P_{\alpha 1_E}(X) = \begin{vmatrix} A - XI & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & A - XI \end{vmatrix} = P_A(X)^m = \text{Irr}(\alpha, K, X)^m. \quad \square$$

Corolario 1.23. Sea E/K una extensión finita de cuerpos de grado n y sea $\alpha \in E$. Si $\text{Irr}(\alpha, K, X) = X^d + a_{d-1}X^{d-1} + \dots + a_0$, entonces d divide a n y si $n = dm$ entonces

$$\text{Nm}_{E/K}(\alpha) = a_0^m$$

Demostración. Sabemos por el teorema anterior que $P_{\alpha|E}(X) = (X^d + a_{d-1}X^{d-1} + \dots + a_0)^m = X^n + ma_{d-1}X^{n-1} + \dots + a_0^m$, con lo que $\text{Nm}_{E/K}(\alpha) = a_0^m$. \square

1.2. Independencia algebraica

Sea E/K una extensión de cuerpos.

Definición 1.24. Sean $\alpha_1, \dots, \alpha_n \in E$. Se dice que $\alpha_1, \dots, \alpha_n$ son *algebraicamente independientes* sobre K si el homomorfismo de K -álgebras

$$\begin{aligned} \varphi : K[X_1, \dots, X_n] &\rightarrow E \\ F(X_1, \dots, X_n) &\rightsquigarrow F(\alpha_1, \dots, \alpha_n) \end{aligned}$$

tiene núcleo $\{0\}$; en caso contrario se dice son *algebraicamente dependientes*. Es decir, $\alpha_1, \dots, \alpha_n$ son algebraicamente dependientes sobre K si existe un polinomio $F(X_1, \dots, X_n) \neq 0$ tal que $F(\alpha_1, \dots, \alpha_n) = 0$, y son algebraicamente independientes si

$$F(\alpha_1, \dots, \alpha_n) = 0 \Rightarrow F(X_1, \dots, X_n) = 0$$

Sea A un subconjunto de E . Se dice que A es algebraicamente independiente sobre K si todo subconjunto finito de A está formado por elementos algebraicamente independientes sobre K ; en caso contrario se dice que A es algebraicamente dependiente sobre K .

Observación 1.25. Si $\alpha_1, \dots, \alpha_n \in E$ son algebraicamente independientes, entonces la aplicación K -lineal inducida por φ y que denotaremos también por φ

$$\begin{aligned} \varphi : K[X_1, \dots, X_n] &\rightarrow K[\alpha_1, \dots, \alpha_n] \\ F(X_1, \dots, X_n) &\rightsquigarrow F(\alpha_1, \dots, \alpha_n) \end{aligned}$$

es un isomorfismo de K -álgebras. Este isomorfismo se extiende a un isomorfismo de cuerpos

$$\begin{aligned} \bar{\varphi} : K(X_1, \dots, X_n) &\rightarrow K(\alpha_1, \dots, \alpha_n) \\ X_i &\rightsquigarrow \alpha_i \end{aligned}$$

donde $K(X_1, \dots, X_n)$ es el cuerpo de fracciones $K[X_1, \dots, X_n]$.

Definición 1.26. Si $\alpha_1, \dots, \alpha_n$ son elementos de E algebraicamente independientes sobre K se dice que $K(\alpha_1, \dots, \alpha_n)/K$ es una extensión *trascendente pura*.

Ejemplos 1.27. (1) $\alpha \in E$ es algebraicamente independiente sobre K si, y solo si, es trascendente sobre K .

(2) $X_1, \dots, X_n \in K[X_1, \dots, X_n]$ son algebraicamente independientes sobre K .

(3) $\alpha \in E$ es algebraicamente dependiente sobre K si, y solo si, es α es algebraico sobre K .

Lema 1.28. Sea $\gamma \in E$ y $A \subset E$. Son equivalentes

(1) γ es algebraico sobre $K(A)$.

(2) Existen $\beta_1, \dots, \beta_n \in K(A)$ tales que $\gamma^n + \beta_{n-1}\gamma^{n-1} + \dots + \beta_0 = 0$.

(3) Existen $\beta_0, \dots, \beta_n \in K[A]$, no todos cero, tales que $\beta_n\gamma^n + \beta_{n-1}\gamma^{n-1} + \dots + \beta_0 = 0$.

(4) Existe un polinomio $F(X_1, \dots, X_m, Y) \in K[X_1, \dots, X_m, Y]$ y $\alpha_1, \dots, \alpha_m \in A$ tales que $F(\alpha_1, \dots, \alpha_m, Y) \neq 0$ y $F(\alpha_1, \dots, \alpha_m, \gamma) = 0$.

Demostración. (1) \Rightarrow (2) \Rightarrow (3) \Rightarrow (1) son triviales.

(4) \Rightarrow (3) Escribimos $F(X_1, \dots, X_m, Y)$ como un polinomio en Y con coeficientes en el anillo $K[X_1, \dots, X_m, Y]$, $F(X_1, \dots, X_m, Y) = \sum F_i(X_1, \dots, X_m)Y^i$. Se cumple (3) tomando $\beta_i = F_i(\alpha_1, \dots, \alpha_m)$.

(3) \Rightarrow (4) Cada β_i puede ser expresado como un polinomio en un número finito de elementos $\alpha_1, \dots, \alpha_m$ de A , es decir, $\beta_i = F_i(\alpha_1, \dots, \alpha_m)$, con $F_i \in K[X_1, \dots, X_m]$. Se cumple entonces (4) con $F = \sum F_i(X_1, \dots, X_m)Y^i$. \square

Definición 1.29. Sea $A \subset E$. Un conjunto $\Gamma \subset E$ se dice que es algebraico sobre $K(A)$ si cada elemento de Γ es algebraico sobre $K(A)$.

Lema 1.30. Si $E = K(\Gamma)$, A es un subconjunto de E y Γ es algebraico sobre $K(A)$, entonces la extensión $E/K(A)$ es algebraica.

Demostración. Si $b \in K(\Gamma)$, existen $\beta_1, \dots, \beta_n \in \Gamma$ tales que $b \in K(\beta_1, \dots, \beta_n)$ y por tanto $b \in K(A)(\beta_1, \dots, \beta_n)$. Dado que β_1, \dots, β_n son algebraicos sobre $K(A)$, por el lema 1.16, la extensión $K(A)(\beta_1, \dots, \beta_n)/K(A)$ es finita y por el lema 1.17, algebraica. Así, b es algebraico sobre $K(A)$. \square

Lema 1.31. (Transitividad de la dependencia algebraica) Sea E/K una extensión de cuerpos, C , S y A subconjuntos de E . Si C es algebraico sobre $K(S)$ y S es algebraico sobre $K(A)$ entonces C es algebraico sobre $K(A)$.

Demostración. Por el lema 1.30, las extensiones $K(A \cup S \cup C)/K(A \cup S)$ y $K(A \cup S)/K(A)$ son algebraicas. Por la proposición 1.18, $K(A \cup S \cup C)/K(A)$ es algebraica. \square

Lema 1.32. *Sea $A \subset E$ y $\beta \in E$. Si A es algebraicamente independiente sobre K y $A \cup \{\beta\}$ es algebraicamente dependiente sobre K , entonces β es algebraico sobre $K(A)$.*

Demostración. Tenemos por hipótesis que existe un polinomio no nulo $F(X_1, \dots, X_n, Y) \in K[X_1, \dots, X_n, Y]$ tal que $F(\alpha_1, \dots, \alpha_n, \beta) = 0$, para ciertos $\alpha_1, \dots, \alpha_n \in A$ distintos. Por ser A algebraicamente independiente sobre K , en el polinomio F aparece la variable Y , por lo que podemos escribir

$$F = a_m Y^m + a_{m-1} Y^{m-1} + \dots + a_0, \quad a_i \in K[X_1, \dots, X_n], \quad a_m \neq 0, \quad m \geq 1.$$

Puesto que $a_m \neq 0$ y los α_i son algebraicamente independientes, $a_m(\alpha_1, \dots, \alpha_n) \neq 0$. Por ser β raíz del polinomio

$$a_m(\alpha_1, \dots, \alpha_n) Y^m + a_{m-1}(\alpha_1, \dots, \alpha_n) Y^{m-1} + \dots + a_0(\alpha_1, \dots, \alpha_n) = 0,$$

llegamos a que β es algebraico sobre $K(\alpha_1, \dots, \alpha_n) \subset K(A)$. \square

1.3. Bases de trascendencia

Sea E/K una extensión de cuerpos.

Definición 1.33. Una base de trascendencia de E sobre K es un conjunto $A \subset E$ algebraicamente independiente sobre K y tal que E es algebraico sobre $K(A)$.

Teorema 1.34. *Sea $\Gamma \subset E$, $E = K(\Gamma)$ y L es un subconjunto de Γ algebraicamente independiente. Existe una base de trascendencia A de E tal que $L \subset A \subset \Gamma$.*

Demostración. Sea

$$\Sigma = \{S \subset \Gamma \mid L \subset S \subset \Gamma, S \text{ es algebraicamente independiente sobre } K\}.$$

El conjunto Σ es no vacío ya que $L \in \Sigma$. Sea T un subconjunto de Σ totalmente ordenado con respecto a la relación de inclusión, y veamos que T está acotado superiormente. Si

$$C = \bigcup_{S \in T} S$$

entonces $C \in \Sigma$. En efecto, si C es algebraicamente dependiente existe $S' = \{\alpha_1, \dots, \alpha_n\} \subset C$, con S' algebraicamente dependiente. Sean $S_1, \dots, S_n \in T$ tales que $\alpha_1 \in S_1, \dots, \alpha_n \in S_n$. Dado que T está totalmente ordenado, existe $j \in \{1, \dots, n\}$ tal que $\alpha_1, \dots, \alpha_n \in S_j$,

luego $S' \subset S_j$ y entonces S' no puede ser algebraicamente dependiente. Por tanto, C es algebraicamente independiente. Además, $L \subset C$, y por tanto $C \in \Sigma$. Así, C es una cota superior de T . Por el lema de Zorn, existe un elemento $A \in \Sigma$ maximal.

Veamos ahora que A es una base de trascendencia de E sobre K . Tenemos que probar que $E/K(A)$ es una extensión algebraica. Sea $b \in \Gamma - A$, el conjunto $A \cup \{b\}$ contiene a L y está contenido en Γ . Dado que A es un elemento maximal de Σ , $A \cup \{b\}$ un subconjunto de E es algebraicamente dependiente sobre K . Por el lema 1.32, llegamos a que b es algebraico sobre $K(A)$. Por tanto, puesto que todo $b \in \Gamma$ es algebraico sobre $K(A)$, tenemos por el lema 1.30 que la extensión $E/K(A)$ es algebraica, y por tanto A es una base de trascendencia de E sobre K cumpliendo las condiciones del enunciado. \square

Corolario 1.35. *Sea $E = K(\Gamma)$. Existe una base de trascendencia de E sobre K contenida en Γ y si Γ es finito, entonces existe una base de trascendencia finita.*

Demostración. Basta tomar $L = \emptyset$. \square

Proposición 1.36. *Un subconjunto S de E es una base de trascendencia de E/K si, y solo si, S es un conjunto algebraicamente independiente sobre K maximal.*

Demostración. Sea S una base de trascendencia de E sobre K , y supongamos que existe un subconjunto $L \subset E$ algebraicamente independiente sobre K tal que $S \subsetneq L$. Supongamos que existe $b \in L$ tal que $b \notin S$. Por ser S una base de trascendencia de E sobre K , la extensión $E/K(S)$ es algebraica y entonces b es algebraico sobre $K(S)$. Por el lema 1.28, el conjunto $S \cup \{b\}$ es algebraicamente dependiente sobre K , lo que contradice que L es algebraicamente independiente sobre K . Por tanto $S = L$, con lo cual S es un subconjunto de E algebraicamente independiente sobre K maximal.

Recíprocamente, sea S un subconjunto de E algebraicamente independiente sobre K maximal, por la demostración del teorema 1.34 tomando $L = \emptyset$ y $\Gamma = E$, tenemos que S es base una de trascendencia de E sobre K . \square

Veremos en el próximo teorema que si una extensión tiene una base de trascendencia finita, entonces cualquier otra base de trascendencia es finita y tiene el mismo número de elementos.

Proposición 1.37. *Sea $B = \{\alpha_1, \dots, \alpha_n\}$ una base de trascendencia de E/K y $L = \{\beta_1, \dots, \beta_m\}$ un subconjunto de E algebraicamente independiente sobre K con $m \leq n$. Existe un subconjunto S de B tal que $L \sqcup S$ es una base de trascendencia de E/K .*

Demostración. Probaremos el resultado por inducción en m .

Para $m = 1$, $L = \{\beta_1\}$. Por ser B base de trascendencia de E sobre K , la extensión

$E/K(B)$ es algebraica y β_1 es algebraico sobre $K(B)$. Por tanto, existe un polinomio $F \in K[Y, X_1, \dots, X_n]$, $F \neq 0$, tal que $F(\beta_1, \alpha_1, \dots, \alpha_n) = 0$. Por ser β_1 trascendente sobre K en el polinomio F aparece necesariamente algún X_i , supongamos que es X_1 . Pongamos

$$F = \sum_{i=1}^s a_i X_1^i, \quad a_i \in K[Y, X_2, \dots, X_n]$$

Si existe $j \in \{1, \dots, s\}$ tal que $a_j(\beta_1, \alpha_2, \dots, \alpha_n) \neq 0$, entonces α_1 es algebraico sobre $K(\beta_1, \alpha_2, \dots, \alpha_n)$.

Si para todo $j \in \{1, \dots, s\}$ con $a_j \neq 0$, $a_j(\beta_1, \alpha_2, \dots, \alpha_n) = 0$, entonces $\{\beta_1, \alpha_2, \dots, \alpha_n\}$ es algebraicamente dependiente.

Sea $a_k \neq 0$ tal que $a_k(\beta_1, \alpha_2, \dots, \alpha_n) = 0$. Por ser β_1 trascendente sobre K , en a_k aparece algún X_i , por ejemplo X_2 . Razonando como antes, α_2 es algebraico sobre $K(\beta_1, \alpha_3, \dots, \alpha_n)$ y por tanto sobre $K(\beta_1, \alpha_1, \alpha_3, \dots, \alpha_n)$, o se tiene que $\{\beta_1, \alpha_3, \dots, \alpha_n\}$ es algebraicamente dependiente sobre K . Repitiendo si es necesario este proceso un número finito de pasos, se llega, ya que β_1 es trascendente sobre K , a que existe $j \in \{1, \dots, n\}$ tal que α_j es algebraico sobre $K(\beta_1, \alpha_1, \dots, \alpha_{j-1}, \alpha_{j+1}, \dots, \alpha_n)$.

Reordenando los elementos $\alpha_1, \dots, \alpha_n$ podemos suponer que $\alpha_j = \alpha_1$, y así α_1 es algebraico sobre $K(\beta_1, \alpha_2, \dots, \alpha_n)$. Se tiene así que E es algebraico sobre $K(\beta_1, \alpha_1, \dots, \alpha_n)$, que es a su vez algebraico sobre $K(\beta_1, \alpha_2, \dots, \alpha_n)$, y por la proposición 1.18, E es algebraico sobre $K(\beta_1, \alpha_2, \dots, \alpha_n)$.

Veamos ahora que el conjunto

$$B_1 = \{\beta_1, \alpha_2, \dots, \alpha_n\},$$

es una base de trascendencia de E sobre K . Si los elementos $\beta_1, \alpha_2, \dots, \alpha_n$ son algebraicamente dependientes por el lema 1.32, β_1 es algebraico sobre $K(\alpha_2, \dots, \alpha_n)$ y entonces $K(\beta_1, \alpha_2, \dots, \alpha_n)$ es algebraico sobre $K(\alpha_2, \dots, \alpha_n)$. Por la proposición 1.18, la extensión $K(\beta_1, \alpha_1, \dots, \alpha_n)/K(\alpha_2, \dots, \alpha_n)$ es algebraica y entonces α_1 es algebraico sobre $K(\alpha_2, \dots, \alpha_n)$, lo cual es una contradicción ya que $\{\alpha_1, \dots, \alpha_n\}$ es algebraicamente independiente sobre K .

Supongamos que el resultado es cierto para $m = r$, $1 < r \leq n - 1$. Reordenando $\alpha_1, \dots, \alpha_n$ podemos suponer, por hipótesis de inducción, que

$$B_r = \{\beta_1, \dots, \beta_r, \alpha_{r+1}, \dots, \alpha_n\}$$

es una base de trascendencia de E/K . Veamos que el resultado es cierto para $r + 1$.

Dado que β_{r+1} es algebraico sobre $K(\beta_1, \dots, \beta_r, \alpha_{r+1}, \dots, \alpha_n)$ existe un polinomio

$$G \in K[Y_1, \dots, Y_{r+1}, X_{r+1}, \dots, X_n], \quad G \neq 0$$

tal que $G(\beta_1, \dots, \beta_{r+1}, \alpha_{r+1}, \dots, \alpha_n) = 0$. Por ser $\{\beta_1, \dots, \beta_{r+1}\}$ algebraicamente independiente sobre K , en G aparece algún X_j , $j \in \{r+1, \dots, n\}$. Razonando como arriba y reordenando $\alpha_{r+1}, \dots, \alpha_n$, podemos suponer que α_{r+1} es algebraico sobre $K(\beta_1, \dots, \beta_{r+1}, \alpha_{r+2}, \dots, \alpha_n)$ y entonces por la proposición 1.18 la extensión

$$E/K(\beta_1, \dots, \beta_{r+1}, \alpha_{r+2}, \dots, \alpha_n)$$

es algebraica.

Veamos que $B_{r+1} = \{\beta_1, \dots, \beta_{r+1}, \alpha_{r+2}, \dots, \alpha_n\}$ es una base de trascendencia de E/K . Si $\{\beta_1, \dots, \beta_{r+1}, \alpha_{r+2}, \dots, \alpha_n\}$ fuese algebraicamente dependiente sobre K , por el lema 1.32, β_{r+1} es algebraico sobre $K(\beta_1, \dots, \beta_r, \alpha_{r+2}, \dots, \alpha_n)$. Dado que α_{r+1} es algebraico sobre

$$K(\beta_1, \dots, \beta_{r+1}, \alpha_{r+2}, \dots, \alpha_n)$$

y $K(\beta_1, \dots, \beta_{r+1}, \alpha_{r+2}, \dots, \alpha_n)$ es algebraico sobre $K(\beta_1, \dots, \beta_r, \alpha_{r+2}, \dots, \alpha_n)$, por el lema 1.31, α_{r+1} es algebraico sobre $K(\beta_1, \dots, \beta_r, \alpha_{r+2}, \dots, \alpha_n)$, lo que contradice que $\{\beta_1, \dots, \beta_r, \alpha_{r+1}, \dots, \alpha_n\}$ es algebraicamente independiente. Por tanto,

$$B_{r+1} = \{\beta_1, \dots, \beta_{r+1}, \alpha_{r+2}, \dots, \alpha_n\}$$

es una base de trascendencia de E sobre K . \square

Teorema 1.38. *Si una extensión de cuerpos E/K tiene una base de trascendencia finita, entonces cualquier otra base de trascendencia es finita y tiene el mismo número de elementos.*

Demostración. Sean $B = \{\alpha_1, \dots, \alpha_n\}$ y B' bases de trascendencia de E/K .

Si en B' hay n elementos distintos β_1, \dots, β_n , entonces por la proposición 1.37, $S = \{\beta_1, \dots, \beta_n\}$ es una base de trascendencia de E/K . Dado que $S \subset B'$ y S es un subconjunto de E algebraicamente independiente sobre K maximal, se tiene que $B' = S$. Así B' es finito y tiene n elementos.

Si B' tiene m elementos, $m < n$, entonces existe un subconjunto S de B con $n - m$ elementos tal que $B' \sqcup S$ es base de trascendencia de E/K . Dado que $B' \subset B' \sqcup S$ y B' es un subconjunto de E algebraicamente independiente maximal se llega a una contradicción. Por tanto $m = n$. \square

Observación 1.39. Se puede probar que dos bases de trascendencia (posiblemente infinitas) de E sobre K tienen el mismo cardinal.

Definición 1.40. Sea E/K una extensión de cuerpos. Se llama grado de trascendencia de E sobre K , y lo denotaremos por $\text{tr deg}_K(E)$, al cardinal de una base de trascendencia de E sobre K .

Por ejemplo, el grado de trascendencia de la extensión trascendente pura $K(X_1, \dots, X_n)$ sobre K es n .

Ejemplo 1.41. Sean $S_1 = X_1 + \dots + X_n$, $S_2 = \sum_{i < j} X_i X_j$, \dots , $S_n = X_1 \dots X_n$, los polinomios simétricos elementales sobre X_1, \dots, X_n . Dado que

$$F(X) = (X - X_1)(X - X_2) \dots (X - X_n) = X^n - S_1 X^{n-1} + S_2 X^{n-2} + \dots + (-1)^n S_n,$$

se tiene que $K(X_1, \dots, X_n)$ es una extensión algebraica de $K(S_1, \dots, S_n)$. Por el teorema 1.34, el conjunto $\{S_1, \dots, S_n\}$ contiene una base de trascendencia de $K(S_1, \dots, S_n)/K$. Dado que el grado de trascendencia de $K(X_1, \dots, X_n)$ sobre K es n , entonces $\{S_1, \dots, S_n\}$ es una base de trascendencia de $K(X_1, \dots, X_n)$ sobre K .

Capítulo 2

Dependencia entera

En este capítulo estudiaremos las propiedades más importantes de la localización de anillos y de dependencia entera; utilizaremos estas propiedades en el capítulo 5 para el estudio de la dimensión de las K -álgebras finitamente generadas que son dominios enteros.

2.1. Anillos de fracciones

Definición 2.1. Se dice que un subconjunto S de A es un subconjunto multiplicativamente cerrado de A si $1 \in S$ y S es cerrado para la multiplicación, es decir si $s_1, s_2 \in S$, entonces $s_1 s_2 \in S$.

Proposición 2.2. La relación \sim en $A \times S$ dada por

$$(a, s) \sim (b, t) \iff \exists u \in S \text{ tal que } (at - bs)u = 0,$$

es una relación de equivalencia.

Si denotamos por $\frac{a}{b}$ la clase de equivalencia de (a, s) y por $S^{-1}A$ el conjunto cociente $(A \times S)/\sim$, entonces $S^{-1}A$ es un anillo con las siguientes operaciones:

$$(a/s) + (b/t) = (at + bs)/st, \quad (a/s)(b/t) = ab/st.$$

La aplicación $f : A \rightarrow S^{-1}A$ dada por $f(a) = a/1$ es un homomorfismo de anillos que en general no es inyectivo. El anillo $S^{-1}(A)$ se llama el anillo de fracciones de A . Si A es un dominio entero, entonces $S = A - \{0\}$ es un subconjunto multiplicativamente cerrado de A . En este caso, $S^{-1}A$ es un cuerpo que se denomina *el cuerpo de fracciones* de A .

El anillo $S^{-1}A$ tiene la siguiente propiedad universal:

Proposición 2.3. Sea $g : A \rightarrow B$ un homomorfismo de anillos tal que $g(s)$ es una unidad en B para todo $s \in S$. Existe un único homomorfismo de anillos $h : S^{-1}(A) \rightarrow B$ tal que $g = h \circ f$.

Demostración. Comencemos viendo la unicidad de tal homomorfismo. Si h satisface dichas condiciones, entonces $h(a/1) = hf(a) = g(a)$ para todo $a \in A$ y si $s \in S$, $h(1/s) = h((s/1)^{-1}) = h(s/1)^{-1} = g(s)^{-1}$. Por tanto, $h(a/s) = h(a/1)h(1/s) = g(a)g(s)^{-1}$, con lo cual h está determinado de manera única por g .

Comprobemos ahora la existencia. Sea $h: S^{-1}A \rightarrow B$ la aplicación $h(a/s) = g(a)g(s)^{-1}$. Veamos que h está bien definida. En efecto, si $a/s = a'/s'$, existe $t \in S$ tal que $(as' - a's)t = 0$, por lo que $(g(a)g(s') - g(a')g(s))g(t) = 0$, y por ser $g(t)$ una unidad en B , llegamos a que $g(a)g(s') = g(a')g(s)$ y entonces $g(a)g(s)^{-1} = g(a')g(s')^{-1}$. Además, h es un homomorfismo de anillos y $h \circ f = g$. \square

Ejemplos 2.4. (1) Si \mathfrak{p} es un ideal primo de A , entonces $S = A - \mathfrak{p}$ es multiplicativamente cerrado. Denotaremos $S^{-1}A$ por $A_{\mathfrak{p}}$. Los elementos $\frac{a}{s}$ con $a \in A$ y $s \in S$ forman un ideal \mathfrak{m} de $A_{\mathfrak{p}}$. Además, $A_{\mathfrak{p}}$ es un anillo local con ideal maximal \mathfrak{m} . Para probar esto, es suficiente probar que los elementos de $A_{\mathfrak{p}} - \mathfrak{m}$ son unidades. Si $b/s \notin \mathfrak{m}$, entonces $b \notin \mathfrak{p}$ con lo que $b \in S$ y por tanto b/s es una unidad en $A_{\mathfrak{p}}$.

(2) $S^{-1}A = \{0\}$ si, y solo si $0 \in S$.

(3) Si $x \in A$ y $S = \{x^n\}_{n \geq 0}$, denotaremos $S^{-1}A$ por A_x .

Proposición 2.5. Sea A un anillo y $T \subset A$, denotaremos por $\langle T \rangle$ el ideal generado por T , es decir el menor ideal de A que contiene a T . Se tiene

$$\langle T \rangle = \left\{ \sum_{i=1}^n a_i x_i \mid a_i \in A, x_i \in T, n \in \mathbb{N} \right\}$$

Demostración. El conjunto $\{\sum_{i=1}^n a_i x_i \mid a_i \in A, x_i \in T, n \in \mathbb{N}\}$ es el menor ideal de A que contiene a T . \square

Si S es finito, entonces se dice que $\langle T \rangle$ está finitamente generado.

Definición 2.6. Sea $f: A \rightarrow B$ un homomorfismo de anillos. Se dice que un ideal \mathfrak{b} de B es un ideal extendido, si existe un ideal \mathfrak{a} de A tal que \mathfrak{b} es el ideal generado por $f(\mathfrak{a})$. Se dice que \mathfrak{b} es la extensión de \mathfrak{a} a B .

Sea $f: A \rightarrow S^{-1}A$, la aplicación dada por $f(a) = a/1$. Si \mathfrak{a} es un ideal de A , denotaremos su extensión a $S^{-1}A$ por $S^{-1}\mathfrak{a}$.

Proposición 2.7. Sea $f: A \rightarrow S^{-1}A$, la aplicación dada por $f(a) = a/1$. Se tiene

(1) Todo ideal de $S^{-1}A$ es un ideal extendido.

(2) $S^{-1}\mathfrak{a} = A$ si, y solo si, $\mathfrak{a} \cap S \neq \emptyset$.

- (3) Si \mathfrak{a} y \mathfrak{b} son ideales de A , entonces $S^{-1}(\mathfrak{a} \cap \mathfrak{b}) = S^{-1}\mathfrak{a} \cap S^{-1}\mathfrak{b}$.
- (4) Si \mathfrak{a} es un ideal de A , entonces los anillos $S^{-1}A/S^{-1}\mathfrak{a}$ y $\overline{S}^{-1}(A/\mathfrak{a})$ son isomorfos, siendo $\overline{S} = p(A)$, con $p: A \rightarrow A/\mathfrak{a}$, la aplicación dada por $p(a) = a + \mathfrak{a}$, para cada $a \in A$.
- (5) Los ideales primos de $S^{-1}A$ están en correspondencia biyectiva ($\mathfrak{p} \leftrightarrow S^{-1}\mathfrak{p}$) con los ideales primos de A que no cortan a S .

Demostración. (1) Sea \mathfrak{b} un ideal de $S^{-1}A$, $x/s \in \mathfrak{b}$, se tiene que $x/1 \in \mathfrak{b}$, con lo que x está en el ideal $f^{-1}(\mathfrak{b}) = \mathfrak{b}'$, y x/s está en el ideal $S^{-1}\mathfrak{b}'$. Llegamos por tanto a que $\mathfrak{b} \subset S^{-1}\mathfrak{b}'$, y como $S^{-1}\mathfrak{b}' \subset \mathfrak{b}$, tenemos que $S^{-1}\mathfrak{b}' = \mathfrak{b}$.

(2) y (3) son inmediatos.

(4) Es claro que \overline{S} es un subconjunto multiplicativo de A/\mathfrak{a} . Sea $g: S^{-1}A \rightarrow \overline{S}^{-1}(A/\mathfrak{a})$ la aplicación dada por $g(a/s) = (a + \mathfrak{a})/(s + \mathfrak{a})$, y veamos que está bien definida. Si $a/s, a'/s' \in S^{-1}A$ y $a/s = a'/s'$, existe $s'' \in S$ tal que $s''(as' - a's) = 0$. Aplicando p a esta identidad, llegamos a que

$$(s'' + \mathfrak{a})((a + \mathfrak{a})(s' + \mathfrak{a}) - (a' + \mathfrak{a})(s + \mathfrak{a})) = \mathfrak{a},$$

con lo que $(a + \mathfrak{a})/(s + \mathfrak{a}) = (a' + \mathfrak{a})/(s' + \mathfrak{a})$. Además, g es un homomorfismo de anillos suprayectivo. Para calcular su núcleo, sea $a/s \in \text{Ker } g$, luego $g(a/s) = (a + \mathfrak{a})/(s + \mathfrak{a}) = \mathfrak{a}/(1 + \mathfrak{a})$, con lo que existe un $s' + \mathfrak{a} \in \overline{S}$ tal que $(s' + \mathfrak{a})((a + \mathfrak{a})(1 + \mathfrak{a}) - (s + \mathfrak{a})\mathfrak{a}) = s'a + \mathfrak{a} = \mathfrak{a}$, y llegamos a que $s'a \in \mathfrak{a}$, con lo que $a/s = as'/ss' \in S^{-1}\mathfrak{a}$. Sea ahora $\alpha \in \mathfrak{a}$ y $\alpha/s \in S^{-1}\mathfrak{a}$, tenemos que $g(\alpha/s) = (\alpha + \mathfrak{a})/(s + \mathfrak{a}) = \mathfrak{a}/(s + \mathfrak{a})$, con lo que $\alpha/s \in \text{Ker } g$, y por tanto $\text{Ker } g = S^{-1}\mathfrak{a}$. Así,

$$S^{-1}A/\text{Ker } g = S^{-1}A/S^{-1}\mathfrak{a} \simeq g(S^{-1}A) = \overline{S}^{-1}(A/\mathfrak{a}).$$

(5) Sea \mathfrak{q} un ideal primo de $S^{-1}A$. El ideal $f^{-1}(\mathfrak{q})$ es un ideal primo de A . Veamos que $f^{-1}(\mathfrak{q}) \cap S = \emptyset$. En efecto, si $f^{-1}(\mathfrak{q}) \cap S \neq \emptyset$, existe $s \in S$ tal que $s \in f^{-1}(\mathfrak{q})$, con lo que $s/1 \in \mathfrak{q}$, pero entonces $s/s = 1 \in \mathfrak{q}$ y el ideal no sería primo. Además, por ser \mathfrak{q} un ideal extendido, $S^{-1}(f^{-1}(\mathfrak{q})) = \mathfrak{q}$.

Sea ahora \mathfrak{p} un ideal primo de A tal que $\mathfrak{p} \cap S \neq \emptyset$ y sea $p': A \rightarrow A/\mathfrak{p}$ la aplicación dada por $p'(a) = a + \mathfrak{p}$ y $\overline{S} = p'(S)$. El anillo A/\mathfrak{p} es un dominio entero. Por (2) tenemos un isomorfismo de anillos

$$S^{-1}A/S^{-1}\mathfrak{p} \simeq \overline{S}^{-1}(A/\mathfrak{p})$$

Dado que $\mathfrak{p} \cap S = \emptyset$, $\overline{S} \neq \mathfrak{p}$, y entonces $\overline{S}^{-1}(A/\mathfrak{p}) \neq 0$. Dado que el anillo A/\mathfrak{p} es un dominio entero, $\overline{S}^{-1}(A/\mathfrak{p})$ está contenido en el cuerpo de fracciones de A/\mathfrak{p} , de donde se sigue que

$S^{-1}A/S^{-1}\mathfrak{p}$ es un dominio. Por tanto, $S^{-1}\mathfrak{p}$ es un ideal primo de $S^{-1}(A)$. Claramente, $\mathfrak{p} \subset f^{-1}(S^{-1}\mathfrak{p})$. Veamos que $f^{-1}(S^{-1}\mathfrak{p}) \subset \mathfrak{p}$. Si $x \in f^{-1}(S^{-1}\mathfrak{p})$, entonces $x/1 \in S^{-1}\mathfrak{p}$, de donde se sigue que existen $a \in \mathfrak{p}$ y $s, s' \in S$ tales que $(xs - a)s' = 0$ y entonces $xss' = as' \in \mathfrak{p}$. Dado que $S \cap \mathfrak{p} = \emptyset$ se tiene que $x \in \mathfrak{p}$. \square

Proposición 2.8. *Sea A un anillo y $h \in A$, los anillos $A[X]/\langle 1 - hX \rangle$ y A_h son isomorfos.*

Demostración. Si $h = 0$ entonces los dos anillos son cero. Supongamos $h \neq 0$, y consideremos la aplicación

$$\begin{aligned} \phi: A[X] &\longrightarrow A_h \\ \sum a_i X^i &\rightsquigarrow \sum_i a_i/h^i \end{aligned}$$

que claramente es un homomorfismo de anillos. Además, $\phi(1 - hX) = 1 - (h/1)(1/h) = 1 - 1 = 0$, con lo que $\phi(\langle 1 - hX \rangle) = 0$, con lo que tenemos el homomorfismo de anillos

$$\begin{aligned} \bar{\phi}: A[X]/\langle 1 - hX \rangle &\longrightarrow A_h \\ \sum a_i X^i + \langle 1 - hX \rangle &\rightsquigarrow \sum_i a_i/h^i. \end{aligned}$$

Consideramos ahora el homomorfismo de anillos $g: A \rightarrow A[X]/\langle 1 - hX \rangle$ definido por $g(a) = a + \langle 1 - hX \rangle$, y veamos que $g(h)$ es una unidad de $A[X]/\langle 1 - hX \rangle$. Puesto que $1 - hX \in \langle 1 - hX \rangle$, aplicando g llegamos a que $1 + \langle 1 - hX \rangle - (h + \langle 1 - hX \rangle)(X + \langle 1 - hX \rangle) = \langle 1 - hX \rangle$, con lo que $X + \langle 1 - hX \rangle = (h + \langle 1 - hX \rangle)^{-1}$. Por tanto, $g(h^n)$ es una unidad de $A[X]/\langle 1 - hX \rangle$ para todo $n \geq 0$ y por la proposición 2.3, existe un único homomorfismo de anillos $\Psi: A_h \rightarrow A[X]/\langle 1 - hX \rangle$ tal que $\Psi \circ f = g$ y que está dado por $\Psi(a/h^r) = g(a)g(h^r)^{-1} = g(a)(g(h)^{-1})^r = (a + \langle 1 - hX \rangle)(X^r + \langle 1 - hX \rangle) = aX^r + \langle 1 - hX \rangle$.

Veamos por último que Ψ es la inversa de $\bar{\phi}$. Si $\sum_i a_i X^i + \langle 1 - hX \rangle \in A[X]/\langle 1 - hX \rangle$, entonces $(\Psi \circ \bar{\phi})(\sum_i a_i X^i + \langle 1 - hX \rangle) = \Psi(\sum_i a_i/h^i) = \sum_i \Psi(a_i/h^i) = \sum_i a_i X^i + \langle 1 - hX \rangle$. Si $a/h^r \in A_h$, $(\bar{\phi} \circ \Psi)(a/h^r) = \bar{\phi}(aX^r + \langle 1 - hX \rangle) = a/h^r$. Por tanto, $\bar{\phi}$ es un isomorfismo. \square

2.2. Dependencia entera

Definición 2.9. Sea B un anillo conmutativo y unitario y A un subanillo de B . Un elemento x de B se dice que es entero sobre A si x es raíz de un polinomio mónico con coeficientes en A , es decir si satisface una ecuación de la forma

$$x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$$

donde los a_i son elementos de A . Si todo elemento de B es entero sobre A , entonces se dice que B es entero sobre A .

Todo elemento de A es entero sobre A por ser raíz del polinomio $X - a$.

Definición 2.10. Se dice que un homomorfismo de anillos $f: A \rightarrow B$ es finito o que B es una A -álgebra finita si B es un A -módulo finitamente generado, siendo B un A -módulo vía f , es decir si existen elementos x_1, \dots, x_m en B tales que cada elemento de B es de la forma $\sum_{i=1}^r a_i x_i$ donde $a_i \in A$, para $i = 1, \dots, n$; escribiremos $B = \langle x_1, \dots, x_m \rangle$. Se dice que el homomorfismo de anillos $f: A \rightarrow B$ es de tipo finito o que B es una A -álgebra finitamente generada, si existen elementos x_1, \dots, x_n , en B tales que cada elemento de B puede escribirse como un polinomio en x_1, \dots, x_n con coeficientes en $f(A)$ y se denota por $f(A)[x_1, \dots, x_n]$ o por $A[x_1, \dots, x_n]$.

Definición 2.11. Sea M un A -módulo. Se llama anulador de M al siguiente ideal de A

$$\text{Ann}_A M = \{a \in A \mid aM = 0\}.$$

Se dice que un A -módulo M es fiel si $\text{Ann} M = 0$.

Proposición 2.12. *Sea A un subanillo de B . Las siguientes proposiciones son equivalentes:*

- (1) $x \in B$ es entero sobre A .
- (2) $A[x]$ es un A -módulo finitamente generado.
- (3) $A[x]$ está contenido en un subanillo C de B tal que C es un A -módulo finitamente generado.
- (4) Existe un $A[x]$ -módulo fiel M que es un A -módulo finitamente generado.

Demostración. (1) \Rightarrow (2) Dado que $x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$, tenemos que $x^n = -(a_1x^{n-1} + \dots + a_1x + a_0) \in \langle 1, x, \dots, x^{n-1} \rangle$. Veamos que $x^{n+r} \in \langle 1, x, \dots, x^{n-1} \rangle$, para todo $r \geq 0$. Razonaremos por inducción sobre r . Para $r = 0$ está probado. Supongamos el resultado cierto para $r - 1 \geq 0$. Existen $c_0, c_1, \dots, c_{n-1} \in B$ tales que,

$$x^{n+r-1} = c_0 + c_1x + \dots + c_{n-1}x^{n-1},$$

y entonces

$$\begin{aligned} x^{n+r} &= c_0x + c_1x^2 + \dots + c_{n-2}x^{n-1} + c_{n-1}x^n \\ &= c_0x + c_1x^2 + \dots + c_{n-2}x^{n-1} + c_{n-1}(-(a_1x^{n-1} + \dots + a_1x + a_0)) \in \langle 1, x, \dots, x^{n-1} \rangle. \end{aligned}$$

Por tanto, $A[x]$ está generado como A -módulo por $1, x, \dots, x^{n-1}$.

- (2) \Rightarrow (3) Basta con tomar $C = A[x]$.

(3) \Rightarrow (4) Tomamos $M = C$, que es un $A[x]$ -módulo fiel puesto que si $y \in A[x]$, $yC = 0$ entonces $y1 = 0$.

(4) \Rightarrow (1) Supongamos que M está generado por $m_1, \dots, m_n \in M$, existen entonces $a_{ij} \in A$, $i, j = 1, \dots, n$, tales que $xm_i = \sum_{j=1}^n a_{ij}m_j$. Si $b_{ij} = a_{ij} - x\delta_{ij}$, siendo δ_{ij} las deltas de Kronecker, entonces $\sum_{j=1}^n b_{ij}m_j = 0$, para $i, j = 1, \dots, n$. Sea

$$N = (b_{ij}) = \begin{pmatrix} a_{11} - x & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} - x \end{pmatrix} \in M_n(A[x]).$$

Se tiene

$$N \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Multiplicando por la izquierda por la matriz transpuesta de la adjunta de N se tiene:

$$(\det N) m_i = 0, \quad i = 1, \dots, n$$

Así, $(\det N)M = 0$ y entonces $\det N \in \text{Ann}_{A[x]}M = \{0\}$. Desarrollando $\det(N)$ se obtiene un polinomio mónico en x con coeficientes en A , y por tanto x es entero sobre A . \square

Corolario 2.13. Sean x_i , $i = 1, \dots, n$, elementos de B cada uno de ellos entero sobre A . El anillo $A[x_1, \dots, x_n]$ es un A -módulo finitamente generado.

Demostración. Lo probaremos por inducción en n . El caso $n = 1$ se probó en la proposición anterior. Supongamos $n > 1$ y sea $A_r = A[x_1, \dots, x_r]$. Por hipótesis de inducción, A_{n-1} es un A -módulo finitamente generado. Dado que x_n es entero sobre A , lo es sobre A_{n-1} y por la proposición anterior se tiene que $A_n = A_{n-1}[x_n]$ es un A_{n-1} -módulo finitamente generado y entonces A_n es un A -módulo finitamente generado. \square

Corolario 2.14. El conjunto C de elementos de B que son enteros sobre A es un subanillo de B que contiene a A .

Demostración. Sean $x, y \in C$, por el corolario anterior $A[x, y]$ es un A -módulo finitamente generado, y por la proposición 2.12, $x \pm y$ y xy son enteros sobre A . \square

Definición 2.15. Se llama clausura íntegra de A en B al conjunto de elementos de B que son enteros sobre A . Si $C = A$, se dice que A es íntegramente cerrado en B . Si $C = B$ se dice que B es entero sobre A . Se dice que un dominio es íntegramente cerrado si es íntegramente cerrado en su cuerpo de fracciones.

Corolario 2.16. *Sea A un subanillo de B . Si $x_1, \dots, x_n \in B$ son enteros sobre A , entonces $A[x_1, \dots, x_n]$ es entero sobre A .*

Demostración. Por el corolario 2.13 $A[x_1, \dots, x_n]$ es un A -módulo finitamente generado. Si $x \in A[x_1, \dots, x_n]$, entonces $A[x] \subset A[x_1, \dots, x_n]$ y por la proposición 2.12 (3), x es entero sobre A . \square

Proposición 2.17. *Todo anillo factorial es íntegramente cerrado.*

Demostración. Sea A un anillo factorial y $a/s \in S^{-1}A$, $S = A - \{0\}$, a y s sin factores irreducibles comunes. Si a/s es entero sobre A , existe un polinomio mónico $F = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in A[x]$, tal que $F(a/s) = 0$. Se tiene

$$a^n + a_{n-1}a^{n-1}s + \dots + a_0s^n = 0.$$

Por tanto, $a^n = -(a_{n-1}a^{n-1}s + \dots + a_0s^n)$, y entonces s divide a a^n . Dado que A es un anillo factorial y A y B no tienen factores irreducibles comunes, entonces s es una unidad en A . Así, $a/s = as^{-1}/1 \in A$. \square

En particular, todo cuerpo, el anillo de los enteros \mathbb{Z} y el anillo de polinomios con coeficientes en un anillo factorial son dominios íntegramente cerrados.

Definición 2.18. Sea $i_B: A \rightarrow B$ un homomorfismo de anillos. Se dice que B es una A -álgebra entera si B es entero sobre $i_B(A)$.

Proposición 2.19. *Una A -álgebra B es finita si y sólo si B es entera sobre A y es una A -álgebra finitamente generada.*

Demostración. Si B es un A -módulo finitamente generado, existen $x_i \in B$, $i = 1, \dots, m$, tales que $B = \langle x_1, \dots, x_m \rangle$ y dado que B es una A -álgebra se tiene que $B = A[x_1, \dots, x_m]$. Si $x \in B$, entonces $A[x] \subset B$ y dado que B es un anillo y un A -módulo de generación finita, por 2.12 (3), x es entero sobre A .

Recíprocamente si $B = A[x_1, \dots, x_m]$ es una A -álgebra entera sobre A , entonces por el corolario 2.13 B es un A -módulo finitamente generado. \square

Lema 2.20. *Sea $f: A \rightarrow B$ un homomorfismo de anillos y M un B -módulo finitamente generado. Consideremos M y B como A -módulos vía f . Si B es un A -módulo finitamente generado, entonces M es un A -módulo finitamente generado.*

Demostración. Si M está generado por m_1, \dots, m_r como B -módulo y B está generado por b_1, \dots, b_s como A -módulo, entonces los elementos $m_i b_j$ para $i = 1, \dots, r$ y $j = 1, \dots, s$ generan M como A -módulo. \square

Proposición 2.21. (Transitividad de la dependencia entera) *Si $A \subset B \subset C$ son anillos y si B es entero sobre A y C es entero sobre B , entonces C es entero sobre A .*

Demostración. Si $x \in C$, por ser C entero sobre B se tiene una ecuación $x^n + b_{n-1}x^{n-1} + \dots + b_0 = 0$, con $b_i \in B$, para $i = 0, \dots, n-1$, y entonces x es entero sobre el anillo $B' = A[b_0, \dots, b_{n-1}]$. Por el corolario 2.13, B' es un A -módulo finitamente generado. Dado que x es entero sobre B' , el anillo $B'[x]$ es un B' -módulo finitamente generado. Por el lema 2.20, $B'[x]$ es un A -módulo finitamente generado y por la proposición 2.12 (3), x es entero sobre A . □

Proposición 2.22. *Sean $A \subset B$ anillos, B entero sobre A*

- (1) *Si \mathfrak{b} es un ideal de B y $\mathfrak{a} = A \cap \mathfrak{b}$, entonces B/\mathfrak{b} es entero sobre A/\mathfrak{a} .*
- (2) *Si S es un subconjunto multiplicativo de A , entonces $S^{-1}B$ es entero sobre $S^{-1}A$.*

Demostración. (1) El anillo B/\mathfrak{b} es un A/\mathfrak{a} -módulo vía el homomorfismo de anillos $g: A/\mathfrak{a} \rightarrow B/\mathfrak{b}$, dado por $g(a + \mathfrak{a}) = a + \mathfrak{b}$, para cada $a + \mathfrak{a} \in A/\mathfrak{a}$. Sea $x + \mathfrak{b} \in B/\mathfrak{b}$. Dado que x es entero sobre A , verifica una ecuación polinómica de la forma

$$x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0, \quad a_i \in A, \quad i = 0, \dots, n-1.$$

Si $p: A \rightarrow A/\mathfrak{a}$ es el homomorfismo de anillos $p(a) = a + \mathfrak{a}$, aplicando $g \circ p$ a esta ecuación se tiene:

$$(x + \mathfrak{b})^n + (a_{n-1} + \mathfrak{a})(x + \mathfrak{b})^{n-1} + \dots + a_0 + \mathfrak{a} = 0.$$

Así, $x + \mathfrak{b}$ es entero sobre A/\mathfrak{a} .

(2) El anillo $S^{-1}B$ es un $S^{-1}A$ -módulo vía el homomorfismo de anillos $h: S^{-1}A \rightarrow S^{-1}B$, dado por $h(a/s) = a/s$, para cada $a/s \in S^{-1}A$. Sea $x/s \in S^{-1}B$. Dado que $x \in B$ es entero sobre A , verifica una ecuación polinómica de la forma

$$x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0, \quad a_i \in A, \quad i = 0, \dots, n-1.$$

Aplicando a esta ecuación el homomorfismo de anillos $f: B \rightarrow S^{-1}B$, dado por $f(b) = b/1$, para cada $b \in B$, se tiene la ecuación

$$x^n/1 + (a_{n-1}x^{n-1})/1 + \dots + a_0/1 = 0,$$

y multiplicando por $1/s^n$ tenemos

$$(x/s)^n + (a_1/s)(x/s)^{n-1} + \dots + a_0/s^n = 0,$$

con lo que x/s es entero sobre $S^{-1}A$. □

Proposición 2.23. Sean B un dominio entero y sea A un subanillo de B . Si B es entero sobre A , entonces el cuerpo de fracciones de B es algebraico sobre el cuerpo de fracciones de A .

Demostración. Sea L el cuerpo de fracciones de B , y sea $b/s \in L$, $b, s \in B$, $s \neq 0$. Veamos que podemos suponer que $s \in A$. En efecto, dado que B es entero sobre A , s verifica una ecuación polinómica con coeficientes en A

$$s^m + c_{n-1}s^{n-1} + \dots + c_0, \quad c_i \in A, \quad i = 0, \dots, n-1.$$

con $c_0 \neq 0$. Sea $d = -(s^{n-1} + c_{n-1}s^{n-2} + \dots + c_1)$. Se tiene que $sd = c_0 \neq 0$ y entonces $b/s = bd/c_0$.

Por ser B entero sobre A , se tiene una ecuación polinómica

$$b^n + a_{n-1}b^{n-1} + \dots + a_0 = 0, \quad a_{n-1}, \dots, a_0 \in A.$$

Multiplicando por $1/s^n$ obtenemos la ecuación polinómica

$$(b/s)^n + (a_{n-1}/s)(b/s)^{n-1} + \dots + (a_1/s^{n-1})(b/s) + a_0/s^n = 0$$

y puesto que los coeficientes están en el cuerpo de fracciones de A , llegamos a que b/s es algebraico sobre el cuerpo de fracciones de A . \square

Lema 2.24. Sea A un dominio entero íntegramente cerrado y sea E una extensión finita del cuerpo de fracciones K de A . Un elemento $\alpha \in E$ es entero sobre A si, y solo si, $\text{Irr}(\alpha, K, X) \in A[X]$.

Demostración. Sea $\alpha \in E$ entero sobre A , existen $a_1, \dots, a_n \in A$ tales que

$$\alpha^n + a_1\alpha^{n-1} + \dots + a_n = 0. \quad (*)$$

Sea $F(X) = \text{Irr}(\alpha, K, X)$ y sea α' otra raíz de $F(X)$ de un cuerpo de escisión del polinomio $F(X)$. Se tiene que $F(X) = \text{Irr}(\alpha', K, X)$ y entonces la aplicación $\sigma: K[\alpha] \rightarrow K[\alpha']$, $\sigma(\alpha) = \alpha'$ es un K -isomorfismo. Aplicando σ a la ecuación (*) llegamos a que

$$\alpha'^n + a_1\alpha'^{n-1} + \dots + a_n = 0,$$

con lo que α' es entero sobre A . Por tanto, si de $\alpha_1, \dots, \alpha_n$ son las raíces de $F(X)$ en un cuerpo de escisión, entonces $\alpha_1, \dots, \alpha_n$ son enteros sobre A . Se tiene

$$\begin{aligned} F(X) &= (X - \alpha_1) \dots (X - \alpha_n) \\ &= X^n - (\alpha_1 + \dots + \alpha_n)X^{n-1} + (\alpha_1\alpha_2 + \dots + \alpha_{n-1}\alpha_n)X^{n-2} + \dots + (-1)^n \alpha_1 \dots \alpha_n. \end{aligned}$$

Por el corolario 2.14, cada coeficiente de $F(X)$ es entero sobre A . Dado que los coeficientes de $F(X)$ están en K y A es íntegramente cerrado se tiene que $F(X) \in A[X]$.

Recíprocamente, si $\alpha \in E$ entonces por ser la extensión E/K finita, α es algebraico sobre K . Si $\text{Irr}(\alpha, K, X) \in A[X]$, entonces α es entero sobre A . \square

Lema 2.25. *Sea A un dominio entero íntegramente cerrado y sea L una extensión finita del cuerpo de fracciones K de A . Si $\alpha \in L$ es entero sobre A , entonces $\text{Nm}_{L/K}\alpha \in A$, y α divide a $\text{Nm}_{L/K}$ en el anillo $A[\alpha]$.*

Demostración. Sea $\text{Irr}(\alpha, K, X) = X^r + a_{r-1}X^{r-1} + \dots + a_0$. Por el corolario 1.23, r divide al grado n de la extensión L/K y $\text{Nm}_{L/K}(\alpha) = a_0^{n/r}$. Por el lema 2.24, $a_0 \in A$ y entonces $\text{Nm}_{L/K}(\alpha) \in A$. De la ecuación $0 = \alpha(\alpha^{r-1} + a_{r-1}\alpha^{r-2} + \dots + a_1) + a_0$ vemos que α divide a a_0 en $A[\alpha]$, y por tanto también divide a $\text{Nm}_{L/K}(\alpha)$. \square

Teorema 2.26. (Lema de Zariski, [1, Proposición 7.9]) *Sea E/K una extensión de cuerpos. Si E es una K -álgebra finitamente generada, entonces es algebraica sobre K , por tanto finita y si K es algebraicamente cerrado $E = K$.*

Definición 2.27. Se dice que un anillo es noetheriano si todos sus ideales son finitamente generados.

Teorema 2.28. (Teorema de la base de Hilbert [1]) *Si A es noetheriano, entonces el anillo de polinomios $A[X_1, \dots, X_n]$ es noetheriano.*

2.3. Lema de normalización de Noether

Probaremos en esta sección que todo dominio entero A que sea un álgebra finitamente generada sobre un cuerpo K contiene un álgebra de polinomios R tal que A es una R -álgebra finita; es decir que existen elementos y_1, \dots, y_r de A que son algebraicamente independientes sobre K y tales que A es una $K[y_1, \dots, y_r]$ -álgebra finita. Comenzaremos con unos lemas.

Lema 2.29. *Sea $F(X_1, \dots, X_d, T) \in K[X_1, \dots, X_d, T]$. Existe $m \in \mathbb{N}$ tal que*

$$F(X_1 + T^m, X_2 + T^{m^2}, \dots, X_d + T^{m^d}, T) = c_r T^r + c_{r-1} T^{r-1} + \dots + c_0,$$

con $c_r \in K - \{0\}$, $c_i \in K[X_1, \dots, X_d]$, para $i = 0, \dots, r-1$.

Demostración. Sea

$$F(X_1, \dots, X_d, T) = \sum a_{i_1 \dots i_{d+1}} X_1^{i_1} \dots X_d^{i_d} T^{i_{d+1}}$$

y sea

$$S = \{((i_1, \dots, i_{d+1}) \in \mathbb{N}^{d+1} \mid a_{i_1 \dots i_{d+1}} \neq 0)\}$$

y $m \in \mathbb{N}$ tal que $m > \max\{i_1, \dots, i_{d+1}\}$ para todo $(i_1, \dots, i_{d+1}) \in S$. Se tiene que el monomio de mayor grado en T del polinomio

$$(X_1 + T^m)^{i_1} \dots (X_d + T^{m^d})^{i_d} T^{i_{d+1}}$$

es $T^{mi_1 + m^2 i_2 + \dots + m^d i_d + i_{d+1}}$.

Para cada $(i_1, \dots, i_{d+1}) \in S$ los exponentes $mi_1 + m^2 i_2 + \dots + m^d i_d + i_{d+1}$ son distintos. En efecto, si

$$mi_1 + m^2 i_2 + \dots + m^d i_d + i_{d+1} = mk_1 + m^2 k_2 + \dots + m^d k_d + k_{d+1}$$

entonces, $i_{d+1} - k_{d+1} \in m\mathbb{Z}$ y dado que $i_{d+1} - k_{d+1} < m$, se tiene que $i_{d+1} = k_{d+1}$. Análogamente, $m(i_1 - k_1) \in m^2\mathbb{Z}$ y por tanto $i_1 - k_1 \in m\mathbb{Z}$ y dado que $i_1 - k_1 < m$, $i_1 = k_1$. Continuando el proceso llegamos a que $i_j = k_j$, para $j = 1, \dots, d+1$. Sea N el mayor de dichos exponentes, se tiene que

$$F(X_1 + T^m, \dots, X_d + T^{m^d}, T) = c_N T^N + c_{N-1} T^{N-1} + \dots + c_0,$$

con $c_N \in K - \{0\}$, $c_i \in [X_1, \dots, X_d]$, para $i = 0, \dots, N-1$. \square

Lema 2.30. *Sea $A = K[x_1, \dots, x_n]$ una K -álgebra finitamente generada que es un dominio entero y supongamos que $\{x_1, \dots, x_d\}$ es una base de trascendencia de $K(x_1, \dots, x_n)$ sobre K . Si $n > d$, entonces existe un $m \in \mathbb{N}$ tal que A es una $K[x_1 - x_n^m, \dots, x_d - x_n^{m^d}, x_{d+1}, \dots, x_{n-1}]$ -álgebra finita.*

Demostración. Si $n > d$, conjunto $\{x_1, \dots, x_d, x_n\}$ es algebraicamente dependiente, por lo que existe un $F \in K[X_1, \dots, X_d, T]$ no nulo tal que $F(x_1, \dots, x_d, x_n) = 0$. Como $\{x_1, \dots, x_d\}$ es un conjunto algebraicamente independiente, T aparece en F , y podemos escribir el polinomio como

$$F(X_1, \dots, X_d, T) = a_r T^r + a_{r-1} T^{r-1} + \dots + a_0.$$

con $a_i \in K[X_1, \dots, X_d]$, $a_r \neq 0$ y $r > 0$.

Si $a_r \in K$, como $F(x_1, \dots, x_d, x_n) = 0$, tenemos que x_n es entero sobre $K[x_1, \dots, x_n]$ y entonces que x_1, \dots, x_n son enteros sobre $K[x_1, \dots, x_{n-1}]$, y por la proposición 2.19, A es una $K[x_1, \dots, x_{n-1}]$ -álgebra finita y el lema se verifica para $m = 0$.

Si $a_r \notin K$, por el lema anterior existe un m natural tal que $F(X_1 + T^m, X_2 + T^{m^2}, \dots, X_d + T^{m^d}, T) = c_r T^r + c_{r-1} T^{r-1} + \dots + c_0$, con $c_r \in K - \{0\}$, $c_i \in K[X_1, \dots, X_d]$. Consideremos el polinomio

$$G(X_1, \dots, X_d, T) = F(X_1 + T^m, X_2 + T^{m^2}, \dots, X_d + T^{m^d}, T) = c_r T^r + c_{r-1} T^{r-1} + \dots + c_0.$$

Dado que

$$G(x_1 - x_n^m, \dots, x_d - x_n^{m^d}, x_n) = c_r x_n^r + c_{r-1}(x_1 - x_n^m, \dots, x_d - x_n^{m^d})x_n^{r-1} \\ + \dots + c_0(x_1 - x_n^m, \dots, x_d - x_n^{m^d}) = F(x_1, \dots, x_d, x_n) = 0,$$

x_n es entero sobre $K[x_1 - x_n^m, \dots, x_d - x_n^{m^d}]$. Como $x_i = (x_i - x_n^{m^i}) + x_n^{m^i}$, los elementos x_i con $i \leq d$ también son enteros sobre $K[x_1 - x_n^m, \dots, x_d - x_n^{m^d}]$, y por la proposición 2.19, A es una $K[x_1 - x_n^m, \dots, x_d - x_n^{m^d}, x_{d+1}, \dots, x_{n-1}]$ -álgebra finita. \square

Teorema 2.31. (Lema de normalización de Noether) *Sea $A = K[x_1, \dots, x_n]$ una K -álgebra finitamente generada que es un dominio entero. Existen elementos $y_1, \dots, y_d \in A$ que son algebraicamente independientes sobre K y tales que A es entero sobre $K[y_1, \dots, y_d]$.*

Demostración. Sea $d = \text{tr deg}_K K(x_1, \dots, x_n)/K$. Si $d = n$, entonces x_1, \dots, x_n es una base de trascendencia de $K(x_1, \dots, x_n)$ sobre K y A es finita sobre A .

Si $d < n$, supongamos que $\{x_1, \dots, x_d\}$ es una base de trascendencia de $K(x_1, \dots, x_n)$ sobre K . Por el lema anterior, existen elementos $z_1, \dots, z_{n-1} \in A$ tales que A es finita sobre $K[z_1, \dots, z_{n-1}]$ y por tanto entera. Por la proposición 2.25 $K(x_1, \dots, x_n)$ es una extensión algebraica de $k(z_1, \dots, z_{n-1})$. Dado que toda base de trascendencia de $K(z_1, \dots, z_{n-1})$ sobre K es base de trascendencia de $k(x_1, \dots, x_n)$ sobre K , se tiene que $\text{tr deg}_K K(z_1, \dots, z_{n-1})/K = d$.

Si $d = n - 1$, entonces z_1, \dots, z_{n-1} son algebraicamente independientes. Si $d < n - 1$, se repite el proceso para $K[z_1, \dots, z_{n-1}]$, y entonces existen elementos $t_1, \dots, t_{n-2} \in A$ tales que $K[z_1, \dots, z_{n-1}]$ es entera sobre $K[t_1, \dots, t_{n-2}]$. Por la proposición 2.25 la extensión $K(z_1, \dots, z_{n-1})$ es algebraica sobre $K(t_1, \dots, t_{n-2})$ y entonces $\text{tr deg}_K K(t_1, \dots, t_{n-2})/K = d$. Además, por la transitividad de la dependencia entera, A es entera sobre $K[t_1, \dots, t_{n-2}]$. Si $d = n - 2$, entonces t_1, \dots, t_{n-2} son algebraicamente independientes. Si $d < n - 2$, se sigue con este proceso hasta encontrar elementos $y_1, \dots, y_d \in A$ tales que A es entera sobre $K[y_1, \dots, y_d]$ y $\text{tr deg}_K K(y_1, \dots, y_d)/K = d$. \square

Capítulo 3

Variedades algebraicas afines

3.1. Variedades algebraicas afines. Topología de Zariski

Sea K un cuerpo. Denotaremos por $K[X_1, \dots, X_n]$ el anillo de polinomios en las variables X_1, \dots, X_n con coeficientes en K . En general denotaremos $F(X_1, \dots, X_n)$ por F y si $P = (a_1, \dots, a_n) \in K^n$, $F(a_1, \dots, a_n)$ por $F(P)$.

Definición 3.1. Sea S un subconjunto de $K[X_1, \dots, X_n]$. Se llama *variedad algebraica afín* o *conjunto algebraico afín* definido por S al conjunto de ceros comunes a todos los polinomios de S :

$$Z(S) = \{P \in K^n \mid F(P) = 0, \forall F \in S\}.$$

Si $S = \{F_1, \dots, F_n\}$, denotaremos $Z(S)$ por $Z(F_1, \dots, F_n)$. Si S es un conjunto de polinomios de grado 1, entonces $Z(S)$ es una variedad lineal de K^n .

Si $S \subset K[X_1, \dots, X_n]$, entonces $Z(S) = Z(\langle S \rangle)$. En efecto, claramente $Z(\langle S \rangle) \subset Z(S)$. Recíprocamente, si $P \in Z(S)$, entonces $F(P) = 0$, para cada $F \in S$ y entonces,

$$\left(\sum_{i=1}^n a_i F_i\right)(P) = \sum_{i=1}^n a_i(P) F_i(P) = 0, \forall a_i \in K[X_1, \dots, X_n], \forall F_i \in S, \forall n \in \mathbb{N}.$$

Así, $Z(S) \subset Z(\langle S \rangle)$. Así, las variedades algebraicas afines son los conjuntos de la forma $Z(\mathfrak{a})$ donde \mathfrak{a} es un ideal de $K[X_1, \dots, X_n]$.

Por el teorema de la base de Hilbert (2.28), todo ideal de $K[X_1, \dots, X_n]$ está finitamente generado. Si $\mathfrak{a} = \langle F_1, \dots, F_r \rangle$, entonces

$$Z(\mathfrak{a}) = Z(F_1, \dots, F_r) = \bigcap_{i=1}^r Z(F_i) = Z(F_1, \dots, F_r)$$

Si K es un cuerpo algebraicamente cerrado y $F \in K[X_1, \dots, X_n]$, $F \notin K$, los conjuntos $Z(F)$ se llaman hipersuperficies. Si $n = 1$ se llaman curvas y si $n = 2$ superficies. Así, toda variedad algebraica afín es intersección de un número finito de hipersuperficies.

Se tiene:

- (1) Si \mathfrak{a} y \mathfrak{b} son ideales de $K[X_1, \dots, X_n]$ y $\mathfrak{a} \subset \mathfrak{b}$, entonces $Z(\mathfrak{b}) \subset Z(\mathfrak{a})$.
- (2) $Z(0) = K^n$ y $Z(K[X_1, \dots, X_n]) = \emptyset$, es decir el conjunto vacío y K^n son variedades algebraicas afines.
- (3) $Z(\mathfrak{a}\mathfrak{b}) = Z(\mathfrak{a} \cap \mathfrak{b}) = Z(\mathfrak{a}) \cup Z(\mathfrak{b})$.
- (4) $Z(\bigcup \mathfrak{a}_i) = Z(\sum \mathfrak{a}_i) = \bigcap Z(\mathfrak{a}_i)$.
- (5) Un punto de K^n es una variedad algebraica afín. En efecto, si $P = (a_1, \dots, a_n)$, entonces $\{P\} = Z(X_1 - a_1, \dots, X_n - a_n)$. Cualquier subconjunto finito de K^n es una variedad algebraica afín.

Las afirmaciones (2), (3) y (4) demuestran que las variedades algebraicas afines de K^n satisfacen los axiomas para ser los cerrados de una topología en K^n : el vacío y todo el espacio son cerrados, una unión finita de cerrados es un cerrado y una intersección arbitraria de cerrados es un cerrado. Esta topología se llama la topología de Zariski de K^n . Si V es un conjunto algebraico de K^n llamaremos topología de Zariski de V a su topología relativa respecto a la de Zariski de K^n ; sus cerrados son los cerrados de K^n contenidos en V .

La topología de Zariski es muy diferente de las topologías usuales; los cerrados son muy pequeños: si K es algebraicamente cerrado, los cerrados en K son los subconjuntos finitos y K y en cambio en K^n los abiertos son muy grandes, dos abiertos no vacíos se cortan siempre, con lo cual la topología no es separada.

Definición 3.2. Sea $F \in K[X_1, \dots, X_n]$, $F \notin K$ y $Z(F)$ la hipersuperficie definida por F . El conjunto

$$D(F) = K^n - Z(F)$$

es un abierto de Zariski de K^n que se llama abierto básico o principal. Los abiertos principales forman una base de la topología de K^n , es decir todo abierto U es unión de abiertos principales:

$$U = K^n - Z(F_1, \dots, F_r) = \bigcup_{i=1}^r (K^n - Z(F_i)) = \bigcup_{i=1}^r D(F_i).$$

3.2. Ideal de una variedad algebraica afín

Definición 3.3. Sea Y un subconjunto de K^n . Se llama ideal de Y al conjunto:

$$I(Y) = \{F \in K[X_1, \dots, X_n] \mid F(P) = 0, \forall P \in Y\}$$

Se tiene:

- (1) Si $Y_1 \subset Y_2$, entonces $I(Y_2) \subset I(Y_1)$.
- (2) $I(\emptyset) = K[X_1, \dots, X_n]$ y si K es infinito $I(K^n) = \{0\}$.
- (3) $I(\bigcup Y_i) = \bigcap I(Y_i)$
- (4) Si V es una variedad algebraica afín, entonces $Z(I(V)) = V$.
- (5) Si V y W son variedades algebraicas afines y $I(V) = I(W)$, entonces $V = W$.
- (6) $I(\{a_1, \dots, a_n\}) = \langle X_1 - a_1, \dots, X_n - a_n \rangle$.
- (7) $\mathfrak{a} \subset I(Z(\mathfrak{a}))$, para todo ideal \mathfrak{a} de $K[X_1, \dots, X_n]$.

Definición 3.4. Sea A un anillo conmutativo y unitario y \mathfrak{a} un ideal de A . Se llama radical de \mathfrak{a} al ideal

$$\text{rad } \mathfrak{a} = \{x \in A \mid \exists r \in \mathbb{N}, x^r \in \mathfrak{a}\}.$$

El radical de \mathfrak{a} es la intersección de todos los ideales primos que contienen a \mathfrak{a} . Si \mathfrak{a} , \mathfrak{b} y \mathfrak{p} son ideales de A y \mathfrak{p} es un ideal primo, entonces

$$\text{rad } (\mathfrak{a} \mathfrak{b}) = \text{rad } (\mathfrak{a} \cap \mathfrak{b}) = \text{rad } \mathfrak{a} \cap \text{rad } \mathfrak{b}, \quad \text{rad } (\mathfrak{p}^n) = \mathfrak{p}, \quad \forall n > 0.$$

Se dice que un ideal es radical si coincide con su radical. Se dice que un anillo es reducido si no tiene elementos nilpotentes distintos de cero .

Se verifica que un ideal \mathfrak{a} de A es radical si, y solo si, A/\mathfrak{a} es un anillo reducido.

Proposición 3.5. Sea V un conjunto algebraico afín de K^n . El conjunto $I(V)$ es un ideal radical de $K[X_1, \dots, X_n]$.

Demostración. Consideremos el anillo de todas las funciones de V en K , $\mathcal{F}(V, k)$, y el homomorfismo de anillos

$$p_V: K[X_1, \dots, X_n] \rightarrow \mathcal{F}(V, k)$$

$$F \quad \rightsquigarrow \quad f$$

siendo $f: V \rightarrow K$ la aplicación dada por $f(P) = F(P)$, para cada $P \in V$. El núcleo de p_V es $I(V)$ que por tanto es un ideal de $K[X_1, \dots, X_n]$. Además, si $F \in \text{rad } I(V)$, entonces existe $r \in \mathbb{N}$ tal que $F^r \in I(V)$ y entonces $F^r(P) = F(P)^r = 0$, para todo $P \in V$. Así, $F(P) = 0$, para todo $P \in V$, de donde se sigue que $F \in I(V)$.

El subanillo imagen por p_V de $K[X_1, \dots, X_n]$ que denotaremos por $\Gamma(V)$ es isomorfo al anillo $K[X_1, \dots, X_n]/I(V)$. El anillo $\Gamma(V)$ se llama anillo de funciones regulares de V y el anillo $K[X_1, \dots, X_n]/I(V)$ anillo de coordenadas de V . \square

Definición 3.6. Sea V un conjunto algebraico afín de K^n . El anillo $\Gamma(V)$ se llama *anillo de funciones regulares* o *anillo de funciones polinómicas* en V o también *álgebra afín* de V y el anillo $K[X_1, \dots, X_n]/I(V)$ *anillo de coordenadas* de V .

El anillo $\Gamma(V)$ es una K -álgebra de tipo finito reducida (no tiene elementos nilpotentes no nulos) y sus elementos se llaman *funciones polinómicas* o *regulares* de V .

3.3. Irreducibilidad

Si consideramos en K^2 la variedad algebraica afín V definida por la ecuación $XY = 0$ vemos que es la unión de dos variedades algebraicas afines, los dos ejes coordenados, es decir, V es unión de dos cerrados de Zariski. Para estudiar una variedad algebraica afín V estudiaremos con frecuencia cada uno de los cerrados que aparecen.

Proposición 3.7. *Sea X un espacio topológico no vacío. Son equivalentes:*

- (1) *Si $X = C_1 \cup C_2$ con C_1 y C_2 cerrados de X , se tiene que $X = C_1$ o $X = C_2$.*
- (2) *Si U y V son dos abiertos de X con $U \cap V = \emptyset$, entonces $U = \emptyset$ o $V = \emptyset$.*
- (3) *Todo abierto no vacío de X es denso.*

Demostración. (1) \Rightarrow (2) Sean U y V abiertos de X con $U \cap V = \emptyset$. Los conjuntos $X - U$ y $X - V$ son cerrados de X . Por las leyes de Morgan, $(X - U) \cup (X - V) = X - (U \cap V) = X$. Por (1), $X - U = X$ o $X - V = X$, con lo que $U = \emptyset$ o $V = \emptyset$.

(2) \Rightarrow (3) Sea U un abierto no vacío de X . Dado que U denso en X si, y sólo si, $U \cap V \neq \emptyset$, para todo V abierto no vacío de X , el resultado se sigue de (2).

(3) \Rightarrow (1) Sean C_1 y C_2 cerrados de X tales que $X = C_1 \cup C_2$. Los conjuntos $X - C_1$ y $X - C_2$ son abiertos de X y si fueran no vacíos $(X - C_1) \cap (X - C_2) \neq \emptyset$, por (3). Por las leyes de Morgan se tendría que $C_1 \cup C_2 = X - ((X - C_1) \cap (X - C_2)) \neq X$, lo cual es una contradicción. En consecuencia, $X - C_1 = \emptyset$ o $X - C_2 = \emptyset$, con lo que $C_1 = X$ o $C_2 = X$. \square

Definición 3.8. Si X es un espacio topológico que verifica una de las tres condiciones equivalentes de la proposición 3.7, entonces se dice que X es irreducible.

Observación 3.9. Con las topologías usuales esta situación no se produce, puesto que son separadas, con lo cual los únicos irreducibles son los conjuntos formados por un punto.

Teorema 3.10. *Sea V una variedad algebraica afín con su topología de Zariski. Se tiene que V es irreducible, si, y solo si, $I(V)$ es un ideal primo de $K[X_1, \dots, X_n]$.*

Demostración. Supongamos que V es irreducible. Sean $F, G \in K[X_1, \dots, X_n]$ tales que $FG \in I(V)$. Se tiene que $V = Z(I(V)) \subset Z(FG) = Z(F) \cup Z(G)$, por lo que podemos escribir $V = (Z(F) \cap V) \cup (Z(G) \cap V)$, donde cada elemento de la unión es cerrado. Por ser V irreducible, $Z(F) \cap V = V$ o $Z(G) \cap V = V$ y entonces $V \subset Z(F)$ o $V \subset Z(G)$ y así $F \in IZ(F) \subset I(V)$ o $F \in IZ(G) \subset I(V)$.

Recíprocamente, supongamos $I(V)$ es un ideal primo, y que V no es irreducible, es decir $V = C_1 \cup C_2$, con C_1, C_2 cerrados, $C_1 \neq V, C_2 \neq V$. Se tiene entonces que $I(V) \subsetneq I(C_1)$ y $I(V) \subsetneq I(C_2)$. Sean $F_1 \in I(C_1) - I(V), F_2 \in I(C_2) - I(V)$, llegamos a que $F_1 F_2$ se anula en C_1 y C_2 y por tanto en V . Así, $F_1 F_2 \in I(V)$, y por ser $I(V)$ es primo, se tiene que $F_1 \in I(V)$ o $F_2 \in I(V)$, lo cual es una contradicción. Por tanto V es irreducible. \square

Corolario 3.11. *Si K es un cuerpo infinito, entonces K^n es irreducible.*

Demostración. Dado que $I(K^n) = \{0\}$, el ideal $\{0\}$ es primo, por ser $K[X_1, \dots, X_n]$ un dominio. \square

Definición 3.12. Si V es una variedad algebraica irreducible entonces el anillo $\Gamma(V)$ es un dominio entero. El cuerpo de fracciones de $\Gamma(V)$ se llama cuerpo de funciones racionales sobre V y se denota por $K(V)$.

Proposición 3.13. *Sea K un cuerpo infinito, $A \in K^n$, U un subespacio de K^n y consideremos la variedad lineal $L = A + U$. Si $\dim_K(U) = r$, entonces L es homeomorfa a K^r .*

Demostración. Sea $A = (a_1, \dots, a_n)$ y sean

$$x_1 = a_1 + a_{11}\lambda_1 + \dots + a_{1r}\lambda_r, \quad \dots \quad x_n = a_n + a_{n1}\lambda_1 + \dots + a_{nr}\lambda_r,$$

unas ecuaciones paramétricas de L . La aplicación $f: K^r \rightarrow L$ dada por

$$f(y_1, \dots, y_r) = (a_1 + a_{11}y_1 + \dots + a_{1r}y_r, \dots, a_n + a_{n1}y_1 + \dots + a_{nr}y_r),$$

es un homeomorfismo. En efecto, f es continua, por ser una aplicación polinómica y es biyectiva.

Los vectores $v_i = (a_{1i}, \dots, a_{ni}), i = 1, \dots, r$ forman una base de U . Supongamos que

$$\Delta = \begin{vmatrix} a_{11} & \dots & a_{1r} \\ \vdots & \ddots & \vdots \\ a_{r1} & \dots & a_{rr} \end{vmatrix} \neq 0.$$

La aplicación f^{-1} es la composición de dos aplicaciones polinómicas, la aplicación $t_{-A}: L \rightarrow U$, dada por $t_{-A}(P) = P - A$ y la aplicación $g: U \rightarrow K^r$, dada por

$$g(b_1, \dots, b_n) = (G_1(b_1, \dots, b_n), \dots, G_r(b_1, \dots, b_n)),$$

siendo

$$G_i(b_1, \dots, b_n) = (\det \Delta)^{-1} \begin{vmatrix} a_{11} & \dots & a_{1i-1} & b_1 & a_{1i+1} & \dots & a_{1r} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{r1} & \dots & a_{ri-1} & b_r & a_{ri+1} & \dots & a_{rr} \end{vmatrix}, \quad i = 1, \dots, r$$

Por tanto, f^{-1} es continua. \square

Corolario 3.14. *Si K es un cuerpo infinito, toda variedad lineal afín de K^n es irreducible.*

Demostración. Si L es una variedad lineal de dimensión r entonces es homeomorfa a K^r . Por ser K^r irreducible, L es irreducible. \square

Notación 3.15. Sea X un espacio topológico e Y un subespacio de X , denotaremos por \overline{Y} la clausura de Y en X , es decir el menor cerrado de X que contiene a Y . Si $Z \subset Y \subset X$, $Y \neq X$, denotaremos por \overline{Z}^Y la clausura de Z en Y considerando Y como espacio topológico con su topología relativa respecto a la de X . Obsérvese que si $Z \subset Y \subset X$, entonces $\overline{Z}^Y = \overline{Z} \cap Y$.

Proposición 3.16. *Sea X un espacio topológico e Y un subespacio de X . Se tiene*

- (1) *Y es irreducible si, y solo si, \overline{Y} es irreducible.*
- (2) *Si X es un espacio irreducible y U un abierto no vacío de X , entonces U es irreducible.*
- (3) *Sea U un abierto de X . Si Σ_U es el conjunto de cerrados irreducibles de U y Σ es el conjunto de cerrados irreducibles de X cuya intersección con U es no vacía, entonces la aplicación*

$$\varphi: \Sigma_U \rightarrow \Sigma$$

dada por $\varphi(Y) = \overline{Y}$ es biyectiva y $\varphi^{-1}(Z) = Z \cap U$.

Demostración. (1) Supongamos primero que \overline{Y} es irreducible, y sean C_1, C_2 cerrados de Y tales que $Y = C_1 \cup C_2$. Entonces, $\overline{Y} = \overline{C_1} \cup \overline{C_2}$. Por ser \overline{Y} irreducible, podemos suponer que $\overline{Y} = \overline{C_1}$. Entonces,

$$Y = \overline{Y} \cap Y = \overline{C_1} \cap Y = \overline{C_1}^Y = C_1$$

y por tanto Y es irreducible.

Supongamos ahora que Y es irreducible, y que existen C_1, C_2 cerrados de \bar{Y} , $\bar{Y} \neq C_1$, $\bar{Y} \neq C_2$, tales que $\bar{Y} = C_1 \cup C_2$. Si $Y \subset C_1$, tendríamos que $\bar{Y} \subset \bar{C}_1 = C_1$, lo cual no ocurre. Por el mismo razonamiento, tenemos que $Y \not\subset C_2$. Pero entonces existirían dos cerrados de Y , $Y \cap C_1$ y $Y \cap C_2$, tales que $Y = (Y \cap C_1) \cup (Y \cap C_2)$, $Y \neq Y \cap C_i$ para $i = 1, 2$, lo cual contradice que Y es irreducible. Por tanto, \bar{Y} es necesariamente irreducible.

(2) Por (1), dado que $\bar{U} = X$, entonces U es irreducible.

(3) Comencemos viendo que la aplicación está bien definida. Efectivamente, sea $Y \in \Sigma_U$, se tiene que $Y = \bar{Y}^U = \bar{Y} \cap U$, y como Y es no vacío por definición, \bar{Y} es un cerrado de X tal que $\bar{Y} \cap U \neq \emptyset$. Además, por (1), como Y es irreducible entonces \bar{Y} también lo es, y así $\bar{Y} \in \Sigma$.

Sean $Y, Z \in \Sigma_U$ tales que $\varphi(Y) = \varphi(Z)$, es decir, $\bar{Y} = \bar{Z}$. Entonces

$$Y = \bar{Y}^U = \bar{Y} \cap U = \bar{Z} \cap U = \bar{Z}^U = Z$$

por lo que φ es inyectiva.

Dado $Z \in \Sigma$, veamos primero que $Z \cap U \in \Sigma_U$. Efectivamente, $Z \cap U \subset U$ y es cerrado en U por ser Z cerrado de X . Además, por ser U abierto de X , $Z \cap U$ es abierto de Z , y por ser Z irreducible, $Z \cap U$ es denso en Z , es decir, $\overline{Z \cap U} = Z$. Entonces, nuevamente por ser Z irreducible, llegamos por (1) a que $Z \cap U$ es irreducible, y así $Z \cap U \in \Sigma_U$. Además, como acabamos de ver, $\varphi(Z \cap U) = \overline{Z \cap U} = Z$, por lo que φ es sobreyectiva.

Por tanto, $\varphi^{-1}(Z) = Z \cap U$. □

Teorema 3.17. [2, p. 17, Teorema 2] *Sea V una variedad algebraica afín no vacía. Se puede escribir V de forma única (salvo permutación) como $V = V_1 \cup \dots \cup V_r$ donde V_i es una variedad algebraica afín irreducible y $V_i \not\subset V_j$, para $i \neq j$. Los conjuntos V_i se dice que son las componentes irreducibles de V .*

Observación 3.18. Si W es un cerrado irreducible de V , W está contenido en una componente irreducible; las componentes irreducibles son los conjuntos cerrados irreducibles maximales de V .

3.4. Teorema de los ceros de Hilbert

En esta sección el cuerpo K es un cuerpo algebraicamente cerrado.

Proposición 3.19. (Teorema de los ceros de Hilbert (forma débil), [2, Capítulo 1, pag 20]) *Si \mathfrak{a} es un ideal de $K[X_1, \dots, X_n]$, $\mathfrak{a} \neq K[X_1, \dots, X_n]$, entonces $Z(\mathfrak{a})$ es no vacío.*

Teorema 3.20. (Teorema de los ceros de Hilbert, [2, Capítulo 1, pag 20]) *Sea \mathfrak{a} un ideal de $K[X_1, \dots, X_n]$. Se tiene que $I(Z(\mathfrak{a})) = \text{rad } \mathfrak{a}$.*

Proposición 3.21. *Sea, \mathcal{I} el conjunto de ideales radicales de $K[X_1, \dots, X_n]$ y \mathcal{S} el conjunto de variedades algebraicas de K^n . La aplicación*

$$\mathcal{V}: \mathcal{I} \longrightarrow \mathcal{S}$$

dada por $\mathcal{V}(\mathfrak{a}) = Z(\mathfrak{a})$ es biyectiva e invierte el orden. Su inversa es la aplicación que lleva una variedad algebraica afín V a su ideal $I(V)$.

Demostración. Sea $\mathfrak{a} \in \mathcal{I}$, por el teorema de los ceros de Hilbert $I(Z(\mathfrak{a})) = \mathfrak{a}$ y si $V \in \mathcal{S}$, se tiene que $Z(I(V)) = V$. \square

Observación 3.22. Por la biyección de la proposición anterior los ideales primos corresponden a las variedades irreducibles y los ideales radicales propios maximales corresponden a los conjuntos minimales no vacíos. Los ideales radicales propios maximales son los ideales maximales de $K[X_1, \dots, X_n]$ y las variedades algebraicas propias minimales son los conjuntos con un solo punto. Dado que $I(\{a_1, \dots, a_n\}) = \langle X_1 - a_1, \dots, X_n - a_n \rangle$, se tiene que los ideales maximales de $K[X_1, \dots, X_n]$ son los ideales de la forma $\langle X_1 - a_1, \dots, X_n - a_n \rangle$.

Ejemplo 3.23. Sea $F \in K[X_1, \dots, X_n]$. Dado que $K[X_1, \dots, X_n]$ es un dominio de factorización única, el polinomio F es irreducible si, y solo si, el ideal $\langle F \rangle$ es primo, con lo cual

$$F \text{ es irreducible} \iff Z(F) \text{ es irreducible}$$

Si $F = \prod F_i^{m_i}$, donde los F_i son polinomios irreducibles distintos, entonces $\text{rad } \langle F \rangle = \bigcap \text{rad } \langle F_i^{m_i} \rangle = \bigcap \langle F_i \rangle$. Por tanto,

$$Z(F) = Z(\text{rad } \langle F \rangle) = Z\left(\bigcap \langle F_i \rangle\right) = \bigcup Z(F_i)$$

es la descomposición de $Z(F)$ en sus componentes irreducibles.

Sea V una variedad algebraica afín de K^n . Si W es una variedad algebraica afín de K^n y $W \subset V$, entonces $I(V) \subset I(W)$. Consideremos el homomorfismo sobreyectivo de anillos (proyección canónica):

$$\begin{aligned} p_V: K[X_1, \dots, X_n] &\longrightarrow \Gamma(V) \\ F &\rightsquigarrow f \end{aligned}$$

siendo $f: V \rightarrow K$ la aplicación dada por $f(P) = F(P)$. Se tiene que $p_V(I(W)) = \{f \in \Gamma(V) \mid f(P) = 0, \forall P \in W\}$. Denotaremos $p_V(I(W))$ por $I_V(W)$ y se tiene un isomorfismo inducido $\Gamma(V)/I_V(W) \simeq \Gamma(W)$. Dado que $\Gamma(W)$ es un anillo reducido, el ideal $I_V(W)$ es radical.

$$\begin{array}{ccccc}
& & I(W) & \longrightarrow & I_V(W) \\
& \nearrow & \downarrow & & \downarrow \\
I(V) & \hookrightarrow & K[X_1, \dots, X_n] & \xrightarrow{p_V} & \Gamma(V) \\
& & \downarrow p_W & & \downarrow \\
& & \Gamma(W) & \longrightarrow & \Gamma(V)/I_V(W)
\end{array}$$

Así, a una variedad algebraica W contenida en V le podemos hacer corresponder un ideal de $\Gamma(V)$ radical. Recíprocamente, si \mathfrak{a} es un ideal de $\Gamma(V)$ podemos definir $Z_V(\mathfrak{a})$ como el conjunto de ceros de las funciones de \mathfrak{a} sobre V

$$Z_V(\mathfrak{a}) = \{P \in V \mid f(P) = 0, \forall P \in \mathfrak{a}\}.$$

Se tiene que $Z_V(\mathfrak{a}) = Z(p_V^{-1}(\mathfrak{a}))$ es una variedad algebraica afín de K^n .

Obsérvese que dado que todo ideal de $K[X_1, \dots, X_n]$ está finitamente generado, todo ideal de $\Gamma(V)$ está finitamente generado. Por tanto, si $\mathfrak{a} = \langle f_1, \dots, f_r \rangle$, entonces

$$Z_V(\mathfrak{a}) = \{P \in V \mid f_i(P) = 0, i = 1, \dots, r\} = Z_V(f_1, \dots, f_r),$$

y si $V = Z(G_1, \dots, G_s)$ y $F_1, \dots, F_r \in K[X_1, \dots, X_n]$ son tales que $f_i(P) = F_i(P)$, para todo $P \in V$ y para $i = 1, \dots, r$, entonces $Z_V(\mathfrak{a}) = Z(G_1, \dots, G_s, F_1, \dots, F_r)$.

Proposición 3.24. *Sea V una variedad algebraica afín de K^n , \mathcal{I}_V el conjunto de ideales radicales de $\Gamma(V)$ y \mathcal{S}_V el conjunto de variedades algebraicas de K^n contenidas en V . La aplicación*

$$\mathcal{V}_V: \mathcal{I}_V \longrightarrow \mathcal{S}_V,$$

dada por $\mathcal{V}_V(\mathfrak{a}) = Z_V(\mathfrak{a})$ es biyectiva. Su inversa es la aplicación que lleva una variedad algebraica afín W contenida en V al ideal $I_V(W)$. Por esta biyección los ideales primos de $\Gamma(V)$ corresponden a las variedades algebraicas irreducibles contenidas en V , los ideales maximales de $\Gamma(V)$ a los conjuntos con un solo punto de V y los ideales primos minimales de $\Gamma(V)$ a las componentes irreducibles de V .

Demostración. Veamos que se verifica que si \mathfrak{a} es un ideal de A , entonces $I_V(Z_V(\mathfrak{a})) = \text{rad } \mathfrak{a}$. En efecto,

$$I_V(Z_V(\mathfrak{a})) = I_V(Z(p_V^{-1}(\mathfrak{a}))) = p_V(I(Z(p_V^{-1}(\mathfrak{a})))) = p_V(\text{rad } p_V^{-1}(\mathfrak{a})) = \text{rad } \mathfrak{a}.$$

Si $\mathfrak{a} \in \mathcal{I}_V$, entonces $I_V(Z_V(\mathfrak{a})) = \mathfrak{a}$. Si $W \in \mathcal{S}_V$, entonces

$$Z_V(I_V(W)) = Z(p_V(I(W))) = Z(p_V^{-1}(p_V(I(W)))) = Z(I(W)) = W$$

Lo que falta por probar se sigue de la proposición 3.21 y de la observación 3.22. \square

Definición 3.25. Sea V una variedad algebraica afín de K^n y $f \in \Gamma(V)$, $f \neq 0$. El abierto de V

$$D_V(f) = V - Z_V(f) = \{P \in V \mid f(P) \neq 0\}$$

se dice que es un abierto básico o principal de V . Denotaremos, generalmente, $D_V(f)$ por $D(f)$ y $Z_V(f)$ por $Z(f)$.

Proposición 3.26. Sea V una variedad algebraica de K^n . Todo abierto de V es unión finita de abiertos principales.

Demostración. Sea U un abierto de V . Se tiene

$$W = V - U = Z(F_1, \dots, F_r) \cap V = Z(f_1, \dots, f_r)$$

donde $f_i \in \Gamma(V)$, está dada por $f_i(P) = F_i(P)$, para todo $P \in V$, y entonces

$$U = V - Z(f_1, \dots, f_r) = V - \left(\bigcap_{i=1}^r Z(f_i) \right) = \bigcup_{i=1}^r (V - Z(f_i)) = \bigcup_{i=1}^r D(f_i). \quad \square$$

Proposición 3.27. Sea V una variedad algebraica afín de K^n , $F \in K[X_1, \dots, X_n]$ y $f = p_V(F) \in \Gamma(V)$. El abierto $D_V(f)$ de V , con la topología relativa, es homeomorfo a la variedad algebraica afín $Z(I(V) + \langle X_{n+1}F - 1 \rangle)$ de K^{n+1} .

Demostración. Veamos que la aplicación

$$\begin{aligned} \varphi: D(f) &\longrightarrow K^{n+1} \\ (x_1, \dots, x_n) &\rightsquigarrow \left(x_1, \dots, x_n, \frac{1}{f(x_1, \dots, x_n)} \right) \end{aligned}$$

es una aplicación continua inyectiva que define un homeomorfismo en su imagen $Z(I(V) + \langle X_{n+1}F - 1 \rangle)$, es decir es un embebimiento topológico.

Pongamos $W = Z(I(V) + \langle X_{n+1}F - 1 \rangle)$ y denotemos por $\bar{\varphi}: D(f) \rightarrow W$ la aplicación inducida por φ . Claramente $\bar{\varphi}(D(f)) \subset W$.

Veamos que $W \subset \bar{\varphi}(D(f))$:

$$\begin{aligned} (x_1, \dots, x_{n+1}) \in W &= Z((I(V)) \cup \langle X_{n+1}F - 1 \rangle) \\ &\Rightarrow G(x_1, \dots, x_n) = 0, \forall G \in I(V), x_{n+1} f(x_1, \dots, x_n) = 0 \\ &\Rightarrow (x_1, \dots, x_n) \in Z(I(V)) = V, f(x_1, \dots, x_n) \neq 0 \\ &\Rightarrow (x_1, \dots, x_n) \in D(f) \end{aligned}$$

Veamos que $\bar{\varphi}$ es continua. Es suficiente probar que $\bar{\varphi}^{-1}(Z(G) \cap W)$ es un cerrado de $D(f)$.

Se tiene

$$\bar{\varphi}^{-1}(Z(G) \cap W) = \{P \in D(f) \mid G(x_1, \dots, x_n, \frac{1}{f(x_1, \dots, x_n)}) = 0\}$$

Pongamos

$$G' = G(X_1, \dots, X_n, \frac{1}{f(x_1, \dots, x_n)}) \in K[X_1, \dots, X_n].$$

Se tiene

$$\bar{\varphi}^{-1}(Z(G) \cap W) = \{(x_1, \dots, x_n) \in D(f) \mid G'(x_1, \dots, x_n) = 0\} = D(f) \cap Z_V(g')$$

siendo $g' = p_V(G') \in \Gamma(V)$.

Veamos que φ es cerrada. Sea $G \in K[X_1, \dots, X_n]$ y $g = p_V(G)$. Se tiene

$$\begin{aligned} \bar{\varphi}(Z(G) \cap D(f)) &= \varphi(Z(g) \cap D(f)) = \{(x_1, \dots, x_n, \frac{1}{f(x_1, \dots, x_n)}) \in W \mid G(x_1, \dots, x_n) = 0\} \\ &= W \cap Z(G). \end{aligned}$$

□

Capítulo 4

Variedades algebraicas proyectivas

En este capítulo vamos a suponer que el cuerpo K es infinito.

Definición 4.1. El *espacio proyectivo* $\mathbb{P}^n(\mathbb{K}^n)$ es el conjunto cociente

$$\mathbb{P}^n(K) = \frac{K^{n+1} - \{(0, \dots, 0)\}}{\sim},$$

donde

$$(x_0, \dots, x_n) \sim (x'_0, \dots, x'_n) \iff \exists \lambda \in K, \lambda \neq 0 \mid (x'_0, \dots, x'_n) = \lambda(x_0, \dots, x_n).$$

Los elementos de $\mathbb{P}^n(K)$ se llaman puntos y son de la forma

$$[(x_0, \dots, x_n)] = \langle (x_0, \dots, x_n) \rangle - \{(0, \dots, 0)\},$$

donde $\langle (x_0, \dots, x_n) \rangle$ es el subespacio vectorial de K^{n+1} generado por (x_0, \dots, x_n) . Denotaremos $[(x_0, \dots, x_n)]$ por $(x_0 : \dots : x_n)$. Se dice que (x_0, \dots, x_n) es un sistema de coordenadas homogéneas de $(x_0 : \dots : x_n)$.

Una diferencia importante entre el espacio afín y el proyectivo es que los polinomios del anillo $K[X_0, \dots, X_n]$ no definen funciones sobre $\mathbb{P}^n(K)$ puesto que sus valores en un punto $\bar{x} \in \mathbb{P}^n(K)$ dependen del sistema de coordenadas homogéneas elegido. Sin embargo puede hablarse de ceros proyectivos de un polinomio.

Definición 4.2. Se dice que un polinomio $F \in K[X_1, \dots, X_n]$ es un *polinomio homogéneo* de grado r , si es de la forma

$$F = \sum_{i_1 + \dots + i_n = r} a_{i_1 \dots i_n} X_1^{i_1} \dots X_n^{i_n}$$

Definición 4.3. Sea $F \in K[X_0, \dots, X_n]$ y $\bar{x} \in \mathbb{P}^n(K)$. Se dice que \bar{x} es un *cero* de F , si se tiene que $F(x_0, \dots, x_n) = 0$, para todo sistema (x_0, \dots, x_n) de coordenadas homogéneas de \bar{x} . Si \bar{x} es un cero de F , escribiremos $F(\bar{x}) = 0$.

Observación 4.4. ([8, Chapitre II, Proposition-définition 4.1]) Si $F \in K[X_0, \dots, X_n]$ es un polinomio homogéneo, entonces es suficiente para que \bar{x} sea un cero proyectivo de F que $F(x_0, \dots, x_n) = 0$, para un sistema de coordenadas homogéneas (x_0, \dots, x_n) de \bar{x} . Si $F = F_0 + F_1 + \dots + F_r$ con F_i homogéneo de grado i , entonces \bar{x} es un cero proyectivo de F si y solo si, $F_i(x_0, \dots, x_n) = 0$ para un sistema de coordenadas homogéneas (x_0, \dots, x_n) de \bar{x} y para $i = 0, \dots, r$.

Definición 4.5. Sea $S \subset K[X_0, \dots, X_n]$. Se llama *variedad algebraica proyectiva* definida por S al conjunto

$$Z_p(S) = \{\bar{x} \in \mathbb{P}^n(K) \mid F(\bar{x}) = 0, \forall F \in S\}.$$

Si K es un cuerpo algebraicamente cerrado y $F \in K[X_0, \dots, X_n]$ es un polinomio homogéneo, $F \notin K$, el conjunto $Z_p(F)$ se dice que es una *hipersuperficie proyectiva* de $\mathbb{P}^n(K)$. Si S es un conjunto de polinomios homogéneos de grado 1, entonces se dice que $Z_p(S)$ es una *variedad lineal proyectiva*.

Observación 4.6. Si I es el ideal generado por S , entonces $Z_p(S) = Z_p(I)$ y por el teorema de la base de Hilbert (2.28), podemos suponer que S es finito; además por la observación 4.4, podemos suponer que S está formado por polinomios homogéneos.

Se tienen las siguientes propiedades análogas a las del caso afín:

- (1) $Z_p(\{0\}) = \mathbb{P}^n(K)$.
- (2) Sea $\mathfrak{m} = \langle X_0, \dots, X_n \rangle$ el ideal de polinomio sin términos constantes. Se tiene que $Z_p(\mathfrak{m}) = Z_p(X_0, \dots, X_n) = \emptyset$. También, $Z_p(K[X_0, \dots, X_n]) = \emptyset$.
- (3) Si S y S' son subconjuntos de $K[X_0, \dots, X_n]$ y $S \subset S'$, entonces $Z_p(S') \subset Z_p(S)$.
- (4) Si $\{S_i\}_{i \in I}$ es un conjunto de subconjuntos de $\mathbb{P}^n(K)$, entonces

$$\bigcap_{i \in I} Z_p(S_i) = Z_p\left(\bigcup_{i \in I} S_i\right),$$

- (5) Si S_1, \dots, S_r son subconjuntos de $\mathbb{P}^n(K)$, entonces

$$\bigcup_{i=1}^r Z_p(S_i) = Z_p\left(\bigcap_{i=1}^r S_i\right).$$

y por tanto, la intersección y la unión finita de variedades algebraicas proyectivas es una variedad algebraica proyectiva.

Los variedades algebraicas proyectivas son los cerrados de una topología en $\mathbb{P}^n(K)$ llamada *topología de Zariski* de $\mathbb{P}^n(K)$. Sobre las variedades proyectivas de $\mathbb{P}^n(K)$ consideraremos la topología relativa. Si V y W son variedades algebraicas proyectivas de $\mathbb{P}^n(K)$ y $W \subset V$, diremos que W es una subvariedad de V .

Definición 4.7. Se dice que un ideal de $K[X_0, \dots, X_n]$ es homogéneo si tiene un conjunto de generadores formado por polinomios homogéneos.

Observación 4.8. Se verifica que un ideal \mathfrak{a} de $K[X_1, \dots, X_n]$ es homogéneo si, y solo si, verifica la siguiente condición: Si $F = F_0 + F_1 + \dots + F_r \in \mathfrak{a}$ y F_i es homogéneo de grado i , para $i = 1, \dots, r$, entonces $F_i \in \mathfrak{a}$, para $i = 1, \dots, r$, [8, Chapitre II, Proposition-définition 7.2].

Definición 4.9. Sea V una variedad algebraica proyectiva de $\mathbb{P}^n(K)$ y sea $p: K^{n+1} - \{(0, \dots, 0)\} \rightarrow \mathbb{P}^n(K)$ la aplicación $p(x_0, \dots, x_n) = (x_0 : \dots : x_n)$. Se llama *cono* de V al conjunto

$$C(V) = p^{-1}(V) \cup \{(0, \dots, 0)\} = \{(x_0, \dots, x_n) \in K^{n+1} \mid (x_0 : \dots : x_n) \in V\} \cup \{(0, \dots, 0)\}.$$

Observación 4.10. Si \mathfrak{a} es un ideal homogéneo de $K[X_0, \dots, X_n]$, $\mathfrak{a} \neq \langle X_0, \dots, X_n \rangle$ y $V = Z_p(\mathfrak{a})$, entonces $C(V) = Z(\mathfrak{a})$ es una variedad algebraica afín; en particular, si $\mathfrak{a} = \langle X_0, \dots, X_n \rangle$ entonces $C(V) = Z(X_0, \dots, X_n) = \{0, \dots, 0\}$.

El concepto de cono permite relacionar un problema proyectivo con su problema análogo afín.

Definición 4.11. Sea S un subconjunto de $\mathbb{P}^n(K)$. Se llama *ideal* de S al conjunto

$$I_p(S) = \{F \in K[X_0, \dots, X_n] \mid F(\bar{x}) = 0, \forall \bar{x} \in S\}$$

Se tiene

- (1) Si $S \subset \mathbb{P}^n(K)$, entonces $I_p(S)$ es un ideal radical homogéneo.
- (2) Sea S y S' subconjuntos de $\mathbb{P}^n(K)$. Si $S \subset S'$, entonces $I_p(S') \subset I_p(S)$
- (3) Si V es una variedad algebraica proyectiva, entonces $Z_p(I_p(V)) = V$. Si I es un ideal de $K[X_0, \dots, X_n]$, entonces $I \subset I_p(Z_p(I))$.
- (4) $I_p(\mathbb{P}^n(K)) = \{0\}$, $I_p(\emptyset) = K[X_0, \dots, X_n]$.

Lo mismo que en el caso afín se tienen los siguientes resultados:

Proposición 4.12. *Si consideramos en cada variedad algebraica proyectiva de $\mathbb{P}^n(K)$ su topología de Zariski, una variedad algebraica proyectiva V es irreducible si, y solo si, $I_p(V)$ es un ideal primo.*

Demostración. Es similar a la demostración en el caso afín. □

Teorema 4.13. (Teorema proyectivo de los ceros, [2, Capítulo 4, pag 61]) *Sea K un cuerpo algebraicamente cerrado y \mathfrak{a} un ideal homogéneo de $K[X_0, \dots, X_n]$ tal que $Z_p(\mathfrak{a}) \neq \emptyset$. Se tiene que $I_p(Z_p(\mathfrak{a})) = \text{rad } \mathfrak{a}$.*

Ejemplos 4.14. (1) Dado que $I_p(\mathbb{P}^n(K)) = \{0\}$, el espacio proyectivo $\mathbb{P}^n(K)$ es irreducible.

(2) Toda variedad lineal proyectiva de $\mathbb{P}^n(K)$ es irreducible. En efecto, si $V = Z_p(F_1, \dots, F_r)$ donde $F_i \in K[X_0, \dots, X_n]$ es un polinomio homogéneo de grado 1, para $i = 1, \dots, r$, es una variedad lineal no vacía, entonces la variedad lineal afín $Z(F_1, \dots, F_r) = C(V)$ es un espacio vectorial de dimensión $s = n+1 - \dim_K \langle F_1, \dots, F_r \rangle$. Sea $B = \{(a_{0i}, \dots, a_{ni}) \mid i = 1, \dots, s\}$ una base de $C(V)$. La aplicación $f: K^s \rightarrow C(V)$, dada por

$$f(y_1, \dots, y_s) = (a_{01}y_1 + \dots + a_{0s}y_s, \dots, a_{n1}y_1 + \dots + a_{ns}y_s),$$

es un isomorfismo de espacios vectoriales y un homeomorfismo de variedades algebraicas afines. La aplicación $\mathbb{P}(f): \mathbb{P}^{s-1}(K) \rightarrow V$ dada por

$$\mathbb{P}(f)(y_1 : \dots : y_s) = (a_{01}y_1 + \dots + a_{0s}y_s : \dots : a_{n1}y_1 + \dots + a_{ns}y_s)$$

es un homeomorfismo de variedades lineales proyectivas.

(3) Si K es un cuerpo algebraicamente cerrado y $F \in K[X_0, \dots, X_n]$ es un polinomio homogéneo irreducible entonces $Z_p(F)$ es una hipersuperficie irreducible.

Proposición 4.15. *Si V es un conjunto algebraico proyectivo no vacío, entonces V se puede escribir de forma única (salvo una permutación) de la forma $V = V_1 \cup \dots \cup V_s$, donde V_i es una variedad algebraica proyectiva irreducible, para $i = 1, \dots, s$, y $V_i \not\subset V_j$, si $i \neq j$.*

Los V_i se llaman componentes irreducibles de V . Si W es una subvariedad de V , entonces W está contenido en una componente irreducible de V . Así, las componentes irreducibles de V son las subvariedades irreducibles maximales de V .

Definición 4.16. Sea V una variedad algebraica proyectiva de $\mathbb{P}^n(K)$ y sea $I_p(V)$ su ideal. Se llama anillo de coordenadas homogéneas de V al anillo cociente:

$$\Gamma_h(V) = K[X_0, \dots, X_n]/I_p(V)$$

El anillo $\Gamma_h(V)$ es un anillo graduado. Se dice que un elemento $f \in \Gamma_h(V)$ es *homogéneo de grado r* si $f = F + I_p(V)$, siendo F un polinomio homogéneo de grado r de $K[X_0, \dots, X_n]$.

Se dice que un ideal de $\Gamma_h(V)$ es *homogéneo* si tiene un conjunto de generadores homogéneos.

Sea $f = F + I_p(V) \in \Gamma_p(V)$. Se dice que $\bar{x} \in V$ es un *cero* de f y escribiremos $f(\bar{x}) = 0$, si $F(\bar{x}) = 0$.

Observación 4.17. El concepto de grado de un elemento homogéneo $f \neq 0$ de $\Gamma_h(V)$ está bien definido. Si $f = F + I_p(V) = G + I_p(V)$ donde F y G son polinomios homogéneos, entonces el grado de F es igual al grado de G . En efecto, se tiene que $F - G \in I_p(V)$ y entonces si el grado de F es distinto del grado de G por la observación 4.8, $F, G \in I_p(V)$, con lo cual $f = 0$.

Los elementos de $\Gamma_h(V)$ no definen funciones polinómicas en V puesto que el valor de f en \bar{x} depende del sistema de coordenadas homogéneas que consideremos. Sin embargo, si $f \in \Gamma_h(V)$ que \bar{x} sea un cero de f no depende del polinomio que represente a f . En efecto, si $f = F + I_p(V) = G + I_p(V)$, se tiene $F - G \in I_p(V)$ y entonces $(F - G)(\bar{x}) = 0$, para todo $\bar{x} \in V$. Así, $F(\bar{x}) = G(\bar{x})$.

Notación 4.18. Si f_1, \dots, f_r son elementos homogéneos de grado > 0 de $\Gamma(V)$ entonces escribiremos $Z_p(f_1, \dots, f_s) = \{\bar{x} \in V \mid f_i(\bar{x}) = 0, i = 1, \dots, r\}$. Si $V = Z_p(G_1, \dots, G_s)$ donde G_i es un polinomio homogéneo, para $i = 1, \dots, s$ y $f_i = F_i + I_p(V)$ donde F_i es un polinomio de homogéneo, entonces $Z_p(f_1, \dots, f_r) = Z_p(G_1, \dots, G_s, F_1, \dots, F_r)$ es un cerrado de V .

Proposición 4.19. *Sea V un conjunto algebraico proyectivo y sea $f = F + I_p(V) \in \Gamma_h(V)$ un elemento homogéneo de grado > 0 . El conjunto*

$$D^+(f) = \{\bar{x} \in V \mid f(\bar{x}) \neq 0\},$$

es un abierto de V .

Demostración. $D^+(f) = V \cap (\mathbb{P}^n(K) - Z_p(F))$. □

Proposición 4.20. *Sea V un conjunto algebraico proyectivo. Todo abierto no vacío de V es unión de abiertos de la forma $D^+(f)$, donde $f \in \Gamma_h(V)$.*

Demostración. Sea U un abierto no vacío de V y sea $V - U = Z_p(F_1, \dots, F_r)$, donde $F_i \in K[X_0, \dots, X_n]$ es homogéneo de grado > 0 . Si $f_i = F_i + I_p(V)$, entonces

$$U = V \cap (\mathbb{P}^n(K) - Z_p(F_1, \dots, F_r)) = V \cap \left(\bigcup_{i=1}^r (\mathbb{P}^n(K) - Z_p(F_i)) \right) = \bigcap_{i=1}^r D^+(f_i). \quad \square$$

Definición 4.21. Sea $F \in K[X_1, \dots, X_n]$ y $F = F_0 + F_1 + \dots + F_r$, donde F_i es un polinomio homogéneo de grado i , para $i = 1, \dots, r$. Se llama polinomio homogeneizado de F respecto a la variable X_0 al siguiente polinomio de $K[X_0, \dots, X_n]$

$$F^{\sharp_0} = F_0 X_0^r + F_1 X_0^{r-1} + \dots + F_r.$$

Si $G \in K[X_0, \dots, X_n]$, se llama polinomio deshomonogeneizado de G respecto a la variable X_0 al siguiente polinomio de $K[X_1, \dots, X_n]$:

$$G^{\flat_0} = G(1, X_1, \dots, X_n).$$

Definición 4.22. La aplicación:

$$\begin{aligned} j_0: K^n &\longrightarrow \mathbb{P}^n(K) \\ (x_1, \dots, x_n) &\rightsquigarrow (1 : x_1 : \dots : x_n) \end{aligned}$$

se dice que es *un encaje del espacio afín K^n en el espacio proyectivo $\mathbb{P}^n(K)$* . El hiperplano $Z_p(X_0)$ se llama *hiperplano de puntos del infinito* respecto al encaje j_0 y sus puntos los *puntos del infinito*.

Definición 4.23. Se llama *complección proyectiva* de la variedad algebraica afín $V \subset K^n$ a la menor variedad proyectiva de $\mathbb{P}^n(K)$ que contiene a $j_0(V)$, es decir a la clausura de $j_0(V)$ respecto a la topología de Zariski de $\mathbb{P}^n(K)$; la denotaremos por \bar{V} . El conjunto $\bar{V} \cap Z_p(X_0)$ se dice que es el conjunto de puntos del infinito de la variedad algebraica V respecto al encaje j_0 .

Lema 4.24. *Se tiene*

- (1) Si $V = Z(F_1, \dots, F_m)$, $F_i \in K[X_1, \dots, X_n]$, para $i = 1, \dots, m$, entonces $j_0(V) = \bar{V} \cap D^+(X_0)$.
- (2) Sea $W = Z_p(G_1, \dots, G_m) \subset \mathbb{P}^n(K)$, $W \not\subset Z_p(X_0)$, donde $G_i \in K[X_0, \dots, X_n]$ son polinomio homogéneos, para $i = 1, \dots, m$, entonces $j_0^{-1}(W \cap D^+(X_0)) = Z(G_1^{\flat_0}, \dots, G_m^{\flat_0})$.

Demostración. (1) Sea para cada $i = 1, \dots, m$, $F_i = F_{i_0} + F_{i_1} + \dots + F_{i_{r_i}}$, siendo $F_{i_k} \in K[X_1, \dots, X_n]$ un polinomio homogéneo de grado k , $k = 1, \dots, r_i$. Entonces, para todo $i = 1, \dots, m$,

$$F_i^{\sharp} = X_0^{r_i} F_{i_0} + X_0^{r_i-1} F_{i_1} + \dots + F_{i_{r_i}} \in K[X_0, \dots, X_n].$$

Veamos que $j_0(V) \subset Z_p(F_1^{\sharp}, \dots, F_m^{\sharp})$. Si $(x_1, \dots, x_n) \in V$, entonces $(1 : x_1 : \dots : x_n) \in j_0(V)$ y se tiene

$$\begin{aligned} F_i^{\sharp}(1, x_1, \dots, x_n) &= F_{i_0}(x_1, \dots, x_n) + \dots + F_{i_{r_i}}(x_1, \dots, x_n) \\ &= F_i(x_1, \dots, x_n) = 0, \quad i = 1, \dots, m \end{aligned}$$

Por tanto, $\bar{V} \subset Z_p(F_1^\sharp, \dots, F_m^\sharp)$.

Veamos que $Z_p(F_1^\sharp, \dots, F_m^\sharp) \cap D^+(X_0) \subset j_0(K^n)$. En efecto,

$$\begin{aligned} (x_0 : x_1 : \dots : x_n) &\in Z_p(F_1^\sharp, \dots, F_m^\sharp) \cap D^+(X_0) \\ &\Rightarrow (x_0 : x_1 : \dots : x_n) = (1 : x_0^{-1}x_1 : \dots : x_0^{-1}x_n), \\ &F_i(x_0^{-1}x_1, \dots, x_0^{-1}x_n) = F_i^\sharp(1, x_0^{-1}x_1, \dots, x_0^{-1}x_n) = 0, \quad i = 1, \dots, m, \end{aligned}$$

y entonces $(x_0^{-1}x_1, \dots, x_0^{-1}x_n) \in V$ y $(x_0 : x_1 : \dots : x_n) \in j_0(V)$.

Dado que $\bar{V} \subset Z_p(F_1^\sharp, \dots, F_m^\sharp) \cap D^+(X_0)$ y $j_0(V) \subset \bar{V}$, se tiene

$$j_0(V) \subset \bar{V} \cap j_0(K^n) \subset Z_p(F_1^\sharp, \dots, F_m^\sharp) \cap D^+(X_0) = j_0(V),$$

y entonces $j_0(V) = \bar{V} \cap j_0(K^n)$.

(2) Si $(x_1, \dots, x_n) \in Z(G_1^\flat, \dots, G_m^\flat)$, entonces $G_i(1, x_1, \dots, x_n) = 0$, para $i = 1, \dots, m$. Así, $(1 : x_1 : \dots : x_n) \in W \cap D^+(X_0)$, por lo que $(x_1, \dots, x_n) \in j_0^{-1}(W \cap D^+(X_0))$.

Si $(x_1, \dots, x_n) \in j^{-1}(W \cap D^+(X_0))$, tenemos que $(1 : x_1 : \dots : x_n) \in W \cap D^+(X_0)$ y entonces $G_i(1, x_1, \dots, x_n) = G_i^\flat(x_1, \dots, x_n) = 0$ para $i = 1, \dots, m$, y por tanto $(x_1, \dots, x_n) \in Z(G_1^\flat, \dots, G_m^\flat)$. \square

Observación 4.25. Si $V = Z(F_1, \dots, F_m)$ es una variedad algebraica afín, se puede probar que $\bar{V} = Z_p(\langle G^\sharp \mid G \in I(V) \rangle) = Z_p(\langle G^\sharp \mid G \in \text{rad} \langle F_1, \dots, F_m \rangle \rangle)$, que en general no coincide con $Z_p(F_1^\sharp, \dots, F_m^\sharp)$ (véase la proposición 3 y el ejercicio 4-20 del capítulo 4 de Fulton [2]). En algunos casos coinciden, por ejemplo si $V = Z(F_1, \dots, F_m)$ es una variedad lineal, entonces $\bar{V} = Z_p(F_1^\sharp, \dots, F_m^\sharp)$ y si $V = Z(F)$ es una hipersuperficie, entonces $\bar{V} = Z_p(F^\sharp)$.

Corolario 4.26. *El encaje $j_0: K^n \rightarrow \mathbb{P}^n(K)$, $j_0(x_1, \dots, x_n) = (1 : x_1 : \dots : x_n)$ es una aplicación biyectiva y continua que define un homeomorfismo en su imagen $D^+(X_0)$.*

Demostración. Se sigue del lema 4.24. \square

Observación 4.27. Las aplicaciones $j_i: K^n \rightarrow \mathbb{P}^n(K)$, $j_i(x_1, \dots, x_n) = (x_1 : \dots : 1 : \dots : x_n)$, para $i = 2, \dots, n$, se dice también que son encajes del espacio afín K^n en $\mathbb{P}^n(K)$; el hiperplano $Z_p(X_i)$ se dice que es el hiperplano de puntos del infinito respecto al encaje j_i . La aplicación j_i es una aplicación biyectiva y continua que define un homeomorfismo en su imagen $D^+(X_i)$.

Definición 4.28. Se dice que un abierto de una variedad algebraica proyectiva es un abierto afín si es homeomorfo a una variedad algebraica afín.

Observación 4.29. Los abiertos $D^+(X_i)$, para $i = 1, \dots, n$, de $\mathbb{P}^n(K)$ son abiertos afines puesto que son homeomorfos a K^n . Se puede probar que si V es una variedad algebraica proyectiva y $f \in \Gamma^+(V)$, entonces $D^+(f)$ es un abierto afín de V .

Capítulo 5

Dimensión

En este capítulo K denotará un cuerpo algebraicamente cerrado.

5.1. Dimensión topológica. Relación con la dimensión de Krull

Comenzaremos dando la definición topológica de dimensión. Deduciremos que toda subvariedad algebraica de una variedad algebraica irreducible tiene dimensión más pequeña que la variedad inicial.

Definición 5.1. Sea X un conjunto. Una cadena de longitud n de partes de X es una sucesión de subconjuntos de X

$$X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_n$$

tales que $X_i \neq X_j$ si $i \neq j$.

Definición 5.2. Sea X un espacio topológico. La dimensión de X es el supremo de las longitudes de todas las cadenas de cerrados irreducibles de X . Es un entero ≥ 0 o $+\infty$. Denotaremos la dimensión de X por $\dim X$.

Proposición 5.3. *Sea X un espacio topológico. Se tiene*

- (1) *Si Y es un subespacio de X , entonces $\dim Y \leq \dim X$.*
- (2) *Si X es irreducible y de dimensión finita e Y es un cerrado de X , $Y \neq X$, entonces $\dim Y < \dim X$.*

Demostración. (1) Sea $C_1 \subsetneq \cdots \subsetneq C_n$ una cadena de subespacios cerrados irreducibles de Y . Por la proposición 3.16 (1), $\overline{C_1} \subseteq \cdots \subseteq \overline{C_n}$ es una cadena de subespacios cerrados

irreducibles de X . Como para $i = 1, \dots, n$, $C_i = \overline{C_i} \cap Y$, por ser $C_i \neq C_j$ si $i \neq j$, necesariamente $\overline{C_i} \neq \overline{C_j}$ si $i \neq j$. Por tanto, $\dim X \geq n = \dim Y$.

(2) Sea $C_1 \subsetneq \dots \subsetneq C_n$ una cadena de subespacios cerrados irreducibles de Y , entonces $C_1 \subsetneq \dots \subsetneq C_n \subsetneq X$ es una cadena de subespacios cerrados irreducibles de X . \square

Proposición 5.4. *Sea X un espacio topológico y X_i , $i = 1, \dots, r$ cerrados de X . Si $X = \cup_{i=1}^r X_i$, entonces*

$$\dim X = \sup \dim X_i$$

Demostración. Por la proposición 5.3 (1), $\dim X \geq \sup \dim X_i$. Sea $p = \sup \dim X_i$, y supongamos que es finito, ya que en caso contrario el resultado es trivial. Supongamos que existe una cadena $C_1 \subsetneq \dots \subsetneq C_{p+1}$ de cerrados irreducibles de X . Se tiene que $C_{p+1} = \cup_{i=1}^n (X_i \cap C_{p+1})$, donde cada elemento de la unión es cerrado. Entonces, por ser C_{p+1} irreducible, necesariamente $C_{p+1} \subset X_i$ para algún i , lo cual contradice que $\dim X_i \leq p$. \square

Ejemplo 5.5. Las variedades algebraicas afines de K^n de dimensión cero son los conjuntos finitos. En efecto, todo conjunto con un único elemento es una variedad algebraica afín de dimensión cero, y entonces por la proposición 5.4, todo conjunto finito es una variedad algebraica afín de dimensión cero.

Recíprocamente, sea V una variedad algebraica afín irreducible de dimensión cero y $P \in V$. Si $\{P\} \subsetneq V$, entonces $\dim V \geq 1$. Por tanto, $V = \{P\}$. Si V es una variedad algebraica afín de dimensión cero pero no es irreducible, entonces es unión finita de variedades algebraicas afines irreducibles de dimensión cero (sus componentes irreducibles), es decir V es un conjunto finito.

Vamos a recordar la definición de dimensión de Krull de un anillo A .

Definición 5.6. Sea A un anillo conmutativo y unitario. Se llama dimensión de A al supremo de las longitudes de las cadenas de ideales primos de A . Se denota por $\dim_{\text{Krull}} A$.

Un cuerpo tiene dimensión cero. Un dominio de ideales principales tiene dimensión 1. El anillo de polinomios $K[X_1, \dots, X_n]$ tiene dimensión $\geq n$ puesto que tenemos la cadena de ideales primos

$$(0) \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq \dots \subsetneq (X_1, \dots, X_n).$$

Veremos que este anillo tiene dimensión n .

Proposición 5.7. *Sea K un cuerpo algebraicamente cerrado, V una variedad algebraica afín de K^n y sea $\Gamma(V)$ su anillo de funciones regulares. Se tiene*

$$\dim V = \dim_{\text{Krull}} \Gamma(V).$$

Demostración. Este resultado es consecuencia de la biyección decreciente (proposición 3.24) entre los cerrados irreducibles de V y los ideales primos de $\Gamma(V)$. \square

Probaremos en la siguiente sección que la dimensión de una variedad algebraica afín irreducible coincide con el grado de trascendencia sobre K del cuerpo $K(V)$ de funciones racionales sobre V .

5.2. Dimensión de las K -álgebras finitamente generadas

En esta sección K es un cuerpo y A es una K -álgebra finitamente generada que es un dominio entero. Probaremos que la dimensión de krull de A coincide con el grado de trascendencia del cuerpo de fracciones de A sobre K . Para simplificar la notación definiremos el concepto de grado de trascendencia de A sobre K .

Definición 5.8. Se llama grado de trascendencia de A sobre K , y se denota por $\text{tr deg}_K(A)$, al grado de trascendencia del cuerpo de fracciones L de A sobre K , es decir

$$\text{tr deg}_K A := \text{tr deg}_K L$$

Obsérvese que el grado de trascendencia de A sobre K es finito por el corolario 1.35, puesto el cuerpo de fracciones L de A es de generación finita sobre K .

Lema 5.9. Si F es un polinomio irreducible de $K[X_1, \dots, X_n]$, entonces se tiene

$$\text{tr deg}_K K[X_1, \dots, X_n]/\langle F \rangle = n - 1.$$

Demostración. Por ser F no constante, existe algún i para el cual la variable X_i aparece en F . Supongamos que se trata de X_n , entonces X_n aparece en todo múltiplo no nulo de F . Por tanto, no existe ningún $G \in K[X_1, \dots, X_{n-1}]$ no nulo que esté en $\langle F \rangle$. En consecuencia, $X_1 + \langle F \rangle, \dots, X_{n-1} + \langle F \rangle$ son algebraicamente independientes. Como $X_n + \langle F \rangle$ es algebraico sobre $K[X_1, \dots, X_{n-1}]/\langle F \rangle$, $\{X_1 + \langle F \rangle, \dots, X_{n-1} + \langle F \rangle\}$ es una base de trascendencia de $K[X_1, \dots, X_n]/\langle F \rangle$ sobre K . \square

Lema 5.10. Sea \mathfrak{p} un ideal primo de A , $\mathfrak{p} \neq \{0\}$. Se tiene

$$\text{tr deg}_K A/\mathfrak{p} < \text{tr deg}_K A.$$

Demostración. Pongamos

$$A = K[X_1, \dots, X_n]/\mathfrak{a} = K[x_1, \dots, x_n], \quad x_i = X_i + \mathfrak{a}, \quad i = 1, \dots, n$$

para cada $f \in A$ denotamos la imagen de f en A/\mathfrak{p} como \bar{f} . En particular, $A/\mathfrak{p} = K[\bar{x}_1, \dots, \bar{x}_n]$. Sea $d = \text{tr deg}_K(A/\mathfrak{p})$. Por el corolario 1.35, existe un conjunto $S \subset \{\bar{x}_1, \dots, \bar{x}_n\}$ con d elementos que es una base de trascendencia de $K(\bar{x}_1, \dots, \bar{x}_n)$ sobre K . Reordenando los elementos $\bar{x}_1, \dots, \bar{x}_n$ podemos suponer que $S = \{\bar{x}_1, \dots, \bar{x}_d\}$. Veamos que para todo $f \in \mathfrak{p}$, $f \neq 0$, los $d + 1$ elementos x_1, \dots, x_d, f son algebraicamente independientes; probado esto ya tenemos que $\text{tr deg}_K A \geq d + 1$.

Si x_1, \dots, x_d, f son algebraicamente dependientes sobre K , entonces existe una relación algebraica de la forma

$$a_m(x_1, \dots, x_d)f^m + a_{m-1}(x_1, \dots, x_d)f^{m-1} + \dots + a_0(x_1, \dots, x_d) = 0, \quad (*)$$

donde $a_i \in K[X_1, \dots, X_d]$, para $i = 0, \dots, m$, y $a_m \neq 0$. Dado que A es un dominio entero, podemos suprimir, si es necesario, potencias de f hasta tener una expresión como la (*) donde $a_0(x_1, \dots, x_d) \neq 0$. Entonces aplicando el homomorfismo $A \rightarrow A/\mathfrak{p}$ que lleva a en $a + \mathfrak{p}$, obtenemos que $a_0(\bar{x}_1, \dots, \bar{x}_d) = 0$, lo que contradice la independencia algebraica de $\bar{x}_1, \dots, \bar{x}_d$. \square

Proposición 5.11. *Sea A un anillo de polinomios y sea \mathfrak{p} un ideal primo de A , tal que $\text{tr deg}_K A/\mathfrak{p} = \dim A - 1$. Existe $F \in K[X_1, \dots, X_n]$ tal que $\mathfrak{p} = \langle F \rangle$.*

Demostración. El ideal \mathfrak{p} es distinto de cero, puesto que A y A/\mathfrak{p} tienen distinto grado de trascendencia. Por tanto, \mathfrak{p} tiene un elemento distinto de cero y por \mathfrak{p} primo contiene un polinomio irreducible F . El ideal $\langle F \rangle$ es primo. Si $\langle F \rangle \neq \mathfrak{p}$, dado que los anillos $(A/\langle F \rangle)/(\mathfrak{p}/\langle F \rangle)$ y A/\mathfrak{p} son isomorfos, por el lema 5.10, $\text{tr deg}_K A/\mathfrak{p} < \text{tr deg}_K A/\langle F \rangle$, y por el lema 5.9,

$$\text{tr deg}_K A/\langle F \rangle = \text{tr deg}_K A - 1 = n - 1.$$

Llegaríamos así a que $\text{tr deg}_K A/\mathfrak{p} < n - 1$, lo cual contradice la hipótesis. En consecuencia, $\mathfrak{p} = \langle F \rangle$. \square

Obsérvese que si V una variedad algebraica irreducible de K^n entonces el anillo de coordenadas $\Gamma(V)$ es una K -álgebra finitamente generada que es un dominio entero.

Teorema 5.12. *Sea V una variedad algebraica irreducible de K^n . Sea $f \in \Gamma(V)$, $f \neq 0$ y tal que f no es una unidad de $\Gamma(V)$ y sea \mathfrak{p} un ideal primo de $\Gamma(V)$ minimal entre los ideales primos de $\Gamma(V)$ que contienen a $\langle f \rangle$. Se tiene*

$$\text{tr deg}_K \Gamma(V)/\mathfrak{p} = \text{tr deg}_K K(V) - 1.$$

Demostración. Sea

$$Z(f) = Z_1 \cup \dots \cup Z_r, \quad (*)$$

la descomposición de $Z(f)$ en componentes irreducibles. Por la correspondencia dada en la proposición 3.24, tenemos que $Z_i = Z(\mathfrak{p}_i)$, donde \mathfrak{p}_i es un ideal primo de $\Gamma(V)$ para $i = 1, \dots, r$. Aplicando I_V a la igualdad (*) se tiene

$$\text{rad}\langle f \rangle = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_r, \quad (**)$$

con $\mathfrak{p}_i \not\subset \mathfrak{p}_j$ para $i \neq j$.

Dado que Z_1 es irreducible y que $Z_1 \not\subset Z_i$, para todo $i \neq 1$, se tiene que $Z_1 \not\subset \bigcup_{i \geq 2} Z_i$. Sea $P \in Z_1 - \bigcup_{i \geq 2} Z_i$ y consideremos el abierto $U = V - \bigcup_{i \geq 2} Z_i$ de V .

Por la proposición 3.26, existe $h \in \Gamma(V)$ tal que $P \in D(h) \subset U$. Dado que $D(h) \cap \bigcup_{i \geq 2} Z_i = \emptyset$, entonces $\bigcup_{i \geq 2} Z_i \subset Z(h)$ y por el teorema de los ceros de Hilbert, $\text{rad}\langle h \rangle = I_V(Z(h)) \subset \bigcap_{i \geq 2} \mathfrak{p}_i$. Así, $h \in \bigcap_{i \geq 2} \mathfrak{p}_i$. Se tiene

$$P \in D(h) \cap Z_1 \Rightarrow h(P) \neq 0, \quad g(P) = 0, \quad \forall g \in \mathfrak{p}_1 \Rightarrow h \notin \mathfrak{p}_1.$$

Sea $S = \{h^n \mid n \geq 0\}$ y consideremos el homomorfismo de anillos $A \rightarrow A_h$ que lleva a en $a/1$. Aplicando este homomorfismo a la igualdad (**) se tiene

$$\text{rad}\langle f/1 \rangle = S^{-1}\mathfrak{p}_1 \cap \dots \cap S^{-1}\mathfrak{p}_r = S^{-1}\mathfrak{p}_1,$$

puesto que $h \in \mathfrak{p}_i$, para $i = 2, \dots, r$, y entonces por la proposición 2.7 (2), $S^{-1}\mathfrak{p}_i = \Gamma(V)$, para $i = 2, \dots, r$. Dado que $\text{rad}\langle f/1 \rangle = S^{-1}\mathfrak{p}_1$, se tiene que $S^{-1}\mathfrak{p}_1$ es un primo minimal entre los que contienen a $f/1$. Teniendo en cuenta que $\Gamma(V)$ y $\Gamma(V)_h$ tienen el mismo cuerpo de fracciones y que lo mismo ocurre con $\Gamma(V)/\mathfrak{p}_1$ y $\Gamma(V)_h/S^{-1}\mathfrak{p}_1$, se tiene

$$\text{tr deg}_K K(V) = \text{tr deg}_K \Gamma(V)_h, \quad \text{tr deg}_K \Gamma(V)_h/S^{-1}\mathfrak{p}_1 = \text{tr deg}_K \Gamma(V)/\mathfrak{p}_1,$$

podemos reemplazar $\Gamma(V)$ por $\Gamma(V)_h$ y suponer que $\text{rad}\langle f \rangle$ es igual a un ideal primo \mathfrak{p} .

Por el lema de normalización de Noether, si $\text{tr deg}_K \Gamma(V) = d$, existen d elementos algebraicamente independientes $x_1, \dots, x_d \in \Gamma(V)$ tales que $\Gamma(V)$ es una $K[x_1, \dots, x_d]$ -álgebra finita. Por la proposición 2.23, $K(V)$ es una extensión finita de $K(x_1, \dots, x_d)$. Si $\alpha \in K(V)$ denotaremos por $\text{Nm}(\alpha)$ la norma de α respecto a esta extensión de cuerpos.

El anillo $K[x_1, \dots, x_d]$ es un dominio íntegramente cerrado, el cuerpo de fracciones de $\Gamma(V)$ es una extensión finita de $K(x_1, \dots, x_d)$ y f es entero sobre $K[x_1, \dots, x_d]$. Por el lema 2.25, $F_0 = \text{Nm}(f) \in K[x_1, \dots, x_d]$ y f divide a F_0 en $\Gamma(V)$.

Veamos que $\mathfrak{p} \cap K[x_1, \dots, x_n] = \text{rad}\langle F_0 \rangle$. Probaremos que $\mathfrak{p} \cap K[x_1, \dots, x_n] = \text{rad}\langle F_0 \rangle$. Probado esto, se tiene que el homomorfismo

$$\varphi: K[x_1, \dots, x_d]/\text{rad}\langle F_0 \rangle \rightarrow A/\mathfrak{p}$$

dado por $\varphi(G + \text{rad}\langle F_0 \rangle) = G + \mathfrak{p}$ es inyectivo. Por la proposición 2.22 (1), A/\mathfrak{p} es una $K[x_1, \dots, x_d]/\text{rad}\langle F_0 \rangle$ -álgebra entera y por la proposición 2.23,

$$\text{tr deg}_K \Gamma(V)/\mathfrak{p} = \text{tr deg}_K K[x_1, \dots, x_d]/\text{rad}\langle F_0 \rangle$$

Dado que $K[x_1, \dots, x_d]$ es un anillo factorial (por ser isomorfo a un anillo de polinomios) y el ideal $\text{rad}\langle F_0 \rangle$ es un ideal primo, entonces existe un polinomio irreducible $G \in \text{rad}\langle F_0 \rangle$, tal que $\langle F_0 \rangle = \langle G \rangle$ y por la proposición 5.9

$$\text{tr deg}_K K[x_1, \dots, x_d]/\text{rad}\langle F_0 \rangle = n - 1$$

con lo cual $\text{tr deg}_K \Gamma(V)/\mathfrak{p} = n - 1$, como queríamos demostrar.

Veamos que $\mathfrak{p} \cap K[x_1, \dots, x_d] = \text{rad}\langle F_0 \rangle$. Dado que f divide a F_0 en $\Gamma(V)$, entonces $F_0 \in \langle f \rangle \subset \mathfrak{p}$. Por tanto $\langle F_0 \rangle \subset \mathfrak{p} \cap K[x_1, \dots, x_d]$, lo cual implica, por ser \mathfrak{p} un ideal radical, que

$$\text{rad}\langle F_0 \rangle \subset \mathfrak{p} \cap K[x_1, \dots, x_d].$$

Sea ahora $g \in \mathfrak{p} \cap K[x_1, \dots, x_d]$. Dado que $g \in \text{rad}\langle f \rangle = \mathfrak{p}$ entonces $g^m = fh$ para ciertos $h \in \Gamma(V)$ y $m \in \mathbb{N}$. Por el corolario 1.23, tomando normas llegamos a que

$$g^{me} = \text{Nm}(fh) = F_0 \text{Nm}(h) \in \langle F_0 \rangle,$$

por lo que $g \in \text{rad}\langle F_0 \rangle$. Llegamos así a que $\text{rad}\langle f \rangle = \mathfrak{p} \cap K[x_1, \dots, x_d]$. \square

Corolario 5.13. *Sea V una variedad algebraica irreducible de K^n . Si \mathfrak{p} un ideal primo minimal de $\Gamma(V)$, $\mathfrak{p} \neq \{0\}$, entonces*

$$\text{tr deg}_K \Gamma(V)/\mathfrak{p} = \text{tr deg}_K K(V) - 1.$$

Demostración. Sea $f \in \mathfrak{p}$ no nulo. Entonces f no es una unidad, y \mathfrak{p} es un ideal primo minimal entre los ideales primos de $\Gamma(V)$ que contienen a $\langle f \rangle$. \square

Teorema 5.14. *Sea V una variedad algebraica irreducible de K^n . Se tiene*

$$\dim_{K^{\text{rull}}} \Gamma(V) = \text{tr deg}_K K(V).$$

donde $K(V)$ es el cuerpo de funciones racionales sobre V .

Demostración. Supongamos que $d = \dim_{K^{\text{rull}}} \Gamma(V)$, y sea $\mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_d$ una cadena de ideales primos de $\Gamma(V)$. Aplicando el corolario 5.13 un número finito de veces, llegamos a que

$$\text{tr deg}_K K(V) = \text{tr deg}_K \Gamma(V)/\mathfrak{p}_1 + 1 = \dots = \text{tr deg}_K \Gamma(V)/\mathfrak{p}_d + d.$$

Como \mathfrak{p}_d es maximal, $\Gamma(V)/\mathfrak{p}_d$ es un cuerpo, y por el Lema de Zariski 2.26, $\Gamma(V)/\mathfrak{p}_d$ es una extensión finita de K , por lo que lo que el grado de trascendencia de $\Gamma(V)/\mathfrak{p}_d$ sobre K es 0. Por tanto $\text{tr deg}_K(\Gamma(V)) = d$. \square

Observación 5.15. El teorema 5.12, el corolario 5.13 y el teorema 5.14 son válidos para cualquier K -álgebra finitamente generada que sea un dominio entero. En efecto, si A es una K -álgebra finitamente generada y es un dominio entero, por la definición 2.10, existen $a_1, \dots, a_n \in A$ tales que $A = K[a_1, \dots, a_n]$. El homomorfismo de anillos

$$\begin{aligned} \varphi : K[X_1, \dots, X_n] &\rightarrow K[a_1, \dots, a_n] \\ F(X_1, \dots, X_n) &\rightsquigarrow F(a_1, \dots, a_n), \end{aligned}$$

es sobreyectivo y su núcleo es un ideal primo \mathfrak{p} . La variedad algebraica $Z(\mathfrak{p})$ de K^n es irreducible y dado que $I(Z(\mathfrak{p})) = \mathfrak{p}$, la K -álgebra A es isomorfa al anillo de coordenadas de la variedad algebraica irreducible $Z(\mathfrak{p})$.

5.3. El teorema algebraico fundamental

Teorema 5.16. *Sea K un cuerpo algebraicamente cerrado, V una variedad algebraica afín irreducible, $\Gamma(V)$ su anillo de coordenadas y $K(V)$ su cuerpo de funciones racionales. Se tiene*

$$\dim V = \dim_{K^{\text{rull}}} \Gamma(V) = \text{tr deg}_K K(V)$$

En particular, la dimensión de una variedad algebraica afín es finita.

Demostración. Por ser V una variedad algebraica afín irreducible, $I(V)$ es un ideal primo y entonces $\Gamma(V)$ es un dominio, por ser isomorfo al anillo $K[X_1, \dots, X_n]/I(V)$. El resultado se sigue de la proposición 5.7 y el teorema 5.14.

Si V es una variedad algebraica afín, entonces V es una unión finita de variedades irreducibles (sus componentes irreducibles). Por la proposición 5.4, V tiene dimensión finita. \square

Corolario 5.17. *Se tiene que $\dim K^n = n$, para $n \geq 1$.*

Demostración.

$$\dim K^n = \dim_{K^{\text{rull}}} \Gamma(K^n) = \text{tr deg}_K K(X_1, \dots, X_n) = n.$$

puesto que $I(K^n) = \{0\}$. \square

Observación 5.18. Para calcular la dimensión de una variedad algebraica afín V descomponemos en unión finita de variedades algebraicas irreducibles V_i y calculamos la dimensión de cada V_i utilizando el grado de trascendencia de $\Gamma(V_i)$ sobre K .

Capítulo 6

Número de ecuaciones de una variedad algebraica afín

Siguiendo el modelo de las variedades lineales vamos a estudiar la relación entre la dimensión de una variedad algebraica afín y el número de ecuaciones que la definen. En este capítulo vamos a suponer que K es un cuerpo algebraicamente cerrado.

6.1. Dimensión de una variedad algebraica afín dadas sus ecuaciones

Proposición 6.1. *Sea $A \in K^n$ y U un subespacio de K^n y sea $L = A + U$ una variedad lineal de K^n . Si $\dim_K U = r$, entonces $\dim L = \dim_K U$.*

Demostración. Por la proposición 3.13, la variedad lineal L es homeomorfa a K^r y entonces por el corolario 5.17

$$\dim L = \dim K^r = r. \quad \square$$

Corolario 6.2. *Si $F_1, \dots, F_r \in K[X_1, \dots, X_n]$ son polinomios de grado 1 y $Z(F_1, \dots, F_r) \neq \emptyset$, entonces podemos calcular la dimensión de la variedad lineal $Z(f_1, \dots, f_r)$. Se tiene*

$$\dim Z(F_1, \dots, F_r) = n - \dim_K \langle F_1, \dots, F_r \rangle \geq n - r.$$

Sea V una variedad algebraica afín de dimensión d y sea $f \in \Gamma(V)$. Vamos a probar que la variedad $Z(f)$ tiene dimensión $d - 1$, como ocurre en el caso de las variedades lineales. Para ello, vamos a pedir a f que no sea una unidad.

Lema 6.3. *Se tiene que $Z(f) = \emptyset$ si, y sólo si, f es una unidad de $\Gamma(V)$.*

Demostración. Sea f una unidad en $\Gamma(V)$, existe entonces $g \in \Gamma(V)$ tal que $fg = 1$. Si existiera $P \in Z_V(f)$, tendríamos que $f(P)g(P) = 1$, lo cual es imposible ya que $f(P) = 0$. Por tanto, $\Gamma(V) = \emptyset$.

Sea ahora $f \in \Gamma(V)$ tal que $Z(f) = \emptyset$. Si $V = Z(\mathfrak{a})$ donde $\mathfrak{a} \in K[X_1, \dots, X_n]$ es tal que $f(P) = F(P)$, para todo $P \in V$, entonces $Z(f) = V \cap Z(F) = Z(\mathfrak{a} + \langle F \rangle)$. Por el teorema de los ceros de Hilbert (forma débil) 3.19, $Z(\mathfrak{a} + \langle F \rangle) = \emptyset$ implica que $\mathfrak{a} + \langle F \rangle = K[X_1, \dots, X_n]$ y entonces $\Gamma(V) = p_V(K[X_1, \dots, X_n]) = p_V(\mathfrak{a} + \langle F \rangle) = \langle f \rangle$. Así, f es una unidad de $\Gamma(V)$. \square

Proposición 6.4. *Sea V una variedad algebraica afín irreducible y sea U un abierto de V . Se tiene*

$$\dim V = \dim U.$$

Demostración. Sea $D(f)$ un abierto estándar contenido en U . Se tiene

$$\dim D(f) \leq \dim U \leq \dim V.$$

Dado que $D(f)$ es un abierto en un irreducible, $D(f)$ es irreducible y entonces por la proposición 3.27 y la proposición 2.8,

$$\begin{aligned} \dim D(f) &= \dim Z(I(V) + \langle X_{n+1}F - 1 \rangle) = \dim_{\text{Krull}} \Gamma(Z(I(V) + \langle X_{n+1}F - 1 \rangle)) \\ &= \dim_{\text{Krull}} \Gamma(V)_f = \text{tr deg}_K \Gamma(V)_f = \text{tr deg}_K \Gamma(V) = \dim V, \end{aligned}$$

por tener $\Gamma(V)_f$ y $\Gamma(V)$ el mismo cuerpo de fracciones. Por tanto

$$\dim D(f) = \dim U = \dim V. \quad \square$$

Definición 6.5. Una variedad algebraica afín se dice que es equidimensional si todas sus componentes irreducibles tienen la misma dimensión.

Claramente si V es irreducible, entonces V es equidimensional; por ejemplo K^n es equidimensional.

Teorema 6.6. *Sea V una variedad algebraica afín irreducible de dimensión n y sea f un elemento de $\Gamma(V)$, $f \neq 0$ y que no es una unidad. Entonces $Z(f)$ es una variedad algebraica afín equidimensional de dimensión $n - 1$.*

Demostración. En el caso $V = K^n$, si F es un polinomio de grado mayor que cero, para probar que $\dim Z(F) = n - 1$, podemos suponer, por el ejemplo 3.23 y la proposición 5.4, que F es irreducible. Por el teorema 5.16 y el lema 5.9 se tiene

$$\dim Z(F) = \text{tr deg}_K(K[X_1, \dots, X_n]/\langle F \rangle) = n - 1.$$

Veamos ahora el caso general. Supongamos ahora que V es una variedad algebraica afín irreducible de K^m , $f \in \Gamma(V)$ y $F \in K[X_1, \dots, X_m]$ es tal que $f(P) = F(P)$, para cada $P \in V$, y que

$$Z(f) = Z_1 \cup \dots \cup Z_s.$$

donde los Z_i son las componentes irreducibles de $Z(f)$. Vamos a probar que todas las Z_i tiene dimensión $n - 1$. Dado que $Z_j \not\subset \bigcup_{i \neq j} Z_i$, existe $P \in Z_j$ tal que $P \notin \bigcup_{i \neq j} Z_i$. Sea $D(g)$ un abierto estándar de V tal que $P \in D(g) \subset V - \bigcap_{i \neq j} Z_i$ y sea $G \in K[X_1, \dots, X_m]$ es tal que $g(P) = G(P)$ para todo $P \in V$. Se tiene

$$D(g) \cap Z(f) = \bigcup_{i=1}^s (D(g) \cap Z_i) = D(g) \cap Z_j.$$

y $D(g) \cap Z_j \neq \emptyset$ es un cerrado irreducible de $D(g)$. Sea

$$\varphi: D(g) \longrightarrow Z(I(V) + \langle X_{n+1}G - 1 \rangle)$$

el homeomorfismo de la proposición 3.27. Pongamos $W = Z(I(V) + \langle X_{n+1}G - 1 \rangle)$. Se tiene

$$\varphi(D(g) \cap Z(f)) = \{(x_1, \dots, x_{m+1}) \in W \mid F(x_1, \dots, x_m) = 0\} = V(F) \cap W = Z(f'),$$

siendo $f' \in \Gamma(W)$, tal que $f'(x_1, \dots, x_m, x_{m+1}) = F(x_1, \dots, x_m)$, para $(x_1, \dots, x_{m+1}) \in W$. Por la proposición 6.4,

$$\dim Z_j = \dim(D(g) \cap Z_j) = \dim(D(g) \cap Z(f)) = \dim Z(f')$$

y $Z(f')$ es irreducible, puesto que $D(g) \cap Z_j$ es irreducible, por la proposición 3.16 (b). Por la proposición 3.24, $I_W(Z(f'))$ es un ideal primo. Dado que $I_W(Z(f')) = \text{rad} \langle f' \rangle$, el ideal $I_W(Z(f'))$ es primo minimal entre los que contienen a f' . Aplicando el teorema 5.12 se tiene

$$\dim_{\text{Krull}} \Gamma(W)/I_W(Z(f')) = \dim_{\text{Krull}} \Gamma(W) - 1.$$

y dado que $\Gamma(W)/I_W(Z(f'))$ es un anillo isomorfo a $\Gamma(Z(f'))$, se tiene

$$\dim Z(f') = \dim_{\text{Krull}} \Gamma(Z(f')) = \dim_{\text{Krull}} \Gamma(W) - 1.$$

Por la proposición 2.8, los anillos $\Gamma(W)$ y $\Gamma(V)_g$ son isomorfos. Así,

$$\begin{aligned} \dim Z_j &= \dim Z(f') = \dim_{\text{Krull}} \Gamma(W) - 1 = \dim_{\text{Krull}} \Gamma(V)_g - 1 \\ &= \text{tr deg}_K \Gamma(V)_g - 1 = \text{tr deg}_K \Gamma(V) - 1 = \dim V - 1. \end{aligned}$$

puesto que $\Gamma(V)$ y $\Gamma(V)_g$ tienen el mismo cuerpo de fracciones por ser V irreducible. \square

Teorema 6.7. *Sea V una variedad algebraica afín irreducible de dimensión n y sean $f_1, \dots, f_r \in \Gamma(V)$. Si W es una componente irreducible de $Z(f_1, \dots, f_r)$, entonces $\dim W \geq n - r$.*

Demostración. Lo probaremos por inducción en r . Para $r = 1$, por el lema 6.3, f_1 no puede ser una unidad, ya que $W \subset Z(f_1)$ es irreducible y por tanto no vacío. Si $f_1 = 0$, entonces $Z(f_1) = V$, con lo cual $W = V$ y $\dim W = n \geq n - 1$.

Si $f_1 \neq 0$, por el teorema 6.6, $Z(f_1)$ es una variedad algebraica afín equidimensional de dimensión $n - 1$, y por la proposición 5.4, $\dim W = n - 1$.

Supongamos el resultado cierto para $r - 1 \geq 1$. Si $f_i = 0$, para $i = 1, \dots, r$, entonces $W = V$ y el resultado es claramente cierto. Supongamos que para algún $j \in \{1, \dots, r\}$, $f_j \neq 0$ y que $j = 1$. Dado que $W \subset Z(f_1, \dots, f_r) \subset Z(f_1) = Z_1 \cup \dots \cup Z_t$, donde Z_1, \dots, Z_t son las componentes irreducibles de $Z(f_1)$ y que W es irreducible, existe $i \in \{1, \dots, t\}$ tal que $W \subset Z_i$ y entonces por el teorema 6.6, $\dim Z_i = n - 1$. Se tiene

$$Z(f_1, \dots, f_r) \cap Z_i = Z(f_2, \dots, f_r) \cap Z_i = Z(\overline{f_2}, \dots, \overline{f_r}), \quad \overline{f_2}, \dots, \overline{f_r} \in \Gamma(Z_i).$$

donde $\overline{f_k}(P) = f_k(P)$, para $k = 2, \dots, r$. Dado que $W \subset Z(\overline{f_2}, \dots, \overline{f_r})$ y que W es también componente irreducible de $Z(\overline{f_2}, \dots, \overline{f_r})$, por hipótesis de inducción

$$\dim W \geq (n - 1) - (r - 1) = n - r. \quad \square$$

Observación 6.8. Las componentes irreducibles de $Z(f_1, \dots, f_r)$ no tienen porque tener todas la misma dimensión. Por ejemplo, si $V = \mathbb{C}^3$, $F = X^4 - X^3 + XZ - Z$ y $G = X^3Y^2 + X^3Z^2 + Y^2Z + Z^3$, entonces se tiene

$$\begin{aligned} Z(F, G) &= Z(X^3 + Z) \cup (Z(X - 1) \cap Z(Y^2 + Z^2)) \\ &= Z(X^3 + Z) \cup \{(1, y, iy) \mid y \in \mathbb{C}\} \cup \{(1, y, -iy) \mid y \in \mathbb{C}\} \end{aligned}$$

que es la descomposición de $Z(F, G)$ en sus componentes irreducibles: una superficie y dos rectas.

Corolario 6.9. *Si V es una variedad algebraica afín irreducible de dimensión n , f_1, \dots, f_r son elementos de $\Gamma(V)$ y $Z(f_1, \dots, f_r) \neq \emptyset$, entonces $\dim Z(f_1, \dots, f_r) \geq n - r$.*

Demostración. Se sigue de 5.4. □

Corolario 6.10. *Sea V una variedad algebraica afín irreducible de dimensión n y W es una subvariedad algebraica de V . Si $\delta(W)$ es el mínimo de las dimensiones de las componentes irreducibles de W , entonces el número mínimo de ecuaciones en $\Gamma(V)$ necesario para describir W como subvariedad de V es $\geq n - \delta(W)$*

Demostración. Trivial. □

Observación 6.11. Si $F_1, \dots, F_r \in K[X_1, \dots, X_n]$ son polinomios de grado 1 y $Z(F_1, \dots, F_r) \neq \emptyset$, entonces

$$\dim Z(F_1, \dots, F_r) = n - \dim_K \langle F_1, \dots, F_r \rangle \geq n - r.$$

Si $r > \dim \langle F_1, \dots, F_r \rangle$, podemos tomar un subconjunto S de $\{F_1, \dots, F_r\}$ y $Z(F_1, \dots, F_r) = Z(S)$.

En el ejemplo de la observación 6.8, $\dim Z(F, G) = 2 > 3 - 2 = 1$, pero no podemos suprimir ninguno de los dos polinomios. En efecto, $\dim Z(F) = \dim Z(G) = \dim Z(F, G) = 2$, pero sin embargo,

$$\begin{aligned} Z(F, G) \subsetneq Z(F) &= Z(X - 1) \cup Z(X^3 + Z) \\ Z(F, G) \subsetneq Z(G) &= Z(Y^2 + Z^2) \cup Z(X^3 + Z) \end{aligned}$$

6.2. Sistemas de parámetros de una variedad algebraica afín

Hemos probado que si en una variedad afín de dimensión n tomamos r ecuaciones algebraicas, entonces se obtiene una variedad de dimensión $\geq n - r$ y en casos buenos igual a $n - r$; recíprocamente, podemos preguntarnos si toda subvariedad de dimensión $n - r$ puede estar definida por r ecuaciones. Si V es una variedad lineal y W es una subvariedad lineal de V de dimensión $n - r$, sabemos por álgebra lineal que W está definida por r ecuaciones lineales; en general, esto es demasiado exigir pero vamos a dar algunos resultados parciales. En el caso $r = 1$ vamos a obtener el recíproco de la proposición 6.6, pero vamos a pedir que el anillo de coordenadas de la variedad irreducible V sea factorial.

Teorema 6.12. *Sea V una variedad algebraica afín irreducible de dimensión n tal que el anillo $\Gamma(V)$ sea factorial. Sea W un cerrado irreducible de V de dimensión $n - 1$. Existe $f \in \Gamma(V)$ tal que $W = Z(f)$.*

Demostración. Por la biyección dada en la proposición 3.24, $I_V(W)$ es un ideal primo que es minimal entre los ideales primos no nulos de $\Gamma(V)$. Veamos que es un ideal principal. Sea $g \in I_V(W)$, $g \neq 0$, con $g = f_1 \dots f_r$, siendo cada f_i irreducible. Como $I_V(W)$ es primo, $f_i \in I_V(W)$ para algún $i \in \{1, \dots, r\}$. Se tiene

$$0 \subsetneq \langle f_i \rangle \subset I_V(W)$$

Por ser $\Gamma(V)$ factorial, $\langle f_i \rangle$ es un ideal primo no nulo, y por la minimalidad de $I_V(W)$, $\langle f_i \rangle = I_V(W)$. Por tanto, $W = Z_V(I_V(W)) = Z(f_i)$.

□

En el caso general nos tenemos que contentar con el siguiente resultado:

Proposición 6.13. *Sea V una variedad algebraica afín irreducible de dimensión n y sea W una subvariedad de algebraica afín irreducible de dimensión $n - r \geq 1$. Para todo s , $1 \leq s \leq r$, existen $f_1, \dots, f_s \in \Gamma(V)$ tales que*

$$(1) \quad W \subset Z(f_1, \dots, f_s).$$

(2) *Todas las componentes irreducibles de $Z(f_1, \dots, f_s)$ son de dimensión $n - s$.*

Demostración. Lo probaremos por inducción en s . Para $s = 1$, sea $f \in I_V(W)$, $f \neq 0$. Se tiene que $\langle f \rangle \subset I_V(W)$ y entonces $Z(I_V(W)) = W \subset Z(f)$. El resultado se sigue del teorema 6.6.

Supongamos el resultado cierto para $s-1 < r$, es decir, existen $f_1, \dots, f_{s-1} \in \Gamma(V)$ tales que $W \subset Z_V(f_1, \dots, f_{s-1})$ y tales que todas las componentes irreducibles de $Z(f_1, \dots, f_{s-1})$ son de dimensión $n - (s-1)$. Sean Y_1, \dots, Y_m , las componentes irreducibles de $Z(f_1, \dots, f_{s-1})$. Dado que $s - 1 < r$, $i \not\subset W$, para todo $i \in \{1, \dots, m\}$ y entonces $I_V(W) \not\subset I_V(Z_i)$, para todo $i \in \{1, \dots, m\}$. Por tanto,

$$I_V(W) \not\subset \bigcup_{i=1}^m I_V(Y_i)$$

y entonces existe $\bar{f}_s \in I_V(W)$ tal que $\bar{f}_s \notin I_V(Y_i)$, $i = 1, \dots, m$. Se tiene que $W = Z(I_V(W)) \subset Z(\bar{f}_s)$. Si $F_s \in K[X_1, \dots, X_n]$ es tal que $\bar{f}_s(P) = F_s(P)$, para todo $P \in W$ y $f_s \in \Gamma(V)$ es tal que $f_s(P) = F_s(P)$, para cada $P \in V$, entonces $W \subset Z(f_1, \dots, f_s)$.

Sea Z una componente irreducible de $Z_V(f_1, \dots, f_s)$. Por el teorema 6.7, $\dim Z \geq n - s$. Se tiene

$$Z \subset Z(f_1, \dots, f_s) \subset Z(f_1, \dots, f_{s-1}) = \bigcup_{i=1}^m Y_i,$$

y entonces existe $j \in \{1, \dots, m\}$ tal que $Z \subset Y_j$. Además $Z \neq Y_j$, puesto que si $Z = Y_j$, $I_V(Z) = I_V(Y_j)$ y $f_s \notin I_V(Y_j)$ pero $f_s \in I_V(Z)$. Dado que Z es un cerrado de V y Y_j es un cerrado irreducible de V y $Z \subsetneq Y_j$, por la proposición 5.3 (2), $\dim Z < \dim Y_j$. Así,

$$n - s \leq \dim Z < \dim Y_j = n - s + 1$$

de donde se sigue que la dimensión de Z es $n - s$. □

Definición 6.14. *Sea V una variedad algebraica afín irreducible de dimensión n y sea W una subvariedad algebraica afín irreducible de V de dimensión $n - r \geq 1$. Si existen $f_1, \dots, f_r \in \Gamma(V)$ tales que W sea una componente irreducible de $Z(f_1, \dots, f_r)$, entonces se dice que los elementos f_i forman un sistema de parámetros de W .*

Corolario 6.15. *Sea V una variedad algebraica afín irreducible y sea W una subvariedad de algebraica afín irreducible de dimensión $n - r \geq 1$. Existe un sistema de parámetros de W .*

Demostración. Por la proposición anterior, dado que $\dim W \geq n - r$, existen $f_1, \dots, f_r \in \Gamma(V)$ tales que $W \subset Z_p(f_1, \dots, f_r)$ y si Z_1, \dots, Z_s son las componentes irreducibles de $Z(f_1, \dots, f_r)$ entonces $\dim Z_i = n - r$, para $i = 1, \dots, s$. Se tiene

$$W \subset Z_p(f_1, \dots, f_r) = Z_1 \cup \dots \cup Z_s$$

y por ser W irreducible, existe $i \in \{1, \dots, s\}$ tal que $W \subset Z_i$. Dado que $\dim W = \dim Z_i$ y W y Z_i son cerrados irreducibles, se tiene que $W = Z_i$. \square

Capítulo 7

Número de ecuaciones de una variedad algebraica proyectiva

En este capítulo vamos a probar para variedades algebraicas proyectivas resultados similares a los estudiados para variedades algebraicas afines; para esto utilizaremos los conceptos de abierto afín y de cono de una variedad algebraica proyectiva. En el caso de una variedad algebraica proyectiva irreducible probaremos además que si el número de ecuaciones es menor o igual que la dimensión de la variedad, entonces la variedad es no vacía. Lo mismo que ocurre en el espacio afín, una variedad algebraica proyectiva tiene dimensión cero, si y sólo si, es finita. El cuerpo K es un cuerpo algebraicamente cerrado.

Proposición 7.1. *Sea V una variedad algebraica proyectiva irreducible y sea U un abierto afín no vacío de V . Se tiene*

$$\dim V = \dim U.$$

Demostración. Si V es una variedad algebraica afín, este resultado se probó en la proposición 6.4. Veamos que si V es una variedad algebraica proyectiva todos los abiertos afines no vacíos de V (que son irreducibles por la proposición 3.16) tienen la misma dimensión. Sean U_1 y U_2 abiertos afines de V y sean $\varphi_1: U_1 \rightarrow V_1$ y $\varphi_2: U_2 \rightarrow V_2$ homeomorfismos, donde V_1 y V_2 son variedades algebraicas afines irreducibles. Por ser V irreducible, el abierto $U_1 \cap U_2 \neq \emptyset$ y se tiene

$$\dim(U_1 \cap U_2) = \dim \varphi_1(U_1 \cap U_2) = \dim V_1 = \dim U_1,$$

por ser $\varphi_1(U_1 \cap U_2)$ un abierto afín no vacío de V_1 y

$$\dim(U_1 \cap U_2) = \dim \varphi_2(U_1 \cap U_2) = \dim V_2 = \dim U_2,$$

por ser $\varphi_2(U_1 \cap U_2)$ un abierto no vacío de V_2 . Así, todos los abiertos afines de V tienen la misma dimensión que vamos a denotar por r .

Veamos que r es la dimensión de V . Supongamos que $\dim V = n > r$. Sea

$$Z_0 \subsetneq Z_1 \subsetneq \dots \subsetneq Z_n,$$

una cadena de cerrados irreducibles de V y $\bar{x} \in Z_0$. Existe $D^+(X_i)$ tal que $\bar{x} \in D^+(X_i)$. Por la proposición 3.16 se tiene la cadena de cerrados irreducibles de $D^+(X_i)$

$$Z_0 \cap D^+(X_i) \subsetneq Z_1 \cap D^+(X_i) \subsetneq \dots \subsetneq Z_n \cap D^+(X_i),$$

de longitud n , lo que contradice que $r < n$. □

Observación 7.2. Si V es una variedad algebraica proyectiva y U es un abierto de V , entonces $\dim U = \dim V$. En efecto, por la proposición 4.20, existe $f \in \Gamma_h(V)$ tal que $D^+(f) \subset U$. Dado que $D^+(f)$ es un abierto afín de V (observación 4.29), $\dim D^+(f) = \dim V$ y entonces $\dim U = \dim V$.

Corolario 7.3. *Se tiene:*

- (1) $\dim \mathbb{P}^n(K) = n$.
- (2) *Sea $L = Z_p(G_1, \dots, G_m)$ una variedad lineal proyectiva no vacía de $\mathbb{P}^n(K)$. Se tiene que $\dim L = n - \dim_K \langle G_1, \dots, G_m \rangle$.*

Demostración. (1) Por $\mathbb{P}^n(K)$ irreducible y $D^+(X_0)$ un abierto afín de $\mathbb{P}^n(K)$, por la proposición anterior $\dim D^+(X_0) = \dim \mathbb{P}^n(K)$. Dado que $D^+(X_0)$ y K^n son espacios topológicos homeomorfos (corolario 4.26), $\dim D^+(X_0) = \dim K^n = n$.

(2) Por la observación 4.14, L es homeomorfa a $\mathbb{P}^{s-1}(K)$, donde $s = n+1 - \dim_K \langle G_1, \dots, G_m \rangle$. Por tanto, $\dim L = s - 1 = n - \dim_K \langle G_1, \dots, G_m \rangle$. □

Teorema 7.4. *Sea V una variedad algebraica proyectiva irreducible de $\mathbb{P}^n(K)$ y f un elemento homogéneo no constante de $\Gamma_h(V)$. Se tiene*

- (1) *La dimensión de las componentes irreducibles de $Z_p(f)$ es $\dim V - 1$.*
- (2) *Si $\dim V > 0$ entonces $Z_p(f) \neq \emptyset$.*
- (3) *Si $\dim V > 0$ se tiene que $\dim Z_p(f) = \dim V - 1$.*

Demostración. Sea $f = F + I_p(V)$, donde $F \in K[X_0, \dots, X_n]$ es un polinomio homogéneo no constante.

(1) Si $Z_p(f)$ tiene componentes irreducibles entonces $Z_p(f) \neq \emptyset$ y existe $i \in \{0, \dots, n\}$ tal que $Z_p(f) \not\subset Z_p(X_i)$. Supongamos que $Z_p(f) \not\subset Z_p(X_0)$. Sean Z_1, \dots, Z_m las componentes irreducibles de $Z_p(f)$ y supongamos que Z_1, \dots, Z_s son las componentes irreducibles de $Z_p(f)$ tales que $Z_i \not\subset Z_p(X_0)$, para $i = 1, \dots, s$, $s \leq m$. Se tiene que $Z_i \cap D^+(X_0) \neq \emptyset$, para $i = 1, \dots, s$.

Por el corolario 4.26, $j_0^{-1}(V \cap D^+(X_0))$ es una variedad algebraica afín irreducible de K^n y $j_0^{-1}(Z_p(f) \cap D^+(X_0)) = Z(f^b)$, donde la función polinómica $f^b \in \Gamma(j_0^{-1}(V \cap D^+(X_0)))$ está dada por $f^b(P) = F^b(P)$, para todo $P \in j_0^{-1}(V \cap D^+(X_0))$ y con $F \in K[X_1, \dots, X_n]$. Dado que $Z_p(f) \not\subset Z_p(X_0)$, $Z_p(f^b) \neq \emptyset$. La función f^b no es una unidad, puesto que si lo es entonces $Z(f^b) = \emptyset$. Además, $f^b \neq 0$, puesto que si $f^b = 0$, entonces

$$j_0^{-1}(Z_p(f) \cap D^+(X_0)) = Z(f^b) = j_0^{-1}(V \cap D^+(X_0)),$$

de donde se sigue que $V \cap D^+(X_0) \subset Z_p(f)$. Dado que $V \cap D^+(X_0)$ es un abierto de V y V es irreducible, $V \cap D^+(X_0)$ es denso en V . Así, $V = \overline{V \cap D^+(X_0)} \subset Z_p(f)$ y $f = 0$, lo cual es una contradicción.

Se tiene,

$$Z(f^b) = \bigcup_{i=1}^s j_0^{-1}(Z_i \cap D^+(X_0)),$$

donde por la proposición 3.16, $Z_i \cap D^+(X_0)$, $i = 1, \dots, s$ son las componentes irreducibles de $Z(f^b)$. Por el teorema 6.6, $Z(f^b)$ es una variedad algebraica afín equidimensional de dimensión

$$\dim Z(f^b) = \dim(V \cap D^+(X_0)) - 1.$$

Dado que $V \cap D^+(X_0)$ es un abierto afín de V , $\dim(V \cap D^+(X_0)) = \dim V$. Por tanto,

$$\dim Z(f^b) = \dim V - 1.$$

Por el teorema 6.6,

$$\dim j_0^{-1}(Z_i \cap D^+(X_0)) = \dim V - 1, \quad i = 1, \dots, s.$$

Dado que $Z_i \cap D^+(X_0)$ es un abierto afín de Z_i ,

$$\dim(Z_i \cap D^+(X_0)) = \dim Z_i$$

Así, todas las componentes irreducibles de $Z_p(f)$ no contenidas en $Z_p(X_0)$ tienen la misma dimensión igual a $\dim V - 1$.

De forma análoga se razona para las restantes componentes, puesto que para todo $k \in \{1, \dots, r\}$, existe $j \in \{0, \dots, n\}$, tal que $D^+(X_j) \cap Z_k \neq \emptyset$.

(2) Sea $V = Z_p(I)$, siendo I un ideal homogéneo distinto de $K[X_0, \dots, X_n]$ y de $\langle X_0, \dots, X_n \rangle$. Se tiene que $I_p(V) = I(C(V))$ y entonces

$$\Gamma_h(V) = K[X_0, \dots, X_n]/I_p(V) = K[X_0, \dots, X_n]/I(C(V)) \simeq \Gamma(C(V)).$$

Dado que V es una variedad irreducible, $I_p(V)$ es un ideal primo y entonces $\Gamma_h(V)$ es un dominio con lo cual $C(V) = Z(I)$ es una variedad afín irreducible.

Denotemos también por f el elemento de $\Gamma(C(V))$ tal que $f(P) = F(P)$, para todo $P \in C(V)$. Se tiene que $(0, \dots, 0) \in Z(f)$, con lo cual $Z(f) \neq \emptyset$. Por la proposición 6.3, f no es una unidad de $\Gamma(C(V))$. Por el teorema 6.6

$$\dim Z(f) = \dim C(V) - 1.$$

Veamos que $\dim V > 0$ implica que $\dim C(V) > 1$. En efecto, supongamos que $\dim V = d > 0$ y consideremos la cadena de cerrados irreducibles de V

$$Z_0 \subsetneq Z_1 \subsetneq \dots \subsetneq Z_d = V,$$

Se tiene la siguiente cadena de cerrados irreducibles de $C(V)$

$$\{(0, \dots, 0)\} \subsetneq C(Z_0) \subsetneq C(Z_1) \subsetneq \dots \subsetneq C(Z_d) = C(V)$$

y entonces $\dim C(V) \geq d + 1$. Por tanto

$$\dim Z(f) = \dim C(V) - 1 > 1 - 1 = 0.$$

Así, $Z(f) \neq \{(0, \dots, 0)\}$ y entonces $Z_p(f) \neq \emptyset$.

(3) Se sigue de (1) y (2). □

Proposición 7.5. *Sea V una variedad algebraica proyectiva irreducible de $\mathbb{P}^n(K)$ y sean $f_1, \dots, f_r \in \Gamma_h(V)$ elementos homogéneos no constantes. Se tiene*

- (1) *La dimensión de las componentes irreducibles de $Z_p(f_1, \dots, f_r)$ es $\geq \dim V - r$.*
- (2) *Si $r \leq \dim V$, entonces $Z_p(f_1, \dots, f_r) \neq \emptyset$.*
- (3) *Si $r \leq \dim V$, entonces $\dim Z_p(f_1, \dots, f_r) \geq \dim V - r$.*

Demostración. (1) Lo probaremos por inducción en r . El caso $r = 1$ es el teorema 7.4 (1). Supongámoslo cierto para $r - 1 \geq 1$. Sea W una componente irreducible de $Z_p(f_1, \dots, f_r)$. Tenemos que $W \subset Z_p(f_1, \dots, f_r) \subset Z_p(f_1) = Z_1 \cup \dots \cup Z_t$, siendo Z_1, \dots, Z_t las componentes irreducibles de $Z_p(f_1)$. Por ser W irreducible, $W \subset Z_i$ para algún i . Por el teorema 7.4 (1), $\dim Z_i = \dim V - 1$. Ahora, $Z_p(f_1, \dots, f_r) \cap Z_i = Z_p(f_2, \dots, f_r) \cap Z_i = Z_p(\overline{f_2}, \dots, \overline{f_r})$,

con $\overline{f_i} \in \Gamma_h(Z_i)$, $\overline{f_i}(P) = f_i(P)$, $i = 2, \dots, r$. Entonces, $W \subset Z_p(\overline{f_2}, \dots, \overline{f_r})$, y W es una componente irreducible de $Z_p(\overline{f_2}, \dots, \overline{f_r})$. Como $\overline{f_2}, \dots, \overline{f_r}$ son homogéneos y no constantes, por hipótesis de inducción, $\dim W \geq (\dim V - 1) - (r - 1) = \dim V - r$.

(2) Por un razonamiento similar al realizado en la demostración del teorema 7.4 (2), tenemos que $(0, \dots, 0) \in Z(f_1, \dots, f_r)$. Por el teorema 6.9, $\dim Z(f_1, \dots, f_r) \geq \dim C(V) - r$. Como $\dim C(V) \geq \dim V + 1$, $\dim Z(f_1, \dots, f_r) \geq \dim C(V) - r > n - r \geq 0$, por lo que $Z(f_1, \dots, f_r) \neq \{(0, \dots, 0)\}$, y entonces $Z_p(f_1, \dots, f_r) \neq \emptyset$.

(3) Se sigue de (1) y (2) aplicando el teorema 5.4. □

Corolario 7.6. *Sea V una variedad algebraica proyectiva irreducible de dimensión n y W es una subvariedad algebraica de V . Si $\delta(W)$ es el mínimo de las dimensiones de las componentes irreducibles de W , entonces el número mínimo de ecuaciones homogéneas de $\Gamma_h(V)$ necesario para describir W es $\geq \dim V - \delta(W)$*

Recíprocamente, se tiene

Proposición 7.7. *Sea V una variedad algebraica proyectiva irreducible y sea W una subvariedad algebraica proyectiva irreducible de dimensión $\dim V - r$. Existen elementos homogéneos $f_1, \dots, f_r \in \Gamma_h(V)$ tales que W es una componente irreducible de $Z_p(f_1, \dots, f_r)$ y la dimensión de las componentes irreducibles de $Z_p(f_1, \dots, f_r)$ es $\dim V - r$.*

Demostración. Se razona como en la demostración de la proposición 6.13 y del corolario 6.15. □

Se dice que f_1, \dots, f_r forman un sistema de parámetros homogéneos de W

Bibliografía

- [1] Atiyah M. F. and Macdonald I. G., *Introduction to commutative algebra*, Addison-Wesley, 1999.
- [2] Fulton W., *Curvas algebraicas*, Reverté, 1971.
- [3] Kunz, E., *Introduction to Commutative Algebra and Algebraic Geometry*, Birkhäuser/Springer, New York, 2015.
- [4] Lang, S., *Algebra*, Aguilar, Madrid, 1971.
- [5] Milne J.S., *A Primer of Commutative Algebra*, Expository Notes, Disponible en www.jmilne.org/math/, 2020.
- [6] Milne J.S., *Fields and Galois Theory*, Course Notes, Disponible en www.jmilne.org/math/, 2020.
- [7] Milne J.S., *Algebraic Geometry*, Course Notes, Disponible en www.jmilne.org/math/, 2017.
- [8] Perrin D., *Géométrie algébrique, Une introduction*, CNRS, Paris, 1995.